

안전하고 신뢰성있는 전자정부 구축을 위한 보안 요구사항

김 명 은*, 오 승 희*, 정 연 서*, 서 동 일*

* 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀

요 약

정보화 시대가 도래함에 따라 세계 각국의 많은 나라들이 전자정부 구현에 많은 관심을 가지고 있으며, 이미 몇몇 선도 국가들은 다양한 민원서비스 및 행정서비스를 인터넷에서 국민들에게 편리하게 제공하고 있다. 인터넷을 통한 전자정부 서비스는 보다 많은 편리성을 제공하는 반면에 중요한 개인정보나 국가기밀이 누출될 수 있는 보안 취약점을 가지고 있기 때문에 많은 국가들이 개인정보를 보호하기 위해 보안 인프라를 구축하고 있다. 본 논문에서는 여러 선도국가들의 전자정부 구축동향을 알아보고 안전하고 신뢰성 있는 전자정부 서비스를 제공하기 위해 필요한 보안 고려사항을 제시한다.

The Security Requirement for Implementation of Secure and Reliable e-Government

Kim, Myungeun* Oh, Seunghee*, Jeong, Younseo*, Seo, Dongil*

ABSTRACT

According as information society has been raised, many countries of the world have taken a lot of interests in e-government implementation. The several guidance countries already have offered people various administrative service and popular enmity service in the Internet conveniently. People can use e-government service more conveniently by the Internet, but important personal information or state secret can be leaked in the Internet. Because of these security vulnerabilities, a lot of countries are constructing security infrastructure that can protect personal information. In this paper, we examine e-government construction trends of the several guidance countries, and propose security considerations to provide safe and reliable e-government service.

1. 서 론

오늘날 정보사회가 대두됨에 따라 세계 여러 나라들은 전자정부의 추진이 필요하다는 점에서

공통적으로 인식을 같이하고, 각국이 처한 상황에 따라 다양하게 전자정부 사업들을 추진하고 있다. 이제 전자정부의 추진은 국가의 경쟁력 향상을 위한 필수 불가결한 선택으로 받아들여지고 있으며, 이러한 국가정보화는 정보사회의 출

현에 따른 21세기의 환경변화에 있어서 국가가 필연적으로 대응하지 않을 수 없는 부분으로 인식하고 있다. 특히 정보화를 선도하는 국가가 앞으로 국제사회의 질서를 주도하게 될 것이라는 주장이 광범위하게 받아들여지고 있는 점을 고려할 때 각국의 정부가 추진하고자 하는 전자정부의 구현은 궁극적으로 국가의 발전과 직결되고 있다. 이러한 기본적인 인식 가운데 각국에서 제시하고 있는 전자정부의 비전은 정부서비스의 제공에 가장 많은 비중을 두고 있으며, 이에 따라 안전하고 편리한 행정 서비스 및 민원 서비스를 제공하기 위하여 개인정보 및 중요 국가정보를 보호할 수 있는 보안 대책 마련이 주요 이슈로 떠오르고 있다.

본 논문에서는 여러 선도국가들의 전자정부 구축동향 및 보안동향을 분석하여 안전하고 신뢰성 있는 전자정부 서비스를 제공하기 위해 요구되는 보안 고려사항을 제시한다.

2. 국내외 전자정부 구축동향

전자정부는 구축형태에 따라 시작단계(Emerging), 발전단계(Enhanced), 상호작용단계(Interactive), 거래단계(Transaction), 유기적결합단계(Seamless)의 5개의 단계로 나눌 수 있다[1]. 1단계인 시작단계는 전자정부 웹사이트를 구축하기 시작하는 단계로 앙골라, 부룬디, 미얀마 등의 국가가 이에 속하며, 2단계인 발전단계는 사용자에게 정보를 전달하는 일방향 정보 제공 단계로 알제리, 카메룬, 모나코 등의 국가가 이에 속한다[3]. 3단계인 상호 작용 단계는 사용자와 정보를 주고받을 수 있는 양방향 정보제공 단계로 러시아, 스웨덴, 일본, 중국 등이 이에 속하며, 4단계인 거래단계는 온라인으로 민원처리가 가능한 단계로 미국, 영국, 싱가포르, 한국 등이 이에 속한다[3]. 마지막으로 최상위 단계인 유기적 결합단계는 통합 온라인 서비스를 제공하는 단계로 모든 서비스가 유기적으로 연동되

어 중단없이(Seamless) 제공되는 단계를 의미한다. 현재까지 유기적 결합단계에 속하는 서비스를 제공하는 나라는 없으나, 거래단계에 있는 많은 선도국가들이 점차 유기적 결합단계로 발전할 것으로 보인다. 다음 절에서는 각 나라별 전자정부 구축동향에 대하여 알아본다.

