정보학연구 제2권 제1호 1999년 3월(pp.35-52)
The Studies of Information Technology, Vol.2, No.1

전자상거래의 보안기술과 지불방법에 관한 연구

조원길*

요 약

구매자와 공급자가 새로운 전자화폐를 통한 결제시스템의 도입에 있어 공급자의 과제는 전자화폐의 유용성에 대한 평가기준인 상업성, 안정성, 제한조건 등의 문제를 중심으로 살펴볼 필요가 있다. 사용자인 구매자와 상인이 안전한 결제시스템을 선택할 경우에 그들의 needs를 분석하여 활용해야 하며, 특히, 상업적조건은 새로운 지불방식에서 필수적으로 고려되어져야 한다. 즉, 사용하기 편리하고 비용이 적게 들어야 함을 물론 다용도로 쓰일 수 있어야 한다. 이러한 사용자의 필요성의 충족 없이(즉, 보안기술의 확보 등)는 궁극적으로 사용자들로부터 외면받게 될 수 있다. 이에 따라 사용자들에게 선택의 폭을 넓게 해 줌으로써 궁극적으로 전자상거래의 활성화에 이바지 할 것이다.

I. 서론

오늘날 전자상거래의 급속한 증가는 개인용 컴퓨터의 빠른 보급 및 확산에서 현실화되고 있다. 이러한 전자상거래는 단순히 전자적으로 업무를 수행하는 것에서 기업의 생산활동 및 고객서비스까지 전과정에 대한 정보적 통합을 가능케 하여, 소비자는 온라인으로 상품을 탐색, 주문, 상품정보를 교환하고, 다른 소비자들로부터 상품정보를 얻어 고품질 상품을 낮은 가격에 협상할 수 있다. 또한 정부차원의 세금징수, 기업간 정보유통, 새로운 시장형성, 국가간 거래 등 모든 경제활동분야에 영향을 미치고 있다.

최근 영국을 비롯한 선진국을 중심으로 컴퓨터와 정보통신기술이 비약적으로 발전하면서 기존의 화폐를 통한 결제 시스템의 문제점을 해결할 수 있는 전자화폐의 개발과 실용화를 위한 노력이 증대되고 있다. 전통적인 결제 방법의 첫 번째 문제는 바로 편리성의 부족 즉, 일반적으로 소비자가 온라인 플랫폼을 떠나 전화를 사용하거나 결제를 위해 수표를 보내야 한다는 점이다. 둘째, 보안의 부족 즉, 인터넷을 통한 전향적인 방법으로 결제를 하기 위해서는 소비자는 카드/결제계정의 상세 내용과 다른 개인적인 정보를 온라인으로 보내야 한다. 인터넷을 떠나 전화와 혹은 우편을 통해 카드/결제계정의 상세내역을 제공하는 것은 보안문제를 야기하게 된다는 것이다. 셋째, 적용범위의 부족 즉, 신용카드는 가입된 상점에서만 사용할 수 있으며, 일반적으로 개인 對 개인 혹은 기업 對 기업의 결제 트랜젝션을 지원하지 못하고 있다. 넷째, 부적합 즉, 잠재적인 구매자가 신용카드와 수표계정에 적절한 신용등급을 모두 가진 것은 아니다. 다섯째, 소액단위의 트랜젝션 지원의 부족 즉, 인터넷을 통한 수많은 결제는 전화 혹은 우편을 통한 결제비용이 너무 높이 여겨질 정도로

* 강남대학교 무역학과 강사

충분하지 않다.

이러한 결제방법을 다루는 비용은 판매자에게는 상당한 부담이 되고 있다. 이러한 문제점들을 보완하기 위해 현재까지 개발되고 실험적으로 실용화되고 있는 전자화폐로는 Mondex를 중심으로한 IC카드형과 네덜란드 Digicash사의 e-cash와 같은 네트워크형으로 구분할 수 있다. 또한 보안유지를 위한 결제 시스템의 차이로 인하여 모든 결제를 중앙에서 확인토록 한 중앙집중식 결제형(closed loop)과 전자화폐의 데이터를 하나의 카드에서 다른 카드로 직접 이체할 수 있는 분산형(open loop)으로도 나눌 수 있다.

IC카드형은 영국을 비롯한 유럽에서 주로 개발 사용되어 왔고 최근에는 뉴욕을 비롯한 미국의 몇몇 도시에서 실험적으로 도입되고 있다. 하지만 미국에서는 광범위한 지역적 특성과 발달된 통신망을 통한 상거래의 증가로 인하여 네트워크에서 결제할 수 있는 시스템개발에 역점을 두고 있다. 그러나 IC형 전자화폐의 경우에도 카드를 판독할 수 있는 전화기나 전용기기가 있으면 통신을 통한 전자상거래에서도 네트워크형과 마찬가지로 결제에 쉽게 사용할 수 있기 때문에 미래에는 전자화폐를 두 가지 형태로 구분할 필요성은 감소할 것이다.

따라서 본 연구에서는 전자화폐를 이용할 수 있는 안전한 지불시스템들의 보안기술과 특징을 살펴보고 현재 사용중인 암호 및 암호를 활용한 안전한 결제모델에 대한 기술적 현황을 분석하여 기업들이 전자상거래를 활용할 때 고려해야 할 기술적 문제들에 대하여 도움을 주고자 한다.

II. 전자상거래 환경

2.1 네트워크와 상거래

전자적인 네트워크를 통해서 사업 활동을 하는 것은 최근에 시작된 일이 아니다. 예를 들어 TV로 광고를 한다든지, 카달로그에 실려있는 상품을 전화나 FAX를 통해서 주문하고 있음에도 불구하고 어떠한 것도 깊게 생각해 보지 않았다. 또 은행의 ATM[1]기가 주변에 가까이 있으며 친근한 존재이다.

기업은 TV를 사용하여 광고를 하고, 그 광고를 본 소비자는 상점에 몰려든다. 폐쇄적이지 않은 프로토콜[2]을 가지고 있는 인터넷[3]을 통해서 전세계가 급속도로 서로 접속될 수 있도록 된다면 판매, 배달, 고객지원을 위해서 일부러 자사(自社)전용 네트워크를 구축하지 않아도, 최대의 시장인 글로벌 시장에 상품을 공급할 수 있을 것이다. 이와 같은 새로운 시장에 진출하려 한다면, 소비자의 흥미를 끌고, 상품에 대한 설명을 하고, 상품을 배달하기 위한 전자적 기술이 상당히 흥미 있을 것이다.[4]

1994년 후반부터 인터넷상에서의 상거래를 생각하는 기업이 급속도로 늘어 오고 있다. 이들 기업들은 모두 인터넷상에서의 상거래가 안전하고 간단하게 가능해지도록, 그리고 그 과정을 통해서 이익을 얻는 것을 목표로 하고 있다. 이러한 목적을 달성하기 위한 방법은 다양하지만 크게 두 가지로 나누어 볼 수 있다. 하나는, 안전성과 신뢰성이 결여된 인터넷상에서도 상거래에 관련된 정보를 유통시키는 것이 가능하도록 안전성과 신뢰성을 높인 채널[5]을 만들어 내는

1) 현금자동입출금기. 현금카드를 이용해서 현금을 입출금할 수 있도록 하는 기계인데. 최근에는 고성능화가 이루어져 계좌이체나 정기예금구좌의 개설도 가능해졌다.

2) 정보통신 네트워크에서는 통신용 약정(통신규약)을 가리킴. 데이터 그 자체의 정의나 데이터를 주고 받기 위한 순서 등으로부터 생성.

3) 인터넷을 한마디로 설명한다는 것은 상당히 어렵다. 여기서는 "TCP/IP라고 하는 공통의 프로토콜"을 사용한 "세계 규모"의 "개방"적인 "네트워크에 접속된 것(네트워크의 네트워크)"라고 정의하겠다. 원래는 학술 분야를 중심으로 연구가 진행되어 왔는데, 그 목적 및 발전 경위로부터 상용(商用)으로 이용하기 위해서는 신뢰성 및 안전성과 관련하여 몇 가지 문제가 제기되고 있다.

4) ピート・ローシン著, エレクトロニック・コマースの實務, ダイヤモンド社, 1996.

것이다.

