情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

# 전자투표 시스템의 안전성

이 윤 호*, 이 광 우*, 김 승 주**, 원 동 호***

요 약

전자 선거는 세계 각국에서 이미 성공적으로 실시되고 있으며 많은 나라에서 이의 도입을 긍정적으로 검토하고 있다. 우리나라에서도 선거관리위원회를 중심으로 2005년 초 전자 선거 도입 일정을 발표하고 본격적으로 전자투표 시스템 개발에 박차를 가하고 있다. 대규모의 전자 선거 실시 경험이 전무한 우리나라에서는 외국의 실시 사례를 면밀히 분석하는 것이 무엇보다 중요한데, 미국에서 많이 사용되고 있는 AccuVote-TS 전자투표 시스템에 대한 안전성 분석 결과는 우리나라에 시사하는 바가 매우 크다고 할 수 있으며 우리나라의 전자투표 시스템 개발에 반드시 참고해야 할 내용이다. 또한, 전자투표에 대한 두 가지 큰 이슈인 오픈 소스 정책에 대한 장단점과 안전한 영수증 발급 방안에 대한 연구도 함께 진행해야 할 것으로 생각된다. 이를 위해 본 고에서는 AccuVote-TS 전자투표 시스템에 대한 안전성 분석 결과를 소개하고, 전자투표 시스템의 안전성과 신뢰성을 높이기 위한 방안으로 오픈 소스 정책과 영수증 발급 방안에 대해 설명하여 향후 전자투표 시스템 개발 및 관련 연구 진행에 도움이 되고자 한다.

## Ⅰ. 서 론

선거 제도는 구성원의 의사를 정책에 반영할 수 있는 효율적인 방안으로서 민주주의의 근간을 이루고 있으며, 고대에서 현대에 이르기까지 보통 선거, 평등 선거, 직접 선거 및 비밀 선거 등 이른바 선거의 4대 원칙이 정립되었다. 선거 결과는 선거에 참여한 구성원만의 의사로 결정되기 때문에 세계 각국은 다양한 방법을 통해 자국민의 선거 참여를 유도하고 있지만 투표 참여율은 계속해서 저하되고 있는데, 이는 세계 각국이 공통적으로 겪는 문제라고 할 수 있다. 이의 원인으로 투표 횟수의 증가나 사회의 복잡성 증대를 들기도 하지만 다른 원인으로 한정된 투표 기간, 제한된 투표 방법, 유권자의 실수로 인한 무효표 발생 및 부정 선거나 개표 오류로 인한 신뢰성 저하 등 여러 가지를 생각할 수 있다.

전자투표는 이러한 문제를 효과적으로 해결하기 위한 방안으로 세계 각국은 기존 종이투표를 대체하기 위해 다각적으로 도입을 검토하고 있으며, 미국, 일본, 호주 및 유럽의 일부 국가에서는 이미 시험 실시하였거나 시행중에 있다. 우리나라의 경우는 중앙선거관리위원회에서 올 해 초 터치스크린 방식의 전자투표기 도입과 인터넷 투표 실시 계획을 담은 전자투표 실시 계획을 발표한 이후 전자투표 도입을 위한 기반 연구와 제품 개발에 박차를 가하고 있다. 전자투표는 기존 종이투표 방식에 비해 선거에 소요되는 시간이나 금전적인 비용을 절감할 수 있고, 무효표를 획기적으로 줄일 수 있으며, 오류 없는 개표 및 집계가 가능하고, 사람의 왕래가 잦은 곳에 설치할 수 있는 키오스크(kiosk) 투표기를 이용할 경우 투표에 따르는 시간, 공간적인 제약을 어느 정도 완화시킬 수 있다는 장점이 있다.

하지만, 전자투표 실시에 신중해야 한다는 의견도 많다. 실제로 미국은 비교적 일찍 전자투표를 도입한 나라 중의 하나인데, 지난 2004년에 실시된 미국의 대통령 선거에서는 전자투표와 관련하여 많은 문제가 발생하였다. 전자투표기의 고장으로 인해 투표가 몇 시간씩 지연되기도 하였으며, 투표기의 투표 용량을 초과하여 이후의 투표 결과가 반영되지 않는 치명적인 문제까지 발생하였다. 전자투표기의 문제뿐만 아니라

* 성균관대학교 정보보호그룹 ({younori, kwlee}@dosan.skku.ac.kr)
** 성균관대학교 정보통신공학부 조교수(skim@ece.skku.ac.kr)
*** 성균관대학교 정보통신공학부 정교수(dhwon@ece.skku.ac.kr)

집계 과정에서도 특정 선거구의 결과가 중복해서 반영되는 등 전자투표와 관련하여 1,444건에 이르는 문제가 보고되었다.[17] 미국의 예에서 보듯이 전자투표 방식은 투표 과정에서 돌이킬 수 없는 심각한 문제를 야기할 수도 있으며 이로 인해 사회적인 혼란을 불러올 수도 있는 만큼 전자투표 전 과정에 대한 보다 철저한 사전 점검이 필요하다고 할 수 있다.

