LayerX Labs

ブロックチェーンのBeyond PoCとトラスト

中村 龍矢（株式会社LayerX）

2021/10/28 BWS2021

LayerX Inc.

自己紹介: 中村 龍矢

- **現在: 株式会社LayerX 執行役員 兼 LayerX Labs 所長**
  - プライバシーテック分野のプロダクト開発
- ブロックチェーン関連の学術研究
  - 主なテーマ: 形式検証、コンセンサスアルゴリズム、シャーディング
  - 東京工業大学との共同研究: 2020年度インターネットアーキテクチャ研究賞(最優秀賞)
  - 2020年度 IPA未踏スーパークリエータ認定
- Ethereumコミュニティでの活動
  - Ethereum 2.0 の仕様策定への貢献
  - Ethereum Foundationのグラント獲得 (日本拠点のチームで初)
- 略歴
  - 株式会社Gunosy データ分析部
  - 東京大学 工学部システム創成学科 (在学中。。。)

DEVCON V
(@大阪, 2019)

アジェンダ

- 背景
  - LayerXとブロックチェーン
  - Anonifyの紹介
- インターネット投票プロジェクトの経験
- 「検証可能性」の技術とBeyond PoC
- 「検証可能性」デモ

LayerXとブロックチェーン

LayerX、LayerX Labsの紹介

- LayerXは3つの事業部からなるスタートアップ
- LayerX Labs: R&Dにより培った技術を活かしたプロダクト開発を行う事業部
  - Anonifyをはじめとするプライバシーテック関連に注力

LayerX

広く

DX(SaaS)事業

自社プロダクト(SaaS)を提供

請求書AIクラウド
LayerX インボイス

LayerX ワークフロー

深く

共同事業

三井物産らとAM合弁会社

MITSUI & CO.
DIGITAL ASSET MANAGEMENT

出資・出向

MITSUI&CO. / LayerX / SMBC日興証券 / 三井住友信託銀行 / JA三井リース

遠く

LayerX Labs

プライバシー保護
/秘匿化技術

Anonify

取り組み実績: プライバシー・秘匿化分野

- 技術のR&Dに止まらず、その業界・分野を理解した上で顧客・ユーザー価値につなげるところまで伴走

協業事例

- 次世代金融におけるプライバシー・秘匿化技術の共同研究
- 秘匿性を担保した複数企業間の取引記録インフラの事業検討・技術検証
- コンセプトペーパーの発表

つくば市

- 市民向けアンケートシステムの回答の匿名性・プライバシーの担保
- 内閣府「スーパーシティ」制度に基づく公職選挙法の規制緩和の提案
- 県立高校におけるネット投票に関する出張授業

非公開（数社）

- プライバシーを担保したデータ分析、利活用の実現に向けた共同研究

メディア掲載（抜粋）

日本経済新聞

NHK

TechCrunch

NIKKEI Financial

NIKKEI BUSINESS DAILY 日経産業新聞

EnterpriseZine

LayerXとブロックチェーン

- 創業から2年はブロックチェーン関連が主力事業
- 徐々に金融分野を中心とした「重たい産業のDX」の文脈での活用可能性にフォーカス
  - いわゆるエンタープライズブロックチェーン
- しかしながら、そもそもブロックチェーン以前の課題の方が重要と気づく
  - そこを解決する自社プロダクト & 共同事業として残る

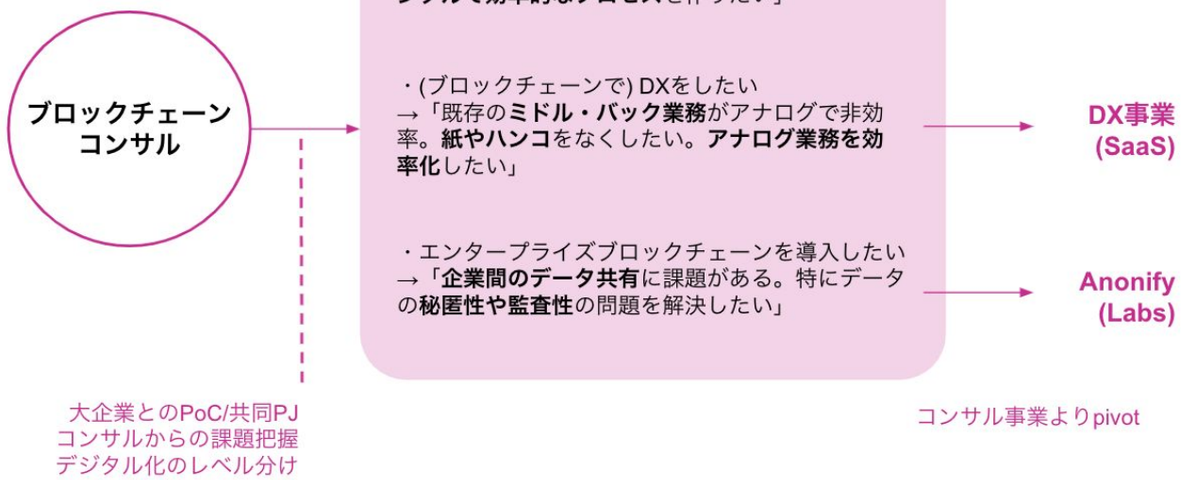
LayerXはブロックチェーンの会社じゃありません、という話

♡ 708

福島良典 | LayerX
2021年8月18日 09:45 フォローする

https://note.com/fukkyy/n/n7f60e18db2c6

ブロックチェーンコンサルから、現在の3事業へ



本日の話の背景: ブロックチェーンのBeyond PoCの難しさに向き合ってきた体験

FAQ: 結局エンタープライズBCは何が便利なのか

- 自分自身は当初R&Dチームとして、Ethereumコントリビューションをしていた
  - 正直なところ、エンタープライズ/プライベート/コンソーシアムBCには懐疑的であった

- 徐々に案件に関わりながら、エンタープライズBCの価値はなんなのか考え始めた
  - 社内では「なぜブロ問題」と呼ばれていた

FAQ: 結局エンタープライズBCは何が便利なのか

- **当時の結論: 監査性・改竄耐性が求められるシステム開発における便利ミドルウェア**
  - **に、将来なるかもしれない（ならないかもしれない）アーキテクチャの総称**

- 多くの人が悩んでいるやつ:「BCじゃなきゃできないことは何か」
  - 多分あんまりない（残念）
- 個人的なアナロジー: 業務ツールとしてのExcel, 調味料としての醤油
  - 個別のユースケースでの優位性は少ないが、使い方を覚えると汎用性が高い
- エンプラBCが世の中で流行る可能性のあるシナリオ
  - 監査性・改竄耐性・レプリケーションの必要なシステム開発のニーズが増える
  - 台帳部分のカスタマイズ性をスマートコントラクトが担保
    - それ以外の部分は、標準化・セキュリティ監査されたものを使いまわせる
    - コントラクト言語の設計の工夫により、個別開発の負担を低減

