情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

국가 IDM을 위한 아이핀 발전 전략

최 광 희*, 정 승 욱**, 이 강 신***, 안 승 호****

요 약

인터넷상에서 무분별한 주민등록번호 사용을 최소화하여 명의도용 등의 피해를 방지하기 위하여 2005년부터 아이핀을 개발하여 보급중이며, 특히 아이핀 서비스를 대폭 개선한 아이핀 2.0이후에는 도입하는 웹사이트와 이용자가 급증하는 상황이다. 본 논문에서는 아이핀이 단순히 웹사이트 회원가입시 실명확인을 대체하는 수단을 넘어 인터넷상에서 국민 전체가 안전하고 편리하게 사용할 수 있는 디지털 ID가 되기 위한 발전 전략을 제시하고자 한다.

Ⅰ. 서 론

주민등록번호는 비대면인 인터넷에서 사용자의 신원을 확인할 수 있는 인터넷상의 신뢰체계로써 장점과 생년월일, 성별 등의 개인정보를 숫자로 담고 있어 편리하게 다양한 서비스에 이용이 가능하다는 이유로 국내 웹사이트에서는 회원가입시 무분별하게 수집하여 활용해 왔다. 하지만 안전하지 않은 주민등록번호의 이용과 저장 때문에 주민등록번호 대량 유출사고와 인터넷상에서 유출된 주민등록번호로 인한 명의도용 등의 2차 피해가 계속 증가하여 인터넷상의 신뢰체계를 손상시키는 위험이 되고 있다.[3][4][5][6][7][8][9]

정부는 이러한 인터넷상 주민번호 오남용으로 인한 문제를 해결하기 위하여 웹사이트 회원가입시 주민등록번호 수집을 대신할 수 있는 아이핀을 개발하여 보급중에 있다. 아이핀은 최초 개발 이후 이용자 측면의 편리성과 사업자측면의 활용성을 지속적으로 개선하면서 '11년 3월말 현재 5,699개 웹사이트에 아이핀이 도입되고 340만개 이상이 발급되어 이용중에 있다. 하지만 ID와 패스워드 형태로 운영되어 ID 도용 등의 아이핀의 안전성 문제와 현재 웹사이트 회원가입시나 게시판에서 실명확인 용도로 사용되는 이용범위의 제한 등으로 인해 주민등록번호, 공인인증서와 같은 기존 인터넷상 본인확인수단 수준으로 이용되지는 못하고 있는 실정이다. 따라서 국민들이 인터넷상에서 편리하고 안전하게 사용하는 범용적 ID 서비스가 되기 위한 아이핀의 향후 발전 전략을 제시하고자 한다.

본고의 구조는 다음과 같다. 2장에서는 아이핀 2.0을 설명하고 3장에서는 아이핀이 IDM으로써 가지는 한계점을 설명하고 4장에서 IDM으로써 아이핀의 발전전략을 설명한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 아이핀 서비스

아이핀은 개인정보 보호조치가 미흡한 다수의 웹사이트에서 직접 주민등록번호를 수집·이용하면서 발생하는 문제점을 보완하기 위해 만들어진 서비스 체계다. 아이핀(i-PIN)은 인터넷상에서 신뢰할 수 있는 인증 서비스 제공을 위하여 아이핀(i-PIN) 발급기관인 본인확인기관, 본인확인기관의 관리·감독 업무를 수행하는 감독기관(한국인터넷진흥원), 아이핀(i-PIN) 서비스를 도입하여 운영하는 웹사이트, 아이핀(i-PIN) ID/패스워드를 발급받아 이용하는 이용자로 구성되어 운영된다.

