통상정보연구 제7권 제3호 (2005년 9월 25일)
논문투고일자 : 2005. 08. 06
게재확정일자 : 2005. 09. 15

유비쿼터스 컴퓨팅 환경 하에서의 전자무역 보안 쟁점과 전략에 관한 소고

A Study on E-trade Security Issue and Strategy in Ubiquitous Computing Environment

정성훈(Sung-Hoon Jung)*
동국대학교 상경대학 국제통상학전공 교수
강장묵(Jang-Mook Kang)
서경대학교 컴퓨터공학과 겸임교수
이춘수(Chun-Su Lee)
고려대학교 기업경영연구원 연구원

목 차

Abstract

The rapidly developed environment by ubiquitous computing make the paradigm from e-trade to u-trade. The purpose of the study is to find out issue and the strategic suggestions that could link together between the e-trade and ubiquitous computing in side of information security. The study include the contents as follows; firstly, the technical explanations under the ubiquitous computing, secondly, e-trade's risks in security technology and lastly, issue and strategic suggestions how link them together in integrated view.

Key Words : Ubiquitous Computing, e-trade, Information Security Strategic

* 주저자임.

Ⅰ. 서 론

최근 정보통신기술의 급격한 발전은 인터넷과 통신기기의 융합을 초래하였고, 더 나아가 네트워크의 상호진화를 통한 유비쿼터스 컴퓨팅 시대(Ubiquitous Computing Area)를 열었다. 즉 모바일 네트워킹의 본격화에 따라 이를 활용한 이동전화, PDA, Note book, MP3 등의 기기를 활용한 모바일 상거래가 일상화 된 것이다. 최근에는 차세대 인터넷주소체계를 비롯하여, 광대역 통합 망, 유비쿼터스 센서 네트워크, 그리드(grid) 기술 등에 대한 논의가 활발히 진행 되고 있다. 유비쿼터스의 사전적인 의미는 라틴어 어원으로 '동시에', '도처에 존재하는', '편재(遍在)하는(omnipresent)'등의 뜻을 지니고 있다. 이러한 사전적인 유비쿼터스 개념을 컴퓨팅, 네트워크, 전자무역과 연계하여 이해하면 "컴퓨팅 기술을 언제 어디서나 네트워크에 연결하여 국제경쟁력과 비교우위를 가지는 제품과 서비스를 개발하고 유통을 가능케 하는 새로운 패러다임"으로 정의내릴 수 있다. 이러한 측면에서, 제한된 자원을 유기적인 네트워크 시스템을 이용하여 경쟁력을 높이는 방안이 부존자원이 부족한 우리나라에서는 필요하다고 여겨진다. 유비쿼터스 컴퓨팅 환경을 통하여 글로벌 전자무역을 활성화함으로써 지식기반사회에서 지능기반사회로 전환하여야 할 필요가 있다. 그리고 이러한 환경 하에서 급속히 개발되고 있는 최첨단 기술에는 정보화의 순기능뿐만 아니라 개인정보 유출, 프라이버시 침해 등 다양한 역기능을 보이고 있으며 이를 방어할 수 있는 전략적 대응 방안이 요구된다. 그러므로 유비쿼터스 컴퓨팅 환경 하에서의 전자무역보안에 대한 중요성 인식과 더불어 이에 대처할 수 있는 기술 방안을 고려하는 것이 화두가 되고 있는 것이다. 따라서 전자무역의 기술진보와 더불어 역효과 및 역기능을 최소화하는 전자적 대응방안 및 해결책을 강구할 필요성이 요구된다.

본 소고에서는 유비쿼터스 컴퓨팅 환경과 전자무역 보안에 대한 고찰을 통하여 유비쿼터스 컴퓨팅 환경이 전자무역보안 환경에 어떻게 영향을 미치며, 주요 이슈(개인정보 유출, 프라이버시, 저작권, 해킹 등)에 대하여 파악하고자 한다. 또한 전자무역 보안에 관련된 전략적 시사점을 유비쿼터스 컴퓨팅의 관점에서 제공하는데 본 연구의 목적이 있다. 특히 유비쿼터스 컴퓨팅의 주요 특징을 문헌조사를 통하여 도출하고 구체적으로 구현될 다양한 서비스와 이슈를 파악하여 전자무역보안전략을 분석하고자 한다. 마지막으로 이를 통하여 인터넷 시대의 초기 전자상거래의 활성화가 기업과 소비자 간의 비대면 상거래에 따른 신뢰구축이었다면 초기 유비쿼터스 컴퓨팅 시대의 전자무역이 기업과 소비자 간의 프라이버시 보호에 있음을 설명하고 이에 관한 이슈와 전자상거래 보안을 통한 글로벌 경쟁력 제고를 위한 효과적 보안 전략을 통해 본 소고의 목적을 달성하고자 한다.

Ⅱ. 유비쿼터스 컴퓨팅 환경

1. 발전 중에 있는 유비쿼터스 컴퓨팅 개념

마크 와이저가 유비쿼터스 개념을 소개한 이후 유비쿼터스 개념은 기술 발전과 함께 그 의미가 확대·발전되고 있는 추세인데 오늘날에는 ‘Computing access will be everywhere'로 정의할 수 있다고 사료된다. 이는 연결성을 강조하는 유비쿼터스 컴퓨팅을 뜻한다. 예를 들면, U-korea, U-government, U-shopping, U-logistics, U-commerce, U-city 등이 있으며 결국 세부 분야에서 유비쿼터스 컴퓨팅 환경을 지원한다는 의미를 가지고 있다. 이와 유사한 세부적인 개념으로 ‘ambient computing’, ‘disappearing computing’, ‘implantable computing’, ‘nomadic computing’, ‘invisible computing’, ‘pervasive computing’, ‘silent computing’, ‘sentient computing’, ‘disposable computing’ 등이 있다. 이와 같이 유비쿼터스 컴퓨팅 개념은 다양하게 구현되는 모습에 따라 여러 가지 용어로 해석되고 정의되고 있음을 알 수 있다. 그렇다면 다양하게 정의되고 있는 유비쿼터스 컴퓨팅 개념과 구현된 서비스의 명칭을 분류하면 다음과 같이 크게 세 가지로 설명될 수 있다.

첫째, 초기 유비쿼터스 컴퓨팅 개념이었던 내장형 컴퓨팅에서 모바일 컴퓨팅으로 개념이 이동하면서 확대되고 있다고 이해할 수 있다. 이와 같은 기술의 세부적인 변화에 따라 초기 유비쿼터스 컴퓨팅 개념이 컴퓨팅 칩의 내재성(pervasiveness)을 강조하였다면 오늘날의 유비쿼터스 컴퓨팅 개념은 칩의 자유로운 이동과 연결성을 중시하는 이동성(mobility)을 강조하는 방향으로 바뀌고 있다.

둘째, 유비쿼터스 컴퓨팅 환경에서 정보를 교환하는 상대는 현재 ‘사람과 사람(person to person)’ 중심에서 ‘사람과 기기(person to device)’로 바뀌고 있으며 ‘기기와 기기(device to device)’간의 통신도 점차 증가하고 있다[1]. 자유로운 의사소통을 위한 인터페이스 개발과 지적 에이전트 기능이 중요하게 부각되는 이유이기도 하다[2]. 즉 P2P 기술, 다양한 지능형 에이전트 기술 등을 통해 기기와 기기간의 자유로운 커뮤니케이션 환경과 통신 규약(protocol) 제정이 요구되고 있다.

셋째, 유비쿼터스 컴퓨팅 환경은 기존의 물리공간(physical space)과 가상공간(cyber space)에서 물리공간에 침투된 가상공간인 유비쿼터스 공간(ubiquitous space)으로 우리가 살아갈 공간과 환경을 변화시킨다. 즉 유비쿼터스 컴퓨팅 기술은 단순한 기술적 진화 단계에서의 편리함과 혜택을 주는 도구로 그치지 않고 인간의 생활양식과 공간을 변화시킬 혁신적인 기술이 되고 있다고 여겨진다.

우리나라의 경우 IT허브로서의 이동전화 개념 도입(삼성의 애니콜 등), 무선인터넷 등 브로드밴드 집중 전략 등으로 이동성의 성격이 강조되고 있다. 즉 오늘날 유비쿼터스 컴퓨팅 개념이란 커뮤니케이션의 시간, 장소, 대상에 구애받지 않고 자유롭게 커뮤니케이션 할 수 있는 것을 뜻한다고 사료된다.

2. 유비쿼터스 컴퓨팅의 일반적 속성에 따른 구현될 발전방향과 보안위험

유비쿼터스 컴퓨팅이 과거와 오늘날의 개념적 진화와 기술 발전 방향에 대한 이해를 통하여 커다란 틀에서의 내재성과 이동성이 구체적으로 구현될 모습을 예측하고 그에 따른 기술적인 보안 위험을 고려해야한다. 즉 유비쿼터스 컴퓨팅의 속성이 구현할 발전방향을 분석함으로 유비쿼터스 컴퓨팅 환경하의 전자무역 발전방향과 나아가 보안의 이슈 및 시사점을 도출할 수 있기 때문이다.

1) 유비쿼터스 컴퓨팅의 일반적 속성

유비쿼터스 속성에 대한 다양한 주장이 제기되고 있다. 이 중에서 보편적인 속성들에 대해서는 류영달(2004)[3]과 하원규(2004)[4]가 분류한 속성에서 공통된 부분을 중심으로 살펴보면 다음과 같이 네 가지로 설명되어진다.

