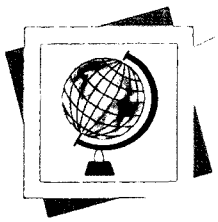
| 특집 07 |



전자선거 국제 연구동향

이윤호 · 이광우 · 김승주 · 원동호
(성균관대학교)

목 차

1. 서 론

1981년 D.Chaum에 의해 디지털 익명(digital pseudonyms)에 관한 논문[1]이 발표된 이후 전자선거에 정보보호 기술을 적용하기 위한 연구가 활발히 진행되었고, 정보 기술 및 관련 인프라의 발달로 현재는 세계 각국에서 전자선거 실시를 적극 검토하고 있거나 시험 실시하는 등 상용화 단계에 있다. 전자선거는 흔히 정보보호 기술의 집합체로 불리는데, 이는 전자선거 시스템을 구축하는데 있어서 암호화나 전자서명과 같은 기반 기술은 물론이고 사용자 인증, 스마트카드, 네트워크/시스템 보안 등과 같은 응용 보안 기술까지 모두 필요하기 때문이다[5]. 전자선거 시스템은 <표 1>과 같은 현재의 종이투표 방식이 갖고 있는 여러 문제점을 해결할 수 있을 것으로 기대되고 있다.

이러한 문제점을 해결하기 위해 투표시 펀치카드, 레버머신 등 기계적인 장치를 이용하거나 개표기를 이용하는 등 투 · 개표 과정을 자동화하는 방법을 사용하기도 하였으나, 2000년 미국 대선에서의 펀치카드 투표 방식의 오류에서 볼 수 있듯이 오히려 개표 결과에 대한 불신만 키울 수 있어 완벽한 해결책이라고 할 수 없다.

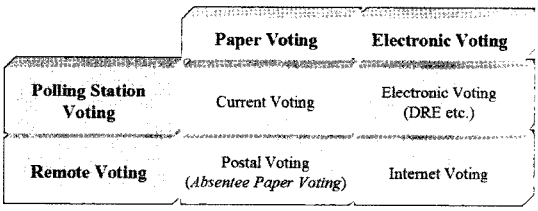
기존 선거 방식의 문제점과 기계적인 자동화의 한계로 인해 전자선거에 대한 관심이 높아지고 있는데, 전자선거는 투표나 개표 과정이 전자적으로 처리되기 때문에 기계적인 오작동이 발생되지 않으며, 투 · 개표에 소요되는 인력을

〈표 1〉 현재 선거 방식의 문제점

선거 관리 비용의 증대	투표 관리 및 개표 인력 투·개표 소요 시간
개표 결과의 신뢰성 저하	재검표시마다 다른 개표 결과가 나옴 개표 결과에 대한 불신으로 각종 소송 발생
시·공간적 제약에 따른 투표율 저하	단기간, 제한된 장소로 인해 투표율 저하
투표자 실수로 인한 사표 발생	매 선거마다 0.9%~2.6%의 무효표 발생 유권자의 정확한 의사 반영이 어려움

획기적으로 절감할 수 있고 상대적으로 짧은 시간 내에 개표할 수 있는 등 여러 가지 장점을 제공하기 때문에 각국은 전자선거 실시에 적극적이다.

전자선거 방식을 투표 기록 방식과 시·공간적 제약 유무에 따라 분류하면 아래의 (그림 1)과 같다.



(그림 1) 투표 방식의 구분

인터넷 투표는 공간적인 제약을 완전히 없앤 전자 투표로서, 인터넷이나 휴대폰 등을 이용하여 언제 어디서나 투표할 수 있기 때문에 궁극적인 투표 방식이지만 매표 행위가 있을 수 있고 해킹 등 각종 위협에 노출될 수 있기 때문에 아직까지는 해외 부재자 투표 등 극히 제한적인 선거에만 적용되고 있다.

