コンピュータセキュリティ　10－31
（2000．　7．25）

投票所方式による電子投票システム

田中　利清　　白石　旭

ＮＴＴアドバンステクノロジ株式会社

tanaka@saki.netwk.ntt-at.co.jp　akira@saki.netwk.ntt-at.co.jp

あらまし

近い将来における、国政選挙や地方自治体選挙への適用を目標に、投票所に設置した電子的端末装置と開票所の集計装置とをオンラインで結び、開票稼働の削減、開票時間の短縮、無効票の消滅を狙いとした「投票所方式による電子投票システム」を研究開発した。本稿では、本システムに要求されるセキュリティ課題とその対策手段、プロトタイプシステムの機能構成、および今後の拡張予定について報告する。

キーワード　電子投票、投票所、投票チケット、暗号

Polling-site electronic voting system

Toshikiyo Tanaka　Akira Shiraishi

NTT Advanced Technology

tanaka@saki.netwk.ntt-at.co.jp　akira@saki.netwk.ntt-at.co.jp

Abstract

With a view to applying it to national and local assembly elections in the near future, we have developed a “polling-site electronic voting system,” which connects electronic terminals at polling sites to the ballot counting site online. Its purpose is to reduce the workforce and time needed for ballot counting as well as to prevent invalid ballots. This paper discusses security issues to be considered in the system and their solutions, the functional structure of a prototype system, and plans for future extensions.

key words　electronic voting system, polling site, voting ticket, cryptography

1．はじめに

近年、社会の各分野において情報の電子化が進み、ネットワークが飛躍的に社会に浸透している。このような背景のもとで、選挙業務に対しても、これを電子化することによる開票稼働の削減および開票時間の短縮が期待されている。既に、欧米を始め世界各国において電子投票システムの開発が進められ、一部の国においては実際の選挙に適用され始めている。

一方、インターネットの発展に伴い、各家庭のパソコンから投票を行うことも可能な環境となり、米国の大統領予備選挙にも部分的に適用されている。ただし、家庭と開票所をオンラインで結んだネットワーク方式の電子投票を我が国の国政選挙や地方自治体選挙に適用するためには、本人認証の方式、本人認証のための情報を格納するICカードなどの導入手段、脅迫や買収を防止する方式、通信履歴やアクセスポイントなどから投票者を特定することを防止する無記名性の確保方式など、解決すべき問題が山積しており、時期尚早と考えられる。

本研究開発においては、近い将来における、国政選挙や地方自治体選挙への適用を目標に、投票所に電子的な端末を設置し、投票所と開票所とをオンラインで結ぶ、「投票所方式による電子投票システム」を研究開発した。

本システムにおいては、現行選挙と同様の投票所に電子端末を設置し、投票者は投票所に出向いて投票を行う。本人認証は現行選挙の方式を踏襲することとし、例えば投票所の受け付けにて各投票者宛に郵送された投票整理券の提出を求め、それと選挙人名簿とを突き合わせることにより本人認証を実施する。投票者は、本人認証終了後、現行選挙の投票用紙の代わりにICカード（投票カード）を受け取り、投票カードを投票端末に挿入して投票を行う。投票カードに格納された投票情報は、投票所の出口端末からオンラインで集計サーバへ送信され、集計サーバのデータベースに格納される。投票締切後、集計サーバにてデータベース内の投票情報が集計され、投票結果が出力される。

本研究開発により期待される効果としては、以下の3点が考えられる。

- 投票所における投票の運用および不正行為の監視等を行う、投票管理者とその補助者や立会人の稼働は現行選挙とほぼ同じであるが、各投票所と開票所をオンラインで結ぶこと、および開票処理をコンピュータ上で実施することにより、投票所から開票所への投票箱の運搬、および開票所における開票作業等の選挙運営に係わる稼働を大幅に削減することができる。
- また、各投票所と開票所をオンラインで結ぶこと、および開票処理をコンピュータ上で実施することにより、投票締切から開票結果判明までの時間を大幅に短縮することができる。
- 公職選挙法の改正を前提とするが、現行選挙における投票用紙への候補者名記入の代わりに、電子端末の画面上に表示した候補者の中から選択する方式を採用することにより、現行選挙で発生しやすい誤記や判読不能等による無効票が無くなる。

