SCIS 2011 The 2011 Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics, Information and Communication Engineers

暗号プロトコルの社会実装に向けた課題と解決の方向性 - エストニアにおけるケーススタディ -

Issues and Directions for Implementing Cryptographic Protocols to Society: The Cases in Estonia

松尾 真一郎 * Risto Laanoja †
Shin'ichiro Matsuo

あらまし 現実社会の様々なセキュリティの課題を解決するために，認証などの基本的な機能から，電子マネー，電子投票に至るまで，様々な優れた暗号プロトコルが研究，提案されている．一方で，それらのプロトコルは，必ずしも社会実装されて広く使われているわけではない．本発表では，PKI や電子投票などが広く普及しているエストニアにおいて，暗号プロトコルの設計，実装，普及の経緯と現状の課題を紹介し，日本において電子投票などの暗号プロトコルが普及するために必要な解決を示す．

キーワード 暗号プロトコル，社会実装，電子投票，PKI

1 はじめに

1.1 研究の背景

インターネットの発展とともに，インターネットを介して利便性の高いサービスを安全に実行するために，様々な暗号プロトコルに関する研究や実装が行われている．例えば，電子マネーや電子投票などはその例である．これらの研究では，現実的なセキュリティ要件を満たすプロトコルから，研究の観点で想定しうる全ての安全性に対する脅威に対応するための（安全性の観点で）究極的なプロトコルに至るまで，様々な角度で研究がなされている．

（学術的に）十分なセキュリティを有する暗号プロトコルの研究が盛んになされている一方で，それらのプロトコルが現実に社会に実装されて利用されるケースは少ない．社会実装される前段階として，想定される脅威について非常に慎重な議論が交わされる一方で，社会的に必要とされる性能要件や，経済的に合理性を持った運用要件などを満たす最適解を導出することができないことが大きな原因であると考えられる．

諸外国において暗号技術や暗号プロトコルを応用したサービスが展開される一方，暗号技術の研究では世界をリードする日本においてその研究成果を社会実装に結びつけられていないとすれば，それは大きな問題である．例えば，日本においては GPKI や公的個人認証サービスを始めとして，暗号や電子署名といった基本的な暗号処理のための基盤が整備されながら，それらの基盤を活用するアプリケーションの利用は伸び悩んでおり，その鍵となる住民基本台帳カードの発行枚数も伸びていない．また，90 年代より，従来の現金に置き換わる電子マネーの研究や，インターネットで選挙が可能になる電子投票プロトコルの研究も盛んに行われている．しかし広く使われている電子マネーのサービスは従来の現金よりも軽いセキュリティ要件に基づく技術であり，電子投票においては投票所タイプの電子投票の実験が過去に行われたが情報システム的における問題で実験が進まず，インターネット投票を実現するにはまだまだ道半ばという状況である．

そこで，暗号プロトコルにおける先端的な研究と，社会実装に適した技術の構築という観点で，“最適解” を導出するための取り組みが必要であり，そのために暗号プロトコルの研究を社会に反映させていく方法を考えることが重要である．

1.2 本研究の貢献

本研究では，社会実装に適した暗号プロトコルを研究すると同時に社会実装を促進する “最適解” を求めるための指針を少しでも得るべく，暗号プロトコルの社会実装という観点で世界的にも最先端を進んでいるエストニ

* 情報通信研究機構, 東京都小金井市貫井北町 4-2-1, National Institute of Information and Communications Technology, 4-2-1, Nukui-kitamachi, Koganei-shi, Tokyo, Japan
† Guardtime AS, Tammsaare Tee 60, 13316 Tallinn, Estonia

アにおいて，どのように社会実装される暗号プロトコルが検討され，それがどのように市民に受け入れられ，どのような問題が認識されて，どのように解決したのかについてのベストプラクティスを調査した．日本において活用が進んでいない（国民的）PKI については，エストニアにおいてほぼ全員の国民が利用しており，特にインターネット投票についてもエストニアでは 3 度の大規模なインターネット投票を実施している．本稿では，インターネット投票を中心に基盤となる PKI も含め，エストニアでの検討，実施，課題解決の状況を紹介し，日本における状況と比較することで，将来の日本における社会実装に対して，暗号プロトコル研究において考慮すべき点を提言する．

