



특집 04

모바일 전자선거시스템의 현황과 전망



이광우 (삼성전자)

-
- 목 차 »
1. 서 론
 2. 국내외 모바일 전자투표 방식 및 현황
 3. 모바일 전자선거 시스템의 안전성과 신뢰성
 4. 결 론
-

1. 서 론

정보통신 기술의 발전은 지난 수십 년간 사회의 패러다임을 바꾸어왔다. 오프라인 서비스를 온라인 서비스로 변경해 왔으며, 배치 시스템을 실시간 대용량 데이터를 처리하는 온라인 시스템으로 변해왔다. 대표적으로 인터넷 뱅킹은 금융 업무를 시간과 장소의 제약에 구애받지 않고 거래가 가능하도록 서비스를 제공하였으며, ATM은 금융 업무에 있어 사람이 해야 할 일을 대신하며 현재 전 세계적으로 신뢰할 수 있는 시스템으로 인정되어 널리 사용되어 사회에 성공적으로 정착하였다. 이러한 정보통신 기술의 변화는 휴대폰, 스마트폰 등의 대중화로 이어지고 있으며, 최근에는 모바일 단말을 이용한 투표 방식이 대의 민주주의를 실현하기 위한 방법의 하나로 선거에 활용되고 있다. 전자선거는 일련의 선거과정에 걸쳐 전체 또는 부분적으로 IT 기술을 활용하는 선거를 관리하는 방식으로 선거인명부 작성 단계에서부터 투표, 개표 절차에까지 적용될 수

있다. 전자선거는 그 동안 사회에 만연해 있던 정치적 무관심을 해결하고, 선거 비용을 절감하며, 국가 전략적으로 전자정부를 표방하여 공공의 효율성을 증대하기 위한 방안으로 꾸준히 언급되었다. 뿐만 아니라, 전자선거는 최근 전세계적으로 심각해지고 있는 투표율 저하와 함께 전통적인 종이 투표 방식에서 발생하였던 선거 부정 문제를 해결하기 위한 방안으로 도입된 바 있다.

현재 전세계적으로 50여 개국이 전자선거의 도입을 시도하거나 시행 중인 것으로 알려져 있다. 특히 스위스의 경우에는 정치적 무관심을 해결하고자 국민적 합의를 통해 전통적인 선거 방식 이외에 새로운 전자선거 참여 방식이 도입되었는데 유권자들에게 거부감 없이 받아들여지고 있으며, 브라질의 경우에는 부정선거를 해결하기 위한 방법으로 도입된 전자투표기를 국외에 수출하는 전자투표 선진국이 되었다. 또한 에스토니아는 인터넷을 이용한 전자투표 방식까지 활용되면서 전자투표 방법이 확대되고 있다. 전자선거를 도입하여 발생하는 수행 효과와 문제점에 관

해서는 큰 논란의 여지가 없다. 이미 우리나라의 경우도 집계 작업시 사용되는 투표지 분류기에 대해서는 그 안정성과 효과가 입증된 바 있다.

하지만, 전자선거의 긍정적인 이면에는 보통선거, 직접선거, 비밀선거, 평등선거라는 민주주의 근간이 되는 선거의 4대 원칙이 흔들리는 문제점도 가지고 있다. 현재 전자투표기의 도입에 성공한 대부분의 국가는 우선 전자투표기의 사용에 대한 국민적 합의가 이루어진 상태에서 전자선거 방식이 도입되었으며, 투표 또는 개표 단계의 일부에 IT 기술을 접목하여 성공한 사례를 바탕으로 그 영역을 점점 확대하고 있다. 이는 전자선거에 대한 사회적 불안감을 해결해야 실제 공직선거에 활용이 가능하기 때문이다. 실제로 전자투표기 도입 이후, 국민들의 신뢰감을 얻지 못한 영국, 네덜란드, 미국에서는 전자투표기의 사용이 전면 금지되는 사태가 발생하기도 하였다. 최근 국내에서도 TV를 통해 ARS 자동응답 서비스나 SMS 문자 메시지를 활용한 모바일 온라인 투표 방식이 널리 사용되고 있다. 하지만, 정당의 경선에 활용된 경우에는 대리투표나 비밀투표 훼손 등의 이유로 현재 많은 사회적 문제를 야기하고 있다. 따라서 모바일 전자 투표 방식에 대한 신뢰성 및 안전성이 이슈가 되고 있다.

