전자무역보안과 전략적 대응방안에 대한 소고

정 조 남[†] · 이 춘 수[††] · 강 장 묵[†††]

요 약

본 연구는 통합적 관점에서 전자상거래보안 분야를 전자무역 분야에 체계적으로 접목하여 솔루션을 제시하였다. 전자무역보안에 적용할 수 있는 통합적 관점에서 3가지 정보보안 공격에 대하여 중점적으로 연구하였다. 첫째, 시스템공격, 둘째, 데이터공격, 셋째, 비즈니스공격에 대한 해결책을 중심으로 그 대응방법을 연구하였다. 각각의 해결책에 대하여 다음과 같이 요약해 볼 수 있다. 전자무역에 관련된 당사자들은 시스템 공격, 데이터공격, 비즈니스공격에 대응하기해서 정부측면에서의 전자무역보안에 대한 정책적 관리와 보안인프라의 구축이 요망되고, 기업차원에서는 보안의식 강화와 정보보호장치 즉, 방화벽, 침입탐지시스템(IDS), 공개키기반구조(PKI), 가설사설망(VPN), 안티바이러스제품, 암호화, 생체인식기술 등의 활용 또는 정보보호전문업체를 통한 아웃소싱을 이용한 전자무역보안의 수단을 강구해야 된다. 결론적으로 전자무역기업은 적절한 보안시스템의 도입과 더불어 관리자들의 최근 해킹기술발전에 대하여 신속히 대처하려는 노력이 무엇 보다 중요하다. 전자무역 분야에도 다양한 보안솔루션과 보안인식의 제고가 강조된다.

A Study on E-trade Securities and Strategic Solutions

Jo-nam Jung[†] · Chun-su Lee[††] · Jang-mook Kang[†††]

ABSTRACT

Recently many company has been cracked by crackers information security and everyday new computer virus come out. so e-trade partners should prevent the disasters. A few studies researched e-trade securities broadly but the new trend in information security division especially focused on electronic payment, EDI, Transportation, Contracts, Insurances and that of subjects have been researched through interdisciplinary evolution. Our research e-trade security on three part, First system attack, second is data attack and third is business attack. the attacks have theirs own solution, so e-trade company use this solution timely and powerfully. It is the most important thing to prepare the cracking with securities system. also manager should catch recent hacking technologies. The research results propose that e-trade firms should use information security policies and securities systems that including H/W and S/W. therefore manager's security mind is very important and also using electronic commerce securities device and should be considered exploiting solutions by each special usage according to e-trade company' environments.

키워드 : 전자무역(E-Trade), 정보보호(Information Security), 정보보호전략(Information Security Strategy)

1. 서 론

1994년부터 인터넷의 급속한 보급은 모든 경제의 패러다임에 영향을 미치면서, 기술적 측면과 제도적 측면 그리고 법률적 측면에서 다각도로 영향을 미치고 있다. 현재 전자무역은 개정대외무역법(2000. 12. 29)에 따라 정보통신기술을 이용한 모든 분야의 기술적 적용을 통하여 전통적 무역행위를 전자적 형태의 무역거래로 설명할 수 있다. 이러한 정보기술의 발전과 확산은 정보화의 순기능적 측면뿐만 아니라 역기능적인 측면도 부각되고 있다. 한국정보보호진흥원 자료에 따르면 국내기업의 누적 해킹 건수가 2002년 6월 현재 1,355건으로 꾸준히 증가세를 유지하고 있다(한국정보보호진흥원, www.kisa.or.kr, 2004. 1). 이러한 대표적인 예로 인터넷무역사기와 정보유출, 컴퓨터 바이러스 유포 등 다양한 네트워크 상의 장애로 나타나고 있다. Riyad(2002)는 B2B 산업에 있어서의 핵심성공요인으로 5가지 요인 즉, 마케팅 전략요인, 웹사이트요인, 외부요인, 글로벌요인, 내부요인으로 파악하고 특히 외부요인에 하위변수로 신뢰, 보안, 성공적 관계, 쉬운 인터넷접속, 고객 수락(Acceptance)을 제시하였다[1].

한국정보보호진흥원의 조사 자료에 의하면 세계 정보보호 시장은 1999년 77억 달러 수준에서 2001년 135억 달러로 시장규모 측면에서 2배에 가까운 성장을 하고 있으며, 연평균

† 정 회 원 : 인하대학교 대학원 컴퓨터정보공학과
†† 정 회 원 : 고려대학교 기업경영연구원 연구원
††† 정 회 원 : 서경대학교 컴퓨터공학과 교수
논문접수 : 2004년 4월 13일, 심사완료 : 2004년 7월 30일

30% 정도 성장하여 2004년도에는 280억불에 달할 것으로 예측된다. 시장구성 측면에서는 1999년 정보보호서비스 중심에서(총 시장규모의 59% 차지) 2004년도에는 시스템 및 네트워크 분야 중심(총 시장규모의 58% 차지)으로 변동이 예상된다[2]. 이러한 보안시장의 성장은 전자상거래의 정보화 역기능을 단적으로 보여주는 예이며, 그러므로 전자무역 시장에서도 정보보호 및 정보보호의 중요성을 인식하고 보안에 대한 대처능력과 대응전략을 제고할 필요성이 있다.

기존 전자무역보안 또는 정보보호에 관련된 연구는 주로 전자결제에 관련된 부분에 집중적으로 이루어져 왔으며, 전자무역 보안상의 문제해결을 위하여, 거래당사자간의 갈등을 줄이고 만족도를 향상하기 위한 신뢰를 모색하고, 급성장하고 있는 정보보호산업을 통하여 전자무역 또한 정보침해 및 시스템의 정상적 작동을 보증할 수 있는 수단과 방법이 요구되고 있다.

본 연구에서는 정보화의 역기능을 시스템공격, 데이터공격, 비즈니스공격의 세 가지 측면에서 나누어 살펴보았다. 각각의 공격에 대한 전략적 대응방법으로 정보보호기술에 기반을 둔 정보보호제품의 파악과 국내외 정보보호관련 입법동향과 국제기구 및 주요국의 동향에 대하여 종합적으로 고찰하여 전략적 대응방법을 제시하고자 한다.

