가상사설통신망 기반 금융전산망 구축 방안

Construction of Financial Networks based on Virtual Private Networks

서문석
대불대학교 컴퓨터응용기술학과

Moon-Seog Seo(msseo@mail.daebul.ac.kr)

요약

자본시장통합법 시행을 계기로 다수의 금융투자회사들이 지급결제서비스 제공을 위해 금융전산망에 추가로 참가하고 있다. 국가 기간 전산망 중의 하나인 금융전산망은 다수의 금융기관을 하나의 통신망으로 연결하여 전자금융서비스를 제공하는 정보통신망으로 금융투자회사들의 신규 참여에 유연하게 대처할 수 있어야 한다. 금융전산망이 경제에 미치는 영향이 지대하므로 금융전산망의 구축 및 운영에는 신용리스크, 유동성리스크 및 운영리스크 등과 같은 다양한 리스크 관리를 요구하고 있다. 본 논문에서는 안전성, 적정 응답성, 경제성 및 안정성 등의 금융전산망의 안정적 운영과 관련한 운영리스크 관리기준을 제시하고 급변하는 금융환경 변화에 효율적으로 대처할 수 있도록 많은 기업들이 기업통신망으로 활용하고 있는 가상사설통신망(Virtual Private Network : VPN) 기술을 금융전산망에 적용한 구축방안을 제안하였다. 또한 제안된 VPN 기반의 금융전산망이 비용 및 운영상의 효율성을 유지하면서 높은 안전성 및 적정 응답성을 갖고 있는지 분석하여 VPN 기술이 금융전산망에 적용 가능함을 보였다.

■ 중심어 : | 금융전산망 | 자본시장통합법 | 금융투자회사 | 가상사설통신망 | 운영리스크 관리 |

Abstract

As enactment and enforcement of capital markets integration law, investment banks are going to be appeared in our financial market and be able to provide payment services. To provide these kinds of services, investment banks need to be participated in the financial network. As the financial network enormously affect the economy, the operation of the network will require a variety of risk managements. In this paper we define operational risk management criteria for the financial network such as security, in-time response, economical efficiency and stability to be required for the healthy economy and propose the configuration of the financial network system based on virtual private networks for investment banks to provide payment services. Finally we analyze that the proposed VPN configuration for financial networks has high security and in-time response with the cost and operation effective.

■ keyword : | Financial Network | Investment Banks | Virtual Private Networks | Operational Risk Management |

I. 서 론

국가 기간 전산망 중의 하나인 금융전산망은 다수의 금융기관을 하나의 통신망으로 연결하여 새로운 전자금융 서비스 제공이 가능한 정보통신시스템이다. 통신망 구축 이후 이를 이용한 전자금융 업무의 활성화로

접수번호 : #090429-002
접수일자 : 2009년 04월 29일
심사완료일 : 2009년 05월 15일
교신저자 : 서문석, e-mail : msseo@mail.daebul.ac.kr

막대한 자금의 흐름이 이루어지고 있으며 경제 전반에 걸쳐 막대한 영향을 미치고 있다[1]. 2009년 2월 자본시장통합법 시행을 계기로 제2금융권에 속해있는 금융기관들이 금융투자회사로 전환됨에 따라 이들 금융기관들이 지급결제서비스를 제공할 수 있는 법, 제도적 여건이 조성되었다. 금융투자회사들이 금융기관 간 송금, 결제 등과 같은 서비스를 제공하기 위해서는 필요한 전산설비 및 통신 인프라 등 기반 설비를 갖추고 금융전산망에 접속하여야 한다. 금융전산망은 경제에 미치는 파급효과가 크기 때문에 신용리스크, 유동성리스크와 같은 금융리스크 관리뿐만 아니라 전산설비, 전기설비 및 건물 등의 운영관리 실패에 따라 발생할 수 있는 운영리스크의 적절한 관리가 요구된다. 다수의 금융투자회사 들이 지급결제서비스 제공을 위해 금융전산망에 추가로 참가함에 따라 이에 유연하게 대처할 수 있는 통신망의 구성이 필요하며 금융전산망 구축 시 운영리스크 관리 측면에서 안전성, 응답성, 경제성 및 안정성이 확보된 시스템을 구축하는 것이 중요하다[2][3].

