情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

금융보안 OTP를 이용한 온라인 본인확인 방안에 대한 연구

정 찬 주*, 김 승 주**, 원 동 호***

요 약

본 논문에서는 금융보안 OTP를 이용한 온라인 본인확인 방안을 제안한다. 현재 국내에서 신원확인 방식으로는 공인인증서를 이용한 전자서명, 휴대폰SMS 발송번호, 신용카드정보 및 금융계좌정보 인증방식을 활용한 본인확인 방식이 사용되고 있다. 하지만, 공인인증서를 이용한 전자서명 방식이외의 방식은 명의도용된 휴대폰을 통한 본인확인과 신용카드 비밀번호 앞2자리 및 금융계좌의 비밀번호 4자리 입력 등 민감한 정보의 노출 위협 등의 문제점이 있다. 본 논문에서는 이와 같은 문제를 금융보안 OTP를 이용하여 안전하게 본인확인할 수 있는 방안을 제안한다. 제안된 방식은 웹사이트 회원가입, 게시판 글쓰기 등 온라인 본인확인이 필요한 경우에 언제든지 이용될 수 있고 아이핀(*i*-PIN)에서 본인확인 수단으로 도입된다면 개인정보를 보호할 수 있어 활용 가치가 높을 것이다.

Ⅰ. 서 론

국내 인터넷의 이용자의 수는 초고속 인터넷 망의 보급 확대에 따라 급속하게 늘어난 상황이다. 인터넷 이용자의 증가와 더불어 인터넷 서비스 제공 분야는 초기 뉴스, 자료 검색 등 정보 공유에서 게임, 쇼핑, 여행 등 정보 이용 및 결제분야로 확대되고 있다. 뉴스, 자료 검색 등의 서비스 제공 시에는 이용자에 대한 본인확인이 불필요하였으나 게임, 쇼핑, 여행 등의 서비스 분야에서는 이용자에 대한 본인확인이 필요하게 되었다. 국내 게임 웹사이트는 게임 내용에 따라 이용할 수 있는 연령을 청소년 보호법에 따라 표기하여 서비스를 제공하고 있고, 회원가입 시 이용자가 제공한 주민등록번호를 서비스 제공 기준으로 활용하고 있다. 국내 쇼핑 및 여행 웹사이트의 경우에도 전자상거래에 관한 소비자보호법에 따라 전자상거래의 기록으로 구매자의 주민등록번호 등을 보관하도록 되어 있어 회원가입 시 구매자가 제공한 주민등록번호를 활용하고 있는 실정이다.

국내 대부분의 웹사이트는 회원가입 시 가입자가 제공한 주민등록번호에 대한 오류검증번호 검증을 수행한 후에 회원가입을 받거나 또는 가입자가 제공한 성명과 주민등록번호를 신용평가사에서 전달하여 성명과 주민번호 쌍이 맞는지를 확인하는 실명확인 서비스를 통해 회원가입을 받고 있다.

하지만, 오류검증번호 검증 및 실명확인 서비스를 통한 회원가입 시 주민등록번호 소유자에 대한 본인여부를 확인할 수 없어 최근 사회문제화 되고 있는 실정이다. '07년 9월 대통합민주신당의 대통령 후보자 경선 투표자 중 노무현 대통령의 주민등록번호를 도용한 사건[1]이 대표적인 사례이다.

본 논문에서는 명의도용의 문제를 해결하기 위해 금융보안 OTP를 이용한 온라인 본인확인 방안을 제안한다. 먼저, 주민등록번호 오류검증번호 검증과 실명확인 서비스의 문제점을 2장에서 알아보고, 이를 개선한 공인인증서를 이용한 전자서명, 휴대폰SMS 발송번호, 신용카드정보 및 금융계좌정보 인증 방식을 통한 본인확

* 성균관대학교 정보통신공학부 (cjchung@security.re.kr)
** 성균관대학교 정보통신공학부 (skim@security.re.kr)
*** 성균관대학교 정보통신공학부 (dhwon@security.re.kr)

1) "노대통령도 신당 선거인단에 등록돼", 연합뉴스 2007년 9월 17일 보도자료

인 방안과 문제점을 3장에서 알아본다. 4장에서는 금융보안 OTP를 이용한 온라인 본인확인 방안을 제안하고, 기존의 방식과 비교하여 제안하는 방식의 우수성을 5장에서 알아본다. 마지막으로, 제안한 방안을 활용할 수 있는 분야와 결론을 6장에서 설명한다.

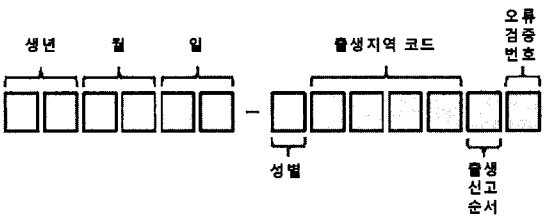
Ⅱ. 인터넷 상의 본인확인 방법

국내 인터넷 서비스가 다른 나라에 비해 다양할 수 있는 이유는 비대면의 인터넷 환경에서 이용자를 식별할 수 있는 주민등록번호가 존재했기 때문이다. 주민등록번호는 인터넷 이용자의 생년월일, 성별, 출생지 등의 정보를 갖고 있으며, 또한 국민 한 사람에게만 유일하게 부여되기 때문에 이용자를 식별할 수 있는 정보로서 활용 가치가 높다. 국내 대부분의 웹사이트는 회원가입 시 이용자의 주민등록번호를 요청하여 받고 있는 상황만으로도 그 이용 가치를 알 수 있다.

본 장에서는 웹사이트 회원가입 시 이용자의 본인확인방법으로 사용하고 있는 주민등록번호 오류검증번호 검증 방법 및 성명과 주민등록번호 일치여부를 확인하는 실명확인 서비스에 대해 알아본다.

2.1. 주민등록번호 오류검증번호 검증 방법

주민등록번호는 생성규칙에 따라 국민 한사람에게 유일하게 부여되는 13자리 숫자이다. 13자리 숫자는 생년월일을 나타내는 앞 6자리(YYMMDD)와 성별(1자리), 출생지(4자리), 출생지에 신고 순서(1자리) 및 오류검증번호(1자리)를 나타내는 뒷 7자리로 구성된다[1]. [그림 1]은 주민등록번호 구성 방식이다. 일반적으로 실명확인 서비스를 이용하지 않는 웹사이트는 이용자가 입력한 주민등록번호의 오류검증번호가 오류검증번호 생성규칙과 일치하는지 확인하는 방법을 사용하고 있다. 오류검증번호는 주민등록번호 앞 12자리에 따라 결정되기 때문에 임의의 주민등록번호 앞 12자리에 대해 10번만 시도를 하면 정확한 오류검증번호를 찾을 수 있다. 주민등록번호 오류검증번호만 검증하여 회원가입을 허용하는 일부 인터넷 웹사이트의 경우에는 10번만 시도하면 임의의 주민번호로 회원가입을 할 수 있는 문제점을 갖고 있다.