2 エストニアにおける暗号プロトコルの社会実装

2.1 ID カードと PKI

エストニアでは PKI に基づく ID カードが，罰則規定はないものの義務化されており，ほぼ全ての国民と在留外国人が所有している．

エストニアの PKI は，民間の CA を政府が常に監査できる体制をとることで構築されている．制度上は複数の CA が存在しえるが，現実には SK というエストニア国内の巨大企業が出資した CA のみが存在し，ID カードの唯一の CA となっている．SK は，ID カードの他に，一般的な Web サーバなどに用いる公開鍵証明書，Mobile-ID と呼ばれる携帯電話等に用いられる公開鍵証明書，OCSP サーバなどへの公開鍵証明書を広く発行している [3]．

ID カードは RSA 暗号/署名を演算する機能を持ち，そのアプリケーションとして電子署名を付与するための署名機能と，認証を行うための機能を持っている．これら 2 つの機能に対して，異なる秘密鍵と公開鍵証明書が格納されている．

ID カードの利用対象となるサービスは，民間を含めて非常に広く取られている．主な応用は以下の通りである．

- 公的サービスにアクセスする際の認証
- 税金に関するサービス
- インターネット投票（後述）
- 医療情報へのアクセス
- 銀行サイトへのアクセスの際の認証
- 一般的なポータルサイトへアクセスする場合の認証
- PC のデスクトップにおける暗号化，署名
- 契約書に対する署名

特に，認証におけるサービスが公的機関だけではなく，民間でも幅広く利用されている．その大きな理由は，CA である SK が署名検証時に利用する OCSP のサーバへのアクセスを公開していること，さらに ID カードを利用するアプリケーションを構築する際に必要なライブラリやドライバを一般に公開しており，誰もが自由にアプリケーションを構築できるようになっている点が挙げられる．これらのドライバは Windows だけでなく，MacOS や Linux など，幅広いプラットフォームをサポートしている．

ID カードの取得費用自体は日本の住民基本台帳カードより少し高い程度であるが，IC カードのリーダライタについては，90 エストニアクローン（約 630 円[1]）となっている．しかし，ID カードの利用自体を金融機関がバックアップしているために，ほぼ無料で入手できることが多い．

罰則規定がないにも関わらず，エストニアにおいて ID カードが普及した要因は，その利便性にある．エストニアで生活する際に，ID カードを所持しないことで受ける不利益はほとんど存在しない．エストニアで（例えば銀行口座を開設する際に）身元確認の書類として利用できるのは，パスポート，運転免許証，ID カードであるが，ID カードが配付され始めた当時，運転免許証のサイズが非常に大きく持ち運びに不便であったため，共通の身元確認書類として ID カードが非常に重宝された．また，先に述べた理由により，民間における認証において ID カードが利用できる機会が多い．例えばオンラインバンキングにおいて，ID とパスワードを入力する代わりに ID カードを利用することで，パスワードを記憶することなく簡単に認証が可能になる．民間利用が進むため，利用機会が増えるという好循環を生んでいる．

利便性が高いという事は，一方で紛失などによる損害への対応を考慮する必要がある．一般的には，PKI ではカードの紛失などに対応して，公開鍵証明書の失効によって対応する．エストニアにおいても同様であるが，先述した通りエストニアにおいては 1 つの PKI，1 つの CA によって運営されており，公開されている OCSP サーバによって認証や署名検証処理を行っているため，失効に必要な時間がきわめて短くできる．全人口が 134 万人と小規模であることを考慮する必要があるが，シンプルな PKI の構造が異常系に対するリスクの低減に役立っている．

2.2 インターネット投票

続いて，本節では，[8] にまとめられた，エストニアにおけるインターネット投票仕組みを述べる．

[1] 本稿執筆時点での数字．2011 年 1 月よりエストニアはユーロに移行するため，その後の価格は調査が必要．

2.2.1 概要

エストニアでは，2005 年 10 月に行われた地方議会選挙において，初めてインターネット投票システムにおける選挙が行われた．その際には，9,317 人がインターネットを介して投票を行い，9,287 票の有効投票を得た（インターネット投票の投票率は 0.9%で，期日前投票の 7.2%に相当）．さらに，2007 年 5 月のエストニア議会選挙，2009 年 6 月の欧州議会選挙，そして 2009 年 10 月の地方議会選挙においてもインターネット投票が行われた．2009 年 10 月の選挙では，104,413 人がインターネット投票に参加し，その投票率は 9.5%，期日前投票に占める割合は 44%だった．

