# 전자 상거래에 있어서 전자식 대금결제 시스템 설계*

권영직** · 조현준***

초 록

본 논문은 전자 상거래 시스템 구현을 위하여 우선 네트워크 구성에 있어서 물리적 시스템, 인증기관, 전자상점 시스템, 전자지불 시스템, 전자 인증서, 발급체계, 전자 상거래 동작체계를 중심으로 설계하여 두었다. 그리고 보안 시스템 설계, 대금결제 시스템 설계, 전자지불 시스템 설계, 전자화폐 설계에 대해서도 제시하여 두었다.

## I. 서 론

전자 상거래의 개념에 대해서는 아직 뚜렷하게 정의내린 것이 없지만, 일반적으로 전자 상거래란 "다양한 형태의 전자적인 매체를 이용하여 상품 및 서비스의 거래에 필요한 정보를 교환하고 거래하는 것"을 말하는 것으로 상행위 이외에도 계약, 건설, 은행업무, 엔지니어링, 운송 등과 관련된 일체의 거래행위를 포괄적으로 의미한다.

전자 상거래의 중요성을 감안할 때 특히 대금 결제를 원할하게 할 수 있는 설계 기법의 개발이 절실하다 하겠다. 따라서 전자 상거래에 있어서 전자식 대금결제 시스템 설계를 위해서는 여러가지 있겠지만 본 논문에서는 네트워크 설계, 보안 시스템 설계, 대금결제 시스템 설계, 전자 화폐 설계로 설정하였으며 연구방법으로는 문헌연구와 구현을 위한 설계에 중점을 두었다.

## II. 이론적 고찰

### 1. 전자 상거래의 개요

일본 통상성에서는 Electronic Commerce를 그대로 전자 상거래로 해석하고 특별한 예고를 하지 않는한 일부 또는 전체 거래를 전자적으로 행하는 모든 것을 총칭해서 이 단어를 사용하고 있다.

전자 상거래(Electronic Commerce ; EC)의 기원은 미국의 Lawrence Livermore National Laboratory가 미국방부의 프로젝트를 수행하면서 처음으로 사용한 용어인데, 거래가 시작되면서부터 끝날 때까지 서류가 사용되지 않는 거래업무를 정보 기술

* 이 논문은 1997학년도 대구대학교 학술연구비 지원(일부지원)에 의한 논문임

** 대구대학교 컴퓨터정보공학부 교수
*** 대구대학교 컴퓨터정보공학과 대학원 박사과정

에 의해 달성하려는데 그 목적이 있었다.

김중한 외 3인(1997)에 의하면 전자 상거래에 대한 프레임 웍을 제시하고 있다. 이에는 첫째 보안/인증, 전자지불 등의 비지니스 서비스 기반구조, 둘째 EDI, E-mail, HTTP, FTP 등의 정보전달 기반구조, 셋째 공중망, 케이블 TV, 무선통신, 인터넷 등의 정보통신 기술 기반구조 그리고 이를 지원하는 정책및 법률, 개인 정보 보호와 같은 사회적 기반이 있다고 제시하였다.

## 2. 전자 상거래의 유형

전자 상거래의 분류 방법은 몇가지 되지만, 우선 거래 당사자와 네트워크의 형태를 중심으로 편의상 세 가지로 나누어 생각하고 있다.

그 첫 번째는 기업과 소비자간의 네트워크, 두 번째는 기업간의 불특정 다수 네트워크, 세 번째는 기업간의 특정 네트워크의 세 종류이다.

이들에 대해 아래에 좀더 구체적으로 고찰하여 두었다.

### (1) 기업과 소비자간 네트워크

① 가상 점포(Virtual Mall)

기업과 소비자간 전자 상거래의 전형적인 예는 전자 점포(이는 가상점포, 사이버 몰, 일렉트로닉스 숍 등으로 불리기도 한다.)를 개설하여 소비자들에게 상품 판매를 하거나 항공권, 철도, 호텔의 예약 서비스를 행하면서 동시에 결제도 행하는 소위 온라인 쇼핑이다.

② KIOSK 단말

소비자를 대상으로 하는 전자 거래에서는 네트워크의 전자 점포에서 소비자가 PC를 통해서 물건을 사는 것이 전형적인 예이지만 현실적으로 점포와의 연속성을 갖는 것도 생각할 수 있다. 대표적인 예가 KIOSK 단말이다. 예를들면 기차역의 KIOSK나 24시간 영업 점포에 단말을 두어 전자 판매를 하는 것 등이다.

③ 전자 통화

전자통화는 다양한 정의를 갖고 있다. 가장 넓은 의미에서 본다면, 지금 행하여지고 있는 대체 계좌에 불입하는 데이터도 하나의 전자통화가 된다. 또 궁극적인 전자통화로서 어느 나라의 통화도 아닌 네트워크 상에서만 유통되는 통화도 이야기되고 있다. 그러나, 지금 우선 이 분야에서 주목받고 있는 전자통화 방식은 IC 카드에 은행 계좌로부터 현금을 전자 데이터 형태로 옮겨서 현실 점포나 전자 점포 양쪽 모두의 결제에 사용되는 카드를 말한다.

### (2) 기업간의 불특정 다수 네트워크

편의상 기업과 소비자간 네트워크와 기업간 불특정 다수 네트워크를 나누어서 정리하고 있지만 사실은 본질적인 차이가 있는 것은 아니다. 전자점포에 의한 온라인 쇼핑 경우에도 소비자가 전자점포에 액세스하여 이 상품이 마음에 들면 전자점포에서 해당 제품을 제조 판매하고 있는 기업에 발주 데이터를 보낸다. 또 전자점포에서 결제를 위

해 신용회사에 신용조회를 해서 결제 데이터가 보내지기 때문에 전자점포 뒷편에서의 정보 흐름은 기업간 거래 그자체가 된다.

(3) 기업간의 특정 네트워크

기업간의 상거래는 통신망을 이용해 자사와 상대기업 간의 상거래에 필요한 정보를 전자적으로 주고받는 기존의 EDI(전자문서교환)나 최근들어 구축 움직임이 활발한 CALS(광속상거래)가 대표적이다.

종래 EDI와의 차이를 개념적으로 정리하면 EDI는 "정보의 교환"을 목적으로 하는 것에 반해 CALS는 "정보의 공유"를 목적으로 한다.

CALS는 예를들면 자동차, 항공기, 플랜트 엔지니어링, 전자부품등 고도의 기술집약형 산업에 있어서 다수기업에 의한 공동개발이라는 업무 처리의 합리화에 위력을 발휘한다.

