인터넷貿易危險의 管理體系에 관한 考察

河 康 憲*

Ⅰ. 序 言

상인간의 商去來에는 항상 危險이 존재한다. 특히, 국적을 달리하는 국제상인과 상거래를 이행하는 국제무역에서는 더욱 그러하다. 國際貿易에 존재하는 전통적인 危險으로는, 매도인이 물품을 매수인에게 인도한 후 매수인으로부터 대금을 수령하지 못하는 信用危險(Credit Risk), 매수인이 매도인에게 대금을 지급하고도 계약에 일치하는 물품을 수취하지 못하는 商業危險(Mercantile Risk), 수입국내의 전쟁 또는 폭동 등에 의하여 매도인이 대금을 결제받지 못하는 非常危險(Contingency Risk), 변동환율제도하에서 외국환시세의 변동으로 매매당사자가 부담하는 換危險(Exchange Risk), 물리적 재화(Physical Goods)의 무역에서 운송기간 동안 물품이 위험에 노출되는 運送危險(Transportation Risk) 등이 있다. 이 중 상업위험은 매수인의 관점에서 매도인에 대한 신용위험으로 볼 수도 있으므로 광의의 신용위험에 포함시킬 수 있으며, 비상위험은 매수인에게도 존재한다. 이렇듯 많은 무역위험이 존재하고 있지만 그 중에서도 국제상인이 느끼는 가장 큰 위험은 信用危險이라 할 수 있다. 운송위험은 운송보험에 의하여 상당부분 그 위험을 관리할 수 있기 때문이다. 비록

* 蠶山大學校 通商學部 招聘專任講師.

신용위험을 관리하는 방법도 발달되어 있지만 최근에 활성화되고 있는 인터넷 貿易에서는 그 危險이 크게 노출되고 있다.

1994년 네스케이프社에서 그 동안 학술용으로만 사용하고 있었던 Web Browser를 상업적 목적으로 개발, 시판한 이래 www를 이용한 전자상거래가 급진적으로 발전하기 시작하였고 특히, 1997년 미국과 EU가 전자상거래분야에 있어 그 주도권을 쥐고자 정책안 및 선언문을 잇달아 발표함에 따라 국제전자상거래(인터넷무역) 또한 폭발적으로 증가하기 시작하였다. 한국무역협회의 조사결과에 따르면 금년에 인터넷을 輸出에 활용하는 比重이 무려 20%에 달하는 것으로 집계되었다.

하지만 인터넷무역의 비중이 증가함에 따라 국제무역에서의 위험은 전통적인 무역에서 보다 훨씬 증가할 수밖에 없게 되었다. 인터넷상에서의 거래인 만큼 상대방의 身元確認이 쉽지 않기도 하지만 인터넷 네트워크 自體에도 여러가지 危險이 도사리고 있기 때문이다. 이에 本稿에서는 전통적인 무역위험에서 중요하게 취급되었던 信用危險을 인터넷으로 관리하는 방법 및 인터넷 네트워크 自體의 危險을 管理[1]하는 방법을 體系的으로 考察해 보고자 한다.

Ⅱ. 信用危險의 管理體系

1. 인터넷貿易에서의 信用危險

인터넷貿易[2]을 하는 당사자는 거래상대방을 직접 볼 수 없기 때문에 상대방을 신뢰하기가 힘들다. 이는 전통적인 무역에서보다 인터넷무역에서 신용위험이 높아졌음을 의미하는 것이다. 실제 이러한 점을 이용하는 인터넷 무역사기

1) 危險管理(Risk Management)란 예상하지 못한 손실이 가져올 수 있는 좋지 않은 영향을 최소화할 목적으로 행하여지는 조직적, 체계적 활동을 말한다.(김두철外, 保險과 危險管理 文英社, 1999, p.13.).

2) 인터넷貿易이라 함은 반드시 인터넷네트워크를 통한 무역거래만을 의미하는 것은 아니며, 무역업무에 컴퓨터네트워크를 활용하는 것을 의미한다. '인터넷'은 이러한 모든 컴퓨터네트워크의 대표명사로 인식되고 있다. 인터넷貿易은 電子貿易(Electronic Trade), 사이버貿易(Cyber Trade), 國際電子商去來(Int'l Electronic Commerce)와 유사내지 동일한 개념으로 보아도 무방하다. (오원석外, 인터넷貿易論, 法文社, 2000, pp.183~184.).

가 급증하고 있다. 인터넷 貿易詐欺의 類型은 대체로 샘플 송부요구, 샘플비용 요구, 거래수수료 선납요구 등이다. 이러한 詐欺는 인터넷무역거래의 초기단계에 집중적으로 행하여지고 있다. 최근에는 그 手法도 多樣해지고 있다.[3]

事例 A) 인터넷 중개무역업체인 A社는 인터넷을 통해 아프리카 토고의 한 수입상과 대형 거래를 추진하다 納品 保證金 등의 名目으로 송금한 3만달러만 사기 당하고 말았다. A社는 이 수입상이 정부에 컴퓨터 1만 5000대를 공급하게 됐다며 인터넷으로 보내 온 410만달러 상당의 거래 제의를 받아들인 뒤 납품보증금, 준비자금, 수수료 등의 명목으로 수 차례에 걸쳐 3만달러를 송금했으나 결국 연락대행업체에 불과한 것으로 확인됐다.

事例 B) 전자부품업체인 B社는 인터넷검색으로 바이어리스트를 서비스하는 미국 LA소재 업체를 찾아 필요한 정보를 제공받기 위해 225달러를 送金했으나 리스트를 보내오지 않음은 물론 아예 연락이 두절되었다.

事例 C) 전자메이커인 C社도 국내 貿易去來斡旋 사이트에서 독일의 D램 공급업체와 접촉해 샘플비로 250마르크를 送金했으나 그 후 연락이 되지 않고 있다.

이렇듯 인터넷貿易의 虛點을 이용한 詐欺가 增加하고 있다. 매도인이 너무 낮은 가격으로 Selling Offer[4] 또는 Offer to Sell[5]을 제시하거나 매수인이 매도인에게 매우 유리한 조건으로 Buying Offer나 Offer to Buy를 제시한다고 하여 무조건 승낙(Acceptance)서나 조회(Inquiry)서를 전송하고 계약체결을 서두르는 것은 결코 바람직하지 못하다. 전통적인 무역에서도 강조되었던 信用調査(Credit Inquiry)의 重要性이 인터넷무역에서는 더욱 커졌다.

2. 信用危險의 管理體系

1) 信用調査

인터넷에 의하여 새로운 貿易去來가 진행되는 경우로는 ① 貿易포털(Portal)

3) 내외경제신문, 2000. 10. 3.

4) E-mail로 직접하는 매도청약.

5) 貿易專門사이트에 등재(Posting)하여 오퍼하는 경우. 이는 법적효력이 부여되는 확정청약으로 보기는 어렵다. 請約의 誘因 또는 去來提議書(Business Proposal)로 보는 것이 타당하다. (박성철, 웹사이트上의 請約의 法的性質에 관한 考察, 韓國貿易商務學會誌, 2000. 2. pp.36~37.).