エストニア議会における選挙は，日本と同様に複数選挙区が存在し，各選挙区に議員定数が割り当てられている．そのため，選挙のプロセスに対する入力は，各選挙区における立候補者のリストと各選挙区の有権者のリストとなる．有権者は，立候補者のリストから投票したい人物の名前を選択し投票する．選挙期間終了後，集計が行われて，最終的な選挙結果として各候補者に対する得票数が出力される．この結果に応じて，法律が定めるところにより当選人が決定される．

2.2.2 インターネット投票に対する要件

エストニアにおける “選挙” に対する要件は憲法によって以下のように定められている[2]．これらの要件は地方議会選挙においても適用される．

- General and Uniform: 各有権者が投票に当たり等しく同じ手段をとれること．各投票は同じように集計されること．多重投票が許されないこと．
- Secret: 各投票者以外は，それぞれの投票内容を知ることができないこと．
- Freshness: 各投票内容は外部から不正に操作されないこと．

これらの要件は，インターネット投票に対しても同様に適用される．

一方，2.1 に示したように，エストニア国民は国民 ID カード（以下 ID カード）を所有している．ID カードには RSA 暗号を演算できる機能が搭載されている．また，認証用，および電子署名用の RSA 暗号/署名の 2 つの秘密鍵が格納されている．そのため，投票者を認証するための仕組みも ID カードを利用している．インターネット投票における ID カードの利用は，Lipmaa らのリスク分析に基づき [6]，2002 年から法制化されている．

プライバシ以外の要件としては，インターネット投票用のサーバは長時間アクセスできないようにならないこと，また DoS 攻撃などについての対策を持っていることなど，可用性の観点も必要である．これらの対策を講じるとともに，可用性に問題が生じた場合，国家選挙管理委員会（National Election Committee）は，電子投票をキャンセルし，紙の投票へ切り替えるオプションを持っている．

2 重投票を防ぐ観点で，電子投票と紙の投票の両方がなされた場合には紙の投票が優先される．

紙の投票の場合，票の秘匿性と公平性は投票の記入を行う投票ブースによって担保されている．インターネット投票の場合は，このような仕組みを採用することは不可能である．とりわけ，インターネット投票では，票の買収への対策が重要となる．そこで，票の買収の効果を薄めるために，インターネット投票を何度でも行えるようになっている．つまり，何度でも投票を可能にすることにより，最後の投票結果を有効とする仕組みとする．さらに，期日前投票の期間であれば紙による投票を行うことで，電子投票の結果を無効化する機能も付け加える．このことにより，現状の紙による投票と同等の秘匿性と公平性の確保にいつでも立ち戻ることができるようにする．このような投票の手続きは，2005 年に法制化された．ただし，紙による従来の投票では，投票内容の変更ということは想定されていないため，この機能についてはその正当性の議論が盛んに行われた．

2.2.3 システムモデル

エストニアのインターネット投票システムは以下のようなシステムモデルで成り立っている．

Vote Forwarding Server (VFS): 投票者の認証，投票者が所属する選挙区の候補者リストの配布，投票者が電子署名を付与した投票データを受け付けを行う．VFS はインターネットに接続されている．

Vote Storing Server (VSS): 署名された投票データを保管し，集計の前に匿名化を行う．VSS は Firewall に守られたセグメントに配置され，VFS との通信は許可されている．

Vote Counting Server (VCS): 票の集計を行うサーバで，VCS の一部は，投票内容を復号するために RSA 暗号の復号鍵を格納した HSM (Hardware Security Module）として実装されている．この鍵は，選挙ごとに生成される．対応する暗号化鍵（公開鍵）は，後述するクライアントアプリケーション EVCA に含まれている．VCS はスタンドアロンの計算機であり，インターネットには接続しない．VSS と VCS の間のデータの移動は，DVD などの物理的媒体を介して行われる．

[2] エストニアのインターネット投票の法的な分析については [9] に詳しい

e-voting Client Application (EVCA): 複数のプラットフォーム（Windows, Linux, MacOS）で動作可能なクライアントアプリケーションで，VFS と通信を行い，候補者リストのダウンロード，投票の入力，投票データへの署名と VFS への送信を行う．

Auditing Application: 監査ログの完全性をチェックするアプリケーション．インターネット投票システムの各サーバはログファイルを持っており，インターネット投票システムに不正が起きていないことを示すための証拠となっている．

2.2.4 投票プロトコル

エストニアにおけるインターネット投票は以下のプロトコルによって実行される．

Pre-election stage: 全てのサーバに必要なソフトウエアをインストールするとともに，候補者リストと投票者リストをインストールする．EVCA を該当する選挙に合わせて構成し[3]，エストニア選挙管理委員会の電子署名を付与する．