※2021年10月現在、今のところこの予想は当たっていない！笑

- シンプルに、上記特性が必要なシステム開発のニーズが世の中で増えていないため
  - 決済・証券・サプライチェーンシステムはそう沢山作るものではない
- 一方、パブリッククラウドはエンプラBC系に絞った台帳DBを再発明 (e.g., AWS QLDB)

Anonify

Anonify

- LayerX Labsで開発した、ブロックチェーンにおけるプライバシー・秘匿性担保のプロダクト
- SCIS2020にて論文を発表

Anonify: プライバシーを保護した検証可能な状態遷移モジュール
Anonify: A Module for Privacy-preserving State Transitions with Verifiability

須藤 欧佑 * 恩田 壮恭 * 中村 龍矢 * †
Osuke Sudo Masanori Onda Ryuya Nakamura

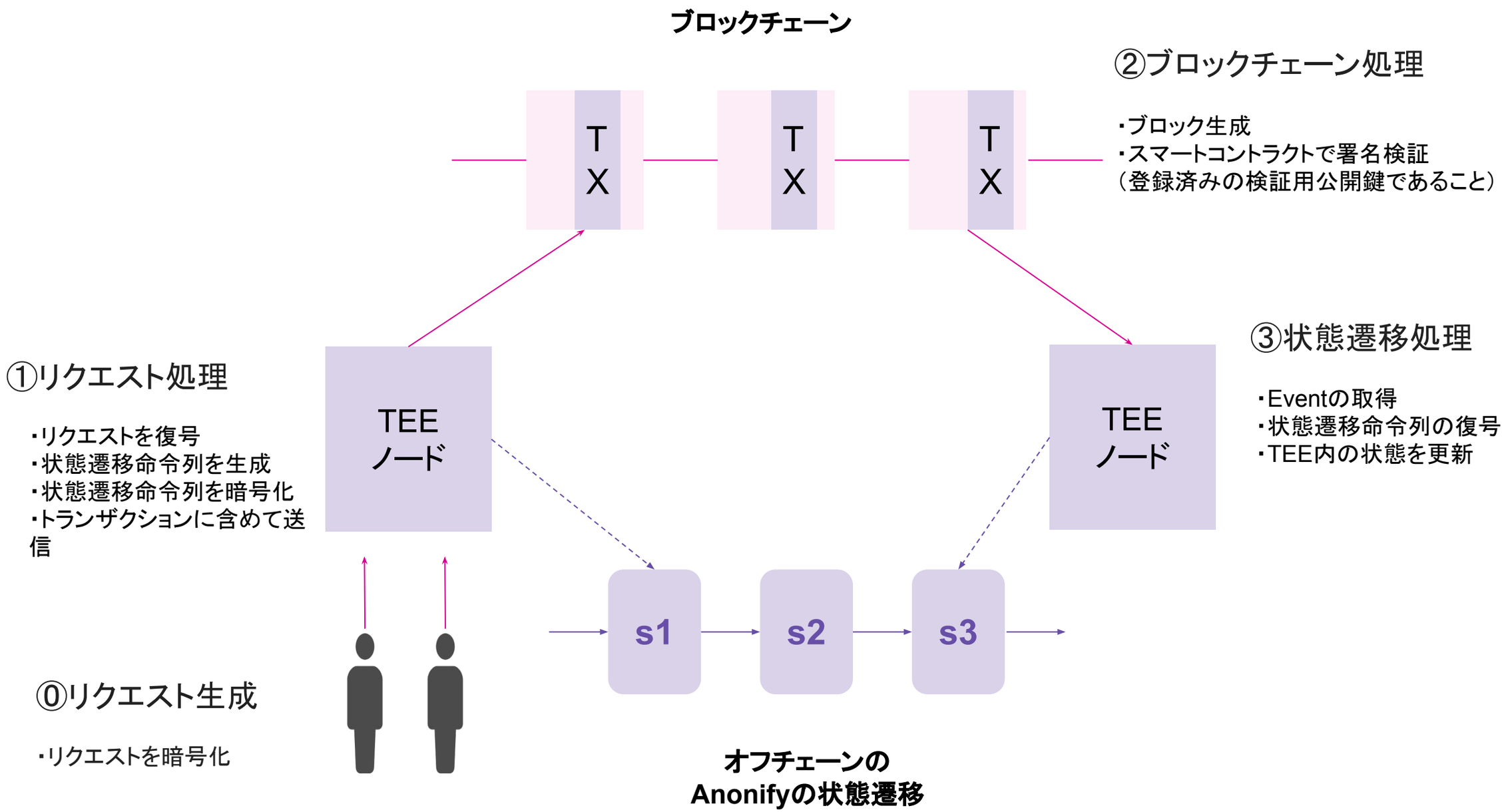
あらまし
社会のデジタル化が進む中で, ユーザのパーソナルデータを利用するサービスや, 複数の企業や組織間で業務データ等を共有するシステムが誕生している. このようなシステムでは, 用途に応じて, データを他の参加者やシステムの運営者に対して秘匿化したまま利活用できることが望ましい.
本稿では, 幅広いアプリケーションにおいて, 状態データを秘匿化して記録したまま, ビジネスロジックを実行可能とするモジュールである Anonify を提案する. Anonify は Trusted Execution Environment (TEE) を用いることにより, データを秘匿化しつつ, 実行されるプログラムの完全性を保証する. また, トランザクションをブロックチェーンに記録することにより, 状態データの改ざんを困難とする. さらに, 特定の主体に対してのみデータを開示する監査機能も提供する.
我々は Anonify のプロトタイプを実装し, デジタルアセット管理のアプリケーションにおけるパフォーマンス評価を行った.

キーワード Trusted Execution Environment (TEE), Intel SGX, ブロックチェーン, プライバシー保護

論文: https://drive.google.com/file/d/1f0syLlRmd7tJDW6fbz3h8CgsA1V7OFb6/view

Anonifyのアーキテクチャ

- TEEとBlockchainを組み合わせることで、秘匿性とブロックチェーンの改竄耐性を両立
- ブロックチェーンに暗号化された命令を記録、オフチェーンのTEEノードが命令を解釈して状態遷移



