정보보호 기술 개발 및 표준화 현황 분석

장희선*

요 약

컴퓨터와 정보통신 기술의 발전으로 사이버테러 및 금융사기를 위한 해킹 기술도 진화하고 있으며 이를 대비하기 위한 선진국 수준의 표준화된 정보보호 기술의 연구·개발이 어느 때보다 중요해지고 있다. 본 논문에서는 주요 정보보호 기술에 대한 국외대비 국내의 기술 및 표준화 수준을 진단함으로서 개선점을 제안하며, 시장·기술적 파급효과와 정부 정책 추진과의 부합성을 분석하여 향후 연구개발 방향을 제시한다. 정보보호 기술은 정보보호기반 및 이용자 보호, 네트워크 및 시스템 보안, 응용보안 및 평가인증의 세 가지로 분류하고 세부적으로 OTP기반 인증, 스마트폰앱 보안, 모바일 전자금융 등 9가지로 구분하여 각각의 세부 기술에 대한 현황을 분석한다. 분석 결과, 전반적으로 국외 대비 표준화 및 기술개발 역량이 다소 부족한 것으로 평가되며, 특히 시장·기술적 파급효과가 큰 스마트폰앱 보안 및 모바일 전자금융에 대한 국제적 수준의 기술개발과 표준화 역량이 강화되어야 하고, 미래인터넷에서의 정보보호 기술에 대한 정부의 지원 정책이 시급한 것으로 평가된다.

Analysis of Standardization Level for Information Security Technology

Jang Hee-Seon*

ABSTRACT

As the hacking technology for cyber-terror and financial fraud evolves, the research and development for advanced and standardized information security technology is growing to be more and more important. In this paper, the domestic level of technology and standardization for information security as compared to advanced country is diagnosed, and future policy is presented by analyzing the influence effect for market and technology. The information security is classified into information security-based & user protection, network & system security, and application security & evaluation validation with details of OTP-based validation, smart-phone app security, and mobile electronic finance, etc. The analytic results indicate that domestic level is some poor for advanced country, the technological development and standardization capability for smart-phone app security and mobile electronic finance is needed, and finally the government's supporting policy for the future Internet is urgently needed.

Keywords : Information Security Technology, Information Security Standard

접수일(2013년 8월 21일), 수정일(1차: 2013년 9월 11일), 게재확정일(2013년 9월 12일)

* 평택대학교 컴퓨터학과

1. 서 론

정보보호란, 정보통신망의 마비, 개인정보의 유출, 불건전 정보의 유통 등 정보통신 환경을 저해하는 위협과 부작용에 대응할 수 있도록 정보통신 시스템 및 데이터의 기밀성(정보유출 방지), 무결성(데이터 위조 및 변조 방지)을 유지하고 시스템의 가용성을 보장하는 기술을 의미한다[2,4,8,11,14,24]. 최근 컴퓨터와 정보통신 기술의 발전과 함께 해킹 기술도 진화하고 있으며, 이와 더불어 정보보호 기술도 발전하고 있다. 전 세계적으로 우수한 정보통신 인프라와 기반 시설을 갖춘 우리나라에서 신뢰성과 안전성을 보장하는 스마트 ICT 융합 서비스[12,13]를 제공하기 위해서 정보보호 기술의 개발과 이에 따른 원천기술의 확보가 시급하다. 특히, 시장·기술적 파급효과가 높고 개인정보보호 및 사이버테러에 대비한 정보보호 기술에 대한 국외 수준의 표준화와 기술개발 역량이 요구된다.

본 논문에서는 한국정보통신기술협회에서 작성한 ICT 표준화 전략맵[17] 중에서 정보보호 분야에 대한 연구결과중 주요 정보보호 기술에 대한 국내 연구개발 수준을 분석한다. 구체적으로 세부 정보보호 기술에 대한 국외 대비 표준화 및 연구개발 수준, 국내의 기여도, IPR(IPR: Intellectual Property Rights) 확보 능력, 시장·기술 파급효과 및 정부 추진 정책의 부합성 측면에서 분석하고 이를 통하여 국내 정보보호 기술의 현황을 진단하며, 향후 표준화 및 시급한 연구개발 분야를 제시한다.

