정보통신망 신뢰성 및 안정성 확보 방안 연구

- 자율규제를 중심으로 -

2009. 8.

정 책 기 획 단 법 제 분 석 팀

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 **『정보통신망 신뢰성 및 안전성 확보방안 연구』**의 연구결과보고서로 제출합니다.

2009. 8.

연 구 기 관 : 한국인터넷진흥원
총괄책임자 : 이창범 팀장(법제분석팀)
참여연구원 : 백승흠 교수(청주대)
양지연 변호사(한국 MS)
최철호 교수(청주대)
최혜선 박사(건국대)
김본미 주임연구원(법제분석팀)
김명아 연구원(법제분석팀)

요 약 문

1. 제목

본 연구는 정보통신망에서의 신뢰성 및 안정성의 확보방안에 대하여 자율규제에 중점을 두고 연구하고자 한다.

2. 연구의 목적 및 중요성

현대사회에서는 정보통신망에서의 활동영역이 가장 중요하고도 일상적인 부분이 되었다. 더 나아가 정보통신망에서의 활동이 사회의 전 영역에 영향을 미치고, 영향력이 커진 만큼 논란 또한 끊이지 않고 있다. 정보통신망, 더 나아가 인터넷에서 나타나는 현상들이 사회 현상이 되고, 각종의 사회적 문제를 양산하기도 한다. 이러한 현상에서도 알 수 있듯이 정보통신망에서의 신뢰성과 안정성의 문제와 사회적 관점의 역할과 위상의 문제 또한 중요한 이슈가 되고 있는 것이다. 정보통신망, 즉 인터넷이라는 공간이 가져온 긍정적인 효과도 많은 반면에 역기능으로 나타나는 그 부정적인 효과를 줄여나가기 위하여 정보통신망에서의 신뢰성과 안정성을 확보하여 부정적 요인들을 줄여나가는 방안이 필요하고 그에 대한 논의가 실질적 내용으로 검토되고 논의되어야 한다.

정보통신망의 신뢰성 및 안정성을 확보하기 위한 방안으로서 법적 규제의 한계와 자율규제의 촉진 방안을 중점으로 하여 살펴보고자 한다. 인터넷으로 대표되는 정보통신망에서의 행위도 현실세계에 분명한 영향력을 미치기 때문에 그에 대한 각종 규제제도가 시행이 되고 있다. 적절한 규제는 이용자에게는 가이드라인 제시의 효과도 있고, 사업자에게는 사업 방향의 구조와 틀을 제시해 하는 효과가 있다. 그러나 정보통신망이라는 공간의 특수성에 대한 인식과 장기적인 안목 없이 만들어지는 규제는 오히려 산업의 위축, 표현의 자유의 제한, 규제의 남용 등의 또 다른 문제를 낳게 되는 것이다.

정보통신망에 대한 규제가 그 규제로 인해 정보통신망에서의 산업 및 문화의 다양성이 위축되지 않고 산업과 사회문화를 다 같이 견인하기 위해서는 규제에 있

어서도 일관성 있는 기준이 있어야 한다.

규제는 적정해야 하고 합리적이어야 한다. 시장이나 산업, 사용자 관점 모두를 배려하여야 한다. 그렇지 않으면 사회에 영향을 미치는 후유증이 만만치 않을 것이기 때문이다. 그렇다면 어떠한 규제의 유형이 적합한지에 대하여 국내의 현황에 대한 논의와 또한 선진국의 규제의 현황을 살펴보고, 합리적이고 적정한 규제의 유형을 검토해보는 것이 필요하다.

해외의 정보통신망 규제의 유형과 현황에 대한 검토를 통하여 효과를 살펴보고, 긍정적 효과를 우리나라의 정보통신망 규제정책에 대한 반영하는 방안을 검토해 보는 것이 실익이 있을 것이다.

해외 선진국들은 규제의 방향을 시장과 산업이라는 관점에서 보고 있으며, 대부분 자율규제를 선호하는 추세이다. 해외 선진국의 자율규제의 정책과 현황을 파악해보고 그에 대한 시사점 등을 살펴보기로 한다.

3. 연구의 구성 및 범위

먼저 정보통신망의 자율규제에 대한 내용으로 현대사회에서의 정보통신망의 개념과 특징을 살펴보고, 특히 인터넷상의 자율규제의 등장배경을 파악해보기로 한다.

자율규제의 유형에 있어 정부의 개입정도에 따른 분류와 사용자와 인터넷서비스 제공자의 선택에 대한 영향에 따른 분류를 해보고자 한다. 또한 행정의 통제로부터 사업자의 자기책임으로의 전환에 대한 부분도 검토해 본다. 자율규제의 장단점을 살펴보고 자율규제기관에 대한 기본 의의와 자율규제기관의 기능과 역할을 살펴본다.

또한 정보통신망의 특징에 따른 자율규제의 도입에 대한 내용으로 인터넷상의 자율규제의 이론적 근거와 주체, 정보통신분야에 있어서 자율규제의 입법적 과제에 대해 검토한다. 또한 자율규제의 현황 및 문제점에 대한 내용으로 우리나라와 미국, 호주, 일본, 독일과 EU에서의 현황을 살펴본다. 자율규제와 더불어 정부규제에 대한 내용으로 우리나라, 미국, 일본, 독일과 EU의 정부규제의 현황을 살펴보고, 정부규제의 한계점은 무엇인지에 대하여 검토해 본다.

마지막으로 정보통신망의 자율적 활성화 방안으로서 우리나라 자율규제의 나아갈 방향으로 이용자 보호 및 권익제고를 위한 자율규제의 활성화와 이해당사자간 갈등조정시스템을 통한 자율규제의 활성화, 그리고 민간 규제 영역의 활성화에 대하여 검토한다. 또한 자율규제 활성화를 위한 업계의 노력과 정부의 역할과 정책의 방향, 이용자의 자정활동에 대하여 검토해 본다.

4. 연구내용 및 결과

미국의 정부규제부분을 살펴보면 미국은 21세기 정보화시대의 주도권을 잡기 위해 정보보호를 위한 다양한 법과 제도를 수립·시행 중이며, 최첨단 암호 알고리즘과 프로토콜 개발 등 정보보호 기술 개발에도 역점을 기울이고 있음을 알 수 있다. 미국의 정보보호 관련 법령으로 「컴퓨터 사기 및 오용에 관한 법률(Computer Fraud and Abuse Act)」과 연방법전의 컴퓨터 네트워크 범죄 관련 규정들이 있다. 「컴퓨터 사기 및 오용에 관한 법률」은 컴퓨터를 통한 국가보안정보, 금융정보, 행정정보 등에 대한 불법적인 접근·취득·사용, 컴퓨터를 이용한 사기, 컴퓨터에 대한 손상 등을 범죄로 규정하고 이에 대한 처벌규정을 수록하고 있다. 연방법전에는 저장된 통신에의 불법 접근과 신분 절취, 스팸 규제, 유선 사기 등에 대하여 규정하고 있다. 국토안보 관련 대통령령(HSPD-7)은 미국 연방정부의 부처와 기관들이 국가의 중요한 기반과 자원보호계획 수립과 연방정부의 부처와 기관들이 국가의 중요한 기반과 자원보호계획 수립과 연방정부·주정부·기업 간의 협력을 통해 미국의 중요기반과 자원에 대한 보호계획수립에 대한 내용을 담고 있다.

미국의 자율규제는 정보의 공유와 위험에 대한 관리, 신뢰에 바탕을 둔 모델을 취하고 있다. 일반 사용자는 National Cyber Security Awareness Month를 정해 여러 파트너사들을 통하여 집중적으로 사용자 교육을 제공받고, StaySafeOnline.org에서는 사용자의 가정에서 컴퓨터를 보호하는 정보를 공유한다. 전력회사, 병원, 통신사 등 중요 인프라를 구축하는 기업용 사용자의 경우 위험관리방식을 통해 위협의 우선순위를 정하고 이슈 파악 후 가장 중요한 이슈에 집중적으로 시간과 자본 등을 투입한다.

일본의 정보통신망 자율규제의 경우 정부가 개입하여 보안 확보를 위한 강제조치를 하는 경우는 거의 없으며, 정부는 다양한 계획과 정책을 발표하여 민관 합동 대응체제를 구축하고자 한다. 일본의 1·2차 정보보호 기본계획 및 안심넷 만들기 촉진프로그램 등은 정부·지방자치단체·주요기반·기업·개인 등이 자발적으로 참여하고 국가는 이들에게 '가이드라인'을 제공하는 선에서 그치도록 운영 중이다. 현재 일본의 정보통신망 규제는 주로 내각관방정보 시큐러티 센터(内閣官房情報 セキュリティ— センタ—)에서 담당하고 있다. 시큐어 재팬 2차 계획으로 일본 정부는 시큐러티 체제의 구축 후 이를 유지·발전하여 IT사회를 구성하는 전 주체의 계몽과 적절한 역할 분담이 필요하다고 평가했다. 제2차 계획에서는 '새로운 민관 제휴 모델'의 유지·발전을 통하여 정책을 더욱 진화시키도록 하고 있다.

EU는 각국이 자율규제에 적극적으로 참여할 수 있도록 핫라인 구축 및 예산지원 등의 자율규제시스템을 지원하고 있다. 대표적인 자율규제기관으로는 INHOPE(Internet Hotline Providers in Europe)와 PEGI(Pan European Game Information)가 있다.

독일은 멀티미디어자율규제협회(FSM)라는 자율규제 기관을 두고 있다. 독일의 멀티미디어자율규제협회(FSM)는 2005년 10월에 '방송과 텔레미디어에 관한 인간의 존엄의 보호 및 청소년의 보호에 관한 주제협정' 제19조에 근거해서 '청소년미디어보호위원회(KJM)'으로부터 인터넷자율규제기관으로서 승인을 받았다. 독일의 온라인상 자율규제 실태의 현황은 청소년보호를 중심으로 이루어져 있고, 청소년보호법은 주로 도서, 잡지, 사진, 비디오카세트, 음반, DVD 등 기록매체를 규제대상으로 하는데 반하여 청소년미디어보호에 관한 주(州) 간 협약은 방송과 텔레미디어(인터넷)를 대상으로 하고 있다. 또한 독일은 다양한 분야에서 청소년미디어보호의 강화를 위한 기업의 자율조치로서 검색엔진제공자 및 채팅제공자의 자율규제 등이 실시되고 있다.

우리나라 자율규제의 현황은 제도적 장치의 측면과 기업의 자율규제 측면으로 나누어 볼 수 있다. 인터넷기업의 자율규제 장치들을 보면, 각 기업들이 내부적으로 모니터링과 부분적인 정보게시제한조치 및 옴부즈맨 제도를 도입하여 이용자 보호정책을 수행중이다. 또한 주요 포털사들은 이용자, 전문가 등으로 구성된 책무

위원회를 운영하는 등의 자율적인 규제 역할을 수행중이다. 또한 사업자단체측면의 자율규제 장치로서 한국인터넷자율정책기구와 한국정보통신산업협회의 개인정보보호마크제도·인터넷사이트 안전마크제를 시행중이다.

정보통신망에서의 규제에 있어서는 정부정책과 사업자의 경제성 및 기술적 역량, 기업윤리, 그리고 이용자들의 이용행위의 자유 등 각 이해당사자들 간의 활동의 영역 및 갈등부분이 모두 고려되어야 할 것이다. 향후 정보통신망의 규제는 각 당사자들의 갈등 조정을 염두에 두고 자율규제를 활성화하는 방향으로 이루어져야 할 것이다.

자율규제의 모델에 있어서 민간 규제의 영역과 정부 규제의 영역의 활성화를 두고 어떠한 것이 적정하고 합리적인 것인지에 대하여 논의의 필요성이 있다. 과거 우리나라는 정부규제에 집중되어 있었으나, 선진국 등 외국의 사례에서도 보았듯이 민간자율규제를 활성화하는 것이 합리적 규제의 방안이 될 것이다.

정보통신망에의 신뢰성과 안전성을 확보하기 위해서는 하나의 일관된 규제 철학을 가지고 통일성 있는 규제정책(자율규제 확산 중심으로)을 시행해 나가야 할 것이다. 또한 개별적 규제들 간의 상호 관련성을 검토하여 각종 규제간의 불일치를 해소하여야 하며, 규제로 인한 부작용을 최소화할 수 있도록 대응방안도 마련되어야 한다. 또한 규제로 인한 산업과 시장 기능이 축소 및 위축되는 것에 대한 방지책과 현실적이고 실천적인 대응방안이 있어야 할 것이다. 또한 자율규제를 활성화하는 것이 규제에 있어 적정성과 합리성을 확보할 수 있고, 그로 인해 정보통신망에의 신뢰성과 안전성을 확보할 수 있는 디딤돌이 될 것이다.

5. 정책적 활용내용

본 연구에서 해외 선진국의 정보통신망의 정부규제와 자율규제의 현황을 살펴보고, 우리나라의 현황을 비교 연구해 본 결과, 정보통신망에의 신뢰성과 안전성을 확보하기 위해서는 하나의 일관된 규제 철학을 가지고 통일성 있는 규제정책(자율규제 확산 중심으로)을 시행해 나가야 할 것이다. 또한 개별적 규제들 간의 상호 관련성을 검토하여 각종 규제간의 불일치를 해소하여야 하며, 규제로 인한 부작용을 최소화할 수 있도록 대응방안도 마련되어야 한다. 또한 규제로 인한 산업과 시

장 기능이 축소 및 위축되는 것에 대한 방지책과 현실적이고 실천적인 대응방안이 있어야 할 것이다.

6. 기대효과

자율규제 활성화 방안에 대한 연구는 정보통신망의 규제에 있어 적정성과 합리성을 확보할 수 있고, 그로 인해 정보통신망에의 신뢰성과 안전성을 확보할 수 있는 디딤돌이 될 것이다.

SUMMARY

1. Title

This research is intended to study with focusing at the self regulation from the method of securing the reliability and stability in information network.

2. Objective and Importance of Research

The range of action in the information network has become the most important and usual part in the modern society. Furthermore, there are endless disputes because the activities in the information network make influence on the total area of the society and it is more influential. The methods to reduce the negative factors arise as the adverse functions are necessary through securing the reliability and stability in the information network to reduce the negative effect, while there are many positive effect brought by the information network, namely internet. This subject has to be reviewed and discussed in reality.

The legal restriction and its limitations and measures to activate self regulation will be the key factors of this study and shall be investigated intensively. Also the methods to secure the reliability and stability in information network will be considered deeply. Many regulating regimes come into effect because the actions in the information network, which is represented by internet, are evidently influential to the real world. The proper regulating has an effect of suggesting guidelines to users and is also effective for suggesting the structure and frame of the business direction for businessmen. However in the long term, the regulations which are prepared without the recognition on the specialty of the information network space may cause other

problems such as reduction of the industry, restriction on the freedom of expression and abusion of regulation etc.

There must be a consistent standard in the regulation in order to lift up the industry and social culture together without diminishing the variety of industry and culture in information network due to the regulation to the information network. The viewpoints of market, industry and users shall be taken into consideration simultaneously. The discussion on the domestic situation and the status of regulation in advanced countries shall be surveyed to find out the appropriate type of regulation. Also, the review of the patterns of reasonable and proper regulation is necessary.

The target of regulating in advanced countries is focused at the viewpoint of market and industry and mostly self regulation is preferred. The policy and status of the self regulation in advanced countries are identified and the indications from such regulation will be surveyed.

3. Contents and Scope of the Research

Firstly, the concept and characteristics of information network in the modern society is investigated, and especially the background of self regulation is identified. The patterns of self regulation will be categorized by the degree of government engagement and influence from the choice of users and internet service providers.

Also, the part to be converted to the service providers' responsibilities from the administrative enforcement will be reviewed. The merits and demerits of the self regulation, fundamental meaning, function and role of the institutions of self regulating will be surveyed. The theoretical basis and subject for the self regulation in the internet and the task of legislation for self regulation in the IT field will be reviewed as a content for the introduction of self regulation according to the information network characteristics. In addition, the

self regulatory status and the limitation of government regulations in Korea, USA, Australia, Japan, Germany and EU countries will be introduced.

Finally, the activations of self regulation for the user protection and improvement of right, through conflict adjustment system among the concerned entities and the restriction area for privates will be reviewed as a target of self regulation in Korea for the method of self regulative activation of the information network. In addition, the efforts from the industry, the role and direction of government policy and the users' self disciplined activities for the activation of self regulation will be surveyed.

4. Research Results

USA has established and executed the various laws and regimes for the information protection in order to take the initiative at the information era of 21st century in the field of government regulating and paying attention to the technology development for information protection such as the cutting edge code algorism and protocol development.

The self regulation in USA adopts the model based on the control on the information sharing, risk and trust. The user education is supported intensively to general users through the many partner companies by determining the National Cyber Security Awareness Month. StaySafeOnline.org share the information which protects the computers in the users' home. The company users decide the priority of threats through the risk management method when they are the users establishing the important infrastructure such as electric power company, hospital and communication company etc. They invest the time and capital on the most important issue intensively after finding the issue.

There are few cases that the forced control for insuring the security through the government's involvement in the self regulation of information network in

Japan. The government tries to establish the joint cooperative system through declaring the various plans and policies. The government, local government, main infrastructure, companies and individuals take part in the 1st and 2nd security basic decoder, promotional program for making safenet voluntarily. The government manages it only to the level for providing the guideline for them. Now, the Security Center of Cabinet Official Information is in charge of the regulation on the information network in Japan. The Japanese government evaluated that the enlightenment of all subjects which constitute the IT community and the proper sharing of the roles are necessary through maintaining and developing the security system as the 2nd plan of Secure Japan. They make the policy evolve through the maintaining and developing of the 'new civil-government alliance model.'

EU supports the regulating system such as the hotline establishment and budget allocation for each country to participate into the self regulation aggressively. INHOPE(Internet Hotline Providers in Europe) and PEGI(Pan European Game Information) are the typical institutions for self regulation.

Germany has a self regulation institution named as Multimedia Self Regulation Association (FSM). The Multimedia Self Regulation Association (FSM) in Germany was approved as the internet self regulating institution from the 'Teenager Media Protection Committee (KJM)' based on Article 19 of 'The subject protocol on the protection of human dignity and protection of teenager from the broadcasting and telemedia' on October, 2005. The reality of the self regulation in online is focused at the protection for the teenager in Germany. The teenager protective laws restrict the recorded media such as the book, magazine, photo, video cassette, music disc and DVD. On the other hand, the agreement among the states mainly restrict the broadcast and telemedia(internet). In addition, the self regulation on the search engine provider and chatting provider is being performed as a self control of the

company to reinforce the protection of teenager from media in various fields in Germany.

The status of self regulation can be classified into the institutional provision and company self regulation in Korea. According to the survey to the self regulation method of internet company, they have performed the user protection policy through the internal monitoring, the partial restriction on the information placement and induction of ombudsman system. In addition, main portal companies have been performing the role of self regulation such as the task committee constituted by the users, specialist. The individual information protection marking system, internet site safety marking system from the Korea Internet Self Policy Organization and Korea Information and Communication Industry Association are effective as the self regulation devices from the business provider's group. The government regulation, pre-restriction, and legal regulation have to be abandoned because it may shrink the market function and the self regulation can be emphasized but to the direction to control the conflicts in consideration of the area of the concerned entities' action and conflicts such as the government policy, economy of businessmen, technological competence, company ethics and the freedom of users etc.

It is necessary to discuss what is proper and reasonable in the activation of private sector and public sector in self regulation model. It was intensified in the government regulation in Korea in past time, the preference of the private self regulation must be the method of reasonable regulation as it was shown in the cases of foreign countries.

The regulating policy in uniformity (based on the self regulation activation) shall be carried out with the strict regulating philosophy in order to secure the reliability and stability in information network. Furthermore, the inconsistency among the regulation shall be dissolved by reviewing the co-relations among individual regulations and the countermeasure has to be provided to minimize

the side effect due to the regulation. In addition, the activation of the self regulation can secure the appropriateness and reasonability in the regulation. It can be a foothold to secure the reliability and stability in information network.

5. Policy Suggestions for Practical Use

According to the comparison between the government regulation and self regulation in information network of foreign countries and the status in Korea, the regulating policy in uniformity (based on the self regulation activation) shall be carried out with the strict regulating philosophy in order to secure the reliability and stability in information network. Furthermore, the inconsistency among the regulation shall be dissolved by reviewing the co-relations among individual regulations and the countermeasure has to be provided to minimize the side effect due to the regulation. And the protective idea, realistic and executable countermeasures for the reduction and diminishing of the industry and market function shall be provided.

6. Expectations

The study of self regulation will help secure the appropriateness and reasonability in the area of information network self regulation. It can be a cornerstone to secure the reliability and stability in information network.

목 차

Contents

표 목 차

그 림 목 차

1장 정보통신망과 자율규제

제1절 현대사회에서의 정보통신망의 개념과 특징[1)]

정보통신망, 특히 인터넷으로 대표되는 사이버공간은 전 세계를 연결하는 네트워크로서 누구나 언제든지 접속하여 정보를 획득하고 배분할 수 있는 유용한 이용수단이다. 또한 정치적으로는 인터넷을 통하여 여론수렴을 할 수 있고, 사이버 교육의 실시로 교육적인 혜택까지 받을 수 있고, 인터넷을 통한 전자상거래로 물품을 구매할 수도 있다. 그러나 이렇게 편리한 이점들의 이면에는 해킹, 악성 바이러스 등으로 인한 사이버위협이 문제가 되고 있는데, 이것은 사이버공간이 개방형 구조로 되어 있어 태생적으로 보안에 많은 취약점을 드러내고 있기 때문이다.

그 특징을 보자면 먼저 접근의 용이성과 신속성이 있다. 이러한 이유로 인터넷 이용자는 지속적으로 증가하고, 인터넷 등의 정보통신망을 이용하여 누구든지 원하는 시간에 정보열람과 전송 등 정보전달 속도가 빨라졌다.

두 번째로는, 복잡성을 그 특성으로 볼 수 있다. 노드의 증가로 인하여 노드사이의 링크가 기하급수적으로 늘어나는 복잡한 구조를 가지고 있는 인터넷 네트워크는 시간이 지나면서 노드사이의 링크가 소멸과 생성을 반복하면서 진화의 과정을 겪게 된다. 또한 노드사이의 링크는 다른 가중치를 가질 수 있으며, 시간에 따라 상태가 달라질 수도 있다. 결국 하나의 네트워크에 수많은 서로 다른 성격의 노드들이 연결되어 있어 전체 네트워크를 파악하기 어려워지고, 이 때문에 인터넷에서 어떤 문제가 발생하였을 때 근원지가 어디인지조차 파악하기 어려워지게 되는 것이다. 이러한 복잡한 네트워크망은 현대사회의 정보통신망의 특징을 결정하는 중요한 구조적 요소 중의 하나이다.[2)]

세 번째, 익명성을 그 특징으로 들 수 있다. 사이버공간에서는 이용자 사이의 대

---

1) 김종보, 유시티건설법과 정보통신망의 법적지위, 경제규제와 법 제2권 제1호, 2008. 12. 138면 참조.

2) 이종환, 사이버상에서의 정보보호를 위한 정부역할 연구 -민간부문을 중심으로-, 박사학위논문, 중앙대학교, 2006. 8면.

화나 정보전달은 익명으로 이뤄지는 경우가 많으며, 이러한 특성으로 인하여 상대방의 성별, 직업, 나이 등의 실제 정보는 상대방의 의견표명을 통하여만 알 수 있다. 이러한 익명성은 현실의 사회규범에서 벗어나 자유롭게 자신의 의견을 표현하고, 위계질서로부터 벗어나 평등한 주체로서 가상공간에서의 또 다른 주체를 형성할 수 있게 한다.[3] 그러나 이러한 장점에도 불구하고 일부 이용자들은 익명성이 보장되는 것을 악용해서 허위사실을 유포하여 타인의 명예를 훼손하거나, 상대방에게 폭력적이며 인격을 모독하는 욕설을 사용하는 등의 일탈 행위들을 일삼는 경우도 있다.

네 번째 특징으로는 부을 들 수 있다. 다른 매체에 비하여 정보통신망은 정보전달이 일방적이 아닌 쌍방향적이다. 이용자들은 스스로 정보생산도 하고, 자신이 원하는 정보를 선택하기도 한다. 특히 인터넷의 웹 환경에서는 텍스트와 텍스트가 독특한 연결망 구조인 하이퍼텍스트로 연결되어 있어 상호연결과 전환이 보다 자유로운 특징을 지니고 있다.

제2절 자율규제의 의미

1. 자율규제의 개념

자율규제란 일반적으로 정부(행정)규제에 대비되는 개념으로 사용되고 있다.

정부(행정)규제란 국가 또는 지방자치단체가 특정한 행정목적을 달성하기 위해서 공권력 작용을 통하여 국민의 권리를 제한하거나 의무를 부과하는 것을 의미한다.

이에 대해 자율규제란 규제의 주체가 정부가 아니고 규제의 상대방인 피규제사업자 내지 피규제사업자단체가 법령상 자신들이 준수해야 할 기준을 스스로 수범하도록 함으로써 규제의 대상이 아니라 규제의 주체가 되는 것을 의미하는 것으로 현행법으로도 정부규제를 대신하는 정책수단으로서 폭넓게 활용되고 있다. 즉, 정부의 개입(행정규제)은 줄이고 시장자율(자율규제)은 확대하는 규제개혁 내지

3) 황주성 외, 인터넷 정치·사회적 파급효과 및 대응방안 연구, 정보통신정책연구원, 2001, 35면.

규제완화를 의미하는 것이다.

법적인 측면에서 자율규제를 정의하면 공적 부분에서의 규제에 대한 권한을 국가가 직접 행사하지 않고 이를 자율규제기관에 위임함으로써 시장의 사적 거버넌스가 촉진된다고 한다.[4)]

그런데 자율규제를 공적규제의 반대개념 또는 탈규제로 이해하는 것은 바람직하지 않다. 왜냐하면 공적규제의 완화나 제거를 목적으로 하는 것이 아니라 보다 빠르게 사전에 피해를 차단하여 산업을 활성화하려는데 그 목적이 있기 때문이다.

2. 자율규제의 분류

인터넷 콘텐츠 등 정보통신 분야에 대한 규제는 자율규제는 행정기관과 사업자의 결합정도, 즉 행정이 가지는 법적 강제로부터의 상대적 자율성의 정도에 따라서 다음과 같은 네 가지의 종류로 분류할 수 있다.[5)]

가. 정부의 개입정도에 따른 분류

1) 명령적(mandatory) 자율규제

명령적 자율규제는 시장에서 특정한 업종에 종사하는 일단의 조직들이 국가의 요청에 의하여 국가가 정한 범위 내에서 자율적인 규제의 형식을 만들고 집행하도록 요청받는 형태를 말한다.

2) 제재적(sanctioned) 자율규제

이 개념은 이를 시행하는 사업자들이 스스로 자율규제의 기본적 구조와 상세한 규정을 만들지만 최종적으로 국가의 승인을 받아야 효력을 발생하는 규제방식을

---

4)Ayers/Braithwaite, Responsive Regulation: Transcending the Deregulation Debate (Oxford: OUP, 1992), p.4.

5) Julia Black, Constitutionalizing Self-Regulation, The Modern Law Review 1996, pp.24-55.

말한다. 대표적인 예로서는 기업과 정부 간에 체결되는 자기통제협약(Selstbeschraenkungsabkommen)을 들 수 있다. 자기통제협약이란 사업자가 행정주체에게 특정한 행위를 하지 않겠다든가 또는 하겠다든가 혹은 일정한 안전 및 환경기준 등의 스스로 준수하겠다는 내용의 약속을 하는 것을 말한다. 자기통제협약은 일종의 신사협정이기는 하지만 사업자가 자신의 약속에 위반하는 경우에는 일정한 제재수단을 받아들이겠다는 내용의 협약의 내용으로 삽입하여 일정 수준의 구속력을 유지한다.

3) 강제적(coerced) 자율규제

강제적 자율규제는 개념적으로 '강제적'이라는 말이 '자율규제'와 조화되지 못하는 것으로 보이기는 하지만, 일단 사업자나 사업자단체가 우선적으로 규제의 형식과 내용을 결정한다는 점에서 자율규제의 범주에 포함되는 것으로 본다. 그러나 만약 규제가 필요한 경우 국가가 이를 요구함에도 불구하고 규제가 이루어지지 않는다면 국가가 직접 나서서 법규상의 규제를 행한다는 점에서 강제적 요소가 발견되기 때문이다.

4) 자발적(voluntary) 자율규제

진정한 의미의 자율규제라고 할 수 있는 자발적 자율규제는 국가의 직접 또는 간접적인 개입과는 전혀 관계없이 사업자 또는 사업자단체 스스로의 판단과 이니셔티브에 의하여 이루어지는 규제를 말한다.

나. 사용자와 인터넷서비스 제공자(ISP)의 선택에 대한 영향에 따른 분류[6)]

1) 인터넷서비스 제공자 자율규제형

6) 황승흠, 인터넷콘텐츠 규제에 있어서 법제도와 사업자 자율규제의 결합에 관한 연구, 공법학연구 제9권 제4호, 2008. 12. 266-268면 참조.

인터넷서비스 제공자들이 필터링 서비스를 제공하고 이용자들은 원하는 바에 따라서 이를 선택한다. 정부의 간섭은 최소한도이다.

이에 따른 인터넷 콘텐츠 필터링 정책은 이용자와 인터넷서비스 제공자 양자에게 최소한의 재정적 부담과 인터넷서비스 실행에 관한 제한적인 영향을 가져오는 효과를 수반한다.

2) 정부의 자율규제 촉진형

정부가 후원자로서 행동하고 바람직하지 않은 내용들을 정의하는 데에 선행적인 역할을 한다. 정부는 잠재적인 서비스제공자이다.

이에 따른 인터넷 콘텐츠 필터링 정책은 인터넷서비스의 실행과 재정적 문제에 최소한의 영향을 주게 된다. 다만 필터링 서비스를 원하는 이용자들에게 더 나은 서비스를 제공하도록 인터넷서비스 제공자에게 영향을 줄 수 있고 또한 최종 이용자들에게 필터링을 이용하도록 권장할 수 있다.

3) 정부의 자율규제 강제형

정부가 인터넷서비스 제공자들에게 필터링을 명령한다. 정부가 인터넷서비스 제공자들에게 바람직하지 않은 모든 내용들에 대한 필터링 서비스를 제공하도록 강제한다. 또한 정부는 바람직하지 않은 것이 무엇인지에 관해서 정의를 내린다.

이에 따른 인터넷 콘텐츠 필터링 정책은 인터넷서비스 제공자들은 하위 접속자들에게 필터링 서비스를 제공하도록 강제될 수 있고 이용자들에게 그 비용을 전가할 것이다. 인터넷서비스의 실행에 일정 부분 영향을 미치게 된다.

4) 정부의 필터링 차단 실행형

정부가 바람직하지 않은 모든 콘텐츠를 차단하고 필터링한다. 정부가 인터넷망 등에 대한 필터링 계획을 구축한다.

이에 따른 인터넷 콘텐츠 필터링 정책은 가장 극단적인 방법인데 인터넷서비스의 실행에 중요한 영향을 미친다. 결국은 인터넷의 발달을 고착화할 가능성이 있다.

3. 행정의 통제로부터 사업자의 자기책임원칙으로의 전환

자율규제가 규제완화와 밀접한 관련을 가지고 있지만 자율규제가 행정의 통제로부터 회피하는 수단으로서 사용되어서는 곤란하고 국민의 건강이나 안전과 관련한 분야 즉, 식품위생행정이나 환경행정, 소비자안전과 관련한 행정의 영역에서는 오히려 규제를 강화해야 할 필요성이 있다. 물론 이 경우에도 규제를 강화한다고 해서 그 방법이 행정에 의한 규제일 필요는 없고 자율규제의 제도 속에서 규제기준을 강화하거나 관련법에 감시나 모니터링제도를 도입하는 방법이 고려될 수 있을 것이다. 종래 규제완화는 "경제적 규제"와 "사회적 규제"로 나누어서 그 정도와 기준을 달리하고 있다. "경제적 규제"는 주로 시장경쟁이 직접적으로 영향을 미치는 기업의 본질적인 생산 활동에 대한 규제로서 특정산업에 대한 진입규제, 가격규제, 설비규제, 수입규제, 독과점 및 불공정거래규제 등의 규제이고, "사회적 규제"는 자율과 시장경쟁원리로서는 해결할 수 없는 사회적 문제를 해결하기 위한 규제로서 국민의 안전・건강의 확보, 환경보전, 재해방지 등의 사회적 견지에서 행해지는 규제이다.[7] 경제적 규제는 원칙적으로 자유이고 예외적으로 규제하지만, 사회적 규제는 주로 국민의 안전・건강의 확보와 관련이 있기 때문에 원칙적으로 규제 예외적으로 자유를 허용한다. 사회적 규제를 완화할 할 때는 법령상의 안전성 기준에 대한 규제의 완화・폐지가 문제된다. 예를 들면 서론에서도 언급했듯이 국민의 건강・위생과 관련 있는 식품위생행정이나 안전성 기준과 관련 있는 고압가스기기의 제조기준 등과 같이 국민의 건강이나 안전 확보를 직접적 내용으로 하는 규제는 자기책임원칙에 따른 자율규제를 중시하여 규제를 필요최소한에 그치게 할 것이 아니라 자기책임을 위한 전제를 만드는 규제의 문제로서 오히려 강화해야 한다는 지적도 있다.[8] 자율규제를 규제형식의 측면에서 본다면 예컨대, 검

7) 增田政章, 經濟活動における規制緩和, 法政論叢 제32권, 1996, 22면.
8) 鈴木深雪, 安全·表示と規制緩和, ジュリスト 제1044호, 1994, 118면.

정제도, 형식승인제도, 인증제도 등과 같이 행정에 의한 통제로부터 사업자의 자기책임원칙을 중시하는 경향이 있다.

최근에 규제완화가 강조되기는 하나 이는 위에서 언급한 경제적 규제는 대폭 완화해야 한다는 것을 뜻하는 것이지만 식품위생이나 위험시설물의 제조설치기준 등과 같이 국민의 안전과 관련한 사회적 규제까지 대폭 완화해야 한다는 논리는 아니다. 따라서 규제완화라는 측면에서의 사회적 규제는 규제의 완화·폐지뿐만 아니라 규제도입·강화의 면까지 검토하여 국민의 이익의 관점에서 그 필요성과 합리성을 판단해야 한다.[9)]

4. 자율규제의 장단점[10)]

가. 자율규제의 장점

1) 국가의 부담경감

행정이 담당할 사무가 확대되어 감에 따라 당연히 규제도 많아지게 되는데 이러한 규제권한을 행사할 행정기관을 무한정 증대시킬 시대적·경제적 여건이 국가나 지방자치단체에는 갖추어져 있지 않다. 이와 같이 행정기관이 대처할 수 없는 규제집행의 흠결을 자율규제로서 보충할 수 있고 이는 정부의 인력과 예산을 절감하여 작은 정부를 가능하게 한다는 것이다.

2) 규제목적과 수단의 균형-행정법상의 비례원칙의 적용확대-

국민의 안전의 확보에 필요한 최저한도를 넘는 목적을 가진 규제의 경우에는 비례원칙의 관점에서 규제수법도 보다 온건한 것으로 해야 한다는 요청에 부응하기 위해서는 행정규제보다는 자율규제가 더 용이하다는 장점이 있다.

---

9) 根岸 哲, 規制緩和と消費者の安全, ジュリスト 제1034호, 1993. 4, 41면.
10) 原田大樹, 自主規制の公法學的研究, 有斐閣, 2007. 3-4면 참조.

3) 행정작용에의 민간참여 확대

민간주체에 의한 공적이익의 실현이 가능하고, 고도의 전문지식이 요구되는 행정영역에 민간의 전문적 지식을 행정과정에 포섭할 수 있는 장점이 있다는 것이다.

나. 자율규제의 단점

1) 행정법 이론의 도피수단으로 악용될 가능성

자율규제의 형식을 취한다면 비례원칙이나 적정절차의 원칙이라고 하는 행정법규율로부터 도피할 수 있는 가능성이 있기 때문에 국가에 의한 규제에서는 허용되지 않는 사업 등이 자율규제에서는 허용될 수 있는 가능성이 있다는 단점이 있다.[11)]

2) 규제내용의 엄격성·중립성의 상실

자율규제에 의한 직·간접적인 영향은 넓게는 제3자에게 파급될 수 있는 데 반해 그 내용형성이나 실시과정에 대한 민주적인 통제가 미치지 않는다. 그 결과 규제수준이 느슨하게 되고 규제의 내용결정이 불투명해서 제3자의 이해가 반영되지 않게 될 우려가 있다.

3) 자율규제의 신뢰성 저하와 비효율성

자율규제는 행정과 업계와의 폐쇄적이고 불투명한 관계 가운데에서 전개되어 자율규제의 이름하에 업계이익만을 대변하는 경우가 발생하여 업계이익만을 추구하는 결과 규제의 유효성과 효율성의 관점에서 본다면 자율규제는 신뢰할 만한 가

11) 三輪芳朗, 規制緩和を阻む日本の業界團體『民民規制』こそ破壞すべし,論爭東洋經濟9號, 1997, 176면.

치가 없다는 비판이 제기될 수 있다고 한다.

4) 신규진입을 제약하는 수단으로의 악용

자율규제를 행하는 사업자단체가 자신들의 기득권을 유지하는 데 이를 이용하면 자율규제는 오히려 경쟁을 제약하게 되어 신규진입을 제약하는 데 악용될 가능성이 있다는 것이다.[12]

5. 자율규제기관

가. 의의

자율규제방식은 자율규제기관(Self-Regulatory Association;이하 SRA라 한다)들이 국가의 위임을 받아 자신의 시장과 회원에 대하여 직접적인 규제를 담당하도록 하는 것이 시장친화적인 규제목적을 보다 효율적으로 달성할 수 있다는 점에 그 토대를 두고 있다. 국가는 SRA가 시장과 회원에 대한 규제를 구체적으로 어떠한 형태와 내용으로 규제해야 하는지 대강의 지침을 법률로서 규정하고 SRA의 정관과 자율규제규정 등을 승인하여 자율규제기관을 간접적으로 감독한다. 또한 국가는 정기적으로 SRA의 규제활동을 감시함으로써 증권분야에서 효율적인 규제와 감독이 이루어지도록 하고 이를 통하여 증권 산업이 스스로 고객과 회원을 보호하고 시장의 안정화를 도모하여 왔다. SRA는 금융 산업 등 특정 사업영역에서 사업자의 사적 이익과 더불어 관련 법규와 제도가 추구하는 공익목적을 적절하게 조절하는 것이 핵심적인 기능이다. 이를 위하여 SRA는 회원구성원의 가입과 탈퇴의 조건 등을 자율적인 규정을 통하여 정하며 규정에 위반한 사업자의 행위에 대하여는 징계권을 행사한다.[13] 최근에 정치학과 법사회학에서는 SRA가 공동체의 상이한 단체나 조직들과의 제도적 연결고리로서 역할을 수행하는 일종의 중재적 권력(intermediary power)으로서의 위상을 가진 것으로 보고 있다. 중재적 권력으

12) 김순양, 작은 정부로 가는 길(Ⅳ)-규제개혁과 자율규제-, 지방자치 112호, 1998.1, 119면.
13) 김성수, 「금융감독법」상 자율규제에 관한 연구, 공법연구 제34집 제1호, 2005. 11. 355면.

로서의 SRA는 '사익을 추구하는 작은 정부'라는 개념으로 설명될 수 있는데 이들이 기본적으로는 자신의 이익을 추구하는 사적 단체이기는 하지만 때로는 사회공동체 내에서 공적인 기능을 수행하면서 결과적으로는 공공정책의 목표를 실현하는데 결정적인 역할을 가지는 것으로 평가하고 있다. 여기에서 SRA가 공적인 기능을 가지고 공공정책을 실현한다는 것은 공동체 내에서 통용되는 구속력 있는 의사결정권을 국가기관과 공유한다는 것을 의미한다.[14]

오늘날 다원화된 사회에서는 국가와 개인 간에 수직적인 법률관계 자체가 성립할 수 없으며 정치는 물론 경제, 법률, 종교 등 모든 사회의 제도들이 극도로 분화되어 있기 때문에 국가와 개인 간의 수직적 법률관계를 대신하여 사회의 다양한 영역에서의 공존이라는 개념이 성립한다. 그러므로 SRA은 공동체의 중요한 작동요소들, 예를 들어 국가, 시장, 자치단체 등 다양한 영역에서 수평적인 방식으로 중재권을 행사한다고 볼 수 있다.[15]

나. 기능적 자치행정 방식

자율규제 가운데 가장 공적 특성이 강하고 강력한 규제권한을 부여하는 방식으로서 당해 규제임무를 위한 별도의 법인인 자율규제기관을 설립해서 자율규제를 하는 방식이다.[16] 이 기능적 자치행정의 주체는 자율적인 규범, 즉 자치규칙의 제정권을 가지는 경우가 많다.[17] 기능적 자치의 특징은 사회의 개별 영역들이 자신의 업무처리에 있어서 정당하다고 생각하는 규범 외에는 이를 준수하려고 하지 않기 때문에 일종의 닫힌 구조를 지향한다. 이러한 법의 폐쇄성을 극복하고 사회의 다양한 자치

---

14) 김성수, 위의 논문, 356면.

15) Teubner, Polycorporatism in Germany (1993) Brighham Young University Law Review p.553; H. Willke, Societal Guidance through Law? in: Teubner/febaarajo (eds), State, Law, Economy as Autopoeitic Systems (Milan: Guiffre, 1992), pp. 51-52.

16) 예를 들면 특정한 공공목적을 달성하기 위하여 관계법령에 의하여 설립된 공단이나 공사 등의 특수법인이 관계법령에 의하여 지도, 검사, 조사, 교육, 영업정지 등의 행정처분 등을 자율적으로 규제할 수 있게 하는 것이다. 예를 들면 「액화석유가스의 안전관리 및 사업법」의 규정에 의한 액화석유가스충전사업 허가사업자, 액화석유가스사용자 등에 대한 시·도지사 또는 시장·군수·구청장의 권한 중 안전성 확인, 검사, 위해방지를 위한 조치명령, 시설 등의 사용정지명령 등의 규제를 「고압가스 안전관리법」에 의하여 설립된 한국가스안전공사가 자율규제 할 수 있도록 하고 있다.(「액화석유가스의 안전관리 및 사업법」 시행령 제19조).

17) 이원우, 앞의 논문, 383면.

기관들을 통합하는 기능을 가지기 위해서는 개별 자치기관들이 사회적 환경에 반응할 수 있도록 법의 역할이 재정립될 필요가 있다.[18]

다. 공무수탁사인에 의한 자율규제

규제 임무를 수행할 공적주체를 새로이 설립하지 아니하고 사인 가운데 당해 임무를 적절히 수행할 자를 선정하여 그에게 공적임무의 수행을 맡겨서 규제를 하는 방식이다. 공적 규제임무를 수행하는 사인은 다음의 2가지의 경우로 구분되는데 공법상의 규제권한을 독립적으로 자신의 이름으로 행사하는 경우를 공무수탁사인이라고 하고, 그렇지 않은 경우를 행정보조자라고 한다. 공무수탁사인의 경우는 입법적 조치이든 행정적 조치이든 일정한 공적 조치에 의하여 공적 규제임무를 사인이 수행하게 되며 이러한 사인의 공적 규제임무는 일정한 법적 효과를 부여받게 된다.

라. 사업자단체에 의한 자율규제

민간단체인 사업자단체(협회)에 행정의 고유권한인 권력적 행정규제를 수행하게 하는 자율규제로서 이것은 주로 조사, 검사, 검정, 시험, 등록, 교육 등의 행정기관의 권력적 규제권한 및 비권력적 사실행위 등을 사업자단체(협회)에 민간위탁의 형식으로 행사할 수 있게 하는 사인에 의한 행정의 한 유형인 것이다. 이 경우의 자율규제는 민간기업 사이에 협정 또는 행정과 민간 사이에 협정 또는 협약을 체결하여 일정한 행위에 대한 규제를 하는 방식으로서 기업 내부에서 자율준수 프로그램을 만들어 자율규제를 하는 방식도 있다고 한다.[19] 현행 법령의 입법례를 살펴보면 관광진흥법에 의하여 설립된 지역별 관광협회는 관광편의시설업 중 관광식당업·관광사진업·여객자동차터미널시설업 및 관광토속주판매업의 지정 및 지정취소에 관한 문화관광부장관의 권한을 행사할 수 있는데(관광진흥법시행령 제65조), 이는 사업자단체(협회)의 자율규제의 유형에 속한다.[20] 이러한 사업자단체에 사업자에

18)Teubner, After Legal Instrumentalism? Stratetigic Models of Postregulatory Law in: Teubner (eds), Dilemma in the Welfare State (Berlin de gruyter, 1985)
19) 이원우, 앞의 논문, 383면.
20) 변호사로서 개업하려면 「변호사법」에 의하여 변호사협회에 등록을 하여야 하고 만약 등록이 거

대한 권력적 행정권한을 위탁하여 자율규제 할 수 있게 한 것은 사업자단체가 자율규제를 빌미로 사업자를 과도히 통제할 우려가 있는 점, 사업자단체와 사업자는 모두 규제의 대상임에도 스스로 위탁대상 행정업무를 실제 수행하게 되어 공정성의 확보가 곤란한 점 등의 이유 때문에 바람직하지 않다는 견해도 있다.[21]

6. 개별법상의 자율규제의 입법형태

가. 자율규제에 대한 입법형태

1) 법정자율규제

행정법 분야의 자율규제란 행정규제권한을 민간에 맡겨서 처리하는 것으로서 사인에 의한 행정이라고도 부를 수 있다. 이러한 사인에 의한 행정은 결국 행정권한의 민간위탁의 한 유형으로 인식되는 것이 일반적이기 때문에 자율규제의 방법은 통상 행정권한의 민간위탁의 방식을 그 예로 들 수 있다. 이에 의하면 행정권한의 자율규제의 방법은 법정자율규제와 지정자율규제로 나눌 수 있을 것이다. 이 가운데 법정자율규제는 위탁되는 행정권한과 수탁자를 법령으로 정하는 것이다.[22] 그

부되면 변호사로서 개업을 할 수 없게 한 변호사법 제7조 (자격등록)와 제8조 (등록거부)도 사업자단체에 의한 자율규제의 유형으로 볼 수 있는데 변호사협회를 일반 사업자단체로 보기 보다는 공공조합으로 보는 견해에 따른다면 특수법인에 의한 자율규제의 예를 적용할 수 있을 것이다.
「변호사법」
제7조 (자격등록)① 변호사로서 개업을 하려면 대한변호사협회에 등록을 하여야 한다.
제8조 (등록거부)① 대한변호사협회는 제7조제2항에 따라 등록을 신청한 자가 다음 각 호의 어느 하나에 해당하면 제9조에 따른 등록심사위원회의 의결을 거쳐 등록을 거부할 수 있다.

21) 김재규, 행정권한의 위임·위탁·대리·대행 관련 입법모델 검토, 입법모델 제2집, 법제처, 2002, 12. 340-341면 참조.

22) 「자본시장과 금융투자업에 관한 법률」 제286조 (업무) ① 협회는 정관이 정하는 바에 따라 다음 각 호의 업무를 행한다.
1. 회원 간의 건전한 영업질서 유지 및 투자자 보호를 위한 자율규제업무
2. 회원의 영업행위와 관련된 분쟁의 자율조정(당사자의 신청이 있는 경우에 한한다)에 관한 업무
제377조 (업무)
10. 유가증권시장·코스닥시장 및 파생상품시장 등에서의 매매와 관련된 분쟁의 자율조정(당사자의 신청이 있는 경우에 한한다)에 관한 업무

런데 법률 자체에서 직접 정부의 사무처리 권한을 민간단체 등에 부여하는 것은 입법론으로서는 바람직하지 않다고 하는 견해가 있다.[23]

2) 지정자율규제

지정자율규제는 법령에 위탁의 근거를 두고 이에 근거하여 행정기관과 수탁자가 위탁계약의 체결을 통하거나 행정기관이 수탁자를 지정함으로써 성립하는 것이다.[24]

나. 자율규제수단의 유형

행정법 분야의 자율규제수단의 유형으로는 자기인증, 신고, 교육, 조사, 검정, 검사, 등록 등이 중요한 내용들이다.[25] 그런데 이들 행정작용들은 사실행위에 해당하는 것도 있으나 대부분 규제적 성질을 가진 권력적·명령적 규제행정행위에 해당하는 것도 다수 포함되어 있다.

1) 자기인증제도

종래에 행정처분 형식으로 행하여져 오던 형식인정이나 법규명령 또는 행정규칙 형식으로 된 안전규격·기준을 근거로 행정이 직접 규제하여 오던 안전성 기준 등을 행정적 관여를 배제한 채 사업자 내지 사업자단체(협회)가 자율적으로 안전규격·기준을 규제하는 제도가 자기인증제도이다. 자기인증제도는 규제가 전혀 없는 것은 아니고 기업이 제조한 물건 등에 대하여 행정이 법령에 의해 허가나 승

---

23) 윤장근·우병렬, 사업자단체에 대한 행정권한위탁의 현황 및 문제점, 법제개선연구 제3집, 법제처, 1997, 17-20면 참조.

24) 「산업안전보건법」 제65조 (권한의 위임·위탁) ①생략
②노동부장관은 이 법에 따른 업무 중 다음 각 호의 업무를 대통령령이 정하는 바에 따라 공단·비영리법인 또는 관계전문기관에 위탁할 수 있다.
1. - 7. 생략
8. 제36조제1항에 따른 안전검사

25) 김승열, 정부업무민간위탁의 한계와 공정성 확보방안, 법제, 법제처, 2000. 9, 62-63면 참조.

인 등을 하는 것이 아니라 기업이 스스로 법령상의 규격이나 기준에 맞는 제품을 생산하면 행정에 허가나 승인 등을 받을 필요 없이 바로 그 안전성, 품질 등을 담보하여 시장에 출하할 수 있는 제도를 말한다.[26]

자기인증제도는 민간단체가 스스로 결정한 기준이 법령에서 규정한 규제와 유사한 규제기준의 효과를 발생시키는 경우도 있다.[27]

이러한 자기인증제도는 일반적으로는 안전성 등이 확보되어 있다면 괜찮지만 경우에 따라서는 규격자체가 충분한 기능을 할 수 없는 경우는 물론 과잉규제로 되는 경우도 있을 수 있고 자기인증자체가 행정규제보다 고비용을 수반하는 경우[28]도 있을 수 있다.

2) 신고의 접수(수리)

순수한 신고영업의 경우 특정 사실의 통지에 해당한다. 신고에 대해 행정청을 대신하여 사업자단체(협회)가 자율규제권의 일종으로 이 영업신고수리를 거부할 수 있는 권한이 법령에 의해 주어져 있거나 사업자단체(협회)가 영업신고를 수리하더라도 신고영업자의 영업상 의무의 준수여부를 감독하여 위반시 행정제재를 부과하는 경우에는 신고가 완화된 허가로서의 본질을 갖고 있다. 또한 신고영업과 관련된 행정조사, 행정처분 등의 업무는 대부분 행정행위의 성질을 가지고 있다고 하겠다.

3) 등록

등록업무도 신고의 경우와 유사하다. 등록은 단순한 확인행위로서의 성질을 갖지만 등록영업인 경우에는 약화된 허가영업으로서의 성질을 갖고 있으므로 권력

---

26) 米丸恒治, 行政介入の手法と規制緩和, ジュリスト1082호, 1996. 25면.

27) 일본의 경우 수도의 급수장치에 JIS규격(일본공업규격)이 없는 것에 대해서 사단법인일본수도협회가 형식심사기준을 정하고 이에 근거해서 형식인정 등을 하고 이 형식인정을 받은 장치의 사용이 조례 등의 수도의 공급규정에 의해 정해짐으로써 규제효과가 발생하는 경우이다.

28) 일본의 경우 자기인증대상상품을 민간의 제3자기관이 인정마크를 붙이는 경우가 국가의 형식승인의 경우보다도 시험료가 비싸지는 문제점이 있다고 한다.

적 행정작용이라 할 수 있는데[29], 사업자의 영업의 등록 및 등록취소 등의 권한이 법령에 의해 사업자단체(협회)에 주어져 있는 경우는 이 사업자단체(협회)에 등록하여야 사업자가 사업을 할 수 있는 자격이 생긴다.[30]

4) 조사

행정조사[31]를 의미하는 조사에는 세무조사와 같은 권력적인 것이 있는 반면에 비권력적인 것도 있어서 일률적으로 말할 수는 없지만 권력적인 (행정)조사는 행정법상 행정강제, 행정벌 내지 행정법상의 의무이행확보수단 등 행정의 실효성확보수단의 하나[32]로서 규제적인 성격을 갖고 있는 것이라고 보는 것이 타당할 것이다.

사업자단체(협회)에 이러한 행정조사권한이 자율규제의 내용으로서 부여되어 사업자단체(협회)가 자율적으로 회원사를 조사하게 되면 회원사는 관계법령에 의하여 수인의무를 부담하고 사생활이 침해되는 등 불이익을 받게 되므로 규제적인 것이 된다. 따라서 행정조사를 행하는 사업자단체(협회)가 조사 권한을 가지고 있음을 명백히 하기 위하여 행정조사를 하는 자에게 권한의 표시로서 증표를 제시할 것을 규정하는데 이러한 증표의 제시는 행정조사의 요건을 이루는 것이고 증

---

29) 2002년 11월 정부가 보험업법 개정안을 국회에 제출하였는데, 당초 주무부처가 마련한 원안에는 보험설계사·보험대리업 및 보험중개업의 등록, 영업정지 명령 및 등록취소권한을 각각 보험협회 및 금융감독원에 부여하는 내용이 포함되었다. 심의과정에서 보험협회는 보험회사가 설립한 사업자단체로서 순수민간단체이고, 금융감독원은 「금융감독기구 설치 등에 관한 법률(현 '금융위원회의 설치 등에 관한 법률')」에 의하여 설치된 무자본특수법인으로서 금융감독위원회의 지시를 받아 금융기관에 대한 조사업무를 수행하고 있는데, 등록 및 등록 취소업무는 직업선택의 자유와 관련이 있는 전통적이 공권력의 행사인바, 법률에서 행정기관이 아닌 사업자단체 또는 금융감독원에 그 권한을 직접 부여하는 것은 「정부조직법」 등에서 규정한 행정업무 수행방식의 기본체제와 부합하지 않은 문제점이 지적되었다. 그 결과, 이들 업무는 원칙적으로 「정부조직법」 제6조의 규정에 의하여 민간위탁의 대상도 되지는 아니하나, 동 행정권한을 금융감독위원회의 권한으로 하고 금융감독위원회가 그 권한의 일부를 위탁하는 형식을 취하도록 하였다(안 제84조 내지 제90조, 제196조 참조).

김재규, 앞의 논문, 339면 참조.

30) 앞의 주 23)의 「변호사법」 제7조 및 제8조 참조.

31) 행정조사에 관한 일반법으로는 「행정조사기본법」이 있는데 동법 제2조 제1호는 행정조사를 "행정기관이 정책을 결정하거나 직무를 수행하는데 필요한 정보나 자료를 수집하기 위하여 현장조사, 문서열람, 시료채취 등을 하거나 조사대상자에게 보고요구, 자료제출요구 및 출석, 진술요구를 행하는 활동"으로 규정하고 있다.

32) 홍정선, 행정법원론(상), 박영사, 2008, 601면.

표의 제시로서 피조사자는 수인의무를 지게 된다.[33]

5) 검정

「소방기본법」 제45조에 의한 소방기구검정은 직접 국민에게 권리·의무에 직접적인 영향을 미치는 사무라고 이해되고 있다.

제3절 정보통신망의 특징에 따른 자율규제의 도입

1. 인터넷상의 자율규제의 등장배경

국가는 전통적인 강제적 법규범의 형성과 유지라는 본연의 임무를 띠고 있는 주체이다. 이러한 국가의 의무는 공익이라는 개념에 의해서 정당화된다. 물론 국가의 공익추구활동은 '공권력'이라는 개념으로 포섭되는바, 이러한 공권력의 행사는 헌법적 한계 내에서 이루어져야 한다는 법치주의의 한계에 의해 제한을 받지만, 특히 국가안보, 사회질서의 유지, 이용자 및 소비자의 보호, 유해정보로부터의 청소년의 보호 등은 인터넷 환경에서 그 정당성이 인정되는 공익개념이라 할 것이다. 둘째, 시장영역은 인터넷기업들에 의해서 주요 형성되는 영역이라고 할 수 있다. 인터넷시장이 지금보다 보다 확대되고, 보다 많은 이용자들이 인터넷을 이용하기 위해서는 인터넷상의 역기능들을 해소할 수 있는 규제시스템이 필요하다. 셋째, 민간영역에서의 또 다른 정보주체인 이용자는 인터넷이 등장하면서 기존의 오프라인상의 매스미디어와는 달리 매체의 특성으로 인해 자신의 정보통제능력이 매우 강화되어 있다. 이러한 측면에서 인터넷은 기존의 매체와는 다른 속성을 가지고 있는 것으로 평가되어 왔고, 규제시스템의 개발에서도 이용자의 존재를 무시한 시스템은 거의 상상하지 못하고 있는 실정이다.

---

33) 영장주의와 관련하여 영장이 필요하다는 견해와 필요치 않다는 견해가 나뉜다.

2. 인터넷 콘텐츠에 대한 규제의 정책적 목표

인터넷 내용규제시스템이 규제의 정책적 목표(인간 존엄성과 청소년의 보호)와 인터넷상의 표현의 자유를 가능한 조화시키기 위해서는, 규제 대상의 상이한 유형들(불법 콘텐츠와 유해 콘텐츠)이 먼저 고려되어야 할 것이다. 또한 인터넷 콘텐츠에 대한 규제적 접근은 각기 다른 차원(정보이용자, 정보제공자/정보제공자 단체들, 국가 및 규제기관의 수준)에서 다양한 장치들의 도입을 필요로 한다. 따라서 정부가 주도하는 법적 규제의 단일한 시스템보다는 사회공동체 기반 혹은 인터넷 관련 제영역이 분권적으로 참여하는 다중적인 시스템, 즉 공동규제시스템(co-regulatory system) 또는 이중적 인터넷 규제시스템(dual system of internet regulation)이 위와 같은 인터넷 규제의 기본방향에 보다 부합한다고 할 것이다.

3. 인터넷상의 자율규제의 이론적 근거

가. 인터넷 매체의 특성에 따른 규제의 차별화

인터넷을 통해 제공되는 새로운 커뮤니케이션 및 정보 서비스들과 세계화의 확대는 이 새로운 기술이 매체규제의 공익적 목표들에 도전하고 있음을 잘 보여주고 있다. 하지만 매체규제의 공익적 목표들은 기술적 변화의 결과로 무의미해지거나 사라지지 않는다. 따라서 이러한 도전이 의미하는 바는 매체규제가 보호하고자 하는 사회적 공익을 구현할 수 있는 적절한 입법과 규제 장치들이 개발될 필요가 있다는 사회적 요구, 즉 규제방식의 변화에 대한 요구로 이해되어야 할 것이다.
그러한 규제방식의 변화는 무엇보다 인터넷 매체의 특성을 충분히 고려해야 한다.[34]

잘 알려져 있다시피, 인터넷은 개방적이고 탈중심적이며 국제적인 네트워크 구조를 지니고 있다. 이러한 네트워크의 구조를 통해 인터넷을 이용하는 의사소통은

34) 이러한 관점에서 어느 정도 설득력 있는 매체규제논리 내지 매체규제이론으로 등장한 것이 바로 '매체특성론' 내지 '매체특성론적 접근방법(a medium-specific analysis)'이라고 할 것이다. 자세한 것은 황성기, "언론매체규제에 관한 헌법학적 연구－방송·통신의 융합에 대응한 언론매체 규제 대응 내지 개선 방안", 서울대학교 법학박사학위 논문(1999.8.), 12~15쪽 ; 황성기, "사이버스페이스와 불온통신규제", "헌법학연구", 제6권 제3호(2000.11.), 한국헌법학회, 176~179쪽 참조.

쌍방향성, 보편적인 접근가능성, 국제성을 띠게 된다. 우선 인터넷의 쌍방향성은 표현물의 유통과정에서 제공자와 이용자의 벽을 허물어 버린다. 본질적으로 수용자인 동시에 제공자이기도 한 인터넷 이용자들은 과거의 매체에서 누려보지 못했던 수준의 권한을 부여받는다. 이러한 상황은 콘텐츠규제가 매체의 기술과 정보전달방식뿐만 아니라 이용자들이 그것을 수용하는 특징을 주요하게 고려해야 함을 의미한다.

또한 보편적 접근가능성은 기존의 법·제도로 통제할 수 있는 인터넷 콘텐츠의 범위를 심각하게 제한하여, 정보이용자들이 법·제도의 진공상태를 경험하게 하는 소위 브로큰 윈도우 효과(broken window effect)를 낳고 있다.[35] 또한 인터넷의 초국가적이고 국제적 특성은 한 나라의 법과 제도로는 정보의 국제적 영향력을 통제할 수 없는 상황을 연출한다. 이러한 상황에서, 매체의 특성을 고려하지 않는 인터넷 콘텐츠 규제는 일단 공익적 목표를 달성할 수 없는 실효성의 문제에 직면하게 된다. 뿐만 아니라 역으로 과도한 규제를 결과하여 인터넷이 지닌 풍부한 가능성을 제한할 위험성을 내포하게 된다.

따라서 효과적인 인터넷 콘텐츠규제시스템은 인터넷의 개방적이고 탈중심적인 네트워크 구조를 지원할 뿐 아니라, 역동적이고 지속적인 혁신과 새롭게 개발되는 기술들에 대해 융통성 있게 대응할 수 있도록 해야 한다. 이러한 매체환경의 변화에 잘 부합하는 규제방식으로서 설득력 있게 제기되고 있는 것이 바로 인터넷콘텐츠 자율규제시스템이다.

자율규제시스템은 강제적인 정부의 딱딱한 규제에 비해 급격하게 진행되고 있는 기술의 발전 속도에 적절하게 대응할 수 있는 장점을 지니고 있다. 또한 일반적으로 자율규제의 장점으로 지적되고 있는 효율성, 융통성, 준수의 자발성제고, 사회적 비용의 절감 등도 인터넷 콘텐츠 자율규제의 중요한 근거로 제시될 수 있을 것이다.[36]

---

35) Herbert Burkert, “The Issue of Hotlines”, in Jens Walterman & Marcel Machill(eds.), Protecting Our Child on the Internet : Toward a New Culture of Responsiblity, Bertelsmann Foundation Publishers, Güersloh,2000, pp. 271-272. 기존의 규제방식을 통해 통제할 수 없는 불법정보들이 인터넷에 많이 존재한다는 사실은 이미 인터넷을 이용하는 모든 사람들이 잘 알고 있는 사실이다. 불법정보를 빈번하게 접촉하거나 그렇지 않더라도 불법정보가 존재할 수 있다는 사실을 반복적으로 접하거나 이용가능한 상황은, 이용자들로 하여금 인터넷에서 현실 공간의 법을 지키지 않아도 된다는 확신을 가지게 한다. Burkert는 무질서에 대한 확신이 또 다른 무질서를 양산하는 이러한 상황을 브로큰 윈도우 효과라고 정의하고 있다.

36) 인터넷 콘텐츠와 관련한 자율규제의 장점에 대해서는 Jens Waltermann & Marcel Machill(ed.), Protecting Our Children on the Internet : Towards a New Culture of Responsibility, Bertelsmann Foundation Publishers, Güersloh, 2000, pp.35-36 참조.

나. 공적 규제의 한계

인터넷서비스 관련 공적규제는 빠르게 변화하는 인터넷서비스 및 기술적 특성을 반영하는데 한계가 있다. 과도한 법적 제재는 인터넷서비스 기업의 신규 서비스 발굴 및 시장진입을 제한하여 인터넷산업의 발전을 저해할 수 있기 때문이다.
또한, 최근 사이버모욕죄 도입논란은 표현의 자유를 고려하지 않은 지나친 규제강화라는 비판적인 견해가 존재하고 있는 것도 공적규제가 가해지기 어려운 상황을 말하고 있다.

4. 인터넷상의 자율규제의 주체

가. 사업자단체에 의한 자율규제

사업자 자율규제는 특정한 산업 전체의 범위에서 행해지는 규제과정으로, 회사의 수준에서 자발적으로 행해지는 개별적인 규제행위들과는 다르다. 사업자 자율규제(industry self-regulation)는 특정 산업 전체를 포괄하는(혹은 대표성을 인정받을 수 있는) 조직이 해당 산업에서 개별 회사들이 준수해야 할 사업방침과 관련된 규범 및 기준을 정하고 회원사들이 그것을 준수하는 규제과정으로 이해될 수 있다.[37]

사업자들의 이러한 자발적 행동을 기대할 수 있는 것은, 사업자 자율규제에 대한 분명한 경제적 동기가 존재하기 때문이다. 인터넷이 사회, 특히 학부모들에게 수용되기 위해서는 반드시 이용자에게 안전한 장소가 되어야 하기 때문에, 불법 및 유해콘텐츠에 대해 자발적인 조치를 취하는 일은 전체적인 인터넷사업자들의 경제적 이해관계에 부합한다.

또한 사업자 자율규제의 동기에는 인터넷의 불법 및 유해콘텐츠와 관련된 법적 상황도 포함될 수 있다. 인터넷을 이용하는 인구가 급격하게 증가하면서, 거의 모

37) Price & Verhulst, "The Concept of Self-Regulation and the Internet Content", in Jens Walterman & Marcel Machill(eds.), Protecting Our Child on the Internet : Toward a New Culture of Responsiblity, Bertelsmann Foundation Publishers, Güersloh, 2000, p. 156.

든 인터넷 이용국가의 법원들은 인터넷 콘텐츠에 대한 인터넷사업자의 책임을 점점 더 엄격하게 적용하려는 경향을 보이고 있다. 많은 사업자들에게 자율규제는 이러한 '속죄양식의 책임부과 체제'에서 벗어나기 위한 최선의 선택으로 받아들여지고 있다. 사업자들이 효과적이고 합리적인 책임의 틀을 스스로 구성한다면, 정부 역시 그들에게 예측 가능한 법적 환경을 제공할 수 있을 것이라고 기대할 수 있기 때문이다.

하지만 사적 이익을 추구하는 개별 사업자들은, 한편으로는 해당 산업의 도덕적 대의와 사회적 책임에 공감하면서도 다른 한편으로는 시장에서의 경제적 이익을 추구하는, 상반된 경향을 띠게 된다. 개별 사업자의 차원에서 행해지는 자율규제는 정부의 관심을 끌어내거나 기존의 법·제도적 틀의 변화를 가져오지 못할 것이다. 또한 인터넷 관련 산업 전반에 적용될 수 있는 표준적인 규범과 절차가 없는 자율규제는 규제과정에서 의미를 지닐 수 있는 법집행기구와의 파트너십을 구축하지 못할 것이다.

따라서 개별적 사업자들의 이해관계를 넘어 해당 산업의 윤리적 관행들의 촉진을 보장할 수 있는 수단이 필요하다. 일반적으로 이러한 사업자 자율규제는 자율규제기구로서의 사업자협회를 통해 구현되고 있다. 세계적으로 가장 거대한 인터넷사업자협회인 범유럽 인터넷서비스 제공자협회(EuroISPA : the pan-European association of the Internet Service Provider)를 비롯하여, 독일의 멀티미디어 서비스 제공자 자율규제협회(FSM : Freiwillige Selbstkontrolle Multimedia Diensteanbieter), 일본인터넷협회(IAJapan : Internet Association Japan) 등이 사업자 자율규제를 실행하고 있는 사업자협회들이다. 이들 협회는 불법 및 유해콘텐츠의 자율규제절차에 대한 상세한 지침을 포함하는 사업자행동강령[38]을 제정하고 회원사들의 강령준수를 감독하여 사업자의 사회적 책임을 담보한다. 또한 이들은 불법 및 유해콘텐츠에 대한 자율규제 장치들(인터넷 핫라인, 인터넷내용등급시스

38) 사업자행동강령은 영어권에서 'code of conduct' 혹은 'code of practice'로 표기되는데, 일반적으로 이는 관련 산업의 행동규범을 포괄적으로 규정하는 윤리강령(code of ethics)과는 달리 회원사들이 지켜야 할 구체적인 행동지침을 의미한다. 행동강령과 윤리강령이 차이에 관해서는 다음을 참조할 것이다. Jacques Berleur, "Self-Regulation : Content, Legitimacy, and Efficiency : Governance and Ethics", INET 2001 Conference Proceedings, ISOC, Stockholm.(http://www.isoc.org/isoc/conferences/inet/01/CD_ proceedings/G06/Berleur.htm).