本システムは、昨年度実施した第1期と、本年度実施している第2期に分けて開発を進めている。第1期においては、町村規模の選挙への適用を目標として、電子投票プロトコルの検討を行い、プロトタイプソフトウェアの開発を行った。第2期においては、国政選挙にも適用することを目標として、電子投票プロトコルの拡張を行い、プロトタイプソフトウェアへ反映するとともに、第1期ではFDを使用したセキュリティカードのICカード化と投票端末画面のGUI化を予定している。また、有権者が投票カードで個人を特定できないことを納得できる方式を検討する。

本稿においては、第1期での主要検討内容、プロトタイプソフトウェアのシステム構成、および第2期で予定している拡張内容について報告する。

2．検討内容

本研究開発の目標は、国政選挙や地方自治体選挙

に適用可能な電子投票システムを研究開発することである。選挙は国民が政治に参画する貴重な機会であることから、二重投票など不正行為が防止でき、公平であり、プライバシーが保証されるなどの安全性の高いシステムが要求される。そのため、この要求条件を満たす電子投票プロトコルを検討し、その実現性を検証するとともに電子投票システムの実装方法を確認するためにプロトタイプソフトウェアを開発した。

主な検討項目を以下に示す。

① 無記名性の実現

異議申し立てや二重投票の防止を実現する上で、無記名性を損なわない方式を検討する。即ち、異議申し立てや二重投票の防止を実現するためには、投票情報を識別する手段が必要であるが、この投票情報識別手段から投票者が特定され、無記名性が損なわれてはならない。そのため、無記名性を損なうことなく、投票情報を識別する手段を実現する方式を検討する。

② 異議申し立ての実現

投票所内に設置する受付端末、投票端末、出口端末は、投票者の目の届く範囲にあるため、不正行為が行われないように投票者本人が監視できる。これに対して、集計サーバは、投票者の目の届かない場所に設置して運用されるため、投票者の不信を招き易い。このため、立会人や投票者が関与できる出口端末にて、集計サーバで投票情報の削除や改ざんや水増しが行われていないかを監視し、不正を検出した場合には集計サーバに対して異議申し立てを行う方式を検討する。

③ 二重投票の防止

一人の投票者が二票以上の投票を行う二重投票を防止する方式を検討する。主な二重投票の手段としては、一枚の投票カードを用いて二回投票する、複写などにより偽造投票カードを作成して密かに投票所に持ち込む、などが考えられる。

④ 安全性の実現

上記の無記名性や異議申し立ての実現および二重投票の防止のために、暗号・認証技術を使用する。この暗号・認証で使用する各種の鍵情報を安全に保管および配布する方式を検討する。

2．1 無記名性の実現

無記名性を保証するために、投票カードには投票者を特定できる情報を一切格納しない。

ただし、異議申し立ておよび二重投票の防止を実現するためには、個々の投票情報を識別するための手段が必要である。これを無記名性を損なうことなく実現するために、投票端末で乱数を生成し、この乱数を投票情報を識別するための手段として使用する。

なお、投票チケットサーバで乱数を生成し、これを投票チケットに包含する方式も考えられるが、この投票チケットが格納された投票カードが複製されて、正規の投票カードに混入された場合、正規に投票した投票情報が多数無効化されることになるため、本システムでは、投票者が投票端末で投票を行い、投票情報が生成される段階で乱数を生成して付加する方式を採用した。

