電子マネー

電子マネーとは

- 電子的な「決済手段」
  電子的に記録されたディジタルデータそのものが「価値」を有するもの
- 電子的な「決済方法」
  他の決済手段（預金など）に対して、価値を移転する指示方法が電子化されているもの。（広義の）電子マネー
  クレジットカード、デビッドカードなど

電子マネーの分類（1）

- 汎用性のあるもの（狭義の電子マネー）
  組織（使える場所）を限定せずに、色々なモノやサービスの支払いに利用できる
- 汎用性のないもの
  - 特定の組織、コミュニティでのみ使える
  - 限定されたモノやサービスの支払いにのみ使える
  - ゲーム内通貨、航空会社マイレージ、ショップのポイント、など

電子マネーの分類（2）

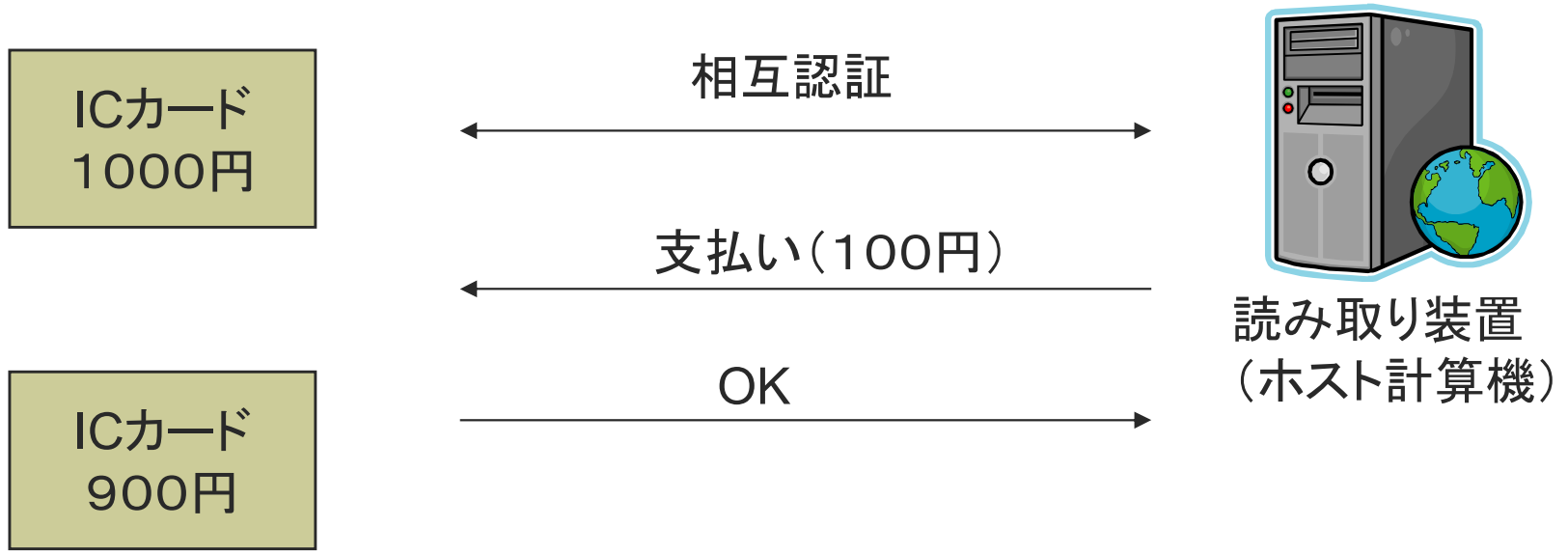
		管理方法		
		サーバ型	端末型	分散型
転々流通性	あり	リバティリザーブ QRコード決済 （PayPayなど）	モンデックス（実験）	ビットコイン、 イーサリウムなど
	なし	WebMoney、 BitCashなど	フェリカ方式 （Suicaなど）	

- 転々流通性のある分散型電子マネーを仮想通貨または暗号通貨と呼ぶことが多い。広義には、転々流通性のあるものを仮想通貨と呼ぶこともある。
- 法定通貨である電子マネーの検討、導入も進められている。