템 등)을 운영 혹은 (재정)지원하는 일을 한다. 이들이 운영하거나 (재정)지원하는 인터넷 자율규제 장치들은 해당 국가의 법·제도적 내용규제절차와 협력하거나 그 규제절차의 일부로서 작용함으로써, 정부의 과도한 규제로부터 인터넷사업자들을 보호한다.

그런데 사업자들의 이러한 노력이 전체적인 인터넷 콘텐츠 규제과정에 긍정적인 영향을 미칠 수 있도록 하기 위해서 중요하게 등장하는 것이 바로 정부의 역할이다. 즉 사업자 및 이용자에게 안전한 사업 환경 및 법적 환경이 조성될 수 있도록 사업자 자율규제를 승인하는 일과 앞서 언급했던 자율규제의 한계를 극복할 수 있도록 감시·보완하는 일을 바로 정부가 수행해야 한다는 점이다.

나. 정부의 역할

자율규제에 대한 정부의 역할은 자율규제의 내용과 기능을 결정하는 데 있어서 가장 중요한 문제라고 할 수 있다.

이 문제를 다루기 전에 분명히 해두어야 할 것은 자율규제와 정부규제 간의 관계 문제다. 자율규제의 사회적 원천이 무엇인가의 문제, 다시 말해 자율규제가 정부의 적극적인 개입의 결과인지 아니면 정부와 사업자가 협력하는 시민문화의 결과인지는 자율규제가 작동하는 사회적 환경에 따라 달라질 수 있다. 하지만 분명한 것은 자율규제가 특히 매체와 커뮤니케이션 분야에 있어서 정부규제를 완전히 대신할 수 없다는 점이다.

자율규제가 성공적으로 정착하더라도, 인터넷 콘텐츠와 관련된 법적 시스템을 보호하는 궁극적인 책임은 정부에게 있다는 사실은 재론할 필요가 없다. 공공의 안녕과 사회적 안전이 염려되는 경우, 정부는 당연히 법적인 조치를 취해야 하며, 그러한 정부의 정당한 역할을 자율규제 절차가 대신해 줄 수는 없을 것이다. 다시 말해 자율규제는 정부규제의 대체물이 아니다.

오히려 정부는 새로운 디지털기술의 등장과 인터넷의 국제적 성격 때문에 전통적인 방식으로는 인터넷의 불법·유해콘텐츠에 적절하게 대응하지 못하게 된 규제환경에서, 내용규제의 정책목표를 달성하기 위해 인터넷 자율규제가 지니고 있는

여러 가지 장점들을 적극적으로 활용해야 할 필요가 있을 것이다.

이는 결국 내용규제의 목표인 사회적 공익을 달성하기 위해 정부의 개입이 필요하고 또한 그러한 정부의 개입을 매개로 하는 구체적인 상호작용이 필요하다는 점을 의미한다.

그런데 현재의 규제환경에서 자율규제시스템이 배태되고 성장하기 위해서는 규제기관[39]의 권한행사가 예측가능성을 담보해야 한다. 그리고 예측가능성을 보장하기 위해서는 규제기관이 보유하고 있는 규제권한의 융통성 있고 신중한 행사가 필요하다. 규제기관에 의한 규제권한의 발동이 융통성 있고 신중하게 이루어져야 하는 이유는, 그 운영의 경직성이 자율규제의 정착을 위한 토대 마련에 있어서 악영향을 미칠 수 있기 때문이다.

규제기관의 권한행사에서 예측가능성이 보장되어야 하는 또 다른 이유는 행동강령에 의한 자율규제나 자율심의가 정착될 수 있도록 하기 위한 기본전제가 되기 때문이다. 즉 행동강령은 자율규범이기 때문에, 행동강령에 의한 자율규제나 자율심의가 이루어진다고 하더라도, 그 자체로 법집행의 대상에서 면제되는 것이 아니다. 다시 말하면 행동강령에 의한 자율규제나 자율심의가 이루어졌다고 하더라도, 콘텐츠의 내용에 대한 법적 책임이 면책되는 것은 아니다. 따라서 이 점은 바로 자율규제의 한계로서도 작용하는데, 결국 자율규제가 정착되기 위해서는 규제기관의 합리적인 권한행사가 필수적이게 되는 것이다.

다. 제3자 및 이용자 영역

인터넷 콘텐츠규제와 관련하여 시민단체 및 이용자(단체)의 역할은 상세히 다루어지지 않아 왔던 문제들 중의 하나다. 즉, 아직까지는 민간단체 혹은 이용자(단체)의 자율규제 관련 활동에 관한 체계화된 논의들이 존재하지 않는다.

이에 관해서는 여러 가지 원인을 지적할 수 있을 것이다. 먼저 그간의 인터넷 콘텐츠규제가 정부 주도로 진행되어 오면서, 정부 이외의 영역이 정부규제의 객체에 머물러 왔다는 근본적인 문제점이 지적될 수 있을 것이다. 이와 아울러, 민간단

39) 여기서 규제기관이란 검찰 등의 사법기관뿐만 아니라 각종 위원회 등의 각종 심의기관들을 포함하는 개념이다.

체들 역시 인터넷 콘텐츠규제에 대한 관심이 아직은 부족하여, 자율규제와 관련된 민간단체의 영향력 있는 활동이 부족하다는 점도 들 수 있을 것이다. 또한 민간단체의 인터넷 콘텐츠규제 관련 논의가 정부규제에 대한 비판에만 머물러 왔다는 점도 규제역량의 문제와 관련하여 지적할 수 있는 문제점이다.

그럼에도 불구하고, 인터넷 매체의 특성을 고려할 때, 인터넷 콘텐츠규제와 관련된 민간단체 및 이용자(단체)의 역할은 매우 중요하다. 우리가 잘 알고 있다시피, 인터넷은 쌍방향적인 매체이다. 인터넷 의사소통구조의 쌍방향성은 이 매체에서 이용자들이 정보의 소비자이자 생산자, 서비스의 고객이자 제공자로서 기능할 수 있도록 한다. 따라서 이 새로운 매체의 윤리 및 규범과 관련하여 이용자들의 역할은 거의 절대적일 수밖에 없다.

자율규제절차들은 이러한 이용자들의 새로운 역할을 배제해서는 안 되며, 또한 배제할 수도 없을 것이다. 이용자의 역할문제와 관련하여, 자율규제시스템은 이용자의 역할증대를 콘텐츠규제의 부정적인 조건으로 보지 않고 긍정적인 조건으로 이해해야 한다. 이러한 이해는 자율규제에 있어 하나의 원칙을 구성하는 바, 자율규제 장치들은 이용자의 권한 및 역할강화를 궁극적인 목표로 설정해야 한다는 것이다.

예를 들어 인터넷이용자는 인터넷 콘텐츠에 대한 이의제기를 통해 인터넷사업자에게 압력을 가할 수 있다는 점에서, 자율규제시스템의 중요한 부분을 담당한다. 따라서 인터넷이용자의 적극적인 참여는 자신들이 단지 인터넷의 수혜자가 아닌 인터넷 발전의 한 축을 담당하는 참여자로서의 책임을 다 할 수 있다. 이런 점에서 관련 민간단체들 역시 이용자들의 정보소비자로서의 요구를 자율규제 과정에 적극적으로 구현할 수 있는 중요한 원천이 될 수 있을 것이다.

5. 정보통신 분야에 있어서 자율규제의 입법적 과제

가. 자율규제에서의 입법의 역할

자율규제에 관한 입법은 사업자의 자율규제의 역량을 강화하거나 자율규제기반

을 조성하는 역할을 해야 할 것이다. 이를 위해서 중요한 것은 사업자의 법적 책임의 한계를 명확히 하는 것인데 그 내용은 자율규제의 기반조성을 위해 면책의 범위를 분명히 제시하여야 한다는 것이다.[40]

나. 공동규제의 검토

자율규제를 위탁한 범위 내에서는 정부(행정)규제를 제외하거나 아니면 정부(행정)규제와 자율규제를 동시에 행하는 방안 등을 검토할 필요가 있다. 정부가 자율규제기관의 설립에 상당한 법적인 영향력을 행사하는 '명령적', '제재적', '강제적' 자율규제[41]를 공동규제의 범주에 포함시키는 견해도 있다.[42]

정부(행정)규제와 자율규제를 동시에 행하는 방안으로서 자율규제기관이 준수하여야 할 행동규약의 근거와 기준을 법에서 규정하고 구체적인 내용은 자율규제기관이 정하도록 하여 이를 준수하도록 하는 방안이 있다. 즉 법에서 자율규제 준수에 따른 법적 책임의 한계를 명확히 하는 것이야 말로 법제도(=정부규제)와 자율규제의 결합이라고 할 수 있는 공동규제의 전형적인 형태를 갖추는 것이라고 한다.[43]

이에 따라 앞으로 우리나라에서 도입, 추진해야 할 인터넷 내용규제정책은 바로 정부와 시민사회가 공동으로 적극적인 역할을 수행할 수 있는 자율규제시스템의 구축에 초점을 맞추어야 한다.

보다 구체적으로는 정부가 갖고 있는 현재의 규제권한을 축소·분산시킬 필요가 있을 뿐만 아니라, 정부는 시민사회의 자율규제역량을 키우고 자율규제토대를 구축하는데 자신의 역량을 집중시켜야 한다. 이러한 점에서 자율규제 장치 중의 하나인 행동강령을 통한 사업자의 자율규제는 그 중요성이 강조되어야 하고, 이를 위한 시스템 구축의 필요성도 강조되어야 할 것이다.

다. 자율규제기관에 대한 감시 및 평가

---

40) 황승흠, 앞의 논문, 281면.
41) 앞의 3. 자율규제의 분류를 참조.
42) 공동규제의 활용방안에 관한 연구, 한국행정연구원 보고서, 2008. 12. 43면.
43) 황승흠, 위의 논문, 282면.

사업자단체(협회)의 활동상황이나 재정운영상황 등의 관련 정보 등을 의무적으로 공개하게 하는 제도가 필요하다. 감시결과와 적절한 성과평가절차를 거쳐서 자율규제 권한을 무제한으로 인정할 것이 아니라 자율규제 권한을 제한하거나 회수하는 방안을 법령에 규정할 필요가 있다.[44]

제2장 정보통신망에서의 자율규제 현황 및 문제점

제1절 우리나라의 정보통신망 자율규제 현황

1. 우리나라 정보통신망 자율규제

가. 우리나라 자율규제의 체계 및 유형

정보통신망에서의 콘텐츠 및 유형의 다양화로 인하여 기존에 예측하지 못하였던 파급효과들이 나타나게 되었다. 그러한 현상들을 야기하는 기술의 수준과 양태, 그리고 그에 부합하는 사회적·법적 제도들을 생각하지 않을 수 없게 되었다.

일반적으로 규제체계를 크게 나눠보면 정부규제, 시장규제, 자율규제로 구분할 수 있다. 정부규제는 정부가 직접 법률을 강제 집행한다는 점에서 규제의 신속성, 공익성은 높지만 제도적 탄력성이 낮고 규제비용이 높다. 반면, 시장규제는 정부개입 없이 기업의 자기통제를 중심으로 규제가 이루어진다는 점에서 규제비용은 낮지만 제도적 실효성과 중립성의 문제가 발생할 수 있다. 자율규제는 기업, 업계, 제3자 등이 규제주체로 나서는 자발적 동조를 토대로 한다.[45]

일반적으로 자율규제는 정부가 민간단체, 협회, 경제주체 등 비정부영역, 즉 민간의 규제 목적과 그에 부합하는 형식적 권한을 법률에 따라 위임하는 경우를 말하는데, 민간 영역이 규제의 필요성을 자각하여 스스로 규제하는 경우도 이에 해

44) 김순양, 앞의 논문, 121면.
45) 황용석·이동훈·김준교, 전게논문. 110면.

당된다.

자율규제는 이용자, 사업자, 민간기구들이 일련의 장치들을 활용하여 주도적으로 규제에 참여하고 국가와 법률이 이를 협력, 지원함으로써 합리성과 실효성을 동시에 추구한다. 예를 들어, 규제대상이 되는 기업 또는 협회가 자율적으로 규제하는 경우가 이에 해당되며, 법령 또는 그에 준하는 행동규칙의 제정, 규범 집행, 위반시의 제재 등이 포함된다.[46] 이렇듯 자율규제의 문제에 있어 민간부분과 정부의 정책이나 법령과의 관계는 상호적이라 할 수 있다.

또한, 자율규제는 상대적으로 효율성, 융통성의 증진, 규제에 따르는 사회적 비용의 절감, 표현 영역에 있어서 정부 간섭의 최소화 등 여러 장점을 지니고 있지만, 자율규제는 위에서 지적한 대로 수많은 위험과 한계에 노출되어 있다. 이러한 위험과 한계들을 극복하기 위하여 자율규제는 자율규제의 절차에 참여하지 않는 사업자에게도 적용할 방안을 찾아보고, 사회적 합의를 바탕으로 구속력 있는 조치들에 대한 고려를 해보아야 하며, 민주적인 절차를 거쳐 이루어지는 법·제도적 규제와의 적절한 관계를 설정할 필요가 있을 것이다. 따라서 자율규제와 정부규제는 서로 독립적으로 운영되는 것이 아니라 상호보완적인 관계로 운영되는 것이 바람직할 것이다. 우리의 민간영역과 정부영역의 적절한 책임분담을 통한 상호보완적인 규제 혹은 공동규제시스템이 자율규제의 효율적 구현에 있어서 가장 중요한 원리라고 생각한다.[47]

자율규제는 개인·기업·산업계 등이 규제의 주체가 되어 자발적으로 만든 기준 또는 정부가 정한 기준에 따라 스스로 원칙을 정하여 규제의 합리화 및 효율성을 추구하는 방식으로 업계가 스스로 기준을 설정하기 때문에 보다 많은 책임감을 부여함으로써 규제에 솔선수범할 수 있다는 장점이 있다. 또한 정부규제와는 달리 업계가 갖고 있는 전문성을 활용하여 새로운 기술 및 서비스에서 발생하는 이슈에 대해 효과적이고 즉각적인 대처가 가능할 것이다.

정보통신 관련 자율규제에 있어 Price & Verhulst의 구분에 따르면 자율규제를 규제시스템에 정부가 얼마만큼 개입하는가에 따라서 명령적 자율규제와 승인적

46) 황용석·이동훈·김준교, 전게논문, 112면.
47) 황성기·최승훈, 인터넷 콘텐츠 자율규제의 개념과 장치들, 정보와 사회, 제3호, 한국정보사회학회, 2001. 231-232면.

자율규제로 분류할 수 있다. 첫째, 명령적 자율규제(mandated self-regulation)는 민간영역이 정부가 정의하는 틀 안에서 규범을 만들고 그것을 강제하도록 분명하게 요구받는 형식으로 정부가 가장 적극적으로 개입하는 방식이다. 둘째, 승인적 자율규제(sanctioned self-regulation)는 민간영역에서 스스로 규제하되, 정부의 승인을 받는 것이다. 셋째, 조건부 강제적 자율규제(enforced self-regulation)는 민간영역이 스스로 규제를 형성하고 의무를 부과하지만, 그러하지 않을 경우 법이 정하는 규제를 강제하는 것이다. 넷째, 자발적 자율규제(voluntary self-regulation)는 정부의 적극적인 개입이 없는 형태를 말한다. 우리나라 인터넷 서비스 자율규제기구의 대부분은 자발적 자율규제유형에 가깝다.

나. 우리나라 정보통신 자율규제체계의 특징

우리나라의 정보통신 자율규제체계의 특징으로 제도적 장치의 측면과 인터넷 기업의 자율규제 장치 측면, 이 두 가지를 살펴볼 수 있다. 먼저, 제도적 장치의 측면에서는 통신서비스 정책과 규제 전반을 총괄하는 방송통신위원회가 있으며, 준행정 기능을 갖춘 민간기구인 방송통신심의위원회가 콘텐츠 규제를 담당하고 있다. 방송통신심의위원회는 「방송법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법") 등에 규정된 방송 및 통신 관련 콘텐츠 전반에 대한 심의, 규제 기능을 수행한다. 둘째, 방송통신심의위원회가 인터넷 콘텐츠 등급제, 핫라인, 분쟁조정 기능 등을 동시에 수행한다. 기존 정보통신윤리위원회가 수행해 온 불법 콘텐츠의 신고처리 기능은 방송통신심의위원회가 불법·청소년유해정보 신고센터로 개칭하여 운영하고 있다. 개인정보보호, 불법스팸, 해킹 등의 문제는 한국인터넷진흥원이 담당하고 있다. 그 외 인터넷 모니터링 기능을 수행하는 기구로 청소년보호위원회(보건복지가족부), 방송통신심의위원회, 영상물등급위원회, 시민단체인 한국사이버감시단, 청소년정보감시단, 학부모정보감시단, YWCA 청소년유해환경매체 모니터 등이 있다.

우리나라의 인터넷 기업들 역시 자율적인 규제기능을 수행하고 있다. 예를 들어, NHN, 다음, SK커뮤니케이션즈 등의 인터넷 기업들도 자율적으로 내부 모니터링,

부분적인 정보게시제한조치 등을 실시하는 중이다. 아울러 옴부즈맨 제도를 도입하여 이용자 보호정책을 수행중이다. 네이버, 다음, 네이트 등의 주요 포털사들은 이용자, 전문가 등으로 구성된 책무위원회를 운영하는 등의 자율적인 규제 역할을 수행중이다.[48]

2. 현행 정보통신망에서의 자율규제 체계의 구현형태

현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 정보통신망의 이용을 촉진한다는 목적과 동시에 정보통신서비스를 이용하는 자의 개인정보를 보호하며, 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다. 이에 따라 정보통신망법 제3조에서는 정보통신서비스 제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력의 향상에 기여하여야 하고 이용자는 건전한 정보사회가 정착되도록 노력하여야 함을 선언하고, 정부는 정보통신서비스 제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년 보호 등을 위한 활동을 지원 할 수 있다고 규정하고 있다. 이외에도 정보통신망법은 정보통신망에서의 이용자 보호, 정보통신망의 안전성 확보, 국제협력 등을 위하여 매우 포괄적인 내용을 담고 있으며, 그에 대한 위반사항이 있을 시에 가해지는 벌칙에 대한 내용까지 폭넓게 규정하고 있다.

이렇게 정보통신망법은 정보통신망의 이용촉진과 정보보호를 위하여 정부의 지원과 시책마련의무를 폭넓게 규정하고 있는데, 이 시책으로서는 정보통신망 관련 기술의 개발과 보급, 정보통신망의 표준화, 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화, 정보통신망을 이용한 정보의 공동 활용 촉진, 인터넷 이용의 활성화, 정보통신망을 통하여 수집·처리·보관·이용되는 개인정보의 보호 및 그와 관련된 기술의 개발·보급, 정보통신망에서의 청소년 보호, 정보통신망의 안전성 및 신뢰성 제고 등이 포함되어야 한다. 이에 따라 행정안전부장관 또는 방송통신위원회는 관련 업계 및 이용자단체 등의 의견을 수렴하고 관계 중앙행정기관

48) 황용석·이동훈·김준교, 전게논문, 123-126.

의 장과 협의를 거쳐 이용자의 개인정보를 보호하기 위한 개인정보보호지침을 정하여 고시하고, 정보통신서비스 제공자 등에게 이를 준수할 것을 권장할 수 있다.

또한, 개인정보의 수집·이용 및 제공의 제한에 관하여 정보통신서비스 제공자는 이용자에가 그에 대한 고지와 동의를 받아야 하는 것, 그리고 정보통신서비스 제공자등은 이용자의 개인정보보호를 위하여 개인정보관리책임자를 지정하도록 하는 등의 규정이 있다.

한편 정보통신망의 안정성 확보를 위하여 기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자는 이 체계가 방송통신위원회가 고시한 기준에 적합한지에 관하여 방송통신위원회나 한국인터넷진흥원이 지정하는 인증기관으로부터의 인증은 받는 인증제도 등을 시행하고 있다.

3. 정보통신망에서의 자율규제의 구체적 현황

가. 인증제도형 자율규제

1) 자율적 정보보호 관련 인증제도

인터넷과 같은 기술적으로 표준화되어 있는 영역에 있어서 국제적으로 통용되는 산업표준을 지키도록 법이 유도할 수 있다. 이와 같은 표준정책 내지 인증제도는 국가가 주도적으로 기준을 설정할 수 있지만 국제사회나 사회에서 자율적으로 형성할 수 있기에 자율규제모델로도 평가받을 수 있다.[49] 임의적인 표준제도는 자율규제의 측면이 같이 작용되는 것이라고 할 수 있다. 이에는 정보보호관리체계 인증제도(ISMS), ISO등 국제공인 인증제도, 각종 마크제도등이 포함될 것이며, 특히 인터넷 등급제, 프라이버시 표준, 프라이버시 인증제, 개인정보보호마크, 인터넷사이트안전마크 등이 인증제도형 자율규제에 속한다 할 것이다.

2) 정보보호관리체계 인증제도(KISA-ISMS)

---

49) 최유, 시장자율규제와 행정지도의 관계에 관한 연구, 현안분석, 한국법제연구원, 2008. 76면.

정보보호관리체계(ISMS : Information Security Management System) 인증제도란 ISO9001(품질경영시스템)과 같이 품질 보증을 위한 기업 내 일련의 활동에 대한 인증과 유사한 개념으로 정보보호를 위한 기업 내의 정보보호관리체계에 대해 한국인터넷진흥원(KISA)으로부터 객관적인 심사를 거쳐 인증을 취득하는 제도이다. 정보보호관리체계는 정보통신망의 안정성을 확보하고 조직의 정보자산을 보호하기 위해 기술적, 관리적, 물리적 정보보호대책을 구현하여 지속적으로 관리·운영하는 종합적 시스템이다. 기업에서는 정보보호관리체계 수립을 통하여 고객의 개인정보(금융정보, 의료정보 등)를 효과적으로 보호할 수 있는 체계를 마련하게 되는 효과가 있다.

KISA-ISMS 인증제도는 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 제47조에 의해 정립되었으며, KISA-ISMS 인증제도의 목적은 종합적 관리체계수립을 지원하고, 정보보호 관리에 대한 인식을 제고하여 보호되어야할 정보통신망 및 정보자산의 안전성, 신뢰성을 강화하고 국제적 신뢰도를 향상시키기 위한 것이다.[50]

정보보호를 위한 기업 내의 일련의 활동에 대하여 137개 심사기준 적합성 여부를 한국인터넷진흥원이 객관적인 심사를 거쳐 인증을 부여하는 제도이다. 2006년까지는 인증대상을 정보통신서비스제공자, '정보통신서비스제공자에게 물리적 시설을 제공하는 자'로서 집적된 정보통신시설을 운영·관리하는 자, 정보통신망을 운영하는 민간사업자로 크게 3개 대상으로 구분하였으나, 2007년에는 대상자 규정을 삭제하여 정보보호관리체계를 수립·운영하고 있는 자는 모두 인증을 받을 수 있도록 정보통신망법을 개정하였다. 정보통신망법에서는 정보보호관리체계를 정보통신망의 안정성을 확보하고 조직의 정보자산을 보호하기 위해 기술적·관리적·물리적 정보보호대책을 구현하여 지속적으로 관리·운영하는 종합적 시스템으로 정의하고 있다.

인증 취득을 원하는 기업이 인증심사를 신청하고 인증서를 발급받기까지 약 3개월의 시간이 소요되며, 인증은 4단계로 진행된다.

---

50) 홍성혁·박종혁·서정택, 국내환경에 적합한 정보보호관리체계 평가 방법론에 대한 연구, 한국항행학회 논문지 제12권 제4호, 2008. 08. 386면.

첫째, 인증신청 및 계약을 준비하는 준비단계, 심사팀(기본 4명으로 구성)이 문서심사 및 기술심사를 한 후 그 결과 발견된 결함사항을 신청기관이 보완조치(보완조치 기간은 1개월)하는 심사단계, 인증위원회가 인증심사결과를 심의하여 인증서를 교부하는 인증단계, 인증취득기관이 정보보호관리체계를 지속적으로 운영하는 지를 심사하는 사후관리단계로 구분된다.

인증심사의 종류는 최초심사, 재심사, 사후관리, 갱신 심사로 구분한다. 기본적으로 인증유효기간은 3년이며, 인증취득 후 1년 에 1회 이상 사후관리심사를 받아야 한다. 최초심사는 정보보호관리체계 인증 취득을 위한 심사이며, 재심사는 인증을 받은 정보보호관리체계의 범위 내에서 중대한 변경이 발생한 경우의 심사이다. 사후관리는 정보보호관리체계를 지속적으로 운영하고 관리하고 있는 지를 1년에 1회 이상 점검하는 심사를 말한다. 갱신 심사는 3년의 인증유효기간 만료일 이전에 인증 유효기간을 연장하기 위한 심사를 말한다.

2002년 제도가 처음 시행된 이후 당해 5월 첫 인증서가 발급되었고, 2009년 3월 현재 총 68건의 인증서를 발급하였다. 2004년까지 통신, 금융, 정보보호컨설팅 전문업체에 집중되던 인증분야가 2005년 이후 특히, 개인정보보호가 중요시 되고 있는 대형포탈, 금융, 의료, 교육 분야 등의 인증분야로 확대되고 있다.

3) ISO27001 ISMS 인증

ISMS는 조직의 전반적인 관리시스템의 일부로서 비즈니스 위험에 기반을 두어 정보보호를 계획, 구현, 운영, 검토 및 개선시키기 위해 조직체계 및 정책, 정보보호 프로세스 및 절차, 정보보호통제 등으로 구성된 관리체계이다.

국제표준인 ISO27001 ISMS인증은 국제표준화기구(ISO)에서 제정한 국제규격으로 BS7799[51] 영국 표준에서 2005년 11월 ISO 국제표준으로 승격된 것으로 ISMS 효과성 측정, 인적보안 강화, 외부업체 보안강화 등을 특징으로 한다.[52]

---

51) 1995년에 처음 제정된 BS7799는 1999년에 개정되었고, 영국·호주·브라질·네덜란드·뉴질랜드·노르웨이 등에서 사용되고 있다. 1999년 10월에 ISO표준으로 제안되어 ISO/IEC DIS 17799-1이 되었다.

52) 김태달, ISO 27001의 ISMS 보안성숙도 측정 모델링에 관한 연구, 한국컴퓨터학회 논문집, 제12권 제6호, 2007.12. 154면.

ISMS의 요구사항을 포함하는 ISO 27001(BS 7799 part 2: 2002 수정판)과 ISMS의 기초적인 통제수단을 수록한 ISO 27002(ISO 17799:2005)가 국제표준화에 성공하여 최근 전 세계적으로 ISMS에 대한 인증 노력이 빠르게 확산되고 있다.[53]

KISA의 ISMS인증기준은 ISO/IEC 27001 국제표준을 모두 포함하고 있고, 이에 더하여, 국내 상황에 맞게 개인정보보호 침해사고예방, 암호화, 전자거래 등의 보안요건을 강화하였으며, 국내 TTA표준(표준번호 TTAS.KO-12.0036)으로 2006년 12월 개·제정 되었으며 정보보호 관리과정, 문서화 요구사항 및 정보보호대책 등 3가지 요구사항으로 구성된다.[54]

4) 개인정보보호마크제도(ePRIVACY)

인터넷을 통한 전자상거래의 이용이 확대된 반면 개인정보와 관련한 피해도 증가하게 되는데 이는 전자상거래 활성화에 큰 걸림돌로 작용하게 된다. 이러한 상황에서는 인터넷 이용자의 개인정보를 효과적으로 보호함으로써 온라인 거래의 신뢰기반을 구축하는 것이 무엇보다 필요하다. 이에 한국정보통신산업협회(KAIT)는 인터넷사이트의 개인정보보호 정책 및 관리수준을 종합적이고 객관적으로 평가하여 일정기준을 충족하는 경우 개인정보보호마크(ePRIVACY)를 부여하는 제도를 시행하고 있다.

한국정보통신산업협회는 개인정보보호마크제도를 통하여 개인정보에 대한 침해 등 인터넷 이용자들의 불안요소를 예방하고 전자상거래를 촉진시키며, 민간의 자율적인 개인정보보호 관리체계를 정착시키는 것에 기대를 걸고 있다. 이와 함께 해외의 개인정보보호마크제도와 협력 체제를 구축하여 개인정보보호마크를 취득한 업체들이 해외에서도 개인정보보호 우수 사이트로 인증을 받을 수 있도록 국제적인 공신력을 제고하기 위한 활동을 하고 있다.

인터넷서비스 제공자(ISP), 취업알선 경매 등 전자상거래 사이트·금융 의료 사이트·포탈 및 검색 게임 사이트 등 인터넷사이트를 통하여 개인정보를 수집·취급·관리하는 국내 사업자 및 단체는 개인정보보호마크 인증을 신청할 수 있지만, 신

53) 홍성혁·박종혁·서정택, 전게논문, 385면.
54) 홍성혁·박종혁·서정택, 전게논문, 386면.

청일 기준 3개월 이내 개인정보관련 법률 위반으로 과태료 부과 및 형사 처벌을 받은 사업자 및 기관은 신청대상에서 제외된다. 인증신청이 들어오면 협회는 현장조사를 실시하고 부족한 부분에 대해서는 보완지시를 한다. 조사 또는 보완지시를 통한 재조사가 완료되면 인증위원회의 최종 심사를 통하여 마크를 부여한다.

개인정보보호마크의 인증기준은 정보통신망법, 개인정보보호지침, 한국정보통신산업협회 인터넷사이트 안전마크 심사기준을 근거로 하여 i) 개인정보의 수집에 관한 조치, ii) 개인정보의 이용 및 관리, iii) 이용자의 권리, iv) 공개 및 책임, v). 만14세 미만의 아동에 관한 특별조치, vi). 이용자 권리구제, vii) 기타 등 7개 분야 59개 항목(필수 17개 항목)으로 구성되어 있으며, 대체로 법령에서 요구하는 정도보다 다소 구체적이다. 인증기간은 개인정보보호마크 사용계약 체결 후 1년이며, 인증 유효기간 만료 1개월 이내에 약식으로 재심사를 신청하고 인증기간을 연장할 수 있다.

한국정보통신산업협회는 인증을 통한 자율규제활동을 촉진하기 위하여 언론과 주관기관의 홈페이지를 통해 개인정보보호마크 취득업체를 위한 광고와 지속적인 홍보를 지원하고 취득업체에 대하여 관련법률, 분쟁조정사례, 국제동향 등의 정보를 제공한다.

5) 인터넷사이트 안전마크(i-Safe)

한국정보통신산업협회는 개인정보보호마크와는 별도로 네트워크상에서 영리 또는 비영리의 목적으로 설치하여 운영 중인 인터넷 사이트를 대상으로 개인정보보호, 시스템 보안, 소비자 보호 등 세 가지 부문에 대한 평가를 통하여 인터넷사이트 안전마크(i-Safe)를 부여하는 제도를 시행하고 있다. 인터넷사이트 안전마크는 금융, 의료 등 고도의 보안이 요구되는 인터넷사이트와 기타의 인터넷사이트를 구분하여 상이한 심사기준을 적용하고 각각 노란색과 녹색의 두 가지 색상으로 부여된다. 인증기간은 개인정보보호마크와 마찬가지로 1년이며, 마크취득 업체에 대하여는 정보보호 시스템보안 전문가를 중심으로 한 무료컨설팅 등의 혜택이 제공된다.

나. 사업자단체 측면에서 자발적으로 실시하는 규제

1) 한국인터넷자율정책기구(KISO)

인터넷의 많은 역기능들로 인하여 인터넷 서비스 제공업체의 사회적인 책임이 요구되는 상황에서 항구적이고 체계적인 자율규제 방안을 모색하기 위한 장치의 일환으로 7개 포털사(다음 커뮤니케이션, 야후 코리아, SK커뮤니케이션즈, NHN, KT하이텔, 프리챌, 하나로 드림)가 2009년 3월 3일에 한국인터넷자율정책기구(KISO : Korea Internet Self-governance Organization)를 발족하였다.

현재 국내 정보통신망 규제의 특수성으로 볼 수 있는 사항으로 행정부 주도의 중앙집권적, 위계적 규제구조 및 강력한 입법 규제전통의 존재한다는 것과 정보통신망 규제에 있어서 민간의 영향력이 매우 낮다는 점이 있다. 방송통신위원회의 경우 민간기구와 행정기구의 결합으로 이루어진 기구이나, 행정기구적인 성격이 강하다. 또한 정보통신망 규제를 하는데 있어서 민간 시민단체 및 이익단체가 적고, 그에 대한 인지도·신뢰도가 적은 것이 사실이다. 실질적인 규제의 성격에 있어서도 내용규제의 성격이 강하여 불법·유해 게시물 검열, 분쟁 조정, 유해정보 신고 등 통합적인 내용규제의 도구를 갖추고 있다.

국내 최초의 인터넷자율규제 민간기구인 한국인터넷자율정책기구(KISO)의 특성으로는 회원사간 게시물 정책공조 및 게시물로 인한 이용자 권익보호 및 피해구조를 위한 공동정책개발 활동과 기존 인터넷 규제기구 기능에 보완을 하여 인터넷 규제와 관련된 제도적 사각지대에 대한 업계의 자율적인 공동대응 활동을 특성으로 볼 수 있으며, 또한 해외의 여러 자율규제 기구와 같은 신고·대응 체계를 가지고 있다는 것이 특징이라 할 수 있다.

KISO의 기능 및 활동 상황으로 이용자 보호를 위한 가이드라인 수립과 이용자 보호를 위한 자율대책 및 공동대응책 마련, 이용자 피해구제 원칙 및 방법에 대한 합의 도출의 노력, 회원사의 인터넷 사이트의 불법·불건전 게시물에 대한 신고접수 및 처리, 인터넷상의 각종 피해에 대한 상담하고 안내한다. 2009년 4월 21일에

명예훼손성 게시물에 대한 KISO 정책위원회의 첫 정책 결정이 있었다. 사회적으로 논란이 되고 있는 실명이 거론된 명예훼손성 게시물의 처리정책을 확정해 발표한 것인데, 이번 KISO의 결정은 인터넷 게시물과 관련된 첫 정책결정으로 7개 회원사의 모든 포털 사이트에 적용된다.

'실명이 거론된 명예훼손성 게시물의 조치를 위한 정책'에 따르면, 인터넷상의 게시물로 명예를 훼손당했다고 주장하는 사람은 '명예훼손 사유'와 '해당 게시물의 주소(URL)'를 명확히 기재해 삭제 등을 요청해야 하며, 이 같은 URL의 적시 없이 삭제 등의 조치를 요구한 때에는 '표현의 자유를 지나치게 제약할 가능성이 있으므로 일시적이고 제한적으로 임시조치를 허용'하는 것으로 되어 있다. 현재 정보통신망법은 명예훼손을 주장하는 당사자의 요청이 있을 때 사업자가 '지체 없이 삭제·임시조치 등의 필요한 조치를 취해야 한다'고 규정하고 있을 뿐 그 구체적인 요건과 사후절차 등을 명확히 하지 않아 이번에 KISO가 그 요건을 합리적인 선에서 마련한 것이다. 특히 정부기관 등이 URL의 적시 없이 포괄적 요청(예컨대 '내 이름이 들어가는 모든 게시물을 삭제해 달라'는 방식)을 남발하는 경향에 대해서는, 임시조치(이른바 블라인드 처리)를 하더라도 이것이 '예외적 조치'로서 '일시적이고 제한적으로만 허용되는 것'임을 분명히 했다. KISO는 또 피해 당사자의 요청이 없더라도 인터넷 사업자가 자율적 모니터링에 의해 문제의 게시물을 삭제 또는 임시조치 해야 하는 의무와 관련해서는 자칫 '사적 검열(private censorship)'을 조장할 수 있다는 우려를 제기했으나 현재 진행 중인 정보통신망법 개정작업과 최근의 대법원 판결 등을 고려하여서 구체적인 개선방안을 마련키로 하고 이번 결정에서는 제외했다.

2) 정보공유분석센터 (ISAC - Information Sharing & Analysis Center)

정보공유분석센터는 「정보통신기반 보호법」 제16조의 정보보호관련 업무를 수행함에 있어서 민간분야의 자생적인 공동대응체계를 구축하여서 각종 전자적 침해행위로부터 회원사간의 정보통신 관련 시설을 보호함으로써 정보통신업무의 안전성과 신뢰성을 제고하기 위하여 설립하였다.

정보공유분석센터는 주로 정보통신망의 사이버테러 취약점과 침해요인, 대응방안에 관한 정보를 가입기관에 제공하고 침해사고가 나면 실시간 경보와 분석업무를 수행하게 된다. 아울러 분야별 여건을 고려, 침해사고 대응체계 구성·운영, 정보통신기반시설 보호시스템 시험, 정보보호관련 교육과 훈련 서비스 등을 부가적으로 제공한다. 이를 통해 회원사간 정보보호를 공동대처함으로써 전문조직 별도 운영에 따른 업무 및 비용을 경감할 수 있다. 또한 정보수집 및 적용, 기술 확보, 인력 및 조직 운영 등 모든 요소들에 대한 문제를 줄일 수 있다.

ISAC(정보공유분석센터)은 미국이 지난 98년 금융부문 ISAC을 비롯하여 통신·국방·교통 등 8개 분야에 ISAC을 운영하면서 세계적으로 관심을 끌고 있으며, 일본과 일부 유럽 국가도 도입을 검토 중이거나 이미 구축해 운영하고 있다.

국내에서는 주요 정보통신기반시설에 대한 사이버테러를 방지할 목적으로 정부차원에서 「정보통신기반 보호법」을 제정, 민간주도의 ISAC설립을 적극 권장하고 있다. 「정보통신기반 보호법」이 제정된 후 센터 설립이 계획되어 2002년에 센터가 발족되었다. 2005년 자율적인 조직으로 독립적인 운영으로 전환되어 독립적인 협회로서 통신정보공유분석협회로 창립하게 되었다. 현재 기간통신사업자 KT 등 11개 사업자가 회원사로 가입되어 있다.

3) 인터넷광고 자율심의기구의 설립

2007년 1월24일, 민간의 사단법인인 한국인터넷기업협회와 한국인터넷마케팅협회를 중심으로 인터넷광고 내용을 심의하는 '한국인터넷광고심의기구' 가 창립되었다.

한국인터넷광고심의기구는 민간이 자율적으로 인터넷 광고에 대한 심의기준을 마련하고 심의위원회를 구성·운영함으로 인터넷광고의 선정성과 폭력성, 위법성 등을 사전에 심의하기 위해 마련된 것이다. 원칙적으로 인터넷 광고를 비롯한 정보통신망에서 유통되는 모든 콘텐츠는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「전기통신사업법」에 의해 정보통신윤리위원회가 사후심의를 하게 된다. 그러나 인터넷 광고는 특성상 빠른 전파성을 지녀 사후심의를 통해 문제를

해결하기 이전에 이미 사회적 문제를 야기하게 되고, 이 때문에 사후심의가 아닌 사전심의의 필요성이 제기되었던 것이다. 정부가 주도하는 사전심의와는 별도로 업계 중심의 자율심의기구가 구성된 것이다. 자율심의기구에는 네오위즈와 다음커뮤니케이션, 드림위즈, 한국마이크로소프트, 야후코리아, 엠파스, NHN, SK커뮤티케이션즈 등 60여개 업체가 참여하고 있다.

4) 개인정보관리책임자협의회

개인정보에 대한 침해 및 분쟁이 증가하는 가운데 정부차원의 개인정보보호 관리 감독 등 사업자에 대한 규제가 강화되는 반면 개인정보에 대한 기업의 관리지침 및 체계는 시장의 요구에 적절히 대응하지 못하고 관련업체간에 정보의 교류가 부족한 까닭에 신속하게 대응책을 마련하지 못하는 경향이 있다. 이러한 현실에서 사업자를 대상으로 한 개인정보보호 교육의 강화와 기업의 정보윤리 및 정보보호 의식의 확산, 업종별 개인정보보호지침의 개발과 보급, 개인정보보호에 관한 기업 간 정보교류 및 협력관계의 강화, 개인정보보호 우수 관리모델 및 정책사례 발굴과 보급, 개인정보보호 관련 법·제도 개선 활동 및 대정부 건의 등을 위한 공동협의체의 필요성이 증가되고 있다는 인식에 따라 2002년 7월 한국정보통신산업협회에 사무국을 둔 개인정보관리책임자협의회(Chief Privacy Officer Council)가 결성되었다.

개인정보관리책임자협의회는 인터넷쇼핑몰, 이동통신사업자, 포털사이트 등 정보통신서비스 제공업체뿐만 아니라 항공사, 호텔, 여행사 등 개인정보를 취급하는 온라인, 오프라인 업체의 개인정보관리책임자(CPO) 또는 관련 단체를 대상으로 하며, 2008년 9월 현재 20여개의 사업자가 참여하고 있다. 개인정보관리책임자협의회는 매 분기별 운영위원회의 개인정보보호 자율규제 기반 정착 및 활성화를 위한 연구, 분과위원회의 업종별 개인정보보호 자율규범 및 가이드라인 연구 등 연구사업을 공동으로 시행한다.

한편, 한국인터넷기업협회도 개인정보보호 관련 정책의 발전적인 육성과 정책결정과정에의 적극적인 참여를 통해 국내 인터넷산업 발전에 기여하기 위한 목적

에 따라 개인정보보호협의회를 설치하고 있다. 개인정보보호협의회는 개인정보보호 관련 정책 의제에 대한 전략의 수립 및 정책의 개발, 공청회, 세미나, 워크숍, 정책간담회 등을 통한 의견수렴, 유관기관, 업계 등과의 협력 등을 수행한다.

다. 사업자들이 자율적으로 시행중인 기술적·관리적 조치

우리나라 인터넷 기업들도 자율적으로 규제기능을 수행하고 있다. 예를 들어, NHN, 다음, SK커뮤니케이션즈 등의 인터넷기업들도 자율적으로 내부 모니터링, 부분적인 정보게시제한조치 등을 실시하는 중이다. 아울러 옴부즈맨 제도를 도입하여 이용자 보호정책을 수행 중이다. 네이버, 다음, 네이트 등의 주요 인터넷 포털사들은 이용자, 전문가 등으로 구성된 책무위원회를 운영하는 등의 자율적인 규제 역할을 수행중이다.[55]

1) 'NHN'의 경우

네이버는 서비스자문위원회를 운영하고 있는데, 자문위원회는 이용자들을 대표하는 사회 각층에서 선별된 전문가들로부터 네이버의 서비스의 사회적 책임과 역할을 함께 생각하고 해결책을 찾는 데에 그 목적을 두고 있다. 서비스자문위원회는 운영목적을 크게 세 가지로 나누어 놓고 있는데, 첫 번째, 서비스 정책과 운영에 대한 감시견 역할이다. 네이버서비스 운영정책에 대한 감시수행자의 역할을 부여하여, 서비스자문위원회는 수많은 이용자들을 대표해서 네이버서비스 운영진에게 보다 나은 서비스를 할 수 있도록 발전방안을 제시하도록 하고 있다. 두 번째, 외부 전문가 집단의 자문을 통한 외부 검증 효과이다. 다양한 서비스 정책 수립에 있어 내부의 일방향적 결정이 아닌, 외부 전문가의 공개 검증을 통한 신뢰도 제고를 위해 네이버서비스 자문위원회를 운영하고 있다. 세 번째, 이용자와 네이버의 소통 중재의 목적이다. 모든 이용자와의 직접적인 소통이 불가능하므로 주요 대표 창구로 자문위원회가 이용자와 네이버 사이의 커뮤니케이션 매개자 역할을 수행

55) 홍성혁·이동훈·김준교, 전게논문, 126면.

하도록 하는 것이다.

2007년 1월 '네이버뉴스이용자위원회'를 기획하여 2008년 6월까지 운영하였으며, 2008년 8월부터는 뉴스뿐만 아니라 다양한 서비스에 산발적으로 퍼져있는 이슈들에 대한 중요순위를 판단하여 아젠다를 설정하고, 외부 전문가들로부터 검증효과를 거침으로써 문제의 원인 파악 및 근본적 해결책을 마련하기 위해 자문위원회를 운영하고 있는 것이다.

또한, 24시간 안내센터를 통하여 언론사에서 제공받은 기사의 오보나 기사로 인한 명예훼손 및 저작권 침해 등으로 문제가 발생한 경우 피해자의 권익을 보호하는 창구를 마련하고 있다. 해당 언론사에서 수정 및 삭제된 기사가 네이버에서 서비스되고 있는 경우의 조치, 기사정정 및 반론신청의 소송중인 기사에 대한 문의, 기사 및 댓글로 인하여 명예훼손이나 초상권 침해가 발생한 경우의 조치, 수정·삭제되었거나 저작권이 있는 기사가 네이버 블로그·카페에 스크랩된 경우의 조치, 저작권이 침해된 경우나 인권침해나 재산상의 피해를 입은 경우 등에는 피해회복에 필요한 조치를 취하게 된다.

2) 'Daum'의 경우

'다음'은 각 분야 전문가들로 구성되어 미디어다음 뉴스편집과, ucc운영에 대하여 사용자 입장에서 비판과 의견을 제시하는 '열린 사용자위원회'를 운영하고 있다.

총 13면의 위원 중 6명은 네티즌 위원으로 공모해 선출하며, 1년을 임기로 하여 현재 2기가 활동 중이다. 또한 24시간 뉴스센터를 통하여 오보와 명예훼손, 저작권 침해 등의 빠른 처리를 위해 24시간 뉴스센터를 운영하고 있다. 기사에 대한 수정과 삭제, 댓글관리와 게시중단 요청 등을 뉴스센터를 통해 받고 있다.

3) 'SK커뮤니케이션즈'의 경우

이용자위원회 성격의 사회적 감시 및 의견수렴기구로서 미디어 책무위원회를 두

고 있으며, 포털뉴스 편집규약 및 강령 제정과 발표하였고, 뉴스로 인한 피해구제 접수창고로서 이용자 피해구제를 하기 위한 신고메일시스템을 운용하고 있다.

제2절 미국과 호주의 정보통신망 자율규제 현황

나날이 복잡해지고 지능적으로 변해하는 사이버보안에 대한 위협은 ISP들과 서비스제공자들에게 각자에게 가장 적절한 대응방법과 위협의 성격과 레벨에 따른 접근 방법을 적용하도록 요구하고 있다. 만일 모든 ISP들이나 정부가 사용자에게 필터링 소프트웨어나 최신 백신프로그램을 사용하도록 강제하여 해결될 수 있는 문제였다면 이미 사이버보안 문제는 해결되었을 것이다. 그러나 안타깝게도 사이버보안에 대한 현실은 한 가지의 답으로 해결될 수가 없는 매우 복잡한 문제이다.
미국의 경우에 네트워크 안전을 포함하여 복잡한 여러 사이버보안 이슈를 해결하기 위한 정부의 제안과 입법 사례들이 있었다. 그러나 입법 과정과 사법적 적용의 구조적인 한계는 입법의 속도보다 빠르게 진화하는 사이버보안에 대해 사전 예방보다는 사후 조치라는 한계 때문에 사이버 위협에 대한 모든 답을 주지 못했고, 미국 정부의 여러 부처의 사이버보안에 대한 제안을 현실화 하는 데에는 정부 부처 간의 조율과 입법 절차 등, 오랜 시간과 노력이 필요하다는 것을 일찍이 깨달았다.

미국의 사이버보안에 대한 노력은 정부의 주도를 중심으로 사기업들의 전문성과 기술력을 활용하는 것으로 요약될 수 있다. 즉, 정부 부처를 중심으로 사이버보안에 대한 국가적 계획을 세우고, 각 산업 또는 분야 별 사이버보안 계획에는 사기업의 전문성과 기술력을 바탕으로 특성에 맞는 분야 별 위협 대처 방법과 절차를 세우는 것이다. 미국의 사이버보안에 대한 노력은 크게 정보의 공유, 위험에 대한 관리, 그리고 신뢰에 기초한 모델이라는 점에 주목할 수 있다.

가정용 사용자의 경우에는 적극적인 사용자 교육을 통하여 정보를 공유하고 (자세한 사용자 교육 모델은 후술), 기업과 전력회사, 병원, 또는 통신사들과 같이 아주 중요한 인프라를 구축하고 있는 운영자들은 위험관리방식을 통하여 위협의 우선순위를 정하고 취약점을 파악하여 가장 중요한 문제점에 집중적인 시간과 자본

을 투입하도록 유도하고 있다. 또한 미국 정부는 사기업들의 적극적인 공조와 자율규제의 장려를 통하여 사기업의 전문성을 적극 활용하고 있다.

미국의 경우 정부 규제는 형사적 처벌을 통한 사후 조치에, 사기업들의 공조는 네트워크 안전에 대한 계획 수립과 기술적인 방지에 집중을 하고 있는 반면 호주와 일본의 경우 네트워크 안전에 대한 구체적인 위협의 대응 방법에 보다 적극적인 노력을 보이고 있다.

본 절에서는 미국의 자율규제 현황과 호주와 일본의 민관 공조를 통한 구체적인 위협의 대응 방법을 살펴보기로 하겠다.

1. 미국의 자율규제 현황

가. 인터넷 보안 진보를 위한 산업연합(ICASI)

인터넷 보안 진보를 위한 산업연합(Industry Consortium for the Advancement of Security on the Internet: ICASI)은 전 세계적으로 사용되고 있는 여러 제품들이 당면하는 보안 위협에 대처하기 위한 비영리 단체로 세계적으로 선도적인 IT 기업들이 참가하고 있다. 이 연합에서는 회원사들이 가지고 있는 기술적 역량을 활용해, 복잡하지만 중요한 보안 문제를 해결하고 있다. 이러한 활동은 기업, 정보, 일반사용자, 그리고 IT 기반시설(infra)을 보호하는 데 이바지한다.[56]

ICASI에는 미국은 물론 미국 외의 IT기업들도 참여하고 있다. 통일된 보안침해 사고사례대응전략(The Unified Security Incident Response Plan: USIRP)과 취약점의 발표와 대응에 대한 공동 프레임워크(Common Frameworks for Vulnerability Disclosure and Response: CVRF)가 대표적인 프로젝트이다.

USIRP은 ICASI가 전 세계적으로 인터넷의 보안을 강화하기 위해 가장 중요하게 생각하는 임무이다. USIRP는 인터넷 보안 강화를 위한 방법을 논의하는 토론의 장 역할을 한다. 보다 구체적으로 USIRP는 인터넷 보안 문제를 효율적으로 해결하기 위해, 회원사들 간의 공조 절차와 기술적 도구를 제공한다. ICASI에서

56) http://www.icasi.org (이하 내용은 ICASI 홈페이지의 내용을 정리)

USIRP를 통하여 취급하고 있는 주제로는 널리 사용되는 소프트웨어들에 대한 취약점, 긴급하거나 최근에 등장하고 있는 보안침해사고사례로 ICASI 회원사 중 셋 이상에 영향을 미치는 문제, 그리고 전략적으로 다루어야 할 장기적인 문제들을 포함한다.

USIRP를 통해서 회원사들은 보안 침해 사고 대응센터의 대응절차와 보안 담당 직원이 공통적으로 적용해야할 정식 대응 체제를 만들고, 보안의 위협에 대한 사례가 있는 경우 중요한 정보의 공유를 통하여 공조를 통한 해결 방안을 찾도록 한다. USIRP에는 다음과 같은 업무들이 포함되어 있다.

- o 보안침해사고사례 처리 지침(Incident Handling Collaboration Manual) 만들기: USIRP 보안침해사고사례의 보고, 대응의 우선순위, 보안침해사고사례 조사 시작에 대한 절차, 기술 인력의 동원 절차, 보안 대응 계획을 세우고 문제를 해결하는 자세한 절차가 기술되어 있다.
- o ICASI Unified Security Incident Response Team(USIRT)의 구성을 통한 각 회원사의 역할과 책임 분담.
- o 회원사들이 협력에 관한 정보를 교환할 수 있는 포탈의 운영
- o 보안침해사고사례 핸들링 시스템의 유지: 보안침해사고사례 처리 체계에는 모그룹으로 항상 최신 정보로 갱신된 사고 처리 협력 지침서(Incident Handling Collaboration Manual), 지원 서식, USIRP 사고 추적 기록(Incident Tracking Log)와 같은 자료들이 포함되어 있다. 하부 그룹으로 각 보안침해사고사례들이 발생할 경우 협조를 해야 하는 팀들이 있다.

USIRP 보안침해사고사례(incident)는 ICASI 회원사가 해당 회사의 절차를 통해 보안침해사고사례 조사 과정 중 회원사 셋 이상과 관련된 내용이라고 판단하면 ICASI의 보안침해사고사례를 발효시킨다. ICASI 회원사들은 USIRP 공조를 위해서 다자 간 비밀유지계약서가 있기 때문에 각 회원사의 지적재산권의 침해에 대한 우려 없이 중요한 기술적 정보들을 다른 회원사들과 공유하고 논의할 수 있다. USIRP는 2009년 2월에 첫 번째 버전이 나왔으며 지속적으로 갱신되고 있다.

취약성 정보 및 그 대응을 위한 공동 체계(Common Frameworks for

Vulnerability Disclosure and Response: CVRF)는 취약점 정보를 여러 기관이 공유하기 위해 만든 체계이다. 물론 과거에도 공통 취약점 사전(Common Vulnerabilities and Exposure Dictionary)[57]과 공동취약점득점시스템(Common Vulnerability Scoring System: CVSS)[58] 등을 운영하며 취약점 정보를 관리해왔었다. 그러나 지금까지의 취약점 보고, 고유의 보안성 평가는 각 회사 별로 고유한 규격을 가지고 있어서, 공동 작업이 힘들었다. 또한 각기 다른 규격은 자동화된 분석 처리도 힘들게 하였다.

이러한 문제점을 해결하기 위해서 ICASI는 CVRF 사업을 시작하였다. 국가기반사업자문협의회(National Infrastructure Advisory Council: NIAC)와 같은 단체들의 작업을 토대로 ICASI의 CVRF 산업협의체는 여러 기업들과 단체가 각각 적용하고 있는 체계보다는 모두에게 적용될 수 있는 공통의 체계를 가지고 취약점을 보고하는데 일관성을 가질 수 있도록 하는 통일화된 규격을 만들고 있다. CVRF는 XML 프레임워크를 이용해 취약점의 보고에 대한 기준 규격을 만들고 있다. 취약점 보고에 대한 표준 규격이 만들어지면 회원사들은 좀 더 신속하게 보고를 받고 또한 필요한 정보를 신속하게 찾을 수 있다. 덕분에 보다 신속한 대응이 기대된다.[59]

나. 국가사이버보안동맹(NCSA)의 STAYSAFEONLINE 활동[60]

NCSA[61]는 2001년에 만들어진 민관 공조 단체로서 사용자들의 안전한 인터넷 사용을 도모하고 정보통신망을 보호하기 위해 만들어졌다. 이 단체에는 미 국토안전부(Department of Homeland Security)와 Microsoft, Cisco, Symantec, SAIC, EMC, McAfee 등 세계적인 IT 기업들과 비영리 단체들이 참여하고 있다. NCSA의 설립 목적은 가정용 사용자와 중소 규모의 사업체, 그리고 초등학교와 중고등학교 학생들을 대상으로 하는 사이버 보안에 대한 인식 향상이다.

---

57) http://cve.mitre.org
58) http://nvd.nist.gov/cvss.cfm
59) CVRF 백서 http://www.icasi.org/docs/CVRF-1.2.pdf
60) http://www.staysafeonline.info/ (이하 NCSA의 홈페이지의 내용을 정리)
61) National Cyber Security Alliance

NCSA는 DHS와 다국적정보교환분석센터(Multi-State Information Sharing and Analysis Center: MS-ISAC)가 주도가 되어 국가사이버보안인식 제고의 달(National Cyber Security Awareness Month)이라는 행사를 현재 6년째 해오고 있다. 제고의 달은 10월로 정해져 있으며 이 기간 동안에 사용자와 가장 가까운 학교나 단체 등의 조직을 중심으로 교육과 웹사이트, 소셜미디어 채널을 통해서 보안에 관한 메시지와 정보를 전달한다. 2008년 한 해에만 약 2천 9백 만 사용자에게 미디어와 교육을 통해 보안에 대한 메시지와 교육을 전달한 것으로 집계되었다.

이 단체가 최종 목표로 삼고 있는 것은 사이버 보안에 대한 메시지가 건강한 식생활, 운동, 안전 운전 등과 같이 사용자의 실생활과 밀접한 관계를 가진 것으로 인식하고, 모든 사용자들이 "보안"을 컴퓨터 사용에 필수적인 요소로 고려하도록 하는 것이다. NCSA의 사용자를 위한 웹사이트는 www.staysafeonline.org이다.

NCSA의 눈에 띄는 최근의 활동으로는 2009 국가사이버보안·사이버보안기초교육(National Cyberethics, Cybersceurity Baseline Study) 운동이다. 여기서 NCSA 초등학교, 중고등 학교에서의 사이버 윤리, 사이버 안전, 사이버 보안을 가르쳤고, 이러한 교육을 위한 교사들을 훈련시켰다. 그리고 학교에서 사이버 보안에 대한 교육을 제공할 수 있도록 컴퓨터 보안 전문가들의 자원 봉사를 위한 교육 등이 포함되어 있다.

다. 안티스파이웨어협회(ASC)[62]

ASC[63]는 스파이웨어와 원치 않는 소프트웨어의 위협에 대응하기 위해 안티스파이웨어를 만드는 회사들과 학자들, 그리고 소비자 단체들이 함께 만든 단체이다. ASC에는 현재 마이크로소프트, 안철수 연구소, AOL, CNET Networks, Dell, HP, Google, Internet Education Foundation, McAfee, National Center for Victims of Crime, National Cyber Security Alliance, Symantec, National Network to End Domestic Violence 등 40여 개가 넘는 회사와 단체들이 회원으로 활동하고 있다.

62) http://www.antispywarecoalition.org/ (이하 내용은 ASC 홈페이지의 내용을 정리)
63) Anti-Spyware Coalition

이 단체는 순수하게 공익활동을 하는 단체와 안티스파이웨어를 만드는 회사들로만 이루어졌기 때문에 위의 두 분류에 속하지 않는 회사나 단체는 회원으로 받아들이지 않고 있으며 입법 등에 영향을 주는 로비 활동 등은 전혀 하지 않고 기술적인 면에만 집중하고 있다.

안티스파이웨어의 활동을 위해 통일된 대응 방법을 발전시키는데 가장 커다란 장애가 스파이웨어의 정의를 내리는 것이라고 인식하고 있는 이 단체는 스파이웨어의 정의를 내리는데 많은 노력을 집중하고 있다. 조사 결과에 따르면 소비자들도 어떤 프로그램이 스파이웨어인지 인식을 잘 못하고 있지만 심지어는 안티스파이웨어 업계에서조차도 동일한 기술을 놓고 스파이웨어인지에 대한 정의의 통일이 이루어지지 않고 있기 때문에 ASC가 집중하고 있는 스파이웨어의 정의가 사용자를 보호하고 안티스파이웨어 툴을 개선하는데 많은 도움을 제공하고 있다.

ASC는 “스파이웨어”의 정의를 협의와 광의, 이렇게 두 가지로 제공하고 있다. 협의의 "스파이웨어"는 "사용자에게 적절한 통보, 동의, 또는 제어를 제공하지 않고 설치된 트래킹 소프트웨어(tracking software)"라고 정의하고 광의의 “스파이웨어”는 "스파이웨어와 잠정적으로 원하지 않는 기술: 사용자의 적절한 동의 없이 그리고/또는 사용자의 컴퓨터 사용경험, 사생활, 그리고 시스템 보안에 영향을 미치는 중요한 변화에 대한 사용자의 제어 능력에 영향을 미치는 기술, 어떠한 프로그램이 사용자의 컴퓨터에 설치되었는지를 포함하여 사용자의 시스템 리소스를 사용하는 기술, 그리고/또는 사용자의 개인정보 또는 다른 민감한 정보의 수집, 사용, 배포를 하는 기술"이라고 정의하고 있다.

그러나 ASC의 "스파이웨어"에 대한 정의를 로드맵 삼아 스파이웨어를 만드는 자들이 스파이웨어의 정의에서는 벗어나되 사용자의 컴퓨터에 사용자가 원하지 않는 프로그램을 설치하는 프로그램을 만들도록 악용되지 않게 하기 위하여 매우 조심스럽게 “스파이웨어”의 정의를 규정하고 있으며 오늘날 존재하는 실패 사례에 중점을 두고 자료를 만들되 이 자료는 항상 새로운 경향에 맞추어 갱신하고 있다.

또한 ASC는 안티스파이웨어 기업들이 자사의 프로그램이 부당하게 스파이웨어로 규정되었다고 항의하는 것을 방지하기 위하여 안티스파이웨어 기업들이 따라야 하는 절차들을 정리한 자료를 만들어서 발표하였다.

ASC는 최근에 "Chain of Trust"라는 활동을 국가사이버보안동맹과 함께 시작하였다. 또한 맞춤형 광고에 대한 모범사례도 선정하여 발표하였고, StaySafeOnline이 진행하는 국가 사이버 보안인식 제고의 달을 인정하는 등 보안관 관련된 자율규제단체들과 공조 하고 있다.

라. 사이버보안산업동맹(CSIA)

CSIA[64]는 개인정보보호, 보안, 그리고 정보 시스템의 신뢰성과 보존성을 목적으로 한 국제정책공조 단체이다. [65] CSIA에는 IBM, Symantec, RSA (EMC의 보안 담당 부서), Lavasoft 등 세계적인 보안 기업들이 그 멤버로 참여하고 있으며, 이 단체는 보안에 대한 국회의 입법 활동을 촉구하는 것을 주목적으로 하며 그 목적은 다음과 같다.

o 미국 내에서 사용자 정보를 보호하기 위한 보안과 관련된 입법 촉구
o 스파이웨어로부터 사용자를 보호하는 것을 강화하는 입법 촉구
o EU의 정보 유출에 대한 통지 의무와 전자 통신업자들의 최소한의 보안 요구사항을 입법화 하는 활동
o 중요한 인프라 보호에 대한 정보와 전문성 제공
o 연방 정부의 정보 시스템에 대한 정책 강화

최근의 활동으로는 범죄를 저지를 것을 목적으로 한 스파이웨어를 사용하는 자들을 방지하고 처벌하기 위하여 미국 연방 정부가 통일된 법안을 제정할 것을 촉구하고 있다. 승인받지 않은 스파이웨어와 피싱 사기들에 의해 민감한 개인정보가 손상되고 있고, 스파이웨어로 인한 미국 국가 전체의 경제에 미치는 막대한 손해와 사용자들의 인터넷에 대한 신뢰 상실, 그리고 스파이웨어가 사용자의 컴퓨터에 설치된 원하지 않는 프로그램을 제거하는 것을 방해한다는 이유로 연방 국회가 다음과 같은 내용을 담은 입법을 할 것을 강력히 촉구하고 있다.

o 이미 미국의 수많은 컴퓨터 사용자들이 스파이웨어로 인한 사기행위로 인해

64) Cyber Security Industry Alliance
65) http://www.csialliance.org/ (이하 내용은 CSIA의 홈페이지의 내용을 정리)

금전적인 손해를 보고 있으며, 이에 대응하여 이미 약 20개의 주에서 스파이웨어에 대응하기 위한 법이 마련되었거나 입법 준비가 진행되고 있지만 이러한 주 차원의 입법 활동은 주마다 다른 정도의 사용자 보호 기준을 제공하므로 연방 정부 차원의 통일된 입법 활동이 필요하다고 촉구하고 있으며,

- o 범죄를 저지르기 위해 스파이웨어를 사용하는 자에게는 강력한 형사적 처벌을 내릴 것을 요구하고,
- o 안티스파이웨어 기술에 대해서는 "착한 사마리안 법"을 적용하고,
- o 연방거래위원회(Federal Trade Commission)의 강력한 조치와 규제를 촉구하고,
- o 특정 기술을 처벌하지 말고 나쁜 행동을 처벌할 것을 촉구하고,
- o 안티스파이웨어에 대한 총체적인 솔루션의 하나로 자율규제와 사용자 교육을 포함할 것을 요구하고 있다.

마. 우수한 코드를 위한 소프트웨어 품질검증 포럼(SAFECODE)[66]

SAFECode[67]는 효율적인 소프트웨어 품질검증(software assurance)을 통해 정보와 기술 제품과 서비스에 대한 신뢰를 회복하기 위해 만들어진 비영리단체이다. SAFECode는 업체들의 국제적인 공조를 통하여 좀 더 안전하고 믿을 수 있는 소프트웨어, 하드웨어, 그리고 서비스를 위한 모범사례를 발굴하고 증진하는데 그 목적이 있다. SAFECode에는 Microsoft, EMC, Juniper Networks, Nokia, SAP, 그리고 Symantec Corp.이 회원으로 활동하고 있다. www.safecode.org는 위의 업체들이 공조로 소프트웨어 품질검증(software assurance)에 대한 종합 정보와 뉴스를 제공하는 사이트이다.

SAFECode에 대한 관심이 높아지게 된 이유는 지금까지는 상업용 소프트웨어는 한 곳에서 개발되어 왔으나 시장의 혁신과 경쟁성에 대한 요구가 커지면서 상업용 소프트웨어 개발사들이 점점 전 세계의 사용자를 대상으로 소프트웨어를 개발하고 있고 또한 사업을 운영하는 여러 나라의 엔지니어들을 고용해 소프트웨어를 개발하게 됨에 따라 좀 더 광범위한 접근 방법이 필요하게 되었기 때문이다.

---

66) http://www.safecode.org/ (이하 내용은 SAFECode의 홈페이지의 내용을 정리)
67) Software Assurance Forum for Excellent in Code

소프트웨어 코드 개발 과정 중의 보안을 위해서 전 세계의 고용 가능한 소프트웨어 개발 인력의 고용을 제한하는 것은 현실적인 대안이 될 수 없다. 그러나 세계 곳곳에 산재하는 소프트웨어 개발 인력을 이용한 개발활동으로 인해 제품에 대한 추가적인 보안 이슈가 등장하자 어떻게 이러한 위험을 평가하고 어떤 방법으로 위협의 발생을 줄일 것인지가 중요한 문제가 되었다. 여러 기업들과 정부, 그리고 중요한 인프라 운영자들이 상업용 소프트웨어 의존하는 정도가 점점 커지면서 위의 문제들은 소프트웨어 개발사뿐만 아니라 기업 사용자와 여러 나라의 정부들에게도 똑같이 중요한 문제가 되었다. 그래서 소프트웨어 개발 과정 중의 보안 문제는 "소프트웨어 공급 체인의 보존성(software supply chain integrity)"라는 이름으로 모아지게 되었다. 아직 소프트웨어 공급체인 보존성과 소프트웨어 공급체인(software supply chain)이라는 용어의 정의조차도 확정되지 않은 상태에서 통제할 수 없는 여러 곳에서 소프트웨어 개발이 함께 이루어지고 있는 현실은 사용자와 개발자가 소프트웨어의 무결점을 어떻게 측정하고, 소통하며, 식별할 수 있는지에 대한 중요한 문제를 던져 주었다.

소프트웨어 개발 과정의 보존성에 대한 방법으로 SAFECode가 2009년 6월에 발표한 The Software Supply Chain Integrity Framework에 따르면 [68] 소프트웨어 품질검증 (Software Assurance)은 소프트웨어 개발사, 서비스 또는 솔루션 사업자, 그리고 사용자가 모두 함께 보안(security), 신뢰성(authenticity), 무결성(integrity) 세 요소에 대해 공동으로 책임을 진다.

- o 보안: 보안에 대한 위협은 소프트웨어 설계, 개발, 시험 단계에서부터 미리 예상하고 다루어야 한다.
- o 신뢰성: 사용자가 사용하는 소프트웨어가 복제품이 아닌 진품이어야 하고 사용자가 이를 확인시켜 줄 수 있어야 한다.
- o 무결성: 소프트웨어 제작 단계에서 제품의 부분을 벤더로부터 공급받고, 개발하고, 소프트웨어 개발이 완성되어 제품을 인도하는 단계에 이르기까지 소프트웨어의 기능이 개발사가 의도했던 대로 개발되고 제작되는 것을 의미한다.

---

68) http://www.safecode.org/news.php#press_release_supply_chain. 이하 SAFECode에 대한 요약 설명은 SAFECode 사이트의 자료를 정리한 것이다. The Software Supply Chain Integrity Framework에 대한 전문 참조는 각주의 링크에 있다.