コンフィデンシャル・コンピューティング/TEEとは

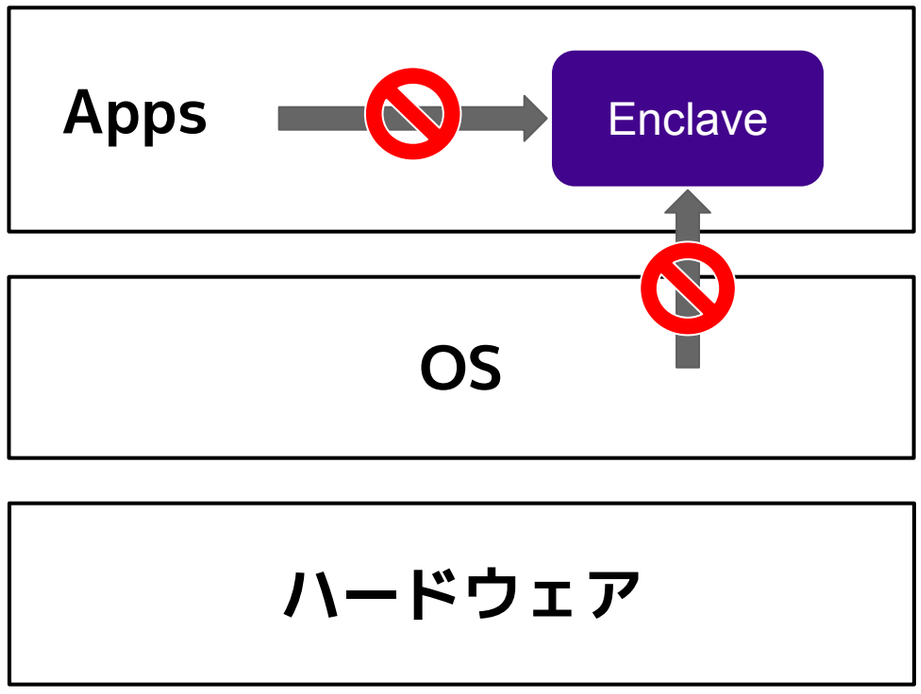
- データを「秘匿化したまま処理」する技術の一種
- 暗号学的な秘密計算手法と異なるハードウェア技術（CPUのセキュリティ機能）
- 今回はIntel® SGXを想定する（他にもArm TrustZone, AMD SEV等、様々な半導体ベンダーが製品化）

秘匿性
（Confidentiality）

Enclaveのデータは平文で外部からアクセスできない

真正性
（Execution Integrity）

実行されたプログラムを外部から検証可能



参考: コンフィデンシャル・コンピューティングへ集まる注目

- Microsoft, Amazon, Googleをはじめとするパブリッククラウドクラウドベンダーが積極投資
- 金融、医療、行政など、データの機密性の高い分野でのクラウド利用を促進

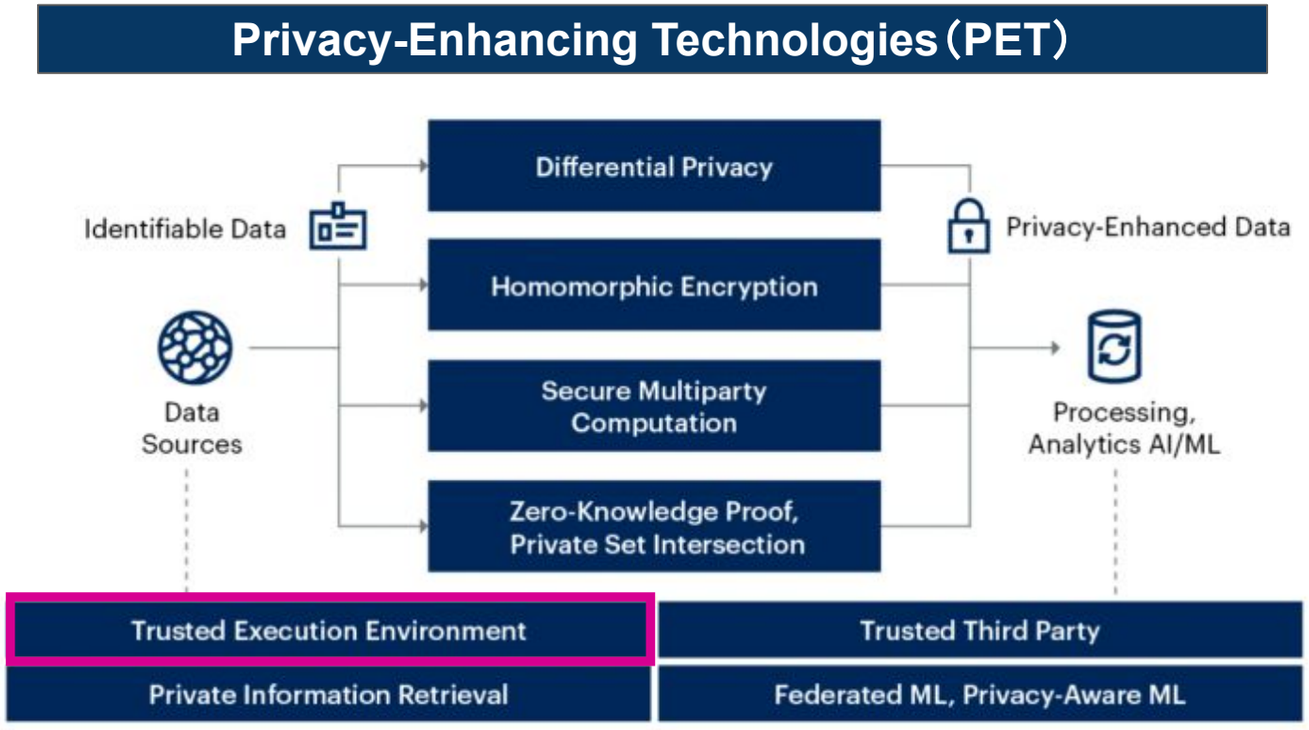
日経XTECH

クラウド以降が進む中次世代のセキュリティ技術として「2021年はコンフィデンシャルコンピューティングが注目を集める年になりそうだ。」

日経クロステック ：「コンフィデンシャルコンピューティング」に注目、ゼロトラストの最後の抜け穴ふさぐ

調査大手Gartner社

戦略的テクノロジーの2021年トップ・トレンドでは差分プライバシーやゼロ知識証明等と合わせてコンフィデンシャルコンピューティング（TEE）がプライバシー保護技術（PET）として選出された。



Gartner Report: Top Strategic Technology Trends for 2021: Privacy- Enhancing Computation