2.1 인증 절차

아이핀(i-PIN) 이용자는 본인확인기관중 1개 기관을 선택하여 아이핀(i-PIN) ID와 패스워드를 등록할 수 있

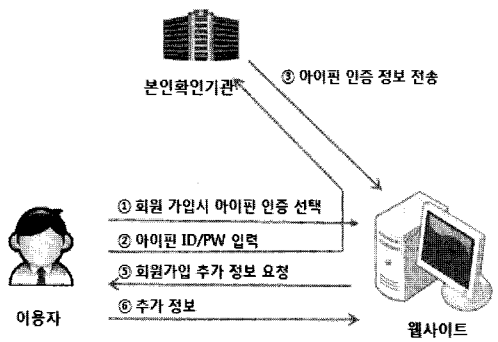
* 한국인터넷진흥원(khchoi@kisa.or.kr)
** 한국인터넷진흥원(swjung@kisa.or.kr)
*** 한국인터넷진흥원(kslee@kisa.or.kr)
**** 전남대학교(shahn@chonnam.ac.kr)

다. 등록과정에서 이용자는 주민등록번호와 실명을 입력하고 입력한 정보를 휴대폰, 신용카드, 공인인증서, 세대원의 주민등록증 발급 일자, 대면확인 등의 수단을 통해 검증하게 되며, 검증이 된 주민등록번호를 이용하여 웹사이트에 제공되는 이용자의 아이핀 인증정보가 생성되어 된다[1].

등록한 아이핀 ID와 패스워드는 발급기관에 상관없이 아이핀(i-PIN)이 도입된 공공과 민간 모든 웹사이트에서 동일하게 사용할 수 있다. 이용자가 웹사이트 회원가입시 실명인증 대신 아이핀(i-PIN) 인증을 선택하게 되면 웹사이트에 아이핀(i-PIN) 서비스를 제공하고 있는 본인확인기관으로부터 아이핀(i-PIN) 인증 요청이 이용자에게 송신된다[2].

이때 이용자는 아이핀(i-PIN) ID와 패스워드를 입력하고 본인확인기관에 송신한다. 본인확인기관에서는 ID/패스워드를 검증하여 이용자 속성정보를 웹사이트에 제공하게 된다. 웹사이트는 본인확인기관으로부터 이용자의 인증정보를 수신하여 기존에 회원으로 가입하였는지 등을 확인한 후, 회원가입에 필요한 추가 정보를 입력하게하고 회원가입을 허용하게 된다.

본인확인기관에서 웹사이트에 제공하는 이용자 속성정보는 주민등록번호를 이용한 서비스를 대체할 수 있도록 성명, 생년월일, 성별 등이 포함되어 구성되어 있다.



〔그림 1〕 서비스 이용 절차도

2.1.1 성명정보

실명확인 및 본인확인을 통해 검증한 이용자의 실명

2.1.2 생년월일정보

웹사이트의 경우 「청소년보호법」 제17조에 따라, 청소년유해매체물을 제공할 경우 인터넷 사이트는 이용자가 청소년인지 식별하기 위해 법적 연령을 확인해야 한다. 따라서 본인확인기관은 본인확인을 통해 검증된 주민등록번호로부터 이용자의 생년월일정보를 추출하여 웹사이트에 제공한다.

2.1.3 중복가입확인정보

웹사이트는 효율적인 IT 자원관리, 회원간의 신뢰 향상 등의 목적으로 회원의 중복가입을 제한하는 경우가 많으며 대부분 주민등록번호를 이용하여 중복가입을 방지하고 있다. 아이핀(i-PIN)은 본인확인기관에서 주민등록번호와 이용자가 가입하려는 웹사이트 정보를 이용하여 1차 해쉬한 값을 만들고, 본인확인기관간 공유한 비밀키를 이용하여 2차로 해쉬한 값을 생성하여 웹 사이트내에서 개개인을 고유하게 식별할 수 있는 정보를 만들어 웹사이트에 제공하고 있다.

2.1.4 연계정보

국내에서는 웹사이트나 사업자간 연계를 통한, 마일리지 등의 서비스가 활발히 제공되고 있다. 이러한 사업자간 연계시 개인을 식별할 수 있도록 이용자의 주민등록번호을 해쉬하여 연계 정보가 제공된다.