안전한 소프트웨어 프로그램은 위의 세 가지 요소가 모두 필수적이지만 현재 SAFECode에서 준비한 자료에는 일차적으로 소프트웨어 개발사가 어떻게 위협에 손상되지 않은 소프트웨어를 개발하여 개발사가 의도한 대로 사용자에게 인도할 수 있는지에 대한 소프트웨어 무결성 문제를 다루고 있다.[69]

소프트웨어 공급사슬 무결성 체계(The Software Supply Chain Integrity Framework)에 의하면 소프트웨어 대부분 파일의 집합체이기 때문에 성공적인 소프트웨어 공급체인에 대한 공격은 기존의 소프트웨어 파일의 변형 또는 소프트웨어 파일의 집합체에 새로운 파일을 추가하는 형태를 띤다고 한다. 공급체인에 대한 공격에 관한 보고서[70]의 결론에 의하면 모든 잠재적인 공격에 대해서 한 가지의 방법으로 방어를 할 수는 없으며, 소프트웨어의 보안을 위해서는 소프트웨어가 개발되는 장소에 집중하기보다는 소프트웨어가 어떤 절차를 거쳐서 개발되고 시험되는지에 집중하는 것이 훨씬 더 효율적이라고 한다. 그리고 때로는 악성 코드가 소프트웨어에 삽입되는 것을 탐지하는 것이 거의 불가능한 경우도 있다는 것을 인식하게 되었다.

물론 소프트웨어의 개발 단계에서 누군가가 악성코드를 심어 놓을 가능성이 있기는 하지만 많은 전문가들은 소프트웨어 제작 공급 단계에서 공격을 할 가능성이 크지 않다고 판단한다. 그러나 제작 공급 단계에서부터 위협이 존재한다면 예방적인 조치를 취해야 할 필요가 있다. 현재까지는 각 개발사들에게는 각 개발사의 고유 절차들이 있었고 개발사들이 공동으로 이러한 문제를 다룰 수 있는 기회가 없었다. 그래서 SAFECode는 다음과 같은 업계 공동의 지침을 발표하게 되었다.

다음은 SAFECode가 발표한 지침의 요약이다.

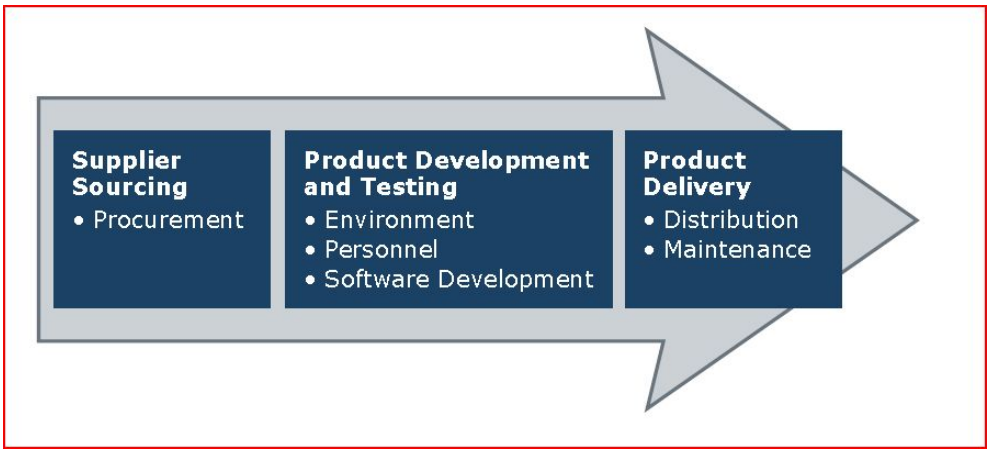
---

69) http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf

70) “Mission Impact of Foreign Influence on DoD Software," U.S. Defence Science Board, September 2007. "Foreign Influence on Software:Risk and Recourse," Center for Strategic and International Studies, march 2007. "Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization," U.S. Committee on national Security Systems, November 2006

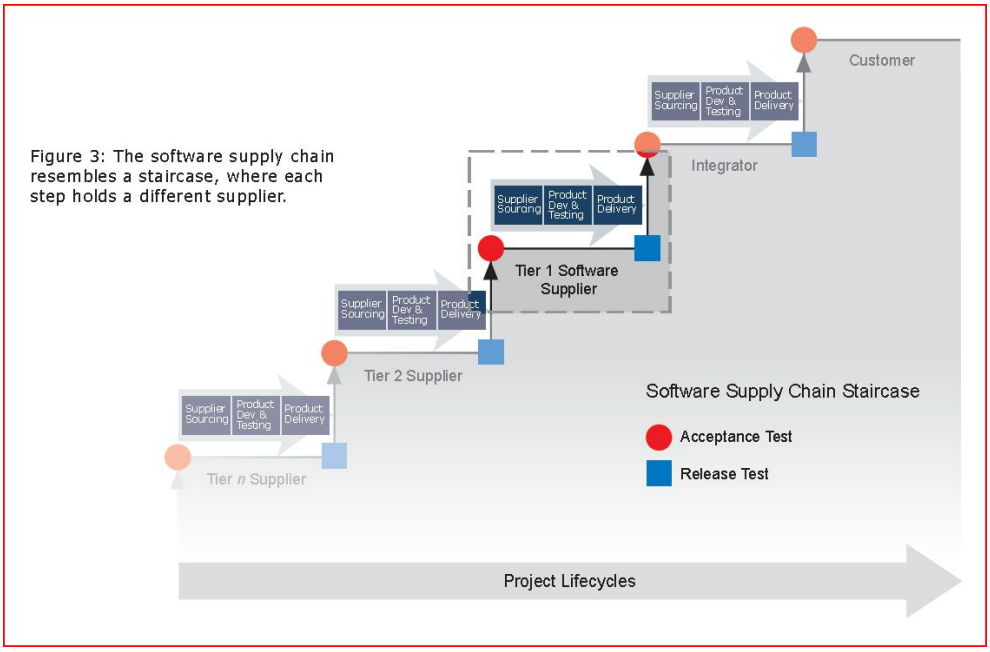
소프트웨어 개발은 다음과 같은 과정을 거친다.

1) 공급의 경로: 소프트웨어 개발이 자체적으로 모두 이루어지는 경우도 있지만 각 컴포넌트 별로 외부에서 제작되는 경우도 있는데, 이 경우 컴포넌트를 제작할 공급자를 선별하고, 공급자에게 기대하는 결과물을 확정하고, 소프트웨어와 하드웨어 결과물을 공급자로부터 제공 받는 단계를 말함
2) 제품의 개발과 시험: 자체개발한 컴포넌트와 외주를 통해 제공받은 컴포넌트들을 취합해 시험을 거쳐 출시하도록 마지막 과정을 거치는 단계
3) 제품의 인도: 완성된 제품을 고객에게 인도하고 제품을 유지하는 단계



<그림1> 소프트웨어 개발과정

그러나 위의 과정을 거쳐 사용자에게 인도된 소프트웨어가 커다란 IT솔루션의 한 부분일 경우 보안 문제는 더욱 복잡해진다. 그런 경우 각 단계 별로 공급자는 각 단계에서 무결성을 확인해야 한다.



<그림2> 단계별 무결성 확인 절차

그리하여 SAFECode는 소프트웨어 무결성에 대한 제어 과정을 디자인할 때 다음과 같은 원칙을 지킬 것을 권장하고 있다.

- o 각 단계에서의 책임 확인: 개발 단계에서 이루어지는 모든 변경이나 단계 완성이 승인된 투명한 절차를 따랐으며 이를 확인하는 것이 가능함
- o 최소한의 권리만 승인하여 접근하도록 함: 데이터에 접근하는 직원은 그 업무를 수행하기 위한 최소한의 권리만 주어질 것
- o 업무 책임의 분리: 직원 한 사람이 일방적으로 코드를 변경하거나 또는 개발 과정을 관리하지 못 하도록 할 것
- o 허락되지 않은 접근을 방지하고 허락되지 않은 접근에 대한 기록의 보존: 승인 없이 접근하는 행위는 금지되어 있으며 승인 없는 접근이 있었을 경우 반드시 이러한 행위가 작업 중에 표시가 되고 또 행위를 취소할 수 있어야 함
- o 지속적인 보호: 개발 장소로부터 옮겨졌을 경우에도 중요한 자료는 지속적으로 보호 될 것
- o 지침 준수에 대한 관리: 보호가 항상 독립적으로 또한 지속적으로 되고 있는지 확인할 수 있을 것

o 코드 시험과 검증: 코드 검사 후 수상한 코드는 제거할 것.

2. 호주의 자율규제 현황

가. Australian Internet Security Initiative (AISI)[71]

호주의 AISI는 2005년 호주의 통신미디어부(Australian Communications and Media Authority: ACMA)와 6개의 ISP들이 모여 만든 민관 협의체이다. AISI의 설립 목적은 봇(bot)을 줄이기 위함이다. 봇이란 인터넷에서 자동으로 특정 업무를 수행하는 인터넷 응용 프로그램을 의미한다. 봇은 스팸 메일을 보낼 이메일 주소 수집 등 악의적인 용도로 쓰이기도 한다. 봇은 좀비컴퓨터(악의적인 작업을 수행하는 해커의 컴퓨터 또는 해커에 의해 감염된 일반인의 컴퓨터)에서 작동하므로, AISI는 이 좀비컴퓨터 수를 줄이기 위해 노력한다. AISI는 2006년도 중반까지 시험 기간을 거쳐서 정식으로 활동을 시작하였고, 현재는 67개의 ISP사들이 회원사로 있다. 2009년 현재 회원 ISP들은 호주 내 ISP 고객의 90% 이상을 커버하고 있다.

대부분의 안티봇들이 봇의 악의적 행동을 무력화하는데 관심을 두는 반면, AISI는 가정용 PC나 소규모 사업체들이 스팸메일을 받지 않는 방법이나, 중요한 정보를 해킹당하지 않기 위한 방안에 중점을 두고 있다.

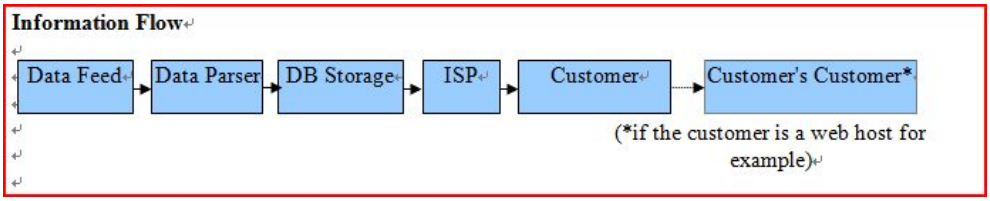
AISI는 봇넷(여러 봇들의 집합)을 줄이기 위해 보다 종합적인 방법을 택하여, 봇넷을 줄이기 위한 기술적인 접근보다는 봇넷을 줄이기 위한 절차에 초점을 맞추었다. 이에 데이터 제공자와 ACMA, 그리고 ISP 간의 협력을 통해 성공적인 자율규제 모델을 구성하였다. 이는 과거 기술적 혁신에만 의존해왔던 과거의 접근방법과는 다른 것이다.

ACMA는 국제통신기구(International Telecommunications Union: ITU)와 함께 봇넷 이주 도구(Botnet Mitigation Toolkit)을 이용해 대응하고 있다. 정보의 제공

71) 자세한 내용은 ACMA's AISI에 대한 General Information 참조한다. 아래의 내용은 AISI에 대한 내용은 AISI로부터 제공받은 AISI General Information, AISI Information for Governments and Industry의 번역 요약이다.

과정은 다음과 같다.

나. AISI의 정보 유통 과정 (**Information Flow**)



<그림3> AISI 정보 유통 과정

위의 정보 유통에 대한 설명은 다음과 같다.

1) 정보제공 (Data Feed)

AISI는 좀비에 감염된 PC에 대해서 정보를 밝힐 수 없는 제3자와 AISI의 스팸 트랩으로부터 정보를 얻는다. 스팸트랩은 스팸 메일을 모으기 위한 목적으로 만든 이메일 계정이다. AISI는 지속적으로 새로운 정보를 수집하고 있다. 입력 데이터가 AISI가 늘 원하는 방식으로 주어지는 것만은 아니기에, AISI는 종종 자료를 수정하여 사용하기도 한다.

AISI는 민관 공조 단체로서 많은 정보를 ACMA에 무상 제공하고 있다. 일부 정보 제공자들은 자신들이 제공한 정보가 공개적으로 공포되는 것을 원하지 않거나 (non-attribution of their data), AISI와의 협력 관계가 알려지는 것을 원하지 않는다. 그래서 그러한 제공자를 위하여 AISI는 협력 관계에 있는 단체나 개인을 밝히지 않고 있다.

2) 데이터 파서 (Data Parser)

ACMA는 AISI의 데이터 파서를 자체적으로 제작하였다. 데이터 파서는 앞 단계

에서 수집된 자료를 의미 있는 단위로 나누는 역학을 한다. 대부분의 데이터는 CSV 타입 파일로 하루에 한 번씩 입력된다. 이 외에도 이메일, HTTPS, RSYNC 등을 통해서도 비슷한 양의 데이터를 수집하고 있다. 이렇게 모아진 자료들 중 필요한 부분은 적절히 가공하여 AISI의 데이터베이스에 저장한다.

ACMA는 스팸 방지 운동을 적극적으로 펼치고 있으며, 그 일환으로 ACMA는 자체 스팸트랙을 운영 중이다. 그렇지만 수집되는 정보의 양도 굉장히 많을 뿐 아니라 자동 시스템의 100% 정확성을 확신할 수 없기 때문에 자동 시스템을 이용해서 스팸 자료를 수집할 때에는 주의해야 한다. 그래서 이러한 위험을 줄이기 위한 노력으로 ACMA는 도메인과 주소를 합법적인 메일에는 절대 사용되지 않도록 스팸트랩을 셋업한다.

사용자가 스팸 메일이라 보고한 것에는 문제가 많다. 실례로 사용자로부터 보고를 받은 스팸 방지 프로그램은, ISP가 보낸 청구서 등도 스팸 메일로 분류한 경우도 있다. 그래서 사용자가 제공하는 데이터는 현재는 사용되고 있지 않다. 스팸은 문제가 많고 지속적인 모니터링이 필요하기 때문에 잘못된 정보를 얻지 않기 위해서는 그 기준을 높이 정해 놓아야 한다.

3) 데이터 저장 (Database Storage)

AISI는 PostgreSQL 데이터베이스에 정보를 저장하고 있으며 Intel에 기반을 둔 리눅스 플랫폼을 사용하고 있다.

4) ISPs

ISP들은 스팸 메일의 본문 내용과, 분석을 위해 추가적인 이메일 정보(이는 주로 탭으로 분리되어 컴퓨터가 쉽게 분석할 수 있다)를 받는다. ISP들은 이 정보를 수동 또는 자동으로 고객지원 추적 시스템(RT Request Tracker 등)에 입력한다. ISP들은 사람이 읽을 수 있는 데이터 기록과 탭으로 분리되어 컴퓨터가 분석하기 좋게 작성된 첨부 파일을 꾸준하게 메일로 받는다. 어떤 ISP는 한 걸음 더 나아가

이 정보를 네트워크 관리 시스템에 넣어서 감염 문제가 해결될 때까지 외부로 발송하는 메일 연결을 제한하기도 한다.

ACMA는 감염 사고가 발생하면, ISP가 사용자들에게 감염되었다는 사실을 통보하도록 강제하고 있다. 이러한 노력을 위해서 ISP는 추가 인력을 고용해야 하는 부담이 있다. 그래서 몇몇 ISP들은 이러한 사용자 대응 노력에 들어가는 비용을 절약하기 위해서 보안제품이나 보안서비스를 고객에게 사전에 제공하기도 한다.

그러나 ISP의 추가 비용 부담에도 불구하고, 2009년도에 실시한 조사에 따르면 대부분의 ISP들이 AISI가 ISP들의 네트워크에 있는 감염 PC를 찾는데 도움이 되고 있다고 대답하였다. 더 나아가 AISI가 (1) ISP와 고객의 상호 관계의 개선, (2) 소스데이타를 통한 감염의 성격을 파악, (3) ISP 자체 내에 있는 감염 PC 보고에 대한 보완 등에 도움이 된다고 응답하였다.

그리고 조사에 의하면 사용자들도 자신의 PC가 감염된 사실을 통보받는 것을 유용하다고 생각하였다.

다. 사용자와 ISP와의 관계

위와 같이 분석이 데이터에 대한 수집과 분석이 끝나고 나면 ISP는 감염된 PC의 사용자에게 감염 사실을 통보한다. AISI의 초기 회원사 중 하나인 호주의 Westnet의 사이트에서 제공하는 사용자 통보를 한 예를 보자면 다음과 같다.

"귀하는 귀하의 PC가 악성 프로그램에 감염된 경우, Westnet로부터 이메일 통보를 받으실 수 있습니다. Australian Internet Security Initiative에 대한 저희의 약속의 일환으로 Westnet은 감염된 모든 PC의 사용자에게 통보하는 것을 목표로 삼고 있습니다. 만일 귀하가 Westnet으로부터 이메일을 받으면 놀라지 마시고 아래의 지시를 따르십시오. 그리고 문제가 계속되면 Westnet의 지원팀으로 연락을 해주시기 바랍니다. 저희 지원팀이 귀하의 문제를 해결하는 데 도움을 드릴 수 있습니다. 만일 문제가 저희 지원팀에 의해 해결이 되지 않으면 컴퓨터 기술자를 방문해 보시기 바랍니다. 그러면 Westnet의 기술자가 도와 드릴 수 있습니다. 그리

고 사용자 계약에 의하여 귀하의 컴퓨터가 감염이 되었거나 취약점이 있을 경우 Westnet은 귀하께서 컴퓨터를 치료할 수 있는 기간을 7일을 드립니다. 만일 이 기간 동안에 문제가 치료되지 않으면 서비스에 제한이 있을 수 있습니다. 만일 문제가 심각하다면 서비스는 자동으로 제한될 수 있습니다."

그리고 업계는 Internet Industry Spam Code of Practice (ACMA에 등록되어 있음)를 만들어서 감염된 PC의 사용자에 대한 조치를 취하는 ISP들을 보호하고 있다. ISP가 취할 수 있는 조치에는 서비스 제한, 서비스 중지, 그리고 심각한 경우에는 서비스 차단을 포함한다. 그러나 ISP로 하여금 그러한 조치를 취할 것을 강제하지는 않는다.

2009년 6월에 호주인터넷산업협회(Australian Internet Industry Association: IIA)는 자율적인 인터넷 보안 실천 규칙(e-security code of practice)을 제정하였다. 이 실천 규칙에서 주요한 점은 ISP가 일관적이고 공정하고 유연하게 조치를 취할 수 있도록 한 것이다. 그리고 이 규칙은 ISP가 AISI와 어떤 절차를 거쳐서 협조를 할 것인가에 대한 내용도 담고 있다. 이 규칙은 2009년 말에 완성될 것으로 예상된다.[72]

라. AISI의 운영에 대한 참고 자료

1) 사용자 측면에서

ACMA는 ISP의 고객들과 직접적인 접촉을 하지 않는다. 감염된 PC의 사용자가 ISP의 통보를 받은 후 ACMA를 직접 연락하지 않는 이상 감염된 PC의 사용자가 누구인지도 알 수가 없다. 이러한 절차를 통하여 사용자가 가지고 있는 개인정보 보호에 대한 우려를 줄이고 있다.

ISP들이 고객을 처리하기 때문에 ACMA는 감염 내용에 대한 자세한 정보를 얻기 힘들다. 감염을 보고한 자료에 따라서 때로는 사용자가 어떤 악성 프로그램을

72) 자세한 내용은 www.iia.net.au를 참조한다.

찾아야 하는지 알기 힘든 경우도 있다. 이런 경우에는 ISP의 고객상담부서(help center)에서도 사용자의 PC에 설치되어 있는 운영체제와 백신 소프트웨어가 최신 프로그램인지를 확인하라는 일반적인 조치만을 취할 수밖에 없다. 안타깝게도 로그를 남기지 않는 방화벽과 함께 사용되는 수동적인 악성코드 탐지 방법은 중소기업이 감염 컴퓨터를 찾아낼 때 필요한 기술 지원에 도움이 될 만한 정도의 상세 내역을 제공하지는 않는다.

사용자들은 ACMA의 노력에 긍정적인 모습을 보였다. 드물게 긍정 오류(false positive)로 인해 실제로 감염되지 않은 컴퓨터의 사용자가 인터넷 사용을 제한받는 경우가 있기도 하지만 이러한 경우에도 사용자들은 보안 문제에 대한 정보를 제공받고, 또 이를 바로 고칠 수 있다는 점에서 긍정적으로 반응하였다.

2) 재정적, 행정적인 측면

2005년에 시범 프로그램으로 출범한 AISI는 호주 광대역 통신과 디지털 경제 부(Department of Broadband Communications and the Digital Economy)에서 재정적인 지원을 받고 있다. 처음 출범하였을 때 하드웨어와 호스팅에 사용된 비용은 약 5만 불, 그리고 인력 비용으로 약 10만 불 정도였다. 그러나 출범 이후에는 인력 비용이 상당히 많이 증가하였다.

AISI는 위의 시스템을 Unix와 유사한 운영체제 그리고 오픈소스 소프트웨어를 사용하여 구축하였다. 현재는 Linux/PostgreSQL/Python 플랫폼과 SUN Niagara24-Core 서버를 솔라리스에서 사용하고 있다. 그러나 인력 구성에 따라 Windows/SQL Server/.NET 프레임워크를 선호할 수도 있다.

ACMA는 앞으로도 업계로부터 더 많은 피드백을 받기 위하여 ISP와의 연계를 좀 더 강화하고자 한다. ACMA와 자료 제공자와의 연락은 항상 기술 인력들이 담당하고 있고, AISI에 전담된 3명의 기술직원은 주로 개발과 시스템 유지, 그리고 ISP의 질의에 응답하고 있으며, 리포트의 정확성을 위해서 스팟 체크를 하고 있다.

3) ISP를 위한 정보

가) AISI에 참여하는 이유

ISP들은 AISI에 참여함으로써 ISP의 사용자들에게 사용자의 컴퓨터의 감염 사실을 알리고 치료를 유도할 수 있다. 또한 호주 인터넷의 전반적인 보안 향상에 기여할 수 있다. 그리고 봇넷에 감염된 PC들이 일으킬 수 있는 신분 절취, DDos 공격, 스팸의 유포, 악성 프로그램의 유포, 불법적인 내용의 유통(어린이 포르노) 등을 차단할 수 있다.

나) ISP가 AISI에 참여하기 위하여 제공하여야 하는 정보

o IP 주소 범위 (CIDR format 선호)
o AISI가 매일 보내주는 감염 리포트를 받을 수 있는 주소 (이 경우 담당 직원이 바뀌어도 변경되지 않는 대표 주소를 선호한다.)
o 그리고 기술적인 내용과 운영 측면에서 정보를 교환할 수 있는 직통 연락 번호
o ISP 의 Autonomous System Number (이 번호가 있으면 ACMA가 제공된 IP 범위정보에 에러가 없다는 것을 확인할 수 있음)
o ACMA 리스트에 기록되고자 하는 회사의 이름

다) 리포트에 포함되는 감염의 종류

ACMA는 여러 경로로 감염된 PC의 IP주소를 받고 있으나 이 경로는 완벽하게 비밀로 유지가 되고, 새로운 경로가 추가되기도 한다. 그리고 탐지를 할 때에도 최신의 방법을 이용한다.

AISI의 일일 리포트에 포함되는 정보는 예를 들어 'Trojan: Beagle/Bagel', 'Trojan: Blaster', 'Trojan: Generic', 'Trojan: Nachi', 'Trojan: Slammer', 'Trojan: Stormworm', 'Trojan: Toxbot' and 'Spam/Misconf.Mailer 등 여러 형태의 트로이

목마를 명시하고 있으므로 대부분의 경우 추가 설명이 필요 없지만 어떤 감염은 좀 더 자세한 설명이 필요한 경우도 있다. 그러한 감염의 목록은 다음과 같다.

- o Malware Serving Host: 종종 나타나는 것은 아니지만 이 경우는 리포트의 맨 위에 나타나며 신속한 조치가 필요한 정보이다. 이름이 명시하듯이 위의 정보는 악성 프로그램을 호스팅 하는 URL로 밝혀진 것이다.
- o Spam/Misconf.Mailer: 이 경우는 리포트 되는 경우 중 대부분을 차지하는 카테고리로서 트로이 목마 메일 송신자의 역할을 하는 감염된 PC에 관한 정보이다.
- o fastflux: 패스트 플럭스는 IP 주소를 빈번하게 바꾸는 기법이다. 불법 호스팅 서버가 이 기법을 이용하면, 인터넷 보안 기관들은 이 불법 서버를 종료시키기 어렵다. 주로 불법 피싱 사이트나 아동 포르노 사이트가 이 기법을 이용한다. 패스트 플럭스에 대한 리포트는 최근 24시간 동안 보고된 IP 주소에 해당하는 URL을 포함한다. 패스트 플럭스를 잡아낼 때, 긍정 오류(false positive)가 발생할 수 있다. 패스트 플럭스 기법은 IP 주소를 계속 바꾸므로, 보고된 주소가 더 이상 감염된 컴퓨터가 아닐 수 있다. 하지만, AISI에 아직 이러한 사례가 보고된 적은 없다.
- o Scanner: 스캐너는 인터넷 포트(port)의 상태를 훑어보는 호스트이다. 스캐너는 본디 악의적인 목적에서 만들어지진 않았다. 그러나 만약 스캐너가 사용자 몰래 실행되고 있다면, 이는 스캐너가 트로이 목마를 미래에 감염시킬 포트를 찾고 있다고 볼 수 있다.
- o openresolvers: Open resolver는 DNS 서버로서 인터넷 상의 모든 컴퓨터들에게 반복적인 검색을 허용한다. DNS 서버의 반응(response) 정보의 양은 요청(request)시의 그것보다 훨씬 많다. 그리고 DNS 쿼리(query; 요청을 보내는 명령)는 UDP로 전송된다. UDP로 전송되는 패킷은 중간에 훔쳐보기가 쉽다. 이렇게 보안상 취약점을 통해, open resolver는 DNS 증폭(DNS amplification)이라 불리는 공격을 허용할 수 있다. DNS 캐시 포이즈닝(DNS cash poisoning) 기법 역시 가능하다. 공개된 웹 프록시나 메일 릴레이를 쓰는 데에는 이론적으로 이러한 보안상 위험 요소가 있다.
- o Trojan:Conficker: Conficker는 Downadup이라고도 알려져 있다. 이 트로이 목

마는 감염된 컴퓨터를 Conficker 제작자의 컴퓨터(Conficker sinkhole)로 연결한다. 이렇게 연결된 피해자의 컴퓨터를 트로이 목마 바이러스 제작자들이 조종할 수 있다. 봇넷 방지 단체들은 Conficker를 막기 위해 이에 사용되는 도메인들을 구매하였다. 구입된 서버들은 접속하는 IP를 ACMA에 보고하였다.

- o Trojan:MEBRoot: MEBRoot는 종종 Torpig 또는 Sinowal 트로이 목마와 함께 나타난다. MEBRoot는 온라인 로그인 정보를 가로채고, 마스터부트정보(MBR: master boot record)를 숨기는 것으로 잘 알려져 있다. 이 트로이 목마는 부트 영역에 상주하므로, 백신 등을 통해 이를 색출하고자 할 때는 '깨끗한 환경'에서 실시해야 한다. 복구 CD 등을 통한 환경이 그 예이다.
- o Trojan: Grum: Grum은 스팸 메일을 통해 퍼진다. "Hot Pictures of Britney Speers(브리트니 스피어스의 화끈한 사진)"가 알려진 스팸 메일의 제목 중 하나이다. 이 메일에는 트로잔이 다운로드 되는 링크가 포함되어 있다. Grum은 Windows의 취약점을 악용하여 WINLOGON.EXE 파일을 감염시킨다.
- o Trojan:Clampi: Clampi는 드롭퍼(dropper)이다. 이는 실제로 악의적인 활동을 할 다른 악성 프로그램을 감염된 PC에 다운받는다.
- o Trojan:Delf.HPT: Clampi는 드롭퍼(dropper)이다. 이는 실제로 악의적인 활동을 할 다른 악성 프로그램을 감염된 PC에 다운받는다. 이 트로이 목마가 접속을 시도하는 주소는 "http://74.208.64.191/hk1xx/getconf.php"이다.
- o Trojan:Delf.FZ: Delf.FZ는 감염된 PC에 수많은 .EXE 파일을 생성한다. 그리고 수많은 원격 URL로 접속을 시도한다. Delf.FZ 역시 드로퍼이다.
- o Trojan:Goldun: Goldun은 마치 HTTP나 SOCKS 프록시처럼 보이게 작동한다. 이 트로잔은 원격지에서 감염 PC를 불법적으로 조종할 수 있도록 백도어(backdoor)를 가진다. 프록시 포트, 감염 PC의 가동 시간, 감염 PC가 PayPal, eBay 등의 계좌 정보를 가지고 있는지 등이 GET 요청(GET request)을 통해 전송된다.
- o Trojan:Zeus: Zeus는 키로거(keylogger; 감염된 PC의 사용자가 키보드에 치는 내용을 악성 프로그램 제작/설치자에게 전송하는 악성 프로그램)이다. 이는 보통 인터넷 뱅킹 정보를 빼내는 데 이용된다. 이 트로잔은 검출을 피하기 위해

루트킷을 이용한다.

3. 마이크로소프트의 자율규제 사례

가. 마이크로소프트사의 악성 프로그램 방지 연구와 대응[73]

바이러스, 트로이 목마, 그리고 다른 악성 소프트웨어들과 스파이웨어, 그리고 원하지 않는 소프트웨어들은 IT 전문가들에게는 끊임없는 우려의 대상이다. 그리고 공격의 방법과 위협이 점점 복잡해질수록 사회공학기법(social engineering; 사용자를 기망하여 정보를 빼내는 기법)이 증가하고 해커들이 시스템을 감염시키려고 하는 시도가 많아진다.

이에 대응하기 위해서는, 네트워크·게이트웨이·응용프로그램·운영체제 등을 모두 포함한 총체적인 보안 체제가 필요하다. 그래서 마이크로소프트에서는 기업과 일반소비자, 모두를 위한 보안 솔루션을 개발하여 정보의 보호와 접근제어를 돕고 있다. 마이크로소프트의 악성 프로그램 방지 솔루션은 우수한 기술과 전담팀, 그리고 철저한 내부 절차 등을 통해 공급되고 있다. 특히 Microsoft Malware Protection Engine과 Microsoft Malware Protection Center는 주목할 만하다.

Microsoft Malware Protection Engine은 악성 프로그램의 정의에 따라 악성 프로그램을 탐지하고 피해를 예방하는 프로그램이다. 이와 함께 Microsoft Malware Protection Center는 새로운 악성 프로그램에 대한 조사와 신속한 대응을 통한 사용자 보호 활동에 중점을 두고 있다.

나. Microsoft Malware Protection Center

Microsoft Malware Protection Center는 사용자들에게 바이러스, 스파이웨어, 그리고 기존의 악성 프로그램과 새롭게 추가되는 악성 프로그램들에 대항한 전방위적인 보안을 제공하는데 그 목적을 두고 있다. 이 센터는 Forefront Client 보안,

73) Understanding Anti-Malware Research and Response at Microsoft, 2007, Microsoft 이하 자료는 위의 자료를 번역정리 하였다.

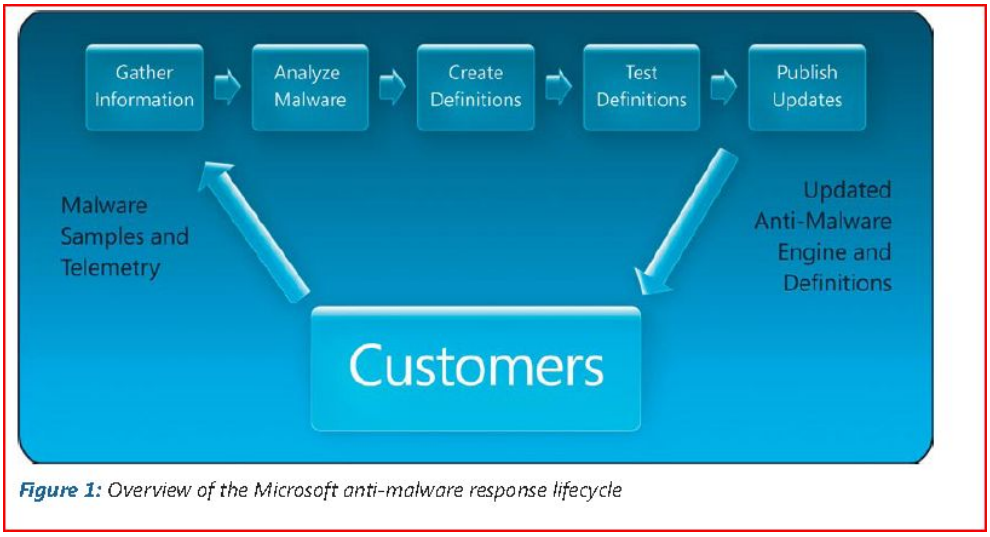
Forefront Server 보안, Windows Live OneCare, Windows Defender를 위한 중요 악성 프로그램 방지 기술과 그 외 기타 마이크로소프트의 보안 솔루션과 기술을 제공한다.

Microsoft Malware Protection Center에서는 악성 프로그램에 대한 끊임없는 연구를 통해 보안 위협에 대한 중요 트렌드와 소프트웨어 취약점에 대한 청사진을 제시한다. Microsoft Malware Protection Center가 연구한 악성코드의 유형은 다음과 같이 진화해 왔다.

- o 경제적 이익을 얻기 위해 특정인 대상의 악성코드 배포(Targeted Malware Distribution): 악성 프로그램 배포의 성격이 달라지고 있다. 과거의 Blaster나 Sasser와 같은 웜들은 굉장히 빠른 속도로 전 세계에 퍼졌지만, 요즘에 나오는 악성 프로그램들은 자기 복제를 하지 않는 트로이 목마와 같이 사용자나 보안 업체들이 감지하기 어렵도록 만들어진다. 예를 들어 악성 프로그램 제작자들은 컴퓨터가 다운되거나 네트워크 트래픽의 증가와 같은 감염의 명백한 현상이 나타나지 않도록 디자인하고 있다.
- o 복잡한 위협의 증가: 악성 프로그램을 만드는 기술들도 점점 발전해 이전에는 악성 프로그램 개발자들이 보안 소프트웨어의 위협에 따라 악성 프로그램들을 변형시켜왔지만, 이제는 미리 여러 가지 버전의 악성 프로그램을 사전에 만들어 놓고 보안을 피하기 위한 준비를 미리 해 놓는다. 악성 프로그램을 만드는 자들은 루트킷이나 패커(packers)를 이용하여 들키지 않도록 하고 있다. 그리고 악성 프로그램을 만드는 자들은 사회공학기법을 이용해서 사용자들이 소프트웨어를 본인의 PC에 다운받도록 하는 방법을 취하고 있다.

이러한 위협을 방지하기 위해서는, 끊임없는 데이터 분석과 조사가 중요하다. 보안에 대한 최근의 위협은 점점 횟수가 증가하고, 복잡해지며, 경제적 이익을 노리고 있는 것이 특징이다.

마이크로소프트의 악성 프로그램 방지 대응 단계는 다음 표와 같다.



<그림4> 마이크로소프트의 악성 프로그램 방지 대응 단계

Microsoft Malware Protection Center는 다단계 과정을 통하여 사용자와 보안업체들과 상호 작용을 하고 있는데 그 과정과 역할은 다음과 같다.

o 업계와의 협력: 보안은 전 세계적인 문제이며 사용자가 어떤 보안 프로그램을 선택하는지 와는 상관없이 컴퓨터들은 서로 연결되어 있어 감염된 컴퓨터가 건강한 컴퓨터를 공격해서 수많은 스팸을 전송하거나 DDoS공격을 하는 컴퓨터로 사용될 수 있는 생태계 안에 있다. 그러므로 업계는 이러한 사실을 인지하고 정보를 공유하여 보안이 한 단계 앞으로 나아가도록 하여야 한다. 업계의 협력을 증진시키기 위한 노력으로 마이크로소프트는 바이러스정보동맹(Virus Information Alliance: VIA)을 만들었다. 안티-스파이웨어협회(Anti-Spyware Coalition)에는 창립회원으로 참가하고 있다. 안티-피싱실무그룹(Anti-Phishing Working Group)의 우선 멤버로도 활동 중이다.

o 전 세계로부터의 정보 수집: 분석의 처음 단계는 악성 프로그램에 대한 데이터의 수집인데 이 정보는 자동화된 수집 도구, 제품지원, 그리고 업계의 샘플 공유와 같은 여러 채널로부터 수집된다. 그러나 가장 유용한 정보는 전 세계 사용자가 제공하는 정보이다.

o 악성 프로그램 연구 분석: 연구팀은 의도적인 은폐(obfuscation)와 같이 악성

프로그램에 의해서 사용되는 기술과 전략들을 분석한다. 현존하는 악성 프로그램으로부터 얻어지는 많은 정보들은 미래의 보안 위협에 대한 대응을 강화하는데 사용된다.

- o 악성 프로그램 대응팀: 대응팀은 사용자 문제에 대한 솔루션을 신속하게 제공한다.
- o 시그니처 정의(Signature Definitions): 악성 프로그램이 분석된 후 나오는 최종 산물은 악성 프로그램 시그니처(malware definition)이다. 이 정보는 엔진이 위협을 찾아서 제거하는데 사용되는 데이터[74]이다. 이 정의는 실시간 사용자 위협에 근거해 조사해야할 중요한 아이템들을 포함한다.
- o 시험: 악성 프로그램 정의가 만들어진 후에는 악성 프로그램 시그니처(malware signiture)가 기대했던 것처럼 작동하는 지에 대한 철저한 테스트가 따른다. 만일 잘못된 분류(misclassification)가 발견되면 업데이트가 따르고, 변경된 정의가 만들어지고 테스트를 거치고 이전 정의를 대치하기 위해 발표가 된다. 이런 방법으로 사용자는 악성 프로그램의 정의를 모아놓은 파일(definition file)에서 새로 나타나는 위협에 대한 보안조치를 취할 수 있다. 악성 프로그램 패턴 갱신(definition update)에는 중요한 악성코드 방지 엔진에 대한 갱신도 포함한다.
- o 배포(Publishing): 악성 프로그램의 패턴이 시험(testing)을 통과하여 인증이 되면 디지털 서명을 거쳐서 사용자 배포를 위한 준비를 한다. 디지털 서명은 파일이 안전하고 인증되었다는 것을 보증하고, 배포용 패키지(distribution package)는 클라이언트를 위한 여러 종류의 부분 또는 전체 업데이트를 돕는다. 얼마나 자주 클라이언트가 업데이트 되는지에 따라 악성 프로그램 시그니처 중 일부만이 변경될 수도 있다. 마이크로소프트는 악성 프로그램 시그니처 업데이트(definition updates)를 하루에도 여러 번 발표된다. 그러면 "관리자"는 Windows Software Update Service 또는 Group Policy 등에 따라 업데이트할 수 있다.
- o 사용자 교육: 위의 과정에 추가로 분석팀은 필요한 정보를 악성 프로그램 백과사전에 입력하여 사용자에게 위협의 성격과 부작용, 그리고 어떤 조치가 필요

74) 정의, 정보 또는 시그니처를 말한다.

한지에 대한 정보를 추가로 제공하기도 한다.

사용자의 피드백은 연구대응팀에게 매우 중요한 정보이다. 사용자들은 악성 코드 목록을 정의하고(definitions) 악성 소프트웨어를 스캔하여 감염컴퓨터의 정보(telemetry information)와 샘플을 Microsoft Malware Protection Center로 보낼 수 있다. 사용자가 적극적인 참여는 악성 프로그램의 경향에 대한 정보를 신속하게 제공하므로 Microsoft Malware Protection Center에서는 업데이트를 통하여 신속하게 대응할 수 있다.

아래 표는 Microsoft Malware Protection Center와 세계적으로 악성 프로그램 연구 시스템을 요약하여 보여준다.

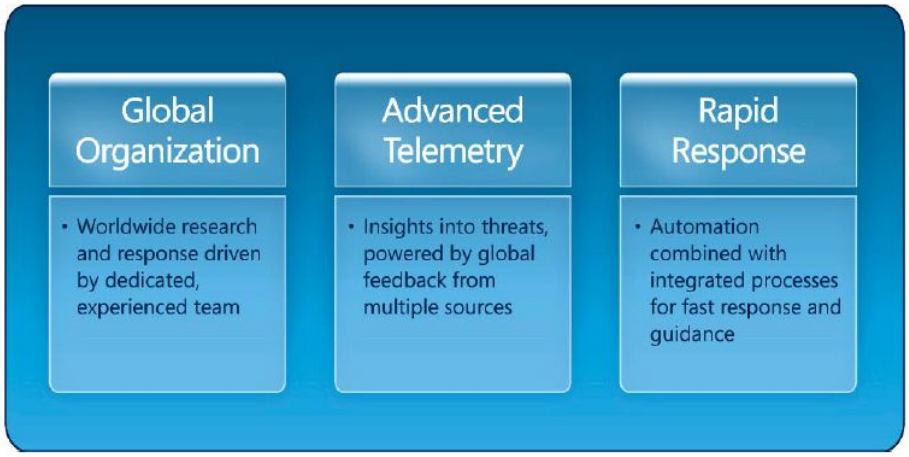


Figure 2: *Key characteristics of the Microsoft Malware Protection Center*

<그림5> 마이크로소프트 악성프로그램 보호 센터 연구시스템

Microsoft Malware Protection Center는 유럽, 미국, 아시아에서 일 년 365일, 하루 24시간 동안 끊임없이 정보를 분석하고 있다. 이 팀은 마이크로소프트의 보안 제품에 대한 지원을 책임지고 있기 때문에 전 세계의 수백만 대의 컴퓨터를 지원과 보안을 통해 얻는 경험의 혜택을 받고 있으며, Product Support Services

Security와 Microsoft Security Response Center와의 정보 공유와 연계활동을 통하여 악성 프로그램 문제를 함께 해결하고 있다.

1) 감염컴퓨터에 대한 상세 정보(Advanced Telemetry)

Microsoft Malware Protection Center는 여러 경로를 통해 수집되는 피드백의 분석을 통해 악성코드의 유형에 대한 글로벌 분석이 가능하다. 마이크로소프트사의 정보의 경로는 Microsoft Forefront Client Security, Microsoft Forefront Server Security, the Malicious Software Removal Tool (MSRT), Windows Live OneCare, Hotmail, Microsoft Exchange Hosted Services 와 다른 Microsoft 보안 기술과 같이 이미 출시된 제품들을 통한 정보 수집과 Product Support Services Security 지원과 다른 데이터 수집 툴을 이용한 마이크로소프트 내부의 정보 등을 포함한다.

악성 프로그램이 날로 발전함에 따라 매일, 그리고 매시간 악성코드의 패턴을 분석하는 것은 매우 중요하다. 이러한 분석을 통해 악성코드에 우선순위가 부여된다. 그리고 다양한 정보 수집 경로를 통해 악성코드에 대한 전방위적인 그림을 그릴 수 있게 되고 새로 등장하는 위협을 찾아 낼 수 있다.

한 예로 Microsoft Windows Malicious Software Removal Tool (MSRT)는 사용자의 컴퓨터에서 주로 만연하는 특정한 악성 코드를 제거하기 위해 개발되었고 Windows 사용자에게는 무료로 제공되고 있다. 2005년 1월에 처음 발표된 이후로 사용자는 2006년 기준으로 이미 3억 1천만대의 PC에 적용되어 약 5십 5억 회 정도 적용되었다. MSRT는 Microsoft Malware Protection Center에서 사용하는 위협대응방법 (threat telemetry)중의 하나이며 전 세계의 사용자의 컴퓨터에서 악성 소프트웨어를 제거하는데 매우 효과적인 방법이다.

일명 SpyNet이라고 불리는 Windows Defender Voting Network (윈도우 투표 네트워크) 또한 Microsoft의 연구팀이 새로이 나타나는 위협에 대한 정보를 어떻게 수집하고 있는 지를 잘 보여 주는 예이다. Windows Defender의 사용자는 새로운 위협을 발견하면 Microsoft에 알려주고, 연구팀이 요청하는 악성코드 샘플로

의심되는 파일들을 자발적으로 제공한다. 2006년 하반기에만 약 3천 8백 만 개가 넘는 악성코드를 찾아냈다. 또한 Windows Live OneCare의 사용자들도 사용자의 컴퓨터에서 발견된 악성코드들을 Microsoft사에 제공하고 있어서 Windows Defender와 Windows Live OneCare의 사용자들로부터 받는 감염 정보들을 통해 가장 빈번한 이슈에 대한 정보 분석을 할 수 있도록 도와준다.

다. 마이크로소프트의 보안의 미래에 대한 전략과 비전

1) 단기적 전략

o 악성 프로그램 시그니처의 품질 및 커버리지(Definition Quality and Coverage): 위협 탐지율을 사용자 및 업계와 공유.

o 악성 코드에 대한 대응 시간(Anti-malware Response Time): 빠르게 진화화고 있는 위협에 대하여 사용자의 기대보다 빠른 대응과 업데이트를 제공하도록 노력.

2) 미래의 비전

o 위협적 행위에 대한 전방위적 대비(Coverage of the Threat Event): 현재 이용 가능한 도구들은 사용자의 컴퓨터에 저장된 파일과 프로그램과 같이 악성코드 감염의 최종 결과에 중점을 두고 있지만, 좀 더 완전한 분석과 예방을 위해서는 감염에 이르기까지의 전 과정에 대한 조사를 통해서 미래의 악성코드 활동에 대한 예측과 경고를 할 수 있어야 한다.
o 미래의 동향에 대한 예측: 악성코드 환경은 지난 10년 간 엄청나게 변하였고 지난 몇 년 간은 더욱 심각하게 진화하였다. 만일 과거가 미래의 척도라면 새로운 위협들은 기술의 발전과 함께 계속 등장할 것이고 스파이웨어, 피싱, 그리고 다른 경제적 목적을 가진 공격들이 계속 될 것이다. 그래서 마이크로소프트

는 연구 팀은 미래의 잠재적인 공격에 대응하기 위하여 공격 유행을 지속적으로 감시하고 있다.

o 지속적인 업계의 참여: 보안은 모든 업계와 관련된 문제인 만큼 업계들이 힘을 합친 솔루션이 필요하다. 지금처럼 모든 컴퓨터가 연결되어 있는 세상에서는 사용자는 같은 생태계 안에서 존재하고 통신하고 있으며 위협이 점 점 더 복잡해질수록 보안업계의 협조가 어느 때보다도 중요하다. 그래서 Microsoft는 Microsoft Virus Initiative(MVI), VIA, ASC과 같은 공조 단체를 통해 보안업계가 악성코드의 근절을 위해서 도구, 정보, 그리고 모범사례들을 공유할 수 있는 장을 마련하였다. 위 자율단체들의 창립 회원으로서 마이크로소프트는 악성코드 방지에 있어 사용자들에게 선택권을 부여할 수 있도록 노력하고 있다.

라. 마이크로소프트사의 End to End Trust 비전 소개[75]

지난 20년 간 인터넷은 우리 사회의 광범위한 영역에 긍정적인 영향을 주고 있지만, 글로벌 네트워크가 확대되고 온라인에 저장하는 중요한 정보의 양이 증가함에 따라 새로운 위험과 사이버범죄 또한 증가되어 왔다. 계속해서 사이버 범죄가 익명성을 가지고 추적할 수 없는 어둠 속에 남아 있게 되면 온라인 범죄에 대한 책임을 추궁하고 범죄를 억제하기가 어려울 것이라는 것은 분명하다.

현실 세계에서는 여러 가지 물리적인 보안 조치와 효과적인 대처 방안이 있지만 사이버 세계의 경우 사전조치 방안을 더욱 효과적으로 개선하고 있음에도 불구하고 범죄자들은 자신의 행동에 대해 처벌받지 않고 더욱 대담해 지고 있다. 인터넷의 잠재력을 최대한으로 실현하고 구상하기 위해서는 보다 안전하고 신뢰할 수 있는 온라인 환경을 만들어야 한다. 이와 같은 목표를 향해 마이크로소프트와 여러 기업들은 보안과 개인정보보호를 강화해 왔다. 마이크로소프트는 지난 2002년 빌게이츠 회장이 "신뢰할 수 있는 컴퓨터 사용 환경 (Trust Worthy Computing)"을 추구해야 할 가치로 천명한 후, 지난 7년 간 제품과 서비스의 보안 및 개인정보보호에 많은 노력을 기울였다. 2002년도는 신뢰할 수 있는 IT 생태계를 만드는

75) 이하 Establishing End to End Trust, 2008, Scott Charney, Microsoft Corporate Vice President가 발표한 자료를 요약하였다.

데 중점을 두었다. 신뢰할 수 있는 컴퓨터 사용 환경에는 신뢰도, 보안, 개인정보의 보호가 포함되어 있다.

1) Secure by Design, Secure by Default, Secure by Deployment

마이크로소프트의 보안 전략은 시간이 지나면서 SD3, 즉 "Secure by Design, Secure by Default, Secure by Deployment"라는 보다 구체적이고 총체적인 접근 방법을 택하였다. 간단히 말해서 소프트웨어가 좀 더 안전하게 설계 및 개발이 되고, 시장에 출시되었을 때 좀 더 안전한 상태로 출시되고(여기에는 기본으로 많은 기능들을 '꺼짐'으로 설정하여 공격에 노출되는 부분을 줄이고, 사용자 설정을 기본적으로 관리자 모드 대신 사용자 모드로 설정해 놓는 것을 포함한다), 시기적으로 적절하게 업그레이드를 할 수 있는 시장에 대한 빠른 반응이 있다면 사용자의 컴퓨터 사용 환경은 좀 더 안전해질 것이다. 이러한 SD3 원칙은 7년이 지난 지금도 중요한 원칙으로 남아 있다.

그러나 SD3에는 구조적인 한계가 있었다. 아무리 Secure by Design, 즉 설계와 개발 단계에서부터 안전하게 구상을 해서 취약점이 획기적으로 많이 감소된다고 하여도 시중에 나와 있는 수많은 복잡한 성격을 가진 모든 제품들에 잠재하고 있는 취약점이 빠른 시일 내에 모두 제거될 수는 없었다. Secure by Default를 통해 위협에 노출되는 취약 부분의 표면을 줄일 수는 있지만 이 또한 위험을 모두 제거할 수는 없었다. 많은 사용자가 원하는 바로 그 기능이 활성화 되어야 하기 때문에 제약이 있었다. 종전에 나왔던 많은 소프트웨어들은 사용자가 "관리자"로 설정이 되어 있어야만 작동을 하는 경우가 많았기 때문에 "일반사용자" 기능으로 운영을 하였을 때의 보안의 혜택을 많이 감소하였다.

마지막으로 "Secure by Deployment"도 중요한 역할을 하였지만 사용자들이 테스트를 하고 패치를 깔기도 전에 패치들이 역설계 (reverse engineered) 되었고 취약점을 노리는 공격이 있었다. 어떤 경우에는 패치가 출시되는 날 그 패치가 뚫리는 경우도 있었다. 그래서 마침내 SD3은 제품의 보안에 중점을 두게 되었고 Secure by Deployment는 특히 보안의 처리능력(manageability)에 집중을 하고 있

기는 했지만 SD3이 취약점에 대한 한 가지 답을 제공할 수는 없었다. 수많은 종류의 소프트웨어 제품들과 그 제품들이 사용되는 셀 수없이 다양한 환경을 고려할 때 모든 취약점과 위협에 대한 노출을 다루기는 힘든 일이다.

2) 심층 방어(Defense-in-Depth)

위와 같은 한계를 깨닫고 SD3은 심층 방어(Defense-in-Depth)로 보충이 되었다. Defense-in-Depth는 보안 기술들이 실패할 수도 있다는 사실과 다른 층단에서의 보안이 총체적인 보안을 제공할 수도 있다는 점을 깨달은 결과였다. 그래서 마이크로소프트가 (1) 코드에서의 취약점을 감소시키고 (2) 디폴트로 여러 기능을 비활성화 시켜서 제품을 출시하고, (3) Windows XP 서비스팩2와 Windows Vista에서 방화벽을 디폴트로 켜 놓고, (4) 사용자들의 교육을 통해 백신 프로그램을 설치하도록 권유하고 백신 프로그램을 제공하고, (5) 사용자들에게 “출처를 모르는 코드”에 대한 경고를 제공하였음에도 불구하고 사용자들은 계속 “출처가 밝혀지지 않은 코드”를 다운로드받아서 컴퓨터를 위험에 노출시켜왔기 때문에 마이크로소프트에서는 Malicious Software Removal Tool(MSRT)를 제공하여 사용자들이 감염된 장치들을 치료할 수 있도록 하였다.

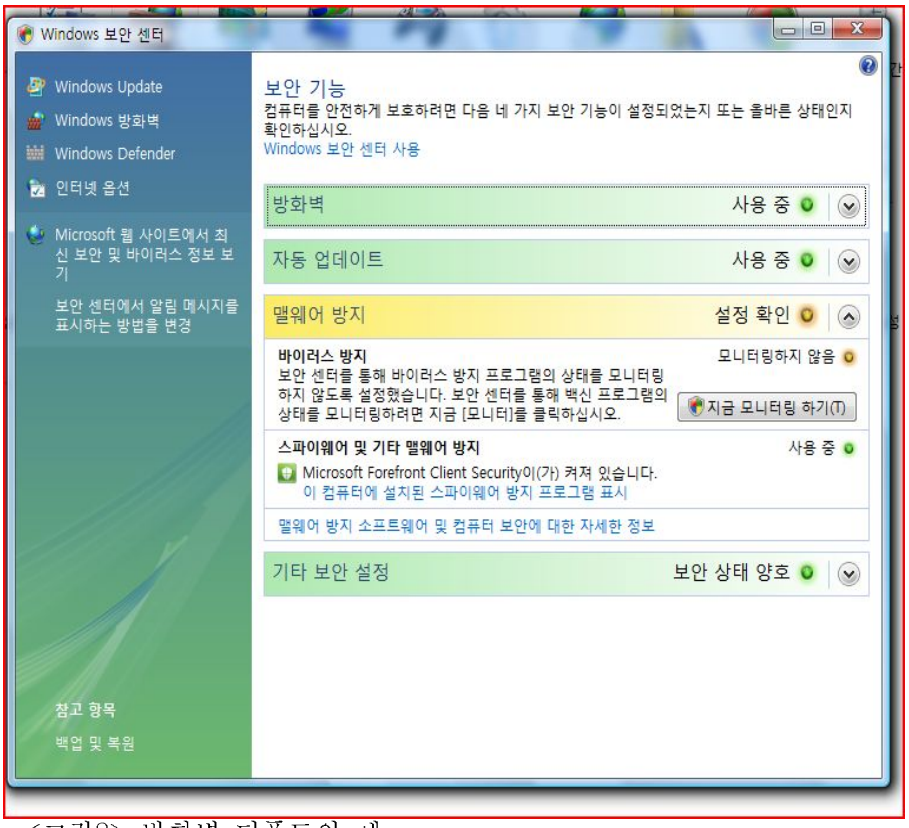
o Microsoft의 심층방어에 관한 전체적인 지도

<그림6> 마이크로소프트의 심층 방어에 대한 전체적인 지도

o 디폴트로 여러 기능을 비활성화 하여 제품을 출시하는 예

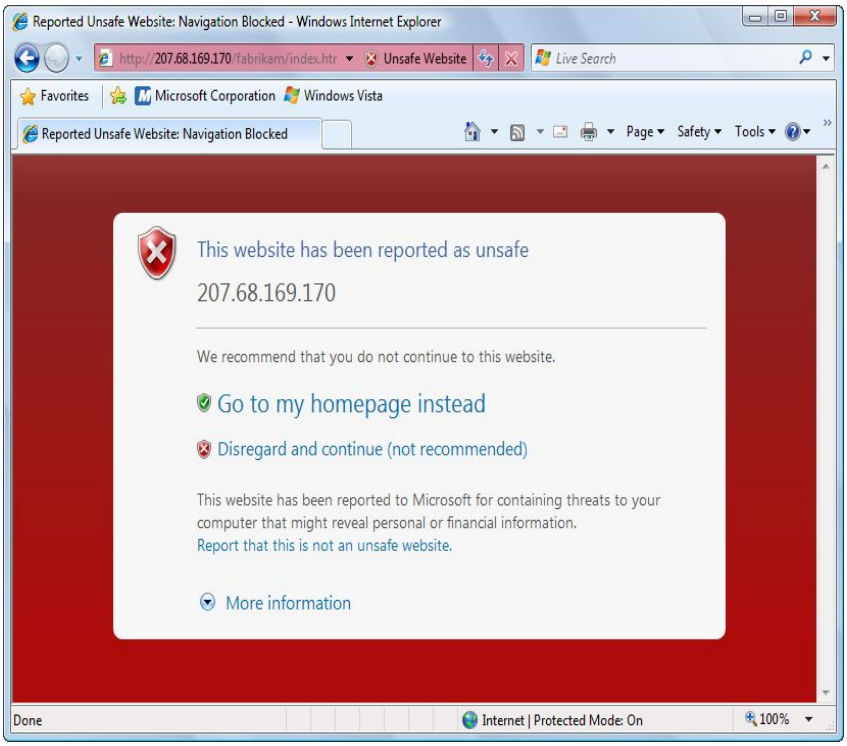
<그림7> 기능 비활성화 출시의 예

o 방화벽을 디폴트로 켜 놓는 예



<그림8> 방화벽 디폴트의 예

o 사용자에게 출처를 모르는 코드에 대한 경고를 보내는 예



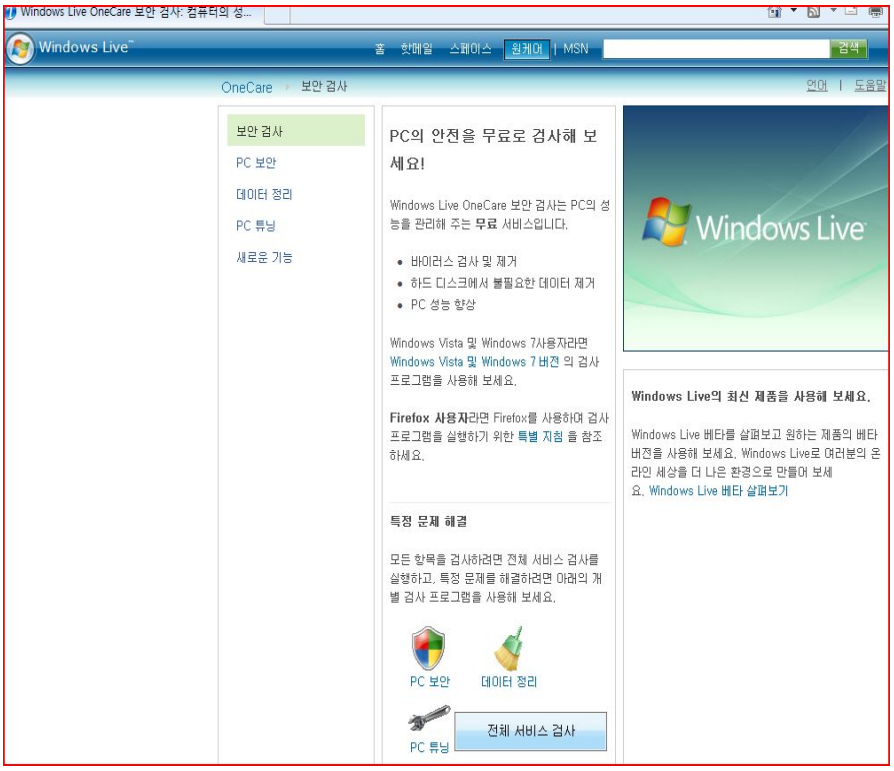
<그림9> 사용자에게 보내는 출처를 알 수 없는 코드에 대한 경고1

<그림10> 사용자에게 보내는 출처를 알 수 없는 코드에 대한 경고2

<그림11> 사용자에게 보내는 출처를 알 수 없는 코드에 대한 경고3

o 사용자에게 제공하는 백신프로그램의 예

<그림12> 사용자에게 제공하는 백신프로그램의 예1



<그림13> 사용자에게 제공하는 백신프로그램의 예2

3) 특정 보안 이슈에 대한 개별적인 대응

그러나 SD3과 심층 방어에도 불구하고 보안에 대한 위협 중 한 가지 다루어지지 않은 문제가 있었다. 예를 들어 스팸은 대부분 취약점을 노리지 않는다. 또한 사용자가 기본 값으로 이메일 기능을 항상 비활성화 해 놓을 수도 없다. 그리고 특정 사용자나 기업이 봇넷에서 오는 DDoS를 예방하기 위해 특별히 할 수 있는 조치도 없다. 그래서 마이크로소프트는 특정 문제에 대한 위협을 막기 위한 대책을 마련하였다.

피싱과 스팸에 대해서는 폭넓은 사용자 교육캠페인을 시작하였고 피싱 필터와 Sender ID기술을 개발하기 시작했다. 그리고 피싱과 봇넷에 대해서는 피싱을 보내는 사람들과 봇넷 족들을 경찰과 협력하여 추적하는데 많은 노력을 기울이기 시작하였다. 현재의 환경을 고려할 때 피싱족과 봇넷 족들을 추적하는 것이 힘들고 추적해서 잡은 후에도 저지는 행위에 비하여 형사적 처벌이 약한 관계로 이러한 노력에 대한 효과가 제한적이라는 것이 굉장히 아쉽다.

4) 보안전략의 진화

사용 환경의 각 단계에서 신뢰할 수 있는 종단 보안을 구축하고 사용자에게는 종단(End to End) 신뢰를 가능하게 하였다.

SD3, Defense-in-Depth와 특정 위협에 대한 감소 대책에도 불구하고 보안과 개인정보보호는 많은 컴퓨터 사용자들에게 중요한 이슈로 남아 있다. 그러나 지금까지 나온 보안에 대한 솔루션은 방어적 기술을 채택한 방법이어서 특정 공격에 대한 위협을 감소시키는 데에는 효과가 있었지만 방법을 바꿔가면서 공격하는 진화하는 공격자들에 대한 대응을 잘 다룰 수 없었다. 예를 들어 운영체제의 보안을 강화하고 나면 공격자들은 응용 프로그램을 공격하거나 현재의 기술로는 예방하기에는 힘든 사회공학기법을 택하여 공격을 하였다.

그러나 그렇다고 해서 위의 보안 전략들이 제 역할을 하지 못 했다는 것은 아니다. 오히려 반대로 위의 보안 전략들은 보안 전략의 근간이 되었으며 심각한 위협

을 효과적으로 감소시켜왔고 앞으로도 계속 그럴 것이다. 전략들이 보다 나은 정적 분석 툴(static code analysis)을 이용하든, 아니면 더 근본적인 변화-이를테면 검증되지 않은 소스를 수행하기 위해 샌드박스(sandbox)를 제공하는 등-를 수반하든지 간에 IT 산업은 그 기본 역할을 지속적으로 수행해야 한다. 그러나 현재의 상태에만 머물러 있어서는 충분하지 않다. 진짜 중요한 문제는 현재의 보안 전략으로는 가장 중요한 현안인 "컴퓨터가 이제는 전 세계와 연결되어 있고, 익명성, 추적 불가능한 인터넷의 세계가 범죄자들을 끌어 들이는 자석과도 같다는 사실"을 인지하는 것이다. 이러한 범죄 행위는 책임 소재가 모호하다는 이유로 제지가 잘 되지 않는다. 게다가 인터넷의 특성 때문에 정직한 사용자들도 인터넷에서 연결되어 있는 다른 사용자가, 또는 자신이 사용하는 프로그램이, 또는 연결된 다른 장치가, 다운로드하는 패킷들이 신뢰할 수 있는 것인지 알 수 없다. 그래서 현실 세계에서 사용자만 조심하면 된다는 원칙이 인터넷에서는 통용되지 않는다.

현재까지는 컴퓨터에 대한 위협에 대한 우리의 반응은 "방어"였다. 그러나 그 동안의 컴퓨터 보안의 역사를 보면 공격자들은 거의 무제한적인 시간과 자원을 가지고 있었다. 그 말인즉슨, 정통적인 관점에서 효과적인 "보안"을 위해서는 전방위 보안을 하여야 한다는 뜻이다. 현실적으로 "공격"은 한 군데 취약점만 찾으면 되므로 "공격"이 "방어"를 항상 이겨왔다는 것을 알 수 있다. 지금까지의 경험을 보면 많은 사이버범죄가 성공적이었던 이유는 사용자, 기기, 소프트웨어, 데이터들이 잘 신뢰할 수 있는 것으로 검증되지 않았고, 조사와 추적이 힘들었다는 데에 있다. 이러한 이유로 범죄자들은 범죄를 쉽게 저지르고, 범죄를 저지른 후에도 그에 상당하는 죗값을 치루지 않았다.

그렇기 때문에 사용자가 이성적이고 효율적이면서도 신뢰에 기초한 결정을 내릴 수 있는 사용 환경을 제공하여야 하고, 이를 통해 범죄를 제지해야 한다. 이러한 목적을 달성하기 위해서 우리는 신뢰에 기초한 종단 보안을 구축하여야 한다. 즉, (1) 하드웨어에 기초한 보안, (2) 신뢰할 수 있는 운영체제, (3) 신뢰할 수 있는 응용 프로그램, (4) 신뢰할 수 있는 사용자, (5) 신뢰할 수 있는 데이터가 차례로 쌓여야만 빈틈없는 보안을 이룰 수 있다.

신뢰할 수 있는 데이터
신뢰할 수 있는 사용자
신뢰할 수 있는 응용프로그램
신뢰할 수 있는 운영체제
하드웨어에 기초한 보안

<표1> 신뢰에 기초한 종단 보안체계

각 단 내에서, 그리고 단과 단사이의 의존성이 높고, 어느 한 단에서 보안이 깨지게 되면 다른 단에 있는 보안도 훼손되기 때문에 각각의 단을 신뢰할 수 있어야 한다. 예를 들어 '신뢰할 만한 사용자'가 '신뢰할 만한 운영체제'와 '신뢰할 만한 하드웨어' 위에서 만들어진 파일을 타인에게 보냈을 때 응용프로그램이 '신뢰할 수 없는' 프로그램이라면 그 파일 전체는 신뢰될 수 없게 된다. 그리고 신뢰가 무너졌다면 신뢰를 깬 자를 추적할 수 있어야 하고 추적한 뒤에는 그러한 신뢰가 다시는 깨지지 않도록 사회적, 정치적인 장치가 있어야 한다. 그래서 적절한 감시를 통해 "책임"을 지도록 하는 체제가 필요하다.

마이크로소프트에서는 Software Development Lifecycle을 도입하여 현재 버전 5.0까지 마련되어 있고 강력한 보안 체제 및 위협을 완화할 수 있는 기술을 개발해 왔다. 마이크로소프트는 업계의 여러 파트너들과 연계하여 보다 안전하고, 개인정보보호를 강화하고, 안정적인 컴퓨터 사용 환경을 지속적으로 구축해 가고 있다. 그러나 마이크로소프트와 업계의 노력만으로는 신뢰할 수 있는 온라인 환경을 만들 수 없다. 업계와 고객, 파트너, 정부와 다른 중요한 지원자들이 모두 함께 신뢰할 수 있는 컴퓨터 사용 환경을 인터넷으로 확대하기 위한 노력에 동참해야 한다.

인터넷의 신뢰를 향상시키기 위해 3가지 핵심적인 방안을 들 수 있다.

첫째는 신뢰할 수 있는 종단 구축이다. 이 단계 구성은 먼저 신뢰할 수 있는 하드웨어에 기반을 두고, 그 위에 각 요소, 즉, 하드웨어 위에 소프트웨어 (신뢰할 수 있는 운영체제, 신뢰할 수 있는 응용 프로그램), 데이터, 그리고 사용자의 신분이 적절한 조건으로 인증이 되어야 한다.

두 번째는 사용자 식별 정보와 관련된 요구 사항의 관리이다. 사용자가 식별 요구 사항(이것이 이름 전체일 수도, 또는 나이나 국적과 같은 일부 정보일 수도 있

다)을 입력하도록 하는 시스템을 구축해야 한다. 또한 이 시스템에서는 인증, 권한 부여, 접근 및 감사 문제가 해결되어야 한다.

마지막으로 기술, 사회, 정치, 경제 기관들이 적절히 협력하여 실질적인 개선을 이루어야 한다. 추구해야 할 목표는 사용자가 컴퓨터 사용 환경을 원하는 대로 제어하고 보안과 개인정보를 강화하며, 익명성 및 언론의 자유와 같이 존중되어야 하는 기타 가치를 유지하는 것이다.

보안에 대한 관심이 고조된 지금이 바로 인터넷 보안을 위한 기회이다. 봇넷, ID 도용 및 온라인상에서의 청소년 보호 등과 같은 심각한 문제들은 보안과 개인정보보호 문제에 대해 많은 사람들에게 경각심을 불러 일으켰다. 전자서명(PKI) 및 스마트카드와 같은 몇몇 주요 기술들은 광범위한 영역에서 도입할 수 있을 정도로 안정화 되었다. 보안과 개인정보보호, 둘 중 어느 것도 희생하지 않고 두 마리 토끼를 모두 잡을 수 있는 방법을 비롯하여 다른 중요한 여러 가지 사항을 고심한 결과 보안과 개인정보보호 둘 다 향상된 인터넷을 만들기 위한 새로운 방안을 마련할 수 있었다. 또한 과거의 경험을 통해 기술, 사회의 힘, 정치적 의지, 시장의 역동성을 조화롭게 결합하여 여러 중요한 문제에 대해 커다란 성취를 얻을 수 있는 방안을 배웠으며, 중요한 노력이 때로는 실패한다는 것도 배웠다.

