인터넷뱅킹 확산에 따른 금융전산망 보안방안 연구

서병삼
동아대학교 경영대학원 경영정보학과
한계섭
동아대학교 경영정보학과 교수

요 약

은행이 급변하는 마케팅환경에 적극적으로 대처하고 인터넷뱅킹 시대를 맞이하여 경쟁의 우위를 점하기 위해서는 안정적인 인터넷뱅킹 서비스의 공급이 필수적이다.

이를 위해서 은행은 기존의 물리적인 고객 접점에서 인터넷의 전자적인 공간을 이용한 가상은행의 구현이 필연적이며 이러한 목표를 달성하기 위해서는 금융전산망의 완벽한 보안이 선결되어야 한다.

이러한 관점에서 국내 은행들이 전자상거래에서 가상은행을 통한 전자지불시스템의 구축시 선행되어야 할 전산망 보안에 관한 연구를 국내 금융기관의 실정에 맞게 모델을 선정하고 발전된 모델을 제시하였다.

Ⅰ. 서론

정보통신기술의 발달은 날로 고도화하고 있으며 산업 전반에 걸쳐 그 파급효과가 나타나고 있다. 금융산업은 전자적인 자료처리 기술을 기반으로 업무처리가 완성되는 특성을 가지고 있으며 거래처리의 목적으로 다른 기업들 보다 정보통신기술에 대한 투자와 활용을 폭 넓게 진행해 온 것이 사실이다. 또한, 국내의 폰뱅킹(Phone Banking), 펌뱅킹(Firm Banking), 홈뱅킹(Home Banking) 이용자수가 점진적으로 증가하고 있으며 전자금융에 대한 수요가 급증하는 것은 전자금융과 전자상거래가 본격적으로 기존 금융환경을 대체하여야 할 시기라는 것을 반증하는 것이라 하겠다.

우리 나라의 금융산업은 대외경쟁력 강화와 수익성개선이라는 절실한 명제 앞에서 기존의 고원가성 고객서비스를 대체할 수 있는 새로운 개념의 금융서비스 시스템도입의 필요성은 기업의 생존권유지와 직결된다고 하겠다.

근래에 와서 자료처리의 전산화를 선두로 하여 CD/ATM, PC뱅킹, POS(Point of sales), 선불카드, 직불카드, 전자지갑 등의 형태로 전자금융 서비스가 광범위하게 진행되고 있으며 많은 은행들이 인터넷을 이용한 웹뱅킹 서비스 구축 및 전자상거래의 참여를 적극 시도하고 있다.

국내 은행들은 그 동안 제도권으로부터 많은 규제를 받아왔으며 전자상거래에 있어 지불결제 시스템으로서의 역할은 거의 전무한 형편이다. 그리고, 인터넷과 같이 누구에게나 공개되어 있는 오픈 네트워크 환경에서 안전한 거래를 보장하는 보안시스템의 구축과 인증이 가장 핵심적인 문제들이라 하겠다.

최근에 한국은행에서는 국내에서 통용될 전자화폐 형태를 발표하는 등 전자상거래 상에서 지불결제매체를 표준화하기 위하여 많은 노력이 진행되고 있다.

이러한 상황에서 은행이 전자지불시스템의 구현을 위하여 특히 고려하여야 할 네트워크의 보안문제는 무엇인지, 또한 은행의 입장에서 문제화되는 것들은 어떤 것인지에 대한 조사를 하여 보고자 한다.

따라서 국내 금융기관을 대상으로 전자지불시스템 구축방향에 대한 관심과 네트워크의 보안현황에 대하여 설문조사를 통하여 분석하고 외국의 가상은행 시스템 네트워크에 대한 보안체제의 문헌조사를 통하여 보충의 필요가 있는 부분을 도출하고자 하며 보다 진보된 시스템구현에 필요한 네트워크 보안 모델을 제시하고자 한다.

Ⅱ. 금융 전자지불시스템 고찰

2.1. 출현요인 및 배경

인터넷 사용의 급격한 증가로 인하여 다양한 욕구를 가진 계층적 사용그룹들이 등장하였으며 이를 이용하는 목적 또한 다양화하였다.

다양한 정보산업기술의 발달은 인터넷상에서의 전자결제구현에 엄청난 변혁을 몰고 왔으며 많은 기업들이 이미 전자상거래시스템을 구축하였고 인터넷상에서 대금 지불 및 결제를 할 수 있도록 서비스 중에 있다.

인터넷상에서의 지불결제를 담당할 가상은행(Cyberbank)은 실제 은행과 연계되지 않은 순수한 인터넷 기술기반의 서버 형태(Server-type)가상은행과 실제은행의 전산시스템과 인터넷 기술을 접목한 레거시게이트웨이 형태(Legacy Gateway-type)가상은행으로 나눌 수 있으며 전자지불시스템은 가상은행이 가지고 있는 가장 중요한 핵심기능이다. 전자지불시스템의 구조는 앞의 두 가지 가상은행 형태에 따라 많은 영향을 받는다. 따라서, 본 연구는 기존 전산자원과의 연계에 의한 가상은행 시스템인 레거시 게이트웨이 형태의 전자지불시스템을 중심으로 하고자 한다.

