International Commerce and Information Review
Volume 16, Number 1, February, 2014: pp. 207~226
통상정보연구 제16권 1호 (2014년 2월 27일)

논문투고일자 : 2013. 11. 22
심사(수정)일 : 2013. 12. 14
게재확정일자 : 2014. 02. 22

전자무역의 글로벌 네트워크 개방시스템 상호연결 활용에 관한 연구*

The Use of Open Global Network System Interconnection in E-Trading

정분도(Boon-Do Jeong)
조선대학교 무역학과 교수(주저자)

윤봉주(Bong-Ju Yun)
조선대학교 무역학과 강사(교신저자)

목 차

Ⅰ. 서 론
Ⅱ. OSI 체재 데이터 전송
Ⅲ. OSI 체재 7계층 분석
Ⅳ. 요약 및 결론
참고문헌
ABSTRACT

국문초록

현재 활용되고 있는 OSI(Open System Interconnection) 체재하의 무역 관련 물류정보화 시스템으로는 항공관제시스템, 항만운영정보시스템, 해운·선원정보시스템, 수출입일괄처리시스템 등이 있는데 이들 시스템들은 우리나라 물류 관련 산업의 운영체계를 보다 편리하고 효율적으로 개선시키는데 많은 부문에 기여하고 있다. 그렇지만 운영 측면에서는 전자문서의 폭발적인 송수신 폭주로 네트워크의 기술적인 문제점들이 적잖게 노출되어 있다. 우리나라가 물류의 정보중심지로 성장하기 위해서는 글로벌 체재속의 IT기술 중 네트워크를 이용한 제어기법들을 충분히 활용하여야 할 때이며 수출입 물류체계를 한층 더 신속 및 정밀화시켜 고도화 단계로 성장시켜야 할 때이다. 따라서 본 논문의 핵심은 OSI 체재하의 전자무역 네트워크의 효율적인 운영을 위하여 부문별 종합 네트워크와 데이터 단위전송의 침입탐지시스템 등의 관리방법 등을 제시하고자 한다. 본 논문에서는 네트워크 기능 배분에 따른 조직과 인력의 조정, 사무의 위임전결 등 내부조직의 합리화 방안과 관련법규의 정비 등은 연구범위에 포함하지 않았다. 그러므로 본 논문은 OSI 체재하의 무역 관련 네트워크를 실무적 관점에서 살펴보고, 향후 해석적 기초를 제시하는데 그 목적을 두었다.

주제어 : 전자무역, 글로벌 네트워크, 개방시스템 상호연결(OSI), 침입탐지시스템, 네트워크 관리.

* 이 논문은 2013학년도 조선대학교 학술연구비의 지원을 받아 연구되었음.

Ⅰ. 서 론

OSI 체재하에서 우리 정부는 물류의 선진화를 위해 물류산업의 위상에 걸맞도록 동북아시아 물류거점화 정책을 다각적으로 추진해 가면서 물류종합 네트워크망을 단계적으로 구축해 가고 있다. 항만해운물류와 관련된 네트워크는 항만관리정보시스템, 국토교통부의 종합물류망과 항공관제시스템, 관세청의 통관망 등을 대표적으로 들 수 있다. 항만관리정보시스템은 출입국관리사무소 및 각 검역소 등 해운물류산업과 관련된 정부기관과 국제 선사 등과 연계되어 각종 정보를 상호 교환하고 있으며, 전국 28개 항만을 전자식 단일 네트워크로 구축 완료하였다. 항만관리정보시스템을 근간으로 한 물류EDI 네트워크가 1999년에 통관·무역 네트워크와 연결되면서 수출입 관련기관(CIQ)과 정보를 공동 활용할 수 있게 되었으며 입출항시 필요한 18종의 필수서류를 9종으로 대폭 통합하고 전국 어디서나 한번 전송으로 모든 수출입 항만 업무를 마무리할 수 있는 온-스톱 서비스를 하고 있다. OSI 체재하에서 해운물류종합 네트워크를 용도별 측면에서 살펴보면, 항만관리정보시스템과 물류관련기관 및 업계간 표준화된 서식과 전자문서를 이용하여 컴퓨터간 정보를 교환하는 복합시스템인 물류EDI시스템 등으로 구성되어 있음을 알 수 있다.

네트워크를 주 활용 수단으로 이용하는 물류·유통 산업이 경쟁력을 확보하기 위해서는 항공사, 선사와 전문 물류업체 등과 자유롭게 종합정보네트워크를 공유 및 연계하여야 한다. 또한 이를 통해 운송, 통관, 보관, 부가서비스 등 다각적인 물류활동을 편리하고 신속하게 처리할 수 있는 네트워크 기반을 조성해야 할 필요성이 있다. 따라서 수출입, 통관, 물류활동을 통합적으로 지원하는 효율적인 네트워크 정보시스템은 필수적이라 할 수 있다(박광로 외, 2000)[1].

업무개선에 따른 부가적 효과는, 처리절차 간소화 및 양식 폐지, 국고수납 자동화에 따른 비용절감, 통합 데이터베이스구축 효과, 기관정보의 공동 활용, 검역기관 EDI 도입효과 등으로 직간접적으로 국가 경제에 이바지 하고 있다. OSI 체재하에서 항만운영정보시스템 중에 무선망을 통한 선박입출항, 수출입 컨테이너 신고업무, 웹 기반의 해운물류 민원사무 처리시스템 등은 우리나라의 물류체계를 대폭 개선하고 관련 산업을 집중적으로 개발 및 육성시켜 동북아시아 주요 허브로 부상시키려는 것이 그 의도라 할 수 있다.

민간 주도 네트워크는 현재 물류EDI시스템을 매개로 하여 업체간 정보를 상호 교환하고

1) 박광로 외, “홈 게이트웨이 기술”, 「한국통신학회지」, Nov. 2000, 한국통신학회, 2000.

있는데 부가통신망(VAN) 사업자인 삼성SDS, 대한통운, 한진, SK 등의 공차중계, 화물알선 등 물류관련 서비스 제공, 한국물류정보통신(KLNet)과 같이 항만 및 물류 관련업체들이 많이 이용하는 시스템과 무역망 및 통관망 전담사업자로 무역 및 통관EDI, 관련 DB서비스, 항공부문 물류정보서비스 제공 등을 하는 한국무역정보통신(KTNET)과 같이 무역업체 및 화주들이 이용하는 종합정보망 등을 대표로 들 수 있다. 개별기업 차원의 종합정보시스템으로 부산항의 신선대터미널, 자성대터미널, 감만터미널, 감천항터미널, 우암터미널, 광양항터미널 등이 대정부 및 고객서비스를 위해 종합정보망을 별도로 운영하고 있다.

국내외에 많은 영업망을 구축하고 있는 한진해운, 현대상선 등 대형 선사들과 대한통운, 한진, 세방기업 등 하역회사 및 운송사도 대고객 서비스 및 대정부업무 등을 처리하기 위해 네트워크 시스템을 각기 운영하고 있다. OSI 체재하에서 물류EDI시스템이 도입될 수 있도록 정책 및 재정을 계속하여 지원하고 있고 원활한 전자문서교환을 위해 관련협회와 공동출자하여 VAN업체인 한국물류정보통신(주)도 1994년에 설립하여 운영하고 있다. 네트워크 활용은 터미널운영의 선진화와 하역 및 야드 운영정보시스템의 개선 등을 통해 하역시간이 단축되고, 선박이 항내 머무는 시간을 최소화(JIT)하는 등 물류비 개선에 크게 기여하고 있으며 물류서비스의 수준을 한 단계 도약 시켰다.