インターネット投票プロジェクト

投票の要件: 透明性

- 現在の投票は、長い歴史の中で培われた**選挙運営における不正を防止するための仕組み**が備わっている

ゼロ票確認
（公職選挙法施行令第34条）

http://fuji-news.net/data/report/politics/201412/0000003448.html

開票の参観
（公職選挙法第69条）

https://mainichi.jp/senkyo/articles/20191221/k00/00m/010/035000c

実際に不正が起きていなくても、有権者がそれを検証できることが重要

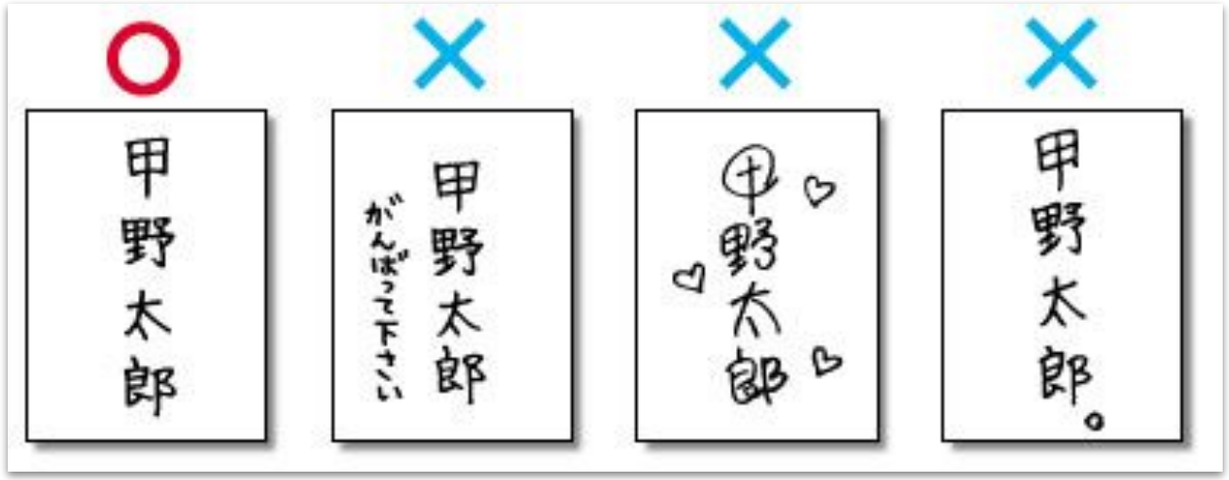
投票の要件: 秘匿性

- **投票の秘密（日本国憲法第15条）**という原則を守るべく、様々なルールが定められている

投票の秘密を守るための投票ブース

https://www.nikkei.com/article/DGXMZO36249940Z01C18A0I10000/

投票用紙への他事記載禁止（公職選挙法68条6項）



https://www.city.yamatotakada.nara.jp/life/senkyo/tohyo-s.html

投票は無記名（公職選挙法46条）

投票の秘密は、「正直」に投票しやすいという心理的な問題だけではなく、強要、買収、報復行為などを防止するための基本要件

インターネット投票での透明性・秘匿性の実現は難しい

- 投票システムの透明性・秘匿性は、通常のシステムにはない難しい要件であり、その両立はさらに困難

透明性の難しさ

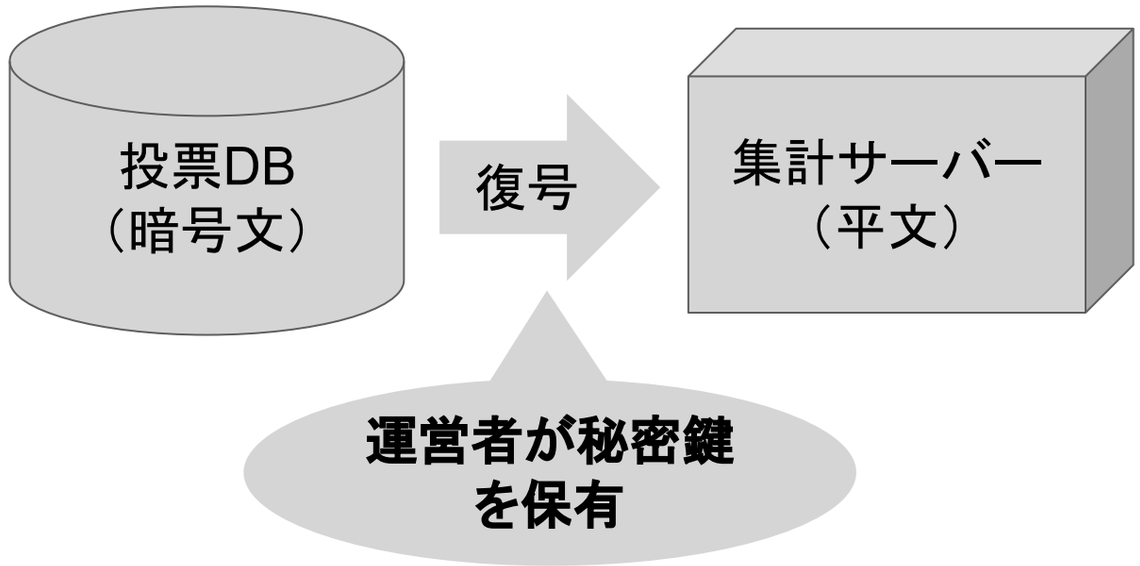
選挙人ID	投票内容
0x12aa	筑波 太郎
0x34bb	東京 花子
0x56cc	茨城 健
0x78dd	筑波 太郎

選挙人ID	投票内容
0x12aa	筑波 太郎
0x34bb	東京 花子
0x56cc	茨城 健
0x78dd	**東京 花子**

通常のデータベースでは、**投票データの改ざん**は検証できない

自分の投票が**記録されずに捨てられていても**検証できない

秘匿性の難しさ



投票データを暗号化して記録しても、
運営者はいつでも復号できる

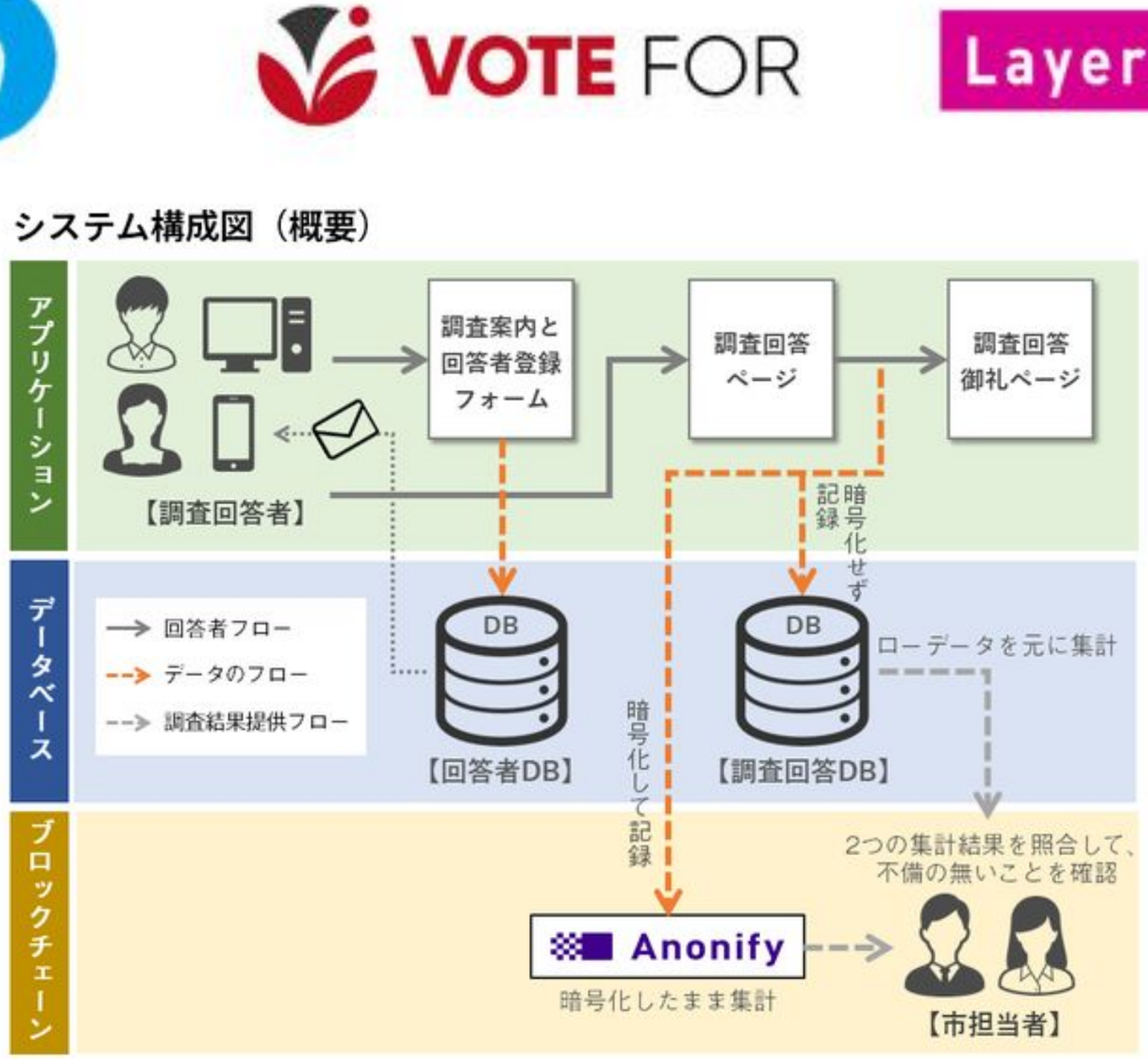
**現実の投票のセキュリティも完璧ではないが、
デジタルでは選挙結果に影響するような大規模な不正が低コストで実行可能**