### 3. 전자 상거래 구성요소

전자시장에서의 전자상거래 구성요소는 소비자가 PC상에서 정보를 검색할 수 있는 정보 검색 소프트웨어, 전자상거래를 하기 위한 서버, 서버상의 전자 카탈로그, 전자상점의 상품 광고 소프트웨어, 수주 및 지불 처리 소프트웨어, 수주 및 지불에 관계되는 서버의 여신시스템, 결제시스템, 상품배송시스템 등으로 구성된다.

## III. 전자식 대금 결제 시스템

### 1. 전자식 대금 결제 시스템의 개요

소비자가 온라인으로 화폐를 사용할 수 있는 체제가 바로 전자식 대금 결제 시스템이다. 전자식 조회 시스템, 제3자에 의한 결제 시스템 또는 전자식 통화 시스템등이 바로 이런 전자식 결제 시스템으로서, 개인간의 가치(금액) 교환을 제공하는 수단들이다.

### 2. 퍼스트 버츄얼 인터넷 대금 결제 시스템

퍼스트 버츄얼이 만든 대금 결제 시스템은 IPS(Internet Payment Systems)로 인터넷을 통해 상품이나 서비스를 판매하는것보다는 주로 정보 판매만을 추구하는 시스템이다. 자동화된 전화시스템을 이용해서 관련자의 대금 결제 정보를 수집하기 때문에 암호 방법(암호화나 디지털 서명)보다는 판매와 구매 감시 밀도를 높혀 사기 사례를 감소시키는 장점이 있다. 퍼스트 버츄얼 시스템의 특징을 살펴보면 <표 1>과 같다.

### 3. 사이버 캐시

사이버 캐시를 이용하려는 고객은 클라이언트 소프트웨어를 다운 로드(down load)하고 적어도 하나의 신용 카드를 서비스에 연계시켜서 사이버 캐시 ID를 초기화 한다.

<표 1> 퍼스트 버츄얼 시스템의 특징

| 항 목 | 세 부 내 용 |
|---|---|
| 시스템의 구성 메카니즘 | 인터넷 신용카드 지불 시스템 |
| 주요 특징 | 전자지불 처리과정 동안 사용자의 신용카드 정보가 유출되지 않음 |
| 익명성에 대한 보장 | 익명성 보장않됨 |
| 부가적인 하드웨어 | 필요없슴 |
| 부가적인 소프트웨어 | 필요없슴 |
| 기타 요구사항 | VISA 또는 Master 카드사의 신용카드 거래자여야 함 |
| 제한사항 | 없슴 |
| 암호화 방식 | VirtualPIN |

이와 같은 서비스 요금은 소비자에게 부과되지 않는다. 사이버 캐시 클라이언트 소프트웨어는 또한 브라우저(browser) 소프트웨어와도 함께 쓰일 수 있다.

사이버 캐시가 제공하는 디지털 대금 결제 매카니즘에서는 특수한 클라이언트/서버 소프트웨어를 통해 구현된 공용/개인 키 암호화와 디지털 서명들을 비롯 현대인 암호기술들을 이용한다.

사이버 캐시가 소비자에게 제공하는 현실적인 가치들은 다음과 같다.

- 대금 결제 정보의 누출 방지(판매 회사에게 조차 누설하지 않음)
- 편리한 전자식 지갑을 제공해서 대금 결제 정보를 저장하므로 구매가 이루어질 때마다 정보를 재입력하지 않아도 가능
- 모든 거래를 처리, 추적, 다큐먼트화하는 거래 로그(log) 유지 관리등이다.

## 4. 보안 시스템

인터넷이 보안에 취약한 이유는 인터넷에서 사용되는 오픈 환경을 지원하는 통신 프로토콜인 TCP/IP와 유닉스(UNIX)를 운영체제로 사용하기 때문이다. 인터넷에서 사용되는 표준통신 프로토콜인 TCP/IP는 공개되어 있어 인터넷과 연결된 다른 컴퓨터에 접속하는 것이 가능하다.

특히 인터넷상에서 전자상거래가 보편화되면 신용카드 번호, 비밀번호등 대금결제를 위한 중요한 개인정보가 네트워크에 노출될 수 밖에 없으므로 안전한 각종 보안대책을 마련해야 한다.

(1) 보안사고의 유형

① 정보유출

② 위장

③ 변조

④ 시스템 침입

(2) 암호방식

현대의 암호방식은 크게 두 가지로 구분된다. 하나는 네트워크상에서 송신자가 특정 키로 암호화해 정보를 보내면 수신자가

이를 암호화에 사용된 동일키를 이용해 복호화하는 공통키 암호방식이다.

공통키 방식으로는 DES(Data Encryption Standard), IDEA(International Data Encryption Algorithm), RC2, RC4 등이 있다.

이 암호방식의 문제점은 암호해독을 위한 비밀키를 메시지 수신자에게 안전하게 전달하기가 어렵다는 것이다.

그래서 새롭게 등장한 것이 공개키 암호방식이다. 수신자와 송신자가 암호화를 할 때 필요로 한는 두 개의 키중 한쪽의 키를 불특정 다수의 사람이 입수해서 암호화 또는 복호화할 수 있도록 공개하는 방식이다. 대표적인 공개키 방식은 RSA 방식이 있다.

현재 대부분의 보안규약에서는 데이터를 암호화해서 전송하기 위한 이 두가지 방식을 적절히 결합시켜 사용하고 있다. 즉 전자서명이나 비밀키 암호방식에서 사용할 비밀키를 전달하는데에는 안전성이 뛰어난 공개키 암호방식을 사용하고 대량의 메시지 전체를 암호화하는 데에는 처리속도가 훨씬 빠른 공통키 암호방식을 병행해서 사용한다.

(3) 전자서명

거래 당사자의 본인 확인을 위해서는 일반 상거래의 인감과 같은 기능이 필요한데 이를 암호기술을 응용한 전자서명이 대신하고 있다.

전자서명의 일종으로서 전자화폐인 E캐시 시스템을 운용하고 있는 디지캐시(digicash)사가 고안한 블라인드(blind) 전자서명이 있다.

이 방식은 일반적인 문서형식과 비교하면, 봉투내에 비밀문서를 넣어 봉인하고 서명자에게는 이 문서의 내용을 보여주지 않고 봉투에 문서의 정확성을 증명하는 서명을 하도록 하는것이다.