2. 정보보호 기술

정보보호 기술은 컴퓨터를 이용한 정보시스템이나 유무선 인터넷과 같은 네트워크를 통하여 전달되는 정보의 위변조, 유출, 무단침입, 서비스거부 등을 비롯한 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하기 위한 기술로, 지금까지 컴퓨터와 정보통신 기술의 발전에 따라 다양한 기술들이 출현하고 정의되었다[1,3,15,16]. 일반적으로 정보보호 기술은 네트워크 보안, 시스템 보안, 웹서비스 제공을 위한 인터넷 보안으로 분류되며[6,7,9,10], 네트워크 보안에서는 네트워크 정보수집, 해킹, 방화벽 구축 기술을 포함하고, 시스템 보안은 계정과 권한 설정, 시스템 해킹, 운영체제 보안, 로그와 침입탐지 및 추적 기술로 나누며, 인터넷 보안은 웹해킹, 웹서버 보안 설정, 전자상거래 암호화, 보안 솔루션 구성 기술 등을 정의한다[5,20,21].

한편, 한국정보통신기술협회에서는 정보보호 기술을 (그림 1)과 같이 정보보호기반 및 이용자 보호, 네트워크 및 시스템 보안, 응용보안 및 평가 인증 기술로 나눈다.

(그림 1) 정보보호 기술[17]

① 정보보호 기반 및 이용자 보호: 암호기술, 인증기술, 권한관리 기술, ID 관리, 개인정보보호, 유해정보 대응 기술을 제공하기 위한 보안 기술

② 네트워크 및 시스템 보안: 정보보호 기반 기술을 활용하여 네트워크 및 시스템에서의 정보보호를 확립하기 위한 스마트폰 보안, 클라우드 보안, 사이버공격 대응, 악성코드 대응, 스마트 네크워크 보안, 미래 인터넷 보안, IoT/M2M 등 통신 및 시스템 보안을 제공하기 위한 보안 기술

③ 응용 보안 및 평가인증: 정보보호 기반 기술과 네트워크 및 시스템 보안기술을 활용한 금융보안, 콘텐츠 접근제어, 빅데이터 보안, 클라우드 응용보안, 스마트 그리드 보안, 바이오 인식 등 다양한 서비스와 제품을 평가하기 위한 기술

먼저, 정보보호 기반 및 이용자 보호 기술에 대한 표준화를 위하여 <표 1>과 같은 세부분야에서 연구가 이루어지고 있다. 주요 기술을 정리하면 다음과 같다[17,18].

<표 1> 정보보호 기반 및 이용자 보호

분류		주 요 내 용
암호 및 활용	경량 암호 알고리즘	IT융합 환경에 적합한 경량암호 알고리즘 규격
	암호 알고리즘 적용	응용서비스에의 암호 알고리즘 활용 방법
디바이스 인증	기기인증 프로파일 및 프로토콜	인터넷 전화기, CCTV, 휴대 단말기, 지능형 가전 등의 디바이스에 대한 식별 및 인증
	기기인증 응용기술	신뢰된 인증 서비스 제공을 위한 기반 및 응용
통합형 인증 체계	통합인증 서비스 프레임워크	계층화된 통합인증 서비스 위탁형 부인방지 서비스 모바일 환경의 멀티팩터 인증
	통합인증 응용 및 보안관리	스마트 기기에 적합한 IC기반 경량 인증 모듈 NFC USIM 기반 사용자 인증 기술 보안 등급별 통합인증관리 및 위협관리 요구사항
OTP 기반 인증	OTP 시스템	키 생성 시스템 및 알고리즘 OTP 알고리즘 프로파일 USIM 기반 OTP 구현 규격
	OTP 응용 프로토콜	OTP-TLS·EAP·Kerberos 등 OTP 암호키 갱신 프로토콜
익명 인증	익명인증 암호기술	익명 인증 요구사항 및 기반 암호 기술
	익명 인증서 프로파일 및 관리 프로토콜 검증 기술	익명 인증 체계 (프로파일, 프로토콜, 검증 등)
Identity 관리	Identity관리	Identity의 프레임워크
	모바일 결제	모바일 단말기 기반 온·오프라인 결제 기술
개인 정보 보호	개인정보보호 정책 및 운영관리	정보보호 정책 관리,DB 보안 온라인 서비스 사용자 및 사용자 본인 확인 기술
유해 정보 대응	유해정보 차단 및 모니터링	유해정보 차단 정책 (차단방식, 등급, 콘텐츠 포맷) 단말 프레임워크 및 인터페이스 유해정보 실시간 특징 추출