つくば市 ネット投票案件

- 今年9-10月に実施した、市科学技術・イノベーション振興指針の策定のための市民意見収集
- 公職選挙でのインターネット投票実現を目指すつくば市の取り組みの一環
- ブロックチェーン × Intel SGXの本番稼働（国内初？）

VOTE FOR

LayerX Labs



https://prtimes.jp/main/html/rd/p/000000083.000036528.html

「検証可能性」の技術と
Beyond PoC

関係者の方に言われたこと

「インターネット投票は効率的だけど、
集計がパッと終わってしまってブラックボックス感がある」

「集計のブラックボックス感」

- **個人的には新鮮な感覚だった**

  - ふとした際のポロッとした「本心から」の言葉だと感じた
    - 様々なブロックチェーン案件に関わってきて、技術者ではない方に本心からシステムの透明性に関して気にされたことはあまりなかったような気がする
      - ビジネス観点 or サイファーパンク的なのは多かった

  - 安直には、ブロックチェーンやTEEの出番
    - しかし、一般の人にとっては技術的に正確に理解することは困難
    - また、技術的に問題ないことと、心から信頼できることは違う
      - 「安心と安全」の違い
    - **ユーザーの「安心感」に貢献して初めてBeyond PoCと言えるのでは？**

→ 一般の人の「集計のブラックボックス感」を解消してもらうには？

ネット投票システムの「透明性・アカウンタビリティ」

- 集計のブラックボックス感をなくすには、投票の記録及び集計処理を外部から検証可能にする

投票システムの透明性

投票の記録

- 全ての有効な投票が（捨てられずに）記録されていること
- 不正な投票が記録されていないこと

集計処理

- 記録された全ての投票が（改竄・除外されずに）集計のインプットになっていること
- 正しい集計プログラムが実行されたこと

※投票システム全体のセキュリティ要件としてはこれでは不十分
（投票の秘密、投票の強要の防止、etc.）

ブロックチェーン/TEEの「真のBeyond PoC」のハードル

- **ブロックチェーン、TEEは広い意味で「システムの挙動を外部から検証可能にする技術」**
- **しかし、「技術的に検証可能であること」を、人間の「信用」に変えるには工夫が必要**

真のBeyond PoCのためのチェックリスト

- ユーザー・ステーホルダーは、実際にどの部分の「検証」をどのようなUX/業務フローで行うのか？
  - 例: 投票システムの監査を行うのは有権者？選挙管理委員会？
- 上記の「検証」の仕組みは、各者のリテラシーやケイパビリティに対して現実的か？
  - 例: ブロックチェーンの状態遷移・ファイナリティ検証できるか
- 上手く検証できなかった人がいても、他の人が代わりに守ってあげることはできるか？
  - 例: スマホに不慣れな高齢の方の投票が取り込まれていることを誰が担保する？
- また、「誰かが検証してくれていること」を信用する、信用の連鎖の構造はあるか？
  - アナロジー: 現在の投票では、多くの人はゼロ票確認にも開票の参観にも行かない、でも各種立会人はいる

→ **“Usable Trust” の重要性**

ネット投票案件における取り組み

- **残念ながら、今回の本番システムの中でフルに検証可能性を活かす機能は使えなかった**
  - **真のBeyond PoCは達成できず**
- **しかし、関係者の方に「ブラックボックス感」を少しでも解消してもらう、ブロックチェーン・TEEの手触り感を持ってもらうためのデモを行った**

