디지털산업정보학회 논문지 제5권 제2호-2009년 6월

전자주민증 도입에 따른 다각적인 분석*

이 영 교** · 안 정 희***

Multilateral Analysis on the Implementation of Electronic Resident Registration Cards

Lee, Young Gyo · Ahn, Jeong Hee

〈Abstract〉

As our society is changed to the information & digital society based on the internet, the requirement that the analog certificate of Korean residence is changed to digital one is increased. The Korean Government selected the smart card of 72 KB for the digital certificate of Korean residence and try to insert the personnel information of 41 items to it. The method that the numerous personnel information is stored in one smart card is convenience to use. If the certificate of residence is lost, the number of personnel information is misused or spreaded thorough the Internet by the hacking. In this paper, we analyze the problem about the digital certificate of Korean residence and propose the countermeasure about the problem. In the proposal, the digital certificate of residence have only the certificate. Therefore, the size of the smart card is minimized and can be canceled at the loss of the certificate of residence. And the exposure worry of personnel information will be decreased.

Key Words : Digital Certificate of Residence, Smart Card, Certificate

Ⅰ. 서론

사회가 인터넷을 기반으로 하는 정보화 및 디지털 사회로 급속히 변모하고 있으며 RFID(Radio Frequency IDentification)를 기반으로 하는 USN(Ubiquitous Sensor Network) 시대로 발전되어 가고 있다. 또한 정부에서도 다양한 컴퓨터가 현실 세계의 사물과 환경 속으로 스며들어 상호 연결되어 언제, 어디서나 자유롭게 이용할 수 있는 최적의 컴퓨팅 환경이 구현되는 사회인 'u-Korea'를 비전으로 제시하고 있다. 그에 따라 그동안 아날로그 형태로 유지되고 있는 주민등록증에 대한 전자화의 필요성 및 요구도 높아지고 있다.

이미 행정자치부는 1990년대 중반에 전자주민증을 도입하려고 추진하였으나 사생활 침해라는 여론에 밀려 전자주민증 도입 사업이 실패로 돌아갔다. 그러나 전자주민증 도입은 디지털을 기반으로 하는 유비쿼터스 시대에 반드시 필요하며 더 이상 미룰 수 없는 일이다. 행정자치부는 2007년, 72KB 용량의 IC 칩이 내장된 새로운 전자주민등록증의 시제품을 완성하고 2008년에 공무원과 시민 등, 1만 명을

* 본 논문은 2008년 서일대학 학술 연구비에 의해 연구되었음.
** 서일대학 인터넷정보과 전임강사 (교신저자)
*** 두원공과대학 컴퓨터정보과 부교수

대상으로 시험 운영할 계획이다. 따라서 본 연구에서는 새로 도입될 전자주민증을 다각적으로 분석하여 도입 후에 야기될 수도 있는 문제점들을 줄이고자 한다. 논문의 나머지 부분은 다음과 같이 구성되어진다. 2장에서는 주민등록증의 발전과정과 전자주민증의 도입배경을 살펴본다. 3장에서는 새로 도입될 전자주민증의 문제점을 분석한다. 그리고 4장에서 이들 문제점들을 해결하기 위한 방법들을 제안하고 마지막으로 5장에서 결론을 맺는다.

II. 주민등록증의 발전과정

본 장에서는 주민등록증의 발전과정과 전자주민증의 도입 배경에 대해 살펴본다.

2.1 주민등록증의 탄생과 발전과정

주민등록증은 대한민국 국민으로서 국내에 주소를 두고 거주하는 주민임을 증명하는 증명서이다. 주민등록증의 시초를 살펴보면 조선시대 호패제도로 거슬러 올라갈 수 있다. 조선 태종 13년에 처음 시행되었던 호패제도는 조선시대 16세 이상의 남자가 소지하던 신분증명서이었다. 호패(號牌)는 허리에 차는 길쭉한 형태의 패로, 한 면에 성명과 태어난 해의 간지를 쓰고 그 뒷면에 관아의 낙인을 찍어 표시하였다. 이 제도는 호적법의 시행을 위한 보조역할을 담당했으며 호구를 정확히 하여 민정(民丁)의 수를 파악하고, 직업과 신분을 명확히 파악하며, 군역과 요역의 기준을 밝혀 백성의 유동과 호적 편성상의 누락과 허위 조작을 방지하기 위한 것이었다[1].

현재 우리가 사용하고 있는 주민등록증의 전신이라 할 수 있는 신분증이 등장한 것은 한국전쟁 직후이다. 6·25 전쟁직후인 1950년에 시민증과 도민증이 급조되었다. 각 시·도는 주민들에게 시·도민증을 발급하였는데 시민증이나 도민증에는 지금의 주민등록증과 달리 개인의 신상에 관한 자세한 내용이 많이 기재되었다.

<그림 1> 도민증의 모습

시·도민증에는 본적, 출생지, 주소는 물론 직업, 신장, 체중, 특징, 언어, 혈액형 등까지 기재하도록 되어 있어서 그야말로 자기소개서나 다름이 없었다. 시·도민증은 1950년부터 1961년까지 사용되었으며 <그림 1>은 당시에 사용되던 도민증을 나타내고 있다[1, 2].

1962년 1월, 기류법이 제정되어 주민등록 신고를 하도록 되었고, 1962년 5월에는 '주민등록증법'이 제정, 공표되었으나 새 신분증의 발급은 진전을 보지 못하다가, 1968년 1·21 사태 직후에 불온분자를 색출하고 주민의 동태를 파악한다는 취지로 법 개정에 속도가 붙었다. 1968년 5월에 주민등록법이 개정되어, 병역사항과 특수기술사항을 신고사항으로 규정하고 주민등록증 제도가 도입되었다.

<그림 2> 1968년 개정 주민등록증

이 때 주민등록증은 만 18세 이상의 성인에게 발급되는 것이었지만 발급 및 부여가 의무적인 사항은 아니었

으며, 또한 이 때 12자리의 주민등록번호제도가 처음으로 도입되었다. 주민등록법이 개정되면서 1968년 10월 20일에 주민등록증이 처음 탄생되었는데 지금처럼 가로형태가 아니라 <그림 2>와 같이 세로로 긴 모양이었다[1, 2].

<그림 3> 1975년 개정 주민등록증

주민등록번호는 앞쪽 번호가 거주 지역을 나타내고 뒤쪽 번호가 일련번호를 나타내는데 예를 들어 110608-100373인 경우 맨 처음 11은 서울, 06은 서대문구, 08은 충정로 3가동이란 뜻이며, 뒷부분은 등록한 사람의 순서, 즉 373번째 등록했다는 의미이다. 이 주민등록증은 1962년부터 1974년까지 사용되었다.