사이트[6]에 등재한 자사의 오퍼를 보고 상대방이 조회를 해오는 경우, ② 業種別로 구성된 貿易보털(Vortal)사이트에 등재된 자사의 오퍼를 보고 상대방이 조회를 해오는 경우, ③ 自社의 인터넷사이트(기업 홈페이지)를 외국의 매수인이 접속하여 오퍼 해오는 경우, ④ 인터넷사이트에 오퍼나 카탈로그를 등재한 적은 없으나 해외의 무역업자가 電子 Yellow Page나 企業Directory를 통하여 문의를 해오는 경우 등으로 구분된다. 어떤 경로로 거래교섭이 시작되었던지 간에 무역업자는 상대방의 얼굴을 직접 대하지 아니한 상태에서 계약체결[7]로 이어지게 마련이다.[8] 이는 인터넷을 활용한 무역이 전통적인 무역보다 상대방을 더 신뢰하기 힘들어지는 요소가 되며, 이로 인하여 무역사기의 가능성은 훨씬 높아지게 되었다. 그러므로 인터넷무역은 전통적인 무역에서보다도 더욱 상대방의 信用調査를 필수적으로 요한다. 대다수의 무역상들은 공적인 기관에서 구축하여 놓은 무역전문사이트[9]는 무조건 신뢰할 수 있다고 생각하거나, 당해 기관에서 그 거래를 보장하고 있는 것으로 오해하는 경향이 있다. 이는 잘못된 생각이다. 貿易去來斡旋사이트의 運營者는 오퍼를 등재 해줄 뿐 당해 오퍼의 내용이나 제공자에 대한 信用을 調査하거나 保障하지는 아니 한다.

信用調査를 하는 方法은 전통적인 무역에서와 크게 다르지는 않다. 상대방의 신용조사를 하는 信用調査 照會處로는 ① 신용조사 전문회사, ② 상대방이 통지해온 은행, ③ 자신의 주거래은행, ④ 신용보증기금, ⑤ 수출보험공사, ⑥ 대한무역투자진흥공사(KOTRA) 등이 이용된다.

---

6) 무역포털사이트는 무역전문사이트라 불러도 무방하다. 무역사이트라고 하면 貿易情報提供사이트와 貿易去來斡旋사이트로 구분하여야 하지만 대부분의 무역사이트는 이 두가지 기능을 모두 수행하므로 결국 무역포털사이트, 무역전문사이트, 무역사이트 등은 同一한 槪念으로 볼 수 있다. 하지만 화학, 철강사이트 등 당해 業種別로 구성된 사이트는 무역보털(Vortal=Vertical+Portal)사이트라 칭하는 것이 옳다.

7) 電子的으로 체결된 契約도 청약과 승낙의 요건을 갖추고 있고 相互 意思合致가 이루어 졌다면 有效한 계약체결이 된다. David I Bainbridge, *Introduction to Computer Law* Fourth Edition, Pearson Education Ltd., 2000, p.274.

8) 인터넷비지니스의 短點 중 하나가 Face to Face 거래가 되지 않는다는 것이다. 음성메일이나 동영상메일이 개발되어 있기는 하나 격국 거래교섭은 인터넷폰으로 하고, 계약체결은 암호화된 E-Mail이나 전자인증기관을 통한 전자문서로 행하여질 것으로 예측된다. 그러나 이 방식도 常用化, 普遍化에는 좀 더 시간이 필요하다.

9) 한국무역정보통신의 EC Korea(www.eckorea.net), 한국무역정보통신이 투자하고 있는 ECplaza(www.ecplaza.co.kr), 한국무역협회 EC21 (www.ec21.net), 대한무역투자진흥공사의 KOBO(www.kobo.org), 산자부와 KOTRA 등 무역관련기관이 참여하고 있는Silkroad21(www.silkroad21.com),중소기업진흥공단의중소기업정보은행(www.smdb.smipc.or.kr), 농수산물유통공사의 KATI(www.kati.net) 등이 대표적이다. 綜合商社에서 운영하는 貿易專門사이트로는 삼성물산의 중소기업 전용인터넷사이트(www.findkorea.com), (주)쌍용의 인터넷무역사이트(www.ssytrade.co.kr) 등이 있다.

인터넷무역계약체결을 위한 신용조사에도 인터넷을 활용하면 편리하다. ①의 信用調査專門機關으로 Dun & Bradstreet, American Research Bureau Inc.[10] 등이 있다. 특히 Dun & Bradstreet는 세계적인 신용평가기관인 Moody's Investors Service 등 20여 개의 자회사를 거느린 정보 서비스 회사로서 155년 이상의 역사를 지니고 있다. 국내은행, 공공기관은 물론 30대 그룹 대부분이 D&B사를 이용하여 위험관리를 하고 있다.[11] ④의 信用保證基金에서는 무역금융, 보증은 물론 신용조사 등의 서비스를 제공하고 있는데 신용조사와 관련된 문제를 인터넷사이트를 통하여 상담할 수 있다.[12] ⑤의 輸出保險公社의 사이버 수출보험에서는 국내 수출업체가 필요로 하는 각종 해외신용정보자료를 수집하여 제공하고 있는데 해외의 8개 사무소, 65개의 해외전문신용조사기관 및 KOTRA 등과의 업무제휴를 통하여 입수한 정보자료를 제공하고 있다.[13] ⑥의 大韓貿易投資振興公社(KOTRA)에서는 KOTRA해외무역관을 통해 상대방의 신용상태를 조사하는 서비스를 제공하고 있다. 역시 인터넷을 통하여 신용조사 신청을 할 수 있는데 조사기간은 약15일 정도이다.[14]

2) 身元確認

(1) 暗號化에 의한 電子署名認證

인터넷무역에서는 상대방에 대한 신용조사의 결과가 만족하다고 하여 무턱대고 상대방과 무역계약을 체결할 수는 없다. 왜냐하면 상대방이 인터넷으로 전자메시지(전자문서)를 전송하고도 電送한 事實을 否認할 가능성이 있기 때문이다. 당사자의 身元을 確認하는 방법으로는 당해 전자문서를 암호화하여 전송하도록 요구하는 방법 즉, 암호화에 의한 電子署名認證을 통하여 確認하는

---

10) http://www.arbi.com, "place an order"로 신청하면 약 15일 정도 조사기간이 소요된다.
11) http://www.dnb.com, "Contact us"에서 지역별, 국가별 담당자에게 신청하면 된다.
12) http://www.shinbo.co.kr, "신용보증기금소개" 참조.
13) http://www.cyber.keic.or.kr:8000/, "신용조사의뢰"를 통하여 신용조사를 의뢰할 수 있다. 비상위험을 관리하는 데에도 수출보험공사를 이용하는 것이 가장 좋은 방법이다. 수출보험공사에서 서비스하는 사이버수출보험(Cyber KEIC)에서는 수출보험도 One-Stop으로 처리할 수 있는 통합서비스를 제공하고 있다.
14) http://www.kotra.or.kr, 고객지원센터, "신용조사"를 통하여 신청할 수 있다. 건당 비용은 12만원정도이다. 주요조사내용은 상대방기업의 설립년도, 고용인수, 업종, 취급품목, 자본금, 거래은행, 연간매출액, 수출입 실적 등이다.

방법이 보편화되어 있다. 암호화한 문서라면 상대방이 전송하고 그 암호화키를 통지해 주지 아니하였다면 수신한 당사자가 그 전자문서를 보유하고 있을 수 없기 때문이다. 그러나 암호화된 전자문서의 수령은 전송사실을 부인하지 못하도록 하는 否認防止效果는 있지만 그러한 전자문서를 전송한 상대방이 명망있는 기업으로 僞裝하고 去來하는 것을 방지해 주지는 못한다. 그러므로 상대방에 대한 신원확인이 필요한데 신원확인(본인인증)의 방법으로는 電子認證書를 요구하는 것이 보편화되어 있다. 전자인증서는 인증기관으로부터 발급 받는데 이러한 방식은 네트워크상의 위험을 관리하는 방법으로도 적합하므로 第Ⅲ章에서 상세히 살펴보고자 한다.