2.1.1 인터넷과 다른 新시스템

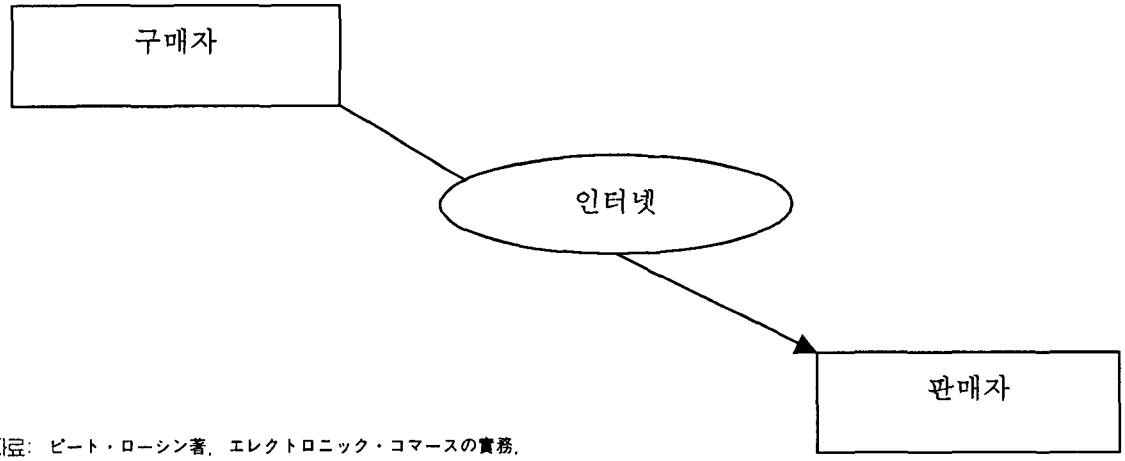
인터넷이 상상을 초월한 짧은 기간동안 넓게 보급됨으로 인하여 많은 사람들이 인터넷의 실체에 관하여 잘 모르고 있는 상태이다. 실제로 인터넷은 1969년(인류가 처음으로 달에 착륙한 해임)에 시작된 인터넷워킹[6]에 기원을 두고, 그 이후 그 규모는 매년 착실히 넓어지고 있다. 인터넷 이외에 1969년 이후에 개발보급된 것을 생각해 본다면, 그간의 눈부신 기술진보가 있었다는 것을 알 수 있다. 예를 들면, 비디오, CATV, ATM, CD, 개인용 컴퓨터, 휴대폰 등이 있다.

인터넷을 일반적으로 표현한 것이 <그림 - 1>이다. 이 그림에서는 인터넷상에서 의사소통을 하는 시스템간에 구매자가 의식할 필요가 없는 구조를 나타내고 있는 것을 강조하기 위하여 타원형으로 나타내고 있다.

이와 같은 구조는 정가운데에 나타난 다수의 컴퓨터나 네트워크로 구성되어 있지만, 인터넷을 이용할 때에는 이러한 실제 구조가 어떠한 것이지 알아야 할 필요가 없다.

전세계 규모의 전화망을 「운영」하는 조직이 없듯이, 인터넷을 운영하는 조직 또한 존재하지 않는다. 그 대신에 접속된 쌍방의 네트워크에 이용자가 따라야 할 규칙(즉, 프로토콜)을 규정한 표준화 조직이 존재한다. 이러한 규칙이 정확히 엄수된다면, 전화, FAX, 컴퓨터로부터 그 네트워크에 통신신호를 보내고 받고 하는 것이 가능하다. 바꿔 말하자면, 네트워크를 이용하려 하는 전화회사가 CCITT[7]의 프로토콜에 적합하고, 상대방의 전화회사 또한 그 프로토콜에 적합한 이상, 글로벌 네트워크에 접속하고 있는 어느 누구와도 통화가 가능하다는 것이다. 만약 독자적인 프로토콜에 의한 전화서비스에 가입한다면, 접속이 가능한 상대편이 그다지 많지 않

〈그림 1〉 구매자와 판매자가 인터넷을 통한 접속방법



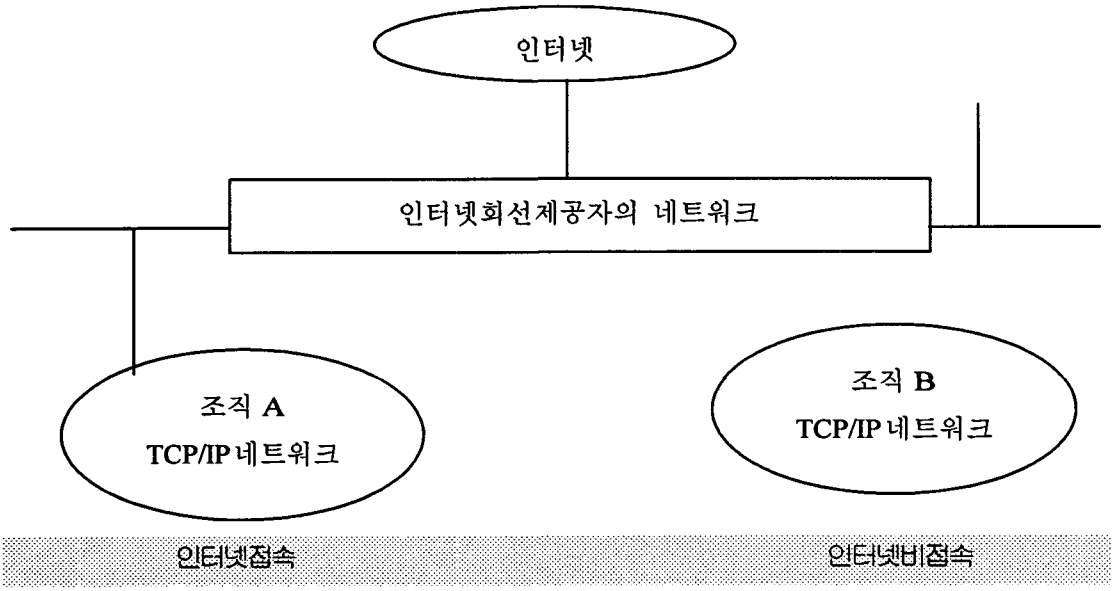
자료: ビート・ローシン著, エレクトロニック・コマースの實務, ダイヤモンド社, 1996, p.16.

5) 경로라는 뜻. 예를 들면 판매 채널이라는 것은 물건을 판매할 경우 필요한 정보가 이동하는 경로나 실제로 그 물건이 유통되는 경로를 의미한다.

6) 복수(複數)의 네트워크간을 접속한 네트워크 전체를 확대시켜 나아가는 것을 말함. 또는 이를 위해서 필요한 일체의 제품, 기술, 정보의 총체.

7) 국제전화자문위원회. 통신망의 표준화에 대한 작업을 하던 국제기관으로 존재하였으나, 현재는 CCIR(국제무선통신 자문위원회)와 함께 ITU(International Tel전자상거래ommunications Union : 국제전기통신연합)의 전기통신 표준화 분야에서 전기통신의 기술, 비용, 요금 등과 관련한 표준화를 검토 보고하는 활동을 하고 있다. URL : http://www.itu.org

〈그림 2〉 프로토콜의 인터넷 접속형태



자료: 전게서, p.18.

을 것이란 것을 쉽게 알 수 있다.

인터넷에서도 같은 의미로 말할 수 있다. IAB (International Architecture Board)[8]가 인터넷의 프로토콜을 평가 제정하는 역할을 하는 IETF (Internet Engineering Task Force)[9]를 감독하고 있어서, 만약 사용중인 컴퓨터가 인터넷 프로토콜에 적합한 네트워크에 접속이 가능하고, 그것이 인터넷에 접속되어 있으면, 네트워크에 접속되어 있는 다른 컴퓨터와 그로벌하게 데이터를 교환하는 것이 가능하다. 만약 인터넷 프로토콜이 아니고, 다른 프로토콜을 통하여 네트워크에 접속하고 있다면 인터넷에 접속을 하게 된 경우 문제가 발생할 것이다.

하지만 실제에 있어서는, 이용하고자 하는 대규모의 네트워크에 접속포인트[10]가 없다면, 적정한 인터넷 프로토콜을 이용하고 있다 하더라도, 반드시 인터넷에 접속이 가능하다고는 할 수 없다. 회사가 기업내의 교환기와 네트워크를 이용하여 각 개인의 책상에 전화기와 컴퓨터를 설치하였다하더라도 외부와 접속을 해 놓지않으면 이러한 설비들은 기업내의 의사소통(communication)에만 이용할 수 있다. 다음 <그림 - 2>에 나타난 것처럼, 기업이 인터넷 프로토콜을 이용하고 있는 외부의 기업과 데이터를 교환하

8) 인터넷을 통하여 여러 가지 정보교환업무을 수행하는 조직인 ISOC(Ineternet Society : 인터넷 협회)의 하부조직. IAB는 표준규격의 제정과 관련한 책임이 있으며, 새로운 규격의 제정이 요구될 경우, 그 문제를 검토하고 표준화 규격을 제정하여 인터넷상에서 통지하게 된다. URL : http://www.iab.org/iab

9) 인터넷 기술 특별조사 위원회. 인터넷의 기술문제를 검토하고 있는 봉사조직. 주로 프로토콜안을 검토하여, IAB에 대해서 그 프로토콜의 표준화를 권고함. IETA에서는 어느 누구도 토론이나 자세한 문제를 검토하는 작업그룹에 참가할 수 있으며, 그 결과는 문서화되어 기본案이 된다. URL : http://www.ietf.org/

10) 네트워크의 네트워크인 인터넷에 접속하기 위한 포인트. 기업내부의 LAN 등과 같은 네트워크를 인터넷에 연결하는 경우나 개인의 컴퓨터를 인터넷에 연결하는 등의 경우가 있다. 동상 인터넷 회선제공자라고 불리우는 접속업자가 인터넷에 접속하기 위한 통로(접속포인트)를 준비하게 된다.