(4) 인증

인증은 송신자의 메시지가 전송도중에 위

<표 2> 전자화폐의 분류

| 구 분 | | 화폐명 | 발행기관 | 주요특징 |
|---|---|---|---|---|
| IC 카드형 | 현금형 | 몬덱스 | 내셔널 웨스트민스터, 미들랜드은행 등의 공동출자회사 | 전용기기(Wallet) 또는 몬덱스용 전화기를 이용하여 카드간 가치이전 가능. 1995년 7월 이후 실험사용 중 |
| | 선불 카드형 | 비자 캐시카드 | 다수의 미국 지방은행 | 96년 ATM, 전화기 등을 통해 가치재충전이 가능한 카드를 발행 |
| 네트워크형 | 현금형 | E캐시 | 네덜란드의 디지캐시사와 미국의 마크 크웨인은행 | 네트워크상에 가상의 화폐를 생성시켜 이것을 전자결제에 이용. 1995년 부터 실용화됨. |
| | 신용 카드형 | 퍼스트 버츄얼 | 미국의 퍼스트 버츄얼사 | 일종의 회원등록처럼 신용카드 번호를 사전에 등록하고 전용의 회원번호에 따라 인터넷상에서 결제함. |
| | | 사이버캐시 | 미국의 사이버캐시사 | 무상으로 제공된 암호통신 소프트웨어를 이용해 인터넷상에서 결제함 |
| | 전자 수표형 | 네트빌 | 미국의 카네기멜론 대학 | 인터넷상에서 기존의 가계당좌수표 사용을 가능하게 함. |

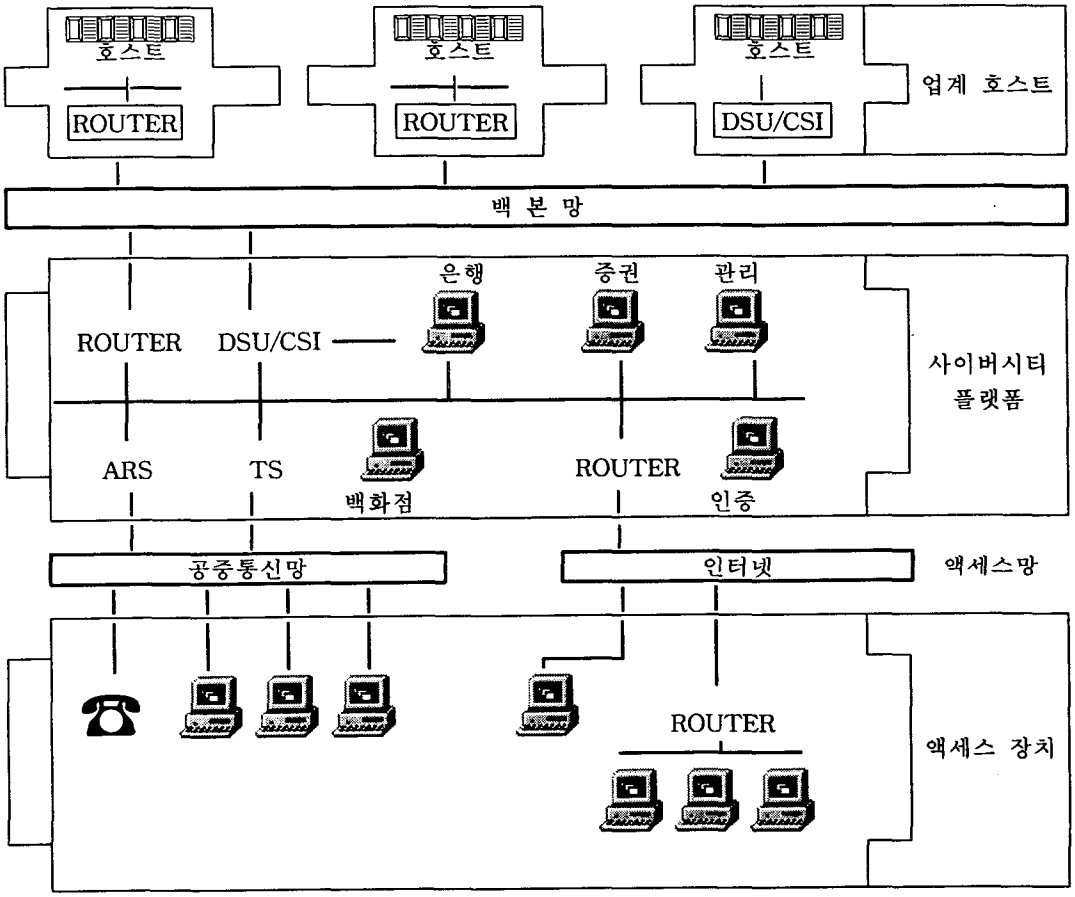
조·변조되지 않고 원문과 다름없음을 확인하는 메시지 인증 기능과 메시지를 보낸 사람이 정당한 수신자임을 확인하는 사용자 인증 기능으로 구분된다. 또한 메시지를 받은 사람이 메시지 수신 사실을 부인하는 것을 방지하는 수신자 부인방지 기능도 인증 기능 이다.

5. 전자 화폐

전자화폐는 일반적으로 전자현금, 전자지갑, 디지털 머니등 다양한 용어로 사용되고 있다. 따라서 몇가지 분류기준으로 현재 실험 및 실용화되고 있는 각종 전자화폐를 분류하고, 각 유형의 성격 및 특징에 대해 다음 <표 2>에 요약 정리하여 두었다.

## Ⅳ. 전자 상거래에 있어서 전자식 대금 결제 시스템 설계

1. 네트워크 설계




<그림 1> 물리적 시스템 구성

(1) 물리적 시스템 구성

앞에서 고찰한 이론적 근거를 토대로 전자 상거래에 있어서 전자식 대금 결제 시스템을 설계하기 위한 네트워크 설계 부분은 물리적 시스템 구성과 인증기관, 전자상점, 전자지불, 전자 인증서 발급 체계, 전자 상거래 동작 체계를 중심으로 <그림 1>에서 <그림 6>까지 설계해 두었다.