2. 전자무역과 정보보호 현황

2.1 전자무역과 정보보호

2.1.1 전자무역

전자무역이란 대외무역법 제2조 제6호 "전자무역이라 함은 무역의 일부 또는 전부가 컴퓨터 등 정보처리능력을 가진 장치에 의하여 정보통신망을 이용하여 이루어지는 거래를 말한다." 개정대외무역법(2000. 12. 29일자)이 공표되기 전에는 학자마다 인터넷무역 또는 사이버무역으로 통일된 용어의 사용 없이 혼용하여 사용하여 왔었다. 따라서 전자무역의 보안은 정보통신망을 이용하는 부분에 대하여 취약성이 노출된 부분으로 확장하여 파악할 수 있다. 전자무역에 있어서 정보보안(보호)분야를 학문적 영역으로 분류하자면, 고윤승·신황호(2001)는 전자무역을 4가지 연구범위(전자무역마케팅, 전자무역 결제, 전자무역 국제법규, 전자무역 정보시스템)로 설정하였다[3]. 연구 분석을 위한 접근방법으로 상관습 및 법리적 접근, 사례접근, 시뮬레이션 접근, 실증적 접근방법 제시하였으며, 전자무역보안은 사이버무역정보시스템 영역으로 포함하여 파악할 수 있을 것이다. 또한 이춘수·이장로(2002)는 전자무역의 학제적 연구의 중요성을 파악하고 인터넷무역의 주제별 분류에서 인터넷무역이론/환경, 인터넷무역전략, 인터넷무역관리 그리고 기타로 크게 네 가지 주제범주를 설정하여 문헌 조사하였다[4]. 또한 보안분야는 인터넷 무역 전략의 세부 주제범주의 무역정보시스템의 영역으로 포함하여 분류하였다. 전자무역에 있어서의 공격요인으로는 크게 다음과 같이 세 가지로 구분하여 파악할 수 있다. 이는 정보보호 위협요소의 대분류로 파악할 수도 있다.

① 시스템 공격

일반적인 컴퓨터 시스템 특히 네트워크에 연결된 컴퓨터는 외부의 특정인이 이 시스템을 침입하여 부당하게 컴퓨터 시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위협이 있다. 일반적으로 이런 해킹위협을 방지하기 위해 방화벽과 침입탐지시스템 같은 시스템을 사용하기도 한다. 그러나 전자적 거래는 불특정 다수인의 접근을 허용하는 응용시스템으로서 방화벽을 사용하는데 있어서 제약을 받을 수도 있다. 특히 시스템을 불법적으로 사용하는 자료를 보면 외부에서의 침입보다는 내부사용자의 불법적 사용이 더 많기 때문에 적절한 시스템의 운영지침과 내부사용자에 대한 보안대책이 중요한 요소가 된다.

② 데이터 공격

전자무역에 있어서 데이터의 공격은 두 가지로 구분해 볼 수 있다. 하나는 시스템 내에 저장된 데이터, 또 하나는 네트워크 상에 흘러 다니는 데이터에 대한 공격이 있을 수 있다. 시스템에 저장된 데이터의 경우는 앞의 시스템 공격에서 언급하였다. 특히 데이터를 시스템에 저장할 때도 암호화를 해서 저장하는 것이 필요하다. 두번째로 네트워크 상에 흘러 다니는 데이터에 대한 공격을 막기 위해 기밀성, 자료의 무결성 등에 대한 보증이 필요하게 된다. 이를 위해서는 디지털 서명 메카니즘을 많이 이용하고 있다. 디지털 서명 메카니즘 중 가장 대표적인 것으로는 비대칭키(Asymmetric) 암호화기술과 해쉬암호 등이 있다. 디지털 서명 메커니즘은 데이터의 무결성, 사용자의 인증(Authentication) 그리고 부인봉쇄(Non-Repudiation) 등의 서비스를 구현하는 역할을 한다.

③ Business 공격

앞에서 언급한 두 가지 공격은 모두 일반적인 컴퓨터 시스템의 보안침해와 동일하다. 그러나 전자무역에 있어서는 상거래라는 특징 때문에 발생하는 제 3의 공격이 있을 수 있다. 이것을 통칭해 비즈니스공격이라 부른다.[5] 상거래에만 일어날 수 있는 사기가 전자적 상거래에도 일어날 가능성이 있다. 이런 요소들을 전자적으로 막기 위한 보안 고려사항들이 추가적으로 필요하게 된다. 암호학 혹은 시스템으로만 모든 것을 다 막을 수는 없기 때문에 제도적인 장치, 법적인 보장, 보험 등의 전자시스템 외적인 보완도 이루어져야 한다.

2.1.2 정보보호

정보보호란 정보화촉진기본법 제2조에 명시되어 있는 인

터넷을 포함한 정보통신 네트워크 및 단말기 등을 이용하여 처리되는 음성, 영상, 데이터 그리고 멀티미디어 서비스에서 정보의 유출 및 손상, 시스템파괴, 바이러스 등의 각종 보안 위협으로부터 정보통신 시스템을 보호하고 정당한 사용자의 신분을 확인함으로써 정보공유 및 시스템 접근 등의 각종 정보 서비스의 가용성을 보장하고 활성화시키기 위한 기술적 활동이라고 의할 수 있다.

<표 1>은 기관별 해킹 건수를 나타내고 있으며, 특히 연도별 기업의 누적 해킹 건수가 2002년 6월 현재 1,355건으로 확대되고 있다.

〈표 1〉 기관별 해킹발생 건수

(단위 : 건)

구 분	1996	1997	1998	1999	2000	2001	2002.6
대학(ac)	95	32	80	262	260	424	247
기업(co)	**46**	**25**	**69**	**248**	**818**	**1,768**	**1,355**
비영리기관(or)	2	1	2	22	6	50	43
연구소(re)	-	3	4	11	3	8	6
지 역	-	-	2	-	48	225	57
기 타	4	2	-	29	808	1,304	1,121
합 계	147	64	158	572	1,943	5,333	2,829

자료출처 : 한국정보보호진흥원(KISA).

<표 2>는 국제 해킹발생 건수를 나타내고 있으며, 특히 1998년 이후로 국내외 해킹 건수가 늘고 있으며, 국외에서국내로의 해킹시도가 전자무역업체에 있어서 그 파장이 더 클 것으로 사료된다.