마이크로소프트사가 발표한 End to End Trust 백서에 대해 많은 사용자들과 전문가들이 제공한 의견은 의외로 하드웨어, 소프트웨어나 데이터 보다는 "사용자" 요소에 집중이 되어 있었다. 많은 사람들이 ID의 요소 (예를 들어 나이)에 기반을 둔 가장 효과적이고 신뢰할 수 있는 결정을 내릴 수 있는 방법에 대한 필요와 온라인상에서의 행위에 대한 책임을 밝히는 것에 가장 많은 관심을 기울인 것으로 나타났다.

익명성과 사용자 선택권에 대해서는 표현의 자유와 같이 중요한 가치를 실현하기 위해 익명성을 얼마만큼 보호할 것인가에 대해서는 많은 우려가 있었다. 그러나 많은 사람들이 사용자가 언제, 무엇을 밝힐 것인가에 대한 선택권을 주는 것이 매우 중요하다는데 의견을 같이 하였다. 또한 "사용자가 익명성을 유지하면서도 온라인상에서의 아이덴터티에 대한 선택권을 가지는 것"이 방법이라는 의견도 있었다. 그러나 너무 많은 선택권을 사용자에게 제공할 경우 사용자가 불편할 수도

있다는 점 또한 기억해야 한다.

마. Security Development Lifecycle v. 5.0 (SDL)[76]

마이크로소프트에서는 보안과 개인정보보호에 대한 모범사례들을 제품과 서비스를 위한 소프트웨어를 개발하는 단계에서부터 적용하고 있다.

SDL은 소프트웨어의 개발단계에 다섯 개의 중요한 체크 포인트를 추가하는 것으로 구성되어 있다. 요구(Requirements), 설계(Design), 구현(Implementation), 확인(Verification), 배포(Release)의 다섯 단계가 그것이다. 이렇게 하여 각 확인 지점마다 필요한 사생활 보호와 보안 요소에 대한 권장사항과 반드시 적용해야 할 사항으로 나누어 관리하고 있으며 이런 방법을 통해서 사용 단계에서 보안과 프라이버시 버그를 줄일 수 있다.[77]

바. 마이크로소프트사의 보안 기술의 예[78]

아래에 마이크로소프트사의 보안기술을 소개하는 취지는 보안과 관련한 대책은 사용자와 개발사, 그리고 정부, 모두의 공동의 노력이 필요하다는 것을 밝히려는 것이다. 마이크로소프트사는 다수의 효과적인 보안기술을 보유하고 있는 바, Windows 운영체제나 Internet Explorer의 국내에서의 시장점유율을 고려해 볼 때, 충분한 사용자 교육을 통해 많은 사용자들이 그러한 보안기술을 효과적으로 사용하게 되면 생각보다 많은 보안 문제에 적절하게 대처할 수 있을 것이다. 한편, 정부 입장에서는 네트워크 안전을 위해 사용자 교육을 장려함으로써 보안을 강화하는 동시에 한정된 정부의 자원을 효율적으로 분배할 수 있는 이중의 효과를 거둘 수 있을 것이다.

---

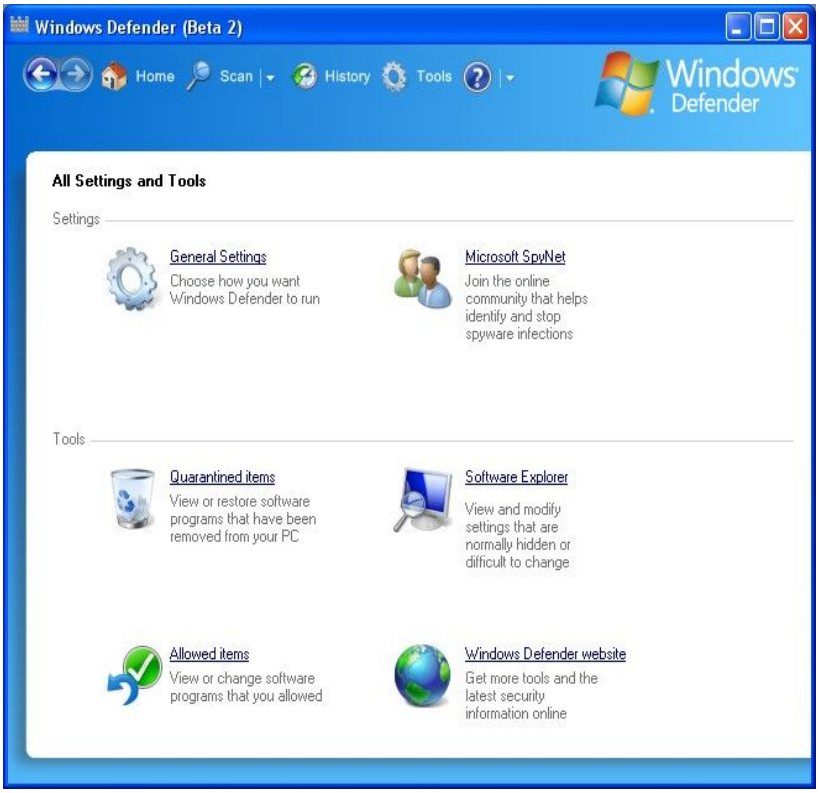
76) 이하 Microsoft Security Development Lifecycle v. 5.0의 내용을 인용.

77) 그러나 SDL은 외부에 공개될 수 없는 내용이 많이 포함되어 있으므로 SDL을 차용하여 만들어진 SAFECODE의 내용을 참조.

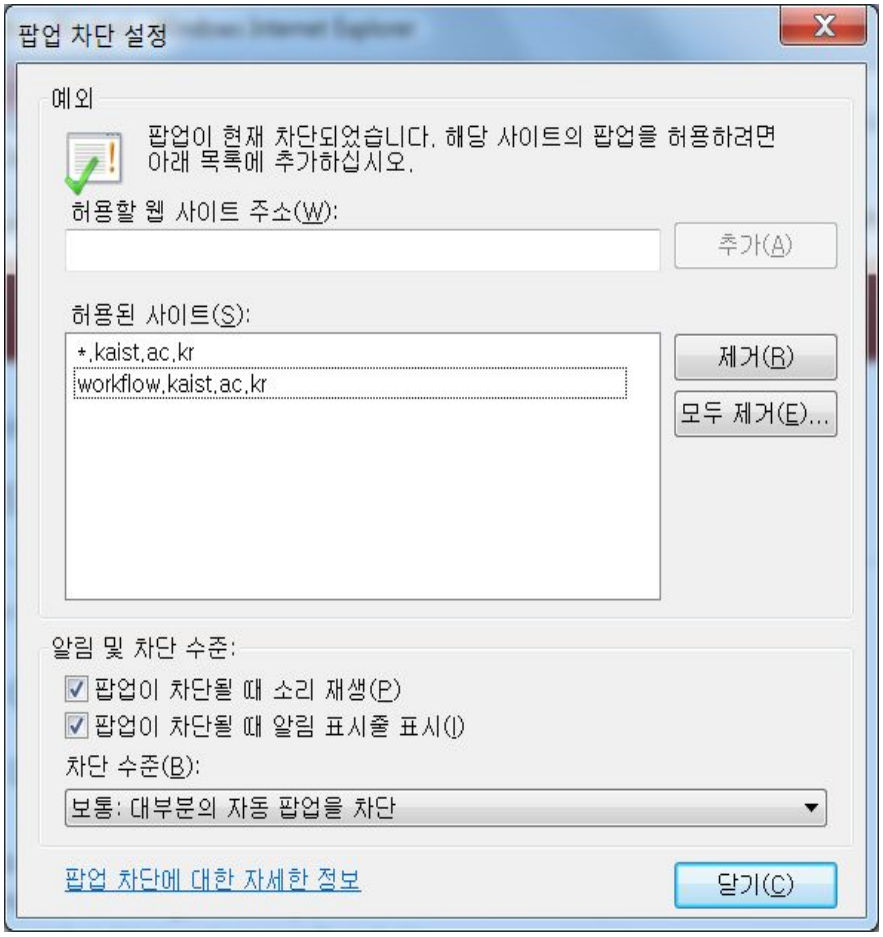
78) http://www.microsoft.com/security/default.aspx 마이크로소프트 security homepage 참조. 이하 아래 화면들은 모두 Microsoft Vista의 보안도구, Internet Explore 7 & 8의 보안도구, Microsoft Office제품의 보안도구, Windows Live의 보안도구의 화면을 떠 왔다.

1) Windows Vista에서의 보안 기술

o Windows Defender (스파이웨어로부터 보호프로그램): Windows Vista에 포함된 Windows Defender라는 스파이웨어방지기술은 스파이웨어나 다른 악성코드의 설치로 인해 컴퓨터가 느려지거나, 개인정보를 빼가거나, 원하지 않는 팝업광고를 띄우는 것을 방지한다. 이 기술은 Internet Explorer7 사용 환경에서 원치 않는 악성코드나 스파이웨어가 설치되어 사용자의 파일이나 설정을 수정할 수 없도록 하고, 사용자에게는 웹브라우징을 할 수 있는 만큼의 권한만 허락한다.



<그림14> Window Defender

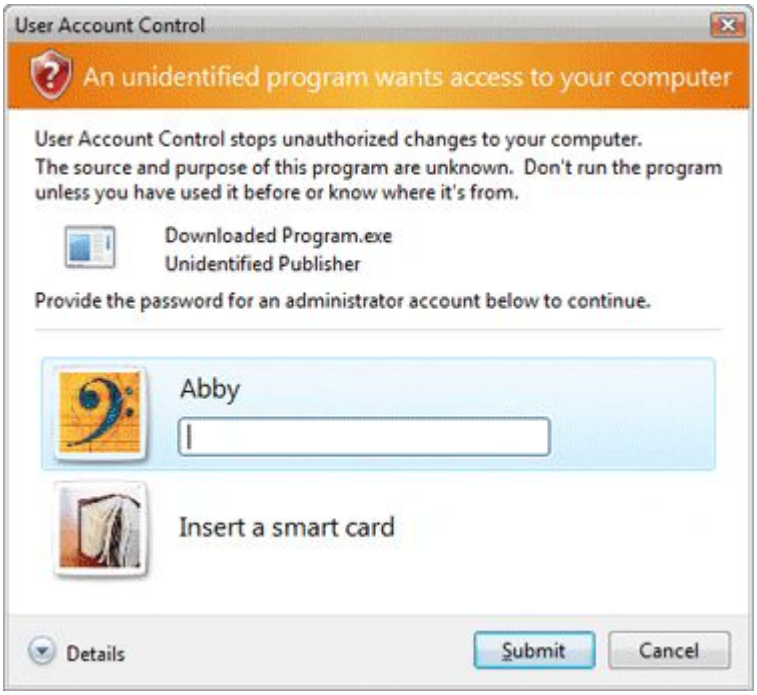


<그림15> Window Defender에서의 권한 설정

o Windows Security Center: 이 기술은 사용자의 보안소프트웨어가 최신으로 업데이트되어 있지 않거나 보안설정이 안전하지 않을 때 사용자가 조치를 취할 수 있도록 사용자에게 알려주는 기능을 한다. Windows Vista에서는 이 기술이 좀 더 개선되어 사용자의 컴퓨터에 설치되어 있는 안티스파이웨어 소프트웨어, Internet Explorer 설정, 그리고 사용자계정컨트롤 설정에 대한 정보도 포함하고 있다.

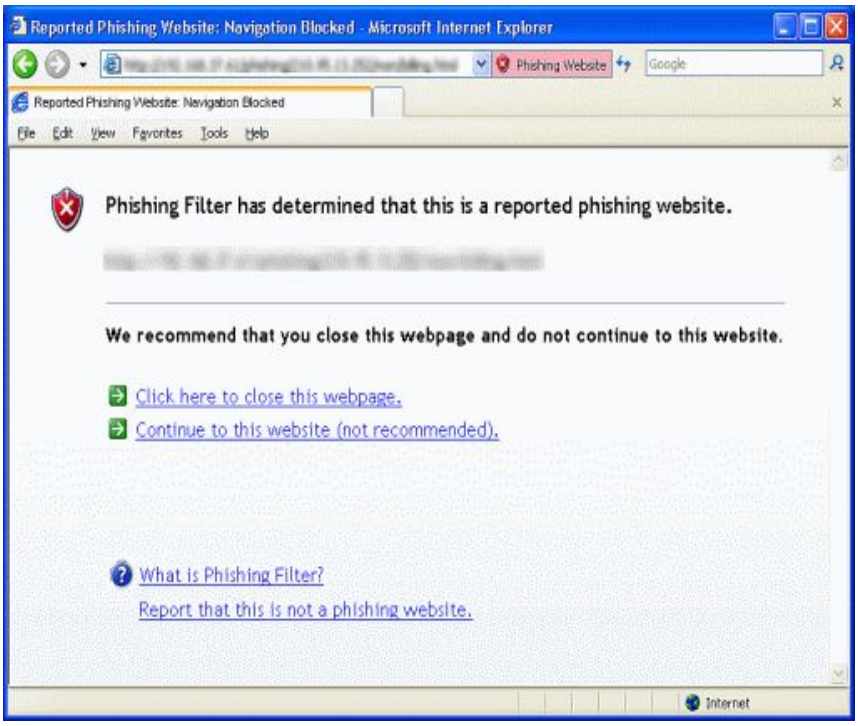
<그림16> Window Security Center

o 관리자모드 사용에 대한 경고: Windows Vista는 디폴트가 “안전모드”로 설정이 되어 있다. 응용프로그램에서 사용자의 컴퓨터에 잠재적으로 위험할 수 있는 “관리자모드”로 설정하도록 요구하면 때 사용자에게 그 프로그램을 열기 전에 그 프로그램을 열어도 되는지 사용자의 동의를 구한다.



<그림17> 관리자모드 사용에 대한 경고

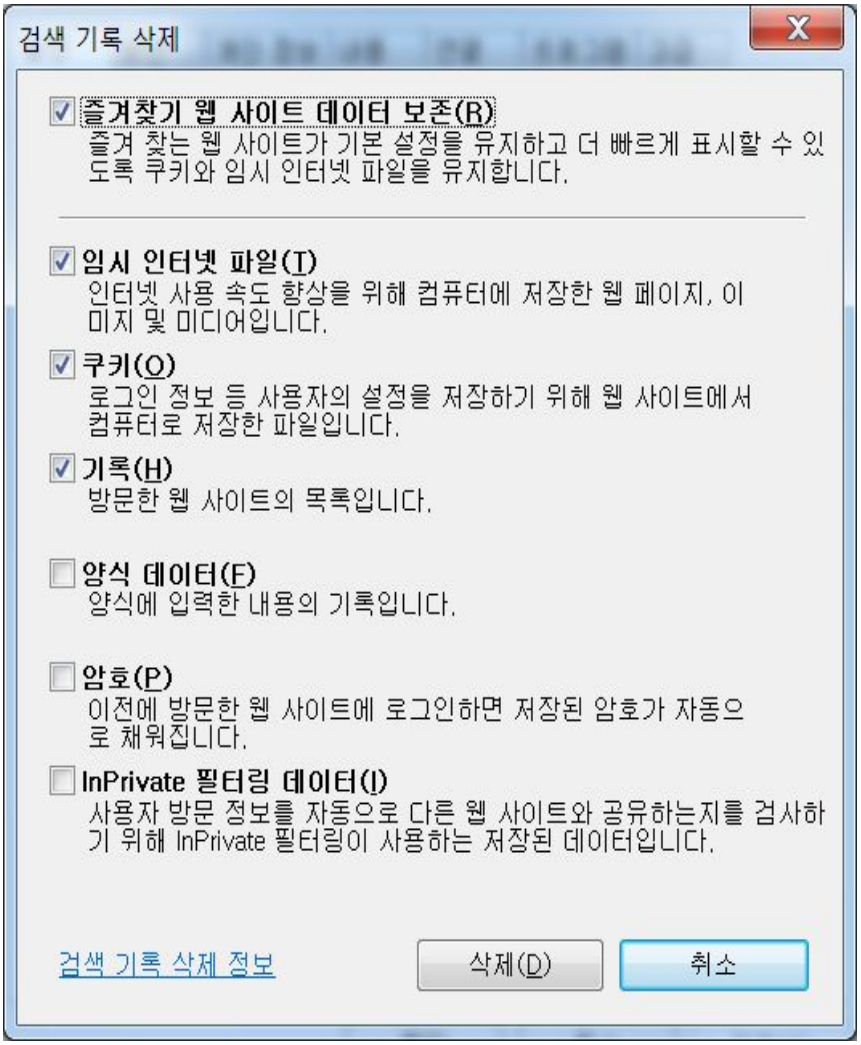
o 피싱사이트 경고 제공: Windows Vista에 탑재된 Internet Explorer7은 사용자의 비밀정보를 빼나가려는 피싱사이트에 대한 정보도 제공하고 있다. 이 필터는 한 시간에도 여러 번 업데이트되고 있는 피싱사이트 리스트 정보를 통해 현재까지 알려진 피싱 사이트에 대한 경고를 사용자에게 제공하고, 아직 데이터베이스에 포함되지 않은 위험 사이트에 대해서도 경고를 한다.



<그림

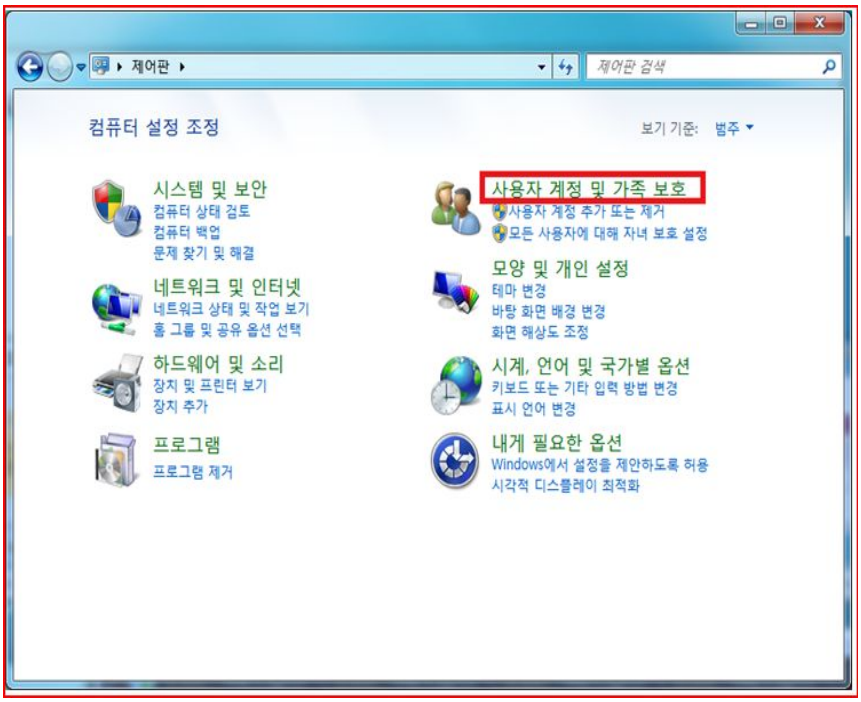
<그림18> 피싱 사이트 대한 경고

o 검색기록삭제: 사용자가 방문한 사이트와 사용자가 제공한 정보들이 컴퓨터의 여러 곳에 저장이 되어 있는데 “검색기록삭제” 기능을 사용하면 사용자의 검색 기록을 모두 삭제할 수 있다.

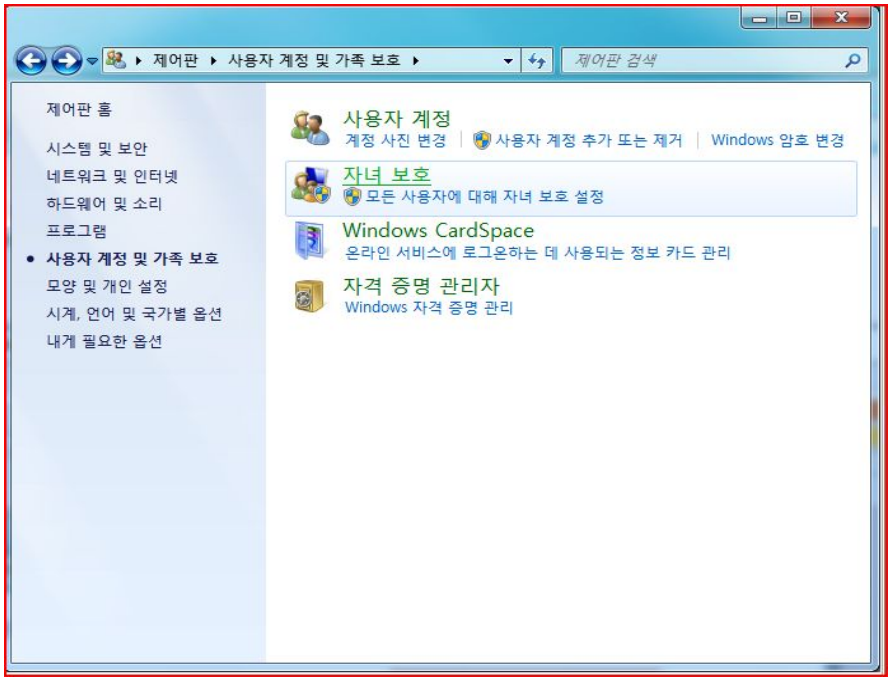


<그림19> 검색 기록 삭제

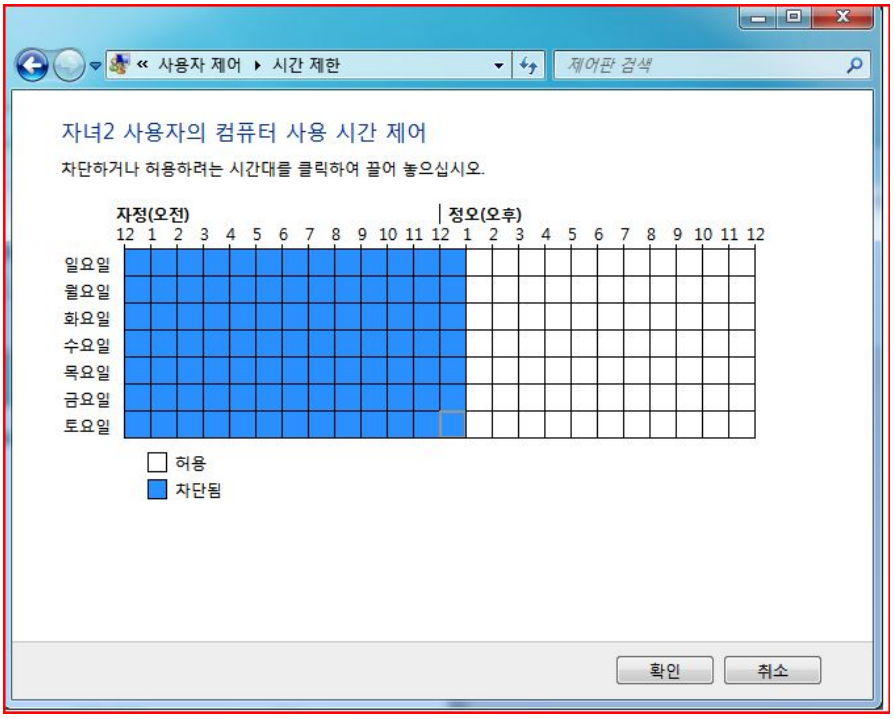
o 자녀보호기능: 자녀보호기능을 사용하면 자녀의 동의하에 자녀의 웹상에서의 행동을 부모가 모니터링할 수 있다.



<그림20> 자녀 보호 기능1

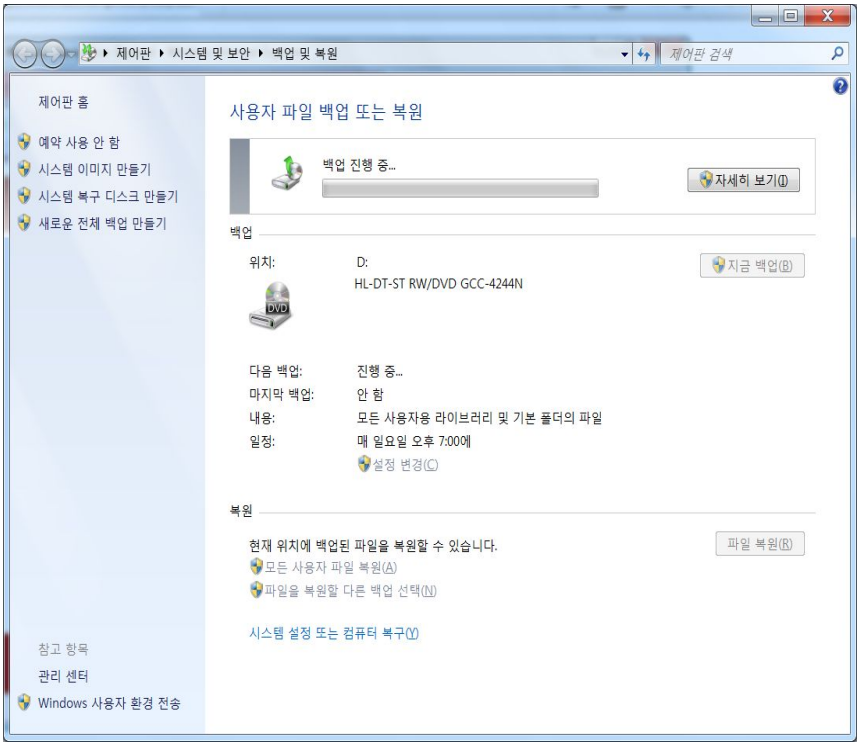


<그림21> 자녀 보호 기능2



<그림22> 자녀 보호 기능3

o Windows Vista 백업도구: Windows Vista에서는 이전 버전에 포함된 백업 도구보다 훨씬 강력하고 쉬운 백업 도구를 제공한다. 새로운 버전에서는, 사용자가 백업을 할 또는 복원을 할 저장위치를 마음대로 지정할 수 있다. 마법사 형태의 백업 도구를 이용하면, 자동적으로 일정을 정해 정기적인 백업을 할 수 있다. 이러한 기능을 통해 사용자는 바이러스 등의 공격에 대비해 자신의 자료를 늘 안전하게 보관할 수 있다.



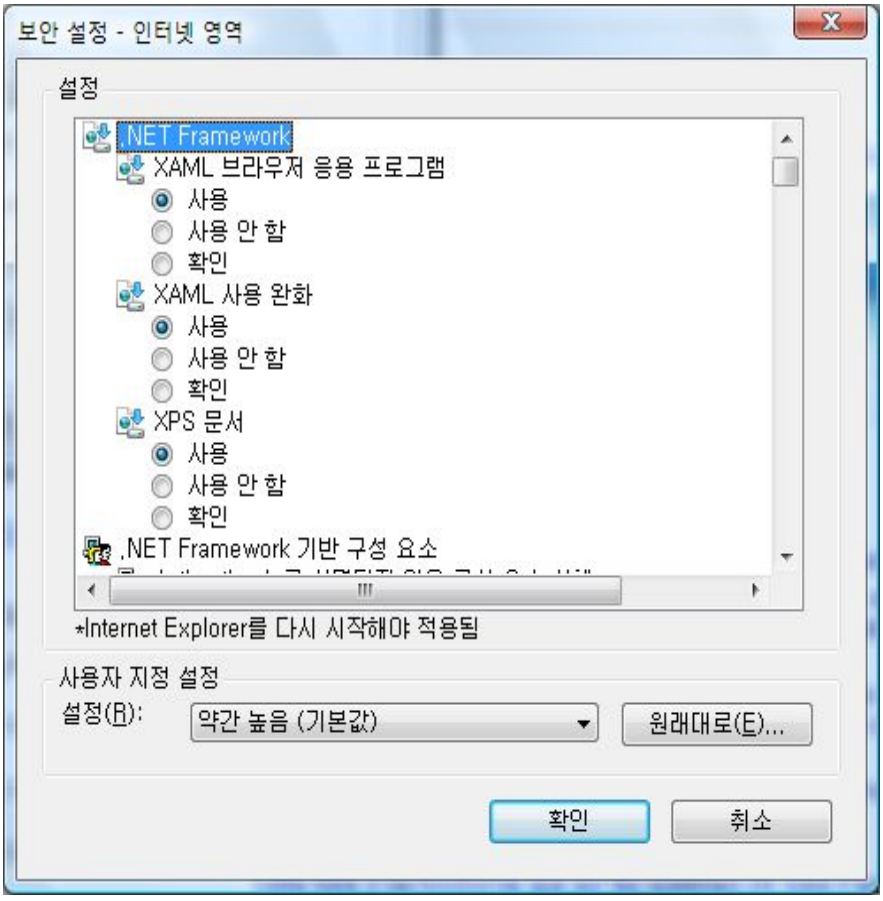
<그림23> Windows Vista 백업도구

2) Internet Explorer의 보안기술

o Internet Explorer는 Windows Defender와 함께 사용자가 용량이 큰 소프트웨어를 다운로드 받을 때 스파이웨어가 사용자도 모르게 다운로드 되어 사용자의 컴퓨터에 설치되는 것을 방지한다. Windows Defender 기술은 Windows Vista에 포함되어 있으며 Windows XP를 사용할 경우 SP2에 무료로 포함되어 있다.

o ActiveX는 애니메이션이나 팝업 메뉴 등 웹페이지의 기능을 향상시키는데 사용되기도 하지만 ActiveX기능은 인터넷 공격자들이 원래 의도하지 않았던 목적으로 사용하기도 한다. 그래서 Internet Explorer7은 ActiveX 옵트인 기능을 포함하여 디폴트로 ActiveX를 비활성화 시켜 놓았다. 사용자가 원하면 Information Bar와 Add-on Manager를 통하여 ActiveX기능을 활성화 시켜놓을 수 있다.

o Internet Explorer7은 사용자의 보안 설정을 디폴트로 “높음”으로 설정해 놓았다. 그러나 어떤 사이트들은 사용자의 보안설정이 좀 더 낮게 설정되어 있을 것을 요구하는 사이트도 있다. 사용자가 보안설정을 위험할 정도로 낮게 변경하는 경우 Internet Explorer7은 이러한 아이템을 빨간 색으로 표시한다. 그래서 사용자가 보안 설정이 낮은 사이트를 방문하는 동안에, 그리고 사용자가 다시 보안 설정을 위험하지 않은 수준으로 높일 때까지 사용자의 보안 설정이 위험할 정도로 낮다는 것을 계속 알려준다.

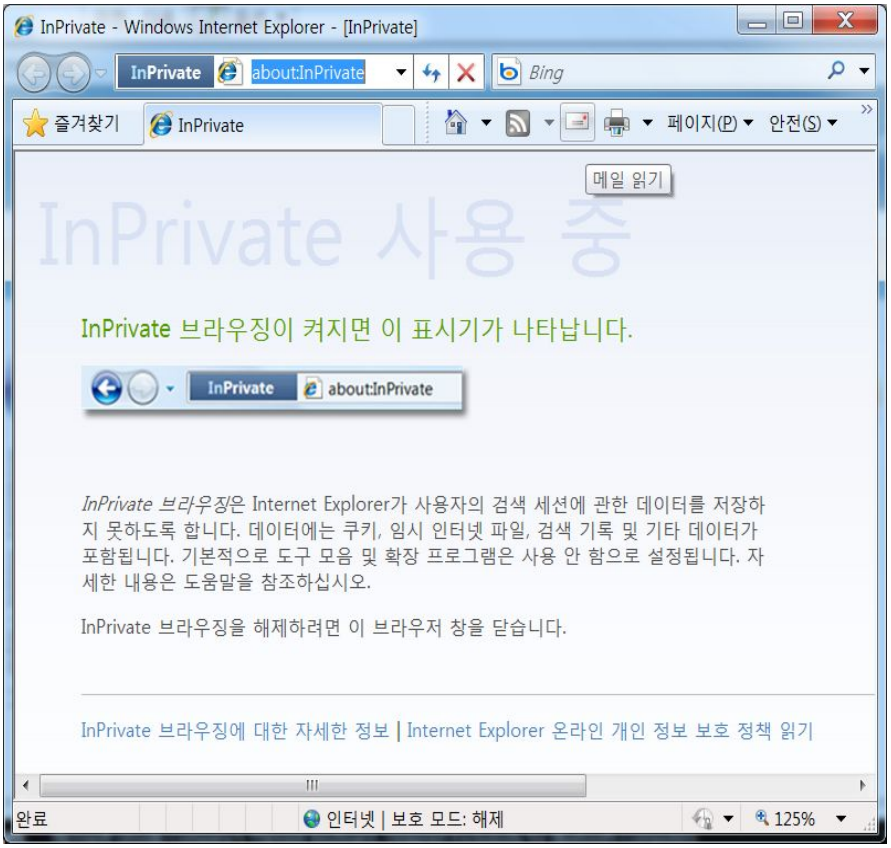


<그림24> Internet Explorer7의 보안설정

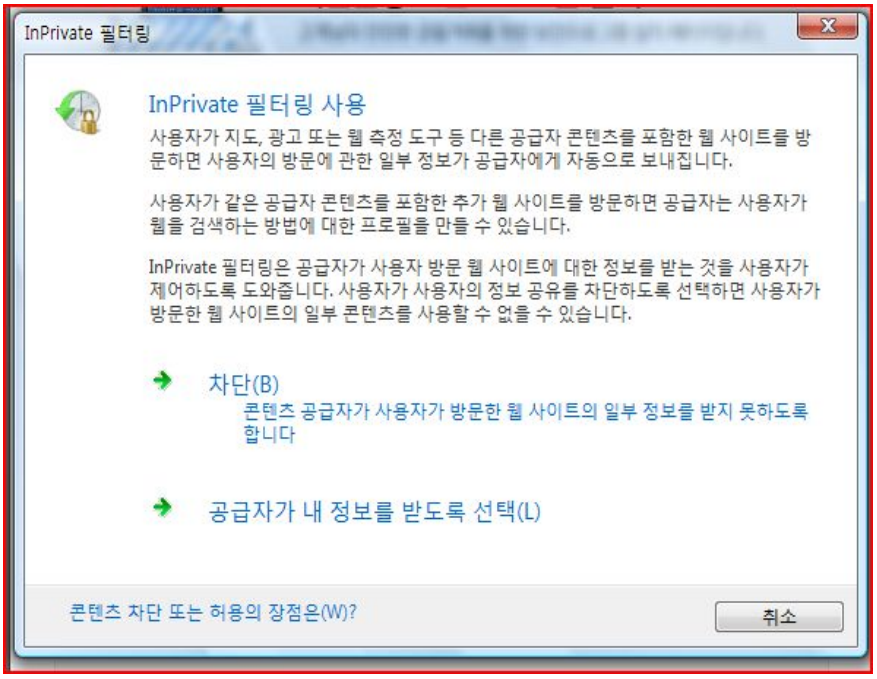
o 온라인 피싱 필터를 사용하여 방문하는 웹사이트에서 사용자의 ID 또는 비밀정보를 빼내가는 것을 방지한다. 이 필터는 로컬분석과 피싱 기술의 공통적인 특징을 찾아내고, 온라인으로 제공되는 피싱 사이트 리스트에 포함된 피싱 사이트를 차단한다.

o Extended Validation (EV) SSL Certificates: EV SSL 인증은 웹사이트에서 이루어지는 통신이 안전하도록 할 뿐만 아니라 Certification Authority가 제공한 SSL Certificate을 통해 웹사이트의 운영자에 대한 정보도 포함한다.

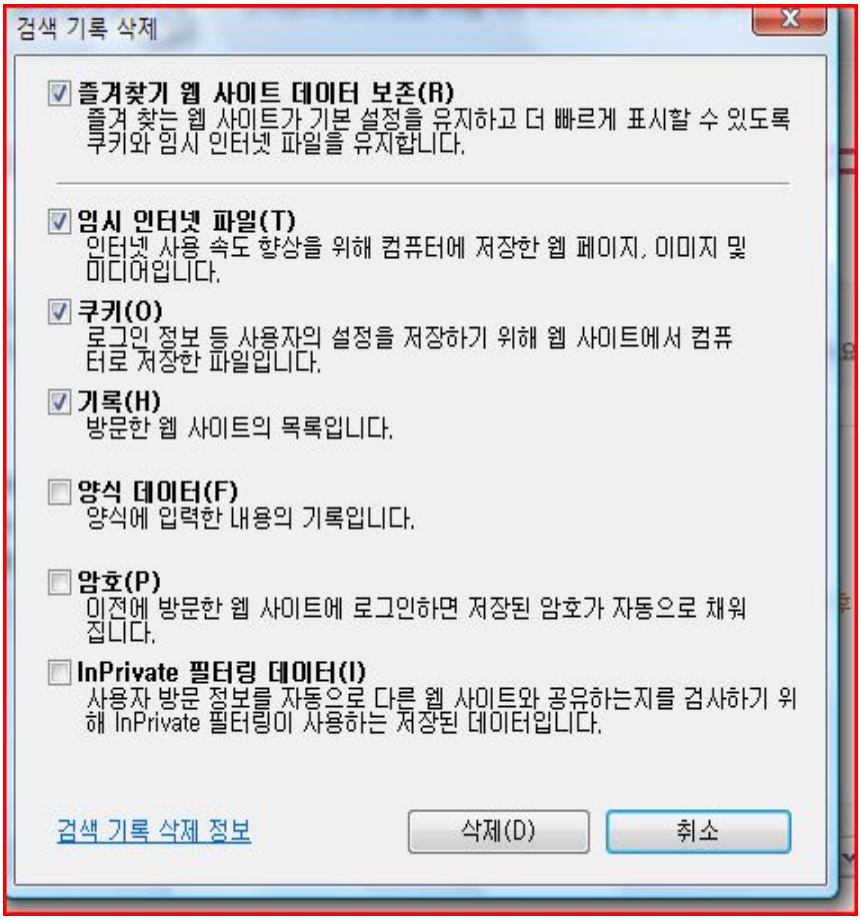
o InPrivate 기능: Internet Explorer8에 포함된 기능으로 InPrivate기능을 켜 놓으면 Internet Explorer가 사용자의 검색 세션에 대한 정보를 저장하지 못하도록 한다.



<그림25> InPrivate 기능1

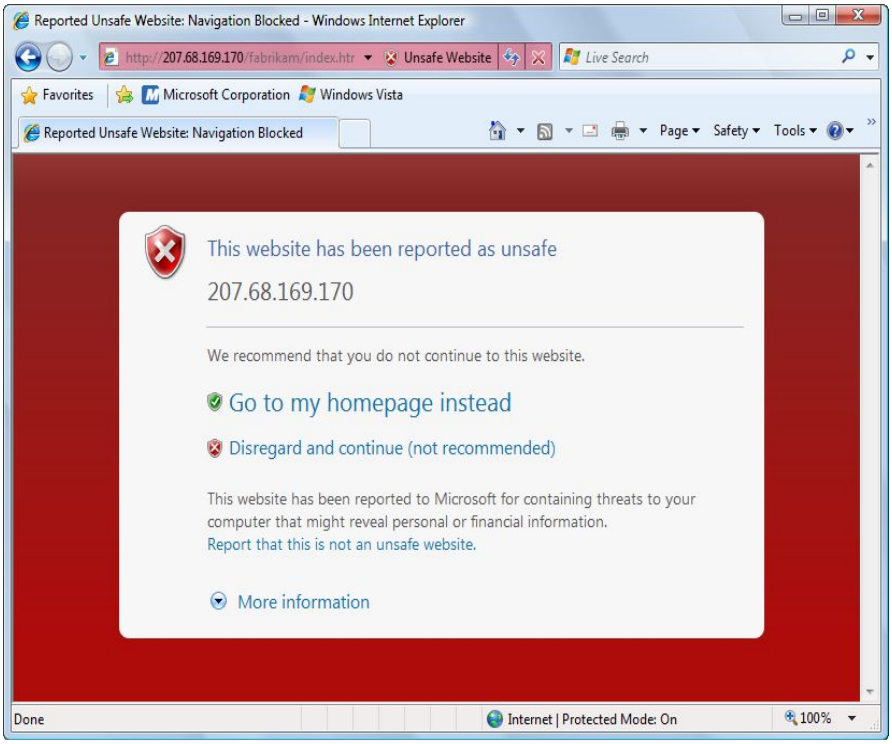


<그림26> InPrivate 기능2



<그림27> InPrivate 기능3

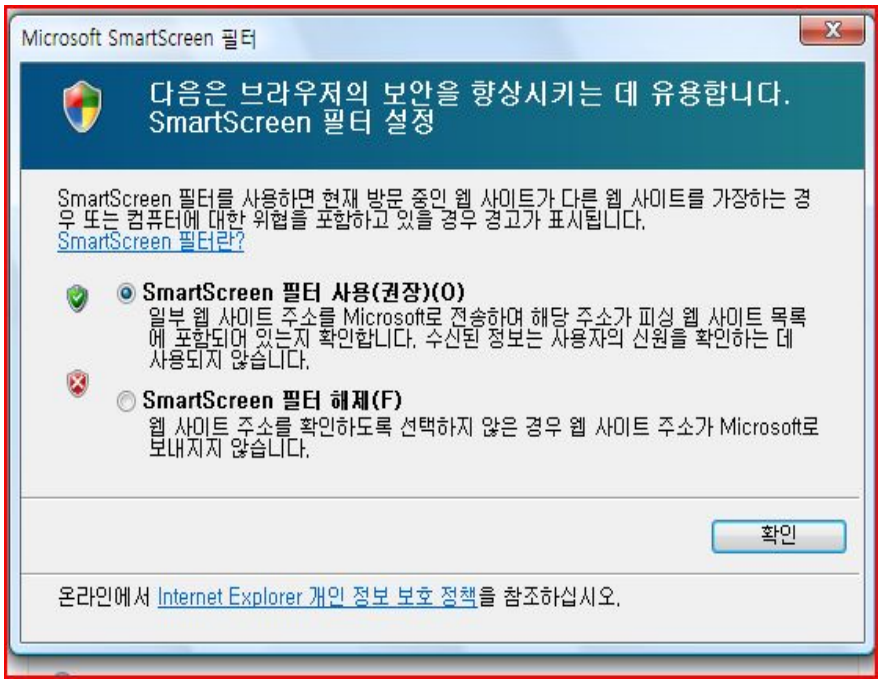
o SmartScreen: Internet Explore 8에 포함된 기술로 사용자가 사용하는 은행에서 온 이메일로 가장하거나, 게임이나 영화 검색 결과로 가장하거나 또는 공짜로 상품을 준다는 메시지나 광고 등으로 가장한 악성사이트들이 사회공학기법을 이용한 위협으로부터 사용자를 보호하기 위한 기술이다. 이 기술은 악성웹사이트를 탐지하여 그 사이트 전체를 차단하기도 하고 합법적인 웹사이트에 올라간 악성코드나 피싱 부분만 차단하여 합법적인 사이트의 다른 내용은 영향을 받지 않고 이용할 수 있도록 하기도 한다.



<그림28> SmartScreen

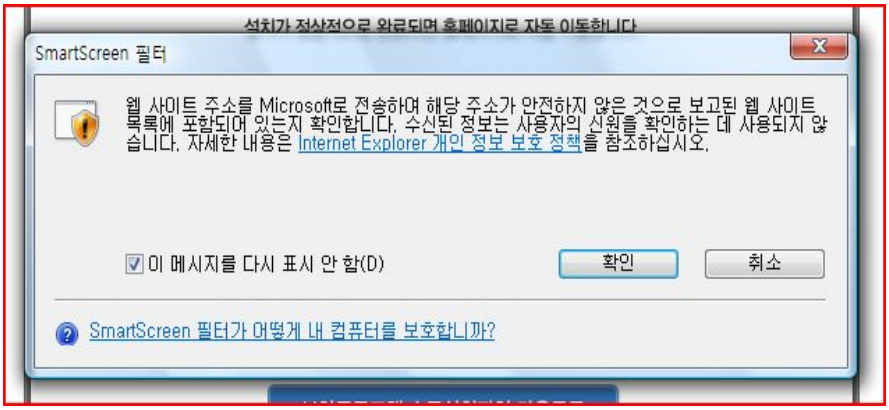
또한 SmartScreen에는 악성코드 다운로드로부터 사용자를 보호하는 기능도 포함되어 있다. 만일 사용자가 안전하니 않은 사이트로부터 다운로드를 받으려고 하면 다운로드를 차단하고 사용자에게 경고를 제공한다. 그러나 사용자가 안전하다고 확신하면 다운로드할 수 있다. 그러나 이 기능은 사용자가 켜놓을 수도 꺼놓을 수

도 있다. 그리고 사용자가 의심되는 악성 사이트에 대해서는 리포트를 할 수도 있다.



<그림29> SmartScreen 필터

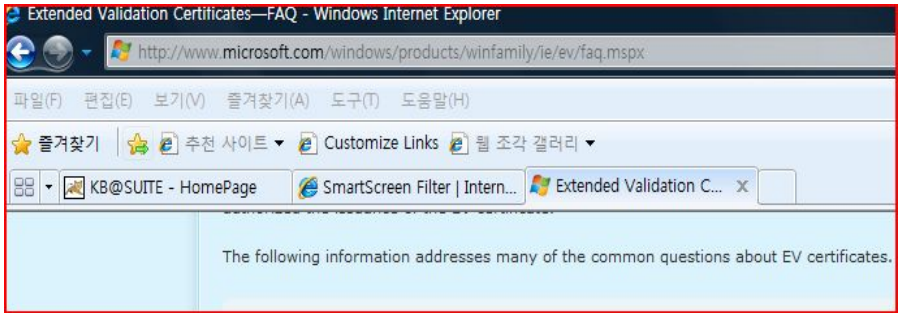
<그림30> SmartScreen의 보안 경고



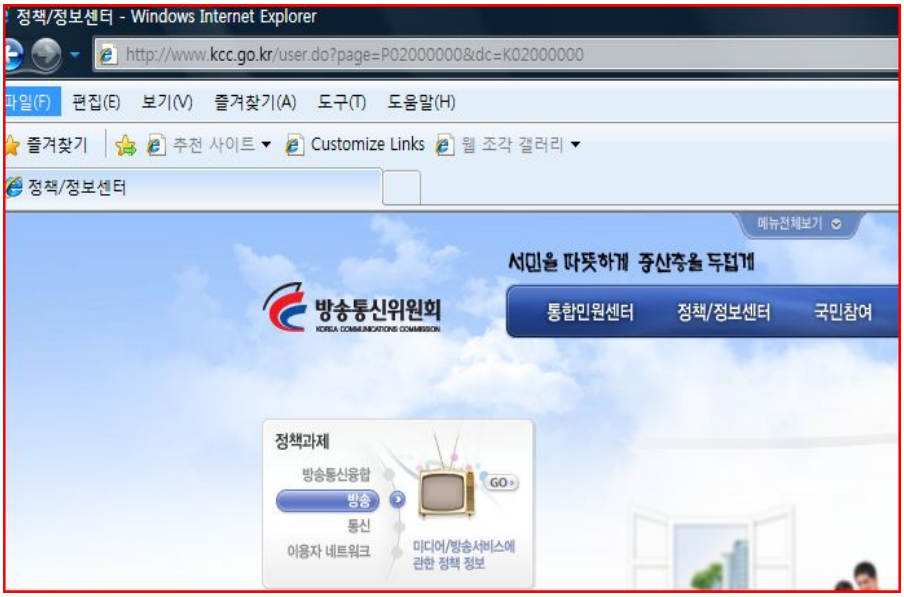
<그림31> SmartScreen 필터2

<그림32> SmartScreen 필터3

o 가짜 웹 주소를 알려주는 기능: Internet Explorer8에 포함된 기능으로 가짜 웹 주소로 사용자를 속이는 웹사이트를 피할 수 있도록 주소창에 도메인네임은 검정색으로, 나머지 주소는 회색으로 보이도록 하여 웹사이트를 잘 식별할 수 있도록 한다.



<그림33> 가짜 웹 주소를 알려주는 기능1



<그림34> 가짜 웹 주소를 알려주는 기능2

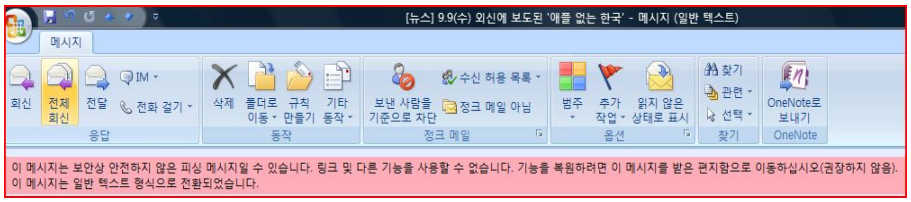
o Cross Site Scripting (XXS) Filter: 감염된 웹사이트에서 작동하는 악성코드(주로 ID도용에 사용됨)를 탐지할 수 있도록 한다.

3) Microsoft Office 2007의 보안기능

o Microsoft Office 보안경고: 사용자의 ID를 도용하기 위하여 사기성 이메일을 이용하거나 가짜 웹사이트를 이용하여 사기꾼들이 사용자로 하여금 민감한 정보를 제공하도록 한다. 마이크로소프트 오피스를 이용하여 작성된 파일에 들어있는 의심되는 링크를 클릭하면 아래와 같은 경고창이 뜬다. 그래서 사용자가 안심할 수 있는 사이트라면 계속 진행하거나 믿을 수 없는 사이트라면 사용을 중지할 수 있다.

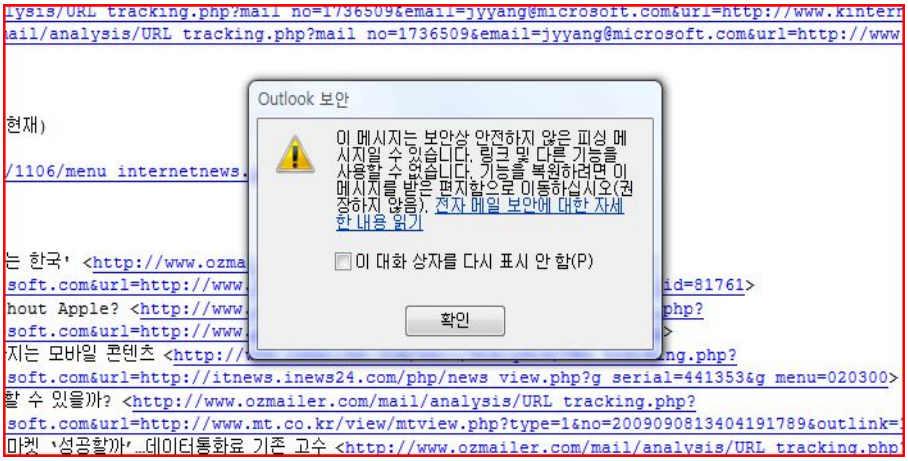
<그림35> Microsoft Office 보안경고

o 만일 이메일 메시지가 스팸의 정의에는 해당하지 않지만 Junk E-mail Filter의 정의에 의해 피싱 메일이라고 분류가 되면 사용자의 메일함에는 들어가 있지만 메시지에 포함된 모든 링크는 비활성화 되어 보인다. 만일 이메일 메시지가 Junk E-mail Filter의 정의에 의하여 스팸이고 또한 피싱 이메일로 분류가 되면 Outlook2007은 그 이메일을 정크이메일 폴더로 보낸다. 그러면 Outlook은 정크메일로 분류된 이메일에 포함된 모든 링크를 비활성화 시키고 메시지를 모두 단순텍스트로 전환한다.



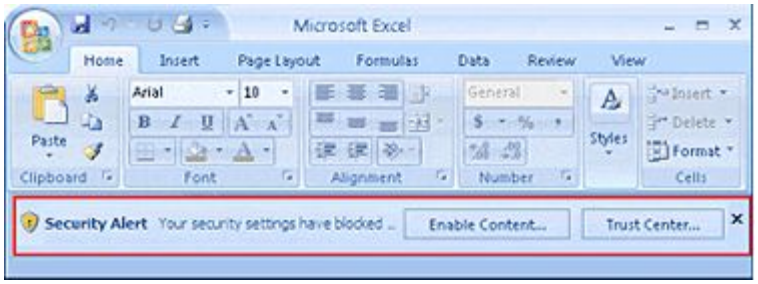
<그림36> Junk E-mail Filter에 의한 스팸·피싱 메일 분류

그리고 피싱 메일에서 비활성화 된 링크를 클릭하면 아래와 같은 보안 메시지가 뜬다.



<그림37> 비활성화 링크 클릭시의 보안 메시지

o 사용자의 보안과 개인정보보호를 위해서 Microsoft Office에서 이미지나 링크된 미디어, 데이터 연결 등 외부의 콘텐츠를 차단하기도 한다. 만일 workbook이나 프레젠테이션에 외부 콘텐츠가 포함되어 사용자가 파일을 열 때 메시지 창에 외부 콘텐츠가 차단되었다는 메시지가 뜬다.

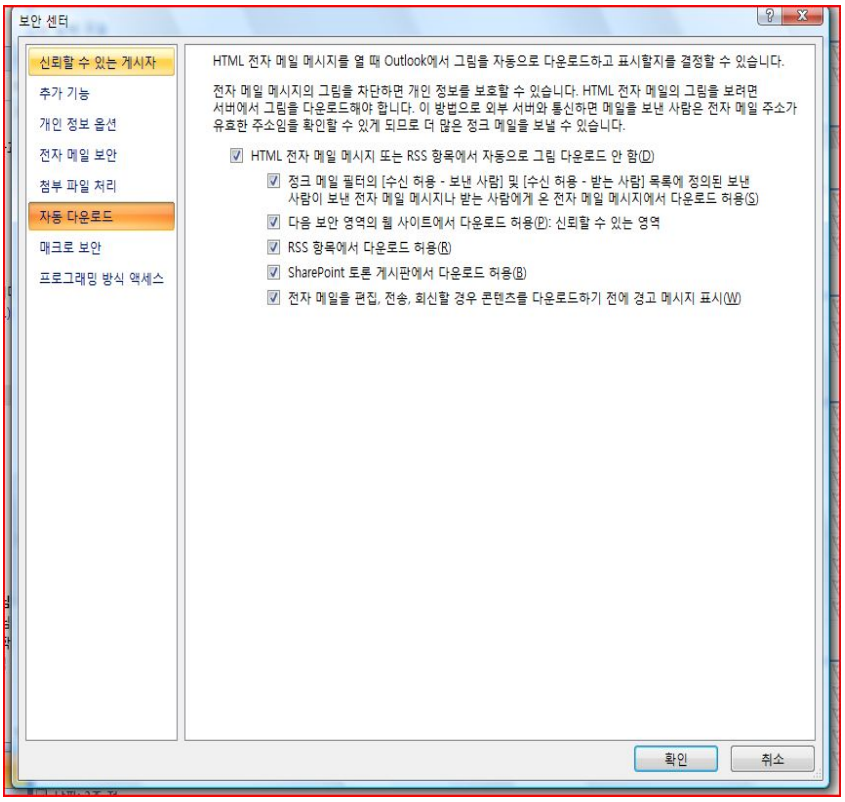


<그림38> 외부 콘텐츠 차단 메시지

사용자는 믿을 수 있는 출처라는 확신할 때에만 외부 콘텐츠의 차단을 풀어야 한다.

<그림39> 외부콘텐츠 차단 해제

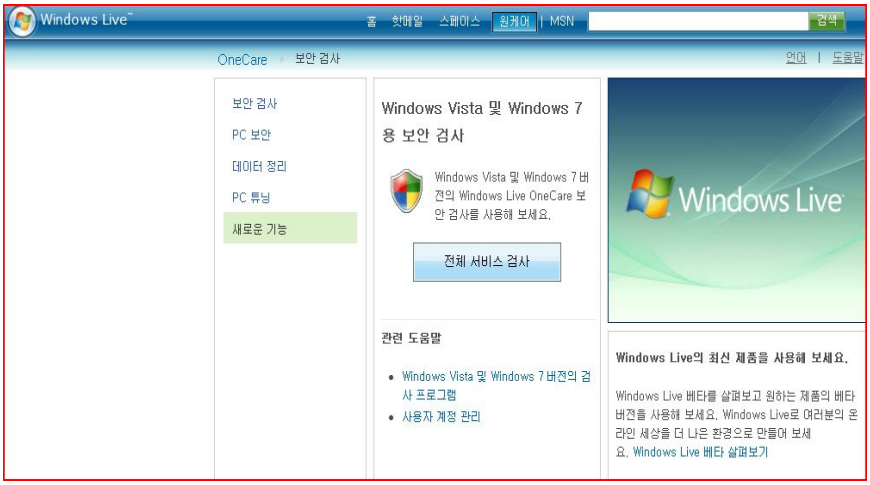
o 보안센터: 보안센터에서 보안설정이나 개인정보보호설정을 변경할 수 있다.



<그림40> 보안센터의 보안설정 및 개인정보보호설정 변경

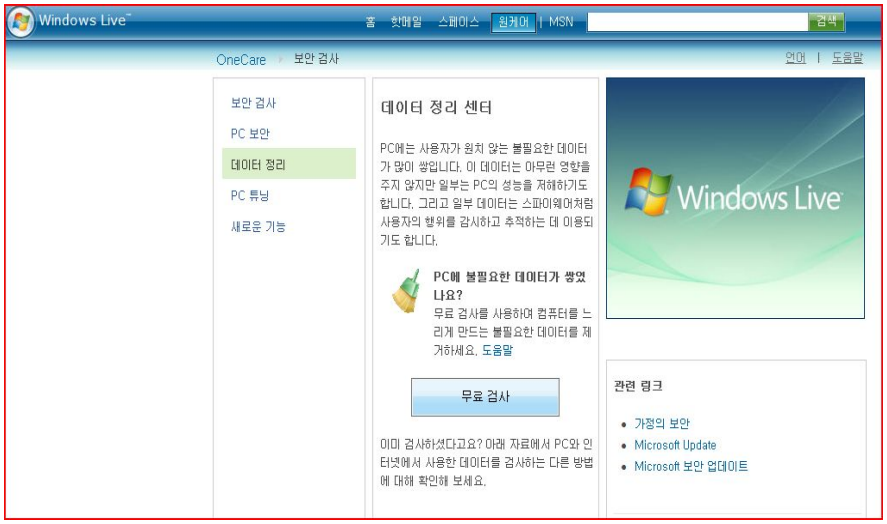
4) Windows Live Messenger와 Windows Live의 보안기능

o Windows Live Messenger,와 Windows Live의 Safety Scanner를 사용하면 바이러스로부터 하드디스크 단편화까지 원거리로 진단하고 치료할 수 있다.



<그림41> Windows Live의 보안기능1

<그림42> Windows Live의 보안기능2



<그림43> Windows Live의 보안기능3

제3절 일본에서의 정보통신망 자율규제 현황

1. 서론

일본에서의 정보통신망 자율규제는 다양한 각도에서 전개되고 있다. 실제로 정부가 개입하여 시큐러티의 확보를 위한 조치를 강제하는 경우(예; 바이러스백신 설치의 의무화)는 찾아 볼 수 없으며, 다양한 계획과 정책을 통하여 민관의 합동 대응체제를 갖추려는 노력을 볼 수 있다.

일본의 제1차 및 제2차 정보보호 기본계획이나 안심넷 만들기 촉진프로그램 등은 정보통신망에서의 시큐러티 확보나 정보보호 측면에서 정부 주도 일변도의 정책에서 벗어나 정보통신망을 이루는 정부·지방자치단체, 중요 인프라, 기업, 개인이 자발적으로 시큐러티를 확보하여 가는 것을 원칙을 삼고, 국가는 이들에게 '가이드라인'을 제공함으로써 밑받침하려는 노력의 일환이다.

현재 일본에서의 정보통신망 시큐러티는 주로 NISC(National Information Security Center)에서 담당하고 있다. 이는 內閣官房情報시큐러티센터라고 하며, 정보시큐러티에 관한 국가센터로서 2005년 4월 25일에 설립되었다.

2. 정보통신망 자율규제 계획

가. 기본 목표의 실현을 향한 대응

1) '새로운 관민 제휴 모델'

시큐어 제팬 계획에 따라 수립된 제1차 기본계획아래에서의 3년이 지난 현 단계에서도 일본은 시큐러티체제의 구축으로부터 유지·발전을 하여, IT사회를 구성하는 모든 주체의 각성을 수반한 참가와 적절한 역할 분담을 추구하는 것이 불가결하다고 평가하여, 제2차 기본계획에서는 제1차 기본계획에서 내걸었던 '새로운 관민 제휴 모델'의 유지·발전을 통하여 정책을 더욱 진화시키도록 하고 있다.

2) 대책 실시 측과 정보 제공 측의 쌍방에서의 검토

제1차 기본계획아래에서의 '새로운 관민 제휴 모델'은 IT사회를 구성하는 모든 주체의 참가를 염두에 두고, 첫째, 대책 실시 주체, 즉 대책을 실제로 적용하고 실시하는 주체(① 정부기관·지방공공단체, ② 중요 인프라, ③ 기업, ④ 개인), 둘째, 문제의 이해·해결을 촉진하는 주체, 즉 대책 실시 주체가 실제로 대책을 적용하고 실시함에 있어, 그 대책의 수법이나 환경 정비를 측면적으로 지원하고 문제의 이해·해결을 촉진하는 주체(① 정책을 입안·실시하는 주체로서의 정부·지방공공단체, ② 초등 중등 교육 기관, 고등교육 기관 및 연구개발·기술개발 실시 기관, ③ 정보시스템의 구축이나 통신 서비스의 제공 등 IT기반을 구축·제공하고 있는 사업자(이하 '정보 관련 사업자'라고 함)나 비영리 조직(이하 '정보 관련 비영리 조직'이라 함), ④ 미디어)를 설정하고 있다. 제2차 기본계획아래에서도 이 구조는 유지하는 것으로 한다.

그러나 '사고 전제 사회'에 대한 대응력 강화와 함께 합리성에서 증명된 어프로치를 실현할 수 있도록 IT시대의 강한 '개인'과 '사회'를 확립하는 관점에서는 대

책의 실시에 관련된 측만을 염두에 두는 것은 충분하지는 않다. 정보보호 대책에 의해 지켜야 할 정보 자산은 대책을 실시하는 주체 자신의 것만이 아니고 다른 주체로부터 맡은 것인 경우도 있다. 정보 수수의 과정에 관련된 모든 주체가 사고의 가능성을 완전하게 배제하는 것을 목표로 했다고 해도 결과가 그렇게는 안 되는 경우를 생각해 두어야 한다고 하는 것에 관해 이해를 깊이는 것이 필요하다.

따라서 제2차 기본계획에서는 정보를 맡기는 측도 정책의 대상으로 하여, 셋째, 대책 실시 주체를 포함한 대책 추진 측 이외에 개인정보와 같은 자기의 정보 등을 맡기는 정보 제공 주체(및 그 반대 측의 입장에서 정보를 맡기는 정보 관리 주체)를 설정한다. 즉, 제2차 기본계획에서는, 첫째, 대책을 직접 실시하는 주체나 대책을 지원하는 주체를 염두에 둔 제1차 기본계획아래에서의 종래의 어프로치를 보완·강화하는 형태로, 둘째, 정보를 맡기는 주체를 염두에 둔 새로운 어프로치를 채용하여 두개의 어프로치로부터 대응을 진행시킨다.

나. 제2차 정보보호 기본계획상의 정책 영역

이상을 근거로 하여 IT안심 이용 환경의 구축을 향해 향후 대응을 진행시키는 정책의 영역은 이하와 같이 몇 개의 측면에서 정리할 수 있다. 이것으로부터도 알 수 있듯이 제2차 기본계획이 취급하는 정책 영역은 상당히 다면적이 된다.

1) 과제의 파악에서 사전 대책, 사후 대응까지의 고려

정보보호 정책을 보다 현실에 입각해서 실효적인 정책으로 하는 관점에서 과제의 파악으로부터 사전의 대책, 또 문제가 발생했을 때의 사후 대응까지를 일관하여 실시하는 영역으로 한다. 그리고 정보보호 정책을 일련의 대응 능력이 높은 정책으로 발전시킨다.

2) 기술면에서의 대응으로부터 제도면, 인적 측면의 대응까지 고려

정보보호 대책의 추진에는 대책과 관련되는 기술적인 측면에 더하여 제도 면이나 대책을 실시하는 인적 측면으로부터의 종합적인 대응이 필요하다. 이러한 균형있는 편성이 필요하고, 제2차 기본계획 아래에서도 기술개발에 관한 대응으로부터 인재육성과 같은 대응까지 종합적으로 대응을 한다. 또 규범을 포함한 제도 면과 관련된 검토도 진행한다.

3) 국내에서 정보보호 대책의 추진으로부터 정보 시큐러티 확보를 위해서 국제적으로 행해지는 활동의 고려

IT의 이용·활용이 국경을 넘어 당연한 일이 되고 있는 것에 비추어 보면, 정보보호 정책은 국내만을 대상으로 하여 추진하는 것은 불충분하다. 국내에서의 대책은 그것으로서 추진하지만 동시에 국제적인 대응과 서로 유기적으로 결합된 정책으로 발전시킨다.

4) 국민의 일상생활이나 경제활동이라는 개별 주체에 직접적으로 관계가 깊은 영역으로부터, 안전 보장이나 문화라는 일본 전체에 관계가 깊은 영역의 고려

제2차 기본계획아래에서 대응을 하는 정보보호 정책의 영역은 개인의 IT활용 시에 있어서의 주의를 환기하는 것이나, 기업의 경제활동에서 맡은 정보를 어떻게 관리하는가라는 개별 주체의 매일의 활동에 직접적으로 관계가 깊은 것이 거례될 수 있다. 이에 더해, 일본의 안전보장상 중요한, 정보 시큐러티와 관련된 위협 정보의 국제적인 파악이나, 정보 시큐러티가 중요하다는 문화의 양성 등 일본 전체에 관계 깊은 영역도 거례되고 있다.

다. 정책의 추진 체제와 지속적 개선

1) 정책의 추진 체제

「성숙한 정보보호 선진국」을 목표로 하면서, 「IT를 안심하고 이용할 수 있는 환경」의 구축을 실시하기 위해서는 모든 주체에서의 의식 공유와 함께 참가가 불가결하다. 일본 정부는 IT시대의 강력한 '개인'과 '사회'의 확립을 도모하면서 제2차 기본계획의 중점 정책을 중심으로 관민에서의 통일적, 횡단적인 정보보호 대책을 추진하기 위하여 전체적으로 적정한 자원 배분을 실시해 갈 필요가 있다고 평가하고 있다.

가) 내각 관방 정보 시큐러티 센터(NISC)의 강화와 역할

NISC는 제1차 기본계획아래에서의 대응과 같이 국제적으로나 국내적으로도 최고의 지혜를 결집해 나가기 위한 체제로서 정부 전체의 추진 체제를 유효하게 기능시키기 위한 핵심으로 강화하는 것을 계속 목표로 하고 있다. 또 횡단적인 정보시큐러티 문제에 관한 국제 POC로서의 역할을 충분히 완수할 수 있도록 계속 강화해 간다.

나아가 NISC는 정보 시큐러티에 관련된 많은 지견이 민간에 축적되고 있는 것으로부터 민간의 인재를 적극적으로 활용하는 것에 노력함과 동시에, 유연하게 정부 내의 인재를 최대한 활용하고 그 능력의 유지·강화를 도모한다. 동시에 정부 직원의 인재육성 핵심 거점으로서 기능하는 것도 목표로 하고 있다.

이 기본계획의 내용에서도 분명하듯이 정보 시큐러티 정책의 정책 영역은 다방면에 걸쳐있다. 이 때문에 NISC는 관련 영역을 담당하는 여러 기관과의 결절점이 됨과 동시에, 과제 마다 해결을 향한 관계 기관의 제휴 체제의 최적화를 유연하게 진행하여 정보 시큐러티에 관련된 과제에 대한 일본 전체에서의 해결 능력의 최대화를 실현하기 위해서 솔선하여 활동하고 있다.

나) 각 부성청의 강화와 역할

각 부성청은 계속 정보보호 정책 회의, NISC를 핵심으로 한 정보보호 정책을 추진하는 구조 하에 부성청의 정보보호 정책 및 관련 영역과 관련된 체제의 충실·

강화를 도모한다. 체제의 충실·강화로서는 필요에 따라 민간 인재의 적극적인 활용을 포함해 유효한 방책을 유연하고 최대한으로 활용한다. 그리고 추진 체제가 종적관계가 되지 않게 충분히 유의하면서 관민에서의 통일적·횡단적인 정보보호 대책의 추진을 하도록 각종 정책의 실시에 계속해 노력한다.