1975년 7월 25일, 앞으로 도래할 정보화시대를 예견하여 주민등록법이 개정되었다. 주민등록번호의 앞 일련번호를 각 개인의 생년월일로 쓰기 시작했으며 바탕색이 변화를 갖는 등 주민등록증이 과도기를 맞게 되었다. 그동안 12자리였던 주민등록번호가 1975년 개정에서 현재와 같은 13자리가 되었다. 주민등록을 거주 사실과 일치시키고 주민등록증 발급대상자 연령을 민방위대 및 전시동원 대상자 연령과 일치시키고자 18세에서 17세로 낮췄다. 이 주민등록증은 1975년부터 1982년까지 사용되었으며 <그림 3>과 같이 전에 사용되었던 주민등록증과 마찬가지로 세로 형태이었다[1, 2].

이전까지는 본적이나 호주가 변경될 경우에 매번 주민등록증을 재발급 받아야 했으나, 1983년 10월부터는 뒷면에 변경내용만 기재할 수 있도록 하고 도안을 변경하며 다시 가로형태의 모양을 갖추어 2차 주민등록증 일

<그림 4> 1983년 개정 주민등록증

제경신이 이루어졌다. 이 주민등록증은 1983년부터 2000년 5월까지 사용되었으며 <그림 4>와 같다[1, 2]. 현재 우리가 사용하고 있는 플라스틱 주민등록증은 새천년을 목전에 둔 1999년 9월에 탄생하였다. 그동안의 주민등록증은 비닐이 씌워진 종이 형태이어서 위·변조 등이 용이하였으며 장기간 사용 시에 훼손이 심했다.

이때에 도입된 주민등록증은 플라스틱 재질에 홀로그램 등의 첨단기술로 제작되어 위·변조가 어렵도록 제작되었다. <그림 5>는 1999년에 개정되어 현재 우리가 사용하고 있는 주민등록증의 모습이다. 이 플라스틱 주민등록증은 2000년 6월부터 전면 사용되었고, 주민등록증 뒷면에 지문을 표시하도록 되었다. 그러나 이 주민등록증은 사진이 아세톤 등의 약품으로 지워지는 등 위·변조가 용이해 범죄에 악용되어, 사회문제로 비화되었다.

<그림 5> 1999년 개정 주민등록증

2.2 전자주민증의 도입배경

국민에게 고유번호를 부여하는 나라는 찾아보기 힘들

다. 워낙 인권침해의 소지가 높다보니 선진국에서는 함부로 채택을 하지 못하고, 아예 위헌이라는 판결을 내린 국가들도 있다. 독일의 경우 주거등록제도와 국가신분증 제도를 두고 있지만, 이 둘은 엄격하게 분리되어있다. 국가신분증을 발급할 때 표시되는 일련번호는 사람이 아니라 증명서 자체에 부여되며 새 신분증을 발급받을 때 부여되는 번호는 단지 의미가 없는 숫자의 나열일 뿐이며 이 일련번호로 DB에서 인적 사항을 추출하는 프로파일링(profiling)이나, 여러 DB자료를 연관시켜 찾아보는 머징(merging)은 엄격히 금지되고 있다[3, 4].

프랑스에서는 개인고유번호를 부여하려는 시도가 몇 번 있었지만, 그때마다 무산되고 말았다. 이미 1979년에 컴퓨터로 읽을 수 있는 형태의 개인신분확인카드(이름과 출생일만 포함되고 개인고유번호는 사용하지 않음) 발급을 계획했지만 그마저 시민 단체의 반발로 취소됐다. 일본 역시 신분등록제도로 호적제도를, 주거등록제도로 주민기본대장제를 두고 있으나, 국민에 대한 개인식별번호제는 채택하지 않고 있다. 주민기본대장카드는 국가가 아니라 시, 읍, 면장이 교부한다. 서비스 제공범위도 법률로 한정되어 있으며 어떤 서비스를 받을 것인지는 주민이 선택하고, 목적 외의 이용은 엄격히 금지된다. 주민표의 코드는 무작위 번호로 주민의 신청에 의해 언제라도 변경이 가능하다[3, 4].

그러나 이와는 정반대되는 움직임도 있다. 신분증이 없거나 허술한 종이신분증을 사용했던 나라들이 하나둘씩 전자신분증의 도입을 추진하는 사례가 생겨나기 시작했다. 이런 시도들은 반대 여론으로 실행되지 못하고 있으나, 편리성과 테러위협 등을 이유로 도입에 찬성하는 목소리도 나오고 있다. 미국의 경우 국민고유번호는 도입하지 못한 대신, 여권이나 비자에 생체인식 칩을 내장하는 방식으로 첨단신분증 도입을 추진하고 있다[4].

"전자주민증" 혹은 "전자주민카드"는 IC(Integrated Circuit) 카드 형태의 주민등록증으로 주민카드라고 한다. 일반 신용카드 크기의 전자주민증 앞면에는 이름과 생년월일, 성별, 사진 등이 담기고 유출 염려가 있는 주민등록번호와 지문정보, 주소 등 개인정보는 내장된 IC 칩에 수록된다. 특히 사진과 글씨는 레이저로 새겨 넣어 탈·변색 등 훼손을 최소화했다. 또 복제를 막고자 자외선을 비추면 태극 문양을 형상화한 문양이 생기도록 했고, '대한민국'이라는 글자를 투명 홀로그램으로 표시했다. <그림 6>은 새로 도입될 전자주민증의 시제품 모습이다.

<그림 6> 새 전자주민증의 시제품

전자주민증에는 주민등록증, 주민등록 등·초본, 운전면허증, 의료보험증, 국민연금증서, 인감 등 7개 분야 41개 항목의 개인정보가 수록된다. 앞으로 신용카드 등과 통합할 계획이며, 사무실 출입카드·교통카드 등의 모든 IC 형태의 카드와도 통합될 것으로 보인다. 지금까지 분리되어 관리되던 여러 분야의 개인정보들이 네트워크상에서 서로 연결되는 것이며, 이를 가능하게 하는 전자주민카드 전산망이 만들어지게 되는 것이다.

Ⅲ. 전자주민증의 문제점

시민단체와 민주사회를 위한 변호사 모임인 민변 언론위원회는 프라이버시 침해와 예산 낭비 그리고 행정자치부와 업체만 배불린다는 이유로 전자주민증 도입에 반대하고 있다[5]. 본 장에서는 먼저 유사 관련 기술에서의 문제점 사례를 살펴보고 전자주민증 도입에 따른 다각적인 분석을 통해 예측되는 문제점들을 제시하고자 한다.