Election stage: VFS へのアクセスが可能となる．投票者は EVCA をダウンロードし，ID カードを用いて認証を行い，投票内容を選択した上で，投票データに対して ID カードを用いて電子署名を付与する．

Revocation stage: Election stage が終了すると投票が締め切られる．全ての投票者のリストが集計され，開票所に送られる．開票所において紙の投票との重複のチェックを行い，重複がある場合には電子投票から取り除かれる．

Tabulation stage: Revocation stage が終了すると，Revoke されていない全ての投票者について，匿名化を行う．匿名化の方法は，暗号化された投票データから電子署名を取り除くことで行う．最終的に，暗号化されたデータを HSM で復号し，集計する．

上記のように，暗号化した投票データに電子署名を付与することで有権者であることの確認と二重投票の防止を図っており，投票データの暗号化により投票内容の秘匿性を保っている．ただし，このままでは選挙管理委員会内部の結託により，容易に匿名性を破ることも可能である．このことを防止するために，(暗号によらない）以下の対策が取られている．

- サーバ側の運用を行う部屋は警察官により厳重に守られており，またカメラにより運用者の行動が監視されている．
- サーバ側の運用は，少なくとも 2 人の選挙管理委員会のメンバが同時に行わないと実行されない．
- 選挙期間中は，公認の監査人がすべての重要なプロセスの監査を行う．
- 集計プロセスは公認のオブザーバとメディアによって監視される．

[3] 鍵ペアの生成と公開鍵の取り込みなどを行う

2.2.5 安全性に関する分析

本方式は，信頼できるサーバの存在を仮定している．この構造では，システム運用者が投票内容の操作や匿名化を破る行為を行うことが可能になる．そのため，前述の暗号によらない対策を徹底することが必要である．

一方で大きな課題となるのは，クライアントプログラムの安全性である．一般的に，投票者が個人で所有している PC が投票に使われることが想定されるが，OS のパッチやウイルス対策ソフトの定義ファイルのバージョンの問題などで，必ずしも安全な状態に保たれている保証はない．そのため，EVCA そのものが問題がある環境で実行されることを想定しないといけない．また，メモリ領域にアクセスできるマルウエアなどが存在する場合，匿名性が失われる可能性もある．電子投票方式そのものの問題ではないが，クライアントプログラムの実行環境を守るために，現在でもコード署名が行われている．しかし，この対策だけではクライアントのプログラム実行環境の問題は解決されているわけではなく，今後投票プロトコルの正当な実行を助ける暗号プロトコルなどを考慮する必要がある．

3 日本における社会実装との比較

3.1 ID カードと PKI

3.1.1 日本における現状

日本における公的な PKI は，GPKI，LGPKI，JPKI の 3 つの PKI で構成されている [2, 5, 4]．GPKi は，電子申請等において申請者から提出された書類，および申請等の結果の通知において，それらの文書のの作成者，および非改ざんの確認を行うために構築されている．LGPKI は，GPKI とほぼ同様の機能を地方公共団体において利用できるようにするために構築されている．また，JPKI は公的個人認証と呼ばれ，住民基本台帳カードを保持している人に対して政府や地方公共団体で実施するサービスにおける認証を行うために構築されている．

インターネット上のサービスにおいて特に重要となるのは JPKI の利用であるが，現状その利用の前提となる住民基本台帳カードの発行枚数は伸び悩んでおり，2010 年 3 月末での公布枚数は 4,447,000 枚（普及率 3.5%）となっている．また，住民基本台帳カード，および公的個人認証を用いて利用可能となるサービスも限定的である．

そのため,（エストニアにおける）ID カードと同等の機能，および PKI の利用が広がっていない．

3.1.2　エストニアにおける特徴

2.1 に示した通り，エストニアにおいては罰則規定はないものの，ほぼ全ての国民が ID カードを所有している．これは，ID カードが政府のみならず，銀行からも強くサポートされていること，開発環境が公開されており民間企業が ID カードを活用するためのハードルがきわめて低い．さらに前述した通り，様々なアプリケーションが存在することによって，ID カード自体の利用のメリットが大きく，それが普及への鍵となっている．アプリケーションにおける連携についても活発に行われており，2011 年には運転免許の取得状況と ID カードの情報のリンクが取られるため，ID カードを所持していれば運転免許証の携帯が不要となる予定である．このように，ID カードを様々な利用シーンにおける認証のインフラとして積極的に活用する意思が強いと言える．