통합형인증체계: 인터넷 서비스 환경에서 여러 서비스 제공자가 공동으로 사용할 수 있도록 하는 상호 운용성 보장 기술이다.

OTP 기반 인증: 일회용패스워드(OTP: One Time Password) 기반 인증기술은 OTP 발생기를 통합 관리하여 사용자의 편의성을 향상시키고 동시에 인증을 강화하기 위한 기술로서, 최근 전자상거래 분야에서 은행 결제 시 인터넷 뱅킹 카드로 소유자 인증을 위해 사용되고 있다.

개인정보보호: 개인정보 획득에 따른 의무와 이용 범위 및 보호수준 등에 대한 정책 관련 기술, 개인정보의 오남용, 도용, 분실 시 사용자, 정보제공자 및 정보이용자의 대응 방법 및 복구 기술, 사용자 개인정보 DB 보안 기술, 사용자 본인 확인 기술 등으로 분류된다.

네트워크 및 시스템 보안은 <표 2>와 같다. 여기서 악성코드란 봇넷(Botnet) 및 C&C(Command and Control) 서버를 통하여 유포되는 유해코드, 모바일 악성코드 등과, 악성코드 은닉·경유·유포 사이트를 통한 유해코드를 포함한다. 주요 기술은 다음과 같다[17, 19].

<표 2> 네트워크 및 시스템 보안

분 류		주 요 내 용
스마트폰	스마트폰 앱 보안	안전한 스마트폰 앱 개발과 사용을 위하여 스마트폰 앱과 앱 마켓에 대한 보안 기준
클라우드	클라우드 보안 관리 및 관제	클라우드 컴퓨팅 서비스의 보안관리 및 보안 컴플라이언스 침해사고에 대한 실시간 모니터링과 대응절차에 대한 체계
	가상 네트워크 침입탐지 분석	가상 네트워크에 대한 침해분석 기반체계와 에이전트, 데이터베이스, 분석 논리 등
사이버 공격 대응	보안 정보 공유 및 통합 제어 프레임워크	유관기관간의 사고 정보공유 협업형 통합제어 프레임워크
악성 코드 대응	악성코드 통합 대응 기능 및 구조	악성코드 수집 정보, 경유 및 유포지 탐지 정보 등의 공유 및 분석
스마트 네트워크	Mobility 보안 구조 및 절차	이종 사업자 또는 네트워크 간의 이동성 제공을 위한 보안 구조 및 절차
	클라우드컴퓨팅 네트워크 보안	Multi-provider 환경에서 클라우드 서비스 제공자의 보안 취약점을 최소화하기 위한 스마트 네크워크 요구사항
미래 인터넷	미래 인터넷 보안 요구사항	미래 인터넷 보안 기술 Trustworthy architecture, intrinsic security, traceability
IoT M2M	통신프라이버시 보호 프레임워크	사물지능통신 환경에서 발생할 수 있는 프라이버시 침해 위협을 정의하고 보안 프레임워크 및 대응방안 제시

스마트폰 앱보안: 스마트폰에서의 정보보호 기술들을 정의하고 스마트폰 플랫폼 및 앱, 무선통신망에서의 스마트폰과 다른 장치간의 인터페이스 등의 보안 기술들로 이루어진다.