2.2 전자지불시스템의 구성요소

전자지불시스템의 설계나 개발을 위해서는 먼저 기본적인 지불체계의 선택을 필요로 하는데 통상 이러한 지불체계는 대략 3, 4가지로 분류하고 있으며 이에 따라 기본적인 구성을 달리하는 특징을 가지고 있다.

Kalakota와 Whinston(1996)은 전자지불시스템을 세 가지 형태로 분류하였는데 첫째가 전자화폐기반의 전자지불 시스템이며 전자현금과 전자수표를 포함한다. 두 번째가 스마트카드이며 세 번째가 신용카드 기반의 전자지불시스템이다. B. Clifford Neuman(1995)은 인터넷을 기반으로 한 전자지불시스템을 전자통화 시스템, 신용-직불(Credit- Debit)시스템, 시스템지원형 신용카드번호 보안모델의 세 가지로 분류하고 있다.

한편, D. O'Mahony, M. Pierce, H. Tewari(1997) 등은 신용카드 기반 시스템, 전자수표 지불시스템, 전자현금 지불시스템, 소액 지불시스템의 네 가지로 분류하고 있다.

본 연구에서는 인터넷상에 현존하고 있는 전자지불시스템을 D. O'Mahony 등의 분류에 따르기로 한다.

(1) 신용카드 기반

신용카드를 이용한 전자지불은 기존의 실세계에서 신용카드를 사용하는 절차와 상당히 유사하게 이루어진다. 신용카드는 1960년대 초반부터 비자사와 마스터카드사에 의하여 사용되었으며 비자사의 경우 1995년 중반까지 18,000개의 금융기관 회원을 통해 4억 2천만 매 이상의 신용카드를 발행하였고 247개국의 1천 2백만 가맹점을 가지고 있다.

원천적 경쟁관계에 있는 마스터카드사는 220개국에 걸쳐 1천 3백만 개의 가맹점과 22,000개의 회원조직을 가지고 있다. 1995년 두 카드사가 발행한 카드는 8억 장에 이르며 연간 1조 3천억 달러에 이르는 거래규모를 가졌다.

국내의 경우 1997년 말 현재 4천 4백만 매 이상의 신용카드가 발행되었으며 70조원 이상의 이용실적을 보이고 있다.

(2) 전자수표 기반

전자수표는 현실세계에서 사용되고 있는 것을 전자적 공간에 그대로 옮겨 놓은 형태적 특징을 가지고 있다. 미국에서는 아직도 많이 사용되는 수표제도가 유럽국가들에서는 환영받지 못하고 있는 이유는 수표를 이용한 업무처리의 경우 비용이 많이 든다는 점이다. 또한 직불(Debit)카드는 기존 수표제도가 가진 불합리한 점을 제외하고 거의 모든 면에서 수표제도의 장점을 취하고 있다. 한가지 명백한 것은 거래 발생시 거래대금이 지불인의 은행계좌에서 수취인의 은행계좌로 이체되어야 하는 수표제도와 비슷한 역할을 하는 지불시스템이 필요하다는 점이다. 은행의 관점에서 본다면 은행간 자금이체는 가급적 많이 이루어지기를 바라고 있다.

(3) 전자화폐지불시스템

통상적인 국가들은 거의 모든 거래에서의 지불수단으로 현금을 이용하는데 이는 약 75%에서 95%수준에 해당한다. 사람들이 어떠한 형태의 전자적인 현금을 선호하리라 추정하는 것은 어려운 일이나 현실세계에서 실물화폐에 대한 선호도를 추정해 볼 때 아래와 같은 점의 충족은 반드시 원하고 있는 것으로 판단할 수 있다.

① 가용성(Acceptability)
② 보증된 지불수단(Guaranteed Payment)
③ 거래수수료가 없음
(No Transaction Charges)
④ 익명성 (Anonymity)

(4) 소액지불시스템

통상적인 거래에 따른 지불수단인 현금, 수표 및 카드 중에서 소액거래에 대한 적합한 지불수단은 현금이다. 어떠한 거래도 최소단위의 화폐가치보다는 많은 거래에 따른 비용을 발생하게 된다. 이는 모든 재화와 용역의 거래에서 제기

되는 기본적인 문제이다. 이는 네트워크 상에서 발생되는 최소 금액의 거래까지 지원하면서 이로 인한 통신부하를 줄일 수 있는 전자지불 시스템의 필요성을 요구하게 된다.