정보통신 및 정보보호기술의 발달로 기업들은 경제적이면서도 안전한 가상사설통신망(Virtual Private Network : VPN) 기술을 활용하여 기업 통신망을 구축 운영하고 있다[6]. 본 논문에서는 이러한 VPN 기술을 활용하여 금융전산망을 구성하고 운영리스크 관리 측면에서 VPN기술이 금융전산망에 적합한지 분석하고자 한다. 2장에서는 자본시장통합법 시행으로 급변하는 금융환경과 금융전산망 현황 그리고 VPN 관련 기술에 대해 살펴보고 3장에서 VPN을 기반으로 하는 금융전산망 구축 방안을 제안하고자 한다. 4장에서는 운영리스크 관리기준에 따라 제안된 VPN 기반 금융전산망의 타당성을 분석하고자 한다.

II. 금융전산망 현황 및 VPN 관련 기술

1. 금융전산망 현황

자본시장통합법의 시행으로 급격한 변화가 예상되는 금융환경에 대해 금융기관의 구성과 금융기관별로 제공되는 금융서비스의 변화에 대해 살펴보고자 한다. 금융기관은 영위하는 업의 종류에 따라 제1금융권, 제2금융권 및 제3금융권으로 분류 할 수 있다. 제2금융권이란 은행을 제1금융권이라고 하는데 반해, 은행을 제외한 금융기관을 통칭하여 부르는 명칭이다. 제1금융권에는 특수은행과 일반은행 및 지방은행 등이 있으며, 주로 제도권 금융기관에서 대출이 힘들 때 이용하는 사채업 등의 금융권을 제3금융권이라고 부른다. 자본시장통합법 시행을 계기로 금융투자업의 겸영이 허용됨에 따라 모든 금융투자업을 종합 영위하는 금융투자회사의 설립이 가능하게 되었다. 이는 전체 금융기관이 은행을 중심으로 한 제1금융권과 금융투자회사 그리고 보험사 등으로 재편성되어질 수 있음을 의미한다. 금융투자회사들은 은행권을 중심으로 구성되어진 지급결제시스템에 가입하여 신용카드 대금 결제, 지로납부, 자동이체 등과 같은 결제업무와 계좌이체, CD/ATM에 의한 수시입출금 등 종합 금융서비스의 제공이 가능하다[4]. 경제주체들이 수표, 어음 및 신용카드 등의 지급수단을 사용하는 경우에는 해당 금액을 지급해야 할 사람의 예금계좌에서 받을 사람의 예금계좌로 금융전산망을 통해 자금을 이전하는 금융기관 간 자금이체라는 별도의 결제 및 청산 절차를 거쳐야 지급결제가 완료된다[3].

금융전산망 사업은 주로 파급효과가 큰 은행 간 전산망 구축에 중점을 두어 추진되어 왔으며, 은행을 제외한 금융기관들도 금융전산망의 일환으로 추진되고 있다. 지급결제서비스 중심의 금융서비스 처리를 위한 금융전산망은 은행 업무의 온라인 처리를 위해 은행 본지점간을 전용회선을 이용하여 연결한 은행내부 전산망과 타행환업무, CD(Cash Dispenser)공동망 업무 등 은행 간 거래 또는 은행 공동 업무 처리를 위해 은행의 본점 Host와 공동망센터의 Host를 Point-to-Point 방식으로 연결한 은행 간 전산망으로 구성되어 있다[1].

금융전산망 구성 시에는 신뢰성 확보를 위해 적정 응답시간을 만족하도록 필요한 회선 용량을 배정하고, 안전성 확보를 위해 회선 장애 시에도 원활한 업무 처리가 가능하도록 별도의 백업 회선을 설치하여 운영하고 있다. 전통적으로 금융기관은 TCP/IP 프로토콜 자체의 취약성, 개방형 네트워크의 안전성을 이유로 인터넷의 접속을 꺼려왔으나 인터넷의 발전으로 인터넷 뱅킹 등

인터넷을 기반으로 하는 금융업무가 개발되어 금융기관의 인터넷 연결이 보편화됨에 따라 [그림 1]과 같이 은행 계정 시스템과는 별도로 외부 망에 접속하여 대외업무를 처리하고 있다.