3.1 관련기술의 문제점 사례

2008년 8월 7일 동아일보에 따르면 "9·11테러 이후 미국을 중심으로 도입된 전자여권이 손쉽게 복제가 가능한 것으로 드러났다고 영국 일간지 더 타임스가 6일 보도했다. 이 신문은 자체 실험을 통해 컴퓨터 탐색기로 영국 국적자 두 명의 전자여권 칩을 복제한 뒤 각각 오사마 빈 라덴과 자살폭탄 테러범의 디지털 이미지를 이식하는 데 성공했다고 밝혔다. 이들 칩은 유엔이 표준으로 삼고 각국 공항에서 사용 중인 전자여권 판독 소프트웨어를 문제없이 통과했다. 이번 실험을 진행한 네덜란드 암스테르담대의 예로엔 판 비크 연구원은 칩을 복제하고 조작하는 데는 1시간도 걸리지 않았다고 밝혔다. 이 신문은 이 같은 실험 결과를 통해 테러리스트와 조직범죄자의 입국을 차단하기 위해 고안된 전자여권의 안전성에 치명적 결함이 있음이 드러났다고 지적했다. 특히 영국에서는 지난달 28일 각국 주재 영국대사관에 우송될 예정이던 새 여권 및 비자 3000장을 도난당한 사건과 관련해 대규모 전자여권 위조 가능성에 대한 우려도 높아지고 있다. 영국 등 각국 정부는 그동안 위조 칩이 판독기에서 국제적으로 공유된 '공인 키 명부(PKD)'의 입력코드와 맞지 않아 곧바로 탐지된다고 강조해 왔다. 그러나 PKD를 공유한 국가가 아직 10개국에 불과하고 정보를 공유하지 않은 국가에서 만들어진 위조 칩은 판독기에서 문제를 일으키지 않는다고 이 신문은 전했다. 현재 45개국에서 약 1억 명이 사용 중인 전자여권은 소지자의 지문, 홍채 등 신원을 확인할 수 있는 생체정보가 마이크로칩에 내재된 여권이다. 한국도 이달 25일 전자여권을 처음 발행할 예정이다[6].

2008년 9월 29일 동아일보에 따르면 "정부가 보안성을 강화한다며 올해 8월부터 보급 중인 전자여권에서 개인정보를 손쉽게 빼낼 수 있는 것으로 나타났다. 정보인권단체인 진보네트워크는 29일 서울 명동 천주교 인권위원회에서 기자간담회를 열고 "전자여권에 삽입된 RFID에서 개인정보를 어렵지 않게 읽어 들일 수 있는 것으로 확인됐다"고 밝혔다. 이날 진보네트워크는 전자여권 뒤표지에 삽입된 RFID 칩의 정보를 판독해 화면에 띄우는 시연회를 열었다. 시연에 쓰인 전자여권은 지난 11일 진보네트워크 관계자가 구청을 통해 일반인과 같은 방법으로 발급받은 것. 판독기를 작동 시킨 지 3분 만에 사진, 성명, 여권번호, 여권만료일, 생년월일 등 여권 첫 장에 적힌 개인정보가 화면에 고스란히 떴다. 이번 시연회를 주관한 진보네트워크의 김승욱 간사는 "판독기는 인터넷에서 10만 원을 주면 누구나 살 수 있는 기종"이라며 "전자여권에 적힌 정보를 해석할 수 있도록 외국 사이트에서 무료 소프트웨어를 내려 받았다"고 설명했다. RFID 칩에 담긴 개인정보를 알아내는 데에는 전자여권 앞면에 적힌 만료일, 생년월일이 '비밀번호' 역할을 했다. 전자여권의 보안 기능은 이 같은 정보를 입력해야만 RFID 칩에 담긴 정보를 볼 수 있도록 구성돼 있다. 김 간사는 "RFID 칩에서 빼낸 개인정보는 여권 앞면에 적힌 개인정보와 같은 수준이기 때문에 큰 의미를 갖지 못한다는 게 정부 입장"이라고 밝혔다. 여권 앞면만 펼쳐봐도 알 수 있는 정보를 RFID 칩에서 다시 열어 본 것에 불과하다는 해석이다. 실제로 이날 진보네트워크가 공개한 화면은 여권 앞면을 촬영한 것과 비슷했다. 하지만 김 간사는 "개인정보를 RFID 칩에 담긴 상태로 잃어버리는 것이 여권 앞면에 프린트된 형태로 잃어버리는 것보다 훨씬 위험하다"고 잘라 말했다. 같은 정보라도 전자화된 정보를 분실했을 때가 더 피해가 크다는 것이다. 여권 앞면에 적힌 정보와 달리 RFID 칩에 담겨 전자화된 정보는 인터넷을 타고 쉽고 빠르게 전파된다. 수천, 수만 명에게 한꺼번에 정보를 전송하는 것도 가능하다. 개인이 분실한 여권이 길바닥에서 나뒹굴다 몇 몇 사람 손에 들어가는 것과는 차원이 다르다는 주장이다. 특히 현재는 여권을 분실하면 소유자가 그 사실을 즉시 알 수 있지만 앞으로는 여권에 담긴 정보를 고스란히 빼앗기고도 여행객은 전혀 그 사실을 눈치채지 못하게 될 수 있다고 김 간사는 경고했다. 김 간사는 "호텔 프런트 데스크, 환전소, 자동차 렌탈 센터 등 여권을 신원확인 수단으로 쓰는

곳에 악한 의도를 품은 사람이 있다면 RFID 판독기를 통해 여권 자체를 빼앗지 않고도 개인정보만 훔치는 일이 가능하다"고 지적했다. 그는 또 "생년월일, 여권 만료일처럼 RFID 칩에 담긴 정보를 열어 볼 수 있는 '비밀번호'를 꼭 여권에서만 얻을 수 있는 건 아니다"며 "영국에서는 여러 경로를 통해 수집한 정보로 봉투 안에 밀봉된 전자여권의 RFID 칩을 읽어 들이는 데 성공한 사례도 있다"고 밝혔다[6].

2008년 10월 27일 동아일보에 따르면 "복제 가능성이 제기돼 논란을 빚고 있는 집적회로(IC)칩 내장 현금카드가 정부 연구소의 실험에서 실제로 복제된 사실이 있었던 것으로 확인됐다. 한나라당 진수희 의원이 26일 입수한 'IC현금카드 복제결과 보고서'에 따르면 한국전자통신연구원(ETRI) 산하 국가보안기술연구소(NSRI)는 8월 IC현금카드에 대한 복제 실험을 실시해 내장 암호키 추출 및 카드 복제에 성공한 것으로 나타났다. 국가보안기술연구소는 보고서에서 '카드를 복제한 뒤 불법 계좌이체를 한 결과 거래가 정상적으로 처리됐으며 명세표도 출력됐다'고 밝혔다. IC카드의 복제가 가능한 것은 한국은행이 '금융 IC카드 표준'을 만들 때 IC칩에 대한 '부(副)채널 공격 안전성 검증 항목을 포함하지 않았기 때문인 것으로 알려졌다. '부채널 분석'이란 칩에 내장된 암호연산규칙이 작동할 때 발생하는 전기소모량, 열 정보 등을 통해 암호를 찾아내는 것. 실험 결과 특정 전류를 칩에 흐르게 하면 암호연산규칙이 다르게 반응해 이 반응을 통해 암호키를 추출할 수 있었던 것으로 알려졌다. 연구소는 이 결과를 청와대, 국가정보원, 한국은행, 금융감독원에 즉시 보고했으나 금융당국은 즉각 조치에 나서지 않았다. 20일 국정감사에서 진 의원이 '복제 가능성' 의혹을 제기하자 금융감독원은 20일 복제 사실은 밝히지 않은 채 "일부 은행의 현금카드에 사용된 특정 칩이 복제 가능성이 있다는 것"이라면서 "국내 신용카드 전부와 다수의 현금카드에서는 문제가 된 특정 칩을 사용하고 있지 않다"라고만 밝혔다. 금융감독원은 현재 현금·신용카드의 무단 복제를 막기 위해 기존 마그네틱(자기 띠) 카드 대신 IC칩이 내장된 신형카드로 전환 중이며, 2010년까지 모든 신용결제가 IC카드로 이뤄지도록 의무화할 방침이다. IC칩이 내장된 현금카드는 3509만여 장(발급된 현금카드의 90%)에 이르며, 신용카드도 76%인 5089만여 장에 IC칩이 부착된 것으로 추산된다[6].

물론 전자여권 및 IC 칩 내장 현금카드와 전자주민증이 그 사용 용도 및 일부 기술이 다르지만 IC 칩을 이용하는 것은 동일하다. 따라서 이러한 전자여권 및 전자 현금카드의 유조 및 복제 가능성은 전자주민증의 도입에도 적지 않은 파장을 불러올 수 있다. 일부 시민단체에서 제기하고 있는 우려도 바로 이러한 것들이기 때문이다.

3.2 예측되는 전자주민증의 문제점

앞에서 살펴본 바와 같은 관련 기술들에서 발생되는 여러 문제점들을 통해 도입될 전자주민증에서 예측되는 문제점들을 제시하고자 한다.

(1) 개인정보의 집중화 및 유출 가능성

전자주민증에는 주민등록증, 주민등록 등·초본, 운전면허증, 의료보험증, 국민연금증서, 인감 등 7개 분야 41개 항목의 개인정보가 수록된다고 한다. 또한 미래에는 신용카드, 교통카드 등 모든 IC형태의 카드와도 통합될 것이라고 한다.

10년 전에도 전자주민증을 추진하던 행정자치부는 전자주민증 앞면에 사진, 성명, 주민등록번호 등 기본적인 인적사항을 인쇄하고, 뒷면에 운전면허 자격사항과 지문을 인쇄하는 외에, IC칩 내에 주민등록, 운전면허, 의료보험, 국민연금, 인감, 지문, 발급기관장 등 총 7개 부문 35가지의 정보를 담겠다는 정책을 펼쳤었다. 그러나 이러한 과다한 정보를 담은 전자주민증 모델은 보안과 정보유출 우려를 불러일으키면서 시민단체 등의 반대운동을 불러일으켰고, 결국은 사업이 백지화되었다. 행정자치부는 당시 128자로 구성된 비밀키와, 암호화 알고리듬, 개인별 비밀번호 등 3중 보안시스템을 이용하면 노출될

우려가 없을 것이라고 주장했지만 반대여론에 사업을 포기할 수밖에 없었다.

이러한 정책은 유비쿼터스 시대에 편리함과 효율성을 높일 수 있다. 그러나 반면에 한곳에 집중적으로 모아둔 정보는 사용하기는 편리하지만 그만큼 일시에 유출될 가능성도 높아지게 된다. 또한 전문 관리자가 지속적으로 관리하는 서버에 저장된 개인정보보다 낮은 계산용량과 제한적인 암호 기술을 사용하는 IC 칩에 저장된 개인정보가 훨씬 유출될 가능성이 높다.

(2) 분실 시에 취소가 불가능

신용카드는 분실이나 도난 시에 신고를 하면 습득자가 더 이상 사용할 수 없게 된다. 또한 분실된 신용카드에서 더 이상 유출될 정보도 없으며 새로 신용카드를 발급받아 이를 대치하면 된다. 그러나 많은 정보가 담긴 전자주민증이 일단 분실되면 신고하더라도 고스란히 담겨있는 정보들이 추후에 공격자에 의해 노출될 수 있다. 전자주민증은 새로 발급받을 수 있지만 분실된 전자주민증에서 타이밍 공격, 단순/차분 전력분석공격, 오류삽입공격의 사이드 채널 공격으로 언제 정보가 유출되어 악용되거나 인터넷에 떠돌아다닐 지 분실자는 불안할 수밖에 없게 된다.

(3) 단말기들이 개인정보를 확인 가능

신용카드와 마찬가지로 전자주민증에 담겨진 정보들은 대부분이 단말기나 단말기와 연결된 컴퓨터의 메모리에 읽혀지게 된다. 암호화되어 있다하더라도 처리를 위해 복호화될 것이며 단말기나 컴퓨터는 인터넷과 연결되어 있으므로 해커의 의도된 공격을 받게 될 수도 있다. 따라서 단말기나 컴퓨터 역시 보안을 유지해야 한다. 또한 관리자에 의한 유출 가능성도 대비하여야 한다. 이렇게 되면 유출 가능성도 그만큼 높아지게 되며 그에 따라 보안상의 관리를 해야 하는 단말기 및 컴퓨터의 수가 증가하게 된다.

(4) 새로 도입된 암호 기술의 적용 문제

스마트 카드에 대한 위·변조를 막을 수 있는 스마트 카드 운영체제 (SCOS : Smart Card Operation System)나 인증 등의 암호 기술에 대한 연구가 활발히 이루어지고 있다[7-12]. 또한 사이드채널 공격, 서비스거부공격 등에 의한 스마트카드의 안전성에 대한 연구도 이루어지고 있다[13-18].