철도운송을 위해 철도화물운송정보시스템(KROIS; Korea Railroad Operating Information System)과 연결하여 화물운송통지서 등 8개 서류를 EDI 방식으로 철도청, 화주, 철도운송업체, 터미널, ICD 등에 제공하고 있다. 현재 활용되고 있는 항공관제시스템, 항만운영정보시스템, 해운·선원정보시스템, 수출입일괄처리시스템 등은 물류 관련 산업의 운영체계를 보다 편리하고 효율적으로 개선시키는데 많은 부문에 기여했다고 볼 수 있지만, 운영 측면에서 전자문서의 폭발적인 송수신 폭주로 네트워크의 기술적인 문제점들이 적잖게 노출되어 있는 것이 현실이다(한국정보화진흥원, 2011)[2].

OSI 체재하에서 최근 글로벌 IT시장은 하드웨어 중심에서 소프트웨어, 모바일 중심으로 급속히 변화하고 있으며, 소프트웨어, PC, 휴대폰 등 비교적 명확했던 IT 경계가 사라지고 융복합화 되고 있어 소프트웨어산업은 IT 산업 전체의 경쟁력을 좌우하는 기반산업으로서 그 역할이 확대되고 있다(이동만·장성희, 2012)[3].

인터넷은 정보 수용자에 불과했던 사람들을 정보의 생산과 공유가 가능하도록 했다. 직접 참여하고 공유하는 웹 2.0 패러다임 환경이 확산되고, 스마트폰 등과 같은 모바일 단말기기

2) 한국정보화진흥원, “ASP/SaaS산업 현황조사”, 한국정보화진흥원, 2011.
3) 이동만 · 장성희, “대구 경북지역의 CEO 특성이 소프트웨어 기술전략과 소프트웨어 개발 기업의 성과에 미치는 영향”, 「인터넷전자상거래연구」, 제12권 제1호, 인터넷전자상거래학회, 2012.

의 기술발전, 더불어 무선데이터 이용량이 폭발적으로 증가하면서 모바일 환경을 기반으로 하는 인터넷 서비스들이 증가하고 있다(장희영·박경자, 2012)[4].

따라서 전자무역을 통한 무역거래 비용 최소화로 대내외적인 경쟁력을 확보하고, 효율성 제고에 의한 무역업무 전반에 걸쳐 모든 서비스(total service)를 One-stop으로 제공하기 위한 전자무역플랫폼과 솔루션 등을 제공함으로서 무역거래의 활성화를 이룩하기 위한 가장 효과적인 경제적 수단이라고 할 수 있다(윤봉주·정분도, 2012)[5].

Ⅱ. OSI 체제 데이터 전송

1. OSI Model

OSI(Open System Interconnection)는 ISO와 CCITT가 중심이 되어 제정한 다른 제조업체의 컴퓨터 사이에서도 통신할 수 있게 하기 위한 기본 모델이다. OSI 모델의 목적은 기본적인 하드웨어와 소프트웨어의 논리적인 변경 없이 시스템간의 통신을 개방하는 것이다. 다음 <표 1>과 같이 각각 특정 기능을 수행하는 7개의 서로 다른 계층으로 구성되어 있다.

〈표 1〉 OSI 7계층

7계층	응용 프로그램 계층(Application Layer)
6계층	표현 계층(Presentation Layer)
5계층	세션 계층(Session Layer)
4계층	전송 계층(Transport Layer)
3계층	네트워크 계층(Network Layer)
2계층	데이터 링크 계층(Data Link Layer)
1계층	물리 계층(Physical Layer)

4) 장희영 · 박경자, “가상 능숙도와 네트워크 효과가 SNS(Social Network Service) 지속적 사용의도에 미치는 영향: 가상 능숙도의 다차원적 관점을 중심으로”, 「인터넷전자상거래연구」, 제12권 제2호, 인터넷전자상거래학회, 2012.

5) 윤봉주 · 정분도, “무역거래 전자화에 따른 파급효과에 관한 연구”, 「통상정보연구」, 제14권 제2호, 한국통상정보학회, 2012.

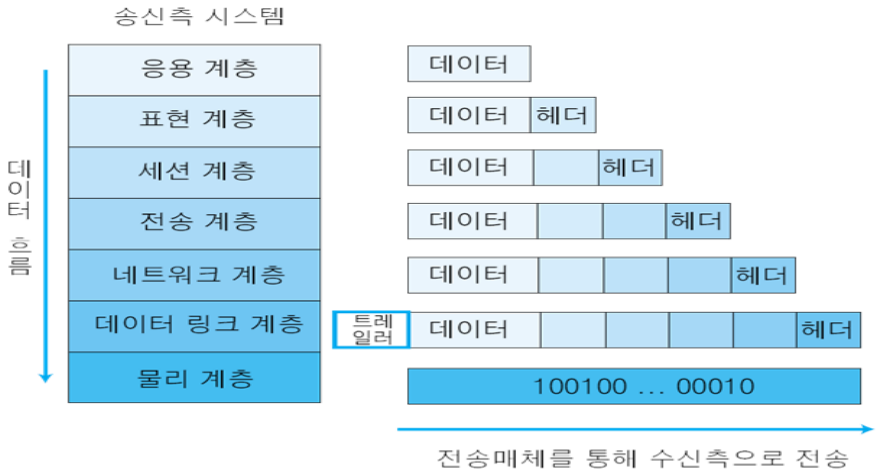
2. OSI 데이터 단위전송 계층

OSI 각 계층의 헤더에는 각 계층의 기능과 관련된 정보가 포함되어 있다. 송신측은 헤더를 생성하여 추가하고, 수신측의 해당 계층이 이 헤더를 사용한다.

OSI 데이터 단위는 데이터를 전송하기 위해서 데이터에 Header와 Trailer를 붙여 전송하는 Data 전송 기본 단위이다. 제어 정보에는 흐름 제어 정보, 에러 제어 정보, 주소 정보 등이 포함되어 있다.[6]

서비스 데이터 단위(SDU)는 상위 계층 혹은 하위 계층 사이에 주고받는 것이며, 프로토콜 데이터 단위(PDU)는 같은 계층 상호 간에 주고받는 것이다. 데이터베이스는 자체의 설계 구성 요소도 중요하지만 응용프로그램에서 코딩의 편리성이나 트랜잭션의 속도 등을 고려하여 각 DBMS의 기능이나 각종 오브젝트들을 이용하는 것도 중요하다.