〈표 2〉 전자선거에 대한 요구 조건

기밀성 (Secrecy)	투표자의 투표 내용은 비밀로 유지해야 한다. 투표 결과로부터 투표자를 구분할 수 없어야 한다.
정확성 (Correctness)	모든 유효 투표는 반드시 집계에 반영되어야 한다.
강건성 (Robustness)	부정한 투표자 또는 외부의 악의적인 공격이 집계 결과에 영향을 미쳐서는 안 된다.
적임성 (Eligibility)	정당한 유권자만 투표에 참여할 수 있다.
이중투표 불가성 (No Double Voting)	모든 투표자는 한 번만 투표할 수 있다.
검증성 (Universal Verifiability)	집계 결과는 누구나 검증할 수 있어야 한다.
비영수성 (Receipt-Freeness)	투표자는 자신의 투표 내용을 증명할 수 없어야 한다.

전자선거가 현재의 종이 투표 방식과 비교해서 여러 가지 장점을 제공하는 것은 분명하지만 모든 과정이 전자적으로 처리되기 때문에 처리 과정에 대한 신뢰성 문제는 반드시 해결해야 하는 과제라고 할 수 있다. 신뢰성 문제는 크게 선거 관리 기관의 부정, 투표자의 부정 및 외부의 공격 등 세 가지로 요약되는데, 선거 관리 기관의 부정은 투표기 조작이나 개표 결과의 조작이 해당되며 투표자의 부정은 중복 투표나 매표 등이 해당되고 마지막으로 외부의 공격은 정상적인 투표 과정이나 개표 과정에 대한 해킹 등이 해당된다. 이런 이유로 전자선거는 <표 2>와 같이 현재의 선거 방식보다 엄격한 조건을 만족해야 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 전자선거에 사용되는 핵심적인 요소 기술로 준동형 암호화(homomorphic encryption), 은닉 서명(blind signature), 믹스넷(mix-net) 및 비밀 분산(secret sharing) 등 네 가지 기술에 대해 설명한다. 3장에서는 1992년 발표된 전자선거 프로토콜을 실제로 구현한 MIT의 EVOX 시스템과 미국, 스위스의 인터넷투표 프로젝트 추진 현황을 통해 현재의 전자선거 기술 개발 동향에 대해 살펴본다. 그리고 이를 바탕으로 4장에서는 향후 우리나라에서 전자선거 시행을 위해 고려해야 할 사항을 정리하고 5장에서 결론을 맺도록 한다.

2. 전자선거 요소 기술

전자 투표 기술에 대한 연구는 지난 20여 년간 활발히 진행되었고 다양한 전자 투표 방식이 제안되었다. 현재까지 제안된 전자 투표 방식을 보면 크게 준동형 암호화, 은닉 서명, 믹스넷 및 비밀 분산 등 네 가지 요소 기술을 복합적으로 사용하고 있다[6].

준동형 암호화를 이용한 전자 투표 방식은

1985년 Benaloh(Cohen)에 의해 처음 제안되었다[2]. 이 방식은 준동형 암호화 성질을 갖는 확률적 공개키 암호 방식(probabilistic public-key cryptosystem)과 비밀 분산 방식(secret sharing)을 기반으로 하고 있다. 이 방식을 이용할 경우 암호화된 각각의 투표 값을 복호화하지 않고 암호화된 전체 투표 결과의 곱을 복호화하면 되기 때문에 개표와 집계에 소요되는 시간이 짧다는 장점이 있지만, 집계 결과의 정확성을 위해 투표자가 자신의 투표 m_i가 정해진 후보 목록 $t=\{t_1, \ldots, t_m\}$에 있음을 증명해야 한다.

