

# 웹기반 하에서 정보보호를 고려한 컴퓨터 게임 정책에 관한 연구

이명숙\*, 신승중\*, 류대현\*

\*한세대학교 컴퓨터공학과

e-mail : samgak4@lycos.co.kr

## A Study on Computer Game Policy Considering Information Security in Web System Environment

Myeong-Suk Lee\*, Seung-Jung Shin\*, Dae-Hyun Ryu\*

\*Dept of Computer Science, Hansei University

### 요 약

컴퓨터 게임은 정보화의 진전, IT기술의 발전과 더불어 그 파급 속도와 사회적 영향력이 가중되고 있으며, 그 특성으로 인한 프라이버시 침해, 해킹 등 정보화의 역기능이 심각해지고 있다. 이 같은 다양한 정보화의 역기능은 u-society에 대한 새로운 도전으로 작용하고 있어 새로운 위협이 상존하는 유티쿼터스 환경 하에서 안심하고 u-IT 혜택을 누릴 수 있도록 하기 위해 보다 심층적인 정보보호 정책 마련이 필요하다. 본 연구는 전문가들의 의견을 수렴하여 정보보호 정책이 정보지수에 미치는 영향을 분석, 도출된 결과를 바탕으로 기업이나 국가에서 정보보호 관련 정책 수립 시 적용할 수 있게 함으로써 국내 정보보호에 대한 수준을 보다 향상시키고자 한다.

### I. 서론

한국의 보안 관련 예산은 경제 선진국의 정부보안투자 예산인 5-8%와 비교할 때 턱없이 낮다. 또한 대부분의 정부부처가 정확한 정보보호 예산 규모를 파악하지 못하고 있으며, 정보보안 담당관(CIO)<sup>1)</sup>에 대해서는 상당 부분이 최고정보관리책임자(CSO)<sup>2)</sup>가 겸직을 하고 있어 실질적인 정보보호 활동은 미약한 실정이다.

2003년 발생한 1·25 인터넷 대란을 계기로 출범한 국가사이버안전센터(NCSC)<sup>3)</sup>를 중심으로 중앙부처 및 주요 기관의 보안 정책은 체계를 잡고 강화기조를 띠고 있으나 해커의 공격이나 사이버 보안 사고에 대해 기관별 긴밀한 역할분담 및 공조체계는 여전히 취약한 관계로 전자정부 1등 국가라는 명성에 비해 보안 수준은 낙후되어 있다. 더군다나 2006년 정부 통합 전산센터가 공식 가동되면서 센터 통합에 따른 인적, 물리적 보안사고 발생 가능성이 커진데다 application과 system의 분리 운영으로 인한 대형 사고 발생 시 신속한 원인분석과 대처가 어려운 만큼 공조체계가 절실하게 요구되고 있다.

본 연구는 국내 정보보호 발전을 위해 정책적으로 지원해야 할 방향제시를 위해 항목을 정의하고, 정보보호 정책

수립에 있어 필요한 부분에 대한 설문을 통해 각 조직의 정보보호 관리 현황에 대한 자료의 수집·분석을 통해 업종이나 경력 등의 세부항목에 따라 정보보호에 미치는 영향을 분석하였다.

### II. 연구 배경

#### 1. 국내 게임 산업의 규모와 동향

게임 산업은 미래 성장 동력으로 빠르게 부상하고 있는 문화산업 중에서도 최근 몇 년 동안 급격한 성장으로 가장 주목받고 있는 분야이다.

[표 1] 국내 게임시장 규모

구분	매출액(억 원)	점유율(%)
온라인게임	22,403	43.5
모바일게임	2,518	4.9
비디오게임	4,201	8.2
PC게임	350	0.7
아케이드게임	352	0.7
PC방	20,801	40.4
아케이드게임장	518	1.0
비디오게임장	293	0.6
합계	51,436	100

매년 두 자리 성장률을 기록하면서 청소년의 전유물에서 여성과 중년층까지 소비층이 확대되고 있으며, [표 1]에서처럼 국내 게임 시장의 경우 온라인 게임과 PC방의 규모가 상대적으로 월등한 것을 볼 수 있으며, 오늘날 국

1) CIO : Chief Security Officer  
2) CSO : Chief Information Officer  
3) NCSC : National Cyber Security Center

내 게임시장이 세계에서 차지하는 비중은 온라인게임 세계 1위, 모바일 게임 세계 3위의 위상을 갖게 되었다. 온라인게임의 경우 2006년의 경우 수입액은 2조 7,900만 불, 수출액은 6조 7,700만 불에 달한다.