이를 위해 본 고에서는 미국에서 대표적으로 사용되고 있는 AccuVote-TS[4] 전자투표 시스템에 대한 분석 사례[1-3]를 정리하여 전자투표 실시를 앞두고 있는 우리나라에서 참고할 수 있도록 하였다. 또한, 전자투표 시스템 개발에 있어서 논란이 되고 있는 오픈 소스 정책이 갖는 장점과 개발 현황을 살펴보고 마지막으로 전자투표 시스템에 대한 신뢰를 제고할 수 있는 영수증 발급에 대해 알아보도록 한다.

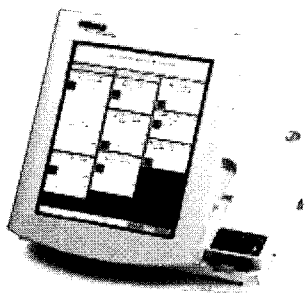
## II. 전자투표 시스템

전자투표 시스템은 크게 지정된 투표소에서 실시되는 투표소 전자투표 방식과 인터넷이나 휴대폰 등을 이용하는 원격 전자투표로 구분할 수 있다. 인터넷 등을 이용한 원격 전자투표는 매표 가능성이나 네트워크 취약점 등으로 인해 아직은 실험적인 단계에 머물러 있거나 해외 부재자 투표 등 극히 제한적인 환경에서만 실시를 고려하고 있다. 이에 반해 현재 실시되고 있는 전자투표는 각 유권자가 지정된 투표소나 키오스크에 설치된 DRE 시스템을 이용하여 투표하면 이를 전자적으로 기록하여 서버에 전송하고 서버에서는 고속으로 집계하는 방식이다. 이 장에서는 DRE 시스템을 이용한 전자투표 시스템과 인터넷 투표 시스템에 대해 간략히 설명하도록 한다.

### 2.1 DRE(Direct Recording Electronic) 시스템

DRE는 투표지에 유권자가 펜이나 도장 등으로 원하는 후보자를 기표하는 종이투표 방식의 여러 문제점을 개선하기 위해 투표 과정을 전자적으로 처리하도록 고안한 장치이다. 일반적으로 DRE는 특수 목적으로 제작된 컴퓨터로 볼 수 있는데, 유권자는 펜과 투표용지 대신 터치 스크린을 이용하여 투표를 하게 된다. (그림 1 참조)

DRE를 이용한 전자투표는 기존 종이투표와는 달리 투표자가 자신의 투표 결과에 대해 물리적으로 검증할 수 있는 방법이 없기 때문에 신뢰하지 못하는 문제가 있다. 즉, 화면에 표시되는 내용과 실제 기록되는 전자적인 내용이 서로 일치하지 않을 수도 있다는 것인데, DRE 시스템의 신뢰성 제고는 전자투표 실시의 성패를 가르는 중요한 문제이다. 하지만 종이투표가 갖는 근본적인 한계, 즉 투표자의 실수로 인한 사표 발생, 투·개표에 소요되는 많은 비용 그리고 개표 결과에 대한 신뢰성 저하를 해결할 수 있는 유일한 대안이 전자투표라는 점에서 언제까지 전자투표 실시를 미룰 수는 없는 상황이다.



[그림 1] AccuVote사의 AccuVote-TS DRE 전자투표 시스템

특히 종이투표 방식에서의 개표 과정은 수작업에 상당 부분 의존할 수밖에 없기 때문에 정확한 개표 결과를 기대하기는 어려운 것이 사실이다. 실제로 미국의 2000년 대선에서도 박빙의 차이로 당락이 결정되었는데, 재검표를 할 때마다 다른 결과가 나와 더 이상 재검표를 하지 않기로 결정하는 등 사회적으로 큰 혼란을 겪기도 하였다.

하지만, 미국에서 이미 오래 전부터 사용되던 DRE 전자투표기인 AccuVote-TS에 대한 안전성 분석 결과는 아직 전자투표가 종이투표 방식의 문제를 완벽하게 해결하기에는 부족함을 보여주고 있다.

### 2.2 인터넷 투표 시스템

인터넷 투표 시스템은 시간과 공간적인 제약을 없앤 궁극적인 전자투표 방식으로서 선거 과정에 많은 변화가 있을 것으로 예상된다. 각 유권자는 자신이 원하는 장소에서 휴대폰, PC 또는 TV 등을 통해 투표할 수 있기 때문에 투표율을 높이면서 선거 관리 인력, 투·개표에 소요되는 시간이나 금전적인 비용을 획기적으로 절감할 수 있을 것으로 기대되고 있다. 반면 인터넷 투표 시스템은 비밀 선거의 원칙이 훼손될 수 있고, 각종 네트워크에 대한 침해를 완벽하게 차단할 수 없으며 유권자가 선거 과정을 신뢰하지 못하는 문제가 발생할 수 있다. 따라서 인터넷 투표 시스템은 전면적인 실시보다는 해외 부재자 등 극히 일부를 대