〔표 1〕 연계정보 생성방법

< CI 생성 방법 >

$$CI = HMAC_{sk}((RN \| Padding) \oplus S_A)$$

- ▷ CI : 서비스 연계를 위한 웹사이트 간 공동 식별자로 64바이트의 암호화된 코드
- ▷ $H()$: 512비트 이상의 출력을 갖는 암호학적으로 안전한 해쉬 함수
- ▷ RN : 주민등록번호 (13byte=104bit)
- ▷ $Padding$: 입력 값을 512bit로 만들기 위해 주민번호 104bit를 제외한 408bit를 채워 넣음
- ▷ S_A : 신뢰기관 보유 비밀정보(64byte=512bit)
- ▷ sk : 신뢰기관 보유 비밀키(64byte=512bit)
- ▷ $\|$: concatenation, 기호의 앞뒤를 연접

연계정보는 주민등록번호을 Keyed Hash하여 생성되는 값이다. 아이핀(i-PIN) 이용자의 주민등록번호에 패딩값을 추가하고 첫 번째 임시값을 생성하고 이 임시값과 신뢰기관에서 보유하고 있는 비밀값을 Xor 연산을

통해 두 번째 임시값을 생성한다. 생성된 임시값은 512bit의 비밀키로 동작하는 Keyed Hash 연산을 통해 연계정보(C)로 만들어지게 된다. .또한 비밀값과 비밀키값은 신뢰기관에서 안전하게 관리 하여 유노출의 유험을 최소화 하였으며, 비밀값이나 비밀키값의 노출 또는 해쉬 알고리즘의 안전성 문제 발생에 대비하여 침해사고 발생시 연계정보(CI)를 갱신할 수 있는 메시지 양식과 절차가 함께 마련되어 운영 중에 있다[1][2][11].

〔표 2〕 아이핀 1.0에서 제공되는 이용자 속성정보

제공정보	내용
성명	본인확인 수단을 이용하여 검증한 이용자의 실명
개인 식별번호	본이확인기관이 이용자에게 부여하는 13자리 정보(발급기관정보 2자리)이외는 난수값)
중복가입 확인정보	웹사이트내에서 이용자를 고유하게 식별할 수 있는 정보
연계정보	웹사이트간 연계서비스시 이용자를 고유하게 식별할수 있는 정보
생년월일	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보
성별	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보
연령대	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보를 분류하여 8단계의 연령대 정보 제공
본인확인 수단	아이핀 발급시 이용한 본인확인 수단

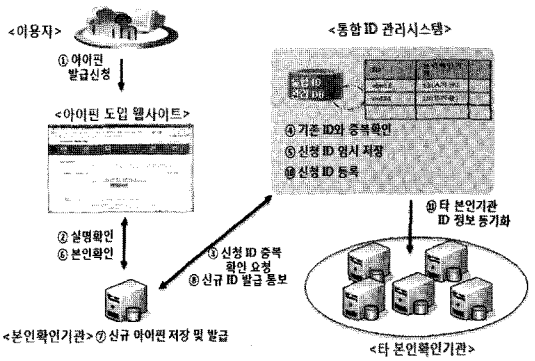
2.2 발급기관 자동 식별

각 본인확인기관별로 발급·관리되던 아이핀(i-PIN) ID를 통합하여 발급기관과 아이핀(i-PIN) ID쌍을 별도 DB에 저장하고 각 본인확인기관이 관련 정보를 실시간으로 공유하게 하는 통합 ID 관리시스템을 구축하여 발급기관을 자동으로 식별할 수 있게되어 이용자는 발급기관을 암기할 필요가 없다.

먼저 통합 ID 관리시스템을 통한 아이핀(i-PIN) 신규 발급 절차를 살펴보면, 이용자는 아이핀(i-PIN)을 신규로 발급받기 위해 실명확인후, 사용하려는 ID가 이미 사용중인지를 통합 ID 관리시스템을 통해 확인하게 된다. 사용 중이지 않는 ID인 경우 임시로 통합 ID 관리시스템에 저장되고, 본인확인기관에서 이용자의 본인확인을 거쳐 최종 아이핀(i-PIN) ID가 발급되면 통합ID 관리시스템상에 최종 등록되고 저장되게 된다. 이렇게 신규로 등록된 아이핀 ID와 발급한 본인확인기관 정보는 타 본인확인기관에 실시간으로 전송되어 각 본인확인기관이 전체 아이핀(i-PIN) ID와 발급기관 현황을 유지할수 있게 된다.