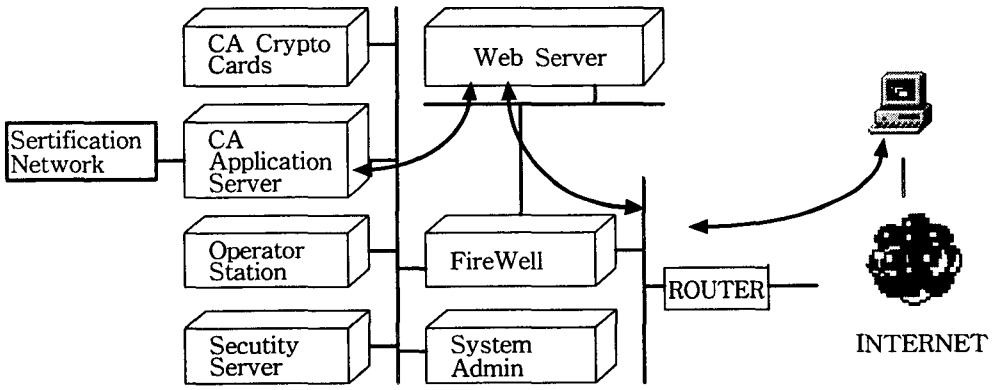
<그림 1>에서 액세스 장치로는 PC, LAN station, 전화이며, 액세스 및 백본망은 공중통신망및 인터넷을 이용한다. 업계 호스트는 정보 source를 제공하며, 전자 상거래 플랫폼은 중앙집중형 온라인 방식으로 요소시스템 및 네트워킹 장치으로 구성되어 있으며 세부적인 내용은 다음과 같다.

· web Server : CA(Cirtificate Authority) applications server의 frontend
· CA application server : 온라인 certificate 발급
· CA crypto card : 암호화 key의 생성, 저장, 삭제 및 암호화
· operator station : 데이터 입력, 수정, 변경, 삭제 등을 위한 운용자 시스템
· security server : 액세스 제어 및 방화벽 제어 서버, 시스템 로그 데이터 수집
· system administration : 시스템 관리의 모니터
· firewall : 외부의 침입 및 불법적인 액세스 차단을 위한 액세스 제어로 구성된다.

(2) 인증기관 시스템 구성

<그림 2>의 세부내용은 다음과 같다.

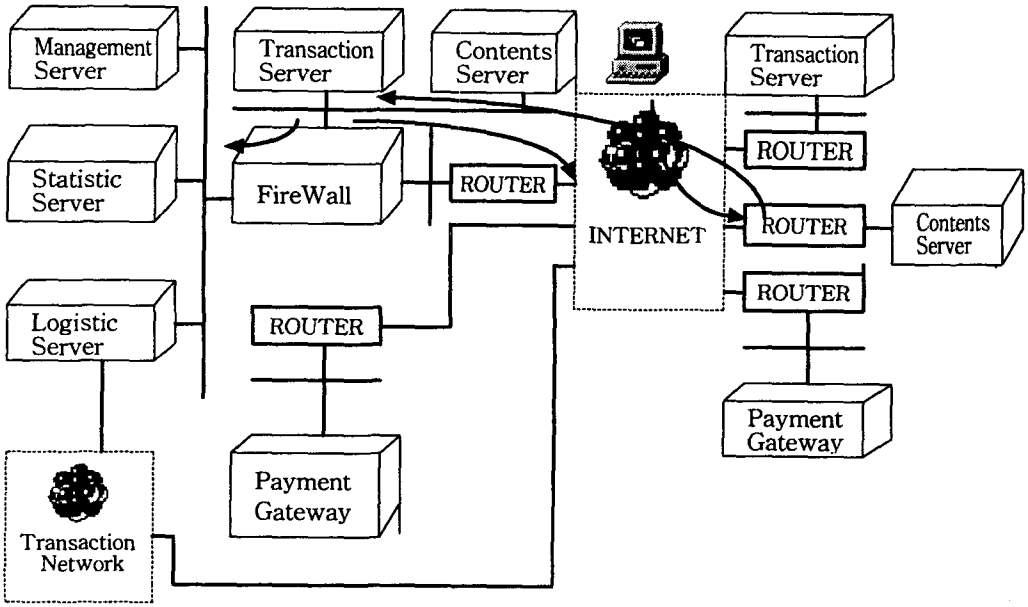
· 인증기관 시스템 : 전자증명서 발급
· 가상백화점 시스템 : catalog, transaction, 택배, 관리, 통계 서비스 제공
· 지불 시스템 : 신용카드, 직불카드, 계좌이체, 전자화폐등 용도별 지불 서비스
· 고객 시스템 : web browser 기반의 전자지갑 (지불 수단별 전자지갑 장착)




<그림 2> 인증기관 시스템

(3) 전자상점 시스템 구성

<그림 3>의 세부내용은 다음과 같다.



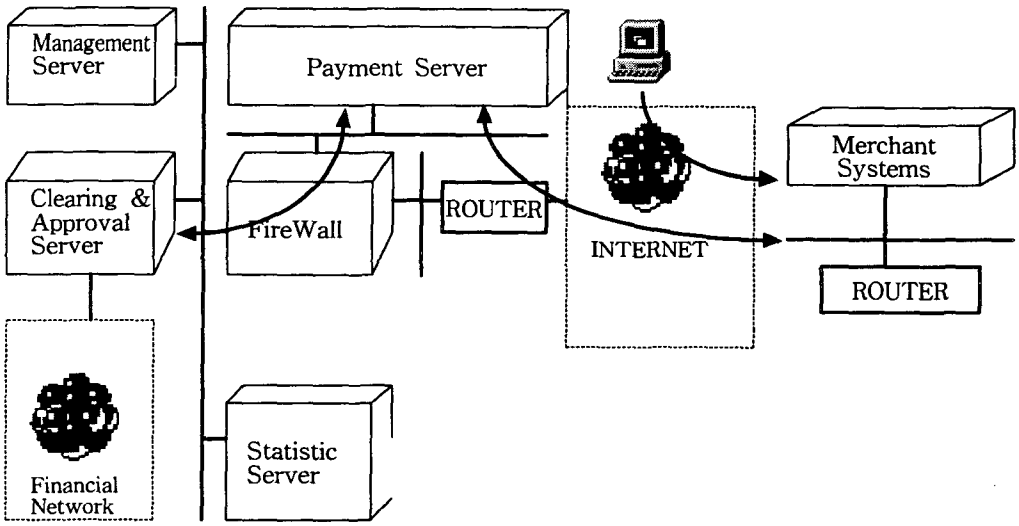

<그림 3> 전자상점 시스템 구성

· contents server : 유통사업자의 shopping mall 및 catalog 서비스

· transaction server : payment system과의 지불처리 및 각종 지불수단 제공

· management server : 거래에 따른 각종 로그정보 및 시스템 관리, 영수증 발급 및 관리

· statistic server : 로그정보 가공을 통한




<그림 4> 전자지불 시스템 구성

통계치 가공정보 제공

· logistic server : 거래에 따른 택배지령 및 추적등

(4) 전자지불 시스템 구성

<그림 4>의 세부내용은 다음과 같다.