(2) 指紋認證

최근 身元確認의 방법으로 새로이 대두되고 있는 指紋認證에 관하여 살펴보고자 한다. 그 동안 출입통제시스템에만 활용되어온 지문인식시스템이 최근 전자상거래의 인증방식으로 급속도로 확대되고 있다.[15] 아직은 국내전자상거래에 한정되어 사용되고 있으나 인터넷무역에도 활용될 가능성이 높다. 이것은 거래 양당사자가 지문인증서비스 제공회사에 먼저 指紋을 登錄해 놓고 指紋認證만으로 상대방에 대한 身元認證을 하는 방식이다. H社의 지문인증시스템은 웹을 기반으로 구축되어 있어 인터넷에서 지문인증만으로 신원을 확인할 수 있으며,[16] B社는 S전자의 기업용 서버컴퓨터에 지문인식시스템을 탑재하여 보안장치의 역할을 하고 있다.[17] P社도 인터넷상에서 지문인증만으로 은행거래가 가능한 생체인증시스템을 개발하여 상용화하고 있다.[18] 지문인증이 인터넷무역전반에 도입되기에는 많은 시일이 필요할 것으로 예상되긴 하지만 인터넷무역절차에 있어 운송계약체결, 보험계약체결, 은행에의 매입신청 등 國內部門의 업무에는 조만간 指紋認證이 活用될 수 있으리라 기대된다.

15) 내외경제신문, 2000. 10. 17, 11. 2일자.
16) www.hunno.com. 참조.
17) www.biovison.ne.kr. 참조.
18) www.pass21c.co.kr. 참조.

3) 信用狀의 活用

신용조사 및 신원인증이 되었다고 하여 매도인이 매수인으로 물품대금을 확실히 지급 받거나, 매수인이 매도인으로부터 계약물품을 확실하게 인도수령한다는 보장은 없다. 그러므로 인터넷 貿易當事者는 기존의 信用狀 制度를 活用하는 것이 바람직하다. 명망 있는 개설은행으로부터 신용장을 입수하는 것이 바람직하며 개설은행 자체의 명성이나 신용상태가 미흡하다면 당해 신용장에 確認(Confirming)을 요구하여야 한다.

인터넷무역시대에는 신용장이 불필요하다고 생각하는 무역업자가 다수 있는데 이는 잘못된 생각이다. 강조하거니와 무역전문사이트에 게시된 Offer to Buy나 Offer to Sell에 대하여 사이트 운영자가 그들의 신용을 보장하는 것은 결코 아니다. 다만 오퍼를 게시해줄 뿐이다. 만일 인터넷상에서 만난 매수인이 신용장 개설을 꺼려한다면 물품대금을 先支給 받는 것이 좋다. 다른 방법으로는 信用狀을 근간으로 하는 國際貿易시스템인 Bolero 시스템을 이용하길 권장하고 싶다. 신용장 없이 무역거래를 하는 것보다는 이 시스템을 이용하는 것이 훨씬 안전하다.

4) 國際貿易시스템의 活用

국제문서전송 및 대금결제시스템(국제무역시스템)으로 주목받고 있는 Bolero[19] 및 T/C(Trade Card)[20] 시스템이 국내에도 도입되었다. 이 중 前者는 信用狀制度를 근간으로 하고 있으나 後者는 신용장 없는 국제무역을 수행하는 시스템이지만 대신 運營主體가 代金支給을 保障한다고 한다. 하지만 이 두 가지의 국제무역시스템이 위험 없는 인터넷무역을 확실하게 보장할 수 있을지의 여부는 좀 더 시간을 두고 판단하여야 한다. 이 중 Bolero는 信用狀을 기반으로 하고 있고 또한 운영주체로 SWIFT(세계 은행간 금융전산망)가 참여하고 있어 현 상태로서는 인터넷貿易[21]의 危險管理에 보다 適合할 것으로 평가된다.

---

19) www.Bolero.net.

20) www.Tradecard.com.

21) 국제문서전송 및 대금결제는 SWIFT망으로 이행되므로 인터넷무역이라는 용어는 엄밀히 분석하면 잘못된 것이라 할 수도 있으나 인터넷貿易의 槪念은 전자적(컴퓨

(1) Bolero 시스템

이 시스템은 무역거래에 필요한 종이문서를 전자적 문서로 전환하여 안전하게 교환할 수 있는 것을 목표로 하여 1994년 6월 영국, 미국, 네덜란드, 스웨덴 등의 운송회사, 은행, 통신회사 등이 컨소시엄 형태로 시작되었는데[22] 선화증권만의 전자화가 아닌, 船貨證券을 포함한 무역서류 전반에 걸쳐 電子化를 추구하고 있다. 이 시스템에서는 무역당사자간의 權利義務關係를 명확히 하기 위해 'Rule Book'[23]을 도입[24]하고 있다.[25] 이 시스템을 운용하는 BOL[26]은 電子署名의 認證機關의 역할을 수행하게 된다. 이 시스템을 이용한다고 하여 화환신용장거래에서 은행이 수행하던 선적서류의 심사를 하지 않는 것은 아니다. 즉 이 시스템은 기존의 은행업무는 그대로 존속하게 되고, 단지 문서의 전송이 전자적으로 이루어지는 것이다. 文書의 標準은 UN/ EDIFACT 표준을 이용하게 되며 文書의 保管管理도 BOL에서 수행하므로 훗날의 분쟁발생시 證據的 效力을 가질 것으로 추정된다.[27] 암호체계는 국제적으로 보편화된 RSA방식[28]을 채택하고 있다.

터)네트워크를 활용한 무역을 代表하는 用語라고 보는 편이 마땅하다.

22) www.Bolero.net, 볼레로넷은 한국무역정보통신(KTNET), 한빛은행, 삼성전자 등과 제휴하여 국내에 진출하였다. 외환은행과 한빛은행은 6월부터 볼레로서비스망을 시범운영한 후 2001년 1월부터 본격서비스에 들어갈 예정이다.(내외경제, 2000. 5. 10.)

23) Rule book에 서명하면 다른 모든 서명자와의 거래에서 공통적으로 적용되므로 일일이 當事者間에 교환약정을 체결할 필요는 없다.

24) J. Livermore & K. Euarjai, "Electronic Bills of Lading: A Progress Report", *Journal of Maritime Law and Commerce* vol. 28. No.1, January, 1997, p.58.

25) Bolero 規約集에서는 본 규약집이 英國法의 적용을 받고 영국법에 따라 해석되어야 한다고 규정(2.5(2))하고 있고, 부록의 미국법조항에서는 美國海上運送法이 삽입된 것으로 간주(규약집 부록(1)(2))하는 등 일국의 법을 準據法으로 지정해 놓은 점, 讓渡可能이라는 용어를 신용장에 적용하는 'transferable'을 사용하고 있는 점 등의 問題가 있기도 하다. (최석범, 글로벌 전자무역시대에서의 볼레로 선화증권의 기능과 문제점, 한국무역상무학회지, 2000. 8, pp.208~209.).

26) SWIFT(세계은행간 금융전산망)와 TT club(Through Transport club ; 해상화물운송의 P&I 클럽)에 의해 설립된 Bolero project의 상업적 서비스 제공회사인 Bolero Operation Ltd를 말한다. 벨기에에 본부를 두고 있는 SWIFT에는 현재 188개국 7000여개 금융기관이 가입하고 있다.

27) 기계적 또는 자동기록장치에 의한 기록은 실제적 증거로 인정되며, '기계적' 또는 '자동의' 범주에는 전자적 기록도 포함된다 法院은 반대의 증거가 없다면, 그 당시 정상적으로 작동하고 있었던 기계에 의한 증거도 實際的 證據라고 본다(the Court of Appeal in R. V. Spiby(1990) 91 Cr. App. Rep. 186). Michael Chissick, Alistair Kelman, *Electronic Commerce : Law and Practice* , London Sweet & Maxwell, 1999, pp.144~145).

28) 대표적인 공개키 방식의 암호알고리즘(변환체계)으로 매우 큰 정수의 소인수분해는 어렵다는 가정하에서 설계된 암호체계이다(Peter Wayner, *Digital Cash Commerce on the Net,* AP Professional, 1996, p.25).