選挙区の有権者数に対して、乱数の桁数を十分大きく取ることにより、同一選挙区内の複数の投票端末で、個別の乱数の種のもとで、同一の乱数が生成される確率は極めて小さくなる。しかし、一票の票の重みを考慮した場合、いかに確率が小さくても同一の乱数が生成されたことにより、ある投票情報が無効化されることは許されない。このため、投票チケットサーバにて投票チケットを生成する時に、投票チケットにシーケンス番号を包含し、このシーケンス番号を、万一乱数が一致した場合に、投票情報をさらに識別するための手段として使用する。

ただし、受付端末の操作者が投票チケット内のシーケンス番号を見ることができると、投票者とシーケンス番号、シーケンス番号と投票情報との対応付けにより、投票者と投票情報とのマッピングが可能となり、無記名性を損なう恐れがある。このため、投票チケット内のシーケンス番号は暗号化して、投票所受け付けの管理者に見えないようにし、投票端末のみで復号する。

なお、乱数を用いず、このシーケンス番号だけで投票情報を識別する方法も考えられるが、上記の乱数の場合で議論したのと同様、この投票チケットが格納された投票カードが複製されて、正規の投票カードに混入された場合、正規に投票した投票情報が多数無効化されることになるため、本システムでは、乱数とシーケンス番号の二つで投票情報を識別する方式を採用した。

2．2　異議申し立ての実現

投票所内の受付端末、投票端末、出口端末は、投票者の目の届く範囲にある。しかし、集計サーバは投票者の目の届かない場所に設置されるため、投票者は集計サーバの不正処理が心配となる。現行選挙では、開票時の不正を監視するために立会人を置くとともに、それ以外の投票人の傍聴も可能である。本システムにおいても、立会人の監視の下で開票が行われることを前提としているが、集計サーバの処理内容に不正が無いかを投票者自身で納得できない。このため、投票者も監視できる出口端末で、集計サーバによる投票情報の削除、改ざん、水増しを監視する異議申し立ての方式を実現した。

異議申し立ての実現方式として、以下の２つの方式が考えられる。なお、以下の議論における投票情報は、投票した候補者名とともに、上記の乱数およびシーケンス番号を含むものとする。また、集計サーバ署名は、集計サーバが出口端末から受信した投票情報に対し、集計サーバ署名秘密鍵を用いて生成したデジタル署名である。

- 直接方式・・・投票者は、投票情報および集計サーバ署名を格納した投票カードを持ち帰る。集計サーバは、集票してデータベース上に保持している全ての投票情報の一覧を、FTP 等により一般投票者に公開する。投票者は、公開された投票情報の一覧の中に自分の投票情報があることを確認する。自分の投票情報が公開された投票情報の一覧に存在しない場合、集計サーバに異議申し立てを行う。集計サーバは、異議申し立てに添付された集計サーバ署名を検証し、集計サーバ署名が正しければ、異議申し立てを認めて、異議申し立ての投票情報をデータベースに追加する。
- 代理人方式・・・投票者は、投票情報および集計サーバ署名を格納した投票カードを投票箱に投函する。集計サーバは、集票してデータベース上に保持している全ての投票情報の一覧を、FTP 等により代理人に公開する。代理人は、投票箱に投函された全ての投票情報が、公開された投票情報の一覧の中にあることを確認する。投票情報が公開された投票情報の一覧に存在しない場合、集計サーバに異議申し立てを行う。集計サーバは、異議申し立てに添付された集計サーバ署名を検証し、集計サーバ署名が正しければ、異議申し立てを認めて、異議申し立ての投票情報をデータベースに追加する。

上記２方式のうち、直接方式にて異議申し立てを行った場合、異議申し立てをした人が誰に投票したかが分かってしまうため、無記名性を損なう。また、投票者が持ち帰った投票カードを証拠として、票の買収あるいは脅迫の行われる危険がある。従って、本システムにおいては、代理人方式を採用した。ただし、代理人が人手で上記投票情報一覧のチェックを行うことは、現行選挙における開票と同等の稼働および時間を費やすこととなり、電子投票を導入する意味が無くなる。このため、本システムでは、出口端末が代理人の処理を実行する方式とした。