**2. 온라인게임 공격 현황**

온라인 게임이 성장한 만큼 그에 따른 문제들도 동반한다. 특히 온라인 게임의 공격 유형을 보면 크게 두 가지로, 서버 공격과 클라이언트 공격으로 나눌 수 있다.

서버 공격은 서버 해킹을 의미하는 것으로, 웜이나 Dos 공격, 패킷 리플라이 공격, 웹 사이트 취약점 공격 등, 악의적인 목적으로 서비스를 마비시키기 위해 서버 다운이나, 소스 코드 탈취 등의 경우가 이에 해당된다.

클라이언트 공격은 자신의 PC에 설치된 클라이언트 파일에 대한 변조나 스피드해킹 사용, 메모리 조작 등이 있다. 흔히 “해킹”이라는 용어가 이 클라이언트 해킹에 속한다.

[표 2] 온라인게임 공격 유형

구 분	서버 공격	클라이언트 공격
내용	게임소스 탈취	스피드 해킹
	Dos, 웜, 패킷 리플라이	매크로
	웹 사이트 취약점	메모리 변조, 파일 변조
	Non Client BOT	패킷 변조
		조준 핵(AimBot) 계정 해킹

**3. 정보화 역기능**

국내의 초고속 인터넷 가입자 수는 2007년 2월 기준으로 14,150,074명을 넘어서고 있으며, 초고속 인터넷의 가입자의 절반이 KT와 하나로 텔레콤의 서비스를 이용하고 있다.[13] 그 중 서비스의 절반 이상이 xDSL과 HFC기반의 서비스를 이용하고 있으며, 중계 유선방송 및 위성을 이용한 초고속 인터넷 서비스는 이용률이 가장 저조한 것으로 분석되었다.

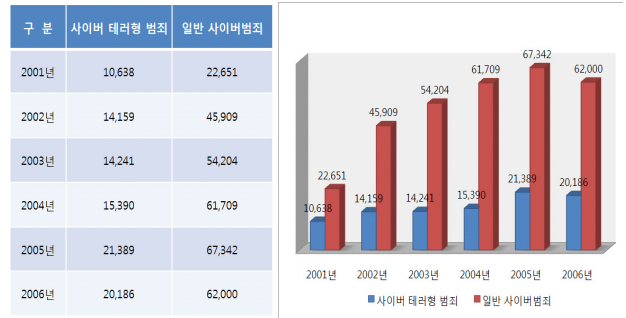
[표 3]과 같이 해킹이나 바이러스로 인한 피해는 지속적으로 update되는 각종 백신 프로그램으로 인해 다소 감소하고 있는 추세이나, 매일 접하고 있는 휴대전화나 이메일에 대한 스팸 메일에 대한 신고 및 상담건수는 계속해서 증가하고 있는 추세이다.[14]

[표 3] 정보화역기능 지수

구 분		년 도		
		2004년	2005년	2006년
해킹·바이러스 피해 및 경보 현황	해킹 피해건수	24,297	33,633	26,808
	바이러스 피해건수	107,99	16,093	7,789
	예·경보	37	1	0
	합 계	132,328	49,727	34,597
스팸메일 신고·상담현황	신 고	314,474	389,371	660,239
	상 담	11,854	7,671	47,940
	합 계	326,328	397,042	708,179
개인정보 침해신고 및 상담현황		17,569	18,206	23,333

[그림 1]에서 보면 사이버 범죄는 계속해서 증가하고 있는 추세이다.

최근 웹 2.0 서비스를 통해 개인 Blog, UDC 등은 인터넷이 가진 ‘개방, 참여, 공유’ 라는 특성과 맞물려 더욱 확산할 것으로 예상되지만 개인정보 및 사생활 노출 피해가 예상되며, 정보 저작권 분쟁, 왜곡된 정보 등 역기능도 증가할 것으로 보인다.



[그림 1] 사이버 및 일반 범죄관련 통계

정보의 전염병인 인포데믹스가 인터넷을 통해 확산되면서 인권이나 프라이버시 침해 및 정보의 왜곡 등으로 인해 사회적으로 문제시 되고 있는 실정이다.[14]

특히 인포데믹스는 국가 경제의 피해를 야기 시키며, 정보의 왜곡으로 인한 공포 분위기를 조성하고, 개인의 인권이나 프라이버시 침해 등을 발생시키고 있다. 따라서 정부나 기업 및 포털 사이트에서는 유해한 인포데믹스 확산에 대비한 ‘리스크 관리전략’을 계획 할 필요가 있다.