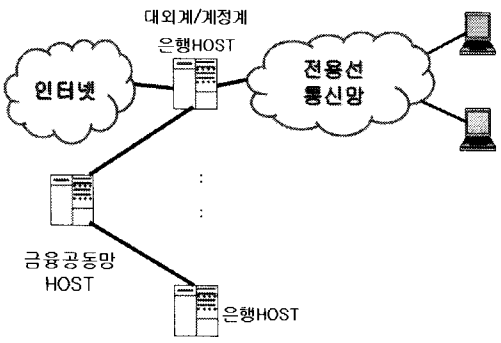

그림 1. 금융전산망 네트워크 구성

2. VPN 관련 기술

기업들이 효율적인 통신망 구성을 위해 활용하고 있는 VPN 관련 요소기술 및 다양한 VPN 솔루션들의 구성내역 등에 대해 살펴보고자 한다.

2.1 VPN의 요소 기술

VPN의 핵심 기술들로는 터널링, 인증, 접근제어, 데이터 기밀성 기술들을 들 수 있으며, 가장 중요한 것으로는 가상의 네트워크를 구성할 수 있도록 해 주는 터널링 기술이 있다. 터널링은 임의의 데이터 패킷(내부 패킷)을 다른 패킷(외부 패킷)으로 캡슐화 하는 것으로 외부 패킷이 라우팅 되는 네트워크에서 내부 패킷의 의미를 상실하게 되는 것을 의미한다. 캡슐화란 하나 이상의 프로토콜 레이어가 반복되는 것을 말하며, 이러한 터널링의 필요성은 내부 패킷이 다른 프로토콜 네트워크로 다수의 프로토콜을 전송하거나, 원래 패킷의 송수신 주소를 감추거나 또는 보안을 위해 내부 패킷을 암호화 하는 등 여러 가지 이유로 네트워크를 가로질러 직접 여행할 수 없는 경우에 적용될 수 있다. 터널링은 어떤 통신계층에도 적용 가능하나 일반적으로 PPTP(Point-to-Point Tunneling Protocol), L2F(Layer Two Forwarding) 및 L2TP(Layer two Tunneling Protocol) 등과 같이 데이터 링크 계층에 적용되는 것과 IPSec과 같이 네트워크 계층에 적용되는 것이 있으며 최근에는 트랜스포트 계층에 적용된 SSL(Secure Socket Layer) VPN이 주목을 받고 있기도 하다[7-9].

사설(Private) 통신이 이루어지기 위해서는 통신전에 상대방의 신원을 확인하여야 하며 이러한 통신 실체의 검증 절차를 인증이라고 부른다. 인증은 데이터를 송신했다고 주장하는 사람이 보낸 것이 정당함을 보장한다. 인증 방식에는 신뢰할 수 있는 제3자의 개입여부에 따라 Two party 인증과 Trusted third party 인증방식으로 분류될 수 있으며, Trusted third party 인증에서 가장 중요한 인증 방법으로는 공개키 기반 구조(Public Key Infrastructure)가 있다. 인증이 완료된 후 통신 당사자들은 통신 채널을 통해 자원에 대해 접근을 요청할 수 있으며 통신의 종단점은 이러한 접근 요청을 수용할지 여부를 결정하여야 한다. 접근제어 프로세스는 두가지 측면을 가지고 있으며 하나는 접근 제어 결정이 이루어질 정보와 접근제어 결정이 정보를 이용하여 어떻게 결정되는 가이다. 사설 통신이 비밀스럽게 이루어질 필요가 있는 경우 적용 가능한 요소기술이 자료의 기밀성 유지이다. VPN은 공유 자원을 이용하여 사설 정보를 제공하기 때문에 데이터가 전송 도중 다른 사람들에 의해 변경되거나 노출될 수 있다. 이를 방지하기 위해 암호화 및 무결성 서비스가 VPN을 통해 전송되는 데이터에 적용되어야 한다[6].