理想的な電子マネーとは

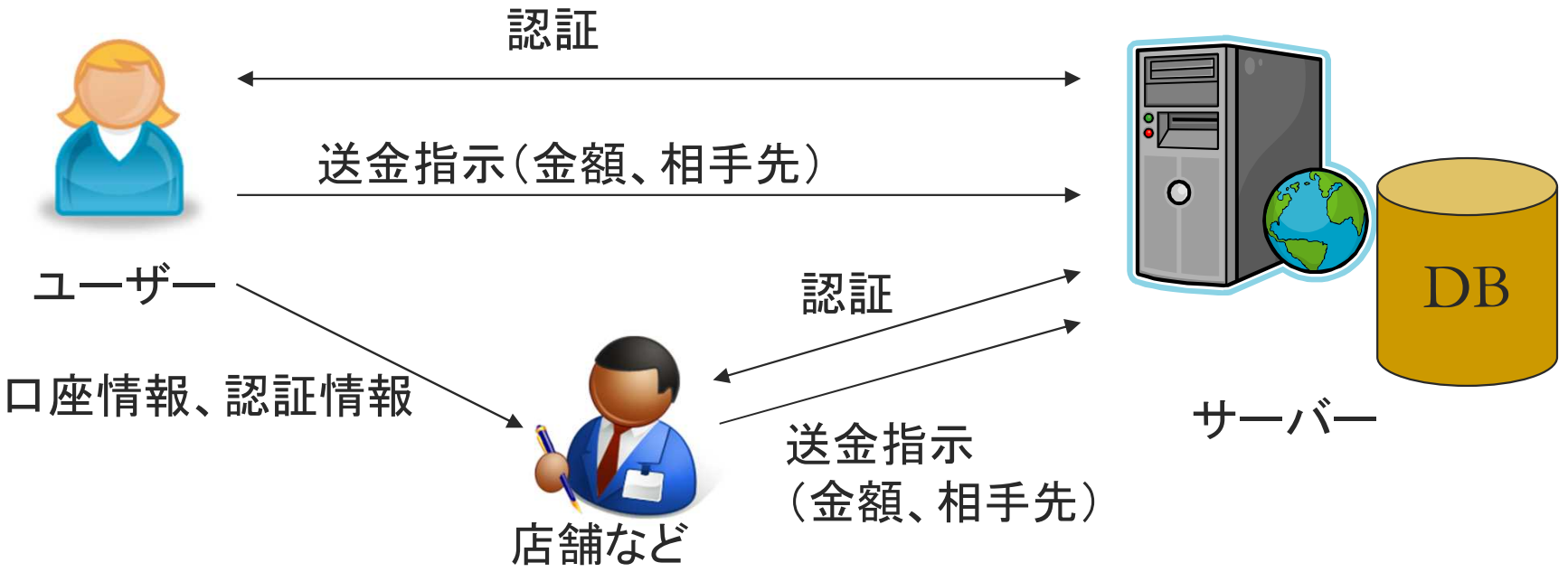
- 独立性：情報のみで価値を持つ
  （物理媒体に依存しない）
- 安全性：コピー、偽造、二重使用ができない
- プライバシー：利用者の購買情報が漏れない
  （一方で、マネーロンダリング等、犯罪利用への対策も必要）
- 転々流通性：不特定相手の支払いに利用でき、他者に譲渡（移転性）することができる
- その他：
  - オフライン支払い（センターへの問合せ不要）
  - 分割可能性（複数回に分けて使える←現金は持っていない性質）

電子マネーの実現（端末型、残高管理方式）



- 実現は比較的容易だが、店舗側の設備投資が必要。
- 安全性は、ICカードの耐タンパ性に依存
  （ISO/IEC14443 TypeA/B, ISO/IEC18092 FeliCaなどの規格がある）
- ホスト側の不正に対応しにくい（架空入金、二重支払い等）
- 移転性（ユーザ間でのやり取り）の実現は困難