이에 본 고에서는 국내외 모바일 전자선거 시스템 동향을 살펴보고, 모바일 전자투표 시스템의 안전성과 신뢰성에 대해 살펴보도록 한다.

2. 국내외 모바일 전자투표 방식 및 현황

국내의 전자선거는 1995년 제1회 전국동시지방선거에 계수기를 도입하였으며, 2002년 제3회 전국동시지방선거부터 투표지 분류기를 사용하고 있으며, 기술적으로는 터치스크린을 이용한 전자 투표기까지 개발 완료되어 현재 널리 사용되고 있는 실정이다. 특히 투표지 분류기를 도입할 당시, 투표지 분류기의 정확성에 대한 많은 문제점이 시민 단체를 통해 제기된 바 있으나, 실제 공직선거 개표과정에서는 투표지 분류기를 이용하여 정당 후보자별로 분류를 진행한 후, 심사/확인/집계의 과정을 거치기 때문에 기계적으로 발생할 수 있는 오류 가능성을 최소화하고 있다.

모바일 투표의 경우에는 현재 과도기를 꺾고 있다. 통합진보당에서 실시한 19대 총선 비례대표 후보자 선출 당내 경선에서는 인터넷 투표 방식에서 특정 IP에서의 투표 집중 및 대리 투표, 선거인명부 조작, 개표 프로그램 오류 등의 문제가 발생하였으며, 선거관리 시스템의 프로그램 변경 내역을 기록하는 형상관리 시스템의 부재, 시스템 관리자의 허가되지 않은 모니터링 시스템 접근 및 수정으로 인해 사회적으로 물의를 일으킨 바 있다. 마찬가지로 2012년 민주통합당 총선 후보 경선 방식으로 채택된 모바일 전자투표에서는 선거인단 모집과정에서 선거인단 대리접수 문제가 발생하여 모바일 투표에 대한 부정적인 인

1. 모바일 투표 선거인단 신청 단계
2. 문자 3회 발송 단계 (2시간 이내의 투표만 유효)
3. 문자에 포함된 URL로 무선인터넷 접속
4. 본인 인증 단계 : 유권자의 주민등록번호 입력, 본인 확인 후 5분 이내에 후보자 선택
5. 투표 단계 (후보자 선택 단계)
6. 확인 단계

(그림 1) 모바일 SMS/무선인터넷 투표 방식

식이 높아졌다. 가장 최근에는 민주통합당 대선 후보 경선에서 SMS/무선인터넷 모바일 투표 및 ARS 모바일 전자투표가 진행되었으며, 이 과정에서 모바일 투표의 공정성 및 신뢰성에 문제가 제기된 바 있다. 이 선거에서 사용된 모바일 전자 투표 방식은 다음과 같다.

이상의 국내 모바일 투표 수행 과정에서 지적되었던 문제점은 다음과 같다.

- 멘트 도중 번호를 누르고 끊으면 유효 투표로 인정이 안 된다.
- ‘눌러주세요’란 말 이전에 누르면 몇 초 지난 뒤 “후보를 선택하지 않으셨습니다. 기호를 다시 듣고 선택해 주세요” 라는 멘트 나옴. 투표 다시 안 하면 유효 투표로 인정되지 않는다.
- ‘눌러주세요’ 이후에 누르면 전화 끊어도 유효 투표로 인정된다.
- 해킹 위험이나 투표 결과 조작 가능성이 제기될 수 있다.
- 개인정보 도용에 따른 대리 투표 및 매표가 가능하다. (선거인단 모집 경재)

- 투표 방식에 따라, 본인 인증을 미리 설정한 비밀번호로도 구현 및 적용이 가능하다.

이러한 방식의 모바일 전자투표 방식은 기존 종이 투표 방식과 같이 통제된 환경에서 기표가 이루어지는 투표 방식이 아니기 때문에 민주주의 선거의 4대 원칙 중 비밀선거 원칙이 실현되기 어렵다. 또한 휴대폰 사용이 어려운 소외 계층이나 노년층 및 회사에서 제공하는 법인 휴대폰을 주로 사용하는 외국계 회사 직원 등에게는 투표 참여의 장벽이 될 수 있어 보통 선거 원칙에 영향을 미친다는 의견도 있다.