一方で，プライバシ保護に関する事項についてはエストニアにおいて特別な事情があったことを述べる．日本において認証に必要な共通 ID を広く民間にも開放する場合，行動の把握などプライバシに関わる問題が懸念される．しかし，エストニア国民自体が，ID カード導入の際にプライバシ保護の問題に対して強い関心を持っていなかったと言われる．そのため，高い利便性を提供する ID カードが急速に普及したといえる．ただし，近年 ID カードの利用において，プライバシに関する問題を指摘する専門家が現れており，ID カード利用におけるプライバシ問題が政府内でも議論され始めている．現状，プライバシ保護に関するコンセンサスは得られていないとのことであるが，現在の ID カードの体系にどのようにプライバシ保護機能を付加していくのかが議論の対象になると考えられている．

3.2　電子投票

3.2.1　日本における現状

日本における電子投票は,「指定された投票所で投票するタイプ（第 1 段階）」,「指定された投票所以外の投票所でも投票できるタイプ（第 2 段階）」,「投票所以外で,個人の PC などでも投票できるタイプ（第 3 段階）」の 3 つのステップで進めていくことを念頭に検討されてきた [7]．現状の法制度では，地方自治体の選挙に限り，該当する地方自治体が希望すれば実施することができる．過去に行われた電子投票は全て第 1 段階の電子投票であり，エストニアで実施されているようなインターネット投票（第 3 段階に相当）は実施されていない．

日本で最初の電子投票は，2002 年 6 月に新見市で行われ，これまでに計 13 回の電子投票が実施されている．これらの電子投票システムは，指定された投票所で投票内容をタッチパネルなどで入力する方式であり，複雑な暗号プロトコルが実装されているわけではなく，既存の紙による投票のごく一部を電子化したものとなっている．しかし．投票そのものの処理で機器のトラブルが発生したり，電子投票そのものを実施するコストが安価ではないため，電子投票自身の実施が減っているのが現状である．そのため，第 3 段階のインターネット投票へ発展していく目処が立っていない．

3.2.2　エストニアにおける特徴

電子投票に関して，エストニアで起こったことの大きな特徴は，投票所タイプなどの中間解を経ずに，最初からインターネット投票を実施することを決めたことである．これは，電子投票の目的として，投票集計に関するコスト削減だけでなく，投票率の向上が民主主義の質の向上につながるという点を大きく掲げたことに関係する．

さらに，暗号プロトコルの設計という観点においては，既存のシステムとの互換性など，社会実装の観点から「既存の仕組みで行えるセキュリティ対策はその対策をそのまま活用し，新たに暗号技術が必要となる部分にのみ暗号プロトコルを適用する」という考え方を取ったことが特徴的である．

インターネット投票に関する安全性要件は,「投票権を持たない人の投票の禁止」,「二重投票の禁止」,「匿名性の確保」,「票の買収の排除」などがある．票の買収の排除に関しては，投票のやり直しを認めることにより買収を企てる攻撃者にとってのメリットを大幅に削減した．また，匿名性の確保においては，Mix-net のような複雑なシステムを採用せずに，運用者の行動を録画を含めて監視できるような運用対処を行っている．その結果，暗号に関わる処理が必要なのは，投票データの暗号化と投票権の確認のための電子署名のみとなっている．電子署名そのものも，ID カードのインフラをそのまま流用できるために，電子投票システム構築に関わるコストを大幅に削減することに成功している．結果として，このような軽い暗号プロトコルにすることにより，集計処理全体は 10 万人規模の投票でも 20 分を切っている．

さらにエストニア国民が，中央のサーバの信頼に大きく依存する（暗号学者にとっては仮定が強すぎる）システムを受け入れた大きな理由も，プロトコルのシンプルさにある．システム管理者が不正を行わないことを，監査やビデオ撮影によって担保する（不正なシステム管理者の不正に対するインセンティブを低下させる）という工夫がある．Mix-net のような複雑な仕組みは一般の国民には理解しづらいという意見も多く存在した．仮に，Mix-net，ブラインド署名，準同形暗号のような特別なプロトコルを導入した場合，既存の ID カードのインフ

ラやPKIのインフラのみでは，そのような処理を賄うことができずに，追加のシステム構築と運用の費用がかかることになる．問題が発生したら紙の投票にいつでも立ち戻ることができるという工夫を含めて，極力既存のインフラとの親和性を保つことが重要であることがわかる．

