i-Voting 方式による電子投票選挙とその特長

一、 エストニア共和国という国

二、 インターネット投票とは

三、 オンライン投票 i-Voting の流れ

四、 二重封筒方式

五、 ブロックチェーン

六、 分散型サービス拒否攻撃（DDoS 攻撃）

七、 複合化方式による鍵管理

八、 インターネット投票の監査

九、 日本市場での可能性

十、 エストニア唯一、ナンバーワン電子投票（i-Voting）専門企業 Cybernetica 社と駐日エージェント契約締結

十一、お問合わせはこちら

一、　エストニア共和国という国

世界最先端の「電子立国」と言われ、NATO のサイバーセンターでもある。

その実態は以下の通りだ。

- 2005 年の選挙で全国的にインターネット投票を導入した世界で最初の国
- 国民のほぼ全ての営みに ID カード使用
- 新会社の設立手続きは 20～30 分で完了
- 銀行取引の 99%はインターネットで処理
- デジタル署名、デジタルカルテが普及
- 税務申告は 5 分で終了
- 閣議は通常スクリーンと PC のみ

等々が特記すべき主な特長である。

Tallinn, Estonia (Shutterstock)

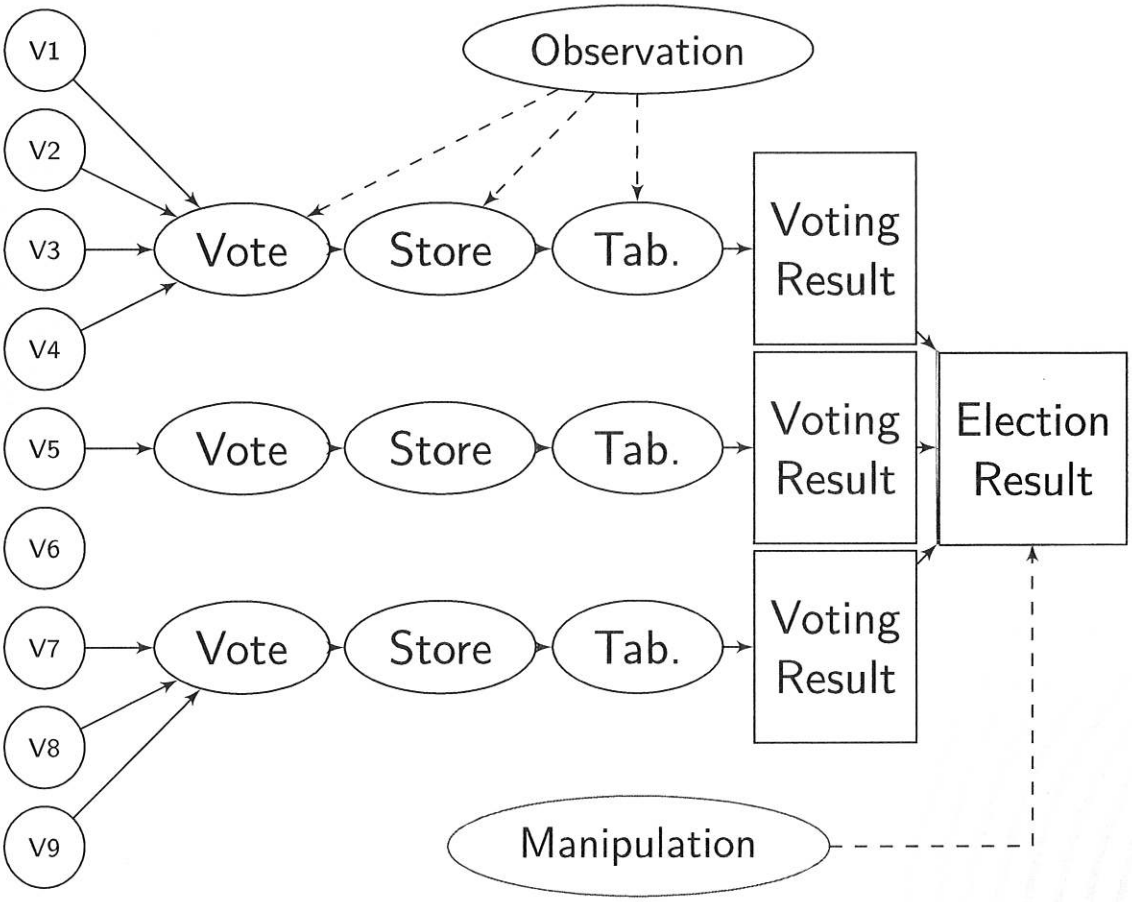
二、インターネット投票とは

- 投票者と電子投票箱の間の通信経路としてインターネットを利用した遠隔地での電子投票のこと。
- 投票者の端末はPC、タブレット、スマートフォンのいずれかとなる。
- この流れを図示すると添付のようになる。より具体的に述べると通常は次のように実施される。
- インターネット投票は通常期日前投票期間中の選挙日の 2 日前までにのみ利用できる。投票日当日のオンライン投票を行うことは出来ない。
- この期間中に各有権者はインターネット投票を数回行うことが出来る。