2.2 VPN의 구성요소

VPN을 구축하기 위해서는 VPN의 요소기술들이 적절한 방법으로 구현된 장비가 필요하다. 이를 위해서는 터널의 종단점에서 수행되어야하는 기능들을 결정하고 이들을 구현하는 것이 중요하다. VPN을 구성하는 것 중 가장 일반적인 것이 VPN 게이트웨이이다. 터널의 종단점이 이곳에서 형성되며 다른 한 끝이 상대방 VPN장비에서 설정된다. VPN 게이트웨이는 보호되어야할 기업 내부의 자원을 위해 이들을 연결하는 기업 네트워크에 설치되어 보안서비스의 창구역할을 수행한

다. 일반적으로 VPN 요소기술에서 언급한 터널링, 인증, 접근제어 및 데이터 기밀성 기술들이 함께 구현되며 두 개 이상의 네트워크 인터페이스를 갖는 다중 홈 시스템 형태이다. 이는 인바운드 데이터에 대해 보안정책에 따라 필터링을 하여 터널로부터 들어오는 데이터에 대해 필요한 처리를 수행한다. 터널링 처리를 하기 전에 터널확립을 위한 협상이 상대방 VPN 장비와 이루어져야 한다. 내부 네트워크에서 생성되어 인터넷으로 나갈 아웃바운드 데이터에 대해서도 정책에 따라 필요한 처리가 이루어져야 한다. 터널링이 요구되는 경우 터널을 새롭게 확립해야 하며 차후 터널을 통과하는 데이터에 대해서는 터널 규칙에 따라 처리되어야 한다.

또 하나의 VPN 구성요소로는 사용자가 자신의 컴퓨터를 통해 원격에서 VPN에 접근하기 위해 사용하는 소프트웨어형의 VPN 클라이언트가 있다. 일반적으로 VPN 클라이언트는 사용자 컴퓨터로부터 지정 VPN 게이트웨이까지 안전한 경로를 생성한다. VPN 클라이언트의 경우도 VPN 게이트웨이와 같은 기술요소들이 구현되어 있어야하나 선택적인 요소들은 생략되어질 수 있다. VPN 게이트웨이가 전용 하드웨어에 구현되고 전문가에 의해 운영되는 반면 VPN 클라이언트는 범용 운영체제 상에서 응용프로그램의 하나로 수행되고 일반 사용자가 사용함에 따라 설치 및 사용이 간단해야할 필요가 있다.

Ⅲ. VPN 기반 금융전산망 구축

1. VPN 기반 금융전산망 구성

VPN을 구축하는데 있어 필수적인 것은 이를 구축하고자하는 조직의 통신 요구사항을 충족하며 구축 후 원활한 관리가 이루어 질 수 있도록 구성요소들을 올바로 조직하는 것이다. VPN의 구축은 인트라넷 VPN, 원격접속 VPN 및 엑스트라넷 VPN 등 3가지 구성 모델로 나누어 생각해 볼 수 있다.

인트라넷 VPN은 하나의 조직 내에서 지리적으로 다른 곳에 다중의 사이트들이 위치하여 운영되는 경우 이들을 VPN으로 연결하고자 할 때 적용가능하다. 각각의 사이트들은 다중 서브네트워크들로 이들의 상호연결이 하나의 인트라넷을 구축하게 되며 VPN은 이러한 사이트들을 상호 연결하여 하나의 네트워크를 형성한다. 개별 금융기관 내에서 각각의 지점들을 서브네트워크로 구성하고 본점에 설치된 VPN 게이트웨이에 연결함으로써 금융기관 전용 인트라넷 VPN을 구성할 수 있다.

원격접속 VPN은 전화망을 통해 접속을 요구하는 모바일 컴퓨터, 케이블 모뎀 또는 DSL(Digital Subscriber Line)을 통해 접근을 요청하는 원격 컴퓨터 등을 연결하기 위해 사용된다. 원격 컴퓨터는 VPN 클라이언트를 이용하여 내부 네트워크에 설치된 VPN 게이트웨이와 터널을 확립하고 내부 자료에 접근하게 된다. 금융기관 직원들이 원격에서 금융기관 내부 네트워크에 접속코자 하거나 일정수준 이상의 일반고객을 대상으로 특화된 서비스를 제공하고자 하는 경우 원격접속 VPN을 활용할 수 있다.