기 위해서는 그 기업의 기업내 네트워크가 인터넷에 접속되어 있어야 한다.

2.1.2 네트워크와 전자상거래의 현재

온라인에 의한 거래[11]를 고찰하기 위해서는 거래의 역사를 뒤돌아보면서 향후에 대하여 예측을 하는 것이 매우 중요하다. 방송네트워크, 특히 TV네트워크는 여러가지 상품을 판매하는 수단으로 이용되어 왔지만, 시청자는 그 미디어(TV)를 주문의 수단으로 사용하지 않는다. 신용카드가 널리 보급된 것에 의해 소비자와 기업은 전화를 이용해서 거래행위를 해오고 있다. 또한 신중한 금융 업계까지도 1970년대 후반부터 ATM기를 도입하였다

이처럼 전자상거래(이하 전자상거래)시장에의 참가자가 인터넷을 통한 상거래의 메커니즘을 이해하고 있으면, 온라인 상에서 판매하는 것은 전화로 개인적으로 물건을 사는 것과 같은 모습으로(또는 그 이상) 간단하게 신뢰성이 높은 방법이라는 것을 쉽게 이해할 것이다.

2.2 전자상거래 모델

인터넷을 통한 상거래는 어떠한 구조를 가지고 이루어지고 있는 것일까? 이것을 이해하기 위해서는, 일반적인 상거래 방법을 이해할 필요가 있다. 서로 다른 형태의 상거래간에는 다른 점이 많이 존재한다. 대기업이 업자로부터 대량의 원재료를 구입하는 거래와 학교에 다니는 어린아이가 과자가게에서 사탕을 사는 거래는 서로 같이 않지만 공통적인 특징도 있다.[12]

11) 상거래는 크게 판매업자와 구매업자가 직접 마주보고 하는 「대면 거래」와 그렇지 않은 「비대면 거래」로 나뉜다. 또한 비대면 거래는 「off line」과 「on line」으로 나뉠 수 있는데, 전자는 통신판매 등을 예로 들 수 있다. 온라인에 의한 거래는 통신회선을 통해서 실시간에 비대면 거래를 하는 것으로서 TV쇼핑 등이 있다.

일반적인 상거래의 과정을 통해서, 전자상거래에서 문제점으로 제기되고 있는 것들에 관해서 검증해 보고자 한다. 아래의 각 항에서, 누구나 가볍게 드나들 수 있는 작은 상점에서의 거래에 대하여 살펴보자.

2.2.1 신뢰관계의 구축

작은 상점에서 상품을 구입할 경우, 일단 그 상점에 들어가지 않으면 안 된다. 보통 상점은 일반 손님들에게 개방되어 있고, 구매자는 단순히 그 상점으로 걸어 들어가는 것만으로 상품을 고르는 것이 가능하다. 그러나 반드시 이러한 형태라고는 단정지을 수 없다. 상품을 사람이 직접 보고 만질 수 있는 곳에 진열하여 판매하는 것도 가능하며, 또는 특정의 단골손님에게만 판매하는 것도 가능하다(판매업자는 중개업자만을 상대로 장사를 할 것이며, 고급상점에서는 소개를 통한 손님에게만 장사를 하는 것도 가능하다.). 상점측에서는 취급품목과 관련하여 구매자나 그 접근방법에 관한 결정권을 가지고 있는 것이라고 할 수 있다.

한편 구매자 쪽에서도 그 상점에 들어가지 전에 어떠한 것을 구입할 것인지를 결정할 수 있다. 종종 구매자는 쇼윈도우를 보는 것만으로, 그 상점에 자신이 찾고 있는 물건이 있는가 그리고 신뢰하고 구입할 수 있는지에 관하여 판단을 내려야 한다. 이 때문에, 상점측에서는 구매자를 끌어들이기 위해 그들이 취급하고 있는 상표를 표시하던지, 취급가능한 지불방법을 스티커로 표시하던지, 참고품을 전시하는 등의 행위를 한다. 유명회사의 이름을 이용한다던지, 잘 알려진 기업의 지점이나 체인점인 것 등을 통해 구매자로부터의 신뢰를 얻는 것이 가능하다.

한편, 상점과 구매자사이에는 어느 정도의 신

12) ピート・ローシン著, op. cit., pp.18~27.

뢰관계가 구축되어 있다. 상점측에서는 구매자는 상품을 구비하고 대금을 지불할 것이라고 생각하고 있다. 또한 구매자쪽에서는, 상점이 자신이 원하는 상품을 준비해 놓고 있으며, 원하다면 상품의 배달(거기에 필요하다면 수리점검까지)도 해 줄 것이라고 기대하고 있다. 다음에 나타난 것처럼 만약에 상점측과 구매자쌍방이 실제로 상거래상의 어떠한 결정(or 약속)에 합의를 한다고 하면 보다 더 높은 수준의 신용이 필요할 것이다.

2.2.2 계약조건의 교섭

대부분의 작은 상점에서는 상품의 진열이나 가격의 결정이 그다지 어려운 일이 아니다. 구매 담당자가 필요한 물품을 사들이고, 그 상품의 가격을 표시한다. 대부분의 경우 단지 이러한 과정만으로 족하다. 그렇지만 색상이나 사이즈 등으로 인하여 소비자가 원하는 상품을 바로 제공할 수 없을 경우, 상점측에서는 그 상품을 주문한다든지, 같은 가격으로 유사한 상품을 소개한다든지(슈퍼마켓에서 특가품으로서 판매하고 있음) 납품을 기다리게 한 후, 큰폭으로 가격할인을 해주는 등의 대체안을 제시할 것이다.

작은 상점에서의 상거래에서는 상점측의 가격결정이 적절한지, 상품은 구매자가 원했던 상품인지 등에 관하여는 간단하게 판단이 가능하다. 하지만 전자상거래에서는 손님이 실제로 주문을 했는지, 또는 판매자가 그 가격으로 실제 거래를 하고 있는지를 확인하기 위해서는 특별한 도구가 필요한 것이다.

전자상거래에서 부정한 거래를 피하고 싶다면 부정방지 장치가 필요 불가결이다. 만약 자기 자신이 직접 상점의 진열대에서 상품을 고르고 대금을 지불한 후, 그것을 가지고 간다면, 무엇을 얼마에 구입했는지 바로 알 수 있다. 또한 카달로그 판매의 상품을 전화로 주문하는 경우에는 카달로그에 게재되어 있는 가격을 보면 된다(이러한 경우에도 상대방이 주문내용을 정확하게 기재하고, 신용카드 번호를 입수한 상태에서 실종되지 않는 한 구매자는 신뢰감이 생긴다.). 그러나 인터넷을 통해서 상품을 주문할 경우에는 제시된 가격이 정확한지 알아본다든지, 구매자가 주문한 상품이 실제로 어떤 상품인지 등을 알아볼 수 있는 직접적인 방법은 없다.

판매자 구매자간 쌍방이 주문이 이루어진 후에 상품의 가격이나 주문된 상품에 관하여 거절하는 것이 불가능하다. 이것이 가능하게끔 하는 장치가 전자상거래에서 필요로 하는 것이다.

2.2.3 지불과 결제

어떠한 거래에 있어서도 그 주요한 목적은 가치의 교환이며 이것은 일반적으로 표준통화와 제품 서비스간에 일어난다. 사람들은 구매에 익숙해져 있기 때문에, 구매를 하는 과정을 매우 간단하게 생각하고 있다. 구매자는 현금수표신용카드 등을 건네주고 그 대신에 상품과 영수증을 건네 받는다.

이러한 행동을 전자적인 형식으로 바꾸는데는 어느 정도의 작업이 필요하다. 혼잡하고 사람이 많은 상점안에서 자신의 신용카드번호를 큰소리로 말하는 사람은 어느 누구도 없을 것이며, 상품에 따라서 익명으로 그 상품을 구입하려 하는 사람도 있을 것이다. 이와 같은 의미로 전자상거래에서도 프라이버시를 보호하는 것이 요구되고 있다. 대금의 지급과 관련된 프라이버시를 보호하는 방법으로는 전자상거래의 대금지급 방법을 암호화 함 완전한 off line상태에서 거래를 하여 제 3 자를 경유하여 결제함 등의 방법이 있다.[13]

13) ピート・ローシン著, op. cit., pp.20~26.

보통의 상점에서는 구매자가 상품의 대금을 지불함과 동시에 거래가 완료된다. 그렇지만 인터넷에서는 정보, 영화, 소프트웨어 등의 네트워크를 통해서 전자적으로 입수가 가능한 상품을 제외하고는, 판매자가 제품을 배달해 준다는 것에 대하여 구매자는 믿을 수 밖에 없다. 이러한 문제를 해결하는 방안중의 하나가 신뢰를 바탕으로 한 인터넷벤더[14]와 거래하는 방법이 있고 또한 인터넷벤더와 문제가 발생하였을 때 보증을 해줄 수 있는 대기업의 신용카드를 사용하는 방법도 있다.