은닉 서명을 이용한 전자선거 방식은 서명을 담당하는 선거 관리 기관과 집계를 담당하는 집계 기관으로 분리 운영된다. 각 투표자는 선거 관리 기관에서 신원 확인을 거쳐 자신의 투표에 서명을 받은 후 집계 기관에 제출한다. 집계 기관은 선거 관리 기관의 서명을 확인하고 투표를 집계에 반영한다. 은닉 서명을 이용한 전자선거 방식은 D.Chaum에 의해 1988년 제안되었지만 실제 적용할 수 있는 방식은 1992년 Fujioka에 의해 제안되었으며[3], MIT에서 구현한 전자 투표 시스템인 EVOX 시스템이 이 방식을 기반으로 하고 있다.

믹스넷은 1981년 D.Chaum에 의해 메일과 전자선거의 익명성 실현 방법으로 처음 제안되었다[1]. 믹스넷이란 n개의 입력 값을 임의로 재배치(shuffle)한 결과를 출력하여 입력 값의 순서를 추적할 수 없도록 하여 익명성을 보장하는 방식이다. 이 방식을 이용할 경우 재배치를 담당하는 기관(믹스)의 부정을 방지하기 위해 각 믹스는 입력을 무작위로 재배치했음을 증명해야 한다.

비밀 분산은 1979년 Shamir에 의해 처음 제안되었다[4]. (t, n)-threshold 비밀 분산이란 비밀 정보 S를 n개의 부분 정보로 분할하고 이 가운데 t개의 부분 정보를 알면 비밀 정보 S를 복원할 수 있도록 한 방식이다. 전자선거에는 암호화된 투표 값을 복호화하기 위해 필요한 비밀 정보를 n개의 독립적인 기관으로 분산시키고 t개 이상의 기관이 협력했을 경우에만 복호화할 수 있도록 응용되고 있다.

3. 전자선거 기술 개발 프로젝트 추진 현황

이 장에서는 MIT의 EVOX 시스템과 미국의 인터넷투표 프로젝트인 SERVE(Secure Electronic Registration and Voting Experiment) 및 스위스의 인터넷투표 프로젝트를 비교해서 살펴보도록 한다. 미국은 이미 오래전부터 종이투표 방식과 함께 레버머신이나 펀치카드, 광스캐너 등 기계적인 방식을 투표에 적용해왔다. 특히 최근에는 투표 내용을 전자적으로 기록하는 DRE (Direct Recording Electronic) 시스템이 점차 확산되고 있는 추세지만, 보다 발전된 전자 투표 방식인 인터넷투표에 있어서는 상당히 보수적인 입장을 보이고 있다. 반면 스위스에서는 이미 전 국민을 대상으로 실시하고 있는 우편투표를 확장하여 인터넷투표를 성공적으로 실시하여 대조를 이루고 있다.

3.1 EVOX 시스템(미국)

EVOX 시스템은 1992년 발표된 은닉 서명 기반 전자선거 프로토콜인 FOO 방식을 기반으로 MIT CIS(Cryptography and Information Security) 그룹의 Rivest에 의해 1997년에 개발되었으며 1999년 MIT의 학생회장 선거에 사용되었다[12]. 이후 EVOX 시스템에 비밀 분산을 적용하여 다수의 기관을 고려한 시스템으로 확장되었고 이 시스템을 보다 개선하여 REVS(Robust Electronic Voting System)가 개발되었다[13]. FOO 방식은 Cranor에 의해 개발된 SENSUS 시스템의 기반이 되기도 했는데, 실제 구현을 통해 검증된 대표적인 방식이기도 하다.

3.2 SERVE 프로젝트(미국)

SERVE 프로젝트는 2001년 미의회의 권고로 국방성(DOD)에서 2004년 미국 대선 적용을 목표로 시작한 실험적인 인터넷투표 프로젝트다. SERVE는 플로리다, 하와이, 워싱턴을 포함한 7개 주의 약 50개 선거구와 해외 부재자 및 군인을 대상으로 적용될 예정이었으며, 약 100,000명의 유권자를 처리할 것으로 예상했었다. SERVE 시스템의 특징을 정리하면 다음 <표 3>과 같다.