상으로 실시하는 것을 검토하고 있는 실정이다. 실제로 미국에서는 국방성 산하 FVAP(Federal Voting Assistance Program)의 주관으로 2004년 대선에 해외 군인 등 일부 부재자를 대상으로 인터넷 투표를 실시하려는 SERVE(Secure Electronic Registration and Voting Experiment) 프로젝트[19]를 추진하였으나, 인터넷 투표가 갖는 여러 문제점에 대한 지적으로 인해 취소되기도 하였다.[20]

인터넷 투표는 위에서 지적한 네트워크 침해 등의 문제와 함께 기본적으로 비밀 선거의 원칙이 지켜지기 어려운 문제가 있지만 스위스에서는 큰 무리없이 인터넷 투표를 성공적으로 실시하고 있어 대조를 이루고 있다.[21] 이것은 사회, 문화적인 차이 때문인 것으로 분석하고 있는데, 스위스에서는 이미 오래 전부터 우편 투표를 실시해온 나라였다. 우리나라에서도 궁극적으로 인터넷 투표 실시를 계획하고 있는데, 기술적인 연구와 함께 사회, 문화적인 연구도 함께 진행되어야 할 것이다.

## Ⅲ. AccuVote-TS 시스템의 취약점

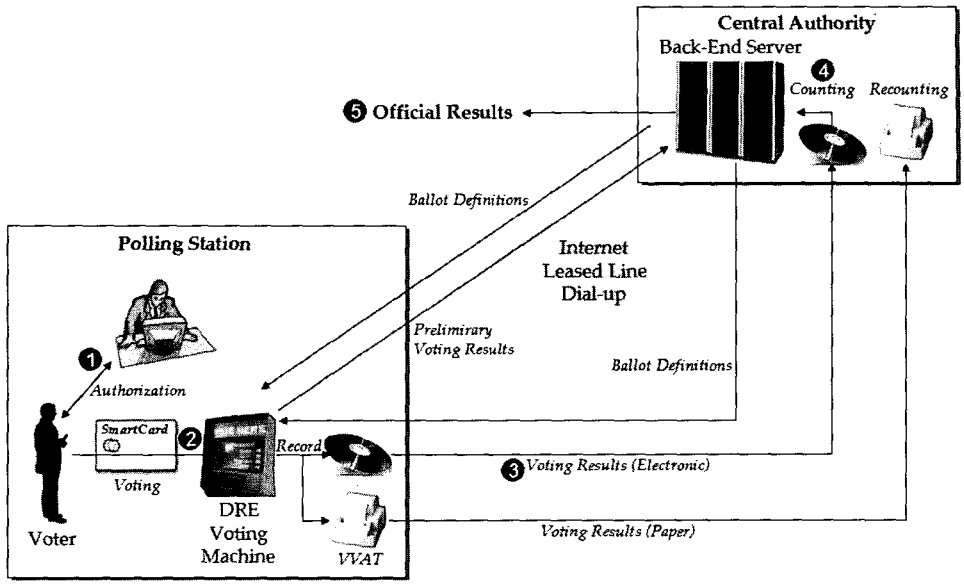
전자투표 시스템에 대한 안전성 분석은 공학적인 접근 뿐만 아니라 법적, 제도적인 측면과 문화적인 측면까지 모두 고려되어야 한다. 예를 들어, 미국의 인터넷 투표 실시 프로젝트인 SERVE는 결국 시행되지 못했지만 스위스 같은 경우는 인터넷 투표를 성공적으로 실시한 대표적인 예이다. 이는 기술적인 차이가 아닌 문화적인 차이로 보아야 하는데, 스위스는 이미 오래 전부터 우편 투표 제도가 잘 정착되어 인터넷 투표에 대한 국민적 합의가 비교적 잘 이루어져 있다고 볼 수 있다. 본 논문에서는 이런 여러 가지 고려 사항 가운데 전자투표 시스템의 기술적인 안전성 측면, 특히 DRE 라고 부르는 전자투표 단말기의 기술적 안전성을 다루도록 한다.

AccuVote-TS 전자투표 시스템[4]은 미국 Diebold사가 개발한 전자투표 시스템으로서 미국 내에서 비교적 오랫동안 널리 사용된 DRE 전자투표 시스템 중의 하나이다. 특히 AccuVote-TS 시스템 S/W에 대한 CVS(Current Versions System) 소스 코드가 인터넷에 공개되어 많은 전문가들로부터 검증을 받기도 하였다.[1-3,6]

이번 장에서는 이 가운데 Tadayoshi Kohno, Adam Stubblefield 그리고 Aviel D. Rubin이 발표한 논문[1]을 중심으로 AccuVote-TS에 대한 분석 결과를 보도록 하겠다. 이 분석 결과는 향후 전자투표 실시를 계획하고 있는 우리나라에서 반드시 참고해야 하는 자료라고 할 수 있다. 표 1은 Tadayoshi Kohno, Adam Stubblefield 그리고 Aviel D. Rubin의 안전성 분석 결과를 전체적으로 정리한 내용이다.