인터넷벤더 측에서도 온라인에 의한 거래를 할 경우에는 같은 종류의 리스크가 존재한다. 그 이유는 신용카드는 네트워크에 의한 결제화사와 연결이 되어 있어 본인의 확인이 자동적으로 이루어지기 때문이다. 이것은 일반적으로 작은 점포에서 점원이 신용카드 확인 단말기[15]를 통해 확인을 할 때와도 같은 경우라 할 수 있다. 온라인에서 상거래를 하는 벤더와 작은 점포 모두 전자서명[16]을 이용하는 것이 편리하다.

14) 인터넷과 관련하여 상품을 판매하는 것을 업으로 하는 者를 의미. 인터넷으로의 접속서비스를 하는 업자를 인터넷 회선제공자라고 한다. (여기서는 인터넷 회선제공자를 의미). 인터넷 회선제공자는 다른 회선제공자와 서로 접속을 한다. 또한 인터넷 네트워크에 접속이 가능한 워크스테이션이나 PC 등의 컴퓨터를 판매하는 업자도 넓은 의미에서 인터넷벤더라고 한다.

15) 신용카드 뒷면에 자기 테이프를 읽고, 앞면의 카드번호를 쳐서 확인하는 등의 작업을 통해, 그 카드가 합법적으로 이용되고 있는 지를 온라인으로 원격지의 컴퓨터에 접속하여 신용을 조회하는 단말기. 통상 CAT (Credit Authorization Terminal)라고 불리운다. 일본의 CAT는 신용조회뿐만 아니라 매상전표정리나 집계도 가능한 다목적 단말기도 있다.

16) 디지털화 된 데이터에 대해서 수학적인 방법 등을 이용하여 만들어진 서명, 통상 디지털화된 데이터는 복제가 용이하지만 디지털 서명을 붙임으로 인해 위조방지나 그 서명자의 특정(特定) 등이 가능하게 된다.

Ⅲ. 전자상거래 보안 기술

3.1 전자상거래 보안

구매자는 자신의 account ID를 비밀로 유지하려 하지만, 인터넷상에 존재하는 것이기 때문에 판매자는 간단히 사용자의 account에 access할 수 있으며, 핵커 또한 access하는 것이 가능하다. Account ID는 판매자·구매자 쌍방에 있어서의 가장 기본적인 증명서이기 때문에 이를 이용해서 양심적이지 못한 판매자가 판매자용 ID를 위조 사용해서 사기 행위를 범할 위험도 존재한다.

퍼스트 버처의 판매 방식이 안전하지 못하다고 생각될지 모르지만, 모든 중요한 정보는 완전히 오프라인의 상태에서 다룬다는 점을 상기해 주었으면 한다. 큰 리스크라고 하면, 구매자가 판매자를 속이는 것, 정보를 도난 당하는 것, 타인에 의해서 부정한 account ID로 조작되는 정도를 들 수 있다.

3.1.1 보안의 현황

여기서는 인터넷상에서의 전자결제시스템에 대하여 검토해 보자. 일단 정보의 내용은 인터넷을 통하여 전송되는 데이터와 그렇지 않은 데이터라는 두 가지로 나눌 수 있다. 인터넷상에서 보내지는 것은 account신청서에 기입된 이름, 전화번호, 전자메일에 관한 데이터이다. 신용카드 정보는 인터넷을 통해서 보내지지도 않으며, 인터넷을 통해서 access가 가능한 시스템상에 저장되지도 않는다. 이 때문에 신용카드 정보의 안전은 확실하다고 할 수 있다. 그러나 account를 새롭게 취득할 때의 정보나 거래정보는 인터넷상에서 모니터링 되기 때문에 전자메일을 도중에 갈취당할 위험성이 존재한다.

다음으로는 대금결제 절차에 대하여 알아보

자. 거래 내용의 확인서가 전자메일을 통해 구매자에게 도착할 때까지 또는 구매자가 스스로 대금지급에 합의한다는 내용의 메일을 보낼 때까지 실질적인 대금결제는 이루어지지 않은 상태이다. 또한 구매자 스스로가 대금지급에 합의한다는 내용의 메일을 보낼 때까지 실질적인 대금결제는 이루어지지 않은 상태이다. 또한 구매자가 부적당한 거래내용의 확인서를 받았다고 하면, 사기적행위가 있었던 것으로 간주하여 그 account ID를 영구 무효화하는 것이 가능하다. 그러나 account ID가 도중에 갈취당하는 것을 완전히 막는다는 것은 어렵다고 할 수 있다. 이에 퍼스트 버쳐에서는 구매자에 대해 정기적으로 전자메일을 확인하도록 권장하고 있다.[17]

이러한 리스크는 어느 정도 존재하지만, 심각한 피해에까지 이르지 않고 있다. 온라인 상에서 판매되고 있는 정보를 도난 당했다 할지라도 판매자의 피해는 없다. 정보를 도난 당했다는 것은 틀림없는 사실이지만, 판매자는 이에 상관없이 평상시처럼 구매자에게 정보를 판매할 수 있다. 이것은 구매자·판매자 쌍방에게 중요한 문제이기 때문에 퍼스트 버쳐는 문서내에 이러한 내용과 관련된 글을 언급하고 있다. 거기에는, 전자메일을 포착하거나 답장을 위조하는 것은 상당히 어려우며 핵커는 핵커의 추적에 필요한 흔적을 반드시 남긴다라고 언급되어 있다. 흥미있는 코멘트로, '이러한 능력을 가진 사람은 판매자가 되어 퍼스트 버쳐를 통해서 물건을 판매하는 것보다도 범죄행위에 더 관심을 가지고 있다'라고 한 것이다. 현실세계에서의 신용카드를 통한 사기 행위와 퍼스트 버쳐에서의 것과는 매우 유사하지만, 퍼스트 버쳐의 account를 갈취하는 것 보다는 신용카드를 위조하는 것이 대부분의 방법이며 수단이다.

궁극적으로 퍼스트 버쳐의 인터넷 결제 시스템이 어떠한 약점을 가지고 있다는 것은 확실하다. 물론 이것은 다른 결제 시스템도 마찬가지이다. 대금지급이라고 하는 가치의 교환행위를 하고 있을 때에는 항상 정보를 훔치려 하는 악의의 공격이라는 리스크가 존재한다. 퍼스트 버쳐에서의 인터넷 결제시스템에서는 판매대상을 "정보"로 한정한과 동시에 구매자의 승인에 의해 거래가 성립되도록 하는 것을 통해 작당한 수준으로 균형을 맞추고 있다고 할 수 있다.

따라서 인터넷을 활용한 결제시스템은 정보판매에 한정되어 있다는 점에서, 퍼스트 버쳐의 인터넷 결제 시스템은 전자상거래를 위한 완전한 해답이라고는 할 수 없다. 이에 반해, 개인이나 소규모의 기업이 디지털 상품을 판매하는 조직으로써 중요한 존재라고 할 수 있다.

3.1.2 암호화와 암호

퍼스트 버쳐가 암호화나 전자서명을 사용하지 않는 이유는 다음과 같다. 첫째, 암호화나 전자서명은 복잡하고 취급하기 어렵기 때문에, 그 처리에 있어서 몇 가지의 단계를 더 추가하여야만 한다. 둘째, 암호화나 전자서명과 같은 암호기술은 복잡하기 때문에, 誤用되어, security에 대한 잘못된 지식을 갖게 될 수도 있기 때문에, 바르게 사용될 수 있도록 하는 또 다른 장치가 필요하다(공개 열쇠 암호 등). 이것은 비용을 증대시켜 판매자가 이를 꺼리도록 유도한다. 셋째, 대금지급 정보를 오프라인을 통해 주고받기 때문에 암호화나 전자서명은 필요가 없다. 마지막 이유가 최대의 point이다. 퍼스트 버쳐의 참가자는 중요한 대금 지급정보와 관련하여서는 절대로 인터넷을 통해 송신하지 않고, account ID를 사용한다.

17) ピート・ローシン著, op. cit., pp.47~56.