(2) T/C 시스템

세계무역센터협회(WTCA)[29]는 FSTS(Full Service Trade System Ltd.)라는 자회사를 구성하여 TradeCard라는 輸出入書類의 전송 및 代金決濟를 電子化하는 시스템을 구축하였는데 貨換信用狀의 개입을 排除하고 있다.[30] 이 시스템에서는 신용장개설은행의 서류심사기능을 대신하며,[31] 은행은 자금의 공여만을 담당하게 된다. 이 시스템은 거래당사자간 전자적 계약의 확인, 계약이행여부의 확인, 대금지급여부의 결정 등 전자적 계약의 체결에서 종료에 이르기까지 중계역할을 한다. 去來當事者의 信用評價는 세계최대 수출신용보험회사인 Coface社가 자체 신용평가시스템으로 거래사의 信用을 評價하고 代金決濟를 保障한다. Rule Book과 같은 규칙협정은 없다. 문서의 교환표준은 UN/EDIFACT에 따르고 있다. 암호체계도 RSA방식을 채택하고 있다.

신용장이나 선화증권을 배제하고도 국제거래에서 큰 위험이 뒤따르지 아니하는 소액거래, 소비자매매 또는 해외자회사와의 거래 등에서는 Trade Card를 많이 활용할 것으로 예측된다. 그러나 信用狀의 개입이 필요하거나 船貨證權의 발행이 필요한 경우[32] 등 대기업의 인터넷무역에서는 Bolero 시스템이 많이 활용될 것으로 예상된다.[33]

5) 電子貿易仲介機關의 活用

인터넷 등 가상공간을 통한 인터넷무역거래에서 최대 난제로 꼽혀온 거래상대방의 신원 보장과 신용 정보, 인터넷 전자문서교환(EDI) 서비스를 제공하

29) 현재 1백1개국 337개 도시에 센터가 있다.

30) www.tradecard.com, 트레이드카드는 LG상사, SK글로벌 등과 공동출자하고 조흥은행과는 업무제휴를 통하여 트레이드카드코리아를 설립하였다. 지난 8월 국내서비스를 개시하였다. 트레이드카드코리아의 자본금은 100만불이다.(내외경제신문, 2000. 8. 3. 참조.).

31) 운송서류로서 전자식 선화증권을 배제하고 있지는 아니하지만 電子式 海上貨物運送狀의 실용화를 표명하고 있는 점에 비추어, 운송 중 전매를 요하지 아니하는 거래에 적합할 것으로 보인다.

32) Bolero 서비스는 Incoterms 2000에서도 전자식 선화증권발행의 例로서 설명되고 있다(Incoterms 2000. Introduction.19).

33) 볼레로시스템에서는 거래주도권을 銀行이 가지고, 트레이드카드에서는 貿易會社가 가진다고 구분하는 견해도 있다. 한국경제신문, 2000. 4. 21. 볼레로는 英國중심이고 트레이드 카드는 美國중심으로 英·美대결이라고 보기도 한다. (내외경제신문, 2000. 8. 3.).

는 電子貿易仲介機關이 내년 중 활동을 시작할 것으로 예상된다. 2000년 5월 산업자원부는 電子貿易仲介機關 設立 등의 내용을 골자로 한 대외무역법 개정 시안을 발표했다.[34]

또 전자거래기본법이나 전자서명법 등 흩어져 있는 전자무역지원관련 규정을 대외 무역법으로 통합, 개편하고 전자무역촉진을 위한 산자부 장관의 시책 수립 및 추진 의무를 명확히 했다. 또 가상 공간에서 눈에 보이지 않는 거래 상대방과 거래할 수 있도록 전자무역 公認認證마크制度[35]가 새로 도입되고 전자무역중개기관을 통한 電子文書나 署名은 기존 법령이 정한 문서나 記名捺印으로 간주된다.

Ⅲ. 네트워크危險의 管理體系

1. 네트워크 危險의 類型

네트워크상에서 保安(security)을 위협하는 공격의 유형은 ① 중요한 정보가 제3자에게 알려지는 機密性 (confidentiability)공격, ② 네트워크상에서 중요한 정보가 개조되는 無缺性(integrity) 공격,[36] ③ 네트워크상에서 누군가로 위장하여 정보를 송신하는 認證性(authenticity) 공격, ④ 전자적으로 메시지나 결제된 금액을 수령하고도 이를 수령치 아니하였다고 하는 否認(repudiation) 공격 등이 주류를 이룬다.[37] 이러한 위험을 제거하기 위하여 암호기술을 이용한 디지털 서명[38]과 같은 인증방식이 사용되고 있다. 그렇다고 하여 인터넷무역

34) 내외경제신문, 2000. 5. 7.

35) 公認認證마크制度가 인터넷무역사이트업자를 인증하는 것인지, 당해 사이트에 오퍼를 게재한 무역업자를 인증하는 것인지는 불확실하지만 前者라면 인터넷무역업자의 위험을 관리하는데 별다른 도움을 주지는 못할 것으로 본다.

36) 가령, 전자결제시 수신계좌가 개조되는 경우. S/W 공급자(Software Server)는 자신의 데이터가 접속자나 해커에 의해 개조되는 위험을 지니고 있다. (Ravi Kalakota, Andrew B. Whinston, *Frontiers of Electronic Commerce,* Addison-Welsley Publishing Company, Inc., 1996, p.183.).

37) 송유진 外, 전자상거래가 세상을 바꾼다.(i포스트, 1999, p.133.).

38) 電子化된 環境에서는 변조흔적 등의 물리적 특성이 이용불가능하기 때문에 그러한 물리적 특성을 사용하지 않고 認證할 수 있는 技術이 필요한데 이 요구에 부응하는 기술이 디지털署名이다. (이임영외 共譯, 현대암호, 생능출판사, 1999, p.179.).

당사자의 위험요소가 모두 제거되는 것은 아니다.[39] 인터넷무역당사자는 보안체계의 기술적인 면을 잘 이해할 수 없을 뿐만 아니라 전적으로 신뢰할 수는 없기 때문이다. 특히 인터넷에서는 타인의 정보에 접근할 기회가 사설망으로 구성된 컴퓨터망에 비해 훨씬 많고 그 방법도 다양하다.

1) 해킹의 類型

인터넷 네트워크상의 공격위험을 좀 더 이해하기 위하여 기초적인 인터넷상의 해킹[40]기법인 Packet Sniffing과 IP Spoofing에 대하여 살펴보고자 한다.

(1) Packet Sniffing

인터넷상에서 정보를 송수신할 때에 가장 기본이 되는 정보 단위는 패킷(Packet)이다. 스니퍼(Sniffer)란 이와 같이 네트워크의 한 호스트에서 실행되어 그 주위를 지나다니는 패킷(Packet)들을 엿보는 프로그램인데 인터넷 사이트에서도 쉽게 구할 수 있다. 일반적으로 패킷들은 이더넷(Ethernet : 네트워크 연결 시스템의 일종) 케이블을 타고 전송되는데 이더넷을 통한 통신방법은 매우 간단하다.[41] 네트워크 보안을 철저히 한 호스트라도 주변의 호스트가 침입을 당해 스니핑(Sniffing)을 위해 사용된다면 무력해 질 수밖에 없다.

---

39) 인터넷 자체가 단순하면서도 공개적으로 데이터를 전송하도록 고안되었기 때문에 인터넷망 자체는 데이커의 가로채기나 정보의 개조를 방지할 수 있는 시스템은 아니다. website를 威脅하는 要素로는 ① 외부적 위협, ② 내부적 위협, ③ 물리적 위협, ④ 데이터관련 위협 등이 있다(Martin Nemzow, *Building Cyberstores-Installation, Transaction Processing, and Management-*, McGraw-Hill, 1997, pp.295~296).