異議申し立ての具体的実現方式を以下に示す。

①　投票時

- 出口端末は、投票カードから投票情報を読み出し、投票情報を集計サーバへ送信する。
- 集計サーバは、出口端末から受信した投票情報に対する集計サーバ署名を生成し、集計サーバ署名を出口端末へ送信する。また、投票情報をデータベースに格納する。
- 出口端末は、上記投票カードから読み出した投票情報と、集計サーバから受信した集計サーバ署名を、データベースに格納する。

②　開票時

- 集計サーバは、データベース内の投票情報の一覧をFTPで公開する。
- 出口端末は、自データベース内の投票情報の全てが、集計サーバから公開された投票情報一覧の中に存在していることを確認する。全て存在している場合は、承認情報を集計サーバへ送信する。存在しない投票情報を検出した場合、該当の投票情報と集計サーバ署名を含む異議申し立て情報を集計サーバへ送信する。
- 集計サーバは、出口端末から異議申し立て情報を受信した場合、異議申し立て内の集計サーバ署名を検証し、署名検証に成功した場合は、異議申し立てされた投票情報をデータベースに格納し、署名検証に失敗した場合は、対応する投票情報を破棄する。
- 集計サーバは、再度、データベース内の投票情報の一覧をFTPで公開する。
- 出口端末は、自データベース内の投票情報の全てが、集計サーバから公開された投票情報一覧の中に存在していることを確認する。全て存在している場合は、承認情報を集計サーバへ送信する。存在しない投票情報を検出した場合、凍結情報を集計サーバへ送信する。
- 集計サーバは、出口端末から凍結情報を受信した場合、開票処理を凍結する。(この後、開票管理者による調査が行われる。)

上記異議申し立て方式では、集計サーバによる投票情報の削除と改ざんは検出できるが、水増しは検出できないため、以下の手順を追加する。

- 出口端末による、1回目の投票情報チェック結果の集計サーバ送信情報(承認情報または異議申し立て情報)に、自出口端末の投票情報数を包含する。
- 集計サーバによる、2回目の投票情報一覧の公開時に、全ての出口端末から受信した各出口端末の投票情報数を包含する。
- 出口端末は、2回目の投票情報チェック時に、集計サーバから公開された自出口端末の投票情報数が正しいこと、および集計サーバから公開された投票情報の総数が公開された各出口端末の投票情報数の合計に等しいことを検査し、不一致を検出した場合には、凍結情報を集計サーバへ送信する。(この後、開票管理者による調査が行われる。)

2．3　二重投票の防止

投票者が当該投票所で投票をする資格があり、かつ1回目の投票であることの確認は、現行選挙の方式を踏襲することとし、例えば投票所受け付けにて各投票者宛に郵送された投票整理券の提示を求め、投票管理者がその投票所に割り当てられた選挙人名簿に投票済みの印を記入することにより行う。

その後、本システムでは、上記確認の終了した投票者に対して、投票管理者が受付端末で受付端末署名を書き込んだ投票カードを交付する。この受付端末署名は、投票端末において検証されるため、事前に投票チケットを複写するなどして偽造した投票カードを投票所に持ち込んでも、受付端末署名が書き込まれていないために投票端末で偽造が検出され、投票することができない。なお、受付端末署名は、受付端末が、投票カードから読み出した投票チケットに対し、受付端末署名秘密鍵を用いて生成した署名である。