〈표 2〉 국제 해킹발생 건수

(단위 : 건)

	국내 → 국내	국내 → 국외	국외 → 국내		N/A	합계
			국외 → 국내	국외 → 국내 → 국외		
1996년	-	6	1			7
1997년	-		11			20
1998년	-		123			141
1999년	48	24	91	183	250	596
2000년	328	84	273	261	1,081	2,027
2001년	285	175	289	408	4,351	5,508
2002.6	38	86	67	138	2,586	2,915

자료출처 : 한국정보보호진흥원(KISA)

<표 3>과 <표 4>는 한국전산원의 정보보호실태 조사에서 나타난 기업부문의 바이러스 바이러스피해현황(한국전산원 자료, 2002)과 정보보호제품 이용현황을 업종별, 매출액별로 기업을 대상으로 조사한 자료이다. <표 3>에서 10회 이상 컴퓨터바이러스 피해를 입은 업체가 전체 362,326사업체 중에서 5,368곳이나 집계되었으며, 매출액규모에 큰 상관없이 1000 여건을 상회하는 것으로 한국전산원의 조사 자료에 나왔다. <표 4>의 정보보호제품이용현황을 보면 주로 기업체에서 방화벽, 침입탐지시스템, 컴퓨터바이러스백신, 인증/암호화제품, 가상사설망, 보안서비스 등을 사용하고 있는 것으로 파악되었다. 2003년도 12월까지 Cyber118에 접수된 해킹상담은 총 6,160건에 달한다(http://ns.cyber118.or.kr).

〈표 3〉 기업부문 바이러스 피해현황

(단위 : 사업체수, 회)

피해 횟수		1번	2~4번	5~9번	10번 이상
전 체	362,326	58,290	19,084	25,627	5,368
업종별					
농림수산업	2,658	602	521	4	77
경공업	36,076	4,396	1,331	2,025	320
중공업	39,732	8,135	2,686	3,999	533
석유화학	18,875	3,626	2,138	1,029	217
건설업	22,984	3,787	1,085	2,251	184
유통업	123,947	16,151	3,776	7,607	2,099
금융보험업	25,824	4,591	1,624	1,394	747
기타서비스업	92,230	17,002	5,922	7,318	1,192
매출액별					
10억 미만	149,855	18,881	7,063	8,196	1,301
10~99억	67,842	18,861	5,819	8,955	1,887
100억 이상	18,610	7,821	1,653	3,221	1,705
모름/무응답	126,020	12,728	4,549	5,255	475

〈표 4〉 기업부문 정보보호제품 이용현황

(단위 : 사업체수)

	민간 사업체	방화벽	침입탐지 시스템	바이러스 백신	인증/ 암호화 제품	VPN (가상사 설망)	보안 서비스	기타
전 체	362,326	14,861	9,452	140,372	9,153	3,523	14,486	1,185
업종별								
농림 수산업	2,658	81	4	504	4	4	4	-
경공업	36,076	533	326	10,350	224	163	380	1
중공업	39,732	1,056	494	13,480	246	200	453	3
석유화학	18,875	321	98	7,606	227	127	274	-
건설업	22,984	259	288	9,327	1,201	52	153	2
유통업	123,947	4,766	1,728	39,544	1,716	1,259	4,515	11
금융 보험업	25,824	4,749	3,958	19,969	3,040	1,319	4,739	179
기타 서비스업	92,230	3,096	2,556	39,592	2,494	398	3,967	989

자료 : 한국전산원, 2002.

3. 전자무역보안 특징

전자상거래 실행상의 문제점으로 보안과 결제분야에 대한 유의점은 전자무역 분야에서도 기업측면에서 혹은 국가측면에서 확장하여 그 특징적 영역을 파악해야 된다[6].

3.1 전자무역보안의 특징

전자무역은 기존의 무역방식과 비교하여 진행순서에는 별다른 차이가 없으나 업무처리 방법과 수단에서 종전에 비해 커다란 차이가 있다. 즉 기업은 전자우편, 인터넷 전화·팩

스 등을 이용하여 저렴한 비용으로 상담을 전개하고 수출계약을 체결할 수 있다. 아울러 상품주문이나 대금결제 등도 인터넷으로 할 수 있으며, 화물의 흐름도 즉시 파악할 수 있다. 또 기업은 인터넷상의 지사 홈페이지나 거래알선 사이트, 유즈넷, 메일링 리스트 등을 통해 자사제품과 서비스를 해외에 홍보하고 신제품이나 거래선 정보를 신속하게 입수할 수 있다[7]. 따라서 이러한 수단과 방법에 대한 전자적 보안 요소도 고려를 하여야 한다. 전자무역에서는 무역카드(trade card), 전자화폐 등을 통해 대금결제가 가능하게 되며, 화주는 화물운송과정을 인터넷상에서 직접 추적 또는 확인해 볼 수 있다. 이러한 전통적 무역과 전자무역 차이를 통한 기술적 보안고려 요인을 <표 5>와 같이 정리하여 볼 수 있다. 즉 무역계약 체결 각 단계인 정보수집, 광고 마케팅, 의사교환, 대금결제, 운송, 사후관리 단계마다 전통무역과는 상이한 수단과 방법이 전자무역에 도입됨에 따라 전자무역의 각 특징들에 대한 보안고려 요소를 파악하고 이를 적극적으로 대처할 필요성이 있다.