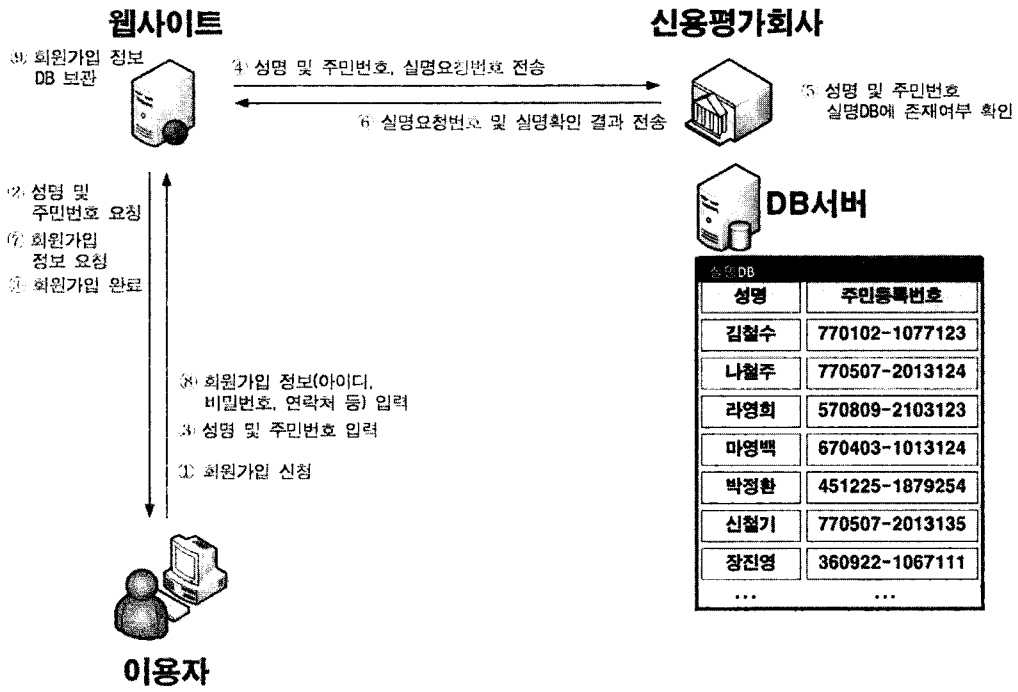


〔그림 1〕 주민등록번호 구성 방식

2.2. 실명확인 서비스

대부분의 인터넷 웹사이트는 주민등록번호 오류검증번호 검증 방법의 문제점을 해결하기 위하여 이용자의 성명과 주민등록번호 일치여부를 확인해주는 실명확인 서비스를 이용하여 회원가입을 진행하고 있다. 실명확인 서비스를 제공하는 신용평가회사는 국민들이 신용카드 발급, 금융계좌 개설, 휴대폰 개통 등에 사용된 성명과 주민등록번호에 대한 정보를 수집하여 실명확인 데이터베이스를 구축하여 성명과 주민등록번호 일치여부만을 확인해 주고, 웹사이트는 일치여부의 결과에 따라 회원가입을 위한 아이디, 비밀번호, 연락처 등의 정보를 요청한 후 회원가입을 완료하게 된다. [그림 2]은 실명확인 서비스에 따른 웹사이트 회원가입 절차를 도식화한 것이다.

회원가입 절차는 이용자가 웹사이트에 회원가입을 신청하면 웹사이트는 이용자에게 성명과 주민등록번호를 요청한다. 이용자가 성명과 주민등록번호를 웹사이트에 전송하면, 웹사이트는 이를 실명확인 서비스를 제공하는 신용평가회사에 전달한다. 신용평가회사는 실명확인 데이터베이스에 전달받은 성명과 주민등록번호가 있는지 조회를 한다. 조회 결과에 따라 'YES' 또는 'NO'의 결과 값만을 웹사이트에 전송한다. 웹사이트는 이 결과 값에 따라 회원가입절차를 진행한다. 하지만, 실명확인 서비스를 통한 웹사이트 회원가입 절차는 다른 사람의 성명과 주민등록번호를 이용하여 회원가입을 할 수 있는 문제점이 있다. 주민등록법 제37조제8항에 따라 다른 사람의 주민등록번호를 도용한 경우에 3년 이하의 징역 또는 1천만원 이하의 벌금을 부과할 수 있으나 인터넷 웹사이트 회원가입 등에 명의 도용은 줄어들지 않고 있는 실정이다. 인터넷을 통해 노출된 주민등록번호로 실명확인 서비스를 이용하는 경우에는 주민등록번호 소유자의 본인여부를 확인할 수 있는 인증방법이 존재하지 않기 때문에 이와 같은 문제는 지속적으로 발생할 수밖에 없다.



〔그림 2〕 실명확인 서비스를 이용한 웹사이트 회원가입 절차

Ⅲ. 개선된 인터넷 상의 본인확인 방법

국내 대형 웹사이트의 경우 주민등록번호 오류검증 번호 검증 방법 및 실명확인 서비스를 통한 회원가입의 문제점을 인식하고 주민등록번호 소유자의 본인확인을 강화하는 방식을 도입하여 운영하고 있다. 공인인증서를 활용한 전자서명, 휴대폰SMS 발송번호 및 소유자 주민번호 확인, 신용카드정보 및 금융계좌정보 및 소유자 주민 주민번호 확인 인증 방식 등이 현재 인터넷 웹사이트들이 적용하고 있는 개선된 본인확인 방법이다.