첫째, 연결되어야 한다. 모든 컴퓨터와 사물 그리고 사람들이 서로 연결되어야 하며 연결이 끊기더라도 자동으로 끊김 없는(seamless) 네트워크를 구성한다. 즉 네트워크의 연결은 5종의 Any(Any-time, Any-where, Any-network, Any-device, Any-service)화를 지향하고 있다. 둘째, '보이지 않는다(disappearing)'는 특징이 있다. 수많은 컴퓨팅 기술이 주변에 편재하여 있으나 사용자들이 거부감을 느끼거나 방해받지 않도록 환경에 스며들 듯이 통합화되어 있어 마치 직물 속의 실처럼 엮어져 보이지 않으며 일상생활 속에 파고들어 있어야 한다는 것이다. 셋째, 조용한 서비스(calm service)이다. 평소에는 배후에 숨어 있어 의식할 수 없지만 필요할 때에는 사용자의 개입을 요구함으로써 인간의 집중력을 효과적으로 활용할 수 있도록 하는 사용자 중심 환경이어야 한다는 것이다. 넷째, 실제적(real)이어야 한다. 즉 물리공간에 실존하며 가상세계의 증강이 아니라 실제 세계를 강화한다는 것이다.

강홍렬(2004)은 유비쿼터스 컴퓨팅의 기술혁신의 진행방향에 대하여 다음과 같이 8개의 방향으로 나아가고 있다고 보았다[5]. 첫째 컴퓨팅과 사물의 결합, 둘째 상황의 인식과 현실 공간 정보의 활용, 셋째 모든 IT의 상호연결성, 넷째 서비스의 노메딕(nomadic)화, 다섯째 IT의 자율성 확대, 여섯째 인간-IT의 인터페이스의 패러다임 변화, 일곱째 융합(convergence)의 진행, 여덟째 현실공간의 보강 등이다.

이와 같이 유비쿼터스 컴퓨팅의 속성과 그에 따른 기술혁신의 진행방향에 대해 공통된 주장은 컴퓨팅 칩의 내재화에 따른 보이지 않고 조용한 서비스의 구현과 이동성의 확대에 따른 모든 사물간의 연결, 연결에 기초한 실제적인 서비스 그리고 이와 같은 속성들이 융합, 상황 인식 서비스, 지능화 서비스, 현실 공간의 보강 등으로 기술혁신이 이루어질 것이란 예측이다. 따라서 이동성과 내재성을 중심으로 한 커다란 특징을 유추하고 이와 같은 유비쿼터스 컴퓨팅 속성이 구체적으로 진화하고 발전하여 구현될 서비스는 조용하고 실제적이고 보이지 않으며 다양한 서비스들이 융합된 모습이 될 것이라고 사료된다. 따라서 전자무역에서 적용될 유비쿼터스 컴퓨팅 기술 역시 이동성과 내재성을 극대화하여 기업의 경쟁력을 높이는 방향으로 발전할 전망이다.

2) 유비쿼터스 컴퓨팅의 발전 방향

마크 와이저는 유비쿼터스 컴퓨팅에 있어서 컴퓨터, 네트워크, 인간 그리고 응용을 주요한 키워드로 제시하였다. 이들 키워드를 중심으로 현재 구현되었거나 장래에 구현될 기술들 중에서 유비쿼터스 컴퓨팅에 활용가능하며 주요한 역할을 담당할 기술들은 아래 [표 1]과 같다[6].

[표−1] 현재 구현되었거나 장래에 구현될 유비쿼터스 컴퓨팅 기술 관점에서의 분류[1)]

유비쿼터스 컴퓨팅 속성	마크와이저의 키워드 기술 분야	현지 구현되었거나 장래에 구현될 기술	유비쿼터스 컴퓨팅 기술의 진화
내재성	컴퓨터	마이크로컴퓨터 칩 나노, 병렬 등 고집적 기술 개인인증, 보안기술	소형화, 내장화, 비가시화 기술
이동성	네트워크	네트워킹(IPv6) 장치접속기술(P2P, Grid 관련 기술 포함)	연속적 이음(seamless) 기술
내재성, 이동성	인간(인터페이스)	수동 능동형 센서기술 근거리무선기술 (블루투스, RF I/F 등)	인간과 사물, 사물과 사물, 인간과 인간간 자율형 직접 인터페이스 기술
이동성	응용	P2P, Grid 기술 WWW, Java, Wap, XML	망 기반 복합응용 미들웨어기술

[표-1]은 유비쿼터스 컴퓨팅 기술을 이동성과 내재성이라는 두 가지 기술적 특징을 가지고 구체적으로 구현될 서비스를 분류하고 있다. 그 이동성과 내재성은 컴퓨터, 네트워크, 인간(인터페이스), 응용분야에 구체적으로 구현되어 진다. 구현된 기술과 구현될 기술의 진화를 내재성과 이동성이라는 두 가지 커다란 속성으로 살펴보면 다음과 같다.

첫째, 내재성의 경우 컴퓨터 칩의 경량화, 소형화 기술을 통해 구현될 것이다. 즉 이동전화, PDA, Printer, MP3, Notebook, 옷, 지갑, 안경 등에 손톱보다 작은 크기의 소형컴퓨터를 내장할 수 있는 기술을 통해 유비쿼터스 컴퓨팅 시대를 앞당길 것이다. 이러한 기술이 가능한 것은 마이크로컴퓨터 칩의 소형화시킬 수 있는 나노[2)], 병렬 등의 고집적 기술의 발전에 기인한다. 그리고 내장된 컴퓨터 칩들은

1) 김완석, 김정국, "*유비쿼터스 컴퓨팅의 발전 전망과 보안에 대한 이슈*", 정보보호학회지, 제14권, 제1호, 2004년 2월, p. 4의 [표-1]을 본 소고의 2-(1)에서 다룬 연구 분석의 결과인 유비쿼터스 컴퓨팅의 이동성과 내재성이라는 속성을 중심으로 수정하여 재구성함.

2) 나노 기술의 경우 나노 사이즈의 센서 및 저소비 전력화기술 등을 개발하고 있으며 수동형 혹은 능동형 센서는 다양

개인인증 등의 보안 기술을 하드웨어적 또는 소프트웨어적으로 구현할 수 있을 것이다. 결국 장래의 내재성 기술은 컴퓨터의 내재성을 인간과 사물 등에 무수히 설치할 수 있을 만큼의 가격저렴화와 소형화를 이루어낼 전망이며 이는 인간의 인터페이스로 인간의 옷, 구두, 시계, 이동전화, 지갑 등에 내재된 컴퓨팅 칩이 사용되는 것을 의미하며 건물의 벽, 인공위성, 가로등, 분수대, 심지어는 바위 등의 사물에 내재된 컴퓨팅 칩을 통한 사물과 인간, 인간과 인간, 사물과 사물 간의 인터페이스의 기본 장치로 초소형 컴퓨팅 칩이 활용될 것을 뜻한다.

둘째, 이동성의 경우 IPv6을 통해 네트워크 가용자원의 한계를 극복하고 있다. 특히 IPv6은 단순한 네트워크 가용 용량의 증설을 뜻하는 것이 아니라 무선인터넷에서의 내장형 보안 기능(IPsec), 최적화된 로밍(route optimization), 자동 주소 설정(auto-configuration)기능 제공, 인터넷 정보가전에서의 항시 연결성(always connected), 플러그 앤 플레이 기능 제공 등이 IPv6을 도입하는 주요 장점 중의 하나이다[7]. 구체적으로 실용화가 완료되어 상용화될 IPv6은 128비트의 주소체계로 340간(澗, 3.4x10의 38승)개의 IP 주소로 60억 인구 중 한 사람 당 5x10의 26승의 IP주소를 할당할 수 있으며 IPv6의 기술을 적용할 경우 IP주소 자원의 제약으로부터 벗어날 수 있다. 따라서 지구상에 존재하는 모래 하나 하나에도 IP를 할당하고도 남는 자원을 확보함으로 네트워크의 근본이 되는 주소 자원을 풍부하게 가지게 되는 것이다. 이는 IP주소로서의 자원의 경우 IPv4에서 IPv6로 전환되면서 무한정 확대된다는 점에서 과거 IP자원의 희소성(scarcity)이 해결됨으로 컴퓨팅 디바이스의 수가 수억 개 이상 확대될 수 있다. 다양한 이동성을 강조하는 네트워크 기술의 구체적인 구현 기술로는 최근 블루투스, RFID와 같은 근거리 무선통신 기술이 각광받고 있다. 근거리 무선통신 기술은 가정에서의 홈 네트워크(세탁기, TV, 거실과 방의 등, 음향기기, PDP 등을 근거리로 네트워킹 하여 구현) 기술로 현재 활용되고 있다. 이와 같은 근거리 무선 통신 장치는 쇼핑 센타, 의료 센타, 학교 등 건물을 중심으로 한 특정 지역에 다양한 기기 간에 실시간 네트워킹을 가능하게 함으로 각각의 기기들을 결합하거나 기능들을 수렴하는 방향으로 발전할 것이다. 즉 근거리 무선통신은 단순한 통신 및 인터페이스의 백본 역할을 넘어 복합장치 간에 'single device multi service'화하고 'location and role'의 기능까지 담당할 전망이다. 따라서 이동성은 무선, 유선 그리고 근거리 무선 통신 기술을 통하여 구체적으로 사물과 인간, 인간과 인간, 사물과 사물간의 네트워킹을 구현할 것이다.

결국 이와 같은 내재성과 이동성은 다양한 기반 기술들과 응용기술들의 조합을 통하여 조용한 기술환경, 지능형 공간 창출(intelligence space), 상황인식 기반 서비스(context awareness service), 사용자 중심 서비스 등을 이루어 낼 것이다. 전자무역에서도 무역 거래 당사자들이 지각하지 않아도 선적, 인도, 운송, 관련 서류, 비용 등에 대한 결정이 필요할 때 전자무역 거래 당사자들에게 인식할 수 있도록 배후에서 서비스를 하다가 필요할 때 서비스를 인지할 수 있도록 하는 상황인식 기반 서비스 등을 이용하여 새로운 부가가치 창출 및 비용절감 그리고 위험[3]을 줄일 수 있을 것으로 예상된다.

하게 개발되어 활용되고 있는 실정이다.