40) 금년 9월말 현재 한국정보보호센터에 신고된 해킹 被害事例는 1475件으로 작년보다 4배 증가하였다. 내외경제신문, 2000. 10. 18. 미국에서의 연간 피해액은 100억달러에 달하는 것으로 추정된다. (내외경제신문. 2000. 4. 21). G8 政府와 민간기업들이 인터넷犯罪 對應策을 논의하기 위한 '하이테크 정부·산업 공동회의'가 5월 15일 파리에서 개최된 바 있다. (조선일보, 2000. 5. 22.).

41) 例를 들어 A라는 호스트가 B라는 호스트로 패킷을 보내고 싶다면 호스트 A는 호스트B와 배타적인 연결을 하는 것이 아니라 그 패킷을 이더넷에 올려 놓는다. 그리고 그 패킷은 일반적으로 수신 주소의 호스트만이 받도록 기대된다. 즉, 자신에게 오지 않는 패킷은 받지 않으므로 호스트 B만이 호스트 A가 보내는 패킷을 받게 된다. 그런데 호스트 B가 아닌 다른 호스트가 그 패킷을 무시하지 않고 그 내용을 해커에게 전달해 준다고 가정하면 문제가 될 수 있다.

(2) IP Spoofing

IP Spoofing은 해커가 머물러 있는 호스트의 IP 주소를 바꾸어서 이를 통해 해킹을 하는 것이다. 즉 자신이 진정한 호스트라고 僞裝하기 위하여 머물고 있는 호스트의 IP주소를 바꾸어 이용하는 것이다.[42]

2) 바이러스의 類型

지난 5월 '러브바이러스', 11월에는 '나비다드'라는 바이러스가 메일로 유포되어 컴퓨터사용자들을 긴장시키기도 하였지만 컴퓨터사용자들은 바이러스에 의한 해킹危險에도 항상 노출되어 있다. 특히, 시스템파괴 바이러스는 인터넷 貿易業者의 소중한 전자문서파일을 한꺼번에 파괴할 수도 있으므로 매우 注意를 요한다. 컴퓨터 바이러스의 종류는 이루 말할 수 없을 정도로 다양한데 여기서는 몇 가지 형태의 바이러스 類型을 살펴보고자 한다.[43]

(1) 화이트바이러스

멜리사보다 더 강력한 국내 최초의 시스템파괴 바이러스다. 15세짜리 중학생이 만들어 유포했는데 매달 31일 활동한다. 화면에 웜 화이트란 창이 뜨면 감염된 것인데 창을 건드리지 말고 컴퓨터의 날짜를 바꾸고 백신으로 치료해야 한다.

(2) 조크 프로그램

시스템에 문제를 일으키지는 않지만 바이러스로 誤認하게 해 사용자에게 혼

42) 例를 들어 A란 호스트와 B란 호스트가 하드디스크를 공유하고 있는데 A란 호스트와 B란 호스트는 보안이 잘 되어서 해킹하기가 어렵다고 할 경우 우선 해커는 자신이 머물러 있는 호스트의 IP 주소를 B의 주소로 僞裝을 한다. 僞裝을 하면 B의 호스트 화면에는 Duplicate IP Address라는 문장이 나타나게 되고 B호스트는 네트워크의 기능을 잠시 상실하게 된다. 이때 해커의 호스트는 A호스트에게 자신이 진정한 B호스트라는 정보를 보내어 A호스트와 같이 하드디스크를 공유하도록 시도한다. 성공하게 되면 해커는 A호스트의 하드디스크에 있는 정보를 A호스트나 B호스트에 잠입하지 않고서도 얻어낼 수 있게 된다.

43) 내외경제신문, 2000. 4. 21. 참조.

란을 주는 가짜 바이러스다. 만우절에는 1만여 건의 피해사례가 접수되기도 했다. 이 프로그램이 작동하면 멈추기를 기다린 뒤 백신으로 처리해야 한다.

(3) 지능형 웹 바이러스

공유기능이 설정된 컴퓨터 중 패스워드가 걸려 있지 않은 것만 골라 침투한다. 전세계로 급속히 확산되고 있다.

(4) 네트워크 자동추적 바이러스

컴퓨터 네트워크를 통해 감염된다. 임의의 IP주소를 결정하고 그 IP의 네트워크를 공유 검색해 PC를 찾아가는 방법으로 전파되기 때문에 감염속도가 빠르고 다수를 공격한다.[44]

2. 네트워크危險의 管理體系

1) 保安시스템에 의한 危險管理

(1) 保安시스템 設置

防火壁(Firewall)[45]은 내부의 전산망을 인터넷 등 외부망과 연결하거나 기업내 사설망을 구축할 경우 외부사용자 또는 기업간 사설망의 전자도청으로부터 내부의 중요한 기밀과 정보를 보호하기 위해 구축하는 침입차단 電子保安시스템이다. 방화벽이 없는 환경에서 네트워크 보안은 호스트 시스템의 보안에 전적으로 의존하게 되며 네트워크에 연결된 모든 호스트가 일정한 역할을 분담한다. 그러나 네트워크가 커지면 보안통제가 어려워지게 된다. 따라서 보안하고자 하는 네트워크의 接近을 統制하는 방화벽 설치가 요구된다.[46]

---

44) 이외에도 상대방 컴퓨터에 몰래 들어가 정보를 빼내는 백오리피스, 상대방 메일 서버에 지속적으로 악의적인 메일을 마구 보내 작동을 멈추게 하는 카붐 3, 타인의 통신 ID를 빼내가는 드리퍼 등이 잘 알려진 컴퓨터 바이러스이다.

45) 방화벽이란 내부정보시스템과 외부정보시스템의 連結地點에 설치되어 각 시스템의 보안수준에 따라 적절하게 제어될 수 있도록 마련된 情報保安시스템이다. 흔히 침입탐지기 또는 침입차단시스템이라고도 한다.

46) 방화벽의 유형으로는 PFF(Packet Filtering Firewall), DGF(Dualhomed Gateway

인터넷 保安 솔루션 提供業體

분 야	업 체
방화벽(Firewall)/ 침입탐지기	시큐어소프트(www.securesoft.co.kr), 어울림정보기술(www.oullim.co.kr), 한국정보공학(www.kies.co.kr), 시만텍코리아(www.symantec.com)
암호화	소프트포럼(www.softforum.com), 이니텍(www.initech.com), 장미디어인터렉티브(www.jmi.co.kr)
전자인증/서명	한국전자인증(www.crosscert.com), 한국정보인증(www.signgate.com), 엠아이시큐리티(www.misecurity.com)
전자메일보안	쓰리알소프트(www.3rsoft.com),
바이러스백신	안철수연구소(www.ahnlab.com), 하우리(www.huari.co.kr)
해킹방지	해커스랩(www.hackerslab.org)
데이터복구	씨앤씨(www.candc.co.kr), 명정보기술(www.myung.co.kr)

방화벽은 외부의 불법침입으로부터 내부시스템을 보호하며 내부시스템의 정보가 외부로 유출되는 것을 막아 내부시스템의 보안을 유지한다. 방화벽이 外部의 접근을 적절히 제어할 수 있는 接近制御 시스템과 內部의 사용자 책임과 권한에 따른 認證制御시스템이 적절한 조화를 이루면 안전한 保安시스템이 구축된다.[47] 우리 나라의 情報通信 서비스提供者는 정보통신 서비스보호지침에 의거 9월 1일부터 防火壁 등 정보보호장치를 義務的으로 設置하여야 한다.

(2) 保安서비스業體에 의한 危險管理

지금까지 保安業體라고 하면 방화벽(Firewall), 침입탐지시스템(IDS), 바이러

Firewall), SHF(Screened Host Firewall), SSF(Screened Subnet Firewall) 등이 있다.