〔표 1〕 AccuVote-TS의 취약점 분석 결과 요약

| | 투표자 | 투표소 요원 (투표 기록장치 접근 가능) | 투표소 요원 (네트워크 접근 가능) | 인터넷 서비스 업체 | OS 개발자 | 투표기 개발자 |
|---|---|---|---|---|---|---|
| 위조 스마트카드를 이용한 중복 투표 | • | • | • | | | |
| 불법적인 관리자 권한 획득, 투표 강제 종료 | • | • | | | • | • |
| 시스템 환경 설정 변경 | | • | | | • | • |
| 투표지 정의 변경 | | • | • | • | • | • |
| Configuration 변경을 통한 투표 누락 | | • | • | • | • | • |
| 가상의 투표기 위장 | | • | • | • | • | • |
| 임의적인 투표의 생성, 삭제, 변경 | | • | • | • | • | • |
| 투표로부터 투표자 확인 | | • | • | • | • | • |
| 감사 log 조작 | | • | • | • | • | • |
| 투표 시작 지연 | | • | • | • | • | • |
| 코드에 backdoor 삽입 | | | | | • | • |




〔그림 2〕 전자투표 실시 과정

### 3.1 전자투표 진행 과정

AccuVote-TS 시스템을 이용한 선거 진행 과정은 다음 그림 2와 같다.

① 유권자 확인
투표할 권한이 있는 유권자는 확인 과정을 거쳐 투표할 수 있는 스마트카드를 발급받는다.

② 투표 및 투표 기록
유권자는 발급받은 스마트카드를 투표기에 삽입하고 화면에 표시된 후보자 목록에서 원하는 후보를 선택한다. 선택한 내용은 최종 확인을 거쳐 전자적으로 기록된다.

③ 투표 결과 전송
선거 종료 후 투표 결과는 중앙 서버로 전송된다. 이 때 투표 결과를 담고 있는 메모리 카드를 오프라인으로 전송하는 것 이외에 투표 중에도 필요하다면 인터넷, 전용선 또는 전화망 등 네트워크를 이용한 전송도 가능하다.

④ 투표 결과 집계
중앙 서버에서는 최종적으로 각 투표소의 전자 투표기에서 전송한 투표 기록을 전자적으로 집계한다.

⑤ 집계 결과 발표 및 재검표
전자적으로 집계된 결과는 공식 발표를 하는데, 집계 결과에 이의를 제기할 경우 별도로 보관하고 있는 VVAT를 이용하여 물리적인 재집계를 거칠 수도 있다.

### 3.2 스마트카드

AccuVote-TS 시스템은 인가된 유권자에게 키와 함께 해당되는 후보자 목록 등을 담고 있는 스마트카드를 발급하도록 하고 있다. 유권자는 투표를 마치면 이 카드를 반납하고 반납된 카드는 다음 유권자를 위해 초기화된다. 일반적으로 투표를 마친 스마트카드는 재사용이 불가능하기 때문에 중복 투표는 불가능하지만 AccuVote-TS 시스템에서 사용하는 스마트카드는 얼마든지 위조할 수 있다는 문제가 발견되었다. 이는 AccuVote-TS 시스템이 스마트카드를 단지 메모리 카드로 사용하고 있어 스마트카드와 투표기의 통신 내용을 한 번만 캡쳐하면 위조된 스마트카드를 만들 수 있기 때문이다. 따라서 위조된 스마트카드를 이용하면 유권자 한 명이 여러 번 투표할 수 있는 심각한 문제가 발생할 수 있다. 이는 투표소 관리자가 사용하는 관리용 카드도 마찬가지여서 위조된 관리용 카드를 이용하여 투표자가 임의로 투표를 종료시킬 수도 있다.