2.1 미국

미국은 1993년 클린턴 행정부 출범이후부터 행정혁신과 연계하여 전자정부 계획을 수립하여 추진하였으며, 1993년 9월 클린턴 행정부가 발표한 NII(National Information Infrastructure)정책 및 NPR(National Performance Review)정책으로 구체화되었다[6]. 1993년에 NPR이 발표한 최초의 전자정부 계획안인 '정보기술을 통한 리엔지니어링'에서는 전자정부 구현 및 지원체계 구축을 위한 13개 사업과 49개 세부 실행계획을 제시하였다. 이후 GITS(Government Information Technology Services)를 통해 지속적으로 추진해왔으며, 2000년 6월에 클린턴 대통령은 2000년 말까지 정부통합 포털사이트를 통하여 약 2만개의 연방정부 웹사이트의 모든 온라인 자료를 검색 가능하도록 하겠다는 대규모 전자정부 추진 계획을 발표하면서, 2000년 9월 22일에 27,000개 연방정부 웹사이트를 검색할 수 있는 정부차원의 포털사이트(www.firstgov.gov)를 구축하였다[2]. 2001년 새롭게 출범한 부시정부는 전자정부 구현의지를 구체화하기 위해 2002년 예산안을 통하여 총 1억 달러를 투입함으로써 전자정부를 조기에 구현하려는 의지를 표명하였으며, 2001년 7월에 전자정부기금 설치, 전자정부 전담팀의 신설 및 운영 등을 통해 가시화하였다. 2002년말 미국은 전자정부 구축에서 상위국으로 평가되고 있으며, 전자정부 활용도에 있어서도 상위국으로 평가되고 있다[3]. 또한 정부통합 포털사이트를 통해 전자적 거래가 가능한 인터넷 행정서비스를 제공하고 있다.

2.2 일본

IT혁명에 대응하기 위해 일본정부는 1995년 2월에 '고도 정보통신 사회추진을 향한 기본방침'을 책정하여 추진하고 1998년 11월에 정부고도 정보통신사회추진본부가 새로운 상황과 정책과제를 포함해서 95년에 수립한 기본방침을 개정하여 전자상거래의 보급, 전자정부의 실현, 인재육성과 정보리터러시의 향상, 정보통신 인프라 정비 등 네가지를 당면목표로 삼고 추진해왔다. 이후 일본은 IT 입국 구축을 목표로 한 시책을 종합적으로 추진하기 위해 2000년 7월 내각에 정보통신기술(IT) 전략본부를 설치하였고 2001년 1월 22일에 개최한 제1회 전략본부회의에서 'IT 기본전략'에 기초한 IT 국가전략으로서의 전자정부를 구현하기 위한 'e-Japan 전략'을 결정했다[11]. 또한 2003년을 전자정부 구축의 완료시점으로 명시하고 정부예산으로 각 부처에서 전자정부를 위한 사업을 집행하였으며, 2002년 7월에 정부포털사이트(e-gov.go.jp)를 구축하여 전 성청 홈페이지 정보를 연계하고 개인/기업의 행정절차 등의 정보를 제공하고 있다.

2.3 영국

영국에서 범정부적으로 전자수단에 의한 정부서비스의 공급을 정부의 핵심전략으로 추진한 청사진이 제시된 것은 1996년 당시 공공서비스처 장관인 Roger Freeman에 의해 발표된 녹서(Green Paper : Government Direct / A Prospectus for the Electronic Delivery of Government Services)에서 비롯한다. 이전까지 전자적인 정부서비스의 제공이라는 용어를 사용하던 영국이 이 녹서에서부터 전자정부의 개념을 제시하고 있으며, 전자적 공공서비스 제공방식과 관련하여 범공공기관 수준의 전자정부 구현 정책 및 지침을 마련하고, 이에 대한 공통적 집행을 도모하고자 하였다. 영국의 전자정부추진 계획에 있어 특히 눈여겨 볼 특징으로는 중앙과