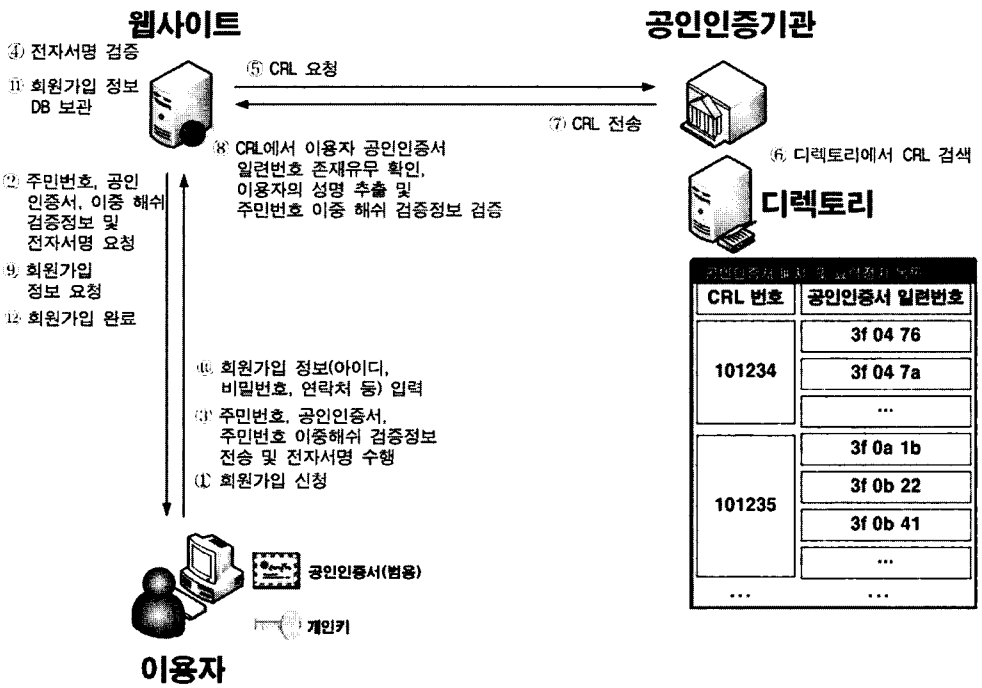
3.1. 공인인증서를 활용한 전자서명 인증 방법

공인인증서를 활용한 전자서명 인증 방법은 공개키 암호기술을 활용한 방법이다. 이용자는 공인인증기관 또는 등록대행기관을 방문하여 신원확인을 하고, 자신이 생성한 공개키와 개인키 쌍을 이용하여 공개키에 대응하는 개인키로 전자서명을 수행하여 공인인증서를 발급 받는다. 공인인증기관은 이용자가 신원확인 시에 제출한 주민등록번호를 이용자만이 알고 있는 비밀정보와 함께 이중 해쉬하여 공인인증서 안에 삽입하여 발급한다.[2]

웹사이트는 이용자 공인인증서의 공개키에 대응하는 개인키로 전자서명한 값을 공개키로 검증하여 본인확인을 수행하게 된다. 이 때 검증 결과에 따라 결과에 따라 회원가입을 위해 아이디, 비밀번호, 연락처 등의 정보를 요청한 후 회원가입을 완료하게 된다. 이외에 부가적으로 공인인증서 안에 이중 해쉬된 주민등록번호와 비밀정보의 값을 생성할 수 있는 값(주민등록번호, 비밀정보)을 알고 있음을 추가적으로 확인하여 본인확인의 정확성을 높이는 방법을 적용하기도 한다. [그림 3]은 공인인증서를 활용한 전자서명 인증 방법에 따른 웹사이트 회원가입 절차이다.

전자서명 인증 방법은 공개키 암호 기술을 이용하여 본인확인을 수행하기 때문에 안전성 측면에서는 다른 어떤 방식보다 안전하다. 하지만, 공인인증서를 웹사이트 회원가입 절차에 적용하기 위해서는 이용자의 공인인증서가 범용 공인인증서인 경우에만 가능하다. 현재 국내 공인인증서 이용자 수는 '08년 5월말 기준으로 약 1821만명이고[2], 이 중에서 인터넷 웹사이트에서 본인확인 용도로 사용할 수 있는 범용 공인인증서를 발급 받은 이용자 수는 200만명이 되지 않아 범용적으로 사

2) 한국경제신문 7월 30일 "사이버보안위협 이렇게 막으세요" 신문기사 참조



〔그림 3〕 공인인증서 전자서명 인증 방법을 이용한 웹사이트 회원가입 절차

용하는데 있어 제한적이다. 또한, 공인인증서 전자서명 인증 툴킷을 인터넷 웹사이트의 서버에 설치하는 비용과 이용자가 1년마다 범용 공인인증서를 갱신해야 하는 비용 부담의 문제를 갖고 있다.

3.2. 휴대폰SMS 발송번호 인증 방법

최근 인터넷을 통한 명의도용의 문제가 증가하고 있어 웹사이트는 이용자들이 보편적으로 갖고 있는 휴대폰을 이용한 본인확인을 수행하고 있다. 2008년 6월말 현재 국내 휴대폰 이용자 수는 약 4498만명[3]이다.

휴대폰SMS 발송번호 인증 방법은 이용자가 휴대폰 개통 시에 이동통신사에 제공한 명의자의 주민등록번호와 휴대폰 소유자가 갖고 있는 휴대폰으로 SMS 발송번호를 전송하고 이를 이용자에게 다시 입력하도록 하여 본인확인을 수행하고 있다.[3] [그림 4]은 휴대폰SMS 발송번호 인증 방법에 따른 회원가입 절차를 도식화 한 것이다.

휴대폰SMS 발송번호 인증 방법은 개선된 본인확인 방법 중 이용자 수가 가장 많다는 장점을 갖고 있다. 하지만, 인터넷을 통한 휴대폰 개통 시에 다른 사람의 신분증을 팩스로 이동통신사 대리점에 전송하여 개통하는 대포폰의 문제로 인해 본인확인의 신뢰도가 떨어지는 문제점을 갖고 있다. 또한, 웹사이트가 휴대폰SMS 발송 및 이동통신사에서 인증 결과에 대한 비용을 발송 및 인증 건수에 따라 부담해야하는 문제도 있으며 개선된 본인확인 방법 중 비용 부담이 제일 크다.