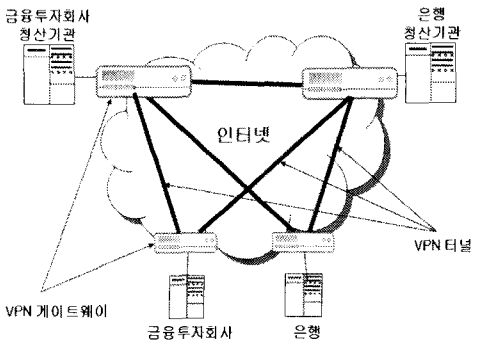

그림 2. VPN 기반 네트워크 구성

엑스트라넷 VPN은 조직 내의 네트워크 자원이 협력사, 하청업체 등 서로 관계가 있는 다른 기업들에 접근을 허용해야할 경우 구축되어질 수 있다. 엑스트라넷 VPN에서는 다른 구축 방법에 비해 좀 더 복잡한 인증 및 접근제어를 수행해야할 필요가 있다. 또한 기업관계는 동적으로 변경될 가능성이 높기 때문에 가상 네트워크 구성 역시 동적 구성이 용이하여야 한다.

금융전산망의 금융기관 간 전산망은 [그림 2]와 같이 공유 네트워크인 인터넷 상에서 VPN을 활용한 엑스트라넷 구성 모델이 가장 적합하다고 할 수 있다. 금융투

자회사의 전산센터 및 은행 전산센터에 VPN 게이트웨이를 설치하고 청산기관별로 VPN 게이트웨이를 설치하여 모든 청산기관들과 지급결제 참가기관들 간에 VPN 터널을 구성함으로서 가상사설통신망 기반의 금융전산망 구성이 가능하다. 이는 금융투자회사들과 은행들의 구분 없이 지급결제서비스 처리를 위해 모든 관련기관들을 중복하여 중계센터인 청산기관에 직접 접속하는 효과를 가진 통신망을 구성한 것이다. 청산기관들 간의 연결에는 VPN을 기반으로 구성하는 것이 가능하고 사설 전용 통신망을 이용하는 것도 가능하다.

2. VPN 기반 통신망 구성 시 업무처리 흐름

금융투자회사 및 은행들이 VPN을 기반으로 통신망을 구성한 경우 모든 참가기관들이 하나의 청산기관만을 경유하는 시스템으로 구성되어진다. 이에 따라 지급결제서비스의 처리흐름은 [그림 3]에서와 같이 기존 은행 지급결제시스템의 지급결제 처리와 동일한 흐름을 가질 수 있다.

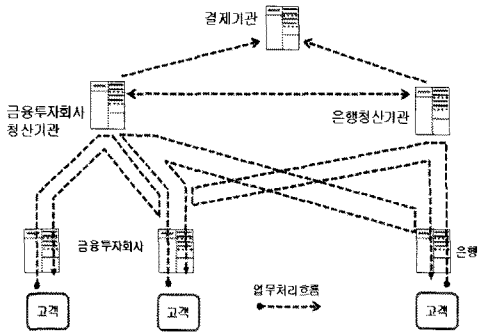

그림 3. VPN 기반 지급결제서비스 처리흐름

그러나 지급결제 정보가 금융권별 청산기관에 분산되어 축적되기 때문에 금융권별 청산기관 간 차액결제 정보의 교환 및 확인 작업이 요구되어 진다. 차액결제 업무는 지정 시점에 일괄 처리되어짐으로 고객에 대한 응답시간에 영향을 미치지 않고 청산기관간의 처리 부담만 존재한다. 다만 고객의 지급결제 요청 시 요청정보를 어느 청산기관으로 보낼 것인지가 결정되어져야 하는데 이는 참가기관의 해당 금융권별 청산기관으로 송신한다면 문제가 없다. 즉, 은행에서 발생한 지급결제 요청정보는 은행 청산기관으로 전송하고 금융투자회사에서 발생한 지급결제 요청정보는 금융투자회사의 청산기관으로 전송하면 된다.

3. 외국의 금융망 VPN 적용 사례

SWIFT(Society for Worldwide Interbank Financial Telecommunication)는 전 세계 198개국 7,000개 금융기관들이 가입해 있는 국제은행간 전기통신협회로 국제은행간 통신망인 SWIFTNet을 통해 결제 정보, 각종 보고서, 및 증권 정보 등 같은 중요한 금융거래정보 등을 전송하고 있다[11][12].

