□사례발표□

한국형 전자상거래 실험사업

이 선 형[1]

◈ 목 차 ◈

1. 서 론

전자상거래는 통신판매를 모태로 하여 PC통신을 통하거나, 케이블TV를 매개체로 하는 홈쇼핑으로 발전하였으며, 현재에는 인터넷의 브라우징 기술의 발전과 더불어 사이버 공간의 쇼핑몰을 통한 본격적인 전자상거래(EC)가 급속도로 확산되고 있다.

전자상거래는 크게 두 가지 유형으로 나눌 수 있으며, 첫번째는 기업과 소비자간의 상거래관계(Business to Customer)이고, 두번째는 기업과 기업간의 상거래(Business to Business)이다. 본 실험사업은 B-to-C를 근간으로 하여 B-to-B의 일부 요소를 포함하고 있다.

세계적으로 전자상거래에 대한 관심과 추진이 급진전되고, 국내에서도 많은 쇼핑몰이 출현하여 전자상거래 환경이 무르익어가고 있었던 97년 초에 커머스넷코리아(CommerceNet Korea)가 설립되어 본 프로젝트를 정보통신부로부터 지원 받아 다음과 같은 목적으로 수행하게 되었다.

첫째는 기존의 쇼핑몰들은 지불처리를 거의 수작업으로 처리하는 불편함이 있어 이를 전자적으로 자동 처리 할 수 있도록 지원함이고, 둘째는 오픈망인 인터넷에서의 상거래에 안전한 환경을 제공하여 소비자와 상점간의 신뢰를 높이므로서 전자상거래의 활성화에 기여하며, 셋째로 신규로 전자상거래에 진입 하고자 하는 중소 기업들 에게 테스트베드로서의 역할 및 인프라를 제공함으로서 사업하기에 쉽게 환경을 조성함 이였다.

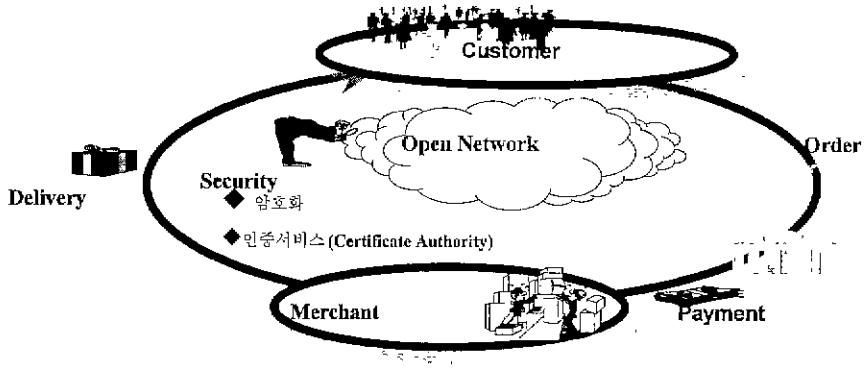
커머스넷코리아는 정보통신부에 소속된 사단법인으로서 국내의 많은 유수기업(데이콤, IBM, Oracle, LG-Soft, 대홍기획, 인터파크, 엔더슨컨설팅 등 25개)들이 참여하여 미국에 본부를 두고 전세계적인 연합 조직인 커머스넷과 공동 프로젝트를 추진중에 있으며, 일본과도 전자상거래 연계 서비스를위한 프로젝트(INGECEP)를 진행하고 있다.

2. 전자상거래 구성요소

전자상거래를 구성하려면 (그림 1)과 같이 여러 요소가 필요하며 상호간의 유기적인 관계를 조화 있게 구축해야 한다.

○ Customer : 전자상거래를 활성화하기 위해서는 물건을 구매하는 소비자가 필수적인 요소로서 시스템적으로 전자지갑(Wallet)이 필요하고 그에 따르는 보안처리가 요구된다.

† 정회원 : (주)데이콤 EC 인터넷사업본부 과장



(그림 1) 전자상거래 구성요소

○ Merchant : 물품을 사이버 공간에 전시하고 판매하는 주체로서 전자상거래를 이끌고 나가야 하는 요소이다. 시스템적으로는 쇼핑몰을 구축 하여야하고, 배송 관련한 EDI시스템 그리고, 대금결제를 위한 지불시스템과의 연계가 필요 된다.