개인정보들을 모아놓은 서버가 새로운 해킹 기술에 의해 위협받는다면 일단 서버의 이용을 차단하고 적절한 방어 기술을 개발하여 수십 개의 서버에 적용할 수 있다. 그러나 전자주민증에 대한 새로운 해킹 기술이 개발된다면 이를 인지하여도 수천만 명에게 이미 발급된 전자주민증에 새로운 암호 기술을 적용하기란 무척 어려우며 상당한 시간적, 경제적 비용이 소요되게 될 것이다.

Ⅳ. 해결 방법

본 장에서는 앞에서 살펴본 전자주민증의 문제점들을 토대로 하여 이러한 문제점들을 개선할 수 있는 방법을 원점에서부터 재검토해 보고자 한다.

4.1 일반적인 개선 방법

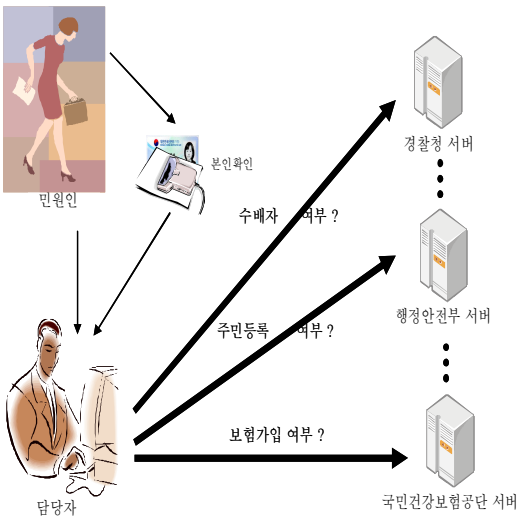
(1) 전자주민증에는 노출되어도 되는 정보만 저장되어야 한다.

정부에서는 전자주민증이 위·변조는 물론 해킹에도 안전하다고 주장하지만 사람들은 많은 개인정보가 저장된 전자주민증이 분실 시에는 언제 어떻게 해커에 의해 노출되어 악용되거나 인터넷에 떠돌지도 모른다는 걱정을 한다. 많은 개인정보가 하나의 카드에 저장되어 있으면 사용 시에는 편리하겠지만 한번 분실 시에는 많은 개인정보가 노출될 수 있기 때문이다. 차세대 전자주민증 도입에 찬성하는 이들 중에는 해킹이 불가능하다는 것을 수학적으로 증명할 수 있고 아직 해킹당한 일이 없으며

향후 50년 동안 해킹의 걱정없이 쓸 수 있다고 주장한다[19]. 그러나 앞에서 살펴본 최근의 관련 기술에 대한 유출 사례를 보면 전자주민증의 도입을 앞두고 불안할 수 밖에 없다. 해커들의 기술은 나날이 증가하고 있기 때문이다. 따라서 많은 개인정보를 전자주민증에 저장하지 말고 본인확인과 인증기능 정도만을 저장하는 것이 바람직하다.

(2) 단말기 등의 외부장치에서도 개인정보의 취급을 최소화해야 한다.

전자주민증에 저장된 개인정보는 단말기에 접촉하면서 꺼내어지게 된다. 즉, 외부 장치와 명령과 명령에 따른 처리 및 응답 메시지 등을 주고받게 된다. 따라서 통신상의 보안이 유지되어야 하며 단말기에서도 보안 기능이 필요하게 된다.



<그림 7> 전자주민증의 이용 절차

전자주민증이 도입되면 단말기도 수백만 대 이상 필요하게 되는데 그만큼 해커들의 공격 대상이 많아지게 되는 것이다. 앞의 항목 (1)과 같이 전자주민증에 본인확인과 인증기능 정도만을 저장한다면 그럴 가능성은 줄어들지만 이러한 정보도 추적 가능성을 피하게 위하여 암호화되어야 한다. 그렇더라도 본인확인이나 인증 등을 수행하기 위하여 서버에 저장된 개인정보를 단말기나 단말기와 연결된 컴퓨터로 가져오는 방법을 이용해서는 안된다. <그림 7>과 같이 단말기는 필요한 최소한의 요청만을 관련 서버에게 보내고 그에 대한 최소한의 응답을 받아 다음의 처리를 행하도록 해야 한다. 예를 들어 경찰관이 불심검문을 위해 휴대하고 다니는 PDA(Personal Digital Assistance) 형태의 무선 단말기에서는 수배자인지의 여부를 묻는 요청을 경찰청 서버로 보내고 그에 대한 응답으로 Yes나 No를 받아 차후 처리를 한다. 병원의 단말기에서는 국민건강보험공단 서버에 가입여부를 묻는 요청을 보내고 응답으로 가입자 및 보험급여를 받는 사람의 인적사항이 응답으로 제공되며 도로의 교통경찰이 휴대하는 단말기에서는 전자주민증 소지자가 운전면허의 소지여부 및 정지나 취소 여부를 묻는 응답을 경찰청 서버로 보내며 그에 대한 응답이 돌아오도록 해야 한다. 이러한 방법은 본인확인을 위해 행정기관도 아닌 사기업이 국민 대다수의 실명, 주민등록번호, 주소, 전화번호 등을 보유하다가 사고나 관리 실수로 유출시키는 등과 같은 유사한 사고들을 피할 수 있다[20, 21].

(3) 전자주민증 사용 시에 비밀번호 입력 및 문자통보를 해야 한다.

현재 신용카드는 철도 승차권 등을 구매할 시에 비밀번호를 요구하도록 되어 있다. 전자주민증을 사용할 때도 마찬가지로 비밀번호를 입력하도록 해야 한다. 이러한 방법은 본인의 동의없이 타인의 전자주민증을 몰래 사용하는 것을 막을 수 있다. 그러나 의식이 없는 응급환자나 비밀번호 입력을 거부하는 취객 및 거동이 수상한 사람들의 경우에는 직권으로 개인정보를 확인할 수 있도록 해야 한다.

그리고 신용카드를 사용 시에 카드 소유자의 휴대폰으로 문자 통보를 해주는 서비스와 마찬가지로 전자주민증 사용 시에도 즉시 소유자에게 문자 통보를 해주도록

하여 분실이나 위·변조에 의한 명의 도용 등의 피해를 보지 않도록 해야 한다. 또한 추후에 자신의 전자주민증에 대한 사용 기록을 인터넷에서 확인할 수 있도록 하는 기능도 제공해야 한다.