이는 소비자가 전자백과사전의 검색, 음반에 수록된 음악타이틀 중에서 한 곡만의 구매, 신문의 특정내용만을 구매하는 등 구매형태의 다양화를 충족시킬 수 있는 지불시스템이다.

2.3. 전자지불시스템의 활용 및 방향

전자지불시스템의 정보기술은 실세계에서 사용되는 지불수단을 반영하고 널리 사용될 것이다. 앞서 고찰한 4가지의 주요한 분류-카드, 수표, 현금과 소액결제수단-는 현재 사용되고 있고 앞으로 제안될 중요한 시스템임에 틀림없다. 산업사회에서 이러한 지불체제별 시스템들은 서로간의 경쟁을 벌일 것이고 하나만이 남을 것이다. 결국, 현실세계의 상거래를 가장 효과적으로 지원하는 시스템만이 위의 4가지 범주에서 하나씩 남게 되고 서로 보완적인 역할을 할 것이라는 것을 의미하는 것이다.

신용카드 기반의 전자지불시스템의 경우에는 SET에 의한 효과적인 시스템 개발로 집중화될 것으로 추정된다.

전자수표 분야의 경우 그 도입 및 실행은 계속 지연되고 있으며 연구기관이나 학술단체에서 개발한 진보된 전자수표 시스템들에 대한 실제 금융기관에서의 도입은 전무하다. 이는 금융기관들이 바라는 시스템의 형태 자체가 기존 수표결제 형태를 포함한 소규모 시스템의 확충에 집중되어 있기 때문이다. 따라서 당분간 전자수표 시스템에 대한 확산은 기대하기 어렵다고 하겠다.

전자현금 역시 집중적 개발투자의 부재에 의한 어려움을 겪을 것으로 전망하고 있다. 전자현금 시스템의 부족한 부분은 Mondex나 EMV 현금카드와 같은 전자지갑시스템에 대한 개발의지로 나타난다.

Micropayment의 출현은 지금까지 존재하지 않았던 상거래에 있어 완벽한 형태로 나타났다. 앞으로 전자상거래 관련 업체들의 인식과 검증을 받는 시간이 다소 요구되겠으나 엄청난 반향을 몰고 올 충분한 가능성을 가지고 있다.

분명한 것은, 이러한 전자적 결제수단이 실물경제의 결제수단을 1%라도 대체할 경우 그 산업적 파급효과는 세계적으로 확산된다는 점이다.

2.4 앞으로의 전자지불시스템

전자지불이 지향하는 목표시스템은 그 기본적인 몇 가지 전제조건의 충족을 필요로 한다. 이러한 전제조건은 실생활에서 결제시스템의 역할을 수행하는 금융산업의 고유한 기능을 가상공간에서 제공하는 것과 전자적인 특성을 이용한 고부가가치 서비스를 구현하는 것으로 구분할 수 있겠다. 이러한 서비스의 구현에는 국가적, 제도적, 관습적인 문제점들이 많이 도출되겠으나 EM(Electronic Marketplaces)에서의 전자상거래는 보다 포괄적이고 다양한 문화적 요소를 수용하여야 할 것이다. 최근에는 정보화사회의 고도화에 따라 정보판매와 같은 새로운 형태의 서비스들이 출현하고 있으며 이러한 것들을 수용할 수 있는 전자지불시스템이 더욱 절실히 필요하게 되어가고 있다.

따라서, 전자지불시스템이 가져야 할 전제조건의 완성이 미래의 전자지불시스템의 모습이 될 것이다. 특히, 아래와 같은 전제조건의 충족이 실현되어야만 진정한 의미의 전자지불시스템이라 정의할 수 있을 것이다.

① 정보의 무결성보장
② 거래처리의 경제성유지
③ 범세계적인 결제수단의 제공
④ 지불단위의 유연성 제공
⑤ 온라인 실시간 거래처리
⑥ 익명성의 보장
⑦ 경제변동에 영향을 받지 않는 시스템 구현

Ⅲ. 전자지불시스템의 네트워크 현황및 분석

3.1 지불체계에 따른 네트워크 구조 및 데이터 흐름

전자지불시스템의 전반적인 구조는 지불체계의 선택에 따라 다양하게 구성하고 설계를 할 수 있다. 지불체계와 더불어 보안정책의 방향에 의하여 시스템 및 네트워크 구조와 데이터의 흐름을 더욱 다양하게 설계할 수 있을 것이다. 뿐만 아니라 다양한 지불체계의 성격을 혼합하여 상호보완적인 지불시스템을 구성할 수 있다. 여기서는 여러 가지 전자지불시스템 중 국내 여건을 감안할 때 가장 구현 가능성이 있는 SET에 의한 신용카드 기반의 지불체계와 전자현금에 의한 지불체계를 기준으로 하여 네트워크 구조와 데이터 흐름에 대하여 설명하고자 한다.