〈표 3〉 SERVE 프로젝트의 시스템 구성

항 목	세부 내용
클라이언트(투표자) PC	-웹브라우저 + ActiveX/Java Applet + Script
서버	-중앙 웹서버 + LEO (Local Election Official)
클라이언트-서버 채널	-128비트 SSL
기타	-추가 소요 하드웨어 및 소프트웨어 없음

별도의 스마트카드나 인증용 하드웨어 없이 ActiveX/Java Applet과 스크립트를 실행할 수 있는 웹브라우저만을 이용하여 중앙 웹서버에 접속하여 투표할 수 있도록 설계되었으며 클라이언트와 서버 간 보안채널은 128비트 SSL을 이용하였다.

미국 내에서 인터넷투표 프로젝트는 SERVE가 처음은 아니다. 이전에도 VOI(Voting Over the Internet) 프로젝트가 있었으며, 정당 대선 후보 경선에 적용된 바 있다[10]. 하지만, 결과적으로 SERVE는 2004년 미국 대선에 적용되지 못했는데, 이는 SERVE에 대한 보안 취약점을 경고한 보고서 때문이다[11]. D.Jefferson, A.D. Rubin, B.Simins 및 D.Wagner 등 4명의 전문가에 의해 발표된 이 보고서를 요약하면 <표 4>와 같다.

〈표 4〉 SERVE 프로젝트에 대한 보안상 취약점

항 목	세부 내용
구현의 정확성	구현 정확성에 대한 공개적인 검증이 없음 내부자(개발자) 공격을 막을 수 있는 VVAT 기능 없음
인터넷 및 PC의 위협 요소	DOS 공격, spoofing, 매표 및 바이러스 공격 등에 대한 대비책이 없으며, 이러한 위협은 현재의 인터넷과 PC를 사용하는 이상 해결책이 없음
집계 결과에 대한 불신	지적한 잠재적인 위협으로 인해 집계 결과에 대한 불신을 초래할 수 있음

이 보고서는 이런 이유를 들어 인터넷투표 대신 Kiosk 방식을 권고하고 있는데, 현재의 인터넷과 PC 환경이 완전히 바뀌지 않은 이상 인터넷투표는 사용하면 안된다고 주장하면서 즉각 SERVE 프로젝트를 중단해야 한다고 경고하였다. 결국 2004년 초 대선 적용 방침이 철회되면서 SERVE 프로젝트는 중단되었다.

SERVE 프로젝트에 대한 취약점 보고서에서 눈여겨봐야 할 것은 영수증 발급이 내부자 공격에 대한 효과적인 대응책이라고 지적한 점과 현재의 인터넷 환경에서는 해킹이나 바이러스 및 매표 행위 등을 막을 수 있는 해결책이 없다고 한 점이다. 하지만, 두 번째 지적은 다음의 스위스 인터넷투표 프로젝트의 성공에서 볼 수 있듯이 사회적인 합의를 기반으로 현재의 기술을 이용하여 어느 정도는 해결할 수도 있다.

3.3 스위스의 인터넷 투표 프로젝트

정보통신의 강국인 미국이 인터넷투표 실시에 있어서는 큰 진척을 보이지 못하는 것과는 달리 스위스에서는 상당히 빠른 속도로 인터넷투표 프로젝트를 진행하고 있다. 스위스는 한 해에 4~5회 투표가 실시될 정도로 투표가 많은 나라 중 하나다. 이런 이유로 우리나라와 같이 대부분 부재자 투표에만 제한적으로 실시되는

우편 투표가 일반 국민을 대상으로 실시되고 있는 나라이기도 하다. 투표 횟수가 많기 때문에 스위스 역시 투표율 저하 문제가 갈수록 심각했었는데, 1995년 우편 투표를 전면 실시한 이후 투표율이 20% 가량 높아졌다[8].