  最後の投票のみが公式の集計に有効となる。
- インターネットで投票した有権者の名前は有権者名簿から削除される。
- 紙の投票がなされた場合、インターネット投票の票はキャンセルされる。

  （紙の投票の優位性）
- 汚染された投票（強制または脅迫された票）のケースでは、有権者は再度投票し、以前の投票を上書きする機会を与えることにより、投票の秘密を保護することを目的とする。
- 投票者は、国民IDカードまたは「モバイルID」で自分自身を識別する。日本の場合はマイナンバーカード、健康保険証が考えられる。

Voting method in the election process



三、 オンライン投票 i-Vorting の流れ

手順は次のようになる。

1．投票するにはインターネットに接続されるコンピューターと国民 ID カード又はモバイル ID の提示が必要。

2．投票アプリケーションがダウンロードされるとソフトウェアによって自動的に投票者に投票権があるか否かが確認される。次に候補者のリストが表示される。

3．投票されると、アプリケーションが投票内容を暗号化して投票集計サーバーに送信する。

4．投票者には投票日時を記録したタイムスタンプが渡される。

5．事後に投票内容が正常に集計サーバーに送られていることを検証することも出来る。

（PC から投票し、モバイル端末から確認可能）

四、二重封筒方式

投票所での投票が困難な人のための投票手段としては次の二つが考えられる。

1) 郵便投票

2) 二重封筒方式

以上のうち、二重封筒方式では有権者は投票を中央データベースに送信し、プラットフォームを介して投票することになる。

匿名の封筒（内側の封筒）に票を入れて封をし、さらに投票者の ID と署名（セッションログ）を記入した封筒（外側の封筒）の中に入れる方式で、以下の図のようになる。即ち、

（内側の封筒では）

投票内容とシステム生成した数字を選挙専用の公開鍵で暗号化する。

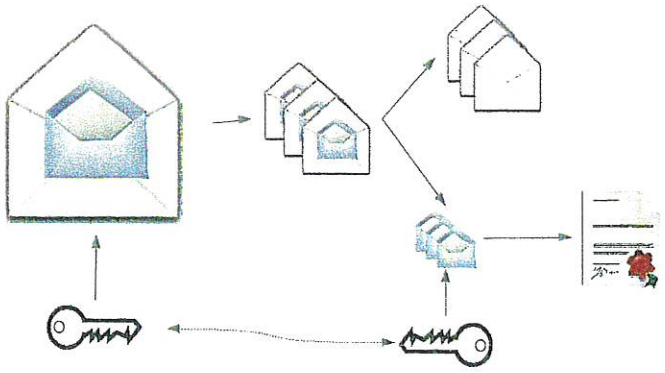
（外側の封筒では）

デジタル署名ツールを用いて署名する。

デジタル署名には有権者の国民 ID が用いられる。

以上の経過を経て、デジタル署名入りの暗号化された電子票は投票所で重複投票の有無を確認した上で、その選挙専用の秘密鍵で複合され集計される。

ダブルエンベロープ



五、　ブロックチェーン

ブロックチェーンは、データベース管理者を含む内部による不正を防止する観点で設計、実施されている自己データ追跡機能のこと。

即ち、「取引履歴」を暗号技術によって過去から１本の鎖のようにつなげ、正確な取引履歴を維持する技術といえる。

・ 一つのブロックは合意された投票記録の集合体と

・ もう一つは各ブロックを接続させるための情報で、

この二つで構成されている。

（改ざんを行うためには、それより新しい投票の全てを改ざんしていく必要があるため、データの破壊・改ざんが極めて難しい。）

通常の集中管理型システムと異なり、複数のシステムが情報を保有し「分散型台帳」という仕組で管理されているため、一部のシステムが停止・故障してもシステム全体の運行稼動に与える影響を抑制することが可能である。

（一社）　全国銀行協会の資料より

六、 分散型サービス拒否攻撃(DDoS 攻撃)