(1) SET에 의한 신용카드 기반

인터넷상의 신용카드 기반의 전자지불 표준이 될 가능성은 매우 크다고 할 수 있는

SET의 지불 프로세서를 살펴보면 먼저 카드소지인(Card Holder)이 재화에 대한 구입 결제를 상점(Merchant)에게 요청한다. 상점(Merchant)은 지불게이트웨이(Payment Gateway)를 통하여 신용카드회사로부터 카드소지인(Card Holder)의 카드에 대한 지불권한을 확인하고 거래를 성립시킨다. 지불게이트웨이는 금융네트워크(Financial Network)와 상점사이에서 거래가 발생할 경우 지불권한을 확인해 주는 역할을 한다. SET을 통한 거래에 참여하고자 하는 모든 당사자는 지불 프로세서 상에서 개별 당사자에 대한 인증을 요구하게 될 것이며 이는 개별적으로 할당된 공개키의 쌍으로 해결할 수 있다.

(2) 전자화폐에 의한 지불체계

전자화폐를 기본 지불체계로 하는 전자지불시스템에서는 인터넷상에서 완전한 익명성을 보장하는 Ecash는 다음과 같다.

Ecash는 실물화폐로서의 기능에 덧붙여 오픈네트워크에서 필요로 하는 보안기능을 가지고 있으며 정보, 재화 및 용역의 대가로 지불이 가능하게 구성되어 있다. Ecash가 익명성을 보장한다는 것은 사용자가 은행으로부터 전자화폐를 인출할 때 은행은 그 인출화폐의 일련번호를 알 수 없기 때문이다. 인출된 화폐는 상점에서 익명으로 사용될 수 있으며 상점이나 은행 또는 은행간에 공모를 하더라도 소비하는 고객을 알 수 없도록 되어 있다. Ecash는 대칭 및 비대칭(공개키)암호화를 이용하여 매우 강력한 보안을 유지하는 전자지불 시스템이다.

3.2 보안에서의 구비해야 할 제반요소

인터넷상에서의 전자지불을 안전하게 구현하기 위해서는 보안문제가 가장 중요하다는 것은 재삼 거론할 필요가 없을 것이다. 이는 인터넷뿐만 아니라 네트워크를 통한 거래 자체가 안고 있는 문제이기도 하다. 특히, 인터넷은 오픈시스템의 개방형 연결지향적 프로토콜인 TCP/IP를 사용하기 때문에 네트워크 상에서의 보안이 취약한 약점을 가지고 있다.

전통적으로 정보의 보안을 위한 노력은 세 가지 기본적인 사항의 충족을 완성하기 위한 형태로 나타나는데 그 내용은 아래와 같다.

- 기밀성 (Confidentiality)
- 무결성 (Integrity)
- 가용성 (Availability)

이에 따라 위의 요건을 충족하기 위해서는 적절한 보안정책이 필요하며 정보보안의 위협요소와 전자지불 시스템의 네트워크 구성에 요구되는 보안요소에 대하여 알아보기로 한다.

(1) 주요 위협요소

주요 위협요소는 다른 위협요소를 선도한다는 데 중요한 의미를 가지는데 크게 침투위협(penetration threats)과 설치위협(planting threats)으로 구분 지을 수 있다.

1) 침투위협((penetration threats)
   - 사칭(Masquerade)
   - 통제우회(Bypassing Control)
   - 권한위반(Authorization Violation)
2) 설치위협 (planting threats)
   - 트로이 목마 (Trojan Horse)
   - 함정 (trapdoor)

(2) 잠재적 위협요소

현재의 환경에서 어떠한 위협요소를 분석하고자 할 때 더욱 포괄적인 위협요소에 대한 연구 및 분석을 선행하여야 한다. 예를 들면 사칭(masquerade)의 경우 모든 잠재적 위협의 근간이 될 뿐 아니라 스스로 정보누출의 역할도 가능하다는 것이다.

3.3 기존 금융전산망 위험분석

위험분석의 가장 큰 목적은 기업내부의 모든 자산에 대한 위험수준을 측정하고 문제 발생시 대응책을 확보하는 데 있다. 위험분석 모델은 위험분석의 전반적인 흐름을 나타내는 위험분석 구조도(Architectural Flow Map)이다. 위험분석은 보안정책의 수립과 보안관리 주기에 대한 연속성을 부여하며 BCP(Business Continuous Plan)와 같은 비상대응계획의 기초 자료가 된다. 위험분석은 자산조사, 분석, 위험산출을 통하여 위험평가를 하게 된다. 위험분석을 기반으로 정보보호정책을 수립하고 보안계획에 의하여 단위 자원에 대한 보안을 진행하여야 한다. 정보보호 정책의 성공은 관리책임의 확실한 규정과 경영진의 관심에 의해서만 가능한 것이다.