지방정부간의 이음매없는(seamless) 행정을 추구한다는 점을 들 수 있다. 영국은 이음매없는 행정의 구현을 위해서, 중앙정부 기관들의 전산망과 지방정부의 전산망을 모두 정부안전인트라넷(government secure intranet)에 연결하여 정부기관간의 의사소통이 원활하게 이루어질 수 있도록 계획하고 있다. 토니 블레어 총리는 당초에 2008년으로 계획된 전자정부의 구현을 2005년으로 앞당기겠다고 발표하였고, 국무장관 Ian McCartney는 2000년 4월 3일 'E-Government : A Strategic Framework for Public Services in the Information Age'를 통해 구체적인 실행계획을 발표하였으며, 2000년 여름까지 정부단일의 포털사이트를 구축하여 중앙정부와 지방정부의 각종 서비스를 제공하겠다는 내용을 포함하였다. 이후 2001년 2월에 정부 포털사이트(www.Ukonline.gov.uk)를 구축하였으며, 영국정부는 게이트웨이(government gateway)를 사이에 두고 공공서비스 포털사이트와 정부안전인트라넷을 연결하였다[2]. 현재 온라인으로 처리가능한 민원비율에 있어서는 2002년말 357개의 온라인 서비스를 제공하고 있으며, 온라인 민원 비율에 있어서는 약 63%를 기록하여 선두국가로 평가되었으나, 전자정부 이용률면에서는 전세계 평균인 30%를 밑도는 13%를 기록하여 하위국 국가로 평가되었다[3].

2.4 싱가포르

1981년에 설립되어 싱가포르의 정보화를 이끌어오던 NCB(National Computerization Board)가 1999년 12월 1일에 TAS(Telecommunication Authority of Singapore)와 통합되어 IDA(Inforcomm Development Authority of Singapore)가 되었고, 현재 싱가포르는 IDA를 중심으로 전자정부 구현계획을 수립하고 민간부문과 함께 정보기술을 통한 대민 행정서비스에 나서고 있다. 싱가포르는 정보화를 1980년대 중반부터 본격적으로 추진해왔으며, 1991년에

제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

IT2000, 1996년에 Singapore One, 그리고 최근의 E-Citizen에 이르기까지 구체적인 계획을 세워 정책을 추진해 오고 있다. 싱가포르의 전자정부 구현에 있어서 선두를 달리고 있는 국가이며 세계최초의 범정부 포털 사이트를 구축한 나라이다[2]. 현재 E-Citizen Centre에서 제공되는 서비스로는 기업부문의 특허신청에서부터 국방부문과 특히 초중고 학교 지원 등을 포함하는 교육부문, 구직과 관련되는 취업관련 부문, 결혼과 출산신고를 포함하는 가정생활, 의료서비스를 지원하는 건강부문, 주거문제를 해결해주는 주택부문, 경찰업무를 포함하는 법률지원 부문 및 해외 여행 및 자동차 운행을 포함하는 교통부문 등이 있다.

2.5 한국

한국은 1차 정보화촉진기본계획에 수용하여 전자정부 계획을 추진하다가 2001년 5월에 전자정부특별위원회에서 '세계 인류국가 도약을 위한 전자정부 구현전략'을 수립하여 범정부차원의 전자정부 정책을 추진하였다. '세계 인류국가 도약을 위한 전자정부 구현전략'은 1998년에 행정부에서 발표한 전자정부종합실천계획을 발전시킨 형태로 정보화를 통한 민원서비스 혁신, 4대 사회보장정보연계시스템 구축사업, 국가종합 전자조달시스템사업, 홈텍스서비스시스템 구축사업, 국가재정정보시스템사업, 시/군/구 행정종합 정보화사업, 교육행정정보시스템구축사업, 전자인사관리시스템사업, 전자결재 및 전자문서유통 활성화 사업, 전자서명 및 행정전자서명 사업, 범정부 통합전산환경구축사업 등의 11개 과제를 포함하고 있다[2]. 이후 2002년 11월 1일에 대한민국의 전자정부와 함께 정부포털사이트(www.gov.go.kr)가 공식 출범하였다. 참여정부가 출범한 뒤 정부혁신/지방분권위원회내에 전자정부 전문위를 설치하여 전자정부를 추진하고 있으며, '세계 최고 수준의 열린 전자정부 구현'이라는 비전아래 10대 아젠다, 31개 과제를 선정

하고, 2단계 전자정부 추진전략을 수립하였다[10]. 1단계인 기반정비단계에서는 2005년까지 행정내부업무 정비 및 공통기반 구축과 선별적 대 국민/기업 서비스를 혁신하는 것을 목표로 하고 있으며, 2단계인 서비스 고도화 단계에서는 2007년까지 행정내부업무 정보화와 고도화, 대국민/기업 통합서비스 확대를 목표로 하고 있다. 현재 정부포털 사이트에서는 4000여종의 민원정보 및 각 기관간 정보활용을 지원하고 있으며, 관련 기관의 홈페이지에 대한 소개를 통해 보다 편리한 민원서비스를 제공하고 있다.