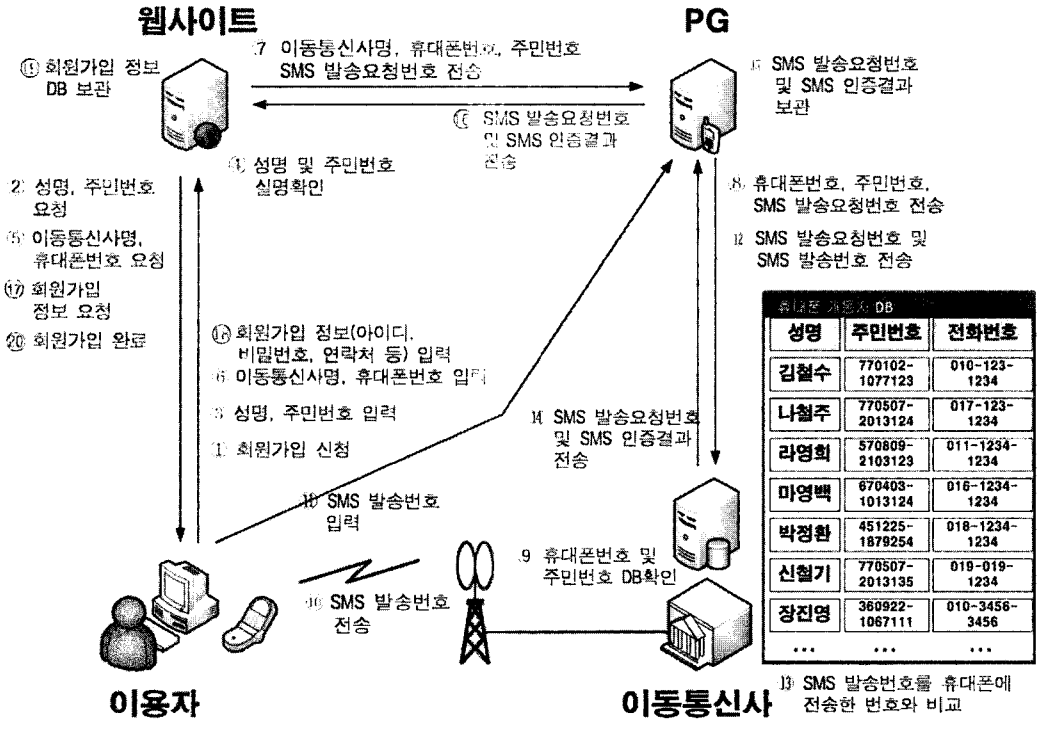
3.3. 신용카드정보 인증 방법

'08년 3월말까지 국내에 발급된 신용카드의 수는 약 9067만장이며[4], 국내 경제인구(2411만명)[5] 한 사람당 약 3.76장의 신용카드를 보유하고 있는 것으로 알려졌다. 신용카드는 신용카드 발급 후 신용카드 수령 시 이용자의 주민등록증, 운전면허증 등을 확인한 이후에 이용자에게 배포된다. 휴대폰 다음으로 본인확인 수단을 갖는 이용자 수가 많아 온라인 본인확인 방법으로 신용카드정보 인증 방법도 사용되고 있다.

3) 방송통신위원회 홈페이지 자료마당-통계자료-정보통신 일반통계 "유·무선 가입자 통계 현황(6월)" 참조

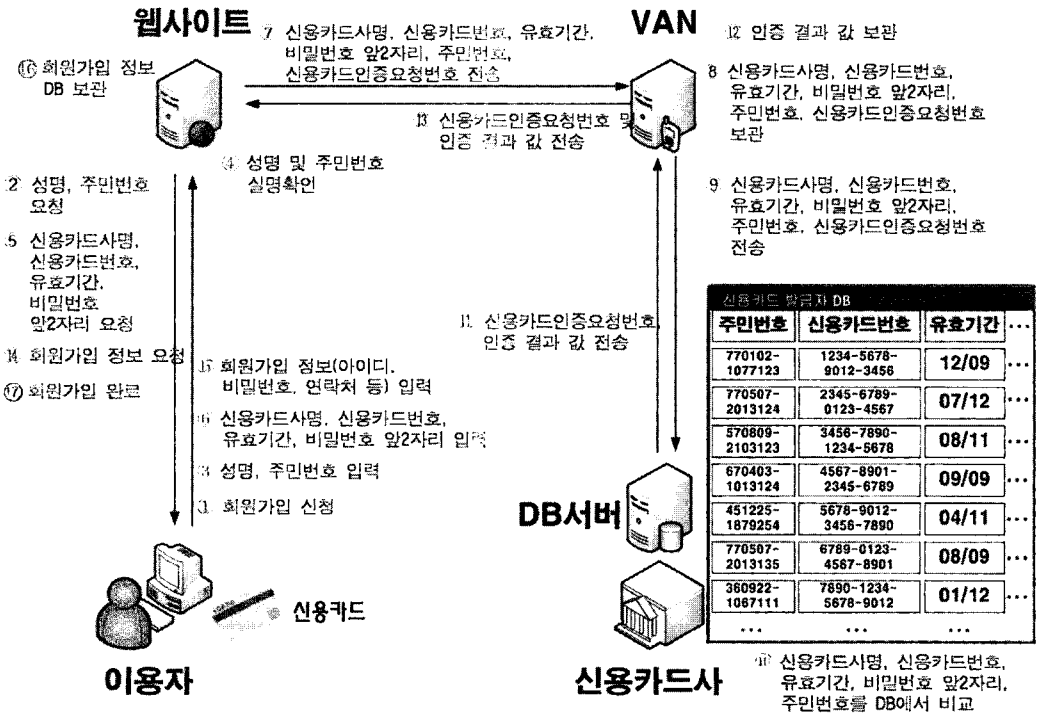
4) 금융감독원 "2008년 1/4분기 신용카드사 경영실적" 보도자료 참조

5) 통계청 국가 통계 포털 "고용·노동·임금 > 고용 > 경제활동인구총괄" 자료 참조



성명	주민번호	전화번호
김철수	770102-1077123	010-123-1234
나철주	770507-2013124	017-123-1234
라영희	570809-2103123	011-1234-1234
마영백	670403-1013124	016-1234-1234
박정환	451225-1879254	018-1234-1234
신철기	770507-2013135	019-019-1234
장진영	360922-1067111	010-3456-3456
...	...	...

〔그림 4〕 휴대폰SMS 발송번호 인증 방법을 이용한 웹사이트 회원가입 절차



주민번호	신용카드번호	유효기간
770102-1077123	1234-5678-9012-3456	12/09
770507-2013124	2345-6789-0123-4567	07/12
570809-2103123	3456-7890-1234-5678	08/11
670403-1013124	4567-8901-2345-6789	09/09
451225-1879254	5678-9012-3456-7890	04/11
770507-2013135	6789-0123-4567-8901	08/09
360922-1067111	7890-1234-5678-9012	01/12
...	...	...