이렇게 각 본인확인기관마다 아이핀(i-PIN) ID와 발급기관 정보가 실시간으로 공유되어 이용자가 아이핀(i-PIN) 인증시 ID를 입력하면 본인확인기관에서 해당 ID의 발급기관을 식별하여 해당 본인확인기관을 통해 아이핀 인증을 처리하게 된다. 따라서 이용자가 일일이 발급기관을 암기하고 아이핀(i-PIN) 이용시 발급기관을 선택하여하는 불편이 해결되게 되었다.

또한 통합 ID 관리시스템이 장애시에는 각 본인확인기관이 자체 보유중인 아이핀 ID 정보로 신규 발급을 수행하고 장애 복구후에 자체 발급된 ID 정보를 통합 ID 관리시스템으로 전송하여 본인확인기관간 동기화가 진행되도록하였다. 이러한 장애대응 절차를 통해 통합 ID 관리시스템에 장애가 발생하더라도 아이핀(i-PIN)을 신규 발급할 수 있도록 하였다[1].

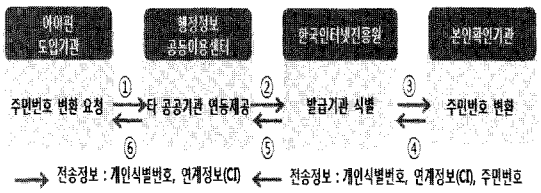


〔그림 2〕 아이핀 신규 ID 발급 절차

2.3 주민등록번호 변환 서비스

웹사이트에 회원 가입시 아이핀을 이용할 경우 해당 웹사이트에서는 주민등록번호를 저장하지 않게 된다. 하지만 공공, 금융, 조세 등 일부 웹사이트는 법률에의해 주민등록번호를 요구할 수 있고, 아이핀을 통해 회원에 가입한 이용자는 해당 서비스 이용을 위해 다시 주민등록번호를 입력해야하는 문제가 발생한다. 이러한 문제를 해결을 위해, 아이핀을 도입한 웹사이트가 아이핀 인증정보를 발급한 본인확인기관에 전송하면, 해당

정보를 주민증록번호로 변환하여 해당 웹사이트에 제공함으로써 이용자는 추가로 주민등록번호를 입력하지 않아도 되고, 해당 웹사이트는 기존 주민등록번호 기반의 서비스 시스템을 변경하지 않아도 된다.



〔그림 3〕 주민등록번호 변환서비스 절차

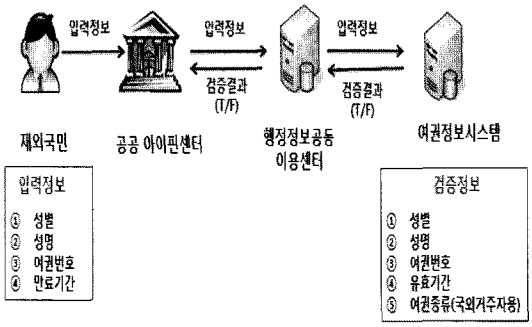
현재 공공기관을 대상으로 서비스 중이며 변환절차는 아이핀 도입기관에서 주민등록번호 변환이 필요한 이용자의 개인식별번호와 연계정보를 한국인터넷진흥원으로 전송하면, 한국인터넷진흥원에서는 개인식별번호에서 발급기관을 확인하여 해당 본인확인기관에 주민번호 변환요청을 전송한다. 본인확인기관에서 개인식별번호를 이용하여 이용자를 식별하고 주민등록번호를 연계정보로 변환하여 전송된 연계정보와 비교하여 검증한 후, 이상이 없을 경우 해당 주민번호를 요청한 기관에 전송하게 된다.

2.4 여권정보와 연동을 통한 재외국민 아이핀 발급

주민등록번호가 말소되었거나, 본인명의로 발급받은 국내 신용카드, 휴대폰, 공인인증서 등의 본인확인 수단이 없는 국외 거주자의 아이핀(i-PIN) 발급을 위하여 외교부 여권정보를 이용한 재외국민 아이핀(i-PIN) 발급 기능이 구축되었다.