우리사회의 정보화에 대한 역기능지수를 종합적으로 분석해볼 때 첫째, 넘쳐나는 지식과 정보의 바다에서는 엄청난 양의 불건전 정보 또한 유통되고 있다. 음란물과 폭력물이 무차별적으로 유통되고 자살과 도박, 범죄를 부추기는 유해사이트가 셀 수 없을 정도로 많으며 스팸 메일이 남녀노소를 불문하고 너무 쉽게 배달되고 있다. 둘째, 급속한 정보화의 발전으로 개인정보가 너무 쉽게 노출되고 심지어 팔리기까지 하여 부당하게 이용되거나 범죄사건에 악용되기도 한다. 셋째, 타인의 권리나 재산에 대해 별다른 가해의식 없이 침해하는 일이 일상적으로 일어나고 있다. 넷째, 정보시스템에 대한 공격이나 악의적인 훼손은 개인적인 불편을 넘어 경제활동에 막대한 지장을 초래하기도 하고 엄청난 사회적 혼란을 불러일으킬 수도 있다. 다섯째, 인터넷과 정보통신 기술의 발전에 따라 감시와 통제에 대한 관심이 증대하면서 보편적인 인권에 대한 감수성이 현저히 떨어지고 있는 실정이다.

**III. 정보보호 정책 요구사항 항목과 수준 연구**

정보보호 정책 요구사항 항목은 정보보안의 여러 측면에 대해 기업과 국가의 정보보호 수준을 측정하며, 정보보호 전략 및 정책수립에 활용될 수 있다. 국내에서 연구된 정보화 지표의 경우와 같이 정보보호 정책 요구사항 항목

은 정보보호의 각 부문에 대해 수치화 된 자료를 이용하여 평가하고 이를 종합적으로 점수화하여 산출한 수치라고 할 수 있다.

기존의 연구에서 도출된 정보보호 정책 요구사항 항목과 계량화 방식을 정보보호 기반/환경 분야, 정보보호에 대한 인식/투자, 정보화의 역기능 등 3가지 관점에서 항목을 분류하고, 단순 가중치 법을 사용하여 정보보호 수준을 지수화 한다.

이와 같은 연구는 정보보호 자체의 완전성을 주목적으로 설계되어 있다. 이는 기업이나 국가의 관점에서 볼 때 정보보호 정책을 조직의 목적에 맞게 활용하려 할 때 정확한 정책 방향을 제공하는데 문제가 있다. 따라서 목적 지향적인 요구사항 항목의 개발이 필요하며 정보보호 역량을 정의하고, 이를 보다 정확하게 측정하여 조직의 정보보호 목적을 달성할 수 있도록 지표를 개발할 필요가 있다.

본 연구에서는 정보보호 정책의 요구사항을 개발하기 위해 3단계에 걸쳐 개발하였으며 각 단계별 수행내용은 다음과 같다. 우선 제 1단계에서는 정보보호 기반시설 및 환경을 파악하였다. 여기에서 기존의 관련 연구를 분석하여 포괄적인 항목 후보를 도출하였다. 2단계에서는 1단계에서 도출된 후보요소에 대해 소분류 항목을 나열하여 정보보호에 대한 인식과 투자에 대해 세부항목을 도출하였다. 또한 3단계에서는 600명에게 설문을 실시하였으며, 후보항목에 대한 파일럿 테스트를 통해 각 설문의 중요성, 상관관계 등에 대한 통계분석을 수행하였다. 이를 통해 바람직한 요구사항 후보항목을 제시하였다.

대분류 항목으로서 [표 4]에서처럼 정보보호 기반/환경 분야, 정보보호에 대한 인식/투자, 정보화의 역기능의 3가지 범주를 설정하였다. 정보보호 기반환경의 세부항목으로 정보보호 업무수행, 정보보호 전담직원 정보보호 제품 등으로 도출하였으며, 정보보호 인식/투자 항목은 국내 정보화 수준 및 정보보호 정책과 중요성에 대한 항목으로 도출하였으며 정보화 역기능 요소로 정보보안 침해에 등을 포함하였다.