3.1.3 코드와 사이퍼(암호)

코드, 사이퍼, 엔클립션, 디사이퍼 라고 하는 말들은 각각 특정의 의미를 지니고 있다. 엄밀히 말해서 코드라고 하는 것은 단어의 위치를 바꾸어, 각기 코드화 된 단어가 특정의 다른 단어로 표현되는 것을 의미한다. 코드에서는 움직임의 규칙을 나타내주는 코드북(code book)이 필요하다. 만약 코드북을 분실했을 경우에는 암호화된 문장을 해독하는 것을 불가능하게 되며, 그 코드북만 가지고 있으며 어느 누구라도 암호의 해독이 가능하다. 사이퍼라고 하는 것은 암호화 수법의 기본이라고 할 수 있다. 사이퍼는 메시지 중에 있는 개개의 문자를 반복 가능한 rule(알고리즘)에 의해 변화시킴으로서 기능을 하게 된다. 알고리즘의 사용법을 결정하는 특별한 번호를 「열쇠」라고 하며, 같은 알고리즘에 대해서 다른 「열쇠」가 사용된다면 역시 다른 암호가 만들어진다. 여기서 암호학의 목적을 다시 한번 생각해 보았으면 한다. 그것은 바로 비밀을 비밀 그 상태로 유지하는 것이다. 앞서 언급한 것처럼 암호화는 메시지가 다른 사람에게 전달되지 않을 것이라는 확신이 없을 경우에 사용된다. 메시지를 보통의 문장 형식 그대로 비밀을 유지하는 것이 이상적이지만, 그것이 언제나 가능하다고는 할 수 없다. 일단 암호화했다면, 사용하고 있는 알고리즘이 악의를 지닌 사람에게 알려지지 않는 편이 좋다. 암호를 파괴할 수 있는 모든「열쇠」를 생각해내는 것이 가능하기 때문이다. 그러나 정말로 좋은 알고리즘은 어딘가에도 노출되어 있지는 않지만, 어느 알고리즘이 사용되고 있는 지를 밝혀 내는 방법은 무수히 많다. 어떤 암호 알고리즘이 사용되고 있는지를 알고 있다 하더라도 안전한 열쇠와 파괴하기 어려운 알고리즘으로 인해 포기하게 되는 것이다.

전통적인 사이퍼는 단 하나의 열쇠를 발신인과 수신인이 공유(그리고 어느 누구도 알지 못하도록)하는 것에 의해서 그 기능을 발휘했다. 발신인이 그 열쇠로 알고리즘을 움직이게 함을 통해 보통의 문장을 암호문으로 변환시키고 수신인은 같은 열쇠로 알고리즘을 역방향으로 움직이게 해서 메시지를 해독한다. 이것이 공유열쇠암호[18]방식으로 알려져 있는 것이다.

3.2 전자상거래에서의 암호방식 응용

기존의 문헌을 통해 다들 이해하고 있겠지만, 암호방식, 특히 공개열쇠 암호는 네트워크트워크트워크상의 온라인에 의한 상거래를 안전하게 하기 위해서 매우 중요한 역할을 담당하고 있다. 암호방식의 응용은 本 연구를 통하여, 또는 다른 곳에서도 끊임없이 언급되고 있다.[19]

3.2.1 암호화

특정의 열쇠를 통해서 정보를 해독할 수 없도록 하는 것을 암호화라고 한다. 열쇠는 대칭적(對稱的)으로 사용이 가능한 공유열쇠이든, 비대칭적인 공유열쇠이든 상관없다. 암호문이 brute force 공격이외의 강력한 암호해독의 공격을 받지 않는다고 할 경우, 열쇠의 길이가 길면 길수록 암호화된 정보가 해독될 가능성은 적어진다. 공개열쇠 암호법에서는 공개열쇠와 배밀열쇠 라는 두 종류를 사용한다. 공개열쇠로 암호화한 메시지를 전송할 경우, 송신자는 수신자의 공개열쇠로 암호화를 해서 보낸다. 그 암호문은 수신자의 비밀 열쇠를 사용하는 것만으로 해독이 가능하게 된다. 실제로 공개열쇠 암호법은 보안

18) 암호화와 복합화에 같은 열쇠를 이용하는 「공유열쇠암호」에 있어서의 열쇠를 의미. 대표적인 암호방식으로 「DES」, 「RC4」, 「IDEA」 등이 있다.

19) ビート・ローシン著, op. cit., pp.74~76.

성이 상당히 높지만 컴퓨터 資源이라고 하는 면에서의 그 대상(代償) 또한 크다고 할 수 있다. 그 결과 공유열쇠 암호법과 동시에 사용하는 경우도 자주 있다. 예를 들면 송신자가 큰 용량의 정보를 암호화한 비밀 열쇠를 공개열쇠 암호법을 사용하여 암호화 한후 전송하는 것이다. 송신자와 수신자는 하나의 공유열쇠를 사용해도 좋고, 그 하나의 열쇠를 기준으로 서로간의 연락을 위한 별도의 몇 가지 열쇠를 새로이 만들어도 좋을 것이다. 공유열쇠의 송수신에 상당히 보안성이 높은 공개열쇠 암호법을 사용하며, 용량이 큰 다른 정보는 다른 암호법이 사용된다.

누군가가 암호화된 문장을 수신하여 해독하려 할 지도 모른다. 그러나 매우 큰 공유열쇠를 사용하여, 그것을 단 1회만 사용하고 두번다시 사용하지 않는다면 이 방법은 비교적 긴밀성이 높은 방법이 될 것이다.[20]

3.2.2 전자서명

송신자가 자신의 비밀열쇠를 사용하여 데이터를 암호화한 후 전송한 경우, 그 암호문은 수신자의 공개열쇠를 가진 사람이라면 누구라도 해독이 가능하다. 이 경우 메시지의 내용을 누군가로부터 지키기 위한 방법은 생각해 낼 필요는 없으며, 누구라도 송신자의 공개열쇠만 가지고 있으면 원래의 문장으로 변환하는 것이 가능하다. 실제로 이것이 문서에 전자적으로 서명을 하는 방법이 되는 것이다. 이와 같이 암호화된 경우, 해독에 필요한 공개열쇠를 가진 주인으로부터 전송된 것이라는 것을 보증 받을 수 있는 것이다. 그러나 모든 메시지를 해독하야만 한다는 의미도 내포하고 있고, 비현실적이다. 또한 공개열쇠를 인증하여 등록해 두는 문제 또한 존재한다.

20) 伊藤賢司 外5人, 電子商取引のすべて, NTT出版, 1996.

전자서명보다 좋은 방법은, 메시지의 내용을 핫슈 계수를 이용해서 보다 취급이 용이한 정보의 뭉치로 요약하는 것이다. 이 뭉치는 송신자의 비밀열쇠에 의해 암호화되고, 메시지의 가장 뒤에 첨가되게 된다. 수신자는 수신한 메시지에 대해서 동일한 핫쉬 계수를 이용해서 요약함과 동시에 송신자의 공개열쇠로 메시지에 내포되어 있는 요약을 보통의 문장으로 바꾼다. 그 용약이 일치하면, 메시지의 내용은 본인으로부터 전송되어 온 것이라는 것이 인증되는 것이며, 일치하지 않을 경우는 인증될 수 없다.

3.2.3 발송부인(發送否認)과 메시지의 일관성 보증

전자서명에서는 두 가지의 副産物이 있다. '발송부인'이라고 하는 것은 메시지의 발송인이 그것을 보낸 것에 대해서 부정할 수 없는 상황을 나타내는 암호학의 용어중에 하나이다. 통상 전자우편은 비교적 가단히 변경하는 것이 가능하기 때문에 이를 부정하는 것이 가능하다. 그러나 전자적으로 서명된 전자우편은 이를 부정하는 것이 불가능하다. 전자서명이 정당하다면, 그 본인 이외에 다른 사람은 그것을 전송하는 것이 불가능하기 때문이다.

전자서명의 중요한 또 다른 부산물(副産物)은 메시지의 일관성 보증이다. 메시지가 전자적으로 서명되어 전송된 경우, 서명을 확인하는 것으로, 그 메시지가 송신자로부터 전송되음에 있어서 타인에 의한 변경이 없었음을 알 수 있다. 두중에 한번 멈추어 변경된 후, 다시 원래의 송신지로 보내진 메시지는 전자서명을 확인하는 것이 불가능하다. 전자서명을 확인할 수 있다는 것은, 메시지가 타인에 의한 수정 변경없이 도착되었다는 것을 보증한다. 더욱이 송신자는 자신이 송신한 메시지를 부인할 수도 없게 된다.

Ⅳ. 전자결제의 방법

4.1 전자결제의 환경

신용카드에 의한 결제는 온라인 거래에서 다양한 결제방법 중 가장 적절한 결제방법이다. 사람들이 전화주문이나 mail order 등 서로 멀리 떨어진 장소와의 거래에 있어서 신용카드를 사용하는 것이 익숙해져 있기 때문이다. 신용카드에 의한 거래에 필요한 것은 매우 단순하다. 주문을 할 때, 신용카드 번호와 유효기간(특히 청구자의 주소도)만을 표시해 주면 된다.

이 정보는 전자우편과 같은 표준 인터넷 application에 의해서 송신되며, 지금까지도 자주 이용되어 왔다. 이것은 현재까지 이러한 방식으로 거래를 하다가 신용카드 번호를 분실했다는 경우를 실제로 들어본 적은 없으나 그 가능성은 충분하다고 하겠다. 단, 인터넷상에서 신용카드에 의한 거래를 안전하게 하기 위해서는 암호화를 이용하면 되고, 이것 또한 그다지 어렵지 않다. 한편 네트워크상에서 현금거래를 한다는 것은 상당히 난해한 일이다. 그 이유로 두 가지를 들수 있다. 하나는 보통「현금」이라고 하는 말로부터 물리적인 수수(授受)를 연상하게 되는 것이고, 다른 하나는 현금지급이라는 것은 익명성을 지니고 있다는 것이다. 현실세계의 화폐를 전자적인 "coin"으로 바꾸어 특정 종류의 정보의 뭉치로서 취급하는 것인데, 현금 지급을 전자화(電子化)하는 데에는 이외에도 해결해야 할 문제들이 산적해 있다. 즉, 공개열쇠 암호와 전자서명을 이용하는 경우에는 중앙은행이 관리하는 시스템을 이용하는 것이 최선일 것이다.