아이핀(i-PIN) 발급시 여권정보를 이용한 본인확인을 하는 방법은 성명, 성별, 여권번호, 여권만료 일자를 입력하면 본인확인기관(공공 아이핀 센터)[1]에서는 외교부 여권정보시스템에 입력한 정보의 진위 및 여권의 유효성 검증을 요청하고 결과가 유효할 경우 아이핀(i-PIN) 발급이 이루어지게 된다.

여권정보를 이용한 아이핀(i-PIN) 발급의 문제점은 여권이 갱신될 경우 여권번호가 변경되어 여권번호를 기반으로 생성된 인증정보인 중복확인정보(DI) 및 연계정보(CI)가 변경되어 여권갱신 전에 가입한 웹사이트와 여권 갱신 후에 가입한 웹사이트에서 동일인을 식별할 수 없는 상황이 발생한다.



〔그림 4〕 재외국민 여권정보 검증절차

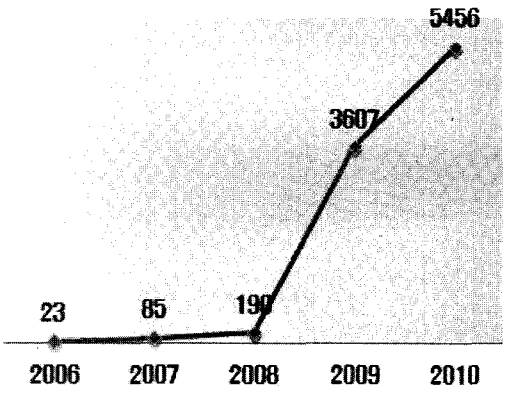
이런 문제를 해결하기 위하여 재외국민의 경우 아이핀(i-PIN) 최초 발급시 여권번호와 갱신된 여권번호를 모두 저장하고 중복확인정보와 연계정보는 최초 가입시 여권번호를 기반으로 생성하여 운영함으로써 이러한 문제를 해결하였다.

Ⅲ. 아이핀 이용 현황 및 문제점

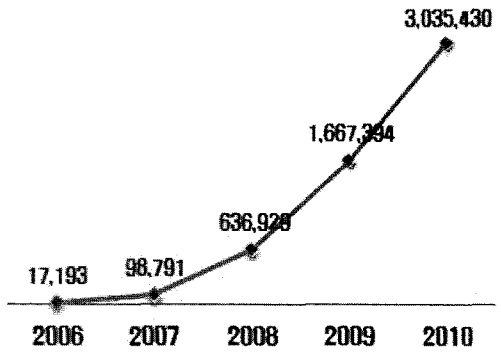
개발 초기 아이핀은 이용자측면에서 13자리 숫자와 발급기관을 암기해야하고, 웹사이트별로도 사용할 수 있는 발급기관이 정해져 있어 외면을 받아 왔다. 또한 사업자들로 주민등록번호가 활용되는 다양한 정보가 제공되지 않는다는 이유로 아이핀을 도입하려고 하지 않았다. 하지만, 2009년 기존의 문제점을 대폭 개선한 아이핀 2.0서비스가 시작되고, 일일방문자수 기준으로 포탈 5만명이상, 기타 1만명이상의 웹사이트에 아이핀 도입이 의무화되면서 이용이 급증하였다. 2011년 3월기준으로 아이핀을 도입한 웹사이트는 5,699개이고, 발급한 아이핀 ID는 340만개를 넘었다. 또한 개인정보보호법 제정에 따라 행정안전부에서는 전체 공공기관 웹사이트에 아이핀 도입을 추진 중에 있어 보급 및 이용이 더욱 확대될 것으로 예상된다.

하지만, 여전히 국민들이 많이 이용하는 웹사이트 아이핀이 도입되지 못하고 있는 실정이다. 이러한 확산에 저해되는 주요한 문제점을 살펴보면 다음과 같다.