[표 4] 정보보호 정책 요구사항 후보항목

정책 요구사항	주요내용	설문 항목수
게임 기반/환경	게임 개발 업무 수행	10
	게임개발 전담직원	
	게임 제품	
	게임마케팅정책유무	
	게임개발의 기업환경	
	게임 관리체계	
	네트워크 시스템 평가	
	게임개발 투자	
	게임개발 관련보안담당자 유무	
	게임개발 관련 부서	
게임담당자 보안업무수행		
게임개발	국내 게임개발 수준	9

인식/투자	게임 산업진흥 예산	
	게임 산업의 위협	
	게임 교육	
	국내 게임 정책	
	게임 발전방향	
	게임개발의 중요성	
	게임에 대한 시장성	
게임제품화 역기능	게임개발의 문제점	4
	음성시장조성	
	정보보안 침해	
	침해에 의한 복구경험	
	게임 데이터 소실	

최근 들어 강조되고 있는 게임정책에 대한 인식과 투자 및 역기능 등을 설문 항목으로 설정하여 전반적인 균형을 이루도록 구성하였다.

#### IV. 제안하는 정보보호 정책 요구사항

본 논문에서 전문가들의 의견을 분석한 결과 정보보호 정책을 위한 요구사항을 [표 5]로 정리하였다.

[표 5] 제안된 정보보호 정책을 위한 요구사항

대분류	중분류	정보보호 정책을 위한 요구사항
게임 기반/환경	게임개발 업무수행	1. 지적연구활동 주력 2. 다양한 개발업무 인원 보강 편성
	게임개발 전담직원	1. 개발전문인력 양성 2. 전문성 강화
	게임 제품	1. 최신개발 프로그램 사용 2. 시스템 보호를 위한 하드웨어 운용
	게임개발 투자	1. 정보보호를 위한 투자/지원 확대 2. 투자회사 연계 유지
게임개발 인식/투자	게임 교육	1. 전문인력 양성 및 전문성 강화 2. 투자회사 연계 유지
	게임 발전방향	1. 게임 산업 육성을 위한 지원책 마련 2. u-게임을 대비한 연구활동 강화 3. 게임 문화운동 확산
게임제품화 역기능	정보보안 침해	1. 프라이버시 침해방지를 위해 정부와 포털 사이트 차원의 관리활동 강화 2. 사이버 범죄에 공조수사 등 능동적인 대처 3. 게임의 역기능에 대한 교육활동 강화

우선 게임 정책의 실효성을 위해 게임 산업을 위한 정책적 지원과 투자 확대를 해야 할 것이다. 게임에 관한 정책은 지금까지 산발적으로 전개되어 왔으며, 급변하는 정보화 환경은 종합적이고 체계적인 정부의 정책적인 접근을 요구하고 있다.

특히 유비쿼터스 사회의 태동을 앞두고 향후 새로운 20년을 대비하는 출발점에 서있는 상황에서 미래 사회의 변화에 대해 미리 대비하는 준비활동이 반드시 필요하다. 다만, 정보기술이 네트워크화 되어가면서 정부의 중앙집권적인 권한 강화 및 정보보호체계의 일원적인 운영과 관리는 신중하게 고려되어야 할 것이다. 과거 정보화 촉진법을 근간으로 정책으로 추진해오면서 우리나라의 정보화가 지금

처럼 상당한 수준에 이를 수 있도록 해온 것과 같이 그 다음 단계인 정보보호 촉진을 범국가적 차원에서 도모할 시기가 왔다는 점을 인식하고, 이를 실제정책에 반영하는 것이 필수적이라는 상황인식이 절실하다.

둘째, 게임개발 전문인력 양성 및 전문성을 강화해야 할 것이다. 기업의 핵심자산이 디지털화되고, 새로운 네트워크를 통해 이러한 자산이 어떻게 통제되고 관리되는지가 관심사로 떠오르면서 핵심자산을 보호하는 보안시스템 관리자가 절실히 요구되고 있다. 또한 정부나 기업에서 보유한 기술과 정보를 외부로부터 보호하려는 움직임이 강하게 대두되고 있음은 물론, 아웃소싱을 통한 24시간 보안체제가 책임여부의 한계를 드러내면서 내부사정에 밝은 임원급 책임자가 요구되고 있다. 정부나 기업에 있어서 게임산업을 위한 최적의 효과를 거두기 위해서는 게임개발을 통한 제반 총체적인 시스템을 구축하고 용역에 대해서는 아웃소싱을 병행하는 것이 중요하며, 외부 전문가를 초빙하여 지속적이며, 전사적인 게임 관련 윤리교육을 시키는 것이 중요하다.

