□특집□

전자상거래 정보보호기술 현황 및 대응방안

김 홍 근† 최 영 철††

◈ 목 차 ◈

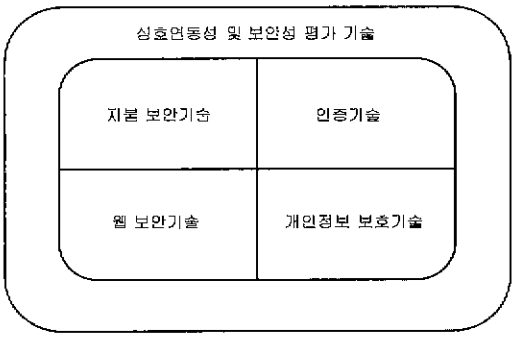
1. 서 론

지구촌 곳곳에서 전개되고 있는 무한 경쟁의 현장이 인터넷 전자공간으로 옮아가고 있다. 인터넷의 무한한 이용 가능성 중에서 상업적으로 적용된 것이 바로 전자상거래이다. 전자상거래는 현실 속의 시장이 갖는 시간과 공간의 제약을 뛰어넘어 더 많은 고객을 확보하는 새로운 이윤 창출의 수단으로 그 가치가 더욱 높아질 것으로 보인다. 그러나 인터넷 본래의 무질서와 함께 신기술의 시험장으로 또는 표준의 각축장으로 인터넷이 만들어내는 전자공간은 마치 서부 개척시대를 연상시키는 혼란과 무질서가 가중되고 있다. 국내외적으로 참가자가 증가 일로에 있는 전자공간에서의 상거래도 글로벌한 질서를 갖기에는 많은 시간과 노력이 요구된다 하겠다. 현재 벌어지는 전자상거래 양상은 누가 먼저 깃발을 꽂느냐 식의 경쟁의 열기로 가득하다. 각자 자국과 자사의 이익을 극대화하려는 관점에서만 접근하고 있다. 이용자의 권리를 확보하고 대변하려는 일부 공익단체나 국가의 노력이 있기는 하나 역부족이다. 우리나라도 정부 정책 담당자로부터 기업 운영자까지 전자상거래라는 게임의 깃발 아래 동참해야 한다고 소리높여 외치고 있다. 그러나 과연 전자상거래로의 진입이 우리나라의 국가적 이익에 얼마나 부합되고 있는지 냉정하게 반문해볼 필요가 있다. 이 새로운 무한 경쟁에서 살아남기 위해 국가·사회·기업이 어떤 전략을 세워야 하는지 숙고해야 한다. 본 글에서는 B-to-C 인터넷 전자상거래의 전개에 있어 정보보호 분야에서의 기술 현황과 지불시스템을 중심으로 대응 방안을 살펴본다. 궁극적으로 전자상거래 환경을 구축하기 위한 제품이나 서비스도 중요한 정보통신시장을 형성하게 되고, 따라서 이러한 시장 형성에 공격적으로 대응해야 할 것이다.

2. 전자상거래 정보보호 기술 분류

인터넷 전자상거래 환경구축 시장은 제품 생산과 서비스 제공의 산업으로 구체화되며, 환경구축 시장에서 경쟁력 있는 제품과 서비스를 제공하려면 관련 기술의 확보가 관건이다. 이러한 환경구축 시장의 주요 분야가 정보보호 기술 분야이며, 이에 대한 전반적인 이해를 위해서 전자상거래 정보보호 기술에 관한 분류가 필요하다. 본고에서는 전자상거래의 정보보호 기술을 그림1과 같이 구분한다.

† 정회원 : 한국정보보호센터 책임연구원
†† 정회원 : 한국정보보호센터 연구원



(그림 1) 전자상거래 정보보호 기술 분류

2.1 개인정보 보호기술

공개망인 인터넷에서는 사용자가 인식하지 못한 채 개인의 정보가 누출되어 프라이버시가 침해될 우려가 있다. 이를 기술적으로 해결하기 위한 프로젝트와 기술의 개발이 진행중이다. Netscape Communications Corporation, Firefly Network, Verisign은 인터넷 서비스에서 사용자의 정보를 보호하기 위해 OPS(Open Profiling Standard) 프로젝트를 수행하고 있으며, 이 프로젝트는 특히 사용자의 데이터를 안전하게 저장하고 전송하며 적절히 제어하는데 초점을 맞추고 있다. W3C의 P3P 프로젝트는 웹사이트가 어떤 목적으로 사용자의 정보를 요구하는지 서술하도록 하고 이에 대해 사용자 에이전트가 사용자의 기호에 따라 정보들의 공개 여부를 결정한다. 즉 사용자 에이전트는 사용자가 자주 방문하는 웹사이트와 사용자가 공개하는 개인 정보의 정도를 저장하여 방문했던 웹사이트를 사용자가 다시 방문하면 사용자 에이전트는 사용자가 개인 정보를 반복적으로 입력하는 것을 대신하여 개인 정보를 공개한다. 그러나 그 외의 웹사이트에 대해서는 웹사이트가 어떤 목적으로 사용자의 정보를 요구하는지 서술한 내용과 사용자의 개인정보보호 공개 정도에 따라 공개 여부를 결정한다. P3P 프로젝트는 사용자가 개인정보를 공개하는데 있어서 편리성을 제공하는데 중점을 둔다.

WWW 트랜잭션 내용에 대한 비밀성 보호를 위한 암호 통신은 점차 보편화 되어가고 있는 추세이다. 그러나 사용자 측면에서는 여전히 웹의 사용으로 사용자의 웹 항해 습관이나 이력 또는 클라이언트 머신에 대한 정보 등 암호화 되기 어려운 정보에 대한 보호는 프라이버시 침해라는 또다른 문제를 불러오고 있다. 이러한 사용자 프라이버시 문제를 기술적으로 대처하기 위해 익명성 기법이 연구되어 일부 실현되고 있다. 익명 접속(anonymous connection)은 내외부자로부터 직간접(active/passive) 도청과 트래픽 분석 공격에 강력하게 대처하면서 정상적인 TCP/IP 소켓 접속 기능을 제공하는 통신 프리미티브이다. 소켓 접속은 실시간에 가까운 양방향 통신 채널을 형성하며, 여기에 익명 접속 기능이 추가되면 통신자 위치 정보등을 가려주는 등 여러 가지 응용에 적용될 수 있다. 앞으로 사이버 공간상에서 활동하는 시간이 증가함에 따라 사용자 프라이버시 문제는 더욱 주목받게 될 것으로 예측되며, 이에 대한 대책의 하나로 익명성 기술에 대한 연구가 더욱 중요한 주제로 부각될 것이다.