- やったこと
  - 1: 要素技術に関して、例え話を用いた概念の説明
  - 2: 実際にシステムの「検証」を行う流れのデモの実施

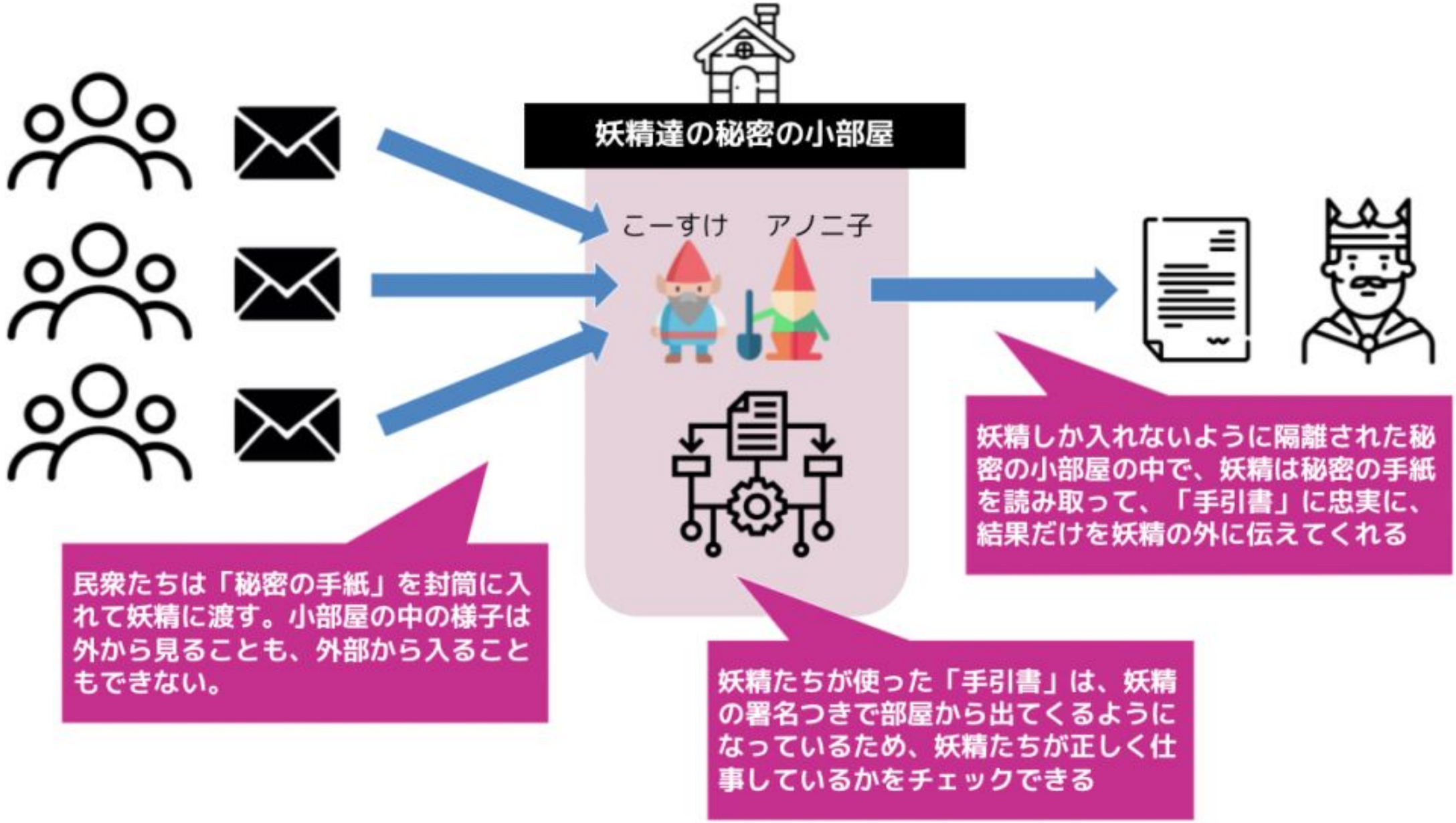
- ターゲットの定義が重要
  - 今回の定義「ブロックチェーン、TEEの専門家ではないが、基本的なIT技術には慣れていて、ハッシュ関数などは知っている」人
  - 「全有権者の方が検証する必要はないが、一部のリテラシーある方が検証できる」ことを目指す
    - 現在のゼロ票確認（一部の人が朝並んでやっている）と近い

本日は時間の関係もあり、TEEのExecution Integrityに絞ってご紹介

1: 要素技術に関する
例え話を用いた概念の説明

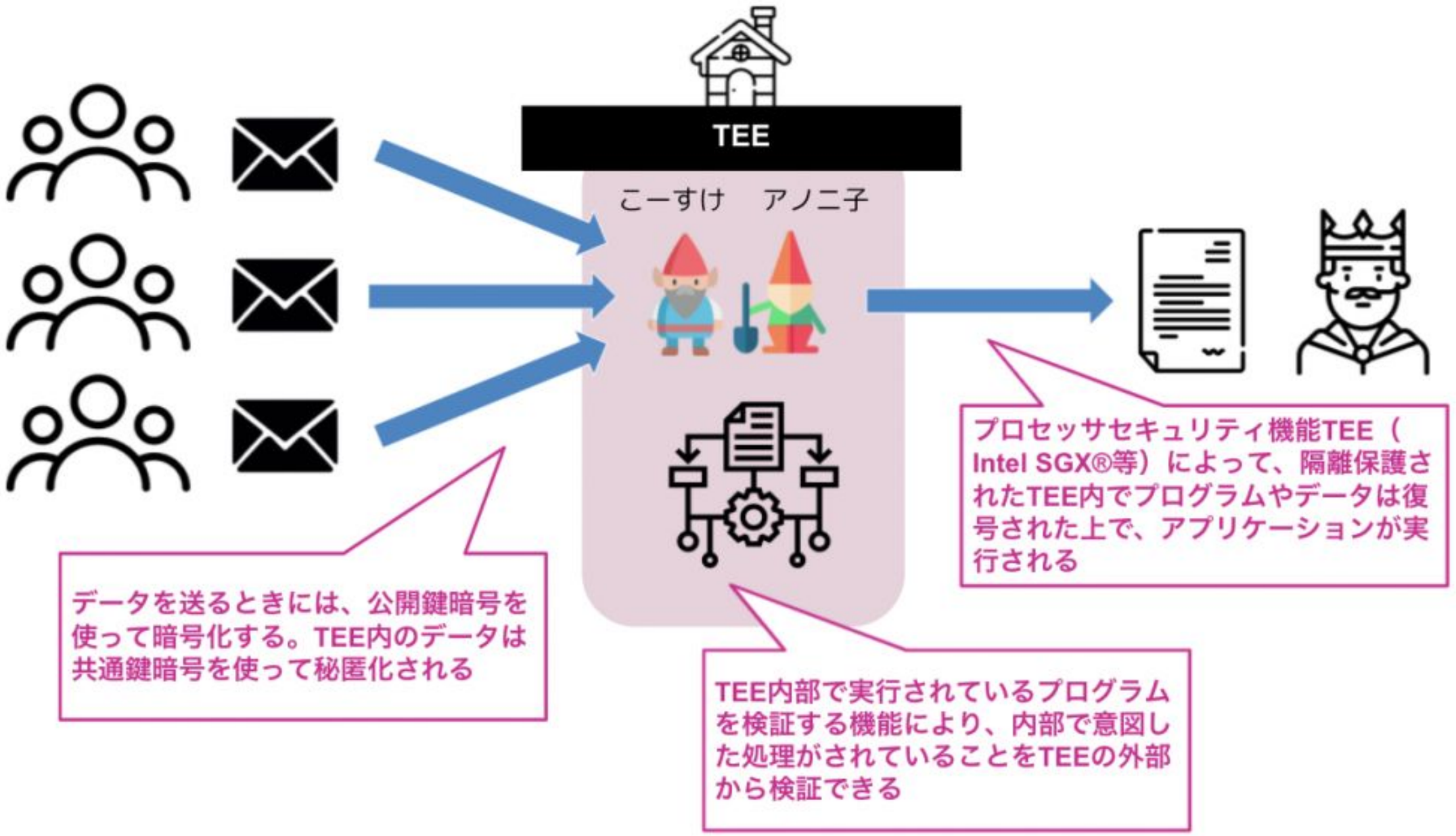
技術詳細に立ち入らない説明　～ 王様と妖精達のものがたり ～

- 民衆の書いた「秘密の手紙」は封筒に入れて小部屋の妖精たちに渡されるため外から内容を見ることはできず、小部屋の中の様子は外から見ることができず、小部屋に外部から入ることもできない。
- 「手引書」は、**妖精の署名つき**で部屋から出てくるため、**妖精が正しく仕事しているかチェック可能**。



技術詳細に立ち入らない説明　～ 王様と妖精達のものがたり ～

- 「妖精たちが暮らす秘密の小部屋」が、CPUのセキュリティ機能によって隔離保護された区画（TEE）
- **TEE内部で実行されているプログラムを検証する機能**により、内部で意図した処理がされていることを**TEEの外部から検証可能とする「監査性・透明性」**を提供。