47) 무리한 방화벽을 설치할 경우 설치자 또한 이에 출입하지 못 할 수도 있다.

스 백신 서버, 가상사설망(VPN), 전자상거래 관련 보안(인증·전자지불·PKI) 등을 수입·판매하거나 개발·판매하는 회사들을 지칭하는 것이었다.

그러나 향후 보안업체의 개념은 보안 솔루션을 전문으로 개발하는 업체와 이런 제품들을 가지고 고객들과 직접 만나 서비스를 제공하는 保安서비스業體로 구분될 전망이다

保安서비스業體의 必要性

保安管理의 問題點	保安서비스業體의 役割
◦보안전담 인력부족 (보안담당자의 기술수준 미흡) ◦전사적인 보안전략 부재 ◦각각의 보안장비 및 소프트웨어에만 지나치게 의존 ◦보안대책의 복잡화, 기능화, 다양화 요구에 대한 통합보안서비스 구현이 어려움	◦모든 보안상황을 24시간 모니터링하며 실시간 온라인으로 보안현황제공 ◦보안전문가에 의한 보안환경분석 및 체계적 관리를 제공 ◦보안정책 수립, 진단, 제품설치, 유지보수교육 등 보안전략컨설팅을 통한 토털솔루션을 제공 ◦효과적인 보안예산의 적절한 집행이 가능

출처 : 내외경제신문, 2000. 10. 7일자.

이제까지 보안시장의 중심은 방화벽과 바이러스 백신서버였다. 95년경부터 시작된 방화벽과 바이러스 백신 시장은 98년까지 공공기관과 금융기관을 중심으로 형성됐으며 99년부터 IDS와 VPN시장이 새롭게 가세하면서 보안시장의 규모는 더욱 커졌다.[48] 그러나 시차를 두고 보안제품들이 설치됨에 따라 설치된 보안제품이 상호연동이나 통합이 되지 않아 기업전체 보안시스템 관리에 문제가 발생하기 시작하였다. 더욱이 보안제품의 설치 이후 이를 效率的으로 管理할 수 있는 인력이 없어 문제되는 경우가 많았는데 이런 문제를 해결해 주는 업체가 保安서비스 業體이다.[49]

48) 금년 인터넷보안시장의 규모는 2000억원 정도이나 매년 2.5-3배 급성장할 것으로 전망된다. (내외경제신문, 2000. 10. 7.).

49) 1999년 말부터 등장하기 시작한 대표적인 보안서비스 업체들은 사이버패트롤(www.cyberpatrol.co.kr), 시큐아이닷컴(www.secui.com), 코코넛(www.coconut.co.kr), 등 5~6개사이다.

인터넷무역업체뿐만 아니라 컴퓨터 네트워크를 보유하고 있는 기업체는 해킹위험을 제거하고 효율적으로 보안시스템을 관리하기 위해서 保安서비스業體를 利用하는 것도 바람직한 방법이다.

2) 制度的 側面의 危險管理

(1) 電子認證機關의 活用

가. 暗號化에 의한 電子認證

受信者가 수령한 내용의 위조 또는 삭제 여부와 상대방의 신분을 確認하는 방법이 電子認證이다. 前者의 인증을 메시지 認證(Message Authentication), 後者의 인증을 本人認證(Entity Authentication)이라 한다.[50] '認證'이라 함은 전자서명검정키가 자연인 또는 법인이 소유하는 전자서명키에 합치한다는 사실을 確認·證明하는 행위를 말한다.[51] 이러한 인증을 수행하는 데에는 암호기술을 이용한 디지털 서명이 효과적이다.[52]

데이터를 暗號化하는 方式은 크게 대칭키 암호방식(symmetric cryptosystem)라 비대칭키 암호방식(asymmetric cryptosystem)으로 구분된다. 대칭키 암호방식은 암호화하는 키와 복호화하는 키가 동일하므로 암호화, 복호화키가 모두 비밀키로 구성된다. 그래서 이를 秘密키(private key) 암호방식이라고도 한다. 비대칭키 암호방식에선 공개된 키가 암호화 또는 복호화 기능을 수행하게 되므로 公開키(public key) 암호방식이라고도 한다.[53]

① 秘密키 暗號方式

데이터를 암호화, 복호화하는 키가 모두 비밀키(공통키, 대칭키)로 동일한 암호방식이다.[54] 이 방식은 1970년대 초부터 상업적인 통신망에서 이용되어 있

---

50) 이만영 外, 전자상거래보안기술, 생능출판사, 1998, p.21.

51) 電子署名法 제2조 제6항.

52) Thomas F.Rebel, Wolfgang Koening., "Key Issues in Ensuring Security and Trust in Electronic Commerce" ; Edited by Jae Kyu Lee, Steven H. Kim, Andrew B. Whinston, Beat Schimid, *Proceedings of The International Conference on Electronic Commerce* '98, International Center for Electronic Commerce, 1998, pp.327~328.

53) Peter Wayner, *op. cit.*, 1996, p.19.

54) 최초로 상업적으로 이용된 공통키 암호방식은 DES(Data Encryption Standard)이

다. 그러나 이 방식은 송신자와 수신자가 同一한 키를 사용하기 때문에 키를 안전하게 전송하거나 키가 너무 많기 때문에 保管하는데 있어 問題點을 드러내기 시작하였다.[55] 비밀키 암호알고리즘은 DES방식이 많이 사용된다.[56]

② 公開키 암호방식

공개키 암호방식은 개인이 소지한 비밀키와 일반에 공개된 공개키가 이용되는 방식이다. 이 방식은 데이터 송·수신자간에 다른 암호키를 사용하므로 수신자가 송신자에게 비밀키를 분배하지 않아도 되며, 自身의 公開키만 공개하면 되므로 便利하다. 공개키 암호알고리즘은 RSA방식이 많이 사용된다.[57]

나. 電子認證機關의 活用

인터넷무역당사자는 당해 거래의 安全性을 확보하기 위해 암호기술을 이용한 전자서명을 이용하여 문서를 전송하게 된다. 그런데 수신자는 이러한 기술적 측면에 대한 완전한 신뢰를 가지지 못하는 것이 일반적이다. 이러한 전자상거래 당사자의 심리적 불안을 제거해 주는데 있어 가장 바람직한 방법이 제3의 신뢰된 기관이 당해 거래의 인증을 해주는 것이다.[58] 인터넷무역업자는 認證機關[59](CA : Certification Authority)[60]으로부터 전자인증서[61]를 발급 받고

다. DES는 1974년 미국 상무성으로부터의 공식적인 요청에 따라 IBM이 개발하였고, 1977년에 미국 연방 표준으로 채택되었다. (M.E. Smid, D.K. Baranstad, "The Data Encryption Standard : Past and Future", Proceedings of the IEEE(Vol. 76), 1988.5, pp.550~559.).

55) 전자상거래에서 비밀키 암호방식이 주도적 역할을 하기는 어렵다. (Ravi Kalakota, Andrew B. Whinston, *Electronic Commerce-A Manager's Guide,* -Addison-Wesley Longman Inc., 1997, p.139.).

56) 비밀키 방식의 암호알고리즘으로는 DES, FEAL, RC5, IDEA 등이 있다. 이 중 DES (Data Encryption Standard)방식이 가장 많이 사용된다. (이민섭, 현대암호학, 교우사, 1999, pp.144~146 참조.).

57) 公開키 暗號方式으로는 RSA, Rabin, LUC, Knapsack, McEliece 등이 있다. RSA 暗號方式은 소인수분해의 어려움에 그 기반을 두고 있는 공개열쇠암호이다. 공개열쇠 암호시스템에 대한 개념을 가장 충실히 반영한 암호방식이 RSA이다.(이민섭, 전게서, p.307.).

58) David Kosiur, *Understanding Electronic Commerce,* Microsoft Press, 1997, p.75.