ネットワークリソースやサービスを一時的または無期限に停止または中断させるなど、意図するユーザーが利用できないようにするサーバー攻撃のこと。

DDoS 攻撃は通常、余計なトラフィックやネットワークリクエストで対象リソースを圧倒し、対象サービスに過剰な負担をかけ、正当なリクエストの履行や有効なリクエストの処理を妨げることを目指す。

DDoS攻撃は、インターネット上のあらゆるシステムに影響を与える可能性があり、したがって、オンライン投票システムにも影響が及ぶ可能性がある。

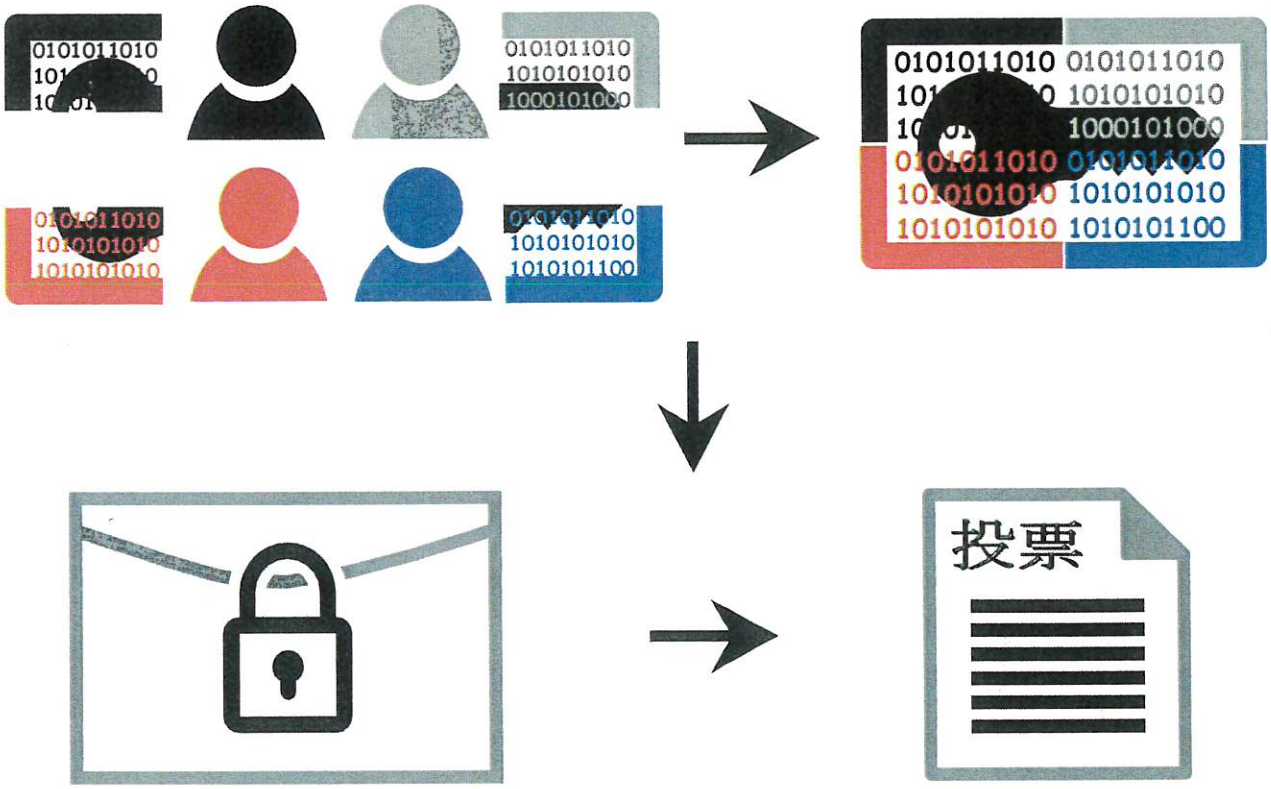
オンライン投票システムに対する DDoS 攻撃の可能性と影響を最小化するための措置を講じることは可能であり、Cybernetica 社のオンライン投票システムは、このような攻撃を排除するために必要な適切かつ合理的な DDoS 保護手段を備えている。

七、 復号化方式による鍵管理

認可された選挙担当者のメンバーは、選挙公式鍵とは別にそれぞれ別の鍵を渡されている。

選挙用公式鍵を再構築し、最終的に投票を復号化するにはこれらの分散保持されている鍵が全部揃う（必要数に達する）ことが求められ必要となっている。

このように Cybernetica 社のオンライン投票システムは、上記の如き複数の鍵管理により投票の秘密性を確保しており、投票者のプライバシーを確保するための非常に有効な方法となっている。