ただし、投票端末で受付端末署名が無いことを検出した場合、あるいは受付端末署名の検証に失敗した場合、投票カードの不良やシステムの動作不良と偽造カードとの切り分けを、投票所で即座に実施することは運用的に困難であることから、投票を行う権利を尊重して、投票カードを再交付せざるを得ない。このように、受付端末で最初に交付した正規の投票カードと、偽造カードの代わりに再交付された2枚目の正規の投票カードを使用して、二重投票が行われる危険がある。本システムでは、投票所の出口で投票管理者が投票者から投票カードを1枚のみ受け取り、その投票カードを出口端末に挿入し、投票情報を集計サーバへ送信するので、2枚の投票カードの使用による二重投票を防止することができる。

また、１枚の投票カードを用いて２回投票しようとしても、１回目の投票時に、投票端末にて投票カード内の投票チケットと受付端末署名を消去するため、２回目の投票の開始において、投票端末に投票を拒否される。

更に、選挙毎に決定する選挙識別子に対して投票チケットサーバ署名秘密鍵を用いて生成した投票チケットサーバ署名を投票チケットに包含することにより、投票チケットの偽造を困難にしている。

また、回線上の投票情報のパケットをコピーし、通信処理上のセキュリティホールを見つけて、同一の投票情報を送信することにより、集計サーバのデータベースに同一の投票情報を複数格納することが考えられる。このため、集計サーバは、開票の始めに乱数およびシーケンス番号の照合を行うことにより、データベース上の投票情報の重複を排除する。

２．４　安全性の実現

暗号・認証に使用する鍵を安全に保管し、配布するために、これらを IC カード（セキュリティカード）に格納する。さらに、IC カードには、IC カードの所有者を認証するための情報として、所有者の