2005년 에스토니아에서는 세계 최초로 공직선거인 지방선거에 인터넷 전자투표를 실시한 바 있으며, 유권자 인증을 위해 카드 리더와 전자주민증(ID카드)을 사용하였다. 또한 2007년 총선에서 모바일 투표를 실시하였다. 또한 2008년에는 휴대폰을 이용한 선거 법안을 에스토니아 의회에서 통과 시킨 바 있다. 국내 실정과는 매우 대조적인 상황이라고 볼 수 있다. 에스토니아에서 시행하는 휴대폰을 이용한 투표 방식은 SIM 카드에 들어있는 디지털 인증서를 이용하고 있다.

1. 모바일 투표 선거인단 신청 단계
2. 음성 ARS 2회 발송 단계
3. 음성 ARS 연결 단계
4. 본인 인증 단계 : 유권자의 주민등록번호로 본인을 인증한다.
5. 후보자 번호 및 성명 안내 단계
 “이번 000 경선에 출마한 네명의 후보들을 기호순으로 불러 드리겠습니다. 누가 적합하다고 생각하십니까? 네 명의 후보를 모두 들으신 후 그 중 한 명의 후보만 선택하고 투표 결과를 반드시 확인해 주세요. 000 후보면 1번, 000 후보면 2번, 000 후보면 3번, 000 후보면 4번을 눌러주세요”
6. 투표 단계 (후보자 선택 단계)
 유권자가 원하는 후보의 번호를 누른다.
7. 확인 단계
 “선생님께서서 000 후보를 선택하셨습니다. 투표 결과가 맞으면 1번, 다시 투표하시려면 2번을 눌러주세요”란 멘트가 나온다. 1번 누르면 투표가 완료되며, 2번 누르면 다시 투표를 진행하게 된다.

(그림 2) 모바일 ARS 투표 방식

현재는 스마트폰을 이용한 전자투표 방식에 관심을 기울이고 연구개발에 투자하고 있다. 에스토니아에서 전자선거가 자연스럽게 정착될 수 있었던 이유에는 1998년 전자정부 프로젝트를 진행하면서 전자주민증(ID카드), 전자투표 등에 대한 교육 시스템을 활발히 추진한 것이 밑거름이 되었다.

3. 모바일 전자선거 시스템의 안전성과 신뢰성

모바일 전자선거 시스템의 안전성과 신뢰성에 의문을 제기하는 가장 큰 이유는 전자선거 시스템에 탑재되는 하드웨어와 소프트웨어의 동작을 신뢰할 수 없다는 것이다. 이를 해결할 수 있는 방법은 전자선거 시스템 내부를 공개하는 것이 있다. 전자선거 시스템 내부를 공개하는 것은 많은 전문가의 검증을 받는 계기가 되기 때문에 전체적인 안전성을 높일 수 있다. 하지만, 시스템에 대한 취약점을 노출시켜 선거 당일 시스템에 대한 안전성을 저해할 수 있는 제로데이가 선거에 활용될 수 있다는 의견도 있다. 이 장에서는 모바일 전자선거 시스템의 안전성과 신뢰성을 높이기 위한 방안을 살펴보고자 한다.

3.1 오픈 소스 개발 정책

대부분의 전자투표 시스템 개발 업체에서는 시스템 내부를 공개하기 꺼려하고 있다. 이는 시스템 내부를 공개함에 따라 전자투표 시스템의 취약점 노출과 함께 안전성 저하 및 저작권 침해를 들고 있다. 반면에 학계나 공개 소프트웨어 진영에서는 공개적인 개발을 통해 취약점을 조기에 발견하여 안전성을 높일 수 있다고 지적한다.

하지만, 대부분의 상업적인 전자투표기 업체에

서는 자사 제품에 대한 저작권 보호와 불필요한 공개로 인한 시스템 안전성 저하를 이유로 자사의 투표기에 대한 세부적인 H/W 구조나 S/W를 공개하기 꺼려하고 있다. 이런 상업적인 제품에 반대하여 공개 프로젝트로 전자투표 시스템을 개발하려는 움직임도 있었다.