3. 국외 전자정부 보안동향

세계 각국에서 국가 경쟁력을 높이기 위해 국가 정보화 및 전자정부 구축에 관심이 증대됨과 동시에 이에 따르는 보안문제에 대한 관심 또한 급증하고 있다. 전자정부 구축을 통해 편리한 민원/행정서비스가 인터넷을 통해 제공된다는 것은 개인정보나 중요 국가기밀이 인터넷상에서 노출될 수 있다는 것을 의미하기도 한다[5]. 이와 같은 문제점을 해결하기 위해 미국을 포함한 여러 나라에서 강력한 보안대책을 수립하고, 보안 인프라를 구축하여 안전한 전자정부를 구축하고자 노력하고 있다. 각 나라별로 안전한 전자정부 서비스를 제공하기 위해 구축하고 있는 보안 인프라 구축 사례는 다음과 같다.

첫째, 미국은 공개키 기반구조 구축을 추진하기 위해 1996년 FPKI 운영위원회를 설립하였고, 1998년 10월 GPEA(The Government Paperwork Elimination Act)를 통해 모든 연방기관들이 전자서명을 활용하여 표준화된 형태의 온라인 거래를 추진하도록 하였다[8]. 또한 1999년 연방총무처는 민간기업들이 연방기관을 대신하여 디지털 인증서비스를 제공하도록 하였으며, 2000년 5월부터 민간기업들이 인증서를 발급하기 시작했다. 이후 2000년 6월 전자서명법을 제

기로 전자문서는 종이문서와 동등한 법적지위를 갖게 되었다[6].

둘째, 일본은 2001년부터 전자정부의 개인정보 보호에 대한 연구 및 법제화를 추진하고 있으며, 2002년 8월 5일부터 주민대장의 내용을 IC카드에 내장하는 방법을 사용하여 개인정보노출을 방지하였다[9]. 또한 전자정부 주요 시스템을 전용망으로 구성하여 내/외부 침입으로부터 보호하고 있으며, 방화벽 및 침입탐지시스템 등의 보안장비를 설치하여 주요시스템을 보호하고, 상호인증 및 데이터 암호화를 통해 통신보호를 제공하고 있다[4].

셋째, 영국은 정부와의 전자거래를 Government Gateway라는 단일 통로를 통해 제공하고 있으며, 단일의 인증서를 통해 정부와의 다양한 전자거래를 수행하고 있다. 또한 플랫폼에 제한받지 않는 XML양식을 사용하였으며, 신원확인을 위해 ID와 패스워드의 조합, 디지털인증의 두 가지 방안을 제시하고 있다[2].

넷째, 싱가포르는 1948년부터 전 국민에게 배포되었던 개인별 고유의 ID카드를 이용해 e-Government를 사용할 수 있도록 하였으며, 접속시 ID카드와 PIN코드로 신원을 확인할 수 있도록 하였다[2]. 또한 시스템의 저근에 대한 인증과 이주의 암호기술을 도입하고 복수의 방화벽을 사용하여 24시간 365일 감시체제를 구축하였다.

4. 안전한 신뢰성있는 전자정부 구축을 위한 보안 고려사항

본 장에서는 안전하고 신뢰성있는 전자정부 서비스를 제공하기 위해 전자정부의 기반구조를 보호하기 위해 시스템상에서 고려해야 할 보안사항과 네트워크상에서 고려해야 할 보안사항을 살펴보고, 더불어 전자정부 서비스를 보호하기 위해 필요한 보안 고려사항을 살펴본다.