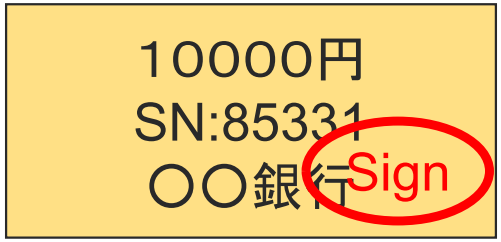
電子マネーの実現（サーバー型）



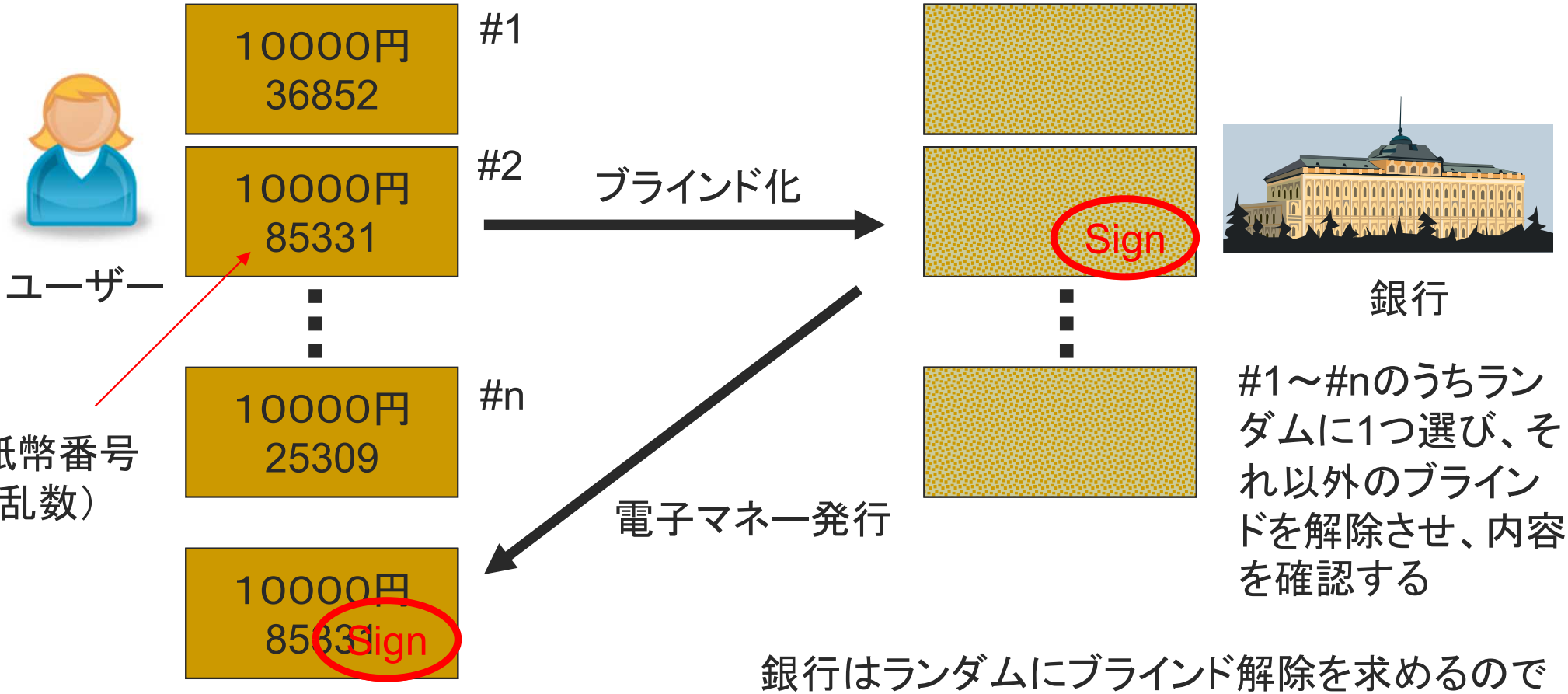
- 実現は比較的容易。ユーザーが送金操作をすれば店舗側の設備不要
- 安全性はサーバーのセキュリティ、認証による
- サーバ側での不正には対応できない
- サーバは、全ての購買、送金記録を把握できる
- 送金情報（QRコード）の盗み見、偽装等の問題がある

電子マネーの実現（電子紙幣方式）

- 発行者（銀行等）の電子署名付きの電子紙幣
- 必ずしも耐タンパデバイスが必要ない
- 移転性（転々流通性）が実現しやすい
- 計算量が多い
- 分割可能性の実現が難しい
- プライバシー保護対策が必要
- 二重支払い対策が必要