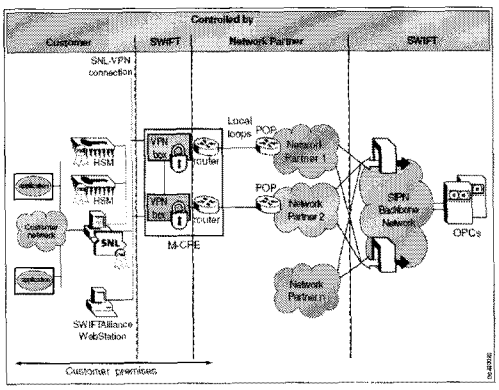

그림 4. SWIFTNet 구성도

SWIFT는 2001년부터 2005년 사이에 자신의 Backbone 네트워크를 전용회선 기반의 X.25 기반구조에서 현재의 SWIFTNet으로 알려진 HSM(Host Security Module), VPN 등과 같은 보안장비를 활용한 안전한IP(Inetrnet Protocol) 네트워크 기반구조(SIPN : Secure IP Network)로 전환하였으며 회원사들이 SWIFTNet에 접속하기 위해서는 [그림 4]와 같이 VPN 장치를 회원사의 역내에 설치하여 SWIFT의 SIPN Backbone 네트워크에 접속하여야 한다. VPN 장치는 SWIFT 운영센터와 회원사 간에 통신경로를 IPSec(IP Security) 표준을 기반으로 암호화 및 인증 처리하여 안전성을 확보하고 있다. SWIFT의 회원사가 VPN을 설치하기 위해서는 SWIFT의 요구조건에 부합하는 장치

를 설치할 필요가 있으며 SWIFT는 이를 위해 다수의 VPN 장치에 대한 성능검사를 통해 협력사를 선정하고 이들을 회원사에 추천하고 있다. 회원사는 이들 중 자신의 처리수준에 부합하는 장치를 선정하여 설치, 운영할 수 있다[11]. 이는 국내 금융전산망에 VPN을 적용하고자 하는 경우에 좋은 운영모델이 될 수 있다.

Ⅳ. 금융전산망에 VPN 적용의 타당성 분석

금융전산망 시스템 구성의 타당성은 운영리스크 관리를 위해 필수적으로 요구되어지는 사항을 기준으로 분석할 수 있다. 운영리스크 관리 기준으로는 금융서비스 업무의 처리흐름 중 권한 없는 자의 불법접근을 막아 정보의 노출을 제어하는 안전성(Security), 고객의 편의를 위해 주어진 시간 안에 금융업무 처리가 완성되어 질 수 있는 적정 응답성(In-time Response), 시스템 구축 및 운영에 있어 적절한 비용의 투자로 지급결제 참가기관 및 고객의 경제적 부담을 줄이는 경제성(Economical Efficiency) 및 장애발생을 최소화 하고 파업 등으로 인한 서비스 중단 없이 지속적인 서비스 제공을 가능하게 하는 안정성(Stability) 등이 있다.

본 장에서는 이러한 운영리스크 관리기준에 의거 VPN 기술이 금융전산망의 통신망 구성에 타당한지 여부를 검토하고자 한다.

1. 안전성 분석

VPN의 터널링 기술로 IPSec을 활용하는 경우 AH(Authentication Header)와 ESP(Encapsulation Security Payload) 프로토콜의 사용이 가능하며 제공되는 보안서비스는 [표 1]과 같다.

표 1. IPSec 보안 서비스

서비스	AH	ESP	AH+ESP
접근제어	O	O	O
무결성	O		O
발신처 인증	O		O
기밀성		O	O
재전송 패킷 거부	O	O	O

이를 통해 VPN 기반 금융전산망에서 송수신되는 메시지에 대한 보안서비스가 이루어지며 안전성 측면에서는 기존의 전용회선을 이용한 구성방식이 통신회선 제공자 및 해커에 의해 통신회선에 대한 직접 감청방식으로 금융정보의 노출이 가능한 반면 VPN 접속의 경우 [그림 5]에서와 같이 인터넷의 종단 간에서 송수신되는 모든 정보가 암호화되므로 통신회선의 감청에 의한 정보 노출을 막을 수 있어 안전성이 높다.

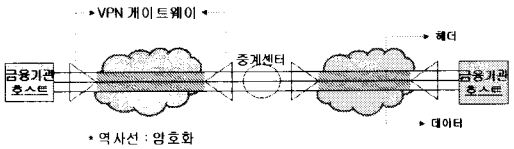

그림 5. VPN 터널링에 의한 정보보호

VPN에 적용하는 암호의 안전성은 암호화 알고리즘과 암호키에 의존적이며 이는 국제적으로 인증된 암호 알고리즘의 사용, 고수준의 암호키 길이 사용 및 공개키 기반 구조의 활용 등으로 검증될 수 있다.

