ETHTerakoya

インターネット投票の実現にむけて

背景

ETHTerakoya

マイナンバー活用の機運

・多くの行政手続きが旧態依然の仕組みのままで効率化が進んでこなかった。
・新型コロナウイルスによる非接触需要の高まりなどを契機に、電子政府化に向けた動きが活発化。
・大きな可能性を持つマイナンバーがガラパゴス化せず活用を広げていくためには、技術の実現可能性や根本設計を前提とした議論が求められている。

インターネット投票への応用

・行政が中心となって行う国政選挙はマイナンバー活用と親和性が高い
・投票では本人証明や秘密投票など、求められる要件がいくつかある
・電子政府化に向けた導入例として、これまで活用が進んでこなかったインターネット投票を題材として議論を行う

デジタル政府の一丁目一番地としての必要性

これまでの紙の投票で実現できなかったことを新しい技術を活用して実現できるような取り組みが、デジタル政府の機運とともに求められていく

現在の投票の課題

ETHTerakoya

投票者の課題

- ☐ 政治への関心の低下に伴う投票率の低さ
- ☑ 高齢者など移動が困難な人の投票ハードルが高い
- ☐ 一票の格差
- ☑ 複雑な手続き

管理者の課題

- ☑ 多くの手作業が非効率
- ☑ 人的労働による集計ミス
- ☑ 改ざん耐性の弱さ

なぜ選挙(=投票)にマイナンバーの活用が必要か？
選挙という国民行事のオンライン化を進めるためには、オンライン上での国民管理が必須である。そのため、マイナンバーという国民IDの活用が求められる。

インターネット投票とは

ETHTerakoya

インターネット投票とは

パソコンやスマホなどからインターネットを使って投票を行うこと。

- ✔ 行政手続きの効率化
- ✔ 投票の効率化

電子投票とは

決められた投票所に行き、タッチパネルのような電子機器を用いて投票を行うこと。

- ✔ 行政手続きの効率化

※現行法上、インターネットへの接続は不可

海外のインターネット選挙の動向

ETHTerakoya

■アメリカ

アメリカでは主に海外からの投票について、アリゾナ、コロラド、ミネソタ、ノースダコタの4つの州では専用のウェブサイトから投票可能。ウェストバージニア州では、ブロックチェーン技術を使ったモバイルアプリが提供されている。他にも19の州ではe-メールないしはfaxを使って投票することができる。しかし、ワシントン州ではスマホ投票の導入によって投票率が改善したという結果を得ることはできなかった。

■ スイス

2003年以来、各州が主導して300を超える選挙や国民投票でインターネット投票を行ってきたスイスでは、連邦政府が主導して2019年10月の連邦議会選挙において全26州のうち少なくとも2/3以上の州でインターネット投票を予定していた。しかし、システム開発費の高騰やセキュリティ面の問題から、2019年の連邦議会選挙ではこれまでにインターネット投票を行っていた州も含めてすべての州でインターネット投票の実施が見送られることになった。

■ ロシア

ロシアでは2020年に二つの地域でブロックチェーンを活用した投票の取り組みが実施される予定で、1つは国営通信会社のロステレコム（Rostelecom）、もう1つはすでにブロックチェーン投票システムを利用した経験を持つモスクワ市の情報技術局（DIT）で実施予定です。ロステレコムのシステムは9月13日にロシアの2つの地域、クールスカヤ（Kurskaya）とヤロスラヴスカヤ（Yaroslavskaya）でのロシア下院補欠選挙に使用されます。前回7月にロステレコムが実施した際にはセキュリティが脆弱なファイルから個人IDを取り出す方法が見つかり、ダークウェブで個人データが売られる事態に発展している。

海外のインターネット選挙の動向

■電子政府先進国 エストニア

国政選挙ですべての国民を対象にしたネット投票を実施している唯一の国。エストニアの国民は、インターネットに接続しているPCとエストニアのIDカードさえあれば、世界中のどこにいても選挙に参加することができる。有権者は選挙用サイトからダウンロードした投票用ソフトウェアをインストールし、IDカードに記載されている数字とパスワードを入力し、候補者を選択するだけ。買収や脅迫に対する対策として、一度投票を行っても期間内であれば投票内容を変更できるシステムになっている。エストニア政府は、人口130万人のうちおよそ30%が電子投票システムを利用していて、1回につき1万1000時間もの選挙関連の労働時間が削減できると述べています。