59) 인증기관이란 認證役務를 제공하는 자를 말하는데 인증업무란 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하는 업무를 말한다. 인증기관의 주요업무는 ① 인증서 발급 ② 인증관련 기록관리로 구분할 수 있다.

60) 認證機關은 公開키 기반을 구조로 한다. 公開키 기반구조(PKI, Public Key Infrastructure)는 두 가지 방식으로 구성되는데, 이는 최상위 인증기관인 Root CA에 바탕을 둔 순수계층 구조방식과, 모든 인증기관이 평면적으로 구성되는 네트워크 구조 방식이 있다. (이만영 外. 전자상거래보안기술, 전게서, pp.163~1674.).

61) 認證書를 發給받는 節次는 먼저, 사용자(A)가 인증기관에 인증서발급을 요청하면 인증기관은 등록기관(RA ; Registration Authority)에게 인증서의 심사를 의뢰하게

전자문서를 송수신하는 것이 바람직하다. 이는 신원 및 메시지 미확인에 따르는 위험을 관리하는데 있어 가장 확실한 방법이다. 그러나 인증기관도 해당국가의 법에 따라 인증기관으로 인정된 公認認證機關[62]과 인증기관 스스로의 신뢰를 바탕으로 인증업무[63]를 행하는 私設認證機關으로 구분하여야 한다. 정보통신부장관은 인증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 공인인증기관으로 지정할 수 있는데,[64] 정부통신부 장관에 의하여 지정을 받아 인증업무를 제공하는 자가 公認認證機關이다.[65] 우리 나라는 공인인증기관제도만을 택하고 있다.[66]

우리 나라는 1999년 7월 1일부터 전자서명법이 시행되어 현재 3개의 公認認證機關을 지정해둔 상태이다.[67] 美國은 몇 개 州를 제외하고는 공인(License) 제도를 채택하지 않고 있다.[68]

향후 國內의 公認認證機關은 SET Co,[69] GTE 등 외국의 사설 인증기관과

된다. 이때 登錄機關은 보안확인과 여신체크 후 인증서 발행의 가부를 판정한다. 등록기관이 인증서 발행이 가능하다고 판정하면 認證機關은 자신의 디지털서명을 부가한 인증서를 발행하여 사용자에게 인증서를 발급하게 된다. 그러면 사용자(A)는 자신의 비밀키로 암호화한 메시지를 전자인증서와 함께 상대방(B)에게 전송하고 상대방(B)은 (A)의 공개키로 복호화하여 메시지가 본인에 의한 것임을 확인하게 된다. 즉, 사용자는 認證機關으로부터 認證書를 발급받지만 그 인증서의 發給與否는 登錄機關에서 결정하게 된다. 디지털 인증서는 보통 ① 사용자의 이름, 기구(단체), 주소 ② 인증기관의 서명 및 ID정보 ③ 사용자의 공개키 ④ 디지털 ID의 유효기일 ⑤ 인증서의 종류 ⑥ 디지털 ID의 인증서 번호 등으로 구성된다(David Kosiur, *op. cit.*, p.76 Figure 4~5).

62) 公認認證機關은 네트워크에서 거래를 하는 당사자의 身元確認, 전송되는 정보의 變質與否, 거래당사자간의 정보송수신에 대한 否認防止 등의 公認認證서비스를 제공한다. (한성일, 인터넷전자상거래계약에 관한 법적 고찰, 한국무역상무학회지, 2000. 8, p.415.).

63) 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하는 업무를 말한다 (전자서명법 제2조 8항).

64) 전자서명법 제4조 1호.

65) 전자서명법 제2조 9항.

66) 유엔 전자서명법 초안(제7조 1. b)에서는 면허를 받지 못한 기관(사설 인증기관)의 경우에도 인증기관으로서의 기능을 수행할 수 있도록 규정하고 있다.

67) 정보통신부는 2000년 2월에 일반상거래 분야에는 한국정보인증(주)(www.signgate.com), 주식거래분야에는 한국증권전산(주)(www.korea-stock.com), 2000년 4월에는 은행업무분야에 금융결제원(www.kftc.or.kr)를 公認認證機關으로 지정하였다. 한국전자인증(www.crosscert.com)은 세계최대 전자인증업체인 미국의 Verysign社와 제휴를 맺고 인증서비스를 금년 1월부터 제공하고 있는데 이는 私設認證機關에 해당된다. 한국전산원(www.nca.or.kr)도 정부의 공인인증을 받기 위해 준비중이다.

68) 유타, 캘리포니아, 플로리다州 등을 제외하고는 공인인증기관에 관한 입법활동이 거의 없다. (Benjamin Wright, *The Law of Electronic Commerce,* 2nd edition, Aspen law & Business, Inc., 1996. pp.16:34~16:35.).

69) SET(Secure Electronic Transaction) Co는 Visa와 Master Card가 네트워크(인터넷포함)상에서 신용카드 결제시 공개키 기반구조(PKI)하에 인증업무를 수행한다.

치열한 경쟁을 벌일 것으로 예상된다. 이러한 인증기관의 기능이 인터넷무역에서 그 역할을 다하려면 國際的인 公認認證機關이 설립되어야 한다.[70] 그러나 현실적으로 국제공인인증기관을 설립하는 것은 쉽지 않으므로 먼저 정부간 兩者協定(bilateral agreement)을 통하여 국가간 相互認證體系를 갖추도록 노력해야 할 것이다.[71]

(2) 保證保險의 活用

최근, 인터넷 네트워크를 통한 상거래에서 발생할 수 있는 위험을 보장하는 인터넷 保證保險 상품을 개발이 활성화 되고있다. 아직 시작초기인 만큼 국내 전자상거래에 중점을 두고 개발하고 있는데, 시장성이 있어 활성화된다면 인터넷무역에서도 이러한 보증보험이 활용될 수 있을 것이다. 인터넷무역업자가 네트워크상의 危險을 管理하는 데에도 保證保險을 이용될 가능성이 높다.

컴퓨터 해킹 사고피해를 보상받을 수 있는 保險商品은 현재 쌍용화재가 주간사가 돼 損害保險社들이 공동 개발해 판매하고 있는 '넷시큐어 안심보험'이 있다. 이 상품은 인터넷 거래 때 네트워크 시스템의 파괴나 오작동으로 인한 개인손실, 기업손실, 고객정보누출로 인한 손해, 기업의 휴업 손해 등을 포괄적으로 보상해준다. 전자상거래 중 발생할 수 있는 컴퓨터 해킹事故가 주요 보상대상이다.[72]

상인의 인증을 위한 MCA(Merchant Certificate authority), 결제 인증을 위한 PCA (Payment gateway Certificate Authority) 등의 인증기관이 있다. (Peter Wayner, *Digital Cash* 2nd Edition-Commerce on the net, Academic Press Limited, 1997, pp.161~162 참조.).

70) 國際電子商去來(인터넷무역)를 활성화시키기 위해서는 國際暗號標準과 協定을 바탕으로 국제비즈니스 공동체가 키 위탁관리에 참여하여야 한다.(Dorothy E. Denning, "International Encryption Policy", edited by Ravi Kalakota, A. B. Whinston., *Reading In Electronic Commerce,* Addison Wesley Longman, Inc., 1997. pp.115~116 참조.).

71) 전자서명법 제27조에서는 정부가 전자서명의 상호인정을 위하여 외국정부와 협정을 체결할 수 있도록 규정하고 있으며, 상호인증협정이 체결되는 경우에는 外國의 認證機關 또는 외국의 승인기관이 발급한 증명서에 대하여 공인인증기관이 발급한 인증서와 同一한 법적 지위 또는 法的 效力을 부여할 수 있도록 규정하고 있다. 정보통신부는 한·일 양국간의 안정적인 전자상거래가 이루어지도록 전자서명 상호인증을 위한 협력체제를 강화하기로 하였다. (조선일보, 2000. 9. 24.).