3.4 금융전산망 구성에 요구되는 보안요소

금융전산망에서는 자금이동 전문이나 금융정보의 전송 등 자금과 관련된 자료의 교환이 이루어져 왔으며 그 동안 금융전산망 자체를 폐쇄적으로 운영함으로서 보안침해사고가 매우 드물었다. 그러나, 최근 오픈네트워크 환경을 접하면서 각종 망간의 연결이 활발히 진행되고 있으며 인터넷과의 연결도 시도되고 있다. 하지만 가장 큰 장애요인인 해커들에 의한 보안침해사고는 예전과 다른 양상을 보이고 있다. 과거와 달리 해커들은 그룹화하고 지능화되는 경향이 뚜렷하다. 또한, 공격수법과 도구들이 우수해지고 빨라지는 경향이 있으며 서로의 정보를 통신망으로 공유하는 사례가 늘고 있다.

이러한 국내외적 환경변화를 감안할 때 금융전산망이 반드시 갖추어야 할 네트워크 보안요소는 여러 가지가 있겠으나 특히 다음과 같은 부분에 대한 체계적 대응이 필요하다.

① 기밀성, 무결성, 암호화
② 인증(Authentication)
③ 권한(Authorization)
④ 부인봉쇄(Non-Repudiation)

3.5 국내 은행의 전자상거래 및 전산보안 설문조사

본 절에서는 국내 금융기관(은행 중심)을 대상으로 구체적인 설문조사를 통한 자료의 수집에 관해서 검토하고 국내 금융네트워크의 보안수준과 전자지불시스템의 추진방향에 대하여 분석적 결과를 제시하고자 한다.

(1) 표본의 선정

본 조사의 모집단은 한국통신 가상은행시스템 참여은행 28개 선정하였다. 그 이유로는 한국통신이 주관하는 사이버시티사업에 국내 은행이 대거 참여하고 있기 때문이며 향후 인터넷 서비스를 제공하기 위하여 추진 중에 있기 때문이며 은행 당 1부씩 총 28부의 설문지를 배포하고 22부를 회수하였다. 회수한 설문지 19개 은행의 19부만 유효한 설문으로 간주하여 67.9%의 회수율을 기록하였다. 응답은행 중 13개는 시중은행이었고 나머지 6개 은행은 지방은행이었다.

응답자의 소속부서는 정보시스템관련 부서가 18개 은행이었으며 고객지원부 소속이 1개 은행으로 나타났고 주로 현업에서 실무를 담당하는 직원이 응답하고 있다.

(2) 설문분석 결과

본 연구에서는 설문문항에 의하여 조사된 금융기관의 네트워크 보안 수준 및 전자지불시스템의 구현 방향에 대한 기초자료를 바탕으로 그 통계분석을 하고자 하였다. 그러나 국내 은행의 총 수가 33개에 불과하고 조사된 은행의 수가 19개로 단순한 산술적 분석만이 가능하였다. 설문지의 측정문항 결과는 <표 1>과 같다.

<표 1> 설문 측정문항 결과표

구 분		응답 항목		구 성 비	
전자상거래	전자지불시스템 구축계획 유무	유		84.2 %	
		무		15.8 %	
	전자지불시스템 결제수단 (복수 응답)	1	신용카드	2	5.3%
		2	선불 IC 카드	3	21.1%
				4	10.5%
		3	전자지갑	6	21.1%
				1 2	5.3%
		4	전자현금	1 3	5.3%
		5	기타	2 3	5.3%
		6	검토한 바 없음	1 2 3	5.3%
				1 3 4	5.3%
				1 2 3 4	10.5%
	전자지불시의 인증기관 (복수 응답)	1	금융결제원	1	61.5%
		2	한국은행	2	11.2%
		3	통신사업자	5	16.7%
		4	외국업체	1 5	5.5%
		5	자체인증	1 3 5	5.5%
	전자상거래팀 운영유무	유		22.2 %	
		무		77.8 %	
네트워크 보안	전사적 보안지침수립 운영여부	여		78.9 %	
		부		21.1 %	
	보안관련팀 운영여부	여		63.2 %	
		부		36.8 %	
	네트워크 보안 도구 사용여부	여		52.6 %	
		부		47.4 %	
	방화벽시스템 설치 여부	여		26.3 %	
		부		73.7 %	
	네트워크 보안정도 에 대한 판단	매우 우수		0.0 %	
		우 수		26.3 %	
		보 통		57.9 %	
		미 흡		10.5 %	
		매우 미흡		5.3 %	

설문결과에 의하면 향후 전자지불시스템 구축계획을 가지고 있는 은행은 84.2%로 거의 대다수 은행들이 해당되며 인증기관은 금융결제원이나 한국은행을 선호하고 있는 것으로 나타났다. 그러나 전자상거래 연구팀을 별도로 보유한 은행은 22.2%에 불과하며 방화벽시스템을 보유한 은행 또한 26.3%에 불과하였다.