〈표 5〉 전자선거에 대한 예상 문제점 및 해결 방안(스위스)

예상 문제점	해결 방안
전자 투표의 분실, 변조	-암호화된 서버 인증서 확인 -128비트 SSL을 이용한 보안 통신 -방화벽으로 보호된 다중 시스템 -투표 기간 동안 인증 코드를 매일 변경 -투표 기간 동안 DNS 서버의 주기적인 refresh
DNS 공격 / DOS 공격	-서버에 특수 제어 장치 및 프로토콜 필터 적용 -주기적인 DNS 서버 refresh -서버 다운시 투표소 투표나 우편 투표로 대체
매표 행위	-투표가 처리되었음을 통보하지만, 내용은 통보하지 않음
재검표 방안	-전자 투표 결과 재검표 -다른 집계 소프트웨어를 통한 재검표 -종이 영수증은 적용되지 않음
전자 투표에 대한 저항(Family voting 및 Digital divide)	-투표 방식의 변경 때마다 나올 수 있는 문제점으로 다수의 의견은 아님(우편투표를 실시할 때에도 제기되었던 문제)

스위스에서의 전자선거 프로젝트는 다른 나라보다 빠른 지난 2000년에 시작되었는데, 이미 우편 투표를 이용한 투표가 전체 투표의 95%에 이를 정도로 원격 투표에 익숙한 환경이기 때문에 인터넷 투표 역시 별다른 거부감 없이 추진되어 2004년 국민투표 당시 제네바 주 내의 일부 시에서 유권자가 기존의 투표 방식과 인터넷 투표를 선택할 수 있도록 하여 성공적으로 실시된 바 있다[9]. 스위스에서는 인터넷투표 실시에 따른 예상 문제점과 그에 대한 해결 방안을 <표 5>와 같이 정리하고 있다.

스위스에서의 인터넷투표 실시 사례는 다른 여러 나라와 비교했을 때 매우 독특하다고 할 수 있는데 이는 전 국민을 대상으로 우편 투표를 실시하고 있는 등 현재의 사회적인 여건과 무관하지 않다. 스위스에서의 인터넷투표는 앞에서 설명한 바와 같이 사용되는 보안 기술이나 환경이 미국의 SERVE와 크게 다르지 않음에도 불구하고 미국과는 달리 성공적으로 인터넷투표를 실시하고 있다. 이를 우리나라에 그대로 적용하기에는 다소 무리가 있지만 참고할 만한 사례라고 할 수 있다.

4. 전자선거 기술 개발 추진 방향

전자선거에 필요한 각종 암호 기술은 이미 충분히 연구되었으며 이론적인 안전성까지 증명되어 있다. 또한, 이를 기반으로 하는 다양한 전자선거 프로토콜도 제안되어 있다. 하지만, 앞서 살펴본 SENSUS나 EVOX의 기반 프로토콜인 FOO 방식을 제외하고는 실제로 구현 및 적용된 사례는 찾아보기 힘들다. 이는 상용화 단계에 이르기까지 아직 검증해야 할 부분이 많다는 이유도 있지만, 대부분의 전자선거를 위한 시스템이 폐쇄적으로 구현되는 것도 한 원인이다.

3장에서 살펴본 미국의 인터넷투표 프로젝트 SERVE의 추진 계획 및 이와 관련한 취약점 보고서와 스위스의 인터넷투표 프로젝트 진행 과정 및 실시 결과는 전자선거 실시를 계획하고 있는 우리나라에게 많은 것을 시사해주고 있으며 이를 잘 정리하면 우리나라 환경에서 향후 전자선거에 대비하여 추진해야 할 기술개발 방향을 정립하는데 많은 도움이 될 수 있다.

주요 쟁점을 정리해보면 크게 전자선거 시스템에 대한 신뢰와 투표 결과에 대한 투표자의 신뢰 및 인터넷을 이용한 원격투표 실시 여부 등 세 가지로 요약할 수 있다.