### 3.3 데이터 저장

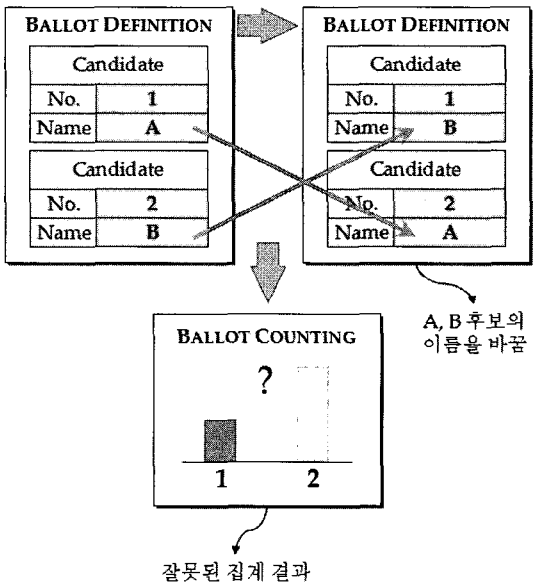
AccuVote-TS 시스템은 유권자의 투표 결과나 시스템 환경 설정 등 각종 중요한 데이터를 보관하는데 있어서 예상되는 여러 가지 문제점을 고려하지 않고 있다. 예를 들어, 중요한 데이터는 일반적으로 데이터 저장소를 분리하여 중복 보관하는 것이 일반적인데 Windows CE를 운영체제로 사용하는 경우에는 /Storage Card가 항상 외부의 메모리 카드를 가리

```
long GetProtectedCounter()
{
  DWORD protectedCounter = 0;
  CString filename = ::GetSysDir();
  filename += _T("system.bin");
  CFile file;
  file.Open(filename, CFile::modeRead | CFile::modeCreate | CFile::modeNoTruncate);
  file.Read(&protectedCounter, sizeof(protectedCounter));
  file.Close();
  return protectedCounter;
}
```

〔그림 3〕 AccuVote-TS의 counter 반환 함수

키는 것이 아니기 때문에 보다 세심한 주의가 필요하다. 또한, 투표기의 일련번호나 스마트카드 리더기와 통신을 위한 COM 포트 등 환경과 관련된 정보는 Windows의 레지스트리(HKEY_LOCAL_MACHINE \Software\Global Election Systems\AccuVote-TS4)에 보관되는데 이러한 중요 정보에 대한 무결성 검증 과정이 포함되어 있지 않아 위조나 변조가 일어나도 이를 확인할 수 있는 방법이 없다는 문제도 있다. 레지스트리 내의 정보 이외에도 중요한 정보 가운데 하나인 투표 카운터가 파일 시스템 내에 특별한 보호 장치없이 보관되고 있다. 이 카운터가 임의로 변경되었을 때는 실제 투표 기록과 카운터의 불일치가 생겨 투표 기록에 대한 신뢰성에 문제가 발생할 수 있다.(그림 3 참조)

더욱 심각한 문제는 투표 형식을 정의한 파일(Ballot Definition)이 암호화나 암호학적 무결성 검증 등의 방법으로 보호되지 않고 있다는 것이다. 이는 매우 심각한 결과를 초래할 수 있는데 예를 들어, 기호 1번이 A후보, 기호 2번이 B후보라고 했을 때 A와 B를 서로 바꾸게 되면 투표 결과는 전혀 엉뚱하게 나타날 수도 있다. 투표 기록에는 후보 신상 정보가 기록되지 않는 것이 일반적이기 때문에 문제는 더욱 심각하다. 즉, 그림 4와 같이 투표자의 이름을 바꾸거나 번호를 바꿔 화면에 표시했을 때 유권자는 잘못된 화면을 근거로 투표할 수 있고 이는 잘못된 집계 결과를 초래하게 된다.




〔그림 4〕 Ballot Definition 변조를 통한 공격

### 3.4 키 관리와 암호 기법의 오용

AccuVote-TS 시스템은 안전한 투표 시스템을 위한 여러 암호 알고리즘이 구현되어 있지만, 구현상의 오류로 인해 안전성이 크게 저하되어 있음이 확인되었다. 대표적인 문제점을 보면 안전하지 않은 난수 발생 알고리즘의 사용, 암호 운용 모드의 잘못된 사용, 잘못된 키 관리, 잘못된 암호 알고리즘 적용 순서 그리고 안전성이 떨어지는 DES 암호 방식 사용 등이 그것이다.

○ 안전하지 않은 난수 발생 알고리즘의 사용

AccuVote-TS 시스템 내에는 사용자 투표 결과에 유일한 시리얼 번호를 무작위로 할당하기 위한 난수 발생 알고리즘으로 LCG(Linear Congruential Generator)를 사용하는데, 이는 암호학적으로 전혀 안전하지 않은 난수 발생 알고리즘이다. 더욱이 seed 값으로 각 단말에 따라 고정된 값이 입력되고 있어 난수 발생기로서의 의미를 상실하고 있다.

○ 암호 운용 모드의 잘못된 사용

비밀키 암호 방식의 운용 모드로서 CBC를 사용하고 있지만 IV 값으로 "00000000"을 이용하고 있

다. IV 값은 당연히 강력한 난수 발생 알고리즘으로부터 생성된 난수 값이어야 한다.

○ 잘못된 키 관리

투표 값이나 각종 중요한 데이터를 암호화하기 위해 사용되는 암호 키는 투표소 또는 투표기마다 달라야 하지만 AccuVote-TS는 전체 투표기에 걸쳐 동일한 것으로 파악되었다. 암호 키는 소스 코드 내에 16진수 값 "F2654hD4"로 고정되어 있었는데, 이는 1998년부터 변경이 없었던 것으로 파악되었다.