특히, 국가안전기획부에서 제정한 국가전산보안업무 기본지침에 의하면 내부망과 외부 상용망의 접속시 내부망과 분리하여 상용망을 별도 구성, 운용하거나 상용망 전용단말기를 별도로 설치하여 운용하게 정해져 있다. 그리고, 국가안전기획부장의 보안성 검토를 받아 승인된 경우에 한하여 외부망과 접속이 가능하며 암호 프로그램도 비도승인을 받은 후 사용하게 되어 있어 많은 개선이 요구된다.

네트워크 보안 정도에 대한 판단 항목에서는 73.7%가 보통이하로 응답하고 있어서 이에 대한 대책의 마련이 중요한 현안임을 알 수 있다.

3.6 전자지불시스템에서 제기되는 문제 분석

국내의 금융기관들은 보안문제의 미해결로 인하여 뱅킹서비스의 제공에도 많은 어려움을 겪고 있으며 인터넷상에서 텔넷을 이용한 PC뱅킹 서비스는 1996년 K대학생의 절도사건이후 폐쇄되었다. 전자지불시스템은 기존 금융권의 인프라를 기반으로 구축되어 질 것이며 그 현황에

대한 문제점과 분석을 통하여 향후 전자지불시스템을 구축할 때 고려하여야 할 주요부분은 아래와 같다.

① 전사적 보안정책의 부재
② 시스템 의존적 보안정책
③ 저수준의 보안방식 사용
④ 네트워크 표준화의 부실
⑤ 회선 임차에 따른 문제

따라서 전자지불시스템을 구축하기 이전에 이러한 전반적인 문제점에 대한 조정과 대책이 수립되어야 할 것이다.

Ⅳ. 효과적인 금융 네트워크 보안방안

4.1 다단계 인터넷 보안모델 적용

인터넷을 통한 금융서비스의 제공은 수많은 인터넷서버를 통한 외부로부터의 액세스를 허용한다는 보안상의 문제를 발생시킨다. 인터네트워킹은 매우 투명(Transparency)한 접근을 보장하는 반면 보안문제에 관해서는 취약한 것이 현실이다. 인터넷은 네트워크간의 상호접속을 기본으로 각종 서버와 사용자들이 상호접속된다는 의미를 갖는다. 따라서, 보안문제는 네트워크적인 측면과 시스템적인 측면으로 나누어 접근할 수 있다. 따라서 네트워크 부분은 네트워크 장비의 물리적인 보안부터 네트워크 자체의 접근제한 등의 보안대책과 절차를 수립할 수 있다. 이러한 제반 요소를 기반으로 구조적이고 일관된 보안절차를 수립하기 위하여 OSI통신규약(OSI 7 layer)을 적용하여 개념적으로 모델링하고 TCP/IP 프로토콜과 비교를 하면 <그림 1>과 같은 다단계 인터넷 보안모델을 구성할 수 있다.

4.2 내부네트워크 보안대책

네트워크 보안은 자원에 대한 ACL(Access Control List)에 의한 접근통제로부터 시작된다. 접근통제는 인가된 사용자만이 특정 시스템 및 자원에 접근하여 인가된 자원만을 사용할 수 있도록 하는 것이다. 또한 네트워크 자원에 대한 불법적인 접근과 같은 위협요소가 발생할 경우 감사추적이 가능하도록 로깅(logging)정보를 기록하여야 한다. 네트워크 자원에 대한 접근통제는 호스트, 서버에 대한 출입통제나 네트워크 케이블링에 대한 물리적 접근통제와 같은 물리적인 보안과 Secure OS나 Key 서버 등에 의한 논리적인 보안으로 구분되며 논리적인 보안방안은 다음과 같다.

① 안전한 운영체제(Secure OS)의 채택
② 사용자 인증 강화
③ 비활동접속 자동차단
④ 실시간 침입탐지체제(Real-Time Intrusion Detection System)의 구축

4.3 외부네트워크 보안대책

최근 국내 은행들은 대외업무와 활발한 연계를 추진함에 따라 외부 네트워크와의 연결이 계속 늘어나는 추세이다. 외부네트워크는 금융결제원을 중심으로 한국은행, VAN업체 등 많은 대외기관이 연결되어 있으며 오픈 네트워크의 발달에 따라 프로토콜도 TCP/IP를 이용하는 경우가 늘어나고 있다. 특히, 한국은행이나 금융결제원은 향후 은행의 전자지불시스템 구축시 인증기관으로서의 역할이 기대되

TCP/IP Protocol Suite	Layer	OSI Reference Model	Layer Name	기 능
Application Layer	7	Application Layer	Policy	기관의 전반적 보안정책
	6	Presentation Layer	Personal	보안교육 및 인식제고
	5	Session Layer	LAN	기관내부의 LAN 및 HOST보안대책
Transport Layer(TCP)	4	Transport Layer	Internal-Demark	기관 내부LAN간의 격리 보안
Network Layer(IP)	3	Network Layer	Gateway	기관 내부와 외부 LAN간의 통로보안
Network Access	2	Data Link Layer	Packet-Filter	기관 내부/외부LAN간의 패킷정보에 의한 보안
	1	Physical Layer	External-Demark	외부연결접점의 보안

<그림 1> 다단계 인터넷 보안모델

며 금융결제원은 현재에도 타행환이나 현금자동인출기 공동이용서비스 등 직접적인 자금교환 데이터들이 전송되고 있어 네트워크관리에 특별한 노력이 요구된다 하겠다. 이에 따라 외부네트워크의 보안대책을 정리하면 다음과 같다.