〔그림 5〕 신용카드정보 인증 방법을 이용한 웹사이트 회원가입 절차

신용카드정보 인증 방법은 본인확인을 위해 신용카드번호 16자리, 신용카드 유효기간 및 이용자가 신용카드사에 등록한 비밀번호 앞 2자리를 확인하여 본인확인을 진행하고 있다.[4] [그림 5]는 신용카드정보 인증 방법에 따른 회원가입 절차이다.

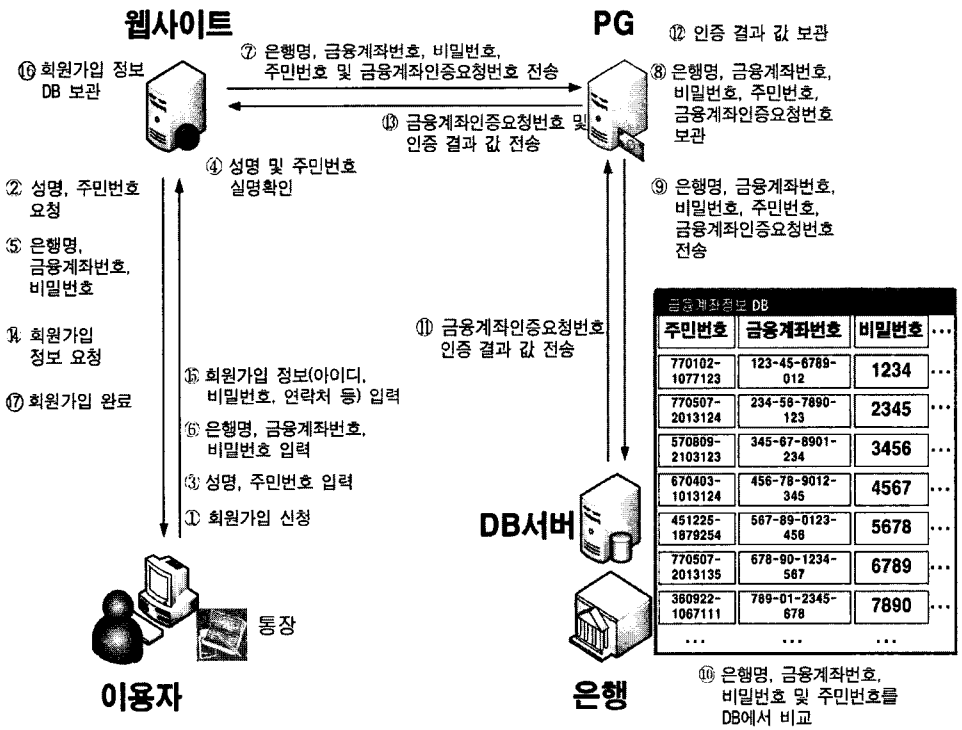
신용카드정보 인증 방법의 경우 신용카드 번호, 신용카드 유효기간 및 비밀번호 앞 2자리 등 민감한 정보를 활용하고 있어 한번 노출되면 그 피해가 다른 본인확인 방법에 비하여 엄청나다고 할 수 있다. 현재 VISA, MASTER 등의 카드의 경우 안전지불(ISP : Internet Secure Payment) 또는 안전결제 등의 인증방법을 사용하여 노출 위협을 최소화하고 있다. 신용카드정보를 활용한 본인확인의 경우 국내 경제활동인구로 제한되는 문제점을 갖고 있다.

3.4. 금융계좌정보 인증 방법

금융계좌정보 인증 방법은 다른 어떤 본인확인 방법에 비하여 본인확인 수단을 보유한 이용자가 가장 많다. 어린 유치원생에서부터 노인에 이르기까지 자신 명의의 통장을 하나 쯤은 갖고 있기 때문이다. 특히 초등학생에서부터 청소년들은 자신 명의의 통장 개설 시 자신의 주민등록번호로 계설되기 때문에 본인확인 방법으로 활용가치가 높다. '07년말 국내 은행수신 계좌수는 1억 6,746만개이다.[6] 휴대폰 및 신용카드의 경우 부모명의로 개통 또는 발급되고 있어 정확한 본인확인이 어려운 경우가 있다. 통장 계설의 경우 금융실명거래 및 비밀보장에 관한 법률에 따라 통장 소유자의 신원을 반드시 확인하도록 되어 있다.

금융계좌정보 인증 방법은 이용자가 계설한 통장의 은행명, 계좌번호 및 통장 비밀번호 4자리를 확인하여 본인확인을 진행하고 있다.[5] [그림 6]는 금융계좌정보 인증 방법에 따른 회원가입 절차를 도식화 한 것이다.

금융계좌정보 인증 방법의 경우 계좌번호 및 통장 비밀번호 4자리 등 예금인출에 민감한 정보를 활용하고 있어 보안카드정보, 공인인증서 개인키 등과 함께 노출되는 경우 그 피해는 이용자에게 직접적으로 영향을 미치는 문제점이 있다.



금융계좌정보 DB

주민번호	금융계좌번호	비밀번호	…
770102-1077123	123-45-6789-012	1234	…
770507-2013124	234-56-7890-123	2345	…
570809-2103123	345-67-8901-234	3456	…
670403-1013124	456-78-9012-345	4567	…
451225-1879254	567-89-0123-456	5678	…
770507-2013135	678-90-1234-567	6789	…
360922-1067111	789-01-2345-678	7890	…
…	…	…	

〔그림 6〕 금융계좌정보 인증 방법을 이용한 웹사이트 회원가입 절차

6) 한국은행 "2007년중 은행수신 동향" 보도자료 참고

Ⅳ. 금융보안 OTP를 이용한 본인확인 방안

2장 및 3장에서는 온라인 본인확인 방법들에 대해서 알아보고, 각각의 방법마다 갖고 있는 단점들을 소개하였다. 본 장에서는 금융보안 OTP를 활용한 본인확인 방안을 제안한다. 제안된 방안은 앞에서 나열한 단점들을 해결할 수 있어 그 활용가치가 다른 어떤 본인확인 방법보다 높다. 먼저, 금융보안 OTP의 발급과 관련한 내용을 알아보고, 제안하는 본인확인 방안에 대해 설명한다.