사이버공격 대응: 사이버 공격 및 진화하는 악성코드 등에 대응하는 정보보호 기술로 분류된다.

미래인터넷 보안: 미래 인터넷 통신 환경을 도입하기 위한 구조이며, 전혀 다른 혁신적인 개념으로 설계

될 미래의 새로운 인터넷에서의 정보보호 기술을 포함한다.

마지막으로, 응용보안 및 평가인증 표준화 기술은 <표 3>과 같고, 주요 기술은 다음과 같다[17,22,23].

<표 3> 응용보안 및 평가인증

분 류		주 요 내 용
콘텐츠 접근제어	연령 검증 프로토콜	사용자 연령 검증 강화 프로토콜 개발
금융 보안	모바일 전자금융 보안 프레임워크	단말 보안기술(TrustZone, TPM 등)을 이용한 전자금융(e-banking, e-payment 등) 보안 프레임워크 개발
	모바일 결제 서비스	스마트폰 기반의 SW(결제앱), 임베디드 SE(Secure Element) 및 HW(USIM) 이용 모바일 결제
	금융 보안관리 프레임워크	금융IT 보안과 통제를 위한 금융 정보보안 기술, 법규, 산업기준
스마트 그리드 보안	기능구조	안전한 스마트 그리드 인프라 구축
	프라이버시 보호	사용자 정보 및 에너지 사용 데이터 등에 대한 안전한 프라이버시
	보안 관리	정보, 시스템 등 자산 보호
	스마트기기 보안	기기에 대한 인증, 저장 및 전송되는 데이터 보안
클라우드 응용	신뢰 클라우드 연동	재난 복구 보장 기술 클라우드 연동, 서비스 연속성보장 안전하고 호환 가능한 Identity연구(Trusted Cloud Initiative))
빅데이터	데이터 보안	데이터 암호화, 관리(접근제어, 보호, 모니터링) 리스크 관리 기술
웹서비스	차세대 웹	웹2.0, 모바일웹2.0, 융합응용 보안 SOA 기반 융합응용 보안 유비쿼터스 웹, 시맨틱 보안
	모바일 웹	모바일웹 어플리케이션·단말 보안 데이터 보호, 모바일 브라우저보안
	웹 프라이버시	웹 프라이버시 정책 협상 프라이버시 데이터 접근 제어
	SOA	SOA 보안, 인증인가, 메시지 보안 서비스 보안정책, 웹기반SaaS보안
바이오 인식	바이오인식 응용 기술	텔리 바이오정보 기반 전자서명 One-time템플릿 기반 바이오인증 원격의료 통합 프레임워크 바이오 보안, 토큰 보안 모바일 디바이스의 바이오인식
	프라이버시 보호	물리보안 결합형 바이오인식융합 CCTV 기반의 프라이버시 보호
보안 평가	보안성 평가 기준	IT 제품의 보안성 평가를 위한 기준 및 체계의 표준화
	보안성 평가 방법론	공통평가기준에 정의된 기준과 평가 증거를 사용하여 평가자가 수행해야하는 평가 행동에 대한 표준화
보안 관리	정보보안 거버넌스 프레임워크	비즈니스 목표 및 전략방향 지원 이를 위한 프로세스, 이사회와 경영진의 책무 제시
	정보보안 성과측정 지침	성과측정을 위한 주요 지표 도출 평가기준, 방법론 및 지침
	정보보안 사고관리 지침	정보보안 사고 모니터링 체계적인 침해사고 대응 절차 및 보안위협에 대한 대책 수립 방안

모바일 전자금융: 하드웨어 기반 스마트폰 단말 보안 플랫폼(예: TrustZone, TPM(Trusted Platform Module) 등)에 적용될 모바일 전자금융 서비스 소프트웨어 프레임워크를 포함한다.