① 외부 기관의 내부 네트워크 접근 보안
② 내부 사용자의 외부 네트워크 접근 보안
③ 방화벽에 의한 네트워크 접근보안
④ Dial-in 서비스의 보안

4.4 금융 네트워크 통합관리 방안

앞서 언급한 다단계 인터넷 보안모델 및 내부, 외부의 네트워크 보안대책에 의하여 기존 금융 네트워크의 통합관리를 위한 방안으로서 중앙감시센터를 이용한 네트워크 구간별 방어대책을 수립할 수 있다. 중앙감시센터는 전반적인 네트워크 보안정책의 수립에 의하여 네트워크 보안을 위한 각 요소를 통합적으로 운영하기 위한 기능을 가지며 네트워크 모니터와 침입탐지 등 제반 보안 활동을 하는 역할을 맡는다. 금융 네트워크에서 중앙감시센터를 중심으로 네트워크의 구간별 방어대책을 수립하면 <그림 2>와 같은 네트워크를 설계할 수 있다.

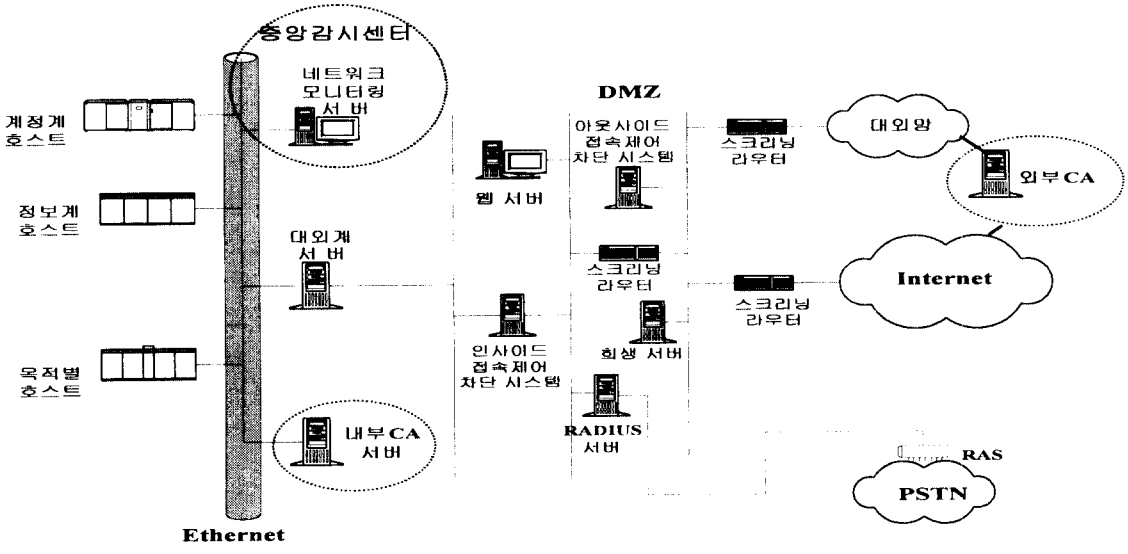
외부네트워크로부터 내부를 보호하는 것에 중점을 둔 모델로서 모든 트래픽은 접속제어차단/시스템을 우회하지 않도록 하여야 한다. 또한 스크리닝 라우터는 정적(static) 라우팅이 되도록 하여 보안장비를 우회하거나 제한지역을 접근할 수 없도록 하여야 한다. 외부 네트워크로부터 받는 모든 트래픽은 스크리닝 라우터가 필터링을 적용하여 이를 통과한 트래픽만 아웃사이드 접속제어차단 시스템에 전달하고 그 밖의 모든 네트워크 트래픽은 거절되어야 한다.

침입자가 스크리닝 라우터를 통과하더라도 아웃사이드 접속제어/차단시스템을 통과하여야 하며 2 단계 방어를 맡고 있는 'choke'라 불리는 두 번째 스크리닝 라우터와 인사이드 접속제어/차단시스템을 모두 통과하여야만 내부네트워크에 도달할 수 있다. 하지만 이 과정 동안에 네트워크 모니터링 시스템이 실시간 네트워크 감시를 통하여 공격이나 침입으로 판명될 때 이를 방어하고 중앙감시센터의 네트워크 관리자에게 알리게 된다.