2.2 지불 보안기술

전자상거래의 비대면 네트워크 환경에서 소비자, 상점, 금융기관 간에 발생하는 결제의 안전한 처리를 위한 기술이 지불 보안기술이다. 지불 수단(Payment Instrument)에 의해 신용카드 기반과 전자화폐 기반으로 분류된다.

1) 신용카드 기반의 지불 보안기술

신용카드 기반의 전자상거래 시스템 구현시 현재 적용되는 기술은 보안 프로토콜과 지불 프로토콜 두가지 이다. 보안 프로토콜은 인터넷 웹 클라이언트와 서버간에 발생하는 트랜잭션의 비밀성을 보장해 주는 기술로 전자상거래 시스템에서 지불 정보에 대한 안전한 전송을 가능케하는 수단으로 사용되고 있다. 대표적인 보안 프로토콜로 S-HTTP(Secure Hypertext Transfer Protocol)와

SSL(Secure Socket Layer)이 있다. S-HTTP는 응용계층에서 적용되며 IETF에서 표준화 작업중에 있으나 현재는 활용되고 있지 않다. SSL은 1993년 웹 서버와 브라우저간의 안전한 통신을 위해 넷스케이프社에 의해 개발되어 세션 계층에 적용된다. 현재 대부분의 전자 쇼핑몰들이 SSL 프로토콜을 지원하는 웹 서버를 구축하고 있으며, 향후 그것의 단순성 및 비용절감 측면을 고려해 볼 때 경쟁력 있는 기술로 고려되고 있다. 1996년 SSL 3.0이 발표된 후, 1998년에는 SSL 3.0이 TLS (Transport Layer Security) 1.0으로 개선된 후 IETF의 표준으로 추진되고 있다. 한편 전자상거래의 모든 참여자 간의 발생할 수 있는 트랜잭션을 정의하고 해당 트랜잭션의 안전성 보장을 위한 별도의 프로토콜을 설계함으로써 전체 시스템에 대한 폭넓은 안전성을 보장하기 위해 SET(Secure Electronic Transaction)와 같은 지불 프로토콜이 개발되었다. SET은 1996년 VISA社와 MasterCard社가 주축이 되어 관련업체 지원아래 개발되었으며, 현재는 SET 1.0이 사용중이고, 향후 SET 2.0에 대한 개발(1997~1999)이 완료될 예정이다. SET 2.0은 SET 1.0의 기능을 강화·확장시킨 형태로서 스마트카드 및 다양한 암호 알고리즘을 지원할 예정이다. 아래 표는 전자상거래 시스템을 구현하기 위해 신용카드 기반의 결제 방식으로 SSL과 SET을 적용하였을 때의 비교를 보이고 있다.

(표 1) SSL과 SET의 적용시 비교

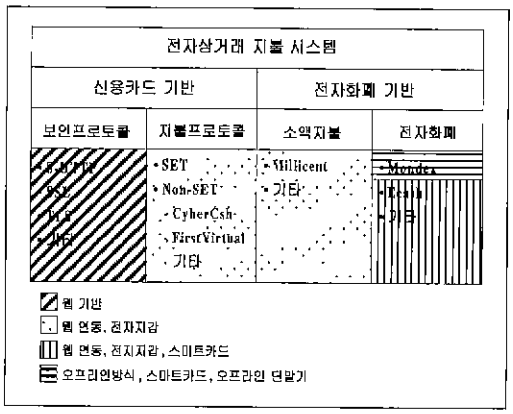
구분	SSL	SET
비용	저비용	고비용
사용편리성	아주 쉬움	다소 어려움
금융기관간의 온라인 결제	제공 않함	제공
안전성	다소 낮음 (상점에 카드번호 노출)	높음(금융기관만이 카드번호 확인)
조작가능성	상점 단독 가능	다자간의 협력 필요

2) 전자화폐 기반의 지불 보안기술

전자화폐란 기존의 상거래 지불 수단이 아닌 새로운 형태의 지불 수단으로서 화폐와 같은 가치를 지닌 디지털 정보를 통칭한다. 전자화폐 기반의 전자상거래 시스템은 현재 유럽을 중심으로 개발 및 상용화 중이다. 전자화폐 시스템은 가치있는 디지털 정보를 화폐로 사용하며, 가치 정보는 스마트카드나 컴퓨터의 하드디스크에 저장되는 형태이다. Mondex는 영국의 NetWest 은행의 Tim Jones와 Graham Higgins에 의해 개발되었으며, 1992년 3월 시범 프로젝트를 거쳐, 현재 영국을 중심으로 세계 20여개국 이상에서 사용중이다. 스마트카드 사용 및 암호기술을 적용한 인터넷 기반이 아닌 오프라인 방식의 전자화폐 시스템으로서 입출금이 용이하며, 개인간의 계좌이체도 가능하다. 1994년 네덜란드 David Chaum에 의해 DigiCash社가 설립된 이후 Ecash 프로젝트가 시작되었고, 1995년 미국의 Mark Twain 은행과 제휴, 인터넷을 기반으로 본격적인 서비스에 돌입한 Ecash는 인터넷 기반의 온라인 전자화폐이다. Mondex와 더불어 최고의 기술을 가진 전자화폐 시스템으로 현재 독일, 호주 등의 업체와 연계하여 지속적으로 사업을 확대해 나아가고 있다. 향후 오프라인 방식도 지원할 것으로 예상된다. 전자화폐 시스템의 일종인 소액지불 시스템은 전자화폐 시스템과 같이 가치를 갖는 디지털 정보를 지불 수단으로 사용하나, 센트 또는 센트 미만과 같은 소액거래에 이용가능 하도록 단순한 암호기술(예:해쉬함수)을 활용한 시스템이다. 1996년 9월 미국의 Digial Equipment社에 의해 연구 개발된 Millicent는 가장 대표적인 소액지불 시스템이다.