· payment server : 지불정보(payment information)처리, 거래 token 생성 및 전송

· clearing & approval server : 거래 승인 처리, 지불 token 매입 및 정산처리

· Management Server : 거래에 따른 각종 로그정보 및 시스템 관리

· Staistic Server : 로그정보 가공을 통한 통계치 가공정보 제공

(5) 전자 인증서 발급체계

<그림 5>의 세부내용은 다음과 같다.

· 인증기관 시스템 (certificate authority) : 전자 증명서 발급

· 지불 시스템 (payment systems) : 신용카드, 직불카드, 계좌이체, 전자화폐등 용도별 지불 서비스

<그림 6>의 세부내용은 다음과 같다.

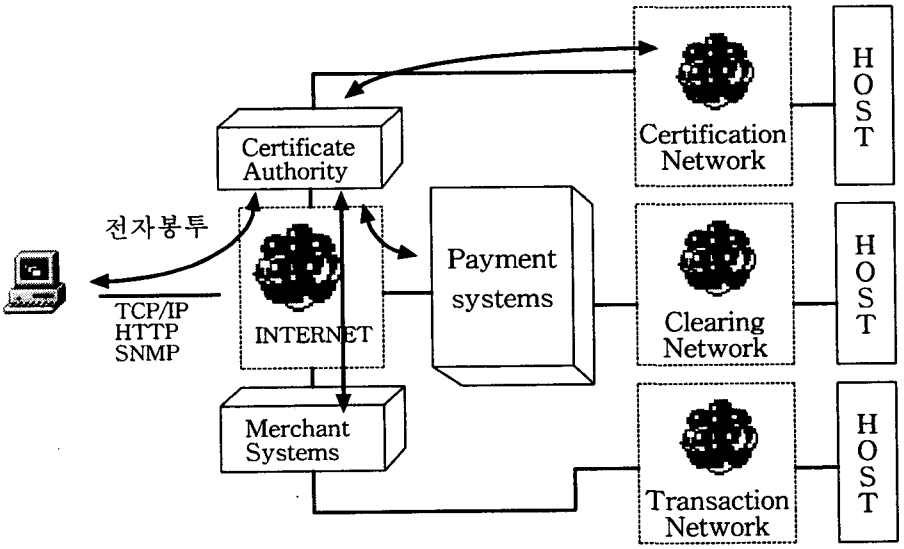
· 인증기관 시스템 (certificate authority) : 전자 증명서 발급

· 지불 시스템 (payment systems) : 신용카드, 직불카드, 계좌이체, 전자화폐등 용도별 지불 서비스

## 2. 보안 시스템 설계

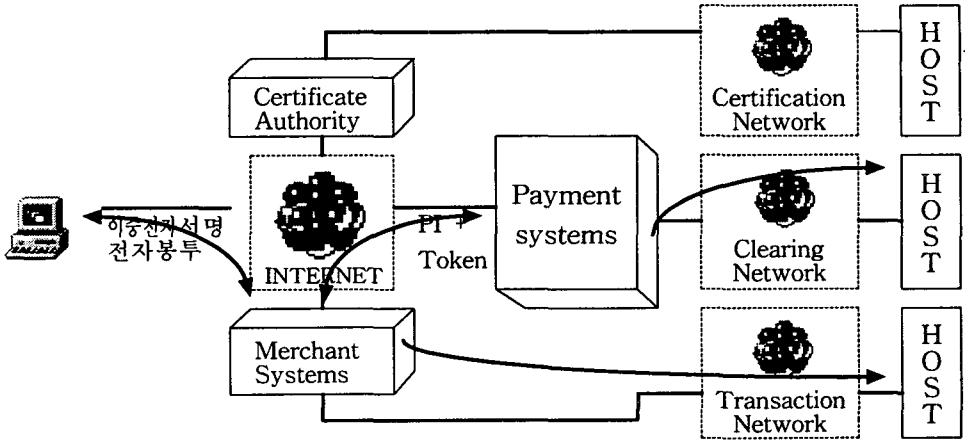
보안 시스템 설계를 위하여 기존의 사례 연구를 실시하였는 바, 몬덱스 카드의 보안 대책은 안전한 전자화폐 시스템을 구현하기 위해 공개키와 비밀키를 같이 사용한다.

디지캐시사의 보안대책은 E캐시에 익명




<그림 5> 전자 인증서 발급체계

(6) 전자상거래 동작체계 : 온라인 지불 시스템 방식




<그림 6> 전자상거래 동작체계

성을 보장하기 위해서는 은행이 일련번호 자체를 몰라도 사용자가 발행한 화폐임을 인증할 수 있는 기능을 가지고 있으며, 이러한 전자화폐에 사용되는 일련번호는 이용자가 부여하는데, 익명성을 보장하기 위해 일련번호에 블라인드 팩터(blind factor)라는 임의의 숫자를 부가해 암호화 한다.

퍼스트 버츄얼의 보안대책은 별도의 전자상거래용 보안 소프트웨어를 사용하지 않고, 신용 카드 번호등 중요한 정보는 인터넷이 아닌 전화나 팩스등 일반 통신기기를 이용해 오프라인으로 보내게 한다.

사이버 캐시의 보안대책은 암호화와 전자서명 기능을 사용해 데이터 보호를 행하기 때문에 RSA 공개키와 DES 공통키 암호 시스템을 같이 사용하고 있다.

비자와 마스터카드의 보안대책 인터넷상에서 신용 카드를 이용한 대금 결제를 안전하게 수행하기 위해 활용되고 있는 암호기술로서는 SET(Secure Electronic Transaction)을 개발하여 암호기술을 통일했다.

세계 최초의 가상은행인 SFNB(Security First Network Bank)는 보안에 가장 큰 비중을 두고 미국방성의 정부보안기관에서 사용하던 보안기술을 도입하여 완벽한 보안체제를 갖추고 있다.

위의 내용을 기반으로 하여 전자 상거래에서 전자지불 시스템상에서의 보안처리 방법에 대해 제안하면 다음과 같다.