72) 인터넷 쇼핑몰이나 인터넷 뱅킹을 통해 거래하던 고객이 신용정보 유출이나 해커 침입으로 비밀번호가 새 나가 被害를 당했을 때 해당 인터넷 기업에 배상을 요구하면 補償받을 수 있다. 사이버 증권거래 때 시스템의 다운으로 주식을 제때 사고팔지 못해도 배상을 요구할 수 있다. 인터넷 기업은 해커 침입으로 損害를 봤을 경우에도 保險金을 청구할 수 있다. (내외경제, 2000. 2. 12.).

서울보증보험, 데이콤, DST(데이콤시스템테크놀로지) 등 3社도 2000년 4월 11일 인터넷 保證商品 및 서비스를 공동으로 개발하는 전략적 제휴(Strategic Alliance)를 체결하였는데, 전자상거래 보증시스템이 구축되면 인터넷을 통하여 보험 청약, 보험료 납부, 보험증권 발급도 가능하게 되어 편리하게 보증보험을 이용할 수 있다.

電子保證業務가 본격화되면 국내 전자상거래는 더욱 활성화되리라 예측되지만 아직 인터넷무역부문까지는 사업목표를 두고 있지는 않은 것으로 보인다. 인터넷 무역에서 네트워크상의 위험을 보증할 수 있는 보험상품의 개발이 되면 인터넷무역당사자는 인터넷 貿易危險을 담보하는 수단으로 保證保險을 활용하는 것도 고려해 볼 수 있다. 이러한 보증보험은 앞서 설명한 保安서비스業體에게도 매우 유용한 위험관리의 수단이 되고 있다. 美國 컴퓨터 保安會社인 C社는 최근 세계최대 보험조합인 영국 로이드와 협력, 고객들에게 해킹피해보험서비스를 제공하고 있다. 기업 고객들이 해커로부터 物質的 被害를 받으면 로이드가 최고 1억달러까지 補償한다는 것이다.[73]

Ⅳ. 結 語

인터넷을 통한 무역거래가 활성화되자 인터넷 貿易詐欺라는 새로운 형태의 貿易危險이 대두되고 있다. 이는 인터넷이라는 매개체를 너무 신뢰하여 발생되는 것이다. 그래서 전통적인 무역에서보다도 오히려 인터넷貿易에서는 상대방에 대한 信用調査를 더욱 必須的으로 요구된다. 하지만 인터넷을 활용하면 예전보다 훨씬 편하게 신용조사를 할 수 있다. 이것도 인터넷무역의 장점 중 하나이다.

상대방에 대한 身元確認을 하는 데에는 암호화에 의한 電子署名認證이 적절한 방법이지만 향후 국내부문에서부터 指紋에 의한 身元確認(認證)도 도입될 가능성이 있다. 신용조사와 신원확인을 하였더라도 信用狀을 根幹으로 무역거래를 수행하는 것이 바람직하다. 아니면 信用狀制度를 바탕으로 하는 國際貿易

73) C社는 외부로부터의 해커 침투를 감시하는 '24x7'이라는 보안 솔루션을 제공하는 회사이다. (조선일보, 2000. 7. 14.).

시스템을 이용하는 것도 위험관리에 적절한 수단이 될 것이다. 내년부터 도입 예정인 電子貿易仲介機關을 통하여 새로운 파트너를 찾는 것도 상대방의 信用危險을 管理하는데 도움이 될 것으로 여겨진다.

네트워크 및 시스템상의 危險을 管理하기 위해서는 保安시스템을 구축하거나 保安서비스業體에 委託하여 管理하는 것도 하나의 방법이 된다. 전자인증기관으로부터 電子認證書를 발급 받고 전자문서를 거래한다면 相對方의 身元確認이나 文書의 缺陷을 防止할 수 있다. 새로운 보험상품으로 개발되기 시작한 인터넷 保證保險을 활용하는 것도 해킹이나 바이러스 등 네트워크 危險을 管理하는데 유익한 수단이 될 것으로 예상된다.

그러나 무엇보다도 인터넷무역위험을 관리하는데 있어 가장 重要한 것은 인터넷貿易業者 스스로가 그러한 危險을 인식하고 管理하고자 노력을 하는 것이다. 위험을 관리하지 않는 자에게 위험은 찾아들게 마련이다.

參 考 文 獻

김두철 外, 보험과 위험관리, 문영사, 1999.

오원석 外, 인터넷무역론, 법문사, 2000.

이만영 外, 전자상거래보안기술, 생능출판사, 1998.

이민섭, 현대암호학, 교우사, 1999.

이임영 外 共譯, 현대암호, 생능출판사, 1999.

박성철, 웹사이트상의 청약의 법적성질에 관한 고찰, 무역상무학회지, 2000. 2.

최석범, 글로벌 전자무역시대에서의 볼레로 선화증권의 기능과 문제점, 무역상무연구, 2000. 8.

한성일, 인터넷전자상거래계약에 관한 법적 고찰, 한국무역상무학회지, 2000.8.

Bainbridge, D.I., *Introduction to Computer Law* Fourth Edition, Pearson Education Ltd., 2000.

Chissick, M. & Kelman, A., *Electronic Commerce : Law and Practice* , London Sweet & Maxwell, 1999.

Denning, D.E., "International Encryption Policy", edited by Ravi Kalakota, A. B. Whinston., *Reading In Electronic Commerce,* Addison Wesley Longman, Inc., 1997.

Kalakota, R. & Whinston, A.B., *Frontiers of Electronic Commerce,* Addi-

son-Welsley Publishing Company, Inc., 1996.

_____, *Electronic Commerce-A Manager's Guide,* -Addison-Wesley Longman Inc., 1997.

Kosiur, D., *Understanding Electronic Commerce,* Microsoft Press, 1997

Livermore, J. & Euarjai, K., "Electronic Bills of Lading: A Progress Report", *Journal of Maritime Law and Commerce* vol. 28. No.1, January, 1997.

Nemzow, M., *Building Cyberstores-Installation, Transaction Processing, and Management-,* McGraw-Hill, 1997.

Rebel, T.F. & Koening, W., "Key Issues in Ensuring Security and Trust in Electronic Commerce" ; Edited by Jae Kyu Lee, Steven H. Kim, Andrew B. Whinston, Beat Schimid, *Proceedings of The International Conference on Electronic Commerce* '98, International Center for Electronic Commerce, 1998.

Wayner, P., *Digital Cash Commerce on the Net,* AP Professional, 1996

_____, *Digital Cash 2nd Edition-Commerce on the* net, Academic Press Limited, 1997.

Wright, B., *The Law of Electronic Commerce,* 2nd edition, Aspen law & Business, Inc., 1996.

기타, 언론보도 및 Web site 자료 다수.

ABSTRACT

A Study on the System of Risk Management in the Int'l Trade by Internet Network

Ha, Kang Hun

There are many kinds of risk in int'l trade by internet network, such as credit risk, mercantile risk, contingency risk, exchange risk, physical risk and the risk on internet network.

Especially, risk management against credit risk and the risk on internet network are very important. The former is conventional but more important these days. The latter is a new risk that has been incurred owing to the int'l trade by internet network.

The system of risk management against the former are firstly, to surely research credit of counterpart by internet, secondly, to certify the entity by password or fingerprint, thirdly, to pay the price under a letter of credit, fourthly, to use the system of int'l trade such as bolero, trade card, finally, to use the authority of electronic trade services.

The system of risk management against the latter are firstly, to install the firewall on the own computer network, secondly, to entrust the management own computer network to the network security services firm, thirdly, to electronically communicate with counterpart through the certification authority, finally, to insure against the own network risk with the security insurance company.

Key words : Credit Risk, Risk Management, Certification Authority, Message Authentication, Entity Authentication,