2. 응답시간 분석

금융전산망에서 고객의 금융서비스 요청은 적정 시간 안에 처리되어야만 고객으로부터 신뢰를 얻을 수 있으며 금융기관은 이를 위해 고객의 요청이 적정 응답시간 안에 처리될 수 있도록 필요한 시스템 및 통신망을 설계하고 있다.

전용회선 기반의 금융전산망에서 금융서비스의 처리시간 T_t은 식 (1)과 같다.

$$T_t = T_b + T_s \quad (1)$$

T_t : 총처리소요시간
T_b : 네트워크지연시간
T_s : 시스템처리지연시간

VPN을 기반으로 하는 금융전산망에서의 금융서비스의 처리시간 $T_{t'}$은 식 (2)와 같이 나타낼 수 있으며, 여기서 VPN 처리지연시간 T_v 는 식 (3)과 같이 계산될 수 있다.

$$T_{t'} = T_v + T_b + T_s \quad (2)$$

T_v: VPN처리지연시간

$$T_v = T_p \times Path \times 2 \quad (3)$$

T_p: $Packet$처리시간

$Path$: 메시지통신경로

금융기관 간 통신망을 VPN 기반으로 구성한 경우 금융서비스 처리를 위한 요청 및 응답 메시지의 이동 경로인 $Path$는 중계센터를 경유하기 때문에 4로 정의 할 수 있다. 단일 VPN 게이트웨이에서 패킷 처리시간은 1Gbps 네트워크에 연결된 Intel P3 프로세서 시스템에 VPN의 IPSec 가속기를 연결하여 3DES+SHA로 디코딩하는 경우 Packet의 크기별로 50Kbyte의 파일을 처리하는데 소요되는 총 처리시간을 검사하여 단위 패킷의 평균처리시간을 구한 [표 2]를 기준으로 계산할 수 있다[5]. 이를 적용한 금융전산망에서의 VPN 처리지연시간은 식 (4)와 같다.

$$T_v = 1.333 \times 4 \times 2 = 10.664\ msec \quad (4)$$

VPN 기반 금융전산망에서의 금융서비스 총 처리시간은 식 (5)에서와 같이 전용회선 기반의 금융전산망보다 $10.664\ msec$ 더 소요된다고 할 수 있다.

$$T_{t'} = T_t + 10.664\ msec \quad (5)$$

국내 금융기관간 업무 처리방식과 유사한 SWIFTNnet의 InterAct 서비스에서 적용하고 있는 보안장치인 HSM의 TPS(Transactions Per Second)를 1로 권장하고 있는 것에 비교해서 VPN은 94 TPS로 전체 처리소요시간에 미치는 영향이 적고 고객의 응답시간 지연에 미치는 영향도 미미하다고 할 수 있다[11].

표 2. 패킷크기에 따른 처리시간 [5]

(단위 : msec)

Packet 크기 (byte)	디코딩 회수	디코딩 지연	총디코딩 지연	총처리 시간	평균처리 시간
128	391	0.5	195.5	196.833	1.333
256	196		98.0	99.337	
512	98		49.0	50.333	

3. 경제성 및 안정성 분석

경제적인 측면에서 모든 금융기관을 개별 금융기관별로 전용회선을 이용하여 통신망을 구성한 기존의 통신망 구성 방식보다 단일 혹은 이중 회선으로 인터넷에 접속하는 VPN 기반 통신망 구성이 적은 회선 및 장비 비용으로 구축 및 운영비용 측면에서 경제적인 효과를 기대할 수 있다. 은행 및 금융투자회사들이 금융권별로 통신망을 구성할 수 있기 때문에 특정 청산기관의 시스템 장애 또는 파업에 따른 서비스 중단에 능동적으로 대처할 수 있으며 각 금융권별 별도의 백업센터 구축 없이 원활한 백업이 가능하여 금융서비스의 안정적인 운영이 가능하다.

위와 같은 운영리스크 관리기준에 의거 기존의 전용회선 기반 금융전산망과 본 논문에서 제시한 VPN 기반 금융전산망을 상대적으로 비교해 보면 [표 3]과 같이 요약할 수 있다.