○ 잘못된 암호 알고리즘 적용 순서

AccuVote-TS 시스템은 무결성과 기밀성 보장을 위한 방안으로 암호화하기 전 데이터에 대한 CRC 값과 암호문을 보관하는 것으로 나타났는데, 이는 암호문을 먼저 생성하고 이에 대한 CRC를 계산하는 것보다 안전한 방법이 아니다. 더욱이 CRC는 키를 이용하는 방식이 아니기 때문에 평문에 CRC를 계산하는 것은 사실상 무결성을 보장한다고 보기는 어렵다. CRC는 HMAC-SHA1 등과 같이 암호학적으로 안전한 체크섬 알고리즘으로 대체되어야 한다.

### 3.5 투표자 추적

AccuVote-TS 시스템은 비밀 투표의 원칙을 지키기 위해 투표 값으로부터 투표자를 추적할 수 없도록 중앙 서버에 투표 값을 전송할 때 각 투표 값마다 고유한 난수를 일련 번호로 할당하고 중앙 서버는 이를 일련 번호 순서대로 정렬하여 원래의 순서를 찾지 못하도록 한다. 하지만, 이러한 순서 재정렬이 서버에서 이루어지기 때문에 사실상 투표자 추적을 막지는 못하게 되어 있다. 따라서 보다 근본적으로 투표자 추적을 막기 위해서는, 투표기에서 투표를 기록할 때 순서를 무작위로 만드는 방안이 필요하다.

## Ⅳ. 전자투표 시스템의 안전성과 신뢰성

전자투표 시스템의 안전성과 신뢰성에 의문을 제기하는 가장 큰 이유는 전자투표 시스템에 탑재되는 소프트웨어의 동작을 신뢰할 수 없다는 것이다. 즉, 화면에는 유권자의 선택을 보여주면서 실제로는 다른 후보를 기록할 수도 있다는 의구심이 있을 수밖에 없는데, 이 점은 기존 종이투표 방식과 비교했을 때 극복해야 할 가장 큰 문제이다. 이를 해결할 수 있는 방법은 전자투표 시스템 내부를 공개하는 것과 종이투표에서의 투표 용지와 같이 유권자가 신뢰할 수 있는 물리적인 증거(영수증)를 남기는 것 두 가지로 생각할 수 있다. 물론 이 두 가지에 대해서도 서로 다른 이견이 있다. 첫 번째로 전자투표 시스템 내부를 공개하는 것은 많은 전문가의 검증을 받는 계기가 되기 때문에 전체적인 전자투표 시스템의 안전성을 높일 수 있다는 의견이 있는 반면 오히려 시스템에 대한 취약점을 노출시켜 안전성을 저해할 수 있다는 의견도 있다. 두 번째로 투표 영수증을 남기는 것에 대해서도 유권자의 신뢰를 높일 수 있고 부정한 전자적 집계를 막을 수 있는 유일한 해결 방안이라는 의견과 투표 영수증의 발급이 안전성 향상에 도움을 주는 것은 아니기 때문에 불필요하다는 의견이 있다.[7,8,13,14]

이 장에서는 전자투표 시스템에 있어서 가장 논란이 되고 있는 이 두 가지에 대해 살펴보고 어떤 방안이 전자투표 시스템의 안전성 향상에 도움이 되는지 알아보도록 하겠다.

### 4.1 오픈 소스 개발 정책

대부분의 전자투표 시스템 개발 업체에서는 시스템 내부를 공개하기를 꺼리고 있는 실정이다. 이런 이유로는 취약점 노출로 인한 안전성 저하와 함께 저작권 침해를 들고 있는데, 학계나 공개 소프트웨어 진영에서는 공개적인 개발이야말로 취약점을 조기에 발견하여 안전성을 높일 수 있다고 지적한다. 이는 AccuVote-TS 시스템에 대한 안전성 분석에서도 잘 나타나고 있다.

하지만, 대부분의 상업적인 전자투표기 업체에서는 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 있는데, "Free e-Democracy"[11]와 "The Electronic Voting Machine Project(EVM2003)"[12]가 대표적이다. 각국의 입장도 이에 대해서는 엇갈리고 있는데, 호주를 제외하고는 대부분 오픈 소스 기반의 전자투표 시스템 도입에 소극적인 입장이다. 이런 이유로 "Free e-Democracy" 프로젝트는 2002년부터 중단된 상태이다.

하지만, 안전할 것이라고 믿고 사용되던 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 긍정적

으로 검토해야 할 사안이라고 할 수 있다.