모바일 웹: 차세대 웹, 모바일웹, 프라이버시와 인프라를 위한 SOA(Service Oriented Architecture) 보안기술들로 이루어진다.

정보보안 거버넌스: IT 제품의 보안요구사항 및 보증 요구사항을 정의하고 평가하기 위한 기준 및 개발자, 평가자가 수행해야 할 활동과 요구사항을 정의한다.

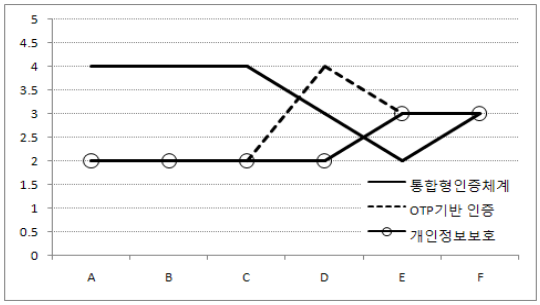
3. 현황 분석

세부 기술의 현황을 분석하기 위하여 <표 4>의 지표를 설정한다. 본 결과는 TTA[17]의 연구결과(전문가 의견, 연구 현황 분석 등) 중 일부를 요약한다.

<표 4> 현황분석 지표

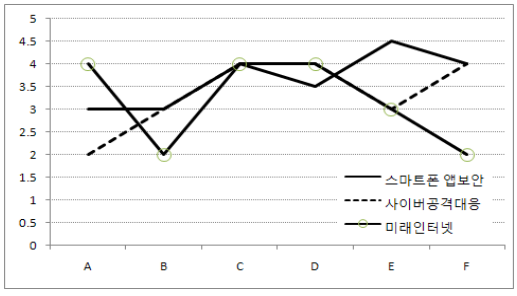
분 류	지 표
A	국외대비 국내 표준화 수준
B	국외대비 국내 기술개발 수준
C	국제 표준화 국내 기여도
D	IPR 확보 가능성
E	시장·기술적 파급효과
F	정책 부합성

(그림 2)는 정보보호기반 및 이용자보호 분야에 대한 결과로 1점(매우 낮음), 2점(낮음), 3점(보통), 4점(높음), 5점(매우 높음)의 Likert Scale로 표현하였다. 통합형인증체계의 경우 국외 대비 표준화 및 기술개발 수준과 국제 표준화에 대한 기여도가 높으나, 시장·기술적 파급효과가 낮은 것으로 나타났다. 개인정보보호의 경우에는 모든 지표에서 개선이 필요하며, OTP기반 인증에서는 IPR 확보가능성에 대하여는 낙관적이지만 다른 분야에서의 노력이 요구된다.



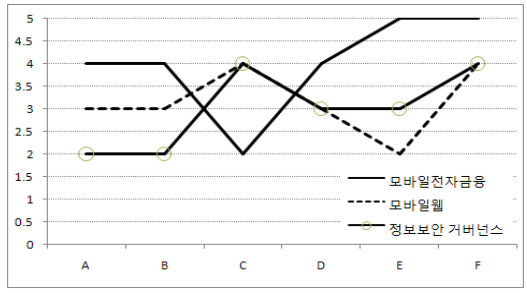
(그림 2) 정보보호기반 및 이용자보호 기술 현황

(그림 3)은 네트워크 및 시스템 보안에 대한 결과이다. 스마트폰앱 보안에서는 모든 분야에 대해서 다소 높은 평가를 나타내며 특히, 시장·기술적 파급효과가 클 것으로 기대된다. 사이버공격대응 분야에서는 국내 표준화 수준이 다소 미흡하지만, 국내 기여도와 IPR 확보 가능성 및 정책의 부합성 측면에서 높다. 미래인터넷에서는 기술개발과 정책 지원이 다소 부족하나 국내 표준화 수준 및 기여도와 IPR 확보 가능성면에서 낙관적이다.