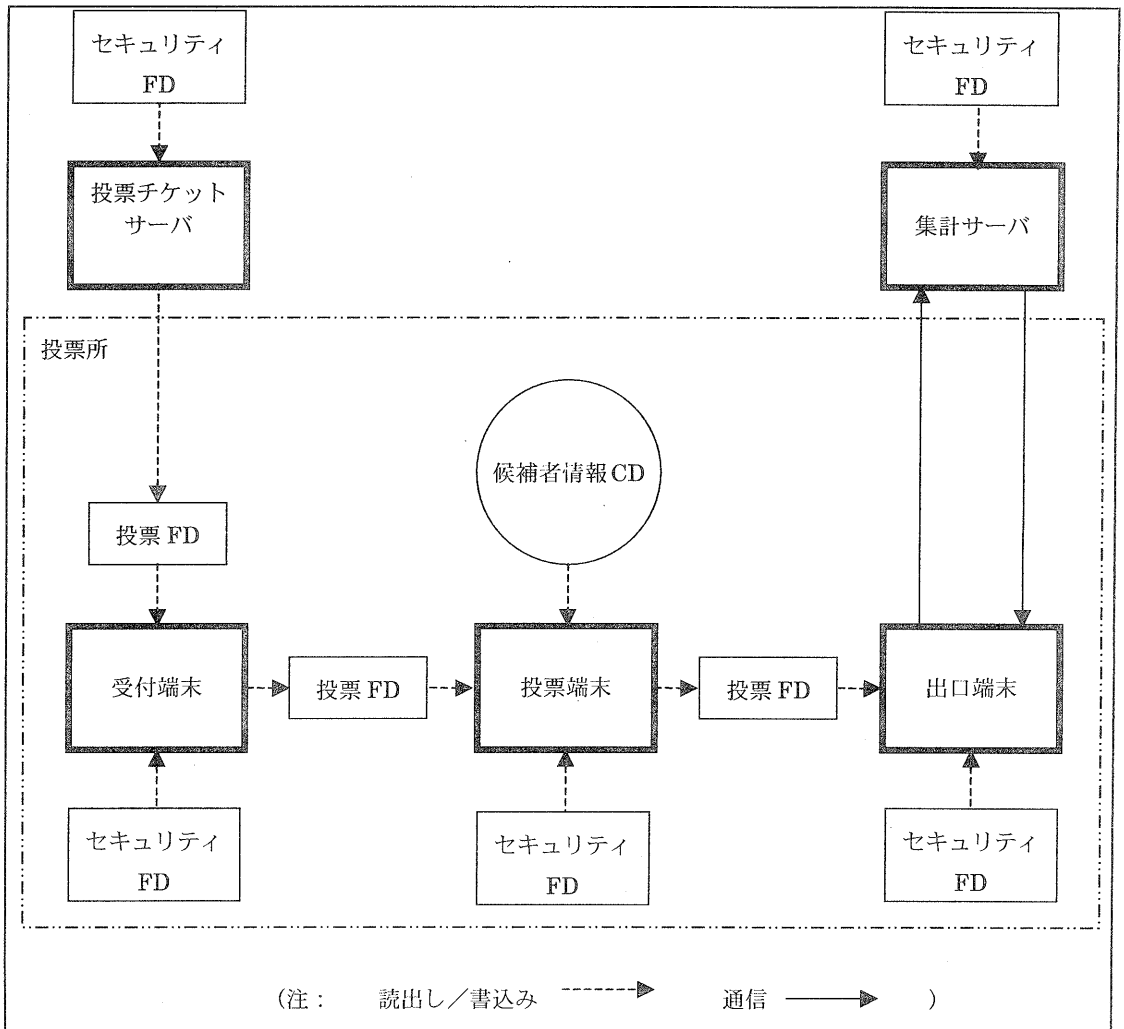

図１　システム構成図（第１期）

識別子とパスワードを格納する。

IC カードの種類は、投票管理者や開票管理者のための管理者用 IC カードと、投票立会人や開票立会人のための立会人用 IC カードの２種類を設ける。管理者用 IC カードには、管理者の識別子とパスワード、立会人（複数）の識別子、鍵情報を格納する。立会人用 IC カードには、立会人の識別子とパスワードを格納する。

また、現行の公職選挙法との整合性を考慮し、例えば投票端末に対しては、１枚の管理者用 IC カードと５枚の立会人用 IC カードを発行し、投票端末の運用開始には、管理者用 IC カードの認証と、２枚以上の立会人用 IC カードの認証を必要とする。

３．プロトタイプソフトウェア概要

上記検討の結果を集約した電子投票プロトコルの実現性を検証するとともに、電子投票システムの実装方法を確認するために、プロトタイプソフトウェアを開発した。

ただし、第１期のプロトタイプソフトウェアは、下記制約のもとで開発した。

- IC カードは使用せず、投票カードおよびセキュリティカードの機能を FD で代替する。
- セキュリティカードを用いた管理者や立会人の認証は行わない。
- 操作者とのインタフェースは、GUI を使用せず、コマンドラインの入出力で代替する。

表１　機能概要

項番	構成要素	機能
1	投票チケットサーバ	● 投票チケットを生成し、投票カードに格納する。投票チケットは、選挙識別子に対する投票チケットサーバ署名と暗号化されたシーケンス番号から構成する。
2	受付端末	● 投票カードから投票チケットを読出し、投票チケットに対する受付端末署名を生成して、投票カードに格納する。
3	投票端末	● 投票カードから受付端末署名と投票チケットを読出し、受付端末署名および投票チケットサーバ署名の検証を行う。 ● 候補者情報を表示し、投票者が選択した投票内容に基づいて投票情報を生成する。投票情報は、投票内容と、投票チケットサーバが発行したシーケンス番号と、投票端末が生成した乱数から構成する。 ● 投票情報に対する投票端末署名を生成し、投票情報と投票端末署名を投票カードに格納する。
4	出口端末	● 投票カードから投票情報と投票端末署名を読出し、投票端末署名の検証を行う。 ● 投票情報を暗号化し署名を添付して、集計サーバへ送信する。 ● 集計サーバから集計サーバ署名を受信し、集計サーバ署名の検証を行う。 ● 投票情報と集計サーバ署名を出口端末データベースに格納する。 ● 集計サーバが公開した投票一覧情報と出口端末データベースの内容との照合を行い、その結果に基づいて承認情報または異議申し立て情報を集計サーバへ送信する。
5	集計サーバ	● 投票情報を出口端末から受信し、署名の検証および復号を行う。 ● 投票情報に対する集計サーバ署名を生成し、出口端末へ送信する。 ● 投票情報を集計サーバデータベースに格納する。 ● 集計サーバデータベース上の投票情報から有効投票情報を抽出する。 ● 有効投票の一覧情報を公開する。 ● 出口端末から承認情報または異議申し立て情報を受信し、異議申し立ての場合は集計サーバ署名を検証して、集計サーバデータベースへ反映する。 ● 候補者毎の得票数を集計する。