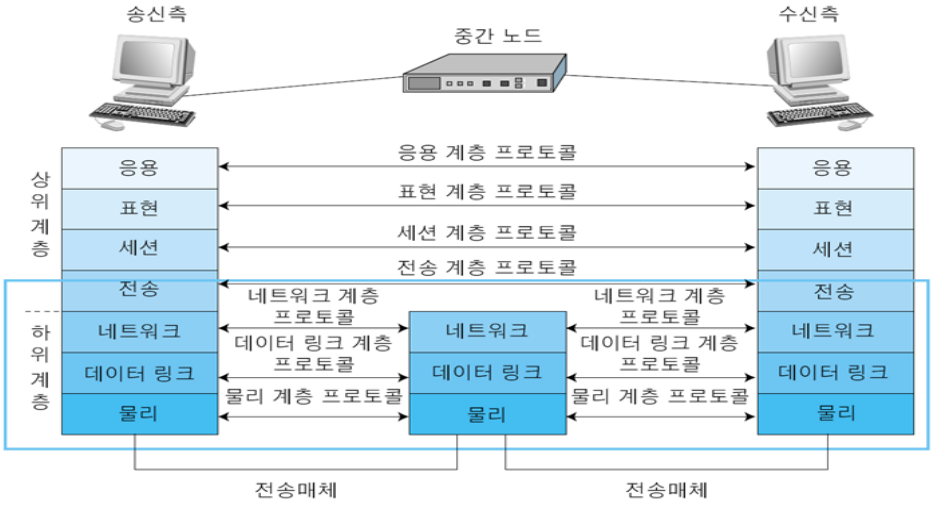
특히 뷰는 통계자료 분석시 아주 중요한 역할을 하며 인덱스는 데이터의 처리속도에 많은 영향을 주므로 업무 특성에 맞게 이들을 잘 이용하여야 한다. 데이터베이스를 물리적으로 설계시에는 트랜잭션을 관리할 수 있도록 고려하여야 하는데, 사용자들이 데이터베이스를 읽거나 쓰고 있다면 트랜잭션을 사용하고 있는 것이며, 이러한 모든 트랜잭션을 기록하는 트랜잭션 로그를 기록할 수 있도록 하여야 한다[7].



<그림 1> OSI 데이터 전송(송신측)

6) 바로 위의 층 또는 바로 아래의 층 사이에 주고받는 데이터인 SDU(Service Data Unit)에 제어 정보인 PCI(Protocol Control Information)을 추가한 것을 의미한다.

7) 로그에 저장되어 있는 정보는 롤백 문이나 프로그램의 비정상적인 종료 또는 통신망 불일치나 디스크 파괴 같은 시스템 실패에 의해 유발되는 복구 필요사항을 위해 DBMS에 의해 사용된다.



<그림 2> OSI 데이터 전송(수신측)

Ⅲ. OSI 체재 7계층 분석

1. OSI 7계층

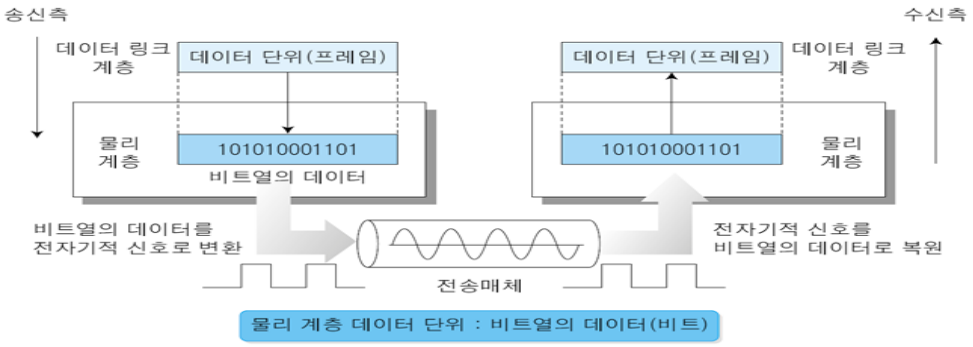
1) Physical Layer(1계층)

1계층(물리 계층)은 실제 장치들을 연결하기 위해 필요한 전기적, 물리적 세부 사항들을 정의한다. 물리 계층은 두 시스템 간의 데이터 전송을 위해 링크를 활성화하고 관리하기 위한 기계적, 전기적, 기능적, 절차적 특성 등이 있다.[8] 1계층은 OSI 모델의 최하위 계층에 속하며, 상위 계층에서 전송된 데이터를 물리매체를 통해 다른 시스템에 전기적 신호를 전송한다.[9]

데이터 단위 전송 송신측은 데이터링크 계층에서 0과 1로 구성된 비트열의 수신지와 목적지 주소와 프로토콜 제어정보와 데이터가 포함된 완전한 하나의 전송단위 데이터를 받아 전송될 수 있는 형태로 변환한 후 전송 매체를 통하여 수신측에게 보낸다.

수신측은 송신측으로부터 받은 전기 신호를 0과 1로 구성된 비트열로 복원하여 수신측의 데이터링크 계층에 전송한다.

8) 허브, 라우터, 네트워크 카드, 케이블 등의 전송매체를 통해 비트(Bit)들을 전송하며, 상위 계층인 데이터링크 계층에서 형성된 데이터 패킷을 전기신호 또는 광신호로 변환하여 송수신한다.
9) 랜카드, 리피터, 케이블, 허브, 라우터와 같은 물리적인 것과 데이터 전송을 위해 사용하는 전압이 물리 계층에 속한다.



〈그림 3〉 물리 계층

2) Data Link Layer(2계층)

2계층(데이터 링크 계층)은 물리계층을 통해 컴퓨터끼리 통신할 때 주고받는 프레임에 에러가 없도록 데이터를 신뢰성 있게 전송하는 계층이다.[10]

2계층은 네트워크를 통해서 데이터가 전송될 때 전송로 역할을 한다.[11] 시스템 간에 오류 없는 데이터 전송을 위하여 네트워크 계층에서 받은 데이터 단위(패킷)를 프레임으로 구성하여 물리 계층으로 전송한다.[12]

데이터 단위 전송은 네트워크 계층으로부터 데이터 단위를 받아서 주소와 제어정보 같은 의미 있는 비트들을 헤더와 트레일러에 추가한다. 이처럼 추가적인 정보를 가지고 있는 데이터를 프레임이라고 한다.

3) Network Layer(3계층)

3계층(네트워크 계층)은 여러개의 노드를 거칠 때마다 경로를 설정하고 제어하는 역할을 하는 계층으로 패킷[13]을 송신측으로부터 수신측으로 전송하며, 상위 계층에 연결하는 데 필요한 데이터 전송과 경로 선택 기능을 제공한다. 네트워크 계층은 라우팅 프로토콜을 사용하여 최적의 경로를 선택한다.

데이터가 전송될 수신측의 주소를 찾고, 수신된 데이터의 주소를 확인하여 내 것이면 전송

10) 네트워크 위의 개체들 간 데이터를 전달하고, 물리 계층에서 발생할 수 있는 오류를 찾아내어 수정하는 데 필요한 기능적, 절차적 수단을 제공하며, 하위 계층에 속하고 물리 계층의 바로 위에 위치한다.

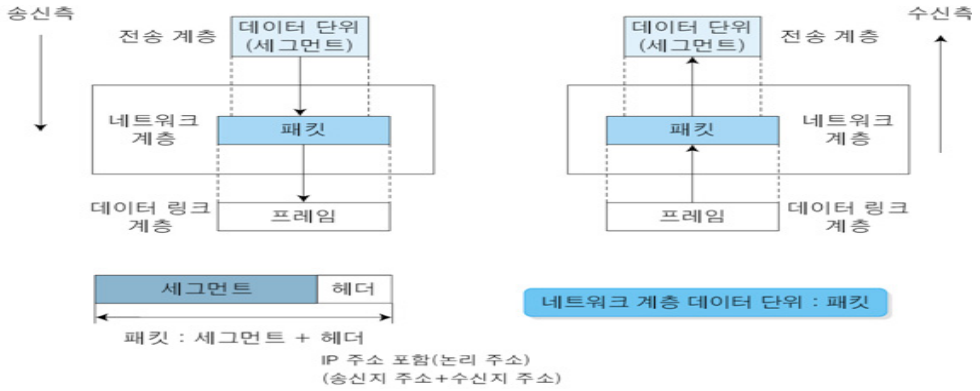
11) 데이터 링크 계층에서는 비트들을 프레임(Frame)이라는 논리적 단위로 구성하는데, 전송하려는 데이터에 인접하는 노드(시스템)의 주소가 더해지며, 이 주소는 최종 수신지의 주소가 아니라 전송되는 다음 노드의 주소가 된다.

