정보보호산업 육성정책의 시스템 다이내믹스 분석

전재호, 최남희, 홍민기
(국립청주과학대학 행정전산학과)

I. 서론

인류 역사를 획기적인 기술혁명을 기준으로 대별할 때, 정보화 혁명을 농업혁명과 산업혁명에 이은 제3의 혁명으로 간주한다. 흥미로운 것은 급속한 기술발전은 긍정적 효과와 더불어 이에 상응하는 부정적 효과를 동반해 왔다는 것이다[1]. 현 시점에서 가시적으로 가장 심각하게 부각되고 있는 정보기술혁명의 부작용은 컴퓨터 바이러스와 해킹에 의한 피해로 나타나고 있다. 2000년의 바이러스 발생건수는 572건이고, 특히 Nimda 바이러스가 출현했던 2001년 9월에는 그 피해사례 접수만도 12,054건에 이르렀다. 또, 2001, 2002년 해킹사고 누적건수는 각각 10,526건과 14,065건으로, 2000년의 해킹사고 총괄 누계인 449건과 비교할 때 23,443%와 31,325%의 급격한 증가세를 보이고 있다(경찰청 사이버테러 대응센터 2003, 황성원 2002, 정보통신부 2001). 이외에도, 정부기관이나 민간기업의 전산시스템에 불법으로 침입하여 정보를 도용하거나, 전산시스템을 마비시키는 등 다양한 형태의 부작용들로 증가추세에 있다(CERTCC-KR, 2002).

이와 같은 정보화 혁명의 부작용은 정보화 혁명의 속도가 빠를수록 파괴적이다. 지난 1994년 이래 국가적 차원에서 초고속정보통신망 구축을 시작한 이후, 세계적인 정보통신 강국으로 등장한 우리나라가 최근의 SQL Slammer Worm에 의한 피해가 가장 컸던 것이 단적인 예라고 하겠다[2]. 그러나, 정보화 기술혁명에 의해 발생가능한 부작용에는 현재까지 나타난 문제에 더하여 국가안보나 사회치안, 개인인권 침해까지 예상된다는 점에 문제의 심각성

1) 농업기술 혁명 이후 나타난 부정적 효과로는 잉여농산물 쟁탈을 위해 인류 최초로 나타난 대규모 전쟁과, 평등사회에서 노예제/신분제 사회로의 이행을 들 수 있다. 산업기술 혁명으로 일부에서는 이상적 사회가 도래할 것이라고 기대하였으나, 산업의 발전으로 축적한 부와 기술을 활용한 제국주의, 세계대전 등의 부작용이 나타났으며, 계급간의 갈등이 심화되었던 바 있다. 정보화 혁명의 부작용은 아직 진행중인 관계로 그 실체가 완전히 드러났다고 할 수 없다. 현재로서는 '정보화 역기능'이라는 표현으로 개인정보 및 프라이버시 침해, 불건전 정보유통, 컴퓨터 바이러스, 정보시스템 불법 침입 및 파괴(해킹) 등과 같이 크게 4가지 종류를 구체적으로 논의하고 있다. 그러나, 이러한 현상들은 정보기술 혁명이 초래할 수 있는 부작용들의 작은 출발점들이고, 본격적인 정보기술 혁명의 부작용에 대해 인류가 적절히 대응할 준비를 하지 못한다면, 과거에 경험하였던 농업기술이나 산업기술혁명의 부작용과는 비교할 수 없는 엄청난 재앙으로 연결될 수 있다는 지적이 조심스럽게 제기되고 있다(김은환 외, 2000).

2) 정확한 피해규모는 추정이 불가능하지만, 각종 언론보도를 종합해보면 전세계적으로 우리의 피해규모가 가장 크다는 것을 유추할 수 있다. 이는 인터넷을 활용한 경제활동의 규모가 큰 것과, SQL서버 프로그램의 불법복제 사용이 빚어낸 결과라는 것이 일반적인 견해이다 (장성원 외, 2003)

이 있다(전재호외, 2000). 반면에 부작용이 커질수록 이 문제의 해결도구에 대한 수요가 급속히 증가하므로써, 정보보호용 제품 및 서비스 자체가 정보화시대의 유망산업으로 주목받고 있는 것도 현실이다.

이에 따라, 미국, 이스라엘, EU, 일본 등에서는 1990년대 중반부터 국가적 차원에서 정보보호 기술 및 산업을 개발 육성하고 있으며, 우리나라의 경우도 2000년부터 정보보호 기술개발과 산업육성등에 대해 국가적 지원책을 실시하고 있다[3]. 그러나, 정보보호의 중요성이 부각된 역사 자체가 일천하고, 정보보호 관련 정책부서가 신설된 것이 최근의 일인 우리의 경우 정책당국이 사용가능한 정책대안 자체가 극히 한정되어 있을뿐만 아니라, 정책효과성에 대한 분석도 이루어지지 못한 것이 현실이다.

본 연구에서는, 현시점에서 정책당국이 주로 채용하고 있는 정책대안들의 효과성을 시스템다이내믹스 시뮬레이션으로 분석하였다. 정보보호 산업은 이미 글로벌 경쟁상황으로 진입하였고, 정보화 역기능(해킹, 바이러스)의 증가에 따라 동태적으로 성장하고 있다. 또, 정보보호 제품 및 서비스는 정보통신 H/W와 S/W의 보급 및 활용정도, 국내외 시장규모, 기술축적정도, 전문인력 보유정도 등 다양한 요인들이 복합적으로 연관된 시스템적 특성을 가지고 있다. 이와 같이, 동태적 · 시스템적 특성을 갖는 정보보호 산업의 육성을 위한 정책대안 분석에 시스템 다이내믹스 방법이 적절하다는 것에는 재론의 여지가 없을 것이다.

현재, 정책당국에서 채용하고 있는 정책대안들은 전통적인 기술개발 지원, 그리고 최근에 시작된 전문인력 양성지원과 해외시장 진출 직접지원정책으로 대별할 수 있다. 정보보호 시장은 그 특성상 무역장벽이 큰 의미가 없는 관계로 이미 상당부분 글로벌 경쟁체제하에 있다. 따라서 본 연구에서는 정부의 지원정책이 없는 경우를 준거모형으로 하여 기술개발지원, 인력개발지원, 해외시장진출 직접지원 정책의 상대적 효과성을 시뮬레이션을 통해 정책의 상대적 효과를 비교분석하였다.

3) 우리나라의 경우 정보통신부내에 정보보호심의관실이 설치된 2000년이 정보보호 지원책을 본격적으로 실시한 원년이라고 할 수 있다. 이전까지는 주로 국방 목적의 암호기술 연구가 주류를 이루고 있었다(전재호외, 2002).

II. 정보보호 산업 및 육성 정책의 현황과 문제

1. 정보보호 체제 개요

정보통신 기술의 진전과 소비자 수요의 확산에 따라, 정보화 사회가 실현되고 있는 반면에, 정보시스템 무단 해킹, 정보전송내용 부인, 정보시스템 사용방해 등 정보시스템의 안전이나 개인의 프라이버시, 또는 전자상거래 등을 위협하는 요소들이 나타남에 따라서 이를 해소하고 안전하게 정보를 주고 받을 수 있도록 하는 정보보호 체제가 등장하였고, 최근 들어 그 중요성이 급격히 확대되고 있다.

정보보호는 정보화촉진기본법 제2조에 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 강구하는 것으로 정의되어 있다. 다시 말해서, 정보통신망, 단말기 등에서 처리되는 음성, 영상, 데이터 멀티미디어 서비스에서 정보의 유출 및 손상, 시스템 파괴, 바이러스 등의 각종 보안 위협요소로부터 정보통신 시스템을 보호하고 정당한 사용자의 신분을 확인함으로써 각종 정보서비스의 가용성을 보장하고 활성화시키기 위한 제반 관리적·기술적 활동을 지칭한다.

따라서, 정보보호 체제란 개인이나 조직이 정보보호 기능을 수행하기 위해 정보보호 하드웨어·소프트웨어 제품을 적절히 구축하고 지속적으로 관리(혹은 관리대행 서비스 이용)함으로써 자신의 정보시스템과 정보내용을 보호하는 시스템을 말한다(Stallings, 2000). 그러나, 정보보호를 등장하게 한 정보시스템 공격의 발전속도가 매우 빠르고 기술적 전문성이 심화됨에 따라서 정보보호 서비스를 전문적으로 제공하는 시장이 급격히 부상함으로써, 이러한 정보보호 서비스까지도 정보보호 체제의 범주에 포함된다(한국전자통신연구원, 2000). 따라서, 정보보호 체제를 크게 제품군과 서비스군으로 구별하는 것은 공통적이지만, 그 이하의 분류체제는 문헌별로 통일되어있지 못하다(정보통신부, 2001; 한국전자통신연구원, 2000; 길민정, 2001; Briney, 2001)[4]. 현재 시점에서 정보통신부와 한국전자통신연구원에서 사용하고 있는 정보보호 체제에 대한 분류와 분류된 제품 및 서비스 각각의 기능은 <표 1>과 같다(정보통신부, 2001; 전재호 외, 2000).

4) 정보보호 제품 및 서비스에 대한 분류체제가 통일되지 못한 것은 일차적으로는 정보보호의 중요성이 부각된 시기가 최근이라는 점에 기인하고 있다. 일부 학자들은 1980년대 후반을 "전자게시판의 전성기이며 동시에 전자게시판 해킹 시대"라고 구분하기도 하지만(Hughes, 1995) 이는 이전의 Stand-Alone형 컴퓨터로부터의 변화된 양상을 강조하고자 한 분류이고, 본격적으로 정보보호의 필요성이 부각된 것은 1990년 초반에 개발된 Internet상의 World Wide Web 시스템과 그 출발을 같이하고 있다는 것이 지배적인 견해이다. 인터넷을 활용한 정보화의 선두그룹에 속해 있는 우리나라의 경우에도, 1996년 4월에 현재의 한국정보보호진흥원의 모태가 되는 한국정보보호센터를 설립하여 본격적으로 정보보호체제를 정비하기 시작하였고, 주무 부처인 정보통신부에 정보보호를 전담하는 심의관실이 신설된 시기가 2000년이었으며, 정보보호에 관한 기본법인 "정보통신망이용촉진및정보보호등에관한법률"을 2001년에 공포했다는 점들이 이를 반증하고 있다. 국내에서 최초로 정보보호 제품 및 서비스에 대한 분류를 시도한 것은 2001년 2월에 정보통신부에서 발간한 "정보보호 기술개발 중장기 계획"에서 이었다.

<표 1> 정보보호 제품 및 서비스 분류

분류		정의 및 기능
정보보호 제품 (S/W 또는 H/W)	바이러스백신 (Anti-Virus)	컴퓨터바이러스의 부착여부 판독, 바이러스 제거 및 시스템 복구용 제품
	침입차단시스템 (Firewall)	외부망에서 해커 등 비인가자가 내부망으로 침입하는 것을 차단시키는 소프트웨어 또는 하드웨어. 방화벽이라고도 함
	침입탐지시스템 (IDS)	네트워크 또는 컴퓨터시스템에서 내·외부사용자에 의한 불법행위를 실시간적으로 탐지하는 소프트웨어
	인증제품 (Authentication)	패스워드 및 전자서명 인증서와 같은 소프트웨어나 혹은 생체인식 또는 IC 보안카드와 같은 하드웨어 등을 통해 사용자 신원을 확인하기 위한 제품. 동일한 인증기술 유형인 PKI와는 독립된 제품으로 간주함
	암호화제품 (Encryption)	저장한 파일내용을 암호화하여 적정한 해독키 없이는 복호화할 수 없도록 하는 보안기능을 지닌 제품. 전자우편 보안, 웹 보안, 디지털컨텐츠 보호 등을 보호하기 위한 암호화에 사용됨
	가상사설망 (VPN)	공공 정보통신망에서 두지점간의 안전한 연결을 만들어 주어 논리적(가상적) 사설망을 실현해주는 제품
	공개키기반구조 (PKI)	공개키 암호기술을 이용한 인증 프레임워크로 인터넷과 같은 개방형 환경에서 공인인증기관이 발행하는 인증서를 통해 전자문서의 무결성, 기밀성, 부인방지 등을 보장해주는 제품
	서버보안제품 (Secure OS)	운영체제의 문제로 인한 보안취약점에 대하여 커널수준에서 접근통제와 같은 보안기능을 수행하여 내/외부 불법침입자의 해킹을 방지 및 차단시키는 소프트웨어. 보안커널이라고도 함
	컨텐츠 시큐리티 제품	전자메일의 송수신이나 혹은 웹사이트 접속시에 전송되는 자료를 판독하여 금지된 내용 및 악의적 코드를 식별하고 처리하는 제품
	보안점검제품	패킷 모니터링, 취약점 점검 등을 통해 정보시스템의 보안취약점을 분석해주는 제품. 위험분석 도구, 취약점분석 도구, 패킷분석기, 스캐너 등 사용자나 관리자가 보안관리를 쉽게 할 수 있도록 도와주는 기능을 수행
정보보호 서비스	정보보호컨설팅	정보보호시스템 구축 및 운영, 정보보호 정책 수립 등 정보보호 전반에 걸쳐 자문 및 기술을 지원하는 서비스
	인증서비스	사용자 신원확인 및 전자문서의 안전·신뢰성을 보장하기 위한 인증기관의 인증서발급 및 검증수단을 제공하는 서비스
	보안관제서비스	업체나 기관들의 시스템·전산망의 보안업무를 보안전문업체가 일괄적으로 대행하는 서비스