八、 インターネット投票（i-Voting）の監査

監査人は投票システムに保存された票が正しく処理されたことを証明することが役目である。

より具体的に述べると

・すべての票がデジタル署名され、署名が正しく検証されたこと。

・保存されたすべての票が正しく集計に送られたこと。

・暗号化された票は、集計の際にすべて正しく複合化されたこと。

の三点がポイントである。

特にオンライン投票システムの監査は

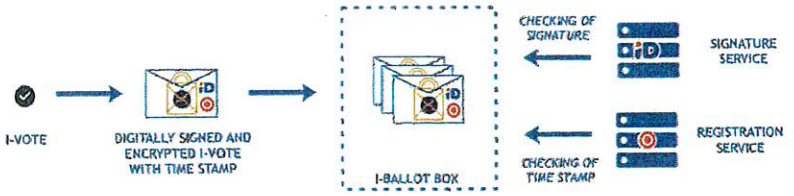
・公式に任命された外部団体、及び

・有権者、又は顧客が個別に監査できることが必要で、その結果、投票結果が正当であることを利害関係者に証明することができることになる。

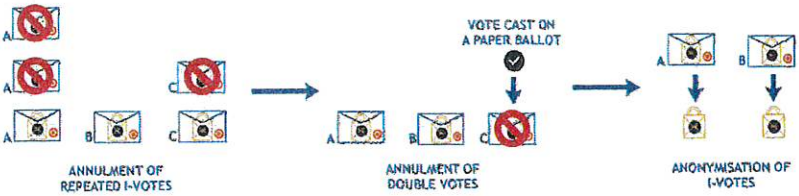
インターネット投票の開票から監査までの流れを次の如く図示した。

インターネット投票の開票と監査1

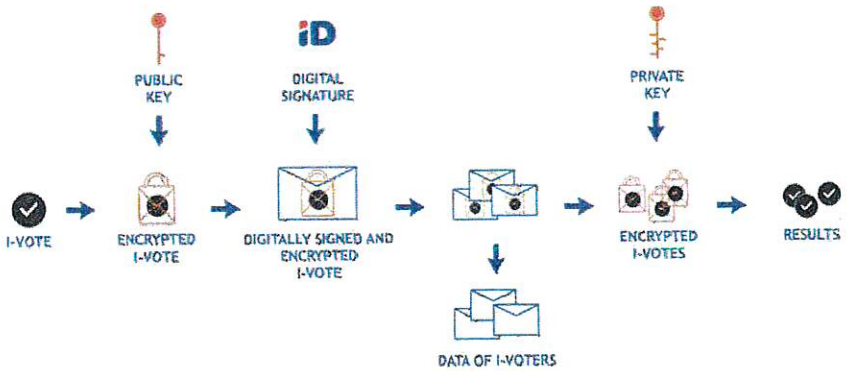
投票ボックス 完全性の確認



複数投票の 無効化



２枚封筒方式



投票データ の混合

投票データ の集計

Jeeadis.jp web site より

九、　日本市場での可能性

日本市場での可能性（マーケットの潜在性）としては少なくとも以下が想定される。

・世界各国在住の日本人の国政並びに地方選挙への参加を i-Voting の形での実現を目指す。総務省選挙部との接渉

・個別団体の選挙（Private Election）

・政界の予備選挙（Primary Election of Political parties）

・ファン投票（Actors or Actresses, Sports Players, Supporter's Ballot）

・その他（Others）

十、 Agent agreement with regard to i-voting between CYBERNETICA AS and Picotec Holdings Inc.

CYBERNETICA AS of Tallinn, Republic of Estonia hereunder called as A and Picotec Holdings Inc. of Tokyo, Japan hereunder called as B wish to enter into an agreement for mutual interest in i-voting business. An agreement is therefore made and entered into effective July 1st of 2023 by and between CYBERNETICA AS and Picotec Holdings Inc. as under;

1. Business relationship The Parties agree that both of us are independent partner

In witness whereof, CYBERNETICA AS and Picotec Holdings Inc. have recognized this agreement to be duly executed as of the July 1st of 2023.

CYBERNETICA AS

By _____
Oliver Väärtnõu

Title CEO

Picotec Holdings Inc.

By _____
Ichiji Ishii

Title President & CEO

十一、お問い合わせ

ご担当者	
電話番号	
メールアドレス	
御社名	
御社住所	〒
代表者名(任意)	
お問合わせ内容	□資料を見たい □説明を聞きたい □その他　（ご自由にご記入ください）