12) 이 계층은 물리적 어드레싱, 네트워크 토폴로지, 회선 사용 규칙, 오류 검출, 프레임 전달 그리고 흐름 제어 등에 관계한다.

13) 패킷은 우체국에서 취급하는 소포를 말하며, 화물을 적당한 크기로 분할해서 행선지 꼬리표를 붙인 형태을 뜻한다.

계층으로 전송한다. 그리고 데이터를 패킷(Packet) 단위로 분할하여 전송한 후 재결합한다. 데이터 링크 계층이 인접하는 두 개의 노드 간의 전송을 담당하는 반면, 네트워크 계층은 각 패킷이 송신지에서부터 최종 수신지까지 정확하게 전송되도록 경로를 책임진다.

스위칭은 네트워크 전송을 위해 물리 링크들을 임시적으로 연결하여 보다 긴 링크를 만드는 것이며, 라우팅은 송신지에서 수신지로 패킷을 보낼 때 다양한 경로 중에서 가장 좋은 패킷의 경로를 선택하는 것을 의미한다.



〈그림 4〉 네트워크 계층

4) Transport layer(4계층)

4계층(전송 계층)은 프로토콜(TCP, SPX, UDP 등)과 관련된 계층으로 오류 복구, 흐름 제어를 담당하며, 두 시스템간의 신뢰성 있는 데이터 전송을 보장한다.[14]

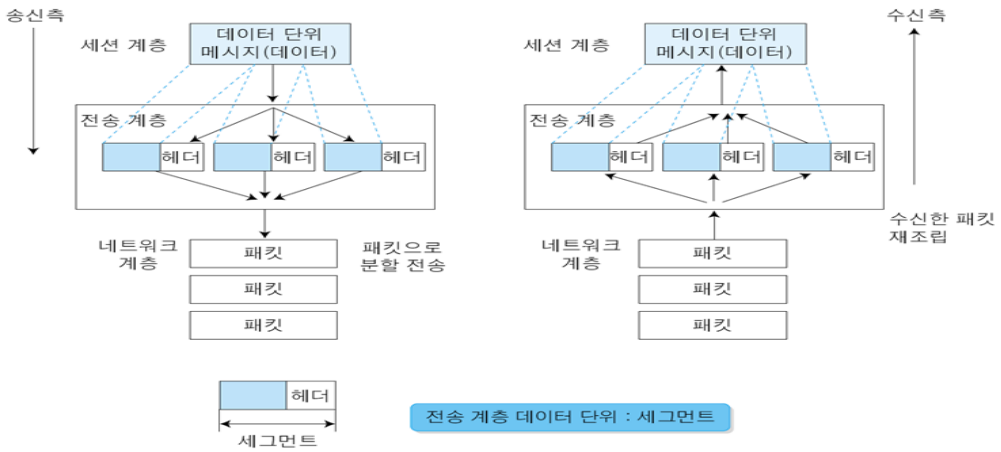
네이버의 웹 서버까지 많은 장비들을 통과할 때 실제 물리 계층, 데이터링크 계층, 네트워크 계층까지만 해당되고, 서버에 도착한 후로는 웹서버가 특정 경로로 전자문서교환(EDI)을 한다. 송신측은 EDI 데이터를 패킷으로 분할하고, 수신측은 다시 결합하여 순서대로 재조립한다. 즉, 2개의 프로세스 간의 데이터 전송을 위해 세션 계층에서 받은 EDI 데이터를 패킷 단위로 분할하여 네트워크 계층으로 전송한다.

데이터 헤더에는 포트 주소 또는 소켓((Socket)=IP+Port) 주소를 포함하며, 헤더에는 순서 또는 세그먼트 번호가 포함된다. 전송 계층이 세션 계층으로부터 온 데이터를 수신할 때, 데이터를 전송할 수 있는 세그먼트로 나누고 수신측에서 수신자가 재조립할 수 있도록 순서를

14) 시스템 종단 간에 투명한 데이터 전송을 양방향으로 행하는 계층이며, 네트워크 계층에서 전송된 데이터와 실제 운영체제의 프로그램이 연결되는 통신 경로라 할 수 있다.

헤더에 표시한다.

네트워크 계층은 전송해야 하는 시스템에게 각 패킷을 전송하는 일을 하고, 전송 계층은 해당 시스템의 응용 프로그램에게 모든 EDI 데이터를 전송하는 역할을 한다.

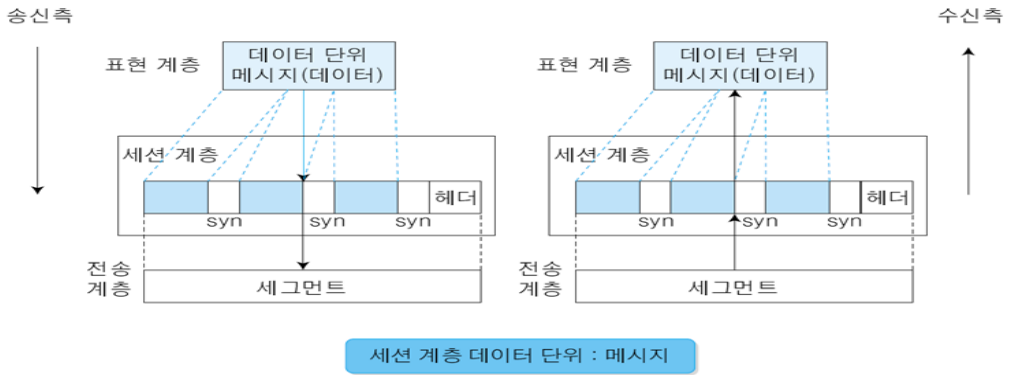


〈그림 5〉 전송 계층

5) Session Layer(5계층)

5계층(세션 계층)은 응용 프로그램 계층 간의 통신에 대한 제어 구조를 제공하기 위해 응용 프로그램 계층 사이의 접속을 설정, 유지, 종료시켜주는 역할을 한다.

또한 통신 장치들 간의 설정을 유지하며 동기화한다. 그리고 세션을 종료할 필요가 있을 때 적절한 시간을 수신자에게 알려준다.