### 4.2 투표자 추적이 불가능한 물리적인 영수증 발급

전자투표 시스템에 투표 결과에 대한 전자적인 기록 장치와 함께 종이 기록 장치도 필요한가에 대해서는 많은 의견이 있다.[13] 불필요하다는 입장에서는 암호학적 기법을 이용하여 유권자가 스스로 자신의 투표가 정확하게 반영되었다는 확신을 줄 수 있고, 전자투표기의 정상 동작 여부를 충분히 감시할 수 있다는 것을 이유로 들고 있는 반면, 반드시 필요하다는 입장에서는 아직 신뢰할 수 없는 전자투표기를 보완하기 위해서는 재검표 해결 방안으로 영수증 역할을 하는 물리적인 수단이 반드시 필요하다는 것을 들고 있다.[14]

하지만 어떤 방식으로든 유권자 자신이 확신을 가질 수 있도록 하기 위해서는 전자적인 처리만으로는 부족하다는 것이 일반적인 견해이다. 이는 현재 대중적으로 사용되는 인터넷 뱅킹과는 조금 다른데, 인터넷 뱅킹 이용자는 물리적으로 영수증을 받지 않더라도 언제든지 자신의 거래 내역을 확인할 수 있지만 전자투표의 경우는 확인하는 것이 불가능하다. 이런 이유로 유권자의 투표 행위에 대한 신뢰를 위해서는 물리적인 영수증 발급이 불가피할 것으로 생각된다.

영수증 발급과 관련한 기술로는 David Chaum의 시각적 암호화를 이용한 영수증 발급 방식,[15] Andrew Neff의 VVPAT 방식,[16] 그리고 VoteHere 사의 scratch ticket 방식 등이 있다.

이 절에서는 VVAT 영수증을 발급할 것인지의 문제보다는 영수증을 발급했을 때 "비밀 투표"의 원칙이 지켜질 수 있는지에 초점을 맞추도록 한다. 즉 물리적인 영수증이 투표 결과로부터 투표자를 추적할 수 없도록 함과 동시에 투표자는 자신의 투표 결과를 증명할 수 없어야 한다. 일반적으로 현재 사용되는 전자투표 영수증은 유권자에게 발급하고 확인하도록 하지만 투표소 밖으로의 반출은 "매표" 가능성 등의 이유로 금하고 있다. 따라서 재검표 등을 위해 보관해야 하는 영수증은 다음과 같이 크게 두 가지 발급 방법이 있다.

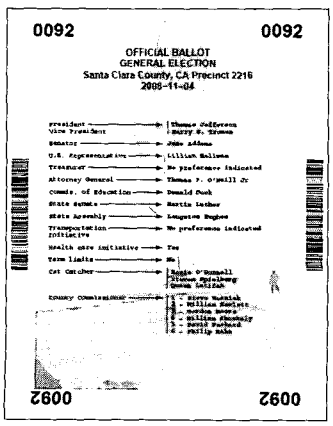
○ 투표 용지 테이프에 기록

영수증을 유권자마다 따로 발급하지 않고 종이 테이프 등에 일렬로 기록하는 방법이다. 일반적으로 유권자는 자신의 투표가 기록된 부분만 확인할 수 있다. 이 방법은 현재 선거관리위원회에서 검토하고 있는 방안으로 전자적인 리더기를 이용하여 재검표를 빠르고 정확하게 할 수 있다는 장점이 있다.

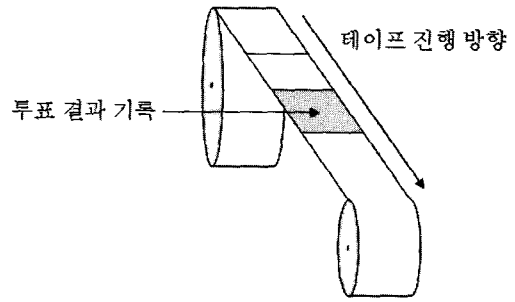
○ 투표 용지 보관함 이용

현재의 종이투표 방식에서 사용하는 투표 용지 보관함과 같이 유권자마다 발급된 투표 영수증을 유권자가 검증한 후 직접 보관함에 투입한다. 재검표에 소요되는 시간은 현재의 종이투표 방식과 비슷하다.

투표 용지 테이프를 이용할 경우 재검표가 빠르다는 장점이 있지만 투표 순서와 기록 순서 추적을 통해 투표자를 확인할 수 있다는 단점이 있다. 하지만, 투표 용지 보관함을 이용하는 방법은 현재의 종이투표 방식과 유사하며 재검표에 소요되는 시간이 현재와 비슷하기 때문에 전자투표 실시가 갖는 신속한 투개표의 장점이 사라지게 된다. 따라서, 빠르고 정확한 재검표를 위해 투표 용지 테이프에 기록하되 기록 순서와 투표 순서를 연결할 수 없도록 하는 방안에 대한 연구가 진행되어야 할 것이다.