○ Payment : 물품을 사고팔 때 기본적인 관계가 대금 지불 방법 으로서 Merchant와 금융기관 그리고 사용자간의 대금의 흐름을 관장하고 처리한다. 시스템적으로는 Payment Gateway가 있어서 Mechant와 금융사간에 안전하게 지불데이타를 전달해주고 처리결과를 Real-time으로 돌려준다.

○ Security : 전자상거래는 오픈 망에서 이루어지므로 보안이 무엇보다도 강조된다. 전자인증, 데이터암호화 그리고 전자서명 등 다양한 보안 방법들이 개발되어 적용되고 있으며, 전자상거래 전반에 걸친 보안 프로토콜로SET (Secure Electronic Transaction)이 발표되어 많은 파일롯 프로젝트가 추진되고 있는데 데이콤과 VISA 그리고 KT와 MASTER가 각기 파일롯을 추진하고있으며, 지방 자치 단체등에서도 SET을 적용한 프로젝트들이 속속 진행되고 있다.

SET프로토콜은 VISA, MASTER등 카드사업자들과 IBM, HP솔루션 프로바이더들이 공동으로 만든 안전한 전자상거래 프로토콜로서 소비자와 쇼핑몰 그리고 지불 시스템간의 상거래 흐름과 그에 부합하는 보안 메커니즘을 하나의 프로토콜로 정립하였다. 여기에 사용되는 IT기술로는 RSA, DES, X.509, ASN1등이 있다 물론 WEB관련 기술인 HTTP, TCP/IP, 등은 기본으로 한다.

○ Delivery : 전자상거래의 마지막 중요한 요소로 배송 부분이 있다. 현재의 많은 쇼핑몰에서 이 배송처리는 거의 수작업에 의한 택배사나 운송업체와 연계를 통해 업무를 처리하고있기 때문에 인력투입 비용이 과다하고, 처리 오류에 의한 문제점들이 상존하므로 배송시스템과 쇼핑몰 시스템간의 시스템 연계를 통한 일사 분란한 처리를 함으로서 소비자로부터의 신뢰도 얻고, 서비스의 효율성도 제고하는 효과를 얻을 수 있다.

3. SET과 한국의 전자상거래 환경

SET은 기본적으로 미국의 환경에 맞게 정의되어있기 때문에 한국의 실정하에서 적용하기에는 몇 가지 문제점이 있다. 이하에서 문제점 및 해결방안을 고찰해 본다.

문제점들의 일부는 한국 자체의 환경문제이기 때문에 그 체제를 개선함으로써 해결 해야 하고, 나머지 문제들은 SET 프로토콜에 요구사항을 반영 하도록 하여 해결하는 것이 바람직하다. 물론 SET은 VISA, MASTER, IBM, HP등 많은 국제 기업들이 만든 프로토콜로서 국제표준프로토콜화 되어가고 있기 때문에 당장 변경 할 수는 없고, 향후 SET 버전의 업그레이드시 우리의 환경에 부합하는 요구사항을 제시하여 반영토록 해야 한다.

가. 금융환경의 차이에 따른 문제점

1) 가맹점 체제의 차이

○ SET : 단일가맹점, 상점은 하나의 카드사와 가맹점 계약을 하면 나머지 카드사에 대한 처리를 그 가맹점에서 처리해줌.

○ 한국 : 복수가맹점, 상점은 취급하는 카드사마다 가맹점 계약을 맺어야 매입이 가능함.

○ 해결방안 : 국내 가맹점 체제를 통합 가맹점체제로 전환 : 지난 몇 년간에 걸쳐 거론되고 일부 진행되고있으나 계획대로 되지못하고 지연됨(99.4 예정).

2) 승인번호체계 차이

○ SET : 모든 카드사의 승인번호는 6자리로 고정되어 있음.

○ 한국 : 카드사 마다 승인번호 자리수가다름 (6자리 혹은 8자리).

○ 해결방안 :

1안) 지불시스템에서 변환 처리를 함.

2안) SET 프로토콜 변경

예) ub-approvalCode INTEGER := 6

ApprovalCode := VisibleString (SIZE(ub-approvalCode)를 아래와 같이 변경함.

ub-approvalCode INTEGER := 8

ApprovalCode := VisibleString (SIZE(1..ub-approvalCode)

3) 할부 개념차이

○ SET : 쇼핑몰에서 분할 처리함 즉, 사용자 Wallet으로부터 할부 요구를 받으면 쇼핑몰에서 분할하여 카드사로 승인 요청을 한다.