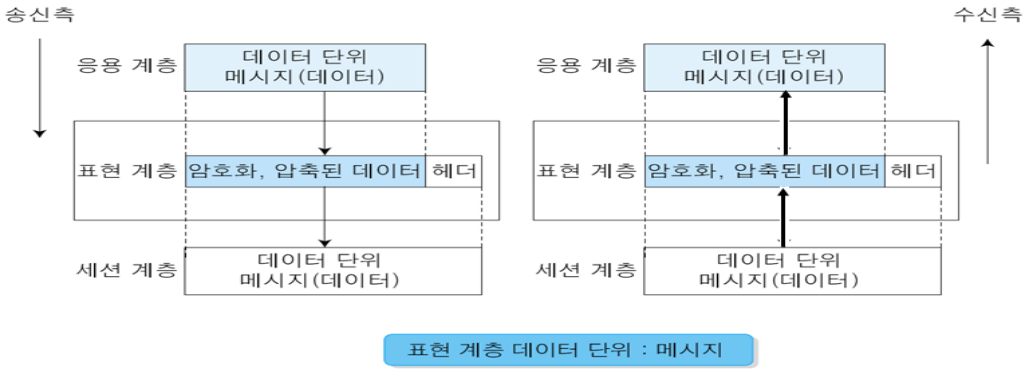


〈그림 6〉 세션 계층

6) Presentation Layer(6계층)

6계층(표현 계층)은 코드간의 번역을 담당하여 사용자 시스템에서 데이터의 형식상 차이를 변환해주거나 공통 형식을 제공함으로 인해 응용 계층으로부터 부담을 덜어 준다. 표현 계층은 송신측과 수신측 사이에서 표준화된 EDI 데이터의 형식에 대해 규정을 한다.[15]

보안을 위하여 송신측에서 암호화하고 수신측에서 복호화하며, 전송률을 높이기 위하여 데이터를 압축한다. 두 시스템 간에 서로 다르게 사용하는 문자 및 그래픽 문자 등을 위해 번역을 수행하여 전송 데이터를 서로 이해할 수 있도록 해야 한다.



〈그림 7〉 표현 계층

7) Application Layer(7계층)

7계층(응용 계층)은 실제 통신의 최종 목표에 해당하는 가장 중요한 계층으로서 OSI 모델의 최상위 계층에 속하며, 사용자와 직접 교류하는 응용 프로그램에서 보내진 요청을 받아들여서 요청을 적절하게 변형하는 역할과 이를 하위 계층으로 보내는 역할을 한다.[16]

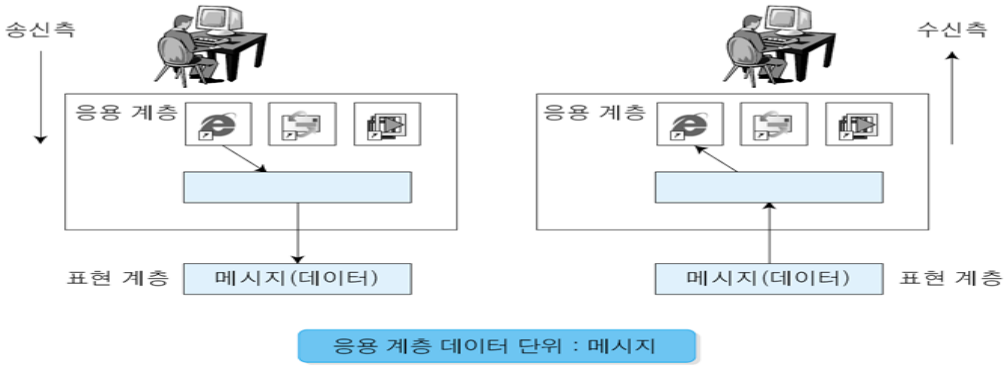
7계층에서 FTP는 가장 오래된 TCP/IP 프로토콜 중 하나이다. 이 프로토콜은 호스트들 사이에서 텍스트 또는 바이너리 파일들을 전송하기 위해 사용된다. FTP는 접근을 제어하는 패스워드를 사용하거나 익명 접근을 허용할 수 있다. 익명 접근을 허용하면 계정이나 패스워드 없어도 유용한 정보를 공공에게 공개할 수 있다. 전자무역의 서류전달 과정 중 인터넷상의 해커들에게 서버가 노출되기 때문에 익명 접근은 조심스럽게 관리해야 한다. 단순한 FTP의 파일

15) 이미지가 bmp인지, jpg인지, 압축이 되었는지 등의 표현과 관련된 구분을 한다. 송신측은 수신측에 맞는 형태로 변환(아스키 코드 => EBCDIC)을 하고, 수신측은 응용 계층에 맞는 형태로 변환한다.

16) 파일 전송에 사용되는 FTP, E-mail 전송에 사용되는 SMTP, POP3, 브라우저를 사용해서 웹 서버에 접속할 때 사용하는 HTTP 등 실제 응용 프로그램에서 사용하는 프로토콜들이 응용 계층에 해당한다.

전송 절차는 FTP의 시작, 파일 데이터의 전송, 연결종료 등으로 이루어진다.(정분도, 2007)[17]

응용 프로세스(사용자, 응용 프로그램)가 네트워크에 접근하는 수단을 제공하여 서로 간에 데이터를 교환할 수 있는 창구 역할을 하며, 사용자로부터 정보를 입력받아 하위 계층으로 전달하고 하위 계층에서 전송한 데이터를 사용자에게 전달한다.[18]



〈그림 8〉 응용 계층

2. EDI 데이터 단위전송의 침입탐지시스템

전자무역에서 침입은 허가되지 않은 접근임은 물론 컴퓨터 시스템의 보안 요소를 침해하는 모든 행위를 말한다.[19] 이러한 침입과 침입을 위한 시도 등에 대해서 보호하고자 하는 호스트나 네트워크에 대해 감시하고 실제 발견시 경고 및 대응하는 행위를 침입 탐지라 한다(Edward G. Amoroso, 1999). 침입탐지시스템은 컴퓨터가 사용하는 자원의 무결성(integrity), 비밀성(confidentiality), 가용성(availability)을 저해하는 행위를 가능한 실시간으로 탐지하는 시스템을 말한다.

최근에 잇따른 주요 무역 알선사이트들의 해킹으로 인해 네트워크 보안이 중요한 문제로 대두되면서 방화벽보다 좀 더 신뢰성 있는 네트워크 보안 솔루션을 제시하는 침입탐지시스템이 차세대 보안 솔루션으로 부각되고 있다. 이처럼 침입탐지시스템이 방화벽에 이은 차세대 보안 솔루션으로 부각되는 주된 이유는, 방화벽이 해킹 되었을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재중 시스템 자체적으로도 해킹 등에 대응할 수 있는 보안 솔

17) 정분도, "전자무역의 베이지안 네트워크 개선방안에 관한 연구", 「통상정보연구」, 제9권 제3호, 한국통상정보학회, 2007.
18) 응용 계층은 파일 전송, DB, 원격 접속, 메일 전송 등 응용 서비스를 네트워크에 접속시키는 역할을 담당하며, 여러 가지 서비스를 제공한다.
19) 전자무역의 침입에는 비밀번호 해킹을 통한 접근과 실제적인 침입을 위한 포트 스캐닝 등 그 종류는 무한하다.

루션에 대한 요구가 늘고 있는 상황에서 침입탐지시스템이 이 같은 요구를 해결할 수 있는 EDI 솔루션으로 대두되고 있다.[20]

〈표 2〉 EDI 단위 전송의 침입탐지시스템

	공격탐지/차단	취약점분석	암호화, 안티-바이라스
네트워크	- 방화벽(네트워크 기반의 접근조절시스템)	- 네트워크 취약점 스캐너	- IP 터널링 - VPN 기구 - 바이러스 필터링 게이트웨이
시스템 (호스트)	- 호스트-베이스 IDS - 호스트-베이스 접근조절시스템	- 호스트(OS) 취약점 스캐너	- 파일 시스템 암호화 - 파일 시스템 보전 - 안티-바이러스 시스템
응용시스템	- PC(클라이언트) 보안과 고급인증	- 데이터베이스 취약점 스캐너 - PC 취약점 스캐너	- 데이터 암호화 - 공개 키 인프라 - 안티-바이러스 시스템

전자무역의 전통적인 네트워크 관리 기반인 SNMP의 중앙 집중형 침입 탐지와 이동 에이전트 기반의 침입탐지의 구체적인 비교를 수식을 통해 적용하며 다음과 같다.