〔그림 5〕 EVM2003의 VVAT




〔그림 6〕 테이프를 이용한 투표 영수증 기록 방법

## V. 결 론

본 고에서는 AccuVote-TS 소스 코드를 이용한 안전성 분석 사례를 통해 기존 전자투표 시스템이 갖는 문제점에 대해 살펴보았고 전자투표 시스템에 대한 두 가지 이슈인 오픈 소스 정책의 여부와 영수증 발급 방안에 대해 살펴보았다. AccuVote-TS에 대한 안전성 분석 결과는 전자 선거를 실시하려는 우리나라에 많은 것을 시사해주고 있으며 이를 충분히 고려하여 추진해야 할 것으로 생각된다. 중앙선거관리위원회는 최근의 여러 가지 해킹 사례에 대해 전자투표 실시계획을 연기하는 경우가 있더라도 충분히 안전성 검증을 하도록 하겠다고 밝혔는데 이는 바람직한 결정으로 세계 각국의 전자투표 실시에 따른 문제점을 보다 면밀히 검토하고 해결 방안을 마련한 이후 실시해도 늦지 않다. 또한, 미국 연방선거관리위원회(FEV)의 투표 시스템 표준[5]과 투표 시스템 및 투표 데이터 호환을 위한 IEEE의 표준[9,10]도 참고해야 할 자료이다. 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] Tadayoshi Kohno, Adam Stubblefield, and Aviel D. Rubin, "Analysis of an Electronic Voting System", IEEE Symposium on Security and Privacy, IEEE, May 2004

[2] SAIC, "Risk Assessment Report - Diebold AccuVote-TS Voting System and Processes", http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf, 2003

[3] RABA, "Trusted Agent Report - Diebold AccuVote-TS Voting System", http://nob.cs.ucdavis.edu/~bishop/notes/2004-RABA/2004-RABA.pdf, 2004

[4] Diebold, Diebold's Election Systems, http://www.diebold.com/ dieboldes/

[5] FEC, "2002 Voting System Standards/ Guidelines", http://www.eac.gov/election_resources/vss.html, 2002

[6] Compuware Corporation, "Direct Recording Electronic(DRE) Technical Security Assessment Report", http://www.sos.state.oh.us/sos/hava/files/compuware.pdf, 2003

[7] David L. Dill, Rebecca Mercuri, Peter G. Neumann, and Dan S. Wallach, "Frequently Asked Questions about DRE Voting Systems", http://www.verifiedvoting.org/article.php?id=5018

[8] Rebecca Mercuri, "Electronic Vote Tabulation Checks and Balances", PhD thesis, Univ. of Pennsylvania, Philadelphia, PA, 2000

[9] IEEE Voting Equipment Standards, http://grouper.ieee.org/groups/scc38/1583/, Project 1583, IEEE

[10] IEEE Voting Systems - Electronic Data Interchange, http://grouper.ieee.org/groups/scc38/1622/, Project 1622, IEEE

[11] Free e-Democracy Project, http://www.j-dom.org/h/n/BIO/HOME/ALL/26/, 2002

[12] The Electronic Voting Machine Project, http://evm2003. sourceforge.net/, 2003

[13] CNN News.com, "E-voting: Nightmare or nirvana?", http://news.com.com/E-voting+Nightmare+or+nirvana/2009-1028_3-5251471.html, 2004

[14] Rebecca Mercuri, "Rebecca Mercuri's Statement on Electronic Voting", http://www.notablesoftware.com/RMstatement.html, 2001

[15] David Chaum, "Secret Ballot Receipts and Transparent Integrity - Better and less-costly electronic voting at polling places", http://www.vreceipt.com/article.pdf

[16] Dennis Vadura and Frank Wiebe, "What is A Meaningful 'Voter Verified Paper Audit Trail?'", http://www.accupoll.com/TheAccuPollAdvantage/WhitePapers/VVPAT.pdf, 2003

[17] Election Incident Reporting System,

https://voteprotect.org/index.php?display=EIRMapNation
[18] 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
[19] FVAP, "Secure Electronic Registration and Voting Experiment (SERVE)", http://fvap.gov/services/evoting.html
[20] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "A Security Analysis of the SERVE", http://www.servesecurityreport.org/, 2004
[21] Internet voting in Geneva, Frequently Asked Questions, http://www.geneve.ch/evoting/english/faq.asp

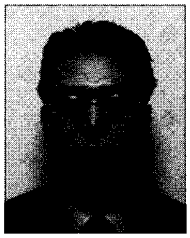
## 〈著 者 紹 介〉

**이 윤 호 (Yunho Lee)**
학생회원

1987년~1993년 : 성균관대학교 정보공학과(학사, 석사)
1993년~2000년 : 한국통신(KT) 연구개발본부 전임연구원
2000년~2005년 : KBS인터넷(주) 기술지원팀장
2005년~현재 성균관대학교 컴퓨터공학과 박사과정
〈관심분야〉 암호이론, 정보보호 응용, 전자투표, 워터마킹

**이 광 우 (Kwangwoo Lee)**
학생회원

2005년 2월 : 성균관대학교 정보통신공학부 졸업(공학사)
2005년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표, 워터마킹



**김 승 주 (Seungjoo Kim)**
종신회원

1994년 2월~1999년 2월 : 성균관대학교 정보공학과(학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회 , 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 6월~현재 : 교육인적자원부 유해정보차단 자문위원
〈관심분야〉 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

**원 동 호 (Dongho Won)**
종신회원

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