4.1. 금융보안 OTP

금융보안 OTP는 은행 또는 증권사 등에 계좌를 개설한 이용자에게 제공된다. 국내 OTP 통합인증센터에 등록된 OTP는 '08년 6월기준으로 331만개이고, 이중 발급된 건수는 185만개이다[7]. 현재 사용되고 있는 OTP 방식은 질의응답, 시간 동기화, 이벤트 동기화 및 조합 방식이 있다.[6,7]

질의응답 방식은 사용자가 서버가 제시한 질의 값을 OTP 생성 알고리즘에 입력하여 얻은 응답 값을 서버에 전송하는 방식이다. 시간 동기화 방식은 임의의 난수 값 대신에 시간을 OTP 생성 알고리즘의 입력값으로 사용하고, 사용자와 서버간에 동기화된 시간정보를 기준으로 OTP를 생성하는 방식이다. 이벤트 동기화 방식은 서버와 OTP 장치가 시간 정보를 대신에 동일한 카운트 값을 기준으로 OTP를 생성하는 방식이다. 조합 방식은 시간 동기화 방식과 이벤트 동기화 방식의 단점을 보완하기 위해 두 가지 방식을 조합하여 OTP를 생성하는 방식으로 입력 값으로 시간 값과 카운트 값을 모두 사용한다.

금융보안연구원은 통합 OTP인증센터에 등록된 하나의 금융보안 OTP를 이용하여 서로 다른 은행 또는 증권사 계좌에 사용할 수 있는 환경을 마련하여 서비스를 제공하고 있다.

4.2. 금융보안 OTP

본 절에서는 금융보안 OTP 토큰 또는 카드를 이용하여 웹사이트에서 본인확인하는 방안을 제안한다. 먼저 OTP 발급 단계에 대해 설명하고, 제안하는 본인확인 방안을 설명한다.

4.2.1. OTP 발급 과정

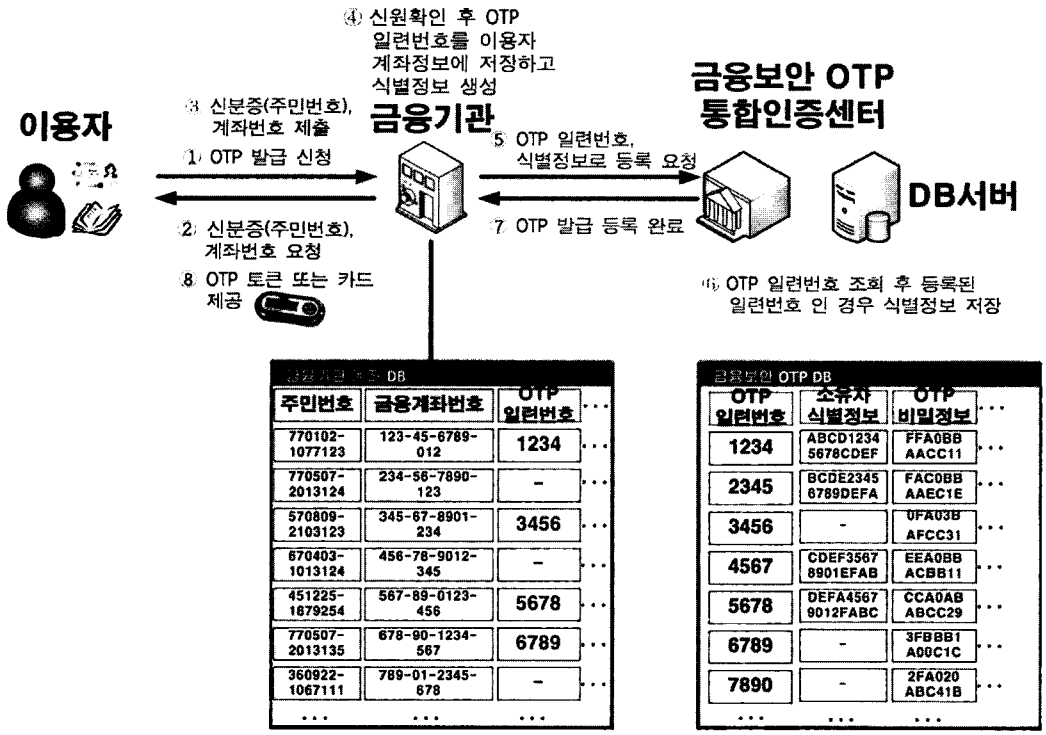
금융기관은 이용자에게 OTP 토큰 또는 카드를 발급하기 이전에 금융보안 OTP 통합인증센터에 OTP 일련번호와 검증번호생성을 위한 비밀키를 사전에 안전하게 등록한다. 이용자는 금융보안 OTP 토큰 또는 카드를 발급 받기 위하여 금융기관(은행 또는 증권사)를 방문한다. 금융기관은 이용자에 신원확인을 위한 계좌개설 정보(통장), 신분증 등을 요청한다. 이용자는 자신이 소지한 신분증과 통장을 금융기관에 제공하여 신원확인 절차를 거치게 된다. 금융기관은 신원이 확인된 이용자에게 금융보안 OTP 토큰 또는 카드를 이용자에게 제공하기 전에 해당 금융보안 OTP 토큰 또는 카드의 일련번호와 소유자 식별정보(예를 들면, 이용자 주민번호와 금융기관명의 해쉬값 등)을 금융보안 OTP 통합인증센터에 안전하게 전송한다. 금융보안 OTP 통합인증센터는 등록된 OTP 일련번호인지 확인한 후 등록된 OTP 일련번호이며 데이터베이스에 식별정보를 저장한다. 금융보안 OTP 통합인증센터는 OTP 발급 등록이 완료되었음을 금융기관에 알린다. 금융기관은 등록된 금융보안 OTP 토큰 또는 카드를 이용자에게 제공한다. [그림 7]은 이상의 절차를 도식화 한 것이다.