3) 상황의 변화의 적시 적절한 파악과 새로운 과제에의 대응

정보 시큐러티 분야는 위협이나 기술 등 여러 가지 측면에서 변화가 빠르다. 때문에 시시각각 변화하는 상황을 적시 적절히 파악함과 동시에 새롭게 발생하는 과제에 대해서 신속하고 적확한 대응을 실시하는 것이 중요하다. 또 새롭게 트렌드가 되는 정책에 관해서도 적절한 검토를 하는 것이 불가결하다. 게다가 정보 제공 주체를 대상으로 한 새로운 대응을 하는 것도 필요하게 된다. 이 때문에 NISC를 필두로 하는 여러 관계 기관·관계자가 제휴하고, 또 정보보호 정책 회의 하에 적절히 설치된 전문 위원회도 활용하여 법률, 기술 계발 등 정책과 관련된 폭넓은 시점 전반에서의 검토를 동적이고 유연하게 진행하는 체제를 강화한다.

라. 다른 관계 기관과의 관계

일본은 제2차 기본계획은 일본의 정보 시큐러티 문제를 조감한 중장기 전략을 정하는 것인데, 정보보호 정책은 국민 생활·사회경제 활동에 넓게 관계하는 것이고 그 실시에서는 제1차 기본계획과 마찬가지로 여러 관계 기관과의 제휴를 추진할 필요가 있다고 파악하였다.

여러 관계 기관 중에서도 IT전략 본부와의 관계에 관해서는 정보보호 정책이 IT정책의 주요한 부분의 하나로서 위치되는 것이고, 한편 제2차 기본계획이 「IT 신개혁 전략」의 정보보호 관련 부분을 실질적으로 담당하는 것임에 유의할 필요가 있다. 또, 총무성 행정 관리국과는 행정 정보 시스템에 관련하는 대응을 중심으로 제휴를 더욱 강화하도록 하는 것이 불가결하다고 평가하고 있다.

중앙 방재 회의와의 관계에서는, 정보보호 정책 중 중요 인프라 관련 부분에서

필요한 제휴를 하는 것이 필요하다고 평가된다. 또, 종합 과학기술회의와의 관계에 대해서는 정보 시큐러티 정책 중 연구개발·기술개발 관련 부분과 전체의 과학기술 정책이 정합해 추진되는 것을 확보할 필요가 있다고 평가하고 있으며, 게다가 국민 생활 심의회와의 관계에 대해서는 개인 정보 보호 등의 관점으로부터 정보를 제공하는 측의 주체와 관련되는 대응을 진행함에 있어 충분히 제휴할 필요가 있다고 평가하고 있다.

정보보호 정책 회의 및 NISC는 이러한 회의의 충분한 협력을 얻으면서 정보보호정책을 추진해 가고 있다.

마. 지속적 개선 구조의 구축

정보 시큐러티를 둘러싼 문제는 새로운 리스크 요인이 차례차례로 발생하고 그 변화가 빠르기 때문에 정책의 효과를 항상 평가하고 개선을 해 가는 것이 필요하다, 이 때문에 일본 정부는 제1차 기본계획아래에서의 대응에 계속하여 다음과 같은 지속적 개선을 위한 구조를 활용하고자 계획하고 있다.

1) 「연도 계획」의 책정과 그 평가

일본 정부는 제2차 기본계획을 실현하기 위해 매년 보다 구체적인 시책의 실시 프로그램을 「연도 계획(시큐어·재팬 20XX)」으로 책정함과 동시에, 그 실시 상황을 사회 정세의 변화와 함께 평가하여 결과를 공표하고 있고, 또 보완 조사를 필요에 따라 실시하여 이 결과도 아울러 「20XX년도의 정보보호 정책의 평가 등」으로서 공표하고 있다. 이 대응에 있어서는 상세한 내용을 정보보호 정책 평가 등의 기반 문서에 의해 정해진 기반에 따르는 것으로 하고 있다. 덧붙여 정부 이외의 관계 기관에 있어서의 대응이 불가결한 것 등 시책을 원활히 진척시키려는 관점에서 중장기적인 계획을 정하는 것이 필요한 것에 관해서는 연도에 집착하지 않고 복수 연도의 방향 설정도 하도록 하고 있다.

2) 연도 계획 실시 중의 긴급사태 대응

일본 정부는 「연도 계획」의 실시 중에도 새로운 리스크 요인이나 상정 할 수 없었던 사고, 재해나 공격의 발생 등 긴급사태에 대응하기 위한 대응을 아울러 실시하도록 하고 있다.

3) 평가 지표의 개선

각 대책 실시 영역 등에서의 정보보호에 관한 평가의 지표는 정보보호 정책의 기반 문서에 의해 설정되어 있는 바, 정부는 동 기반 문서에서 정한 방법에 의해서 향후 계속 평가 지표의 개선을 도모하고 있다. 덧붙여 중요 인프라의 영역에 관해서는 제2차 행동계획에서 선행적으로 평가지표의 개선을 하고 있기 때문에 동 기반문서에서 평가 지표의 개선에 관해서는 제2차 행동계획에서의 평가 지표를 기본으로서 검토하는 것으로 하고 있다.

4) 제2차 정보보호 기본계획의 재검토

일본 정부는 제2차 기본계획에 대해 3년 후에 재검토를 실시하는 것과 동시에, 환경 변화가 생겼을 경우에는 기간 중이라도 재검토를 실시하도록 하고 있다.

3. 민간 자율규제를 향한 정부의 주도 및 지원

일본에서는 휴대전화 필터링 도입 촉진과 그 개선을 향한 검토를 전후하여 국회에서는 여야당의 쌍방에 대해 인터넷상의 위법·유해 정보 대책으로서 법규제의 도입을 목표로 한 검토의 장이 연달아 설치되었다. 또 지방공공단체에서도 히로시마시와 같이 독자적으로 조례를 제정하는 움직임을 볼 수 있었다.

여야당에 있어서의 법안의 검토 단계에서는, 국가가 유해 정보를 정의하고, 사이트 관리자 등에게 유해 정보의 열람 방지조치를 의무화 하는 등 규제색이 강한

안이 신문지상에서 보도되었다. 이것에 위기감을 가진 학식 있는 경험자나 민간단체는 법 규제 도입 반대의 공동성명을 발표했다.

또 콘텐츠 관련 기업 등도 법 규제 도입에 대한 염려를 표명하는 기자회견을 실시하거나 자사 사이트의 유해 정보 대책의 강화를 발표하거나 하는 등 민간 측의 움직임이 활발해졌다. EMA 등의 제삼자 기관의 설립도 민간의 자주적 대응을 법 규제에 선행시키려고 하는 시도로서 파악된 면도 있다. 또 사단법인 일본신문협회가 2008년 5월 29일 및 6월 6일에, 사단법인 일본 민간방송 연맹이 6월 2일, 6일 및 11일에 유해 정보의 판단에의 국가의 관여 등을 염려하는 의견을 발표했다.

제169회 국회(상회) 회기 말이 가까워진 5월 하순 이후, 여야당 사이에 각각의 안에 근거한 법안의조정이 급피치로 행해져 6월 6일, 중의원의 청소년 문제에 관한 특별 위원회에 대해 「청소년이 안전하게 안심하고 인터넷을 이용할 수 있는 환경의 정비 등에 관한 법률안」[79](이하 '청소년 인터넷 환경 정비법'이라고 함)이 위원장 제안에 의해 제출되었고, 6월 10일에 참의원 내각 위원회에서의 참고인 질의 및 법안 제출자에 대한 질의를 거쳐 다음 11일에 참의원 본회의에 대해 가결되어 성립했다.

참의원 내각 위원회의 참고인 질의나 법안 제출자에 대한 질의에서는 기본계획이나 필터링 추진 기관의 등록 등에 대해서, 유해 정보의 기준 책정 등에 국가가 관여하는 방향으로 운용되는 것은 아닌가 하는 염려가 있어 부대 결의에서 정부가 "사업자 등이 실시하는 유해 정보의 판단, 필터링의 기준 설정 등에 간섭하는 경우가 없게 할 것"이라고 하였다.[80]

여기에서 확인할 수 있듯이 일본에서는 민간에서 뿐만 아니라 정부에서도 법률에 의한 규제를 원하지 않고 민간의 자율적 규제를 지원하는 움직임이 강하다.

다만 정부는 민간이 자율적 규제를 할 수 있도록 제도적 기술적 지원에 배려하고 있을 뿐이며, 이러한 민관의 협력체제의 조성을 위하여 정부가 적극적으로 나서서 주도하고 합의를 도출해 가고 있는 것이다.

---

79) 2008년 12월 10일에 공포된 동법 시행령에 의해 2009년 4월 1일에 시행되었다. 동법 부칙 제3조에서는 시행 후 3년 이내에 이 법률의 상황에 관해 검토하고, 그 결과에 기해 필요한 조치를 강구하도록 하고 있다.

80) 「청소년이 안전하게 안심해 인터넷을 이용할 수 있는 환경의 정비 등에 관한 법률안에 대한 부대결의」(2008년 6월 10 일 참의원 내각 위원회)

민간에서는 정부나 지방공공단체의 정보보호정책이나 가이드라인을 참고로 하여 기업이나 단체에서 개별적으로 가이드라인을 만들어 시큐러티를 확보해 가고 있는 중이다.

4. 민간기구

가. 일본컴퓨터긴급대응센터(JPCERT/CC)

1996년 10월 임의단체로 설립되었으며 2003년 3월 중간법인이 되었다. JPCERT 코디네이션센터는 인터넷을 매개로 발생하는 침입이나 서비스방해 등의 컴퓨터 시큐러티 인시던트에 관해 일본 내의 사이트에 관한 보고의 접수, 대응의 지원, 발생상황의 파악, 범죄수법의 분석, 재발방지를 위한 대등한 검토나 조언 등을 기술적인 입장에서 하는 곳이다. 특정한 정부기관이나 기업으로부터는 독립한 중립조직으로서 일본에서 정보보호대책활동의 향상에 적극적으로 대응하고 있다.
JPCERT/CC는 취약한 소프트웨어에 관해 주의 환기 정보를 보내며, 나아가 조기 경계하도록 하고 있다.

1) 주의환기

심각하고 영향범위가 넓은 취약성 등에 관한 정보를 고지하는 것이다.

2) 조기경계정보의 제공

JPCERT/CC에서는 국민의 사회 활동에 큰 영향을 주는 인프라, 서비스 및 프로덕트 등을 제공하고 있는 조직에서의 정보 시큐러티 관련 부서 혹은 조직 내 CSIRT를 향해 위협 정보나 분석·대책 정보를 조기 경계 정보로서 제공하고 있다.
조기 경계 정보의 주된 제공 대상은 국민의 사회 활동에 큰 영향을 주는 인프라, 서비스 및 프로덕트가 제공되고 있는 조직 및 단체에 있어서의 정보 시큐러티 관

련 부서 혹은 조직 내 CSIRT에서 제공하는 정보 취급 등에 대해 사전에 합의를 받을 필요가 있다. 조기 경계 정보 제공의 대상 조직의 예는 다음과 같다.

- 정부계 조직
- 각종 공공단체 (지방공공단체, 공공 조합, 영조물 법인, 독립 행정법인 등)
- CEPTOAR (중요 인프라 10개 분야의 각 사업자에게 있어서의 정보 공유·분석 체제)
- 중요 인프라 사업자
- 중요 인프라에 관련되는 제품발행을 하고 있는 사업자
- 산업 기기의 제어 등을 하는 편성 기기의 개발·제공을 하고 있는 사업자
- 국민에게 널리 서비스나 인프라를 제공하고 있는 사업자
- 국민에게 널리 이용되는 전자 제품이나 제어기기 등을 제공하고 있는 사업자
- 조직의 정보 시큐러티 관련 부서 또는 조직 내 CSIRT
- 조기 경계 정보의 구체적인 제공자는 비공개로 하고 있다.

3) 취약성대책정보

2004년 7월 7일에 경제산업성에서 공시된 「소프트웨어 등 취약성 관련 정보 취급 기준」에서 JPCERT/CC는 일본 내의 취약성 관련 정보 유통을 위한 조정 기관으로서 지정되었다. 동 지정 고시에 의해 정보의 접수 기관과 지정을 받고 있는 독립 행정법인 정보처리 추진 기구 (IPA)와 제휴하여 일본 내에서의 취약성 관련 정보 유통을 실시한다. 또 상기 기준을 근거로 하여 IPA, 사단법인 전자 정보기술 산업 협회 (JEITA), 사단법인 정보 서비스 산업 협회 (JISA), 사단법인 컴퓨터 소프트웨어 협회 (CSAJ), 특정비영리 활동 법인 일본 네트워크 시큐러티 협회 (JNSA)와 공동으로 취약성 관련 정보의 유통에 관련된 관계자, 관계 업계로서의 지침 「정보 시큐러티 조기 경계 파트너십 가이드라인」을 만들었다.

나. 정보처리추진기구(IPA)[81]

81) Information-technology Promotion Agency

1970년 정부산하기관인 정보처리진흥사업협회로 설립되었으며, 2004년 1월 정보처리추진기구로 이름을 바꾸었다. 주요기능으로는 프로그램개발 및 이용촉진, 정보산업 지원 및 육성, 소프트웨어 연구개발, 정보보안 기술개발사업을 추진하고 있다. 산하조직으로 1997년 1월 '시큐러티센터'를 설치하여 안전한 컴퓨터이용환경을 구축하기 위한 바이러스대책, 신종 바이러스 정보, 부정액세스대책 발표 등 정보보호 대책의 강화 및 정비를 추진하고 해킹·웜 바이러스 신고접수 및 관련취약점 정보를 게시하고 있다.

다. 일본컴퓨터시큐러티협회(JCSA)

컴퓨터프로그램·시스템 및 데이터 등의 안전에 대한 조사·연구·감시를 통해 컴퓨터시스템을 보호하는 한편, 정보보호의식 향상 등 관련정보를 제공하고 있다.

라. 일본네트워크시큐러티협회(JNSA)

네트워크사회의 정보보호의식 제고 및 최신정보보호기술육성, 정보보호에 대한 위협관련정보를 제공하고 있다.

마. 일본의 사이버클린센터(Cyber Clean Center)[82]

호주의 AISI와 비슷한 민관 협동 자율규제 단체가 일본에도 있다. 일본의 사이버클린센터는 ISP와의 공조로 봇 바이러스와 같은 악성 프로그램들을 방지하기 위해, 일본의 총무성(Ministry of Internal Affairs and Communications), 경제산업성(Ministry of Economy, Trade and Industry), Telecom-ISAC Japan, JPCERT Coordination Center, Information-Technology Promotion Agency, ISP, 백신 프로그램 개발사, 보안업체들이 함께 참여하는 프로그램이다.

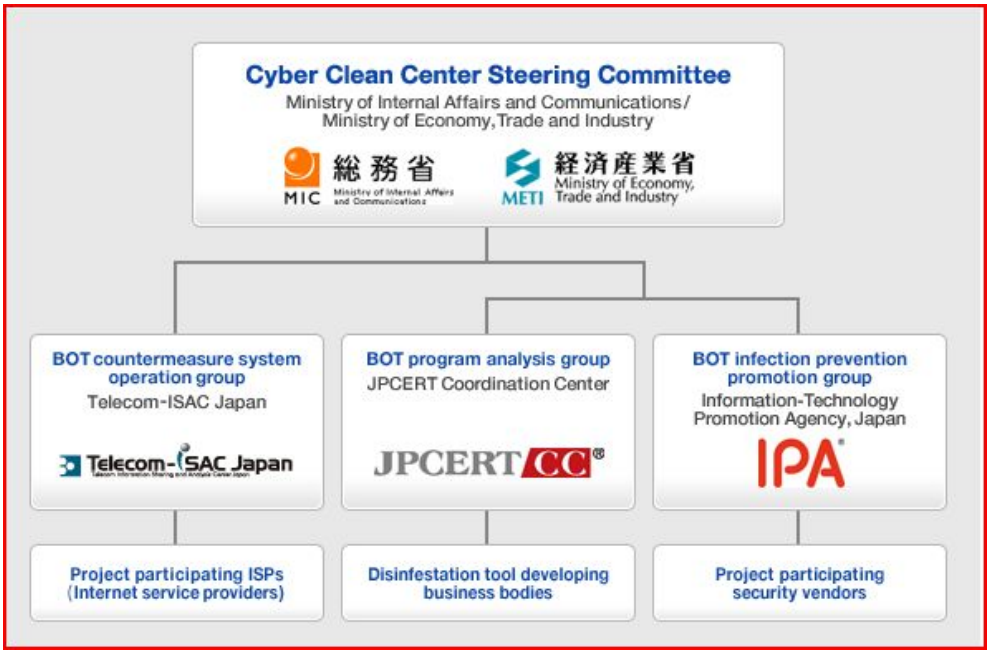
일본은 MSRT 감염정보와 SIR 자료[83]에 의하면 항상 Botnet감염 비율이 가장

82) 일본 Cyber Clean Center웹사이트 https://www.ccc.go.jp/en_index.html 의 자료를 참조한다. 이하 Cyber Clean Center에 대한 자료 요약은 위의 사이트의 자료를 참조하였다.

낮은 것으로 나타나고 있다. 일본의 사이버클린센터의 경우 Botnet 대응 방법에 있어서는 세계에서 가장 성공적인 모델로 고려되고 있다. 일본의 성공적인 예에 나타나듯이 사이버보안에 있어 중요한 점은 규제 중심이고 다소 유동적이지 않을 수 있는 정부 주도의 대응 방법보다는 ISP들과 보안 사업자들, 그리고 정부, 그리고 마이크로소프트와 같은 운영체제 개발자들의 유연한 공조를 통한 총체적인 접근 방법이라는 것이다.

1) 사이버클린센터의 구조

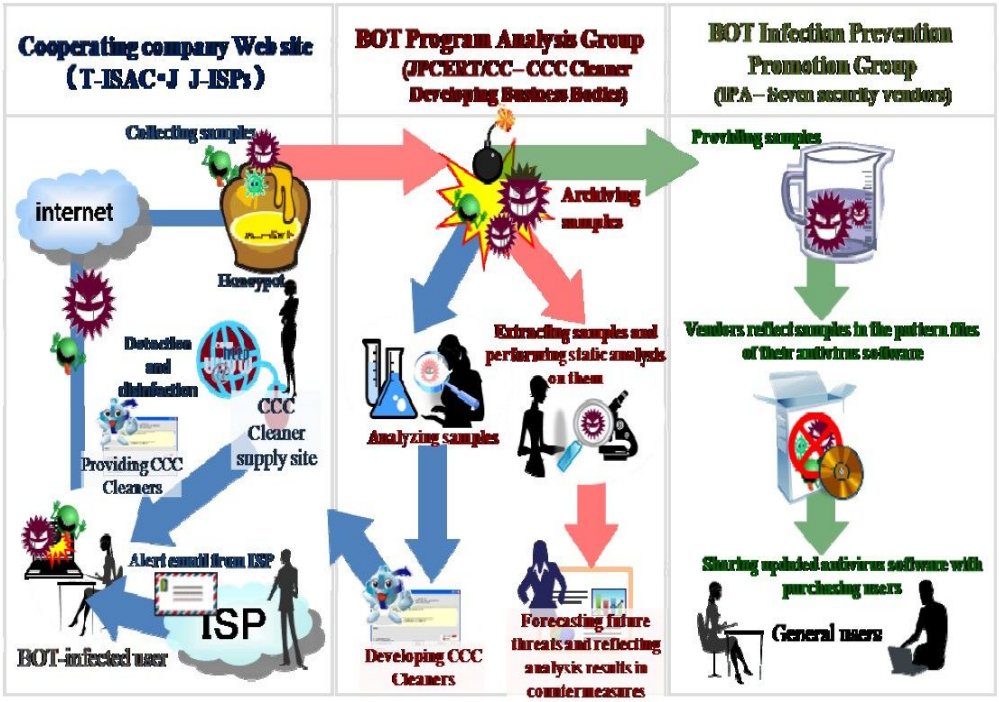
사이버클린센터에는 사이버클린센터 운영위원회(Steering Committee)와 그 아래에 세 개의 실무 그룹(working group)이 있다.



<그림44> 사이버클린센터의 운영 구조

83) MSRT 툴을 통해서 지역적으로, OS 언어별로, OS 버전과 서비스 팩 별로 악성코드 감염에 대한 통계를 내고 있음. 그리고 이 통계 자료가 Microsoft의 반기별 보안 리포트에 상세히 설명되는데, 이 리포트의 이름이 Security Intelligence Report, 즉 SIR이라고 불린다. (http://www.microsoft.com/sir)

이 사이버클린센터에서는 가짜 서버인 “honeypots"를 제공해서 감염된 컴퓨터의 IP주소를 얻고 ISP와의 협조를 통해 감염된 컴퓨터의 사용자에게 통보를 한다. 대부분의 사용자에 대한 통보가 이메일로만 행해지는데 비해 사이버클린센터에서는 사용자에게 이메일과 함께 웹사이트 링크를 제공한다. 이러한 방법으로 감염된 컴퓨터의 사용자에게 봇 치료를 할 수 있는 웹사이트의 URL을 함께 보내고 있다.



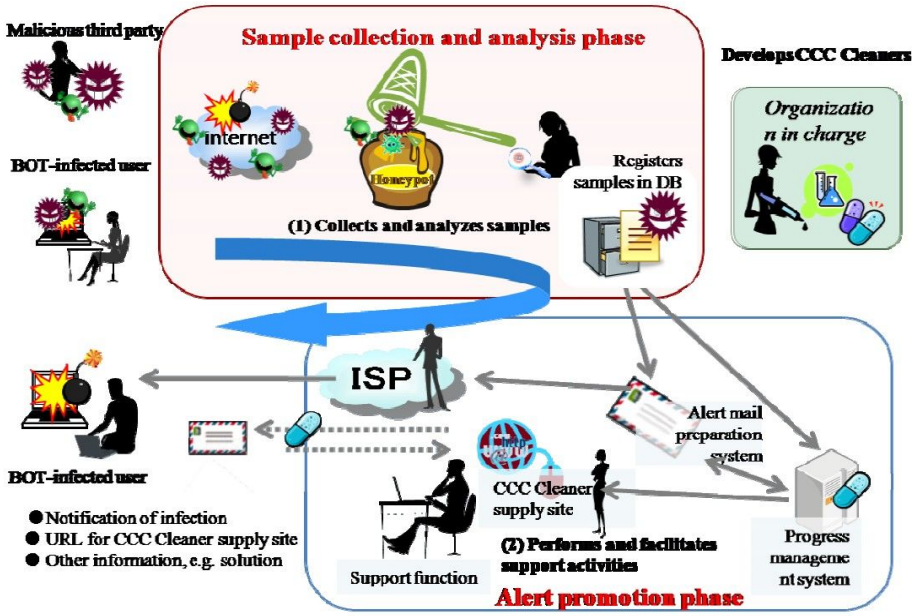
<그림45> BOT 프로그램 분석그룹의 운영방식

가) BOT 대응시스템 운영그룹(Telecom-ISAC Japan)

총무성은 통신을 관할하며 산하기구인 Telecom-ISAC-Japan을 통해 봇 대응 시스템 운용 그룹에서 네트워크상의 악성프로그램(Malware)을 "honeypot"을 이용하여 수집하는 역할을 한다.

BOT 대응시스템 운영그룹은 사이버클린센터의 백본 시스템(backbone system)을 운영하는 그룹으로, "honeypot" 등의 샘플 수집 및 분석시스템·경보시스템 운

영, BOT정보 수집 및 감염 PC 이용자에 경고 발령을 통해 참여하는 ISP의 PC치료, 기타 BOT 대응을 위한 여러 가지 활동을 전개하고 있다. 동 그룹은 수집한 BOT 샘플을 'BOT 프로그램 분석그룹'에 전달하여 CCC 클리너의 패턴 파일에 반영할 수 있도록 지원한다. 동시에 이 샘플을 'BOT 감염방지 그룹'을 통해 주요 프로젝트 참여 보안업체에 전달하여 백신소프트웨어의 패턴 파일에 반영할 수 있도록 지원하기도 한다.



<그림46> BOT 대응시스템 운영그룹의 운영방식

(1) 샘플 수집과 분석

BOT 대응시스템 운영그룹은 "honeypots"라고 불리는 유인 시스템(decoy system)을 통해 OS의 취약점을 고의적으로 노출해놓고 BOT 샘플을 수집한다. 수집되는 BOT 샘플에 대하여 동 그룹은 우선 복제체(duplicate)가 아닌지를 확인하고 아닌 경우 기존의 백신 프로그램으로 대응 가능한지를 파악한다. 마지막으로 샘플의 BOT은 실제 자가 실행되는 BOT인지 확인한다. BOT으로 확인된 샘플은 'BOT 프로그램 분석그룹'에 전달되어 CCC 클리너 개발을 위해 지원된다.

(2) 경보 활동

BOT 대응시스템 운영그룹은 honeypot으로 탐지한 공격 이벤트(공격진원지의 IP주소 및 시간정보)의 정보를 토대로 BOT 감염된 PC 이용자들에게 BOT 바이러스에 감염 가능성을 경고한다. BOT 감염에 대한 경고시 동 그룹은 공격 진원지의 IP주소를 이용하여 관련 ISP에게 먼저 경보를 주면, 관련 ISP는 BOT 감염 PC의 이용자에게 경고의 내용을 담은 이메일을 전송하는 방식을 취한다. 동 그룹은 사이버클린센터 홈페이지에 경고 이메일을 받은 PC이용자들을 위하여 대처할 수 있는 방법(CCC 클리너, 백신소프트웨어 설치, 윈도우즈 업데이트 등)을 제공하는 정보를 게재하고 있다.

나) BOT 프로그램 분석그룹

SW를 관할하는 경제산업성은 산하 정보처리추진기구(IPA)를 통해 'BOT 감염방지 그룹'으로 소프트웨어, 웹 보안취약점 점검 및 관련 사업을 시행한다. BOT 프로그램 분석그룹은 'BOT 대응시스템 운영그룹'이 수집한 BOT 샘플의 특징과 기술을 분석하고, CCC 클리너소프트웨어 개발자(CCC Cleaner software developer)들과 협력을 통해 CCC 클리너의 개발과 관련된 활동을 한다. 이 그룹은 또한 효율적인 분석시스템에 대한 연구를 진행하며, CCC 클리너소프트웨어 개발자와 함께 대응기술을 개발한다.

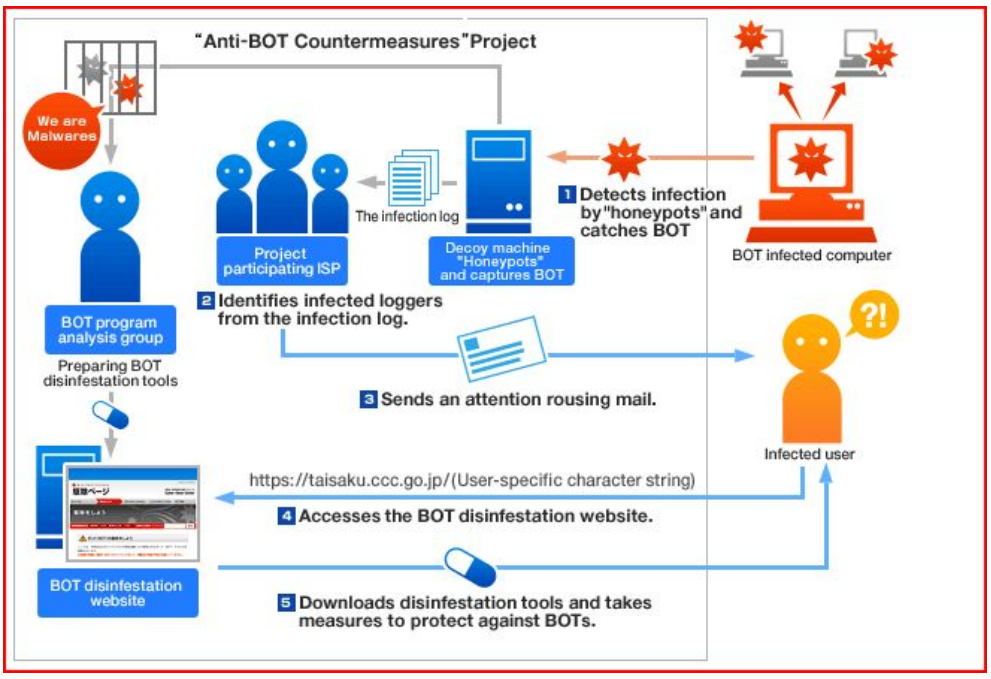
다) BOT 감염방지 그룹

IPA는 프로젝트에 참가한 정보보호 벤더(vendor) 들과 공저 하에 Clean-up Tool(악성바이러스·코드 백신)을 생산하여 사이버클린센터에 업로드 하는 등 일반 유저가 봇에 감염되지 않도록 하는 예방 사업을 추진 BOT 감염방지 그룹은 수집된 BOT 샘플을 기초로 BOT 감염예방 방책을 고안하며 참여 보안업체에 샘플을

제공하여 업체의 백신소프트웨어 개발에 사용할 수 있도록 지원한다. 동 그룹에 협조하는 참여 보안업체는 안철수 연구소(AhnLab Incorporated), 마이크로소프트, 시만텍(Symantec Corporation), 맥어피(McAfee Incorporated), Kaspersky Labs Japan Limited, Sourcenext Corporation, Trend Micro Incorporated 등이 있다.

2) 사이버클린센터의 작동 과정

아래 표를 통해 사이버클린센터가 작동하는 과정을 볼 수 있다.



<그림47> 사이버클린센터의 운영 개요

가) 봇 잡기

사이버클린센터는 이 공조에 참여하는 ISP들의 인터넷 라인과 함정 및 유인의 역할을 하는 컴퓨터(decoy machine)인 Honeypot을 연결해서 봇을 잡는다.

나) 감염된 컴퓨터 사용자의 식별

센터에서는 Honeypot에 잡힌 봇 감염 로그기록 (IP주소, 날짜, 시간)을 ISP에 보내서 해당 IP주소를 사용하고 있는 사용자를 찾아낸다.

다) 감염된 컴퓨터의 사용자에게 경고 메일 보내기

해당 ISP는 봇에 감염되었으니 조심하라는 경고의 메일을 사용자에게 보낸다. 이 메일에는 봇을 치료할 수 있는 웹사이트의 URL이 포함되어 있다. 이 URL에는 ISP로 하여금 사용자의 치료 과정을 모니터링을 가능하게 하는 사용자 식별 문자 (tracking ID)도 포함되어 있다.

라) 봇을 치료하는 웹사이트에 접속

봇에 감염되었다는 메일을 받은 사용자는 통보받은 URL에 가서 봇의 위험에 대한 안내를 받고 봇을 치료하는 툴을 다운로드 받는다.

마) 봇 치료 도구의 다운로드와 봇 바이러스의 치료

감염된 컴퓨터의 사용자가 무료로 봇 치료 도구를 다운로드 받아 바이러스를 치료하고 나면 사용자는 Windows 업데이트를 실행하고 백신프로그램을 설치한 후 이러한 사실을 웹사이트를 통해 알린다. 이런 전 과정을 거쳐서 센터에서는 사용자의 컴퓨터 치료과정이 완료되었다는 사실을 확인한다.

3) 사이버클린센터의 운영

사이버클린센터는 법적근거는 없으나 "BOT 대책 추진 프로젝트"를 통해 운영하고 있다. 사이버클린센터는 2005년 4월 25일, 내각관방에 정보보호센터(National

Information Security Center) 설치하여 동년 5월 30일, 내각 관방 IT전략본부에 「정보보호정책회의」를 설치하여 매년 기본계획을 수립·실시하고 있다. 이에 따라 2006년도에서 2008년도까지 제1차 정보보호 기본전략을 실시한 이후 2009년 제2차 정보보호 기본전략에 따라 BOT정책을 수립하여 추진 중이다.

현재, 사이버클린센터는 Telecom-ISAC-Japan의 15명, JPCERT-CC의 5명, 정보처리추진기구(IPA)의 5명, 총 23명이 전담하고 있으며 모두 엔지니어로 구성되어 있다. 다만, 매월 1회 사이버클린센터 운영위원회(CCC-SC)를 운영하면서 총무성, 경제산업성 공무원이 참석하는 6명의 운영위원회가 개최되어 법제도적 운영방안을 결정하고 있다.

제4절 독일과 EU에서의 정보통신망 자율규제 현황

1. 자율규제기관에 의한 정보보안 정책

가. EU의 인터넷상의 자율규제기관

EU는 각국이 자율규제에 적극적으로 참여할 수 있도록 핫라인 구축 및 예산지원 등의 규제시스템을 지원하고 있다. EU의 자율규제기관으로서는 INHOPE(Internet Hotline Providers in Europe)과 PEG(Pan European Game Information)를 들 수 있다.

INHOPE는 '좀 더 안전한 인터넷환경을 위한 실행계획(Safer Internet Action Plan)'에 설립·실행근거를 두고 있으며, EU의 재정지원을 받고 있는데 주요 임무는 다음과 같다.

· 각국의 인터넷 핫라인 링크를 제공(1999)

· 인터넷상 아동포르노물을 제거하며 불법정보 유해물의 유통 저지

PEGI는 인터렉티브소프트웨어연맹(ISFE) 행동강령에 심의근거를 두고 있으며, 자문위원[84]의 대부분이 정부 측 인사이다. 따라서 이를 이유로 PEGI를 완전한 자

84) 그러나 자문위는 정부와 PEGI의 의사소통경로 역할을 할 뿐 심의기준과 절차에는 관여하지 않

율규제기관으로 보기 어렵다는 주장도 있다.

PEGI의 주요 임무는 기존의 개별 국가연령등급시스템을 대체하여 게임등급심의를 하는 것이다.

나. 독일의 멀티미디어자율규제협회(FSM)

인터넷과 관련하여 2005년 10월에 '방송과 텔레미디어에 있어서 인간의 존엄의 보호 및 청소년의 보호에 관한 주제협정' 제19조에 근거해서 독일의 멀티미디어자율규제협회(FSM)가 '청소년미디어보호위원회(KJM)'으로부터 인터넷자율규제기관으로서 승인을 받았다.[85]

'방송과 텔레미디어에 있어서 인간의 존엄의 보호 및 청소년의 보호에 관한 주제협정'의 주요 내용은 청소년에 유해한 콘텐츠로부터 청소년을 보호하기 위하여 제정한 규율인데 이는 방송과 인터넷에 공통하여 규제하는데 규제기관으로는 청소년미디어보호위원회(KJM)가 관할하고 있다.

승인을 받은 멀티미디어자율규제협회(FSM) 가맹 사업자는 청소년미디어보호위원회(KJM)로부터 직접적으로 규제를 적용받지 않게 된다. 단, 문제가 있는 경우 청소년미디어보호위원회(KJM)는 멀티미디어자율규제협회(FSM)를 지도할 수 있다.

독일의 FSM은 기업이 자율규제기구에 가입하여 활동하는 경우 청소년미디어보호국가협정에 따라 청소년미디어보호관리자 배치의무를 면제하고 있다.

2. 독일의 온라인상 자율규제 실태

독일에서 온라인상 자율규제는 주로 청소년보호와 관련하여 이루어지고 있다. 청소년보호와 관련한 주요 법률은 「청소년보호법(Jugendschutzgesetz, JuSchG)」, 청소년미디어보호에 관한 주간협약(JMStV), 그리고 형법이다. 「청소년보호법」은 주로 기록매체(Trägermedien), 즉 도서, 잡지, 사진, 비디오카세트, 음반, DVD 등

는다.

85) 이를 일종의 규제된 자율규제기관이라 부른다.

을 규제대상으로 하고 있고, 이에 반하여 청소년미디어보호에 관한 주간협약은 방송과 텔레미디어(인터넷)를 대상으로 한다.

주간협약의 등장배경은 독일에서 원래 방송매체는 주관할이고, 전신적 성격이 강한 전자통신매체는 연방의 관할인 점에 기인하다. 그러나 인터넷과 같은 새로운 매체가 발생하여 이를 규율하기 위하여 연방과 주정부가 모여서 내용이 동일한 법률을 만들게 되었다. 연방에서는 1997년 「정보통신서비스법(IuKDG, Informationss- und Kommunikationsdienste-Gesetz, 정식명칭은 정보통신서비스의 기본조건을 규율하기 위한 법률)」이 제정되고, 각 주 차원에서는 미디어서비스에 관한 주간협약(Mediendienste-StV)이 각각 제정되었다. 청소년미디어보호에 관한 주간협약도 이러한 맥락을 같이 한다.

연방의 「정보통신서비스법」은 11개의 법률이 개별 절로 구성된 항목법률이다. 동 법률 제1절에 「텔레서비스법(TDG)」이 제정되어 규정되어 있었는데, 이 법률은 2007년 2월 현재의 「텔레미디어법(TMG)」으로 변경되었다. 이 법률이 연방차원에서 인터넷을 규제하기 위한 법률이다. 중요한 규정이 바로 서비스제공자의 책임에 관한 것이다.

독일의 '청소년미디어 보호법에 관한 주간협약(JMStV)'에 의하면 온라인상에서 자율규제기관을 둘 수 있다(동 협약 제19조 1항). 이러한 자율규제기간을 승인하는 기관은 청소년미디보호위원회(KJM)이다(동 협약 제14조).

동 주간협약(JMStV)은 방송과 인터넷서비스 제공자의 독자적인 책임을 강화하고 사전통제의 가능성을 원활히 하기 위하여 "규제되는 자율규제의 원칙"(Prinzip der regulierten Selbstregulierung)을 따르고 있다. 자율규제기관에게 미디어감독에만 제한하여 심사할 수 있도록 법률상 규정된 결정의 틀이 승인되어 있다. 자율규제기관은 청소년미디어보호위원회로부터 승인을 받아야 한다.

3. 규제되는 자율규제 시스템

2003년 이후 청소년미디보호를 위해서 텔레미디어 분야에서 적용되기 시작한 규제된 자율규제는 청소년미디어보호를 위한 원칙에 국가와 기업체의 협력이 예정

되어 있다. 이 말은 국가는 법률상의 틀과 이에 상응한 구조를 만들고, 이 틀의 내용은 서비스제공자의 책임으로 채워질 수 있도록 위임한다는 것이다.

특히 내용의 국제성과 신속성으로 표현되는 인터넷 분야에서 서비스제공자를 통한 자율규제시스템은 아주 중요한다. 자율규제는 비용이 많이 드는 입법 활동에 대한 법률적 해결인 국가의 규제에서보다는 훨씬 융통성이 있고 보다 신속하게 변화에 대응할 수 있다. 공동체(사회)의 도덕과 가치관의 변화뿐만 아니라 새로운 기술의 발전에 적응하기 위해서 항상 필요한 대응도 할 수 있다.

국가기관의 기준보다는 기업들의 기술적 기준이 훨씬 낫기 때문에, 신속한 대처가 가능하다. 미디어 발전의 역동성을 통해서 이러한 측면은 항상 많은 의미를 가진다. 국가의 규제에 대한 자율규제가 가지는 더욱 중요한 장점은 국제적인 네트워크화에 있다. 특히 인터넷과 같은 국제적인 미디어는 이의제기기관의 초국가적인 상호협력을 통하여 형식적이고 느린 공적인 협력의 과정보다는 훨씬 신속하게 법익침해에 대응할 수 있다. 뿐만 아니라 자율규제는 국가의 부담을 상당히 덜어주게 된다.[86]

자율규제기관의 승인요건은 아래의 동 주간협약 제19조 3항에 규정되어 있다.

4. '청소년미디어 보호법에 관한 주간협약(JMStV)' 제19조 자율규제기관

제1항 방송과 텔레미디어를 위해서 자율규제기관을 둘 수 있다.

제2항 규약에 따른 업무의 범위 내에서 해당 제공자가 동 주간협약 및 이에 근거한 규약 및 지침의 준수여부를 심사한다.

제3항 다음의 요건에 해당하는 경우에는 동 주간협약에서 의미하는 자율규제기관으로써 인정될 수 있다.

1. 자율규제기관이 선정한 심사위원의 독립성과 전문성이 보장되고 이 경우 특히 청소년문제를 다루는 사회단체의 대표자가 고려되고 있고,

86) 관련자료 : http://www.fsm.de/de/Regulierte_Selbstregulierung
http://web1.blm.de/apps/documentbase/data/pdf1/regulierte_selbstregulierung.pdf

2. 다수의 서비스제공자로부터 적정한 설비가 갖추어져 있고,
3. 심의실무에서 아동과 청소년의 효율적인 보호를 보장하는데 적합한 규정들이 심사위원의 결정을 위해서 존재하고,
4. 심사의 범위, 사업자에게는 제출의무 및 가능한 제재를 규정한 절차규정이 존재하고 주 법률에 규정된 청소년보호 담당자의 신청에 의해 결정을 심사할 가능성이 규정되어 있고,
5. 해당 서비스제공자는 결정에 앞서서 그 결정에는 서면으로 그 근거가 제시되고 참여자에게 통지되는 사실이 알려짐이 보장되어 있고,
6. 이의제기수단이 보장되어 있는 경우.

제4항 관할 주미디어기관은 KJM을 통하여 결정한다. 당해 자율기관이 그의 소재지를 가지는 주의 주미디어기관이 관할권을 가진다. 이에 따라 관할이 없는 경우에는 승인신청이 있었던 주미디어기관이 관할을 가진다. 자율기관은 승인조건을 심사를 위해서 필요한 서류를 KJM에게 제출한다. 승인은 4년의 기간이 정해져 있다. 연장이 가능하다.

제5항 승인의 조건이 사후에 탈락하거나 자유기관의 심의관행이 현행 「청소년보호법」과 일치하지 아니하는 경우에는 승인이 취소될 수 있다. 승인의 취소를 통한 재산 손해에 대한 보상은 보장되지 않는다.

제6항 승인된 자율규제기관은 동 주간계약의 적용에 대해서 동의를 해야 한다.

이러한 요건을 갖추어 승인을 받은 자율규제기간은 규약에 따른 업무의 범위 내에서 해당 제공자가 동 주간협약 및 이에 근거한 규약 및 지침의 준수여부를 심사한다.

이러한 규제된 자율규제의 원칙에 따라 KJM에 의해서 승인된 현재 대표적인 자율규제기관은 멀티디미어 서비스 제공자의 자율규제기관(Freiwillige Selbstkontrolle Multimedia-Dinesteanbieter, FSM)이다. 이 기관은 2004년 11월

23일 청소년미디어보호위원회(KJM)로부터 동 주간협약(JMStV)의 자율규제기관으로 승인을 받았다. 이 자율규제기관은 1997년 미디어단체와 온라인 기업에 의해서 사단법인으로 설립되었다.

이 기관과 관련한 중요 사항들을 규정한 것으로는 정관[87], 행동강령[88], 이의제기 규정[89] 등이 있다.

FSM의 정관 제5조에 따른 정회원은 AMANGO pure Entertainment GmbH, AOL Deutschland GmbH & Co. KG, CYBITS GmbH, Deutsche Telekom AG, Inter Publish GmbH, t-info GmbH, die T-Online International AG 등 이다.

5. 멀티미디어 서비스 제공자의 자율규제기관[90]

가. 멀티미디어 서비스 제공자의 자율규제기관이란?

멀티미디어 서비스 제공자의 자율규제 기관(FSM)은 청소년미디어보호에 관한 주간협약(JMStV) 이후 텔레미디어(온라인 내용) 분야에서 유일하게 승인된 자율규제기관이다. 이 기관의 목적은 온라인 미디어에서 청소년미디어보호의 강화, 불법적이고 청소년 유해적인 온라인 내용의 척결, 청소년보호 기술적 조치의 장려 그리고 특히 아동과 청소년들을 위한 미디어 전문지식의 전달 등이다(정관 제2조 참조). 현재 이 기관에는 통신, 방송, 온라인 분야에서 망라된 44개의 기업과 단체들이 등록되어 있다.[91]

나. 멀티미디어 자율규제기관의 업무 개관

멀티디미어 자율규제기관의 사무소는 베를린에 그 소재지를 두고 있다(정관 제1

87) http://www.fsm.de/de/Satzung
88) http://www.fsm.de/de/Verhaltenskodex
89) http://www.fsm.de/de/Beschwerdeordnung
90) 아래 내용은 FSM 홈페이지 내에 있는 2008년 연도 보고서를 토대로 설명한 것이다.
http://www.fsm.de/de/Jahresberichte
91) Jahresberichte 2008, S. 4

조 2항). 사무소장 Sabine Frank 외에 12명의 직원이 상임직으로 활동하고 있으며 이 기관의 다양한 업무영역을 담당하고 있다. 이 기관은 자율규제 승인기관으로서의 업무와 청소년미디어보호의 문제에 있어서 회원들에게 포괄적으로 책임을 지고 조언하는 업무에 해당하는 모든 일을 담당하고 있다.

지난 11년 동안 FSM은 인터넷상에서의 청소년미디어보호 문제에 관해서 정치적 사회적 담당자로서 확고한 위치를 지켜왔다. 특히 사무소는 지속적으로 입장표명을 통해서 정치적 의사형성의 과정에서 그의 전문적 지식을 제시해 왔다.

사무소의 핵심적인 업무(구체적인 업무에 대해서는 정관 제2조 2항 참조)는 적극적으로 회원들을 책임지고 돌보는 것(Betreuung)이다. 즉 회원들에게 최근의 법률적 기술적 발전에 관한 정보를 제공하고 구체적인 질문에 자문을 하는 것이다. 이 외에 FSM은 기업이 원하는 경우에는 법률상 규정된 범위 내에서 청소년보호담당관을 대리한다. 청소년미디어보호에 관한 주간협약(JMStV) 제7조에 의하면 상업적 온라인 제공자는 청소년보호담당관을 두도록 되어 있다. 기업이 FSM에 이를 위임하게 되면 기업은 이러한 의무로부터 벗어난다. 이러한 자율규제기관에의 위임은 기업이 독자적으로 청소년보호담당관을 갖출만한 규모가 되지 않는 경우 중요한 의미를 가진다.

또한 FSM은 지속적으로 회원의 온라인 제공물을 심사하여, 청소년유해적인 내용이 인터넷상에서 호출되지 않도록 확보한다. 이리하여 모든 회원들은 기업에 제기되어 있는 법률적, 미디어학적 또는 기술적 문제가 평가되는 감정위원회(die Gutachterkommission)에 호출될 가능성이 있다.

「청소년보호법」상의 문제제기에 있어서 전 분야의 통일적인 기준을 정하기 위해서 FSM은 또한 회원들과 함께 각 주제 분야별로 자유로운 행동강령을 제정한다. 이것은 기업에게 각 분야 내에서의 비교가능성을 제공하고 온라인 미디어에서 청소년보호를 강화하기 위한 본질적인 요소이다. 이 조치는 매번 법률상의 조치를 통해서 하는 것보다는 훨씬 적시에 전환될 수 있기 때문이다.

FSM의 업무에서 두 번째 중요한 것은 FSM의 이의제기부서이다. 모든 인터넷 사용자는 청소년미디어보호의 영역에서 가벌적이고 청소년에게 유해하고 청소년의 성장을 저해하는 온라인 내용에 대해서 이의를 제기하고 이에 상응하는 심사

를 하도록 하기 위해서 이 부서를 무료로 이용할 수 있다.

세 번째 핵심 분야는 포괄적인 이용자 계몽과 아동의 미디어능력을 촉진하는데 있다. 이와 관련하여 FSM은 다양한 프로젝트와 관련한 활동을 하고 있다. 이 프로젝트는 아동이 의식적으로 인터넷 및 핸디에 친숙해지도록 하고 기회와 위험에 대해서 정보를 알려주는 것이다.

마지막으로 FSM은 텔레미디어 분야에서 효율적인 청소년보호에 있어서 최근 발전에 관한 토론회나 전문가강연회와 같은 정기적인 행사를 회원 기업들, 전문가 대중, 정치계의 대표자들 위해서 실시한다.[92]

다. FSM의 구체적인 업무

1) 회원의 관리(Mitgliederbetreuung)

가) 회원을 위한 청소년보호담당관(업무)의 대리

청소년미디어보호 주간협약 제7조에 의하면 청소년유해적인 내용을 포함하고 있는 공공 텔레미디어를 상업적으로 제공하는 서비스 제공자는 청소년보호담당관을 임명해야 한다. 하지만50인 이하의 직원 또는 한 달 평균 천만번 이하의 접속수를 가지는 텔레미디어 제공자는 그가 FSM과 같은 자율규제기관에 가입해 있고 이 기관이 이러한 업무의 수용에 의무를 지는 경우에는, 청소년보호담당관을 지명하지 않을 수 있다. FSM을 통한 업무의 인수는 특히 그들이 제공하는 온라인 내용물에 대해서 청소년보호담당관을 임명할 재정적 능력이 없는 중소규모 기업에게는 매력적이다. 2008년에는 FSM은 11개 회원으로부터 이러한 서비스를 위임받았다. 그러나 2008년 회원회의에서는 FSM을 통한 청소년보호담당관의 대체의 가능성을 다음의 경우에는 제한하기로 결정했다. 그것은 청소년보호담당관의 업무의 인수가 구체적인 제공물을 위해서 특별히 높은 심사비용과 자문비용이 예상되는 경우이다. 특별히 높은 심사 및 자문비용은 일반적으로 제공물이 본질적으로 이용

92) Jahresberichte 2008, S. 5

자에 의해서 생성되는 내용이거나 아니면 내용이 특별히 광범위한 경우이다.

나) 감정(평가)위원회(정관 제13조)

감정위원회는 FSM회원으로부터 법률적, 미디어학적 그리고 기술적 문제를 위해서 소집될 수 있다. 감정은 감정위원회의 3인의 위원, 소위 감정소위원회(Gutachterausschuss)를 통해서 이루어진다. 감정위원의 선정에 있어서 학제성과 특히 기술적 전문성이 각각 고려된다. 감정위원회는 2008년 자주 소환되었다. 10번의 소위원회가 활동하였는데, 이것은 2007년의 3번의 소위원회의 개최와 비교된다. 감정의 중점은 청소년미디어보호 주간 협약 제4조 2항 2문(폐쇄이용자 그룹)의 나이검증시스템의 조화가능성의 문제에 있었다. 다른 주제는 일반약관의 청소년보호와의 합치성의 심사 및 청소년보호의 관점에서 외설적 단어나 문장 및 그래픽(Teletext)의 감정이다.[93]

2) 다양한 분야에서 청소년미디보호의 강화를 위한 기업의 자율 조치

가) 검색엔진제공자의 자율규제

검색엔진제공자의 자율규제는 2005년 2월 AOL Deutschland, Deutsche Telekom AG, Google Germany, Lycos Europe, MSN Deutschland, t-info, Yahoo Deutschland 등 기업에 의해서 FSM에 만들어졌다. 2007년에는Ask.com 기업이 FSM의 검색엔진제공자의 자율규제로 추가되었다. 검색엔진 제공자의 자율규제의 기초는 검색엔진 행동강령이다. 이 행동강령에는 기업들이 특정한 조치의 전환 이외에 특히 이용자들에게 높은 투명성을 보장하기 위해서 검색엔진의 기능에 대해서 아주 강력한 정보를 제공할 의무를 부여하도록 되어 있다. 기본적인 목적은 인터넷에서 소비자 및 아동과 청소년의 보호를 개선하는 데 있다. 이러한 시도는 전세계적으로 처음 있는 일이다. 왜냐하면 이것은 가장 중요하게 시장을 결정하는

93) Jahresberichte 2008, S. 5

기업들이 함께 발견한 기준이고 통일적이고 서비스 제공자를 초월하는 기준에 대해서 자유로운 참여와 관련하여 일치를 보았기 때문이다.[94]

나) BPJM 모듈의 전환

검색엔진제공자를 위한 FSM 행동강령의 핵심은 소위 BPJM 모듈(BPJM-Modul)의 이행이다. 검색엔진 제공자들은 특히 검색결과에서 청소년유해미디어 연방심사청(BPjM)에 의해서 법률상 규정된 절차에서 지정되어 있는 인터넷 내용물이 나타나지 않도록 할 의무가 있다. BPjM과의 이러한 협력은 청소년미디어보호에 있어서 검색엔진의 자율규제의 중심점이다. FSM에 가입한 제공자는 BPjM 모듈을 설치한다. 이 모듈에는 자동처리를 위해서 데이터 목록이 포함되어 있는데, 여기에는 완전히 표시된 도메인 외에 표시된 서브도메인, 하위표시 또는 개별 데이터를 나타낼 수 있다. 이것은 BPjM에 의해서 암호화되어 서버에 설치되어 있다. 이로부터 각각 최근 표시된 데이터는 검증 후에 이행에 자격이 있는 검색엔진제공자를 통해서만 검색서비스에서 호출될 수 있다.[95]

3) 채팅제공자의 자율규제

2008년에는 4개의 채팅제공자, 즉 Knuddels, LYCOS Europe, RTL interactive, Super RTL - den Verhaltenskodex Chat 기업이 채팅 행동강령을 수용했다. 이것은 자유로이 접근이 가능한 채팅 제공물로부터 아동을 이전보다 더욱 강력하게 보호하고 계몽하도록 하고 있다. 기업은 기술적 정보적 조치를 전환해야 할 의무가 있다.

라. 최신 텔레미디어 영역의 발전에 적극적 참여

최신 텔레미디어 영역의 발전에 적극적인 공동 작업을 위한 새로운 작업그룹이

94) Jahresberichte 2008, S. 6
95) Jahresberichte 2008, S. 6-7

FSM 내에 만들어졌다. 그것은 텔레텍스트(AG TELETEXT), 접근(AG ACCESS), 청소년보호와 웹 2.0에서 데이터 보호(AG JUGENDSCHUTZ UND DATEN-SCHUTZ IM WEB 2.0), 청소년보호프로그램 작업그룹(AG JUGENDSCHUTZPROGRAMME) 등 이다.

마. 불법 온라인 내용의 척결

1) 이의제기절차 과정[96]

FSM은 청소년유해내용에 관해서 무료로 이의제기를 할 수 있도록 모든 시민이 문서로 제출할 수 있는 이의제기부서를 운영하고 있다. 이것은 www.fsm.de에서 접근할 수 있는 이의제기양식에 아주 간단하게 할 수 있다. 이의제기부서에 제공한 정보는 비밀로 유지된다. 이의제기자가 이메일 주소를 입력해야 한다. 하지만 그가 이 정보를 제공받기 위해서 그리고 이의제기절차의 과정을 보고받을 수 있기 위해서 이의제기자의 개인정보는 어떠한 시점에도 관청이나 제삼자에게 전달되지 않는다.

FSM의 이의제기규정에는 익명의 이의제기는 일반적으로 처리되지 않는다고 규정하고 있다. 하지만 아동포르노 내용에 관한 이의제기는 예외로써 처리된다. 이의제기가 접수된 후 이의제기부서의 직원은 사전심사를 하게 되는데, 거기서 사실관계가 조사되고 내용물이 법적으로 평가된다. 이의제기가 명백하게 근거를 갖추고 FSM의 회원에 대한 이의제기가 아닌 경우에는 익명으로 직접 관할 관청에 이송할 수 있다.

FSM의 회원에 대해서 제기된 이의제기가 명백하게 근거를 갖춘 경우에 대해서는, 회원기업이 이의제기에 대해서 이미 사전에 스스로 시정하지 아니한 경우에 한해서 이의제기위원회가 결정한다. 회원기업의 자력구제 사례인 경우에는, 이의제기가 청소년보호 위원회를 통해서 또는 주 법률에 규정된 청소년보호 담당자를 통해서 FSM에 의뢰된 경우에는, 이의제기위원회는 동일하게 결정한다. 이의가 제

96) 정관 제12조, 이의제기규정 : http://www.fsm.de/de/Beschwerdeordnung

기된 제공물이 독일 「청소년미디어 보호법」의 규정에 위반하여 그 이의제기가 근거를 가진다고 이의제기위원회가 결론을 내린 경우에는, 단계화된 징계(시정조치, 징계, 벌금 또는 제명 등)의 가능성에 대한 수단을 사용할 수 있다.

이의제기가 사람의 생명과 신체가 위험에 빠져 있다는 구체적인 추론이 가능한 경우에는, FSM은 관할 관청에 이의제기의 내용을 송부한다. FSM이 이의제기를 통해서 아동포르노 내용의 링크를 확보한 경우에는 이것을 간단한 사전심사 후 직접 연방범죄수사청의 담당자에게 송부한다. 이것은 2007년 이후 상호협력에 관한 협약에 따른 것이다. 또한 국제적인 네트워크 INHOPE와 관련한 것인 경우에는 관할 담당 이의제기부서에 송부한다.

2000년과 2008년 사이에 FSM이의제기부서는 13.000 건의 이의제기를 처리했다. 인터넷상에서 불법적이고 청소년의 성장을 침해하는 내용을 억제하기 위한 중요한 공헌을 수행했다.[97]

2) 2008년도 이의제기 개관

2008년도에는 FSM의 이의제기부서는 전체 1.835건의 이의제기를 처리했다. 이는 전년도와 비교하여 24%의 증가를 의미한다(2007년: 1.479 건, 2006년: 1.585 건). FSM의 회원에 대해서는 단지 3건에 불과하다(2007: 8%, 2006년: 12%).

이의제기의 약 3분의 1(37%)은 독일에서 제공하는 내용물이고; 약 5분의 1(19%)은 미국에서 운영되는 웹사이트였다. 대부분의 의의제기는 아동포르노 내용이다(26%; 2007년: 23%, 2006년도 20%). 극우적인 내용에 대한 이의제기(9%; 2007년: 17%, 2006 : 12%)는 전년도보다 확실히 줄어들었다.

이의제기 상대방은 직접 FSM의 이의제기부서를 통한 내용의 이의제기나 이의제기위원회를 통한 결정에 의해서 직접 시정한 것은 전년도보다 두 배 이상 많았다(23%; 2007년 : 12%, 2006: 10%).

이의제기부서를 통한 항의는 항상 상세하게 근거가 있고 구체적으로 법적인 토대가 설명되고 있음으로 FSM은 청소년미디어보호의 문제에서 제공자에게 해명을

97) Jahresberichte 2008, S. 9-10

위해서 이러한 방법으로도 기여한다.[98]

3) 이의제기 위원회의 결정

FSM 이의제기위원회의 6개 심의위원회는 2008년도에 전체 7개의 웹사이트를 심의했다. 그 중 한 절차는 회원 기업의 제공물이었다. 이의제기 위원회로부터 심사되고 결정되었던 그 밖의 텔레미디어는 이전에 거의 100명의 다양한 사람들에게 전달되었다. 항의가 제기된 웹사이트에는 제공자는 텍스트나 화상으로 개와 개의 행동에 대해서 비판을 제기했다.[99]

98) Jahresberichte 2008, S. 10-11
99) Jahresberichte 2008, S. 11

<인터넷 온라인 수색에 관한 판결>

전자적으로 유통되어 축적되는 정보의 증대에 따라 인터넷으로 연결된 컴퓨터의 하드디스크 안을 수색하는 「온라인 수색」은 경찰이나 정보기관에 있어 매력적인 수사 수단이 된다. 이 수법에서는 정보를 훔치기 위해서 개발된 특별한 스파이웨어를 인터넷을 통해서 특정의 컴퓨터에 보내어 하드디스크에 축적된 정보나 인터넷의 이용, 전자 메일의 송신 등의 데이터를 은밀하게 찾기 시작한다.

연방 내무장관은 테러 대책으로서 온라인 수색의 수법을 사용하는 전략을 2006년에 밝혔다. 또, 동년 12월에는 노르트라인·베스트파렌주가 주 레벨에서는 최초로 주의 헌법 옹호 기관에 대해 온라인 수색을 실시하는 권한을 주는 「헌법옹호법」 개정을 실시했다.

<온라인 수색에 관한 판결의 내용 및 평가>

2008년 2월 27일 연방헌법재판소는 노르트라인·베스트파렌주 헌법옹호법 중의 온라인 수색에 관한 규정에 대해 위헌 무효로 하는 판결을 내렸다. 「남독일 신문」(2008년 2월 28일)은 이 판결을 「역사적 판결」이라고 평가하고 있다.

연방헌법재판소는 정보기술 시스템(=컴퓨터)의 이용이 시민의 인격의 발전에 있어 중심적인 의미를 가지게 된 현대 사회에서 이러한 시스템의 이용을 감시하고 축적된 미디어에 존재하는 데이터를 이용하는 것은 프로파일의 작성으로 연결될 수 있으므로 이용자의 인격을 광범위하게 추측하는 것을 가능하게 하기 때문에 기본권에 관계되어 상당한 보호의 필요성이 생긴다는 인식을 나타냈다.

게다가 종래의 '전기 통신의 비밀'(기본법 제10조) 및 '주거의 불가침'(기본법 제13조)의 보장 및 연방헌법재판소의 판례에서 생성된 일반적 인격권의 형태(개인적 영역의 보호의 보장, 정보의 자기결정권의 보장 등)에서는 이 필요성에 충분히 응할 수 없다고 하여 새롭게 일반적 인격권의 특별한 형태로서 「정보기술 시스템의 기밀성과 불가침성의 보장에 대한 기본권」이라고 하는 개념을 창출했다.

연방헌법재판소는 이 「정보기술 시스템의 기밀성과 불가침성의 보장에 대한 기

본권」에 대한 침해는 예방적 목적을 위해서든 형사 소추의 목적을 위해서든 정당화되지 못하며, 헌법에 합치한 법률상의 근거에 기초를 두지 아니면 안된다고 하면서 그 기준을 나타냈다.

즉, 전통적인 정보원을 양과 다양성에서 압도적으로 웃도는 데이터저장고에의 액세스를 가능으로 하는 온라인 수색에 의한 기본권 침해의 크기를 고려하면, 헌법상 용서되는 것은 각별하게 중요한 법익(사람의 신체·생명·자유, 위협받으면 국가의 존립의 기초나 인간의 생존의 기초와 관계되는 공공의 재산)에 대한 구체적인 위험의 실제의 근거가 존재하는 경우에 한정된다. 게다가 비밀의 접근 권한을 주는 경우에는 대상자의 이익을 헌법상 보장하기 위해서 적당한 법률상의 예방조치를 취하지 않으면 안 되고 원칙적으로 재판소의 명령을 얻지 않으면 안 된다.

<연방 정부의 대응>

연방 내무장관은 연방제 개혁에 의한 연방 형사청의 임무의 확대에 수반해 「연방 형사청법」의 개정이 필요했기 때문에 그 때에, 동 법 중에 제20-k조로서 연방 형사청에 온라인 수색을 인정하는 규정을 신설하는 것을 제안하고 있었다. 그러나 연방 내무장관과 인권을 중시하는 연방 법무장관(사회민주당)의 사이에 합의가 성립하지 않고 법안은 좀처럼 결정되지 않았다.

이번에 연방 헌법재판소의 판결에서 법 정비의 기준이 나타남으로써 「연방 형사청법」의 개정 문제는 겨우 움직이기 시작했다. 연립 여당의 내무 정책 담당자는 2개월 이내에 법안의 기초 작업을 끝내 여름 휴회까지 개정법을 성립시킬 의향을 나타내고 있다.

사회민주당 의원단의 내무 정책 대변인은 '정보기술 시스템의 기밀성과 불가침성의 보장에 대한 기본권'을 기본법으로 규정하는 일도 제안하고 있다.

제3장 정보통신망에서의 정부규제의 한계

제1절 우리나라의 정보통신망 정부규제 현황

1. 정보통신망에의 정부의 개입

가. 정보통신망에의 정부규제의 요인

1) 사이버위협

컴퓨터와 인터넷 이용자가 증가함에 따라 편리한 사용을 위해 시스템, 서비스 및 소프트웨어 등이 지속적으로 개발되고 있다. 반면에 이러한 시스템 및 소프트웨어가 내포하고 있는 보안상의 취약성 또한 증가하고 있다. 악의적 목적을 가진 사용자는 이러한 취약성을 이용하여 해당 시스템을 해킹하고 바이러스 등 악성코드를 유포를 유포하여 자신의 목적을 달성하려고 한다.

사이버위협은 다양한 형태로 존재하는데 크게 해킹 및 인터넷침해, 악성 소프트웨어, 이메일을 통한 위협 등으로 구분하여 볼 수 있다. 다만, 최근에는 시스템의 융·복합화 추세에 따라 해킹의 파괴성과 바이러스 전염성이 결합된 신종 사이버테러가 발생하고 있고, 바이러스와 웜이 결합된 악성코드와 DDoS공격도 일반화되고 있어 이러한 사이버테러 유형의 구분은 점차 모호해지고 있다.

해킹은 넓은 의미에서는 해커들이 저지르는 모든 불법적인 행위를 말하며, 좁은 의미에서는 정보시스템의 취약성이나 설정의 오류를 이용하여 보안 침해사고를 유발시키는 행위를 말한다. 해킹의 대표적인 기법으로는 사용자 도용(impersonation)이 있다. 공격자는 컴퓨터에 사용자가 입력하는 내용을 기록하도록 프로그램을 설치하고 이러한 사실을 모르는 일반 사용자들이 ID와 패스워드를 입력하면 이를 도용당하게 된다.

서비스거부공격(DOS: Denial of Service)은 한 사용자가 시스템의 자원을 모두

독점하여 그 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하는 것을 말한다. 이 기법을 확장한 분산서비스거부공격(DDoS: Distribute Denial of Service)은 하나의 컴퓨터가 아닌 다수의 컴퓨터가 공격을 담당한다는 점에서 DoS 공격보다 훨씬 더 강력한 파괴력을 가지고 있다. 2000년 2월 아마존, 이베이, 야후 등 전자상거래관련 사이트들이 DDoS 공격을 받아 운영이 불가능해진 사건이 발생하면서 일반에 널리 알려지기 시작하였으며, 최근 우리나라에서도 지난 7월. 7일, DDoS 공격으로 국가 주요 사이트가 장시간 접속이 불가능한 사건이 일어났다.

2) 정보보호 수요의 증가

해킹공격의 기술과 유형이 보편화됨과 동시에 다양화 되면서 해킹사고는 전 세계적으로 급증하고 있다. 특히, 우리나라의 경우 90년대 중반 이후 정보화가 급속히 진전되었고, 이로 말미암아 주요기반시설의 정보통신시스템이 상호 연계됨으로써 특정 정보시스템에 대한 사이버공격이 다른 정보시스템에도 영향을 미치게 되었으며, 이처럼 고도화된 정보인프라는 자연히 국제해커들의 공격목표가 되고 있어 사이버공격을 통해 금융 및 통신서비스의 장애, 전기 공급 중단, 항공관제시스템의 마비, 주요 행정DB의 파괴 등의 사고가 발생할 경우 그로 인한 피해는 이루 말할 수 없을 정도로 크게 될 상황이다. 특히 최근의 사이버공격은 해킹과 바이러스가 결합된 형태의 고도의 공격기법을 구사하여 전 세계의 네트워크를 위협하고 있다.[100]

최근의 사이버공격은 개별 시스템에 대한 공격에서 네트워크에 대한 공격으로 변화하고 있다. 개인·기업·정부의 시스템이 네트워크로 상호 연계됨에 따라서 사이버공격으로 하나의 시스템이 감염되었을 경우 피해가 연쇄적으로 확산된다. 최근 일어난 DDoS공격의 사례를 보아도 알 수 있다. 이러한 사이버위협의 속도가 급속도로 가속화되고 있다. 사이버공격 속도가 증가하는 이유로는 첫째, TCP/IP 네트워크 구조와 MS 윈도우 운영체제로 대표되는 획일화된 인터넷환경, 둘째, 초

100) 이종화, 전게논문, 21면.

고속 정보통신 인프라의 고도화로 네트워크와 서버의 성능이 향상되어 이에 따른 웜·바이러스 전파속도의 가속화, 셋째, 사이버공격의 자동화로 피해자가 또 다른 가해자가 되어 본인도 모르는 사이에 다른 시스템을 공격함으로써 기하급수적으로 피해 시스템이 증가한다는 것 등을 들 수 있다.[101]

3) 새로운 정보통신환경에서의 사이버위협

최근에는 초고속통신망 및 정보시스템의 활용이 확산되면서, 물류, 발전, 에너지 분야 등 국가 주요기반구조들의 정보시스템 의존도가 높아짐에 따라 인터넷의 재해가 단순한 가상세계의 피해로 한정되는 것이 아니라, 현실 세계로 피해가 파급되어가고 있는 실정이다. 이러한 기반구조들의 연계성으로 하나의 기반구조가 피해를 입었을 경우, 다른 기반구조가 연쇄적으로 피해를 입을 가능성이 증가한다. 네트워크가 융합되는 환경이 도래할 경우 사이버공격에 취약한 무선망, 인터넷망에서 발생된 위협이, 음성통신망, 방송망까지 피해가 확산될 수 있다.

해킹사고의 접수·처리건수에 대한 통계를 살펴보면, 2009년 1월부터 6월까지 9,747건에 이르고 있다.[102] 우리 사회 각 분야가 정보통신기반으로 재편되면서 요구되는 정보보안의 수준도 더욱 강화되고 있다. 정보보안은 우리 사회의 안전과도 직결되는 것이고, 사회기반을 흔들어놓을 수 있는 위협이 되고 있다는 점에서 정보보안의 중요성이 강조되고 이에 대한 국가 및 국민 개개인의 의식 향상 노력이 따라야 할 것이다.