エストニアのインターネット投票の脆弱性

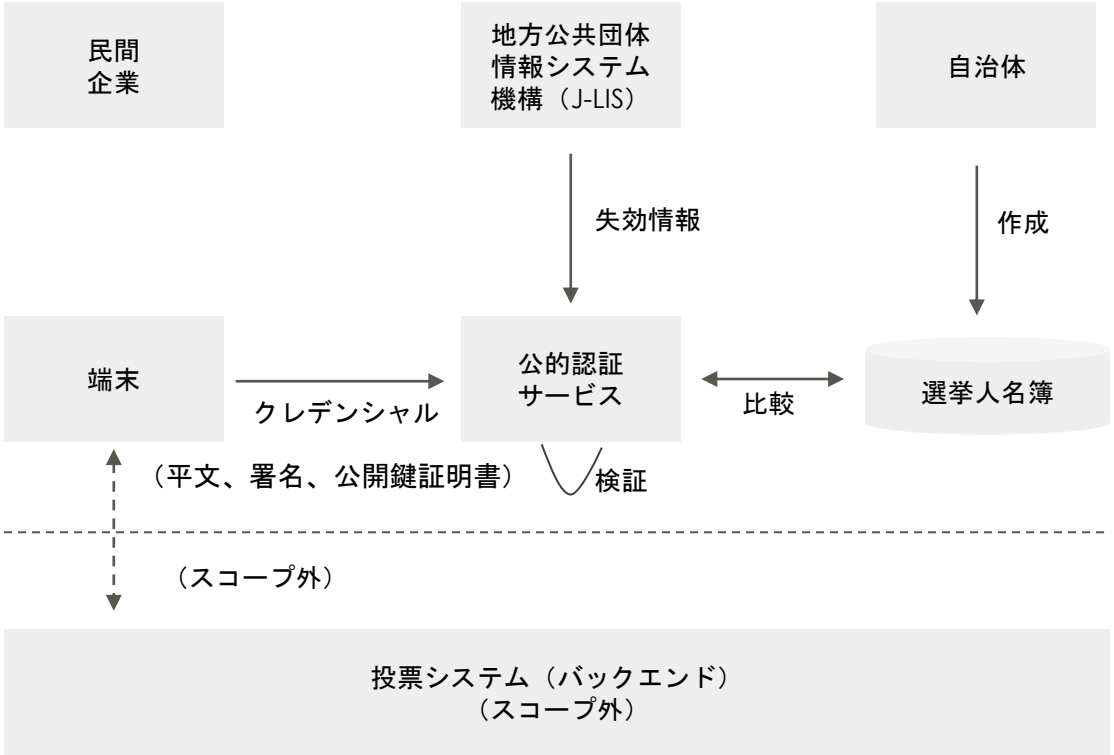
2014年、ミシガン大学でコンピューターサイエンス分野の准教授であるアレックス・ヘルダーマン氏は、エストニア国内で利用されている電子投票システムの安全性を調査するため、実際のシステムと同じ構成を持つダミーシステムを研究室内に構築し、一連の投票の手順でどのような問題があるかという検証を実施。その結果、投票者のコンピューターへのハッキングと、投票システムにマルウェアを仕込むことの両方の方法で、選挙結果を操作できることが判明。

各国でオンライン化の流れは進んでいるが、主にセキュリティ面の懸念から導入に成功している国や範囲は限定的である。特に選挙の場合、国の方向性に関わり、巻き戻しが困難なため、リスクを取ることは難しい。

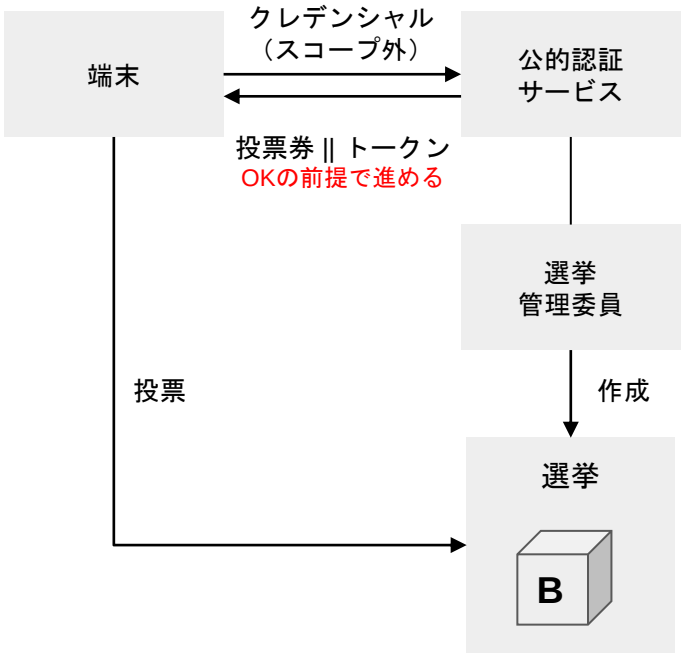
現在の投票との比較および電子投票の実現性リスト

項目	内容	現在の紙での投票	電子投票での技術的実現性	技術要素
秘密投票/機密性	投票の全期間を通じて誰がどの候補者に投票を行ったのか秘密を守る	○	○	ゼロ知識証明, 準同型暗号, Mixnet, ブラインド署名
認証/有権判定	投票権の確認	○	○	生体認証 + マイナンバー電子証明書
本人確認	替え玉の防止	×	△	オンライン投票になると可能か？
一人一票	二重投票の防止	○	○	スマートコントラクトを使った コイン投票
改竄耐性/信頼性	投票箱が空であることの確認	×	○	コントラクトのtx履歴
	投票内容が改竄されていない事の証明	×	○	BCの改竄耐性に依存
買収の防止	買収の防止	×	×	現状難しいか？
平等性	全有権者への投票機会の確保	△	△	発行機関に依存か？
正確性/検証性/透明性	投票の反映の検証性/信頼性	×	○	自己集計システム, ex: OpenVote

目指すスコープ：認証


民間
企業
地方公共団体
情報システム
機構（J-LIS）
自治体
失効情報
作成
端末
クレデンシャル
公的認証
サービス
比較
選挙人名簿
（平文、署名、公開鍵証明書）
検証
（スコープ外）
投票システム（バックエンド）
（スコープ外）

目指すスコープ：投票


端末
クレデンシャル
（スコープ外）
公的認証
サービス
投票券 || トークン
OKの前提で進める
選挙
管理委員
投票
作成
選挙
B

目指すスコープ：集計