또한 네트워크상에서 수표를 사용하는 것은 비교적 간단하다. 수표라고 하는 것은 매우 정형화된 정보(은행번호, 계좌번호, 수취인, 금액 등)가 기록되어 있고 구좌 보유자가 서명을 한 단순한 서류에 지나지 않는다. 현실세계에서 인쇄된 수표를 전자수표화 할 때에는, 네트워크상에서 안전하게 전송하는 방법과 전자서명을 하는 방법만이 요구된다. 이것은 어떤 의미에서는「전자현금」과 비슷하지만, 수표에「기재하다」라는 측면에서 볼때 익명성에 대한 배려가 필요없기 때문에 보다 단순하다고 할 수 있다.[21]

4.1.1 안전한 전자결제

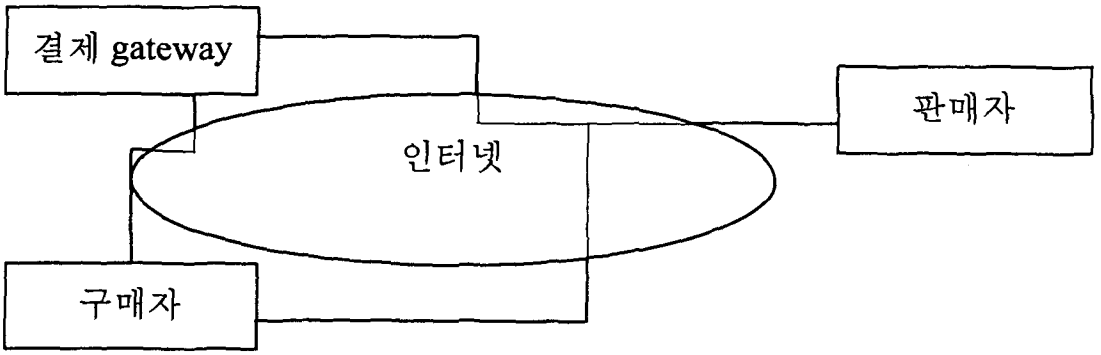
네스케이프社가 제공하는 결제 프로토콜은, 전자상거래상에서 다음과 같은 세가지의 서로 다른 욕구를 충족시켜 주고 있다. 즉, 구매자, 판매자, 신용카드의 여신기관이 제공하고 있는 결제gateway[22]을 들수 있다. <그림 - 3>에 나타난 것처럼 구매자와 판매자는 보안채널[23](예를 들면 SSL)을 통해서 통신을 하고, 판매자와 결제 gateway간에도 보안채널을 통해서 통신한다는 것을 상정하고 있다.

여기서 중요한 것은, 그 채널은 두 지점 사이에서 만 안전하게 기능을 한다는 것이다. 보안채널에 의해 송신된 데이터는 송신지에 도착했을 때에 암호가 풀리게 된다. 전자결제 프로토콜은, 대금결제 정보가 두개 이상의 보안 채널을 통과할 대에도 그 전달 루트의 끝에서부터 끝까지 보안기능을 제공하여야만 한다.

첫째, 구매자로부터 판매자, 판매자로부터 결제 gateway, 결제 gateway로부터 판매자에게 전송되는 상거래 데이터에 있어서의 전자서명, 둘째, 구매자로부터 판매자, 판매자로부터 결제 gateway, 결제 gateway로부터 판매자에게 전송

21) 伊藤賢司 外5人, op. cit., pp.77~83.
22) 결제 gateway. 인터넷상에서 신용카드 등을 이용하여 결제를 할 경우, 결제 시스템과 외부와의 통신을 하기 위해 설치된 조직을 의미.
23) 기밀누설 등과 같은 것에 대해서 안전성이 확보된 채널을 의미.

〈그림 3〉 보안이 확보된 네트워크 프로토콜의 보안 채널



자료: 伊藤賢司 外5人, op. cit., p.113.

되는 상거래 데이터의 부인불가(否認不可), 셋째, 정보가 그 발신자(예를 들면 구매자)에 의해 암호화 되고, 다음의 주체(예를 들면 판매자)에게 전송되게 되는데, 세번째의 주체(예를 들면 결제 gateway)에 의해서 만이 암호를 푸는 것이 허가되도록 하는 또 다른 암호(예를 들면 신용카드 번호) 모든 주체들(구매자, 판매자, 결제 gateway)의 욕구를 충족시키기 위해서는 위에 열거한 기능들이 전자결제 프로토콜에 필요하게 되고, 또한 이를 위해서는 다음의 사항들이 필요하게 된다. 첫째, 구매자의 신용카드 정보(PIN, 다른 인증 정보, 고객정보 등이 이에 속함)를 공개하지 않는다(판매자에 대해서). 둘째, 다른 정보들(가격, 제품, 품질, 구매자 등)을 (결제 gateway에)공개하지 않는다. 이들 각각이 발신자 인증[24]작업을 실시하고, 부인불가성(否認不可性)[25]을 확보(예를 들면 구매자가 자신이 주문한 것을 나중에 부인할 수 없도록 함)하기 위해서는 모든 주체간의 통신에 전자서명을 한다.

4.1.2 전자결제에 필요한 요소

전자상거래에 참여하는 사람들은 각기 여러 가지의 염려들을 하고 있지만, 그 중에서 상거래상의 보안을 확보한다는 것은 모두에게 있어서 이득을 줄 수 있는 것이라고 할 수 잇다. 여기서의 보안을 확보한다고 하는 것은, 상거래의 정확한 정보를 보호하는 것, 개개의 참가자가 부인불가성을 가지고 전자서명이 된 통신을 통해서 각기 자신의 행동에 책임을 지는 것이라고 할 수 있다.

구매자는 어떠한 상황이라 할 지라도 상거래 정보를 공개하지 않는다고 상정할 수 있다. 모든 상거래 정보는 보안 채널을 통해서 도청자로부터 보호되어야 한다. 은행 판매자가 권한외의 목적으로 그 정보를 이용할 수 있는 가능성이 있기 때문에 신용카드 정보를 판매자에게 알리

24) 통상 네트워크에서 전송되어 오는 데이터가 누구로부터 보내진 것인지를 특정(特定)하는 기술.

25) 네트워크를 통하여 발신자로부터 수신자에게 전송되는 데이터에 대해서 발신자수신자 쌍방이, 발신한 사실, 수신한 사실 등에 대해서 부인을 할 수 없도록 하는 장치를 구축한 상태.

지 않는다고 생각할 지도 모른다. 그러나 그 상거래에 대해서 이의가 제기된 경우에 신용카드 번호를 포함한 거래를 뒷받침해 줄 수 있는 증거를 제시하는 것은 판매자의 의무이다. 이와 마찬가지로 판매자나 구매자 또한 주문 정보가 누군가에게 알려지는 것은 원하지 않는다고 생각할지도 모른다. 판매자는 상거래의 여신정보를 받기 위해 결제 gateway에 충분한 구매정보를 전달하려 하며, 결제gateway는 그 서비스에 동의하고 내용을 정확히 해석하여 요구를 승인한 판매자로부터 상거래 정보를 받으려 한다.[26]

4.2 전자상거래 결제 모델

전자결제를 이행하기 위한 수단을 기술적으로 설치하는 것과 실제로 그것을 사용할 수 있게 되는 것, 사용하기 편리하게 하는 것 등은 또한 각기 다른 문제이다. 인터넷을 상업적으로 이용하기 위한 수단으로서 WWW가 각광받고 있는 것은 그것이 판매자 구매자 모두에게 있어서 상품의 전시공급구입 등에 편리한 환경을 제공해 주기 때문이다. 하지만 최초의 WWW는 상거래를 목적으로 한 것이 아니고 정보의 發信을 목적으로 만들어진 것이기 때문에 안전하게 상거래를 하기 위해서는 security 기능이나 특별한 프로토콜을 추가하지 않으면 안된다. 단, 그 security 기능이라고 하는 것은, 그 자체의 정보를 안전하게 전송하는 것만을 보증하면 되는 것이고, 실제 대금지급과는 관계가 없다. 대금지급 정보가 受理되면 그후의 처리는 다른 차원에서 해결하여야 한다.

대금지급 정보의 송수신이 가능한 것만으로는 전자상거래가 상업 활동이 가능한 환경이라고 말할 수 없다. 우선 서버가 안전하게 데이터를 수신할 수 있는지에 대한 확인부터 해보아야 한다. 일반적으로는 대금지급 정보만이 안전하고 정확하게 송신되면 된다고 생각하고 있는데, 배달, 제공가격 등의 정보 또한 전자 서명과 함께 송신될 수 있도록 한 시스템도 있다. 또한 security 라고 하는 것은, 주문정보를 암호화한다는 의미에 그치는 것이 아니고, 마치 신용카드 정보를 수신할 수 있는 점포인양 행세를 하는 범죄를 막는 다는 의미까지도 포함되어 있다. 더욱더 중요한 것은 그러한 고객들의 신용카드 정보를 축적하고 있는 점포의 서버시스템에 대한 안전 확보상의 문제이다.