나. 정보통신망 정부규제의 근거

정보통신망은 접근의 용이성과 신속성으로 인해 언제, 어디서나 자유롭게 접속하여 정보를 교환할 수 있다. 게다가 무선네트워크의 보급으로 접근의 용이성은 갈수록 강화되고 있다. 그러나 이러한 특성으로 인해 악의적인 목적으로 접근하는 사람을 원칙적으로 막을 수 없는 한계 또한 나타나고 있다. 신속성은 또한 이런

101) 이종환, 전게논문, 30면.
102) 한국인터넷진흥원, 2009 June 인터넷 침해사고 동향 및 분석 월보

부작용으로서 피해를 입히는데 걸리는 시간을 단축시켜 피해규모 증가에 일조를 하고 있다. 또한 복잡성은 정보통신망에서 문제가 발생 했을 때 이를 해결하는데 어려움을 겪게 한다. 문제발생의 근원지를 쉽게 파악하기 힘든 결과를 낳는다.

이렇게 정보통신망의 특성요인들과 그로 인한 역기능으로 인하여 정보통신에 대한 정부개입의 근거와 더불어서 정보보호라는 측면에서 정부의 개입이 더욱더 강력히 요구되고 있다. 즉 정부에서는 이러한 기반시설의 구축을 위해 노력해야 하지만, 이를 통해 나타나는 각종 사회적인 문제 등을 해결하는 것이 중요한 임무이다.

정보통신망의 정보보호에 있어서 정부개입, 규제의 근거를 살펴보면, 첫째, 정보통신기반에 대한 의존도 증가로 인한 정보보호영역의 확대를 들 수 있다. 정보의 위·변조와 유출이 문제시 되면서 정부는 이를 해결하기 위하여 법제도의 정비나 기술적인 지원 등의 수단을 통해 개입하고 있다.

둘째, 정부의 역할로서 국가사회의 질서유지와 국민의 안전 보호가 있다. 정보통신, 즉 사이버공간에서의 각종 피해로 국민의 재산과 생명에 대한 위협, 사회질서의 혼란, 국가안전의 위협 등의 사이버공간에서의 문제점이 곧 사회의 문제로 이어지기 때문에 이를 보호하기 위하여 정부규제가 이루어지는 것이다.

2. 정보통신망에서의 정부규제의 구체적 현황

가. 정보보호 및 정보보안 관련 법·제도의 연혁

1986년에 제정된 「전산망 보급 확장과 이용촉진에 관한 법률」은 우리나라 최초의 정보화에 관한 법률이다. 이 법은 정보화를 국가가 선도하기 위해 국가기간 전산망을 구축하고 이의 이용을 촉진하기 위한 국가의 시책과 제도를 규정한 법률로서 전산망의 보호를 위한 일부 규정이 있었으나, 현재와 같은 정보보호 및 보안에 관한 중요성을 충분히 반영하지 못한 것이었다. 본격적인 정보보호에 관한 제도라고 볼 수 있는 1995년에 제정된 「정보화촉진 기본법」에서는 정보화의 촉진을 위한 규정과 함께 정보보호에 관한 기본적인 규정도 마련하였다. 또한 1995

년에는 형법이 개정되어 전자기록 위작·변작죄 및 전자기록에 대한 비밀침해죄 등이 규정되었고, 인터넷 보급의 본격화에 의한 인터넷 전자상거래의 이용 증가에 따라 1999년에는 개인 및 기업의 정보유통과 중요정보를 보호하기 위하여 「전자서명법」의 제정을 비롯하여 「전산망 보급 확장과 이용 촉진에 관한 법률」을 「정보통신망 이용촉진 등에 관한 법률」로 전면 개정하는 등 정보화 역기능에 대비한 규정의 재정비작업이 이루어졌다.

본격적으로 정보보호 및 보안에 관한 중요성이 논의되고 관련 제도가 정비되고 강화된 것은 2000년대에 접어들면서부터 이다. 2001년에는 금융·통신·에너지 등 주요 정보통신기반시설을 특별히 보호하기 위하여 「정보통신기반 보호법」을 제정·공포하였고, 「정보통신망 이용촉진 등에 관한 법률」도 명칭을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하고 정보보호 등에 관한 규정을 대폭 보완하였다. 2005년에는 국가안보를 위협하는 해킹·컴퓨터바이러스 등 사이버 공격으로부터 국가정보통신망을 보호하기 위하여 사이버안전에 관한 조직 및 운영에 대한 사항을 체계적으로 정립한 '국가사이버안전관리규정'이 대통령 훈령으로 발령되었다. 지식정보화사회로의 발전에 따라 다양한 정보시스템이 도입·운영되고 있으나 이를 체계적으로 관리할 수 있는 체제가 마련되지 못하여 발생하는 중복투자 및 시스템 간 연계 미흡 등의 문제점을 해소하고 정보시스템을 효율적으로 구성하기 위하여 정보기술 아키텍처의 활용을 촉진하고, 정보시스템 감리제도를 확립하여 공공기관 등에 정보시스템이 효율적으로 도입·운영될 수 있는 기반 구축을 목적으로 하는 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」도 제정되었다. 2006년에는 국가 핵심기술의 수출이 국가안보에 심각한 영향을 줄 수 있는 경우 또는 신고하지 아니하거나 허위로 신고하여 국가 핵심기술을 수출한 경우에는 그 국가 핵심기술의 수출중지·금지·원상복귀 등의 조치를 위할 수 있도록 하는 내용을 담은 「산업기술의 유출방지 및 보호에 관한 법률」이 제정되었다.[103]

현재 국내의 정보보호에 관련한 법으로는 정보보호 추진체계 관련 법령, 국가기밀보호 관련 법령, 중요 정보의 국외유출 방지에 관한 법령, 전자서명 및 인증 관

103) 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009 국가정보보호백서

련 법령, 정보통신망과 정보시스템의 보호추진 관련 법령, 침해행위의 처벌에 관한 법령으로 분류할 수 있다.

정보보호 추진체계는 국가 정보보안 체계, 국가 사이버안전 체계, 정보통신기반 보호체계, 개인정보 보호체계로 나눌 수 있다. 특히, 개인정보보호 체계와 관련한 법령으로 공공부문에서는 「공공기관의 개인정보보호에 관한 법률」, 「전자정부법」 등이 있으며, 민간 부문에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등의 개별법이 있다.

정보통신망과 정보시스템의 보호조치 관련 법령으로 해킹, 바이러스 유포 등 사이버 침해행위로 인하여 국가 및 민간의 정보통신망과 정보시스템에 대한 위협이 증가함에 따라 국가 차원의 체계적인 보호조치가 필요하게 되었다. 정보통신망과 정보시스템의 보호조치와 관련한 법령으로는 「정보화촉진 기본법」, 「정보통신기반 보호법」, 「전자정부법」, 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」, 「전자거래기본법」, 「전자무역 촉진에 관한 법률」, 「산업기술혁신 촉진법」 및 「물류정책기본법」 등이 있다.

나. 집적정보통신시설의 보호

1) 집적정보통신시설의 개요

1998년 초고속인터넷 붐을 타고 생겨나기 시작한 온라인 사업모델과 서비스들이 점차 구체화되고 대형화됨으로써, 기존의 인터넷 전용선을 자체 전산실에 연결하여 서버를 운영하기에는 많은 비용과 인력이 필요하고, 정전, 항온항습, 보안 등 안정성 확보에는 더욱 어려움이 있었다. 이러한 필요에 의해 IDC(Internet Data Center)가 탄생하게 되었으며, 서버, 스위치(Switch), 스토리지(Storage) 등 네트워크 장비를 가지고 인터넷서비스를 주 사업으로 하는 포털, 검색사이트, 게임사이트, 인터넷쇼핑몰 등의 인터넷 기업들이 자사의 전산장비를 자체 전산실이 아닌 IDC에 두고 운영하게 되었다.

2) 집적정보통신시설관련 정부정책

정보통신망법 제46조에서 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하도록 규정하고, 집적된 정보통신시설의 멸실, 훼손 그 밖의 운영 장애로 발생한 피해를 보상하기 위하여 대통령령이 정하는 바에 따라 보험에 가입하도록 규정하고 있다. 또한 정보통신망법 제46조의2에서는 집적정보통신시설 사업자는 집적정보통신시설을 이용하는 자의 정보시스템에서 발생한 이상 현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우나 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우, 그리고 중대한 침해사고가 발생하여 방송통신위원회나 한국인터넷진흥원이 요청하는 경우에는 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있도록 하고 있다.

2001년에는 인터넷데이터센터(IDC)가 갖추어야 할 물리적·기술적·관리적 보호조치를 규정한 '집적정보통신시설 보호지침'이 만들어졌다. 지침의 세부기준으로 물리적·기술적 보호조치와 관리적 보호조치가 마련되었다. 물리적·기술적 보호조치에는 접근제어 및 감시, 가용성, 방호성, 방재성에 대한 지침을 내용으로 하였으며, 관리적 보호조치로는 보호관리의 체계화와 관리용 정보시스템 장비 보호에 관한 내용을 담고 있다.

집적정보통신시설에서의 현안으로 집적율의 증대로 인한 서버장비의 전기 사용량뿐만 아니라, 항온 항습을 위한 전기사용량의 증가, 이에 따르는 수·배전 설비 증설 부담과 발전기와 UPS용량 증설 부담 등 전력사용료 부담과 더불어 안정성 확보를 위한 신규설비 투자 부담 등이 있다. 또한 사용트래픽의 고도화로 인한 기반 장비의 업그레이드, 연동망의 증설 부담등도 수익성을 악화시키는 원인이 되고 있다. 더 넓게는 이러한 문제들이 법령과 해당 지침상의 규정과 연관이 되어 규제사항으로 작용되고 있다.

다. 정보보호 안전진단의 의무화

정보보호 안전진단 제도는 주요정보통신서비스 제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 정보보호조치의 관리적·물리적 보호조치를 이행하고 안전진단 수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다.

정보통신망법 제46조의3에서는 「전기통신사업법」 제2조 제1항 제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다), 집적정보통신시설 사업자, 정보통신서비스 제공자로서 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자로 하여금 자신의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 받도록 하고 있으며, 이 경우 안전진단 수행기관은 15명 이상의 정보보호 기술 인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인이어야 한다는 규정을 두고 있다.

또한 정보보호 안전진단을 받는 사업자는 관련 정보의 제공 및 시설·장소에의 출입 허용 등 안전진단 수행기관의 정보보호 안전진단 업무에 협력하고, 대통령령으로 정하는 바에 따라 정보보호 안전진단의 결과를 방송통신위원회에 제출하도록 하고 있다. 안전진단 수행기관은 제1항에 따른 정보보호 안전진단을 받은 사업자에게 안전진단의 결과에 따라 정보보호조치의 개선을 권고할 수 있고, 정보보호조치의 개선을 권고하였으면 그 권고내용 및 처리 결과를 방송통신위원회에 통보하여야 한다. 방송통신위원회는 제출된 정보보호 안전진단의 결과와 통보내용에 따라 필요하면 정보보호 안전진단을 받은 사업자에게 정보보호조치에 관한 개선명령을 할 수 있다. 또한, 방송통신위원회는 제1항 제3호(정보통신서비스 제공자로서 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자)의 요건에 해당하는지를 확인하기 위하여 필요하면 관계 행정기관, 관련 자료 보유기관 또는 정보통신서비스 제공자에 대하여 필요한 자료의 제공 또는 사실의 확인을 요청할 수 있도록 규정하고 있다.

현행 기준에서 정의한 안전진단 대상자 유형은 주요정보통신서비스제공자, 집적정보통신시설사업자, 정보통신서비스 제공자이다. 이 기준에 따라 방송통신위원회에 신고 된 전기통신사업자 목록 및 관련 협회 자료, 신용평가기관 등의 자료를 활용하여 대상자가 선정된다. 또한 쇼핑몰 등 정보통신서비스 제공자에 대하여 매출액 100억 원 이상인 사업자는 국세청의 자료를, 일일평균 이용자수 100만 명 이상인 사업자 목록은 관련 기관에서 입수하고 있다.

이러한 기준들을 통해 안전진단 대상자 선정에 있어서의 문제점들을 도출할 수 있다. 첫째, 다중이용 서비스 제공자의 경우, 현행 총매출액 100억 원 이상이거나, 평균 일일 이용자수가 100만 명 이상인 업체를 대상으로 하고 있다. 그러나 소규모 업체로서 사이트에서 금융거래가 이루어지거나 다수의 사용자 정보를 다루는 업체의 경우, 금융 사고나 해킹사고가 발생할 경우 불특정 다수에 대한 피해를 유발할 가능성이 높기 때문에, 이러한 사업자들에 대해서도 안전진단을 받게 할 필요가 있다.

둘째, 안전진단대상 중 '쇼핑몰 등 기타 정보통신 서비스제공자'의 선정 기준은 100억 원 이상의 정보통신 서비스 매출액을 별도 구분하여 관리하지 않고 임의적으로 정보통신 서비스 매출액을 산출하고 있다. 또한 기업분할 등으로 매출액을 분리하는 방법 등을 통해서 의무를 회피하는 문제가 있을 수 있다. 셋째, 영세업체의 경우, 안전진단 수수료 부담, 전문적인 기술 인력의 미보유 등의 측면에서 제도에 대한 불만이 높다. 그러나 이들이 제공하는 서비스의 중단 혹은 정보통신설비에 침해사고가 발생하면 고객피해는 물론, 국가차원의 사회적·경제적인 피해 위험성이 제기될 수 있다.[104]

라. 이용자에 대한 정보보호조치 의무화

현행 정보통신망법 제47조의3에서 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있도록 규정하고 있다. 또한, 주요정보통신

104) 안연식, 정보보호 안전진단 대상자 선정 기준의 개선 방안 연구, 한국IT서비스학회지, 제8권 제1호, 2009. 3.

서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다. 또한「소프트웨어산업 진흥법」제2조[105]에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알리도록 규정하고 있다.

한편 정보통신망법 개정안 제48조에서도 이용자에 대한 보호조치로서 위의 내용에 덧붙여 정보통신서비스 제공자는 자신의 서비스를 이용하는 이용자의 정보통신망에 장애가 발생할 가능성이 있는 경우에는 이용약관으로 정하는 바에 따라 그 이용자에게 보호수단을 제공하고 이를 실행하도록 요구할 수 있다는 조항을 정하고 있다.

---

105)「소프트웨어산업 진흥법」[시행 2009. 7.31] [법률 제9401호, 2009. 1.30, 타법개정]
第2條 (정의 <개정 2007.12.21>) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2005.12.30, 2007.12.21>

1. "소프트웨어"라 함은 컴퓨터·通信·自動化 등의 裝備와 그 周邊裝置에 대하여 命令·制御·入力·처리·貯藏·出力·相互作用이 가능하도록 하게 하는 指示·命令(音聲이나 映像情報 등을 포함한다)의 集合과 이를 작성하기 위하여 사용된 記述書 기타 관련 資料를 말한다.
2. "소프트웨어産業"이라 함은 소프트웨어의 開發·製作·生産·流通 등과 이에 관련된 서비스 및 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」 제2조제1호의 規定에 의한 情報시스템의 構築·운영 등과 관련된 産業을 말한다.
3. "소프트웨어사업"이라 함은 소프트웨어産業과 관련된 經濟活動을 말한다.
4. "소프트웨어事業者"라 함은 소프트웨어사업을 영위하는 者를 말한다.
5. "소프트웨어기술자"란 「국가기술자격법」에 따라 정보처리 분야의 기술자격을 취득한 자 또는 소프트웨어 기술 분야에서 대통령령으로 정하는 학력이나 경력을 가진 자를 말한다.
6. "소프트웨어프로세스"란 소프트웨어를 개발하고 유지·보수하기 위하여 사용하는 일련의 방법·절차·활동 등을 말한다.
7. "소프트웨어振興施設"이라 함은 소프트웨어事業者와 그 支援施設 등을 집단적으로 誘致함으로써 소프트웨어事業者의 영업활동을 지원하기 위하여 第5條의 規定에 의하여 지정된 施設物을 말한다.
8. "소프트웨어 진흥단지(振興團地)"라 함은 소프트웨어사업자와 그 지원시설 등을 집단적으로 유치함으로써 소프트웨어사업자의 영업활동을 지원하기 위하여 제6조의 규정에 의하여 지정·조성된 지역을 말한다.

마. 웹사이트 운영자 등의 침해사고 예방의무

정보통신망법 제47조의3제3항에서 「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다고 규정하고 있다. 한편, 정보통신망법 개정안 제47조에서는 방송통신위원회는 악성프로그램 또는 악성프로그램의 감염을 유인하는 전자적 정보가 숨겨져 있는 웹사이트를 발견한 경우 그 운영자 등에게 해당 프로그램 또는 정보의 삭제를 요청할 수 있도록 규정하고 있고, 웹사이트 운영자 등은 특별한 사유가 없는 한 이에 따르도록 하고 있다.

바. 사업자의 정부요청에 따른 침해사고 대응

현행 정보통신망법 제48조의2에서는 침해사고의 대응과 관련하여 대통령령으로 정하는 바에 따라 주요정보통신서비스 제공자, 집적정보통신시설 사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자는 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하여야 하도록 규정하고 있다. 또한 방송통신위원회는 위의 내용에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있고, 방송통신위원회나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 주요 정보통신서비스 제공자, 집적정보통신시설 사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자에게 인력지원을 요청할 수 있도록 규정하고 있다.

정보통신망법 개정안 제46조에서는 방송통신위원회는 침해사고가 발생한 정보통신망에 대한 취약점 점검, 기술지원 등의 조치를 위하여 긴급히 필요한 경우 이에 대한 접속을 해당 정보통신서비스 제공자에게 요청할 수 있도록 하고 있다. 또한 취약점 점검, 기술지원 등을 하는 자는 해당 정보통신망에 의해 처리되는 정보를

취약점 점검, 기술지원 등의 목적 외로 열람하지 못하도록 하는 규정을 두었다.

또한 동법 개정안 제50조에서는 침해사고 관련 정보의 제공과 관련하여 주요정보통신서비스 제공자, 집적정보통신시설사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자는 침해사고의 유형별 통계, 해당 정보통신망의 소통량통계 및 접속경로별 이용통계 등 침해사고의 예방 및 대응에 관한 정보를 방송통신위원회나 한국인터넷진흥원에 제공하도록 정하고 있다. 동 조항 제3항에서 방송통신위원회는 침해사고가 발생한 경우 피해확산을 방지하기 위하여 정보통신서비스 제공자에게 해당 정보통신서비스 이용자의 연락처를 제출할 것을 요청할 수 있도록 규정하고 있다.

제2절 미국의 정보통신망 정부규제 현황

1. 총설

미국은 21세기 정보화시대의 주도권을 잡기 위해 정보보호를 위한 다양한 법과 제도를 수립·시행하고 있으며, 최첨단 암호 알고리즘과 프로토콜 개발 등 정보보호 기술 개발에도 역점을 기울이고 있다.

최근에 오바마 행정부는 국가 사이버 보안관련 정책과 활동을 총괄 조정하는 사이버보안정책관(cybersecurity policy official)을 백악관에 신설하는 등 사이버스페이스 보안 강화를 위한 강력한 정책의지를 반영한 범정부 차원의 전략보고서[106]를

106) CYBERSPACE POLICY REVIEW : Assuring a Trusted and Resilient Information and Communications Infrastructure. 동 전략보고서는 2008. 12월 미국 CSIS(국제전략연구소)가 작성한 차기 오바마 정권을 위한 보안정책 권고 보고를 토대로 2009년 오바마 정권 출범 이후 오바마 대통령의 지시에 따라 작업이 추진되어 2009년 5월 29일 5대 사이버보안 일정을 발표한 것이다. △최상위 수준에서의 리더십 발휘 : CIA, FBI, NSA 등으로 분산되어 있는 사이버 보안 기능을 백악관에서 통제하고 이에 대한 성과평가를 함으로써 사이버 보안정책 시행의 강력한 추진력 확보, △디지털국가 역량 구축 : 사이버 보안 수준 강화를 위한 근본적 해결방안은 이용자의 인식수준 향상에 있음을 인식하고 이를 위한 범국가적 인식제고 사업 추진, △사이버보안 책임 공유 : 정부네트워크와 민간네트워크 간의 구분된 사이버 보안을 추진할 수 없음을 인식하고 정부·민간·산업간 협력 및 공동대응 체계 구축과 보안 책임 공유 필요, △효과적인 정보공유 및 사고대응 체계 구축 : 사이버보안 관련 연방정부 기관간 또는 민간기관과의 정보 공유 및 사고 공동 대응 체계 구축을 통한 사고 예방 및 대응 역량 강화, △혁신 촉진 : 빠르게 발전하는 IT패러다임에 선제적으로 사전예방적으로 대응할 수 있는 정보보호 정책 추진을 위한 R&D정책 및 법제 정비 추진. 이재일, "미국 오바바 정부의 정보보호 정책", 미국 오바바 정부의 정보보호 정

발표(2009. 5. 29) 하였고, 이와는 별도로 현재 상원에서는 국가 사이버 보안 강화를 위해 사이버보안 위기시 대통령에게 인터넷의 사용을 일부 정지시키는 것을 허용하는 등 강력한 조치를 담고 있는 「2009 사이버보안 법안(Cybersecurity Act of 2009)」[107]이 논의 중에 있다.

이하에서는 컴퓨터 네트워크와 인터넷상의 정보처리 및 유통과 관련 범죄적 행위를 규제하는 미국의 법률[108]을 중심으로 미국의 정보통신망에 대한 정부규제 현황을 살펴보도록 하겠다.

2. 정보보호 관련 법률 현황

미국은 1980년대 초 컴퓨터 범죄가 급증하고 기존의 연방 형사법 규정으로는 이들을 모두 규율할 수 없게 됨에 따라 1984년 미국 연방의회는 연방법전 제 18편 제 1030조(18U.S.C.§1030)에 컴퓨터와 컴퓨터 네트워크에 대한 비인가된 접근과 이용을 규율하는 규정을 포함시켰다.[109] 이후 1986년 이를 개정하여 컴퓨터 관련 범죄를 일괄적으로 규정한 「컴퓨터 사기 및 오용에 관한 법률(Computer Fraud and Abuse Act : CFAA)」을 제정하여 컴퓨터 정보처리에 대한 범죄적 행위를 규제하고 있으며, 동 법은 컴퓨터 범죄가 나날이 지능화·정교화 해짐에 따라 그동안 7차례의 개정[110]을 한 바 있다.[111]

「컴퓨터 사기 및 오용에 관한 법률」 외에도 크게 「전자통신보호법(Electronic Communications Privacy Act: ECPA)」라고 불리는 커다란 타이틀 아래 연방법전 18편에서 18U.S.C.§2701(저장된 통신에 대한 불법 접근), 18U.S.C.§2511 (유선도청), 18U.S.C. §250 (Pen Register) 등에서 전자적통신의 보호에 대한 규정을 하고

책 시사점 및 우리의 발전방향 토론회 발표자료. http://imnews.imbc.com/news/forum/2379104_5492.html, 상세한 내용은 후술한다.

107) 2009. 4. 1일 상원의원 제이 록펠러(Jay Rockefeller), 올림피아 스노위(Olympia Snowe), 빌 넬슨(Bill Nelson) 이름으로 상원에 법안 제출하였다. 상세한 내용은 후술한다.

108) 미국 연방법(U. S. Federal Law)을 중심으로 살펴보고자 하며, 미국 각주의 컴퓨터관련 범죄 법률에 대해서는 한국정보보호센터, 「국내외 정보보호관련 법제도 현황」, 1996. 12. pp. 81-85 참조.

109) 종합 범죄 통제법 : Comprehensive Crime Control Act of 1984

110) 1988, 1989, 1990, 1994, 1996, 2001, 2002, 2008

111) http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.html

있으며, 18U.S.C.§1028(a)(7)(신분 절취), 18U.S.C.§1028A(가중된 신분 절취), 18U.S.C.§1029(접근장치 사기), 18U.S.C.§1037(CAN-SPAM법), 18U.S.C.§1343(유선 사기), 18U.S.C.§1362(통신 방해) 등에서 컴퓨터 네트워크 관련 범죄를 규정하고 있다.[112]

3. 컴퓨터 사기 및 오용에 관한 법률(Computer Fraud and Abuse Act : CFAA)[113]

「컴퓨터 사기 및 오용에 관한 법률」은 컴퓨터를 통한 국가보안정보, 금융정보, 행정정보 등에 대한 불법 접근과 취득 및 사용, 보호되는 컴퓨터를 이용한 사기, 보호되는 컴퓨터에 대한 손상 등을 범죄로 규정하고 이에 따른 처벌을 규정하고 있다.[114]

가. "컴퓨터"와 "보호되는 컴퓨터"의 개념 정의

1) "컴퓨터"[115]라 함은 전자적, 전기적, 광학적, 전기화학적, 또는 기타 고속처리장치로서 논리적, 산술적, 또는 저장의 기능을 수행하는 것을 의미하며, 이런 장치에 직접 관련되어 있거나, 이런 장치와 맞물려 작동하는 자료 저장 장치나, 통신 장치를 말한다. 그러나 자동화된 타자기나 식자기, 휴대용 소형 계산기 또는 이와 유사한 장치들은 포함되지 않는다.

2) "보호되는 컴퓨터"[116]라 함은 ① 금융기관 또는 미국 정부가 전용하는 컴퓨터를 의미하며, 그렇게 전용하지 않는 경우에는, 금융기관이나 미국 정부에 의하여

---

112) http://www.usdoj.gov/criminal/cybercrime/ccmanual/03ccma.html
113) 18U.S.C.§1030. 동 규정은 컴퓨터 관련 범죄를 일괄적으로 규정하고 있어 미국 연방법전 중에서 우리나라의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 가장 유사한 조문이라 고할 수 있다. 참고로 원문과 번역문은 별도 첨부된 부록을 참조한다.
114) 형사적 처벌과는 별도로 손상 또는 손해를 입은 사람은 불법행위자에 대하여 민사상 보전적 손해배상 청구와 금지명령, 기타 형평법상의 구제조치를 청구할 수 있다. 18U.S.C.§1030(g)
115) 18U.S.C.§1030(e)(1)
116) 18U.S.C.§1030(e)(2)

사용되거나 금융기관이나 미국 정부를 위하여 사용되는 컴퓨터로서, 범죄를 구성하는 행위가 금융기관이나 미국정부에 의한, 또는 금융기관이나 미국정부를 위한 사용에 영향을 미치는 경우나 ② 이러한 컴퓨터가 주 간(州間) 또는 외국과의 통상이나 통신에 사용되는 경우를 말하는데, 미국과의 주 간(州間) 또는 외국과의 통상이나 통신에 영향을 미치는 방식으로 사용되는 경우 미국 외에 있는 컴퓨터를 포함한다.

"보호되는 컴퓨터"는 1996년 법 개정을 통해 새롭게 도입된 정의 규정으로 간단히 말해 인터넷과 같이 주 간(州間) 또는 외국과의 통상에 사용되는 컴퓨터와 미국 연방정부와 금융기관의 컴퓨터를 포괄하는 개념으로 "컴퓨터" 개념 정의 외에 "보호되는 컴퓨터"에 대한 개념 정의 규정이 없었던 1996년 법 개정 이전에는 주 간(州間) 통상에 사용되지 않는 미국정부나 금융기관의 컴퓨터는 보호 대상에서 제외되는 것으로 해석되었으나 주 간(州間) 또는 외국과의 통상이나 통신에 사용되는 경우를 포함시킴으로써 이를 보완한 것이다. 그 이후에도 미국 내 공격자가 해외의 컴퓨터 시스템을 공격하거나, 외국 거주자가 해킹을 하면서 미국을 통하여 통신문을 발송할 때 연방법전 제 18편 제 1030조(18U.S.C.§1030) 규정 적용여부가 애매했으나 2001년 소위 「미국 애국법(USA PATRIOT Act)」 개정을 통해 미국과의 주 간(州間) 또는 외국과의 통상이나 통신에 영향을 미치는 방식으로 사용되는 경우 미국 외에 있는 컴퓨터도 보호되는 컴퓨터에 포함시킴으로써 이 문제를 해결했다.[117]

나. 범죄 구성행위와 이에 따른 처벌

1) 정당한 권한 없이 또는 허가된 접근 범위를 넘어 고의로 컴퓨터에 접근함으로써 미국 정부가 행정명령이나 법률에 의거 국방 또는 국제 관계의 견지에서 무단 공개되지 않도록 보호하기로 한 정보 및 1954년의 「원자력법」 제 11조 y항에서 규정한 것과 같은 제한된 자료를 취득한 뒤, 이렇게 하여 취득한 정보가 미국을

117) http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.html (이하 아래 CFAA의 대한 설명은 대부분 미법무부의 위 자료에서 참조)

해치고 어느 외국을 이롭게 하는데 쓰일 수 있다고 믿을 이유를 가지고, 이를 받을 자격이 없는 사람에게 함부로 통지, 배달, 전송하거나 통지, 배달, 전송되게 하거나, 통지, 배달, 전송할 것을 기도하거나, 통지, 배달, 전송되게 하도록 기도하거나, 이러한 정보를 정당하게 받을 자격이 있는 미국 정부 공무원이나 고용원에게 고의로 제대로 배달하지 않는 경우와 이상의 범죄행위를 기도했을 경우에는 10년 이하의 징역이나 벌금, 또는 이를 병과할 수 있으며, 재범시에는 20년 이하의 징역이나 벌금, 또는 이를 병과할 수 있다.[118]

이 조항은 내부의 행위자가 허가된 접근 범위를 넘어서 접근하는 경우와 정당한 권한이 없는 외부 행위자의 접근 모두를 포함한다. 행위자는 이 조항의 위반을 통하여 행위자가 취득한 정보가 미국의 이익을 해치거나 외국의 이익을 위해 이롭게 쓰일 수 있다는 믿음을 가지고 있는 것을 요건으로 한다. 그러나 이 요건은 국가 보안 정보가 제한되어 있거나, 비밀 정보라는 사실과 행위자가 그러한 인지를 하고 있었다는 사실만 증명하면 비교적 쉽게 만족시킬 수 있다.

2) 정당한 권한 없이 또는 허가된 접근 범위를 넘어 고의로 컴퓨터에 접근함으로써 ① 금융기관이나 15U.S.C.1602(n)에서 규정한 카드 발급자의 금융기록에 포함된 정보 또는 「공정신용보고법(Fair Credit Reporting Act)」[119]에서 정의된 용어에 따른 소비자보고기관의 파일에 들어있는 정보, ② 미국의 각 정부부처 또는 행정기관으로부터 나온 정보, ③ 주 간(州間) 또는 외국과의 통신에 포함되어 보호되는 컴퓨터로부터 나온 정보를 취득하는 경우와 이상의 범죄행위를 기도했을 경우에는 1년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범 시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다. 그리고 이상의 범죄행위가 ① 상업적인 이익이나 사적 금융이익을 위한 경우, ② 헌법이나 미국 또는 어느 주의 법률에 위배하여 범죄적인 또는 불법행위적인 행위를 진행시키기 위하여 저질러졌을 경우, ③ 취득한 정보의 가치가 $5,000을 넘을 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[120]

---

118) 18U.S.C.§1030(a)(1), 18U.S.C.§1030(c)(1)
119) 15U.S.C.1681 참조
120) 18U.S.C.§1030(a)(2), 18U.S.C.§1030(c)(2)

이 조항의 위반은 특별히 가중될 만한 사실이 없는 한 경범죄에 해당한다. 특이할 만한 사항으로 이 조항에서는 위반으로 인한 금전적 손해에 대한 최소한의 기준이 없는데 그 이유는 사생활의 침해가 반드시 금전적인 손해로 이어지는 것은 아니지만 여전히 연방정부의 보호를 받을 필요가 있기 때문이다. 그러나 위반의 요건으로 금전적 손해에 대한 최소한의 기준은 정해져 있지 않지만 위반으로 인해 취득한 정보로 인한 금전적 가치가 경범죄인지, 또는 중죄인지를 결정하는 중요한 요소이다.

3) 고의로, 미국의 각 정부부처 또는 행정기관의 비공개 컴퓨터에 접근할 권한이 없이, 미국정부가 전용하는 정부기관 또는 대행기관 컴퓨터에 접근하는 경우, 또는 그 컴퓨터가 미국 정부의 전용이 아니라 하더라도 그것이 미국 정부에 의하여 또는 미국 정부를 위하여 사용될 경우, 이러한 정부에 의한 또는 정부를 위한 사용에 영향을 미치는 경우와 이상의 범죄행위를 기도했을 경우에는 1년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[121]

이 조항은 외부인이 미국 정부 부처의 컴퓨터에 접근한 경우 그 접근으로 인하여 비록 아무런 정보를 취득하지 하였을 경우에도 이를 범죄로 규정한다. 미 의회에서 이 조항에 내부인을 포함하지 않고 외부인으로 한정한 것은 내부인이 접근하였을 때 행정적인 처분이 더 적절함에도 불구하고 형사적인 처벌을 받는 것을 방지하기 위해서였다. 그러나 미 의회는 위반자가 속해 있는 부처 외부 부처의 컴퓨터에 대한 권한 없는 접근(intra-departmental trespass)은 이 조항에 의해 처벌을 받도록 의도하였다.

4) 고의로, 사취할 목적으로, 정당한 권한 없이 또는 허가된 접근 범위를 넘어 보호되는 컴퓨터에 접근하고 이렇게 함으로써 의도된 사취를 더 진행시키고 이득을

121) 18U.S.C.§1030(a)(3), 18U.S.C.§1030(c)(2)

취하는 경우(다만, 사기의 목적과 얻은 이익이 단지 컴퓨터를 사용하는데 그치거나 사용의 가치가 1년간 $5,000 이하인 경우에는 제외한다)와 이상의 범죄행위를 기도했을 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[122]
미국 검찰에서는 컴퓨터 해킹 사건을 기소할 때 만일 사기의 증거가 있다면 컴퓨터에 대한 접근이 경범죄로 다루어지는 §1030(a)(2)보다는 이 조항에 의해 중죄로 기소할 것을 권장하고 있다. 또한 검찰은 이 조항과 비슷한 범죄 요건을 갖추었지만 더욱 강력한 처벌 조항을 가지고 있는 "유선사기" 18 U.S.C. § 1343을 적용할 것을 권장하고 있다.

5) 고의로 프로그램, 정보, 부호, 또는 명령을 전송하게 하여, 보호되는 컴퓨터에 정당한 권한 없이 손상을 입히는 경우와 이상의 범죄행위를 기도했을 경우에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 20년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다. 그리고 이상의 범죄행위가 고의로 또는 무모하게 발생하여 심각한 신체적 손상을 입히거나 이를 기도했을 경우에는 20년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며, 사망에 이르거나 살인을 기도했을 경우에는 최고 종신형이나 벌금, 또는 이를 병과 할 수 있다.[123]

6) 정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 무모하게 손상을 입히게 하는 경우와 이상의 범죄행위를 기도했을 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 20년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[124]

7) 정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 손상을 초래하는 경우와 이상의 범죄행위를 기도했을 경우에는 1년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할

122) 18U.S.C.§1030(a)(4), 18U.S.C.§1030(c)(3)
123) 18U.S.C.§1030(a)(5), 18U.S.C.§1030(c)(4), 18U.S.C.§1030(c)(5)
124) 18U.S.C.§1030(a)(5), 18U.S.C.§1030(c)(4)

수 있다.[125]

「컴퓨터 사기 및 오용에 관한 법률」에서 특히 DDoS와 같은 공격을 범죄로 규정하는 조항은 위의 5) 6) 7)에 해당하는 18 U.S.C. § 1030 (a)(5)이다. 동 조항은 범죄자가 여러 형태로 컴퓨터에 손상을 가하는 것을 대상으로 하고 있는데 여기에는 DDoS와 같이 불필요한 정보를 전송함으로써 합법적인 사용자가 정보에 접근하는 것을 방해하는 행위, 바이러스나 웜을 유포하여 기업 네트워크 등을 다운시키거나, 바이러스나 웜을 유포하여 컴퓨터의 보안을 무력하게 하여 파일을 삭제하거나 컴퓨터를 다운시키거나 악성 소프트웨어를 심거나 또는 다른 형태로 컴퓨터의 기능을 저하시키는 것을 포함하여 §1030 (a)(5)은 사용자가 사용자의 컴퓨터를 운영하고자 하는 대로 운영하지 못하게 하는 다양한 행위에 대한 범죄로 규정하고 있다.

동 조항을 좀 더 자세히 살펴보면 (a)(5)(A)(i)은[126] 행위자가 "1. 코드나 프로그램, 정보, 그리고 명령을 알면서 전달되도록 하고, 2. 그러한 행위로 인하여 보호되는 컴퓨터에 승인 없이 의도적으로 손상을 가하는 행위"가 명시되어 있고, (a)(5)(A)(ii)는 행위자가 "1. 의도적으로 보호되는 컴퓨터에 승인 없이 접근하여, 2. 그러한 행위의 결과로 무모하게 손상을 초래" 라고 명시하고 있고, (a)(5)(A)(iii)는 "1. 의도적으로 보호되는 컴퓨터에 승인 없이 접근하여 그러한 행위의 결과로 손상을 초래" 하는 행위라고 규정하고 있다.

특이할 만한 사항은 (a)(5)(A)에는 의도적인 접근과 의도적인 손상초래, 의도적인 접근과 무모하게 손상 초래, 그리고 의도적인 접근과 손상 초래, 모두가 포함되어 있다. (ii)와 (iii)는 행위자가 의도적으로 승인 없이 컴퓨터에 접근했다면 해를 끼칠 의도가 없었다고 하더라도 책임을 지도록 명시하고 있다.

반면에 (i)은 정부가 행위자가 "접근"을 하였다는 것을 증명할 필요가 없다. (i)에 의하면 승인 없이 컴퓨터에 해를 미치는 코드나 프로그램을 알면서 전송하였다는 사실만 증명하면 된다. 웜이나 트로이 목마 바이러스는 행위자가 시스템에 접근하지 않고도 자기복제를 할 수 있기 때문에 컴퓨터에 접근하지 않고도 컴퓨

125) 18U.S.C.§1030(a)(5), 18U.S.C.§1030(c)(2), 18U.S.C.§1030(c)(3)
126) 위의 5)에 해당한다.

터에 손상을 초래할 수 있기 때문이다.

(a)(5)(A)의 몇 가지 중요한 요건, "접근" "전송" "권한 없이" "손상"의 정의에 대해서는 법원의 판례를 참고할 필요가 있다. (i)의 경우 행위자의 "접근"에 대하여 행위자가 컴퓨터에 접근할 수 있는 권한을 가지고 있거나 (내부자) 또는 권한을 가지고 있지 않거나 (외부자) 또는 시스템에 전혀 접근을 하지 않은 경우 모두 적용된다. 여기서 "프로그램, 정보, 코드, 명령"은 매우 광의로 해석되어 "컴퓨터의 운용에 영향을 미칠 수 있는 모든 전송"을 포함한다. 그리하여 시스템의 취약점을 노리는 것을 목적으로 하는 소프트웨어 코드, 소프트웨어 명령, 네트워크 패킷이 모두 포함된다.

행위자가 웜이나 DDoS공격과 같은 행위를 시작하였을 경우 정부로서 "전송"이 있었다는 것을 증명하기는 쉽다. 그러나 물리적인 행위, 즉, 컴퓨터의 스위치를 끈다거나 하는 행위에는 "전송"이 적용되지 않으며 다른 법의 적용을 받는다.

행위자가 (i)에 해당하기 위해서 직접적으로 전송을 할 필요가 없다. United States v. Sullivan 사건[127]에서 피고가 소프트웨어에 악성코드를 삽입하였는데 4개월간 그 코드가 비활성화 상태로 있다가 활성화되면서 다른 악성코드들을 다운로드 받아 사용자로 하여금 컴퓨터에 접근을 할 수 없게 한 경우 재판부는 피고가 "전송" 행위를 하였다고 판단하였다.

(ii)와 (iii)에는 "허락된 범위를 넘어서"라는 요건이 없고 둘 다 "권한 없이"를 그 요건으로 하고 있다. "권한 없는" 또는 "허락된 범위를 넘어서"에 대한 정의는 다음과 같다.

많은 경우에 행위자가 다른 사람의 컴퓨터의 보안의 취약점을 이용하거나 또는 손상을 초래하기 위하여 명령을 전송하는 경우 명백한 "권한 없는 접근"이라고 볼 수 있다. 그러나 법원은 행위자가 다른 사람의 보안을 무력하게 하는 자동, 자기복제 프로그램을 배포하는 것과 같은 간접적인 수단을 사용하는 것도 "권한 없는 접근"이라고 판단하였다. [128]

"손상을 초래하는"은 다음과 같다. "손상을 초래하는"의 요건은 행위자가 컴퓨터에 손상을 초래하였다는 것만 증명하면 된다. 손상을 입은 컴퓨터가 행위자가 손

127) United States v. Sullivan, 40 Fed. Appx. 740 (4th Cir. 2002)
128) United States v. Morris, 928 F.2d. 504, 509-10 (2d Cir. 1991)

상을 초래하려 했던 컴퓨터와 동일하지 않아도 된다. “손상”은 광의로 해석되며, “손상”앞에 “어떠한”이라는 단어를 추가함으로써 일반적으로 생각하는 그러한 물리적인 손상 이상을 포함한다는 것을 알 수 있다.

“손상”은 데이터, 프로그램, 시스템, 정보의 원래 상태로의 보전에 영향을 미칠 때 일어난다. 그리하여 행위자가 컴퓨터 시스템에 접근함으로써 데이터나 정보가 삭제되거나 변경되는 경우 이에 해당한다. 비슷하게 행위자가 컴퓨터가 작동하는 방법을 변경하도록 하는 것도 “손상”에 해당되며, 행위자가 사용자의 컴퓨터의 보안 프로그램을 변경하여 컴퓨터에 접근하는 자를 탐지하지 못 한 것도 “손상”에 해당한다.

또한 정보나 데이터를 변경하는 것 외에도 정보에 접근을 하지 못하는 것 자체도 ″손상″에 해당한다. 그리하여 행위자들이 컴퓨터의 모든 리소스를 사용하고 있어 비록 데이터나 소프트웨어가 변경되지 않았다고 하더라도 컴퓨터를 사용할 수 없는 경우 “손상”에 해당한다.

많은 경우에 침입자의 의도는 단순히 정보를 빼내거나 사기 행위를 할 의도였지만 시스템에 해를 끼치는 경우가 많다. 예를 들어 침입자들은 시스템 관리자가 침입자가 네트워크에 접근하였다는 사실을 모르게 하기 위하여 로그파일을 지우려고 시도하는데, 로그파일을 삭제하는 것도 1030(a)(5)의 “손상”에 해당한다. 비슷한 경우로는 컴퓨터에 나중에 다시 접근할 수 있도록 시스템 프로그램을 변경하거나 새로운 프로그램을 설치하는 행위는 컴퓨터와 프로그램의 원래 상태로 보전하는 것을 손상하는 행위이므로 이러한 행위도 “손상”에 해당한다.

8) 고의로 그리고 사취할 목적으로 암호 또는 이와 유사한 정보를 거래(제 1029조에서 규정한 바와 같이) 함으로써 정당한 권한 없이 컴퓨터에 접근하는 경우(다만, 이런 거래가 주 간(州間) 또는 외국과의 통상에 영향을 미치는 경우, 또는 접근한 컴퓨터가 미국 정부에 의하여 또는 미국 정부를 위하여 쓰이는 경우가 전제)와 이상의 범죄행위를 기도했을 경우에는 1년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[129]

9) 자연인, 회사, 협회, 교육기관, 금융기관, 정부조직체, 기타 법인으로부터 금전이나 기타 가치 있는 물건을 강제로 탈취하기 위하여 주 간(州間) 또는 외국과의 통상에서 보호되는 컴퓨터에 손상을 입힐 것을 위협하는 통신문을 전송하는 경우와 이상의 범죄행위를 기도했을 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[130]

129) 18U.S.C.§1030(a)(6), 18U.S.C.§1030(c)(2)
130) 18U.S.C.§1030(a)(7), 18U.S.C.§1030(c)(3), 18U.S.C.§1030(e)(12)

범죄구성 행위*	처벌 형량**
국가보안정보 등의 불법적인 취득, 통지, 배달, 전송 등	10년(20년) 이하의 징역이나 벌금, 또는 이의 병과
금융정보, 행정정보, 주 간(州間) 또는 외국과의 통신정보 등의 불법 취득	1년(10년) 이하의 징역이나 벌금, 또는 이의 병과 상업적인 이익을 위한 경우, 취득한 정보의 가치가 $5,000을 넘을 경우 등 특별한 경우에는 5년 이하의 징역이나 벌금, 또는 이의 병과
정부부처 또는 행정기관의 비공개 컴퓨터 등에 대한 불법접근, 사용 방해 등	1년(10년) 이하의 징역이나 벌금, 또는 이의 병과
보호되는 컴퓨터에 대한 불법접근과 이를 통한 사취	5년(10년) 이하의 징역이나 벌금, 또는 이의 병과
고의로 프로그램, 정보, 부호, 또는 명령을 전송하게 하여, 보호되는 컴퓨터에 정당한 권한 없이 손상을 입히는 경우	10년(20년) 이하의 징역이나 벌금, 또는 이의 병과 피해자에게 심각한 신체적 손상을 입혔을 경우에는 20년 이하의 징역이나 벌금, 또는 이의 병과 피해자가 사망했을 경우에는 최고 종신형이나 벌금, 또는 이의 병과
정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 무모하게 손상을 입히게 하는 경우	5년(20년) 이하의 징역이나 벌금, 또는 이의 병과
정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 손상을 초래하는 경우	1년(10년) 이하의 징역이나 벌금, 또는 이의 병과
암호 등의 거래를 통한 불법적인 컴퓨터 접근	1년(10년) 이하의 징역이나 벌금, 또는 이의 병과
주 간(州間) 또는 외국과의 통상에서 보호되는 컴퓨터에 손상을 입힐 것을 위협하는 통신문 전송	5년(20년) 이하의 징역이나 벌금, 또는 이의 병과

<표2>「컴퓨터 사기 및 오용에 관한 법률」의 범죄구성 행위와 이에 따른 처벌

* 모든 범죄구성 행위에는 미수범도 포함

** 처벌 형량 중 괄호안의 연수는 재범시 형량

4. 기타 컴퓨터 네트워크 범죄 관련 연방법전 규정[131]

가. 저장된 통신에 대한 불법 접근

연방법전 제 18편 제 1030조(18U.S.C.§2701)는 정당한 권한 없는 접근으로부터 전자우편이나 음성메일을 보호하는데 중점을 두고 있다. 동 조문은 메시지가 완전히 의도된 수령자에게 전달될 때까지 전자통서비스제공자에 의해 저장된 통신의 기밀성, 무결성, 가용성[132]을 보장하기 위한 역할을 한다.

동 조문에 따르면 고의로 정당한 권한 없이 전기통신서비스가 제공하는 설비에 접근하거나, 고의로 그러한 설비에 대한 허가된 접근범위를 넘어 시스템 내 전자적 저장 상태에 있는 유선 또는 전자통신에 대한 접근권을 얻거나 변경하거나 방해하는 경우에는 ① 그 행위가 상업적인 이익이나 악의적인 파괴 및 손상 또는 사적 금융이익을 위한 경우이거나 미국 헌법이나 연방법 또는 주법 규정 위반으로 범죄행위나 불법행위를 증진하기 위한 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며 재범시에는 10년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며, ② 다른 경우에는 1년 이하의 징역이나 벌금, 또는 이를 병과할 수 있으며 재범시에는 5년 이하의 징역이나 벌금, 또는 이를 병과할 수 있다. 하지만 유선 또는 전자통신서비스를 제공하는 개인이나 조직체, 그 자신의 통신과 관련되거나 의도된 서비스 사용자에 의해 허가받은 행위인 경우와 다른 조문(§2703, §2704, §2518)에서 인가된 행위는 이러한 처벌이 예외적으로 적용되지 않는다.[133]

이 법에서 행위자는 "전자통신서비스를 제공하는 설비"에 접근하는 것을 요건으로 하는데 "전자통신서비스"란 "사용자가 음성 통신 또는 전자적통신을 전송 또는 수신할 수 있도록 제공되는 서비스"를 의미하며 모든 컴퓨터나 서버가 "설비"로

---

131) http://www.usdoj.gov/criminal/cybercrime/ccmanual/03ccma.html

132) 기밀성(confidentiality), 무결성(integrity), 가용성(availability)은 컴퓨터 보안의 3대 목표 내지 원칙이다. 기밀성이란 권한 있는 사람이나 시스템만이 보호되는 자료(컴퓨터 관련 자산)에 접근이 가능해야 된다는 것이고, 무결성이란 그러한 자료는 권한 있는 당사자에 의해서만 정해진 절차에 따라 변경이 가능하다는 것이고, 가용성이란 그러한 자료가 권한 있는 당사자에게 필요할 때 적시에 제공되어야 한다는 것으로 서비스 거부(denial of service)의 반대 개념이다. Charles P. Pfleeger and Shari Lawrence Pfleeger, 「Security in Computing(3rd edition)」, Pearson Education, Inc., 2003, pp9-12.

133) 18U.S.C.§2701(a), (b), (c)

규정되는 것은 아니다. 예를 들어 사용자가 사용하는 컴퓨터는 “설비”에 해당하지 않는다. 그 예로 한 법원은 가정용 컴퓨터에 해킹하는 것은 “설비”의 접근에 해당하지 않는데 그 이유는 가정용 컴퓨터는 제3자에게 전자통신서비스를 제공하지 않기 때문이라고 하였다.[134] 또한 다른 사건들에서 법원은 업무에 사용되는 컴퓨터와 팩스는 전자적통신 서비스가 제공되는 설비가 아니며, 웹사이트를 운영하거나 인터넷 접근을 이용하는 것 자체가 전자통신서비스의 설비에 해당하지 않는다고 하였다. [135]

"전자적 저장 상태에 있는 통신“ 이란 단순히 ”전자적 수단에 의해 저장된 정보“를 의미하는 것이 아니고 ”유선 또는 전자적통신의 전자적 송수신에 수반하는 임시적이고 중간적인 저장, 그리고 전자통신서비스제공자가 그러한 통신을 백업하기 위한 목적으로 저장하는 것“을 의미한다. 만일 사용자의 서비스 제공자에게 메일이 도착하였으나 사용자가 아직 그 메일을 열지 않았다면 그 메일은 ”전자적 저장“상태에 있다. 그러나 사용자가 이메일이나 보이스메일에 접근하여 메일을 확인한 후에는 그 메일은 최종 목적지에 도달하였으므로 더 이상 ”임시이며 중간적인 저장상태“에 있지 않기 때문에 ”전자적 저장“상태로 보지 않는다.

나. 신분 절취

연방법전 제 18편 제 1028조 (a)항 (7)호(18U.S.C.§1028(a)(7))는 1998년의 「신분 절취 및 편취 방지법(Identity Theft and Deterrence Act of 1998)」의 일부로서 제정되었고 2004년에 「신분 절취 처벌 증진법(Identity Theft Penalty Enhancement Act)」에 의해 개정되어 관련 네트워크 범죄에 적용되고 있다.

이에 따르면 연방법을 위반하거나 적용 가능한 주법 또는 지방법 하에서 중죄에 해당하는 불법행위를 범하거나, 방조하거나 교사할 목적으로 또는 공모하기 위하여 다른 사람의 신분인식 수단을 법적 권한 없이 고의로 이전, 소지, 또는 사용하는 경우에는 5년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있으며, 재범시에는

134) United States v. Steiger, 318 F.2d 1039, 1049 (11th Cir. 2003)

135) State Wide Photocpy Corp. v. Tokai Fin. Services, Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995), Dryer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1999 (D.N.D. 2004)

20년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다. 하지만 ① 신분인식문서, 인증용 특징, 또는 허위 신분인식 문서가 미국이 발행하거나 미국의 허락을 받고 발행한 신분인식문서나 인증용 특징 이거나 출생증명서, 운전면허증, 또는 개인 신분증명카드 중에 포함되거나 그렇게 추정되는 경우에 이를 제작 또는 이전하는 경우와 ② 동 행위로 인해 1년 동안 $1,000 이상에 해당하는 가치의 이득을 얻었을 경우에는 15년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다. 한편, 동 범죄행위가 §929(a)(2)에서 규정한 마약거래 범죄를 용이하게 하거나, §924(c)(3)에서 규정한 폭력범죄와 관련될 경우에는 20년 이하의 징역이나 벌금, 또는 이를 병과할 수 있으며, §2331(5)에서 규정한 국내테러와 §2331(1)에서 규정한 국제테러 행위를 촉진하기 위해 저질러진 경우에는 30년 이하의 징역이나 벌금, 또는 이를 병과 할 수 있다.[136]

다. 가중된 신분 절취

2004년 7월 12일 발효된 연방법전 제 18편 제 1028A조(18U.S.C.§1028A, Identity Theft Penalty Enhancement Act)는 가중된 신분 절취 범죄행위를 새롭게 규정하고 있다.

동 조문에 따르면 피고가 연방법전 제 18편 제 1028조(a항 7호 제외), 1029조, 1030조, 1037조, 1343조를 포함하여 연방 범죄행위로 규정된 중범죄 기간 동안 이와 관련하여 다른 사람의 신분인식 수단을 법적 권한 없이 고의로 이전, 소지, 또는 사용하는 경우에는 2년의 징역을 추가한다. 한편 1030조 a항 1호(18U.S.C.§1030(a)(1))와 관련된 것을 포함하여 테러관련 가중 신분 절취의 경우에는 5년의 징역을 추가한다.

라. 접근장치 사기

네트워크 범죄와 관련된 접근장치는 패스워드, 전자은행 계좌번호, 신용카드번호

136) 18U.S.C.§1028(a), (b)

등이 포함된다.

연방법전 제 18편 제 1029조(18U.S.C.§1029)에 따르면 권한 없는 접근장치[137]나 위조접근장치의 제작, 사용, 소지, 또는 거래뿐만 아니라 전기통신서비스를 권한 없이 사용하기 위하여 개조되거나 변조된 전기통신기구의 제작, 사용, 소지, 또는 거래 활동 등은 금지되고 이를 위반하면 처벌을 받는다.

마. CAN-SPAM법

2004년 1월 1일 발효된 2003년의 「CAN-SPAM법」에 의해 다량의 요구하지 않은 상업적 전자우편(스팸)을 보내는 자를 기소할 수 있게 되었다. 동 법은 스팸 발송자가 수신자, ISP, 법집행기관에게 신분이나 스팸의 원천을 숨길 경우 이에 대한 조치를 강구하고 있다.

동 법에 따르면 주 간(州間) 또는 외국과의 통상에 있어서, 또는 이들에 영향을 미치는 경우에, ① 고의로 권한 없이 보호되는 컴퓨터에 접근하여 그 컴퓨터로부터 또는 그 컴퓨터를 통하여 고의로 다량[138]의 상업적 전자 우편 메시지의 전송을 시도하는 행위, ② 메일 발송자에 대해 수신자나 인터넷접속 서비스를 속이거나 오도할 목적으로 다량의 상업적 전자 우편 메시지를 중계하거나 전송하기 위하여 보호되는 컴퓨터를 사용하는 행위, ③ 다량의 상업적 전자 우편 메시지의 헤더 정보를 물리적으로 왜곡하고 고의적으로 그러한 메시지의 전송을 시도하는 행위, ④ 실제 등록자의 신분을 물리적으로 왜곡하는 정보를 사용하여 5회 이상 전자 우편 계정이나 온라인 사용자계정 또는 2회 이상 도메인 이름을 등록하고 고의로 그러한 계정과 도메인 이름의 조합을 통해 다량의 상업적 전자 우편 메시지의 전송을 시도하는 행위, ⑤ 5개 이상 IP주소의 등록자가 되기 위해 거짓으로 자신이 등록자나 합법적인 승계자인 것처럼 나타내면서 고의로 그러한 주소를 통해 다량의 상업적 전자 우편 메시지의 전송을 시도하거나 그렇게 공모하는 행위는 금지되고

---

137) 권한 없는 접근장치(unauthorized access device)는 분실되거나, 도난당하거나, 사용기간이 만료되거나, 사용효력이 철회되거나 취소된 접근장치 또는 사취할 목적으로 획득된 접근장치를 의미한다. 18U.S.C.§1029(e)(3)

138) 다량(multiple)은 24시간 동안 100개 이상, 30일 동안 1,000개 이상, 1년 동안 10,000개 이상 전자우편 메시지를 의미한다. 18U.S.C.§1037(d)(3)

이를 위반하면 처벌을 받는다.

CAN-SPAM에는 15. U.S.C. § 7704(d)에 의해 법제화 된 추가 형법 조항이 있는데 그 조항은 "노골적인 성인물"이라는 것을 제목에 포함하지 않거나 노골적인 성인물이라는 것을 밝히지 않은 채 그러한 내용을 이메일로 전송하는 행위"를 금지하고 있다.

바. 유선 사기

연방법전 제 18편 제 1343조(18U.S.C.§1343)에 따르면 금전이나 재물을 취득할 목적으로 주 간(州間) 또는 외국과의 통상에서 유선(전화), 라디오, TV 통신을 통한 사기행위는 금지되고 이를 위반하면 처벌을 받는다.

동 조문이 네트워크 범죄와 관련되는 이유는 미국 법원이 동 조문에서 사기행위를 금지하는 통신수단에 팩시밀리, 텔렉스, 모뎀, 인터넷 전송이 포함되는 것으로 해석하고 있기 때문이다.

사. 통신 방해

연방법전 제 18편 제 1362조(18U.S.C.§1362)에 따르면 고의 또는 악의로 미국에 의해 운영 또는 통제되는 다양한 통신수단과 미국 방위를 위해 사용되거나 사용될 계획인 통신수단을 손상시키거나 파괴하는 행위, 통신선로 또는 시스템의 작동이나 사용을 방해하는 행위, 통신의 전송을 방해하거나 지연시키는 행위와 이러한 행위를 시도하거나 공모하는 행위 등은 금지되고 이를 위반하면 처벌을 받는다.

동 조문이 네트워크 범죄와 관련되는 이유는 동 조문상의 통신수단과 시스템에 전자우편 서비스를 제공하기 위해 사용되는 것들을 포함하기 때문이다.

아. 유선도청

연방법전 제 18편 제 2511조(18U.S.C. § 2511)에 따르면 고의로 유선, 구두, 또는

전자적통신의 내용을 장치를 이용한 도청(또는 다른 이로 하여금 도청하도록 하는 행위)은 금지되고 이를 위반하면 처벌을 받는다. 1968년 제정 당시에는 이 법은 통신의 프라이버시를 효과적으로 보호하기 위한 것이 목적이기도 하지만 동시에 어떠한 예외적인 경우에 유선 또는 구두 통신의 내용을 도청할 수 있는지 명시하기 위한 것을 그 목적으로 한다고 하였다. 동 조는 (1) 고의로, (2) 도청, (3) 내용을, (4) 유선, 구두 또는 전자적통신, (5) 장치를 이용하여, 라는 다섯 가지 요건을 필요로 하며, 제정 당시에는 유선과 구두 통신만 포함하였으나 1986년에 전자적통신도 포함하도록 개정되었다. 1986년 개정을 통하여 「유선도청법」은 실시간 정보를 포착하는 컴퓨터 범죄를 처벌하는 대안으로 사용되기도 한다.

이 조항의 요건 중 하나인 "고의로"는 행위자가 「유선도청법」을 위반하려는 의도가 아니라 고의로 통신을 도청하려는 의도만 가지고 있으면 그 요건이 충족된다. 또한 두 번째 요건인 "내용"의 경우 법조문에서는 통신의 취득이 통신의 송신과 동시에 이루어질 것을 요구하지는 않지만 「유선도청법」과 「전자적통신 보호법」의 다른 타이틀과의 구분을 위해서는 통신의 송신과 통신의 취득이 동시에 이루어지는 것을 의미하는 것으로 해석된다. 대부분의 판례에서 법원은 위의 두 법을 구분하기 위하여 통신의 취득이 통신의 송신과 동시에 이루어지는 경우에만 통신이 도청되었다고 판단하였으며 통신의 저장된 복사본에 접근하는 것은 도청이 아니라고 판단하였다.

동 조문 하에서 도청이 되기 위해서는 반드시 "내용"의 취득이 있어야 한다. 여기서 "내용"이란 통신 사실기록 또는 통신이 있었다는 사실과는 구분이 되어야 한다는 이유로 1986년 개정을 통해 "내용"이란 "통신의 실질적 내용, 목적, 또는 의미"라고 규정하였다. 그러나 전체 (full path) URL의 경우 내용을 담고 있는 지로 해석이 될 수 있는지에 대한 논란이 있을 수 있다.

그러나 동 조문은 고용주가 직원의 업무 수행을 위해서 직원이 고객과 통화하는 내용을 모니터링 하는 행위에는 적용되지 않는다.

동 조문의 법적인 예외로써 유선 또는 전자통신서비스를 위해 시설이 사용되고 있는 스위치보드의 운영자, 직원, 또는 유선 또는 전자통신서비스 제공자의 대리인이 서비스를 제공하기 위해 필요한 행위이거나 또는 그 서비스 제공자의 권리 또

는 재산을 보호하기 위해서 통신을 도청하거나 밝히는 행위는 불법이 아니라고 명시하였다. 그러나 서비스 제공자의 권리나 재산을 보호하기 위한 예외는 사기나 서비스의 도난을 막기 위해서 협의로 적용되어야 한다. 예를 들어 이동통신서비스 제공자가 대포폰의 유래를 추적하기 위하여 대포폰의 통화 내용을 도청하는 행위에 대해서 법원은 허락된 행위라고 판단하였다.[139] 그러나 위의 예외가 서비스 제공자가 제한 없는 모니터링을 할 수 있도록 허용한 것은 아니다. 예를 들어 불법으로 장거리 전화를 사용하고 있는 사용자의 경우 통신사가 불법 장거리 통화가 시작된 후 2분씩 도청한 것은 법에서 허용된 행위라고 판단하였다.[140] 서비스 제공자가 권리와 재산의 보호와 서비스 사용자의 사생활의 보호 사이의 균형을 위한 적절한 모니터링만 허락된 것으로 보아야 한다.

서비스 제공자가 경찰의 요청에 의해서 권리와 재산을 보호하기 위해 통화 내용을 경찰에 제공한 경우에도 법원은 법에 명시된 절차를 이행했는지 자세히 살펴보았다. 한 사건에서는 대포폰의 사용자가 전화회사에게 납치 사건의 조사와 관련하여 경찰의 부탁을 받고 통신서비스 제공자에게 통화 내용을 도청한 사건에서 법원은 통신 회사가 원고의 전화 내용을 도청하였을 당시 통신 회사가 정부의 대리인으로써 행동하고 있었는지에 대한 사실에 대한 논의가 있기는 하지만, 동 조문에서 명시하고 있는 법적 절차를 따르지 않고 경찰에서 서비스 제공자에게 통신 내용을 제공할 것을 요청하여 통신 도중에 도청하는 것은 허락되지 않는다고 명시하였다.

자. PEN REGISTER ACT

PEN REGISTER는 1984년 「전자통신보호법(ECPA)」의 일부로 제정되었을 때에는 특정 전화번호로부터 건 모든 번호를 기록하는 전자장치를 의미하였으나 2001년 소위 미 「애국법」을 통해 그 의미가 인터넷 통신을 기록하는 장치로까지 확대되었다. PEN REGISTER는 TRAP AND TRACE장치와 비슷한 기능을 하는 기구로 TRAP AND TRACE 장치는 특정 번호로 걸려온 전화번호를 기록하는데 반해

139) United States v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997)
140) United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)

PEN REGISTER는 특정 번호로부터 건 전화번호를 기록한다. 기술이 발전한 지금은 전화 통신, 인터넷 통신, 모두 이 두 기능을 합친 의미로 사용된다.

1967년의 미 대법원에서[141]에서 Wiretap을 사용하기 위해서는 수색 영장이 필요하다고 판결하였으나, 10년 뒤 다시 대법원에서 Pen Register는 수색이 아니라는 판결을 내림으로써[142] Pen Register의 사용은 헌법의 보호 밖에 있게 되었다. 그래서 1986년 「전자통신보호법(ECPA)」를 통해 사적인 영역과 수사를 위한 영역, 둘 다에서 Pen Register 기기를 사용하는 것을 제한하도록 하였다. 그래서 사적인 영역에서는 일반적으로 Pen Register를 사용하는 것이 제한되어 있고 예외적으로 통신을 제공하는 사업체에서 사업이 적절하게 운영되고 있는지를 확인하기 위한 기능으로서만 사용할 수 있다. 그리고 수사 영역에서 감시를 위해서 Pen Register를 사용하기 위해서는 법원의 허락을 받아야 하는데 이 경우 Pen Register를 사용하여 얻는 정보가 진행되고 있는 범죄의 수사와 연관이 있다는 것만 증명하면 된다. 이 요건은 ECPA의 세 조항 중 법원의 허락을 받는데 가장 낮은 기준을 요구하는데 그 이유는 Pen Register를 통해서는 통화 내용이 아니라 통화 기록에 대한 정보를 받게 되므로 프라이버시를 덜 침해한다는 이유이다.

미 정부가 PEN REGISTER ACT가 계속 존재하고 또한 인터넷 통신에도 적용이 되도록 하는 데에는 중요한 이유가 있는데 만일 PEN REGISTER ACT가 없다면 정부가 인터넷서비스 제공자에게 통신기록을 제공하라는 명령을 내릴 수 없고, 정부로서는 사기업보다 기술력이 떨어지는 경우가 대부분임에도 불구하고 정부의 장비와 소프트웨어, 기술, 그리고 비용을 이용하여 통신기록을 모니터링 해야 하기 때문에 정부로서는 PEN REGISTER ACT가 유용한 수단일 수 있다. [143]

5. 2009 사이버보안 법안[144]

「2009 사이버보안 법안(Cybersecurity Act of 2009)」는 2009. 4. 1일 민주당 상원의원 제이 록펠러(Jay Rockefeller)와 빌 넬슨(Bill Nelson), 그리고 공화당 상원의

141) Katz v. United States 389 U.S. 347 (1967)
142) Smith v. Maryland, 443 U.S. 735m 744 (1979)
143) PEN REGISTER, Wikipedia, http://en.wikipedia.org/wiki/Pen_register
144) http://www.govtrack.us/congress/billtext.xpd?bill=s111-773

원 올림피아 스노위(Olympia Snowe) 등의 공동 발의로 「백악관 내 국가사이버보안자문관실 설립을 위한 법안[145](A Bill to Establish, within the Executive Office of the President, the Office of the National Cybersecurity Advisor)」과 함께 미국 상원에 제출되어 현재 논의 중인 법안이다.

동 법안의 발의자들은 동 법안의 목적이 미국 내에서의 상거래의 자유로운 흐름의 보장, 사이버상의 통신 보안 확립을 통하여 국제 교역 파트너들과의 자유로운 거래 보장, 상기 목적을 위한 인터넷과 인트라넷 통신의 지속적인 개발과 이용 제공, 사이버위협에 대한 효과적인 사이버 보안 방어를 유지하고 증진시키기 위한 정보기술 전문가 양성이라고 밝히고 있으나, 동 법안이 발의되자 많은 반론이 제기되고 있다.

대표적인 문제점으로 지적되는 것은 동 법안이 대통령에게 사이버 비상사태를 선포하고 국가보안을 위해 비상시에 불가결한 정보 네트워크에서의 인터넷 트래픽을 정지시키거나 제한할 수 있는 권한을 부여하면서 비상시에 불가결한 정보 네트워크나 사이버 비상사태에 대한 정의도 없이 그러한 해석이 대통령에 달려 있다는 것이다. 더불어 동 법안은 상무부장관에게 접근을 제한하는 기존의 법령규정이나 정책과는 별도로 비상시에 불가결한 정보 네트워크 관련 자료에 대한 접근을 인정하고 있는데 이로 인해 프라이버시 법령을 무시하고 사적 또는 공적 네트워크에서 자료에 대한 통제와 접근이 가능하다는 것이다.[146]

이하에서는 「2009 사이버보안 법안」 중에서 컴퓨터 네트워크와 인터넷상의 정보처리 및 유통과 관련된 주요한 내용을 발췌하여 소개하도록 하겠다.

가. 사이버보안 자문위원단 설립[147]

---

145) http://www.govtrack.us/congress/billtext.xpd?bill=s111-778
동 법안에 따르면 국가사이버보안자문관은 대통령이 임명하고 상원의 인준을 받도록 되어 있다. 국가사이버보안자문관은 사이버보안 관련 미국 법령 집행에 대한 대통령 자문 및 조언, 다른 법령규정이나 정책에도 불구하고 사이버 구획 또는 특별접근프로그램에 대한 접근권 인정, 행정관리예산국에 제출되는 사이버보안 관련 예산요구 검토 및 승인, 연방 정부부처 및 기관 등에 대한 사이버보안 관련 자문과 자원의 활용 등 막강한 기능과 권한을 부여받는다.