셋째, 다국화/국제화 되어가는 사이버 범죄에 대한 공조체계를 확립해야 할 것이다. 정보기술이 네트워크화 되어가면서, 네트워크 기반을 견고히 한다는 측면에서 정보보호체계 및 전략의 총괄적이며 일원적인 운영과 관리가 재검토되어야 할 것이며, 정부통합전산센터와 부처 간, NCSC 및 정보보호진흥원 등 유관기관 간 사전 정보공유 및 일사불란한 대응체계를 구축해야 한다.

넷째, 지속적으로 변화하는 정보보호 산업에 대한 정부와 기업 주무부처의 끊임없는 육성과 지원 정책이 필수적으로 수반되어야 한다. 산업과 기술은 계속해서 발전해 나가고 있으며 이를 뒷받침 해줄 지원정책은 지속적으로 지원되어야 할 것이다.

다섯째, 인포데믹스 확산으로 야기될 개인의 프라이버시 침해방지를 위해 정부와 포탈의 노력이 필요하다. 인포데믹스의 주요 전파통로인 포털 사이트는 건전한 인터넷 문화 구현을 위한 사회적 책임과 역할과 완수를 위한 노력이 요구되고 있다.

마지막으로 유비쿼터스 인프라에 대한 사이버 위협에 대응하는 정보보호 대응체계를 구축해야 할 것이다. 이를 위해 정부 주요부처와 학계 및 업계전문가를 중심으로 유비쿼터스 보안에 관한 정보 교류와 정책 제안 등 긴밀한 협력증진체계를 마련하여 도래하는 유비쿼터스 환경에 적합한 국가차원의 신정보보호 체계를 구축해나가야 할 것이다.

## V. 결론 및 제언

본 연구는 게임정책에 대한 인식과 수준을 측정하여 게임정책과 관련된 정부와 기업의 정책 수립에 적용할 목적으로 연구되었다. 특히 정부 및 게임관련업체 개발담당자 등 관련 전문가의 설문을 통해 의견을 반영하였다.

또한 상대적 중요성 및 상관관계 등 설문조사 결과를

분석하여 각 후보 항목에 대한 요소로서의 타당성을 도출하였으며, 도출된 결과의 상당부분에서 후보항목이 바람직한 항목인 것으로 분석되었고, 정책을 위한 의지와 총체적인 중요성을 전달하려는 의도에서 정책방향의 의미를 전달하는데 필요한 항목임을 알 수 있었다.

향후 본 연구는 게임정책분야와 관련된 해외의 세부적인 사항을 조사하여 보완할 필요가 있으며 정보보안에 대한 보다 수치화된 데이터를 제시할 수 있도록 발전시킬 필요가 있고 국내 우수기업의 참여를 통한 구체적인 수출실적의 창출 및 글로벌 비즈니스 파트너, 채널 구축 기회 획득을 통해 경쟁력을 강화해야 한다.

이렇게 하여 수치화된 지표가 완성되면 정부, 주요 공공기관 및 대표적인 일반기업을 중심으로 각 조직의 정보보호 수준을 평가하여 전반적으로 우리나라의 정보보호를 기반으로 한 게임정책에 대한 수준을 재조명하여 문제점을 도출하고 개선방안을 제시할 필요가 있다.

## 참고문헌

- [1] 정보보호진흥원, 정보보호 실태조사, 2006.
- [2] 국가정보원, 정보보호 백서, 2006.
- [3] 정보통신부, cyber korea 21, 2001.
- [4] 정보통신부, IT839 전략, 2006.
- [5] <http://www.ncsc.go.kr>
- [6] 정보사회진흥원, 주요국 정보보호 동향 조사, 2007.
- [7] 국가보안기술 연구소, 911 테러이후 미국 정보보안 정책동향, 007.
- [8] 김유향, 정보보호의 현황과 과제, 2005.
- [9] 유지연, 정보통신 정책 17권 12호 통권 373호, 2005.
- [10] 정보보호진흥원, EU의 정보보호 전략 및 시사점, 2006.
- [11] 영국 내무부, Investigation of Protected Electronic Information, 2006.
- [12] 국가보안기술 연구소, 프랑스 정보보안 시스템에 관한 총리 훈령, 2006.
- [13] 통계청, 초고속 인터넷 가입 현황, 2007.
- [14] 정보보호진흥원, 인터넷 침해사고 동향 및 분석 월보, 2006.
- [15] 경찰청 사이버 테러 대응센터, 사이버 범죄현황, 2007.
- [16] 박지형, 국가 사이버 안전체계 개선에 관한 연구, 2004.