먼저 네트워크 통신량의 수치화를 위한 가정으로 탐지 대상의 수 N, 탐지 대상에 보내질 에이전트 수 A, 서버에 보내질 데이터의 크기 d로 놓을 때, 네트워크 패킷으로 바뀐 전체 데이터의 크기를 D라 하면, $D = \alpha(d) + \beta(d)d$ 이다.

여기서 $\alpha(d)$는 통신 컨트롤을 위한 정보의 크기이고, $\beta(d)d$는 데이터 d가 네트워크 패킷으로 바뀐 크기이다.

이 경우 $D = \left\{\frac{\alpha(d)}{d} + \beta(d)\right\}d$ 로 나타내며, $\left\{\frac{\alpha(d)}{d} + \beta(d)\right\}d$ 는 통신 오버헤드 함수를 나타내는데, 이를 $\eta(d)$로 놓으면, 전체 통신 데이터의 크기인 $D = \eta(d)d$로 나타낼 수 있다. (단, $\eta(d)$>1) 위 식을 통해 분석한 각 관리 모델의 통신량 계산은 다음과 같다.

$$T_{RPC} = \sum_{n=1}^{N}\sum_{q=1}^{Q}(\eta(I_q)I_q + \eta(R_{q,n})R_{q,n}) \quad (1)$$

(단, $I_q, R_{q,n}$는 각각 SNMP질문과 이에 따른 결과의 크기)

20) ISO/IEC에서 정의하는 침입탐지의 기본모델은 원시 데이터(raw data source), 사건 탐지(event detection), 분석(analysis), 대응(response), 데이터 저장소(data storage)의 5가지 요소로 구성된다.

$$D_{MA,n} = \sum_{m=1}^{n-1} \sum_{q=1}^{Q} R_{q,m} \quad (2)$$

(if n = 1, $D_{MA,n}$ = 0, m은 관리대상 수)

$$T_{MA} = \sum_{n=1}^{N+1} (\eta(C_{MA} + D_{MA,n})(C_{MA} + D_{MA,n}) \quad (3)$$

(단, C_{MA}, $D_{MA,n}$는 각각 코드와 관리 결과 데이터의 크기)

식 (1)과 (2), (3)은 각각 중앙 집중형과 이동 에이전트 방식의 관리에 대한 전체 통신비용이다. 이를 토대로 할 때 중앙 집중형 방식의 관리는 관리 대상의 수 N과 관리 명령에 따라 전체 통신비용이 증가하게 되며, 이동 에이전트를 이용한 관리에서는 마찬가지로 이동해야 될 관리 대상의 수 N과 이동 코드와 데이터의 크기가 중요한 요소로 자리 잡고 있다. 따라서 특정한 대상의 자원을 사용하지 못하게 하는 분산 서비스 거부 공격(DDoS)과 해외 해커들의 국내 전산망을 우회 루트로 활용하여 공격하는 행위에 대하여 적극적인 탐지가 어렵기 때문에 호스트에서 로그 분석을 통해 침입 사실을 확인하는 방법과 네트워크에 유입되는 다양한 트래픽을 분석함으로써 침입을 발견하는 패킷분석 기법을 주로 사용한다. 이동에이전트가 생성되어 각 호스트를 순회하는 에이전트가 패킷 정보를 수집하여 전송한 결과와 침입탐지 횟수와의 상관관계를 보여 준다.[21]

Ⅳ. 요약 및 결론

OSI 체재하의 전자무역 네트워크 기반 침입탐지시스템(IDS; Intrusion Detection System)은 패킷 스니퍼(packet sniffer)[22], 패킷 모니터(packet monitor) 도구의 발전으로 볼 수 있다. OSI 체재하의 전자무역 네트워크의 모든 트래픽에 대해 패킷을 수신하고 분석하여 침입을 발견하는 일은 매우 복잡한 것이나 이를 자동으로 처리해 주는 것이 바로 네트워크 기반 IDS라고 볼 수 있다. OSI 체재하의 네트워크 기반 IDS는 특히 권한 없이 접근한다거나 권한을 초과하는 접근에 대한 탐지에 뛰어나다. 또한 네트워크내의 호스트나 서버의 별도의 설정 없이

21) 황인선, "이동 에이전트 기반 네트워크 침입탐지시스템", 목포대학교 대학원 박사학위논문, 2004. pp.95-96.
22) 네트워크를 통해 오가는 데이터 패킷을 가로채는 기술을 뜻한다. 주로 비밀번호를 수집할 때 사용한다.

사용이 가능하며, 방화벽이나 라우팅처럼 특별한 역할을 담당하지 않기 때문에 오류 발생시에 큰 피해를 주지 않게 된다.

OSI 체재하의 전자무역 네트워크 기반 IDS는 성능에 대한 요구사항 때문에 서명 분석을 하는 경우가 많은데 이는 일반적으로 알려진 공격을 탐지하는 데는 뛰어나지만 복잡한 정보를 가진 위협요소에 대한 공격은 탐지하기가 어렵다.

또한 분석을 위해 엄청난 양의 데이터 교환을 필요로 한다. 이를 위해 분석을 위한 데이터를 축적 과정을 통해 필터링하여 모든 패킷에 대한 분석을 더 정확하게 탐지한다. OSI 체재하의 전자무역 네트워크 기반 IDS는 암호화 세션에 대한 침입 탐지에는 뛰어나지 않다. 침입탐지에는 두 개의 상호보완적인 방법이 있다.

첫째, 공격에 관한 축적된 지식을 사용하여 어떤 공격을 사용하고 있다는 증거를 찾는 방법이다.

둘째, 감시중인 시스템의 정상행위에 관한 참조모델을 생성한 후 정상행위에서 벗어나는 경우를 찾는 방법이다.

전자무역의 지식기반 침입탐지 방법은 알려진 침입행위를 이용하여 침입을 탐지하고, 정해진 모델과 일치하는 경우를 침입으로 간주한다.[23]

실시간 침입탐지를 위한 효과적인 방법은 네트워크를 구성하는 여러 가지 시스템과 장치에서 발생하는 보안에 관련된 여러 행위에 대해 모니터링하고 조치하는 것이다.

실시간 행위 감시 모니터링은 단일 시스템과 매니저·에이전트와 같이 두 가지로 분류하며 단일 시스템의 감시 프로그램은 오직 한 시스템에서만 실행된다.[24]

전자무역에서 침입탐지시스템은 서브네트 상의 모든 EDI 네트워크 패킷을 수집하여 이를 감시 자료로 사용하기 때문에 보안 영역으로 지정된 호스트들의 감시가 가능하고 실시간으로 침입을 탐지하는 것이 가능하다.

전자무역에서 침입탐지시스템은 크게 감시자료 수집모듈과 탐지모듈로 이분화되어 있다. 감시자료 수집 모듈은 보안영역으로 설정된 특정 호스트의 패킷만을 포착하여 감시자료를 생성하여 탐지모듈에서 분석하게 된다.[25]

---

23) 이러한 방법에는 전문가시스템(Expert System), 시그너처 분석(Signature Analysis), 페트리넷(Petri-net), 상태전이분석(State Transition Analysis), 신경망(Neural Network), 유전 알고리즘(genetic algorithm) 등이 있다.