146) Steve Aquino, "Should Obama Control the Internet?", 2009. 4. 2. http://www.motherjones.com/politics/2009/04/should-obama-control-internet, 2009. 8. 15일 23시 현재 245개의 댓글이 붙어 있을 정도로 활발한 논쟁이 이루어지고 있다.

147) 법안 제 3조

대통령은 산업계, 학계, 비영리조직, 이익집단, 지원조직, 주와 지방정부의 전문가 중에서 적임자를 위원으로 위촉하며, 사이버보안 자문위원단[148]은 국가 사이버보안 프로그램과 전략 관련 문제에 대해 대통령에게 자문하고, 그러한 것들을 평가하며 매 2년마다 평가결과를 보고한다.

나. 실시간 사이버보안 경보[149]

상무부장관은 행정관리예산국과 협의하여 동 법 발효 후 90일내에 상무부에 의해 관리되는 모든 연방정부 정보시스템과 네트워크의 실시간 사이버보안 상태와 정보 취약성 등을 제공할 시스템을 집행할 계획을 개발하고 동 법 발효 후 1년 이내에 동 계획을 집행한다.

다. 주 및 지역 사이버보안 증진 프로그램[150]

상무부장관은 사이버보안 표준의 증진과 집행을 위한 지역 사이버보안센터의 설립을 지원하며, 동 센터의 목적은 미국 중소규모의 기업체들의 사이버보안을 증진시키는 것이다. 재정지원을 받는 각 센터는 상무부장관이 위촉하는 평가위원단으로부터 3년마다 평가를 받는다.

라. 국립표준기술원(NIST)의 표준개발 및 표준의 준수[151]

국립표준기술원(NIST)은 동 법 발효 후 1년 이내에 모든 연방정부 및 연방정부와 계약을 맺은 자, 그리고 민간사업자 등이 운영하는 주요 기반시설 정보 시스템과 네트워크들을 측정하고 감사할 수 있는 사이버보안 표준을 개발해야 한다. 표준 마련의 대상으로는 사이버보안 매트릭스 연구, 보안 통제, 소프트웨어 보안,

148) Cybersecurity Advisory Panel
149) 법안 제 4조
150) 법안 제 5조
151) 법안 제 6조

Software Configuration Specification Language, Standard Software Configuration, Vulnerability Specification Language, 모든 소프트웨어에 적용되는 국가 준수 표준 등이 있다.

국립표준기술연구원(NIST)은 현실에 부합하는 시스템이나 네트워크의 지정과 표준 마련을 위해 기존의 법령 규정과는 별도로 국가 보안 시스템으로서의 정보 시스템이나 네트워크를 지정하고 표준을 마련하며 표준의 준수를 집행한다.

마. 사이버보안 전문가 면허 및 인증[152]

동 법 발효 후 1년 이내에 상무부장관은 사이버보안 전문가들에 대한 국가 면허, 인증, 주기적인 재인증 프로그램을 개발, 조정, 통합해야 한다.

바. 민관 정보 교환센터[153]

상무부는 연방정부와 주요 기반시설 정보 시스템과 네트워크를 소유하는 민간 부문을 위해 사이버 위협과 취약 정보에 관한 교환센터(Public-Private Clearinghouse)로서의 역할을 한다. 상무부장관은 다른 법령이나 접근을 제한하는 정책과 관계없이 네트워크 관련 자료에 접근이 가능하고, 연방정부와 네트워크 운영 및 관리자 사이에 사이버 위협과 취약 정보의 공유를 관리하며, 주기적으로 의회에 위협 정보에 대한 보고를 한다.

사. 사이버보안 의무 및 권한[154]

1) 대통령은 동 법 발효 후 1년 이내에 장기적인 국가 사이버보안 청사진을 담은 종합적인 국가 사이버보안 전략을 개발하고 집행해야 한다.

2) 대통령은 사이버 비상사태를 선포하고 연방정부나 미국의 주요 기반시설 정보

152) 법안 제 7조
153) 법안 제 14조
154) 법안 제 18조

시스템이나 네트워크의 인터넷 트래픽을 제한하거나 정지시키는 명령을 발할 수 있다.

3) 대통령은 사이버보안 비상사태 선포에 의해 영향을 받는 연방정부나 미국의 주요 기반시설 정보시스템이나 네트워크의 반응과 복구를 조정할 권한을 갖는 기관을 지정할 수 있다.

4) 대통령은 적절한 정부부처나 기관을 통해 사이버보안 공격 후에 필요한 대책을 평가하고, 전략을 개발한다.

5) 대통령은 연방정부와 미국의 주요 기반시설 정보시스템이나 네트워크의 관련성을 주기적으로 검토하고, 그러한 과정의 효율성을 평가할 매트릭스를 개발한다.

6) 대통령은 국가보안을 위해 어느 연방정부와 미국의 주요 기반시설 정보시스템이나 네트워크와의 접속차단을 명할 수 있다.

7) 대통령은 과학기술정책국을 통해 모든 연방 사이버 기술연구와 개발투자에 대한 연례보고를 감독한다.

8) 대통령은 국가 사이버보안 실태를 개선하기 위하여 적절한 연방 공무원에게 원래의 분류 권한을 위임할 수 있다.

9) 대통령은 적절한 정부부처나 기관을 통해 사이버보안 관련 연방 전문가 책임을 규정한 규칙을 공표하고, 의회에 그러한 규칙의 연방기관 준수에 대한 연례보고를 한다.

10) 대통령은 연방규칙을 위반할 경우, 추가보상을 보류하고, 연방직원에 대한 행동 교정을 명하고, 그런 조치를 취한 후 48시간 이내에 의회에 보고해야 한다.

11) 대통령은 미국시민에게 사이버 관련 법적 자격을 부여한 후 48시간 이내에 의회에 통지해야 한다.

아. 합동 정보위협 평가[155]

국가정보국장과 상무부장관은 사이버보안 위협, 주요국가정보의 취약점, 통신, 데이터 네트워크 기반시설에 관한 평가 및 보고를 매년 의회에 제출해야 한다.

---

155) 법안 제 20조

6. 연방정부의 정보보안관리에 관한 법률(FISMA[156])

「연방정부의 정보보안관리에 관한 법률(FISMA)」은 각 연방정부의 부처들이 정보와 정보시스템을 보호하고 부처의 업무와 자산을 보호하기 위하여 각 부처별로 필요한 프로그램을 고안하고 적용할 것을 요구하고 있다.

FISMA의 목적은 각 연방정부의 부처들과 국가표준기술연구원(NIST: National Institute of Standards and Technology), 그리고 예산관리처(OMB: Office of Management and Budget)에게 정보 시스템 보안을 위한 특정 책임을 부과하고 긴밀하게 연결된 연방정부의 네트워크를 인식하고 적절한 보안 프로그램을 채택할 것을 요구하고 있다. FISMA는 연방 정부의 정보보안에 관한 법률이기 때문에 본 보고서에서는 생략하도록 한다.

7. 사이버보안에 관한 미하원에서의 증언[157][158]

2009년 6월, 미국의 Government Accountability Office (GAO) 는 미 하원의 과학기술위원회 소속의 "기술과 혁명 세부위원회"에서 미 국토안전부가 주관하고 있는 사이버 보안에 대한 감사보고서를 발표하였다. 이 보고서는 주로 미국 연방정부의 중요한 정보와 정보시스템의 보호에 중점을 두고 있지만 연방 정부의 정보시스템의 보호뿐만 아니라 사기업의 인터넷 장애의 복구를 위해 미 국토안전부에 제안하는 내용이 있어 간단하게 언급하고자 한다.

이 보고서는 미 국토안전부의 주도로 행하여지고 있는 사이버보안과 중요한 국가 인프라의 보호에 있어 민관 협력이 부족하다는 것을 지적하고 있다. 또한 보고서에는 2006년도에 행한 미국의 연방정부 시스템, 주 정부 시스템, 외국 정부 시스템, 그리고 사기업의 시스템에 대한 모의 사이버 공격 (Cyber Storm)에 대한 훈

156) Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. §3541, et seq)

157) GAO가 발표한 자료는 http://science.house.gov/에 제공된 자료를 번역 정리하였다.

158) Cyber Security - Testimony Before the Subcommittee on Technology and Innovation, Committee on Science and Technology, House of Representatives

련에서 부족한 것으로 지적되었던 점 중에서 민관 협력뿐만이 아니라 정부 기관끼리의 협력도 부족한 점이 현재까지 개선이 되지 않았다고 지적하며 미 국토안전부가 사이버 공격에 대한 관의 다른 부서와의 협력, 기업과의 협력을 강조하면서 산업별로 적용되는 산업별 사이버 공격에 대한 대응 방안을 강구할 것을 요구하였다. 이 보고서는 또한 민관 협력을 높이기 위해서 정부가 민간 사업자와의 협력을 촉구하기 위한 세금 감면, 또는 자금 혜택 등의 경제적 동기를 사기업에 부여하거나 정부가 부가가치가 높은 서비스, 예를 들어 사이버 위협에 대한 유용한 정보나 분석 자료를 제공할 것을 제안하였다.

8. HSPD-7[159]

2003년도, 부시 대통령 재임시 발효된 대통령령은 미 연방정부의 부처와 기관들이 국가의 중요한 인프라와 주요 자원을 보호하기 위한 계획을 수립할 것과 연방정부, 주정부, 그리고 사기업 간의 공조를 요구하고 있다. 그리고 이 대통령령은 미 국토안전부와 분야별 지정된 기관이 사기업과의 협력을 통해 어떻게 미국의 중요 인프라와 주요 자원을 보호할 것인지에 대한 계획을 세울 것을 요구하고 있다.

9. 미국 주요 인프라 보호 계획[160]

미국 국토안보부(Department of Homeland Security)는 좀 더 안전하고 안정적이며 여러 종류의 외부 위협에 유연하게 대처하여 미국의 중요한 인프라와 주요 자원(critical infrastructure and key resources, 줄여서 CIKR이라고 명칭함)을 보호하기 위한 통합적인 계획으로 2009 National Infrastructure Protection Plan (NIPP)보고서[161]를 발표하였다. 이 NIPP 2009는 2006년도에 준비된 NIPP를 업데이트한 자료로서 미국 영토의 보안을 위한 국가적 전략 (The National Strategy

159) Homeland Security Presidential Directive-7
160) National Infrastructure Protection Plan
161) National Infrastructure Protection Plan by Office of Homeland Security, Sector Specific Plans on IThttp://www.dhs.gov/files/programs/editorial_0827.shtm

for Homeland Security), 「국토안보법(Homeland Security Act of 2002)」, 사이버 보안을 위한 국가적 전략(National Strategy to Secure Cyberspace), 중요한 인프라와 주요 자원을 보호하기 위한 국가적 전략(National Strategy for Physical Protection for Critical Infrastructure and Key Assets), 미국영토의 보호를 위한 대통령령(Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection)에 그 근간을 두고 있다.

NIPP 2009 보고서는 다시 17개의 각 분야 별 보고서로 나뉘고 각 분야 별 보고서에는 미국의 연방정보와 지방정부, NGO들과 기업들의 협력을 통해 "위험"에 대한 정의를 내리고 위험을 관리하는 절차와 방법을 적고 있다. 이 보고서는 미 국토안보부(Department of Homeland Security)와 정보기술에 대한 정부 협력 기구(Information Technology Government Coordination Council, "ITGCC")의 멤버들과 협의된 내용을 담고 있으며 ITGCC에는 미국 상무부, 국무부, 법무부, 내무부, 재정부, 예산관리처, 국가정보처 등이 포함되어 있다. 이 보고서는 위험관리를 통한 예방과 보호, 정확한 상황분석, 미국의 정보기술인프라에 대한 위협에 대한 대응, 복구를 통해 자국의 보호를 강화하는 내용을 담고 있다.

여기에 참가한 회사들은 ISACs (Information Sharing and Analysis Centers)라고 알려진 기구의 실무 회사들로서 회원사들은 현존하는 위험과 미래의 위험, 그리고 운영상의 위험을 줄이고 관리하는 방법에 대해서 논의한다.

Homeland Security Presidential Directive 7 (HSPD-7)에 명시된 중요 인프라에 대해서는 ISAC 멤버들이 인프라의 물리적 재해가 있거나 사이버 테러 등의 위협이 있을 때 함께 방안을 논의하고 위험에 대처하는 방법을 연구한다. NIPP 2009의 회원인 ISAC이라는 기구는 금융 분야 ISAC (Financial Services ISAC), 교통 분야 ISAC (Transportation ISAC), 정보기술 분야 ISAC (IT-ISAC), 통신 분야 ISAC (Telecom ISAC, 또는 National Communication System이라고 알려짐) 등, 각 분야의 ISAC들로 구성되어 있다. 이 각각의 ISAC들은 사이버 위협이나 물리적인 위협이 있을 때 각 네트워크 운영자와 소유자들이 함께 대응방안을 논의하고 정보를 공유하도록 하는 논의 기구이다.

각 산업 분야 별로 별도의 ISAC이 존재하는 이유는 네트워크의 구성과 성격이

다르고 또한 위협이 다른 네트워크를 정부가 요구하는 한 가지 방법으로는 효율적으로 보호할 수 없기 때문이다. 이에 미국 정부는 기업들의 전문성과 산업별 차이점을 인정하고 각 산업 별로 ISAC를 구성하였고, 정부와 민간의 공조가 중요하다는 것을 인식하고 각 산업 별 ISAC와 민관공조를 통하여 사이버 보안을 이루고자 하였다.

미국 정부의 예에서 보듯이 너무나도 광대한 여러 종류의 산업들과 여러 종류의 네트워크 타입을 고려할 때 정부가 한 가지 방법을 채택하여 모든 산업에 적용하도록 하는 것은 부적절한 것으로 보인다. 그 이유는 통신 산업에 맞는 사이버보안 솔루션이 금융 산업에 적절하지 않을 수 있고, 마찬가지로 교통 산업, 식수 산업 등 각 산업의 네트워크 환경에 따른 적절한 위협에 대한 대처 방법이 필요하기 때문이다. 그래서 가장 이상적인 것은 각 네트워크의 운영자가 각 네트워크에 가장 적절한 방법으로 사이버 위협에 대처하도록 하고 정부는 민관 협조가 이루어질 수 있는 환경을 제시하는 것이라고 할 수 있다.

10. 사이버공간 정책 검토 보고서[162)]

2008년 11월, 미국의 오바마 대통령 인수위원회가 준비한 사이버공간 정책 검토 보고서(Cyberspace Policy Review)에는 당시 미국 정부의 사이버보안에 대한 현황과 문제점, 그리고 사이버보안을 개선하기 위한 제안 등을 담고 있다. [163)]

사이버 공간 정책 검토 보고서(Cyberspace Policy Review)에서는 현재 미국의 사이버보안에 대한 문제점으로 다음과 같은 점을 지적하였다.

- 미국에서는 사이버보안에 대한 책임이 너무 여러 부처와 기관에 분산되어 있고,
- 업무가 겹치는 부서도 있으며 반면에 어떤 부처도 부처끼리의 마찰에 대한 일관된 해결책을 내놓을 수 있을 만큼 권한을 가지고 있지 않기 때문에 점점 증

162) Cyberspace Policy Review
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

163) Cyberspace Policy Review는 미국 정부의 사이버보안에 대한 현황과 문제점, 그리고 제안을 담고 있지만 사이버보안에 대한 총체적인 보고서라는 점에서 우리에게도 많은 시사점이 있으므로 꼭 일독을 권한다.

대하고 있는 사이버보안에 대한 효율적인 대응책을 세우지 못하고 있으며,

- 그렇기 때문에 정부가 총체적인 접근과 비전을 가지고 사이버보안에 대한 경쟁적인 관계에 있는 이익 집단을 통일할 필요가 있다고 제안한다.
- 정보와 통신 네트워크의 많은 부분이 미국 기업 또는 다국적 기업들에 의해 소유되고 운영되고 있다는 사실을 감안할 때 사이버보안은 국가의 주도만으로는 이루어질 수 없고 민관 협조와 국제적인 공조와 국제적 기준을 마련하는 것이 반드시 필요하다고 지적한다.
- 또한 미국 정부가 사이버보안과 위협에 대한 사용자들의 인식을 제고하기 위한 노력과 동시에 개인정보보호와 헌법에서 보장된 시민의 자유를 고려한 통합된 접근을 하도록 제안하였다.
- 정부가 사이버보안의 취약점에 대응하고 동시에 미국의 경제적, 국가적 보안에 대한 요구를 충족시킬 수 있는 연구에 더 많은 투자를 할 것을 촉구하고 있다.

11. 소결

미국의 사이버보안에 대한 연방법과 미국정부 보고서를 살펴본 결과 미 연방법에서는 타인의 컴퓨터나 네트워크에 접근하여 타인의 컴퓨터나 시스템에 손상을 입히는 여러 행위들을 규정하되 사생활의 보호와 범죄의 방지와 처벌이라는 두 가지 가치의 공존을 위한 균형을 조심스럽게 찾고 있다. 정부보고서에서는 미 정부가 강력한 리더십을 가질 것을 제안하지만 정부의 일방적인 주도에 의한 사이버보안보다는 정부와 민간기업의 공조를 통한 사이버 보안을 이룰 것을 촉구하고 있다.

정부의 일방적인 주도에 의한 사이버보안은 사생활의 보호, 정부의 지나친 규제라는 업계와 시민단체의 반발, 그리고 인터넷의 특성인 개방성을 고려할 때 정부가 의도하지 않았던 사업의 제한 등, 필요치 않은 부작용과 오해를 나을 수 있다. 그러한 우려 때문에 다른 나라의 경우 좀비나 웜에 감염된 컴퓨터가 숙주로 활동하는 것을 방지하기 위한 방법으로 정부가 주도적으로 감염된 컴퓨터를 찾아내기

보다는 각 ISP들과 사용자 간의 최종사용자계약을 통해 사용자가 악성코드나 악성 소프트웨어를 타인에게 전달하지 않고 컴퓨터를 안전하게 사용할 계약 조건으로 서비스를 제공하는 방법을 택하였다.

미 국토안보부도 시스템 네트워크의 보안을 위한 여러 가지 방안을 제안하고 고려하였지만 아직까지 사용자의 컴퓨터에 최신 백신 프로그램이 설치되어 있는지 확인하는 방법은 고려하지 않았다고 한다.[164]

미국의 자율규제 환경을 살펴보면, 정부주도의 규제보다는 모범 사례의 발굴 및 홍보를 통하여 사용자 보안을 추구하는 것이 보다 효율적이라는 미국 정부의 인식을 엿볼 수 있다. 그 어떤 분야보다도 발전의 속도가 빠른 IT산업의 특성상, 정부는 네트워크의 위험을 줄이고 치명적인 의존 상태가 어디에 있는지 찾아내어 위협을 감소시킬 수 있는 방법을 제시하는 역할에 충실하고, 그 구체적인 적용에 대해서는 각 산업별로, 그리고 서비스제공자별로 모범 사례를 찾아서 널리 장려하는 방법이 효과적이라고 미국 정부는 본 것이다.

NIPP 2009 보고서 역시, 채택 가능한 모든 보안 방법을 적용할 것을 모든 네트워크들에게 요구하고는 있지만 정부가 ISP들을 통하여 사용자 환경을 모니터링 할 것까지 요구하지는 않았다. 정부 주도의 규제 방식, 특히 정부가 주체가 되어 사용자 컴퓨터 사용 환경을 모니터링 하는 방식에는 사용자와의 "신뢰 모델"을 깨뜨릴 수 있다는 위험이 상존하며, 그러한 경우 정부로서는 "사생활의 보호"와 "정부와 사용자간 신뢰 구축"이라는 두 가지 문제를 해결해야 하는 부담을 안게 된다. 그러한 이유로 미국 정부는 "신뢰 모델"과 "사후 조치 모델"이라는 기조를 취하게 된 것이다.

충분한 사용자 교육을 전제로 하여, 업계의 자율적 규제를 보충하고 사후 처벌을 위한 수단으로 사용될 때 정부 규제는 그 효과를 극대화할 수 있을 것으로 보인다.

---

164) Microsoft Inc.의 보안담당 변호사 Cristin Goodwin과의 회의 내용을 참조하였다.

제3절 일본의 정보통신망 정부규제 현황

1. 서론 - 일본의 정부주도의 정책 개관

일본 정부의 정보통신망 분야에서의 정부규제정책은 다양하게 전개되고 있지만, 여기서는 크게 나누어 정보시큐러티분야와 위법·유해정보에 대한 대응정책으로 분류하여 고찰한다.

가. 정보보호 분야

일본의 정보보호 문제에의 대응은 2005년 4월에 내각관방에 정보시큐러티센터(이하 'NISC'[165]라고 함)가, 그리고 동년 5월에 고도정보통신네트워크사회 추진전략본부(이하 'IT전략본부'라고 함)에 정보시큐러티정책회의가 설치되면서 발본적인 강화가 개시되었다.

구체적인 강화책은 e-Japan 중점계획 등의 일부인 정보시큐러티의 문제를 개별 중점적으로 파악한 후, 전략적 사고에 근거한 체계적인 계획을 구축 하는 것이었다.

즉, 2006년도부터 2008년도까지의 3개년 중장기 전략인 제1차 정보보호 기본계획(이하 '제1차 기본계획'이라고 함)의 책정이라는 형태로 결실된 것이다. 이후 NISC가 주도적인 역할을 담당하는 형태로 官民의 각 주체에 의해 2년 이상에 걸쳐 여러 가지 대응책이 전개되어 충실한 대책을 마련하여 실시해 오고 있다.

한편 최근의 사회정세는 증권거래시스템이나 금융기관의 현금자동입출금기, 자동개찰시스템 등에서의 장애의 발생, 부정액세스에 의한 카드정보의 대량 절취, 파일공유 소프트 및 컴퓨터 바이러스에 의한 중요 정보의 누설 등 이미 사회 기반화되었다고 할 수 있는 정보기술(이하 'IT'라고 함)을 이용·활용하는데 있어서의 리스크가 여전히 존재하고 있다.

또 봇 넷(BotNet)[166] 등에 의한 위협이 심각해지고, 소셜 엔지니어링을 구사하여

165) National Information Security Center의 약칭임.

166) 봇넷이란 보트라 불리는 바이러스의 일종이 구성하는 네트워크의 총칭으로, 수백~수만대의 규

특정 조직·개인을 노리는 표적형 공격(스피아형 공격)과 같은 공격 수법 등 새로운 리스크도 날마다 발생하고 있다. 게다가 사회에서의 IT 활용 방법은 예를 들면, 지상파 디지털 방송의 전개와 함께 가전 이용에서 네트워크 활용이 국민 생활에 있어 지극히 중요하게 되고 있는 것이나, 자동차내비게이션의 네트워크 접속의 진전이 일반화되어 있는 것, 일상생활에 필요한 행정 절차의 전자화 추진 등 해마다 진화를 이루어 제1차 기본계획 책정시와는 크게 변화되고 있다. 이러한 상황에 맞추어 정보 시큐러티가 대상으로 해야 할 사정도 변화되고 있는 것이다.

그렇기 때문에 제1차 기본계획에 근거한 각종 대응의 진전이나 사회 환경의 변화 등을 근거로 하여 계속해서 일본 전체적으로 정보시큐러티 문제에 대한 대응을 강력하게 추진하기 위해서 2009년도 이후를 염두에 둔 제2차 정보보호 기본계획(이하 '제2차 기본계획'이라고 함)을 책정하게 되었다. 정보시큐러티에 대해서는 중장기적 시점에서 본 계속적인 대응이 필요한 한편, 이것을 둘러싼 환경 변화가 현저한 것을 근거로 제2차 기본계획기간에 관해서는 제1차 기본계획과 같이 3년간(2009년부터 2011년까지)을 대상으로 한다.

그리고 향후 제1차 기본계획시의 대응과 같이 이 기본계획에 근거하여 2009년부터 연도 마다 추진 계획을 책정하는 것으로 한다.

제2차 기본계획은 제1차 기본계획아래에서의 대응 상황, 정보보호 정책회의에 설치된 기본계획 검토위원회의 제1차 제언, 동 제언을 감안한 정부에서의 대응, 마찬가지로 정보보호 정책회의에 설치된 중요 인프라 전문위원회에서의 검토 등을 근거로 하여 책정되고 있다.

이것에 의해 제2차 기본계획아래에서의 정보보호 정책의 대응은 이 기본계획을 정책 전체의, 즉 전체 설계도로 하여 그 아래에 정부기관 분야, 중요 인프라 분야, 그리고 정책 전체의 평가 등에 관한 문서가 개별 설계도로서 합쳐지는 형태로 이루어지게 된다. 개별 설계도는 구체적으로는 「정부기관의 정보보호 대책을 위한

모로 구성된다. 봇넷은 통상의 바이러스나 웜과는 달리 HERDER(목부) 또는 MASTER로 불리는 인간의 지시에 의해 DDoS 공격이나 SpamMail의 송신과 같은 다양한 활동을 실시한다. 봇넷의 상당수는 IRC 메커니즘을 사용해 네트워크를 구성한다. IRC 메커니즘을 이용하는 보트를 IRC 보트, IRC 보트로 구성하는 보트 넷을 IRC 봇넷이라고 부른다. 덧붙여 IRC 메커니즘 외에 P2P(Pear to Pear)나 Web 구조를 이용하는 보트도 존재하기 때문에 제어의 중심이 되는 서버를 C&C(Command and Control) 또는 C&C 서버(Command and Control Server)라고 부르는 경우가 많다.

통일 기준」(이하 '정부기관 통일기준'이라 함), 「중요 인프라의 정보보호 대책과 관련되는 제2차 행동계획」(이하 '제2차 행동계획'이라 함), 「시큐어·재팬의 실현을 향한 대응의 평가 및 합리성을 가진 지속적 개선의 추진에 대하여」 및 「정보보호의 관점으로부터 본 일본 사회의 마땅한 모습 및 정책의 평가 - 시큐어 재팬의 실현을 향한 정보보호 정책의 PDCA 사이클 확립에 -」(이하 이들 2문서를 '정보보호 정책 평가 등의 틀 문서'라고 함)의 각 문서가 된다. 이것들은 각각 관계 부성청등에서의 검토나, 중요 인프라 전문 위원회와 같은 전문 위원회에 의한 검토를 근거로 해 책정된 것이며, 전체 설계도가 가리키는 대응의 큰 방향성 등을 구체화하는 것이다.

이러한 정책의 전체 구조 아래에서 전체설계도인 이 '기본계획'에서는 제1장에서 제1차 기본계획아래에서의 대응을 기본이념이나 기본 목표 등을 포함하여 간단하게 되돌아보고, 그 결과, 2009년 현재 어떠한 상황이 되고 있는지를 기술하고 있다. 제2장에서는 제1장에서 정리한 상황을 근거로 하여 제2차 기본계획아래에서 실시하는 대응에 관한 기본이념이나 기본목표 등의 요소에 관해 명확하게 한 후, 제2차 기본계획의 대응 기간 후인 2012년에 어떠한 상황이 된다고 생각하고 있는지를 기술하였다. 그리고 제3장에서는 제2차 기본계획아래에서 정부가 향후 3년간에 대응을 하는 중점 정책에 관해서 기술하는 것과 동시에, 마지막 제4장에서는 이것들을 실현하고, 계속해 가기 위한 정책의 추진 체제를 나타냈다.

덧붙여 2009년의 상황, 2012년의 모습, 중점 정책의 어느 것에서도 기본적으로는 제1차 기본계획아래에서의 대책 실시 4 영역, 횡단적 기반 4 영역의 구조에 따라 분야 마다 기술한다. 다만, 요즈음의 상황을 근거로 하여 2009년의 상황 및 2012년의 모습에 관해서는 자신이 갖는 정보를 다른 주체에 맡기는 주체(정보 제공 주체)에 관해서도 별도로 기술을 한다. 또 중점 정책에서는 정보 제공 주체에 관한 대응은 대책을 실시하는 주체의 대응 중에서 함께 취급하는 것으로 한다.

제2차 기본계획에 있어서의 중요한 메시지의 하나는 "事故前提社會"에의 대응력 강화이다. 이것은 제1차 기본계획아래에서의 대응이 사전 대책에 중점을 두는 형태로 진행된 것을 이어 받아, 만일의 사태에 있어서의 넓은 범위에서의 대응이나 복구의 준비에도 주력하는 것을 의미한다. 물론 계속해서 모든 주체가 정보 시큐

러티상의 문제의 발생을 방지할 수 있도록 사전 대책에 관해 최대한의 노력을 경주할 필요가 있음은 말할 것도 없다. 제2차 기본계획을 통하여 모든 주체는 사전부터 사후까지 일관된 정보보호 대책을 진행시킬 것을 기대한다.

나. 위법·유해정보에 대한 대응정책

1) 배경과 경위

일본에서도 인터넷의 보급이 눈부시고 빠르고, 국민의 사회 활동, 문화 활동, 경제활동 등 모든 활동의 기반(사회적 인프라)으로서 이용되게 되어 국민 생활에 필요 불가결한 존재가 되고 있다.[167] 「언제라도, 어디에서라도, 누구라도」 넷으로 연결되는 유비퀴터스넷 사회가 현실이 되고 있다고 할 수 있다. 본격적인 고령화 사회(少子高齡化)를 맞이하는 가운데, 국제 경쟁력의 유지·강화를 꾀해 가기 위해서도 인터넷의 유효한 활용은 더욱 더 중요해질 것이다.

한편, 급속한 인터넷의 보급은, 위법·유해 정보의 유통 등 부정적인 측면도 확대시키고 있다.

인터넷상의 위법·유해 정보에 대해서는, 총무성에서도 최근에는 2005년 8월부터 2006년의 8월에 걸쳐 '인터넷상의 위법·유해 정보에의 대응에 관한 연구회'(이하 '연구회'라고 함)를 개최해 아래 그림과 같이 위법·유해 정보를 4개로 분류한 다음[168] 각각의 대응을 검토했다.

위법한 정보	위법하지 않은 정보
(1) 권리침해정보	(2) 공서양속에 반한 정보
**은 섹슈얼해러스먼트를	사람의 존엄을 해하는 정보(사

167) 일본에 있어서의 인터넷 이용 인구는 증가를 계속하고 있어 2007년 말에 있어서의 인터넷 이용인구는, 약 8,811 만명, 인구 보급율은 69%가 되고 있다. (2008년판 정보통신 백서 88면)

168) 「위법한 정보」에 대해서는, 「권리침해 정보」와「그 외의 위법한 정보」로 나누고 있다. 「위법은 아닌 정보」안에 이른바 「유해한 정보」가 존재하지만, 이것에 대해서는 사람을 자살로 유인하는 정보와 같은 「공서양속에 반하는 정보」와, 성인 정보와 같은 「청소년에게 유해한 정보」의 2개로 나누고 있다.

하고 있다(명예훼손) 음악파일(저작권침해) ↓대책 사업자에 의한 정보의 삭제 등 자주적 대응 및 발신자 정보개시에 의한 피해구제를 지원	체화상) 자살을 유인하는 기입 ↓대책 사업자에 의한 약관에 기한 정보의 삭제 등의 自主的 대책을 지원
프로바이더 책임제한법 및 관계가이드라인	「違法・有害情報に 대한 対応 等에 関한契約約款モデル条項」(06年11月)에 基한事業者의 自主的인 対応을 支援

(2) 기타의 위법한 정보 아동포르노·외설물 마약매매의 광고 ↓대책 事業者에 의한 情報의 削除 等의 自主的對策을 支援	(2) 청소년에게 유해한 정보 어덜트·만남계사이트 폭력적인 표현 ↓대책 필터링서비스의 제공을 일층 촉진 總務大臣要請에 基한 모바일필터링의 원칙화(친권자의 의사 확인)
「인터넷상의 違法한 情報에 대한 対応에 関한 가이드라인」	青少年이 安全하고 安心하여 인터넷을 이용할 수 있는 環境의 整備 等에 関한 法律 (平成20年 法律 第79号)

<표3> 인터넷상의 위법·유해 정보에 관한 총무성의 대응

연구회에서는 인터넷상의 위법·유해 정보에 대해서 "행정의 지원의 아래, 전기통신사업자 및 이용자에 의한 자주적인 대응이 촉진되어 표현의 자유에 배려하면서 각자가 인터넷의 편리성을 향수할 수 있는 것 같은 환경의 정비가 바람직하다"고 하고 있듯이,[169] 민간의 자주적 대응을 중심으로서 구체적인 시책을 제언하고

169) 研究會, インターネット上の違法·有害情報への對應に關する檢討會 - 最終取りまとめ, 38面.(이

있어, 그 대부분이 실제로 착수되어 왔다.

가) 중간 정리까지

최근 휴대전화를 중심으로 한 만남계 사이트의 이용에 의해, 18세 미만의 청소년이 범죄에 말려 들어가는 사건이 적잖이 발생하고,[170] 게다가 청소년에 의한 이용이 진행되고 있는 커뮤니티 사이트를 계기로 하여 범죄에 말려 들어간 사안이 널리 보도된 것, 또 이른바 「학교 뒤 사이트」에 있어서의 이지메의 문제가 매스컴을 떠들썩하게 한 것 등에 의해 청소년 보호의 관점으로부터의 문제의 지적이 계속되었다. 또 2007년 9월에는, 휴대전화 인터넷상에 개설된 사이트를 계기로서 결성된 범행 그룹에 의한 愛知 여성 납치 살해 사건과 같이 참혹한 사건의 발생도 있었다.

이러한 상황을 반영하여, 매스컴이나 국회에 있어서의 논의 등에 있어 인터넷상의 위법·유해 정보 대책의 낙후를 지적하는 소리나, 법규제의 도입도 포함한 대응책의 강화를 꾀해야 할 것이라는 소리가 커져 왔다. 이러한 요청에 응하여 「연구회」에서 최종보고를 정리하고 나서 1년 정도 밖에 지나지 않았음에도 불구하고, 2007년 11월부터 총무성에서 '인터넷상의 위법·유해 정보에의 대응에 관한 검토회'를 개최하는 것으로 했다.

이 검토회를 개최하는 한편으로, 총무성은 특히 청소년 보호 대책을 신속하게 강화하기 위해, 2007년 12월에, 휴대전화·PHS 사업자 등에 대해서, 필터링 서비스의 도입 촉진을 강화하는 것에 대하여 총무대신이 요청을 했다. 이 요청에 근거해 휴대전화 사업자 등이 청소년에 대한 필터링 설정의 원칙화에 시급하게 착수한 것을 계기로서 휴대전화 필터링이 안고 있는 제과제가 표면화 되었다.

이것을 근거로 하여 2007년 11월부터 2008년 4월까지의 6회에 걸치는 검토회의 회합은 인터넷상의 위법·유해 정보에의 대응이라고 하는 큰 과제 가운데, 청소년이 사용하는 휴대전화 등에 있어서의 필터링 서비스의 도입 촉진을 꾀하는 것과

하 [최종보고서]로 함)

170) 경찰청 「平成 19년 중의 이른바 만남계 사이트에 관계된 사건의 검거 상황에 대하여」에 의하면, 2007년의 만남계 사이트 관련 사건의 피해자 건수 가운데, 18세 미만의 피해자가 1,100명(약 85%)이 되고 있다.

동시에, 휴대전화 필터링의 과제를 추출해 그것을 개선하기 위한 방책을 검토하게 되었다. 그 성과는, 2008년 4월 25일에 「중간 정리 ~휴대전화 필터링 서비스의 실효성 있는 보급을 목표로 하여~」(이하 「중간 정리」라고 함)로서 검토회에 보고되어 휴대전화 필터링의 도입 촉진에 테마를 좁혀 단·중기적 대응을 제언한다.

인터넷상의 콘텐츠의 평가를 실시하는 제삼자 기관으로서 모바일 콘텐츠 심사·운용 감시 기구(EMA)[171]가 활동을 개시한 것도 근거로 하여 중간정리와 같은 날에, 총무 대신이 휴대전화 사업자 및 PHS 사업자의 4사 등에 대해서 재차 요청을 실시했다. 구체적으로는, 필터링의 도입 촉진에 있어 특정 분류 액세스 제한 방식으로 제삼자 기관의 대응이 반영되도록 하는 것, 친권자의 신고가 없는 경우로 설정하는 서비스는 특정 분류 액세스 제한 방식으로 하는 것, 이용자의 선택사항을 늘리는 서비스 제공의 검토를 실시하는 것 등의 요청이다.

이에 따라 휴대전화 사업자 등은 필터링 서비스의 개선에 착수함과 함께, EMA는 사이트 인정 작업을 개시해 휴대전화 사업자와 인정 리스트의 필터링에의 실장(實裝)에 대해 협의를 하고 있다. 또 별도로 휴대전화 사업자는 이용자의 선택사항을 늘리는 서비스의 실시도 예정하고 있다.

나) 청소년 인터넷 환경 정비법의 제정

상기와 같은 휴대전화 필터링의 도입 촉진의 대응과 그 개선을 향한 검토를 전후하여, 국회에서는 여야당의 쌍방에 대해 인터넷상의 위법·유해 정보 대책으로서 법규제의 도입을 목표로 한 검토의 장이 연달아 설치되었다. 또 지방공공단체에서도 히로시마시와 같이 독자적으로 조례를 제정하는 움직임을 볼 수 있었다.

여야당에 있어서의 법안의 검토 단계에서는, 국가가 유해 정보를 정의하고, 사이트 관리자 등에게 유해 정보의 열람 방지조치를 의무화 하는 등 규제색이 강한 안이 신문지상에서 보도되었다. 이것에 위기감을 가진 학식 있는 경험자나 민간단체는 법 규제 도입 반대의 공동성명을 발표했다. 또 콘텐츠 관련 기업 등도 법규제 도입에의 염려를 표명하는 기자회견을 실시하거나 자사 사이트의 유해 정보

171) Content Evaluation and Monitoring Association의 약자이다.

대책의 강화를 발표하거나 하는 등 민간 측의 움직임이 활발해졌다. EMA 등의 제삼자 기관의 설립도 민간의 자주적 대응을 법 규제에 선행시키려고 하는 시도로서 파악된 면도 있다. 또 사단법인 일본신문협회가 2008년 5월 29일 및 6월 6일에, 사단법인 일본 민간방송 연맹이 6월 2일, 6일 및 11일에 유해 정보의 판단에의 국가의 관여 등을 염려하는 의견을 발표했다.

제169회 국회(상회) 회기 말이 가까워진 5월 하순 이후, 여야당 사이에 각각의 안에 근거한 법안의조정이 급피치로 행해져 6월 6일, 중의원의 청소년 문제에 관한 특별 위원회에 대해 「청소년이 안전하게 안심하고 인터넷을 이용할 수 있는 환경의 정비 등에 관한 법률안」[172](이하 '청소년 인터넷 환경 정비법'이라고 함)이 위원장 제안에 의해 제출되었다. 같은 날, 중의원을 통과해 6월 10일에 참의원 내각 위원회에서의 참고인 질의 및 법안 제출자에 대한 질의를 거쳐 다음 11일에 참의원 본회의에 대해 가결되어 성립했다.

참의원 내각 위원회의 참고인 질의나 법안 제출자에 대한 질의에서는 기본계획이나 필터링 추진 기관의 등록 등에 대해서, 유해 정보의 기준 책정 등에 국가가 관여하는 방향으로 운용되는 것은 아닌가라는 염려가 논의되어 부대 결의에서 정부가 「사업자 등이 실시하는 유해 정보의 판단, 필터링의 기준 설정 등에 간섭하는 경우가 없게 할 것」이라고 한다.[173]

청소년 인터넷 환경 정비법은 인터넷상의 위법·유해 정보 대책 가운데 청소년을 유해 정보로부터 보호하는 것으로 목적을 좁혀, 인터넷의 이용 환경 정비의 본연의 자세에 대해 향후의 대응의 방향성을 명확히 한 것이다. 제3조의 기본이념에 명확히 되고 있듯이, 이른바 「넷 규제」적인 색채는 부족하고, 표현의 자유 등에 배려해, 민간의 자주적 대응이나 리터러시 교육의 중요성을 강조하고 있다. 또 구체적인 유해 정보 대책으로서는 필터링이라고 하는 수단의 보급과 그 성능 향상에 다대한 기대를 걸고 있다.

---

172) 2008년 12월 10일에 공포된 동법 시행령에 의해 2009년 4월 1일에 시행되었다. 동법 부칙 제3조에서는 시행 후 3년 이내에 이 법률의 상황에 관해 검토하고, 그 결과에 기해 필요한 조치를 강구하도록 하고 있다.

173) 「청소년이 안전하게 안심해 인터넷을 이용할 수 있는 환경의 정비 등에 관한 법률안에 대한 부대결의」(2008년 6월 10 일 참의원 내각 위원회)

2) 최종 정리의 목적

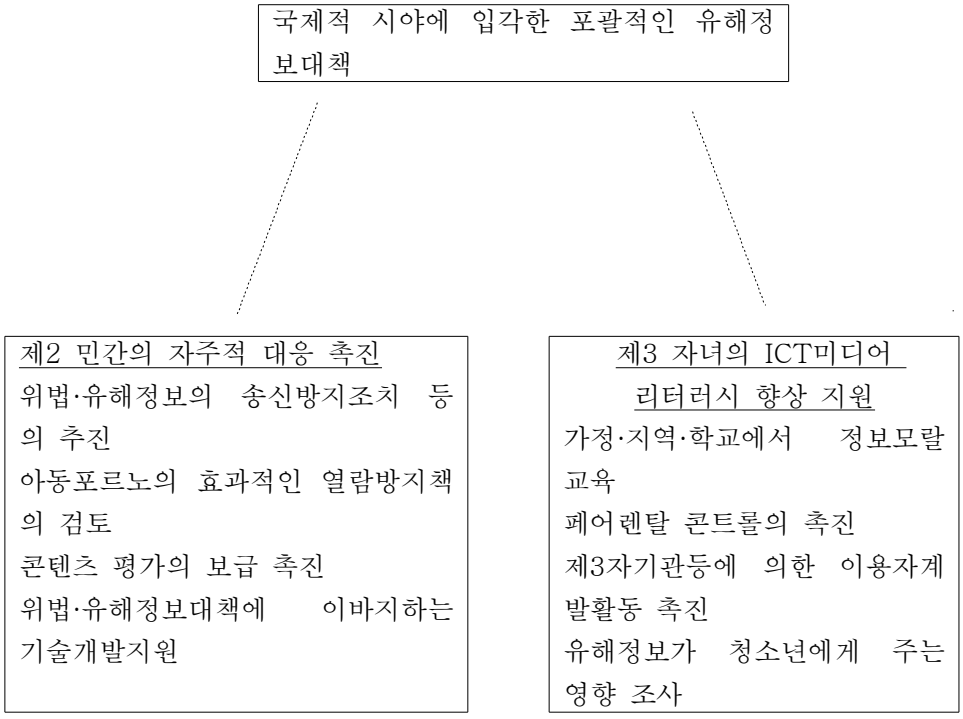
이상과 같이 검토회가 개최된 2007년 말부터 2008년 여름경에 걸쳐, 인터넷상의 위법·유해 정보 대책에 대해서는 사회적으로도 큰 관심을 갖는 과제로서 주목받아 휴대전화 필터링의 도입 촉진을 계기로 한 제삼자 기관의 설립, 「청소년 인터넷 환경 정비법」의 제정 등 지금까지 없던 급격한 변화를 경험했다.

또 「청소년 인터넷 환경 정비법」의 성립 직전에는, 교육 재생 간담회의 제1차 보고가 발표되어 휴대전화를 초등·중학생에게 갖게 하는 것의 是非나 휴대전화 필터링의 한층 더 검토의 필요성이 향후의 주요한 논점으로서 다루어지고,[174] 그 후도 휴대전화 문제에 관한 워킹 그룹이 설치되어 계속적으로 논의를 하고 있다. 게다가 황화수소에 의한 자살 유인 사이트의 문제나, 2008년 6월 8일에 일어난 아키하바라에서의 사건에서의 전자 게시판상의 범죄 예고 등, 인터넷상의 위법·유해 정보 대책으로서 민간의 자주적 대응에 맡기는 것이 아니라, 오히려 규제를 강화해야한다는 소리를 지지하는 것 같은 사안도 계속해 발생하고 있다.

이러한 상황에서 직접적으로는 「청소년 인터넷 환경 정비법」의 성립을 근거로 해 2008년 7월 15일 총무 대신이 '안심 넷 만들기' 촉진 프로그램의 책정에 대해 발표했다. 인터넷상의 위법·유해 정보에의 대응에 대해, 지금까지의 대응을 정리한 다음, 향후의 방향성을 분명히 하는 것을 목표로 한 것이고, 구체적으로는 「청소년 인터넷 환경 정비법」의 기본이념에 근거하는 시책의 전개를 염두에 두고 '안심 가능한 인터넷 환경을 실현하는 기본적 범위의 정비', '민간의 자주적 대응 촉진' 및 '부모와 자식의 ICT 미디어 리터러시 향상 지원'이라는 3개를 축으로 한 종합적인 정책 패키지로 하여 검토회의 최종 정리로 삼은 것이다.

제1 안심을 실현하는 기본적 구조의 정비
안심네트 이용을 위한 기본법제의 정비
국제제휴추진을 위한 구조의 제안
지방공공단체의 대응 촉진
관민실무가 라운드테이블의 지원 등

174) 교육 재생 간담회 「지금까지의 심의의 통계 －제1차 보고-」(2008년 5월 26 일)



<표4> 「안심 넷 만들기」 촉진 프로그램의 구성

이 총무 대신의 발표에 이어서 검토회 제7회 회합에서 「안심 넷 만들기」 촉진 프로그램으로 연결되는 최종 정리를 목표로 하여 검토회 아래에 「기본적 범위 WG」, 「자주적 대응 WG」, 「부모와 자식의 ICT 미디어 리터러시 WG」 및 「기술 검토 WG」의 4개의 WG를 설치해 검토를 하는 것으로 했다. 전술한 3개의 축에 대응하는 WG에 가세해 민간의 자주적 대응의 일환으로서 국가의 기술지원의 본연의 자세를 검토하는 WG를 별도 마련한 것이다.

최종 정리에서 제언한 바는 기본적으로는 총무 대신 발표시에 나타난 「안심 넷 만들기」 촉진 프로그램의 구성을 답습하여 3개의 축에 근거하여 각각의 축에 해당하는 구체적인 시책에 관해 검토하고 있다.

2. 법제의 정비

가. 고도 정보통신 네트워크사회 형성 기본법(IT기본법)

2001년 1월부터 시행된 「IT기본법」에서는 정보통신 기술의 활용에 의해 세계적 규모로 발생하고 있는 급격하고 대폭적인 사회경제 구조의 변화에 적확히 대응하는 것의 긴급성과 필요성에 비추어 고도정보통신 네트워크 사회의 형성과 관해 기본이념(3－9조) 및 시책의 책정과 관련되는 기본방침(16－24조)을 정하고, 국가 및 지방공공단체의 책무(10－12조)를 분명히 하며, 고도 정보통신 네트워크 사회 추진 전략 본부를 설치(25－34조)함과 동시에, 고도 정보통신 네트워크 사회의 형성에 관한 중점 계획의 작성(35조)에 대해 정하여 고도 정보통신 네트워크 사회의 형성에 관한 시책을 신속하고 중점적으로 추진하도록 하고 있다.

동법에서는 국가·지방공공단체와 민간과의 역할 분담(7조)을 정하고 있는데, 민간이 주도적 역할을 담당하는 것을 원칙으로 하고, 국가·지방공공단체는 공정한 경쟁의 촉진, 규제의 재검토 등 고도 정보통신 네트워크 사회의 형성을 저해하는 요인의 해소, 기타 민간의 활력이 충분히 발휘되기 위한 환경 정비 등을 중심으로 한 시책을 실시하도록 하고 있다.

이러한 시책의 기본방침으로서 고도 정보통신 네트워크의 확충 등의 일체적인 추진(16조), 세계 최고 수준의 고도 정보통신 네트워크의 형성(17조), 교육 및 학습의 진흥과 인재의 육성(18조), 전자상거래 등의 촉진(19조), 행정의 정보화(20조), 공공 분야에 있어서의 정보통신 기술의 활용(21조), 연구개발의 추진(23조), 국제적인 협조 및 공헌(24조) 등을 정하고, 특히 고도 정보통신 네트워크의 안전성 및 신뢰성의 확보, 개인정보의 보호 기타 국민이 고도 정보통신 네트워크를 안심하고 이용할 수가 있도록 하기 위해 필요한 조치를 강구하도록 하는 고도 정보통신 네트워크 사회의 안전성의 확보 등(22조)을 기본방침으로 정하여 정보시큐러티의 필요성을 지적하고 있다.

또한 '고도 정보통신 네트워크 사회 추진 전략 본부'(25~34조; IT전략 본부)를 내각에 설치하여 고도 정보통신 네트워크 사회의 형성에 관한 중점 계획('중점계획')의 작성과 그 실시를 추진하며, 고도 정보통신 네트워크 사회의 형성에 관한 시책으로 중요한 것의 기획에 관해서 심의하거나 그 시책의 실시를 추진한다.

나. 부정접속행위의 금지 등에 관한 법률(2000년 2월 시행)

부정 접속 행위의 금지 및 처벌에 관하여 규정하고, 시스템에 대해 방어 조치를 실시하도록 하는 의무를 관리자에게 부과한 법률이다. 이와 동시에 재발 방지를 위한 행정기관의 지원 조치 등을 정하여, 전기통신 회선을 통하여 행해지는 범죄의 방지 및 접근 제어 기능을 통해 전기통신에 관한 질서의 유지를 도모하고, 이를 통해 고도 정보 통신 사회가 건전하게 발전하는 것을 목적으로 하고 있다.

다. 정보보호정책

2000(평성12)년 1월에 발생한 일련의 각 부처 홈 페이지의 개찬 사건에 의해 중앙 부처에서 지금까지의 정보 시큐러티에 관한 대응이 충분하지 않음이 드러났다. 2003년도까지 그 기반을 구축하는 전자 정부의 실현을 위해 정부로서는 정보의 안전성 및 신뢰성을 확보하는 것이 필요 불가결하고, 따라서 체제 정비는 매우 중요한 과제이다.

'해커 대책 등의 기반 정비와 관련되는 행동 계획'(2000년 1월 21일 정보 시큐러티 관계 부처 국장 등 회의 결정)은 이러한 문제에 대한 구체적 조치를 제시하는 것이다. 그 하나의 조치로서 정보보호 대책 추진 회의는 각 부처전용의 '정보 보호 정책에 관한 가이드라인'을 책정하였고, 각 부처는 이 가이드라인을 근거로 2000년 12월까지 정보보호정책을 책정하여 이에 근거한 종합적·체계적인 정보보호 대책을 모색하는 것으로 하고 있다.

3. 정보보호 분야의 정책 수립

가. 제1차 정보보호 기본계획

1) 의의

제1차 기본계획은 일본에서의 정보보호 정책의 시작과 모든 주체에게 '각성을

주기' 위한 전략이었다. 즉, 제1차 기본계획에 의해 정보보호를 IT 관련의 정책 중에서도 개별·중점적인 정책 분야로 시작하고, 이후 정부기관·지방공공단체, 중요 인프라, 기업, 개인 등의 관민의 각 주체가 국민 생활·사회경제 활동에서 의존도가 높아지고 있는 IT의 안전·안심인 이용을 가능하도록 해야 한다는데 지견을 집중시켜 대응해 왔다.

구체적으로는, 관민의 각 주체는 고품질, 고신뢰성, 안전·안심을 실현하기 위해서, 정보 시큐러티상의 문제가 발생하지 않는 수준의 달성을 목표로 하고, 매년도의 연도계획인 "시큐어 재팬(Secure Japan)"에 기하여 적극적으로 대응을 해 왔다.

2) 일본의 국가목표와 정보 시큐러티

제1차 기본계획에서는 'IT의 이용·활용과 국가 목표의 실현'의 관계에서 정보 시큐러티의 자리 매김을 분명히 해 왔다. 구체적으로는, ① IT의 이용·활용을 통한 경제의 지속적 발전, ② IT의 이용·활용을 통한 보다 좋은 국민 생활의 실현, ③ IT의 이용·활용에 의해 발생하는 위협으로부터의 안전 보장에 관련하여, 정보 시큐러티를 'IT기반을 실로 의존 가능하고 강고한 것으로 하기' 위한 것으로서 자리 매김을 하고 있다.

3) 기본이념 - 정보 시큐러티 선진국

제1차 기본계획에서는 "시큐러티 입국"의 사상('고품질, 고신뢰성, 안전·안심'의 대명사로서의 '재팬 모델'의 확립과 그 세계로의 전개를 시야에 넣는 것)에 근거한 대응을 추진하는 것을 주창해 왔다, 그리고 일본의 향후의 본연의 모습을 '정보 시큐러티 선진국'이 되는 것으로 해 왔다.

4) 실현해야 할 기본 목표 - IT를 안심하고 이용 가능한 환경의 구축

일본의 정보보호 분야에서 가장 중요한 목표는 IT이용시에 안전·안심을 확보하는 것이다, 제1차 기본계획에서는 「고도 정보통신 네트워크 사회형성기본법(IT기본법)」 제22조에 주장되고 있는 '고도 정보통신 네트워크를 안심하고 이용 가능한 환경'(이하 'IT 안심 이용 환경'이라 함)의 구축을 기본 목표로 해 왔다. 제1차 기본계획에서는 단지 안전할 뿐 아니라, '예방', '(대책이 시행된 환경의)인식·체감', '사업 계속성'이라고 하는 세 가지 조건을 만족시키고, 이용자가 안심을 실감하면서 IT를 이용·활용할 수 있는 환경을 구축하는 것을 목표로 하고 있었다.
한편, 실제로 제1차 기본계획아래에서 개별 분야마다의 목표나 대응 시책의 상당수는 사전 대책을 염두에 둔 것이었다.

5) 기본 목표의 실현에 있어서의 과제와 해결의 방향성 - 새로운 관민 제휴모델의 구축

제1차 기본계획에서는 IT안심이용환경을 구축하는 때의 과제 해결의 방향성으로서 'IT사회를 구성하는 모든 주체가 정보 시큐러티 문제에 대한 대응의 중요성에 관한 공통의 인식아래 스스로의 책임을 자각하면서 각각의 입장에 따른 적절한 역할 분담아래에서 대책을 실시'하는 '새로운 관민 제휴 모델'의 구축을 제시해 왔다. 그리고 일본 전체적으로 국가적 시야에서 정보 시큐러티 문제에 대응해 가는 것으로 해 왔다.

6) 정보 시큐러티 문제에 대응함에 있어서의 기본방침

제1차 기본계획에서는 일본 전체적으로 국가적 시야에 입각한 정보 시큐러티 문제에 대한 대응을 함에 있어서 자원의 중점적·전략적 투입의 강화를 향한 기본방침을 설정했다. 구체적으로는 '관민 각 주체의 공통 인식의 형성', '선진적 기술의 추구', '공적 대응 능력의 강화', '제휴·협조의 추진'의 4개를 기본방침으로 해 왔다.

나. 제2차 정보보호 기본계획

1) 제1차 정보보호 기본계획 하에서의 대응 결과와 제2차 정보보호 기본계획

일본의 지금까지의 상황을 근거로 하면, 제1차 기본계획에 근거하는 대응은 대개 당초의 계획대로 실현될 수 있었다고 할 수 있다. 그러나 현실의 사회 정세를 보면 대응의 진전에 반해 정보 시큐러티상의 리스크가 반드시 감소하고 있다고 할 수 없다. 리스크는 적어도 기업 간(B to B), 소비자전용(B to C) 전자상거래의 확대나 여러 가지 분야에서의 정보 시스템에 의한 기간(基幹) 업무의 수행 등 IT의 사회기반화가 한층 더 진전됨으로써 보다 대규모적인 사이버 공격이나 IT장애의 발생의 가능성으로, 또 특정 조직이나 개인을 노리는 표적형 공격이나, 검지(檢知)나 감염의 인식이 곤란한 보트로 대표되는 사이버 공격의 교묘화 등에 의해 더욱 눈으로 발견하기 어려운 것으로 변질하기 시작하고 있다.

이 때문에 제1차 기본계획으로부터의 이행에 있어서는 제1차 기본계획 하에서의 대응을 현실을 근거로 하면서 필요한 개선을 꾀하는 것으로 보다 좋은 것으로 만들 여지가 있다.

제2차 기본계획은 이것을 염두에 둔 일본 전체를 조감한 중장기적인 전략이다.

2) 제1차 정보보호 기본계획으로부터의 '계속'과 '발전'

제2차 기본계획은 제1차 기본계획의 '계속'의 관점에서 제1차 기본계획의 정신을 기본적으로 계승한다. 제1차 기본계획 하에서는 정보 시큐러티의 문제가 생기지 않는 수준을 실현할 수 있도록, 예를 들면, 조직에서 미리 기본방침을 정해 대책 추진 체제를 구축하고, 정보 취급이나 기술 대책에 관한 룰을 정해 적절히 운용한다고 하는, 사전 대책에 특히 초점을 맞춘 대응을 추진했던 것이었지만, 이러한 대응은 제2차 기본계획아래에서도 계속해서 실현되는 것이 바람직하다. 그리고 그 실현을 향해 각 주체는 계속 최대한의 진력을 다해야 한다. 특히, 멀웨어(malware)나 부정 액세스에 의한 피해나 개인정보 누설의 발생 등 현시점의 정보 시큐러티 수준으로는 충분하다고 하지 못하여, 대책을 계속 추진하여 수준을 향상

시키는 것이 불가결한 것을 관계자는 충분히 인식하는 것이 필요하다.

한편, 제1차 기본계획으로부터의 '발전'이 필요한 측면도 있다. 예를 들면, 제1차 기본계획아래에서 추구된 수준은 때로는 절대적인 무류성의 추구라고 해도 과언이 아닌 수준이었다. 정보 시큐러티와 관련되는 리스크의 상황에 비추어 보면, 이러한 수준의 사전 대책을 실현하는 것은 현실에서는 용이하지 않다. 실현 가능성이나 결과를 추구하기 위한 코스트와의 밸런스, 정보 시큐러티의 확보와 교환(트레이드 오프)이 될 수 있는 편리성과 밸런스라는 관점을 고려할 필요가 있기 때문이다. 또 이러한 절대적인 무결성을 추구한다고 해도 날마다 정보 시큐러티와 관련된 리스크가 변화하는 가운데 리스크가 현실화될 가능성을 무시해서는 안 된다. 이 때문에 사전 대책을 중심으로 하는 종래의 대응을 계속하여 착실히 추진하는 것이 불가결한 것은 말할 필요도 없지만, 현실에 맞는 대책을 실시할 수 있는 정책 체계를 구축하여 리스크가 현실이 되었을 때에 여러 주체가 보다 실제적인 대응을 취할 수 있도록 대응한다고 하는 시점도 필요하다,

제2차 기본계획은 제1차 기본계획을 이하의 3개의 관점에 근거해 계속·발전시키고 있다.

가) 구체적 대응의 지속적인 추진과 새로운 과제에의 정책적 대응

첫째, 제2차 기본계획아래에서도 제1차 기본계획아래에서의 대응과 마찬가지로 각각의 주체가 노력을 계속할 필요가 있는 것은 말할 필요도 없다.

한편, 제1차 기본계획아래에서의 대응은 정보 시큐러티 분야의 시작이라고 하는 것도 있고, 구체적 대응의 기초가 되는 기반 만들기가 적지 않았다. 제2차 기본계획에서는 관계자는 제1차 계획아래에서 구축된 기반을 활용하고, 구체적 대응을 실제로 기능시켜 가야 하는 것이다.

또 오조작 가능성의 고조와 같은 고령화 사회에 있어서의 IT의 이용·활용에의 불안에 대한 대응이나 사람의 국제적인 이동의 증가나 사업 활동의 국제전개의 증가와 같은 글로벌화 아래에서의 IT이용의 안전·안심의 확보 등 종래 충분한 대응을 해 왔다고 할 수 없는 새로운 과제에의 정책적인 대응을 과감하게 실시하는

것도 필요하다.

나) '사고 전제 사회'에 대한 대응력 강화

둘째, 제2차 기본계획아래에서는 사고가 생길 수 있는 것을 전제로 한 형태에서의 대응력을 강하게 하는 것, 즉 '사고 전제 사회'에의 대응력 강화를 실현한다. 이 때문에 관계자는 사전 대책의 대응에도 불구하고 정보 시큐러티상의 문제가 생겼을 경우를 생각해 사태의 인지·분석, 정보 연락, 신속한 대응·복구 등의 사후 대응에도 충분한 안배를 한다. 즉, 모든 관계 주체는 정보 누설, 정보 시스템 서비스의 기능 저하·정지 등의 정보 시큐러티상의 문제 발생을 방지할 수 있도록 사전 대책에 최대한의 노력을 하면서, 그런데도 만일의 사태가 있을 수 있는 것을 인식하여 이것을 위한 준비를 게을리 하지 않는다. 그리고 만일의 사태에 대해서는 그 영향 범위, 영향의 정도, 긴급도, 원인 등의 사실 관계를 분명히 하면서, 신속한 대응·복구를 널리 진행하는 것으로 사업 계속성을 확보한다.

'사고 전제사회'에의 대응력 강화를 위해서는 사고의 가능성을 완전히 배제하는 정보보호 대책의 실현은 쉽지 않다고 하는 점에 관한 이해를 사회 전체에서 증진할 필요가 있다. 또, 만약 한 문제가 표면화되어도 이를 각성하여 스스로 생각하는 주체가 과민한 반응을 일으키지 않고, 사실을 냉정하게 받아들여 적절한 대응을 신속히 실시하기 위한 대응이 불가결하다,

덧붙여 여기서 '사고 전제사회'란 사고가 있을 수 있기 때문에 단념하여 예방을 위한 대책을 하지 않는다는 것이나, 피해를 당하는 것은 어쩔 수 없는 것이므로 단념한다는 것을 의미하는 것은 결코 아니다.

다) 합리성에서 증명된 어프로치의 실현

셋째, '사고 전제 사회'에서 최적인 수준(항상 계속 변화하는 리스크에 관해, 각각의 주체 및 사회 전체에 객관적으로 허용 가능한 범위 내에서 관리할 수 있는 정보 시큐러티 수준)의 대책을 효과적·효율적으로 실시하는 것, 즉 합리성에서 증

명된 어프로치를 실현한다. 정보 시큐러티의 대응에 의한 안전·안심의 실현에서는 코스트와 효과의 밸런스를 실현하는 것 및 정보 시큐러티의 대응을 진행시켜도 편리성은 없어지지 않고 오히려 정보 시큐러티의 대응에 의해 편리성이 더욱 확고한 것이 되는 것이 유용한 것이기 때문에 이 어프로치는 중요하다,

이때에는 어프로치의 합리성을 유지하기 위해서 아울러 대책의 내용이나 수준에 관한 설명 책임 등을 확실히 완수해야 한다. 구체적으로는 리스크의 파악과 변화하는 리스크에의 유연한 대응을 하는 기능의 강화나, 최적인 대책 수준의 설정, 설명 책임의 명확화라고 하는 대응의 실현이 불가결하다.

3) 제2차 정보보호 기본계획에 있어서의 기본적 사고방식

가) 실현해야 할 기본 목표 - IT를 안심하고 이용할 수 있는 환경의 구축

IT의 이용·활용이 진행되는 가운데, 그 안전·안심을 확보함으로써 사회 전체의 발전을 재촉하는 것은 정보보호 정책의 근본적인 목적의 하나이다. 이 때문에 제2차 기본계획에서도 제1차 기본계획에서 기본 목표가 된 IT안심 이용 환경의 구축을 계속해서 기본 목표로서 중심에 두고, 구축을 위해서 해결이 필요한 정책 과제에 대한 대응을 도모한다.

제2차 기본계획아래에서 여러 주체가 진행하는 대응은 최종적으로는 IT안심 이용 환경의 구축으로 연결되는 것이다.

나) 대응에 있어서의 기본이념

(1) 성숙한 정보 시큐러티 선진국으로

기본 목표의 실현을 위해서는 기본적인 이념, 즉 정보 시큐러티의 관점에서 보아 바람직한 일본 본연의 자세를 염두에 두면서 대응을 해 가야 하는 것이다. 제1차 기본계획에서는 전술한 바와 같이 '시큐러티 입국'사상에 기한 대응을 추진하

고, 일본이 '정보 시큐러티 선진국'이이 될 것을 주장해 왔다.

그러나 "'사고 전제 사회'에 대한 대응력 강화"및 "합리성에서 증명된 어프로치 실현"의 관점도 감안하면서 정보보호 정책을 발전시켜 갈 것을 생각하면 '시큐러티 입국'사상에는 ① 냉정하고 신속한 대응 및 ② 최적 수준 대책의 효과적·효율적인 실시와 설명 책임의 명확화라고 하는 새로운 요소가 더해지는 것이 필요하다. 또 고품질이나 고신뢰성이라고 하는 개념은 제1차 기본계획아래에서는 사실상 추상적으로 완벽을 요구하는 것을 의미해 왔다고 할 수 있지만, 제2차 기본계획에서는 보다 현실에 입각해서 정보 시큐러티상의 문제가 발생하지 않게 하기 위해 주체 마다 요구되는 최적 정보 시큐러티 수준을 달성할 수 있는 높은 수준의 품질이나 신뢰성이라고 생각해야 한다.

정보 시큐러티에 관해서 제2차 기본계획아래에서 목표로 해야 할 일본의 본연의 자세는 정보 시큐러티상의 문제가 발생하지 않게 하기 위한 최적 수준의 대응과 결과의 실현이기는 해도 절대적인 무결성의 추구는 아니다. 오히려 '냉정하고 신속한 대응, 최적 수준 대책의 효과적·효율적인 실시와 설명 책임의 명확화, 주체 마다 요구되는 최적 정보 시큐러티 수준을 달성할 수 있는 고품질이나 고신뢰성, 이용자의 안전·안심의 확보'라는 '시큐러티 입국'사상의 성숙에 의한, 보다 현실에 입각하여 실효적인 정보보호 대책이 냉정하게 실현되는 '성숙한 정보 시큐러티 선진국'이다. 덧붙여 이른바 정보 약자나 고령자 등 정보 시큐러티에 관련된 대응을 스스로 실시하고 싶어도 충분히 할 수 없을 가능성이 있는 주체에 관해서는 최적 정보 시큐러티 수준을 달성할 수 있도록 지지해 가는 것도 중요하다.

(2) IT시대의 강력한 '개인'과 '사회'의 확립을 위하여

성숙한 정보 시큐러티 선진국의 실현을 염두에 두면서 정보보호 대책을 진행시키려면 여러 가지 측면에서의 대응이 필요하다. 이 대응은 IT와 관련되는 기술이나 제도 측면의 구체적인 대책이 기본이 된다.

그러나 이것들에 더하여 정보보호 대책을 실시하면서 IT를 이용·활용함에 있어서는 국민이나 개개의 주체의 모임에 의해 성립되는 사회 전체의 의식 개혁도 불

가결하다. 즉, 일본 국민이나 사회가 시큐러티에 관한 절대적인 무류성의 추구로부터는 탈각하여, 첫째, (대책과 관련된 최대한의 노력은 필요하지만) 사고의 가능성을 완전하게 배제한 사전 대책을 목표로 했다고 해도 결과가 그렇게는 안 되는 경우를 생각해 둘 필요가 있다고 이해하는 것, 둘째, 만일 실제로 정보 시큐러티상의 문제가 발생했다고 해도 당사자는 적절히 대처하여 문제를 해결하고, 주위는 문제의 본질 및 피해의 규모를 이해하면서 사태의 심각 정도를 파악할 수 있는 것 등이 필요하다.

이것을 위해서는 정보보호 대책의 실시 주체가 진지하게 또 투명성을 갖고 대책을 추진하는 것이 대전제이지만, 그 전제하에서 국민이나 사회 전체가 절대적으로 완벽하지는 않다고 하는 의미에서 수용해야 하는 일정한 리스크를 수용하고, 이러한 현실을 주체적으로 지지할 수 있도록 되는 것이 필요하다. 즉, 스스로 이성적이면서 주체적으로 생각하는 IT시대의 강력한 '개인'과 '사회'의 확립이 불가결하다.

(3) 세계와의 협조, 주도권의 발휘

성숙한 정보 시큐러티 입국 사상을 염두에 두고 대응을 추진함으로써 일본의 정보보호 정책은 IT안심 이용 환경의 구축을 향한 보다 현실에 입각한 것이 된다. 일본의 정보 시큐러티의 대응은 국제사회와의 관계에서도 보다 받아들이기 쉽게 되고, 실로 IT선진국으로서 발신이나 공헌을 할 수 있는 상태에 도달했다고 할 수 있게 된다.

일본은 성숙한 시큐러티 입국 사상아래 자국의 대응에 자신을 갖고 세계와 협조하여 그 가운데 적당한 주도권을 잡아 간다.