전자상거래의 환경은 우선 시장과 비지니스에 따라 대금지급 방법을 달리할 수 있게 하는 등 가능한 한 유연성을 지니고 있어야 한다. 다음으로, 판매자가 구매자와 관련된 정보를 적절히 가능한 범위 내에서 수집하는 것이 가능하도록 support 해줄 수 있는 것이 요구된다. 이는 최종적으로는 종합적인 비지니스 환경에 통합되어야만 하는 것인데, 그 과정은 상품의 배달지시, 결제 행위, 구좌상태 보고, 주문상태 보고, 마케팅 정보의 수집이라고 하는 주문처리의 결과로 발생되는 행동들에 대해서 이를 정보로서 취득하는 것이 된다.

인터넷상에서는 secure server[27]를 구입하여 네트워크 소프트웨어를 설치 하는 것만으로 판매자가 될 수 있다. 인터넷상에서의 주문을 편지나 전화에 의한 주문과 동일하게 수작업(手作業)으로 처리하면 된다. 이렇게 하는 편이 보다 통합적인 어프로치 보다는 낮은 비용이 들기 때

26) 伊藤賢司 外5人, op. cit., pp.116~120.

27) 개방적인 네트워크사에서 클라이언트와 안전한 통신을 할 수 있는 구조를 가진 서버. WWW서버에서는 SSL을 이용한 Netscape Communicator Server 등이 security server라고 할 수 있다. Netscape Communicator Server에서는 클라이언트로부터 통신 상대가 「올바른 서버」인지를 나타내는 "서버 인증"과 "서버/클라이언트 간의 통신을 암호화하여 제 3 자의 침입을 막는 기능"을 가지고 있다.

문에 대량의 주문을 기대하지 않는 판매자에게 있어서는 매력적일지도 모른다. 그러나 온라인의 이점을 최대한 살리려고 하다면, 전자상거래의 환경을 보다 완성도 높은 것으로 만들 수 있는 투자가 필요하다.[28]

4.2.1 온라인 및 오프라인에서의 거래

일반에게 인터넷을 통해 상거래 정보를 직접 전송하는 경우, 일정의 암호기술을 이용해서 그 정보에 대한 공격으로부터 방어를 하고 있다. 암호화에 의해「훔쳐보기」라고 하는 인터넷상의 거래에 있어서의 최대의 범죄(라고 들 생각하고 있는데, 실제로는 그렇지 않다.)로부터 정보를 지키는 것이 가능하다. 적절한 강도(强度)로 암호화된 데이터는 그러한 종류의 범죄로부터 완벽하게 안전하다. 라고 하는 것은 암호화된 신용카드의 번호를 해독하는데 몇년이상 걸려서 해독해도 수억엔의 비용이, 즉시 해독을 해도 수억 앤 규모의 비용이 든다고 하면 이보다 간단한 방법을 사용할 것이라는 것이다.

그러나 중요한 정보를 전송하는 데에 더욱더 적절하고 안전한 방법이 있음에도 불구하고 과연 굳이 개방적인 네트워크를 통해서 정보를 전송하려 할 필요가 있을 것인가? 예를 들면 거래처와 거래에 관한 이야기를 할 때에는 전화보다도 실제로 만나서 이야기하는 것이 보다 안전하다고 생각이 들것이다. 국가 기밀과 같은 특수한 경우를 제외하고, 직접 만나서 이야기를 하면 누군가가 도청하고 있다는 것을 바로 눈치챌 수 있기 때문에 안심을 할 수 있는 것이다. 직접 만나서 이야기를 하는 것보다는 전화를 통한 대화가 도청의 가능성이 높지만(합법 비합법적인 여러 가지 도청기나 개별 회선에 의한 도청, 휴대폰이나 무선전화기의 도청 등 그 방법은 무수히 많다.), 최소한의 배려만 있다면, 전화를 통한 대화에서도 어느 정도의 안전성을 확보할 수 있다. 우편이나 fax에 의한 송신을 경우도 같은 종류의 노하우가 적용될 수 있다. 즉 중요한 정보를 전송하는 수단은 인터넷만 있는 것이 아니다. 인터넷 시스템을 이용한 상거래 시스템 중에는, security의 확보에 소프트웨어를 사용하지 않고, 이러한 비교적 안전한 다른 수단을 이용한다고 하는 해결 방법을 취하고 있는 것도 있다. 고객에게 전화나 fax, 인쇄물의 우편송신 등을 통해 신용카드번호, 고객의 이름, 주소 등을 보내게끔 하고 있다.

또한 온라인에 의한 상거래모델은 기업에 있어서 가장 간단한 것은 서버의 운영이나 주문, 콘텐츠의 관리를 전자 몰의 운영자나 인터넷 서비스 제공자라고 하는 다른 기업에 위탁하는 것이다. 단, 이러한 경우에도 주문을 받고 처리할 수 있는 체제를 준비하는 작업은 필요하다. 지금까지 언급한 것처럼, 인터넷상에서 직접적인 비지니스를 하는 거장 간단한 방법은 secure sever를 설치하고, 웹 페이지를 만든 후, 주문을 받을 수 있는 form을 만드는 것이다.[29]

4.2.2 판매자로부터의 요구사항

지금까지 언급한 것처럼 판매자가 secure sever를 구축한 것 만으로는 EC가 가능한 환경이라고 할 수 없다(이용자 측에서는 보안기능이 있는 브라우저만 있으면 완벽한 온라인 쇼핑의 환경을 구축했다고 할 수 있다). 전자상거래에서는 버킷[30] 인프라가 필요한 것이다. 이 중에는 신용카드의 조회에 필요한 네트워크로의 접속 등 대금결제수단의 supporter가 포함되어 있다.

28) David Kosiur, Understanding Electronic Commerce, Microsoft Press, 1997.

29) 八木 勤, 電子商取人(EC)入門, 1996, pp.93~107.

30) front end의 반대. 사용자로부터 보기 어려운 부분의 application.

판매자는 매상을 올리기 위해서 구매자에게 구매에 있어서의 편리성을 제공해 주어야만 하는데, 이를 위해서는 여러 가지의 대금지급 방법을 받아들여야 한다.

전자상거래 환경을 제공하고 있는 기업은, 인터넷을 이용하는 판매자에게 통합적인 완전한 해결책을 제공해 주려고 노력하고 있다. 이러한 환경에 포함된 것들로서 WWW콘텐츠의 제작도구, CM의 제공, secure sever software, WWW서버의 관리를 위한 도구, 신용카드나 전자적 대금결제 방법을 이용한 결제 시스템으로의 링크 등을 들 수 있다.

이에 온라인상에서 제품을 판매하기 위해서 필요한 기능으로서는 우선 최소한 다음과 같은 환경이 필요하다. 첫째, 인터넷상으로 받은 여신서비스 기관[31]에 대급지급 정보를 송신할 수 있는 환경. 둘째, 신용카드의 여신 서비스기관으로부터 받은 구매자의 정보를 자동으로 처리할 수 있는 환경. 셋째, 이용자로부터의 주문과 관련하여 전자서명 등 동의 증거를 남길 수 있는 환경. 넷째, 전자적 영수증, 이용명세서, 주문에 관련한 내부서류 등 거래 내역의 확인에 필요한 정보를 작성할 수 있는 환경. 그리고 온라인거래라 할지라도 전화나 FAX에 의한 주문을 받을 수 있는 환경도 필요하다.

이러한 조건들은 온라인상의 비지니스에서 필요한 것들이기 때문에, EC환경을 제공하는 업체는, 최소한 이 정도의 기능을 갖추고 있어야 할 것이다. 이러한 설비에서 요구되는 기능들은 EC환경 중에도 제공되고 있을지 모르지만, 그것은 단순히 판매자들에게 편리하도록 제공되고 있는 것이기 때문에, 판매자 측에서는 간단하게 설비를 조달하고, 또는 다른 제공업체에 위탁하는 것이 가능하다.

31) 상품구매에 따른 대금지급에 있어서 현금으로 일괄 지급하는 것이 아니고, 다른 방법으로 결제를 할 때에, 그 구매자가 대금지급 능력이 있다는 것을 증명해 주는 기관. 보통 신용카드회사, 소비자 금융회사가 그 기능을 담당하고 있다.

4.2.3 구매자에게 요구되는 사항

구매자가 상점에 access할 수 있고, 구매의사를 표시하는 것이 가능하다면, 구매자측에서는 전자상거래 환경이 준비된 것이라고 할 수 있다. 하지만 현실세계의 상거래와 마찬가지로 구매자가 희망하는 대금결제 방법이 이용될 수 있도록 하는 것이 바람직하다. 즉, 전용의 전자결제 방법뿐만 아니라 주요한 신용카드에 의한 결제도 가능하도록 해야 한다.

구매자도 판매자와 마찬가지로 결제명세서나 이용명세서가 필요할 것이며, 이는 디지털 상품을 구입했을 경우에는 더욱더 그러할 것이다. 영수증이나 월별 결제 청구서, 이용명세서 등이 제공되지 않으면, 온라인 상에서의 많은 판매자들을 구분 비교하는 것이 힘들어 질 것이다.

Ⅳ. 결론

지금까지 인터넷상의 상거래 데이터를 지키는 secure sever 및 보안기술에 대해서 알아보았다. 또한 전자화폐나 그 외의 다른 결제시스템이라고 하는 것은 protector를 설치한 전자데이터라고 하는 형태로 가치를 인터넷상에서 주고 받는다고 하는 것을 의미한다. 전자화폐와 결제시스템은 secure sever나 EC의 환경과 같은 개념으로 비교되어서는 안 된다. 가치를 교환하는 방법을 추가하는 것으로, EC환경을 보강해주는 존재이다.

이러한 서비스를 제공하고 잇는 회사들은 두 종류의 접근방법을 취하고 있다. 하나는 사용자가 일반적으로 사용하는 결제수단(신용카드, 수

표 등)을 서비스 제공업자에 의해 관리되고 있는 온라인상의 신분 증명서에 링크시키는 방법이다.

다른 하나는 전자화폐를 이용하는 방법이다. 보통, 전자화폐 서비스를 제공하는 금융기관에 구좌를 개설하는 것 만으로 전자화폐의 이용이 가능하다.

본 연구에서 언급해 온 選擇肢는 모두 구매자와 판매자간의 secure channel, application 이 통신하는 데이터의 암호화라고 한 특정의 온라인 security 가 존재한다는 전제에 기초하여 왔다. 하지만, 기업가(起業家)나 개발자가 온라인 비지니스에 대하여 연구하는 것과 함께 다음의 두 가지 접근법이 유효하다. 즉, 암호기술에 의해 channel의 security를 확보하고, 온라인 거래에 알고리즘을 통해 거래를 수행하고, 기밀성이 높은 데이터에 대해서는, 온라인 이외에 보다 안전한 경로를 통해 전송한다는 것이다. 또한 개발자의 입장에서 보면 channel 의 security를 확보하기 위해서는 암호기술은 필수불가결한 조건이다. 하지만 암호기술을 설치하여 이용하는 데에는 많은 비용이 소요되고, 그 비용으로 인해 그 이점이 상쇄되어 버리는 경우도 많다. 이러한 비용에는 다음과 같은 요소가 포함되어 있다. 즉, 암호도구의 허가와 관련된 라이센스料, 새로운 브라우저와 서비스의 개발과 보급, 공개열쇠 증명서[32]의 관리, 거래를 위해 필요한 컴퓨터의 처리 비용의 증대, 강력한 암호도구에는 수출규제가 있으며, 미국 이외의 나라에 암호기술을 반출하는 것이 금지되어 있는 것 등이다.

앞서 언급한 것처럼 긴밀성이 높은 데이터를 인터넷 이외의 다른 것을 통해서 전송하도록 한다면, secure경로나 안전한 대금결제를 위한 프로토콜을 설치하지 않아도 비교적 안전한 EC환경을 구축할 수 있다. 사용자의 입장에서 중요한 것은, 이러한 종류의 시스템을 제작하는 것에 의해 security를 고려한 새로운 프로토콜을 장착한 특별한 소프트웨어를 버젼업한다든지 새로 구입한다든지 할 필요가 없다는 것이다. 이것에 의해 기존의 channel(WWW 서버, 파일 전송, 터미널 에뮬레이션, 전자몰 등)을 모두 상거래에 이용하는 것이 가능하다. 더욱이, 향후 등장할 어떠한 application이나 네트워크라 할지라도 아무 변경 없이 간단하게 support하는 것이 가능한 것이다.

이와 같이 각국에서는 Mondex와 같은 IC카드형과 e-cash와 같이 라인상에서만 결제할 수 있는 형태의 전자화폐개발과 실험이 이루어지고 있다. 우리나라의 경우 최근 몇몇 은행과 기업을 중심으로 전자상거래에 있어서의 결제시스템 개발을 시도하고 있다. 또한 기존에 시용하던 각종 직불카드나 버스카드등을 통합한 IC카드를 부분적으로 개발하여 실험하고 있다. 그러나 이러한 전자화폐의 개발은 몇가지 상업적조건, 안전성에 관한 조건, 그리고 제한성에 관한 조건 등에 적합한 시스템에 중점을 둬야 할 것이다. 우리가 기존에 신용카드를 이용한 전자상거래의 결제방식과 개인간에 이체가 이루어지지 않는 단순한 IC형 카드는 향후 외국의 보다 편리하고 안전하며 비용이 적게 드는 결제시스템이 도입될 경우 경쟁력에서 뒤떨어지게 될 것이다. 따라서 전자상거래의 결제에 필요한 호환성이 높은 전자지불시스템 개발과 실용화가 시급하다.

32) 증명서 발행국(CA)가 발행하는 「공개키」에 대한 증명서. CCATT에서 권고된 X.509라고 하는 증명서 형식으로 발행된다.

참고 문헌

기술과 법연구소, 전자상거래 : 그제도적·기술적과제, 1997

박춘식 譯, 전자상거래, 이한출판사, 1997.

北澤 博, EDI入門, EDIFACT日本委員會, 1991.

권도균, "전자상거래 활성화의 열쇠 디지털 화폐와 지불 시스템", Internet, 1997

국민경제연구소, "전자금융시대의 도래와 은행의 대응 전략", 1997

금융결제원, 전자상거래 보안 프로토콜 SET 조사연구 보고서, 1997

김영진 역, Yoshiyuki Inoue지음, "전자화폐란 무엇인가 ?" 1997.

김현일 역, 이와사키 가즈오, 사토 모토로리 지음, "전자화폐 전쟁", 1995

인터넷, "전자상거래 활성화의 영쇠 디지털 화폐와 지불시스템", 1997

전국은행연합회, "전자화폐시대의 도래와 그 대응방안", 1997

전자신문, http://www.etnews.co.kr/etnews, 1998

정보통신협회, "한국형 전자화폐를 활용한 유통 시스템 모델 개발", 1996

제일금융연구원, "새로운 돈의 혁명: 전자화폐", 1997.

한국금융결제원, 1997, "전자상거래 보안 프로토콜 SET 조사연구보고서", 전자금융연구소

한국전자거래표준원, "전자상거래 시대의 금융기관의 대응방안", 1998

한국금융연구원, 전자금융. 화폐 국제심포지움. 1996.

한국금융연구원, 주간국제금융동향, 제5권 40호. 1996.

Benjamin, R. and Wigand, R., "Electronic Markets and Virtual Value Chains on the Information Superhighway," Sloan Management Review, 1995.

Cash, J. I., eccles, R. G., Nohria, N.; and Nolan, R. L. Building The Information-Age Organization: Structure, Control, and Information Technologies, Homewood, Illinois, Irwin. 1994.

Kambil, A., "Electronic Commerce: Business Practice and Strategy," Business economics, Vol.30, 1995.

Michael N. Gualtieri, "Turning the ec Vision into Reality", *EDI World,* November 1996.

Pushpendra Mohta, "The Internet:Where Businesses Do Business",*ec World,* Sep. 1997.

Ravi Kalakota & Andrew B. Whinston, Frontiers of Electronic Commerce, Addison-Weley Publishing Company, Inc, 1996.

Rocklelein, W., "System for Purchases on the Internet Requirements and Evaluation," Fifth Symposium on Research and Teaching in Electronic Commerce in Bled in Slovenia, www.whu-koblenz.de/wi/Purchases/, 1995.

Singley, R.B. and Williams, M.R., "Free riding in retail stores: An investigation of its perceived prevalence and costs.", Journal of Marketing Theory & Practice , Vol. 3 No. 2, 1995.

The Banker, "Shopping for Money," 1996.

A study on Secure Payment Method & Security Technology of Electronic Commerce

Won-Gil Cho*

Abstract

This study introduced th e new technologies that are expanding the realm of electronic commerce to the Internet and small business. Each of the key components of electronic commerce(contracts, signatures, notaries, payment systems and adult trails)are supported in the new electronic commerce.

Electronic commerce is more than just handling purchase transactions and funds transfers over the internet. Despite Electronic commerce's past roots in transactions between large corporations, banks, and other financial institutions, the use of the internet as a way to bring Electronic commerce to the individual consumer has led to a shift in viewpoint. Over the past few years, both the press and the business community have increased their focus on Electronic commerce involving the consumer

Effective payment system should be established for the internet commerce. In this study, we examined the current development and application of Electronic payment system. Two different payment systems are used and under application. One is IC-card type of payment system which has gained popularity in England, Hong-Kong, and many other countries as a substitution of cash. The other type of payment system is e-cash, which is used more conveniently for the payment through internet. The question of which method is better fitted for the internet commerce should be evaluated in the view of cost and benefit since the associated technology is still under evolution. This study conducted a study on Secure Payment Method & Security Technology of Electronic Commerce

* Dept. of International Trade, Kang-Nam University.