자료 : 정보통신부. 2001.「정보보호 기술개발 중장기 계획」

<표 1>과 같이 규범적으로 분류된 정보보호 제품과 서비스는 다시 정보보호 기능의 강화 및 발전단계에 따라 ① 1단계 방어장치로서의 바이러스백신과 침입차단시스템 그룹, ② 2단계로서 정보흐름을 보호하기 위한 PKI와 VPN 그룹, ③ 3단계는 1, 2단계에 문제가 있을 경우를 대비한 침입탐지시스템, 컨텐츠 보안, 보안관리 등의 세 가지 범주로 재구분하기도 한다(남택용, 2002). 이와 같은 분류는 정보보호 체제 그 자체의 분류뿐만 아니라 정보보호 체제 등장 및 발전의 원인인 정보침해 기법의 발전 추세에도 동일하게 적용된다. 이 같은 정보보호 체제의 발전단계에 따라 정보보호는 단일 시스템 보호에서 네트워크 시스템 보호로, 수동적/방어적 보호에서 능동적 보호로 그리고 폐쇄적 보호에서 개방적 보안으로 전이해 가고 있다(손승원, 2000). <표 1>의

분류를 3단계 분류로 재구성하면 <표 2>와 같다.

<표 2> 정보보호 제품 및 서비스의 기능단계별 분류

정보보호 기능단계	구분기준 및 보호대상	단계별 제품 및 서비스
1단계	• 기계적/물리적/방어적으로 악의적인 코드의 존재여부 체크 • 보호대상 : 단일시스템이나 단일조직내의 시스템	바이러스 백신, 침입차단시스템
2단계	• 기계적/물리적/방어적으로 보호기능을 수행한다는 점은 1단계와 동일하지만, 단일시스템이나 단일조직에 국한되기보다는 이들간의 연결네트워크 보호에 중점을 두고 있음 • 보호대상 : 다수의 시스템들과 이들간의 연결네트워크	인증제품, 암호화제품, 가상사설망, 공개키기반구조, 서버보안제품
3단계	• 기계 및 인간에 의해, 지능적/능동적 보호기능을 수행하고 논리적(내용적)보안기능이 추가된 형태 • 보호대상 : 1/2단계의 보호대상에 더하여 정보내용자체도 보호	침입탐지시스템, 컨텐츠시큐리티, 보안점검, 정보보호컨설팅, 인증서비스, 보안관제서비스

2. 정보보호 산업 현황 및 문제점

정보보호의 보안대상이 되는 정보는 가장 부가가치가 높은 상품이면서 동시에 새로운 부가가치 창출의 원료로 활용된다. 또, 국가 및 기업경영, 그리고 개인활동에 관련된 정보의 안전한 보호여부에 따라 국가·기업·개인의 흥망성쇠가 결정될 것이다. 따라서, 고도 정보화와 정보보호는 지식기반사회의 국가발전이라는 수레의 두 바퀴처럼 상보적 발전이 불가피한 관계이다. 이는 다른 말로 하면 어느 한쪽의 정체가 다른 쪽의 발전을 저해한다는 의미를 담고 있다. 이를 산업의 측면으로 이전하여도 같은 결론을 도출할 수 있다. 즉, 정보보호 산업은 정보통신산업과 동반 성장할 것이며, 특히, 정보시스템, 네트워크, 컨텐츠 및 어플리케이션에 걸친 정보통신 전 영역에 대한 정보보호를 통해 부가가치를 창출하는 산업으로써 타 IT 산업분야에 비해 약 2.5배 이상의 고성장을 기록할 것으로 전망된다.

<표 2> 정보보호산업과 다른 IT산업의 성장률(2001-2007)비교

구 분	정보통신산업	소프트웨어산업	정보보호산업
세 계	11.7%	16.3%	28.8%
국 내	19.5%	26.8%	36.2%

자료 : 한국전자통신연구원. 2002. 「2002 정보통신 기술·산업 전망」

이와 같이, 유망 고성장 산업으로 판단되는 정보보호 산업의 국내/세계 성장전망치를 살펴보면 대단히 실망스럽다. 세계 정보보호 시장규모는 2001년 168억달러에서 연평균 28.8%로 성장하여 2007년에는 766억달러로 대략 4.6배의 증가세를 보이는 것으로 나타나고 있다. 반면 국내 정보보호 시장은 2001년 3,755억원에서 2007년 2조 4천억원 수준으로 6.4배의 성장을 보임으로써 성장률에서는 세계규모를 앞지른다. 그러나, 총액규모를 대비해보면 전세계 시장의 1.5% ~ 2.5% 대를 차지하므로써 국내시장규모가 극히 미미하다는 것을 알 수 있다. 이러한 현실은 장기적으로 국내업체들이 해외시장으로 진출해야만 한다는 사실을 확연히 보

여주고 있다. 그러나, 국내 정보보호 업체들 대부분이 자체 기술력이 부족하고 영세하여 상당수의 업체들이 외국업체의 판매채널로서의 기능을 수행하고 있다는 현실을 감안한다면 정보보호 산업육성 정책의 필요성이 절실히 필요하다고 하겠다[5].

<표 3> 세계 정보보호 시장 전망

(단위:백만달러)

분류	2001	2002	2003	2004	2005	2006	2007	CAGR*
제품	8,533	11,181	14,785	19,217	24,606	32,582	43,222	30.8%
서비스	5,739	7,152	8,869	11,341	14,085	17,361	21,402	24.5%
기타	2,532	3,285	4,270	5,554	7,118	9,230	11,968	29.5%
합계	16,804	21,618	27,924	36,112	45,809	59,173	76,592	28.8%

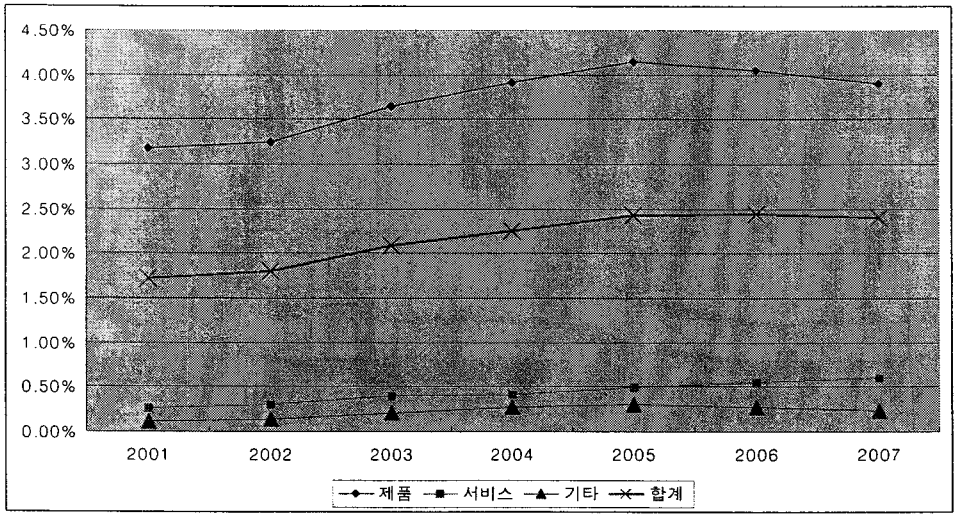
* CAGR : Compound Annual Growth Rate
자료 : 한국전자통신연구원. 2002. 「2002 정보통신 기술·산업 전망」

<표 4> 국내 정보보호 시장 전망

(단위 : 억원)

분류	2001	2002	2003	2004	2005	2006	2007	CAGR
제품	3,530	4,721	7,003	9,772	13,254	17,178	21,887	35.5%
서비스	191	275	450	610	911	1,241	1,685	43.8%
기타	34	56	110	195	280	320	365	48.5%
합계	3,755	5,052	7,563	10,577	14,445	18,739	23,937	36.2%

자료: KISA · KISIA. 2001. 「국내 정보보호산업실태조사」



* 환율 : 1$ = 13,000원으로 계산

<그림 1> 세계시장 대비 국내시장 규모의 상대적 비율 추이

5) 국내 정보보호 업체의 수는 2002년 4월 현재 144개이다. 이들중 상당수는 설립된지 5년 미만의 신생 벤처기업으로 규모가 작아 장기적인 경쟁력 배양에 문제가 있는 것으로 나타나고 있다. 국내 정보보호 업체들의 평균 자본금은 20.6억, 평균매출액 21.7억원 수준이며 매출액 대비 평균 R&D 투자비율은 35.4%로 높은 수준이나 평균 절대 투자금액은 7.7억원 수준으로 매우 미약한 수준이다(정보통신부 2002).

국내 업체들중 가장 대표적인 정보보호 업체로 부상한 안철수 연구소의 매출액이 2001년 현재 254억원으로 세계적인 정보보호업체인 Symantec사의 2000년도 매출액의 1%수준이라는 것이 우리 업체의 영세성을 극명하게 보여주고 있다.

<표 5> 국내외 정보보호 주요 업체간 매출액 비교

(단위 : 억원)

업체명	매출액	업체명	매출액
Symantec	24932	안철수연구소	254
Computer Associates	24254	니트젠	225
IBM	22218	한국정보공학	195
Network Associates	17639	어울림정보기술	191
Check Point	14586	시큐아이닷컴	190
RSA Security	11533	시큐어소프트	140

* 외국업체의 매출액은 2000년 12월 기준이고, 국내업체의 매출액은 2001년 공시자료
* 환율 : 1$ = 1,300원 적용
자료 : Gartner Group. 2002. 「정보보호전문기업 편람」

또, 현재 시점에서 우리 업체들의 해외 진출정도를 가늠해볼 수 있는 수출액도 총 매출액에 대비하여 매우 미미한 실정이다. 즉, 현재까지는 규모가 작은 국내시장 위주로 판매가 이루어지고 있고, 수출도 극히 소수의 업체들에 의해 이루어지고 있는 것이 현실이다. 다만, 연평균 수출증가율이 305%를 넘어서고 있다는 점이 우리 업체들이 수출확대를 위해 노력하고 있음을 단적으로 보여준다고 하겠다.

<표 6> 국내 정보보호 업체들의 매출중 수출 현황

(단위 : 억원)

구분	2000년	2001년	2002년(추정)	CAGR
매출(A)	1705	3962	5568	80.7
수출(B)	44	349	722	305.1
매출대비 수출비율	2.6%	8.8%	13.0%	

자료 : KISA · KISIA. 2001. 「국내 정보보호산업실태조사」

정보보호 산업은 기술집약적 산업이다. 특히, 수학, 통계학, 전산학, 전자공학이 결합되어 제품을 생산해야 하는 복합적 기술산업이다. 여기서 암호 알고리즘과 같은 기초학문분야의 기술은 정보보호 제품에 핵심요소이면서 이분야의 기술격차를 만회하기가 매우 어렵다는데, 문제의 심각성이 있다. 더구나, 영세한 우리 업체들이 중장기적으로 이러한 기술개발을 위해 막대한 연구개발 투자를 실행할 능력이 없다는 것은 전술한 바와 같다. 따라서, 이부문에 대한 정부차원의 지원책은 필수불가결하다고 하겠다. 현재 정보보호 산업분야를 선도하고 있는 주요 선진국과 우리의 기술격차는 다음 <표 7>에 나타난 바와 같다. 표에 나타난 기술격차가 그리 크지 않은 것으로 보일 수 있으나, 학습효과가 초기에는 느리게 증가하다가 일정수준 이상의 지식축적이후에 가속도가 발생하는 것을 감안한다면, 이 격차를 만회하기 위해서는 집중적이고 장기적인 연구개발 투자가 필수적이라고 하겠다.

<표 7> 선진국과 국내의 정보보호 기술 수준 비교

대분류	중분류	기술 격차 (년수)	기술 수준	
			선진국	국내
정보 보호 기반 기술	암호 기술	3-5	- 대부분의 암호기술 확보 및 상용화	- '98년 SEED개발, 상용화 추진
	인증 기술	1-3	- 인증 기술 상용화 및 상호 인증 기술 개발 중	- 관련 법, 제도의 조기 정착 - 인증 기술 개발 중
	정보보호 표준화 및 평가기술	3-5	- 전체 정보보호분야의 평가를 수행 - CC기반 평가 수행	- 부분적으로 추진중 - CC 도입 준비중
	평 균	2-5		
시스템/ 네트 워크 정보 보호 기술	시스템보호기술	3-6	- Secure OS 등 최상급 운영체제 기술 확보	- 연구초기 단계
	보안 IC카드기술	1-2	- 32비트 IC카드 상용화	- 32비트 IC카드 개발중
	네트워크보호기술	3-5	- multicast 보안, 무선N/W보호 기술력 확보	- VPN 등 고전적 N/W 보호 제품에 대한 기술 보유
	해킹 및 대응기술	1-2	- 탐지 및 역추적 등 대응 기술의 연구 및 개발	- 침입차단과 Anti-Virus 백신 제품은 국제경쟁력 확보 - 시스템취약성 분석 및 침입 탐지기술은 아직 미약
	평 균	2-4		
응용 정보 보호 기술	전자거래 정보보호 기술	1-2	- B2B 정보보호 기술 상용화	- B2C 정보보호 기술 개발
	응용서비스 보호기술	1-2	- 응용서비스 원천 기술을 확보하고 있어 정보 보호 기술 적용이 용이	- 응용 서비스에 대한 부분적인정보보호 기술은 개발 - 인터넷뱅킹, 사이버트레이딩 관련 기술력은 확보
	평 균	1-2		

자료 : ETRI. 2002「2002 정보통신 기술·산업 전망 (2002년~2006년)」

기술집약적 산업은 다르게 표현하면 전문기술인력에 의해 성패가 좌우되는 분야라고 하겠다. 국내 정보보호 산업이 태동한 것이 최근이고, 정보보호 기술자체가 학제적 결합을 필요로 하는 관계로, 현시점에서 전문인력의 부족이 산업발전에 걸림돌로 작용하고 있다. 정보보호 시장의 규모가 급속히 증가하고 있는 반면, 인력 공급은 서서히 증가함에 따라서 인력부족 문제는 상당기간 지속될 것으로 예측되고 있다. <표 8>에 나타난 바와 같이, 2003년부터 2007년까지 누적적으로 22,000여명의 인력부족이 예상되고 있다.

<표 8> 연도별 국내 정보보호 인력 수급 전망

(단위 : 명)

구 분	2002	2003	2004	2005	2006	2007	합계(2003~7)
총 종사인력	13,332	17,208	22,198	28,632	36,915	47,586	-
신규인력 수요	-	3,876	4,990	6,434	8,283	10,671	34,254
인력공급	-	1,312	1,688	2,172	2,795	3,596	11,563
수급차	-	-2,564	-3,302	-4,262	-5,488	-7,075	-22,691

* 정보보호인력 수요는 정보보호산업체 종사자 및 관련분야의 정보보호업무 종사자를 기준으로 한국정보보호산업협회(2001.12)와 한국정보통신산업협회(2002.5)가 조사한 자료이며, 인력공급은 전문대학, 대학, 대학원에서 배출되는 인력을 기준으로 조사된 자료임

자료 : 정보통신부. 2002. 「중장기 정보보호 기본계획」

3. 정보보호 산업 육성정책 현황과 문제점

현시점에서 정보보호 산업을 육성하기 위한 정책은 크게 세가지 그룹으로 대별할 수 있다. 일차적으로는 과거 정보통신 기술 개발 정책의 연장선상에서 이루어지고 있는 기술개발 지원정책이다. 다음으로는 2000년부터 시작된 인력양성정책으로 현재 전국 4개 대학을 선정하여 정보보호센터를 운영지원하고 있다. 마지막으로 2002년 후반기부터 기획단계에 있는 해외진출 직접지원정책을 들 수 있다. 그러나, 정보브호 산업의 태동과 정책당국의 신설이 모두 최근에 이루어진 관계로 아직까지 충분한 정책대안이 마련되지 못한 것이 현실이다. <표 9>에서 볼 수 있는 것처럼 대부분의 정책이 "계획"단계에 머물러 있음을 알 수 있다. 추가적으로 보다 근원적인 문제점이라고 지적할 수 있는 것은 소프트웨어 산업의 해외진출 지원체제와의 연계가 미비한다는 것이다. 정보보호 제품 및 서비스는 S/W와 H/W의 결합형태이므로 소프트웨어 산업과의 연합을 통한 해외진출 추진은 상호호혜적일 것이다. 현재와 같은 독립적 정책추진은 정책주무부서와 실무부서가 이원화되어있음으로 인해 나타나고 있는 결과라고 하겠다[6].

6) 소프트웨어 산업육성은 정보통신부내 정보통신정책국 소트웨어산업과가 담당하고 있고, 실무담당기관은 한국소프트웨어진흥원이다. 반면, 정보보호산업은 정보통신부 정보화기획실내에 신설된 정보보호산업과가 정책담당부서이고, 실무담당기관은 한국정보보호진흥원이다. 소프트웨어산업분야의 해외진출지원정책은 상당한 진전을 이루고 있으므로, 정보보호 산업의 해외진출시에 소프트웨어산업분야의 해외진출지원 정책대안과 인프라를 공동활용한다면 보다 효과적일 것이다(전재호외, 2002).

<표 9> 정보보호 산업 육성정책 현황

정책 대안	세부 정책
기술개발 지원	- 국책연구소를 통한 기술(기초기술, 산업화기술) 개발 지원 - 대학 정보보호 센터 기술개발 지원 - 기술·제품 시험용 고가장비 지원(계획) - 국제수준의 정보보호시스템 평가체제 구축(계획)
인력개발 지원	- 대학 정보보호 센터 육성을 통한 인력양성 지원(현재 4개인 대학 정보보호 연구센터이외에 생체인식분야 신규센터 설립 및 지원기간과 규모 확대) - 해외 유수대학 및 대학원 과정에 향후 5년간 50명 선발 유학지원(계획)
해외진출 직접지원	- 해외전시회 비용 지원 - 해외 시장정보 조사·분석 및 제공(계획) - 국내 정보보호 산업 포탈사이트 구축(계획) - 해외시장 개척단 파견(계획) - 해외 i-Park와의 연계 강화(계획) - 현지 전문 마켓채널, 채널사업자를 통한 기업상담회 개최(계획) - 해외 대형 구매자 초청 마케팅 행사 개최(계획) - 제품사양, 매뉴얼 등을 진출대상국에 맞추어 현지화하도록 지원(계획) - 한·중·일 3국간 정보보호 협회, 단체등을 연계하여 상호정보제공, 공동 기술개발 및 표준화 추진(계획) - 국제 공통기준 평가인정협정(CCRA) 가입추진(계획) - 국제적 인증획득을 위한 기술평가 비용 일부 지원(계획)
기타(내수진작)	- 국가기관 및 민간분야 정보보호 투자확대 유도(계획)

자료: 정보통신부. 2002. 「정보보호 중장기 기본계획」에서 정리

III. 정보보호 산업 육성정책 모델링

정부차원의 정보보호 산업 육성정책은 크게 기술개발, 인력양성, 해외진출 지원부문으로 대별될 수 있음은 전술한 바와 같다. 그러나, 보다 세부적으로 살펴보면 매우 다양한 요인들이 결부되어 정책의 효과가 나타나게 된다는 것이 명백한 사실이다. 이에 더하여, 정책적 노력의 투입과 정책효과의 발현은 상당한 시간차이를 두고 동태적으로 발생한다. 다양한 요인으로 구성되어진 문제는 시스템적 관점의 접근을 필요로 하며, 시간의 경과에 따른 효과의 변화라는 특성은 정태적 분석이 아닌, 동태적 분석이 적합하다는 것을 말해주고 있다. 본 절에서는 이와 같은 문제의 특성을 고려하여 시스템의 동태적 분석에 적합한 시스템 다이내믹스(System Dynamics) 시뮬레이션 기법을 사용하여, 정보보호 산업 육성 관련 주요정책을 분석하였다.

그러나, 본절에서 이루어진 시뮬레이션 분석은 상당한 수준으로 단순화되고 통합되어진 형태로 한정되어져 있다. 본 연구에서 고려되고 있는 정보보호 산업 지원 정책 시스템을 조작적 관점(Operational Perspective)에서 살펴보면 정보보호분야에 국한되기는 하지만 국내

외 시장을 포괄해서 기업간 협력 및 경쟁을 고려해야 하는 거시경제 시스템 분석에 해당된다. 따라서, 세분화되고 완성도가 높은 시스템 다이내믹스 시뮬레이션 모델의 구축과 분석은 상당한 양의 세부 자료를 필요로 하므로 이에 상응하는 인력과 시간의 투입이 요구되는 작업이다. 뿐만 아니라, 일반적인 시스템 다이내믹스 분석의 진화단계 관점에서도 본 장에서 이루어진 분석이 적절하다고 하겠다. 일반적으로 시스템 다이나믹스 분석의 진화단계는 크게 ①해당 정책 시스템 구조 분석(Structure Analysis), ②소규모 직관기반 모델(Small & Insight-Based Model) 개발 및 분석, ③ 세부화 / 미세조정 모델(Detailed & Calibrated Model) 개발 및 분석, ④ 모델을 활용한 지속적인 정책전략 관리(지속적인 모델 수정작업 포함)으로 대별한다(Lyneis, 1999 & 1998)[7]. 본 절에서 논의된 분석은 이중 ①, ②단계에 해당하는 것으로 주로 정책담당자와 함께 대상문제의 횡적 범위(Model Breadth)를 설정하고 문제범위에 포함된 주된 인과관계를 파악하는데 활용한다. 또, 세부 현실 데이터를 활용하기보다는 상대적/직관적 데이터를 사용하여 정책시스템의 전반적 행태(Behavior)를 살핌으로써 개략적인 정책 시사점을 도출하게 된다.

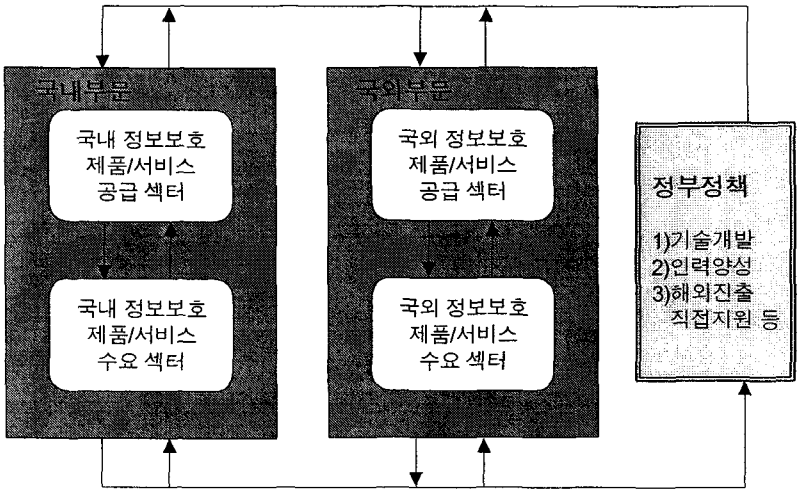
1. 정보보호 산업 육성정책 시스템 구조 분석

정보보호 산업 육성정책 시스템 분석은 국내외 정보보호 제품과 서비스의 공급측면과 수요측면을 포괄적으로 고려하는 것을 필요로 한다. 본 연구에서 주된 내용으로 다루고 있는 국내 정보보호 산업은 이미 글로벌 경쟁체제에 돌입하였기 때문이다. 따라서, 본 절에서 상정하고 있는 정보보호 산업 육성정책 시스템의 기본적인 구조는 다음 <그림 2>와 같다. 그림에 나타난 바와 같이, 본 절에서 고려하는 구조는 상당한 수준으로 통합화/단순화되어 있다. 즉, 정보보호 분야의 다양한 제품 및 서비스를 통합해서 고려하고 있고, 전세계 여러 국가의 상황이 상이함에도 불구하고 국내와 국외로만 대별하고 있다. 전술한 시스템 다이내믹스 분석의 진화단계에서 제 2단계까지의 주된 목적은 가장 기본이 되는 인과관계를 파악하는 것이므로, 이러한 단순화/통합화를 통해 최대한 모델링을 단순화한 것이다[8]. 분석의 3단계로 진행해간다면 이와같이 2단계에서 개발된 기본 인과관계를 국가별(혹은 국가군별), 개별 상품별로 확장해가게 된다.

---

7) 여기에 제시한 "분석의 진화단계"는 "분석의 단계"와는 상이한 개념이다. 분석의 진화단계는 해당문제에 대한 모델의 깊이(Depth)를 심화해가는 과정이고, 분석의 단계는 동일한 깊이를 사용해서 일정한 순서에 따라 문제를 분석해가는 과정이라고 볼 수 있다. 따라서, 분석의 진화단계는 매 진화단계마다 분석의 모든 단계(①문제정의, ②인과지도(Causal Map) 작성, ③ 모델구축, ④시뮬레이션, ⑤타당성 평가, ⑥정책분석; 김도훈 외, 1999)를 반복적으로 수행해야 한다는 것이다.

8) 시스템 다이내믹스 모델링을 포함하여 거의 대부분의 모델링 목적이 복잡한 현실에서 특징적인 주요 요인만을 추출하여 현실의 상태를 모사하는 것이라고 할 수 있다. 특히, 시스템 다이내믹스 모델링에서는 모델링의 목적(관심대상이 되는 문제현상)이 설정되면, 가능한한 단순하게 관심대상이 되는 문제행태를 재현하는 것이 선행과제라고 하겠다. 이러한 개념은 15세기 영국의 철학자 Occam에 의해 처음으로 구체화되었고, 그의 이름을 따서 Occam's Razor라고 한다(High Performance System, 2001).



<그림 2> 정보보호 산업 육성 정책 시스템의 개괄적 구조

위 <그림 2>와 같이 단순화/통합화된 시스템 구조를 상정하게 되면, 직관에 기초한 상대적 데이터를 사용해서 비교적 빠르게 단순직관 기반 모델을 구축할 수 있고, 이를 활용하여 일차적인 시뮬레이션 분석을 수행할 수 있지만, 세부적인 정책대안을 모두 비교평가하거나, 정책집행 최적시기(Policy Timing)를 파악하는데에는 한계가 있다. 이러한 한계는 모델 구조의 단순성에만 기인하기도 하지만, 모델구축에 사용된 데이터가 직관적/상대적 크기로 입력되었다는 것에 더 큰 원인이 있다고 하겠다. <그림 2>의 개괄적인 시스템 구조는 국내외 정보보호 산업분야의 수요/공급을 모두 고려하고 있으므로, 이에 상응하는 현실 자료를 단기간에 수집하기 어렵기 때문에 본 연구에서는 2단계 단순모델링까지만 분석이 진행되었다.

2. 정보보호 산업정책 시스템 인과지도

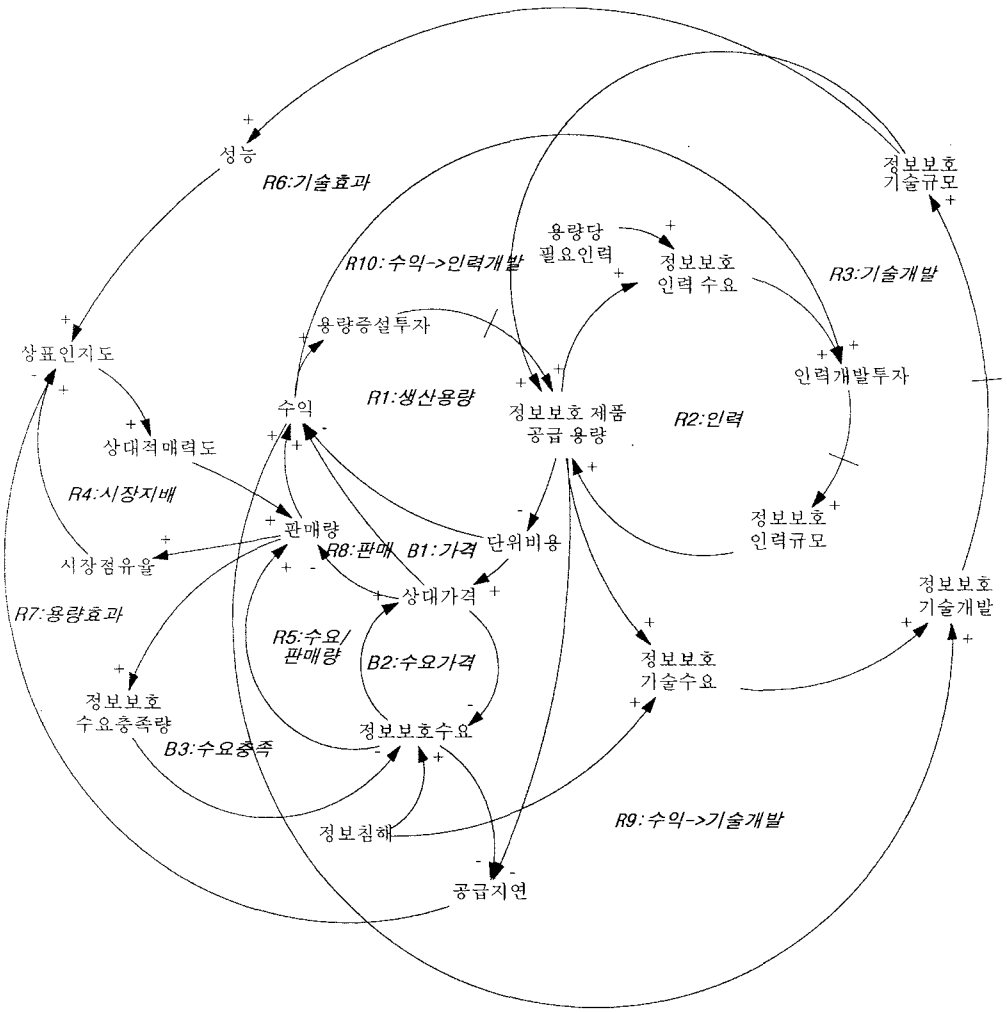
전술한 시스템 구조범위 내에서 정보보호 산업 성장에 핵심적인 역할을 하는 요인들간의 인과관계를 고려하여 인과지도(Causal Map) 작성을 수행하였다. 인과지도는 다음과 같은 동태적 가정들을 기반으로 하여 작성하였다.

가정1 : 국내외의 정보보호 산업 수요기반이 되는 인터넷 활용정도의 증가세는 현시점에서 큰 차이를 보이지 않는다[9](이 가정에 의해서 인터넷 활용정도의 증가세는 본 인과지도에서

9) 정보보호는 주로 인터넷을 활용하는 정보시스템을 대상으로 이루어진다. 따라서, 인터넷 활용정도에 따라서 정보보호에 대한 수요가 상당한 영향을 받는 것이 사실이다. 그러나, 본 연구에서 주로 고려하고 있는 것은 정보보호 산업의 글로벌 경쟁체제에서 우리와 경쟁상대가 되는 국가 및 시장이다. 따라서, 경쟁상대가 되는 국가의 범위는 인터넷 활용측면이나 정보보호 산업의 발전측면에서 OECD 회원국이나 EU회원국 정도로 한정할 수 있다. 이때, 국가별 인터넷 이용정도의 성장세를 비교할 수 있는 대표적인 지표로 활용되는 것이 "국가별 인터넷

고려하지 않는다.).

가정2 : 국내 정보보호 산업의 해외진출 정도는 전세계 시장에서의 국내 정보보호 업체가 갖는 상대적 매력도에 의해 결정된다(이는 진출/진입에 대한 인위적인 무역장벽이 없음을 가정하는 것이고, 외국 정보보호 업체의 국내시장 진출도 동일한 기준이 적용됨을 가정하고 있는 것이다.).



<그림 3> 정보보호 산업 시스템 인과지도

가정3 : 상대적 매력도는 상대적 가격, 성능(기술지원 포함), 상표인지도(공급신속성, 시장점

호스트 성장률"이다. 1998년에서 2000년사이의 국가별 인터넷 호스트 연평균 증가율을 보면, 우리나라가 21.0%이고, OECD평균 증가율이 20.9%, EU평균 증가율이 21.1%로 큰 차이를 보이지 않는다(KRNIC, 2001).

유율 등의 효과 포함)등에 의해 결정되고 유동적으로 변화한다.
가정4 : 정보침해 정도에 따라 정보보호 필요성이 누적적으로 증가하고(반대로 일정기간이 경과하도록 정보침해가 발생하지 않으면 정보보호 필요성이 일정비율로 감소), 정보보호 필요성이 증가함에 따라서 국내외 정보보호 수요가 증가한다.

가정5 : 본 모델에서는 정보보호 산업 육성관련 주요 정책의 효과를 상대적으로 비교평가하는 것을 주된 목적으로 하므로, 분석시점에서의 누적수익은 국내외 모두 0에서 시작한다고 가정한다.

가정6 : 본 모델에서 시장규모 확장의 주된 동인인 정보침해는 국내외 모두 2004년부터 주기적으로 발생하는 것으로 가정한다(현실에서의 정보침해는 무작위적으로 발생하지만, 모델내에서 이와 같이 설정했을 경우 시뮬레이션마다 결과가 다르게 나타나기 때문에 주기적으로 발생한다고 가정하였다.)

<그림 3>에 나타난 인과지도는 국내외 업체를 불문하고, 개별 업체들에게 공통적으로 적용되는 주요 인과관계를 개략적으로 작성한 것이다. 피드백 루프들중에서 R로 표시된 루프는 자기강화(Self-Reinforcing)적 성격의 갖는 양의 피드백 루프(Positive Feedback Loop)이고, B로 표시된 루프는 시간경과에 따라서 스스로 균형점을 찾으려는 특성(Balancing)을 갖는 음의 피드백 루프(Negative Feedback Loop)이다. 본 인과지도에 명시적으로 표시된 루프는 13개이다.

양의 피드백루프들 중 R1으로 표시된 루프는 생산용량 증설의 자기강화적 효과를 나타내고 있다. 여기서 생산용량이라는 용어는 일반적인 생산용량에 더하여, 현재 기업내부적으로 보유하고 있는 기술, 전문인력, 투입가능 자원등을 포괄하는 총체적 개념으로 사용하였다. 수요가 공급을 초과하는 경우를 상정한다면 생산용량의 증대는 단위당 고정비용을 감소시킴으로써 전체적인 단위당 비용을 감소시키고, 이를 통해 수익을 증대시켜 다시 생산용량 증대 투자에 긍정적인 효과를 가져온다는 것이다(물론, 이 양의 피드백 루프가 수요감소에 의해 비용증대로 선회하게 되면 지속적으로 비용증대를 가져오는 악순환(Vicious Circle)의 역할을 할 수도 있다.)

R2 루프는 생산용량이 증대되었을 경우 인력에 대한 수요가 증가하고 이는 인력개발에 대한 투자를 가져온다. 인력개발 투자는 가용인력규모를 증대시킴으로써, 다시 생산용량 증대에 긍정적 효과를 가져오게 된다. 물론 이경우도 이와 같은 선순환(Virtuous Circle)로만 작용하는 것이 아니라, 생산용량이 축소되는 경우는 악순환으로 작용하게 된다. R3 루프는 기술개발 효과를 표시한다. 생산용량의 증대는 추가적인 기술수요를 발생시키고, 이를 통해 기술개발 투자가 이루어지면, 다시금 생산용량 증대에 긍정적 효과를 갖는다. R4 루프는 다양한 긍정적 요인들에 의해 판매량이 증가하게 되면, 이는 시장점유율 향상과 이를 통한 인지도 향상으로 상대적 매력도를 상승시켜서 판매량의 증가로 나타난다는 양의 피드백을 나타내고 있다. R5는 수요증가-수익증가-용량증설투자증가-단위비용 하락-상대가격 하락-수요

증가로 연결되는 양의 피드백 루프이다. 즉, 수요의 증가는 단기적으로는 추가수요증가를 유발한다는 것이다. 그러나, 중장기적으로는 공급지연으로 연결됨으로써 제품매력도를 하락시켜서 수요를 감소시키는 쪽으로 작용한다. R6루프는 기술축적이 제품성능(제품 자체의 성능과 사후 서비스의 기술적 능력도 포함) 향상으로 이어지고, 이는 제품매력도를 상승시켜서 수익을 증가시키고 이는 다시 기술개발 투자의 여지를 증대시키는 양의 피드백을 형성하고 있다. R7은 충분한 생산용량을 구축하게 되면 수요에 대한 반응속도가 빨라지게 됨으로써 역시 상대적 매력도를 높이고, 이는 다시 수익으로 이어져 생산용량 확대여력을 증대시키는 양의 피드백 루프를 형성하고 있다. R8 루프는 용량증대-단위비용하락-단위가격하락-판매량증가-수익증가-용량증설투자 확대-용량증대의 선순환을 내포하고 있다. R9 루프는 정보보호 업체의 수익 증가가 기술개발 투자를 증가시킴으로써 보유기술규모가 증가하고 이로인해 공급용량의 증대로 수익이 증가하는 양의 피드백을 형성하고 있다. R10루프는 수익이 인력개발투자로 이어짐으로써 다시 수익증대로 연결되는 피드백 루프를 나타낸다.

이상의 열가지 루프가 대표적인 양의 피드백을 형성하고 있는 반면, 음의 피드백루프는 상대적으로 적은 세가지 경우가 포함되어져 있다. 첫 번째 음의 피드백 루프는 용량증대에 의해 단위당 비용이 하락하면, 경쟁압력에 의해 단위당 가격도 하락함으로써, 수익이 감소하고 이로 인해서 추가적인 용량증대 여력이 감소한다는 것을 나타내고 있다. B2 루프는 수요와 가격의 상쇄작용을 설명하고 있다. B3 루프는 정보보호 산업의 특징을 반영한 음의 루프로, 정보보호 제품 혹은 서비스의 판매는 구매자로 하여금 일정기간동안 추가적인 수요를 발생시키지 않도록 하는 현상을 반영하고 있다. 정보보호 제품 및 서비스는 구매이후 일정기간 동안은 추가적인 투자가 멈추게 되는 내구재의 성격을 갖기 때문이다.

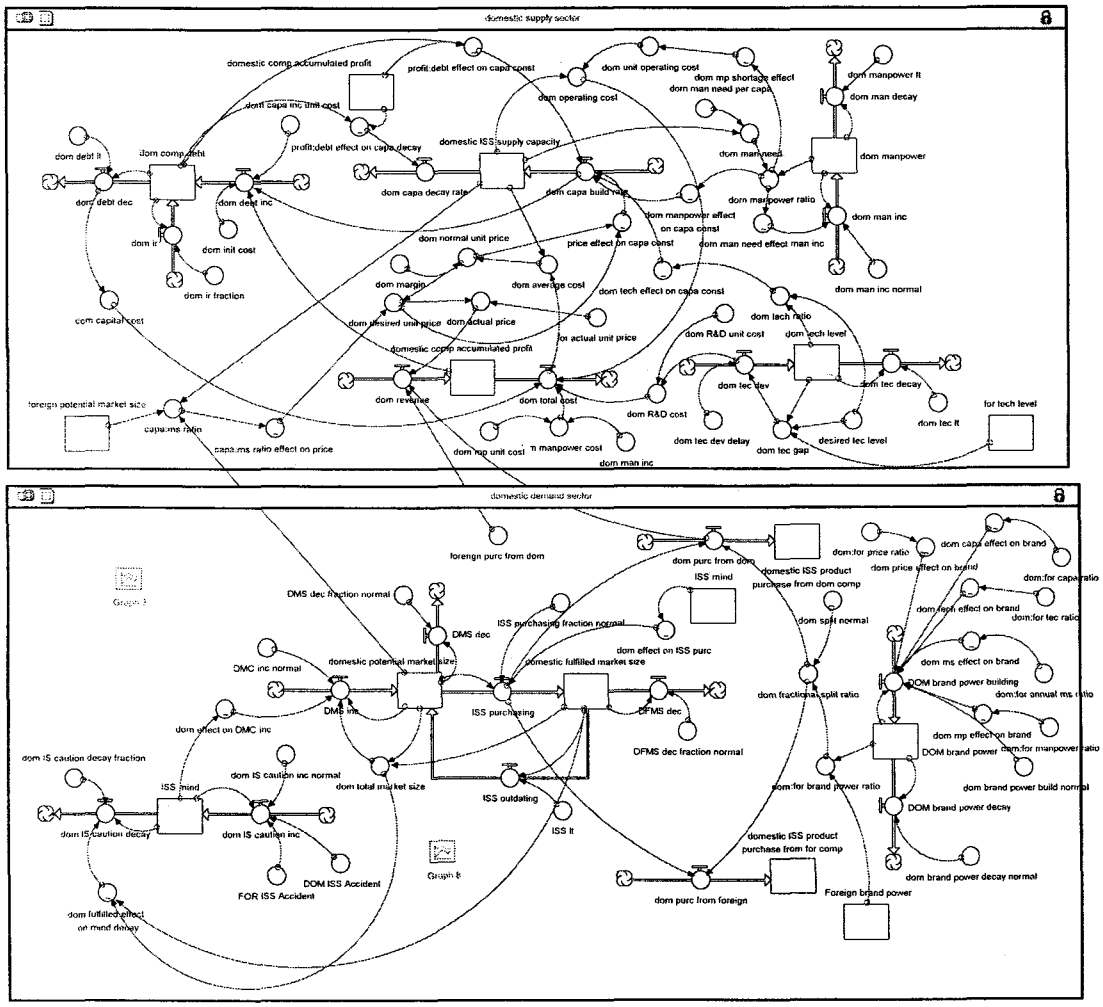
위에서 본 바와 같이 양의 피드백 루프가 음의 피드백 루프보다 상대적으로 많이 고려되고 있는 이유는 다음과 같다. 즉, ①핵심적인 주요 인과관계 위주로 표현이 되었다는 측면과, ②이 인과지도는 국내/국외 부문중 한쪽만의 인과관계를 내포하고 있으며, 실제 모델링에서는 본 인과지도와 동일한 형태의 인과지도가 대칭적으로 추가되어, 상대적 매력도에 의해 전체시장에 대해 양측이 시장점유율 경쟁을 하게 된다는 점이 본 인과지도 작성의 의도이기 때문이다.

3. 정보보호 산업정책 시스템 모델링

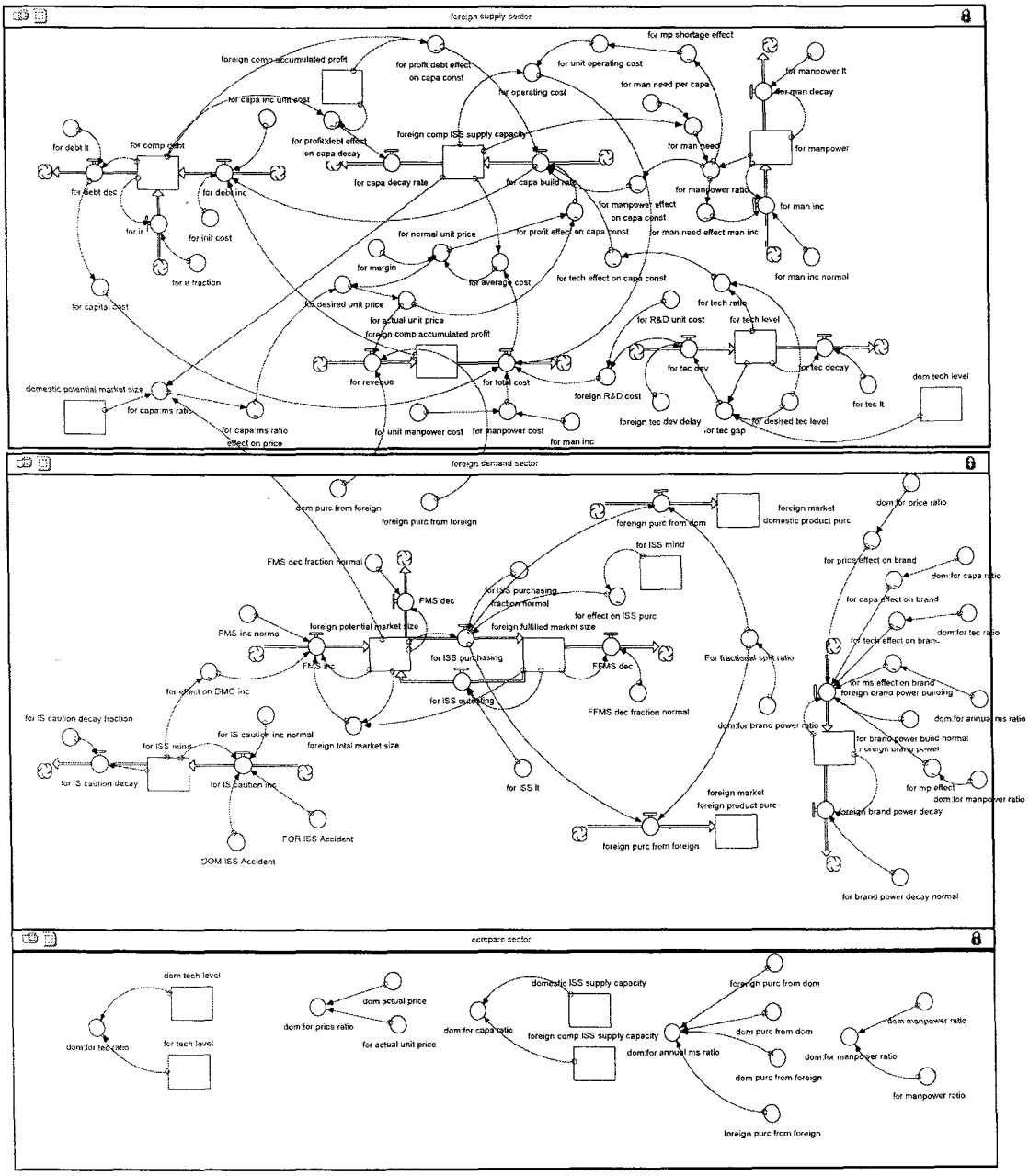
이상에서 핵심적인 인과관계 중심으로 작성된 인과지도를 보다 조작적/사실적 관점(Operational Perspective)에서 물질/정보의 흐름과 저장을 나타내는 Stock-Flow 다이어그램으로 변환하면 <그림 4, 5>와 같다.

전술한 바와 같이 본 모델은 직관에 기초한 단순모델로서, 각 변수에 입력된 자료는 정확한 현실자료가 아닌, 직관에 기초한 상대적 자료이다. 그러나, 직관적/상대적 자료를 사용해서도 시스템의 상대적 결과 행태를 살핌으로써, 주요정책의 효과를 비교평가할 수 있다. 또, 변환과정에서 인과지도에서는 포함하지 않았던 자본비용부문이 추가되어졌다. 국내 부문

에 대한 상세한 Stock-Flow Diagram은 다음 <그림 4>와 같고, 국외 부문 섹터와 비교 섹터에 대한 Stock-Flow Diagram은 <그림 5>에 나타나 있다. 또, 각 변수별로 입력된 수식과 자료값은 부록에 나타난 바와 같다. 국외 부문은 국내부문과 대칭을 이루고 있으므로 형태는 유사하다. 다만 입력되어진 수식과 데이터에서 차이를 보인다. 현재 국내외 양쪽에 대해서 이용가능한 자료는 국내외 시장현황과 예측자료뿐이고, 이로부터 국내의 시장규모가 대략 세계시장의 1% 내외인 점을 감안하여 초기값을 설정하였다. 그리고 비교섹터는 국내부문과 국외부문의 주요 비교지표를 비교하여 상대적 매력도를 산출하는 기초자료로 활용된다.



<그림 4> 정보보호 산업시스템 국내 부문 Stock-Flow Diagram



<그림 5> 정보보호 산업시스템 국외 및 비교 부문 Stock-Flow Diagram

IV. 정책대안별 시뮬레이션 결과 및 함의

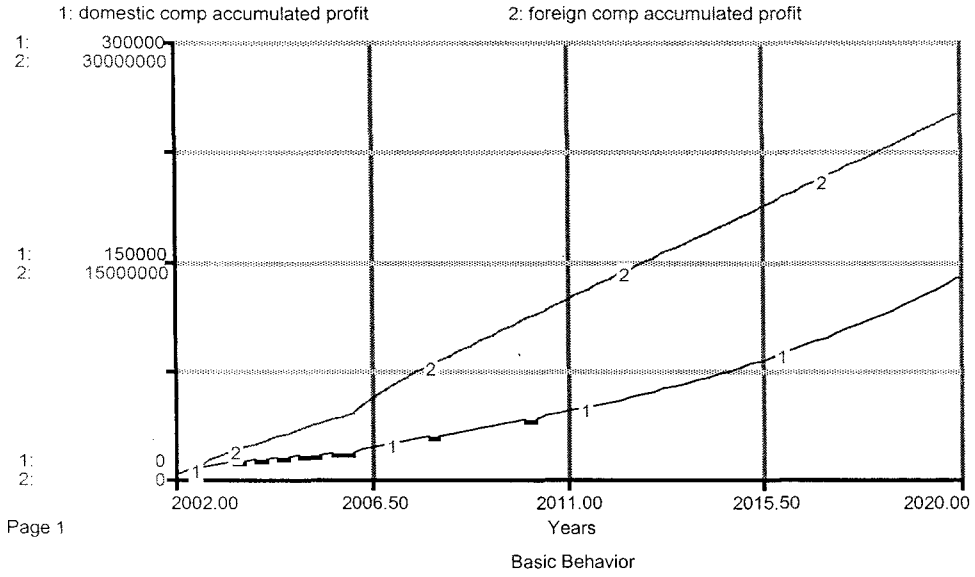
이상에서 구축된 단순 모형을 사용하여 주요 정책의 효과를 비교해보면 다음과 같다. 단, 전술한 [동태적 가정4]에 의해, 정보보호 시장규모는 빈번한 정보침해에 의해 증대되는 것으로 설정하였다. 동일한 규모의 정보침해가 지속적으로 발생하는 경우에 있어서, 각 정책에 대한 국내외 정보보호 업체의 수익규모나, 국내수요자가 국내에서 구매하는 규모와 해외에서 구매하는 규모를 비교함으로써, 정책효과성을 상대적으로 비교하였다.

시뮬레이션 분석에 있어서, 일차적으로는 아무런 정책개입이 없는 경우를 준거로 삼는 경우가 일반적이다. 따라서, 본 연구에서도 ①정책개입이 없는 경우, ②기술개발 정책이 실시된 경우, ③인력양성 정책이 실시된 경우, ④해외진출 직접지원책으로서의 상표인지도 고양정책이 실시된 경우로 대별하여 결과를 살펴보았다.

1. 정책개입이 없는 경우의 시뮬레이션

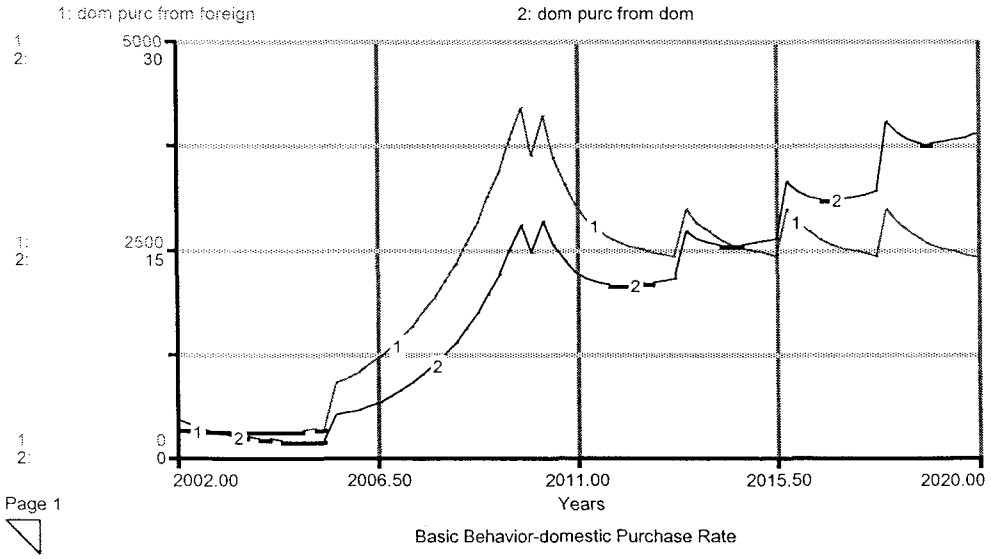
기본 모델에 2004년 이후부터 정보침해가 빈번히 발생하도록 설정한 경우의 누적 수익(총매출액 - 총비용)의 변화 행태가 다음 <그림 6>에 나타나 있다. 그래프에서, 1번 선이 국내업체의 누적 수익을, 2번 선이 외국업체의 누적 수익을 표시하고 있다. 주목할 점은 기본 모델에서 초기 국내시장/생산규모가 해외시장/생산규모의 1%정도로 설정되어 있으므로, 국내업체의 수익규모도 지속적으로 외국업체의 1%내외로 유지되고 있다는 점이다. 그러나, 수익의 성장세는 국내업체가 외국업체보다 상당히 완만한 형태를 보이고 있다. 이는 기술수준이 낮은 우리업체가 필요한 기술을 획득하기까지는 일정기간의 시간지연이 개입되기 때문인 것으로 풀이된다.

다음 <그림 7>은 국내 수요자가 국내업체와 해외업체로부터 구매하는 물량규모를, 그리고 <그림 8>은 해외 수요자가 국내업체와 해외업체로부터 구매하는 규모를 각각 나타내고 있다. 특기할 점은 정책적 개입이 없는 경우에 국내수요자가 국내외 공급자로부터 구매하는 비율은 시장상황에 비례해서 유동적으로 변화하는데, 국내공급자로부터의 구매비율이 해외로부터의 구매비율에 비해 아주 작다는 것이다(1% 미만). 다만, 2014년경 이후에 국내로부터 구매하는 비율이 약간의 증가추세를 보인다. 이는, 국내업체들의 자체적인 기술개발, 상표인지도 확산 등에 의해 나타나는 효과로 볼 수 있겠다. 반대로 해외공급자로부터의 구매비율은 증가나 감소추세 없이 일정한 비율을 유지하는 것으로 나타나 있다. 또, 이러한 현상은 외국 수요자의 구매 비율 행태에서도 비슷하게 나타나고 있다. 즉, 국내업체가 외국 수요자에게 판매하는 비율도 2010년경부터 상승세를 보이고 있다. 물론 절대규모는 외국공급자에 비해 여전히 1% 미만의 열세를 보이고 있다.



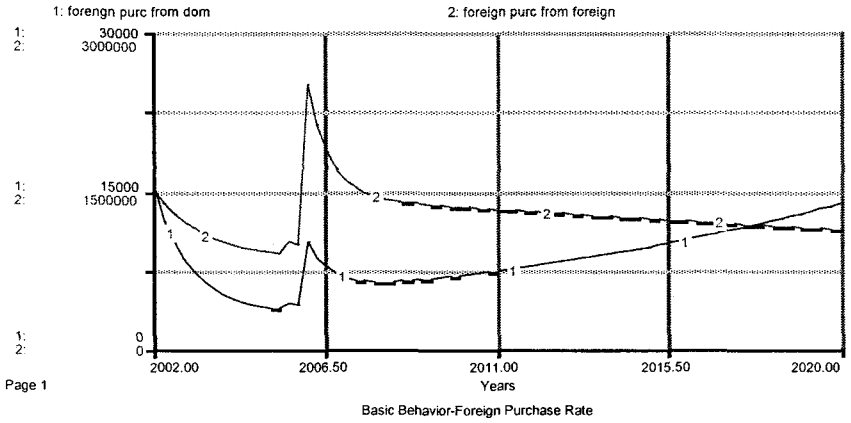
[범례] 선1 : 국내업체의 누적 수익 추이 / 선2 : 국외업체의 누적 수익 추이

<그림 6> 정책개입이 없는 경우의 국내/해외 기업의 누적 수익 추이



[범례] 선1 : 국내수요자가 국내 공급자로부터 연간 구매하는 비율 추이
선2 : 국내수요자가 외국 공급자로부터 연간 구매하는 비율 추이

<그림 7> 국내 수요자의 국/내외 공급자로부터의 구매행태 변화

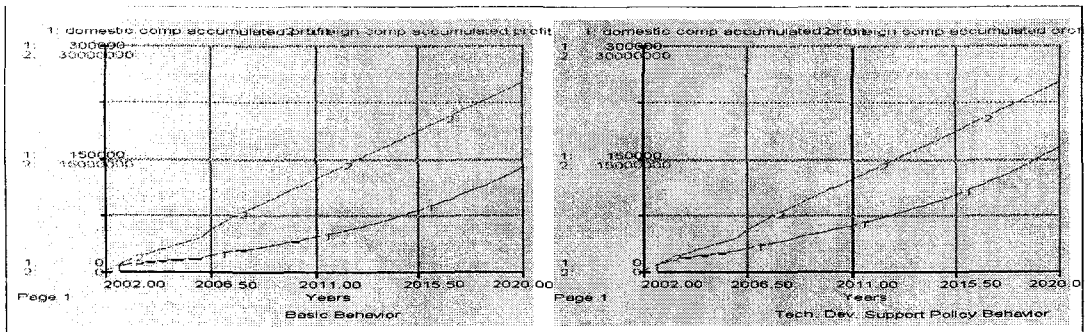


[범례] 선1 : 외국수요자가 국내 공급자로부터 연간 구매하는 비율 추이
선2 : 외국수요자가 외국 공급자로부터 연간 구매하는 비율 추이

<그림 8> 외국수요자의 국내외 공급자로부터의 구매행태 변화

2. 기술개발 지원정책을 실시한 경우의 시뮬레이션

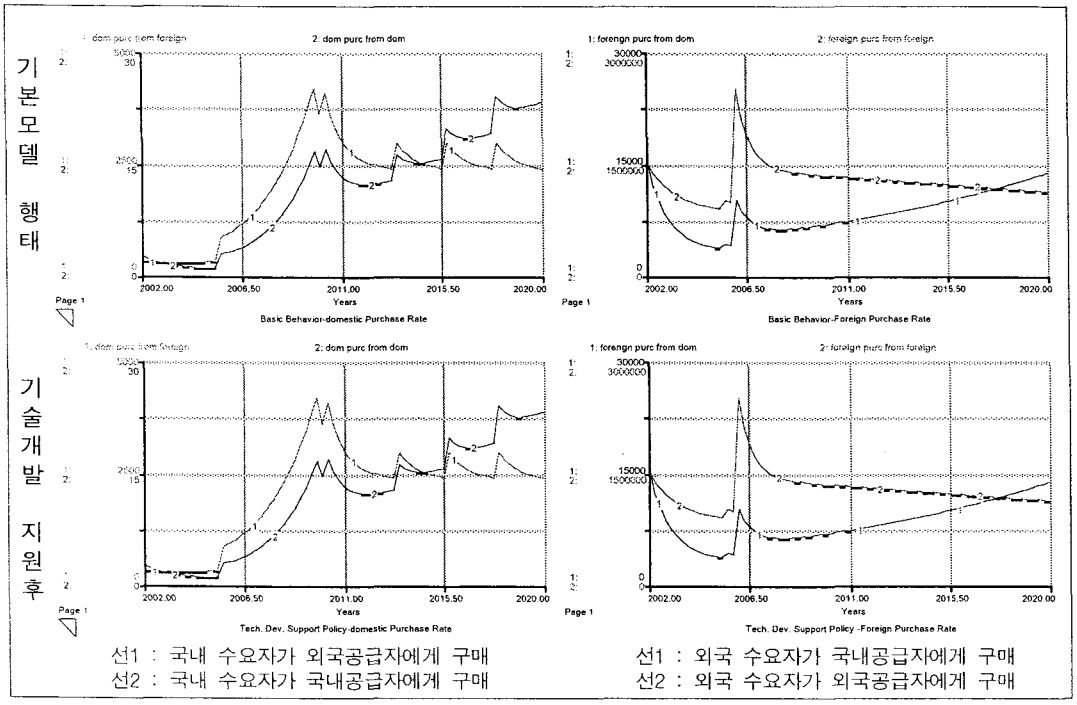
수요증대로 생산용량 증대의 필요성이 발생했을 경우, 이에 소요되는 기술개발 비용의 90%를 정부가 직·간접적으로 지원하는 경우에 대한 시뮬레이션 결과가 아래 <그림 9>에 나타나 있다. 이 경우, 외국업체의 누적수익 추이는 큰 변화가 없는 반면에, 국내업체의 누적수익 증가세가 약간 강화되었음을 볼 수 있다. 그러나, 국내 수요자의 국내외 공급자로부터의 구매 비율이나, 외국 수요자의 국내외 공급자로부터의 구매비율 행태에는 큰 영향을 주지 않는다는 것을 <그림 10>으로부터 알 수 있다. 이러한 현상은 외국 주요업체의 경우는 자체적으로 지속적인 기술개발 노력을 투입하고 있기 때문에, 국내업체의 기술개발이 실제 소비자의 구매정도에는 아주 미미한 변화를 가져온 결과로 풀이된다.



기술개발 지원정책 실시전 기술개발 지원정책 실시후

[범례] 선1 : 국내업체의 누적 수익 / 선2 : 외국업체의 누적 수익

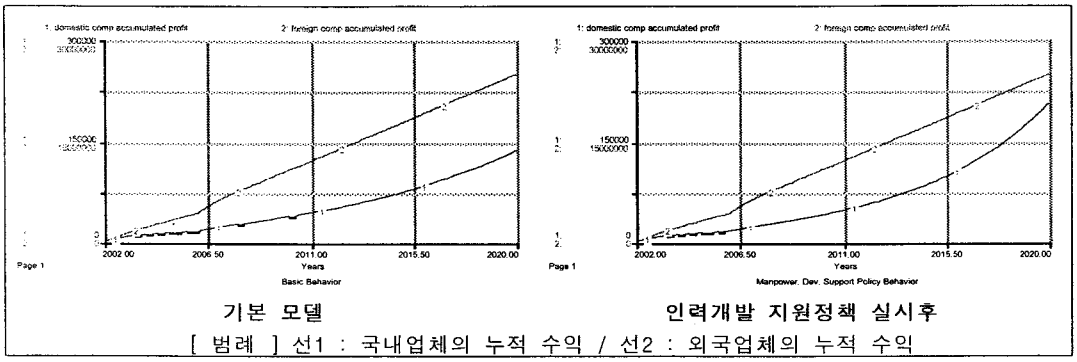
<그림 9> 기술개발 지원정책 실시전후의 국내외 업체의 누적수익 변화



<그림 10> 기술개발 지원정책 실시전후의 국내외 수요자 구매행태 변화

3. 인력양성 지원정책을 실시한 경우의 시뮬레이션

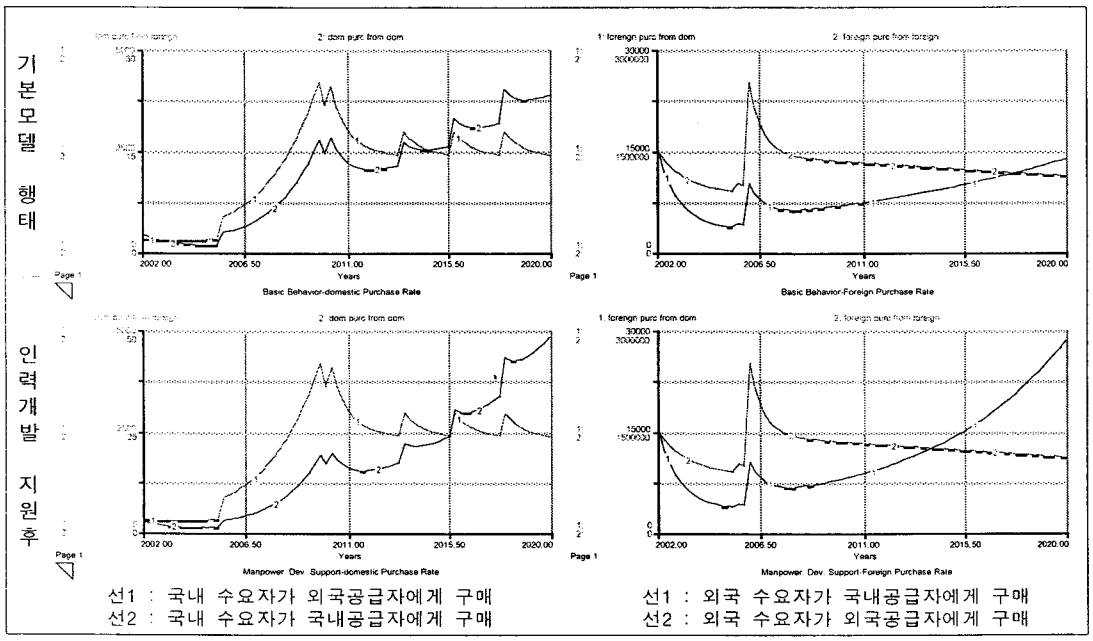
정보보호 분야의 소요 인력 양성을 정부가 지원하는 정책(소요되는 비용의 90% 정도를 정부가 부담; 기술인력 및 마케팅 인력등을 포함하여 양성)을 실시하는 경우, 일정기간의 시간지연후에 상당한 효과를 발생시키는 것으로 나타난다(<그림 11, 12> 참조). 이러한 현상은 인력양성은 기본적으로 5~10년의 시간을 필요로 하기 때문인 것으로 풀이된다. 특기할 점은 국내외에 대한 국내업체의 판매량이 절대규모 측면에서는 여전히 해외업체보다 상당히 뒤지지만, 증가세가 두드러지게 향상된다는 것이다. 이 결과는 정보보호 기술개발이나, 국내외 시장 개척에서 전문인력의 중요성을 보여주고 있다. 현재, 진행중에 있는 대학의 정보보호 센터 지원사업과, 계획중인 해외유학 지원사업이 기술인력 양성 프로그램에 해당된다. 이와 병행하여 정보보호 산업의 해외진출을 현장에서 직접 수행할 전문 마케팅 인력의 확보도 인력양성 지원정책에 포함된다고 하겠다.



기본 모델 인력개발 지원정책 실시후

[범례] 선1 : 국내업체의 누적 수익 / 선2 : 외국업체의 누적 수익

<그림 11> 인력개발 지원정책 실시전후의 국내외 업체의 누적수익 변화



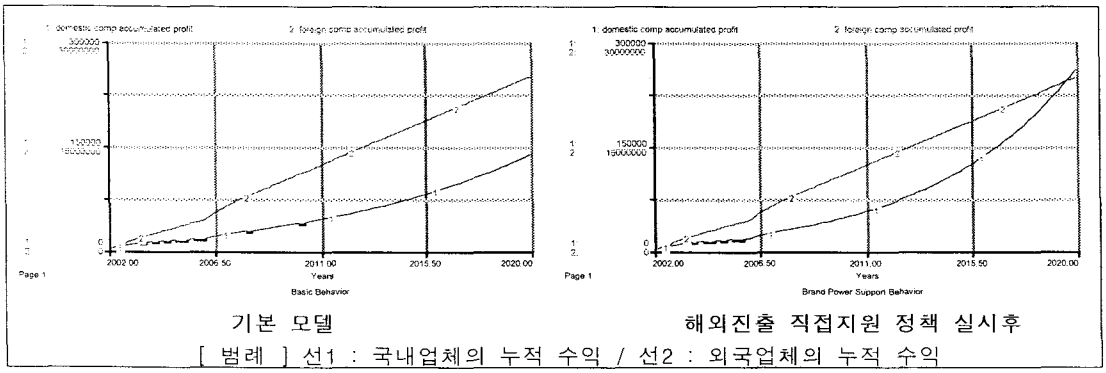
선1 : 국내 수요자가 외국공급자에게 구매
선2 : 국내 수요자가 국내공급자에게 구매

선1 : 외국 수요자가 국내공급자에게 구매
선2 : 외국 수요자가 외국공급자에게 구매

<그림 12> 인력개발 지원정책 실시전후의 국내외 수요자 구매행태 변화

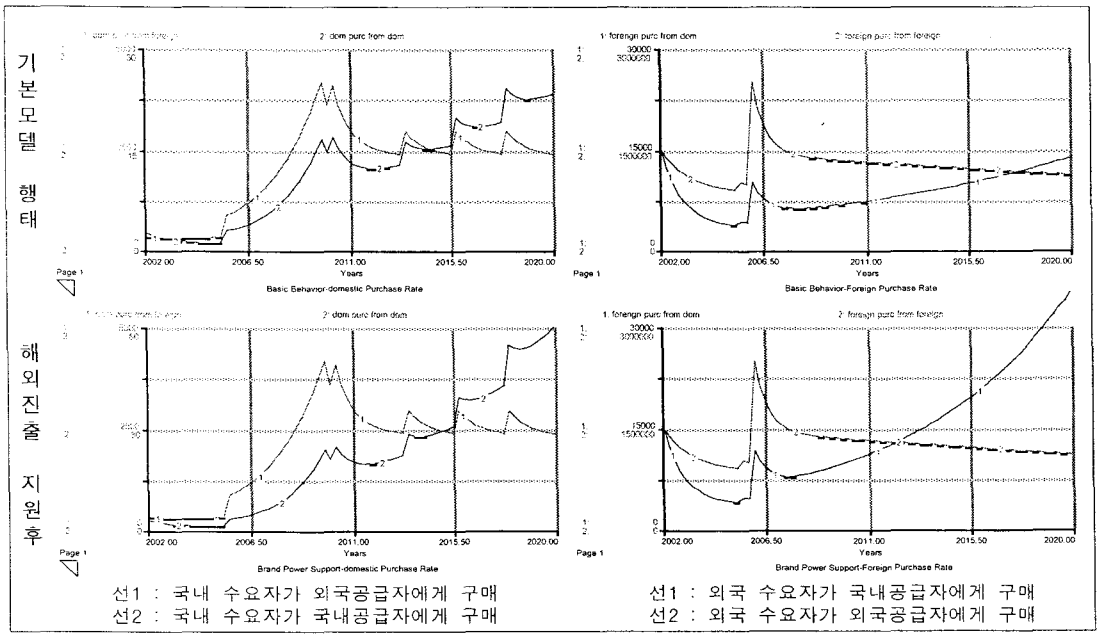
4. 해외진출 직접지원 정책을 실시한 경우의 시뮬레이션

본 시뮬레이션에서 해외진출 직접지원 정책은 해외 시장개척을 위한 국가차원의 모든 지원을 포괄하는 개념이다. 이에는 국가간 협력체제 구축, 우리 정부와 해외 시장관련 민간기관과의 협력체제 구축, 우리 민간단체와 현지 민간단체간의 교류지원 등 거시적 정책과, 해외 i-Park을 통한 지원, 해외 판매채널 형성 지원, 해외 전시회 지원등 미시적 정책등이 있다.



<그림 13> 해외진출 지원정책 실시전후의 국내외 업체의 누적수익 변화

이러한 해외진출 직접지원 정책을 실시했을 경우의 시뮬레이션 결과는 <그림 13, 14>와 같다. 정책의 효과측면에서 기술개발지원 정책이나 인력개발 지원정책보다 빠른 수익상승 및 판매상승을 가져오는 것으로 나타나고 있다. 이는 기술개발지원이나 인력개발지원이 상대적으로 간접지원 정책이고, 지원과 효과사이에 상대적으로 많은 시간지연이 개입되는 반면에, 직접지원정책은 단위 지원노력당 효과가 상대적으로 빠르고 크게 나타나기 때문인 것으로 해석된다. 그러나, 해외진출 직접지원정책도 우리 업체의 상표인지도가 향상되어야 하고, 현지 채널형성이 공고히 되어야만 본 궤도에 진입한다는 특성으로 인해 일정기간의 시간지연 이후에 효과가 나타나는 것을 볼 수 있다.



<그림 14> 해외진출 직접 지원정책 실시전후의 국내외 수요자 구매행태 변화

5. 시뮬레이션 결과의 정책적 함의

정보보호 산업분야는 수요시장이 제품과 서비스로 양분되어진다. 이들 중 현재시점에서 국내시장은 90%이상, 해외시장은 60%정도가 제품(하드웨어)시장으로 구성되어져 있다. 이에 더하여 정보보호 시장은 일단 제품이 공급되면 일정기간 동안(공급된 제품의 유효기간 동안)은 공급된 제품에 의해 시장이 축소되어진다는 특성을 가지고 있다[10]. 이러한 현상은 서비스 부문에서도 서비스 계약기간동안 동일하게 나타난다. 이에 반하여, 새로운 정보침해 기법이나 바이러스가 정보시스템을 심각하게 손상시키는 충격이 빈발할수록 잠재시장의 규모는 커진다는 특성을 가지고 있다. 종합해보면, 단기적으로는 시장규모가 일정하고 제품/서비스 공급에 의해 잔여시장의 크기는 축소되지만, 중장기적으로는 전체시장의 규모가 정보화의 진전과 정보침해의 증가로 인해 지속적으로 확산된다. 따라서, 본 연구에서는 이와 같은 특성의 시장 및 산업시스템의 중장기적 동태 분석에 적합한 분석틀인 시스템 다이내믹스 기법이 활용되어졌다.

이상의 주요 정책 시뮬레이션 결과들을 종합해 보면, 시뮬레이션에서 고려한 세가지 정책(기술개발 지원, 인력양성 지원, 해외진출 직접지원)이 모두 필요하다고 할 수 있다. 기술개발 지원정책은 선진국들에 비해 열세에 있는 정보보호 분야의 기술을 지속적으로 축적해야 한다는 당위성과, 기술축적에 의한 장기적 경쟁력 확보의 필요성을 확인시켜 주었다. 인력양성 정책 분야에서는 현재 실시중인 기술개발 인력위주의 양성에 더하여 해외시장 개척에 직접적으로 투입될 마케팅 인력양성까지 이루어져야 한다는 점을 유추할 수 있었다. 마지막으로 직접적인 해외진출 직접지원정책이 나머지 두 정책보다 직접적인 효과가 높게 나타나는 것으로 분석되었다.

그러나, 본 연구에서 개발된 시뮬레이션 모델은 상당히 단순화/통합화 되어 있으므로 개략적인 정책효과성만을 확인할 수 있다는 한계점을 가지고 있다. 이러한 한계에도 불구하고, 시스템 구조분석과 시뮬레이션 과정에서 파악된 정책적 시사점을 재정리하면 다음과 같다.

일차적으로는, 해외진출 직접지원 정책의 중요성을 확인하였다. 그러나, 정책의 중요성만을 확인하였을 뿐이고, 세부적인 정책개발은 지속적인 연구과제로 남게 되었다. 특히, 본 시뮬레이션 결과와 마찬가지의 정책효과를 발휘하기 위해서는 해외진출 지원정책중에서 해외시장에서 우리 업체의 상표인지도나 신뢰도를 신속하게 제고할 수 있는 정책이 집중적으로 추진되어야만 한다. 이러한 정책대안 설계시에 참고할 수 있는 사례로는 현재 몇몇 국내 선도업체의 외국시장 진출시 성공요인을 살펴볼 수 있겠다. 즉, 이들 성공업체들은 탄탄한 기술력을 바탕으로 하고 있으면서, 동시에 해외 진출시에 철저한 현지화 및 현지의 유수업체와 제휴하여 강력한 마케팅 채널구축을 통해 초기 Brand Power의 열세를 극복하고 있다. 따라서, 정부에서는 현재 전세계 주요국에 설치되어 있는 i-Park의 기능과 용량을 보다 강화함으로써, 국내업체의 신속한 해외진출에 실질적인 전초기지로서의 역할을 수행하도록 해야 할 것이다[11].

---

10) 예를 들어, 한 회사가 백신을 구입한다면, 일정기간동안은 추가로 백신을 구매하지는 않는다는 것이다. 이러한 현상은 백신과 같은 SW제품보다는 Firewall과 같은 HW 제품의 경우에서 더욱 강하게 나타난다.

11) 정보보호 산업보다 약간 앞서 해외진출을 시도하여 성공사례를 만들어내고 있는 소프트웨어 산업분야에서도

두 번째로 효과가 높은 인력개발 정책도 이와 같은 효과를 발휘하기 위해서는 기술, 연구개발 인력에 더해서 마케팅 인력의 양성까지도 포괄적으로 이루어져야 한다. 특히, 각 국가별로 현지문화와 시장상황을 정확히 알고 있으면서 동시에 국제무역에 대한 지식을 갖춘 마케팅 인력양성이 필요하다. 현재 국내 정보보호 업체의 영세한 상황을 감안한다면, i-Park에 이 역할을 전담해서 수행할 인력의 보강을 고려해 볼 수 있겠다. 또 이 업무 담당인력의 현장경험과 지식을 지속적으로 국내 업체에 보고할 수 있는 시스템 구축도 추진되어야 하겠다.

마지막으로 기술개발 지원정책도 지속적으로 진행되어야 하겠다. 정보보호분야의 세계적인 기술수준과 우리 업체의 기술수준 격차가 상당한 것으로 분석되고 있고, 이에 더하여 우리업체들의 영세성으로 인해 기술개발 투자능력이 추약하기 때문이다. 단, 기술개발의 방향설정에 있어서, 단기적인 효과를 발생시키는 상용화 기술개발과 장기적 관점의 원천기술 개발이 병행되어야만 우리업체들이 해외진출을 지속적으로 실현시킬 수 있다 하겠다. 해외진출의 성패 관건은 상표인지도의 지속적인 제고이고, 이를 위해서는 기술적 뒷받침이 필수적이기 때문이다.

이상의 시뮬레이션 결과에 더하여, 정부가 고려할 수 있는 지원정책으로는 국내시장의 확장정책이 있을 수 있다. 시뮬레이션을 수행하지는 않았지만, 모델 구축시에 필수적으로 업체들의 비용부분을 고려하게 되는데, 시장규모가 클수록 단위당 소요비용이 감소하게 되는 것은 주지의 사실이다. 특히 소프트웨어가 많이 포함될수록 단위당 소요비용은 급격히 감소한다. 그러므로, 국내시장규모의 확장은 업체들의 경쟁력 제고에 직접적인 기여를 하게 된다. 뿐만아니라, 국내업체의 해외진출은 필연적으로 외국업체나 기관과의 협력을 필요로 하는데, 내수시장 규모의 확장은 이들과의 협상력을 증대시키는 효과를 가져온다는 점도 간과할 수 없겠다.

본 장의 정보보호 산업 육성 정책 시스템 시뮬레이션 분석을 통해, 결론적으로 재확인한 사실은 정부의 주요 정책 대안중에서 해외진출 직접지원 정책의 중요성이다. 지금까지 정부정책의 핵심은 기술개발 지원에 주로 초점이 주어져 있었고, 인력개발 지원과 해외진출 지원쪽은 상대적으로 미약한 지원의 초기단계이었다. 이러한 사실은 정부가 직접적인 지원책을 제시하기 어려운 부분에도 기인하고 있지만, 정책효과에 대한 회의적 시각에도 어느정도 그 원인이 있다고 하겠다. 따라서, 본 연구를 출발점으로 하여 보다 구체적이고 효과적인 해외진출 지원정책 대안이 지속적으로 발굴되고 실현되어야 할 것이다.

V. 결론

본 연구에서는 현재 태동기에 있는 국내 정보보호 산업을 정부차원에서 육성하기 위해 시도 혹은 계획되고 있는 주요 정책대안의 상대적 효과를 시스템 다이내믹스 방법으로 분석하

대부분의 성공업체들은 "강력한 현지 마케팅 채널 확보"와 "마케팅 인력 현지 채용"에 상당한 투자를 한 것으로 나타나고 있다(한국소프트웨어진흥원 외, 2001)

였다. 전 세계적으로도 정보보호 산업이 독자적인 산업영역으로 등장한 시기가 최근이므로 시뮬레이션 모델에 필요한 충분한 자료가 부족한 것이 현실이다. 또, 정보보호 산업은 그 특성상 등장시점부터 국내외 시장의 경계가 큰 의미를 갖지 못하고 있으므로, 국내외 시장과 기업을 포괄적으로 고려하는 것이 타당하였다. 이와 같은 한계로 인해, 본 연구에서는 국내외 기업과 시장에 대해 상당한 수준으로 통합되어지고 추상화된 형태의 모델링만이 이루어졌다.

시뮬레이션 결과 해외진출 직접지원정책의 효과성이 가장 크고, 다음으로 인력양성 지원정책과 기술개발정책의 효과가 순차적으로 효과가 크다는 것을 알 수 있었다. 이러한 결과는 해외진출 직접지원정책이 가장 시장에 가까운 정책이고, 정책시행과 효과발현간의 지연이 가장 짧기 때문인 것으로 풀이된다. 인력양성 지원정책의 경우 5년에서 10년의 시간지연이 개입되고, 기술개발지원정책의 경우는 지연시간은 이와 비슷하거나 약간 짧지만, 선진 주요사업자도 지속적으로 기술개발을 수행함으로써 상대적인 효과가 약하게 나타나기 때문인 것으로 풀이된다. 그러나, 정책 효과성의 상대적 비교를 정확히 수행하기 위해서는 각 정책에 소요되는 비용과 효과를 함께 고려하는 것이 필수적이지만, 현재 정책당국의 투입비용자료는 기술개발에 대해서만 나타나 있으므로 비교가 불가능하였다. 또, 세가지 주요정책의 효과성을 비교한다 할지라도 이 정책들이 상호 배타적이기 보다는 상보적인 관계에 있으므로 지속적인 실행이 필요하다. 다만, 해외진출 직접지원정책은 단기적으로 효과를 발현하고, 반면에 인력개발과 기술개발 지원정책은 중장기적은 관점에서 지속적으로 추진해야 한다는 점을 재확인할 수 있었다.

전술한 바와 같이, 본 연구에서는 상당한 수준으로 통합화되고, 추상화된 모델을 구축하였고 이를 통해 분석이 이루어졌으므로 정책당국에서 실효성있게 활용하기에는 역부족이다. 따라서, 본 연구에서 구축된 모델을 출발점으로 하여, 지속적인 현장자료 조사와 관련 문헌자료 보강을 통해 모델을 보다 세분화해 나가야만 할 것이다. 즉, 인터넷 이용자수, 인터넷 이용형태(정보침해에 피해가 큰 전자상거래, 인터넷결재 등의 이용여부) 등 정보보호 산업 이용환경 세분화, 정보보호 제품 및 서비스별 세분화, 전세계 지역별 정보보호 수요특성 세분화 등을 통해 정보보호 산업 분야별, 진출대상지역별 정책대안 분석 모델로 다양하게 추가적인 연구가 시도되어야 할 것으로 사료된다.

참고 문헌

길민정. 2001.「2001 상반기 국내 정보보호 시장현황」한국정보보호진흥원

김도훈 · 문태훈 · 김동환. 1999. 「시스템 다이내믹스」서울:대영문화사

김은환 · 박번순 외. 2000. 「뉴 밀레니엄의 의미와 과제」삼성경제연구소

경찰청 사이버테러 대응센터. 2003. 범죄통계 - 유형별 발생 현황

남택용. 2002. 차세대 네트워크 보안 구조.「ICAT 2002 발표논문집」

손승원. 2000. Active Security 기술 발전 방향.「Sigcomm Review」제1권 1호

장성원 · 이승준 · 김종현. 2003. 「인터넷 강국의 취약성과 대응과제」 삼성경제연구소 CEO Information 386호

전재호 · 최용환. 2002. 국내 정보시스템 보호현황 분석과 정책적 함의. 「충북개발연구」 제13권 1호: 79-101

전재호 · 윤상흠 · 김현종. 2000. 「국내 정보보호 산업현황 및 발전전략」 한국전자통신연구원

전재호 · 윤상흠 · 홍민기 · 최남희 외. 2002. 「정보보호 산업역량 분석 및 향상방안 연구」 한국전자통신연구원

정보통신부. 2001. 「정보보호 기술개발 5개년 계획」

_____. 2002. 「중장기 정보보호 기본계획」

한국정보보호진흥원. 2001. 「국내외 정보보호 산업동향 및 통계조사」

한국전자통신연구원. 2000. 「정보보호시스템 기술/시장 보고서」

_____. 2002. 「정보보호시스템 기술/시장 보고서」

황성원. 2002. 2001년 정보화역기능 실태조사. 한국정보보호진흥원 정보보호뉴스

CERTCC-KR. 2002. CERTCC-KR 통계

Gartner Group. 2002. 「정보보호전문기업 편람」

KISA · KISIA. 2001. 「국내 정보보호산업 실태조사」

KRNIC. 2001. 「OECD회원국의 정보통신 현황 비교 보고서」

Briney, A. 2001. 「2001 Information Security Industry Survey」 Information Security

High Performance Systems, Inc. 2001. 「An introduction to system thinking」

Hughes, K. 1995. 「From Webspace to Cyberspace」 Enterprise Integration Technologies

Lyneis, James M. 1998. System dynamics in business forecasting: a case study of the commercial jet aircraft industry. *Proceedings of the 1998 International System Dynamics Conference.* Quebec, Canada.

Lyneis, James M. 1999. System dynamics for business strategy: a phased approach. *System Dynamics Review* 15(1): 37-90.

Stallings, W. 2000. 「Network Security Essentials: Applications and Standards」 New Jersey: Prentice-Hall