4.1 전자선거 시스템에 대한 신뢰

전자선거 시스템에 대한 이론적인 안전성을 입증하는 것이 구현의 정확성까지 입증하는 것은 아니기 때문에 투표자로 하여금 투표기기를 신뢰할 수 있도록 하는 방안을 마련하는 것이 중요하다. 실제로 여러 보안 전문가는 미국에서 널리 사용되고 있는 전자 투표기인 DRE가 투표자의 투표결과와는 무관한 내용을 기록하더라도 이를 확인할 수 없다고 지적하는데, 이는 집계 결과에 대한 신뢰성과 연결되어 전자선거 실시를 반대하는 주요 이유가 되고 있다. 이를 해결하기 위한 방안으로 H/W 및 S/W 시스템을 공개하여 구현 정확성을 대중적으로 검증받는 방법이 있으나 대부분 전자선거에 사용되는 시스템은 보안을 이유로 공개하지 않고 폐쇄적으로 개발되고 있다. 하지만 호주의 경우는 구현된 S/W 코드를 공개하여 안전성과 신뢰성을 동시에 높이고 있다.

시스템 공개와 함께 추가 안전장치로서 효율적인 방법은 전자적인 투표 결과 기록 이외에 종이 기록을 추가하는 것이다. 이는 추후에 발생할 수 있는 재검표 요구를 수용하기 위해서도 필요한 것으로서 SERVE에 대한 취약점 분석 보고서에서도 지적한 바와 같다. 이때의 종이 기록은 다음에서 다룰 영수증과 함께 사용되거나 별도로 처리될 수 있는데, 전자선거에서 사용되는 종이 기록 방식은 다음 두 가지 조건을 만족해야 한다.

(1) 현재 종이투표의 개표 방식보다 효율적으로 개표할 수 있어야 한다.

(2) 투표자의 투표 내용에 대한 기밀성을 보장하기 위해 기록된 내용과 순서로부터 투표자를 추적할 수 없어야 한다.

4.2 투표 결과에 대한 투표자 신뢰

앞서 지적한대로 전자선거 시스템을 공개하여 검증한다고 해도 100% 완벽한 시스템이라고 확신할 수는 없을 것이다. 따라서, 투표자가 자신이 투표한 결과 그대로 집계에 반영될 것임을 확신하도록 하는 방안이 필요한데, 가장 효율적인 방안은 투표 내용을 기록한 영수증을 발급하는 것이다. 하지만, 영수증 발급은 매표에 이용될 수도 있기 때문에 간단히 처리할 수 있는 문제가 아니다. 이런 이유로 대부분의 전자선거 시스템은 영수증을 투표소 내부에서만 확인한 후 안전한 투표소에 보관하도록 하여 향후 재검

〈표 6〉 전자선거에 대한 쟁점

쟁점	주요 내용 (미국, 스위스)	해결 방안
시스템 공개	-공개하지 않음	-H/W, S/W 시스템에 대한 공개 검증
인터넷 위협 요소	-현재의 인터넷에 대한 위협 요소를 완벽하게 해결할 수는 없음(미국) -현재의 기술을 최대한 활용하여 인터넷투표 실시(스위스)	-인터넷 투표는 매표, 해킹 등에 대한 대응책 마련이 선행되어야 함 -투표소/kiosk 투표 실시
투표자의 투표 확인	-내부자 공격을 막을 수 있는 방법이 없음(비공개 시스템) -투표 직후 스크린을 통해 확인하는 것 이외에는 확인할 수 있는 방법이 없음	-비영수성을 갖는 영수증 발급 -추후 영수증을 이용하여 투표 여부 검증
매표 방지	-추후 투표 결과 증명을 통한 매표는 불가능하지만, 투표시의 매표는 막지 못함	-투표소/kiosk 투표를 통해 전자선거 실시
재검표 방안	-전자적인 재검표 이외의 다른 재검표 방안 없음	-별도의 종이 기록 필요

표에 활용하도록 하고 있다.