4.2.2. 본인확인 과정

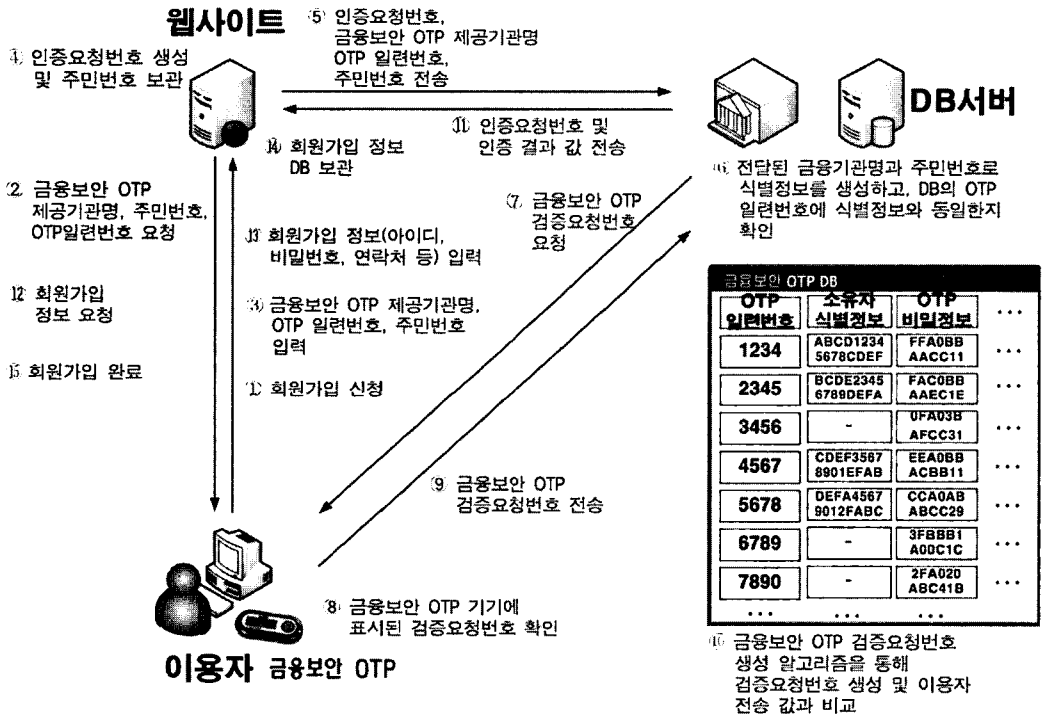
이용자는 자신이 가입하고자 하는 웹사이트에 접속하여 회원가입을 신청한다. 웹사이트는 이용자에게 본인확인을 요청하기 위해 팝업창을 띄어 본인확인을 위한 정보(금융보안 OTP 제공기관명, OTP 일련번호, 주민등록번호)를 요청한다. 이용자는 본인확인을 위한 정보를 팝업창에 입력한다. 이때 웹사이트는 본인확인을 위한 인증요청번호를 생성하여 주민등록번호와 함께 보관하고, 금융보안 통합 OTP센터에 인증요청번호, 금융보안 OTP 제공기관명, OTP 일련번호, 주민등록번호를 전송한다. 금융보안 통합 OTP센터는 전달받은 정보를 기반으로 등록된 이용자인지 확인하고 등록된 이용자인 경우에는 이용자에게 금융보안 OTP 토큰 또는 카드에 표시된 검증요청번호를 요청한다.

이용자는 자신이 소유한 금융보안 OTP 토큰 또는 카

7) 디지털데일리 2008년 6월 13일 "'잔치는 끝났다' OTP 업계, 수익성 급속 악화" 신문기사 참조



〔그림 7〕 금융보안 OTP 발급 과정



〔그림 8〕 금융보안 OTP를 이용한 웹사이트 회원가입 절차

드에 표시된 검증요청번호를 통합 OTP 인증센터로 전송한다. 금융보안 OTP 통합인증센터는 데이터베이스에 보관된 이용자의 금융보안 OTP 비밀정보를 활용하여 검증요청번호를 생성한다. 생성된 검증요청번호와 이용자로부터 전달받은 검증요청번호가 동일한지 확인하고 동일여부에 따라 'Yes'또는'No'라는 검증 결과 값을 인증요청번호와 함께 웹사이트에 전송한다. 웹사이트는 금융보안 OTP 통합인증센터로부터 받은 인증요청번호와 검증 결과 값의 'Yes' 또는 'No'에 따라 이용자의 회원가입 절차를 진행한다. [그림 8]은 금융보안 OTP를 활용한 온라인 본인확인 방안에 따른 회원가입 절차를 도식화 한 것이다.

V. 제안된 방안의 비교

본 장에서는 앞에서 알아본 인터넷 상의 본인확인 방법과 제안하는 금융보안 OTP를 이용한 본인확인 방안에 대하여 비교하여 알아본다. [표 1]은 비교한 대상 및 내용이다. 제안하는 방식은 공인인증서와 같이 그 소유자만이 금융보안 OTP 토큰 또는 카드를 OTP 제공기관으로부터 직접 신원확인 후 발급 받기 때문에 명의도용 위협이 매우 낮다. 또한 휴대폰의 경우 최근 인터넷을 통해 타인명의의 휴대폰을 쉽게 발급 받을 수 있으나, 금융보안 OTP는 휴대폰과 달리 개인의 자산이라는 개념이 높기 때문에 타인에게 대여하는 일은 없을 것으로 판단된다. 금융계좌정보 인증 방식은 민감한 계좌비밀번호를 제공해야 했지만, 제안하는 방식은 일회성 OTP 검증요청번호만이 제공되기 때문에 계좌비밀번호 노출 등의 문제를 해결할 수 있는 장점이 있다.

VI. 결 론

인터넷 서비스 제공분야가 뉴스 및 자료 검색에서 게임, 쇼핑, 여행 등 다양한 분야로 확대되면서 이용자에 대한 본인확인의 필요성에 대한 요구가 더욱 증가하고 있는 상황이다. 본 논문에서는 오프라인 대면확인을 통해 발급받은 금융보안 OTP 토큰 또는 카드를 이용하여 본인확인하는 방안을 제안하였다. 특히 민감한 정보 노출 위협을 갖고 있는 신용카드정보 및 금융계좌정보 인증방법에 비해 민감한 정보를 노출하지 않는 장점이 있다. 또한 금융보안 OTP가 모든 은행, 증권 등의 모든 이용자에게 배포되어 이용된다면 범용 공인인증서 이용자 약 200만명, 신용카드 발급건수 9067만장 보다 많은 보유자를 확보할 수 있고, 신용카드의 경우 경제인구로 제한되는 점이 있으나 금융보안 OTP는 금융계좌를 갖고 있으며 OTP를 발급 받은 모든 국민이 이용할 수 있