○ 한국 : 카드사에서 할부 처리함 즉, 사용자 Wallet에서 할부 요구를 하면 그 요구사항을 카드사로 전달하여 카드사가 할부처리를 한다.

○ 해결방안 : 쇼핑몰에서 사용자의 할부 요구사항에 대한 처리를 국가의 환경에 맞게 적용 해야 한다. 즉, 쇼핑몰 시스템 구축시 이를 반영 해야함.

예) 아래의 프로토콜에서 'instalRecurData'에트리뷰트에 값이 있으면 쇼핑몰에서는 분할처리를 하지말고, 지불시스템으로 보내 카드사에서 할부처리를 하도록 한다.

```
PIData ::= SEQUENCE
    piHead          PIHead,
    panData         PANData

PIHead ::= SEQUENCE
    transIDs        TransIDs,
    inputs          Inputs,
    merchantID      MerchantID,
    installRequrData [0] InstallRecurData OP,
                                        . . .
```

나. 암호화 정책에 따른 문제점

○ 국가안전기획부등 정부기관에서는 국산 암호화알고리즘을 전자상거래에 이용하도록 권고하고있고, 이를 위해 전자서명용 알고리즘과, 데이터 암호화용 알고리즘을 발표하려고 준비하고 있다. 그러나, SET 프로토콜에서는 보안에 필요한 알고리즘을 RSA와 DES로 고정하여 사용하게 정의되어 있다.

○ 해결방안 : SET Version 2.0에서 보안 알고리즘에 대해 복수로 지정 할 수 있도록 개

정하려고 하는 노력을 하고 있으므로, 한국에서 사용 하고자 하는 보안 알고리즘도 'SET Committee'에게서 인정을 득하여 SET 프로토콜에 반영토록 해야 한다.

예) 아래의 프로토콜에서 밑줄친 부분을 추가하면 가능하다. 물론 id-KRSec는 가칭이고, 그에 따른 Object Identifier는 ISO로 부터 득 해야 한다.

```
ContentEncryptionAlgorithms ALGORITHM-IDENTIFIER ::= {
 { CBC8Parameter IDENTIFIED By id-desCDMF } |
 { CBC8Parameter IDENTIFIED BY id-desCBC } |
 { CBC8Parameter IDENTIFIED BY id-KRSec }
}
```

다. 인증체계의 문제점

○ SET 관련 인증체계는 최상위에 Root CA 가 있고, 그 밑에 Brand CA가있으며, 그 아래에 MCA, CCA, PCA가 계층구조를 이루고 있다.

○ Root CA는 SET Committee(SETCo)가 운영하고, Brand CA는 VISA, MASTER등이 관장하고 있다.

○ 이러한 체계를 유지하면 국내의 카드사들은 독립적인 Brand로서의 위치를 얻기가 매우 어렵고, VISA나 MASTER등의 국제적인 카드 Brand에 종속되기 쉽다.

라. 사용자 환경의 문제점

○ 사용자들이 SET을 통한 전자상거래 행위에 불편함을 느낌에 따라서, 단순한 SSL정도의 보안처리를 선호한다.

○ 현재 CNK에서 실험서비스를 통해 얻어진 수치를 보면 95% 이상이 SSL을 이용하고 있다.

마. 법.제도적인 문제점

○ 인증기관 체계에 대한 법.제도적인 정비가 되어있지 않다.

○ 전자서명, 암호화에 대한 정책이 확정되어 있지 않다.

○ 현재, 전자서명법 및 전자상거래 기본법이 국회에 상정되어 있으나 SET Committee에 의한 제도 및 프로토콜에 적용하기에는 부적합한 요소가 있다.

예) SET에서의 Root CA는 SETCo에서 주관하는데 국내에서 별개로 Root CA를 두어 인증체계를 유지 하려함.

바. 쇼핑몰 환경에따른 문제점

○ SET을 이용하는 쇼핑몰은 카드사로부터 가맹점계약을 해야 하는데, 쇼핑몰 운영업체 대다수가 소규모이기때문에 카드사로부터 가맹점 계약을 못함.