24) 이러한 방식으로 구현된 프로그램은 Win NT 용의 IDI의 Kane Security Monitor와 TIS의 Web Stalker가 있는데, 이들은 stand-alone, single-system tool이므로 멀티 플랫폼 환경에서는 적당하지 않다.

25) 전자무역에서 활용되고 있는 침입탐지시스템은 호스트 기반과 네트워크 기반의 침입탐지시스템으로 분류하여 살펴보았을 때 호스트 기반은 침입탐지시스템을 목적지 호스트에 설치해야 하므로 해당 호스트의 성능이 저하되고 데이터를 얻기 위해 로깅 등에 대한 설정이 번거로우며 목적지 호스트가 있는 네트워크 내의 다른 호스트들이 공격을 당해도 알 수가 없다.

전자무역의 네트워크 기반 침입탐지 시스템은 네트워크 패킷을 캡쳐하여 이더넷 프레임 패킷 중에서 데이터 부분을 검출하여 IP 데이터그램과 TCP, UDP 각각의 세그먼트에 대한 패킷을 필터링한다.[26]

감시자료 탐지모듈이 최대 초당 30,000프레임을 캡쳐할 수 있고 네트워크 상에 초당 60,000 프레임이 입력된다고 하면, 많은 프레임이 정상적으로 침입탐지 모듈로 전달될 수 없을 것이다. 이는 프레임을 받아들이는 감시자료 수집 모듈과 프레임을 분석하는 탐지모듈이라는 두 개의 활동으로 이분화 되어 있기 때문이다.

대부분의 침입탐지 시스템의 구조는 감사자료 수집 모듈에서 캡쳐한 프레임을 버퍼에 저장하고 침입탐지 모듈을 버퍼에 있는 내용을 탐지하는 구조를 가지고 있고, 이 경우에 버퍼의 용량이 남아있으면 탐지 모듈의 과부하에 상관없이 패킷을 캡쳐하는 구조를 가지고 있다. 그러므로 고속 네트워크에서는 보다 고성능의 침입탐지 시스템이 필요하다. 또한 감시기록 추적모델 설계 및 구현을 이용하면 침입탐지시스템의 감시 기록 수집 모듈과 탐지 모듈간의 속도 차이 문제를 해결할 수 있고, 침입을 미리 차단하므로 과부하 문제도 해결되므로 감시기록 추적 모델 설계 및 구현이 필요하다.

따라서 네트워크 환경이나 비용 등을 고려하여 충분히 분석한 후 가장 현실적인 네트워크 전략을 세워야 한다. 네트워크는 무조건 수행해야 하는 게 아니라 어떤 오류나 장애시에는 어떠한 백업내용이 필요한 것인지 충분히 인식해야 하기 때문에 네트워크의 구조를 알아야 하는 것은 당연하다고 볼 수 있다. 이때의 데이터 마이닝은 복잡하고 다양한 데이터에서 특정 규칙이나 트랜드를 찾아주는 분석 방법으로 신경 네트워크 클러스터링 알고리즘, 의사결정 트리 등의 다양한 기술로 구성되어 있다. 클러스터링 알고리즘과 의사결정 트리는 고객의 세분화에 중점적으로 활용되며, 신경 네트워크는 고객의 향후 트랜드 분석 및 수요예측에 주로 사용된다(정분도, 2008)[27].

OSI 체재하의 전자무역 활용 침입탐지시스템의 네트워크가 높은 품질의 정보와 서비스를 제공한다고 할지라도 페이지 전환속도가 느리거나 접속이 자주 끊기는 등 원활하게 정보를 전달하지 못한다면 정보시스템에 대하여 불안정한 인식을 갖게 될 것이고 경우에 따라서는 사용하던 정보시스템 사용을 중단하는 상황이 나타 날 수 있다(김근형·윤상훈, 2012)[28].

---

26) 전자무역에서 네트워크 트래픽이 감시자료 수집모듈의 캡쳐링 속도 보다 빠르다면 감시자료 적체 현상과 사용자의 입력과 침입유형을 비교하는 침입 판정 엔진에 과도한 오버헤드를 초래하게 되므로 침입탐지시스템의 성능에 악영향을 줄 수 있다.

27) 정분도 · 장기영, “전자무역의 물류/유통 개선에 대한 RFID/USN의 진보적인 활용방안 연구”, 「통상정보연구」, 제10권 제3호, 한국통상정보학회, 2008.

28) 김근형 · 윤상훈, “SNS사용자 만족도의 영향요인 도출 및 서비스 형태별 비교 분석”, 「인터넷전자상거래연구」, 제12권 제1호, 한국인터넷전자상거래학회, 2012.

참 고 문 헌

김기홍, “e-비즈니스의 경제적 효과측정에 대하여 : 일반적 효과, 연구현황, 향후과제를 중심으로” 「e-비즈니스연구」, 제17권 제2호, 국제 e-비즈니스학회, 20006.

김계수, “인터넷 포털사이트의 서비스품질전략에 관한 연구,” 「경영학연구」, 제31권 제1호, 한국경영학회, 2002.

김근형·윤상훈, “SNS사용자 만족도의 영향요인 도출 및 서비스 형태별 비교 분석”, 「인터넷전자상거래연구」, 제12권 제1호, 한국인터넷전자상거래학회, 2012.

김승철, “한국 수출기업의 전자무역 활용 수준과 성과에 관한 연구”, 「중앙대학교 박사학위논문」, 중앙대학교, 2003.

김용재, “전자무역 활성화를 위한 전략에 대한 연구” 「e-비즈니스연구」, 제9권 제5호, 국제e-비즈니스학회, 2008.

_____, “ebXML 등록저장소를 이용한 e-Trade 활성화 방안” 「e-비즈니스연구」, 제8권 제1호, 국제e-비즈니스학회, 2007.

김창봉, “전자무역 활용과 성과에 관한 실증연구: 한국의 수출기업의 내・외부 환경요인을 중심으로”, 「무역학회지」, 제36권 제4호, 한국무역학회, 2011.

김학민・김종철, “전자무역 성과평가 체계에 관한 연구”, 「통상정보연구」, 제9권 제2호, 한국통상정보학회, 2007.

_____, “전자무역 계획수립 가설에 관한 연구”, 「통상정보연구」, 제7권 제2호, 한국 통상정보학회, 2005.

김태환 외 3인, “한국의 전자무역 네트워크 구축사업의 현황과 개선방안에 관한 연구”, 제8권 제1호, 한국관세학회, 2007.

김효정, “고객 로열티에 영향을 주는 웹사이트 요소에 관한 연구,” 전남대학교 대학원 석사학위논문, 2003.

공정열, “한국 중소기업의 전자무역 확대 방안에 관한 연구”, 「전자상거래학회지」, 제7권 제4호, 한국전자상거래학회, 2006.

교육과학기술부 보도자료, 디지털Life실현을 위한 Digital Home 구축계획, 2013.

박광로 외, “홈 게이트웨이 기술”, 「한국통신학회지」, 한국통신학회, Nov. 2000.