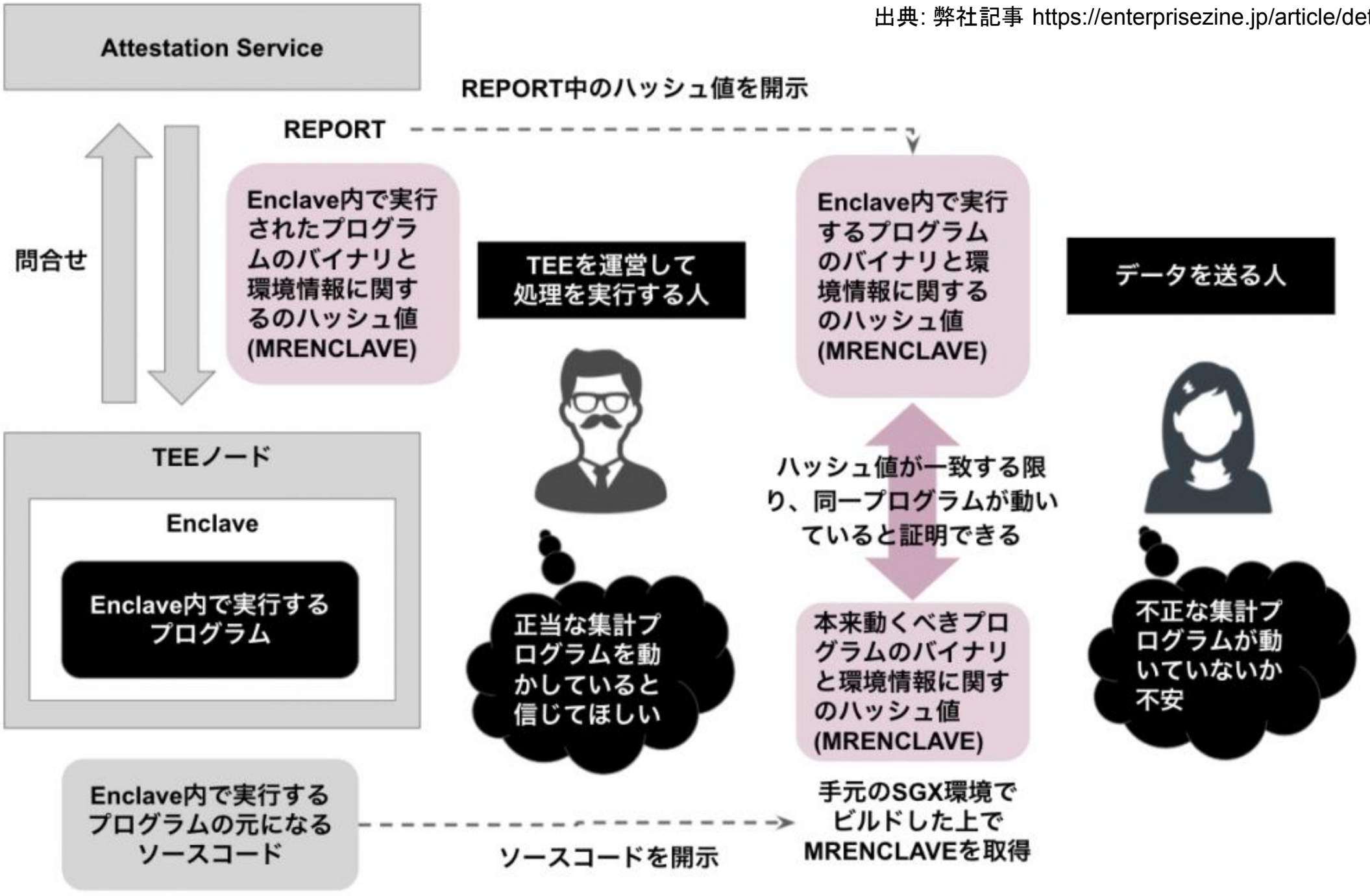


2: システムの検証の流れのデモ

コンフィデンシャル・コンピューティングにおけるIntegrity

- TEEのExecution Integrityの性質により、実行されているプログラムは外部から検証可能
- 具体的には、実行プログラムに基づくハッシュ値 (MRENCLAVE) で確認