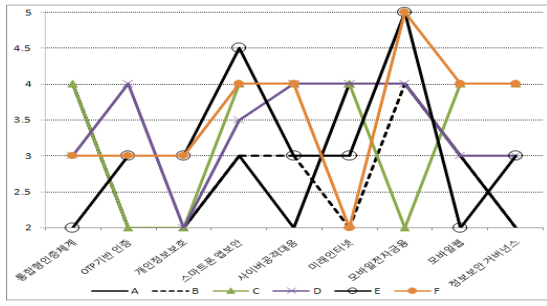
(그림 3) 네트워크 및 시스템 보안 기술 현황

마지막으로 (그림 4)는 응용보안 및 평가인증의 세 가지 기술에 대한 결과이다. 모바일전자금융 분야는 국제 표준화에 대한 기여도는 다소 미흡하나, 다른 분야에서는 우수하며, 특히 시장기술적 파급효과가 높아 국내 정책 수립시 적극적으로 활용되고 있다. 모바일웹 분야에서는 시장기술적 파급효과가 다소 미흡하지만, 표준화에 대한 국내 기여도가 높고 정책 부합성이 높다. 정보보안 관리를 위한 거버넌스 측면에서의 분석 결과, 국외대비 표준화 및 기술개발이 미흡하지만, 국내 기여도가 높고 정책 부합성이 높은 것으로 평가된다.



(그림 4) 응용보안 및 평가인증 기술 현황

평가결과를 요약하면 (그림 5)와 <표 5>와 같다. 전반적으로 세부 정보보호 표준화 기술에 대한 국외 수준의 표준화와 기술개발이 이루어져야할 필요가 있고 특히 개인정보보호와 OTP기반 인증에 대한 표준화 및 기술개발이 시급함을 알 수 있다. 그리고 시장기술적 파급효과가 높은 스마트폰앱과 모바일전자금융에 대한 국제적 수준의 기술개발과 표준화 역량 강화가 요구되며, 미래인터넷에 대한 정부의 지원 정책이 필요함을 알 수 있다.



(그림 5) 정보보호 기술의 국내 수준

<표 5> 정보보호 기술별 현황

분류	낮음(2점)	보통(3점)	높음(4점)
통합형인증체계	E	D,F	A,B,C
OTP기반인증	A,B,C	E,F	D
개인정보보호	A,B,C,D	E,F	-
스마트폰앱보안	-	A,B,D(3.5)	C,E(4.5),F
사이버공격대응	A	B,E	C,D,F
미래인터넷	B,F	E	A,C,D
모바일전자금융	C	-	A,B,D,E(5),F(5)
모바일웹	E	A,B,D	C,F
정보보안거버넌스	A,B	D,E	C,F

4. 결 론

본 논문에서는 주요 정보보호 기술에 대한 국내 역량과 시장기술 파급효과 및 정책의 적절성을 분석하였다. 정보보호 기술은 크게 정보보호기반 및 이용자 보호, 네트워크 및 시스템 보안, 응용보안 및 평가인증으로 분류하였으며 세부적으로 통합형인증체계, OTP기반 인증, 개인정보보호, 스마트폰 앱보안, 사이버 공격 대응, 미래인터넷, 모바일 전자금융, 모바일웹, 정보보안 거버넌스로 분류하였다. 분석 결과, 국외와 비교하여 국내 표준화 및 기술개발 역량이 다소 부족한 것으로 나타났으며, 특히 개인정보보호와 OTP기반 인증에 대한 연구개발이 시급한 것으로 평가되었고 시장기술적 파급효과가 높은 스마트폰앱과 모바일 전자금융에 대한 국제적 수준의 기술개발과 표준화 역량 강화가 필요하며, 미래인터넷에서의 정보보호 기술에 대한 정부의 지원 정책이 마련되어야 할 것으로 평가되었다. 향후 다양한 정보보호 기술에 대한 평가와 함께 진단 결과에 따른 개선점 및 시사점을 보다 세부적으로 제시할 필요가 있으며, 모든 정보보호 기술에 대한 공통 분모인 원천기술 확보 전략과 정책 지원 방안에 대한 연구가 이루어져야 한다.