(4) 전자주민증에 인증서를 저장해도 좋다.

많은 개인정보를 전자주민증에 저장하지 않고 본인확인과 인증기능 정도만을 저장하는 것이 바람직하다면 인증서를 전자주민증에 저장하는 것도 한 가지 방법이 될 것이다. 인증서를 전자주민증의 IC 칩에 저장하면 전자주민증을 분실하더라도 추가적인 피해가 발생하지 않는다. 공인인증서는 현재 우리나라에 구축된 NPKI (National Public Key Infrastructure)에서 수년간 운영되어 해킹 등에 대한 안전성이 입증되었으며 구두 대면을 통한 신원 확인을 거쳐 발급되므로 신뢰성을 보유하고 있다. 인증서는 공개키와 개인키를 포함하여 그 크기가 4~5 Kbyte정도 밖에 되지 않아 스마트카드의 메모리 용량이 작아도 된다. 이럴 경우 전자주민증을 분실하더라도 기존의 인증서는 신고하여 폐기하고 새로운 인증서를 발급받아 이를 저장한 새 전자주민증을 발급받으면 된다. 그리고 전자주민증을 분실한 사람은 자신의 개인정보가 노출되어 악용되거나 인터넷에 떠돌지도 모른다는 걱정을 하지 않아도 된다.

(5) 새로운 인프라를 구축해야 한다.

많은 개인정보를 전자주민증에 저장하지 않고 인증서와 같은 본인확인과 인증기능 정도의 최소한의 개인정보만을 저장한다면 전자주민증의 효과는 반감될 수도 있다. 반면 개인 사용자들이 느끼는 보안 효과는 증가하게 될 것이다. 이렇게 되면 전자주민증 자체에 대한 보안 기능에 집중적인 기술 개발을 줄이고 대신 기본 정보만을 보유한 전자주민증을 가지고 각 서버에 저장된 개인정보를 이용한 서비스들을 개발해야 할 것이다. 필요하다면 현재 구축된 각종 민원 서비스를 수정하거나 재설계해야 하고 새로운 온라인 서비스들을 개발해야 한다. 물론 이들 수정이나 개발은 앞의 (2) 항목에서처럼 최소한의 정보를 요구하며 Yes나 No의 서명된 응답만을 돌려받도록 하여 개인정보의 노출을 원천적으로 막을 수 있는 방향으로 이루어져야 할 것이다.

(6) 전자주민증의 제작비용이 줄어들 수 있다.

행정자치부는 72 Kbyte용량의 IC 칩이 내장된 새 주민등록증의 제작비용은 장당 1만원 내외이고 제작비와 개발 및 운영비 등을 포함해 모두 5000억 원의 예산이 소요될 것으로 전망하고 있다. 반면 전자주민카드를 반대하는 시민단체에서는 1조원 이상이 들 것으로 추정하고 있다[22, 23]. 그러나 전자주민증에 인증서를 저장한다면 5 Kbyte 미만의 메모리 용량이면 충분하며 따라서 전자주민증 한 장당 제작비용이 그만큼 줄어들 수 있다.

<표 1> 기존의 방법과 제안하는 방법의 비교

항 목	기존의 방법	제안하는 방법
저장 정보	7개 분야 41개 항목의 개인정보	인증서와 같은 기본정보
암호화 필요성	필요	불필요
IC 칩 용량	72 Kbyte	5 Kbyte
비밀번호 기능	추가	기 탑재
보안성	높음	높음
분실시 취소	불가능	가능
사용자의 신뢰성	중간	높음
제작비용	높음	중간
재활용	가능	불가능
인프라 구축	기존 사용	수정, 개발

이상과 같이 전자주민증의 도입에 따른 개선점을 제시하였다. 기존에 행정자치부에서 추진하는 방법과 본 논문에서 제안하는 방법을 비교하면 <표 1>과 같다. 기존에 행정자치부에서 추진하는 방법과 본 논문에서 제안하는 방법을 비교해보면 제안하는 방법은 인증서를 탑재하므로 추가적인 암호화의 필요성이 없으며 인증서에서 제공하는 비밀번호를 사용할 수 있으며 분실 시에 취소

를 할 수 있고 제작비용이 다소 저렴해지며 무엇보다도 운용상이나 개인이 느끼는 안전성이 향상된다는 것이다. 단점으로는 기존 인프라의 수정이나 개발이 불가피하며 전자주민증의 앞면에 내장된 인증서의 일련번호가 표시되므로 인증서의 유효기간이 지났거나 분실 등의 사고로 폐기되는 전자주민증은 재활용될 수가 없다는 것이다.

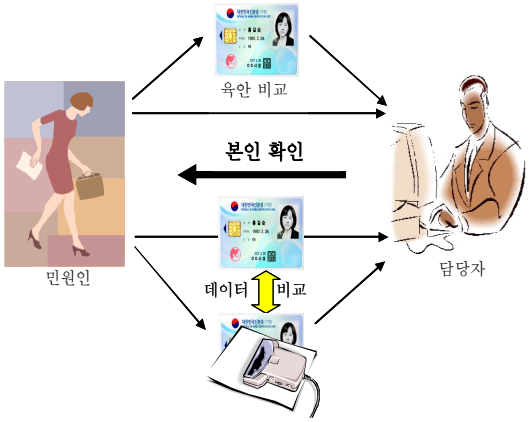
4.2 인증서 탑재시 기술적인 고려사항

일부 학자들은 이미 1999년의 주민등록증 개정 때에 주민등록증에 인증서의 삽입을 주장하기도 하였다. 또한 편리성을 위해 스마트카드에 인증서를 다운받아 사용하는 사례도 있다. 그러나 이러한 사례들은 인증서를 주민등록증 혹은 학생증 등에 부가적으로 추가하여 편리하게 사용하고자 하였던 것인 반면 본 연구에서는 많은 개인정보대신 본인확인 및 인증을 위한 정보로써 인증서를 사용하고자 하는 것이다. 그러기 위해서는 다음과 같은 것들이 고려되어야 한다.

(1) 1차적인 위·변조 검사

전자주민증은 일반 신용카드 크기로서 앞면에는 이름과 생년월일, 성별, 사진 등이 담기고 유출 우려가 있는 주민등록번호와 지문정보, 주소 등 개인정보는 내장된 IC 칩에 수록된다. 뒷면에는 증 발급번호와 한자와 영문 이름이 들어 있다. 특히 사진과 글씨는 레이저를 이용해 주민증 표면에서 150㎛ 아래에 양각해 현재의 플라스틱 주민증처럼 탈·변색으로 훼손되는 것을 방지했다. 복제를 막기 위해 자외선을 비추면 태극 문양을 형상화한 문양이 생기도록 했고 '대한민국'의 글자를 투명 홀로그램으로 표시한다고 한다. 따라서 물리적 위·변조는 어느 정도 차단할 수 있을 것으로 사료된다.