1) 여권정보를 이용한 재외국민 아이핀 발급은 현재 공공 아이핀센터에서만 가능



〔그림 5〕 아이핀 도입 웹사이트 수



〔그림 6〕 아이핀 발급 수

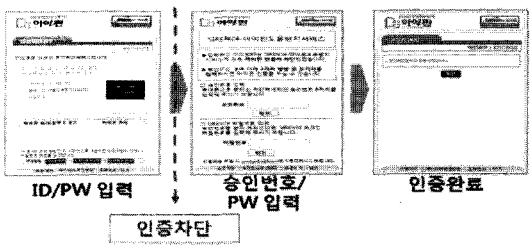
첫째, 아이핀 ID 도용 우려 : 아이핀은 이용자 편의를 고려하여 ID와 패스워드 형태로 운영된다. 하지만 많은 이용자들이 다른 웹사이트와 동일한 ID와 패스워드를 아이핀에서도 사용하고 있다. 이에 해커는 보안이 취약한 사이트를 해킹하여 ID와 패스워드를 획득한 후 아이핀에 대입하는 공격을 통해 아이핀 ID/패스워드 도용이 가능하다는 문제가 제기된다. 현재 아이핀을 사용할 때마다 이용자에게 이메일을 통해 알려주고 있으나 사후 피해확산방지에는 효과적이나 도용을 예방할 수는 없는 상황이다.

둘째, 동일한 속성 정보 제공 : 웹사이트마다 제공하는 서비스에 딸 필요한 이용자의 속성 정보가 상이하다. 예를 들면 전자상거래를 위해서는 이용자의 전자서명값이나 공인인증서가 필요할 수 있다. 하지만 아이핀은 현재 주민번호의 기능만을 속성값으로 제공하여 활용되는 서비스가 확대되는데 한계가 있다.

Ⅳ. 발전 전략

아이핀의 활용도를 높이고 범용적 ID 정책으로 발전하기 위해서 아이핀 인증 강화가 필수적이다. 일괄적인 인증강화 보다는 사용자가 인증수단을 선택할 수 있도록 다양한 인증방법을 제공하고 인증수단의 안전성에 따라 활용할 수 있는 속성정보도 이용자가 선택할 수 있도록 하는 이용자의 자기정보통제권을 강화하는 형태로 발전시켜야 할 것이다.

현재 아이핀은 인증 수단으로 ID/패스워드 만을 사용하여 주민번호와 같은 도용 위험이 지속적으로 제기 된다. 실제 이용자들이 웹사이트와 동일한 ID/패스워드를 아이핀에서도 사용하고 있어 이러한 위험이 상존하는 것이 사실이다. 이러한 문제를 해결하기 위하여 실시간으로 이용자가 아이핀 인증을 확인하고 통제할 수 있은 방안 마련이 필요하다.



〔그림 7〕 도용방지 절차

이용자가 아이핀 ID/패스워드를 입력하고 본인확인기관에서 이용자의 인증정보를 웹사이트에 전송하기 전에 휴대폰 등을 통해 실시간으로 이용사실을 통보하고 이용자가 인증을 허가하는 추가적인 인증 프로세스를 통해 ID/패스워드 도용을 방지할 수 있는 통제 수단이 우선 고려될 수 있다.

또한, 아이핀 사용자가 ID/패스워드 이외에 OTP(One Time Password)와 같은 안전성이 강화된 인증 수단도 선택할 수 있도록 하여 도용 위험을 최소화 할 수 있도록 발전시켜야 한다.

이러한 보안성이 강화 된다면, 현재 아이핀 인증시 웹사이트에 제공되는 속성정보를 좀 더 다양화 할 수 있다. iD/패스워드 이외의 추가적인 인증 수단을 사용하는 이용자는 [표 2]에 기술된 한정된 속성 정보이외에 이메일주소, 주소, 전화번호, 공인인증서 등 다양한 속성 정보를 본인확인기관에 저장하고 재사용할 수 있

는 기능을 추가하는 방안도 마련 할 수 있다.

V. 결 론

본고에서는 우선 아이핀 2.0 서비스를 자세히 소개하였다. 이어서 현재 아이핀 2.0이 가지고 있는 한계점을 지적하고 아이핀이 단순히 웹사이트 회원가입시 실명확인을 대체하는 수단을 넘어 인터넷상에서 국민 전체가 안전하고 편리하게 사용할 수 있는 디지털 ID로써 발전 방향을 제시하였다.