참고문헌

[1] 경찰청 사이버테러대응센터, http://www.ctrc.go.kr.
[2] 국가사이버안전센터, http://service2.nis.go.kr.
[3] 김점구, 노시춘, “분산컴퓨팅 환경에서의 고가용성 클러스터링 프레임워크 기본설계 연구,” 융합보안 논문지, 제13권, 제3호, pp.17-24, 2013.6.
[4] 박용규, “사이버 대피소를 통해 본 ‘12년도 DDoS 공격동향 분석,” Internet & Security Focus, pp.39-58, 2013.2.
[5] 박종훈, “구글의 프라이버시 정책 변경과 개인화 검색의 함의,” 주간기술동향, 제1532호, pp.28-29, 2012.
[6] 양대일, 정보보안개론-큰 그림을 그려주는 정보보안 입문서,“ 한빛미디어, 2011.7.
[7] 이강신, “국내외 정보보호 관리 모델에 관한 고찰,” 정보보호학회지, 제11권, 제3호, pp.24-37, 2001.
[8] 임유석, 김상진, “스마트미디어 시대의 테러 네트워크에 관한 고찰,” 융합보안 논문지, 제13권, 제2호, pp.85-94, 2013.5.
[9] 장희선, 신현철, 이현창, “멀티미디어 콘텐츠의 서비스거부 방지 알고리즘 성능분석,” 한국컴퓨터정보학회 논문지, 제15권, 제4호, pp.19-25, 2010.4.
[10] 장희선, “사이버 범죄 현황과 웹취약성 평가,” 주간기술동향, 제1595호, pp.15-25, 2013.5.
[11] 장희선, “정보보호 기술과 국내 개발 현황,” 주간기술동향, 제1600호, pp.17-26, 2013.6.
[12] 장희선, “u-City 통합운영센터에서의 정보보호 요구사항,” 주간기술동향, 제1519호, pp.11-22, 2011.10.
[13] 장희선, “u-City에서의 비즈니스 모델,” 주간기술동향, 제1406호, pp.1-13, 2009.7.
[14] 전정훈, “보안 프로그램의 취약성 및 문제점에 관한 연구,” 융합보안논문지, 제12권, 제6호, pp.77-84, 2012.12.
[15] 한국인터넷진흥원, http://www.kisa.or.kr.
[16] 한국정보화진흥원, http://www.nia.or.kr.
[17] 한국정보통신기술협회(TTA), ICT 표준화전략맵 Ver.2013, 2013.
[18] David Gourley and Brian Totty, HTTP: The Definitive Guide, O'Reilly Media, 2002.
[19] Frost & Sullivan, The 2011(ISC)2 Global Information Security Workforce Study, 2011.2.
[20] IDC, Worldwide Identity and Access Management 2010-2014 Forecast: A First Look in 2010, 2010.3.
[21] IDC, Worldwide Mobile Security 2010-2014 Forecast and Analysis, 2010.3.
[22] ISO/IEC, Guidelines for the Management of IT Security(GMITS), TR13335, 2000.
[23] K.Vieira, A.Schulter, C.Westphall and M.Westphall, " Ensuring Data Storage Security in Cloud Computing," IT Professional, Vol.12, pp.38-43, 2010.
[24] OWASP, http://www.owasp.org.

[저 자 소 개]

장 희 선 (Hee-Seon Jang)

KAIST 산업공학과(공학박사)

평택대학교 컴퓨터학과 교수
관심분야: 트래픽 엔지니어링

e-mail : hsjang@ptu.ac.kr