4 日本で “使われる” 暗号プロトコルを設計するために

3.2.2 で述べたように，社会実装に適した暗号プロトコルは，(1) 既存のサービスを提供するインフラとの親和性，(2) 利用者に理解しやすいシンプルさ，(3) 追加のシステム構築コストを発生させないようなシンプルさが重要なポイントとなる．それらのポイントを満たすためには，複雑な暗号プロトコルを設計するのではなく，必要なセキュリティ要件のうち既存のインフラや運用を活用することによって暗号技術の利用が不要なものについては，そのようなセキュリティ対策を採用するということが重要になる．

例えば，エストニアのインターネット投票の例を見ると，投票内容の変更を認めることにより票の買収を企てる攻撃者のインセンティブを低下させたり，運用のビデオ撮影や監査のこまめな実施により，運用者の内部犯行のインセンティブを低下させるシステム設計となっている．このように，攻撃者のインセンティブを分析して，様々なセキュリティ対策によってそのインセンティブを低下させることが大きなポイントとなる．

暗号プロトコル研究の世界では，2002 年頃からゲーム理論に基づく安全性モデルの研究が盛んになっている．既存の研究の多くは，暗号プロトコルという狭い領域に閉じた中で厳密な安全性定義を試みている．しかし，社会実装に必要な暗号プロトコルの設計においては，サービスで必要とされるセキュリティ要件と攻撃者のインセンティブを入力として，ゲーム理論的な観点でリスク分析を実施し，既存の対策によって攻撃者のインセンティブの低下を図れない部分について，暗号技術的解決を行うというアプローチが有効であると考えられる．

エストニアのインターネット投票については，2007 年に Buldas らによってゲーム理論的なアプローチで安全性の分析が行われている [1]．エストニアのインターネット投票の基本的なスキームの設計において，前もって学術的な体系をもってゲーム理論的なセキュリティ設計が行われたわけではないようであるが，実際に設計されたシステムは，上記の考え方おいて（結果的に）合理的な設計となっていると考えられる．今後の暗号プロトコルのセキュリティ要件の抽出において，システム設計におけるゲーム理論的リスク分析のような考え方の体系化と実践が重要になってくると考えられる．

5 まとめ

本稿では，利便性と安全性を兼ね備えた暗号プロトコルが社会実装されるために考慮すべき事項について，エストニアにおけるインターネット投票の事例のケーススタディを実施した．エストニアにおける検討状況を日本にそのまま当てはめることはできないが，インターネットを利用しない既存の仕組みとの互換性を確保すること，そのために既存の仕組みで対応可能な部分と暗号プロトコルを必要とする部分の分析を十分に行うことが，“使われる” 暗号プロトコルになるための 1 つの重要な取り組みであることを示した．

謝辞

本研究，およびエストニア国内での調査を実施するに当たり，タリン工科大学，およびタルトゥ大学の Ahto Buldas 教授に非常に有益な議論と多大なる協力をいただいた．ここに感謝の意を表する．

参考文献

[1] A. Buldas, T. Magi, “ Practical security analysis of e-voting systems,” In the Second International Workshop on Security (IWSEC) 2007. Nara, Japan, October 29-31, 2007. LNCS 4752, pp.320-335, 2007.

[2] 総務省行政管理局, “政府認証基盤 (GPKI) について,” http://www.gpki.go.jp/documents/gpki.html.

[3] I. Jung, “- Presentation about Estonia from Porvoo 16 meeting -,” http://www.ants.interieur.gouv.fr/evenements /IMG/File/05%20P16_Estonia.pdf

[4] 公的個人認証サービス都道府県協議会, “ 公的個人認証サービスとは, ” http://www.jpki.go.jp/jpkiguide/index.html.

[5] 総合行政ネットワーク運営協議会, “地方公共団体組織認証基盤,” http://www.lgpki.jp/.

[6] H. Lipmaa and O. Murk, “E-valimiste realiseerimisvoimaluster analuus,” (Analysis of e-voting implementation choices, in Estonian); 2001; http://www.vvk.ee/public/dok/lipmaamyrk.prf.

[7] 松原, 松尾, 佐古, 大塚, “電子投票と暗号技術,” 第 21 回理財工学研究センターシンポジウム資料集, 2004, 東京工業大学

[8] S. Heiberg, “Internet Voting - the Estonian Experience,”, Proc. in Information Security Summit 2009.

[9] 湯淺墾道, “エストニアの電子投票, ” 社会文化研究
所紀要 65 号