만약 투표소 외부로 반출할 경우에는 매표 방지를 위해 투표 결과를 증명할 수 없도록 해야 하는데, 이런 비영수성을 만족하는 영수증 발급 기술은 전자선거 시스템의 안전성과 신뢰성을 높일 수 있는 핵심 기술 가운데 하나다.

투표 영수증 발급 기술은 visual cryptography를 이용한 D.Chaum의 방식과 VVAT(Voter Verified Audit Trail) 및 암호화된 영수증 발급 방식 등이 제안되어 있지만 D.Chaum의 방식은 현실적으로 구현이 어렵다는 단점이 있고 VVAT는 투표소 밖에서는 검증이 불가능하다는 점과 재검표 방식이 기존 종이투표와 같다는 것이 단점이 있으며 암호화된 영수증 발급 방식은 매표 방지가 불확실하다는 단점이 있어 실용화하기에는 미흡한 실정이다[7].

〈표 7〉 현재의 영수증 발급 방식 비교

영수증 발급 방식	장점	단점
Chaum의 방식	-투표소 밖에서도 검증 가능 -매표 불가능	-현실적으로 구현이 어려움
VVAT	-투표 결과에 대한 신뢰가 높음 -종이투표와 같은 방식으로 익숙	-투표소 밖에서는 검증 불가능 -재검표 방식이 현재와 동일
영수증 암호화	-투표소 밖에서도 검증 가능	-매표 방지가 불확실

4.3 인터넷을 이용한 원격 전자 투표

원격 전자 투표인 인터넷투표가 실시되기 위해서는 각종 DOS 공격, 웜 바이러스, 해킹 등을 효과적으로 해결할 수 있는 네트워크 보안 기술과 함께 매표를 방지할 수 있는 기술이 개발되어야 한다. 현재는 보안상의 이유로 투표소/kiosk 등을 이용한 전자 투표 시스템도 네트워크에 연결하지 않거나 공개되지 않은 사설 네트워크만 연결하는 것이 일반적이다. 즉, 현재의 보안 기술 수준으로는 인터넷투표를 실시하는데 필요한 안전성을 충분히 확보하기 어렵다는 것이 일반적인 견해이며, 이를 해결하기 위한 응용 보안 기술 개발이 필요하다. 이러한 응용 보안 기술에는 네트워크 보안 기술 외에도 웹사이트 보안, 데이터베이스 보안 등이 포함된다. 사실 인터넷투표는 기술적인 관점에서의 안전성 문제도 있지만 공개 투표에 따른 매표 가능성으로 인해 실시에 많은 논란이 있을 것으로 예상되며, 이를 기술적으로 완벽하게 해결하는 것은 불가능할 수도 있기 때문에 무엇보다 사회적인 합의가 선행되어야 할 것이다.

5. 결 론

이상과 같이 전자선거를 실시하기 위한 요소 기술과 실시 사례를 통한 각국의 기술 개발 동향 및 우리나라에서 전자선거를 실시하는데 고려해야 할 기술 개발 방향에 대해 간략하게 살펴 보았다. 전자선거는 현재 가장 많이 사용되는 종이 투표 방식의 단점을 대부분 해결할 수 있을 것으로 기대되기 때문에 세계 각국은 전자선거 도입에 적극적이며 우리나라에서도 중앙선거관리위원회를 중심으로 전자선거 실시 로드맵을 발표하는 등 도입을 활발히 추진하고 있다.

최근 세계 각국의 전자선거 기술 개발 동향을 분석해 보면 전자선거를 위한 프로토콜이나 요소 기술 개발보다는 영수증 발급 기술 또는 전자선거 시스템의 안전성 분석 및 안전한 전자선거 시스템을 위한 요구사항 정립 등 응용 보안 기술과 안전성 분석에 더 많은 노력을 기울이고 있다. 또한, 전자선거 시스템은 기술적인 요소는 물론이고 각국의 고유한 사회·문화적인 특성도 많이 반영되기 때문에 먼저 국내의 환경을 정확하게 분석하고 예측하는 것이 매우 중요하다.