出典: 弊社記事 https://enterprisezine.jp/article/detail/14749



デモ（※当日は動画で紹介）

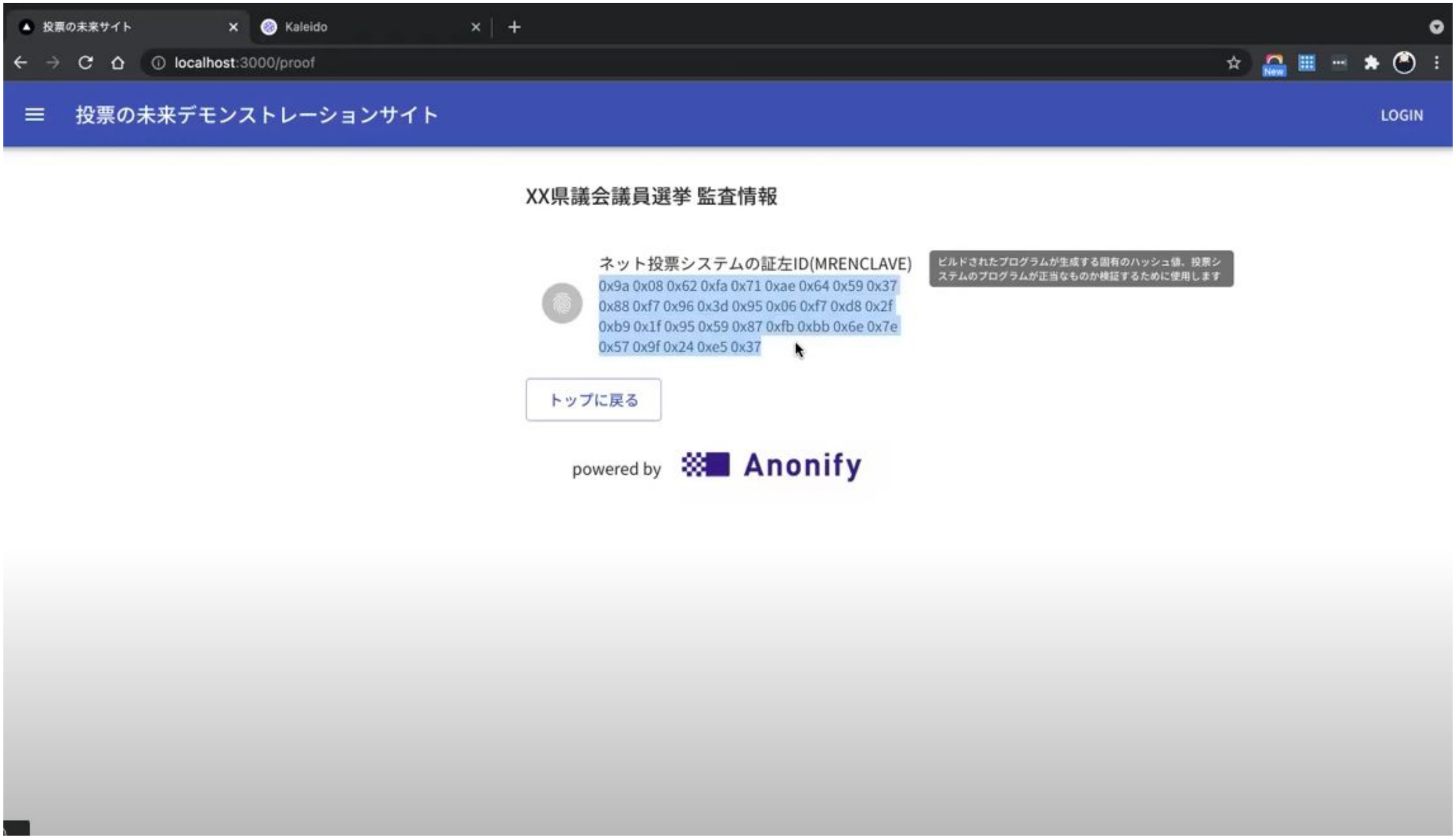
正しい集計プログラム

github.com/glassonion1/rust-101/blob/main/sgx-sdk/examples/measurement/enclave/src/lib.rs#L30

```rust
pub extern "C" fn ecall_vote(ballot: *const u8, ballot_len: usize) -> sgx_status_t {
    let ballot_slice = unsafe { slice::from_raw_parts(ballot, ballot_len) };

    let ballot = String::from_utf8(ballot_slice.to_vec()).unwrap();
    println!("I vote {}.", ballot);

    let mut votings = get_votings();

    votings.push(&ballot);

    let mut result_taro = 0;
    let mut result_hanako = 0;
    let mut result_natsuko = 0;

    // Summarize
    for v in votings {
        if v == TARO {
            result_taro += 1;
        }
        if v == HANAKO {
            result_hanako += 1;
        }
        if v == NATSUKO {
            result_natsuko += 1;
        }
    }

    println!("taro: {}", result_taro);
    println!("hanako: {}", result_hanako);
    println!("natsuko: {}", result_natsuko);

    sgx_status_t::SGX_SUCCESS
}
```

デモ（※当日は動画で紹介）

正しい集計プログラムに基づくMRENCLAVEの値



デモ（※当日は動画で紹介）

投票プログラムを改竄（TAROの票を二重カウント）

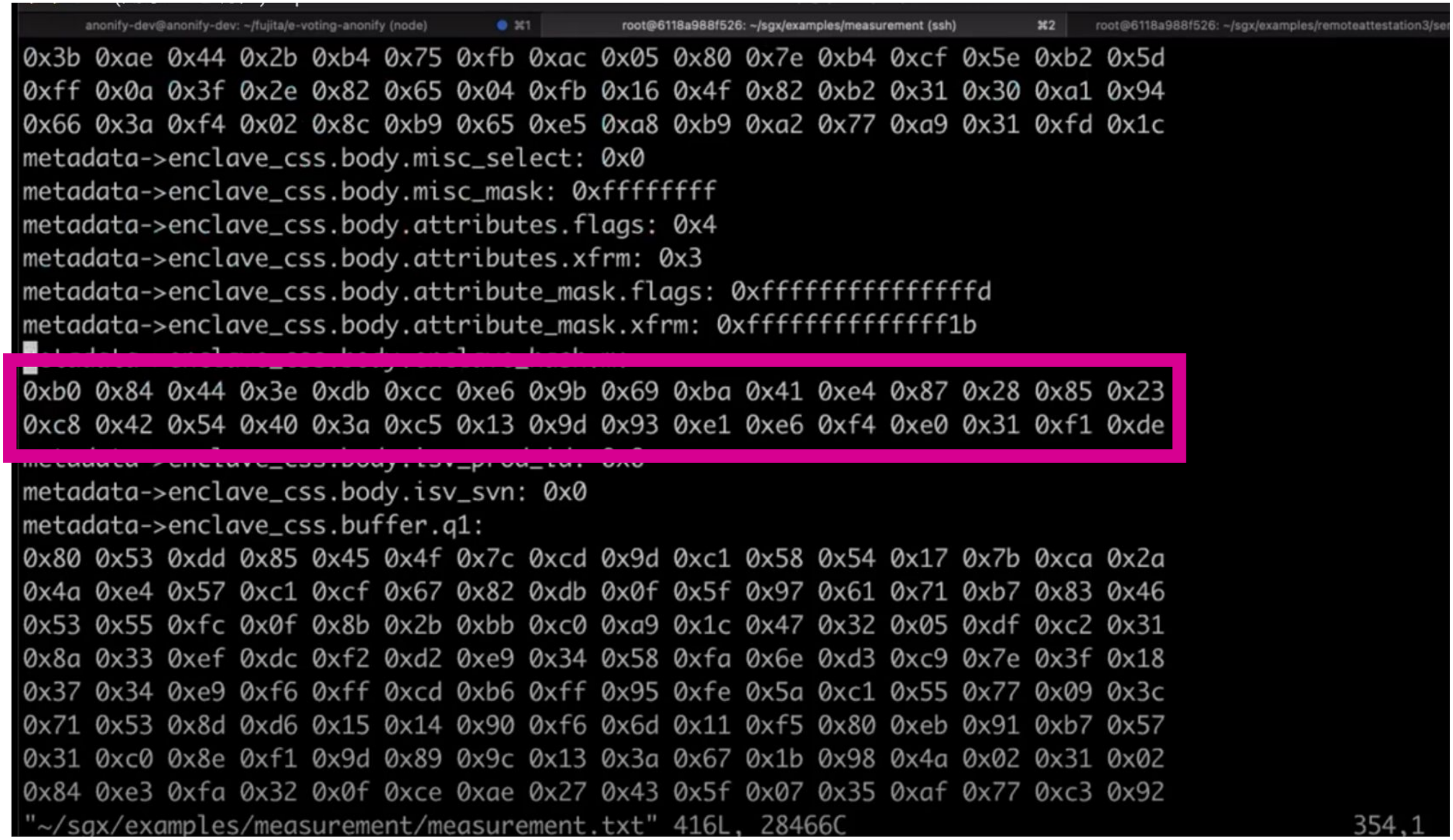
anonify-dev@anonify-dev: ~/fujita/e-voting-anonify (node) ⌘1 | root@6118a988f526: ~/sgx/examples/measurement (ssh) ⌘2 | root@6118a988f526: ~/sgx/examples/remoteattestatic

```
let mut votings = get_votings();

votings.push(&ballot);

let mut result_taro = 0;
let mut result_hanako = 0;
let mut result_natsuko = 0;

// Summarize
for v in votings {
    if v == TARO {
        result_taro += 2;
    }
    if v == HANAKO {
        result_hanako += 1;
    }
    if v == NATSUKO {
        result_natsuko += 1;
    }
}

println!("taro: {}", result_taro);
```

48,9

デモ（※当日は動画で紹介）

MRENCLAVEが変化




LayerX