3) 기존의 무역 거래에서는 거래의 전 과정이 실시간으로 관련담당자에게 전달되지 못하거나 시차를 가짐으로 문제발생

3) 유비쿼터스 컴퓨팅의 응용 기술과 보안 위험

유비쿼터스 컴퓨팅 기술의 두 가지 커다란 특징인 내장성과 이동성이 구체적으로 구현될 기술들이 잠재적으로 보유한 응용 기술과 보안 위험을 살펴보면 다음과 같다.

오늘날 유비쿼터스 컴퓨팅의 가장 중대한 쟁점으로 프라이버시 문제가 제기되고 있다. 윤용민(2004)은 우리나라의 사회적 신뢰가 낮은 수준에 있기 때문에 유비쿼터스 컴퓨팅 시대를 맞이하여 심각한 혼란에 빠질 수 있음을 지적하였다. 이에 대한 예방으로 국가적으로 프라이버시 보호에 관한 획기적인 대책과 관련 법 제도 정비 그리고 PETs 개발에 적극 나서야 한다고 주장하였다[8]. 이호영·유지연(2004)은 RFID의 역기능으로 사생활 침해가 증대할 것이라고 주장하였으며 유비쿼터스 컴퓨팅 기술이 지구상의 네트워크 시스템을 하나로 연결시킴으로 위험이 대형화될 것이라고 주장하였다[9]. 또한 유비쿼터스 컴퓨팅 환경 하에서는 개인정보의 노출에 따른 프라이버시 침해 문제가 심각해질 것을 예견할 수 있다.

이와 같은 프라이버시 쟁점을 전자무역보안 분야에서 고찰해보면, 제품의 출고, 운송 등에 모든 과정을 추적하면 원산지 표시 등의 효과성 못지않게 사용자에 대한 프라이버시 침해 위협으로 상거래 등에 영향을 미칠 것으로 예상된다고 설명할 수 있다.[4] 위와 같은 일반적인 유비쿼터스 컴퓨팅 환경에서의 보안에 대한 위협이 구체적인 구현 환경 속에서는 어떠한 보안을 위협하는 공격 기술이 있는지 살펴보면 아래와 같다.

유비쿼터스 컴퓨팅 환경은 기존의 세부 연구 분야인 무선 인터넷, 무선 랜, 블루투스, 홈 네트워크 등의 기술을 통합한 융합 환경이다. 즉 유비쿼터스 컴퓨팅 환경은 무선 통신을 기본으로 기기들 간에 통신을 하게 된다. 따라서 유비쿼터스 컴퓨팅 환경에서 발생할 수 있는 위협으로는 장치의 절도 및 분실, IP 스푸핑(Spoofing), Dos(Denial of Service) 공격, Rogue AP, 트로이 목마, Worm, 바이러스, 신호방해 공격, 배터리 소진 공격 등에 취약 할 수 있다[10]. 이런 유형의 위협은 결국 데이터 보안이 취약할 경우 기존의 컴퓨팅 환경보다 심각한 문제를 발생시킬 수 있다는 점을 시사한다. 이는 물리공간에 가상공간이 침투되어 확대된 유비쿼터스 컴퓨팅 공간이 가지는 속성이 열린 공간이기 때문이기도 하다.[5] 또한 한번 수집된 데이터가 오·남용되어 원하지 않는 사람에게 전파되거나 이용될 경우, 사회 전체의 심각한 프라이버시 문제를 유발할 수 있다. 따라서 위험의 규모가 폭발적으로 증대되었으며 한번 유출

시 시의적절한 대응의 어려움, 원활한 커뮤니케이션의 어려움으로 인한 무역거래의 손실 발생 가능성 그리고 전 과정을 투명하게 상호 신뢰관계 속에서 진행할 수 없는 시스템적인 한계에 따른 위험이 있었다. 유비쿼터스 컴퓨팅 기술을 이용한 실시간 조회 및 이동 중인 물품의 상태 및 위치 조회 등이 RFID, 위성 등의 새로운 통신기술로 가능해졌으며 전 과정을 시스템화하여 배후서비스를 가능하게 한 후 의사결정권자의 인지가 필요한 사항에 시의적절한 서비스를 하게 함으로 거래 당사자 간의 시스템적인 신뢰 구축 등을 꾀할 수 있다. 하지만 개방형 시스템이 됨에 따른 해킹, 관련 정보의 유출 문제 등 보안의 문제는 광범위하게 증대할 것임을 알 수 있다.

4) 김현곤, “해외 유비쿼터스 추진현황 조사·분석”, 한국전산원, 2005년 3월. p. 58. 에서도 일본의 경우 1989년 이후 매년 프라이버시 침해가 증가했다고 생각하는 사람이 10%식 증가하였다고 밝히고 있다.

5) 다양한 기기간의 통신이 가능한 환경은 결국 다양한 기기와 사람으로부터 정보를 제공받고 서비스를 제공할 수 있는 열린 구조(open architecture)라는 뜻이다. 열린 구조는 원하지 않는 공격자로부터 실시간으로 다양한 기기를 통한 공격(해킹, 스푸닝, DOS공격, 바이러스 등)을 받을 수 있는 환경이란 뜻이다. 결국 위험이 증대된 공간이다.

된 디지털 정보는 유비쿼터스 컴퓨팅 공간에서 회수할 수 없기 때문에 더욱 큰 문제에 봉착할 것이다.[6] 이러한 문제는 유비쿼터스 컴퓨팅 환경으로 가는 발전에 심각한 걸림돌로 작용하고 있다. 또한 전자무역에 있어서도 전자무역을 담당하는 기업 그리고 전자무역을 통해 관련 상품 또는 서비스를 제공받을 고객에게 유비쿼터스 컴퓨팅 기술을 적용한 전자무역이 가지는 정보유출 등의 위협으로 전자무역의 활성화에 커다란 걸림돌로 작용할 것이다. 이와 같은 보안의 쟁점들에 관하여 전자무역 보안에 관한 연계을 통해 어떻게 해결되어져야 바람직할지에 대하여 고찰해보겠다.

Ⅲ. 전자무역 보안

1. 전자무역

전자무역이란 대외무역법 제2조 제6호에서 “무역의 일부 또는 전부가 컴퓨터 등 정보처리능력을 가진 장치에 의하여 정보통신망을 이용하여 이루어지는 거래를 말한다.”라고 정의하였다. 따라서 전자무역의 보안이란 정보통신망을 이용할 때 야기되는 노출된 위험으로 확장하여 파악할 수 있다. 또한 유비쿼터스 컴퓨팅 환경에서의 전자무역의 보안이란 단순히 노출된 위험의 수준을 넘어 전자적으로 거래되는 모든 무역 환경에서 노출된 위험에 대한 전방위적인 보안으로 확대·해석할 수 있다.[7]

전자무역에 있어서 정보보호분야를 학문적 영역으로 분류하자면, 고윤승·신황호(2001)는 전자무역을 4가지 연구범위(전자무역마케팅, 전자무역 결제, 전자무역 국제법규, 전자무역 정보시스템)로 설정하였다[11]. 연구 분석을 위한 접근방법으로 상관습 및 법리적 접근, 사례접근, 시뮬레이션 접근, 실증적 접근방법 제시하였으며, 전자무역보안은 사이버무역정보시스템 영역으로 포함하여 파악할 수 있을 것이다. 또한 이춘수·이장로(2002)는 전자무역의 학제적 연구의 중요성을 파악하고 인터넷무역의 주제별 분류에서 인터넷무역 이론 및 환경, 인터넷무역전략, 인터넷무역관리 그리고 기타로 크게 네 가지 주제범주를 설정하여 문헌 조사하였다[12]. 또한 보안 분야는 인터넷 무역 전략의 세부 주제범주의 무역정보시스템 영역으로 포함하여 분류하였다.

---

6) 오늘날 디지털 공간은 정보의 배포 비용은 저렴하다. 그러나 한번 배포되어 여러 사람의 컴퓨터 하드디스크, CD 등에 저장된 정보를 회수하는 비용은 배포비용과 비교할 수 없을 만치 높다. 따라서 한번 배포된 디지털 정보는 100% 완벽하게 회수하기가 어려운 것이 기술적인 특징이다. 현재 이와 같은 문제가 가장 첨예하게 문제로 부각된 분야로는 영화, 음악 등 컨텐츠에 대한 불법적인 사용이 많은 디지털 저작권 분야이다.

7) 과거의 무역은 물리공간에서의 위험이었다면 오늘날의 전자무역 보안이란 가상공간(인터넷)에서의 위험이 보안의 주요 대상이었다. 하지만 유비쿼터스 컴퓨팅 환경에서의 전자무역의 보안이란 물리공간 속에 스며든 가상공간이 확장시킨 유비쿼터스 공간에서의 위험을 보안의 주요 대상으로 한다. 따라서 보안의 범위가 전자적 거래와 RFID 칩 등을 통해 실시간으로 파악되는 상품의 무역거래 전체 가치 사슬 속에서의 위험으로 확대되었고 사료된다.

2. 전자무역 위협과 대응방안

전자무역에 있어서의 위험을 야기하는 보안 위협 요인으로는 크게 시스템 위협, 데이터 위협, 비즈니스 위협으로 파악될 수 있으며 자세히 살펴보면 다음과 같다.

1) 시스템 위협과 방안

유비쿼터스 컴퓨팅 기술로 긴밀하게 네트워킹 된 컴퓨터는 외부의 특정인이 이 시스템을 침입하여 부당하게 컴퓨터 시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위협이 있다. 일반적으로 이런 해킹위협을 방지하기 위해 방화벽과 침입탐지시스템(IDS)같은 시스템을 사용하기도 한다. 그러나 전자무역 거래는 불특정 다수인의 접근을 허용하는 개방 시스템으로서 방화벽을 사용하는데 있어서 제약을 받을 수도 있다. 특히 시스템의 불법사용은 내부자의 소행인 경우가 외부에서의 침입보다 많기 때문에 적절한 시스템의 운영지침과 내부 사용자에 의한 사회 공학(social engineering)적 공격에 대비한 보안교육이 중요한 요소가 된다.

이와 같은 전자무역에 활용되는 컴퓨터 시스템은 다양한 운영요소로 구성되어 있고, 결국 기업 컴퓨터 시스템의 기능장애를 초래하는 위험요소는 아래와 같이 세 가지로 살펴볼 수 있다.

첫째, 전통적·물리적 위험으로서 화재, 누수, 도난, 정전, 자연재해 등의 위험이 존재한다. 전자무역을 담당하는 컴퓨터 시스템 또는 네트워크가 설치된 건물이 화재, 자연재해, 누수[8], 정전 등으로 손상되거나, 서버 역할을 하는 컴퓨터가 도난[9]되는 경우에 전자무역을 담당하는 컴퓨터 시스템의 작동은 중단되고, 결국 기업은 막대한 손해를 입게 된다. 이러한 물리적 위험은 기업에 대하여 컴퓨터, 컴퓨터 시스템, 네트워크 장비에 대한 물리적 손해를 초래할 뿐만 아니라, 컴퓨터에 저장되어 있는 기업경영 관련 기본 데이터(재무기록, 인사기록 등), 고객정보, 전자무역 관련 서류 등의 상실로 인한 손해를 초래하게 된다.

둘째, 컴퓨터 시스템을 운용하는 소프트웨어의 결함, 프로그래밍 상 오류, 네트워크에 연결된 이기종의 컴퓨터와 소프트웨어간의 인터페이스와 프로토콜 등의 불일치로 인한 오류 등은 전자무역 거래를 담당하는 컴퓨터 시스템에 치명적인 영향을 초래한다. 기업 컴퓨터 시스템의 구성요소 중 하드웨어에 해당하는 컴퓨터에 대한 물리적 위험도 전체 시스템의 파괴를 초래하지만, 소프트웨어에 해당하는 소프트웨어의 결함, 프로그래밍 상의 오류도 전체 시스템에 치명적인 영향을 미친다. 특히 운영체제 등 전 세계적으로 알려진 보안 취약점이 발견될 경우, 빠른 소프트웨어적인 보안 패치파일 업데이트를 실

8) 2000년 9월 28일 발생하였던 D증권사의 전산사고는 대표적인 예를 제공한다. 즉 이 회사의 경우에 당시 일일 약정규모 3000 억 원의 75-80%가 사이버거래로 이루어지고 있었으나, 전산실의 누수에 의한 전산시스템의 파괴로 이 회사의 사이버거래는 이틀 동안 완전히 중단되었다.

9) 영국 보험자협회(Association of British Insurers)의 추산에 의하면 영국의 경우 매년 약 100,000대의 컴퓨터가 도난되고 컴퓨터 칩의 도난으로 인하여 매년 약 10억 파운드의 경제적 손실이 발생한다(C.C. Nicoll, “Insurance of e-commerce risks”, International Journal of Insurance Law, 1999년 10월, p. 295.)고 추정하였다.

시하지 않을 경우 주요 공격의 대상이 될 수 있다. 따라서 소프트웨어적인 결함뿐만 아니라, 오류 및 보안 미비점을 추가적으로 패치하거나 업데이트하는 소프트웨어의 관리도 중요한 요인으로 작용한다. 발견된 하드웨어에 해당하는 손상부분은 상대적으로 신속하게 수선이나 교체가 가능하지만, 기본적인 데이터나 소프트웨어는 복구에 상당한 시간을 요한다. 물론 복구에 소요되는 시간은 당연히 백업 시스템의 존재, 백업 시스템의 가동성 여부, 안전성 및 백업 시스템 간 상호작용에 요구되는 시간에 절대적으로 의존하게 된다[13].

셋째, 해킹, 바이러스, 스니핑, Dos공격 등 외부자의 공격은 주로 전자무역 거래에 필수적인 프로그램, 시스템운용과 관계되는 고객 정보와 물품 정보 등의 변경, 삭제, 파괴를 통하여 기업 컴퓨터 시스템에 치명적인 영향을 미친다. 도난이나 화재와 같은 물리적 위험의 경우 도난경보기나 연기탐지기의 설치로 인하여 어느 정도 위험을 통제하는 것이 가능하나, 해킹이나 바이러스[10] 등 외부자의 공격은 시스템 관리자의 입장에서 볼 때 가장 방어하기 어려운 위험이다. 왜냐하면 이 형태의 위험은 IT 기술 또는 전자상거래의 발전보다 더 신속하게 발전하여 왔으며, 현재도 진화하고 있기 때문이다.[11] 물론 시스템 관리자가 컴퓨터 시스템에 바이러스를 탐지하는 안티바이러스 프로그램을 설치하고 정기적으로 운용 및 업데이트하거나, 전문 보안업체에 의뢰하여 방화벽을 설치한다면 기술적으로는 어느 정도 외부자의 공격 위험을 회피할 수 있으나, 외부공격의 기법은 지금까지 개발된 시스템 보안기술 보다 항상 한발 앞서 발전하고 있다는 점을 감안하면 통제하기 어려운 위험이다. 또한 웜, 바이러스, 해킹 등으로 인한 직접적인 공격 외에도 스팸 릴레이, 피싱 경유지, 홈페이지 변조 등 컴퓨터 시스템 또는 소프트웨어의 자원을 잠식하거나 처리 속도를 현저하게 저하시키는 악성 프로그램에도 위험이 노출된 경우가 많다. 특히 전자무역 거래를 담당하는 시스템의 소프트웨어적인 다양한 위험의 노출은 기업의 전자무역 거래의 안전에 관한 신뢰도를 떨어트리고 거래에 있어서의 실제적인 비용 증가 등을 유발한다.

이와 같은 시스템 위협은 전자무역 거래에 있어서의 안정성을 보장하지 못하고 해킹 등을 통한 전자무역 시스템에 무단침입하여 정보의 위조와 변조, 손괴, 교란 그리고 개인정보 유출 등을 통한 사생활 침해 등을 야기할 수 있다.

2) 데이터 위협과 방안

전자무역에 있어서 데이터의 공격은 두 가지로 구분해 볼 수 있다.

---

10) 인터넷침해사고대응지원센터(www.krcert.or.kr)에서 발표한 해킹 및 바이러스 통계를 살펴보면 우리나라의 경우 웜과 바이러스의 경우 107,994건, 해킹사고처리의 경우 29,109건 등이 2004년도만에 집계되었으며 계속 증가하는 추세이다.

11) 최근 인터넷 사용자는 스파이웨어, 바이러스, 웜, 피싱 사기, 서비스거부 공격 등으로 곤란을 겪고 있는데, 최근에는 신종 공격수법인 '랜섬웨어'까지 등장하여 사용자를 더욱 곤란에 빠뜨리고 있다. '랜섬웨어'는 어린이를 납치(kidnap)한 후 보상금(ransom)을 요구하는 전통적인 범죄수법을 모방하고 있다. 즉, 랜섬웨어는 기존의 해킹이나 바이러스처럼 사용자 컴퓨터의 파일을 삭제·파괴하거나, 사용자의 ID를 도용하는 것이 아니라, 사용자의 중요한 파일을 열지 못하도록 만들고(kidnap), 이를 인질로 삼아 보상금(ransom)을 요구하는 신종 사이버범죄수법이다. 다시 말하자면, 사용자가 악성 코드가 포함된 웹 사이트에 접속하는 경우, 악성 코드는 사용자 컴퓨터에 담긴 약 15종의 데이터 파일을 암호화하고, 특정 주소로 전자메일을 보내야만 암호를 풀 수 있다는 메시지를 남긴다. 사용자가 전자메일을 발송하면, 특정 은행구좌로 소정의 금액을 송금하면 암호를 풀어 준다는 답장이 반송된다(야후 ITnews, 2005. 5. 25, http：//kr.blog.yahoo.com/everitnews).

첫째, 시스템 내에 저장된 데이터(내장성)에 대한 공격에 대한 위협이다.

둘째, 네트워크 상에 흘러 다니는 데이터(이동성)에 대한 공격이 있을 수 있다.

시스템에 저장된 데이터의 경우는 앞의 시스템 공격에서 언급하였으며 해결방안으로는 데이터를 시스템에 저장할 때 암호화를 하는 것이다. 네트워크 상에 흘러 다니는 데이터에 대한 공격을 막기 위해 기밀성, 무결성 등에 대한 인증이 필요하게 된다. 이를 위해서는 디지털 서명 메카니즘을 많이 이용하고 있다. 디지털 서명 메카니즘 중 가장 대표적인 것으로는 비대칭키(asymmetric) 암호화 기술과 해쉬 암호 등이 있다. 디지털 서명 메커니즘은 데이터의 무결성, 사용자의 인증(authentication), 부인 봉쇄(non-repudiation) 등의 서비스를 구현하는 역할을 한다.

3) Business 위협과 방안

앞에서 언급한 두 가지 공격은 모두 일반적인 컴퓨터 시스템의 보안침해와 동일하다. 그러나 전자무역에 있어서는 상거래라는 특징 때문에 발생하는 제 3의 공격이 있을 수 있다. 이것을 통칭해 비즈니스 공격이라 부른다[14]. 일반적인 상거래에만 일어날 수 있는 사기가 전자적 상거래에도 일어날 가능성이 있다. 이런 요소들을 전자적으로 막기 위한 보안 고려사항들이 추가적으로 필요하게 된다. 소프트웨어적인 암호와 하드웨어적인 시스템에 대한 기술만으로 모든 위협을 예방할 수 없기 때문에 제도적인 장치, 법적인 보장, 보험, 규범에 대한 교육 등의 전자시스템 외적인 보완도 동시에 이루어져야 한다[15]. 특히 전자무역의 위험을 최소화하는 보험을 통한 위험 분산 전략이 좋은 대응방안이다.

2. 전자무역보안 특징

전자상거래 실행상의 문제점으로 보안과 결제분야에 대한 유의점은 전자무역 분야에서도 기업측면에서 혹은 국가측면에서 확장하여 그 특징적 영역을 파악할 수 있다[16]. 전자무역은 기존의 무역방식과 비교하여 진행순서에는 별다른 차이가 없으나 업무처리 방법과 수단에서 종전에 비해 커다란 차이가 있다. 즉 기업은 전자우편, 인터넷, 전화 및 팩스 등을 활용하여 저렴한 비용으로 상담을 전개하고 수출계약을 체결할 수 있다. 아울러 상품주문이나 대금결제 등도 인터넷으로 할 수 있으며, 화물의 흐름도 RFID 등을 이용하여 실시간으로 파악할 수 있다. 또 기업은 인터넷상의 자사 홈페이지나 거래알선 사이트, 유즈넷, 메일링 리스트 등을 통해 자사제품과 서비스를 해외에 홍보하고 신제품이나 거래선 정보를 신속하게 입수할 수 있다[17]. 따라서 이러한 수단과 방법에 대한 전자적 보안 요소도 고려를 하여야 한다. 전자무역에서는 무역카드(trade card), 전자화폐 등을 통해 대금결제가 가능하게 되며, 화주는 화물운송과정을 인터넷상에서 직접 추적 또는 확인해 볼 수 있거나 이동전화 등으로 실시간으로 확인받을 수도 있다. 특히 현행 형법에서는 전자 화폐와 다양한 사이버 물체 등의 형법상의 재산개념을 포함시키지 못하고 있다. 따라서 현재로서는 법이 아닌 가상공간의 규약으로 보호해야해야하는

문제점이 있다[18].

이러한 전통적 무역과 전자무역 차이를 통한 기술적 보안 고려 요인을 [표-2]와 같이 정리하여 볼 수 있다. 즉 무역계약체결의 각 단계인 정보수집, 광고 마케팅, 의사교환, 대금결제, 운송, 사후관리 단계마다 전통무역과는 상이한 수단과 방법이 전자무역에 도입됨에 따라 전자무역의 각 특징들에 대한 보안고려 요소를 파악하고 이를 적극적으로 대처할 필요성이 있다.

[표-2] 전통무역과 전자무역의 비교에 따른 단계별 보안요인[19]

구분	전 통 무 역	전 자 무 역	보 안 요 인
정보 수집	거래알선기관, 직접방문, 해외전시회 참관 등	국내외 거래알선 사이트 등 전자 정보검색	네트워크 장애, 해킹
광고 · 마케팅	카달로그, 매체광고, 전시회, 상담회 참가 등	홈페이지 구축, 유즈넷, 메일링리스트, 무역알선사이트 등록, 사이버 전 전시회	웜 바이러스, 시스템 장애 등
의사 교환	국제전화, 팩스, 우편, 해외출장 등	전자우편, 인터넷 전화/팩스, 화상대화시스템 등	네트워크 장애, 웜 바이러스 등
대금 결제	신용장, D/A, D/P 등 (은행)	무역카드, 전자화폐, 전자자금이체 등	인증, 무결성 파괴 등
물류 운송	포워더, 해운, 항공운송	온라인 전송, 특급 운송 등	전자서류 위조 등
사후 관리	클레임과 중재, 소송 등	전자거래 약정 콜센터, DB 마케팅 등	인터넷사기행위, 법률위반 등

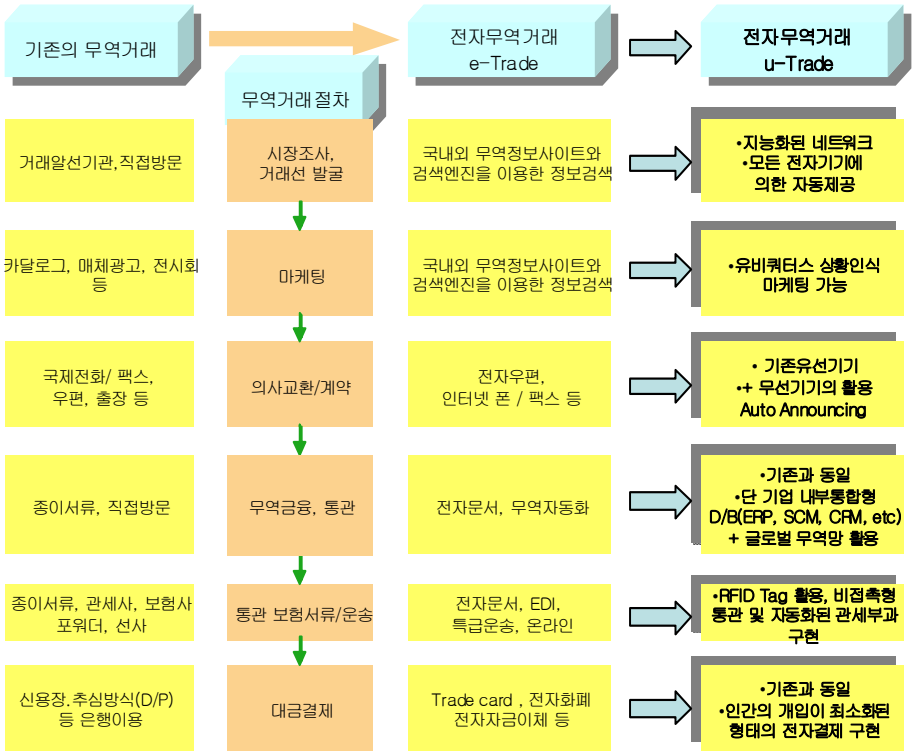
* : 현재는 전자무역 대금 결제 분야에 대한 보안 연구를 중심으로 연구가 활발히 진행되고 있다.

Ⅳ. 유비쿼터스 전자무역보안의 쟁점과 전략

1. 유비쿼터스 컴퓨팅과 전자무역보안

e-Trade에서 u-Trade로 패러다임이 변화되면서전자무역은 “거래선 발굴, 상담, 계약, 원자재 조달, 운송, 통관, 대금 결제에 이르는 제반 무역 업무를 인터넷 및 다양한 IT기술을 사용하여 시간과 공간의 제약 없이 처리하는 새로운 거래 형태”라고 설명되어 지고 있다. 따라서 급격히 진보하고 있는 무선통신환경과 스마트 정보기기 관련 IT기술의 활용은 필연적이라고 할 수 있다. <그림 2>는 유비쿼터스 컴퓨팅 기반하의 전자무역 변화 전망에 대하여 보여주고 있다.

<그림 2> 유비쿼터스 컴퓨팅 기반 하의 전자무역 변화 전망



기존의 전자무역(e-Trade)에 비해 유비쿼터스 컴퓨팅 기술이 접목된 전자무역(u-Trade)은 다음과 같은 특징이 있다.

첫째, u-Trade는 u-Commerce의 3대 요소인 모바일(mobile), 무선(wireless), 조용한 기술(silence)의 접목이 가능해 진다. 즉, 수단적 측면에서 e-trade는 유선 인터넷과 웹 기술을 활용하지만 u-Trade는 무선 인터넷과 웹 기술 그리고 증강현실을 연계하는 유비쿼터스 컴퓨팅 환경을 활용한다.

둘째, e-Trade는 사람들의 의식적인 컴퓨터 활용을 통해 상거래 활동이 이루어지지만 u-Trade는 사람들이 의식하지 않아도 자율 컴퓨팅 기능을 갖는 기기와 사물들에 의해 무의식적으로 상거래 활동이 발생하는 계기를 탄생시키고 이행하게 된다. 즉 지능화된 컴퓨팅 기술에 의해 상거래 활동의 전 활동이 고도의 지능화된 시스템으로 움직인다.

셋째, e-Trade가 주로 PC기반의 유선 네트워크를 기반으로 하는데 반해 u-Trade는 기본의 PC네트워크는 물론, 휴대폰, PDA나 휴대용 컴퓨터와 같은 다양한 유형의 차세대 휴대기기를 사용하고 이들 휴대기기의 네트워크를 기반으로 한다.

넷째, e-Trade의 정보화 영역은 주문, 결제와 같은 상거래 과정을 네트워크로 연결하고 이를 전자적으

로 처리하는 것에 국한된다. 그러나 u-Trade에서는 상품이나 그 상품과 연계된 물리적 생활공간 속의 사물과 기업의 비즈니스 공간에 존재하는 사물들까지 지능화, 네트워크화하는 것으로 정보화 영역이 확대될 뿐만 아니라 더 나아가 지능화된 새로운 유비쿼터스 공간 즉 u-Trade 공간의 창출이라는 새로운 공간이 구현된다. 따라서 e-Trade에서는 온라인으로 진행되는 상품거래과정과 오프라인에서 이루어지는 제조, 물류, 상품진열, 매장관리가 별도로 수행되지만, u-Trade 에서는 온라인과 오프라인을 모두 통합한 상거래 구현이 가능해짐에 따라 거래의 주문과 처리의 효율화가 실시간으로 구현할 수 있게 된다.

다섯째, 기존의 e-Trade에서는 사업영역이 아니었지만 u-Trade에서는 생활, 경제, 산업, 교통공간과 그 속의 사물, 기계, 상품 등 필요한 모든 것에 센서, 칩, 마이크로머신, RFID Tag 등이 삽입되고 이들이 유비쿼터스 네트워크로 연결됨으로써 과거에는 없었던 새로운 비즈니스들과 비즈니스 프로세스들의 혁신이 일어난다.

여섯째, e-Trade에서는 지식기반의 마케팅 활동이 주를 이루었지만, u-Trade에서는 고도화된 지능기반의 마케팅 활동이 주를 이룰 것이다. 즉 e-trade에서는 고객이 회원으로 가입할 때 입력한 DB의 컴파일링을 통한 마케팅 활동이 주가 되었지만, u-Trade에서는 보이지 않는 기기와 사물 속에 내장된 단말기기와 사물에 식재된 센서, 칩, 태그, 라벨이 고객의 상황정보는 물론이고 상품의 상황정보도 언제어디서나 실시간, 연속적으로 인식, 추적, 의사소통이 가능하도록 하여 고객의 요구를 예측하고 추적하여 발굴하는 지능화된 마케팅이 가능하다. 마케팅 자원과 활용에서 단순한 DB조합과 컴파일링의 수준을 넘어 수요와 공급을 예측하고 패턴을 추출할 수 있는 지능화된 마케팅 활동이 주를 이룰 전망이다.

일곱째, e-Trade에서는 상거래에 관여하는 몇몇 전문가 그룹 또는 업자들에 한정된 상거래활동이었지만, u-Trade에서는 실시간 글로벌 유비쿼터스 네트워크 환경으로 일반 소비자, 상거래 전문가 그룹, 유통업자 등 상거래에 관련된 전 구성원이 상황을 추적하고 관여하는 환경으로 바뀜으로 상거래 참여자가 늘어날 것이다.

이와 같은 7가지 특징들은 앞에서 언급한 유비쿼터스 컴퓨팅의 일반적인 속성들과 연관이 깊으며, 유비쿼터스 기술 관점에서의 내재성과 이동성이 구체적인 서비스로 구현될 때 나타날 수 있는 함축된 특징들이다.

2. 유비쿼터스 컴퓨팅 환경 하에서의 전자무역보안 쟁점

새로운 유비쿼터스 컴퓨팅 환경에서 야기되는 전자무역 보안의 쟁점이 무엇이고 이러한 쟁점을 효과적으로 관리할 전략이 무엇인지를 고찰해보면 다음과 같다.

1) RFID와 전자무역 보안

u-Trade환경에서는 RFID(radio frequency ID) 기술 적용에 따른 보안의 문제가 심각히 제기되고 있다.

RFID 시스템은 그 편리함에도 불구하고 개인정보나 보안에 대해 취약하기 때문이다.

우선, RFID의 특징을 정리하면 아래와 같다.

첫째, 데이터의 송신과 수신이 가능하다는 점이다.

둘째, 비활동성(passive)태그는 전지 없이도 작동한다는 점이다.

셋째, 전지가 내장된 경우에는 스스로 전파를 발생시키는 활동성(active)태그가 된다는 점이다.

넷째, 얇고 작게 만들어 물건의 속에 집어넣을 수 있다는 점이다.

다섯째, ID정보를 읽기만 할 수 있는 저가형에서부터 각종 데이터를 읽고 쓸 수도 있으며 암호화 모듈 및 연산 작동이 가능한 보안 시스템을 포함시킬 수 있는 고기능 제품까지 다양하다는 점 등이다. 또한 RF방식을 이용하는 ID(RFID)에 대한 논의가 최근 급속히 확산되는 배경에도 저가형에서 고가형에 이르는 다양한 응용 시제품이 가능하기 때문이다. 특히 기존의 bar code에 비하여 신축적인 정보의 저장이 가능하고 history의 context 수용이 용이하다는 점에서 유비쿼터스 컴퓨팅 환경에서 각광받고 있다. 그러나 RFID에 저장된 정보를 누구든지 확인 가능하다는 취약점이 있다.

기존의 자동인식 시스템으로 바코드, 광학문자판독(OCR) 등이 있으나, RFID기술은 무선정보처리의 대량 공급이 가능한 새로운 기술, 비접촉식 인식 방법, 인식 거리, 인식 속도, 데이터 저장능력과 고객정보 수집 및 분석 등에서 정보를 보다 빠르고 효과적으로 기업에 전달할 수 있어 전자무역에서도 혁신적인 자동인식 시스템이 될 전망이다. 특히 유비쿼터스 컴퓨팅 기술을 접목하면 새로운 어플리케이션 서비스도 다양하게 구현할 수 있을 전망이다. 특히, 전자무역에 있어서는 컨테이너 등의 유통, 물류, 교통 등에서 운송과 요금징수 등과 같은 분야와 상품이나 물건의 이동 경로 추적 등에 활용하여 경비를 줄이고 부가가치를 창출할 수 있다.

그러나 RFID기술에 대한 문제점으로 다음과 같은 것들이 있다.

첫째, 소형화, 내재화, 자동 인식 기술 등 편리한 기능이 많지만, 데이터의 저장 용량이 낮고 OTP(one time programming)로 태그를 프로그래밍하여 데이터의 수정이 불가능하다는 단점을 가지고 있다.

둘째, 현재 RFID를 이용한 시스템을 운영하는 부분 내에서만 활용되는 폐쇄형 시스템으로 타 시스템과 호환되는 개방형 시스템이 되기 위해서는 까다로운 보안 요구 사항과 이기종간의 호환의 문제를 해결하여야한다. 특히 전자무역은 무역업자 등의 자유로운 접근과 서비스 요청 등이 가능한 개방 시스템이다. 따라서 현재의 RFID 시스템 운영을 개방시스템으로 전환할 때 금융거래와 운송과 물품 상태를 실시간으로 확인할 수 있는 장점 못지않게 보안의 요구 사항을 높여야 전자무역의 효과를 극대화할 수 있다.

셋째, 물리적 충격에 의한 RFID칩의 파괴에 대한 보안이 요구되어진다. 더불어 칩의 오동작에 따른 손해배상 문제 이슈가 제기될 수 있으며 칩을 바꿔치기하거나 복제를 통한 사기문제가 발생할 수 있다. 또한 RFID의 전자파는 전파의 특성상 금속물질, 일부 액체 및 물체 표면의 성격에 따라 인식률의 차이를 보일 수 있어 정보의 왜곡이 가능하다.

또한 유비쿼터스 컴퓨팅 환경에서는 정보보안 기술이 요구되어지는데 태그에 저장된 정보가 허가되

지 않은 리더기에 노출되지 않는 기술적 솔루션이 필요하며 태그와 태그 소유자 사이 장기간 유지되는 추적 관련 정보를 만드는 것 등으로부터 안전하지 않은 채널이 가정되어 있다면 암호화 기법으로 보호되어야 한다. 접근제어 메커니즘을 제공하는 것 이외에 태그와 리더 사이의 상호인증이 가능하도록 하여 태그와 리더 사이에 신뢰할 수 있는 기술적 기반을 마련하여야 한다. 이를 통해 리더와 리더기 사이의 세션 가로채기(hijacking), 재생(replay)공격, 중간자 공격(man in the middle attack)에 대해 안전할 수 있는 유비쿼터스 컴퓨팅 환경 하에서의 전자무역 방안이 구축되어야 한다.

2) 전자무역보안과 개인정보보호

오늘날 정보통신기술이 발전함에 따라서 방대한 양의 정보가 용이하게 수집·저장·교환되고 있는 반면, 기업이 전자상거래와 관련하여 고객에 대하여 개인정보(예를 들면, 개인 신상, 개인 신용 및 개인의 구매습관 등에 관한 정보)를 제출하도록 요구함으로써, 그러한 정보의 유출·오용·남용·악용에 의한 프라이버시 침해는 심각한 사회문제로 대두되고 있다. 미국의 한 조사에 의하면, 인터넷 이용자 중 81%가 온라인에서 개인 프라이버시에 대한 침해를 우려하고 있고, 우리나라의 경우에도 인터넷을 통한 전자상거래의 기피사유로서 개인 및 신용정보의 유출에 대한 우려가 두 번째 순위를 차지하는 것으로 나타났다.[12)]

피보험자가 전자상거래를 수행하는 과정에서 자기의 부주의 또는 시스템보안 상의 문제에 기인하여 법적으로 보호되어야 할 개인정보를 유출하거나 개인 프라이버시를 침해한 경우에는 불법행위에 해당하고, 개인정보의 수집목적이나 이용방법의 사유가 위법인 경우에는 민사상 손해배상청구의 대상이 된다.

3. 유비쿼터스 컴퓨팅환경 하에서의 전자무역의 담보 가능 범위

유비쿼터스 컴퓨팅 환경 하에서는 전자무역의 위협이 개방형 시스템으로 바뀜에 따라 크게 증가할 것이다. 이를 해결하기 위한 방안으로서는 기존의 인터넷을 이용한 전자무역에서의 시스템 위협, 소프트웨어적인 위협 그리고 비즈니스 위협에 대한 대응방안을 고려해 볼 수 있을 것이다. 본 소고에서는 신건훈(2005)의 전자상거래하의 보험쟁점에 대한 논의를 중심으로 기존의 해결방안 외에 제도적인 해결방안으로 전자무역 거래에 있어서의 보험에 대하여 요약정리 한다. 특히 보험의 대상이 될 수 있는 전자무역보안부분에서 컴퓨터 시스템의 하드웨어적인 손실에 대한 보험, 소프트웨어 및 하드웨어의 파괴에 따른 간접비용 발생 부분에 대한 보험 그리고 불법행위에 따른 민사 및 형사상의 책임에 따른 문제에 대하여 살펴본다. 이는 유비쿼터스 컴퓨팅 환경 하에서 야기될 수 있는 다양한 이슈들 중에서 오늘날 보험 환경 하에서 고려해 볼 수 있는 보호 가능한 보험의 대상이다.

---

12) 정영화·남인석, 『전자상거래법』, 다산출판사, 2000, p.212.

1) 컴퓨터 시스템의 기능상실

컴퓨터 시스템의 장애로 인한 전자무역에서의 비용손해는 본인손해담보 하에서 보상될 수 있다. 다만 화재나 도난과 같은 물리적 위험은 전자무역의 정상적인 무역거래에서 발생하는 고유한 위험의 범주에서 벗어나는 전통적인 위험으로서 전통적인 보험에 의하여 보호될 수 있다. 즉 화재나 도난의 경우, 화재보험이나 도난보험에 의하여 보호되거나 기업재산보험에 의하여 보호된다. 한편 기업의 입장에서 물리적 위험에 부수하는 업무장애 위험을 최소화하기 위해서는 기업의 물리적 영업장소 외부의 안전한 장소에 백업 시스템을 구축해 두거나, 위험의 분산을 위하여 중요한 네트워크 구성요소를 물리적으로 상이한 공간에 설치해 두는 것이 바람직하다. 최근에는 어플리케이션 서버, DB서버, 백업장치를 물리적으로 다른 곳에 배치함으로 화재, 도난, 누수 등의 위험을 분산하고 있지만 물리적 공간을 따로 확보함에 따른 추가 비용이 발생하는 단점이 있다.

한편 소프트웨어의 결함 또는 컴퓨터 프로그램의 오류에 기인한 기업 컴퓨터 시스템의 기능상실 또는 기능저하에 의한 전자무역거래에서의 손해는 일반적으로 본인손해담보 하에서 보상되지 않는다. 본인손해담보 하에서 제외되는 기업의 비용손해를 구체적으로 열거하면 다음과 같다[20]. 첫째, 정부기관 등 공권력의 행사에 의한 보험목적물의 징발, 몰수, 국유화 또는 파괴되어 피보험자에게 직·간접적으로 손해를 유발한 경울 둘째, 컴퓨터 시스템의 일상적인 마모 또는 점진적인 성능저하의 결과 발생한 손해 셋째, 인공위성의 고장으로 인한 손해 넷째, 전기시설, 데이터 송신라인 또는 사회간접자본의 고장으로 인하여 초래되는 전력차단, 불안정한 전력의 흐름 등으로 인하여 초래된 손해 다섯째, 소프트웨어 또는 프로그램의 사용불능 또는 성능의 결함으로 인하여 초래된 손해 여섯째, 퇴사한 종업원이 컴퓨터 시스템에 대하여 무단으로 접속한 결과 발생한 영업비밀의 노출에 따른 손해이다.

위와 같은 경우 중 영업비밀보호법에 의해 퇴사한 종업원이 영업에 중대한 정보를 악용할 경우 법적 대응을 할 수 있으며 기타 다른 법률적 및 제도적 보안 대책으로 위험을 최소화할 수 있다.

2) 영업장애로 인한 간접비용

전자무역을 담당하는 기업은 건물, 기계 등 자산을 보유하고 종업원에 대한 급여 , 영업비용 등을 지출하는 전 과정에서 기업의 영리활동을 추구한다. 물론 전자무역을 위한 단순한 오파상과 같은 중계업무를 담당하는 업체도 있으나 공급사슬과 소비사슬의 부가가치망을 하나로 통합하여 기업의 비용을 줄이고 이익을 극대화하는 전략을 유비쿼터스 컴퓨팅 환경 하에서 추구할 것으로 예측할 때 전자무역을 담당하는 기업은 오늘날 단순한 종합상사 수준에서 제품 생산과 납품에 이르는 전과정을 수직적으로 통합한 기업이 경쟁우위를 가질 것으로 예상된다. 기업의 영리활동은 물적 재산의 직접손해에 기인하여 위축되거나 중단되기도 하지만, 직접손해에 후속하여 발생하는 영업이익의 상실이나 추가경비 등의 간접손해에 의해서도 기업의 영리활동은 상당한 영향을 받는다. 일반적으로 기업의 물적 재산은 재산보험이나 기업종합보험에 의하여 보호되지만, 기업의 영업능력은 이들 보험에 의하여 보호되지 않는

다. 예를 들면 화재로 인한 기업의 물적 손해는 화재보험에서 담보되지만, 화재로 인한 영업이익의 상실분이나 추가경비 등 간접손해는 일반적으로 업무장애보험이나 간접손해보험[13] 하에서 담보된다. 업무장애보험에서 보험금은 업무중단기간동안의 영업이익의 상실분에 영업비용을 더하여 산정하고, 추가로 피해복구를 위하여 피보험자가 지출한 추가비용도 보험금에 산입된다.

전자무역 보험 하에서 보상되는 간접 비용 손해는 컴퓨터 시스템의 손상이나 파괴에 후속하여 발생되는 영업이익의 상실, 복구비용 및 데이터 재수집·재입력에 소요되는 비용이다. 이러한 비용은 배상책임담보 하에서는 담보되지 않고, 전자무역종합보험 하에서 피보험자의 선택에 의하여 본인손해에 대한 추가담보로서 본인손해담보와 함께 구매가 가능하다. 영업중단으로 인한 간접손해는 주로 시간요소에 기인한 유형의 비용에 의하여 산정된다. 따라서 손해산정 시에 시스템의 교체기간 중 발생한 수익의 상실, 시스템의 재설정 시간, 상실된 데이터의 복구 시간, 데이터의 재수집·재입력 시간, 사고조사 시간이 중요한 요인으로 고려된다.

결국 당해 담보주제 하에서 영업중단기간 중 피보험자에 대하여 발생하는 무형의 손해, 즉 영업중단으로 인한 기업의 명성이나 신뢰도의 하락으로 인한 손해, 기업의 이미지를 제고하기 위하여 지출하는 이미지광고비용 등은 담보되지 않는다.

3) 불법행위책임

전자무역에 종사하는 기업 또는 컴퓨터 시스템의 관리자는 본인의 고의나 과실에 기인하여 타인 또는 여타 기업에 대하여 손해를 초래하는 경우, 민·형사상 법적 책임을 면할 수 없게 된다. 전자무역보험에서 담보되는 법적 책임은 민사상 불법행위에 기하여 초래된 타인에 대한 손해배상책임으로서, 피보험자가 현행 법률을 위반함으로써 초래되는 형사상 징벌적 성격의 형사처벌, 벌금 또는 피보험자가 피해자에게 위로금 성격으로 제공하는 금전 등은 보상의 대상이 되지 못한다.

한편 전자무역 또는 인터넷활동과 관련하여 기업이 민사상 불법행위책임, 즉 피해당사자에 대하여 손해배상책임을 부담하는 경우, 그러한 책임은 일반적으로 전자상거래종합보험의 제3자에 대한 책임담보(third-party liability coverage) 또는 별도의 사이버배상책임보험(cyber liability insurance) 하에서 담보된다. 다만 보험원칙의 문제로서 불법행위책임의 유형에 상관없이 당해 불법행위가 피보험자의 과실, 즉 실수, 착오, 오류 등에 의하여 행하여진 경우에 한하여 담보가 제공된다. 따라서 당해 불법행위가 피보험자의 고의적 또는 악의적 의사에 의하여 행하여진 경우, 보험자는 면책이다. 그리고 이 담보주제와 관련하여 유의할 사항은 다음과 같은 것들을 지적할 수 있다.

첫째, 태만 또는 주의의무 위반과 관련하여 담보범위는 피보험자와 '거래하는 자' 또는 '거래를 위하

13) 일체의 간접손해, 즉 시장상실이나 계약체결기회의 상실로 인한 손해도 담보가능하지만, 영업이익의 상실분이나 추가경비가 표준적인 담보영역이므로 이 보험을 이익상실보험(loss of profit insurance)이라고도 한다(Nicholas Legal-Jones(ed.), *MacGillivray on Insurance Law*, 9th ed., Sweet & Maxwell, 1997, p.856 ; D.S. Hansell, *Introduction to Insurance(2nd ed.)*, LLP, 1999, p.57 참조).

여' 피보험자가 구축한 웹 사이트에 접속하는 자에 한정한다는 점이다. 여기서 피보험자와 '거래하는(doing business) 자'의 개념이 문제가 될 수 있다. 만약 소비자가 거래와 관련한 문의를 하고 이에 대한 회신목적으로 전송된 이메일을 통하여 바이러스가 전송된 경우라면 그러한 문의 자체로서 '거래'라고는 하기 어렵고, 영리추구를 목적으로 하지 않는 자선단체의 활동에 '영업상'이란 개념이 적용될 여지는 없을 것이다.[14]

둘째, 전자무역 기업, 온라인 중개인 또는 온라인 전문직상담자에 의한 태만한 부실표시에 대한 배상책임은 일반적으로 전통적인 전문직배상책임보험 하에서 담보되는 위험으로서, 전자상거래 보험 하에서는 담보되지 않는다.

셋째, 불법행위책임 담보와 관련하여 가장 중요한 예외로서, 피보험자의 특허권 침해행위와 관련한 일체의 배상책임은 전자상거래 보험 하에서 담보되지 않는다. 이 면책은 보험증권의 형식 또는 발행국가를 불문하고 명시적으로 면책으로 규정하고 있다.

이와 같은 전자무역에 대한 구체적인 보험을 통해 위험을 극소화하고 유비쿼터스 컴퓨팅 환경을 최대한 활용한 개방형 네트워킹 구조로 전환한다면 기업의 부가가치는 상승할 것으로 기대된다.

V. 결 론

유비쿼터스 컴퓨팅 환경은 전자무역에 필연적인 영향을 미칠 것으로 예견되며, 이를 활용할 경우 비용절감 및 시간단축 등 상당한 효율성 제고가 될 수 있을 것으로 기대된다. 그러나 이러한 유비쿼터스 환경의 도래에 따라 전자 무역의 관점에서 다음과 같은 문제점을 요약해보고 함께 지적하고 전략들을 제시해 볼 수 있다.

첫째, 유비쿼터스 관련 기술의 활용에 따른 경쟁력 제고의 측면이다. 즉 아직 기술 도입기인 유비쿼터스 최신 기술들이 항만, 교통, 산업, 전자정부, 시민 생활 등을 컴퓨터의 접속망으로 묶어 종합적인 유비쿼터스화에 따른 시너지를 얻을 수 있도록 전방위적인 노력이 필요하며 시스템의 표준과 인프라가 갖춘 연후에 효과가 극대화될 것이기 때문이다. 특히 유비쿼터스화란 거점도시를 중심으로 확대, 발전시키는 전략이 유효할 것으로 예상되므로 부산 등 주요 항만도시에 항만시스템을 도시 전체의 유비쿼터스화에 포함시켜 비용을 낮춤으로 전략적인 우위를 점할 수 있어야 한다.

둘째, 전자 무역 프로세스의 재정립이 필요하다. 최근 정부는 21세기 무역 강국으로 부상하기 위한 정책의 일환으로 '무역업무 BPR/ISP'를 추진하고 있다. 이러한 사업은 매우 시의적절하며 이러한 사업이 성공적으로 수행되었을 경우 높은 성과를 나타낼 것으로 기대된다. 다만, 이러한 사업을 수행하는 과정에서 유비쿼터스 환경의 도래라는 측면을 고려한 프로세스를 정립시킬 경우 보다 높은 수준의 성

14) C.C. Nicoll, *op. cit.*, p.301.

과를 나타낼 수 있을 것이다. 특히, 물류/유통 부분에서 선적/수령에서 파레트 또는 컨테이너와 각 상품에 RFID를 부착하여 비용을 절감하고 배송정보를 제공할 수 있다. 따라서 RFID기술 도입에 따른 선적 과정의 단축 및 포장 시간을 단축함에 따른 무역 프로세스에 대한 재정립이 필요하다[20].

셋째 프라이버시에 관한 문제이다. 만일 RFID 태그(Tag)가 부착된 제품의 경우 모든 Historical Data가 축적되기 때문에 RFID의 보안상의 취약점이 사회적으로 문제가 될 수밖에 없음을 중요시해야 한다.[21] 이와 같은 RFID의 문제점을 기술적으로 해결하기 위한 방안으로는 Faraday Cage, Active Jamming, 'Kill' Tag, Blocker Tag, Silent Tree-walking, Hash-Lock Access Control, Re-Encryption, On-Time Pad 등이 있다.

따라서 우리나라에서도 이와 유사한 수준의 관련 법규 내지는 '지침'이 필요하다고 판단되며 기존의 "정보통신망이용촉진및정보보호에관한법률"과 "공공기관의개인정보보호에관한법률"은 유비쿼터스 환경이 고려되지 않은 형태로 입법되었기 때문에 이들 법률의 개정 내지 보완입법이 필요하다고 판단된다. 부차적으로 이러한 법제가 미비한 상태에서 유비쿼터스 환경이 본격화 될 경우, 우리나라의 제품이 미국 일본 등 국가에 판매될 경우 해당국의 법률에 대한 저촉문제가 제기될 수 있기 때문이다. 이에 대비해 개인 정보보호를 위한 법과 제도의 제정과 더불어 이를 뒷받침할 수 있는 관련 정보보호 기술 개발을 동시에 추진할 필요가 있다. 기본적으로 프라이버시와 관련된 RFID의 위변조, 복제, 도청과 불법 태그 및 리더 공격으로부터 안정성을 제공할 수 있도록 접근 제어, 태그와 리더간 상호 인증, 디지털 ID기반 권한 관리, 초경량저전력 암호 등 RFID에 적합한 보안 기술들을 개발할 필요가 있다. 나아가 안전한 RFIS/USN 보안 인프라를 설계, 구축해 네트워크에서 유통되는 개인정보보호, 위치정보보호, 추적방지, 네트워크안정성, 서비스의 안전성 등을 제공할 수 있어야 한다. 특히 이들 분야는 비교적 선진제국과의 기술격차가 크지 않다는 점을 고려한다면 관련 산업의 발전을 통하여 유비쿼터스 환경 하에서 국내 관련 산업의 보호와 함께 또 다른 수출 동력으로 글로벌 경쟁력 수단이 될 수 있을 것이다.

본 소고에서는 유비쿼터스 컴퓨팅 환경 하에서 전자무역기업이 기존에 인터넷 환경에서 가지고 있는 위협을 최소화하는 방안에 보험이라는 제도적 방안을 통해 위험을 최소화시키는 것을 전략적으로 제안하였다. 이는 유비쿼터스 컴퓨팅 환경이 기존의 폐쇄형 환경이 아닌 개방형 환경으로 전환됨에 따른 위험의 증대와 다양한 공격 방법과 기기에 노출되기 쉬운 환경이기 때문이다. 그러나 유비쿼터스 컴퓨팅 환경을 전자무역기업이 전사적으로 활용하여 기업의 경쟁력을 제고해야함은 피할 수 없는 선결과제이다. 따라서 전자무역기업은 기존의 부가가치사슬을 유비쿼터스 컴퓨팅 기술을 최대한 활용하여 생산, 운송, 판매, 소비자 피드백 등의 전 과정을 수직적으로 통합하는 기술적 인프라로 활용하여 기업의 비용을 최소화하고 이윤을 극대화하여야 한다. 또한 이러한 새로운 기술적용에 따른 위험을 관련 법규, 표준의 빠른 채택 등을 시행하여 국가에서 빠른 유비쿼터스 컴퓨팅 전자무역 환경으로 만들어주어야 한다. 그리고 기업은 다양한 담보범위를 제공하는 보험 상품의 개발 등을 통해 새로운 기술적용에 따른 위험을 최소화하여야 할 것이다. 본 소고에는 장래에 유비쿼터스 컴퓨팅 환경 하에서 기업에 노출된 위협을 최소화하여 경쟁력을 극대화할 수 있는 전략을 제시하고 이와 같은 기업의 전사

적 노력 속에 제기될 수 있는 쟁점을 분석해봄으로 시사성 있는 연구를 진행한 것에 그 의의가 있다고 사료된다. 마지막으로 본 연구의 한계점으로 유비쿼터스 컴퓨팅환경 하에서의 전자무역보안에 대한 쟁점과 전략에 대에 대하여 탐색적 연구를 통한 새로운 연구 아이디어와 시사점을 도출하기 위한 학제간 연구를 시도한 의의는 있으나 좀 더 구체적이고 세부적인 대응전략의 제시가 미흡하다. 따라서 향후 연구에서는 실제적인 실증분석을 위해 전자무역에서의 보안과 위험에 대한 결정요인이 무엇인지 통계적 분석방법을 분석하여 이에 대한 적절한 대응전략을 개발하는 것도 중요할 것으로 생각된다.

참 고 문 헌

[1] 윤용근·정병주, “유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형 분석”, 「정보화 정책 이슈」, 한국전산원, 제4권 제7호, 2004년 6월, p. 4.

[2] 김용수, “유비쿼터스 기술의 확장과 서비스”, 「IT Review」, 삼성SDS, 2003년 4월, p. 3.

[3] 류영달, “유비쿼터스 사회의 발전단계와 특성”, 「NCA CIO REPORT」, 한국전산원, 2004년 12월, p. 7.

[4] 하원규, 박상현, 연승준, “주요국의 유비쿼터스 IT 정책 동향과 한국의 SWOT 분석”, 「유비쿼터스 IT 전략 연구 시리즈」, 한국전자통신연구원, 제4권 제1호, 2004년 6월.

[5] 강홍렬, “유비쿼터스 논의에서 읽는 IT의 기술혁신 방향”, 「KISDI 이슈리포트」, 정보통신정책연구원, 제4권 제26호, 2004년 10월, pp. 38-159.

[6] 김완석·김정국, “유비쿼터스 컴퓨팅의 발전 전망과 보안에 대한 이슈”, 한국정보보호학회, 정보보호학회지, 제14권 제1호, 2004년 2월, p. 4. [표 1] 인용.

[7] 신명기·김용진·박치항, “차세대 인터넷을 위한 국내 IPv6 진화 방안에 관한 연구”, 한국정보처리학회, 한국정보처리학회 논문지, 제7권 제11호, 2000년 11월, p. 3614.

[8] 윤영민, “U-컴퓨팅의 사회문화적 수용 : 프라이버시 보호 관점에서 본 전망과 대책”, 한국정보보호학회, 정보보호학회지, 제14편 제1호, 2004년 6월, p. 56.

[9] 이호영·유지연, “유비쿼터스 통신환경의 사회문화적 영향연구”, 「연구보고서」, 정보통신정책연구원, 제4권 제5호, 2004년 12월, pp. 123-127.

[10] 조명섭·조상래·유인태·진승헌·정교일, “유비쿼터스 컴퓨팅의 보안요구사항 분석”, 한국정보처리학회, 한국정보보호학회지, 제14권 제1호, 2004년 2월, pp. 22-29.

[11] 고윤승·신황호, “전자무역의 연구범위와 연구방법에 관한 고찰”, 한국무역학회, 무역학회지, 제26권 제4호, 2001년 9월, pp. 75-97.

[12] 이춘수·이장로, “한국인터넷무역 논문의 분류와 분석”, 한국통상정보학회, 통상정보연구, 제4권 제1호, 2002년 6월, pp.149-172

[13] 박석재·신건훈, “전자상거래 보험의 문제점과 해결방안”, 한국무역학회, 무역학회지, 제26권 제4호, 2001년 9월, p. 154.

[14] 김홍근·최영철, “전자상거래 경쟁력 강화와 정보보호기술 개발 전략”, 한국정보보호진흥원, 2004년 1월.

[15] 류종현·강장묵, “사이버세계의 眞과 善”, 21세기 출판사, 2005년 1월, p. 78.

[16] 이정호, “전자거래의 확산에 따른 기업의 대응 방안에 관한 연구”, 한국국제상학회, 국제상학, 제15권 제1호, 2000년 6월, p. 436.

[17] 이승영·문희철·심상렬, “인터넷 전자무역 창업에 관한 연구”, 한국무역학회, 무역학회지, 제24권 제1호, 1999년 10월, p. 212.

[18] 이정원, “가상고간에서의 Cyber물체에 대한 침해행위와 형법적 평가”, 중앙법학회, 중앙법학학회지, 제6권 제1호, 2003년 2월, p. 139.

[19] 정조남·이춘수·강장묵, “전자무역보안과 전략적 대응방안에 대한 소고”, 한국정보처리학회, 정보처리학회논문지 C, 제11권 제5호, 2004년 10월, p. 580.

[20] 신건훈, “전자상거래 보험의 쟁점에 관한 고찰”, 한국무역학회, 2005 무역학자 전국대회 발표논문지, 2005년 8월, p 13.

[21] 이은곤, “RFID 확산 추진 현황 및 전망”, 정보통신정책연구원, 정보통신정책, 제16권 제6호, 2004년 4월, p. 18.

[22] 강전일·박주성·양대헌, *“RFID 시스템에서의 프라이버시 보호기술”*, 한국정보보호학회, 정보보호학회지, 제14권 제6호, 2004년 12월, p. 31.