2.3 웹 보안기술

전자상거래가 이루어지는 인터넷 전자공간은 월드와이드웹 기술을 근간으로 클라이언트-서버 기술, 분산처리 기술, 실시간 데이터베이스 기술이

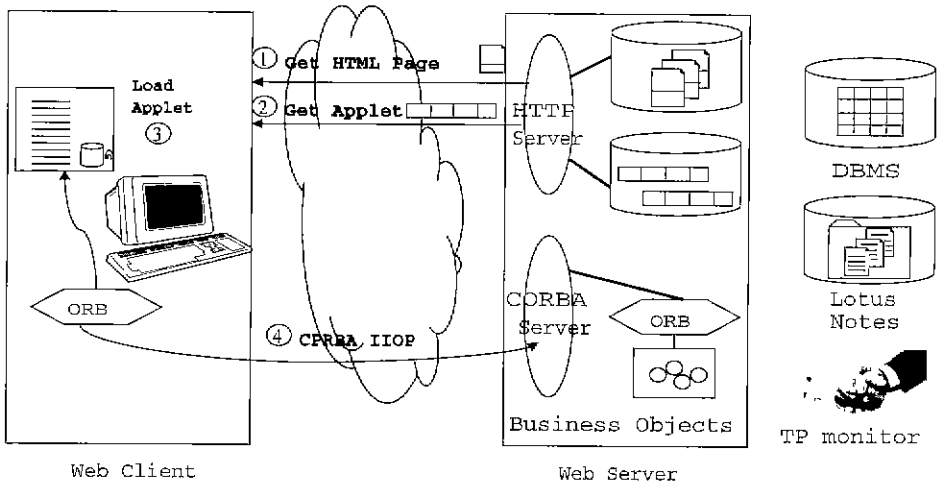


〈그림 2〉 전자상거래 지불 보안기술 분류

요구된다. 이용자와 상점은 웹이 제공하는 환경에서 거래 행위를 하므로 웹 기술의 보안 취약성은 전자상거래의 미래를 결정짓는 중요한 해결 요소이다. 사용자가 인터넷을 접속하고 행동하는 수단인 웹 클라이언트 소프트웨어는 전자상거래의 최종단말로서 보안상 문제점이 사용자에게 직접적인 영향을 미치는 중요한 요소이다. 상업적으로 시장을 대부분 점유한 넷스케이프사의 네비게이터와 마이크로소프트사의 익스플로러 브라우저의 보안취약성은 많이 알려져 있고, 앞으로도 보안성이 강화된 secure 브라우저가 사용되어야 할것

침해의 주요 대상이 될 것이다. 궁극적으로 보안이나, 아직까지 브라우저의 보안성에 대한 개념조차 확립되지 못한 상황이다.

웹 서버는 홍보용, 정보공유, 광고를 비롯한 상거래용 등의 목적으로 구축되고 있다. 이러한 웹의 불특정 다수를 위한 적용으로 방화벽 시스템 외부에 웹 서버가 동작하는 호스트가 설치됨에 따라 해킹등의 공격에 쉽게 노출된다. 또한 내부 데이터베이스와의 연동으로 웹서버 호스트가 공격당하면 내부 자료도 노출될 가능성이 많아지므로 더욱 웹 서버 호스트의 보안이 중요하다. 웹 서버용 소프트웨어도 시장에서 수십종 경쟁되고 있으나, 보안취약성에 대한 설계시의 고려가 아직도 미흡하다. 지금의 웹 기반의 보안은 방화벽 시스템과 같이 보안 전담 소프트웨어를 이용하여 한번에 해결하려는 경향을 보이나, 총체적으로 개별 시스템의 보안성 기능이 고려되지 않는다면, 기대하는 보안성을 확보하기 어려우며, 이는 궁극적으로 전자상거래의 미래를 불투명하게 만드는 요인으로 작용할 것이다. 방화벽 시스템은 개별 안전한 웹 기반 요소가 설계되고 통합됨에 따라 발생하는 보안취약성을 해결하는 수단으로 이해되어야 한다.



〈그림 3〉 Object Web의 예 : HTTP, CORBA, Java 기술의 연동[Robert97]

웹 기술이 Hypertext Web, Interactive Web, Object Web(그림 3 참조)으로 진화함에 따라 복잡한 기능이 웹 페이지에 부가되고 있다 [4]. 이러한 복잡성은 Push 기술, Mobile Code 기술 등의 신개념이 충분한 보안성 검토없이 웹에 적용되어 더욱 웹기반을 보안에 취약하게 만들고 있다.

2.4 인증 기술

인터넷 전자공간의 비대면 특성을 보완하고 상거래 행위의 신뢰성 보장을 위하여 거래 당사자(양자 혹은 다자)간 신분 확인이 이루어져야 한다. 전자공간에서의 신뢰 구축에 필수적인 거래 당사자의 신분 확인은 전문적이고 신뢰할 수 있는 기술을 이용한 인증 기술 및 서비스를 통하여 거래사실 부인 및 거래내용 시비 등 제반 분쟁 해결에 사용된다. 따라서 인증 기술의 개발 보급은 국내외 상거래 및 민원업무 등 전자거래의 활성화에 주요 기반 요소가 된다. 현재 암호기법에 기반한 디지털 서명 방식, 사람의 생체특성 방식 등의 기술 개발이 이루어지고 있다. 공개키 암호법을 이용한 전자서명 기술은 수학적으로 그 안전성을 증명할 수 있는 가장 확실한 인증 기법이다. 대표적인 구현은 전자 인증서를 전자상거래에 참여하는 객체에 부여하여 필요할 때마다 전자인증서를 첨부하는 방식이다. 이 경우 인증서 관리 인프라가 구축되어야 하며, 전자상거래가 전세계적으로 전개되므로 글로벌한 단일의 인증서 관리 인프라가 구축되거나, 또는 지역별로 별개의 인프라를 구축하고 이들간을 상호연동시키는 등의 많은 노력과 시간을 필요로 한다. 사용자 ID 및 password를 기본으로 하는 기존의 인증 시스템은, 쉽게 타인에게 노출, 위조되거나 잊어버릴 수 있는 낮은 안전성의 문제가 있으므로, 사용자 개개인 고유의 생체 특성 정보를 이용한 Biometric 인증 시스템이 연구 개발되고 있다. 전자상거래의 활성화 추세에 맞추어 개방형 네트워크 상에서의 신뢰성 있는 인증 기술이 요구됨에 따라 생체 특성에 기반한 인증 기술은 기술 발전 추이 및 잠재 시장성 부분에서 주목받는 분야이다.

2.5 상호연동성 및 보안성 평가 기술

전자상거래 시스템간의 상호연동성은 이 분야의 표준화 작업이 걸음마 단계에 있으므로, 각 벤더마다 채택하는 보안 기술이 다르다. 설령 SET과 같은 표준을 따라 구현되었다 하더라도 실제 제품의 세부 구현 방식은 다를 수 있어 상호연동성에 문제를 발생시킨다. 이러한 현상은 글로벌한 환경 구축에 장애를 가져오며, 궁극적으로 전자상거래의 확산을 저해하는 또다른 요인이 된다. 한편 일부 IT 제품에 적용되고 있는 보안성 평가 기준의 마련이나 평가 작업은 전자상거래용 IT 제품의 증가 속도를 따라잡지 못하고 있다. 따라서 신뢰성이 검증되지 않은 제품들로 구현된 전자상거래 환경은 더욱 취약하게 될 것이다.

□ 지불수단 보안기술 상호연동성 및 보안성 평가
- SET 및 Non-SET 기반의 통합형 전자지불 처리기술
- 지불처리 게이트웨이 구축 기능
- 금융망 인터페이스를 위한 프로토콜 변환 기능

□ 인증기술 상호연동성 및 보안성 평가
- 암호 라이브러리 기술
- X.500 디렉토리 서비스 기술
- 인증기관(CA) 서버 기술

□ 웹 소프트웨어의 보안성 평가
- 웹 서버 보안성 평가 기준 및 자동화된 평가 도구
- CGI Script 보안성 평가 기준 및 도구

3. 국내 현황 및 문제점

3.1 선도적 기술 개발의 부재

전자상거래의 핵심요소인 정보보호 기술 분야에서 미래의 선도적 기술 개발에 대한 투자가 활발히 이루어지고 있지 않다. 기업체는 연구자본 부족과 개발 후 시장의 불확실성으로 인하여 선도 기술에 대한 연구를 추진하지 못하고 있다. 최근에는 많은 정보보호 기술 개발 업체들이 창업되고 있으며, 더불어 정보보호 제품들에 국산화 작업이 활발히 이루어지고 있으나, 창의성 있는 선도적 기술의 개발은 아직도 미흡한 편이다. 외국의 경우에는 거대 자본을 가진 기업체 또는 기업체들간의 컨소시움 형태나 국가 지원 방식의 프로젝트 수행을 통하여 전자상거래 정보보호 기술 개발 및 시험용 시스템 구축 작업을 진행하고 있다 [2].

3.2 전자상거래 정보보호기술 개발을 위한 체계적인 산학연 협력체계의 부재

전자상거래 정보보호 기술의 산학연 협력 체계를 선도할 구심점의 부재로 민간기술의 역할과 정부 연구기관 및 산하기관의 역할 정립이 이루어지지 못해 일부 기술 개발에 대한 중복투자 및 마스터플랜 작성 부재 현상이 발생하고 있다. 전자화폐 시스템 연구 및 개발의 경우 금융권이나 학회측에서 산발적으로 이루어지고 있으며, SET 제품 구현에 관한 연구 및 개발은 민간 및 정부 연구기관 등에 의해 일부 중복해서 이루어지고 있다.

3.3 핵심원천기술의 부재에 따른 경쟁력 확보의 어려움

보안 프로토콜 분야는 웹 및 TCP/IP에 대한 기반기술을 요구하므로 개발하기가 어려우며, 더욱이 개발하더라도 웹 관련 핵심기술(웹 서버 및 웹 브라우저 제작기술)을 보유하지 않는 한 경쟁력 확보가 어렵다. 지불 프로토콜 분야는 응용레벨의 형태이기 때문에 국내기술에 의해 충분히 개발 가능하나(실제로 현재 몇몇 업체에 의해 Non-Set 형태의 시스템이 개발되고 활용되는 상태임), 국내의 표준화 부재, 국내업체의 단결력 부족 등으로 인해 세계 주요 카드회사인 비자카드社와 마스터카드社가 개발한 SET 지불 프로토콜에 시장 경쟁력이 다소 떨어지고 있는 형편이다. 전자화폐 시스템 분야는 다음과 같은 두 가지 핵심기술을 요구하며, 현재 국내에는 기반기술 확보가 이루어지지 않고 있는 상태이다. 첫째, 전자화폐 프로토콜 개발을 위한 암호기술인 전자서명 알고리즘, 해쉬함수 알고리즘, 블록암호 알고리즘 등은 현재 국내에서 개발 또는 표준화 추진중이나, 이것을 응용한 전자화폐 프로토콜에 필요한 암호기술(예:은닉서명기술 등)에 대한 기술개발은 미진한 상태이다. 둘째, 스마트카드 관련 하드웨어 기술 분야로 전자화폐 시스템을 구축하기 위해서는 스마트카드 관련 하드웨어 제작 기술이 필수적으로 요구된다. 국내의 스마트카드 기술은 몇몇 기업체에서 8비트 마이크로프로세서용 카드 운영체제(COS: Card Operating System)와 읽기/쓰기용 단말기 정도만이 개발된 실정이다. 현재 스마트카드 기술은 유럽의 수준이 가장 뛰어난 상태로서, 16 비트 마이크로프로세서, 32비트 RISC 마이크로프로세서 등이 연구되고 있다.

4. 대응 방안

국내 전자상거래 정보보호 기술 분야는 외국에 비해 취약한 상태이며, 지불 프로토콜 분야에서만 개발이 이루어지고 있는 상태이다. 보안 프로토콜, 지불 프로토콜, 전자화폐 시스템 등 3분야로 나누어 국내 대응 방안을 살펴보고자 한다.

4.1 보안 프로토콜 분야

보안 프로토콜 분야는 인터넷의 TCP/IP를 기반으로 한 고도의 웹 기반기술(웹서버 및 웹브라우

저 제작 기술)을 요구하기 때문에 국내에서는 개발하기 어려운 실정이다.

1) 기술 개발 현황

보안 프로토콜 분야는 미국의 넷스케이프나 마이크로소프트와 같은 웹 관련 핵심기술을 보유하고 있는 기업체나, IETF와 같은 인터넷 관련 표준단체들에 의해 이루어지고 있으며, 국내 기업체나 연구기관의 참여도는 거의 없는 실정이다.

2) 시장성 및 비용

국내에서는 대부분의 전자쇼핑몰들이 SSL 기능을 갖는 웹 서버를 구축 운영하고 있다. 향후에도 지속적으로 성장 및 발전이 예상된다. 보안 프로토콜은 주로 웹 기반이므로 웹 서버 및 웹 브라우저를 판매하는 기업체들에 의해 별도의 수수료 없이 웹 관련 프로그램에 탑재되어 판매되는 형태를 취하고 있다. (SSL의 경우에는 무료로 설치할 수 있는 프로그램이 존재, 예:Apach-SSL 웹 서버) 그러나, SSL을 설치하는 경우 서버의 인증서가 필요하기 때문에 현재 250개 이상의 국내 전자쇼핑몰들이 외국의 인증기관으로부터 인증서 발급 서비스를 이용하고 있다. 미국의 VeriSign의 경우 SSL 서버용 인증서 수수료가 1년에 $349이다. 현재 국내에는 인증기관 서비스를 상업적으로 운영하는 업체가 없는 관계로 대부분의 전자쇼핑몰들이 외국의 인증기관을 이용하는 상태이므로 대략잡아 한해 약 $87,250(=250개 전자쇼핑몰×$349)의 외화가 손실되고 있다.

3) 국내 개발 가능성 및 타당성

보안 프로토콜 분야는 인터넷의 TCP/IP를 기반으로 한 고도의 웹 기반 기술을 요구하기 때문에 개발하기 어려우나, 보안 프로토콜 내에 필요한 암호 알고리즘 등에 국산 암호 알고리즘을 적용하는 시도는 있어야 할 것이다. 또한, 전송계층이나 세션계층이 아닌 응용계층의 특화된 보안 프로토콜(예를 들면, 웹 브라우저의 플러그인 형태의 보안 프로토콜 등)을 개발한다면, 경쟁력이 있을 것이라 예상된다.

4.2 지불 프로토콜 분야

지불 프로토콜 분야는 SET과 Non-SET으로 분류되며, 국내에서는 SET 1.0 사양에 따른 제품 개발이 완료 또는 진행되고 있는 상태이고, 일부 업체들은 자사만의 Non-SET을 개발하고 있는 상황이다.

1) 기술개발 현황

현재 지불 프로토콜의 대표적인 예로는 비자와 마스터카드를 주축으로 개발된 SET 1.0이 있으며, Non-SET으로는 미국의 CyberCash, First Virtual 등이 있다. 국내의 경우 SET 관련하여 커머스넷 코리아(CNK:CommerceNet Korea)에서 한국형 전자상거래 사업을 추진하고 있으며, 데이콤 등이 기술개발을 담당하여 SET 시스템을 구축하고 현재 운영 중이다. 한국과학기술원의 국제전자상거래 연구센터(ICEC : International Center for Electronic Commerce)는 메타랜드를 설립하여, SET 시스템을 개발·운영하고 있다. 비씨카드 등 4개 신용카드사와 한국통신 등은 공동으로 코리아사이버페이먼트(KCP : Korea Cyber Payment)를 설립하여 SET 시스템을 구축 중이다. Non-SET과 관련하여 이니텍 전자지불 시스템이 이니텍(주)에 의해 개발된 바 있다.

2) 시장성 및 비용

SET 개발에는 많은 비용이 소요되며, 더욱이 개발된 제품의 인증을 받기 위해서는 미국의 검사기관인 SETCo에 많은 수수료를 납부해야만 하는 실정이다. 국내에서 개발된 제품들은 현재까지 SETCo에 인증 신청을 하지 않은 상태이며, 이것

은 국제호환이 아닌 국내에서만 사용가능하다는 것을 의미한다. SET용 인증기관은 별도로 마스터카드나 비자카드의 인증기관으로부터 인증을 받아야 하며, 그 과정에서 수만불에 이르는 수수료가 요구된다. 이러한 SET 시스템 구축의 어려움으로 인하여, Non-SET 형태인 독자적 지불 프로토콜이 일부 업체에서 개발되고 있으며, 그 예로 강원도청 전자상거래 사업에는 이니텍(주)이 참여하여 자사의 지불 시스템을 구축한 바 있다. CNK의 인증기관 서버는 IBM Registry 인증기관 서버를 도입하였고, KCP는 GTE CyberTrust 인증기관 서버를 도입하여 시험 운용 중이다.

(표2) 국내 보안업체에 의해 개발된 인증기관 서버

업체명	제품명	비고
소프트포럼	SFCA V2.5	개발완료, 판매중
이니텍	이니텍 CA V2.5	개발완료, 판매중
잠미디어 인터렉티브	JMI CA V2.0	개발완료
에버 소프트	Es-CA	개발완료(시제품)
삼성SDS	Trust Pro	개발완료(시제품)
세넥스	ASSURE CA	개발완료(시제품)

3) 국내 개발 가능성 및 타당성

Non-SET 유형의 지불 프로토콜은 이미 몇몇 업체에 의해 개발, 사용 중이며, 그 기술 또한 우수하다고 평가할 수 있다. 국내 SET 시스템 구축 업체가 국제 경쟁력을 갖기 위해서는 사용자 전자지갑, 머천트 서버, 지불게이트웨이 서버 등의 국산화가 이루어져야 하며, 더불어 SETCo의 인증마크 획득을 통하여 대외 수출의 기반을 마련해야만 할 것이다. 미국의 IBM, HP 등은 자사의 H/W에 머천트 서버나 지불게이트웨이 서버를 탑재한 시스템을 turnkey 방식으로 일괄 판매하는 등, SET 관련 솔루션의 판매에 많은 관심을 기울이고 있다. 따라서 지불 프로토콜 분야는 보안 프로토콜과는 달리 응용 계층에서의 작업이기 때문에 설계 및 개발이 국내 기술에 의해 추진될 수 있으며, 지불 프로토콜에 대해 SET과 같은 형식의 국내 표준을 제정함으로써 국내 보안관련 업체들의 중복투자를 방지하고 특화된 기술을 확보할 수 있을 것이다.

4.3 전자화폐 시스템 분야

전자화폐 프로토콜 분야는 몇몇 연구기관에 의해 일부 연구되고 있는 실정이나, 국가 프로젝트나 기업체 차원에서 진행되고 있는 사례는 없다.

1) 기술개발 현황

전자화폐 분야는 인터넷 기반이 아닌 오프라인 방식의 일반 직불카드와 유사한 기능을 갖는 시스템으로 개발되기 시작하였으나, 현재는 인터넷 전자상거래와 접목되어 개발 전개되고 있는 추세이며, 유럽의 Mondex나 Ecash가 가장 앞선 기술을 보유하고 있다. 일본의 NTT는 1997년부터 전자화폐 시스템 개발을 추진하고 있으며, 1999년부터 시범 서비스를 예정하고 있다. 국내에서는 금융결제원을 중심으로 은행권, 한국정보통신진흥협회 산하의 "전자화폐연구회" 등에서 소규모 연구가 이루어지고 있다. 전자화폐 시스템은 보안 프로토콜이나 지불 프로토콜과는 달리 웹 기반 기술보다는 스마트카드나 관련 장비에 대한 하드웨어 및 소프트웨어 기술이 요구되며, 국내의 하드웨어 기술은 유럽의 수준과 많은 격차를 보이고 있다.

2) 시장성 및 비용

Mondex는 현재 유럽을 중심으로 폭넓게 사용되고 있으며, 일본 및 호주도 Mondex 시스템을 도입 구축하고 있다. Ecash는 미국의 Mark Twain 은행과 협력하여 전자화폐 발행 서비스를 제공하고 있으나, 아직까지는 크게 확산되고 있는 상태는 아니다. 그러나, 전자화폐 시스템은 지불 프로

토콜에 기반을 둔 지불시스템을 대치할 미래지향적 기술로 뛰어난 안전성, 사용의 편리성(온라인 및 오프라인 지원), 사용자 프라이버시 보장 등의 강력한 기능을 제공함으로서 미래 전자상거래 시장의 독점적인 지불수단으로 각광받을 것으로 예상된다. 일반 지불 프로토콜 개발에 비해 기술개발 및 구현이 다소 어려우며, 특히 암호기술의 적용이 필수적으로 요구된다.

3) 국내 개발 가능성 및 타당성

전자화폐 시스템 개발은 프로토콜 설계 부분과 시스템 구축 부분으로 구분할 수 있다. 프로토콜 설계 부분은 전자서명 알고리즘, 은닉서명 알고리즘 등의 요소기술 알고리즘을 필요로 하며, 더불어 그것들을 기반으로 인출 프로토콜(은행과 사용자간), 지불 프로토콜(사용자와 상점간), 예치 프로토콜(은행과 상점간)에 대한 설계능력이 요구된다. 국내에는 현재 KCDSA 전자서명 알고리즘이 표준화 중이나 나머지 프로토콜 설계 부분에 대한 기반기술은 확보치 못하고 있는 상태이다. 그러나 국산 전자서명 알고리즘을 보유하고 있기 때문에, 적절한 연구개발이 진행된다면 개발 가능성은 충분하다. 시스템 구축 부분은 스마트 카드 및 관련 시스템의 하드웨어 및 소프트웨어 기술 개발에 대한 투자가 필수적이다. 결론적으로, 단기적인 성과보다는 장기적인 안목을 통해 집중적인 전략사업으로 육성한다면, 경쟁력을 확보할 수 있다.

5. 결 론

전자상거래 환경구축을 위해 필요한 하드웨어, 소프트웨어, 서비스 등도 주요한 정보통신 시장을 형성하고 있다. 여기에는 웹 관련 제품, 인증기관 구축 제품, SET 관련 제품 및 서비스, 전자화폐 관련 제품 등이 대표적인 예이며, 전자상거래의 비지니스 모델[3]이 확장됨에 따라 관련 신기술이 채택된 제품이나 시스템이 출현할 것이다. 이에 따라 선진국보다 기술 수준이 열세인 우리나라의 경우 필연적으로 이들 시스템이나 제품 도입으로 인한 외화 지출이 증대할 것으로 예상된다. 이러한 전자상거래 환경구축 시장의 규모에 대한 정확한 산출 데이터는 없지만 [3]에 의하면 기업간 전자상거래 규모에 버금갈 정도의 수천억 달러에 이를 것이라고 전망하고 있다.

궁극적으로 인터넷 전자상거래 환경구축 시장에서 우리의 목표는 환경구축 기술 개발을 통한 제품 국산화 및 수출 시장 확보이다. 즉 미국 중심의 기술 및 제품으로 국내 전자상거래 환경구축에서 벗어나 우리의 기술과 제품으로 국내 환경을 구축하고, 나아가 동남아나 전자상거래 기반을 구축하는 후발 국가의 시장을 점유하는 것이다. 본 글에서는 환경구축 시장의 주요이슈인 정보보호 기술을 분류하고, 이들 기술의 국내외 현황을 살펴보았다. 여기에 더하여 국내 지불 보안기술 분야의 대응방안을 제안하였다. 이러한 전략적 고려를 통하여 전자상거래 전개가 국가경쟁력 증대에 기여하도록 적극적인 노력이 요청된다 하겠다.

부록 : 인증 서비스 고찰 및 현황분석

1. 개 요

인증이라 함은 일반적으로 크게 두 가지 의미로 대별된다. 첫번째는 사용자 인증이나 메시지 인증을 의미하는 「Authentication」이고, 두번째는 비대칭형(공개키) 암호 방식에서 공개키의 무결성을 보장하기 위해 인증기관이 발행하는 인증서의 의미를 갖는 「Certification」이다. 일부 학자들은 「Certification」을 「보증」이라는 단어로 칭하여 인증(Authentciation)과 구별을 하기도 하지만, 일

반적으로 혼용되고 있는 상태이다. 최근 전자상거래에서 화두가 되고 있는 인증 서비스는 일반적으로 인증기관으로부터 파생되는 「Certification」 서비스를 지칭하는 것이며, 이것은 「Authentication」과는 구분되어야 한다.

인증 서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 안전한 전자상거래 환경의 구축을 위해서는 인증, 무결성, 기밀성, 부인봉쇄 등의 정보보호 서비스가 필요하게 되며, 인증, 무결성, 부인봉쇄 등의 서비스는 전자서명 기술을 활용함으로써 해결가능하다. 현재 안전성을 정량화시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증 서비스가 필요하게 된다. 인증기관은 전자서명을 이용하고자 하는 사용자들에 대해 인증서 발급 서비스를 제공해줌으로써 이윤을 창출하거나 기업내 안전한 전산망 구축을 담당하는 하나의 조직을 일컫는 것이며, 인증 서비스란 인증기관이 제공해주는 인증서 발급, 인증서 관리 등 일련의 인증관련 서비스를 통칭하는 것이다.

2. 인증 서비스의 분류

인증 서비스의 분류는 인증기관이 발급하는 인증서의 응용 분야에 따라서 나뉘어진다. 현재 정보통신망과 컴퓨터 네트워크 기술의 발전으로 말미암아 대부분의 영역에서 정보보호 필요성이 대두되고 있으며, 이것에 대한 해결책으로서 암호기술의 사용이 권장되고 있다. 이중에서도 공개키 암호 알고리즘을 이용한 전자서명 기술의 활용은 상기에서도 고찰한 바와 같이 인증, 무결성, 부인봉쇄 등의 정보보호 서비스를 제공해주는 효과적인 솔루션으로 자리잡고 있다. 이러한 배경으로 인하여 컴퓨터 네트워크 보안과 관련된 많은 국제 표준화 단체나 개발 업체들이 공개키 암호 기술이 적용된 프로토콜이나 제품들을 출시하고 있는 상태이며, 이것은 상업적 목적을 갖는 인증기관 탄생의 기반이 되었다.

일반적으로 인증 서비스는 두 가지 분류로 나뉘어진다. 첫 번째는 상기에서 언급한 바와 같이 범용적인 보안 프로토콜의 확산으로 인해 요구되는 인증 서비스로서, 이 경우 인증기관은 각 객체들에 대해 인증서를 발급하고, 이에 대한 수수료를 받음으로써 경제적 이득을 취하게 된다. 두 번째는 안전한 인트라넷, 익스트라넷, 기업망, 폐쇄 네트워크 시스템 등의 구축을 위해 요구되는 인증 서비스로서, 이 경우 사업자는 인증서 발급에 대한 수수료를 목적으로 하는 것이 아니라 자사의 안전한 네트워크 환경 구축을 목적으로 한다.

3. 인증 서비스 현황

인증 서비스는 앞절에서 고찰한 바와 같이 크게 두 가지로 대별된다. 일반적으로 상업적 인증 서비스를 제공하는 인증기관들은 범용 프로토콜 지원을 목적으로 하는 인증서를 발급하고 있기 때문에, 특정 도메인에서 안전한 네트워크 환경 구축을 위해 제공되는 인증 서비스는 현황파악에서 배제하고자 한다. 현재 세계적으로 제공되고 있는 상업적 목적의 인증 서비스 종류는 (표1)과 같다.

(표 1) 인증 서비스 종류

종 류	용 도
S/MIME	안전한 전자메일용(암호화 · 전자서명)
SSL	웹 보안 프로토콜인 SSL을 웹 서버에 적용하기 위해 필요한 인증서(미국외 512비트)
Global 서버 ID	미국외에서 강한 SSL을 사용하고자 하는 경우 필요한 인증서(1024비트,미국 상무부의 허가 필요, 금융권으로만 제한)
OFX를 위한 금융 서버 ID	OFX 프로토콜 적용에 필요한 인증서
EDI 서버 ID	안전한 EDI 구현에 필요한 인증서
MicroSoft AuthenticCode ID	OCX, CLASS, CAP 등 마이크로소프트사에서 제공하는 기술을 사용하여 제작한 S/W의 온라인 판매시 사용되는 인증서
Nescape Object Signing	JavaScript, Java 등으로 제작된 S/W의 온라인 판매시 사용되는 인증서
SET	SET 프로토콜 구현에 사용되는 인증서

4. 인증기관 현황

인증기관(Certification Authority) 현황은 일반적으로 인증 서비스를 행하는 업체나 조직을 말하는 것이나, 본 고에서는 개발 업체와 서비스 업체로 분류하여 인증기관 서비스 업체 및 관련 개발 업체등을 동시에 고찰함으로써 전체적인 현황 파악을 용이케 하고자 하였다. 최근에는 개발 업체가 서비스 업체의 역할도 수행하는 등 그 구분이 모호해지고 있으나, 현재까지는 개발 및 서비스 업체가 분류될 수 있는 상태라고 사료된다.

4.1 국내 현황

1) 국내 개발 업체 현황

국내 개발 업체들은 현재 SSL(Secure Socket Layer)이나 S/MIME(Secure Multi-purpose Internet Mail Extension)용 인증서 발급이 가능한 인증기관(CA) 서버를 개발한 상태이며, 아직까지는 다양한 인증서 발급 서비스(예:SET, OFX 등)들을 지원하는 인증기관 서버는 개발되지 않은 상태이다. 현재 국내 인증기관 서버 개발 현황은 시장 형성 초기 단계이며, 향후 지속적인 발전이 있을 것으로 사료된다. 국내 인증기관 서버 개발 업체 현황은 본문의 (표2)에 기술하였다.

2) 국내 서비스 업체 현황

현재 국내에서 상업적 목적을 가지고 공식적으로 인증서 발급 서비스를 행하고 있는 업체는 SET(Secure Electronic Transaction) 지불 시스템을 구축 · 운영하고 있는 일부 업체들 외에는 전무한 실정이다. 그러나 보다 엄밀히 말한다면, SET 인증기관 서비스는 SET 프로토콜을 위한 전용 인증기관이기 때문에 일반적인 인증기관 서비스라고 보기 어렵다. 즉, 현재까지 일정 발급 수수료를 받고 SSL이나 S/MIME 등의 인증서를 발급해주는 국내 인증 서비스 업체는 전무한 실정이며, 단지 개발 업체들만의 제품 시범 서비스만이 존재할 뿐이다.그러나, 조만간 전자서명법 시행후 여러 가지 인증 서비스가 활성화될 것으로 판단된다.

(표 2) 국내 인증기관 서비스 업체 현황

업 체 명	인증 서비스	인증기관 서버
한국통신	SET 인증서	GTE CyberTrust
CNK (Commerce Net Korea)	SET 인증서	IBM Registry
메타랜드	SET 인증서	자체개발

4.2 국외 현황

1) 국외 개발 업체 현황

현재 국외에는 수 많은 개발업체들이 있으며, 이러한 업체들은 인증기관 서버 뿐만 아니라 공개키 기반구조(Public Key Infrastructure) 구축을 위한 토탈 솔루션을 제공하고 있다. 또한, 여러가지 인증서 발급이 가능하도록 다양한 인증기관 서버들을 제공하고 있다.

2) 국외 서비스 업체 현황

현재 세계 각국에 많은 인증 서비스 업체들이 존재하며, 최근 그 수가 폭발적으로 증가하고 추세이다. 초기에는 SSL이나 S/MIME용 인증서 발급 서비스로 국한되던 것이 현재는 EDI, IPSEC 등 다양한 프로토콜들을 위한 인증서 발급 서비스가 제공되고 있다. 기술이나 규모면에서 가장 앞서고 있는 서비스 업체는 미국의 VeriSign으로써 다양하고 폭넓은 서비스를 제공하고 있으며, 국내에 SSL 보안 프로토콜을 사용하는 많은 전자쇼핑몰 업체들도 VeriSign의 인증 서비스를 활용하고 있는 상태이다.

(표 3) 국외 인증기관 서버 개발 업체현황

국가	업체명	제품명	URL
일본	Hitachi	Certificate Authority 01-00	www.hitachi.co.jp
	Fujitsu	CommerceSTAGE Secure Certificate Authority v1.0	www.fujitsu.co.jp
캐나다	Entrust Technologies	Entrust CommerceCA WebCA	www.entrust.com
미국	GlobeSet	GlobeSet CA v1.2	www.globeset.com
	GTE Cybertrust	CyberTrust Certificate Management Systems	www.bbn.com/products/security/cytrust/index.htm
	IBM	IBM Registry	www.software.ibm.com/commerce/payment
	Certco	Root Certauthority Commerce Certauthority	www.certco.com

(표 4) 국외 인증기관 서비스 업체현황

국가	회사명	특징	홈페이지 URL
미 국	Digital Signature Trust Company	유타주정부 공인인증기관	www.digsigtrust.com
	Arcanvs	유타주정부 공인인증기관	www.arcanvs.com
	USER TrustCompany	유타주정부 공인인증기관	www.usertrust.com
	ARINC	컨설팅 및 구축 서비스	www.digsig.arinc.com
	Verisign	인증서 발급 서비스	digitalid.verisign.com
영 국	Trustwise	인증서 발급 서비스	www.trustwise.com
프랑스	Certplus	인증서 발급 서비스	www.certplus.com
일 본	Verisign Japan	인증서 발급 서비스	www.verisign.co.jp
대 만	HiTRUST	인증서 발급 서비스	www.hitrust.com
남아공	SACA	인증서 발급 서비스	www.saca.net
	Thawte Consulting	인증서 발급 서비스	www.thawte.com

참고문헌

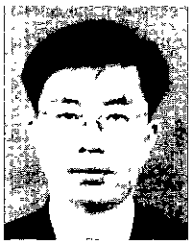
[1] 전자상거래 주요현안 및 대응방안, 한국전산원 CALS/EC팀, 1998년 6월.

[2] G. Lacoste, "SEMPER: A Security Framework for the Golbal Electronic Marketplace", IBM France, August 1997.

[3] Paul Timmers, "Business Models for Electronic Markets", Electronic Market, Vol.8, No.2, April 1998.

[4] Robert Orfali & D. Harkey, Client/ Server Programming with Java and Corba, Wiley, 1997.

[5] Anup K. Ghosh, E-Commerce Security: Weak Links, Best Defenses, Wiley, 1998.



김 홍 근

1985년 서울대학교 컴퓨터공학과
1994년 서울대학교 컴퓨터공학과 박사
1994년-1996년 한국전산원 선임 연구원
1996년 현재 한국정보보호센터 책임연구원
관심분야 : 암호이론, 전자화폐, 전자상거래 보안

최 영 철

1996년 성균관대학교 공과대학 정보공학과
1998년 성균관대학교 일반대학원 정보공학과 석사과정
1987년 현재 한국정보보호센터 연구원
관심분야 : 암호이론, 전자화폐, 전자상거래 보안

제11회 춘계학술 발표대회 논문 모집 및 행사안내

◉ 일시 : 1999년 4월 9일(금) ~ 10일(토) 2일간
◉ 장소 : 동국대학교(경주캠퍼스)
◉ 행사내용 : 등록, 논문발표, 초청강연, 튜토리얼, 임시총회, 축하연
◉ 논문마감 : 1999년 3월 5일(금)
◉ 특이사항 : 당일등록을 사전등록으로 변경
- 학회지 후면 안내팜플렛 내용 참조
◉ 협조사항 :
- 초청연사 및 튜토리얼 강사 추천
- 좌장 모집
- 연구회 및 기타회의 개최 사전 접수