電子マネープロトコルの例（電子マネー発行）

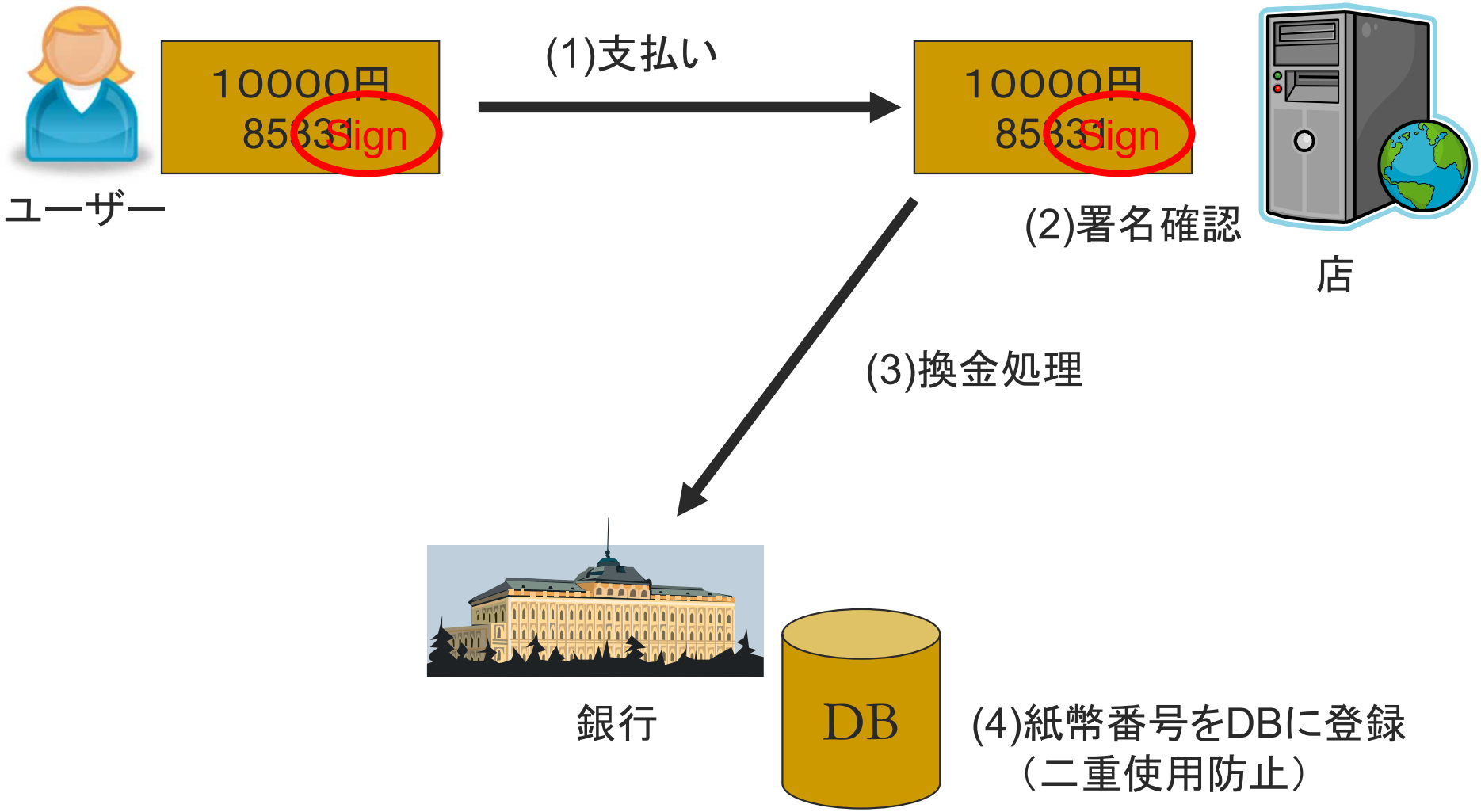


#1～#nのうちランダムに1つ選び、それ以外のブラインドを解除させ、内容を確認する

プライバシー保護のため、紙幣番号からユーザーの使用履歴が辿れないようにしたい

銀行はランダムにブラインド解除を求めるのでユーザーが銀行に不正なデータに対して署名をさせることは困難。

電子マネープロトコルの例（電子マネーの使用）



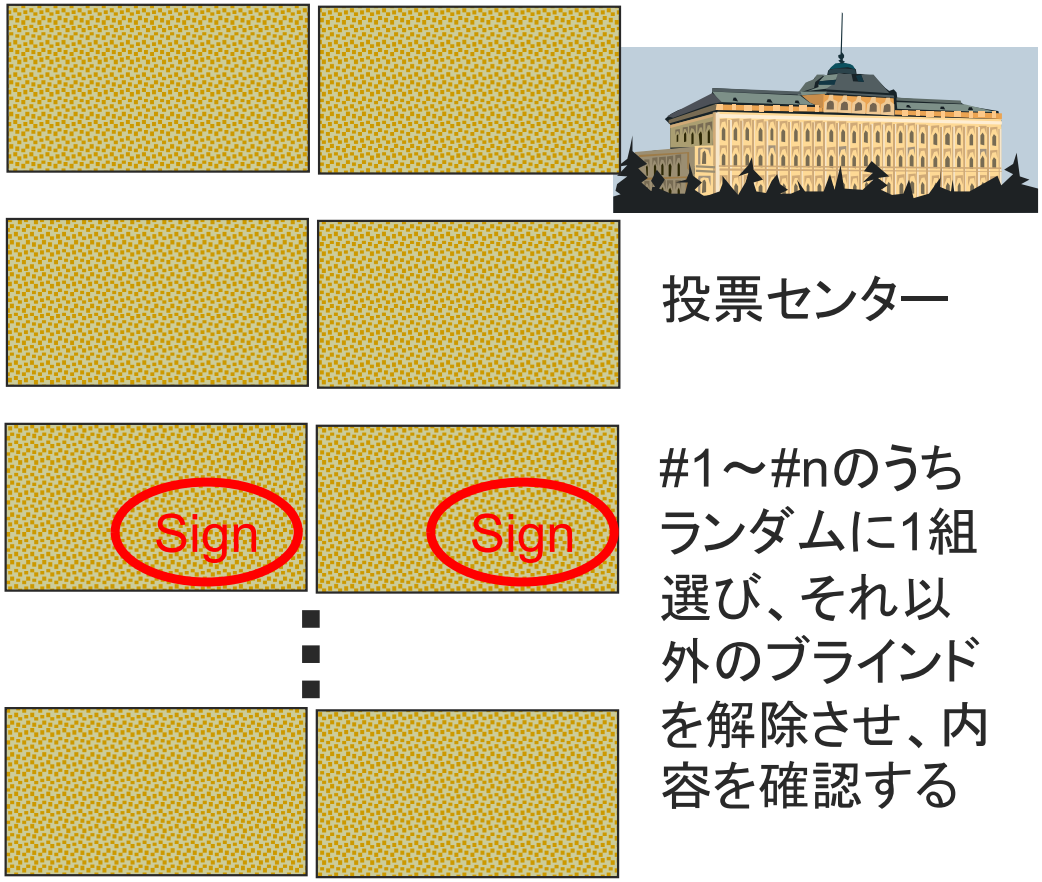
電子投票プロトコルの例（投票用紙の発行）

投票者

賛成	反対	
71109	71109	#1
98785	98785	#2
89977	89977	#3
13400	13400	#n

投票ID（乱数）

ブラインド化



投票センター

#1～#nのうちランダムに1組選び、それ以外のブラインドを解除させ、内容を確認する