하지만, 안전한 전자투표기로 간주되었던 AccuVote-TS 전자투표 시스템도 소스 공개 후 많은 심각한 문제점이 발견되었듯이 오픈 소스 정책을 택하면 많은 전문가의 사전 검증을 받을 수 있는 장점이 있다. 우리나라의 선거관리위원회에서는 아직 전자투표 시스템의 소스 공개에 대한 입장을 밝힌 바는 없지만, 긍정적으로 검토해야 할 사안이라고 할 수 있다. 에스토니아는 오픈 소스 개발 정책을 적용하여 모든 컴포넌트를 간소하게 설계하고, 안전성, 신뢰성 및 간소화에 초점을 맞추어 투명하게 개발함으로써 전자투표 시스템에 대한 안전성을 확보한 대표적인 성공 사례라고 볼 수 있다.

3.2 정보보호제품 인증

국내에서는 정보보호제품에 대해 인증을 제공하고 있다. 대표적인 제도로 CC인증, 보안적합성 인증, 국가용 암호제품 지정제도 등이 있다. 국내에서는 통합진보당의 온라인 전자투표 시스템을 통해 정보보호제품에 대한 사전 품질 조사 및 오류, 보안 검증이 얼마나 중요한지를 보여준 단편적인 사례라 볼 수 있다. 기존 다른 선거를 통해서도 온라인 투표와 관련해 기권자의 표가 유효 투표로 잘못 집계됐거나 선거관리 시스템의 사전 품질 오류·보안검증이 전혀 이뤄지지 않는 등 다수의 부실 사례가 발견되기도 했다. 이러한 문제를 해결하기 위해서는 전자투표 시스템에 대한 보안 기능에 대해서는 기존 정보보호제품 인증

제도를 활용할 수 있으며, 보안감사로그 및 형상 관리가 철저하게 이루어져야 한다. 에스토니아의 인터넷 전자투표 시스템은 감사로그와 형상관리에 대해 명확한 요구사항을 가지고 있다.

3.3 전자투표 시스템 운영 환경에 대한 안전성

영국과 네덜란드는 전자투표 시스템이 적용되는 시점에 안전성과 신뢰성이 전자투표를 도입 및 유지하는데 얼마나 중요한지 보여준다. 영국은 2001년 다양한 방식의 전자투표 시스템을 도입하여 대중화 및 홍보에 노력하였으나, 2008년 지방 선거에서 개표 결과가 투표 결과를 제대로 반영되지 않는 문제점이 발생하여 결국 전자투표 계획이 무산되었다. 전자투표는 전통적인 종이 투표 방식을 IT 기술의 힘을 빌려 전산화한 방식으로 기존 방식에서 전자투표 방식에서 없었던 새로운 문제점이 발견되면 시민사회로부터 질타의 대상이 된다. 네덜란드의 경우도 영국과 마찬가지로이다. 네덜란드는 전자투표 시스템이 널리 보급되어 사용 중이었으나, 2006년 전자투표기에 대한 취약성이 발표되면서 전자투표가 전면 금지되었다. 또한 미국의 경우, 2004년 5월 캘리포니아 주정부 선거시 저전압으로 인해 장애를 일으킨 더블드 모델을 사용 금지 시켰으며, 2004년 전국적으로 실시된 인도의 경우 처음 시행되는 전자투표로 인한 투표자 혼란, 기계조작에 익숙하지 않은 유권자들의 오작동으로 인한 시스템 다운, 투표조작 등의 문제가 발생했다. 이러한 각국의 도입 사례를 통한 결과를 통해 우리나라의 전자투표 사업 실시시 확보되어야 할 다양한 부작용들에 대한 사전 준비가 요구된다.