참고문헌

[1] 최광희, 안종찬, 이강신, 안승호, "인터넷상 주민번호 이용을 대체하기 위한 아이핀 2.0 서비스 프레임워크" 한국정보보호학회지 20(6), pp.88-95, 2010년 12월.

[2] 정찬주, 김윤정, 김진원, 박광진, " 주민번호 대체수단(i-PIN) 개발을 위한 기술표준과 서비스 프레임워크" 한국정보보호학회지 18(6) pp.20-27, 2008년 12월.

[3] 강달천, 허진수, 김동환, "2009 개인정보분쟁조정사례집", 한국인터넷진흥원 pp.14, 2010년 6월.

[4] 장인용, 염흥열, "인터넷상의 본인수단인 아이핀의 활성화 방안 연구", *한국정보보호학회지* 19(5), pp.81-92, 2009년 10월.

[5] EBN 산업뉴스, "옥션 해킹 피해자 1천863만 확정", http://www.ebn.co.kr/news/n_view.html?id=429093

[6] YTN, "GS 칼텍스 고객 1,100만명 개인정보 유출", http://www.ytn.co.kr/_ln/0103_200809081037189548

[7] Newsis, "LGT, 170명 주민등록번호 등 개인정보 유출", http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=003&aid=0002061600

[8] 전자신문, "다음, 개인정보 유출 소송 본격화", http://www.etnews.co.kr/news/detail.html?id=200808030022

[9] views&news, "다음 비밀번호 등 개인정보 유출은 없어", http://www.viewsnnews.com/article/view.jsp?seq=38090

[10] 노컷뉴스, "개인정보 무단 열람한 국민건강보험공단 직원 검거", http://www.cbs.co.kr/Nocut/Show.asp?IDX=800853

[11] 한국경제, "툭하면 전화 온다했더니…하나로텔레콤, 600만명 개인정보 유출 '파문'", http://www.hankyung.com/news/app/newsview.php?aid=2008042473737

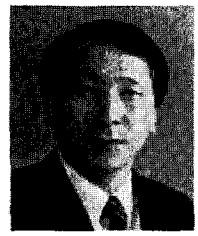
[12] *i-PIN 2.0 도입 매뉴얼*, 한국인터넷진흥원, 2009년 12월.

〈著者紹介〉

최 광 희 (Kwang-Hee Choi)
정회원
1997년 2월 : 중앙대 산업정보과 학사
2002년 2월 : 중앙대 정보시스템과 석사
2007년 2월 : 전남대 정보보호협동과정 박사 수료
2002년 1월~2009년 7월 : 한국정보보호진흥원
2009년 7월~현재 : 한국인터넷진흥원
관심분야 : PIMS, IDM, 정보보호 거버넌스

정 승 욱 (Seung Wook Jung)
정회원
1998년 2월 : 숭실대학교 전자공학과 학사
2000년 2월 : 숭실대학교 전자공학과 석사
2006년 2월 : 독일 지겐 대학교 컴퓨터공학과 박사
2006년 12월~현재 : 한국인터넷진흥원
관심분야 : 정보보호

이 강 신 (Gang-Shin Lee)
정회원
1987년 2월 : 한양대 수학과 학사
1989년 8월 : 한양대 수리통계 이학석사
2005년 8월 : 고려대 정보보호대학원 공학박사
2000년 9월~2009년 7월 : 한국정보보호진흥원 팀장
2009년 7월~현재 : 한국인터넷진흥원 인터넷기반·개인정보보호단 단장
2006년 9월~현재 : 건국대학교 겸임교수
관심분야 : 개인정보보호, 네트워크 보안



안 승 호 (Seung-Ho Ahn)
정회원
1981년 8월 : 전남대 수학과 이학석사
1985년 2월 : 전남대 수학과 이학박사
1987년 12월~1989년 12월 : 미국 미시건 대학 수학과 방문 교수
1983년 5월~현재 : 전남대학교 수학과 교수
관심분야 : 암호학 분야