그동안 관공서나 은행 등에서 주민등록증을 제시하면 창구 담당자가 실제의 본인 얼굴과 주민등록증의 사진을 육안으로 비교하여 본인 여부를 확인하였다. 그러나 전자주민증이 도입되면 <그림 8>과 같이 이러한 기본적인



<그림 8> 전자주민증을 통한 본인확인 (전체)

확인 절차는 물론 IC칩에 저장된 인증서의 내용과 전자주민증의 외부에 표시된 기재 사항을 동시에 비교하여야 한다. 다음과 같은 도용이나 남용의 가능성이 있기 때문이다.

- 전자주민증의 사진과 비슷한 타인이 도용하는 경우
- 타인의 전자주민증 사진을 자신의 사진으로 대치하는 경우
- 타인의 전자주민증에 자신의 인증서를 삽입하는 경우

전자주민증에 인증서를 탑재하는 경우 허가받지 않은 사람이 불법적으로 전자주민증의 IC칩에 저장된 인증서에 대해 위·변조를 행할 가능성은 현존한다. 즉 타인의 전자주민증을 습득하여 거기에 자신이나 다른 사람의 인증서를 탑재하는 것이다. 이러한 사실은 이미 이성은 등의 논문에서 지적되어 그에 대한 다른 해결방법이 연구된 바가 있다[11].

그러나 인증서는 CA(Certificate Authority)에 의해 서명되어 발급되므로 인증서의 내용 자체를 변조하기는 불가능하다. 따라서 전자주민증의 앞면에 표시된 성명과 인증서내의 주체를 비교하면 1차적인 위·변조를 확인할 수 있다.

<그림 9> 전자주민증을 통한 본인확인 (데이타 비교)

(2) 2차적인 위·변조 검사

인증서에는 소유자의 이름 즉, 주체이외에는 기타 인적사항이 표시되지 않으므로 동명이인의 인증서로 대치된다면 이를 알아내지 못할 가능성이 있다. I-PIN (Internet Personal Identification Number) 도입시 기존의 인증서에 주민번호의 해쉬값을 포함시켜 I-PIN으로 사용하자는 방법도 주장된 바가 있다. 어쨌거나 이러한 동명이인을 이용한 위·변조를 막기 위해서는 <그림 9>와 같이 인증서의 일련번호를 전자주민증의 앞면에 표시하여 2차적인 위·변조를 막을 수 있겠다.

전자주민증의 사진과 실제 얼굴이 비슷하며 게다가 성명까지 똑같은 타인이 있을 수 있다. 이런 경우를 대비하여 인증서에 생년월일을 추가하여 이를 구별해낼 수도 있다. 그렇지만 기존의 인증서 구조에 추가적인 정보를 넣는 것은 바람직하지 않으며 CA가 인증서를 발급할 시에 대면 면접과 서류 등을 검토하므로 동명이인에게 같은 일련번호가 발급될 수는 없기 때문이다. 그러나 전자주민증의 사진과 실제 얼굴이 비슷하며 게다가 성명까지 똑같은 경우 본인 여부를 판단하는 담당자가 일련번호를 자칫 빠뜨릴 수 있다. 따라서 이러한 경우를 대비하여 일련번호보다 식별하기 편리한 생년월일을 추가하는 것도 좋은 방법이 될 수 있다.

(3) 인증서 비밀번호의 해킹

인증서는 숫자 및 알파벳을 이용한 7자리 이상의 비밀번호를 사용하도록 되어 있어 숫자 4자리만을 이용하는 ATM(Automatic Teller Machine)보다는 월등한 안전성을 보유하고 있다. 그러나 이러한 비밀번호도 해킹에 의해 유출되어 타인이 사용할 가능성을 전혀 배제할 수 없다. 일단 그러기 위해서는 전자주민증이 장시간 타인에게 노출되어야 하는데 이는 전자주민증의 분실에 해당하기 때문에 이를 신고하여 더 이상 사용할 수 없도록 할 수 있다. 전자주민증이 주민등록증, 주민등록 등·초본, 운전면허증, 의료보험증, 국민연금증서, 인감 등 여러 기능으로 사용되기 때문에 장시간 사용하지 않는 경우는 발생하기 어려우나 그런 경우에 분실 사실을 모른다면 전자주민증의 사용을 문자로 통보해주므로 이를 1차 사용시에 적발할 수 있다. 또한 국내에서 공인인증서가 발급되기 시작한 2003년 이후로 공인인증서의 비밀키가 해킹당한 사례는 보고되지 않고 있을 정도로 안전성이 높다.

(4) 단말기의 불법 행위

전자주민증용 단말기는 기본적으로 CA가 발급하는 인증서를 역시 탑재해야 할 것이다. 전자주민증의 스마트카드가 자체 연산 기능이 있으므로 NPKI에 해당하는 CA에서 발급받은 인증서를 탑재했는지 여부를 확인함으로써 불법 단말기인지의 여부를 확인할 수 있다. 적법한 단말기이더라도 관리자가 악의적으로 사용자의 인증서를 저장하여 이용할 수 있다. 그러나 이런 경우도 역시 인증서를 이용하여 서버에 접속할 때에, 서버가 개인 정보의 사용에 대한 통지를 전자주민증의 소유자 본인에게 휴대폰의 문자로 통보해주므로 1차 사용시에 이를 적발할 수 있다. 물론 그러기 위해서는 휴대폰의 실명제가 확

립되어야 하며 휴대폰 번호의 변경시에 즉시 이를 서버에 통보하도록 하는 시스템이 구축되어 있어야 한다.

(5) 전자주민증의 유효기간

이미 우리나라는 전자상거래를 목적으로 한 NPKI와 행정을 목적으로 한 GPKI(Government Public Key Infrastructure)가 구축되어 있다. 물론 그동안 수년동안 운영되어 왔으므로 어느 정도 안전성 및 효율성 입증되어 있다. 인증서는 일반적으로 그 유효기간이 1년이며 따라서 인증서를 도입한 전자주민증의 유효기간도 1년이 된다. 앞에서 설명하였듯이 전자주민증의 앞면에 내장된 인증서의 일련번호가 표시되므로 전자주민증은 1년이 지나면 더 이상 사용할 수 없으며 재활용도 될 수 없게 된다. 인증서의 유효기간을 늘릴 수도 있지만 그동안 운영되어온 공인 인증서의 효율성이나 안전성에 영향을 줄 수 있다. 따라서 유효기간이 지난 전자주민증 소지자는 구청이나 동사무소를 방문하여 본인 확인을 거친 뒤 새로운 인증서가 탑재된 새 전자주민증을 발급받게 된다. 유효기간 따른 이러한 재발급은 1년 단위로 국민들의 신원을 재확인할 수 있으며 전자주민증에 새로운 정보나 정보보안 관련 기술을 적용할 수도 있다.