3.4 비밀 투표에 대한 보장

인터넷 전자투표와 모바일 전자투표의 가장 큰 문제점 중의 하나는 비밀투표에 대한 보장이 어렵다는 것이다. 통합진보당 투표 결과에 대한 진상조사는 많은 시사점을 보여주었다. 각 유권자의 투표값이 SHA256 해쉬함수를 적용하여 유권자의 투표 결과를 확인할 수 없는 것으로 알려져 있었으나, 설계상의 오류로 유권자의 투표값이 모두 추적되는 문제점을 보여주었다. 정보보호 제품에 암호 알고리즘을 적용하는 경우나 보안 프로토콜을 새로 설계하여 제품에 구현하는 경우에는 반드시 안전하게 설계되었는지에 대한 안전성 검증이 이루어져야 한다. 특히, 키관리 및 암호화 방법에 대해서는 안전하지 않은 난수 발생 알고리즘을 사용하고 있지 않는지, 안전하지 않은 암호화 알고리즘의 사용하는지, 키 관리가 잘못되어 있지 않은지, 암호 알고리즘 적용 순서가 적절한지에 대한 검토가 절실히 필요하다.

4. 결론

본 고에서는 전자투표 시스템 중 최근 널리 사용되고 있는 모바일 전자투표 시스템에 대해 설명하고, 모바일 전자투표 시스템에서 발생할 수 있는 문제점을 살펴보았다. 또한 모바일 전자투표 시스템에 대해 제기되고 있는 이슈에 대해 살펴보았다. 전자투표 시스템에 대한 안전성과 신뢰성은 기술적인 접근뿐만 아니라 법적, 제도적, 문화적 측면까지 모두 고려되어야 한다. 기존에 미국의 인터넷 부재자 투표 프로젝트는 결국 시행되지 못했지만, 스위스 같은 경우는 인터넷 투표를 성공적으로 실시한 바 있다. 이는 기술적인 차이가 아닌 문화적인 차이로 보아야 하는데, 스위스는 이미 오래 전부터 우편 투표 제도가 잘 정

착되어 인터넷 투표에 대한 국민적 합의가 비교적 잘 이루어져 있다고 볼 수 있다. 아직 국내에서는 공직자 선거에 모바일 전자선거를 도입할 계획이 없다. 하지만, 당내 경선 과정에서 다양한 방법으로 모바일 선거방식이 활용되고 있다. 국내 중앙선거관리위원회는 최근의 여러 가지 해킹 사례에 대해 충분히 안전성 검증을 할 필요가 있다. 이와 함께 전자투표 시스템의 안전성과 신뢰성을 높이기 위한 방안으로 H/W, S/W 시스템 구조를 공개하는 오픈 소스 정책을 통해 각계의 전문가들로부터 검증을 받는 것도 긍정적으로 고려해야 할 것으로 판단된다.

참 고 문 헌

- [1] Rebecca Mercuri, "Rebecca Mercuri's Statement on Electronic Voting", <http://www.notablessoftware.com/RMstatement.html>, 2001
- [2] David Chaum, "Secret Ballot Receipts and Transparent Integrity - Better and less-costly electronic voting at polling places", <http://www.vreceipt.com/article.pdf>
- [3] Dennis Vadura and Frank Wiebe, "What is A Meaningful 'Voter Verified Paper Audit Trail?'", <http://www.accupoll.com/TheAccuPollAdvantage/WhitePapers/VVPAT.pdf>, 2003
- [4] Election Incident Reporting System, <https://voteprotect.org/index.php?display=EIRMapNation>
- [5] 중앙선거관리위원회, "전자투표 추진계획 및 로드맵", <http://www.nec.go.kr/dev/multiboard/board.jsp?id=b04&groups=0&key=subject&search=&order=&desc=&code=0&mode=view&idx=701>, 2005
- [6] FVAP, "Secure Electronic Registration and Voting Experiment (SERVE)", <http://fvap.gov/services/evoting.html>

- [7] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "A Security Analysis of the SERVE", <http://www.servesecurityreport.org/>, 2004
- [8] Internet voting in Geneva, Frequently Asked Questions, <http://www.geneve.ch/evoting/english/faq.asp>

저 자 약 력



이 광 우

이메일 : kwangwoo.lee.korea@gmail.com

- 2005년 성균관대학교 정보통신공학부(학사)
- 2007년 성균관대학교 컴퓨터공학과(석사)
- 2011년 성균관대학교 전자전기및컴퓨터공학과(박사)
- 2011년 성균관대학교 박사후연구원
- 2012년~현재 삼성전자 책임연구원
- 관심분야: 암호이론, 보안성 평가, 전자투표, 정보보호 제품 취약점 분석