4.1 시스템상에서의 보안 고려사항

전자정부를 구성하고 있는 주요 시스템을 보호하기 위해서는 다음과 같은 보안 고려사항들이 존재한다. 첫째, 전자정부를 구성하고 있는 시스템을 물리적으로 안전하게 보호하기 위해 허가되지 않은 출입자에 대한 강화된 출입통제, 재난 대비를 위한 자가발전 시스템 구비, 스마트카드나 생체정보를 이용한 접근통제 등이 요구된다. 둘째, 주요 데이터를 보호하기 위한 방안으로 정기적인 시스템 로그저장 및 데이터 백업이 필요하고, 재난시 시스템 파괴를 대비하여 원격 자료 백업시스템을 설치하는 것이 요구된다. 셋째, 다변화되고 지능화되는 사이버 공격으로부터 주요 시스템을 보호하기 위해 스팸메일 차단 시스템, 항 바이러스 프로그램, 호스트 방화벽과 같은 보안 장비의 설치 및 지속적인 관리 및 업데이트가 요구된다.

4.2 네트워크상에서의 보안 고려사항

전자정부 서비스를 제공하는 주요 시스템간의 안전한 통신을 위해서 요구되는 보안 고려사항은 다음과 같다. 첫째, 전자정부의 기반이 되는 주요 시스템과 시스템이 설치된 네트워크는 외부 네트워크와 물리적/논리적으로 분리되어 운영되어야 한다. 즉, 다양한 해킹과 불법적인 정보 유출을 원천적으로 차단하기 위해 전자정부 서비스를 위한 전용망 구축이 필요하고, 외부 네트워크와의 접속점에서는 보다 강화된 인증 및 접근제어를 통해 내부 네트워크의 자체 보안 및 액세스 제어정책수립이 요구된다. 둘째, 외부의 공격 및 침입으로부터 지속적인(Seamless) 전자정부 서비스를 제공하기 위한 네트워크 생존성 기술이 제공되어야 한다. 네트워크 생존성을 보장하기 위해서는 네트워크 장애 및 외부로부터의 공격으로 발생하는 서비스 중단 방지를 위해 이중망(Dual Network) 구조로 주요 네트워크를 설계하는 것이 필요하며, 과다

한 트래픽 유입으로 인해 발생하는 네트워크 장애를 예방하기 위한 유해트래픽 폭주 방지기술 및 고속의 침입탐지/차단 기술이 요구된다. 또한 망 자원을 고갈시켜서 정상적인 네트워크 서비스를 마비시키는 바이러스와 웜을 차단할 수 있는 네트워크 보안장비의 설치와 공격이 진행되는 동안에도 신속하게 피해 시스템을 복구할 수 있는 기술이 요구된다. 셋째, 모든 정부기관에 대한 안전한 접속기능 구현이 요구된다. 안전한 접속기능 구현을 위해 모든 정부기관간의 통신은 VPN을 도입하여 상호인증, 데이터의 무결성 및 기밀성을 보장하고 데이터의 중요도에 따라 암호화 방식을 선택적으로 적용할 수 있어야 한다. 또한 추후 IPv6망으로의 진화를 고려하여 VPN과 유무선 단말과의 통신을 위한 방안도 고려해야 한다. 넷째, 잠재적인 네트워크 보안 위협에 대한 취약점을 분석하여 체계적인 침입대응을 제공하기 위해 망 전체에 대한 통합 보안관리가 필요하다[4]. 즉, 주요 전자정부 서비스 제공시스템에 접근하는 모든 트래픽에 대하여 24*7*365 모니터링이 필요하며, 다양하고 지능화된 침입에 대해 전역적인 네트워크 모니터링을 통하여 즉각적이고 능동적으로 대응할 수 있는 방안이 필요하다. 또한 네트워크 및 보안 장비의 취약점을 분석하여 주기적인 보안패치를 수행해야 한다. 이외에도 유비쿼터스 시대로의 진화를 고려한 유무선 통합망 환경에서의 전자정부 환경을 위한 정보보호 방안 수립이 요구되며, Ipv6로의 진화를 고려한 네트워크 보안 방안도 고려되어야 한다.

4.3 서비스상에서의 보안 고려사항

안전한 전자정부 서비스 제공을 위해 고려해야 할 서비스 측면의 보안 고려사항은 인증, 암호화, 문서보안 그리고 웹서비스 보안 측면으로 나누어 볼 수 있다. 첫째, 인증 측면에서 볼 때 유무선 통합환경으로의 전이를 고려하여 경량화된 키교환 방식 도입 및 무선단말기 인증이 요