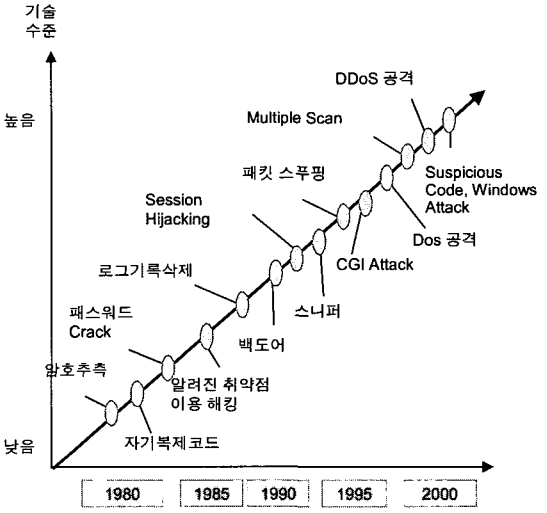
〈표 5〉 전통무역과 전자무역의 비교에 따른 단계별 보안요인

구분	전 통 무 역	전 자 무 역	보 안 요 인
정보 수집	거래알선기관, 직접방문, 해외전시회 참관 등	국내외 거래알선 사이트 등 전자 정보검색	네트워크 장애, 해킹
광고 · 마케팅	카달로그, 매체광고, 전시회, 상담회 참가 등	홈페이지 구축, 유즈넷, 메일링리스트, 무역알선 사이트 등록, 사이버 전 전시회	웜 바이러스, 시스템 장애 등
의사 교환	국제전화, 팩스, 우편, 해외출장 등	전자우편, 인터넷 전화/팩스, 화상대화시스템 등	네트워크 장애, 웜 바이러스 등
대금 결제	신용장, D/A, D/P 등 (은행)	무역카드, 전자화폐, 전자자금이체 등	인증, 무결성파괴 등
물류 운송	포워더, 해운, 항공운송	온라인 전송, 특급 운송 등	전자서류 위조 등
사후 관리	클레임과 중재, 소송 등	전자거래 약정 콜센터, DB 마케팅 등	인터넷사기행위, 법률위반 등

3.2 해킹기술의 변화

공격 기술의 진화단계를 간단하게 살펴보면, 예전의 해킹 방법은 외부에서 시스템의 최고 관리자 권한인 관리자(root)권한을 획득하여 정보유출/변조 또는 시스템 Crash, 자료 삭제, Backdoor 설치 등을 하는 작업에 목표를 두었고 그 대상이 UNIX 계열 OS에 초점이 맞추어져 있었다고 한다면, 최근의 해킹동향은 OS를 불문하고 (UNIX, Windows NT, Network 장비, 미들웨어, 하드웨어 일체형 장비) 이루어지고 있으며 관리자(root) 권한을 획득하기 보다는 서비스 장애를 유발하도록 하는 공격방법이 더욱 두드러지고 있다.

(그림 1)은 연대별 시간의 변화에 따른 해킹 기술의 고도화를 중심으로 해당 해킹기술의 발생시점과 종류를 설명하는 그림이다. (그림 1)에서 보는 봐와 같이 해킹기술은 시간이 지날수록 점점 더 고도화, 지능화, 복잡화되어 지는 경향을 나타내고 있다. 따라서 전자무역을 담당 하고 있는 업체와 관련 당사자들은 해킹에 대한 이해와 전반적인 기술의 변화에 대한 기본 지식을 가지고 능동적으로 대처할 준비를 해야 한다.



자료 : www.sans.org

(그림 1) 해킹기술의 변화

4. 전략적 대응방법

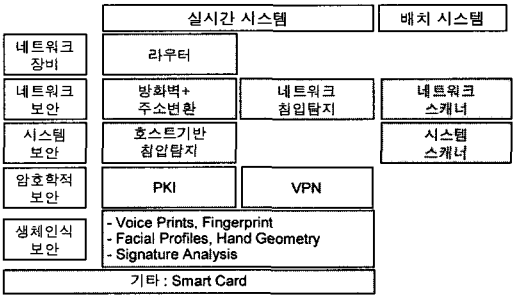
4.1 시스템 공격에 대한 전략적 대응방법

전자무역에 있어서 시스템 공격에 대비하기 위해서는 앞에서 언급한 보안위협요소 중 네트워크에 대한 공격을 방어할 수 있는 안전장치를 마련하여야 한다.

2001년부터 2005년까지 국내 정보보호 산업의 시장규모를 살펴보면, 2001년에는 전년 대비 86% 정도 성장한 3,160억원 정도로 추정되며 방화벽(Firewall), 공개키 기반구조(PKI), 침입탐지시스템(IDS), Antivirus, 가상사설망(VPN) 제품이 전체 시장의 70% 정도를 점유한 것으로 분석된다[8].

4.1.1 전자무역 보안장치

(그림 2)는 전자무역 보안장치를 네트워크장비, 네트워크 보안, 시스템보안, 암호학적 보안, 생체인식보안 단위로 구분하고, 각 단위에 대한 장치를 구분하고 있다. 또한 보안장치는 처리시간에 따라 실시간 시스템 또는 배치(일괄)처리 시스템으로 구분한다((주)인젠, 정보보호, 교육자료, 2001).



(그림 2) 보안장치 분류

<표 6>은 한국정보보호진흥원에서 2001년도 정보보호 산업 실태조사를 바탕으로 시스템 및 네트워크 제품, 보안서비스 그리고 기타분야 등 총 3개의 분야로 분류하여 놓고 있으며, 정보보호서비스분야를 세분화하여 보안컨설팅 및 보안관제서비스로 나누어 정의하고 요약한 표이다. 특히 앞의 <표 4> 기업부문 정보보호제품 이용현황에서 보안서비스를 보안컨설팅과 보안관제서비스로 분류하고 '기업이나 기관의 정보보호 취약점을 분석하고 그에 맞는 최적의 보안솔루션을 제공하는 서비스'와 '기업이나 기관의 보안업무를 통합하여 아웃소싱하는 서비스'로 각각 정의하였다.

〈표 6〉 정보보호기술 분류

구 분	제품 및 서비스	정 의
시스템 및 네트워크 보안 제품	바이러스 백신	컴퓨터바이러스 등 시스템 유해요소 진입 차단 및 손상된 시스템 복구용 제품
	방화벽 (침입차단시스템)	외부망에서 해커 등 비인가자의 내부망으로의 침입을 차단시키는 S/W 또는 H/W
	가상사설망 (VPN)	공공망에서 지점간 안전한 터널링을 설정하여 전용회선을 사용하는 것처럼 실질적인 사설망 기능을 제공해주는 제품
	침입탐지시스템 (IDS)	실시간 네트워크 또는 컴퓨터시스템상 내외부 사용자에 의한 불법행위를 탐지하는 S/W
	공개키기반구조 (PKI)	인증, 부인방지, 전자서명과 같은 기능을 제공하는 공개키 암호기술을 응용한 제품
	PC 보안	개인용 컴퓨터의 정보보호를 위한 S/W 또는 솔류션
	전자우편보안	전자우편의 보안상 취약점을 개선해주는 기능을 가진 제품
	리눅스 보안	소스코드가 공개된 리눅스시스템의 보안상 취약점을 해결하는 제품
	보안IC카드	스마트카드와 같이 IC카드에 암호알고리즘을 이식, 접근제어나 사용자 신원확인 기능을 수행하는 제품
	보안관리 ESM (Enterprise Security Management)	여러 형태의 정보보호제품을 통합하여 관리하는 S/W
보안 서비스	보안컨설팅	기업이나 기관의 정보보호 취약점을 분석하고 그에 맞는 최적의 보안솔루션을 제공하는 서비스
	보안관제서비스	기업이나 기관의 보안업무를 통합하여 아웃소싱하는 서비스
기 타	무선인터넷보안	모바일 인터넷의 정보보안을 해결해주는 제품
	생체인식	망막, 지문, 음성, 얼굴 등 개인의 신체적 특성을 이용해 신원을 확인하는 시스템

자료 : 한국정보보호진흥원, 2000.

4.1.2 정보보안컨설팅

정보보호전문업체는 기반시설에 대한 취약점 분석·평가 및 보호대책 수립 업무를 지원하는 민간업체로 정통부에서 2001년 7월 1일부터 시행된 정보통신기반보호법에 따라 당해 업체의 정보보호컨설팅 수행능력과 신뢰성을 심사해 지정한다. 정보보호 전문업체는 한국정보보호진흥원(KISA)·한국전자통신연구원(ETRI) 등과 함께 금융·통신·운송·에너지·행정 등 국가사회에 미치는 영향이 큰 기반시설에 대한 취약점 분석·평가와 보호대책 및 침해사고 대응 업무를 지원하게 된다[9]. 정보보호컨설팅은 기존의 단편적이고 개별적인 내용에서 더 나아가 경영정보(MIS)기술, 비즈니스 프로세스(Business Process), 보안기술, 시스템제조업체들이 보유하고 있는 정보기술(IT), 인터넷서비스업체(ISP)들이 가지고 있는 인터넷서비스 기술, 교육 및 훈련 (Education & Training), 정책 및 절차 등을 고려한 관리기술 등이 종합적으로 구성되어 조직의 보안상황을 체계적으로 진단·분석하여 문제를 해결하는 방향으로 변화되고 있다. 즉, 기존의 제품위주의 정보보호 인증체계에서 네트워크 및 시스템 보안감사 업무, 전문적인 보안진단 및 경영전반에 걸친 진단업무 등이 협력제휴 형태로 이루어져 종합적인 글로벌 정보보호 지원시스템을 지향하고 있다[10].

따라서 보안에 대한 전문성이 부족한 전자무역업체의 경우, 정보보호 전문업체에 보안관련 아웃소싱 등을 통하여, 보다 효율적이고 안정적인 보안환경을 구축할 수 있을 것이다. 또한 일반 기업체의 경우 정보보호 컨설팅을 받는 경우 침입차단시스템(F/W : FireWall), 침입탐지시스템(IDS : Intrusion Detection System)등의 소프트웨어와 기타 하드웨어를 구입하는데 만족하는 안일한 대응을 하는 경우가 많다. 보안의 취약점은 불특정 다수나 모르는 외부인보다 내부자의 소행이 많으며 특히 사회공학적인 취약점으로 인한 보안의 취약점이 두드러진다고 사료된다. 사회공학적인 취약점과 내부자의 보안 취약점을 줄이기 위해서라도 시스템과 정책 그리고 법제도적인 측면에서 종합적인 컨설팅이 필요하다.

4.2 데이타 공격에 대한 전략적 대응방법

전자결제 상에서 특히 문제점이 많이 발생할 수 있다고 지적하고 암호화, 메시지인증, 디지털서명, 인증, 방화벽 블라인드 서명 등의 기술이 중요하다. 인증이란 불법적인 사용자가 정당한 사용자로 가장하여 침입하거나 정보에 대한 위협을 가하는 행위를 방지하는 과정을 의미한다. 또한 메시지인증을 통하여 진정성을 파악하는 과정을 의미하기도 한다. <표 7>은 인증에 관련된 데이터보안 중요 요인들이다.

〈표 7〉 데이터보안 요소

구 분	내 용	필요기술
인증(Authentication)	사용자인증 : 정당한 사용자 메시지인증 : 메시지 진정성	전자서명
무결성(Integrity)	메시지 진정성	전자서명
비밀성(Confidentiality)	정당한 사용자만이 메시지확인가능	암호화
부인방지 (Non-reputation)	메시지 작성 또는 송수신에 대한 부인 불가능	전자서명

자료 : KISDI, 2000. 6.

데이터 전송과정에 적용되는 데이터 발신처 확인과 자격 유무를 제공하는 서비스, 통신 당사자 간의 신분 확인과 자격 유무의 점검과 대등 실체 간의 신뢰성 있는 연결의 확립에 적용되는 서비스인 실체 확인을 의미한다. 기본적인 웹 보안 기술에는 기본 인증, IP 필터링(filtering)이 있으며, 응용계층에서의 보안 기술로는 NCSA Mosaic과 Http의 PGP · PEM, EIT의 Secure-HTTP, Message Digest Authentication, Kerberos 및 Yaksa 방식 등이 있다. 또한 네트워크 부분에서의 보안을 제공하는 SSL(Secure Socket Layer) 및 TLS (TransportLayer Security) 등과 같은 기술이 있다. 한편 웹 상에서 정보의 보안을 위해서 제공되어지는 보안 프로토콜(Secure Socket layer), SHTTP(Secure HTTP) 등이 개발되어 상용화되고 있다. 또한 시스템의 정보보호를 위해 다양한 보안정책에 유연하게 대처할 수 있는 Secure OS 및 Secure DBMS가 개발 중에 있으며, 인터넷 환경에서의 정보보호를 위한 다양한 프로토콜개발, 특히 산업계에서 인터넷 정보보호 기술로 IPsec 표준기술을 채택하고 있다[11].

XML은 현재 인터넷에서 데이터 교환을 위해 널리 쓰이고 있고 HTML을 대신할 데이터 교환 표준으로 자리 잡고 있으며, XML의 이러한 장점들을 이용해 다양한 거래형태를 전자상거래로 구현하려는 연구가 국내외에서 활발히 수행되어 왔었다[12].

XML기반의 어플리케이션의 경우 오픈 시스템으로 누구나 쉽게 거래에 참여할 수 있는 장점을 지니고 있지만 그에 따른 상이한 지불, 결제문제 및 보안문제는 기존의 상거래보다 복잡하고 상위의 거래표준이 필요하다. XML과 관련된 지불 및 결제에 대한 표준은 1997년 OFX(Open Financial Exchange)을 시점으로 해서 점차 늘어나고 있는 상황이다. OFX는 지불 및 결제 관련 데이터 교환 시 사업자 및 고객을 보호할 수 있도록 되어 있다. 예를 들어 사업자는 XML로 표시된 분석 데이터를 통해 사기 여부를 쉽게 분석할 수 있으며, 소비자측면에서는 웹쇼핑 에이전트가 월간 계산서와 함께 보내진 마케팅 데이터에 접근을 통해서 경쟁사의 서비스를 비교하여 줌으로써 이익을 얻을 수 있다. 또한 다수의 은행을 포함하여, 최근에 개시된 IFX((Interactive Financial Exchange), 전자구매 시 상업적 카드를 위한 비자표준, Verisign의 지불 프로세싱, XML Pay, XML기반의 OFX 2.0 등 몇 개의 표준에 의해 XML기반의 전자지불 표준이 실제 거래에 활용될 수 있도록 하고 있다[13]. 최근에는 사이버 공격에 대한 어플리케이션을 보호하는 기존의 접근 방법에서 탈피하여 사이버 공격을 당하여도 중요한 업무의 경우에는 미들웨어, 프로토콜 등을 통한 어플리케이션 감내 시스템(침입 감내 시스템)을 개발하여 시스템의 안정성과 신뢰성을 높이는 방법도 중요한 전자 거래 시스템의 경우에는 고려해 볼 수 있다[14].

4.3 비즈니스 공격에 대한 전략적 대응방법

4.3.1 인터넷관련 국내외 법규

① 국내 법제정현황

인터넷과 관련하여 최근 중요한 입법은 <표 8>과 같다.

〈표 8〉 정보통신 거래 관련 법규

법	제(개)정일	제 정 목 적	주 요 내 용
전자거래기본법	1999. 2. 8 1999. 7. 1 시행	전자적거래 안정적 확산 도모	◦ 전자문서의 개념 및 법적효력 등에 관한 사항규정 ◦ 전자서명 및 인증제도에 관한 최소한의 규정마련 ◦ 전자상거래관련민간의 암호기술 사용에 관한 내용반영
전자서명법	1999. 2. 8 1999. 7. 1 시행	전자거래의안전과신뢰성보장	◦ 전자서명 및 인증기관의 지정 ◦ 관리에 관한 사항을 규정
정보통신망이용촉진 등에관한법률	1999. 2. 8	「전산망보급확장등에관한법률」 전면개정 인터넷이용 활성화와 보호도모	◦ 전자문서에 대한 처리절차를 간소화 ◦ 개인정보의 수집, 이용제한, 이용자의 권리에 관한 규정을 신설 ◦ 정보통신망으로 유통되는 정보내용물의 개발촉진지원 근거마련
정보화촉진기본법	1999. 1. 21 개정	국가정보화사업의 체계적인 추진을 위해 정보화책임관 및 정보통신부의 총괄기능강화	◦ 정보자원의 개념, 정보화책임관, 정보자원의 효율적 관리 원칙신설 ◦ 정부의 암호기술개발과 이용 촉진 의무규정 신설 ◦ 초고속통신망사업자제도폐지
사무관리규정	1999. 8. 7 개정	행정사무처리의 합리화도모	◦ 전자매체를 통한 결재 ◦ 유통·보존원칙규정
표시광고의공정화에 관한법률	1999. 2. 5	공정거래질서유지	◦ 허위과장광고, 기만적인광고, 부당하게 비교하는 광고, 비방광고 등을 금지
정보통신기반보호법	2001. 1	정보통신기반을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정보장을 도모	◦ 전자적 침해행위에 대비하여 주요정보통신 기반 시설의 보호에 관한 대책을 수립·시행함
디지털 콘텐츠법	2001. 12. 6	온라인디지털콘텐츠산업의 기반 조성	◦ 온라인디지털콘텐츠 및 해당 기술적 보호조치의 보호(온라인 디지털 콘텐츠 제작자의 보호)

이밖에도 1999년 정기국회에서는 국가 또는 지방자치단체 등에 산재되어 있는 지식정보자원을 체계적으로 관리·보존하기 위하여 지식정보자원관리위원회를 설치하고 지식정보자원관리기본계획을 수립하도록 하는 지식정보자원관리법이 통과되었다. 또한 공정거래위원회는 「표시광고의공정화에관한법률」과 「통신판매표시·광고에 관한 공정거래지침」을 인터넷 환경에서 구체화하는 전자거래소비자보호지침(공정거래위원회 고시 제2000-1호)을 발표하였다. 위에서 언급한 많은 법률이 전자문서 및 전자서명에 의한 업무처리의 경우 그 전자문서 및 전자서명을 관련 법령이 요구하는 (종이)문

서 및 서명날인과 같은 것으로 간주하는 규정을 두고 있다. 전자거래기본법, 전자서명법은 기본법이고 무역업무자동화촉진에관한법률, 화물유통촉진법, 정보통신망이용촉진등에관한법률, 증권거래법, 외국환거래법, 산업기술기반조성에관한법률, 항만법 등은 해당 분야별로 전자문서 이용을 촉진하고 있다[15].

우리나라에서도 최근 이와 같은 개별적인 법규들을 모아 CyberLaw라는 학문적 틀을 갖추고 사이버스페이스(Cyber-Law)에 대한 기술적 특성들을 반영한 실질적인 구속력을 행사할 수 있는 법률에 대한 연구가 활발하게 진행되고 있는 실정이다[16].

② 국제기구 법제정현황

ㅇ UN(UNCITRAL)

UNCITRAL은 각국의 전자문서 사용 관련 입법에 유용한 가이드로서'전자상거래에 관한 UNCITRAL 모델법'을 채택하였으며 '전자서명모델법'의 작업이 진행되었다. 모델법은 법적 구속력은 없으나 인테넷을 이용한 국제거래가 보편화됨에 따라 각국의 관련법 제정시 중요한 지침으로 활용되고 있다(UNCITRAL, '전자서명모델법', 2001).

ㅇ OECD

OECD에서 가장 최근에 채택한 전자상거래 관련 규범은 사기·기만 거래, 프라이버시 침해, 소비자 불만처리 곤란 등 소비자 문제를 해결하기 위한 '전자상거래 소비자보호 가이드라인'이다. OECD 소비자정책위원회(Committee on Consumer Policy)가 전자상거래 확산에 따른 피해 예방 및 효과적인 구제를 위해 1997년부터 추진한 작업이 오타와 각료회의 선언에 힘입어 1999년 12월 마침내 결실을 맺게 된 것이다. 동 가이드라인은 가장 최근에 이루어진 전자상거래 관련 합의라는 의미 외에 각국이 서로 상이한 소비자 보호 관련 법규와 정책의 조화를 도모한 결과라는 점에서 그 의미있다.

ㅇ WIPO

WIPO(세계지적재산권기구)는 1996년 12월 제네바 WIPO 외교회의결과 'WIPO 저작권조약'과 'WIPO 실연·음반조약'을 채택하여 인터넷 환경에서의지적재산권법제의기본원칙을 제시하였으며, 최근에는 인터넷 도메인 이름과 관련한 분쟁해결을 위한 권고를 ICANN 이사회에 제안하였다. WIPO 도메인 이름 프로세스 최종보고서는 상표권과 도메인 이름 중 상표권을 우선권으로 인정하지 않으며, 선사용권자를 우선적으로 보호하며, 국제적 유명상표와 동일한 도메인 이름을 유명상표의 소유자가 아닌 제3자가 등록할 수 없도록 배제하는 장치가 필요함을 지적하였다.

③ 주요국 법제정현황

ㅇ 미국

미국은 1995년 2월 정보수집비용의 절감과 정부의 업무수행 개선을 목표로 하는 '문서작업감축법'을 제정하였고, 1996년 2월 통신사업의 경쟁 제한적 요소 철폐와 공정경쟁제도의 강화를 골자로 통신법을 개정하였다. 연방정부의 상품 및 용역계약에 정부차원의 전자상거래시스템인 FACNET(Federal Acquisition Computer Network)을 도입하는 등 연방 조달절차를 개혁하기 위해 1994년 1월에 '연방조달효율화법(Federal Acquisition Streamlining Act)', 1996년 '연방조달개혁법(Federal Acquisition Reform Act)'을 제정하였다. 민간부문의 인터넷 이용과 관련해서는 1998년 '디지털 밀레니엄 저작권법'을 제정하여 인터넷 환경에 맞추어 저작권법을 종합정비 하였으며, 1999년에는 '청소년인터넷사생활보호법'을 제정하여 소비자보호에도 관심을 기울이고 있다.

ㅇ 유럽과 일본

1999년 현재 EU는 공동체 차원에서 채택한 '데이터베이스 보호에 관한지침', '개인정보보호에 관한 지침' 등의 역내 국가 내 이행을 확보하는 절차를 밟고 있다. EU 회원국 중 독일이 1997년 7월 제정한 '정보통신서비스법'은 일련의 패키지법안으로 고도정보서비스법, 전자서명법, 개인정보보호법(이상제정), 형법, 질서위반법, 청소년유해 제작물보급법, 저작권법, 가격표시법 및 동법시행령(이상개정) 등 9개 법령으로 구성되어있으며 다른 국가의 인터넷관련 법제정비에 큰 영향을 미치고 있다. 일본은 1997년과 1999년에 WIPO 신조약을 반영하는 저작권법 개정을 단행하여 디지털 환경도래에 대응하고 있다.

ㅇ 사이버범죄협약

유럽의회(Council of Europe)가 승인한 사이버범죄협약은 사이버 공간상에서 발생할 각종범죄들을 처벌할 수 있도록 각국의 국내법을 정비하도록 하고 다양한 국제공조절차를 따르도록 함으로써 국제사회의 사이버범죄에 효율적으로 대처하기 위해 만들어진 최초의 국제협약이라는 데에 그 의의가 있다.

사이버범죄협약은 주로 다음의 네 가지를 이루기 위하여 제정되었다[17]. 첫째, 컴퓨터 시스템·네트워크 및 정보의 오용뿐만 아니라 이에 대한 기밀성(confidentiality)·무결성(integrity)과 유용성(availability)을 침해하는 행위 등을 범죄화하여 사이버 범죄로부터 사회의 안전을 도모하도록 한다. 둘째, 정보기술의 개발과 이용에 대한 법적 보호를 강화하고 사이버범죄에 관한 국가간·기업간 상호협력을 제고하도록 한다. 셋째, 사이버범죄에 대한 효과적인 처벌을 위하여 형사사건에 있어서 신속하고 원활한 국제공조방안을 마련하도록 하기 위한 목적이 있다. 넷째, 국내적·국제적 차원에서 사이버범죄행위에 대한 수사, 기소 및 탐지를 지원하고 신속하고 공정한 국제협력을 의무화함으로써 동 범법행위에 효과적으로 대응하기 위한 목적이 있다.

끝으로, 컴퓨터 시스템이나 자료와 관련된 범죄의 효과적인 수사 및 기소를 위해 기존의 형사사법공조조약이나 범죄인인도조약을 보충하고, 사이버범죄의 전자증거 수집을 지원하기 위함에 있다[18].