인터넷 뱅킹과 전자지불시스템은 지불체계에 의하여 그 기본적인 구조가 크게 달라질 수 있으며 네트워크 보안 또한 그러하다. <그림 2>는 국내 은행의 네트워크 환경을 위주로 레가시 게이트웨이 형태(Legacy Gatrway-type) Cyberbank를 구현할 경우 고려해 볼 수 있는 보편적 네트워크 보안모델이며 개별 은행의 업무흐름에 따라 많은 첨삭이 가해져야 할 것으로 판단된다.

V. 결론

본 연구는 은행기관이 인터넷 뱅킹서비스를 하기 위하여 갖추어야 할 네트워크 보안수준에 관한 연구라 할 수 있다. 특히, EM(Electronic Marketplaces)상에서 가장 중요한 역할인 지불결제를 담당하여야 할 은행기관으로서는 보안에



<그림 2> 금융 네트워크 보안 설계 모델

대한 대책이 절실히 요구되며 이는 곧 은행기관의 생존권과 직결되는 중요한 사안이다. 이러한 측면에서 인터넷뱅킹 구현에 요구되는 금융전산망의 보안을 위하여 전자지불시스템에 대한 조사와 국내 금융네트워크의 실태를 파악하고 효과적인 네트워크 보안방안을 제시하기 위한 연구를 하고자 하였다.

조사 및 분석결과에 의한 내용을 살펴보면 다음과 같다.

첫째, 인터넷뱅킹에 대한 금융전산망의 보안은 기본적인 지불체계의 선택에 따라 다양하게 설계될 수 있다는 점이다. 기본적인 네트워크 보안요소는 별반 차이가 없으나 내부네트워크와 외부네트워크의 접속방식에는 많은 차이가 있다는 것이다.

둘째, 국내 은행기관의 전자지불시스템 구축의지는 매우 높게 나타났으나 전문적인 연구활동은 저조하였으며 네트워크 보안수준도 낮다는 것을 알 수 있었다. 이러한 점이 시사하는 바는 은행기관이 오랫동안 정부정책에 의한 통제로 인하여 보안에 관한 자율적인 연구개발 및 투자가 제대로 이루어지지 않았다는 점이다.

셋째, 네트워크 보안은 전사적인 위험분석과 보안정책에 의하여 수립되고 운영되어야 한다는 점이다. 네트워크 보안은 모든 전산자원과 연관되어 있으므로 네트워크 보안만을 강화한다고 보안문제가 해결되는 것은 아니며 내부 시스템과 내부 네트워크 및 외부 네트워크와의 통합적인 보안을 유지하여야 효과적인 것으로 나타났다.

참 고 문 헌

1) 국가안전기획부, "국가전산보안업무 기본지침", 1997. 1.

2) 금융정보화추진분과위원회, "1998년도 금융정보화촉진 시행계획", 한국은행, 1997.

3) 정보통신부, "네트워크 보안관리 지침서", 1996. 12.

4) 주재훈, "SET표준과 우리 나라 인증기관의 구성방안", 동국대학교, 한국정보시스템학회 추계학술발표 논문집, 1997. 11.

5) 한국전산원, "93년도 국가기간전산망 사업 추진실적 및 전산자원 현황", 1994. 12, http://ncalib.nca.or.kr/HTML/1994/94840/94840.htm

6) Bellare M., et al., "iKP - A Family of Secure Electronic Payment Protocols", Proc. 1st USENIX workshop on Electronic Commerce, New York, NY, July. 1995, http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html

7) Clifford Neuman, B., and G. Medvinsky, "Requirements for Network Payment: The NetCheque perspective", Proc. IEEE Compcon '95, San Francisco, CA, Mar. 1995, http://nii.isi.edu/info/netcheque/documentation.html

8) Clifford Neuman, B., "Security, Payment, and Privacy for Network commerce", IEEE Journal. 1996.

9) D. O'mahony, M. Peirce, H. Tewari. , "Electronic Payment Systems", Artech House, London, 1997.

10) DEPARTMENT OF DEFENSE, "Trusted Computer System Evaluation Criteria", Dec. 1985, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

11) Europay International S.A., MasterCard International Incorporated, and Visa International Service Association, "EMV '96: Integrated Circuit Card Specification for Payment Systems", June 1996, http://www.mastercard.com/emv/

12) Financial Services Technology Consortium, About the FSTC, U.S.A., 1995, http://www.fstc.org/about.html

13) Ford, Warwick, 'Computer communications security', Prentice Hall, New Jersey, 1994.

14) Kalakota, R. and Whinston, A., "Frontiers of Electronic Commerce", Addison Wesley, Messachusetts, 1995.

15) Rivest, R., and A. Shamir, PayWord and MicroMint: Two Simple Micropayment Schemes, Maym 1996, http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps