인터넷 결제시스템의 비교연구

주재훈
동국대학교 상경대학 경상학부 조교수
(givei@mail.dongguk.ac.kr)

인터넷 전자상거래에서는 탐색 및 통신비용을 비롯한 거래비용을 낮출 수 있고, 다양한 판매자로부터 특정 제품 및 가격에 대한 정보를 소비자에게 상세하게 제공할 수 있어 거래의 효율성을 개선시킬 수 있다. 한편 몇몇 안전장치가 유지되고 있는 폐쇄 네트워크에서와는 달리 인터넷 상거래에서는 개방·분산 네트워크로서의 특성상 안전한 거래가 보장되지 않는다. 즉, 인터넷 상거래의 효율성을 높이기 위해서는 비밀정보의 전송, 메시지 무결성, 거래 당사자간의 인증, 대금결제 기능을 제공해 주는 안전한 결제시스템이 구축될 필요가 있다. 따라서 본 연구에서는 현재 개발 또는 운영되고 있는 6개의 제3자에 의한 결제시스템을 조사·분석하므로써 다음 질문에 대한 해답을 찾고 이들에 대해 논의하고자 한다:

현재 어떤 결제시스템이 존재하며, 이들은 어떻게 보안서비스를 제공하고 있는가?
각 결제시스템의 장점과 한계점은 무엇인가?
결제시스템을 설계할 때 고려해야 할 주요 요인은 무엇인가?
이들 요인간에는 어떤 상반관계가 존재하며 어떻게 이를 고려할 것인가?

I. 서 론

1.1 문제 제기와 연구 필요성

인터넷 상거래란 전자적으로 거래가 이루어진다는 점에서 전자상거래의 일종이다. Kalakota와 Whinston(1996)은 전자상거래란 컴퓨터 네트워크를 통해 정보, 제품, 서비스를 구매하고 판매하는 것이라 정의하고 있다. 한편 Bloch와 Pigneur 등(1996)은 전자상거래란 전자 인프라를 통해 어떤 형태의 사업거래를 지원하기 위해 인터넷웹을 사용하는 것이라 정의하고 있다. 인터넷 상거래에서는 주문에서 지불에 이르는 과정의 모든 거래자료가 인터넷을 통해 전자적으로 처리된다. 특히, 정보제품(소프트웨어, 게임, 뉴스레터, 논문, 재무정보, 온라인 서적 등)의 경우는 제품 자체도 인터넷을 통해 인도되기 때문에 인터넷은 새로운 분배채널로서 기능을 하게 된다.

시공간을 초월하여 전세계를 하나의 전자시장으로 연결하고, 판매자와 구매자 모두에게 거래의 편리성을 제공하며, 일반 상거래에서는 불가능했던 기능을 제공할 수 있는 능력이 인터넷 상거래에 내재되어 있다. 예를 들면, 판매자는 고객에 대한 정보를 기초로 개별 마케팅이 가능하며, 인터넷을 새로운 분배채널로 이용할 수 있다. 특히 인터넷 상거래에서는 다양한 제품과 가격에 대한 정보를 쉽게 입수할 수 있고, 거래가 신속하게 이루어지며, 거래비용이 감소되어 효율적 시장(efficient market)이 형성

논문 접수일 : 97. 3 게재확정일 : 97. 7

될 수 있다[1].

그러나 인터넷은 분산·개방 네트워크이므로 시스템의 자산을 파괴하거나 이용하지 못하도록 하는 가로막기(interruption), 비인가된 사람(프로그램 또는 컴퓨터)가 시스템에 접근하여 정보를 도청하거나 가로채기(interception), 전송 중인 자료를 수정하기(modification), 비승인된 자가 시스템에 위조 프로그램을 삽입하는 것(fabrication) 등의 보안상의 위협이 내재되어 있다(정범석·한인구, 1996). 또한 인터넷에는 관리 및 보안정책과 법체제의 미비로 인한 많은 위협이 내재되어 있으며, 전세계의 불특정 다수가 참여하는 가상공간에서는 사기와 속임수가 발생할 가능성이 높다.

따라서 제품 검색, 협상, 구매주문, 지불 등의 인터넷 상거래 과정을 지원하는 안전한 결제시스템이 구축될 때, 인터넷 상거래에 따른 위험을 최소화하고 효익을 최대화할 수 있다. 현재까지의 결제방법은 다음 4단계로 발전해 왔다.

첫째 단계는 주문은 인터넷을 통해 이루어지고 지불은 인터넷 외부에서 이루어지는 방식이다. 이 경우에는 거래가 완성되기까지 처리시간이 오래 소요되어 인터넷 상거래의 효익을 최대화할 수 없다.

둘째 단계는 보안이 유지되지 않는 상태에서 인터넷을 통해 신용카드번호와 재무정보를 송수신하여 결제하는 방식이다. 인터넷에서 송수신자간에 교환되는 메시지는 평균적으로 10개의 컴퓨터를 경유하게 되는데(Borenstein, et al., 1995), 네트워크의 중간 지점에서 메시지를 읽고 훔치는 스뉴퍼(snooper)가 신용카드번호를 가로챌 수 있다. 또한 인터넷을 통과하는 메시지를 검색하여 신용카드번호를 알아내는 프로그램이 개발되어 배포되기도 한다(Gable, Cossio, and Celbulski, 1996). 따라서 이 경우에는 비밀정보가 누출될 수 있고, 판매자는 신용카드를 사용하는 사람이 그 소유자라는 것을 입증할 수도 없기 때문에 인터넷 상거래의 안전이 유지되지 않는다.

셋째 단계는 암호방식을 이용한 신용카드 및 전자수표에 의한 결제방법이다. 현재 판매자 중심의 많은 상거래시스템에서는 이 결제방식을 채택하고 있다. 넷스케이프 내버게이터에서는 SSL을 지원하고 있고, 모자익에서는 PEM(Privacy Enhanced Mail)과 PGP(Pretty Good Privacy)를 지원하고 있어, 판매자들은 신용카드번호와 같은 비밀정보의 기밀성을 유지하는 결제시스템을 구축할 수 있다. 그러나 판매자의 거짓 대금 청구와 구매자의 지불거절과 같은 문제를 제도적으로 방지하는 메카니즘을 제공하지 못하는 경우가 많다[2]. 그 외에도 판매자 중심의 결제시스템에는 다음과 같은 몇가지 문제점이 내재되어 있다.

① 소비자는 다음과 같은 불편성을 감수해야 한다. 소비자가 여러 판매자와 거래하는 경우, 그는 판매자별로 여러 개의 고유번호와 비밀번호를 갖고

1) Zabih(1996)은 컴퓨터 주변장치에 대한 가격 정보를 제공하는 웹사이트(http://www.priceweb.com/)를 통해 효율적 시장 형성의 가능성을 실험하고 있다. 그 외에도 판매자의 웹사이트에서 온라인으로 가격정보를 수집하여 제공하는 Computability (http://www.computability.com/), BargainFinder(http://bf.cstar.ac.com/), CyberSave Shopper (http://cybersave.com/) 등이 있다. Barua 등(1994)의 연구에 따르면, 표준제품(컴퓨터 디스켓, 인쇄용지 등)의 경우에는 일반 거래에 비하여 전자상거래에서 검색비용, 통신비용, 평가비용 모두가 낮아질 수 있으나, 비표준제품(특수 목적의 기계류, 전문 소프트웨어 등)의 경우에는 검색 및 통신비용은 낮아지나 평가비용이 상승될 수 있다.

2) 예를 들면, 우리 나라에 최초로 1996년 말부터 운영되고 있는 데이콤의 interpark(http://www.interpark.com)에서는 SSL을 이용하여 신용카드번호를 암호화하여 전송하고 있으나 전자서명 기능을 제공하고 있지 않다. 따라서 구매자와 판매자간에 분쟁이 발생했을 때 결제메카니즘으로 이를 해결할 수 있는 방안이 없다.

있어야 한다. 또한 판매자별로 인터페이스가 서로 달라 사용자는 이를 이용함에 있어서 불편을 느낄 수 있다. 소비자가 여러 판매자들에게 동일한 고유번호와 비밀번호를 사용하는 경우라 할지라도 이를 입력하는 빈도가 높을수록 침입자에게 도난당할 가능성이 높아지므로 그 만큼 보안상의 허점이 드러날 가능성이 높다. 소비자는 구매 및 개인에 관한 정보를 판매자에게 쉽게 노출할 수 있다.

② 거래시 마다 결제가 이루어지는 경우에는 제품가격에 비해 거래비용이 높아 소액거래가 활성화되지 못한다.

이들 문제점을 해결하는 한가지 방안은 판매자와 소비자간의 중개 역할을 하는 신뢰할 수 있는 제3자에 의한 결제시스템이다. 인터넷 서비스 제공업체, 소프트웨어 개발업체, 은행과 신용카드회사를 비롯한 금융기관 등은 결제시스템을 구축하여 운영하는 기관이 될 수 있다. 소비자는 신뢰할 수 있는 제3자를 통해 판매자와 거래하게 되므로 판매자로부터 프라이버시를 보호할 수 있다. 또한 이 시스템에서는 다양한 판매자의 제품을 소개하고, 일정시간 간격 또는 특정 구매자의 총누적 거래대금이 일정수준에 이를 때에 결제함으로써 신용카드를 지불수단으로 사용하는 경우에도 소액거래를 지원할 수 있다.

넷째 단계는 전자화폐에 의한 결제 방법이다.

인터넷 상거래가 소비자와 판매자를 비롯한 사용자들에게 널리 수용되어 안전하고 편리하게 이루어지기 위해서는 신뢰할 수 있는 결제시스템이 그 전제 조건이 된다. 따라서 본 연구는 셋째 단계의 제3자에 의한 결제시스템과 전자화폐에 의한 결제시스템을 연구대상으로 하고 있다. 결제시스템이 잘못 설계되는 경우, 판매자·소비자·결제기관 내부의 사기, 프라이버시 보호, 사용자 불편성 등으로 인해 인터넷 상거래로부터 기대되는 효익을 최대화할 수 없을 뿐만아니라 인터넷 상거래에 대한 신뢰가 저하되고 커다란 재앙을 초래할 수 있다. 따라서 현재 초기 단계에 있는 인터넷 상거래를 활성화하기 위해서는 기존의 결제시스템에 대한 비교연구를 통해 결제시스템 설계시 고려되어야 할 중요한 요인이 무엇이며, 이들 요인간에는 어떤 상반관계가 발생하는가를 분석할 필요가 있다. 이러한 연구는 향후 우리 나라 인터넷 상거래 결제시스템 구축에 필요한 중요한 지침이 될 수 있다.

1.2 연구목적과 방법

본 연구는 현재 개발·시험중에 있거나 운영 단계에 있는 결제시스템을 비교함으써 인터넷 결제시스템 설계시 고려되어야 할 중요한 요인을 분석하고, 각 요인간에 발생하는 상반관계를 분석하는데 그 목적을 두고 있다. 먼저 본 연구에서는 제3자에 의한 결제시스템의 현황을 파악하고, 각 결제시스템의 장점과 한계점을 분석한다. 다음으로는 이들 요인에 대한 분석과 판매자 및 소비자의 요구사항을 분석하여 결제시스템 설계시 고려해야 할 다차원적 요인을 파악하고자 한다. 끝으로 이들 몇가지 요인을 기준으로 하여 각 결제시스템에 대해 비교·토의하고자 한다.

본 연구는 기본적으로 사례 분석 방법을 채택하고 있다. 제3자에 의한 결제시스템의 사례를 찾기 위해서 본 연구에서는 야후, 라이코스 등 다양한 검색엔진을 사용하여 인터넷 상거래 또는 결제시스템 관련 웹사이트를 조사하였고, 인터넷 상거래 또는 결제시스템 관련 웹사이트 목록을 제공하는 10개 웹사이트를 조사하였다. 본 연구에서는 이들 결제시스템을 상호 비교하기 위해 각 결제시스템에

대해 부분적으로 논의되어 왔던 다양한 문헌을 조사하고, 각 결제시스템에서 개발하여 시범운영 또는 실제 운영 중인 소프트웨어를 조사하며, 각 결제시스템의 웹사이트에서 제공하고 있는 사용자들에 대한 질문과 응답(FAQ)을 조사·분석한다. 일부 결제시스템의 경우는 아직 개발 또는 시범운영 단계에 있고, 일부는 운영의 초기단계에 있기 때문에 실제 사용자를 대상으로 운영시스템의 안전성, 수용성, 편리성 등에 대한 실증분석을 실시하기가 쉽지 않다. 따라서 각 결제시스템에 대한 사용자들의 질문과 그에 대한 시스템 관리자의 응답을 통해 도출할 수 있는 판매자와 소비자의 요구사항은 결제시스템을 비교분석하는 좋은 자료원이 될 수 있다.

전용망에서와는 달리 인터넷에서는 보안이 유지되지 않기 때문에 무엇보다도 인터넷 결제시스템에서는 기밀성, 인증성, 메시지 무결성, 부인방지 등의 보안서비스가 제공되어야 한다(RSA, 1995e; Open Market, 1996)[3]. 본 연구의 대상이 되는 결제시스템에서는 이들 보안서비스가 제공되는 결제 프로토콜을 채택하고 있다. 인터넷의 기본적인 보안서비스를 제공해 주는 결제시스템으로는 CyberCash, First Virtual, NetBill, NetCheque, FSTC의 ECheck, LETSystem, ecash, Mondex, CAFE, Check-Free, NetChex, GC Tech 등이 있다. 이들 시스템은 신용카드 또는 전자수표에 기초한 모형에 기반을 두고 있거나 전자화폐 모형에 기반을 두고 있다. 본 연구에서는 이들 수많은 결제시스템 중에서 다음의 기준을 만족하는 결제시스템으로서 신용카드 모형에 기반을 결제시스템, 전자수표 모형에 기반을 둔 결제시스템, 전자화폐 모형에 기반을 둔 결제시스템, 각각에서 2개씩을 선택하였다. 이들은 결제시스템 목록을 제공하는 웹사이트에서 보편적으로 인용되고 있는 결제시스템들이다(Clarke, 1995; CommerceNet, 1995; CommerceNet, 1996; Fox, 1996; Hallam-Baker, 1995; Peirce, 1996; SIC, 1996; UCLA at Berkeley, 1996; Waidner, 1996).

조건 1: 인터넷 상거래 또는 결제시스템 관련 자원을 소개하는 웹사이트에서 공통적으로 소개되고 있는 결제시스템

조건 2: 현재 개발되어 운영되고 있거나 시범운영되고 있는 결제시스템

조건 3: 결제시스템에 대한 개요, 세부적인 결제 메카니즘에 관한 자료를 소개하고 있는 결제 시스템

조건 4: 자사의 특정 제품을 판매할 목적으로 개발되지 않고, 제3자의 입장에서 개발

3) 다양한 결제 프로토콜에서는 공개키 암호방식을 이용함으로써 이들 보안서비스를 제공하고 있다(Diffie and Hellman, 1976). 기밀성은 메시지를 암호화하여 전송함으로써 유지된다. 메시지 송수신자의 실체를 파악하는 인증성, 전송중인 메시지의 수정이나 변경을 확인할 수 있도록 해 주는 무결성, 메시지의 실제 송수신자가 송수신 사실을 부인할 수 없도록 하는 부인방지 등의 기능은 전자서명을 통해 가능하다. 전자서명(digital signature)이란 송신자가 자신의 비밀키로 암호화한 메시지 다이제스트(message digest)이다. 메시지 다이제스트는 서로 다른 메시지에서 같은 다이제스트가 산출될 수 없도록 메시지의 텍스트에서 산출된 간단한 문자열이다. 이는 송신시 우연히 메시지가 변경되는 일없이 메시지를 송신할 수 있도록 하는데 유용하다. 메시지 다이제스트에 사용되는 함수가 잘 알려져 있기 때문에 고의적인 메시지의 변경을 방지할 수는 없다. 즉, 악의의 제3자가 다이제스트와 함께 전송되는 메시지를 가로채어 메시지를 변경하여 새로운 다이제스트를 산출하여 송신할 수 있다. 그러나 송신자가 비밀키를 사용하여 메시지 다이제스트를 암호화한 전자서명이 있는 경우에는 송신자 외의 사람이 메시지를 변조하기란 어렵다. 악의의 제3자가 그 메시지를 가로채어 변경하고 새로운 메시지를 산출할 수는 있다. 그러나 송신자의 비밀키없이 다이제스트를 암호화할 수 없기 때문에 수신자는 그 메시지가 변조되었는지를 확인할 수 있다. 따라서 메시지 다이제스트와 전자서명은 어떤 메시지가 특정인으로부터 송신되었고 그 내용이 변조되었는지를 확인하는 데 사용된다.

또는 운영중인 결제시스템

II. 결제시스템의 특성과 한계점

2.1 인터넷 결제시스템 현황

2.1.1 사이버캐시

1) 개요

1994년에 설립된 사이버캐시사에서는 신용카드를 이용하는 인터넷 상거래 결제시스템인 사이버캐시(CyberCash)를 개발하여 운영하고 있다. 이 시스템의 주요 구성요소는 소비자용 소프트웨어(CyberCash Wallet), 판매자용 SMPS(Secure Merchant Payment System) 소프트웨어, 판매자·소비자·은행간의 상호연결 및 결제처리기능을 수행하는 게이트웨이 서버이다[4].

소비자는 컴퓨터에 Wallet 소프트웨어를 설치하여 시스템에 ID를 설정하고 신용카드 정보를 컴퓨터에 저장해 두면, 이 시스템에 등록된 판매자의 웹사이트에서 제품 또는 서비스를 구매할 수 있다. 이 시스템의 거래과정을 다음과 같다:

〔1〕 소비자는 웹브라우저를 사용하여 판매자의 웹사이트에서 쇼핑을 하고, 어떤 품목에 대한 구매의사를 표시한다. 판매자의 서버에서는 품목, 가격, 거래 ID 등을 고객에게 제시한다.

〔2〕 소비자가 지불 버튼을 누르면, 웹브라우저가 자동적으로 Wallet 소프트웨어를 실행시킨다. 소비자는 이 소프트웨어에서 어느 신용카드로 대금을 지불할 것인지를 선택하고, 확인 버튼을 눌러 판매자에게 주문 정보 및 결제 정보를 송신한다. 이 때 Wallet 소프트웨어에서는 결제정보를 암호화하여 송신한다.

〔3〕 판매자는 결제정보에 판매자 확인정보를 추가하여 암호화하고, 비밀키로 전자서명을 하여 이 결제정보를 사이버캐시 서버에 보낸다. 이때 판매자는 암호화된 소비자의 신용카드 정보를 볼 수 없다.

〔4〕 사이버캐시 서버에서는 방화벽이 설치된 시스템내에서 모든 정보를 수신하고, 구매자와 판매자의 신원을 확인하여 거래를 처리한다. 게이트웨이 서버에는 특수 장치가 설치되어 있어 모든 메시지를 복호화할 수 있다. 그후 서버에서는 전용선을 통해 판매자 거래 은행에 거래 정보를 송신한다.

〔5〕 판매자 은행에서는 카드회사를 경유하여 발행은행 또는 직접 카드회사에 승인 요청서를 보낸다. 그후 사이버캐시 서버에서는 소비자의 신용상태에 따라 승인 또는 거절 코드를 수령한다.

〔6〕 사이버캐시 서버에서는 승인(이 경우에는 디지털 영수증을 판매자에게 송신한다), 또는 거절 코드를 판매자에게 송신하고, 판매자는 이 코드를 소비자에게 송신한다.

4) 사이버캐시 Wallet은 윈도우즈와 매킨토시 운영체제에서 작동되는 소프트웨어로서 소비자가 인터넷에서 쇼핑을 할 때 넷스케이프와 모자익 등의 웹브라우저와 연결되어 신용카드 사용에 따른 보안 기능을 제공해 준다. 현재 이 소프트웨어는 사이버캐시사에서 무료로 제공되고 있다. SMPS는 사이버캐시사에서 판매자에게 제공하는 소프트웨어로서 구매자의 사이버캐시 및 사이버캐시 게이트웨이 서버와 연결되어 판매자가 인터넷에서의 신용카드 거래를 처리할 수 있도록 해준다. 또한 이는 카드처리, 거래상태조사, 회계 및 재고관리를 지원하는 데이터베이스 기능을 수행한다. 800번 전화 주문, 팩스와 전자우편 주문에 대한 결제처리기능도 수행한다. 사이버캐시 게이트웨이 서버는 판매자, 소비자, 은행을 상호 연결해 주는 소프트웨어 및 하드웨어 플랫폼으로서 방화벽이 구축되어 인터넷과 다른 금융 네트워크와의 자료 교환, 사이버캐시 Wallet ID의 유지 및 인증, 메시지 추적 기능 등을 수행한다.

사이버캐시사의 보고에 따르면, [1]에서 [6]까지 처리되는 데는 약 15-20초가 소요된다.

2) 사용 현황

사이버캐시사에서는 1995년 5월부터 이 시스템을 통해 인터넷 상거래를 실시하고 있다. 이 시스템에서는 매일 수천건의 거래가 이루어지고 있으며, 미국에서 80% 이상의 은행이 이 시스템과 연결되어 있다.

현재 이 시스템의 사용자는 미국 은행에 계좌를 소유하고 어메리칸 익스프레스, 비자, 디스카버, 마스트카드, 아멕스 등의 신용카드 소유자에 한정되어 있다. 이 시스템에서는 향후 전자동전인 사이버코인(CyberCoin)과 전자수표에 의한 결제시스템을 추가할 것으로 알려져 있다.

2.1.2 퍼스트 버츄얼

1) 개요

퍼스트 버츄얼 홀딩스(First Virtual Holdings)에서 개발한 퍼스트 버츄얼(First Virtual: FV) 시스템은 신용카드번호와 같은 민감한 정보를 인터넷으로 전송하지 않고 전자우편을 통해 소비자의 구매의사를 확인하는 절차로 구성된 신용카드 모형에 기반을 인터넷 상거래 결제시스템이다.

이 시스템을 이용한 상거래 과정은 다음과 같다:

[1] 판매자는 일반 우편으로 은행계좌번호를 FV에 통보하여 버츄얼 핀((PIN)을 발급받아 등록을 한다. 그리고 판매할 정보제품을 판매자의 웹서버 또는 퍼스트 버츄얼사의 인포호스(InfoHaus) 서버에 웹사이트를 개설한다.

[2] 소비자는 전화로 FV에 신용카드번호를 알리고 등록하여 사용자 고유번호에 해당하는 버츄얼 핀을 발급받는다. 판매자나 소비자는 동일한 버츄얼 핀으로 정보제품을 판매하고 구매할 수 있다. 소비자는 웹브라우저, 텔렛, FTP, 전자우편, 그 어느 것을 이용하여서도 정보제품을 구매할 수 있다.

[3] 소비자는 판매자의 웹사이트 또는 인포호스에서 쇼핑을 하고, 구매 요청을 하면, 판매자는 구매자의 핀을 요청한다.

[4] 구매자가 정보를 다운로드하기에 앞서, 판매자의 서버 또는 퍼스트 버츄얼 인포호스에서는 구매자의 핀을 확인한다.

[5] 퍼스트 버츄얼사에서는 구매자에게 전자우편을 보내어, 구매자가 정보제품을 구입할 것인지에 대한 동의를 받는다.

[6] 구매자는 퍼스트 버츄얼의 전자우편 메시지에 "예", "아니오", 또는 "사기"형태로 응답한다.

[7] 구매자의 구입의사가 확인된 경우, 퍼스트 버츄얼에서는 판매자에게 이를 통지를 하고, 구매자의 퍼스트 버츄얼 계좌에 거래를 추가한다. 정기적으로 퍼스트 버츄얼에서는 구매자의 모든 누적 거래에 대한 요금을 신용카드를 통해 청구한다. 결제시 퍼스트 버츄얼에서는 수수료를 공제하고 자금을 판매자 계좌에 이체한다.

2) 사용 현황

퍼스트 버츄얼 홀딩스사는 1994년에 설립되었고, 1995년 10월에 퍼스트 버츄얼로 서비스를 개시하였다. 1996년 현재 이 시스템에 등록한 판매자의 수는 3,300이며, 정보제품만을 취급하고 있다. 향후 이 시스템에서는 정보제품 외에도 유형의 재화를 취급할 예정인 것으로 알려져 있다.

소비자가 이 시스템을 이용하기 위해서는 2불의 등록비를 지불해야 하고, 결제처리비용으로 2불을

지불해야 한다. 한편 판매자는 10불의 등록비, 매 거래시 29센트와 거래 대금의 2%에 해당하는 수수료를 지불해야 하고, 정기적으로 거래 대금이 결제될 때 1불의 결제처리비용을 부담해야 한다.

2.1.3 네트빌

1) 개요

카네기멜론대학에서 개발한 네트빌(NetBill)은 전자수표 또는 전자선불카드(electronic debit card) 방식에 의한 인터넷 상거래 결제시스템이다. 이 시스템은 인터넷에서의 소액거래를 지원하도록 설계되었고, 현재로서는 정보제품만을 취급하고 있다.

네트빌에 등록한 구매자는 판매자의 웹서버에 접속하여 암호화된 정보제품을 수령하고, 판매자는 구매자로부터 정보제품을 수령했다는 영수증을 받아 이를 네트빌에 제시하여 지불승인을 받는다. 그런 다음 판매자는 구매자에게 정보제품을 복호화할 수 있는 비밀키를 전송한다. 소비자는 지불에 앞서 정보제품을 수령하고, 판매자는 결제가 이루어진 후 비밀키를 송신하므로 소비자와 판매자 모두가 상호 신뢰할 수 있다.

소비자와 판매자는 웹브라우저에서 작동되는 네트빌의 소프트웨어(Money tool)를 사용하여 거래정보를 교환한다. 네트빌 서버에서는 소비자와 판매자 계정을 유지·관리한다. 이들 계정은 각자의 거래은행 계좌와 상호 연결되어 있다. 판매자가 소비자에게 정보제품과 비밀키를 송신하면, 소비자의 네트빌 계정에서 판매자 네트빌 계정으로 거래대금이 이체된다. 필요한 경우, 소비자 거래 은행으로부터 네트빌 계정에 자금이 전송되고, 판매자 네트빌 계정에서 그 거래은행의 계좌에 자금이 이체되기도 한다.

2) 사용 현황

이 시스템은 1996년 12월부터 카네기멜론대학에서 시범 운영되고 있다. 카네기멜론대학에서는 모자익·넷스케이프 등의 웹브라우저에서 작동될 수 있는 소비자용 클라이언트 소프트웨어와 판매자용 서버 소프트웨어를 개발하고 있다.

2.1.4 네트체크

1) 개요

네트체크(NetCheque) 시스템은 DES 암호알고리즘을 이용한 인증프로토콜인 커버러스(Kerberos)에 기반을 전자수표에 의한 결제시스템이다(Neuman and Ts'o, 1994). 네트체크 시스템의 서버에 등록한 사용자들은 인터넷을 통해 다른 사용자 또는 판매자에게 전자수표를 발행하여 제품 또는 서비스 대금을 결제할 수 있다.

네트체크에 의한 전자수표가 발행되어 사용되는 방법은 인터넷에서 전자적으로 사용된다는 점을 제외하고는 일반 수표와 매우 유사하다. 네트체크를 발급하는 은행의 계좌를 갖고 있는 사용자는 지불인 이름, 금융기관명, 계좌번호, 수취인명, 금액 등을 기재한 전자수표를 발행한다. 그 모든 정보는 인터넷을 통해 암호화되어 전송된다. 전송되는 정보를 암호화하는 데는 대칭키 암호 알고리즘인 DES가 사용된다. 일반 수표에 지불인이 서명을 하는 것과 마찬가지로 계좌 소유자가 수표를 발행했다는 것을 인증하는 방법으로 전자서명이 이용된다. 일반 수표와 마찬가지로 수취인은 전자수표에 자신의 전자서명을 통해 이를 배서할 수 있다. 네트체크는 인터넷에서의 소액거래를 지원할 수 있도록 설계되어 있다.

2) 사용현황

사우스캘리포니아대학 정보과학연구소(ISI)의 GOST (Global Operating Systems Technology) 그룹에서는 현재 네트체크 시스템을 개발하고 있으며, 네트체크 데모 계정을 통해 시험 중에 있다. 전자수표의 무결성을 보호하며 전자서명을 지원하고 웹브라우저와 연동되는 네트체크 소프트웨어인 nc 프로그램도 개발 중에 있다. 또한 ISI에서는 네트체크와 결합하여 사용할 수 있는 전자화폐의 일종인 네트캐시(NetCash)도 개발 중에 있다.

2.1.5 이캐시

1) 개요

1990년에 설립된 디지캐시(DigiCash)사는 네덜란드의 암스테르담에 본사를 두고 있다. 이 회사에서 개발한 이캐시(ecash) 시스템은 이캐시라는 전자동전을 사용하는 인터넷 상거래 결제시스템이다. 이 시스템에서는 이캐시 소프트웨어가 사용된다. 사용자는 디지캐시사의 웹사이트에서 이캐시

〈표 1〉 신용카드 및 전자수표 모델에 기초한 결제시스템

	CyberCash	First Virtual	NetBill	NetCheque
URL	http://www.cybercash.com/	http://www.fv.com/	http://www.netbill.com/	http://nii-server.isi.edu/NetCheque/
설립년도 및 조직	1994년, CyberCash	1994년, First Virtual Holdings	카네기멜론대학	사우스캘리포니아 대학, ISI의 GOST 그룹
운영현황	1995. 5., 수천건거래/일, 미국 은행의 80%	1995. 10. 1996년 현재 3,300개의 판매업체의 등록	시범운영 중	데모계정을 통해 시험 중
거래 제품 및 서비스	재화와 정보제품	정보제품	정보제품	재화 및 정보제품
소비자 사용조건	등록 및 CyberCash Wallet 소프트웨어(MS Windows와 Macintoch에서 지원됨)	등록, 웹브라우저, FTP, 전자우편	소비자용 클라이언트 소프트웨(money Tool)	등록 및 클라이언트 소프트웨어
판매자 사용조건	등록 및 SMPS 소프트웨어(Solaris, BSDI, SunOS, Windows NT 등에서 지원됨)	등록 및 웹사이트 개설	판매자용 서버 소프트웨어 개발 중	등록 및 판매자용 소프트웨어
결제모형	신용카드	신용카드	전자수표	전자수표
프로토콜	비공개	공개	공개	공개
계획 중인 지불수단	전자동전(CyberCoin)과 전자수표	고액거래를 위한 암호방식의 도입	없음	전자화폐(NetCash)

소프트웨어를 무료로 다운로드받을 수 있다. 사용자는 인터넷웹로 이캐시 발행은행의 계좌를 개설할 수 있다. 사용자는 웹브라우저에서 실행되는 이캐시 소프트웨어를 작동하여 고객이름 및 기타 세부사항을 묻는 박스의 빈칸을 채움으로써 쉽게 은행계좌를 개설할 수 있다.

등록된 고객은 이캐시 계좌에서 전자동전을 인출하여 자신의 하드디스크에 저장해 둔다. 그리고 그는 판매자의 웹사이트에 접근하여 제품 또는 서비스를 구매하고 판매자에게 일정 금액의 전자동전을 지불한다. 판매자는 고객의 이캐시를 수락하기에 앞서 고객의 발행은행에 이캐시를 제시하여 유효여부를 확인하고, 이캐시 수령증과 함께 구매 품목을 고객에게 전달한다. 전자동전을 수령한 판매자는 이를 새로운 동전으로 대체하여 그의 하드디스크에 저장해 둘 수도 있고, 그의 이캐시 계좌에 입금할 수도 있다.

이캐시를 취급하는 판매자가 되기 위해서는 은행으로부터 이캐시 판매계정을 개설해야 한다. 이 시스템을 사용하는 고객간에도 이캐시가 교환될 수 있다.

2) 사용현황

디지캐시사에서는 1994년부터 1년 동안 가상화폐인 사이버벅(Cyberbuck)을 통해 이캐시를 시험적으로 운영한 바 있다. 사이버벅은 일반 화폐와는 교환될 수 없고 이 시스템을 이용하는 판매자로부터 제품이나 서비스를 구매하는 데만 사용될 수 있도록 하였다. 사이버벅 시범운영에는 약 30,000명의 소비자와 100명 이상의 판매자가 참여하였다.

소비자가 이캐시를 사용하기 위해서는 발행은행에 계좌를 개설하고, 이캐시 소프트웨어를 PC에 설치하면 된다. 판매자는 발행은행의 판매자 계정을 개설하고 웹사이트를 개설한다. 이캐시 시스템을 이용하고자 하는 은행에서는 특수한 암호화 하드웨어를 설치해야 한다. 디지캐시사에서는 이캐시의 기술 공급자로서 은행 및 기타 금융기관에 라이센스를 공급하는 정책을 채택하고 있다. 디지캐시사는 직접 결제시스템을 운영하지 않고, 라이센스를 취득한 은행에서 이 결제시스템을 운영하게 된다. 1995년 10월 이래로 미국의 마크트웨인 은행(Mark Twain Bank)에서는 미달러 표시의 이캐시를 발행하게 되었다. 마크트웨인 은행의 "세계화폐 구좌(World Currency Access Acount)"의 1차 계좌는 달러 한정으로 이캐시와 직결되어 있는 것에 비하여 2차계좌는 소비자나 상점이 임의의 통화를 지정할 수 있다. 2차계좌는 일반의 보통예금의 성격을 띤다. 따라서 1차계좌는 예금이자가 붙지 않지만 2차계좌는 보통예금이자가 붙는다. 1차 및 2차 계좌는 미정부의 예금자보호법의 대상이다. 그러나 이캐시는 미정부의 예금자 보호법의 대상에서 제외된다. 1996년 3월부터 이유네트(EUnet)에서는 핀란드 마르크로 이캐시를 발행하게 되었다. 또한 독일의 도이취 은행에서도 이캐시를 발행할 예정인 것으로 알려져 있다.

2.1.6 몬덱스

1) 개요

몬덱스(Mondex)란 마이크로칩에 암호화된 전자현금을 저장하고 있는 스마트카드(smart card)로서 현금과 마찬가지 형태로 거래에 따른 결제수단으로 사용될 수 있다. 이는 인터넷에서는 물론이고 몬덱스 관련 특수 장치가 설치된 일반 소매점에서도 제품 또는 서비스 구매에 따른 대금결제에 사용

될 수 있도록 설계되어 있고, 현금과 마찬가지로 개인간의 가치교환에도 사용될 수 있다. 몬덱스 카드는 한 번에 5종류의 화폐를 취급할 수 있도록 설계되어 있어 여러 국가에서 교환수단으로 사용될 수 있다.

몬덱스를 이용하기 위해서는 발행은행에 계좌를 개설하여야 하는 것은 물론이고, 몇몇 특수 장치를 필요로 한다. 소비자가 몬덱스를 사용하기 위해서는 최소한 몬덱스카드와 잔액판독기가 필요하고, 판매자는 가치전송터미널을 설치해야 한다. 그 외도 특수 장치로는 몬덱스 ATM, 몬덱스 전화, 몬덱스 Wallet 등이 있다[5].

소비자가 몬덱스를 사용하기 위해서는 최소한 몬덱스카드와 잔액판독기가 필요하다.

2) 사용 현황

내트웨스트 은행(NatWest Bank)과 미들랜드 은행(Midland Bank)은 몬덱스 UK라는 합작투자 회사를 설립하였고, 그 후 영국전신전화사(British Telecommunications: BT)와 협력하여 런던 근교의 스윈던(Swindon)에서 1995년 7월부터 몬덱스를 시험 운영하고 있다. 이 시험 운영에는 40,000명의 소비자들과 1,000개의 소매점이 참여하였다. 또한 샌프란시스코에 위치한 웰스파고(Wells Fargo) 은행의 500명의 종업원들이 약국, 커피숍, 서점, 레스토랑 등의 22개 판매자와의 거래에서 몬덱스를 이용하고 있다. 그 외도 홍콩과 캐나다 등에서 시험 운영할 계획을 갖고 있는 것으로 알려져 있다. 영국, 호주, 캐나다 등 세계 17개 은행이 몬덱스에 참여할 것으로 알려져 있다[6].

몬덱스는 소매점에서 이용될 수 있는 전자화폐로 개발되었기 때문에 인터넷 상거래에 이용되기 위해서는 컴퓨터에 장착할 특수한 장치가 필요하다. 현재 일본의 히다치사에서 이 특수 장치를 개발하고 있다.

---

5) 몬덱스 ATM이란 몬덱스 카드를 사용하여 은행에서 현금을 인출하여 그 가치를 카드에 저장하고, 카드에 저장된 현금을 은행의 계좌에 예금하거나 카드에 있는 잔액을 확인하는데 사용될 수 있도록 ATM에 몬덱스 IC 카드의 판독/쓰기 장치가 설치된 특수한 장치이다. 몬덱스 전화란 전화망을 통해 현금을 전송할 있는 특수 장치의 전화기이다. 몬덱스 전화기에는 기존의 전화기 기능 외에도 LCD 디스플레이가 장착되어 있어 카드 사용자가 원격지에 있는 은행과 소매점에 가치를 교환하고, 몬덱스 카드 사용자간에 현금을 교환하는 기능이 추가되어 있다. 현재 히다치에서는 이들 특수 장치를 개발하고 있다(Hitachi, 1996).
몬덱스 Wallet은 키보드와 스크린이 장착된 호주머니에 넣어 다닐 수 있는 크기의 전자지갑으로서 여기에 카드를 삽입하여 다른 몬덱스 사용자의 카드에 가치를 전송할 수 있다. 예를 들면, 몬덱스 Wallet을 사용하여 아들의 몬덱스 카드에 용돈을 전송해 줄 수 있고, 택시기사가 손님의 카드로부터 요금을 수령할 수 있다. 또한 이 전자지갑을 사용하여 카드에 필요한 최소 금액만을 저장할 수 있으며, 카드 잔액조회도 가능하다. 따라서 카드를 분실하는 경우에는 카드에 저장된 금액만 분실된다. 히다치에서 이 전자지갑을 개발하고 있다.
잔액 판독기(balance reader)는 몬덱스 카드의 잔액을 조회할 수 있는 소형 장치로서 카드 판독기와 스크린이 장착되어 있다.
몬덱스 가치 전송 터미널(mondex value transfer terminals)은 소매점에서 몬덱스 카드로 결제 및 가치 전송을 위해 사용되는 장치로서 출력화면과 영수증 발급을 위한 프린터가 장착되어 있다. 이 터미널의 몬덱스 카드 판독/쓰기 장치에서는 몬덱스 카드의 유용성을 판별할 수 있어 별도의 인증 절차를 밟을 필요가 없다. 신문 배달원과 같이 자주 이동하면서 판매 및 요금 수령을 하는 사용자를 위해 밧데리가 장착된 이동식 터미널도 개발되고 있다.

6) 영국의 NatWest와 Midland 은행, 홍콩의 Hongkong and Shanghai Banking Corporation Limited, 캐나다의 Canadian Imperial Bank of Commerce와 Royal Bank of Canada, 호주의 Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia 등, 뉴질랜드의 ANZ Banking Group Limited와 Bank of New Zealand 등, 미국의 Wells Fargo Bank와 AT&T 등.

〈표 2〉 전자화폐 모형에 기초한 결제시스템

	ecash	Mondex
URL	http://www.digicash.com/ecash/	http://www.mondex.com/mondex/
설립년도 및 조직	1990년, 네덜란드의 DigiCash	NatWest은행, Midland은행의 합작투자회사: Mondex UK(BT참여)
운영현황	1994년부터 1년간 Cyberbuck의 시험 (판매자: 300, 소비자: 30,000명), 1995년 10월부터 Mark Twain은행에서 전자동전을 발행	1995년 7월부터 Swindon에서 시범운영 (40,000명의 소비자, 1,000개의 소매점)
발행은행	마크트웨인 은행, 기타 독일 및 핀랜드 은행	영국, 캐나다, 홍콩, 호주 등 세계 17개 은행
거래 제품 및 서비스	재화와 정보제품	재화와 정보제품
소비자 사용 조건	계정개설 및 ecash 소프트웨어	Mondex card, card reader(기타 특수 장치의 전화기, PC 등)
판매자 사용조건	계정개설 및 웹사이트 개설	Mondex 터미널
결제모형	전자동전(signature-transporting card)	전자현금(signature-creating card)

2.2 신용카드와 전자수표 모형에 기초한 결제시스템의 특성과 한계점

2.2.1 특성 비교

사이버캐시와 퍼스트 버츄얼은 기존의 신용카드 거래 시스템을 최대한 활용하고 있다. 따라서 신용카드 사용자들은 시스템의 개념적 틀을 쉽게 이해할 수 있고, 인터넷 웹의 사용법을 알면 이들 시스템을 쉽게 사용할 수 있다. 특히 퍼스트 버츄얼의 경우는 전자우편을 통해서도 상거래가 가능하다. 판매자 입장에서도 기존의 POS 구조를 이용하여 운영절차만을 변경하고도 인터넷 상거래에 참여할 수 있다는 것이 이들 시스템의 특징이다.

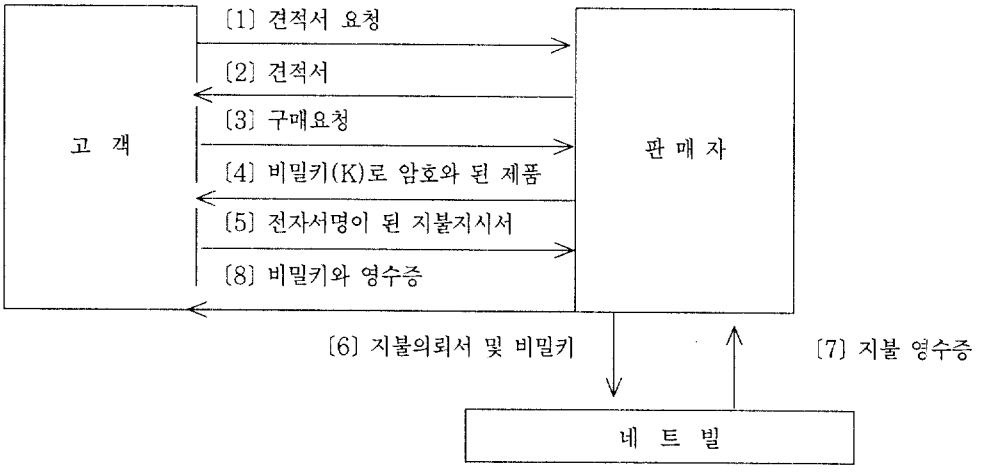
사이버캐시를 이용하고자 하는 소비자는 사이버캐시 웹사이트에서 무료로 제공하는 Wallet 소프트웨어를 설치하고, 판매자의 경우는 SMPS 소프트웨어를 설치해야 한다. 소비자용 Wallet 소프트웨어에서는 구매내역을 관리하고, 판매자용 SMPS 소프트웨어에서는 구매자별 또는 신용카드별 거래정보를 관리할 수 있다는 점에서 일반 신용카드거래에 비하여 사용자의 편리성이 증가된다. 또한 이 시스템에서 소비자의 신용카드번호를 비롯한 비밀정보는 Wallet 소프트웨어에 의해 소비자의 컴퓨터에 암호화되어 저장되고, 소비자는 비밀번호를 사용하므로써 타인의 접근을 방지하고 거래시마다 신용카드번호를 입력하지 않아도 된다. 퍼스트 버츄얼의 경우, 판매자는 특수한 장비와 소프트웨어 또는 인터넷 웹서버가 없는 경우에도 정보제품을 판매할 수 있어 사용하기가 단순하고, 소비자와 판

매자는 웹, FTP, 전자우편 등 어느 하나만 이용할 수 있는 경우라도 인포호스에서 정보제품을 사고 팔 수 있다.

두 시스템간의 중요한 차이점 중의 하나는 보안을 유지하는 방법이다. 사이버캐시 시스템에서는 DES 대칭키 및 RSA 공개키 암호방식을 이용하여 메시지의 기밀성을 유지하고, 전자서명을 통해 판매자와 구매자의 신원을 파악하도록 함으로써 인터넷 보안을 유지하고 있다. 또한 사이버캐시 시스템과 금융네트워크를 연결하는 게이트웨이 서버에는 방화벽이 설치되어 기존의 금융 네트워크와 연결된다. 이 시스템에서 구매자는 판매자에게 전송하는 신용카드정보를 암호화하기 때문에 판매자가 이를 알 수 없다. 따라서 판매자가 구매자의 신용카드를 남용할 가능성이 제한된다. 이 시스템의 서버에서는 금융기관을 통해 구매자의 신용상태를 파악하고, 판매자는 구매자에게 전자지불영수증을 발급함으로써 구매자의 제품수령 또는 반환을 보증하고 있다. 퍼스트 버츄얼에서는 암호방식을 이용하지 않고 있다. 이 시스템에서는 인터넷에서 보안이 유지되어야 할 민감한 정보(신용카드번호, 은행계좌번호 등)과 인터넷을 통해 전송해도 되는 정보를 분리하여 민감한 정보를 인터넷으로 전송하지 않고 단지 버츄얼핀만을 인터넷을 통해 전송하는 전략을 펴고 있다. 실제 구매자가 아닌 타인에 의한 사기를 방지하기 위해 이 시스템에서는 소비자에 대한 구매의사를 확인하는 방법으로 전자우편이 이용되고 있다.

기본적으로 전자수표 모형에 기반을 두고 있는 네트빌과 네트체크의 경우, 사용자는 이들 웹사이트에서 제공하는 소프트웨어를 설치해야 한다. 현재 네트빌의 경우는 소프트웨어를 개발하여 시범중에 있고, 네트체크의 경우는 소프트웨어를 개발하고 있는 것으로 알려져 있다.

네트빌의 중요한 특성은 소비자와 판매자가 상호 신뢰할 수 있도록 보증하는 방법이다. 〈그림 1〉의



출처: NetBill: An Internet Commerce System Optimized for Network Delivered Services, http://www.cmu.edu/NETBILL/, p. 3

〈그림 1〉 네트빌의 거래 프로토콜

거래 프로토콜을 살펴보면, 이 특징을 쉽게 이해할 수 있다.

〔1〕 구매자는 판매자에게 견적서를 요청한다.

〔2〕 판매자는 소비자가 제시하는 커버러스 티켓으로 승인된 구매자인지를 확인하고, 전자서명을 한 견적서(제품ID, 가격, 거래ID 등)을 구매자에게 송신한다.

〔3〕 구매자는 전자서명을 한 구매요청서를 판매자에게 송신한다.

〔4〕 판매자는 비밀키(K)로 암호화된 제품을 소비자에게 전송하고, 암호 메시지(정보제품)의 체크섬(checksum)을 계산한다.

〔5〕 정보제품을 수령한 구매자는 암호 메시지의 체크섬을 계산하고, 전자서명을 한 EPO (Electronic Payment Order: 제품 ID, 가격, 체크섬, 타임스탬프 등)을 판매자에게 송신 한다(이는 한장의 전자수표를 발행하는 것과 같다). EPO에는 판매자와 네트빌 서버 모두가 판독할 수 있는 정보와 네트빌 서버만이 판독할 수 있는 정보가 들어 있다.

〔6〕 판매자는 EPO를 수령하여 송신시 계산해 둔 체크섬과 EPO의 체크섬을 비교하여 일치하는 경우, 정보제품이 오류없이 전달되었다는 것을 확인한다. 판매자는 전자서명을 한 송장과 EPO를 네트빌 서버에 송신한다.

〔7〕 네트빌 서버에서는 제품, 가격, 체크섬을 조사하여 소비자와 판매자의 거래가 완전한지를 조사한다. 또한 여기서는 구매자 계정의 지불 능력을 조사하여, 구매자의 네트빌 계정에서 판매자 계정으로 거래금액을 이체하고, 거래를 기록하고 복호키의 복사본을 저장해 둔다. 그 후 서버에서는 전자서명을 한 영수증을 판매자에게 송신한다. 이 전자서명에는 DSA(Digital Signature Algorithm)가 이용된다.

〔8〕 판매자는 복호키를 구매자에게 송신한다.

소비자가 주문한 제품이 판매자가 인도한 제품과 다를 경우, 소비자는 그가 주문한 제품, 결제금액, 네트빌에 저장해 둔 복호키 등의 네트빌 영수증을 통해 분쟁을 해결할 수 있다. 〈그림 1〉의 거래과정에서 알 수 있듯이 구매자입장에서는 결제에 앞서 정보제품을 수령하고, 결제후 복호키를 수령하지 못한 경우에는 네트빌 서버에서 이를 제공한다는 점에서 제품인도를 확신할 수 있다. 또한 판매자 입장에서는 결제 후에 복호키를 제공함으로써 미결제의 위험을 제거할 수 있다. 〈그림 1〉의 과정 〔5〕에서 EPO는 구매자가 전자서명을 한 전자수표이다. 전자수표의 내용은 암호화되어 있고, 판매자는 구매자의 비밀이 되는 정보를 판독할 수 없고 네트빌 서버에서만 이 정보를 판독할 수 있다. 따라서 구매자는 판매자로부터 구매능력에 관한 정보를 비밀로 유지할 수 있다는 점에서 부분적인 프라이버시가 보증된다.

RSA 암호방식에 의한 사용자의 비밀키는 사용자가 기억하기 어려운 관계로 네트빌에서는 사용자가 비밀번호를 사용하여 전자서명을 할 수 있도록 하고 있다. 사용자 비밀번호에 의한 대칭키로 암호화된 비밀키는 네트빌 서버에 저장되어 사용자가 비밀번호를 입력하면, 자동적으로 전자서명이 이루어진다는 점에서 사용자 편리성이 제공된다.

네트체크에서는 공개키 암호방식이 아닌 비밀키 암호방식에 기반을 둔 커버러스 인증 시스템을 이용하고 있다(Neuman and Ts'o, 1994). 여기서는 커버러스를 이용함으로써 인증을 위한 전자서

명, 정보의 기밀성, 자료의 무결성 등의 보안 서비스가 제공된다. 따라서 처리속도 관점에서 이 시스템은 공개키 암호방식을 이용하는 시스템보다 효율적이라 할 수 있다(Mankin, 1994). 커버러스 시스템을 이용하여 산출되는 특수한 티켓인 전자수표는 배서될 수 있으며, 은행간에도 교환될 수 있도록 설계되어 있다는 점이 네트빌과 비교하여 이 시스템의 특징이라 할 수 있다. 네트빌과 마찬가지로 사용자는 웹브라우저와 연동되는 소프트웨어를 사용하여 단순히 전자서명을 함으로써 한 장의 수표를 발행하게 된다.

사이버캐시나 버스트버츄얼과 같은 신용카드 모형에 기반을 둔 시스템에 비하여 네트빌과 네트체크의 경우는 소액거래를 잘 지원할 수 있다. 퍼스트 버츄얼에서는 신용카드 거래의 한계점이라 할 수 있는 소액거래상의 문제를 해결하기 위한 한가지 방안으로 특정 구매자에 대해 일정 시간 또는 누적 거래액이 어느 한도에 도달할 때 결제처리를 하는 방법을 채택하고 있다.

2.2.2 한계점 비교

판매자 중심의 결제시스템과 비교해 볼 때, 위에서 제시된 4개의 시스템에서는 구매자의 계정번호와 신용카드 번호 등의 비밀이 되는 정보를 판매자에게 노출시키지 않는다는 점에서 어느 정도 구매자의 프라이버시를 보호하고 있다. 그러나 신용카드와 수표의 일반적 특성상 모든 거래 관련 정보는 시스템의 서버에 저장되기 때문에 전자화폐의 경우만큼 익명성과 구매자의 프라이버시를 보증하지는 못한다.

4개의 모든 시스템에서의 공통된 한계점 중의 하나는 오프라인(off-line) 기능이 없기 때문에 각 시스템의 안전성은 인터넷 자체의 안전성과 서버의 안전성에 의존한다는 점이다. 사이버캐시, 네트빌, 네트체크 등의 소프트웨어 기반의 이들 시스템에서 이러한 한계성을 극복하기란 현재의 기술로서는 어려울 것으로 보인다. 이와 더불어 이들 시스템에서는 온라인만으로 거래가 이루지는 만큼 서버의 과부하도 하나의 문제점으로 지적된다. 서버의 과부하 문제를 해결하기 위해서는 오프라인 능력을 제공하거나 분산화하는 것인데 네트체크를 제외한 3개의 시스템에서는 아직 이 문제를 해결하기 위한 방안이 제시되지 않고 있다. 네트체크에서는 한 개 서버에서의 과부하를 줄이기 위해 다수의 인증 서버에 부하를 분산화하는 방안을 채택하고 있다.

퍼스트 버츄얼을 제외한 암호방식을 사용하는 3개의 시스템에서도 보안상의 문제가 지적되고 있다. 사이버캐시에서는 신용카드정보를 사용자 소프트웨어에 저장해 두는 방법을 이용하고 있다. 퍼스트 버츄얼의 Borenstein 등(1995)의 연구와 퍼스트 버츄얼사(1996)에 따르면, 메시지가 암호화되기 전에 키보드로 입력되는 메시지를 포착하여 분석하는 (키보드 드라이브에 부착되는) 프로그램(pre-encryption program)을 개발하여 신용카드 번호를 입력하는 결제시스템의 위험을 예시한 바 있다. 또한 이 실험에 따르면, 사용자의 비밀번호도 이 프로그램으로 포착할 수 있다. 네트빌의 경우 모든 사용자의 비밀번호가 네트빌 서버에 저장된다. 이는 네트빌 서버에서 문제가 발생하는 경우에 전체 사용자들의 비밀번호가 재발급되어야 하고, 계속적으로 사용자 비밀번호의 노출 상태가 추적되어야 함을 의미한다. 네트체크는 커버러스 인증 프로토콜에 기반을 두고 있는 만큼, 커버러스 프로토콜의 한계점을 극복하기 어렵다(Bellovin and Merritt, 1990). 특히 해커의 비밀번호 추정 및 타임스탬프 사용에 따른 문제점이 크게 지적되

고 있다. 네트빌의 경우와 마찬가지로 네트체크의 데이터베이스에는 모든 사용자들의 비밀키가 저장되어 있어 서버에 보안상의 문제가 발생하는 경우에는 위조 또는 사기거래가 가능하게 되고, 모든 사용자들은 새로운 비밀번호를 사용해야 한다. 네트체크에서는 서버간 상호 인증을 가능하게 하기 위해 다수의 인증 서버에 사용자의 비밀키가 공유되기 때문에 비밀키가 노출될 가능성이 높다.

퍼스트 버츄얼에서는 현재 암호방식을 사용하고 있지 않고 단지 전자우편만으로 구매자를 확인하고 있기 때문에 몇가지 보안상의 문제점이 노출될 수 있다. 예를 들면, 이 시스템에서 침입자가 먼저 스니핑(sniffing)으로 버츄얼 핀을 훔치고, 전자우편 주소를 알아낸 다음, IP 스퓨핑(spoofing)을 통해 구매자의 컴퓨터에 전송되는 전자우편을 가로채는 경우, 그는 다른 구매자 명의로 거래를 완성할 수 있다.

각 시스템에서 취급하는 거래 상품의 다양성 측면에서 볼 때, 사이버캐시와 네트체크에서는 유형의 재화와 정보제품에 대한 거래를 지원하고 있으나 네트빌은 정보제품에 대한 거래만을 지원하도록 설계되었다. 퍼스트 버츄얼의 경우는 현재 정보제품만을 취급하고 있으나 향후 유형의 재화도 취급할 수 있도록 시스템을 확장해 갈 것으로 보인다.

끝으로 퍼스트 버츄얼의 경우, 소비자는 정보제품에 대한 구매 결정에 앞서 평가 목적으로 그 제품을 다운로드 받아볼 수 있어 소비자 관점에서는 정보제품을 사전에 점검해 볼 수 있는 기회를 갖게 되나, 이는 판매자 관점에서 한계점이 될 수 있다. 모든 판매자가 의무적으로 이를 허락하지 않아도 되지만 대부분의 판매자는 결제에 앞서 정보제품을 평가해 볼 수 있도록 하고 있다. 소비자가 수령한 정보제품에 만족하지 못하는 경우, 소비자가 그 대금을 지불하지 않을 수도 있다. 한편 평가 목적용 버전을 제공하는 판매자에겐 소비자에게 제품에 대한 광고효과를 기대할 수 있다는 점에서 이 방안은 장점으로 작용하기도 한다.

〈표 3〉에서는 각 시스템에서 메시지 기밀성, 상대 인증, 메시지 무결성, 부인방지 등의 기본적인

〈표 3〉 보안서비스 및 거래 당사자간의 신뢰성

	CyberCash	First Virtual	NetBill	NetCheque
암호방식	DES와 RSA	비밀을 유지해야 하는 정보를 인터넷으로 전송하지 않음	DES와 RSA	DES
기밀성	암호화	전자우편, 기타 통신	암호화	암호화, 체크섬
인증성	전자서명	전자우편에 의한 확인	전자서명, Kerberos 티켓, Time stamp	Kerberos 티켓, 전자서명, 타임스탬프
무결성	전자서명	별도 방안이 없음	전자서명	전자서명, 체크섬
부인방지	전자서명	전자우편에 의한 확인	전자서명,	전자서명, 타임스탬프
지불 및 인도(반품과 반환) 보증	CyberCash 서버에서 발행하는 전자영수증	구매자는 정보제품을 검토하고 구매하지 않을 수 있음	전자영수증 및 전자서명	Kerberos 티켓
시스템의 안전성	암호알고리듬, 금융네트워크와 CyberCash를 연결하는 방화벽	전자우편의 보안 능력, InfoHause 서버의 보안능력	암호알고리듬, NetBill 서버의 안전성	Kerberos 프로토콜, 인증서버의 안전성

보안 서비스가 어떻게 이루어지며, 소비자 보호 차원에서 제품 인도를 어떻게 보증하고, 시스템의 안전성에 영향을 주는 요소를 나타내고 있다.

2.3 전자화폐 모형에 기초한 결제시스템의 특성과 한계점

2.3.1 특성 비교

전자화폐의 일반적 특성을 살펴보면 다음과 같다. 고객이 은행에 일정 금액의 전자화폐를 신청하면, 은행에서는 일련번호가 부여된 전자화폐에 전자서명을 하고 소비자의 공개키로 암호화한 전자화폐를 고객에게 송신함과 동시에 고객의 계좌에서 발행한 전자화폐만큼을 공제한다. 고객은 판매자의 웹사이트에서 제품 또는 서비스를 구입하고 전자화폐를 지불한다. 판매자는 은행에 전자화폐를 제시하여 그의 계좌에 입금할 수 있고, 새로운 전자화폐를 발행받을 수도 있다. 전자화폐는 중앙은행에서 발행하지 않고 일반 화폐에 기반을 두고 있으므로 법정화폐는 아니다. 또한 전자화폐는 디지털 자료로 전송선을 통해 그 가치가 교환되므로 특수한 방식으로 설계되지 않을 경우에는 쉽게 복사하여 이중으로 사용될 수도 있다.

현재까지 다양한 유형의 전자화폐가 개발되어 사용되고 있거나 개발 중에 있다. 이들 전자화폐는 전화카드와 같이 특정 전용망에서 일회성으로 그 사용이 제한되는 것, LETSystems(1995)와 같이 한 국가 화폐로 표시되지 않고 특정 사용자들간에 교환되며 한 번 전자화폐로 발행되면 일반화폐로 교환될 수 없는 것 등에서 사용자의 익명성이 보장되고 가분성 조건이 충족되며 다수 국가의 법정화폐와 교환될 수 있는 전자화폐에 이르기까지 그 종류가 다양한다.

이캐시나 몬덱스와 같은 전자화폐에 기반을 결제시스템에서는 일반화폐를 이용하는 경우에 비해 사용자들에게 다음과 같은 편리성을 제공해 준다. 첫째로 사용자는 잔돈을 거슬러 줄 필요가 없고, 사용자의 거래내역을 상세하게 관리할 수 있다. 둘째는 사용자만이 아는 일련번호를 은행에 신고함으로써 분실한 전자화폐를 회수할 수 있다.

몬덱스는 카드 소유자가 비밀번호를 사용하여 다른 사람이 승인없이 카드를 사용하는 것을 방지할 수 있도록 설계되어 있다. 카드를 분실 또는 도난당한 경우, 비밀번호를 알지 못하는 사람은 그 카드에 저장된 가치를 사용할 수 없기 때문에 카드 소유자 외의 사람에게는 쓸모가 없다. 또한 카드의 마이크로 칩에는 카드발행은행에서 기록한 16비트(digits) 크기의 고유번호가 저장되어 있고, 이는 발행은행의 데이터베이스에도 저장되어 있어 분실카드가 정당한 소유자에게 반환될 수 있다. 몬덱스 카드에는 최근 10개의 거래에 대한 내역을 저장할 수 있다. 비밀번호를 알고 있는 카드 소유자만이 전자지갑에 카드를 삽입하여 어디에서 어떤 용도로 카드를 사용했는지에 대한 정보를 알 수 있다. 또한 이 카드에서는 한 번에 다섯 종류의 서로 다른 화폐를 저장 또는 교환할 수 있다.

이캐시 시스템에서는 컴퓨터의 고장 또는 시스템의 불안정으로 인해 발생한 분실 동전을 회복하는 절차를 마련하고 있다. 사용자 컴퓨터에 고장이 발생하여 저장해 둔 동전을 잃어버리게 된 경우, 이를 회수하기 위해서는 발행은행의 거래 기록 및 서버에 저장된 특수 회복키(recovery key)가 이용된다. 사용자가 전자동전을 도난당하거나 잃어버린 경우, 사용자가 분실한 동전의 일련번호를 은행에 보고하면, 은행에서는 이 동전을 어떤 계좌에 입금

되는 것을 방지하고, 동전의 유통과정을 추적하여 분실한 사용자의 계좌에 이를 입금한다. 몬덱스의 경우 카드에 거래내역이 저장되지만 이캐시에서는 사용자 소프트웨어에서 이캐시의 사용에 대한 내용을 참조할 수 있는 기능을 제공하고 있다.

몬덱스와 이캐시는 신용카드나 전자수표에서와 같이 별도의 정산과정을 필요로 하지 않는다. 따라서 이들 시스템에서는 수취인이 지불인의 신원을 파악하거나 신용 등급을 파악하는 절차를 필요로 하지 않는다.

이캐시와 몬덱스의 공통적인 특성은 이들 시스템에서는 이중사용(double spending) 방지 능력을 지니고 있고 여러 국가의 화폐를 지원할 수 있다는 점이다. 두 전자현금간의 중요한 차이점은 이캐시는 인터넷 상거래 지불수단으로 개발되어 소프트웨어 기반의 전자현금인 한편, 몬덱스는 소매점에서 사용할 목적으로 개발된 하드웨어 기반의 전자현금이라는데 있다. 두 번째 차이점은 몬덱스가 오프라인 능력을 제공하고 있는 한편, 이캐시는 온라인 능력만을 제공하고 있다는 점이다. 세 번째는 차이점은 이캐시는 사용자가 소프트웨어를 사용하여 온라인 상태에서 은행의 전자서명이 된 동전을 전송하는 카드인 한편, 몬덱스는 카드소유자가 이를 사용할 때마다 카드에 내장된 마이크로칩에서 전자서명을 산출하는 일종의 서명산출카드(signature-creating card)라는 점이다(Chaum, 1995). 몬덱스는 부정방지 마이크로칩이 내장된 카드에서 거래시 마다 전자서명을 산출하여 가치를 교환하는 결제시스템이다. 몬덱스 카드에는 현금이 디지털 자료로 저장되어 있고, 이 카드의 마이크로칩에서는 다른 몬덱스 카드 또는 기타 몬덱스 관련 장치에서 인식할 수 있는 고유의 전자서명을 산출하게 된다. 이 전자서명에 의해 그 가치의 유효성과 다탕성이 확인되고, 정당한 사용자라는 것이 확인된다.

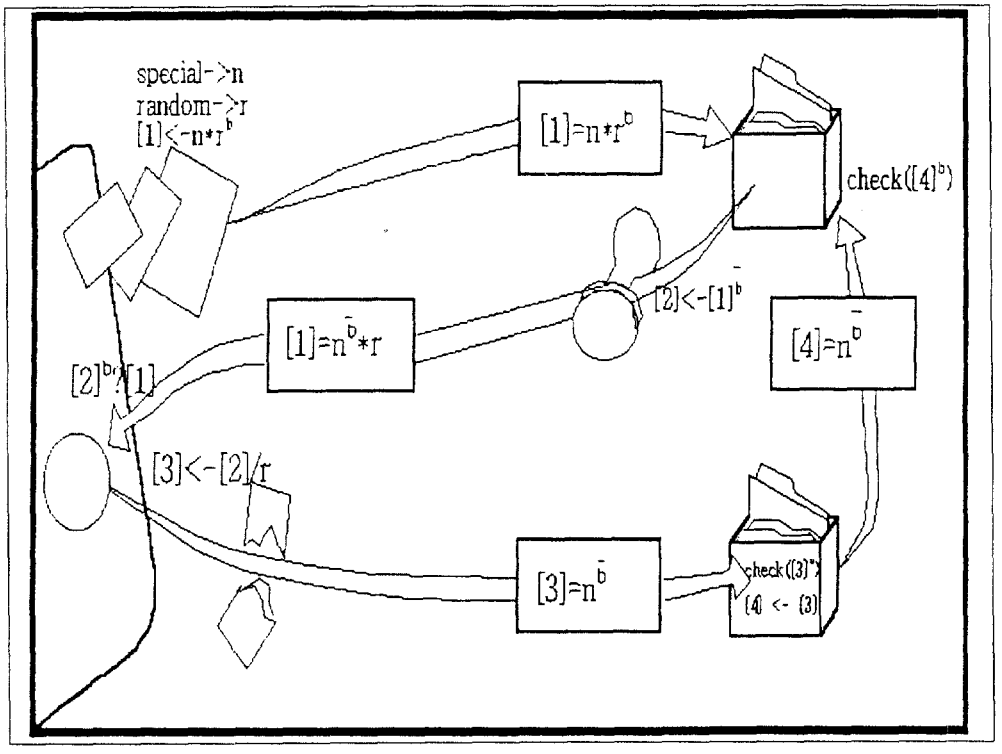
이캐시의 중요한 특성은 무색 전자서명(digital blind signature)을 통해 지불인의 익명성을 보장한다는 점이다(Chaum, 1992). 무색전자서명이란 공백 동전을 봉투에 넣고 밀봉하여 봉투에 서명을 함으로써 동전에 서명을 새기는 방법이다. 〈그림 2〉에서는 무색전자서명을 통해 이캐시의 무결성과 지불인의 익명성이 보장되는 과정을 나타내고 있다. 이캐시 사용자는 소프트웨어를 사용하여 충분한 크기의 난수인 동전의 일련번호 n과 난수요인(random factor) r을 산출한다(이는 공백의 동전과 전자봉투를 산출하는 것과 같다)[7]. 소프트웨어에서는 [1] 〈- $n \cdot r^b$의 계산을 수행한다(단, b는 은행의 공개키이다. 이는 일련번호가 부여된 동전을 봉투에 밀봉하는 것과 같다). 그 계산 결과가 은행에 전송된다. 이를 수신한 은행에서는 사용자의 계좌에서 일정금액을 공제하고 비밀키로 서명을 하여([2] 〈- $[1]^{\bar{b}}$), 그 결과를 사용자에게 반송한다. 사용자 PC에서는 은행의 공개키 b로 은행의 전자서명을 확인하고($[2]^b$), 그 결과에 난수 r을 나누어([2]/r: 이는 전자봉투에서 동전을 끄집어내는 것과 같다), 그 결과를 판매자에게 전송한다. 판매자는 공개키로 전자서명을 확인하고(check($[3]^b$)), 은행계좌에 입금하기 위해 ([4] = $n^{\bar{b}}$) 메시지를 은행에 전송한다. 은행에서는 이 메시지를 확인하여(check($[4]^b$)), 유효한 경우 해당 금액을 판매자의 계정에 입금한다. [4]와 [2]의 관계를 성립하게 하는 r은 단 하나 존재하므로 r을

7) 이 시스템에서는 공백 동전의 일련번호가 이중으로 산출되는 것을 방지하기 위해 100단위 크기의 난수를 산출하고 있다.

알지 못하고는 [1]을 추적할 수 없다. 동전을 산출한 사용자만이 r을 알고 있기 때문에 사용자의 익명성이 보장된다.

무색전자서명으로 은행에서는 어떤 일련 번호의 동전이 어느 고객에게 발행되었는지를 알 수 없다. 수취인이 이캐시를 수락하기에 앞서 은행에 그 유효여부를 확인할 때도 은행에서는 지불인의 신원을 알 수 없다. 따라서 이 시스템에서 지불인의 익명성이 보장된다. 그러나 수취인의 익명성은 보증되지 않는다. 수취인이 은행계좌에 동전을 입금하게 되면, 은행에서는 동전의 일련번호와 입금계좌목록을 기록·유지하여 같은 동전이 두 번 이상 사용될 수 없도록 하며, 수취인의 입금 내역을 파악할 수 있다. 따라서 돈세탁, 조세회피, 뇌물 등의 불법적 목적으로 이캐시가 사용될 가능성이 제한된다. 이 시스템에서는 사용자가 이캐시 계좌에서 전자동전을 인출할 때 비밀번호를 사용하므로 다른 사람이 계좌에 접근하는 것을 방지하고 있다.

이캐시 수취인의 발행은행을 통한 온라인 확인 과정과 발행은행에서 한 번 사용한 동전의 일련번호의 저장 과정을 통해 이캐시가 이중으로 사용되지 못하도록 하고 있다. 각 전자동전에는 고유한



출처: Chaum, D. (1992), "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of ACM*, Vol. 28, No. 10, p. 1041.

〈그림 2〉 무색전자서명 과정

일련번호가 부여되어 있고, 은행에서는 한번 사용한 동전의 일련번호를 데이터베이스에 저장하고 있다. 수취인이 지불인으로부터 이캐시를 수령할 때, 그 동전의 유효여부를 확인하기 위해 온라인으로 은행에 이를 제시하기 때문에 은행에서는 같은 동전이 두 번 사용되는 것을 방지할 수 있다.

2.3.2 한계점 비교

이캐시의 커다란 한계점은 오프라인 능력이 제공되지 않는다는 점이다. 전자동전의 수취인은 그 동전의 유효여부, 즉 한 번 사용된 동전이 아닌지를 온라인 상태에서 발행은행에 확인해 보아야 한다. 은행에서는 데이터베이스에 저장된 사용된 동전의 일련번호를 확인하여 동전의 유효여부를 확인하게 된다. 온라인 확인 과정에 의존하므로 시스템의 신뢰성은 네트워크의 신뢰성에 의존하게 되고, 발행은행의 서버에 과부하가 초래될 수 있어 서버가 병목구간이 될 수 있다. 전자동전은 단 한 번 사용될 수 있고, 수취인은 이캐시를 수령할 때마다 발행은행에 그 유효여부를 확인한다. 그리고 사용자의 거래 규모에 대한 제한은 없다. 따라서 어떤 시간대에는 은행 서버에 과부하가 걸릴 수 있다. 또한 은행의 데이터베이스에는 한 번 사용된 동전의 일련번호가 저장된다. 이캐시가 널리 보급되어 사용됨에 따라 이는 더 많은 데이터베이스 기억 용량을 필요로 할 것이다. Chaum(1995)에 따르면, 이 문제를 해결하기 위해 전자우편 메시지에 이캐시 메시지를 삽입함으로써 오프라인 능력을 제공할 계획인 것으로 알려져 있다(DigiCash, 1996).

몬덱스 시스템에서는 마이크로칩이 내장된 카드를 사용하기 때문에 카드발급 비용이 소요되며, 사용자에 따라 몇몇 하드웨어 장치를 필요로 한다. 또한 인터넷에서 몬덱스가 사용되기 위해서도 컴퓨터에 장착할 특수 장치가 필요하다.

보안 시스템의 중요한 요소 중의 하나는 미래에 발생가능한 공격에 대비하여 새로운 보안 기술과 암호알고리듬을 정기적으로 또는 수시로 적용하고 개선해 가는 것이다. 이캐시의 경우는 소프트웨어를 사용하기 때문에 새로운 버전을 사용자에게 제공하므로써 이들 변화를 반영할 수 있다. 몬덱스는 카드의 IC 칩간에 가치를 전송하는 프로토콜에 기반을 두고 있다는 점에서 고객이 사용하는 장치에 영향을 주지 않고 보안 메카니즘을 갱신해 가기란 쉽지 않다. 위변조를 방지하기 위해 일반 화폐의 디자인을 정기적으로 변화시키는 것과 마찬가지로 몬덱스의 발행은행에서는 정기적으로 새로운 카드를 발행하고, 카드의 IC 칩에 내장된 이이피롬(EEPROM)에 여유 기억공간을 두어 수시로 암호알고리듬을 갱신하는 방법을 채택하고 있다.

이캐시와 몬덱스는 모두 암호방식에 의존한 전자현금이다. 암호방식에 문제가 발생하는 경우, 발행은행과 온라인 상태에서 가치가 교환되는 시스템에 비하여 몬덱스와 같이 오프라인 상태에서 가치가 교환되는 시스템에서 더 큰 위험에 직면할 수 있다. 따라서 사기·위조·변조 등의 범죄활동이 드러날 가능성을 최대화하고 사기활동으로 혜택을 얻을 수 있는 기회를 최소화하는 전략으로 몬덱스에서는 카드에 16비트 크기의 고유번호를 부여하여 은행의 데이터베이스에 이를 저장해 두는 것을 비롯하여 중앙은행의 기능을 수행할 오리지네이터(orignator)를 한 국가에 하나씩 두는 방안을 고려하고 있는 것으로 알려져 있다(National Westminster Bank, 1996).

〈표 4〉에서는 12개 차원에서 이캐시와 몬덱스를 비교하여 나타내고 있다.

〈표 4〉 이캐시와 몬덱스의 비교

기 준	ecash	Mondex
실행형태	소프트웨어로 가치를 저장하고 관리·운영함	마이크로프로세서가 내장된 카드(IC 카드), 물리적으로 부정 복사를 방지하는 IC 카드에 가치를 저장함
익명성	지불인의 익명성이 보장됨	익명성이 보장않됨
이중사용방지 방법	ecash를 발급한 서버와 온라인으로 연결하여 확인	카드내의 부정방지 장치에 의해 확인됨
통화공급 효과	약간(개인간 가치 교환이 가능하나 발행은행의 서버에 온라인 확인과정을 거치야 함)	매우 크다(전자지갑을 통해 개인간 가치교환이 가능함)
인터넷 상거래 지불수단	소프트웨어만을 설치함으로 가능함	PC에 카드판독기를 부착하여야 함(몬덱스 프로젝트에서는 PC용 몬덱스 단말기를 개발하고 있음)
일반 소매점에서의 거래	지원하지 않음	소매점의 ATM, 전화기 등을 통해 이용하기 쉬움
일반 화폐에 비하여 제공되는 편리성	소프트웨어로 지불내역을 관리함	최근 10회의 지불내역을 관리하여 가계부 기능을 제공함.
고장 및 분실시의 처리	동전의 일련번호를 발행은행에 제공해야 함. 따라서 이 경우에는 지불인의 익명성이 보장되지 않음	◦ 몬텍스 카드를 발행한 은행에서 잔고를 파악하여 재발행해 줄 수 있으나 최악의 경우에는 가치의 권리가 상실됨. ◦ 비밀번호를 사용함으로 일반 화폐와는 달리 부정이용을 방지할 수 있고 악용될 가능성이 적어 다시 되돌아올 가능성이 높다
사용가능 통화의 종류	현재 발행은행의 통화로 한정됨	5가지 통화
발행비용	무료로 소프트웨어를 구입함	카드발급비
주변기기	별도의 주변기기가 필요하지 않음	잔액판독기, 전자지갑, ATM, 전화기, 소매점용 단말기 등
유통형태	개방형	개방형

III. 결제시스템의 비교 및 토의

3.1 결제시스템 설계상의 고려 요인

분산·개방 네트워크인 인터넷을 통해 비밀정보와 가치가 교환되는 상거래를 지원하는 성공적인 결제시스템은 안전성, 신뢰성, 수용성, 편리성, 효율성을 높여야 한다. 따라서 여기서는 이들 네가지 목표에 영향을 미치는 다차원적 요인을 파악하고자 한다. 이들 요인을 분석하기 위해 먼저 II에서 사례의 대상이 된 결제시스템의 특성과 한계점을 파악하였다. 다음으로 각 시스템의 웹사이트에서 제공하고 있는 FAQ를 조사하여 판매자와 구매자의

〈표 5〉 구매자와 판매자의 요구사항

구매자 요구사항	판매자 요구사항
1. 판매자 신원 및 메시지 인증성	1. 구매자 신원 및 메시지 인증성
2. 메시지 무결성	2. 메시지 무결성
3. 구매주문 및 지불에 대한 확인 및 부인방지	3. 지불 보증 및 부인방지
4. 프라이버시와 익명성의 통제 능력	4. 구매자에 대한 프로필 및 구매 양식
5. 구매 제품의 다양성	5. 판매 제품의 다양성
6. 지불수단의 다양성	6. 결제수단의 다양성
7. 해외 제품의 구매 가능성	7. 익명성
8. 지원 서비스와 편리성	8. 지원 서비스 및 편리성

요구사항을 분석하였다. FAQ에는 시스템의 사용자들이나 시스템에 대한 의문점을 가진 사람들이 시스템 관리자에게 제시한 질문과 그에 대한 응답으로 구성되어 있다. FAQ로부터 도출한 구매자와 판매자의 요구사항을 요약하면, 〈표 5〉와 같다.

본 연구에서는 결제시스템의 주요 요인을 안전성, 신뢰성, 편리성, 효율성, 수용성 측면에서 살펴보고자 한다.

결제시스템의 안전성이란 인터넷 연결성, 접근용이성, 통신 등의 인터넷 자체의 안전성에 의해서도 영향을 받게 된다. 인터넷 자체의 안전성은 데이터베이스 및 네트워킹 기술의 발전에 따라 점차 개선되어 가고 있다. 여기서 고려하는 안전성이란 결제시스템이 고장이나 어떤 장애, 부하상태 등에 관계없이 운영될 수 있는 능력을 의미한다. 이에 영향을 미치는 요인으로는 견실한 결제 프로토콜, 고장시의 회복 능력, 오프라인 능력, 결제시스템 서버에의 적절한 부하 및 확장성 등이다.

신뢰성이란 결제시스템이 의도되었던 제기능을 수행하고, 사용자들이 안전하다고 믿을 수 있도록 사기거래를 방지할 수 있는 정도를 의미한다. 결제시스템이 의도했던 제기능을 수행하기 위해서는 먼저 기본적인 보안 서비스를 제공할 수 있어야 한다. 그 첫째는 시스템에의 접근권한이 없는 사람(또는 시스템)을 제한할 수 있어야 한다. 둘째는 거래 상대 및 수신 메시지의 정당성을 인증할 수 있어야 한다. 예를 들면, 구매자는 판매자가 사칭하는 자가 아닌 실제 판매자라는 것을 확인할 수 있어야 하고, 판매자는 구매자의 신원을 확인할 수 있어야 한다. 또한 구매자(판매자)는 판매자(구매자)로부터 수신한 메시지가 실제 판매자(구매자)가 발송한 것인지를 확인할 수 있어야 한다. 셋째는 비밀 정보에 대한 기밀성을 유지할 수 있어야 한다. 예를 들면, 신용카드번호와 계정정보 등 판매자·구매자·금융기관간에 송수신되는 메시지를 다른 사람(또는 시스템)이 가로채어 볼 수 없도록 해야 한다. 넷째는 메시지의 무결성이 유지되어야 한다. 예를 들면, 구매자(판매자)는 판매자(구매자)가 송신한 메시지를 위변조되지 않은 원안대로 수신했다는 것을 확인할 수 있어야 한다. 다섯째는 거래 상대가 거래 사실을 부인했을 때 이를 입증할 수 있어야 한다. 예를 들면, 구매자가 구매주문을 하고 이를 부인했을 때, 또는 판매자가 구매 대금을 수령하고 거래 사실을 부인했을 때, 판매자와

구매자 각자가 상대가 거래사실을 부인하고 있다는 것을 입증할 수 있도록 해야 한다. 기본적인 보안 서비스 외에도 결제시스템의 신뢰성에 영향을 주는 요인으로는 결제 프로토콜의 강건성과 공개정도, 프라이버시와 익명성, 소비자와 판매자의 보호 능력, 금융기관의 법집행기관에의 보고 정보 제공 능력, 관리철차와 내부에서의 사기나 부정을 방지할 수 있는 능력, 공개키 암호방식을 사용하는 경우의 공개키의 인증성, 전자화폐의 이중사용방지 능력, 오프라인능력 등이다.

편리성이란 개념과 절차가 간편하여 사용하기 편리하고, 사용자들에게 지원서비스를 비롯한 다양한 능력을 제공할 수 있는 정도이다. 편리성에 영향을 미치는 요인으로는 플랫폼과의 독립성, 접근용이성 및 인터페이스의 단순성, 시스템 개념 및 사용절차의 단순성, 상호운영성, 소액거래의 지원정도, 거래제품의 다양성, 다양한 지불수단, 사용자 거래관리의 지원 능력, 국제적 접근능력, 지능형 결제능력 등이 있다.

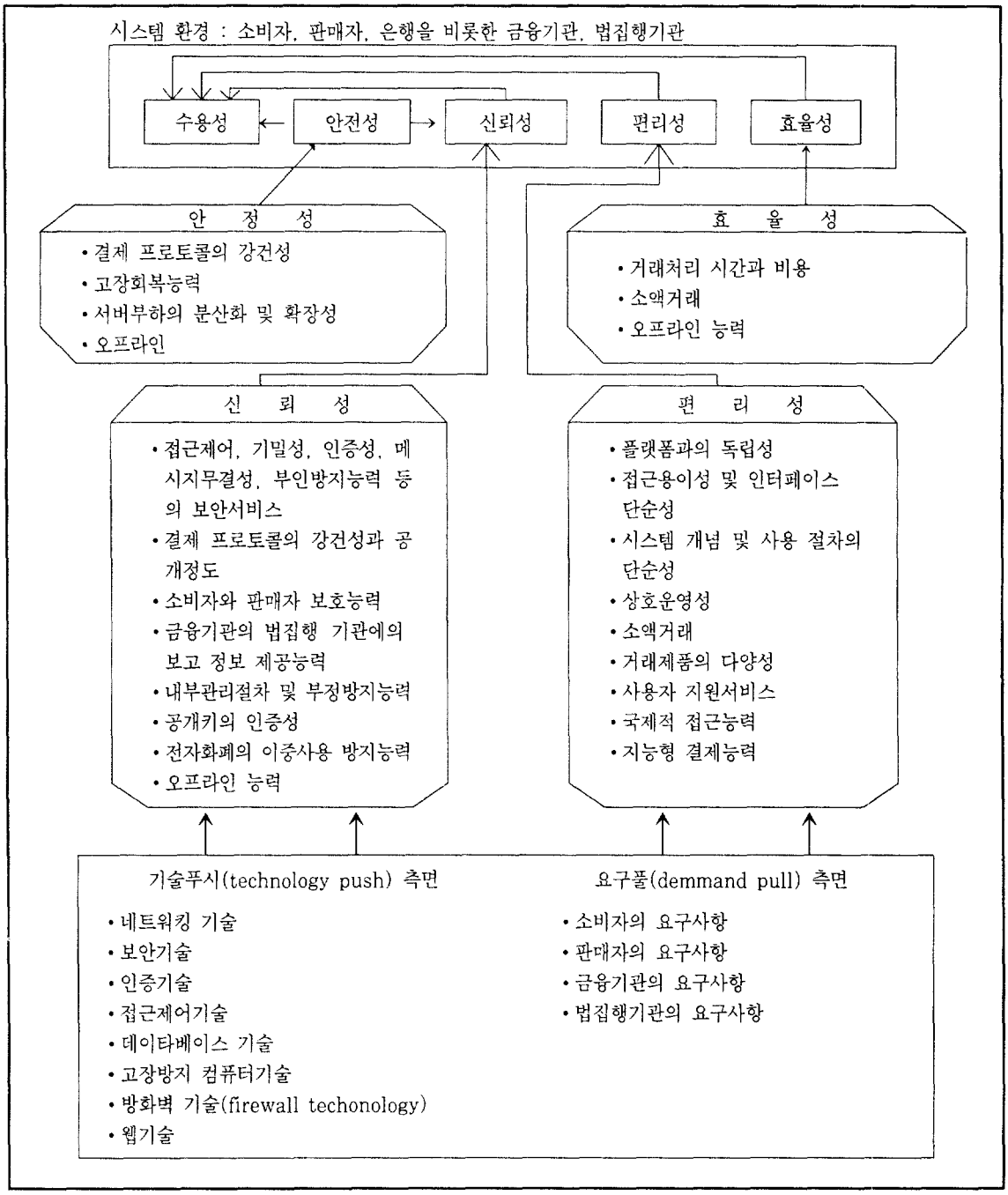
효율성이란 시스템 거래처리의 효율성, 구매자와 판매자의 거래 수수료의 적정성을 의미한다. 효율성에 영향을 미치는 요인으로는 거래처리 시간과 비용, 소액거래의 지원정도, 오프라인 능력 등이 있다.

수용성이란 소비자, 판매자, 금융기관 등에서 시스템이 안전하고 편리하고 효율적이며 신뢰할 수 있어 널리 사용되는 정도를 의미한다. 따라서 〈그림 3〉에서 결제시스템의 안전성 · 신뢰성 · 편리성 · 효율성이 높을수록 그 수용성이 증가된다. 또한 시스템의 안전성이 높을수록 그 신뢰성이 증가된다. 한편 안전성 · 신뢰성 · 편리성 · 효율성 간에는 상반관계가 발생하기도 한다. 예를 들면, 결제시스템의 보안 능력을 증가시킬수록 시스템의 효율성이나 편리성이 저하될 수 있다. 소비자와 판매자 관점에서의 시스템에 대한 요구가 이를 운영하는 기관이나 법집행기관에서의 요구와 상반될 수도 있다. 또한 소비자 보호측면에 대한 요구는 판매자의 요구를 저해할 수도 있다. 이들 요인간의 상반관계에 대해서는 3.2에서 분석하기로 한다.

〈그림 3〉에서는 결제시스템의 환경으로 결제시스템에 관련된 소비자, 판매자, 은행, 법집행기관을 나타내고 있다. 결제시스템은 대학, 연구소, 소프트웨어 개발업체, 인터넷서비스 제공업체 등에서 설계 · 개발될 수 있다. 결제시스템 설계시에는 〈그림 3〉의 다차원적 요인, 시스템 환경과 요인의 적합성 등이 고려되어야 한다. 또한 결제시스템 설계시에 개발자는 기술 푸시(technology push) 측면에서 네트워킹 기술과 보안기술 등의 결제관련 기술 발전 동향을 파악하고, 소비자와 판매자 등의 전자상거래에 대한 요구사항을 분석하여야 한다. 따라서 〈그림 3〉에서 나타낸 바와 같이 결제시스템 관련 기술발전과 소비자와 판매자 등의 요구사항으로부터 21개의 다차원 요인이 도출된다. 결제시스템을 운영하는 주체는 대개 은행을 비롯한 금융기관이 될 것으로 전망된다. 왜냐하면, 소비자와 판매자가 신뢰할 수 있는 기관에서 결제시스템을 운영할수록 초기단계에서 인터넷 결제에 대한 신뢰도가 증가할 수 있기 때문이다.

3.2 결제시스템의 비교 및 토의

〈그림 3〉에서 제시한 결제시스템 설계시 고려되어야 할 21개의 요인은 결제시스템 비교의 기준이 될 수 있다. 그러나 결제시스템은 개발 또는 운영의 초기단계에 있으며, 자료수집에도 한계가 따른



〈그림 3〉 결제시스템 설계상의 고려 요인

〈표 6〉 요인에 대한 설명

요 인	설 명
1. 보안서비스	접근제어, 기밀성, 인증성, 메시지 무결성, 부인방지
2. 결제 프로토콜의 강건성	거래 및 지불 프로토콜은 결제시스템의 기반이 되는 표준이다. 사례분석 결제시스템의 기반이 된 결제 프로토콜 외에도 안전한 신용카드 거래를 지원하는 SET, 소액거래를 지원하는 W3C(1995)의 MPTP(Micro Payment Transfer Protocol)와 Manasse(1995)의 Millicent, 기타 다양한 전자화폐 표준 등이 개발되고 있다. 일반적으로 강건한 결제 프로토콜의 개발자는 이를 공개함으로써 신뢰를 높이고자 한다.
3. 프라이버시와 익명성	거래자가 개인정보를 비밀로 유지할 수 있을 때 프라이버시가 보호된다. 또한 거래자가 자신의 신원을 노출하지 않을 때, 익명성이 보증된다.
4. 고장회복 능력	컴퓨터 고장 또는 인터넷 통신 장애시 이를 회복할 수 있는 능력. 고장 후 컴퓨터에 저장되었던 가치를 복구할 수 있는 능력
5. 서버부하의 분산화 및 확장성	결제시스템의 한개 서버에 거래처리 업무가 집중되지 않고 여러 서버에 분산되어 과부하되지 않고 많은 거래를 처리할 수 있는 정도. 그리고 구매자, 판매자, 거래은행 등간의 기존 거래구조의 변화를 최소화하면서 시스템을 적용할 수 있는 능력
6. 오프라인 능력	결제시스템 서버와 온라인 상태가 아닌 경우에도 거래를 지원하는 정도. 오프라인 능력은 서버의 부하를 분산화할 수 있고 네트워크의 장애시에도 거래를 지원할 수 있어 시스템의 안전성·신뢰성·효율성을 높일 수 있다.
7. 소비자와 판매자의 보호능력	착오나 실수 등으로 부정거래가 발생하여 정당한 소비자나 판매자가 손실을 감수해야 할 때, 이를 보상해 줄 수 있는 능력
8. 금융기관의 법집행기관에의 보고정보	법집행기관에서 조세회피, 뇌물, 돈세탁 등을 방지할 목적으로 결제시스템 운영기관에 요구하는 정보를 제공할 수 있는 능력
9. 내부관리절차 및 부정방지능력	결제시스템 내에서의 다단계 보안 절차, 종업원의 운영지침, 내부 부정을 방지할 수 있는 능력, 불량 고객이나 판매자를 관리하고 이를 알릴 수 있는 능력 등
10. 공개키의 인증성	공개키 암호방식을 사용하는 경우, 공개키로 그 정당한 사용자를 확인할 수 있는 능력
11. 전자화폐의 이중사용방지 능력	전자화폐를 복사하여 이중으로 사용할 수 없도록 하는 능력. 기타 전자화폐를 작은 단위로 분할할 수 있는 가분성(divisibility), 발행한 전자화폐를 계속적으로 교환할 수 있는 내구성(durability) 등은 전자화폐의 수용성에 영향을 미치는 요인이 된다.
12. 플랫폼과의 독립성	소프트웨어 기반의 결제시스템에서 컴퓨터 하드웨어나 운영체제(유닉스, 윈도우즈, OS/2 등) 등 어떤 플랫폼도 지원할 수 있는 정도, 방화벽 내의 사용자들도 쉽게 이용할 수 있도록 지원되는 정도. 결제시스템에 하드웨어가 사용되는 경우, 기존의 하드웨어나 소프트웨어에 호환되는 정도.
13. 접근용이성 및 인터페이스의 단순성	소비자와 판매자는 전자우편, FTP, 웹 등 다양한 방법으로 상호 접근할 수 있어야 하며, 사용자 소프트웨어의 인터페이스가 단순하고, 다른 응용과도 호환되며, 설치절차도 단순해야 한다.

요 인	설 명
14. 상호운영성	소비자와 판매자가 선택할 수 있는 지불수단의 종류. 다양한 지불수단(예를 들면, 신용카드, 전자수표, 전자현금 등)간 상호 교환될 수 있는 정도. 신용카드의 경우, 다양한 신용카드로 상호 결제할 수 있는 정도.
15. 시스템 개념 및 사용절차의 단순성	기존의 보편적인 결제 절차의 변화를 최소화하고, 거래 및 지불절차가 단순하여 사용자가 이해하기 쉬운 정도
16. 소액거래	소액거래를 지원하는 정도
17. 거래제품의 다양성	유형의 재화와 정보제품 등의 어떤 제품거래를 지원하는 정도
18. 사용자 지원 서비스	소비자와 판매자의 거래 내역에 관한 관리를 지원하고, 온라인 세금 처리 및 거래관련기관 정보에의 접근성. 판매자와 금융기관 정책의 지원 정도
19. 국제적 접근 능력	각국 은행 및 화폐의 지원정도. 다양한 국가와 지역에서 이용가능한 능력
20. 지능형 결제능력	안전한 거래에 필요한 보안 수준과 거래 비용의 관계를 자동적으로 고려하는 정도
21. 거래처리시간과 비용	거래 및 지불 처리 시간과 그에 따른 비용을 감소시킬 수 있는 정도

다. 따라서 본 연구에서는 다음의 4가지 범주에서 관측가능한 몇몇 요인을 중심으로 결제시스템을 비교·토의하고자 한다.

3.2.1 암호방식을 이용한 결제시스템에 내재된 가정

지금까지의 논의에서 암호방식을 적용한 결제시스템에서 비승인된 사람이나 시스템에 의해 결코 암호알고리듬이 깨어지지 않는다는 가정하에서 결제시스템의 보안이 유지된다고 보았다. 그러나 암호방식이 완전한 것은 아니다. 예를 들면, DES 방식은 키의 영역 64비트 중 56비트가 실효 암호키이며 특정 암호키를 찾기 위해서는 2^{56}패턴을 이용하면 된다. 이를 실행하기란 쉽지 않지만 병렬 컴퓨터를 이용하면 며칠 또는 경우에 따라 몇시간 내에 발견할 수도 있다. RSA 방식은 필요에 따라 여러 크기의 암호키가 이용되며 암호키가 길수록 그것을 망가뜨리는 것이 쉽지 않다. RSA 방식의 암호키를 알아내는 방법에는 2^{56} 퍼턴과 소인수분해에 의한 방법 등이 있다(RSA, 1995d). RSA 방식의 키가 소인수분해에 의해 망가졌다는 사례도 있지만 현재는 일정 시간내에 실현가능한 해독방법은 발견되어 있지 않다.

일반적으로 서버의 보안을 강화할수록, 특히 원격지에서 시스템을 관리하기란 쉽지 않다. 또한 암호방식을 이용하는 경우에는 다음과 같은 몇가지 문제에 대한 결정을 해야 한다. 첫째, 키의 수명을 얼마로 할 것인가? 둘째, 키의 크기를 얼마로 할것인가? 일반적으로 키수명이 5년인 1024비트 키는 키수명이 1개월인 512비트 키보다 범죄자들에게 드러날 위험이 높다(Borenstein, et al., 1995).

이런 관점에서 볼 때, 키의 크기보다 키의 수명을 짧게 하는 것이 범죄활동을 방지할 가능성이 높다. 그러나 키를 자주 변경할수록 사용자들의 불편성은 증가하게 된다. 또한 암호정보를 해독하므로써 얻는 가치가 높은 경우일수록 범죄자의 활동은 증가하게 된다. 따라서 소액거래를 지원하는 시스템에서 보다 고액거래를 지원하는 시스템에서 높은 보안서비스가 요구된다. 사례분석에서 살펴본 모든 시스템에서는 거래에 관계없이 같은 수준의 보안서비스를 제공하고 있다. 유연하고 강건한 결제 프로토콜이란 거래의 종류에 따라 서로 다른 보안서비스를 제공할 수 있는 표준을 의미한다.

암호방식을 이용하지 않는 유일한 결제시스템은 버스트 버츄얼이다. 이 시스템은 전자우편의 안전성에 의존하게 된다. 그러나 침입자는 전자우편을 가로챌 수 있고, 이를 통해 사기거래를 할 수도 있다. 현재 퍼스트 버츄얼에서는 100불 미만의 거래만을 지원하고 있다. 그러나 고액거래를 지원하기 위해서는 결국 암호방식을 적용해 갈 것으로 보인다.

이미 살펴본 바와 같이 암호방식을 이용하는 것만으로 결제시스템의 보안이 유지된다고 할 수 없으므로 다양한 다단계 보안능력이 제공되도록 결제시스템이 설계되어야 한다. 이는 웹공간에서 거래당사자간의 신뢰성을 제고할 수 있는 방안에서 결제시스템 내부의 관리절차 및 결제시스템 내부 종사자 대한 교육·훈련 방안이 마련되어야 함을 의미한다. 그러나 보안시스템이 복잡하고 지나치게 엄격한 경우 도리어 사용자의 불편성을 초래할 수 있고, 그에 따른 비용발생으로 인해 소액거래가 활성화되지 않을 수 있다. 따라서 결제시스템을 설계할 때, 고액거래와 소액거래에 따라 선택적으로 보안능력이 제공되도록 하는 것은 이러한 문제를 해결하는 하나의 방안이 될 수 있다.

3.2.2 익명성·프라이버시와 효율성 등

전자상거래가 널리 이용되는 시대에는 다음의 두 가지 극단적인 경우가 초래될 수 있다. 그 하나는 자동화된 전자시스템을 통해 모든 소비자의 구매행동을 쉽게 추적할 수 있는 경우이다[8]. 즉, 어떤 소비자가 언제, 어디서, 무엇을, 얼마만큼, 몇번 구매했는가에 대한 대한 자료가 중앙의 데이터베이스에 전자적으로 기록된다. 최악의 경우, 독재정권하에서는 국민들의 모든 활동을 통제하고 억제하는 도구로서 이 시스템이 활용될 수 있다. 다른 하나는 거래와 관련된 프라이버시와 익명성이 완전히 보장되는 경우이다. 후자의 경우에도 문제가 없는 것은 아니다. 안전한 익명성이 보장되는 결제시스템에서는 거래를 추적할 수 있는 감사궤적이 남아있지 않은 관계로 이는 불법적인 돈세탁, 밀수거래, 조세회피의 수단으로 활용될 수 있다. 따라서 양극단의 한계점을 극복할 수 있는, 즉 비합법적으로 활용되지 않도록 적절한 감사궤적을 마련하면서 개인의 프라이버시와 익명성이 보장되는 결제시스템이 이상적이다. GVU(1996)의 설문조사에 따르면, 대부분의 인터넷 사용자들은 인구통계학적 정보를 자신들이 통제할 수 있기를 바라며, 기업에 이들 정보가 판매되지 않기를 바란다.

8) 정교한 패턴분석 기술인 데이타마이닝(data mining)을 이용하여 기업에서는 어떤 개인에 대한 주어진 정보를 조작하여 쉽게 접근가능한 형태로 조직화하고 상관관계를 분석하여 개인의 프라이버시를 침해할 수 있다(Decker and Focardi, 1995). 또한 기업에서는 고객선호도, 구매내역, 신용내역, 단계별 생활양식 등을 파악하여 고객을 유인할 수 있는 한편, 데이터마이닝으로 산출된 정보가 조직간 상호 판매용으로 이용될 수 있다.

Froomkin(1996a)은 통신에서 송신자의 정체가 어느 정도 숨기지는가에 따라 추적가능한 익명성(traceable anonymity)과 추적불가능한 익명성(untraceable anonymity)을 제시하고 있다. 사이버캐시, 네트빌, 네트체크, 퍼스트버츄얼 등의 신용카드 및 전자수표에 기반을 둔 결제시스템은 거래에 관한 정보를 결제시스템의 서버에 저장해 두기 때문에 추적가능한 익명성 수준을 보장해 준다. 이런 유형의 결제시스템에서는 프라이버시에 관한 보안수준이 낮지만, 특별한 경우가 아니면 거래자의 신원이 드러나지 않기 때문에 사람들은 많은 경우에서 만족하게 된다. 한편 이캐시와 같은 전자동전에서는 무색전자서명을 통해 지불인의 추적불가능 수준의 익명성이 보장된다. 또한 ISI에서 개발하고 있는 네트캐시도 이런 수준의 익명성이 보장되는 것으로 보고되고 있다. 그러나 네트캐시에서 어떤 프로코콜을 이용하여 익명성을 보장하는지에 대해서는 공개되어 있지 않다. 한편, 전자현금 모델에 기반을 둔 몬덱스의 경우는 추적불가능 수준의 익명성이 보장되는지에 대해서는 논란의 여지가 있다. 왜냐 하면, Ⅱ에서도 언급한 바와 같이 몬덱스에는 일련번호가 부여되어 있고, 발행은행의 서버에도 이것이 저장되어 있기 때문에 분실한 전자현금을 회수할 수 있다. 이는 결국 전자현금의 거래를 추적할 수 있다는 것을 의미하기 때문이다.

신용카드나 전자수표 모형에 기반을 둔 결제시스템에서는 거래정보의 이용성이 증가되고, 법집행기관(국세청등)에 대한 보고의무를 이행하기도 쉽다. 또한 판매자와 소비자에게 다양한 정보를 제공할 있어 사용자 편리성을 증가시킬 수 있다. 그러나 지불인의 익명성이 추적불가능 수준에서 보장되는 이캐시의 경우에는 금융기관이 거래정보를 법집행기관에 보고하기 위해서는 판매자의 협조를 요청해야 한다.

전자수표나 신용카드 모델에 기반을 둔 결제 시스템에서는 신용카드회사나 은행을 통해 정산되기 때문에 얼마의 금액을 결제하던 비가분성의 문제가 야기되지 않는다. 신용카드와 선불카드에 기반을 둔 모형은 기존의 네트워크 기반자원을 활용할 수 있으며, 사용자들이 널리 사용해 왔기 때문에 결제과정을 잘 이해하고 있어 사용자가 이 시스템에 친숙할 수 있다. 나라에 따라 다르기는 하지만 미국의 경우, 신용카드의 분실등으로 인하여 거래상에 문제가 발생하게 되면 소비자는 최대 50불(추가로 신고 및 분쟁에 따른 불편과 시간상의 손실이 발생한다)로 그 책임이 한정되어 있다. 우리 나라의 경우 신용카드의 부정사용에 따른 손실은 보험회사의 신용카드보험과 회원은행의 신용카드보상으로 보상되고, 소비자는 20,000원의 보험금 및 보상청구 요금을 지불하면 된다. 또한 기존의 신용카드 시스템에서와 같이 신용카드로 결제하는 경우, 일정기간 후에 정산이 이루어지기 때문에 구매자는 외상구매의 효과를 누릴 수 있다.

한편, 엄격히 말해, 전자동전에 기반을 이캐시의 경우는 가분성 조건이 충족되지 않는다. 전자동전이 전자화폐로서 가분성을 만족하기 위해서는 사용자의 프라이버시를 희생시키거나 결제시스템의 비효율적 운영을 감수할 수 밖에 없다. 예를 들면, 가격이 35원인 웹정보를 받아보기 위해서 구매자는 몇 개의 전자동전을 모아야 한다. 적은 금액의 동전으로 고가의 상품을 구입하는 경우에는 많은 동전이 필요하다. 이는 결국 가치전송상의 지연이나 어느 정도의 정보처리비용을 초래하게 한다(Camp, Sirbu, and Tygar, 1996). 그러나 디지캐시사의 이캐시를 사용하는 경우, 현실적으로 비가분성이 큰 문제가 되지 않는 것으로 알려져 있

다(DigiCash, 1996a). 몬덱스와 같이 스마트카드를 사용하는 경우, 적은 금액의 많은 동전을 저장하기 위해서는 많은 기억량을 필요로 하게 되어 결국 카드발급비용을 높이게 될 수 있다. 또한 판매자는 구매자에게 잔돈을 거슬러 주기 위해 많은 동전을 저장하고 있어야 한다.

신용카드에 기반을 둔 모델에서는 소액거래를 지원하기 어렵다. 현실의 일반 상거래에 비하여 인터넷 상거래가 갖는 장점 중의 하나는 소액거래가 활성화될 수 있다는 점이다. Pays(1996)에 따르면, 1994년 미니텔(Minitel)의 25,000여종 온라인 서비스에 의한 13억불의 거래에서 평균거래금액은 약 0.5불이었다. 또한 미니텔에 의한 거래의 70% 이상이 부가가치정보에 관련된 것이었다. 따라서 온라인 거래에 관한 프랑스에서의 경험으로 비추어 볼 때도 인터넷 결제시스템의 소액거래 지원 여부는 결제시스템 평가의 대단히 중요한 요소라 할 수 있다. 웹정보, 논문, 뉴스, 그림 등의 몇십원에서 몇백원에 이르는 거래에서 신용카드에 의한 결제는 적절하지 못하다. 그 이유는 신용카드에 의한 결제에 따른 수수료가 높기 때문이다(우리 나라의 경우 거래액의 1.5% - 5%). 미국의 경우 신용카드거래의 평균 거래금액은 60불이다(Cross-Industry Working Team, 1996). 그러나 네트빌, 이캐시, 몬덱스, 네트캐시 등은 소액거래를 지원할 수 있는 결제시스템이다.

암호방식으로 비대칭키 알고리듬을 이용한 커버러스에 기반을 둔 네트체크 시스템이 처리시간 측면에서 효율적인 것으로 평가되고 있다. 신용카드 모형에 기반을 둔 사이버캐시에 비하여 정산과정을 필요로 하지 않는 몬덱스가 결제처리시간이나 결제비용측면에서 효율적일 수 있다. 그러나 몬덱스 카드를 발급하는 데는 비용이 소요되기 때문에 소프트웨어에 기반을 둔 시스템에 비하여 사용자의 전체비용이 낮아진다고는 하기 어렵다. 소액거래를 지원하기 위해서는 결제처리비용이 낮아야 하는데, 일반적으로 소액거래를 지원하는 네트빌, 이캐시, 몬덱스 등이 결제비용측면에서 다른 시스템에 비해 효율적이라 할 수 있다.

사용자들에게 다양한 지불수단을 제공하는 시스템일수록 상호운영성이 높다. 사이버캐시에서는 신용카드 뿐만 아니라 전자현금인 사이버코인을 개발하고 있어 사용자의 지불수단이 다양해 질 것으로 예상된다. 또한 네트체크에서는 전자수표와 전자현금인 네트캐시를 상호 교환할 수 있도록 할 것으로 보인다. 신용카드회사에서 서로 다른 카드로 상호결제할 수 있는 시스템을 도입하게 되면, 현재의 시스템에서 보다 상호운영성은 개선될 것이다.

3.2.3 공개키의 인증 및 결제시스템의 신뢰성

공개키 암호방식의 전자서명을 통해서도 거래 당사자들은 상호간 상대를 완전히 신뢰할 수는 없다. 전자서명을 이용하는 시스템에서는 공개키가 다른 사람을 사칭하지 않은 실제 전자서명을 한 당사자의 것이라는 전제하에서 상대를 인증할 수 있도록 해 준다. 공개키 암호방식을 이용한 전자서명에서는 송신자가 자신의 비밀키로 메시지에 서명하고 수신자에게 송신자의 공개키를 분배한다. 수신자는 자신의 공개키로 메시지를 해독하고 송신자의 공개키로 전자서명을 확인한다. 수신자는 비밀키를 알고 있는 자신만이 메시지를 해독할 수 있다고 믿고 있다. 그러나 수신자는 송신자의 공개키를 믿을 수 있는지, 수신자 자신의 정확한 공개키가 배포되었는지를 확인할 수 없다. 만약 "병"이 "갑"을 사칭하여 어떤 결제시스템을 이용하는 경우, 즉 "병"이

"갑"의 이름으로 결제시스템에 등록한 경우라면, "병"은 "갑"의 이름, "병"의 전자우편 주소, "병"의 공개키로 거래하게되므로 "병"과 거래하는 당사자는 상대가 "갑"인지 "병"인지를 알 수 없게 된다. 이러한 문제를 해결하기 위해 두 가지 접근법이 제시되고 있다.

그 첫째는 결제시스템을 운영하는 은행이나 신용카드회사 등, 구매자와 판매자 외의 신뢰할 수 있는 인증기관(certification authority)에서 발급하는 인증서를 이용하는 방법이다(Froomkin, 1996c). 전자상거래를 위한 전자인증서비스를 제공하는 대표적인 조직으로는 베리사인(VeriSign)사를 들 수 있다. 이 회사는 1995년 RSA 데이터시큐리티사의 자회사로 설립되었다. 베리사인사에서는 전자인증서를 발급하기에 앞서 신청자의 신원을 얼마나 정확하고 상세하게 파악하는가에 따라 3종류의 전자 인증서로 구분하고 있다. 클래스 1은 신청자 이름과 전자우편 주소만을 증명하고, 전자우편으로 이를 확인하여 발급한다. 클래스 2는 이름과 전자우편 외에도 개인신상에 관한 추가 정보를 증명하고, 상용 데이터베이스나 기타 확인절차를 걸쳐 이들 정보를 확인한다. 가장 엄격한 증명서인 클래스 3은 공증인 또는 베리사인이 승인한 지역 등록국의 확인을 거친 후 제시된 문서를 기초로 발급된다.

전자 인증서(electronic certificate)란 전자서명을 한 사람이 주장하는 자신의 속성에 대한 사실여부를 제3자가 거래 당사자로 하여금 이를 확인할 수 있도록 해주는 전자적으로 발급하는 증명서이다. 이러한 전자인증서의 신뢰성은 인증서에서 제공하는 거래 당사자에 대한 증명 내용, 인증기관의 신뢰성, 인증서취소목록의 관리정도에 의존하게 된다.

인증서를 통해 확인할 수 있는 내용은 사용자의 공개키와 실제 거래자의 이름을 연결하여 거래자의 신원을 확인해 주는 인증서에서 거래자의 이름과 공개키 뿐만 아니라 주소, 나이, 특정 제품의 구매권한을 입증해 주고 전자 타임스탬핑 서비스를 제공하는 인증서에 이르기까지 다양한 형태가 있을 수 있다. 단순히 공개키만을 입증하는 인증서로는 거래 상대가 다음과 같은 상황에서 거래자를 신뢰할 수 없다. 성인인 소비자만이 구입할 수 있는 제품을 어떤 구매자가 구입하고자 하는 경우 판매자는 단지 공개키만으로 그 구매자를 신뢰할 수 없고, 그가 성인이라는 것을 입증하는 전자 인증서를 필요로 하게 된다. 미연방정부에서는 사전허가없이 미국에서 고급의 암호 알고리듬을 수출할 수 없도록 규정하고 있다. 신뢰할 수 있는 인증기관에서 이 암호 알고리듬을 배포하고자 하는 자가 미국에 살고 있는 시민이거나 미국에 거주하는 외국인이라는 것을 전자 인증서를 통해 입증할 수 있을 때, 소송에 따른 위험을 제거할 수 있다.

대개 판매자와 구매자와는 별개의 제3자에 의해 운영되는 결제시스템에서는 판매자와 구매자가 시스템에 등록할 때 그들의 신원을 파악하게 된다. 또한 신문이나 잡지 등에서 공개키 목록이 제공되기도 한다. 만약 신뢰할 수 있는 제3자가 비밀키로 서명한 인증서에 공개키를 저장하여 배포하는 경우, 사용자는 그 공개키의 정당성을 신뢰할 수 있다. 따라서 결제시스템에 등록시 판매자와 구매자의 신원을 얼마나 정확히 파악하는가는 불특정다수가 참여하는 전자상거래의 신뢰성 및 소비자 수용성을 확장하는데 있어서 중요한 문제이다. 본 연구의 사례로 제시한 6개의 결제시스템에서는 온라인으로 등록과정을 마치게 된다. 이는 결국 이들 시스템에서 베리사인의 클라스 1에 해당하는 수준의 인증성만을 제공함을 의미한다. 한편 결제시스템

등록절차가 지나치게 엄격한 경우, 신청자들은 등록에 따른 불편을 겪기 때문에 도리어 결제시스템의 사용자 수용성을 저해할 수 있다. 따라서 이러한 상반되는 문제를 해결하기 위한 한가지 방안은 사용자가 결제시스템 등록시 베리사인과 같은 인증기관에서 발행하는 인증서를 제시하게 하는 것이다. 인증기관의 전자인증서와 결제시스템이 호환되는 경우, 사용자는 인증기관으로부터 인증서를 발급받아 이를 제시함으로써 어떤 결제시스템에 등록할 수 있다. 그러나 이 경우에도 완전히 문제가 해결되는 것은 아니다. 왜냐하면 인증의 정도에 따라 다르긴 하지만 사용자가 인증기관으로부터 전자 인증서를 발급받기 위해서는 수수료를 지불해야 하기 때문이다. 이는 전자상거래의 신뢰성을 높이는 만큼 비용을 치려야함을 의미한다.

신용카드 거래에서 신용카드의 효력이 정지되었는지를 온라인으로 확인할 수 있는 것과 유사한 방법으로 인증기관에서는 사용자들이 증명서의 유효여부를 확인할 수 있는 인증서취소목록(Certificate Revocation List: CRL)을 계속적으로 갱신하여 제공해야 한다. 또한 시간에 따라 공개키 소유자의 신분변화 또는 전자우편 주소의 변화 등으로 증명서의 정확성이 변화될 수 있다. 따라서 구매자와 판매자는 CRL을 쉽고 편리하게 조회할 수 있도록 인증기관에서 이를 관리해야 한다.

두 번째 접근방법은 별개의 인증기관을 이용하지 않고 웹사용자간에 공개키를 인증할 수 있도록 하는 것이다. 여기서는 웹사용자들이 알고 있고 신뢰할 수 있는 사람들의 공개키를 인증해 줌으로써 어떤 공개키가 특정인을 사칭하는 사람이 아닌 정당한 사람의 공개키라고 다른 사람들이 믿을 수 있게 한다. 예를 들어 "갑"이 알지 못하는 "병"을 신뢰하게 되는 경우를 살펴보자. "을"은 "병"을 알고 그를 신뢰하므로 "병"의 공개키를 인증하는 전자서명을 한다. "갑"은 "병"을 알지 못하지만 "병"의 공개키에 "을"의 전자서명이 되어 있으므로 "병"의 공개키를 믿을 수 있다. 이와 같이 다양한 사용자들간에 인증 체인이 구성될 수 있다. 예를 들어, "갑"은 "을"을 알지 못하지만 "갑"의 친구인 "병"이 "정"의 공개키에 서명을 했고, "정"이 "을"의 공개키에 서명을 했다. 이 경우에는 "갑"의 친구인 "병"이 "을"의 공개키를 인증하는 경우보다 못하지만 "갑"은 "을"의 공개키를 어느 정도 믿을 수 있다. 인증 체인의 길이가 길수록 공개키에 대한 신뢰도는 떨어지게 된다. 그러나 인증경로가 어느 정도 긴 경우에도 서로 다른 몇 개의 공개키 목록으로부터 여러 사람들의 서명을 확인하게 되면 신뢰도는 증가하게 된다. 이러한 형태로 웹사용자들이 상호 공개키를 인증하여 제공하므로써 신뢰할 수 있는 웹공동체를 구성하게 된다. 웹공동체를 구성하여 공개키를 인증하는 대표적인 예로는 PGP(Pretty Good Privacy)가 있다 (Electronic Frontiers Houston, 1996)

전자서명 또는 전자 인증서에 의한 인증을 통해서도 인터넷 상거래에서의 사기와 부정을 완전히 방지할 수는 없다. 어떤 판매자가 결제시스템에 등록하여 어느 정도 신뢰를 얻은 다음 많은 양의 주문을 받아 대금지불을 받은 뒤에 상품을 인도하지 않고 사라지는 경우, 판매자가 고의적으로 불량품을 인도하는 경우, 결제기관 또는 그 종업원의 부정행위 등은 결제시스템에서 어느 한 수준의 보안체계만으로는 방지하기가 어렵다. 이러한 문제들은 결제시스템의 다단계 보안체계, 웹환경을 수용하는 법과 제도의 정비, 신뢰할 수 있는 웹공동체의 구성을 통해서 해결될 수 있다.

3.2.4 전자화폐의 통화공급효과

신용카드나 전자수표 모형에 기반을 둔 결제시스템에 비하여 전자화폐를 이용하는 경우에는 다음과 같이 통화공급효과를 갖는 장점이 있다. 몬덱스와 같은 오프라인 능력이 있는 전자현금의 등장으로 법정화폐의 공급량은 증가하지 않아도 통화속도가 증가하여 통화공급효과가 나타난다.

Petersen(1995)에 따르면, 다음 식에서 알 수 있는 바와 같이 기존의 통화대신 전자화폐와 같은 새로운 지급결제수단에 의한 거래가 확대되면 M의 증가율은 낮아지고 수식상의 V^*는 커지는 것으로 나타난다. 통화유통속도는 기존의 통화자산을 대체하는 새로운 유사통화와 결제수단이 등장할 때마다 변화게 된다.

$MV = PY$(모든 거래가 전통적인 통화량 M에 의해서만 결제되는 경우)

단, M: 통화량, V: 통화속도, P: 물가, Y: 거래량

$a + M V^* = PY$(a: 새로운 지급결제수단에 의해 제시되는 부분)

현금발행액이 동일한 경우에도 전자화폐 이용이 확대되면, 증가된 전자화폐에 비례하여 현금의 민간보유가 감소하고 현금이 은행에 예치된다. 따라서 은행의 신규예금이 증가되어 파생통화가 창출되고 통화승수가 상승하게 된다. 특히, 우리 나라와 같이 개인수표이용이 관행화되어 있지 않고 고액권의 액면도가 낮은 점을 감안하면 전자화폐의 이용도가 높을 것으로 예상된다.

Ⅳ. 결 론

본 연구에서는 신뢰할만한 제3자에 의한 결제시스템 사례를 신용카드 또는 전자수표 모형에 기반을 결제시스템과 전자현금 모형에 기반을 둔 결제시스템으로 구분하여 각 시스템의 장점과 한계점을 비교분석하였다. 또한 본 연구에서는 사례분석과 6개의 각 결제시스템에서 제공하고 있는 FAQ 분석을 기초로 결제시스템의 수용성, 안전성, 신뢰성, 효율성을 개선하기 위해 결제시스템 설계시 고려되어야 할 21개의 요인을 제시하였다.

신용카드 및 전자수표에 기반을 둔 결제시스템에서는 어떻게 사용자의 익명성과 프라이버시를 보호할 것인가가 가장 큰 문제라 하겠다. 비록 근본적으로는 이 모형에 기반을 둔 결제시스템에서 익명성을 보장하기 어렵지만, 어떤 형태로 결제메카니즘을 구성하는가에 따라 사용자들의 프라이버시에 대한 통제력이 달라진다. 즉, 판매자 중심의 결제시스템과 비교하여 볼 때, 신용카드번호와 계정번호 등의 정보가 판매자에게 노출되지 않는다는 점에서 어느 정도의 기밀성이 유지된다. 네트빌, 이캐시, 몬덱스 등은 소액거래를 잘 지원할 수 있다는 특징을 지니고 있다. 다른 결제시스템과는 달리 퍼스트 버츄얼에서는 암호방식을 사용하고 있지 않는 점이 그 특징이라 할 수 있다. 이캐시의 경우는 무색전자서명이라는 독특한 방법을 통해 지불인의 익명성을 보증하고 있다는 점이 그 특징이라 할 수 있다. 몬덱스는 다른 시스템과는 달리 하드웨어에 기반을 둔 시스템으로서 유일하게 오프라인 능력을 제공하고 있다.

본 연구에서는 결제시스템 설계시 고려되어야 할 요인간에는 상반관계가 발생함을 분석하였다. 오프

라인 능력을 제공하기 위해서는 어느 정도 시스템의 효율성을 저하시키거나 비용을 유발하게 된다. 예를 들면, 소프트웨어 기반의 결제시스템에서는 무료로 소프트웨어를 제공하고 있다. 그러나 몬덱스에서는 오프라인 능력을 제공하고 있지만 소비자는 몬덱스 카드와 잔액판독기를 구입해야 하고, 판매자는 특정 하드웨어 장치를 설치해야 한다. 결제시스템의 사용자는 프라이버시 보호와 익명성을 요구하지만, 결제시스템 운영기관에서는 법집행기관에 보고할 정보를 보유할 수 있기를 바란다. 결제시스템의 수용성을 증가시키기 위해서는 이들 요인간의 상반관계를 해결해야 함은 물론이고, 공개키의 인증성, 극소액거래·저중가거래·고가거래 등에 따라 서로 다른 수준의 보안서비스를 제공함으로써 결제처리에 따른 비용을 감소시키는 방안도 고려되어야 한다.

본 연구의 비교를 통해 어느 결제시스템이 최적인가를 찾기란 어려운 문제였다. 각 결제시스템에서는 서로 다른 결제 프로토콜에 기반을 두고 있으며, 상이한 지불수단을 제공하고 있다. 지불수단의 선호도는 개인에 따라 다르므로 모든 환경에 최적인 결제시스템이 존재한다고 할 수 없다. Singh (1994)의 연구에 따르면, 세금공제가 되는 지출항목과 그렇지 않는 경우에 따라 지불수단의 선호도가 다르다. 일반적으로 공공요금을 지불할 때는 지불 증명이 남는 지불수단을 선호하고, 사업상 수반되는 지출에는 신용카드결제를 선호한다. 지불수단의 선호도가 개인에 따라 상황(소비자 계층, 거래유형, 생활양식 등)에 따라 다르듯이 어떤 환경에서도 최선인 결제시스템이 존재하다고는 할 수 없다. 소프트웨어, 뉴스, 신문, 웹정보 등 정보제품을 거래하는 경우에는 네트빌과 같은 시스템이 적합할 수 있고, TV나 컴퓨터 등 고가의 제품을 구매하는 경우에 소비자는 신용카드에 의한 결제시스템이 적합할 수 있다. 이런 관점에서 볼 때, 결제시스템의 지불수단에 대한 상호운영성은 사용자 수용성을 증가시키는데 중요한 작용을 하게 된다. 따라서 사이버캐시와 네트체크에서는 신용카드와 전자수표에 추가하여 전자현금을 지원하는 형태로 시스템을 확장해 가고 있다. 익명성을 요구하는 거래에서 구매자는 이캐시와 같은 전자동전을 선호할 수 있다. 현재까지 시범운영 중이거나 운영 중인 결제시스템에서 어떤 시스템이 널리 수용되어 사용될 것인지를 단언할 수는 없다. 그러나 점차 사용자들은 부정방지 하드웨어를 장착한 전자지갑과 같은 오프라인 능력을 제공하는 전자화폐를 선호하면서 다양한 지불수단을 공유하여 사용해 갈 것으로 보인다.

본 연구가 이론적 측면과 실무적 측면에서 시사하는 바는 다음과 같다:

첫째, 본 연구의 비교분석 결과는 인터넷 상거래 관련 연구의 기초가 될 수 있다. 특히 본 연구의 사례분석 결과와 인터넷 상거래 결제시스템 설계시 고려되어야 할 다차원 요인은 향후 인터넷 결제시스템의 성공요인을 파악하는데 지침이 될 수 있다.

둘째, 신뢰할 수 있는 제3자에 의한 결제시스템이 구축되어 있지 않는 우리 나라에서 통신업체와 소프트웨어 개발업체 등이 본 연구 결과를 결제시스템 구축시 틀과 지침으로 활용할 수 있다.

셋째, 인터넷 결제시스템의 사용자가 될 소비자, 판매자, 은행을 비롯한 금융기관에서는 결제시스템을 선택하는데 있어서 본 연구 결과를 지침으로 활용할 수 있다.

끝으로 사례분석의 대상이 된 대부분의 결제시스템이 개발 또는 시범운영의 초기 단계에 있는 관계로 본 연구에서는 소비자, 판매자, 운영기관의 경

험을 토대로 한 실증분석을 실시하지 못했고, 몇가지 설계상의 고려 요인이 현실적으로 어떻게 반영되어 그 효과를 나타내고 있는지를 밝히지 못했다.

참 고 문 헌

정범석 · 한인구 (1996), "A Study on Risk Analysis and Security Mechanisms for the Internet Security," 한국경영정보학회 춘계발표 논문집, 496-510

Bakos, J. Y. (1991), "A Strategic Analysis of Electronic Marketplaces," *MIS Quarterly*, 15, 3, 295-310.

Bakos, J. Y., and E. Brynjolfsson (1993), "Information Technology, Incentives and Optimal Number of Suppliers," *Journal of Management Information Systems*, 10, 2, 37-53.

Barua, A., B. Lee, and A.B. Whinston (1994), "Strategies for Smart Shopping in Cyberspace," *Working Paper, http"//cism.bus.texas.edu:80/suri/shopper.html.*

Barua, A., S. Ravindran, and A.B. Whinston (1994), "Supplier Selection Strategies for the Smart Internet Shopper," *Working Paper, http"//cism.bus.texas.edu:80/suri/shopper1.html.*

Bellovin, S. M. and M. Merritt, (1990) "Limitations of the Kerberos Authentication System," *Computer Communication Review*, 20, 5, 119-132.

Berners Lee, et al. (1994), "The World Wide Web," *Communications of ACM*, 37, 8.

Billare, M., et al. (1995), "iKP Family of Secure Electronic Payment Protocol," http://www.zurich.ibm.com/technology/security/extern/ecommerce/

Bloch, M., Y. Pigneur, and A. Segev (1996), "On the Road of Electronic Commerce -- A Business Value Framework, Gaining Competitive Advantage and Some Research Issues," *Working Paper.*

Borenstein, N.S., et al. (1995), "Perils and Pitfalls of Practical CyberCommerce: The Lessons of First Virtual's First Year," *Working Paper*, http://www.fv.com/pubdocs/fv-austin.txt

Boynton, A.C., and R.W. Zmud (1987), "Information Technology Planning in the 1990's," *MIS Quarterly*, 11, 1, 59-71.

Brands, S. (1995) "Electronic Cash on the Internet," *Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security*, Feb., 16-17.

Camp, L. J., M. Sirbu, and J. D. Tygar (1996), "Token and Notational Money in Electronic," http://www.cs.cmu.edu/afs/cs.cmu.edu/user/jeanc/www/usenix.html

Chaum, D. (1992) "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of ACM*, 28, 10, 1030-1044.

Chaum, D. (1995), "Prepaid Smart Card Techniques: A Brief Introduction and Comparison," http://www.digicash.com/publish/card.html

Clarke, R., (1995) "Electronic Payment Mechanisms," http://www.anu.edu.au/people/Roger.Clarke/EC/EPMIntro.html.

Clemons, E. K., S.P. Reddi, and M. P. Row (1993), "The Impact of Information Technology on the Orgnaization of Economic Activity: The "Move to the Middle" Hypothesis," *Journal of Management Information Systems*, 10, 2, 9-35.

Clifford, B., and T. Ts'o (1994), "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications*, 32, 9, 33-38.

CommerceNet (1995a), "Electronic Commerce Jumpstation," http://www.commerce.net/directories/jumpst-

ation/index.html

CommerceNet (1995b), "Electronic Commerce Jumpstation: Payment Systems for the Internet," http://www.commerce.ne/directions/jumpstation/payment.html.

CommerceNet (1995c), "EDI Resources," http://www.commerce.net/directories/humpstation.edi.html

CommerceNet (1996d), "Payments Task Force Resources," http://www.commerce.net/work/taskforces/payments/resources.html.

Cox, B., J. D. Tygar, and M. Sirbu (1996), "NetBill Security and Transaction Protocol," http://www.ini.edu/NETBILL/publications/Usenix.html

Cronin, M. J. (1994), "Doing Business on The Internet: How the Electronic Highway is Trasforming American Companies," Van Nostrand Reinhold, NY.

Cross-Industry Working Team (1996), "Electronic Cash, Tokens and Payments in the National Information Infrastructure," http://WWW.CNRI.Reston.VA.US:3000/XIWT/documents/dig_cash_doc/ElecCashToC.html

CyberCash, http://www.cybercash.com/

Decker, K. M. and S. Focardi (1995), "Technology Overview: A Report on Data Mining," *Technical Report*, Swiss Scientific Computing Center.

Denning, D. E. and G. M. Sacco (1981), "Timestamps in Key Distribution Protocols," *Communications of the ACM*, 24, 8, 533-536.

Diffie, W. and M. Hellman (1976), "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 22, 6, 644-654.

DigiCash (1996), "An Introduction to ecash," http://www.digicash.com/publish.ecash_intro/ecash_intro.html

DigiCash (1996), "Money on the Internet," http://www.digicash.com/

Digital's Microcommerce System, Millicent (1995), http://www.research.digital.com/src/millicent/

EIT (1996), "Secure HTTP,", http://www.eit.com/creations/s-http/

Electronic Frontiers Houston (1996), "EFHPretty Good Privacy Workshop," http://www.efh.org/pgp/

Elgamal, T. (1995), "Commerce on the Internet: Credit Card Payment Applications over the Internet," http://home.netscap.com/newsref/std/credit.html.

Fox, D. (1996), "E-commerce: Payment Mechanism," http://www.kweb.com/e-commerce/paymentm.html.

Froomkin, A. M. (1995), "Anonymity and Its Enmities," http://acr.law.miami.edu/~froomkin/articles/

Froomkin, A. M. (1996a) "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases," http://www.law.miami.edu/~froomkin/articles/ocean.html

Froomkin, A. M. (1996b), "It Came From Planet Clipper: The Battle Over Cryptographic Key 'Escrow'," http://www.law.miami.edu/~froomkin/articles/

Froomkin, A. M. (1996c), "The Essential Role of Trusted Third Parties in Electronic Commerce," http://www.law.miami.edu/~froomkin/ articles/

Froomkin, A. M. (1996d), "The Internet as A Source of Regulatory Arbitrage," http://www.law.miami.edu/~froomkin/articles/ocean.html

Gable, T., D. Cossio, and A. Cebulski (1996), "First Virtual Holdings Identifies Major Flaw on Software-Based Encryption of Credit Cards; Numbers Easily Captured by Automated Program," http://www.fv.com/gabletxt/release2_7_96.html

Garfinkel, S. (1994), *PGP: Pretty Good Privacy*, O'Reilly Associates.

Goodhue, D. L., M. D. Wybo, and L. J. Kirsch (1992), "The Impact of Data Integration on the Costs

and Benefits of Information Systems," *MIS Quarterly*, Vol. 16, No. 3.

Gupta, A., D. O., Stahl and A. B. Whinston (1995), "Pricing of Services on The Internet," in IMPACT: *How ICsup4(2) Research Affects Public Policy and Business Markets*, Fred Phillips and W.W. Cooper eds., Greenwood Publishing, CT.

Gupta, A., D. O. Stahl, and A. B. Whinston (1995), "The Internet: A Future Tragedy of the Commons," *Working Paper*, The University of Taxas at Austin, *http"//cism.bus.texas.edu:80/suri/*

GVU (1996), "GVU's 5th WWW User Survey," http://www.cc.gatech.edu/gvu/user_surveys/

Hallam-Baker, P. M. (1996), "User Interface Requirements for Sale of Goods," http://www.w3.org/pub/WWW/Payments/

Hallam-Baker, P. M. (1995), "Electronic Payment Schemes," http://www.w3.org/pub/WWW/Payments/roadmap.html.

Hitachi (1996), http://www.hitachi.co.jp/Div/nfs/introduction/index-E,html

Jennifer, G. B. Steiner, C. Neuman, and J. I.. Schiller (1988), "Kerberos: An Authentication Service for Open Network Systems," *USENIX Winter Conference*, 191-202.

Kalakota, R. and A. Whinston (1996), *Frontiers of Electronic Commerce*, New York: Addison-Weley.

Kaffy, Braun and Polyzos (1994), "Tracking the Long-Term Growth of the NSFNET," *Communications of ACM*, 37, 8.

Kienzle, J., and A. Perrig (1996), "Digital Money : A Divine Gift or Satan's Malicious Tool?," http://didecs1.epfl.ch/~aperrig/memoirel/memoire1.html

Klein, S. (1996), "The Strategic Potential of Electronic Commerce-An Introduction for Beginners," http://www-iwi.unisg.ch/iwi4/cc/genpubs/ecintro.html

LEtSystems, "Frequently Asked Questions about LETSystems," http://www.u-net.com/gmlrts/faq.html

LETSystems (1995), http://www.u-net.com/

MacKie-Mason, J. K. and H. R. Varian (1994), "Some FAQs about Usage-Based Pricing,"

MacKie-Mason, J. K. and H. R. Varian (1994), "Economic FAQs about the Internet," *Journal of Economic Percepectives*, 8, 3.

Malone, T. W. (1987), "Modeling Coordination in Organizations and Markets," *Management Science*, 33, 1317-1332.

Malone, T. W., J. Yates, and R. J. Benjamin, "Electronic Markets and Electronic Hierarchies," *Communications of ACM*, 30, 484-497.

Manasse, M. S. (1995), "The Millicent Protocols for Electronic Commerce," http://www.research.digital.com/src/millicent/

Mankin, E. (1994), "The Check is in the E-mail...(and, coming soon, electronic greenbacks)," University of Southern California Chronicle, November 7.

MarketNet, "BankNet Electronic Banking Service," http//alpha,mkn.co.uk/help/bank/info.html

Mark Twain Banks, http://www.marktwain.com/

Moore, J. C., W. B. Richmond, and A. B. Whiston (1991), "A Decision Theoretic Approach to Information Retrieval," *ACM Transactions on Database Systems*, 15, 3, 311-340.

Natioanl Westminster Bank Plc, (1996), *Mondex*, http://www.mondex.com/mondex

NetChex, (1996), http://www.netchex.com/

NetMarket, (1996), http://www.netmarket.com/

Netscape Communications Corporation, "The SSL Protocol," http

Netscape Communications Corporation, (1996), "Netscape White Papers," http://www.netscape.com/newsref/std/index.html

Neuman, B. C., and T. Ts'o (1994) "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications Magazine*, 32, 9, 33-38, http://nii.isi.edu/publications/kerberos-neuman-tso.html

Open Market, Inc. (1996), "Security on the World Wide Web," http://www.openmarket.com/

Pays, P. (1996), "An Intermediation and Payment System Technology," *Fifth International World Wide Web Conference*, http://www5conf.inria.fr/fich_html/papers/P27/Overview.html

Petersen, D. J. (1995), "Monetary Aggregates, Payments Technology, and Instituional Factors," *Economic Review*, Federal Reserve Bank of Atlanta, November/December.

Peirce, M. (1996), "Payment Mechanisms Designed for the Internet," http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html.

Pirce, M. and D. O'Mahony (1995), "Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set," *4th International World Wide Web Conference*, Boston, http://www.w3.org/pub/Conferences/WWW4/Papers/228/

Ravindran, S., A. Barua, B. Lee, and A.B. Whinston (1994), "Strategies for Smart Shopping in Cyberspace," *Fifith Conference on Organizational Computing, Coordination and Collaboration*, University of Taxas at Austin, http://cism.bus.utaxas.edu:80/suri/shopper1.html.

Rinaldi, A. H. (1996), "The Net: User Guidlines and Netiquette - Index," http://www.fau.edu/rinaldi/net/

Rivest, R. L., A. Shamir, and L. Adleman (1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 21, 2, 120-126.

RSA Data Security, Inc., "All About S/MIME," http://www.rsa.com/rsa/S-MIME/

RSA Data Security, Inc. (1995a), "RSA's Frequently Asked Questions About Today's Crytography," http://www.rsa.com/

RSA Data Security, Inc. (1995b), "RSA's Frequently Asked Questions About Today's Crytography: Capstone, Clipper, and DSS," http://www.rsa.com/

RSA Data Security, Inc. (1995c), "RSA's Frequently Asked Questions About Today's Crytography: DES," http://www.rsa.com/

RSA Data Security, Inc. (1995d), "RSA's Frequently Asked Questions About Today's Crytography: Factoring and Discrete Log," http://www.rsa.com/

RSA Data Security, Inc. (1995e), "RSA's Frequently Asked Questions About Today's Crytography: General," http://www.rsa.com/

RSA Data Security, Inc. (1995f), "RSA's Frequently Asked Questions About Today's Crytography: Key Management," http://www.rsa.com/

RSA Data Security, Inc. (1995g), "RSA's Frequently Asked Questions About Today's Crytography: Miscellaneous," http://www.rsa.com/

RSA Data Security, Inc. (1995h), "RSA's Frequently Asked Questions About Today's Crytography: NIST and NSA," http://www.rsa.com/

Schneier, B. (1994), *Applied Cryptography: Protocol, Algorithms, and Cource Code in C*, New York: John Wiley & Sons.

SIC (1996), "Visit a Variety of Electronic Commerce Sites in the World: Electronic Commerce Islands," http://www.park.or.jp/ECommerce/index_e.html.

Singh, S., (1994) "Marriage, Money, and Information:

Australian Consumers," *Doctoral Dissertation*, La Trobe University, Melbourne, Australia.

Tygar, J. D. (1996) "Atomicity in Electronic Commerce," *ACM/IEEE 21st Conference on Principles of Distributed Computation*.

UCLA at Berkeley (1996), "Commerce: Digital Cash, Network Payment, and Online Banking," http://www.sims.berkeley.edu/resources/infoecon/Commerce.html.

VeriSign, "About VeriSign, Inc," http://www.verisign.com/

VISA (1996), "SET Specifications," http://www.visa.com/cgi-bin/sf/set/intro.html

W3C (1995), "Micro Payment Transfer Protocol(MPTP) Version 0.1, W3C Working Draft 22, Nov, http://www.bilkent.edu.tr/pub/WWW/TR/WD-mptp.html.

Waidner, M. (1996), "You are Interested in ...," http://www.zurich.ibm.com/Technology/Security/sirene/pointers_complete.html.

Waidner, M. (1996), "You are Interested in: Electronic Commerce, Payment Systems, and Security," http://www.informatik.uni-hildesheim.de/Ecommerce.html

Wayner, P. (1994), "Agents Away," *Byte*, May, 113-118.

Zabih, R. (1996), "Creating an Efficient Market on the World-Wide Web," http://www.priceweb.com/curr/essay.html.

A Comparative Study on the Payment Systems of Electronic Commerce on the Internet

Jaehun Joo*

Abstract

By lowering the transaction cost including unit search and communication costs, and providing detail informations on a specific product and its price from many different suppliers to consumers, the electronic commerce on the the Internet holds the promise of increasing the efficiency of commerce. On the other hand, because of the nature of open and distributed network, the Internet does not ensure the secure commerce unlike the closed networks on which some kinds of safeguards are granted. To improve the efficiency of electronic commerce on the Internet, we need the secure commerce payment system providing the means of making the secure payments, sending confidential messages, and authenticating identities of buyer and supplier.

Thus, in this paper, we answered and discussed the following problems by surveying and reviewing the payment systems developed and/or being operated by six third parties:

What kinds of payment systems exist and how do they provide security services including confidentiality, authentication, integrity of messages, and non-repudiation?

What are their advantages and disadvanges?

What are key elements that should be considered when designing a successful payment system?

What trade-offs have to be resolved?

* Assitant Professor, Division of Business Administration and Economics, Dongguk University