5. 결론 및 시사점

기업의 정보침해 및 각종 컴퓨터바이러스 사고는 해마다 폭증하는 추세로, 전자무역을 활용하고 있는 당사자들에게

는 간과할 수 없는 분야이다. 기존 전자무역에 있어서는 전자결제분야에서 특히 보안을 강조하였다. 그러나 본 논문에서는 전자무역에서 발생할 수 있는 정보화의 역기능인 정보보호(보안)적 측면에서 시스템 및 네트워크 장애 그리고 침해사고에 대하여, 시스템공격, 데이터공격 그리고 비즈니스 공격으로 크게 세 가지 유형에 대하여 분석하고 전략적 대응방안을 제시하였다는데 의의와 독창성을 주장할 수 있다. 부연하면 전략적 대응 방안을 정보보호(보안)장치와 기술적 측면 그리고 국내외 인터넷관련 법률과 국제기구들의 동향을 가지고 전략적 대응 전략을 제시하였다. 특히 전자무역의 보안은 전자무역거래 당사자간에 신뢰성을 제고시키고 각종 무역당사자간의 분쟁 및 사고의 소지를 줄일 수 있는 중요한 분야이다. 전자무역에 관련된 당사자들은 시스템공격, 데이터공격, 비즈니스공격에 대응하기해서 정부측면에서의 전자무역보안에 대한 정책적 관리와 보안인프라의 구축이 요망되고, 기업차원에서는 보안의식 강화와 정보보호장치 즉, 방화벽, 침입탐지시스템(IDS), 공개키기반구조(PKI), 가설사설망(VPN), 안티바이러스제품, 암호화, 생체인식기술 등의 활용 또는 정보보호전문업체를 통한 아웃소싱을 이용한 전자무역보안의 수단을 강구해야 된다. 위와 같은 연구결과를 가지고 다음과 같은 시사점과 향후 연구방향을 제시해 볼 수 있다. 우선 인터넷보안 관련 연구를 이제는 전자무역 분야에도 적극적으로 활용하여야 한다. 전자무역을 담당하고 있는 당사자들 간에 정보보호의 중요성을 다시 한번 강조하고 재확인해야 한다. 둘째, 끊임없이 발전하고 있는 해킹기술과 기법에 대응하기 위한 충분한 정보와 기술을 언제가 새롭게 갱신하는 것이 중요하다. 특히 전자무역중개를 하는 업체의 경우 데이터베이스의 중요성은 더욱 보호할 가치가 있는 자산이다. 마지막으로 폭넓은 정보보호의 체계 및 분야에 대하여 통합 보안적 측면에서 모든 그 해법을 제시하지 못한 것이 본 연구의 한계라고 할 수 있다. 향후 연구는 보다 통합적이고 종합적인 시각에서 전자무역과 정보보호를 접목하여 학제간 연구를 할 수 있는 기틀이 만들어져야겠다.

참 고 문 헌

[1] Riyad Eid, Myfanwy Trueman, Abdel Moneim Ahmed, A cross-industry review of B2B critical success factors, *Internet Research : Electronic Networking Application and Policy*, Vol.12, No.2, p.114, 2002,

[2] 한국정보보호진흥원, 2001년 주요 민간부문 정보보호 실태조사, Dec., 2001.

[3] 고윤승 · 신황호, "전자무역의 연구범위와 연구방법에 관한 고찰", 한국무역학회, 무역학회지, 제26권 제4호, pp.75-97, Sep., 2001.

[4] 이춘수 · 이장로, "한국인터넷무역 논문의 분류와 분석", 한국통상정보학회, 통상정보연구, 제4권 제1호, June, 2002.

[5] 김홍근, 최영철, 전자상거래 경쟁력 강화와 정보보호기술 개발 전략, KISA, Jan., 2004.

[6] 이정호, "전자거래의 확산에 따른 기업의 대응 방안에 관한 연구", 한국국제상학회, 국제상학, 제15권 제1호, p.436, 2000.

[7] 이승영 · 문희철 · 심상렬, "인터넷 전자무역 창업에 관한 연구", 한국무역학회, 무역학회지, 제24권 제1호, p.212, 1999.

[8] 한국전산원, http://stat.nca.or.kr/main03.html, Jan., 2004.

[9] http://www.wins21.com/wins_board/read.php?table=news&no=404, Jan., 2004.

[10] http://www.kisa.or.kr/K_trend/KisaNews/200006/opinion.html.

[11] 한국전산원, 한국인터넷백서, 제5장 보안 인증기술, 2000.

[12] http://www.etri.re.kr/news_m/news/news0111_29.htm.

[13] 정부연 · 신일순, XML을 통한 B2B 비즈니스 모델의 변화 및 시사점, 정보통신정책연구원, 정보 통신정책 ISSUE, 제13권 제6호 통권 130호, p.42, Sept., 2001.

[14] Hartman, J. and Evans, W., Fault tolerant application enhanced network-Project A project under the DARPA Fault Tolerant Networks Program, Hompage. Internet URL, http://www.cs.arizona.edu/ftn, Jan., 2000, 2004.

[15] 이창한, 전자거래에 관한 국제기구의 논의 현황과 한국의 법제화 동향, 인터넷법률, 제10호, Sept., 2002.

[16] 성선제, 류종현, 강장묵, 네티즌을 위한 e-헌법, Cyberlaw, 길벗출판사, 2003.

[17] 이정현, 사이버범죄협약에 대한 소고, 한국정보보호진흥원, July, 2001.

[18] Council of Europe, DRAFT CONVENTION ON CYBER-CRIME AND EXPLANATORY MEMORANDUM RELATED THERETO, Draft Explanatory Report, Strasbourg, June, 2001.

정 조 남

e-mail : jjn10@korea.com
1992년 전북대학교 대학원 컴퓨터공학과 (공학석사)
2004년 인하대학교 대학원 컴퓨터정보공학과 박사과정 수료
1994년~1997년 서울기능대학 교수
2000년~현재 유니사이버캠퍼스 대표이사
관심분야 : 정보보안, 생체인식, 패턴인식, 영상처리, 인터넷, 컴퓨터그래픽스, 전산교육 등

이 춘 수

e-mail : cybertrade@korea.ac.kr
1995년 동국대학교 무역학과(상학사)
1997년 성균관대학교 대학원 무역학과 (경제학석사)
2003년 고려대학교 대학원 무역학과 경영학 박사과정 수료
2003년~현재 고려대학교 기업경영연구원 연구원
관심분야 : 전자무역, 정보보호, B2B 등

강 장 묵

e-mail : mooknc@naver.com
1999년 고려대학교 일반대학원(경영학석사)
2003년 고려대학교 정보보호대학원 공학박사 수료
1996년~1997년 (주)쌍용정보통신 컨설팅팀 컨설턴트
1998년~현재 (주)슈퍼테크놀러지 연구소장
2001년~현재 서경대학교 컴퓨터공학과 교수
관심분야 : 유비쿼터스, 정보보안(프라이버시), 저작권(DRM) 등