〔표 1〕 기존의 본인확인 방식과 제안한 방식의 비교

방안 / 구분	오류검증 번호	실명확인	공인 인증서	휴대폰 SMS	신용카드 정보	금융계좌 정보	제안방안
본인확인 방법	오류 검증번호	성명과 주민번호	전자서명 및 이중 해쉬 검증 값	SMS 발송번호 및 주민번호	신용카드정보 및 주민번호	금융계좌정보 및 주민번호	OTP 일련번호, 검증요청번호 및 주민번호
이용자 범위	4867만명 (2008년 6월 추계인구)	4867만명 (2008년 6월 추계인구)	범용 공인 인증서 발급건수 약 200만명 (2008년 6월)	휴대폰 소유자 4498만명 (2008년 6월)	신용카드 발급건수 9067만장 (2008년 3월)	금융계좌수 16746만개 (2007년 12월)	OTP 발급건수 185만개 (2008년 6월)
명의도용 방법	오류 검증번호 생성규칙	성명과 주민번호	개인키 및 주민번호	휴대폰 및 주민번호	신용카드번호, 비밀번호 2자리 및 주민번호	계좌번호, 비밀번호 및 주민번호	OTP 일련번호, 검증요청번호 및 주민번호
명의도용 가능성	매우 높음	높음	매우 낮음	보통	낮음	낮음	매우 낮음
민감한 정보	주민번호	주민번호	이중 해쉬 검증 값	주민번호	카드번호, 유효기간, 비밀번호 및 주민번호	계좌번호, 계좌비밀번호 및 주민번호	주민번호
웹사이트 도입비용	없음	실명확인 수수료 (건당 무료~50원)	공인인증 툴킷비용 (서버당 2~3천만원)	휴대폰SMS 인증수수료 (건당 20~50원)	신용카드정보 인증수수료 (건당 1~100원)	금융계좌정보 인증수수료 (건당 100~200원)	미정

기 때문에 온라인 본인확인의 새로운 분야로서 자리 잡을 수 있을 것이다. 은행 또는 증권사와 같이 금융보안 OTP를 제공하는 기관은 금융보안 OTP를 활용한 새로운 사업 분야 발굴로 사업적 가치가 높다고 할 수 있다.

최근 인터넷 상의 개인식별번호(i-PIN) 서비스의 경우 본인확인 수단으로 공인인증서, 휴대폰 SMS, 신용카드정보 등 제한된 정보를 활용하고 있어 전체 국민을 대상으로 서비스하는데 어려움이 있는 실정에서 새로운 본인확인수단으로서 도입된다면 금융보안 OTP는 활용가치가 높다고 할 수 있다[8].

제안하는 방식 자체만으로는 웹사이트 중복가입여부를 확인하기 위해서는 주민번호가 웹사이트에 제공되어야 하지만, 이를 개인식별번호(i-PIN) 서비스와 연계함으로서 i-PIN 서비스를 제공하는 본인확인기관에만 주민번호를 제공하고 웹사이트에서는 가상의 13자리 PIN 번호와 중복가입여부를 확인할 수 있는 중복가입확인정보를 제공하는 방식으로 웹사이트의 개인정보 수집을 제한할 수 있다[9]. 현재는 금융보안 OTP의 발급건수가 국내 총인구의 약 4%정도 밖에 안되지만 '08년 6월 기준 국내 개인 인터넷 이용자 약 4624만명[8] 수준까지 확대된다면 전국민 대상으로 온라인 본인확인 서비스를 제공할 수 있는 방식으로서 가치를 갖게 될 것이다.

참고 문헌

[1] 장종인, "개인정보시장에서 주민등록번호의 이용", 정보통신정책연구원, 정보통신정책 제17권 제18호 통권 379호, pp. 26-50, 2005.

[2] 한국정보보호진흥원, "식별번호를 이용한 본인확인 기술규격", 전자서명인증체계 기술규격, 2002.

[3] 강경석, 민상원, 심상범, "VM의 자동 변수 생성 방식 기반 모바일 지급결제 시스템", 한국정보과학회 논문지 제12권 제6호, pp. 367-378, 2006.

[4] 김인석, "전자금융과 정보보호에 관한 연구", 정보통신정책연구원, 우정정보 2006 가을, pp. 39-58, 2006.

[5] 이원철, 이석래, 이재일, 김인석, "전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구", 한국정보보호학회지, 제15권 제4호, pp. 44-49, 2005.

[6] 서승현, 강우진, "OTP 기술현황 및 국내 금융권 OTP 도입사례", 한국정보보호학회지, 제17권 제3호, pp. 18-25, 2007.

[7] 강수영, 이임영, "OTP를 활용한 UICC(Universal IC Card) 기반의 인증 메커니즘에 관한 연구", 한국정보보호학회 논문지, 제18권 제2호, pp. 21-31, 2008.

[8] TTA, "i-PIN 서비스 프레임워크", 정보통신단체표준, TTAS-KO-12-0054, 2007.

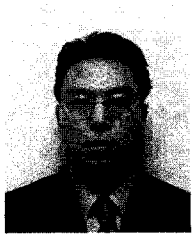
[9] TTA, "본인확인서비스 중복가입확인정보", 정보통신단체표준, TTAS-KO-12-0038, 2006.

8) 한국은행 "2008년 2/4분기 국내 인터넷뱅킹서비스 이용현황" 보도자료 참조

〈著者紹介〉

정 찬 주 (Chan-Joo Chung)
특별회원

1993년~1999년 : 강남대학교 전자계산학과 학사
1999년~2001년 : 성균관대학교 전기전자컴퓨터공학과 석사
2003년~2005년 : 성균관대학교 컴퓨터공학과 박사 수료
2000년 12월~현재 : 한국정보보호진흥원 선임연구원
2005년 3월~현재 : TTA 정보보호 기술위원회(TC5) 개인정보보호 및 ID관리 프로젝트 그룹(PG502) 위원
<관심분야> 암호이론, PKI, 개인정보보호



김 승 주 (Seung-Joo Kim)
종신회원

1994년~1999년 : 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년 : 한국정보보호진흥원 팀장
2004년~현재 : 성균관대학교 정보통신공학부 부교수
2004년 1월~현재 : 한국정보보호학회 이사
2005년 6월~2006년 6월 : 교육인적자원부 유해정보차단 자문위원
2006년 : Marquis Who's Who in Asia (2007:1st Edition) 인명사전 등재
2006년 3월 : 국가정보원장 국가사이버안전업무 유공자 표창
2007년 : Marquis Who's Who in the World (2008:25th Edition) 인명사전 등재
2007년 5월~현재 : 대검찰청 디지털수사자문위원
2007년 12월~현재 : 전자정부서비스보안위원회 사이버침해사고대응 실무위원
2008년 1월~현재 : 기술보증기금 외부 자문위원
2008년 2월~현재 : 수원시 지역정보화 촉진 협의회 위원
2008년 4월~현재 : 한국은행 금융정보화추진분과위원회 자문위원
2008년 4월~현재 : 법무부 법률서비스산업 경쟁력강화위원회 위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dong-Ho 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
2002년~현재 : 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
2007년~현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장
<관심분야> 암호이론, 정보이론, 정보보호