구되며, 다양한 사용자로부터 주요시스템을 보호하기 위해 PMI(Privilege Management Infrastructure) 기반의 서비스 방식이 요구된다. 또한 다양한 전자정부 서비스 연동시 서비스 제공 시스템간의 효율적인 인증체제가 요구된다. 둘째, 암호 측면에서 볼 때 전자정부 서비스를 위한 통합 키관리 구조(KMI : Key Management Infrastructure)가 필요하며[7], 유무선 통합환경에서 전자정부 서비스 제공시 무선 단말기의 성능을 고려한 경량화된 암호화 방식의 개발이 요구된다. 추후 범국가적 안보 차원에서 자체 암호 알고리즘 개발에 대한 지속적인 지원이 요구된다. 셋째, 문서보안 측면에서 볼 때 전자문서의 무결성/기밀성 및 전자문서의 무분별한 복제/유포를 방지하기 위해 워터마킹, 핑거프린팅 등의 문서보안 기능이 고려되어야 한다. 넷째, 웹서비스 보안 측면에서 볼 때 송수신되는 문서간의 호환성과 확장성을 지원하기 위해 XML을 적용한 보안 프레임워크가 필요하다. 또한 온라인 민원서비스, 종합 국세 서비스, 국가 물류 종합 서비스와 같은 전자정부 서비스를 위해 전자거래 정보보호기술의 도입이 요구된다..

5. 결 론

본 논문에서는 세계 각국에서 진행중인 전자정부 구축동향을 살펴보고, 더불어 정보보안이 필요한 주요 전자정부 서비스를 보호하기 위해 각 나라에서 구축하고 있는 보안 대책을 분석함으로써 향후 전자정부 선도국가로서 국가경쟁력을 가지기 위해 국내 전자정부에 도입되어야 할 보안 고려사항을 시스템 측면, 네트워크 측면, 서비스 측면으로 나누어 제시하였다. 본 논문에서 제시한 보안 고려사항을 전자정부 구축시 적용한다면 보다 안전하고 신뢰성 있는 전자정부를 설계할 수 있을 것이다.

참고문헌

- [1] “전자정부의 발전단계“, UN e-Government Index, 2002. 6.
- [2] 류석상, 이연우, 박정은, “주요 4개국 전자정부 비교■분석“, NCA 정보화이슈분석, 2003. 5.
- [3] 황종성, 김현곤, 류석상, 박양열, “주요국의 전자정부 우수사례“, NCA 정보화이슈분석, 2003. 4.
- [4] 안문석, 박성진, 맹보화, “전자정부 정보보호 대응체계 구축방향에 관한 연구“, 정보통신학회지 13권 3호, 2003. 6.
- [5] 이경호, 김소정, 임종인, “전자정부와 프라이버시“, 정보통신학회지 13권 3호, 2003. 6.
- [6] 김대호, 오일석, “미국 전자정부 정보보안 법제동향“, 정보통신학회지 13권 3호, 2003. 6.
- [7] 장홍중, 박인재, 이정현, “전자정부 구현을 위한 효율적인 GPKI 구축 방안“, 통신정보처리학회논문지 10권 4호, 2000. 12.
- [8] “전자서명 한 개씩 갖자(13) PKI 해의 활용 현황“, 전자서명인증관리센터, 2002. 9.
- [9] “일본 전자정부의 개인정보보호“, 정보통신정책 13권 21호, 2001. 11.
- [10] “참여정부의 전자정부 추진전략과 현황“, <http://www.changhak.pe.kr>
- [11] <http://www.soumu.go.jp/e-gyousei/daityo/jukida1.html>

김 명 은



1996년 숭실대학교 소프트웨어 공학과 공학사
 1998년 서강대학교 전산학과 공학석사
 1998년 4월 ~ 1999년 9월 동양시스템하우스 근무
 2000년 9월 ~ 현재 한국전자통신연구원 정보보호연구본부 네트워크보안구조팀

연구원

오 승 희



1999년 전북대학교 컴퓨터과학과 이학사
 2001년 이화여자대학교 컴퓨터학과 공학석사
 2001년 ~ 현재 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 연구원

정 연 서



1994.2 : 청주대학교 전자계산학과 학사
 1996.2 : 충북대학교 컴퓨터공학과 석사
 2001.8 : 충북대학교 컴퓨터공학과 박사
 2000. 6 ~ 현재 : 한국전자통신연구원 네트워크보안연구그룹/선임연구원

서 동 일



1989년 : 경북대학교 전자공학과 공학사
 1994년 : 포항공과대학교 정보통신학과 공학석사
 2002년 : 충북대학교 전자계산학과 (박사과정 수료)
 1989. 1. ~ 1992. 2. : 삼성전자종합연구소
 1994. 3. ~ 현재 한국전자통신연구원 네트워크보안구조연구팀장