전자선거는 개표 시간 단축과 소요 인력 감

소를 통해 선거 관리 비용을 절감할 수 있고, 투표 장소에 대한 제약을 완화하여 투표율을 높일 수 있으며, 투표자의 실수로 인한 무효표를 획기적으로 감소시켜 민주주의의 정당성을 확보할 수 있도록 하는 등 여러 가지 장점을 제공하지만 기기의 오작동이나 이로 인한 개표 결과 불신 등 여러 가지 문제가 발생될 수 있는 만큼 사전에 철저한 준비를 해야 할 것이다. 특히 시스템 H/W, S/W 공개를 통한 검증이나 영수증 발급 기술 개발 및 전자선거 시스템에 대한 안전성 분석 등 전자선거에 대한 신뢰성을 높이기 위한 연구에 보다 많은 투자가 있어야 할 것이다.

참고문헌

[1] D.L.Chaum, "Untraceable, electronic mail, return address, and digital pseudonyms", Communications of the ACM, 24(2), pp.84-88, 1981.

[2] J.D.Cohen(Benaloh), M.J.Fischer, "A Robust and verifiable cryptographically secure election scheme", Proc. 26th IEEE Symposium on the Foundations of Computer cience(FOCS), pp.372-382, IEEE, 1985.

[3] A.Fujioka, T.Okamoto, and K.Ohta, "A practical secret voting scheme for large scale elections", In Advances in Cryptology-AUSCRYPT'92, pages 244-251, 1992.

[4] A.Shamir, "How to Share a Secret", Communications of ACM, Vol.22, No.11, pages 612-613, 1979.

[5] 원동호, "현대 암호학", 도서출판그린, 2003.

[6] 김동균, 김은정, "공개키 암호학과 전자 투표", 청문각출판사, 2003.

[7] 이임영, "E-Vote 종이 영수증 발급 기술", An International Conference on E-Voting and Electronic Democracy: Present and the Future, 2005.

[8] http://www.geneve.ch/evoting/english/

[9] T.Christin, A.H.Trechsel, "Who votes via the Internet?", http://www.geneve.ch/evoting/english/doc/rapports/200409_rapport_carouge_meyrin.pdf, 2004.

[10] http://fvap.gov/services/evoting.html

[11] D.Jefferson, A.D.Rubin, B.Simins, D.Wagner, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", http://www.servesecurityreport.org/, 2004.

[12] "Cryptography and Information Security Group Research Project: Electronic Voting", http://theory.lcs.mit.edu/~cis/voting/voting.html

[13] R.Joaquim, A.Zúquete, P.Ferreira, "REVS - A Robust Electronic Voting System", IADIS International Conference e-Society 2003, 2003.

저자약력

이 윤 호

1991년 성균관대학교 정보공학과(공학사)
1993년 성균관대학교 대학원 정보공학과(공학석사)
1993년~2000년 한국통신 연구개발본부 전임연구원
2000년~2005년 KBS인터넷(주) 기술지원팀장
2005년~현재 성균관대학교 컴퓨터공학과 박사과정 재학중
관심분야 : 암호이론, 정보보호 응용, 전자투표, 워터마킹

이 광 우

2005년 성균관대학교 정보통신공학부(공학사)
2005년~현재 성균관대학교 대학원 컴퓨터공학과 석사 과정 재학중
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표, 워터마킹

김 승 주

1994년 성균관대학교 정보공학과(공학사)
1996년 성균관대학교 대학원 정보공학과(공학석사)
1999년 성균관대학교 대학원 정보공학과(공학박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2001년~현재 한국정보보호학회 논문지편집위원
2002년~현재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재 성균관대학교 정보통신공학부 교수
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
현재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정통부지정 정보보호인증기술연구센터 센터장
관심분야 : 암호이론, 정보이론, 정보보호