이동만・장성희, “대구 경북지역의 CEO 특성이 소프트웨어 기술전략과 소프트웨어 개발 기업의 성과에 미치는 영향”, 「인터넷전자상거래연구」, 제12권 제1호, 인터넷전자상거래

학회, 2012.
이봉수, “전자무역 기반사업의 구현에 관한 연구”, 「통상정보연구」, 제12권 제1호, 한국통상정보학회, 2010.
이유재, “고객만족의 정의 및 측정에 관한 연구,” 「서울대 경영논집」, 제29권, 1998.
이재원, “기업간 전자상거래의 확산과 성과의 결정요인 : 인간관계모형”, 「무역학회지」, 제26권 제2호, 한국무역학회, 2001.
이창숙・강원진, “신용장거래에서 전자기록의 심사에 따른 문제점에 관한 고찰”, 「통상정보연구」, 제12권 제2호, 한국 통상정보학회, 2010.
윤봉주・정분도, “무역거래 전자화에 따른 파급효과에 관한 연구”, 「통상정보연구」, 제14권 제2호, 한국통상정보학회, 2012.
지식경제부 : 세계 최초 e-Nego (전자적 수출환어음 매입) 시스템 구축 성공, 2010.
지식경제부 무역정책과 보도자료, “우리 기업을 위한 One-Stop 전자무역 서비스 시스템 구축”, 2012.
장희영・박경자, “가상 능숙도와 네트워크 효과가 SNS(Social Network Service) 지속적 사용의도에 미치는 영향: 가상 능숙도의 다차원적 관점을 중심으로”, 「인터넷전자상거래연구」, 제12권 제2호, 2012.
정분도, “전자무역의 베이지안 네트워크 개선방안에 관한 연구”, 「통상정보연구」, 제9권 제3호, 한국통상정보학회, 2007.
정분도, “국내 기업의 e-CRM 도입사례 분석과 향후 발전전략 고찰”, 「통상정보연구」, 제10권 제1호, 한국통상정보학회, 2008.
정분도・윤봉주, “전자무역의 SaaS모형 UPnP 네트워크 활용방안에 관한 연구”, 「통상정보연구」, 제14권 제4호, 한국통상정보학회, 2012.
정분도・장기영, “전자무역의 물류/유통 개선에 대한 RFID/USN의 진보적인 활용방안 연구”, 「통상정보연구」, 제10권 제3호, 한국통상정보학회, 2008.
채진익, 「전자무역론」, 도서출판 두남, 2009.
_____, “전자무역시스템 하에서 전자무역전문서비스업자 제도의 문제점과 개선방안”, 「e-비즈니스연구」, 제11권 제1호, 국제e-비즈니스학회, 2010.
최용록, “글로벌 e-비즈니스의 새로운 도약 : 전망과제”, e-비즈니스연구」, 제10권 제5호, 국제e-비즈니스학회, 2009.
_____, “전자무역활성화를 위한 Metamediary의 기능과 역할”, 「무역학회지」, 제27권 제4호, 한국무역학회, 2002.

최용민・김우종, “무역절차의 그린화, 전자무역의 경제적 효과분석”, Trade Focus 제19권 제64호, 국제무역연구원, 2010.

황인선, “이동 에이전트 기반 네트워크 침입탐지시스템”, 목포대학교 대학원 박사학위논문, 2004.

한국전자통신연구원, “네트워크 정보가전기술/시장보고서”, 「한국전자통신연구원」, 2012.

Cox, J. and Dale, B. G, “Service Quality and E-Commerce : An Exploratory Analysis,” Managing Service Quality, 2012.

Davis, J. and S. Merritt, “The Web Design Wow! Book; Show casing the Best of on-Screen Communication,” Peachpit Press, 2012.

Debabroto C. Segars A. H. & R. T. Watson, “Realizing the Promise of E-business : Developing and Leveraging Electronic Partnering Options,” California Management Review, Vol.48, Issue4, 2011.

Eid R., Elbeltagi L. & Zairi M, “Marking Business To Business International Internet Marketing Effective : A Study of Critical Factors Using a Case-Study Approach,” Journal of International Marketing, Vol.14, Issue4, 2012.

Franken, D. A. and W. F. Van Raajj, “Satisfaction with Leisure Time Activities,” Journal of Leisure Research, 13(4), 2003.

Grönroos, C, “A Service Quality Model and its Marketing implications,” European Journal of Marketing, 18(4), 1984.

Hanson, W, The Principles of Internet Marketing, South-Western College Publishing, 2012.

Hoffman, D. L. and T. P. Novak, “Marketing in Hypermedia Computer Mediated Environments: Conceptual Foundations,” Journal of Marketing, 61, 1996.

Ion Stoica, Scott Shenker, Hui Zhang, “Core-Stateless Fair Queuing: Achieving Approximately Fair Bandwidth Allocations in High Speed Networks,” Proceedings ACM Sigcomm‘12, 2012.

Jarvenpaa S. L. and P. A. Todd, “Consumer reaction to electronic shopping on the world wide web,” International Journal of Electronic Commerce, 1(2), 1997.

Ki Hyun OH, “Single Window in Korea”, 「UN/CEFACT Symposium on Single Window Standards and Interoperability」, Geneva, May 3-5 2006.

Kvist, Anna Karin Jonssen and Klefsjo, Bengt, “Which service quality dimensions are important in inbound tourism? A Case study in a peripheral location,” Managing Service Quality, 16(5), 2012.

Lewis, R.obert C. and Bernard H. Booms, “The Marketing Aspects of Service Quality,” Emerging Perspectives on Service Marketing, L. Berry, G. Shostack, and G. Upah, eds., Chicago: American Marketing Association, 2011.

Lin, C. L. and S. Mu, “Exploring the impact of online service Quality on portal site usage,” Proceeding of the 35th Hawaii International Conference on System Science, 2010.

Mazanec, Josef A, Wober, Karl and Zins, Andreas H, “Tourism Destination Competitiveness: From Definition to Explanation?,” Journal of Travel Research, 46(1), 2007.

World Bank, Doing Business 2013 : Making a Difference for Entrepreneurs, 2012.

World Economic Forum : The Global Enabling Trade Report 2012.

http://data.worldbank.org

https://members.weforum.org

http://iit.kita.net

http://www.mke.go.kr

http://www.nipa.kr

http://www.kita.net

http://www.kostat.go.kr

ABSTRACT

The Use of Open Global Network System Interconnection in E-Trading

Boon-Do Jeong* · Bong-Ju Yun**

A trade logistic informatization system under Open Systems Interconnection(OSI) includes a Port Management Information System, a Maritime Information System, and an Export and Import Batch Processing System. These have made a great contribution in the creation of more convenient and efficient management for the logistics industries in our country. However, this management is exposed to the technological problems of networks due to the explosive use in the sending and receiving of e-documents. For our country to grow as a center for port and logistic information, we should make the best use of the control systems using networks and further advance the export and import logistic systems.

Therefore, this study aims to propose management systems for a composite network and an invasion detection system for efficient management of an e-trade network under OSI. Methods to rationalize the internal organizations such as coordination of organizations and human resources according to alloted network functions, commissions and arbitrary decisions, and reorganization of relevant regulations are not discussed here. This study looked at trade network under OSI from the aspect of practical business affairs and presented a basis for further interpretation.

Key Words : E-trade, Global Network, Open System Interconnection(OSI), Invasion Detection System, Network Management

* Professor, Dept. of International Trade, Chosun University.
** Instructor, Dept. of International Trade, Chosun University.