사. 비용문제

○ SET 프로토콜을 구현한 프러덕트들은 SET Committee(SETCo)로부터 SET Mark를 획득해야 하는데 그 비용이 매우 많이 필요 하다. Wallet : $25,000, Merchant : $45,000, Payment GateWay : $55,000, Certificate Authority : $50,000

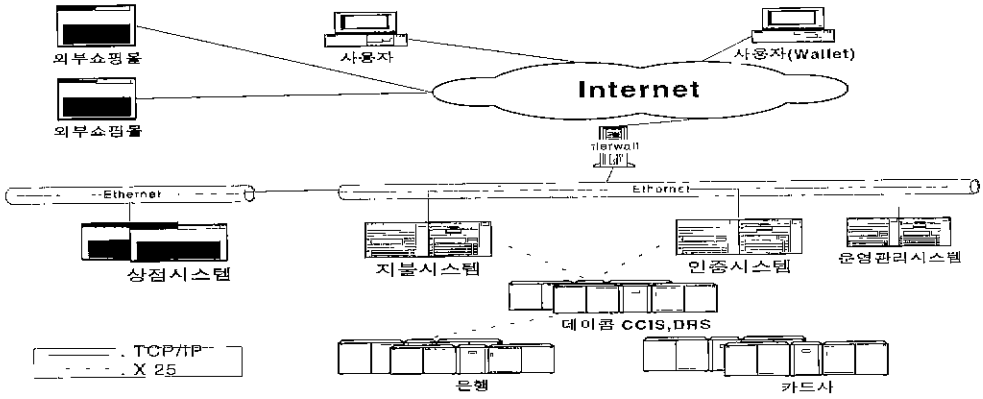
○ CA 의 계층구조를 유지하기위해서는 VISA, MASTER등의 Brand CA로부터 인증을 받기 위한 비용이 든다.

4. 시스템 구성 및 특성

한국형 전자상거래 시스템은 (그림 2)와 같이 전자상거래의 기본 요소를 모두 갖추고있으며, 3절에서 언급한 문제점들을 최대한 해결하고자 시스템을 구축하였다.

가. 사용자 시스템

편리성과 보안측면을 고려하여 Wallet을 통한 지불처리와 SSL을 통한 지불처리를 모두 수용하



(그림 2) 시스템 구성

였으며, 사이즈를 최소화하여 사용자로 하여금 쉽게 Wallet을 통한 안전한 상거래를 할 수 있도록 고려하였다.

Wallet은 개인키와 공개키의 쌍을 생성하여 공개키를 인증기관에 제출하고 인증서를 수령 하므로서 제 기능을 수행하게 된다. 그리고 모든 전문은 암호화되며, 전자서명을 하여 쇼핑몰로 전달하게 됨으로써 인터넷상에서의 해킹을 방지하며, 전문의 변조나 부인방지의 보안기능을 제공한다

나. 상점시스템

Mall & Mall개념으로 구성하여 소규모업체에서 중.대규모 업체까지 다양하게 유치 할 수 있으며, 상품검색엔진을 탑재하여, 타 쇼핑몰의 상품까지도 검색한 후 바로 Link할수 있도록 하였다

쇼핑몰은 물건을 진열하고 구매를 진행시키는 프론트 기능과 구매요청후 배송 및 정산 그리고 각종 운영관리 기능들인 백오피스 기능으로 구성된다.

사용자에게 제공하는 지불방법을 다양화 하여 Wallet에 의한 카드 지불과 계좌이체방법 그리고 SSl을 이용한 신용카드 방법을 지원하며, 지불시스템과 연계하여 안전하고 신속하게 처리하여 사용자로 하여금 신뢰감을 주도록 하였다.

다. 지불시스템

Wallet을 이용한 크레디트카드 지불 수단외에 SSL을 이용한 크레디트카드처리 및 계좌이체처리를 지원하며, 소규모 쇼핑몰들에게는 가맹점대행 서비스를 할 수 있도록 구축하였다

카드사 와 은행 연계는 데이콤의 기존서비스인 CCIS(Credit Card Information System)과 DRS(Dacom Realtime System)을 통하여 전용선으로 구축하였으며, 프로토콜은 X.25위에 금융권의 통신프로토콜을 적용하였다.