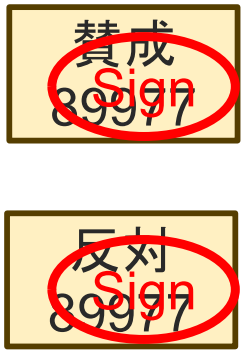
Sign Sign

ブラインド解除

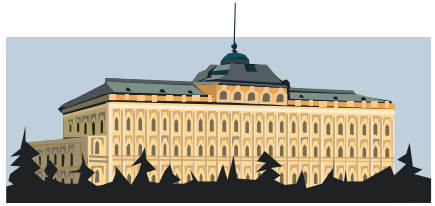
（注）事前に投票者の有権者認証が行われているものとする

電子投票プロトコルの例（投票および集計）

投票者

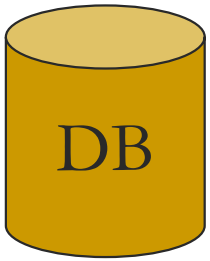


匿名通信路



投票センター

1. 署名を確認
2. 投票IDがDBに登録されていないか確認
3. 投票IDをDBに登録
4. 投票内容をカウント



- 投票用紙の発行時にブラインド署名しているので、投票センターは、投票IDと投票者を紐づけられない
- 投票済みの投票者が再度投票しても、投票IDが既に登録されているので拒否される
- 投票者が自分の意志で投票しているか（脅迫、強要されていないか）、確認する必要がある