V. 결론

우리나라의 주민등록증 소지자는 3, 700만 여명 수준으로 알려져 있다. 전자주민증은 대한민국 성인이면 누구나 사용하는 것이므로 새로 도입하려면 막대한 비용과 시간이 요구되며 일단 도입하면 추후 수정이 어렵게 된다. 따라서 도입하기 전에 충분한 연구가 선행되어야 한다. 정부에서는 새로운 전자주민증에 IC 칩이 탑재된 스마트카드를 선정하고 7개 분야 41개 항목의 개인정보를 수록하려고 하고 있다. 그러나 시민단체에서는 많은 개인정보가 한 장의 카드에 수록되는 것에 대해 반대를 하고 있다.

따라서 본 논문에서는 전자주민증의 도입에 따른 다각적인 분석을 통하여 문제점을 제기하고 이를 해결할 수 있는 방법들 중에 하나를 제시하였다. 제시된 방법은 기존의 인프라를 수정하거나 개발해야 하는 단점이 있지만 전자주민증에 인증서를 저장함으로써 IC 칩의 저장용량이 작아도 되는 경제효과도 있을 뿐만 아니라 전자주민증을 분실하더라도 취소가 가능하며 노출된 인증서에 의한 피해가 극히 적어 사용자를 충분히 안심시킬 수 있다.

참고문헌

[1] 정신문화연구원, “한국민족문화대백과사전”, 1989.

[2] 한국조폐공사, http://www.komsco.com.

[3] 삼성경제연구소, http://www.seri.org.

[4] 전자신문, http://www.etnews.co.kr.

[5] 조선일보, http://www.chosun.com.

[6] 동아일보, http://www.donga.com.

[7] 김세일 · 이현숙 · 이동훈, “익명성을 제공하는 스마트카드 사용자 인증 프로토콜”, 한국정보보호학회 논문지, 제17권, 제2호, 2007, pp. 139-144.

[8] 전일수, “스마트카드를 이용한 새로운 패스워드 기반의 원격 사용자 인증 프로토콜”, 한국산업정보학회논문지, 제10권, 제2호, 2005, pp. 59-66.

[9] 송영상 · 신인철, “서명을 이용한 스마트카드 사용자 인증을 위한 COS 설계”, 한국전자공학회논문지, 제41권, 제CI편, 2004, pp. 103-112.

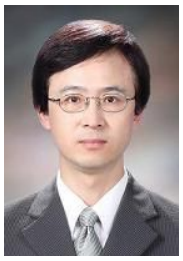
[10] 김현성 · 정연기, “지문과 스마트카드를 이용한 사용자 인증”, 한국멀티미디어학회지, 제7권, 제4호, 2003, pp. 197-204.

[11] 이성은 · 장홍종 · 박인재 · 한선영, “다중 암호화 기법을 활용한 하이브리드 스마트카드 구현”, 한국정보보호학회논문지, 제13권, 제2호, 2003, pp. 81-89.

[12] 김증섭 · 조병호 · 김효철 · 이종국 · 유기영 “다양한

응용을 위한 스마트카드 운영체제", 정보과학회논문지, 제8권, 제3호, 2002, pp. 277-288.
[13] 신광철, "서비스거부공격에 안전한 OTP 스마트카드 인증 프로토콜", 한국컴퓨터정보학회논문지, 제12권, 제6호, 2007, pp. 201-206.
[14] 한동호 · 박제훈 · 하재철 · 이성재 · 문상재, "사이드 채널 공격에 대한 스마트카드 안전성의 실험적 분석", 한국정보보호학회논문지, 제16권, 제4호, 2006, pp. 59-68.
[15] 이대식 · 윤동식, 안희학 "스마트카드를 이용한 원 카드 시스템의 설계 및 보안", 한국정보보증논문지, 제5권, 제2호, 2005, pp. 57-63.
[16] 오홍룡 · 윤호선 · 염흥열 "스마트카드에 적용 가능한 분산형 인증 및 키 교환 프로토콜", 한국인터넷정보학회논문지, 제6권, 제3호, 2005, pp. 17-30.
[17] 조은성 · 원동규 · 양형규 · 김승주 · 원동호, "스마트카드의 보안성에 관한 연구", 한국정보보호학회논문지, 제15권, 제2호, 2005, pp. 54-62.
[18] 황선태 · 박종선 "스마트카드 기반의 효율적인 해킹 방지 시스템 설계", Journal of Information Technology Applications & Management, 제11권, 제2호, 2004, pp. 179-190.
[19] 매일경제신문, http://www.mk.co.kr.
[20] 미디어다음 뉴스, http://www.daum.net.
[21] 한겨레 뉴스, http://www.hani.co.kr.
[22] 국민일보, http://www.kmib.co.kr.
[23] 프리존뉴스, http://www.freezonenews.co.kr.

■ 저자소개 ■



이 영 교
Lee, Young Gyo

2008년 3월~현재 서일대학 인터넷정보과 전임강사
2006년 8월 성균관대학교 컴퓨터공학부 (공학박사)
1999년 2월~2001년 6월 LG정보통신중앙연구소 선임연구원
1993년 3월~1998년 9월 대우통신종합연구소 선임연구원
1991년 8월 한양대학교 전자공학과 (공학석사)
1986년 2월 한양대학교 전자공학과 (공학사)
관심분야 : 정보보안, PKI, 암호이론
E-mail : younggyo@seoil.ac.kr

안 정 희
Ahn, Jeong Hee

1996년 3월~현재 두원공과대학 컴퓨터정보과 부교수
2000년 2월 성균관대대학교 정보공학과 (공학박사)
1993년 2월 성균관대학교 정보공학과 (공학석사)
1988년 2월 성균관대학교 정보공학과 (공학사)
관심분야 : 정보통신 보안, 전자상거래 보안, 트래픽 제어
E-mail : jhpro@doowoon.ac.kr

논문접수일 : 2009년 2월 20일
수 정 일 : 2009년 4월 1일
게재확정일 : 2009년 4월 5일