현재 국내 5대카드사(국민, 외환, BC, 삼성, LG)를 포함하여 VISA, MASTER, AMEX등의 외국계 카드사를 연계하여 서비스 중에 있으며, 또한 조흥,상업은행등 10개의 은행과 연계되어있다.

라. 인증시스템

SET Committee의 조건에 따르는 인증체계를 갖는 동시에 국내여건을 반영한 인증체계를 수용할 수 있도록 복수의 루트를 수용하는 시스템으로 구축하였으며, 또한 SSL용 인증서도 발급 할 수 있는 체제로 되어있어 향후 B-to-B용 인증서 발급에 적용할 계획이다.

카드사와는 전용선으로 연계하여 리얼타임으로 인증서를 발급 할 수 있도록 하였으며, 인증서는

X.509 표준을 따른다.

키 생성의 신속성과 키 관리의 안전성을 고려하여 크립토(Crypto) 디바이스를 채용하였으며, 보안 알고리즘은 DES 56비트, RSA 1024비트를 채택했다.

5. 시범 서비스 현황 및 전망

한국형 전자상거래 시스템은 올 6월22일에 시범서비스를 개시하여 현재 6개월여를 진행하고 있으며, 지불시스템에 연계되어 서비스를 받고있는 쇼핑몰이 70여개에 이르고 있다. 물론 상품의 거래에 따른 트레픽의 증가도 매월 100%이상을 이루고 있다.

전자지불서비스를 이용하는 쇼핑몰들을 분류하면 크게 세가지 부류가 있는데 첫째가 일반적인 물품을 판매 하는것 이고, 둘째는 신용정보나 부동산 정보등을 제공하는 서비스이고 셋째는 예약 대행 등 서비스를 팔고 그 댓가를 지불받는 부류이다. 초기의 쇼핑몰들은 첫번째의 부류가 많았으나 점차 두세번째의 쇼핑몰들이 그 숫자나 트래픽면에서 큰 증가세를 보이고있다.

현재 국내의 전자상거래용 지불 방법은 신용카드에 국한되어있으나 신용카드에의한 지불방법은 수수료가 너무 크기 때문에 소액결제에 대한 대응방안으로서 계좌이체나 전자화폐에 대한 요구가 점차 증대되고 있다.

요즈음 메스컴을 통해 전자상거래의 중요성 및 활성화에 대한 전망 등이 비교적 흐전되고 있으나 아직까지는 쇼핑몰을 통한 이익을 추구하기에는 이르다고 본다. 따라서, 각 기업에서는 단순한 기업과 일반소비자간의 상거래를 탈피하여 기업과 기업간의 상거래로의 확장을 꾀하고 있으며, 기존의 EDI나 물류망 등을 연계한 종합적인 상거래 시스템을 구축하고 있다. 일반기업 뿐만 아니라 우체국 등 정부부처 그리고 지방 자치단체 등에서도 전자상거래의 시스템들을 속속 구축하고 있으며 그에 따른 시너지 효과가 99년에는 분명히 나타날 것이다.

6. 결 론

전자상거래는 앞에서도 언급 했듯이 여러 요소가 함께 구성되어 있기에 이를 수행하기 위해서는 많은 기관 및 기업이 긴밀히 협조체제를 유지하며 발전시켜야 하는데 근간에 국내 현실은 조금은 중복적인 투자와 과당 경쟁으로 인한 파벌이 나뉘어 상호간에 협조가 원활하지 못하고 있어 앞으로의 전자상거래 발전에 저해요소가 되고 있다.

CNK에서는 일본과의 전자상거래 연계 프로젝트를 추진코자 정부의 자금 지원을 받아 일본의 INGECEP 추진 조직인 ECOM과 합의서를 교환하고 상호 방문 및 기술 협의를 진행 중에 있다. 이는 한국의 전자상거래가 국제적인 무대로 진출하는데 밑거름이 될 것이다.

참고문헌

[1] SET Specification Book1 : Business Description Version 1.0 May 31, 1997

[2] SET Specification Book2 : Programmers Guide Version 1.0 May 31, 1997

[3] SET Specification Book3 : Formal Protocol Definition Version 1.0 May 31, 1997

이 선 형

1985년 중앙대학교 전자계산학 (학사)
1987년 중앙대학교 전자계산학 (석사)
1989년-현재 ㈜데이콤 과장
관심분야 : MHS, EDI, EC