第１期のプロトタイプソフトウェアのシステム構成図を図１に、各構成要素の機能概要を表１に示す。

４．今後の予定

投票所方式による電子投票システムの研究開発の第２期として予定している拡張項目について以下に示す。

- 第１期の研究開発においては、町村規模の地方選挙を適用対象としている。これを県や国政レベルの全国規模に適用するためには、集計サーバでの集計結果をさらに集約する階層化したシステム構成の方式検討が必要である。第２期の研究開発においては、集計サーバの階層化について検討し、その結果を電子投票プロトコルに反映するとともに、プロトタイプソフトウェアの拡張を行う。
- 第１期のプロトタイプソフトウェアでは、ICカードの代替として FD を用いて、鍵情報の保管・配布を行った。鍵情報の安全な保管・配布のためには、ICカードの導入が必須であり、第２期ではセキュリティカードの IC カード化を行う。またこれと同期して、ICカードを用いた管理者および立会人の認証機能を実装する。
- 第１期のプロトタイプソフトウェアでは、操作者とのインタフェースとして、テキストメッセージの出力およびキーボード入力を使用している。投票端末は、投票者が直接操作する端末であり、電子投票システムを投票者に受け入れ易くするためにも、第２期でインタフェースの簡易な GUI 化を実施する。
- 第１期では電子投票プロトコルの観点から無記名性の実現について検討し、プロトタイプソフトウェアに実装した。しかし、投票者が匿名性に関する確実性を容易に理解でき、安心して投票できることが重要であり、第２期では、投票者が投票カードで個人を特定できないことを納得できる方式について検討を行う。

５．おわりに

２期に分けて研究開発している投票所方式による電子投票システムについて、第１期で実施した電子投票プロトコルの検討、プロトタイプソフトウェアの開発について報告するとともに、第２期の実施予定項目について述べた。

特に電子投票プロトコルの検討に当たっては、①二重投票の防止と無記名性の実現を両立させること、②トラブル発生時の投票カード再発行を利用した二重投票を防止すること、③投票者の目の届かない場所で処理が行われる集計サーバの不正を防止すること、に重点を置いた。①に対しては、投票端末で生成した乱数と投票チケットに包含されたシーケンス番号を併用することにより、無記名性を損なうことなく、投票情報を識別する方式を確立した。②に対しては、投票情報を出口端末から集計サーバへ送信することにより、投票カードの再発行を利用した二重投票を防止する方式を確立した。③に対しては、集計サーバの集計結果を出口端末が検証し、不正検出時には異議申し立てを行う方式を確立した。

本研究開発は、情報処理振興事業協会「情報セキュリティ関連研究開発事業」の一環として行っているものである。

[参考文献]

[1] 藤崎英一郎、太田和夫、岡本龍明：投票所を仮定した実用的な電子投票方式、信学技報、ISEC93-24、1993

[2] 藤岡淳、藤崎英一郎、岡本龍明：電子投票方式、NTT R&D、44、No.10、pp939-946、1995

[3] 白石旭、田中利清：投票所方式による電子投票システム、Cyber Security Magazine、vol.2、pp28-31、1999