현재 인터넷 상에서 사용되는 지불방식은 text형태로 신용카드번호를 전달하는 방식이나 SSL 이나 S-HTTP를 이용한 전달방식, 사용자를 가입시킨후 지불하게 하는 방법등이 있다. 그러나 이러한 세 가지 방법 모두 신용카드번호의 유출이라는 경우 사용자의 불편을 초래할 수 있기 때문에 앞으로 확장될 방법은 아니다. 이러한 현실을 바탕으로 하여 네트워크상에서 흐르게 되는 정

보를 암호화해서 보내게 되는 암호화방법을 고려해야 한다.

암호화 방법에는 우선 대칭형을 제안할 수 있는데, 이것은 암호화와 복호화가 빠르다는 장점과 다양한 암호화 방법이 개발되어 있다는 장점이 있지만 복수의 사용자가 같은 자료를 사용할 때에는 키공유에 어려움이 있다.

비대칭형 암호화 방식은 네트워크상에서 정보를 주고받을 때 키에 대한 보호가 이루어지지 않는다는 대칭형의 단점 때문에 개발 되었다. 이 방식으로는 많은 방법들이 제안되고 있다. 또 완벽한 암호화가 이루어져서 기밀성을 지킬 수 있다고 할지라도 메시지에 대한 발신인의 보증은 불가능하게 된다.

여기에 기인하여 메시지 인증과 디지털 서명에 대해 제안을 한다. 인증 방법으로는 공개키 방법에 의한 메시지 암호화와 oneway hash 방식을 사용하는 방식등이 있다. 디지털 서명은 송신자의 확인, 수신자 보증 등의 기능이 포함되어 지는데 대부분 공개키 암호화방식을 이용한다.

WWW 시스템 자체의 보안도 제안하는데, 여기에는 IP address authentication, basic authentication, message digest authentication 등의 서버설치를 통해 firewell이나 기타 논리, 물리적인 보안을 구현하기 위한것이다.

프로토콜을 기반으로 한 보안 시스템을 제안하면 S-HTTP, SSL, SEA, PGP, Shen, GSSAPI integratio등이 있다. 그러나 이러한 프로토콜 기반의 보안시스템의 경우에는 근본적으로 WWW 브라우저와 WWW 서버간의 관계를 기반으로 설계되었고 보안이 구현되었기 때문에 일반적인 전자지불 시스템의 구조인 고객과 상점 그리고 브로크를 잇는 3자구조를 가지고 있기 때문에 더욱 많은 보안기능들을 요구하게 된다.

사용자에 대한 프라이버시에 대한 보증과 지불 부인에 대한 방지기능, 또 상점 측에서 가지게될 고객정보의 보호, 또 사용자들의 이용에 불편함이 없게 하는 인터페이스의 통일까지 많은 부분이 추가 되어야만 한다.

또 소액거래의 경우 거래를 통해 발생되는 이익이 거래자체에 소요되는 비용보다 작게 되는 경우에는 거래자체가 일어날 수 없으므로 지불 시스템에 대한 비용의 절감도 중요한 요소가 된다.

## 3. 대금 결제 시스템 설계

대금 결제 시스템 설계를 위하여 기존의 사례연구를 실시하였는바, 현재의 소비자들이 상품과 서비스 대금을 결제하는 방법은 현금, 수표, 신용 카드 등을 이용하는 것이다.

위의 내용을 기반으로 하여 전자 상거래에 있어서 대금 결제 시스템을 아래에 설계하여 두었다.

현금을 디지털화하는 과정에서 해결해야 할 많은 문제들이 있다. 이 과정에서는 실제 화폐를 디지털 '코인'으로 대체시킨다. 디지털 코인은 데이터 청크(chunk)들로 재현된다. 가장 확실한 방법은 중앙은행이 관

리하는 테두리 내에서 디지털 서명과 공용키 암호화를 이용하는 시스템이다.

온라인 상거래 환경은 단순한 결제정보 전송 이상의 것이어야 한다. 그렇지만 온라인 상거래 환경의 토대는 바로 그 대금 결제 정보의 전송과 데이터 전송의 보안 유지이다.

대금 결제 정보는 실질적인 전송 보안 유지를 요하는 유일한 거래 부분이지만 선적, 지시, 제시 가격, 디지털 서명을 통한 기타 주문 정보와 같은 정보를 보증하는 방법들을 제공하는 시스템들이 있다. 그러나 보안 유지는 주문 정보를 암호화하는 것을 넘어, 소비자 신용 카드 정보를 받을 수 있는 권한을 부여받은 판매 회사로 가장한 범죄자들을 격리시킬 수 있어야 한다. 더욱 중요한 것은 신용 정보를 저장하고 있는 판매 회사의 서버 시스템의 보안 유지이다.

직불 카드를 신용 카드와 거의 흡사하게 이용할 수 있는 것처럼, 디지털 조회 방식도 그와 같은 테크닉들을 이용할 수 있다. 즉 소비자들이 카드를 판매 회사에게 제시하면 그 판매 회사는 구매에 대한 승인을 받아야 한다. 대금 결제 방식은 월말에 청구서를 발행하는 것이 아니고 구매 승인이 떨어지는 즉시 고객의 계좌에서 인출되도록 한다.

실제 디지털 통화를 이용하는 방식은 대금 결제 시스템 이용 방식과는 상반된다. 디지털 통화 서비스를 제공하는 금융 기관에 계좌를 개설하면 누구든지 디지털 통화를 이용할 수 있게끔 한다.

관계자의 컴퓨터 상에서 클라이언트 소프트웨어를 이용해서 계좌에서 돈을 인출하고, 잔액을 조회하고, 액면 금액이 입금되는 '디지털 지갑'을 유지 관리할 수 있도록 한다.

사용자와 은행간의 현금 교환에는 암호 기술을 이용한다. 디지털 서명으로 현금 양도를 보증하고 거래를 암호화 시킬 수 있도록 한다. 현금이 은행에서 사용자에게 배포될 때는 '디지털 코인' 형식으로 이루어져야 되며, 디지털 코인은 디지털 서명을 받은 일련 번호로서 은행에 등록되게끔 한다.

## 4. 전자지불 시스템 설계

전자지불 시스템 설계를 위하여 기존의 사례연구를 실시하였는바, 전자현금시스템은 사용자의 익명성 보장문제와 이중사용의 문제 즉, 불법적인 현금의 복사 문제 등의 기술적인 문제와 경제적인 가치 척도로서의 사회 경제적인 문제를 안고 있다.