표 3. 접속방안별 상대비교

(◎:상, ○:중, ×:하)

구 분	전용회선 접속	VPN 접속
안 전 성	○	◎
응 답 성	◎	○
경 제 성	×	◎
안 정 성	○	◎

V. 결론

본 논문에서는 금융환경의 변화로 금융투자회사들이 지급결제서비스 제공을 위해 금융전산망에 참여하고 있는 시점에서 금융전산망의 운영리스크를 최소화하기 위한 금융전산망 구성방안을 제시하고 운영리스크 관리 기준에 따라 분석해봄으로써 제안 방안의 타당성을 검증하고자 하였다.

금융전산망이 경제, 사회 전반에 미치는 영향이 지대하므로 운영리스크를 최소화하여야 하며 이를 위해 시스템 구축 시 안전성, 경제성, 적정 응답성 및 안정성의 구축 목표를 달성하는 것이 중요하다. 본 논문에서는 금융투자회사 및 은행들이 개별 청산기관에 직접 접속

하여 업무처리 시 하나의 청산기관만을 경유하도록 통신망을 구성하기 위해 전용회선 기반의 통신망을 이용하는 대신 공유 네트워크인 인터넷 상에서 VPN을 활용하여 금융전산망을 구성하는 방안을 제안하였으며 이 방안이 경제적이면서도 안전하며 고객에 대한 적절한 응답성 확보가 가능한 방안임을 검증하였다. 금융서비스 제공을 위한 통신망에 VPN의 적용은 SWIFTNet의 예에서도 볼 수 있듯이 안전성이 검증되었다고 할 수 있으며 이러한 시스템 구성은 금융권별 통신망의 백업시스템 역할도 수행할 수 있어 안정성 확보에도 기여할 수 있을 것으로 판단된다. 향후 구성방안의 실현 단계에서 경제적 효용성의 계량화된 분석이 추가적으로 이루어질 필요가 있다.

참 고 문 헌

[1] 금융결제국, *2006년도 금융정보화 추진 현황*, 한국은행, 2007.

[2] 한국은행, *미국 소액결제시스템에서의 비은행기관 참가와 리스크 관리*, 지급결제정보 제2007-9호, 2007.

[3] 금융결제국, *지급결제의 이해*, 한국은행, 2008.

[4] 이명훈, *전자금융의 발달과 경제정책의 새로운 패러다임*, 집문당, 2003.

[5] 윤연상, 류광현, 박진섭, 김용대, 한선경, 유영갑, "기가급 VPN을 위한 IPSec 가속기 성능분석모델", 한국정보보호학회논문지, 제14권, 제4호, pp.141-148, 2004.

[6] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, and A. Malis, *A Framework for IP-Based Virtual Private Networks*, Informational Request for Comments 2764, 2000(2).

[7] Microsoft, *Understanding Point-to-Point Tunneling Protocol(PPTP)*, Microsoft Windows NT Server White Paper, http://www.microsoft.com/NTServer/comserv/tecdetails/prodarch/understanding_pptp.asp, 1997.

[8] Ould-Brahim, B. Gleeson, G. Wright, T. Sloane, R. Bach, R. Bubenik, and A. Young, *Network Based IP VPN Architecture using Virtual Router*, Internet-Draft, Jul. 2000.

[9] B. Patel, Aboba, *Securing L2TP using UPsec*, Internet-Draft, 1999(2).

[10] J. Shriver, *IPsec DOI Textual Conventions MIB*, Internet-Draft, 2001(6).

[11] SWIFT, *SWIFTNet Connectivity Packs*, 2007(2).

[12] SWIFT, *SWIFTNet Connectivity Implementation Service Overview*, 2007(2).

저 자 소 개

서 문 석(Moon-Seog Seo) **정회원**

- 1988년 2월 : 단국대학교 전자계산학과(이학사)
- 2000년 2월 : 한국정보통신대학교 정보보안(공학석사)
- 1989년 4월 ~ 2000년 3월 : 금융결제원 연구역
- 2000년 4월 ~ 2002년 8월 : 시큐아이닷컴 부장
- 2002년 9월 ~ 현재 : 대불대학교 컴퓨터응용기술학과 교수

<관심분야> : 전자금융, 공개키기반구조, 암호이론