디지털산업정보학회 논문지 제11권 제2호-2015년 6월
http://dx.doi.org/10.17662/ksdim.2015.11.2.011

아이핀 대량 부정발급 사고에 대한 개선방법 연구*

이 영 교** · 안 정 희***

A Study of the Improvement Method of I-pin Mass Illegal Issue Accident

Lee Younggyo · Ahn Jeonghee

〈Abstract〉

The almost of Web page has been gathered the personal information(Korean resident registration number, name, cell-phone number, home telephone number, E-mail address, home address, etc.) using the membership and log-in. The all most user of Web page are concerned for gathering of the personal information. I-pin is the alternative means of resident registration number and has been used during the last ten-year period in the internet. The accident of I-pin mass illegal issue was happened by hacker at February, 2015. In this paper, we analysis the problems of I-pin system about I-pin mass illegal issue accident and propose a improvement method of it. First, I-pin issue must be processed by the off-line of face certification in spite of user's inconvenience. Second, I-pin use must be made up through second certification of password or OTP. The third, the notification of I-pin use must be sent to the user by the text messaging service of cell-phone or the E-mail. The forth, I-pin must be used an alternative means of Korean resident registration number in Internet. The methods can reduce the problems of I-pin system.

Key Words : I-pin, Korean Resident Registration Number, Fraud Detection System, Personal Information

Ⅰ. 서론

온라인에서 주민등록번호의 대체수단으로 사용되고 있는 아이핀이 대량 부정으로 발급되어 불법 사용되는 사고가 발생하였다. 아이핀은 인터넷상에서 주민등록번호의 유출을 막기 위하여 구 정보통신부가 도입한 실명확인용 대체수단이다. 그 이전에는 아이디와 비밀번호로 로그인을 허용하던 웹사이트들이 점차 실명인증이라는 이유로 사용자들의 주민등록번호와 실명을 요구하게 되었다. 그에 따라 사용자들은 자신의 실명과 주민등록번호가 여러 웹사이트를 통하여 유출되는 것을 불안하게 생각하게 되었고 실제로 웹사이트들 중에는 사용자들의 실명, 주민등록번호, 휴대폰번호, 주소 등의 개인정보를 축적하였다가 관리소홀로 대량 유출사고를 발생시키기도 하고 불

*본 논문은 2015년도 서일대학교 학술 연구비에 의해 연구되었음.
** 서일대학교 인터넷정보과 부교수 (교신저자)
*** 두원공과대학교 스마트소프트웨어과 부교수

법적으로 타 기업에 판매하기도 하였다. 2006년, 구 정보통신부는 이러한 국민의 불안을 해소하기 위하여 주민등록번호 대신에 인터넷의 여러 웹사이트 등에서 사용할 수 있는 아이핀을 도입하였다. 아이핀은 2013년 2월 18일, 온라인상에 주민등록번호 수집과 이용을 제한하는 법률(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의 2항)이 시행되면서 확대 적용되어 오다가 2015년 3월, 75만건의 부정발급 사고가 발생하게 되었다.

그에 따라 정부는 이번 사고에 대해 원인을 다각도로 분석하고 있으며 그 결과에 따른 후속대책을 마련하려고 하고 있다. 따라서 본 연구에서는 이번 아이핀 대량 부정발급사고와 그 이전의 사고들을 분석해보고 이를 개선할 수 있는 방법을 모색해보고자 한다. 논문의 나머지 부분은 다음과 같이 구성되어진다. 2장에서는 먼저 아이핀 시스템에 대해 살펴본다. 3장에서는 아이핀의 발급사고들에 대한 원인을 분석하여 문제점을 제시한다. 4장에서는 전반적인 문제점과 정부의 개선책에 대한 분석을 수행한다. 5장에서는 제시된 문제점을 개선할 수 있는 방법을 제안하고 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

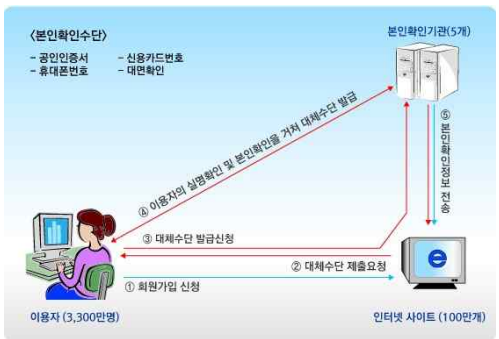
2.1 아이핀의 개념

아이핀(i-PIN)은 “Internet Personal Identification Number”의 약자로서 인터넷 상에서 주민등록번호를 대신하는 번호인데 아이디와 패스워드를 이용하여 본인확인, 즉 실명인증을 하는 수단이다. 아이핀의 아이디와 패스워드를 이용하면 인터넷상의 여러 웹사이트에서 주민등록번호를 일일이 입력하지 않아도 회원가입 및 기타 서비스 등을 이용할 수 있다. 아이핀 아이디를 발급하는 곳은 <그림 1>과 같이 방송통신위원회가 관리 및 감독하는 서울신용평가정보, 나이스신용평가정보, 코리아크레딧뷰로 등 3개 민간 본인확인기관과 행정안전부 산하 한국지역정보개발원이 제공하는 공공아이핀이 있다.

I-PIN 바로가기	SIREN24	NICE i-PIN	KCB 아이핀	공공 I-PIN
기관명	서울신용평가정보	나이스신용평가정보	코리아크레딧뷰로	공공아이핀센터
연락처	1577-1006	1600-1522	02)708-1000	02)818-3050
링크주소	siren24.com	idcheck.co.kr	ok-name.co.kr	gpin.go.kr

<그림 1> 민간 및 공공 아이핀 발급기관 (출처 : 한국인터넷진흥원)

위의 기관에서 제공하는 웹사이트에 접속하여 신원확인을 거치게 되면 사용자에게 유일한 아이핀 아이디를 부여하게 된다. 사용자는 이후에 인터넷 상의 다른 웹사이트들에서 주민등록번호와 실명대신에 부여받은 아이핀 아이디와 비밀번호를 입력함으로서 인증을 받아 해당 웹사이트에서 제공하는 여러 서비스들을 이용할 수 있다. 물론 그러기 위해서는 해당 웹사이트가 아이핀을 이용한 인증서비스를 제공하고 있어야 한다. <그림 2>는 2006년에 구 정보통신부가 공개한 아이핀의 개념도이다.



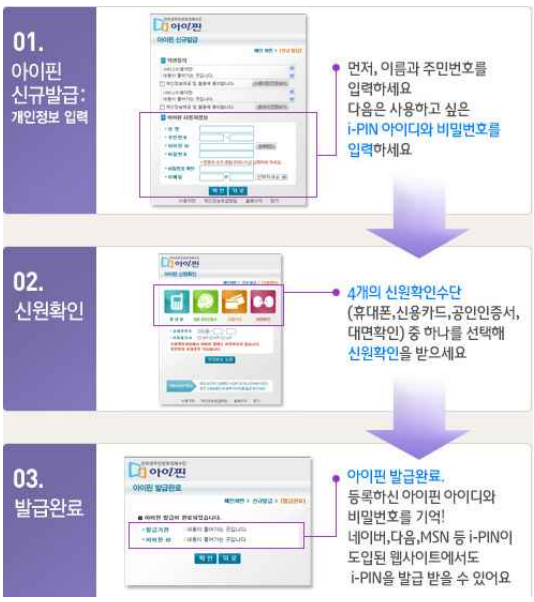
<그림 2> 2006년, 구 정보통신부가 공개한 아이핀 개념도

Daum, Naver, MSN 등 국내 유명 266개 사이트에서 본인확인 방법으로 아이핀을 사용하고 있으며 2009년 1월에 신설된 정보통신망법 시행령의 기준에 따라 주민등록번호 외 회원가입수단 도입 대상 사업자가 공시됨으로 인하여 아이핀 인증을 도입한 인터넷 웹사이트가 증가하고 있다 [1].

2.2 아이핀 발급절차

아이핀의 발급 절차는 다음과 같다. 앞에서 언급한 4곳의 기관에 접속하여 "아이핀 신규발급"버튼을 누르면 먼저 "서비스 약관동의", "개인정보 수집 및 이용에 대한 동의", "개인정보의 제3자 제공에 관한 사항 동의", "고유식별정보 처리 동의"의 4가지에 대한 창이 뜨게 되며 동의 버튼을 눌러야 다음 단계로 넘어갈 수 있다. 다음 단계에서는 신규발급을 위한 개인정보 입력단계인데 성명, 주민번호, 아이디 자동생성 방지 이미지의 문자 입력, 아이핀 아이디, 비밀번호, 비밀번호 확인, 이메일 주소를 입력하게 된다. 물론 아이핀 아이디는 중복검사를 통하여 유일한 것을 부여하게 되며 비밀번호도 생성규칙에 부합하는 것을 선택하였는지를 확인하게 된다 [1].

다음은 신원확인을 위한 단계인데 휴대폰, 신용카드, 공인인증서, 대면확인의 4가지 방법 중에 한 가지를 선택하여 수행하게 된다. 휴대폰 신원확인은 본인 명의의 휴대폰만이 사용이 가능하며 공인인증서 신원확인은 범용 공인인증서가 필요하다. 신용카드 신원확인에는 물론 본인 명의의 신용카드가 필요하며 체크카드도 가능한데 신용카드 뒷면의 번호를 입력하도록 되어 있다. 그러나 이 신원확인 방법은 분실되었거나 폐기된 카드를 이용하여 불법적으로 아이핀을 발급받은 사례가 발생하여 더 이상 서비스되고 있지 않다. 대면확인 신원확인 방법은 회원가입을 한 후에 주민등록증을 지참하고 주민센터를 방문하여 직접 본인인증을 받아야 하는 불편함 이존재하는 방법이다.



<그림 3> 아이핀의 발급 절차 (KISA 홈페이지)

Ⅲ. 아이핀의 유출사고 및 문제점분석

3.1 아이핀의 유출 사고

1) 2010년 6월 7일, YTN의 "'아이핀' 불법 발급받아 거래한 일당 검거"라는 기사에 따르면 "경찰청 사이버테러대응센터는 다른 사람 명의로 인터넷 개인식별번호인 '아이핀'을 만들어 돈을 받고 거래한 혐의로 김 모 씨 등 8명을 검거했다고 밝혔습니다. 김 씨 등은 지난해부터 해킹으로 유출된 주민등록번호를 이용해 아이핀을 만든 뒤 중국 게임업체 등에 팔아넘긴 혐의를 받고 있습니다. 경찰조사결과 김 씨 등은 해킹으로 빼낸 주민등록번호로 대포폰과 무기명 선불카드를 만들어 본인 인증을 받은 것으로 드러났습

니다. '인터넷 신분증'으로 불리는 아이핀은 아이디와 비밀번호만으로 인터넷 상거래와 사이트 가입을 자유롭게 할 수 있으며 내년부터 국내 모든 인터넷 사이트에 의무 도입될 예정입니다 [2]."

2) 2014년 2월 27일, 국민일보 쿠키뉴스의 "'주민등록번호 대체하는 '아이핀'도 뚫렸다"라는 기사에 따르면 "[쿠키 사회] 남의 명의를 도용하는 '대포폰' '대포통장'에 이어 '대포아이핀(I-PIN)'까지 등장했다. 아이핀은 인터넷에서 주민등록번호를 대신하는 인증수단이다. 아이디와 비밀번호만으로 본인 확인을 할 수 있다. 최근 금융정보 대량유출 사태 이후 주민번호 대체제로 조명을 받았다. 그러나 경찰 수사에서 대포아이핀이 개인정보처럼 거래되고 있는 것으로 드러나 대책이 시급하다는 지적이 나오고 있다. 서울서대문경찰서는 27일 개인정보를 사들여 되판 혐의(정보통신망법 위반 등)로 조선족 이모(25)씨와 한국인 박모(37)씨를 구속했다. 이씨는 지난해 3월부터 중국 메신저 서비스를 통해 접촉한 중국 스미싱 조직으로부터 개인정보 1만여건을 건당 6000원에 사들인 혐의를 받고 있다. 이씨는 이를 박씨에게 넘겼고, 박씨는 온라인 게임 이용자들에게 되팔아 1억7000여만원을 챙겼다. 이들이 중국 스미싱 조직에서 넘겨받은 개인정보에는 아이핀 600여건이 포함돼 있었다. 스미싱 조직이 한국인 개인정보를 수집한 뒤 이를 활용해 타인 명의로 아이핀 600여건을 발급받은 것이다. '온라인상의 주민번호'인 아이핀이 '대포' 신세로 전락한 것은 허술한 발급 과정 탓이다. 아이핀을 발급하는 곳은 안전행정부(공공 아이핀)와 민간업체(민간 아이핀) 3곳이다. 공인인증서와 주민등록증 발급일자 확인 등 까다로운 절차를 거치는 공공 아이핀과는 달리 민간 아이핀은 '휴대전화 인증'을 통해 발급받을 수 있다. 휴대전화에 문자메시지로 전송된 인증번호를 입력하면 본인 확인 절차가 끝난다. 간편한 절차 때문에 지난해 12월 기준 전체 아이핀 발급자 1452만명 중 민간 아이핀 발급자가 81.7%(1186만명)나 된다. 중국 스미싱 조직은 수집한 주민등록번호와 휴대전화 번호 등을 조합해 타인 명의로 직접 민간 아이핀을 발급받았다. 문자메시지 인증 절차는 스미싱으로 해결했다. 갖고 있던 대량의 휴대전화 번호에 무작위로 스미싱 문자메시지를 보낸 뒤 이를 눌러본 사람의 휴대전화에 악성코드를 심었다. 그리고 이 번호로 아이핀에 가입하면서 휴대전화에 전송된 인증번호를 악성코드를 통해 가로챈 뒤 스미싱 조직의 서버로 전송했다. 휴대전화 주인에게는 문자메시지가 전송되지 않아 피해자들은 자신 명의로 아이핀에 가입된 줄도 모르고 있었다. 정부 관계자는 "민간에서 아이핀 발급 서비스를 먼저 시작했기 때문에 공공 아이핀만 사용하도록 제한하기는 어렵다"며 "다만 정보 유출에 대한 국민 우려가 높아지고 있어 공공 아이핀 활용도를 높이는 방안을 고려해보겠다"고 말했다. 이들로부터 개인정보를 구매한 사람들은 대부분 게임 사이트 이용자였다. 고스톱이나 포커 등 온라인 도박 게임을 하다 보면 이용 정지 등 제재를 받는 경우가 많아 게임 계정을 여러 개 보유하려고 불법 개인정보를 사들인 것이다. 경찰 관계자는 "민간 아이핀은 휴대전화 인증만으로 손쉽게 가입할 수 있어 스미싱 조직의 표적이 되고 있다"고 말했다 [3]."

3) 2015년 3월 5일, 조선일보의 "'아이핀, 대량해킹 유출사고 발생해..."아이핀, 너마저도""라는 기사에 따르면 "주민등록번호 대체수단으로 지난해 도입된 공공아이핀이 해킹에 의해 대량으로 유출되는 사고가 발생했다. 담당 부처인 행정자치부는 이같은 사실을 사흘간이나 숨긴 것으로 드러나 비난이 일고 있다. 행자부는 5일 지역정보개발원에서 관리하고 있는 공공아이핀시스템에서 지난 달 28일부터 이달 2일까지 75만 건의 아이핀이 부정 발급되는 사고가 발생했다고 밝혔다. 이후 추가 부정발급을 차단하고 부정발급된 아이핀 전부를 긴급 삭제조치 했다. 동일한 해

킹 방지를 위해 공공아이핀센터에 비상대응팀을 꾸려 24시간 집중 모니터링체계를 운영 중이다. 이번 사고는 공공아이핀 정상발급 절차를 우회(프로그램 취약점 이용)해 아이핀을 대량으로 부정 발급하는 방식으로 벌어졌다는 것이 확인됐다. 부정발급 받은 아이핀의 주된 사용처는 게임 사이트의 신규 회원가입과 기존 이용자 계정 수정·변경 등에 쓰였다. 행자부 관계자는 “이번 사고로 인한 2차 피해를 최소화하기 위해 민간 아이핀 기관과 관련 게임사에 사용내역을 전달하고 긴급 사용자 보호조치를 취했다”며 “관련 게임사에서는 부정 발급된 아이핀으로 신규 회원가입을 한 경우 회원 탈퇴 조치하고 사용자 정보를 수정·변경한 경우는 임시 사용중지 조치를 했다"고 설명했다. 행자부는 또 이번 사건을 경찰청에 긴급히 수사 요청해 현재 수사 중에 있다고 덧붙였다. 아직까지 해킹 사고로 인한 피해는 보고되지 않았으며, 해킹으로 유출된 공공아이핀은 모두 같은 공인인증서와 패스워드가 쓰인 것으로 알려졌다 [4].”

3.2 유출사고의 문제점 분석

1) 2010년의 아이핀 불법발급 및 거래사건

이 사고는 불법조직이 인터넷에 유출되어 있는 주민등록번호, 실명 등의 개인정보를 불법 수집한 뒤 대포폰과 무기명 선불카드를 이용하여 본인인증을 하여 아이핀을 발급받아 유통한 형태이다. 우리나라에서 경제활동을 하는 대부분의 국민이 현재 주민등록번호를 비롯한 개인정보들이 인터넷에 유출되어 거래되고 있는 실정이기 때문에 대포폰과 무기명 선불카드를 통한 본인인증만 제공된다면 얼마든지 불법적으로 아이핀을 발급받을 수 있다.

2) 2014년의 아이핀 불법발급 및 거래사건

이 사고는 2010년의 사고보다 한 단계 진일보한 불법 발급 및 거래 사건이다. 대폰폰과 무기명 선불카드를 이용하여 본인인증을 거쳐 아이핀을 발급받았던 방법이 한계를 보이자 불법조직은 스미싱을 이용하였다. 이미 많은 국민들의 개인정보를 가지고 있던 이 조직은 대량으로 스미싱 문자를 발송하여 이에 속은 사람이 스미싱 문자에 포함된 URL를 누르게 되면 악성코드를 스마트폰에 설치하였다. 그리고 이 사람의 개인정보를 이용하여 아이핀 발급을 신청하고 휴대폰 인증을 신청한 뒤 악성코드를 이용하여 인증문자를 가로채어 아이핀을 발급하였다.

<표 1> 아이핀 사고들의 비교

발생년도	2010	2014	2015
아이핀 수량	10여건	600여건	75만건
불법 형태	부정발급	부정발급	부정발급
사용 사이트	게임, 도박	게임, 도박	게임, 도박
본인인증방법	휴대폰 인증, 카드인증	휴대폰 인증	공인인증서
인증통과방법	대포폰, 불법카드	스미싱	파라미터 위변조 (우회공격)
아이핀 종류	-	공공 및 민간	공공
당시 대책	신용카드인증 방법폐지	백신설치	모니터링, 유효기간, FDS 도입 등

3) 2015년의 아이핀 75만건 대량 부정발급 사건

아이핀이 75만건이나 대량으로 부정 발급된 이 사건은 처음에는 아이핀 시스템이 해킹되었을 지도 모른다는 추측을 낳기까지 했다. 2015년 2월 28일 오전

12시 30분부터 3월 2일 오전 9시까지, 56시간 30분이라는 긴 시간동안 75만개의 아이핀이 부정 발급된 것이다. 민간 아이핀 시스템이 아닌, 지역정보개발원이 관리하는 공공 아이핀이 타켓이었으며 하나의 IP에서 수천개의 아이핀을 발급받은 셈이다. 조직의 해커는 파라미터 위변조라는 방식을 통하여 아이핀 발급과정중에 본인인증 절차를 우회 즉, 건너뛰는 방법을 사용하였다. 이번 부정발급에는 국내 IP 2,000 여개가 동원되었고 중국어 버전의 해킹 SW가 사용되었으며 불법 발급된 공공 아이핀에는 동일한 공인인증서와 패스워드가 사용되었다. 부정발급된 75만건의 아이핀 중에 17만건이 게임사이트에서 사용되었는데 특히 이중 12만건이 특정 3개 게임사이트의 신규회원가입, 이용자 계정 수정 및 변경 등에 이용된 것으로 파악되었다 [4-6].

Ⅳ. 정부의 개선책을 포함한 제도적, 절차적 문제점

본장에서는 먼저 여러 부정발급 사고에 대한 아이핀의 전반적인 문제점들을 지적하고 정부의 개선책도 분석해보고자 한다.

4.1 전반적인 문제점

그동안 상용화되고 있는 아이핀에 대한 연구는 [7-10] 등의 관련 논문에서 일부 다루어지고 있다. 또한 공인인증서를 이용한 주민등록번호 대체수단에 대한 연구도 이루어지고 있다 [11].

1) 아이핀 발급시 개인정보 입력문제

2006년 아이핀이 처음 도입될 때부터 제기되어온 문제중에 하나는 아이핀 발급을 위해서 주민등록번호와 실명을 필요로 한다는 것이었다. 2006년 당시에도 주민등록번호, 실명 등을 포함한 개인정보는 여러 해킹 및 유출사고로 인하여 경제활동 인구의 대부분이 인터넷에 유출되어 불법적으로 거래되고 있는 실정이기 때문이었다. 물론 신원확인을 위한 절차가 있지만 이번 사고들에서 보았듯이 불법카드나 대포폰, 스미싱 그리고 우회공격 등으로 얼마든지 아이핀을 부정 발급받을 수 있음을 알 수 있다. 또한 "2)의 신원확인 방법의 한계성"과 연관이 있는데 인터넷상의 주민등록번호라는 이유로 오프라인 신원확인 방법을 사용하지 않고 인터넷상에서 편리하게 발급받을 수 있도록 되어 있는 것도 문제점으로 지적될 수 있다.

2) 신원확인 방법의 한계성

아이핀의 신원확인 방법으로 4가지 즉, 휴대폰, 신용카드, 공인인증서, 대면확인 방법이 제공되어 지고 있다. 이중 가장 확실한 인증방법인 대면확인은 사용자들이 주민센터를 방문하기 번거로워 해서 잘 사용을 하지 않는다. 두 번째로 강력한 인증방법인 공인인증서는 그 자체가 초기 발급시에 은행을 방문하여 오프라인으로 대면인증을 거치기 때문에 안전하며 사용시 마다 비밀번호를 입력하도록 되어 있다. 그러나 공인인증서의 재발급이 온라인으로 이루어지기 때문에 다소간의 한계성도 존재한다. 개인정보를 획득한 해커가 사용자의 인증서를 폐기하고 새로운 인증서를 발급받은 사고도 보고되기 때문이다. 휴대폰 인증은 본인 명의의 휴대폰으로 수신되는 본인확인 문자를 아이핀 발급화면에 입력시키는 것인데 앞의 사고들에서 보았듯이 대포폰, 스마트폰 스미싱으로 무력화되었다. 신용카드 인증방법은 신용카드 뒷면에 표기된 숫자정보를 입력하는 것인데 비밀번호의 개념이 아니기 때문에 도난 혹은 습득한 타인의 신용카

드, 무기명 선불카드, 폐기된 신용카드 등을 이용하여 얼마든지 신원확인을 통과할 수 있다. 이러한 본인확인의 한계성은 [9,10]에서도 지적된 바 있다.

3) 사용 시 추가인증 및 사용통보의 부제

아이핀은 일단 발급을 받으면 아이디와 비밀번호만 알고 있으면 아이핀 인증 서비스를 이용하는 웹사이트에서 언제 어디서든지 사용을 할 수 있다. 이러한 편리함이 자칫 부작용을 초래할 수 있는데 타인의 아이디와 비밀번호를 몰래 알아낸다(시각, 촬영, 해킹 등)던지 아니면 이번 사고들에서처럼 부정발급을 받아 소유자 몰래 사용할 수 있기 때문이다. 이는 사용시마다 추가 인증을 하지 않기 때문인데 공인인증서의 경우에는 사용시마다 보안카드나 OTP(One Time password)를 입력하도록 되어 있다. 아니면 아이핀을 사용할 때마다 다른 루트의 통신을 이용하여 즉, 문자나 이메일로 이를 사용자에게 통보해주는 것도 좋은 방법이 될 수 있다.

4) 민간과 공공 아이핀의 이원화 체계

이번 아이핀의 대량 부정발급사고는 아이핀 시스템이 민간 아이핀과 공공 아이핀으로 이원화되어 있는 데에도 문제가 있다고 할 수 있다. 민간 아이핀은 2005년 7월부터 시행되었으며 서울신용평가정보, 나이스신용평가정보, 코리아크레딧부로의 3개 발급기관으로 구성되어 있으며 방송통신위원회의 관리 및 감독을 받는다. 공공 아이핀은 2008년 8월부터 시행되었으며 한국지역정보개발원에서 발급을 해주며 행정자치부에서 관리 및 감독을 받는다. 처음에는 발급 및 이용이 이원화되어 있었으나 상호연계시스템을 갖추면서 민간 아이핀이나 공공 아이핀에서 아이핀을 발급받으면 어느 영역에서나 사용을 할 수 있도록 되었다. 민간 아이핀은 나름대로의 보안대책을 꾸준히 수립하여 준비하였고 공공 아이핀은 그렇지 못하다보니 허점을 노린 해커의 공격 목표가 되고 말았다 [12]. 이원화되어 있더라도 정보교류를 통하여 시스템에 대한 상호 발전, 유지, 보수가 꾸준히 이루어져야 한다.

5) 상시 모니터링 체계 부제

아이핀 시스템에 대한 모니터링 체계가 없었다는 것도 문제점으로 지적되고 있다. 전국민을 대상으로 인터넷상에서 사용하는 주민등록번호 대체수단을 발급하는 시스템인데 이에 대한 실시간 모니터링 시스템(인적 자원 포함)이 없었다는 것은 문제점이 아닐 수 없다.

4.2 정부의 개선책 분석

1) 전면재발급-본인확인후 재사용

정부는 5월부터 아이핀을 전면 재발급할 예정이며 본인 확인후에 재사용을 할 예정이다. 이는 아이핀 시스템을 폐기하지 않는 한 불가피한 사항인데 재발급시 그 절차와 방법은 더 이상이 혼란이 발생하지 않도록 정확하고 간결하며 신속하게 이루어져야 할 것이다. 그러나 이미 아이핀에 대한 신뢰가 떨어져서 얼마나 재발급을 받으려는 사용자가 있을 런지는 의문일 수 밖에 없다 [12].

2) 해킹방지기능 및 2차 패스워드 인증기능 추가

공공 아이핀에도 민간 아이핀에서 사용하는 해킹방지 기능과 2차 패스워드의 추가 인증 기능을 도입하는 것이다. 해킹방지 기능은 일방향성을 갖는 해쉬

함수를 이용하여 검증을 하는 것이며 2차 패스워드 인증기능은 인터넷뱅킹에서 공인인증서 사용시에 인증서 비밀번호이외에 보안카드나 OTP를 사용하는 즉, 추가적인 인증기능을 말한다. OTP는 아니어도 보안카드 정도의 2차 인증기능 도입은 적절하리라 판단된다 [13].

3) 모니터링에 의한 의심 IP 접속차단

이번 아이핀 대량 부정발급 사건은 사실상 간단하고 기본적인 모니터링 체계가 존재했다면 초기에 발견 및 조치가 이루어졌을 사건이다. 동일한 IP에서 1개 이상의 아이핀을 발급받아도 의심스러운 상황으로 인지할 수 있는데 동일한 IP에서 수천개의 아이핀을 발급받는 것을 전혀 인지하지 못한 것이다. 따라서 이러한 모니터링 기능은 반드시 필요한 기능이며 체계이다.

4) 부정방지 시스템(FDS) 도입

부정방지 시스템 혹은 사고예방모니터링시스템으로 불리우는 FDS(Fraud Detection System)는 국내보다는 국외에서 활성화되어 있는 일종의 모니터링 시스템이다. 예를 들어 한 지점에서 신용카드 결재후에 다른 지점에서 또 결재가 이루어졌는데 이 두 장소를 아무리 빠른 이동수단을 이용해도 갈 수 없다면 이는 결국 위조에 의한 불법신용카드 사용이 되는 것이며 이를 모니터링으로 발견하고 거래정지 등의 조치를 취하는 것이다. 그러나 이는 금융거래에서 주로 이루어지는 모니터링 시스템인데 이를 아이핀에 도입하는 것은 다소 무리가 있어 보인다, 아이핀은 인터넷상에서 단지 주민등록번호를 대신하여 사용되는 목적을 갖고 있기 때문이다 [14].

5) 모의 해킹 실시

화이트 해커 즉, 착한 해커를 활용하여 실제 공격상황과 맞먹는 모의해킹을 아이핀에 정기적으로 실시하여 취약점을 분석하고 이를 강화해나가는 것이다. 그러나 이는 아이핀 시스템을 개발하고 유지 및 보수하는 담당자들이 맡아야할 업무이며 자칫 화이트 해커가 아이핀의 취약점을 발견하고 이를 은밀히 블랙해커(악의적인 해커)에게 판매할 수도 있기 때문에 의려가 되는 대책이다.

6) 3개월마다 비밀번호 변경하기 캠페인 실시

3개월마다 아이핀의 비밀번호를 변경하는 캠페인을 실시하는 것도 좋은 방법일 수 있다. 그러나 첫 발급시에 본인확인에 대한 확실한 인증방법과 사용시에 2차적인 추가인증 방법만 안전하다면 비밀번호 변경은 필요하지 않다.

Ⅴ. 제안하는 개선방법

본장에서는 앞의 분석 등을 통하여 아이핀 시스템의 개선을 위한 방법을 제시하고자 한다.

5.1 개선방법

1) 발급 시 개인정보 입력금지

우리나라 경제활동인구의 대부분은 현재 주민등록번호, 실명, 휴대폰번호, 주소, 성별 등의 개인정보가 인터넷에 유출되어 불법적으로 전매되고 있는 상황이다. 따라서 개선되는 아이핀 시스템에서는 발급시에 손쉽게 구할 수 있는 개인정보를 입력하도록 요구

해서는 안된다.

2) 대면인증을 통한 발급

아이핀은 인터넷상에서 사용하는 주민등록번호 대체수단이다 보니 편리하게 인터넷상에서 본인확인을 하도록 되어 있으며 결국 부정발급도 대량으로 이루어지게 되었다. 은행 지점이나 주민센터 등을 신분증을 지참하고 방문하여 대면인증을 통하여 발급이 이루어진다면 발급에 대한 불편함은 생기지만 이번 사고와 같은 대량부정발급 사고는 발생할 수 없게 된다.

3) 사용 시 오프라인 매체에 의한 2차 인증

아이핀은 아이디와 비밀번호만 알면 누구든지 사용할 수 있는 편리한 도구이다. 역설적으로 말하면 그 두가지만 누군가 몰래 알아낸다면 인터넷에서 다른 사람의 행세를 할 수 있기도 한 것이다 [10]. 공인인증서 사용시 추가적으로 요구되는 보안카드나 OTP 같은 도구를 사용한다면 단지 아이핀의 아이디와 비밀번호의 유출만으로 이루어지는 불법사용은 훨씬 줄일 수 있다.

4) 아이핀 사용 통보 서비스

아이핀 사용시 소유자에게 문자나 이메일 등을 이용하여 사용일시, 사용 사이트 주소 등을 알려준다면 사용자는 자신의 아이핀에 대한 사용 및 분실여부와 그에 따른 신고 등을 손쉽게 할 수 있으며 결과적으로 부정발급 및 사용은 근절될 수 있다.

5) 아이핀 사용에 대한 아웃라인 설정

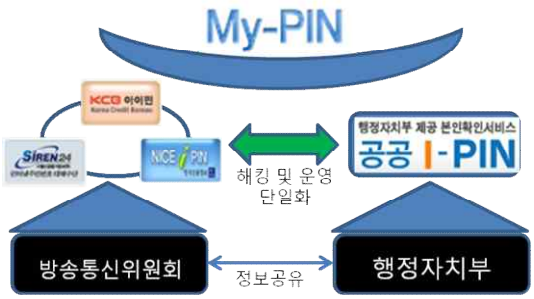
아이핀은 주민등록번호를 대신할 뿐이지 공인인증서 등을 대신할 수는 없다. 이번 대량부정 발급사고를 통해서 발급된 아이핀이 일부 게임 및 도박 사이트에서 사용된 것은 게임머니나 포인트, 아이템 등을 통하여 금전을 획득하기 위한 것이다. 금전으로 변경될 수 있는 것은 반드시 공인인증서 등과 같은, 강력한 본인인증 수단을 통하여 이루어져야 하며 아이핀은 단지 주민등록번호를 대체할 뿐이다.

6) 아이핀 보안강도에 대한 아웃라인 설정

앞의 5)번과도 연관성이 있는 사항인데 아이핀은 단지 인터넷상의 주민등록번호이므로 FDS와 같은 보안강화 수단의 도입은 자제되어야 한다. FDS는 신용카드 등과 같은 결재수단의 복제 및 분실이나 탈취에 의한 불법 사용을 막기 위한 도구이기 때문에 단지 인터넷상의 주민등록번호인 아이핀에 도입하는 것은 무리가 있다.

5.2 운영방법

이러한 개선방법들을 기반으로 아이핀 시스템은 다음과 같이 개선된 방향으로 운영되어야 한다.



<그림 4> 제안하는 민간 및 공공 아이핀 시스템 운영 개념도

<그림 4>에서와 같이 현재 민간 아이핀은 방송통신위원회에서, 공공 아이핀은 행정자치부에서 관리

및 감독을 하고 있다. 따라서 방송통신위원회와 행정자치부가 긴밀한 정보공유를 하거나 아니면 제3의 기관에 맡겨 해킹대비 및 운영에 대한 단일화가 이루어져야 한다. 운영에 관한 내용을 좀더 구체적으로 표로 정리하면 <표 2>와 같다.

아이핀의 유효기간은 1년이 적절하며 첫 발급시에는 오프라인 인증 즉, 대면인증이 반드시 이루어져야 한다. 재발급은 오프라인 혹은 온라인으로 선택적으로 하되 3~5년 마다 대면인증을 통하도록 한다. 아이핀을 발급받아 사용시에 1차 인증은 아이핀의 아이디와 비밀번호로 하고 2차 인증은 2차 비밀번호나 금융권에서 사용하고 있는 OTP를 사용할 수 있도록 한다. 고객의 아이핀이 유출되었거나 불분명한 사유로 재발급을 할 시에는 반드시 대면인증을 거치도록 한다. 아이핀을 사용하게 되면 사용자에게 문자로 사용 정보를 서비스하도록 하여 부정한 사용을 추후 적발할 수 있도록 한다.

아이핀은 인터넷상에서 주민등록번호를 대체하는 수단으로만 사용되어야 하며 포인트나 아이템 거래 등을 포함한 금융거래에는 절대로 사용되어서는 안 된다.

<표 2> 아이핀 시스템 운영 방법

	운영 방법
관리, 감독	방송통신위원회와 행정자치부의 긴밀한 유대 혹은 제3의 기관
아이핀 유효기간	1년
최초 발급시	오프라인 인증 (대면 인증)
재발급시	오프라인 혹은 온라인 인증 (3~5년마다 오프라인 인증)
1차 인증	아이디, 비밀번호
2차 인증	2차 비밀번호 혹은 OTP
사고시 재발급	오프라인 인증 (대면 인증) 필수
해킹대비	공공 및 민간 전문가들의 협의체를 통한 대책 수립
사용 확인	문자 서비스 제공 (필수)
용도제한	금융거래(포인트, 아이템 거래 등 포함)과는 무관한, 순수한 주민등록번호 대체수단
모니터링 (개인별)	동일 시간대에 동일 아이피에서 2개 이상 발급시 재확인필요
모니터링 (전체)	시간대별 아이핀의 발급지역, 발급수 등의 변화량에 대한 24시간 상시 모니터링 필요

VI. 결론

아이핀은 인터넷상에서 무분별하게 사용, 저장, 유출되는 주민등록번호의 오남용를 막기 위한 필요성에 의하여 도입이 되었다. 그동안 부당한 본인 인증을 통한 소량의 부정발급 및 판매 사고는 있어 왔지만 어느 정도 안전한 시스템이라는 신뢰를 갖고 있었으며 확대 사용이 되고 있다가 이번과 같이 75만건이라는 대량 부정발급 사건이 발생하게 되었다. 그 원인은 앞에서 살펴본 바와 같은 여러 가지 문제점에서 살펴볼 수 있으나 한편으로는 작년 가을에 발효되어 계도기간을 거쳐 2015년 2월 7일부터는 주민등록번호를 무단으로 수집하게 되면 3천만원이하의 과태료 처분을 받게 되어 있는 현행 주민등록번호 수집 법정주의가 그 배경에 있다. 즉, 주민등록번호를 온라인 상에서 더 이상 사용할 수 없게 된 해커조직이 아이핀 아이디와 비밀번호를 확보하기 위하여 벌인 해킹 사건인 것이다. 아이핀은 <그림 4>와 같이 오프라인용인 마이핀(먼저 아이핀에 가입한 후 제공)으로도 확대되어 사용되고 있다. 따라서 그 근간이 되는 아이핀 시스템의 운용 및 관리는 중요하다고 하겠다.

앞에서 살펴본 아이핀의 문제점과 정부의 대책 그리고 본 논문에서 제안한 개선방법에서 알 수 있듯이 현재 관련 기술이 확보되지 않아 일어난 사건은 절대로 아니다. 일관성이 있는 정부 정책과 꾸준한 유지보수 및 관리만이 이러한 사건을 미리미리 막을 수

있을 것으로 판단된다. 아울러 2015년 5월에 시행되는 아이핀의 재인증 절차 역시 앞으로 아이핀의 지속 여부를 판가름할 중요한 절차가 될 것으로 사료되는 바이다.

참고문헌

[1] 한국인터넷진흥원, http://i-pin.kisa.or.kr/kor/issue/method.jsp.

[2] "'아이핀' 불법 발급받아 거래한 일당 검거," ytn 뉴스, http://news.mt.co.kr/mtview. php?no=2007081715265696833&type=&., 2010. 6. 7.

[3] "'주민등록번호 대체하는 '아이핀'도 뚫렸다," 국민쿠키뉴스, http://news.kukinews.com/article/view.asp?page=1&gCode=soc&arcid=0008086907&cp=nv., 2014. 2. 27.

[4] "아이핀, 대량해킹 유출사고 발생해... "아이핀, 너마저도"," 조선일보, http://news.chosun.com/site/data/html_dir/2015/03/05/2015030503316.html, 2015. 3. 5.

[5] "56시간30분 이상유무 감지 못한 '공공 아이핀'," 아이뉴스24, http://news.inews24.com/php/news_view. php?g_serial=886146&g_menu=020200&rrf=nv, 2015. 3. 8.

[6] "주민번호 대체 '아이핀' 해킹사고, 보완책 시급," 중소기업신문, http://www.smedaily.co.kr/news/articleView.html?idxno=54067, 2015. 3. 5.

[7] 이형효, "주민등록번호 대체수단 요구사항 연구," 한국정보기술학회, 한국정보기술학회하계학술대회논문집, 2010, pp. 398-401.

[8] 이형효, "개인정보보호를 위한 주민등록번호 대체수단 및 관리체계," 한국정보기술학회, 한국정보기술학회논문지, 제8권, 제6호, 2010, pp. 49-58.

[9] 안정희, "인터넷상의 주민등록번호 대체수단의 문제점과 해결방법," 디지털산업정보학회, 디지털산업정보학회논문지, 제4권, 제3호, pp. 78-89, 2008.

[10] 최윤성, 이윤호, 김승주, 원동호, "주민등록번호 대체수단에 대한 구현 취약점 분석," 정보보호학회, 정보보호학회논문지, 제17권, 제2호, pp. 145-185, 2007.

[11] 이영교, 안정희, "공인인증서를 이용한 주민등록번호 대체수단에 관한 연구," 디지털산업정보학회, 디지털산업정보학회논문지, 제10권, 제3호, pp. 107-117, 2014.

[12] "공공아이핀 전면 재발급…주민번호 대체 근본책은," 세계일보, http://www.segye.com/content/html/2015/03/25/20150325004362.html?OutUrl=naver, 2015. 3. 25.

[13] "아이핀 관리체계 民·公 '따로' …보안·개인정보 정책도 '따로'", 머니투데이뉴스, http://www.mt.co.kr/view/mtview. php?type=1&no=2015031113304730789&outlink=1, 2015. 3. 12.

[14] "5월부터 전면 재발급 '공공아이핀', 본인 확인 후 재사용…부정사용방지시스템 도입'", 동아일보, http://studio.donga.com/View?idxno=201503250041&c=00030003, 2015. 3. 25.

■ 저자소개 ■

이 영 교
Lee Younggyo

1986년 2월 한양대학교 전자공학과 (공학학사)
1991년 8월 한양대학교 전자공학과 (공학석사)
1993년 3월~1998년 9월
대우통신종합연구소 선임연구원
1999년 2월~2001년 6월
LG정보통신중앙연구소
선임연구원
2006년 8월 성균관대학교 컴퓨터공학부
(공학박사)
2008년 3월~현재
서일대학교 인터넷정보과 조교수

관심분야 : 정보보안, PKI, 암호이론
E-Mail : younggyo@seoil.ac.kr

안 정 희
Ahn Jeonghee

1988년 2월 성균관대학교 정보공학과
(공학학사)
1993년 2월 성균관대학교 대학원 정보공학과
(공학석사)
2000년 2월 성균관대학교 대학원 정보공학과
(공학박사)
1996년 3월~현재
두원공과대학교
스마트소프트웨어과 부교수

관심분야 : 정보통신 보안, 전자상거래 보안,
트래픽 제어
E-Mail : jhpro@doowon.ac.kr

논문접수일: 2015년 4월 15일
수 정 일: 2014년 5월 7일
게재확정일: 2014년 5월 15일