신용 카드 기반시스템은 두 가지로 분류할 수 있다. 퍼스트 버츄얼(first virtual)이나 CyberCash같은 기술력을 기반으로 신용카드를 이용한 전자적 지불을 지원하는 경우와 VISA나 MASTER CARD 같은 신용카드 회사에서 직접 전자적 지불을 지원하는 경우로 나눌 수 있다.

전자수표 시스템은 실세계의 수표를 그대로 인터넷상에서 구현한 것으로 사용자는 은행에 신용계좌를 갖고있는 사람으로 제한된다. 전자수표 시스템은 발행자와 인수자의 신원에 대한 인증을 반드시 거쳐야 하는

문제를 갖고 있다. 이를위해 여러 가지 보안 기법이 사용되기 때문에 트랜잭션 비용이 많이 드는 단점을 갖고 있으나 거액의 상거래시 지불수단으로 적합하다.

위의 내용을 기반으로 하여 전자 상거래에 있어서 전자지불 시스템을 설계해 놓은 것이 다음과 같다.

일반적인 전자 상거래 절차를 기준으로 인증 기술의 적용을 위한 인증 정책을 수립하고 전자 화폐의 익명성과 확장성에 대한 기술적인 대안을 근거로 지불 프로토콜의 구성상의 절차에 따른 기술 처리 절차는 다음과 같다.

1단계 : 전자 상거래를 위한 전용 인증 서버(certificate authority)는 별도의 통신 채널 또는 암호키 교환 방식에 의하여 공개키 등록을 요청하고 이를 인증 서버에서 처리하여 인증 서비스 제공을 준비한다.

2단계 : 구매자는 판매자의 웹(WWW) 서버로 접속을 시도한다.

3단계 : 구매자는 판매자의 공개키를 전용 인증 서버에게 요청한다.

4단계 : 전용 인증 서버는 구매자의 신원을 확인하고 확인된 경우 판매자의 공개키를 확인하여 인증서에 첨부하여 발급한다. 만약 구매자의 신원이 확인되지 않으면 구매자에게 해당 메시지를 보내어 공개키 등록을 하도록 한다. 또한 판매자의 공개키가 등록되지 않은 경우, 역시 구매자에게 해당 메시지를 보냄과 동시에 판매자에게도 이러한 사실을 알려준다.

5단계 : 구매자는 판매자의 공개키를 전용 인증 서버의 인증서를 통하여 받고, 또한 자신의 개인키를 가지고 판매자의 웹 서버에 연결하여 요청 메시지와 함께 공개키 암호화 처리한 암호문을 판매자에게 보낸다.

6단계 : 판매자는 구매자로부터 수신한 암호문을 읽기 위하여 전용 인증 서버에게 구매자의 공개키 요청을 한다.

7단계 : 전용 인증 서버는 4단계와 같이 판매자의 요청을 처리한다.

8단계 : 판매자는 자신의 개인키와 함께 전용 인증 서버에서 받은 구매자의 공개키로 공개키 암호화 방식에 의하여 암호문을 평문으로 처리하여 내용을 읽고 웹 서버 연결 승인을 취한다.

9단계 : 구매자는 판매자의 웹을 검색하여 원하는 상품의 구매 요청을 한다.

10단계 : 판매자는 구매자의 구매 요청에 대하여 구매자에게 확인 요청 메시지를 공개키 암호화 기법을 사용하여 전송한다. 즉, 판매자는 자신의 개인키와 구매자의 공개키로 구매자의 요청 내용을 구매자에게 보낸다.

11단계 : 구매자는 판매자의 확인 요청을 받고 이를 확인한 후 확인 결과를 판매자에게 공개키 암호화 기법을 사용하여 전송한다. 즉, 구매자는 판매자와 전용 인증 서버에게 자신의 거래 확인 요청에 대한 결과를 전송한다.

12단계 : 판매자는 구매자의 통지 결과에 구매자로 부터 받은 전자 화폐를 구매자 또는 판매자의 거래 은행에 구매자의 지급 요청을 처리하도록 거래 은행에게 판매자의

개인키, 구매자와 거래 은행의 공개키를 사용하여 공개키 암호화 기법을 사용하여 지급 요청 메시지를 보낸다. 일반적으로 지급 방식은 판매자가 거래하는 은행의 판매자의 구좌에 입금되도록 요청한다.

13단계 : 거래 은행은 전용 인증 서버에게 구매자와 판매자의 공개키를 요청하고 4단계와 같이 전용 인증 서버는 거래 은행에게 구매자와 판매자의 공개키를 발급한다. 거래 은행은 판매자가 보내온 메시지의 내용을 읽고 구매자의 신원을 확인한 후 지급 요청을 처리한 후 처리 결과 메시지를 구매자와 판매자의 공개키 및 거래 은행의 개인키를 이용하여 전송한다. 판매자의 수입과 관련하여 세금 관련 금융 정보 처리 시스템에서 세금 징수를 원천적으로 실시한 후 입금이 되도록 하고 세금 징수 내역을 판매자에게 별도로 통지한다.

14단계 : 판매자는 전용 인증 서버에게 거래 은행의 공개키를 요청하여 발급 받고 판매자의 개인키와 구매자의 공개키로 거래 은행의 메시지를 읽은 후 정상적인 지급 결과 통보일 경우, 구매자에게 판매자의 상품을 인도하고 동시에 영수증을 발급하여 거래를 정상적으로 종료한다.

15단계 : 구매자는 판매자의 송신 메시지를 판매자의 공개키와 구매자의 개인키로 평문 변환을 하여 상품(또는 상품 배달 증명서) 및 영수증을 확인한다.

## 5. 전자 화폐 설계

전자 상거래에서 가장 중요한 문제는 지불 방법에 관한 것이다. 가장 일반적으로 사용할 수 있는 방법은 신용 카드를 이용하는 것이다. 그러나 신용 카드를 이용하게 되면 은행은 사용자의 거래내역을 추적할 수 있어 개인이 어디서 무엇을 구매했는지에 관한 모든 정보를 알 수 있는 문제점이 생긴다. 즉 정보화 사회에서 핵심인 개인의 프라이버시를 침해하는 문제가 발생한다.

기본적으로 전자화폐는 은행(bank), 상점(shop) 그리고 사용자(구매자 혹은 consumer)로 구성되어 사용자와 은행간에 이루어지는 발행단계(withdrawal phase), 발행단계에서 발급 받은 전자화폐를 이용하여 물건을 사고 상점에 전자화폐를 지불하는 지불단계(payment phase), 그리고 사용자로부터 받은 전자화폐를 은행에 제출하여 상점의 계좌로 자금 이체를 시켜주는 결제단계(deposit phase)로 구성되어 있다.

D. Chaum은 프라이버시가 제공될 수 있는 전자화폐를 위하여 은닉 서명방식(blind signatures)을 제안하였다. 은닉서명방식은 메시지를 숨기는 서명방식으로 제공자(provider : 서명을 받는 사람)의 신원과 메시지를 연결시킬 수 없는 익명성을 유지할 수 있는 서명방식이다.

이 방법을 토대로 RSA 서명방식으로 은닉 서명방식을 이용한 만원권 전자화폐를 아래에 설계해 두었다.

### (1) 화폐 발행단계

① 은행은 만원에 해당하는 은행의 RSA

공개키(n,e)와 비밀키(p,q,d)를 생성하여 공개키(n,e)를 일반 사용자들에게 공개한다.

② 사용자는 화폐의 기본 정보(일련번호 등)가 기록된 전자문서 m을 준비하고 난수(random number) r을 임의로 선택하여 z를 계산한 후 은행에 보낸다.

$$z \equiv r^e \cdot m(\mathrm{mod}\ n)$$

③ 은행은 비밀키 d를 이용하여 z에 대한 RSA 서명 $\bar{s}$를 다음과 같이 생성한다.

$$\bar{s} \equiv z^d \equiv r \cdot m^d(\mathrm{mod}\ n)$$

④ 은행은 사용자에게 서명 $\bar{s}$를 전송한 후 사용자의 계좌로 부터 만원을 빼낸다.

⑤ 사용자는 자신만이 알고 있는 난수 r을 이용하여 $s \equiv \bar{s}/r\ m^d(\mathrm{mod}\ n)$을 계산하면 (m,s)가 은행으로 부터 받은 전자화폐가 된다.

(2) 화폐 지불단계

① 사용자는 은행의 서명(m,s)을 전자화폐로써 사용한다. 사용자는 원하는 물건을 사기 위해 상점에 전자화폐 (m,s)를 지불한다.

② 상점은 구매자가 제시한 전자화폐에 있는 은행의 도장을 확인한 후 은행의 데이터베이스에 접속하여 화폐에 기록된 일련 번호가 이미 사용된 적이 있는지를 확인한다. 정당한 화폐이면 상점은 구매자가 요구한 물건을 제공한다.

(3) 결제단계

① 상점은 후에 사용자로 부터 받은 전자화폐(m,s)를 은행에 제시한다.

② 은행은 상점의 계좌에 만원을 넣어준 후 은행의 데이터베이스에 (m,s)의 일련번호를 기록하여 다른 상점들에게 전자화폐(m,s)가 이미 사용되었음을 알린다.

위에서 사용자가 전자화폐의 기본 정보를 생성하므로 은행과 상점이 결탁하더라도 사용자의 프라이버시 정보가 노출되지 않는다.

그리고 위와 같은 전자현금의 가장 큰 현실적인 문제는 이중사용 방지를 위해 은행에서 이미 사용된 모든 전자화폐들에 대한 데이터베이스를 구축해야 한다는 것이다.

이러한 목적으로 개발된 전자현금 시스템으로는 chaum, Fiat, Naor 등의 cut-and-choose 방식을 이용한 전자화폐, S. Brand 등의 제한적인 은닉 서명기법(restrictive blind signatures)과 표현 문제(representation problem)를 이용한 전자화폐 등이 있으며 또한 전자지갑내에 은행이 발행하는 temper-resistant 모듈(TRM)인 관찰자를 적재하여 전자화폐의 이중 사용을 감시하게 하므로써 이중 사용을 사전에 방지하는 사전 방지 방법 등이 있다.

## V. 결 론

인터넷은 누구에게나 열려져 있는 오픈 네트워크라고 할 수 있다. 누구나 사용할 수 있는 인터넷의 범용성은 전세계의 모든 사용자를 고객으로 삼을 수 있는 전자 상거래의 가장 큰 장점으로 이어진다. 그러나

인터넷은 오픈 환경을 지원하기 때문에 악의의 목적을 가진 해커들에게도 노출되어 있어 보안에 취약하다고 할 수 있다. 인터넷이 보안에 취약한 이유는 인터넷에서 사용되는 오픈 환경을 지원하는 통신 프로토콜인 TCP/IP와 유닉스를 운용체제로서 사용하기 때문이다.

본 논문에서는 인터넷상에서 전자 상거래가 보편화될 경우 전자식 대금 결제를 위한 네트워크 설계, 보안 시스템 설계, 대금 결제 시스템 설계, 전자지불 시스템 설계, 전자화폐 설계와 각종 보안대책을 제시하였다.

그리고 전자식 대금 결제 시스템은 일반 분야와는 달리 학문적인 가치뿐 아니라 산업계에서도 파급효과가 크므로 산업계와 학계가 연계해 발전시켜야할 분야이다. 향후 연구 과제로는 전자식 대금 결제 시스템 설계 기술의 확보는 물론 설계된 내용을 중심으로 실제 시스템을 구현하기 위한 기술이 요망된다.

## 참 고 문 헌


권도균, 『WWW보안과 전자화폐』, http://madang.dacom.co.kr/~dgguen/.

김상균, 『21C 신경제의 새로운 비전 SET』, 데이터베이스 월드, 1997, 10

김정평, 김충수, 『전자 상거래와 인터넷』, 경영정보연구, 제1호, 1997.6.

김중한 외 3인, 『전자 상거래 기회와 도전』, 정보처리, 제4권 제1호, 1997.1.

신동민, "전자 상거래의 추진현황 및 향후 전망", 『신한리뷰』, 1997. 3., pp. 60-77.

제일금융원, "전자화폐", 『한국경영신문사』, 1997.

한국과학기술원 전자 상거래 연구실, "전자 상거래의 구성요소", 『월간 INTERNET』, 1996. 5.

Loshin, Pete, 『전자 상거래의 모든 것』, 성안당, 1997.

Elgamal, Taher. "CREDIT CARD PAYMENT APPLICATIONS OVER THE INTERNET" http://home.netscape.com/newsref/std/credit.html, July 14, 1995.

Medvirsky, Gennady and B. Clifford Neuman, "NetCash: A Design for Practical Electronic Currency on the Internet, Proceedings of the First ACM Conference on Computer and Communication Security", Nowember, (1993)

VISA, Master Card, SET(Secure Electronic Transaction) http://www.visa.com. http:// www.mc.com/.