또 동시에 세계에서 최고 수준의 대응이나 최첨단 기술이나 최신 리스크 동향 등에 관해서도 정보 수집을 게을리 하지 않도록 하는 등의 충분한 안배를 실시하여 일본의 대응이 세계 수준에 늦지 않도록 하는 주의도 필요하다.

다. 향후 3년 간 대응할 중점정책

1) 대책 실시 4 영역

가) 정부기관·지방공공단체

(1) 정부기관

정부기관에서는 제1차 기본계획 기간 중에 결정한 정부기관 통일 기준과 거기에 기한 평가·권고라는 구조를 유지하면서 이하의 대책에 중점적으로 대응해 가는 것으로 한다.

(가) 모든 정부기관에서 능동적으로 정보보호 대책에 대응하는 체제의 확립

① PDCA 사이클의 각 프로세스에서의 매니지먼트 강화

각 정부기관에서는 정보 시큐러티 거버넌스의 확립을 도모하기 위해 최고 정보 시큐러티 책임자아래에서 해당 기관의 정보보호 대책에 관해 책임을 갖고 통괄하는 것이 가능한 체제를 정보 시스템 통괄 부문(PMO) 또는 그것과 동등한 권능을 가지는 부문에서 정비한다. 또, 최고 정보 시큐러티 책임자를 보좌하는 전문적 지견을 가지는 최고 정보 시큐러티 자문관을 두는 것과 동시에 그 스탭이 되는 인재를 필요에 따라서 확보하고, 상기의 체제 아래에서 이러한 전문가의 지시나 어드바이스가 조직 전체에 신속하고 확실히 반영될 수 있는 구조를 구축한다.
각 정부기관에서는 행정에 대한 국민의 신뢰 확보를 위해 정보보호 대책과 관련된 설명 책임을 분명히 하는 관점에서, 각각의 정보 시스템의 현상을 파악한 다음, 정보 시큐러티에 대한 생각, 정보보호 대책과 관련된 목표나 계획 및 그 실적과 평가 등 각각의 정부기관에서 PDCA 사이클이 유효하게 기능하고 있는가의 여부를 수치 지표 등의 객관적 지표를 적극적으로 활용해 기술한 '정보 시큐러티와 관련된 연차보고서'(정보 시큐러티 보고서)를 작성한다. 그 때 정보 시큐러티 보고서의 객관성을 확보하는 관점에서 최고 정보 시큐러티 자문관이 그 작성에 참가하

는 것 외에 외부감사 제도의 활용에 관해서도 도입 가능한 정부기관에서는 적극적으로 추진하는 것으로 한다. 또, 작성한 정보 시큐러티 보고서는 최고 정보 시큐러티 책임자가 정보 시큐러티 정책 회의아래에 설치되어 있는 '정보보호 대책 추진 회의' 등의 장소에서 보고하여 공표한다.

각 정부기관에서의 정보보호 대책의 밸런스를 확보함과 동시에 더욱 충실·향상을 추진하는 관점에서 정부기관의 정보 시큐러티 보고서 작성을 위한 가이드라인을 책정함과 함께, 각 정부기관이 작성한 정보 시큐러티 보고서의 정량적 평가 등을 하여 그 결과를 정보보호 정책 회의에 보고한다. 또, 각 정부기관의 최고 정보 시큐러티 자문관이 모이는 회의체를 설치하고, 정보 시큐러티 보고서의 비교·평가 등을 하는 것과 동시에 그것들을 통해서 얻을 수 있는 지견의 공유나 피드백을 적극적으로 도모하는 것으로 한다.

기술이나 환경의 변화를 근거로 하여 정부기관에서의 정보보호 대책을 항상 최신이고 적절한 것으로 하기 위해서 정부기관 통일 기준에 관해서는 매년 계속 그 재검토를 실시한다.

정부기관에서 특별히 은닉해야 할 정보(특별 관리 비밀)를 취급하는 시스템과 관련된 정보보호 대책에 관해서는 정부기관 통일 기준에 기한 PDCA 사이클을 기본으로 하면서 '대(對)정보활동 기능의 강화에 관한 기본방침'에 기하 특별 관리 비밀과 관련된 기준을 근거로 한 대책을 각 정부기관 스스로의 책임으로 착실하게 강구하는 것으로 하여 그 실시 상황을 중층적으로 체크하는 구조를 카운터 정보(intelligence)센터를 중심으로 하는 내각 관방 및 관계 정부기관이 협력하여 구축한다.

② 정부기관에서의 인재의 육성·확보 및 직원의 의식 계발

정부기관에서의 정보 시큐러티 관련 업무를 조사·검증하고, 이러한 업무에 종사하는 인재에게 필요한 스킬을 정리한다.

각 정부기관에서는 정리된 스킬을 근거로 하여 정보보호 대책에 관련된 내부 인재의 교육이나 확보·등용 등과 관련된 구체적인 계획을 '행정 기관에 있어서의 IT

인재의 육성·확보 지침'에 근거해 작성한 'IT 인재육성·확보 실행 계획'에 명기하고 그것을 추진한다.

또, 각 정부기관에서는 정보보호 대책과 관련된 민간 전문가의 활용을 촉진하기 위해 최고 정보 시큐러티 자문관이나 그 서포트 스탭의 활용 등의 전략적인 아웃소싱(outsourcing)을 진행시키는 것 외에 임기부 채용 제도 등의 적극적인 활용을 도모한다.

각 정부기관에서는 관민 인사 교류 제도의 활용에 의한 인재육성의 촉진 외에, 계층별 연수에 정보 시큐러티에 관한 내용을 포함시키는 등 간부 직원도 포함한 전 직원의 정보 시큐러티에 관한 의식의 향상 방책을 인사 담당 부문과 정보 시스템 부문의 밀접한 협력 하에서 추진한다.

③ 정보보호 대책을 적시에 실시하기 위한 예산 면에서의 대응

정보보호 대책은 적시의 대처가 필요하기 때문에 각 정부기관에서는 미리 가능한 한도의 상정을 함과 동시에 보수 계약 등에 대해서도 적시에 적절한 대응이 가능하게 되는 계약을 주고받는 등의 대응이 필요하지만, 그 때에는 '성과 중시 사업'제도의 활용도 검토 등의 궁리를 하는 것 외에 회계 부문과 정보 시스템 부문이 밀접하게 협력하여 예산의 효율적 활용에 배려하여 대책을 진행시킨다.

④ 운용·관리를 위탁하고 있는 정보 시스템의 정보보호 대책의 강화

각 정부기관에서는 정부기관 외의 조직에 운용·관리를 위탁하고 있는 정보 시스템에 관해 정부기관 통일 기준 등을 근거로 한 적절한 계약에 의해 위탁처의 정부기관의 정보보호정책의 준수를 확보함과 동시에 적절한 운용을 하고 있는지를 확인하기 위한 대응을 진행시킨다.

⑤ 기술면의 지견을 축적·활용하는 구조의 구축

정보보호 대책의 추진에 있어서 일본에서의 정보 시큐러티와 관련된 기술적·전문적인 지식이나 경험의 이용을 도모하기 위해 관련된 독립 행정법인이나 정보 시큐러티 관계 단체 등의 연구자·실무가의 지견을 집합적으로 활용하기 위한 구조의 구축을 추진한다.

⑥ 정보 시큐러티에 관련된 법령과의 정합성 확보

현재 검토가 진행되고 있는 문서 관리 법제 등도 포함하여 정보 시큐러티와 관련이 깊다고 생각되는 법제도 등과 정부기관 통일 기준과의 정합성의 확보가 도모되도록 필요한 조정을 추진한다.

(나) 정부 전체를 통해서 정보 시스템에 정보보호 대책이 적절히 편입되는 구조의 구축

정부기관에서의 각종 정보 시스템의 구축을 실시함에 있어, 토탈 코스트의 억제나 편리성·유연성의 실현, 정보 시큐러티의 확보라는 여러 가지 방향성을 가진 요건을 지양하는 관점에서 정보 시스템의 구축이나 운용 단계뿐만 아니라 기획·설계 단계로부터의 정보보호 대책의 편입에 관해서도 의식하기 위한 방책(Security by Design)을 업무·시스템의 최적화의 대응과 일체적으로 추진하는 구조의 구축을 도모한다. 그 때, 정부 전체로서 정보보호 대책을 포함한 정보 시스템의 TCO(Total Cost of Ownership : 시스템의 도입, 유지·관리 등에 드는 비용의 총액)의 저감을 추진하기 위한 방법에 관해 검토를 한다.

또, 정보 시스템이나 물품의 조달시에 필요한 정보보호 대책을 설정하기 위해서 참고가 되는 각종 정보를 제시하여 그 활용을 도모한다.

(다) 전자 정부의 편리성·정보보호 레벨의 향상

행정 서비스의 편리성 향상과 행정 운영의 효율화·고도화를 추진함과 동시에 정

보보호 레벨의 향상을 도모하는 관점으로부터, 전자 정부와 관련된 시스템의 보호 기능의 마땅한 모습에 관해 검토하는 것으로 하고, 특히 이용자와의 인터페이스와 관련되는 것에 관해서는 이용자의 편리성을 향상시키고 또 안전을 확보할 수 있는 것이 되도록 비용 대비 효과를 감안한 다음 실장 방법을 포함해 검토를 한다.

(라) 정부기관에 있어서의 사업 계속성 확보·긴급 대응 능력의 강화와 관련된 검토

현재 중앙 방재 회의가 책정한 '수도직하지진대책대강(首都直下地震對策大綱)'(2005년 9월)에 기해 각 정부기관에서 대해 수도 직하형 지진을 대상으로 한 업무 계속 계획의 책정은 행해지고 있지만, 그 외의 재해나 장애 발생시에도 행정의 계속성을 확보하는 관점으로부터 각 정부기관은 보유하는 정보 시스템의 재해·장애시 대응의 필요성·우선도에 관해 결정하는 것과 동시에 필요한 것에 관해서는 업무 계속 계획을 책정한다.

또, 정부기관이 보유하는 중요한 시스템이나 정보의 백업 체제에 관해 정부 횡단적인 방향성을 검토한다.

긴급시에 있어서의 대응력(리스폰스·리커버리)의 강화를 꾀하는 관점으로부터 2008년도에 본격 운용을 개시한 GSOC[175]를 핵으로 하여 각 정부기관이나 국내외의 관계 기관과의 제휴를 보다 깊게 하여 긴급시의 연락 체제나 공격 등의 분석·해석 및 대책 입안 기능을 강화함으로써 정부 전체적으로 사이버 공격 등에 대한 긴급 대응 능력을 향상시키는 것과 동시에 일본의 안전 보장 체제의 강화를 도모한다.

(마) 독립 행정법인 등의 정보보호 대책의 추진

독립 행정법인 등의 정보보호 대책을 추진하기 위해 독립 행정법인 등을 주관하는 정부기관은 중기 목표 안에 정보보호 대책과 관련된 사항을 명기하고, 독립 행

175) Government Security Operation Coordination team의 약칭이다.

정법인 등이 조직으로서 정보보호 대책에 대응하는 체제를 구축시킨다.

각 독립 행정법인 등은 그 업무 특성 및 대책의 실시 상황에 따라 정부기관 통일 기준을 포함한 정부기관에 있어서의 일련의 대책을 근거로 스스로의 정보보호 대책과 관련된 PDCA 사이클을 구축한다. 또, 독립 행정법인 등 및 독립 행정법인 등을 주관하는 정부기관은 긴급시를 포함한 실효성이 있는 연락 체제를 정비한다.

(바) 그 외 개별 정보보호 대책의 추진

① 정부기관의 정보 시스템의 IPv6 대응화

IPv4 주소 고갈에의 선도적인 대응을 실시하는 관점에서 정부기관에서는 각 정보 시스템의 새로운 개발(도입) 또는 개정에 맞추어 IPv6 대응을 계획적으로 진행하여 특히 전자 정부 시스템을 시작으로 하는 외부와 직접 통신을 실시하는 정보 시스템에 관해서는 원칙적으로 2010년까지 IPv6 대응을 도모하는 것으로 하고 있지만, 그 때 IPv4로부터 IPv6로의 이행기에서의 시큐러티상의 과제에 적절히 대응한다.

② 정부기관에 대한 성취해의 방지

악의의 제삼자가 완전히 정부기관 또는 정부기관의 직원이 되어 일반국민이나 민간기업 등에 해를 미치는 경우가 없게 정통 정부기관 또는 정부기관의 직원인 것을 쉽게 확인 가능하게 하기 위해 전자 메일이나 웹 서버에서 도메인명으로서 정부기관의 도메인인 것이 보증되는 도메인명을 사용하는 것이나, 정부기관으로부터 발신하는 전자 메일에의 전자서명의 부여 등 전자 증명서의 활용과 관련된 대응을 추진한다.

③ 정부기관에 있어서의 안전한 암호 이용의 추진

전자 정부의 안전성 및 신뢰성을 확보하기 위해 정부기관에서 사용되고 있는 추

천 암호에 관해 그 안전성을 계속적으로 감시·조사함과 함께, 기술 동향 및 국제적인 대응을 근거로 하여 현행 '전자 정부 추천 암호 리스트'의 2013년도 개정을 향해 관계 기관에서 요한 작업을 진행시킨다. 또, '정부기관의 정보 시스템에서 사용되고 있는 암호 알고리즘 SHA-1 및 RSA1024와 관련된 이행 지침'의 책정시의 경험을 적절히 계승하여 안전성이 저하된 암호에 관해 신속하게 안전한 암호로의 이행을 진행시킨다.

(2) 지방공공단체

(가) 소규모의 지방공공단체도 포함한 합리적·자주적인 정보보호 대책의 촉진

소규모의 지방공공단체도 포함해 모든 지방공공단체에서 바람직한 정보보호 대책이 실시되는 것을 목표로 하여 대책의 촉진을 실시한다. 구체적으로는 대책이나 감사의 기본이 되는 정보 자산의 리스크 분석의 실시를 촉진함과 함께, 정보보호 정책 책정 등의 검토나 감사의 실시를 위한 가이드라인의 재검토, 업무 계속 계획의 책정에 이바지하는 가이드라인의 보급 등을 실시한다. 또, 인재 면에서는 대응을 담당하는 직원 등의 능력 향상을 위한 공동 스터디 그룹이나 지역 세미나의 개최 등을 추진한다.

(나) 복수 지방공공단체 간에서의 정보보호 대책의 제휴를 위한 노력의 후원

지방공공단체에 대해 정보보호 대책에 투자할 수 있는 리소스의 한도를 고려해 복수 지방공공단체 간에 효율적으로 대책을 실시하기 위한 제휴를 위한 노력을 응원한다. 이를 위해서 전국의 지방공공단체에 대한 베스트 프랙티스(best practice)의 소개나 전형적인 사례가 생기는 것과 같은 응원을 실시한다. 또, 지방공공단체의 오랜 이해 촉진을 위한 스터디 그룹이나 검토회를 실시하여 조직 탑의 의식을 높임과 동시에, 예를 들면, 상호 감사 등의 대응에 있어서의 자문관의 파견 등을 검토한다.

(다) 지방공공단체의 대응을 후원하는 주체의 강화

지방공공단체의 대책을 추진하려면 대응을 후원하는 주체를 강화하는 것이 유효하다. 이 때문에 관·민·NPO에 의한 공동 스터디 그룹을 개최하는 등 정보 시큐러티에 유용한 지견을 가지는 모든 주체의 협력 체제를 구축함과 함께, LGWAN(종합 행정 네트워크) 내의 포털 사이트를 활용한 자치제 전용 지원 체제의 강화 등을 추진한다.

(라) 지방공공단체가 담당하는 폭넓은 행정 분야에서의 대응 촉진

국가 행정 조직과 지방공공단체의 담당 조직 사이의 개별 관계를 근거로 한 형태로 지방공공단체가 담당하는 폭넓은 행정 분야에서의 정보보호 대책을 촉진한다. 예를 들면, 학교에서의 IT기반의 정비시에 정보 시큐러티라는 관점도 충분히 가미하는 것이나, 관계 부처로부터 도도부현 교육위원회에 대해 정보보호 대책상 효과 있는 방책을 전달하는 것이나, 베스트 프랙티스를 소개하여 도도부현 교육위원회의 의식 향상을 촉진한다고 하는 것 등이 고려된다.

(마) 지방공공단체 간, 지방공공단체와 정부기관 간에서의 베스트 프랙티스의 상호 활용 촉진

약 1800개에 달하는 지방공공단체의 정보보호 대책을 촉진함에는 지방공공단체 간에 베스트 프랙티스를 상호 활용하는 것이 효율적이다. 이것을 위해서 LGWAN(종합 행정 네트워크) 내에 설치되어 있는 포털 사이트를 이용해 지방공공단체 간에서의 정보 공유를 촉진한다. 또, 베스트 프랙티스를 지방공공단체의 장이나 현장 담당자 등의 여러 계층에서 공유할 수 있도록 검토회나 의견교환회 등을 개최한다.

나아가 지방공공단체와 같이 공적 조직인 정부기관과의 사이에서의 베스트 프랙

티스의 상호 활용도 효과가 있다고 생각되기 때문에 이것을 위한 방책의 검토를 실시한다.

(바) 지역의 정보보호 대책의 담당자의 육성 지원

지역에서 정보보호 대책을 담당할 수 있는 인재의 육성에 있어서는 지방공공단체에 의한 촉진 활동이 효과적이기 때문에 지방공공단체의 이러한 활동이 실시되기 쉬워지는 환경 정비를 한다. 구체적으로는 지방공공단체나 정보시큐러티를 테마로 한 주민용 교양 강좌 등을 개최하기 쉽도록 강좌로 활용할 수 있는 참고 자료 등을 작성, 소개한다. 또, Teaching teachers(가르칠 수 있는 인재의 교육·육성) 발상에 근거하여 지방에서 인재육성이 촉진되는 대책을 실시한다.

나) 중요 인프라

중요 인프라의 정보보호 대책에 관한 관계 주체는 제2차 행동계획에 근거하여 각각 중요 인프라 서비스의 유지에 노력하고 또 IT장애 발생시의 신속한 복구 등을 확보하는 것에 노력하는 것으로 한다. 또, 정보보호 대책의 실시 상황에 대해 지표를 이용한 검증을 매년 실시함과 함께, 행동 계획의 평가를 실시하여 개별적 대응의 계속적 개선을 도모하는 것으로 한다.

(1) '안전기준 등'의 정비 및 침투

제1차 행동계획에서 책정된 지침에 대해 사업 계속의 관점으로부터 구체적 내용의 보충을 포함해 지침의 위치설정이나 기재 내용의 구체성 레벨의 재검토를 실시한다. 또, 중요 인프라 사업자 등의 PDCA 사이클과의 정합성을 근거로 한 안전기준 등의 정비 추진 등의 향상에 이바지하는 대응뿐만 아니라, 3년 마다 개별적으로 선진적인 대책을 늘려 그 침투를 도모하는 관점에서의 대응도 추진한다.

(2) 정보 공유 체제의 강화

제1차 행동계획에서 구축된 세프타(CEPTOAR),[176] 세프타 위원회(CEPTOAR Council)를 포함한 관계 주체 간에서 공유하는 정보에 대한 정리를 하여 정보 제공, 정보 연락 등에 필요한 환경 정비 등을 추진함과 함께, 각 세프타, 세프타 위원회의 자주적 활동의 충실을 강화한다.

(3) 공통 위협 분석

제1차 행동계획에서 실시해 온 어느 중요 인프라 분야에 IT장애가 발생했을 경우에 다른 어느 중요 인프라 분야에 영향이 파급되는가 하는 상호의존성 해석을 계속함과 함께, 중요 인프라 분야 공통에 일어날 수 있는 위협이 무엇인지를 파악하기 위한 검토를 실시한다.

(4) 분야 횡단적 연습

제1차 행동계획에서 얻을 수 있었던 만큼 분야횡단적인 연습 방법에 관한 지견을 근거로 해 각 중요 인프라 소관 부처, 각 중요 인프라 사업자 등 각 중요 인프라 분야의 세프타 등의 협력을 얻어, IT장애의 발생을 상정한 중요 인프라 분야 횡단적인 연습을 실시한다.

(5) 환경 변화에의 대응

사회 환경이나 기술 환경 등의 상황 변화에 맞추어 정보보호 대책을 기민하게 대응시켜 가기 위해서 제2차 행동계획 책정시에 상정하지 않았던 환경의 변화를 살펴서 아는 능력의 향상에 노력한다. 또, 이러한 환경의 변화에 대해서 제2차 행동계획의 구조만으로는 충분히 대응할 수 없는 경우는 내각 관방은 필요한 대응

176) CEPTOAR(Capability for Engineering of Protection, Technical Operation, Analysis and Response의 약어로 이는 중요인프라 분야마다 정비된 정보공유·분석기능을 일컫는 말이다.

이 가능해지는 체제의 검토를 실시한다.

다) 기업

(1) 정보 시큐러티 거버넌스의 '경영의 일환으로서의 자리 매김'의 확립

정보 시큐러티 거버넌스를 경영의 일환으로서 자리 매김을 하기 위해 그것을 위한 대응을 추진하고, 경영층에 대한 계발 활동의 추진, 합리적인 정보 시큐러티 거버넌스 확립 프로세스 모델 개발 등의 대응을 실시한다. 또, 경영자에게 의식 향상을 꾀하기 위한 체제의 강화를 목표로 하는 것과 동시에, 정보보호관리체계(ISMS) 적합성 평가나 정보 시큐러티 감사, IT시큐러티 평가 및 인증제도, 암호모듈 시험 및 인증제도 등의 제도, 정보 시큐러티 보고서 모델, 정보보호 대책 벤치마크 등 툴의 보급·개발·개선 등을 더욱 추진해 구체적인 대응이 침투하는 것을 목표로 한다, 게다가 정보 시스템 등의 정부 조달의 경쟁 참가자에 대해서 필요에 따라서 이러한 제도나 제삼자 평가의 결과 등을 활용한 정보보호 대책 레벨의 평가를 입찰 조건 등의 하나로 한다. 나아가 정보 시큐러티 거버넌스를 위한 대응이 기업에 있어 과도한 부담이 되지 않게 투자 효율을 측정하는 수법을 실제로 활용 가능하게 하기 위한 검토를 추진한다. 또, 정보 시큐러티 거버넌스가 '경영의 일환으로서 자리 매김'하는 것을 확보하려면 관련 법제와의 관계에서 정리가 필요한 논점도 있다.

이 때문에 관련 법제도의 분석 정리를 실시해 가이던스로서 정비하는 것과 같은 대응도 추진한다.

(2) 기업의 정보 시큐러티 향상에 이바지하는 제품이나 서비스의 제공 촉진과 활동의 추진

기업에 있어서의 정보보호 대책이 진전하도록 기업이 이해하기 쉬운 형태로 필요한 정보보호 대책을 선택할 수 있는 환경을 정비한다. 제1차 기본계획에 계속하

여 기업의 정보 시큐러티 관련 리스크에 대한 정량적 평가 수법의 실용화를 목표로 한 연구를 촉진함과 함께 IT시큐러티 평가 및 인증제도의 활용을 촉진한다.

또, 정보 시큐러티 향상에 이바지하는 제품이나 서비스의 제공 촉진과 활동의 추진을 위해서는 대책 지원 주체 측의 대응의 강화도 필요하다. 대책을 용이하게 하는 SaaS나 ASP 등의 활용 촉진이나, 스팸메일 대책의 강화, 암호 기술이나 인증 기술, NGN/IPv6 이행 환경의 시큐러티 평가 시스템 등의 기술개발 촉진 등의 대응을 진행시킨다. 덧붙여 대응에 있어서는 TCO에도 안배한 제품이나 서비스의 제공이 촉진되는 시점도 중요하다,

(3) 기업에 있어서의 정보 시큐러티 인재의 육성·확보

경영층의 정보보호 대책에 대한 이해 증진과 함께, 기업의 정보보호 대책의 추진을 담당하는 인재의 육성·확보가 필요 불가결한 것이기 때문에 인재육성을 위한 세미나 개최 등의 홍보 계발을 추진한다. 또, 대책에 대해서는 새로운 IT의 이용·활용 등 환경의 진화에 유연하게 대응할 수 있는 인재나 기업의 매니지먼트 전체를 조감 한 다음 판단할 수 있는 스킬을 가진 인재 등의 육성·확보도 필요 불가결하다. 그 때에는 정보 시큐러티 인재가 목표로 하는 캐리어 패스(직무경력)를 고려하는 것도 중요하다. 이러한 것을 근거로 해 관민의 적절한 역할 분담 아래 객관적인 인재 평가 메커니즘인 각 스킬 표준의 정합화를 도모한 공통 캐리어·스킬 체제와 거기에 준거한 정보처리 기술자 시험의 활용 및 민간의 인재육성에 관한 체제나 각종 자격시험의 활용을 촉진한다. 또, 산학 제휴에 의한 고도 정보 시큐러티 인재를 육성하여 유익한 커리큘럼 정비나 교원 강화, 인턴십의 충실 등에 대응하기 위한 체제를 정비한다.

또, 기술자전용의 정보 시큐러티와 관련된 모델 개발 계획의 책정이나 전문가 커뮤니티에의 지원을 진행시키는 것으로 널리 기업의 정보 시큐러티를 담당할 수 있는 인재의 육성·확보에 대응한다.

게다가 향후의 과제가 되는 NGN/IPv6에의 이행 등이 새로운 환경에의 이행에 대응할 수 있는 실천적인 정보 시큐러티 인재나 법령 준수, 정보 자산이나 사업

계속 등에 관한 리스크를 특정하면서 정보보호 대책을 실천할 수 있는 인재의 육성을 추진한다.

(4) '사고 전제 사회'에의 대응력 강화를 위한 사업 계속성 확보·긴급 대응 체제 등의 강화

컴퓨터 바이러스나 취약성 등의 정보 시큐러티상의 문제에 대한 적확하고 실효적인 대응을 실시하기 위해 평시부터 정보 공유를 위한 연락 체제의 구축, 주체간의 제휴 강화가 도모되기 위한 대응을 추진한다. 또, 사업 계속성 확보를 강화하기 위해서 기업에 있어서의 사업 계속 계획 책정의 촉진을 꾀하는 것과 동시에, 그것을 위한 사업 계속 계획 책정 가이드라인의 보급, 개선의 대응을 추진한다. 게다가 정보 시큐러티상의 문제가 발생했을 경우에 신속하고 실효적인 대응을 하기 위해서 필요한 긴급시 대응 체제의 강화를 추진한다.

(5) 중소기업의 정보보호 대책의 추진

인원, 예산, IT인프라 등 주로 자원 부족으로 인하여 대책이 지연되기 십상인 중소기업의 정보보호 대책이 촉진되도록 여러 대책 중에서 적절한 대책을 용이하게 선택할 수 있는 환경을 정비한다. 예를 들면, 적절한 정보 시큐러티 레벨을 측정하기 위해서 활용되는 정보 시큐러티벤치마크를 계속 개선하여, 자사의 정보 시큐러티 레벨을 객관적 평가로서 제시하기 위한 통일적인 대조표의 개발, 보급을 도모한다.

또, 중소기업의 정보보호 대책을 촉진하기 위해서는 간편하고 염가의 정보보호 대책 툴을 제공하는 등의 효과적인 대응이 필요하기 때문에 SaaS나 ASP등의 활용 촉진 및 이들 서비스 제공 사업자에 있어서의 정보보호 대책 기준의 제시·계발 등의 대응을 실시한다.

게다가 중소기업의 경영자, 정보 시스템 담당자 등의 정보 시큐러티에의 이해를 심화하기 위해 세미나의 개최 등 보급·계발 활동을 추진해 정보보호 대책의 촉진

을 꾀한다.

(6) 일본계 기업의 글로벌한 사업 전개를 지지하는 정보보호 정책의 추진

일본 기업이 글로벌한 사업 전개를 함에 있어서 일본 외의 비즈니스 거점에서 정보 시큐러티를 확보하기 위한 대응을 추진한다. 예를 들면, 아시아 등 일본 기업의 사업 활동에 관계 깊은 나라나 지역을 염두에 두고, 원활한 아웃소싱(outsourcing)을 할 수 있는 환경 만들기나 시큐어한 네트워크 환경의 구축을 향한 국제 제휴·협력을 추진한다.

라) 개인

(1) 정보보호 교육의 강화·추진

IT의 이용·활용에는 적극적이지만, 리스크의 인식이나 정보보호 대책의 중요성 인식이 충분하다고 할 수없는 아동·학생이나 보호자에 대한 교육·계발을 추진한다. 이러한 관점도 감안하면서 학교나 지역에서의 정보 모럴 등의 교육을 추진한다.

또, 소비자인 개인이 여러 서비스 등의 이용에 대해 생길 수 있는 리스크를 인식해 그 리스크를 피해로 전환시키지 않기 위한 환경을 정비한다. 개인에 대한 계발 활동과 함께 서비스 제공 사업자나 대책 지원 주체에 의한 리스크 정보, 대책 정보의 적절한 제공, 사고 발생시의 대응 등의 대응을 촉진한다,

(2) 개인의 향상을 위한 보다 효과적인 보급·계발 활동의 실현

개인의 향상을 위해 주지·계발 활동을 관계 부성청이 더욱 제휴하여 보다 효과적으로 실시할 수 있는 대응을 진행시켜 나간다. 또, IT에 관해서 자세히 알지 못하는 개인을 포함한 일반 이용자의 시큐러티 레벨을 효과적으로 올리기 위해서

질문에 대한 적절한 어드바이스나 방문 대응을 실시할 수 있는 서포터의 육성, 지역단체 네트워크의 실현을 촉진한다.

(3) 대책이 곤란한 개인을 포함한 정보보호 수준 향상을 향한 대응

대책의 필요성을 인식하고 있어도 대책을 실시하지 않는 개인 등 대책이 곤란한 개인을 포함한 정보보호 수준의 향상을 위해서 대책 지원 주체에 의한 대응이 필요 불가결하다. 이를 위해서 스팸메일대책의 강화나 전기 통신사업자가 예방적 조치로서 실시하는 정보보호 대책의 이용 촉진 등의 대응을 촉진한다.

(4) 횡단적인 정보보호 기반의 강화와 발전

(가) 정보 시큐러티 기술 전략의 추진

2012년에의 모습을 실현하기 위해서 민간이나 대학에 있어서의 자주적인 연구개발을 재촉하는 것과 동시에 산학관은 적절한 역할 분담을 실시하면서 제휴해 나가는 것이 필요하다. 그 중에서 정부는 리스크가 높은 분야, 공공성이 높은 분야, 기초적인 분야, 혹은 다양한 분야에 공통적인 연구개발 지원의 환경 정비 등 매우 중요하지만 민간이나 대학 등에서는 실시 곤란한 것에 대해서 중점적으로 대처한다.

① 정보 시큐러티 기술개발의 중점화와 다양성의 유지

기반으로서의 IT의 강화 및 국민이 안심하고 IT를 이용할 수 있는 환경의 실현을 목표로 한 연구개발·기술개발을 중점적으로 촉진한다. 경제 환경이 어려움을 늘리는 가운데 IT를 이용해 생산성 향상을 꾀하는 것으로 그 분야에서 장래에 주도적이거나 우위인 지위를 확보한다고 하는 시점을 갖고 연구개발·기술개발을 추진하는 것이 종래 이상으로 요구된다. 구체적으로는 이용자에게 대책에 대한 과도

의 부담을 강요하지 않고, 사전에 정보보호 대책이 들어간 안전·안심인 기기의 실현이나 이용자 환경의 제공을 중점적으로 대처해야 할 과제로서 대응을 추진한다.

한편, 연구개발·기술개발의 다양성을 확보하기 위해 시장으로서 성립하고 있지 않기 때문에 기업이 대응하지 않는 분야나 장래적인 리스크에 대항하기 위한 선행적인 개발, 개발비가 거대한 분야 및 기초 연구 등 일본으로서 전략적으로 유지해야 할 분야에 대해서는 정부가 적극적으로 대처하는 것으로 한다.

② '그랜드 챌린지형'연구개발·기술개발의 추진

정보보호 대책에 대해서는 매우 중요한 대응이 필요하지만 대책이 충분하지 않은 과제나, 중장기적인 시야에서 발본적인 기술 혁신 등의 실현이 요구되는 과제가 존재한다. 이러한 대책이 곤란한 과제에 대응하기 위해 '그랜드 챌린지형'의 연구개발·기술개발을 추진한다.

매우 중요한 과제의 해결을 위해서는 요소 기술의 통합화·실장화로 신속한 대응을 꾀한다.

또, 이미 개발이 끝난 상태여도 제도나 교육이 쫓아가지 못했던 등의 이유로부터 기술성과가 이용되지 않는 경우가 있어, 조직·인간계의 관리 수법의 고도화나 이용자의 계발과 병행해 통합적인 대책을 추진하는 것이 효과적이다.

중장기적인 연구개발의 추진을 위해서는 장래의 사회상을 예측해 거기서 필요정보 시큐러티 기술을 검토하는 것으로써 연구개발·기술개발 테마의 개척을 행한다. 구체적으로는 설계 단계부터 제품에 시큐러티를 만들기 위한 수법의 확립이나, 개발 노하우의 축적은 단기적으로 실현할 수 있는 것은 아니고, 또 많은 지견을 집약할 필요가 있기 때문에 중장기적인 비전과 실시 체제 및 지원 환경을 가지고 맞는 것이 바람직하다.

③ 연구개발·기술개발의 효율적인 실시 체제의 구축과 기반의 정비

국가가 지원하는 프로젝트에 대해서는 그 투자 효과를 최대화하기 위해서 연구

개발·기술개발의 계획 책정시에 프로젝트의 도중에 얻을 수 있던 성과를 활용하는 순서(프로세스)를 넣는 것과 동시에, 프로젝트의 내용 및 실시 상황의 공개를 촉진한다. 또, 정보 시큐러티를 둘러싼 환경의 변천이 격렬한 가운데 사회 정세 변화나 기술 혁신의 영향을 평가해 필요성이 높은 경우에는 계획 변경이 가능한, 유연한 프로젝트 관리 구조를 도입해 새로운 위협에의 신속한 대응을 가능하게 한다.

게다가 직접적인 연구개발·기술개발의 대응에 가세해 정보 시큐러티 분야의 특수성에 비추어, 연구개발 지원의 환경 정비를 관민의 제휴에 의해 적극적으로 추진한다, 구체적으로는 리스크의 표기법이나 평가방식의 공통화, 정보 시큐러티에 관한 데이터베이스의 정비와 공유 및 격리 워크벤치[177]의 구축 등에 의해 연구개발의 지원과 가속을 꾀한다.

(나) 정보 시큐러티 인재의 육성·확보

① 정부기관에 있어서의 인재의 육성·확보 및 직원의 의식 계발

정부기관에 있어서의 정보 시큐러티 관련 업무를 조사·검증해 이러한 업무에 종사하는 인재에게 필요하게 되는 스킬을 정리한다.

각 정부기관에서는 정리된 스킬을 근거로 하여 정보보호 대책에 관련되는 내부 인재의 교육이나 확보·등용 등과 관련된 구체적인 계획을 '행정 기관에 있어서의 IT인재의 육성·확보 지침'에 기해 작성한 IT 인재육성·확보 실행 계획에 명기해 그것을 추진한다.

또, 각 정부기관에서는 정보보호 대책과 관련되는 민간 전문가의 활용을 촉진하기 위해 최고 정보 시큐러티 자문관이나 그 서포트 스탭의 활용 등의 전략적인 아웃소싱(outsourcing)을 진행시키는 것 외에 임기부 채용 제도 등의 적극적인 활용을 도모한다.

각 정부기관에서는 관민 인사 교류 제도의 활용에 의한 인재육성의 촉진 외에 계층별 연수에 정보 시큐러티에 관한 내용을 포함시키는 등 간부 직원도 포함한

177) 멀웨어(malware) 등을 실제로 동작시켜 연구를 하기 위한, 네트환경을 모형으로 한 실험설비를 말한다. 현실의 인터넷으로부터는 격리시켜 두고, 멀웨어는 물리적으로 봉해두고 있다.

전직원의 정보 시큐러티에 관한 의식의 향상 방책을 인사 담당 부문과 정보 시스템 부문의 밀접한 협력 아래서 추진한다.

② 기업에 있어서의 정보 시큐러티 인재의 육성·확보

경영층의 정보보호 대책에 대한 이해 증진과 함께, 기업의 정보보호 대책의 추진을 담당하는 인재의 육성·확보가 필요 불가결한 것으로부터 인재육성을 위한 세미나 개최 등의 홍보 계발을 추진한다. 또, 대책에 대해서는 새로운 IT의 이용·활용 등 환경의 진화에 유연하게 대응할 수 있는 인재나 기업의 매니지먼트 전체를 조감한 다음 판단할 수 있는 스킬을 가진 인재 등의 육성·확보도 필요 불가결하다. 그 때에는 정보 시큐러티 인재가 목표로 하는 캐리어 패스를 고려하는 것도 중요하다. 이러한 것을 근거로 해 관민의 적절한 역할 분담, 객관적인 인재 평가 메카니즘인 각 스킬 표준의 정합화를 꾀한 공통 캐리어·스킬 체제와 거기에 준거한 정보처리 기술자 시험의 활용 및 민간의 인재육성에 관한 체제나 각종 자격시험의 활용을 촉진한다. 또, 산학 제휴에 의한 고도 정보 시큐러티 인재를 육성하기 위한 커리큘럼 정비나 교원 강화, 인턴십의 충실 등에 대응하기 위한 체제를 정비한다.

또, 기술자전용의 정보 시큐러티와 관련된 모델 개발 계획의 책정이나 전문가 커뮤니티에의 지원을 진행시키는 것으로써 널리 기업의 정보 시큐러티를 담당할 수 있는 인재의 육성·확보에 대처한다.

게다가 향후의 과제가 되는 NGN/IPv6에의 이행 등이 새로운 환경에의 이행에 대응할 수 있는 실천적인 정보 시큐러티 인재나 법령 준수, 정보 자산이나 사업 계속 등에 관한 리스크를 특정하면서 정보보호 대책을 실천할 수 있는 인재의 육성을 추진한다.

③ 정보 시큐러티 인재가 보유하는 스킬의 가시화 추진

정보 시큐러티 분야에 인재를 모아 높은 능력을 가지는 인재에 의지한 정보 시

큐러티를 구축하기 위해서는 장기적인 시점으로부터 정보 시큐러티 인재가 스스로의 능력을 높이는 것이 업무에 결합되도록 하고, 인재의 옆에서 캐리어 패스를 그릴 수가 있도록 하는 것이 유효하다.

이를 위해서 실제의 업무에 대해 구할 수 있는 스킬을 명확하게 함과 함께 인재가 보유하는 스킬이 외부로부터 알기 쉽게 하기 위한 정책을 실시한다. 예로서는, 정보 시큐러티 자격제도·교육제도와 업무에서 요구되는 스킬이나 정보 시큐러티 인재가 목표로 하는 캐리어 패스의 관계를 보기 쉽게 하기 위한 대응이나, 공통 캐리어·스킬 체제 : ITSS5[178]나 민간의 인재육성에 있어서의 각종 유효한 프레임 워크의 활용에 의해 보유하는 스킬을 외부에 명시할 수 있는 구조를 구축하는 대응을 들 수 있다.

(다) 국제 제휴·협조의 추진

제2차 정보보호 기본계획아래에서의 대응을 통한 2012년의 모습을 실현하기 위해 정책, 오퍼레이션, 표준의 영역에서 지역의 특성 등을 고려해 이하의 6개의 관점으로부터 정책을 추진한다.

① 정보보호 정책에 관한 POC 기능의 강화와 정보 공유의 촉진

제1차 기본계획에 계속해 NISC는 여러 국제기관이나 포럼에 대해 정보보호 정책을 횡단적으로 다루는 POC로서의 역할을 명확히 하는 노력을 계속해 그 기능을 강화하는 것을 목표로 한다.

구체적으로는 세 가지 관점으로부터의 대응을 실시한다. 첫째, 국가 안전 보장, 중요 정보 인프라 방호, 글로벌한 경제활동의 계속성 확보, 사이버 범죄 방지 등의 여러 관점으로부터 논의를 하는 정보 시큐러티 관련의 국제 회합 등의 기회에 최신 동향의 파악·수집을 보다 강력하게 진행한다. 그것을 위해서는 신뢰(Trust)의 양성 및 얼굴이 보이는 공헌이 필요하기 때문에 이러한 국제 회합 등을 기회로

178) IT스킬표준(Information Technonogy Skill Standards)을 말한다.

횡단으로 파악·수집하는 기능을 강화한다. 두 번째로, 높은 신뢰 관계를 통해서 파악·수집한 동향에 대해서는 국내의 필요한 관계 기관·관계자에게 적절히 공유하는 것으로 처음으로 의미 있는 것이 된다. 이것을 충분히 근거로 하여 NISC는 POC로서 국내의 정부 관계 기관에 대해서 적절한 룰에 근거한 공유를 진행시켜 정부 관계 기관의 정책 입안·실시에의 의미 있는 공헌을 목표로 한다. 셋째, 글로벌 하게 IT를 안전·안심하고 이용할 수 있는 환경을 구축하는 관점으로부터, 일본의 동향에 관해 필요하면서 적절한 것에 관해서는 POC를 통해서 공식적으로 발신하는 것으로써 세계에 공헌하는 것을 목표로 한다.

② 세계의 위협 동향을 파악하기 위한 관민 제휴의 확립과 효율적·효과적인 국제 제휴 활동의 추진

사이버 공간의 안전·안심의 확보를 위해 정부에 그치지 않고 국가 레벨의 CSIRT60,[179] ISP나 여러 기업 내의 CSIRT, 연구기관 등의 주체도 종래부터 긴밀한 국제 제휴를 진행시켜 오고 있다. 이러한 상황을 근거로 해 정부는 특히 강점을 발휘할 수 있는 분야에 주력 한다. 또, 세계의 위협 동향의 파악이나 침해사고에의 대응을 필두로 하는 정보 시큐러티 관련의 국제적인 활동에 관해서 일본 전체적으로 효율적·효과적으로 진행하기 위한 관민 제휴 체제를 구축한다. 이것에 의해 이미 활동을 실시하고 있는 국내의 관계 기관과 국제 제휴 활동에 있어서의 보완·공조의 관계를 축적하는 것을 목표로 한다.

구체적으로는 세 가지의 관점으로부터 대응을 실시한다. 첫째, 일본정부가 가지는 관민 제휴 체제에 대해 해외에 적극적으로 발신하여 국제 제휴에 관한 관민의 역할 분담을 명확히 한다. 두 번째로, 관민 제휴를 통해서 일본으로부터 발신이 가능한 정보를 명확화하기 위한 국내의 제휴 강화를 실시한다. 셋째, 여러 나라의 정부 내외 기관과의 신뢰 관계를 향상시키고 정보 공유를 가속화하기 위해 국제적인 정보 공유와 관련된 사고방식을 정리한다.

덧붙여 상술한 정부가 특히 강점을 발휘할 수 있는 분야로서는 종래부터 여러

179) Computer Security Incident Response Team

나라 정부기관 등과의 사이에 진행해 온 최신의 정책 동향에 관한 의견교환에 더해, 예를 들면, 정부기관, 중요 인프라에 관계가 깊은 위협이나 취약성 등의 리스크 정보의 공유, 정부기관, 중요 인프라 분야에 있어서의 침해사고 대응의 국제적인 제휴 체제 구축이 생각된다. 그 때에는 관계 기관 등에 의한 기존의 국제적인 활동을 활용하면서 진행하는 것으로 한다.

③ 아시아에 있어서의 지혜의 결집과 정보 시큐러티 수준의 향상(One－Asia의 실현)

부정 액세스, fishing, 스팸메일, 표적형 공격, 웹 사이트로부터의 멀웨어(malware)의 감염 등의 위협은 국경을 넘어 생기는 것과 동시에, 지리적, 문화적, 정치적으로 관계 깊은 지역에 있어 어느 정도 공통의 특징이 존재한다. 따라서 이미 유럽 지역 내나 미국을 중심으로 하는 지역에 있어 상징적으로 보여지듯이, 지역 내에 있어서의 제휴를 하게 되어 있다. 이러한 상황을 근거로 해 일본은 아시아에 있어서의 위협에 대응해 정보보호 대책의 강화를 위한 제휴를 추진할 수 있도록 이하의 대응을 실현하는 것을 목표로 한다.

대응은 3개의 관점으로부터 실시한다. 첫째, 사람의 연결의 필요성을 인식해 아시아에 있어서의 위협 동향의 파악·분석을 일본과 함께 실시하는 전문가·연구자를 적극적으로 양성한다. 두 번째로, 현재 국제기관이나 국제 포럼 등에서 논의되고 있는 아시아에 있어서의 공동의 위협 동향의 파악 기능 창설을 위한 대응에 대해 일본에 있어서도 큰 메리트가 있는 형태로 지원을 실시한다. 셋째, 일본은 제1차 기본계획 기간 중에 구축한 미국, 유럽과의 제휴를 더욱 강화하고, 베스트 프랙티스의 공유나 공동의 대응을 통해서 얻을 수 있던 교훈, 정보를 아시아 지역에 적극적으로 환원해 나간다.

덧붙여 대응의 추진에 즈음해서는 효율성을 중시해 기존의 구조를 최대한 활용함과 함께 관계 기관과 제휴하는 것으로 한다.

④ 경제활동의 글로벌화에 대응한 정보 시큐러티의 확보

정부는 일본계 기업의 글로발한 경제활동의 안전·안심을 확보하기 위한 비즈니스 환경 구축을 향한 대응을 실시한다. 즉, 해외의 비즈니스 거점에 있어 중요한 정보 자산이 확실히 지켜질 수 있고 높은 사업 계속성이 확보되는 것을 목표로 한다.

⑤ 표준화를 포함한 일본의 전략적 공헌의 실현

정보보호 대책과 관련되는 통일적인 기준 마련이나 표준화는 종래부터 여러 국제기관에서 행해지고 있다. 최근 표준화의 대응은 종래와 같은 기술적인 영역뿐만 아니라 정책적인 영역에 대해서도 행해지고 있다. 논의는 다방면에 걸쳐 있고, 정보 시큐러티의 분야에 한정해도 폭넓은 활동 중에서 정부가 모든 활동에 관여하는 것은 매우 곤란한 상황이 되고 있다. 한편, 일본에서는 표준화에는 수많은 기업을 포함한 관계 기관이 계속적인 참가·공헌을 통해서 개별적으로 가고 있다.

⑥ 정보 시큐러티 문화의 양성

정보 시큐러티 문화의 양성은 제1차 기본계획에서도 목적의 하나로서 거론한 것이다. 최근 정보 시스템, 인터넷의 분야와 관계가 깊은 국제기관에 있어서의 논의를 통해 의식도 국제적으로 높아지고 있는 상황이다.

진정한 정보 시큐러티 문화의 양성을 위해서는 기업에 있어서의 경영자의 의식 향상이 필요한 것과 같이 세계의 정부 하이레벨의 인식의 공유를 통한 대응이 필요한 것을 인식해 정부는 여러 나라의 정부기관과 협력하면서 G8, APEC 등의 하이레벨의 장소를 활용한 대응을 목표로 한다.

(라) 범죄의 단속 및 권리 이익의 보호·구제

① 범죄 단속을 위한 기반 정비의 추진

법집행기관에 있어서의 단속 체제의 강화, 기능의 향상, 국제 협조의 추진 등의 기반 강화를 한층 추진한다.

게다가 원인 특정이나 범행 과정 해명에 불가결한 정보 제공이 이루어져 피의자의 검거나 피해의 확대 방지에 연결할 수 있도록 법집행기관과 피해자등과의 문의 양호한 협력 관계의 구축을 한층 추진하는 등 범죄에 강한 IT사회 구축을 위한 관민 제휴를 향한 대응을 추진한다.

또, 사이버 테러에 대해서도 그 특성을 고려한 상기의 대응에 의해 준비를 강화한다.

② 범죄 억제를 위한 홍보 계발의 추진

국민이 사이버 범죄의 피해자가 되지 않게, 범죄의 피해 상황이나 수법, 구체적인 대책의 방법 등에 관한 홍보 계발을 한층 추진한다.

③ 권리 이익의 보호·구제를 위한 기반 정비의 추진

국민의 기본적 인권에 충분히 배려하면서, 사이버공간의 권리 이익의 보호·구제를 위한 기반의 한층 더 정비에 노력한다. 구체적으로는, 정보를 맡기는 측의 권리 이익을 정보를 맡는 측이 보호·구제하는 대응과 관련되는 정보개시의 촉진, 사이버공간의 안전성·신뢰성을 향상시키는 기술의 개발·보급 등에 대처한다.

4. 기구의 정비

일본의 정보 시큐러티는 정부가 주도하여 민간의 참여를 적극적으로 이끌어 내는 형태이다. 따라서 정부의 각 기관이나 회의의 기능이 강화되고 있고, 이들은 다양한 방법으로 민간의 참여를 유도하고 있다.

가. 내각관방 정보시큐러티대책추진실

정보시큐러티대책추진실은 인터넷의 급속한 이용확대 등 국민생활의 IT발전에 따른 부정액세스(해킹), 컴퓨터 웜 바이러스 확산 등에 대처하기 위해 2000년 2월 내각관방장관 산하에 설치되었다.

주요역할은 각 정부부처와 협력하여 민관전문가로 구성된 비상근팀의 조언을 받아 전자정부의 정보보호 확보 및 중요인프라 사이버테러 대책 등 민·관의 정보보호 확보를 위한 정책추진을 총괄·전담하고 있다.

또한 내각총리대신 산하 내각 '고도정보통신네트워크사회추진 전략본부(IT전략본부)'에 설치된 정보시큐러티대책추진회의와 민간전문가로 구성된 정보시큐러티 전문조사회의 사무국을 담당하면서 각 부처 업무조정 역할을 한다.

1) 긴급대응지원팀(NIRT: National Incident Responce Team)

'전자정부의 정보시큐러티확보를 위한 액션플랜'(2003.10)을 근거로 전자정부나 민간 중요인프라사업자 등의 정보시스템에 대한 사이버테러 등 국민생활에 중대한 영향을 줄 우려가 있는 정보보호에 관련사항에 대해 각 성·청의 정보보호대책 입안시 이에 대한 필요한 조사·조언 등을 실시하기 위해 2002년 4월에 설치하였다.

민 관 컴퓨터보안전문가 17명으로 구성되어 있고, 총괄·지도는 독립행정법인인 '통신총합연구소'의 '비상시통신그룹장'이 담당하고 있다.

주로 사이버공격 등으로 전자정부·중요인프라사업자 등의 정보시스템에 관한 장애가 발생하거나 장애발생이 예상되어 정부차원의 위기관리대응이 필요한 정보시큐러티 관련 사안에 대한 대응활동을 하고 있다.

2) 전문조사팀

정보보호시책의 시행에 대하여 중장기적 관점에서 조언을 하고 중요 인프라 방호를 위한 사이버테러대책을 강구하기 위해 정보시큐러티 대책추진실 산하에 설

치하였다.

주요 추진실적으로는 2000년 12월 '중요인프라의 사이버테러대책에 관한 특별행동계획'을 발표하여, 사이버테러 등 정보통신네트워크, 정보시스템을 이용한 국민생활이나 사회경제활동에 중대한 영향을 끼칠 가능성이 있는 어떠한 공격으로부터도 중요 인프라를 방호하기 위한 정책을 심의·수립하였다.

나. 내각 고도정보통신네트워크사회추진 전략본부(IT전략본부)

정보통신기술의 활용에 따라 세계적으로 진행 중인 급격하고도 대폭적인 사회경제구조의 변화에 신속·정확하게 대응할 필요성을 고려하여 고도정보통신네트워크사회의 형성에 관한 시책을 신속하고도 중점적으로 추진하기 위해 2001년 1월 내각에 설립되었다.

전략본부는 고도정보통신네트워크사회 형성에 관한 중점계획을 작성, 그 시행을 추진하며, 기타 고도정보통신네트워크사회의 형성에 관한 중요시책을 심의하고 이를 위해 사안별 민관 전문가를 소집하여 '전문조사회'를 운영하고 있으며, 이 조사회는 목적이 완료되면 해체된다.

'시큐러티대책추진회의'는 내각관장 부장관을 의장, 내각위기관리감을 부의장으로 하여 정부부처 국장급으로 구성되며, 저오보호 대책추진을 담당하고, '정보시큐러티 전문조사회'는 민간전문가들로 구성되어 민관분야의 정보보호 대책추진에 관한 사항의 조사, 검토를 전담한다.

다. 경찰청 사이버포스 센터

하이테크범죄, 사이버테러를 예방하고 피해확대를 방지하기 위해 2001년 경찰청 정보통신국 사이버테러 대책기술실에 설치되었다.

전국 경찰기관에 설치되어 있는 인터넷 접속점의 IDS(Intrusion Detection System)[180]를 24시간 감시하여 관련정보를 수집·분석하는 관제장비인 '검지네트워

180) 통신회선을 감시하여 네트워크에의 침입을 검지해 관리자에게 통보하는 시스템. 네트워크상을 흐르는 패킷을 분석하여 패턴 조합에 의해 부정 액세스라고 생각되는 패킷을 검출하여 관리자에

크시스템'을 운영하여 사이버테러 조기탐지 및 긴급대응 업무와 함께 관련분야 연구개발과 전문 인력에 대한 고육훈련을 실시하고 있다.

경찰청에서는 시큐러티 포털사이트@Police(http://www.cyberpolice.go.jp)를 운영하고 있는데, 여기서는 민간부문과의 협력 체제를 바탕으로 세계정보보호 동향, 인터넷 치안정세정보를 비롯하여 보안취약점, 웜 바이러스의 예, 경보, 보안권고문 등 광범위한 자료와 함께 어린이·개인컴퓨터유저·서버관리자 등을 대상으로 강의자료를 통한 기초지식 함양에도 주력하고 있다.

라. 총무성

총무성 정보통신정책국 정보유통진흥과는 '국민을 위한 정보시큐러티 사이트(http://www.soumu.go.jp/joho_tsusin/security/index.htm)를 개설하고 일반국민이 안심하고 인터넷을 사용할 수 있도록 정보보호 필요성, 기초지식, 용어설명, 실제 일어날 수 있는 사고·사례를 소개하고, 이용대상별 정보보호대책을 구분하여 최종사용자(학생·일반이용자), 홈페이지 개발자(인터넷서비스 제공업체, 사설서버이용자), 기업·조직 업무이용자(직원·정보관리담당자) 등을 대상으로 상세한 보안대책을 제시하고 있다.

그 자세한 내용을 살펴보면, 현재의 인터넷의 일반적인 사용법은 전자 메일의 이용, 홈 페이지로부터의 정보수집, 쇼핑 사이트의 이용 등인데, 이러한 일반적인 이용 방법에 관해 필요한 정보보호 대책을 제공하고 있다. 우선 인터넷의 익명성에 관해 알려주고, 개인정보의 취급에 관한 유의사항, 프라이버시의 보호, 바이러스 감염에 주의할 것과 악의가 있는 홈 페이지 등에 조심하도록 하며, 봇넷 등에 감염되지 않기 위해서 소프트웨어를 최신으로 유지하도록 지시하고, 넷 옥션에 있어서의 위험성을 알려주고, 나아가 쇼핑 사이트의 이용, 체인 메일의 문제점, 스팸메일에의 대응, 상시 접속의 위험성, 스파이웨어와 fishing 사기에 주의할 것, 휴대전화에 있어서의 시큐러티 확보의 중요성과 대책, 파일공유소프트웨어의 이용과

게 통지한다. 제품에 따라서는 의심스러운 통신을 절단 하는 등 방위 조치를 강구하는 경우도 있다. 부정 액세스로 자주 이용되는 수단을 패턴화하여 기록해 두고 실제로 흘러오는 패킷과 패턴을 비교하는 것에 의해 정상적인 통신인지의 여부를 판단한다.

위험성, 「원클릭 사기」, U S B 메모리로부터의 바이러스 감염, 나아가 마지막으로는 총무성에서 경제산업성과 제휴하여 추진해 가고 있는 보트 방지를 위해 일반인들이 알아야 할 보트의 위험성과 대책을 설명하고, 인터넷에 있어서의 안전성의 확보를 위한 일반 유저들의 주의사항을 제공하고 있다.

마. 경제산업성

경제산업성은 '정보시큐러티에 관한 정책, 긴급정보 사이트'(http://www.meti.go.jp/policy/netsecurity/index.html)를 운영 중이다. 일본정부의 각종 IT정책은 물론 정보보호통합전략 등을 한곳에 모아 놓은 종합포털사이트로 정보보호 각 부문별 상세자료를 수록하고 있다.

1) ISO/IEC15408에 근거한 IT 시큐러티 평가인증 스킴의 창설

정보 시스템의 개개의 제품·시스템 등의 시큐러티 기능을 정의·공통화 하여, 개별 제품 등에서의 시큐러티 요건을 정하고 그 기능을 보증하는 레벨을 마련하여 객관적으로 평가한 후 그 평가가 적정한 방법인 것을 인증하는 것을 말한다.

2) 암호 기술의 평가(CRYPTREC)

CRYPTREC이란 Cryptography Research and Evaluation Committees 의 약어이며, 전자정부 추천암호의 안전성을 평가·감시해 암호모듈 평가기준 등의 책정을 검토하는 프로젝트이다.

총무성 및 경제산업성이 공동으로 개최하는 암호기술 검토회와 독립행정법인 정보통신연구기구(NICT) 및 독립행정법인 정보처리추진기구(IPA)가 공동으로 개최하는 암호 기술 감시위원회 및 암호모듈위원회로 구성된다.

일본이 목표로 하는 세계 최첨단의 IT 국가를 구축하려면 기반이 되는 전자 정부의 시큐러티를 확보할 필요가 있어, 안전성이 뛰어난 암호 기술을 이용하는 것

이 불가결하다. 이 목적으로 인해 객관적인 평가에 의해 안전성 및 실장성이 뛰어난다고 판단된 암호 기술을 리스트화하는 암호기술 평가프로젝트가 2000년도부터 3년간의 예정으로 조직화되어 CRYPTREC(Cryptography Research and Evaluation Committees)이라고 불리게 되었다.

CRYPTREC은 공모된 암호 기술 및 업계에서 널리 이용되고 있는 암호 기술을 평가·검토해, 안전성 및 실장성이 모두 뛰어난 것을 선택했다. 총무성과 경제산업성은 이 평가 결과를 근거로 2003년 2월 20일에 「전자정부」에 있어서의 조달을 위한 추천해야 할 암호의 리스트(전자정부추천 암호리스트)를 공표했다.

2003년 2월 28일에는 행정 정보 시스템 관계 과장 연락 회의에서 각 부성이 정보 시스템을 구축해 암호를 이용하는 경우에는 가능한 한 전자 정부 추천 암호 리스트에 게재된 암호의 이용을 추진하는 취지의 「각 부성의 정보시스템 조달에 있어서의 암호의 이용방침」이 승낙되었다.

총무성 및 경제산업성은 2003년도 이후에도 전자 정부의 안전성 및 신뢰성을 확보하기 위해서 CRYPTREC 프로젝트의 활동을 계속하는 것을 결정했다. 전자 정부 추천 암호 리스트에 게재된 암호의 안전성을 감시·조사하기 위한 암호 기술 감시위원회가 새롭게 설치되고, 또 암호를 실장한 암호 모듈의 일본에 있어서의 평가 기준을 확립하기 위해서 암호 모듈 위원회가 설치되어 오늘에 이르고 있다.

3) 정보 security management의 인증제도(ISMS 적합성 평가제도)의 창설

ISMS(Information Security Management System)란 기업이나 조직이 자신의 정보 시큐러티를 확보·유지하기 위해서 규칙(정보보호정책)에 근거한 시큐러티 레벨의 설정이나 위험율 평가의 실시 등을 계속적으로 운용하는 구조를 말한다. ISMS에 요구되는 범위는 ISO/IEC15408 등이 정하는 것 같은 기술적인 정보보호 대책의 수준은 아니고, 조직 전체에 걸친 시큐러티 관리 체제를 구축·감사하여 위기관리를 하는 것이다.

ISMS를 그 조직이 보관·유지하고 있는지의 여부를 제삼자가 인정하는 제도를 'ISMS 적합성 평가제도'라고 한다. '정보처리 서비스업 정보 시스템 안전 대책 실

시 사업소 인정 제도'에 대신하는 정보처리 서비스업 사업자에 대한 ISO/IEC17799 : 2000 및 BS7799-2 : 1999에 근거한 평가 인정 제도가 있다. 현재 일본정보처리개발 협회(JIPDEC)를 중심으로 2002년부터 정식 운용되고 있다.

제4절 독일과 EU의 정보통신망 정부규제 현황

1. 정보통신망에 대한 정부규제의 의의

사이버 위험은 네트워크와 정보기술로 인해 사이버 공간에서 발생할 수 있는 발생 가능한 손실 가능성이라고 할 수 있으며 사이버 위험의 특징은 네트워크화와 정보화의 진전으로 정부, 기업, 학교 등 사회 전반에서 인터넷망에 대한 의존도가 심화되고 모든 영역이 개방형 네트워크로 연결되면서 어느 한 곳에 대한 사이버 공격으로 인해 특정 기술의 약한 고리에서 발생한 위험이 전 사회를 총체적 위기로 몰아갈 수 있는 잠재적 가능성이 상존하게 된다. 즉 초국가 네트워크로서의 사이버 공간의 특성상 영역 간, 국가 간 물리적 경계가 존재하지 않기 때문에 사이버 공간 내의 어느 한 곳의 네트워크가 위험에 처하게 되면 전체의 네트워크에 파장을 미치고 우리의 삶 한 부분에 한정되지 않고 삶 전체를 위험에 처하게 만드는 네트워크 도미노 현상을 일으킬 수 있게 된다.

2009년 7월 초순에 발생한 인터넷상의 DDoS 사태는 사이버 위험이 현실화됨으로써 사회에 미칠 수 있는 파국적 영향력과 금융거래 중단 등을 이어지는 네트워크 도미노 현상을 보여줌으로써 사이버 세상의 위험성을 각인시켰다.

2. EU 및 독일의 정보통신에 관한 보안 법제 현황

가. EU 사이버 정보 보안 법제현황

오늘날 사이버 공격의 지능화, 다양화로 인해 기존의 기술적 대응만으로는 한계가 있으므로 새로운 유형의 악성코드 및 봇넷, 피싱과 같은 사회공학 공격의 사전

적 예방을 위한 정보보호 인식의 확산이 요구되고 있다. 이와 관련하여 EU는 정보 보안 인식제고에 지속적인 노력 및 투자를 행하여 왔으며, 최근 정보 보안 인식 실태조사 및 가이드라인 개발 등 활발한 연구를 계속하여 진행 중이다.

EU의 정보 보안 인식제고 노력은 EU집행위원회 산하 정보사회와 미디어 이사회(INFSO DG: Information Society and Media Directorate and General)와 유럽 네트워크 및 정보 보안기구(ENISA·European Network and Information Security Agency)의 정보화 및 정보 보안 정책에 잘 나타나고 있다. INFSO DG의 관련 정책으로 "eEurope", "안전한 정보사회를 위한 전략", "미디어 리터러시(literacy)", "안전한 인터넷 플러스 프로그램" 등이 있으며, ENISA는 "ENISA의 역할과 비전" 및 각종 가이드라인을 통해 활발한 정보 보안 인식을 제고하며 활동을 수행하고 있다.

EU의 정보 보안 인식제고 활동은 다음과 같은 특징을 가진다. 첫째, 정보 보안 인식제고를 위한 프로세스의 마련 및 효과성 측정을 위한 핵심성과지표 개발 등 체계화된 정보 보안 인식제고 프로그램을 마련하는 것이다. 둘째, 정부와 다양한 분야의 민간기업간 긴밀한 협조체계를 구축함으로 효율적, 효과적 정보보호 인식제고 업무가 수행될 수 있도록 하는 것이다. 셋째, 각종 멀티플라이어(multiplier)를 활용한 대상별, 수준별 정보보호 교육 및 훈련의 중요성을 강조하는 것이다. INFSO DG 및 ENISA의 연간보고서 및 가이드라인 등에 대한 분석을 통해 우리 법제에 많은 시사점을 도출해낼 수 있을 것이라 여겨진다.

나. 독일 인터넷 정보 보안 법제현황

1) 정보통신법

독일은 온라인 공간의 정보보호를 위하여 2004년 「정보통신법(Telekommunikations- gesetz: TKG)」을 제정하였다. 이는 정보기관의 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷서비스 제공자 등 정보통신서비스를 제공하는 모든 책임자에게 고객정보를 정부에서 접근 가능한 상

태로 유지할 의무를 규정하고 있으며, 그러한 데이터는 정부의 감시기관이 직접 접근할 수 있어야 한다고 한다.

「정보통신법」은 상업적인 인터넷서비스 제공자뿐만 아니라 비상업적인 서비스제공자나 전자게시판 운영자에 대해서도 적용되다. 만일 정보통신서비스제공자가 이러한 조치를 실행하지 않을 경우 그 운영을 중지시킬 수 있다. 게다가 동법이 요구하는 기능실행을 위한 시스템 설치비용은 정보통신서비스 제공자 스스로 부담해야 한다.

2) 연방법률관보

연방법률관보는 연방정보기술보안국(BSI: Bundesamt fur Sicherheit in der Informationstechnik)을 설치하고 연방정보기술보안국의 임무, 권한과 관련한 법률을 1990년에 제정하여 1991년부터 발효하고 있다. 연방은 내무장관의 관할 하에 연방정보기술보안국을 독립적인 연방관청으로 설립하여 정보기술의 보안을 제고하기 위한 임무를 다음과 같이 규정하고 있다.

(i) 정보기술을 적용했을 때 야기되는 보안 위험을 연구하고 보안 조치, 정보보기술 보안을 위한 정보기술적 방법 및 장치 개발

(ii) 정보기술 시스템 및 그 구성요소를 검사하고 평가하기 위한 기준, 방법 및 도구 개발

(iii) 정보기술 시스템 및 그 구성요소의 보안을 검사하고 평가하여 보안인증서 부여

(iv) 제도적으로 보호되어야 할 정보(비밀정보)를 가공하고 전송하기 위해 사용될 정보기술 시스템 또는 그 구성요소를 인가하여 인가된 코딩 장치의 운영을 위해 필요한 키 데이터를 생성

(v) 자문 또는 감독 임무를 맡고 있는 정보기술보안 담당자는 연방기관-연방정보보호관리청-을 지원

(vi) 경찰 및 형사소추 기관의 법적 임무 수행 지원

(vii) 테러활동을 감시하거나 정보활동을 하면서 수집한 정보를 활용하고 평가하는 작업지원
(viii) 정보기술보안 문제 발생시 생산자, 유통자 및 사용자에게 자문 요청

3) 통신서비스법(Teledienstegesetz, TDK)

(i) 인터넷서비스 제공자의 정보차단의무

일정한 요건 하에서 위법한 정보를 인지한 경우의 인터넷서비스 제공자의 정보차단의무를 규정하고 있으며 의무를 이행하지 않은 경우에는 면책되지 않는다.

(ii) 인터넷서비스 제공자의 면책 조항

자신의 정보와 타인의 정보를 구분하고 타인의 정보를 제공한 경우에도 캐싱(caching)[181]과 호스팅(hosting)[182]의 경우를 별도로 분류하여 특정 사유에 해당하는 경우 인터넷서비스 제공자가 면책됨을 규정하고 있다.

4) 연방데이터보호법(BDSG)

독일은 개인정보를 보호하기 위한 기본법으로서 「연방데이터 보호법(Federal Data Protection Acts)」을 제정하여 시행하고 있다. 동 법은 개인정보의 정의에서부터 정보주체의 권리와 정보처리자의 각종 의무, 제3국으로의 정보이전, 비디오감시, 익명성, 스마트카드, 민감한 정보의 수집 등에 대한 내용을 담고 있다.

5) 정보통신서비스 정보보호법(TDDSG: Teledienstdatenschutzgesetz),

---

181) 캐싱이란 명령어와 데이터를 캐시 기억장치 또는 디스크 캐시에 일시적으로 저장하는 것을 의미한다.
182) 호스팅이란 인터넷 접속 서비스 제공자가 제공하는 서버의 보관 서비스로 일반적인 경우 콘텐츠 제공자가 서비스 제공자의 시설 설치 장소를 빌려서 독자적인 서버를 설치하는 것을 의미한다.

동 법은 정보통신서비스 이용관계에서의 개인정보의 수집·처리에 관하여 규율하여 인터넷 포털사이트 운영자, 이메일서비스 제공자, 온라인 게임서비스 제공자 등의 정보통신서비스 제공자가 고객정보를 이용·처리하는 행위에 직접적으로 적용된다. 동 법은 정보 보안 범위, 서비스제공자의 사용자의 개념 정의, 정보 보안 원칙, 서비스제공자의 의무, 보호되는 정보의 내용, 연방정보보안감독관의 역할 등에 대해서 규정하고 있다.

6) 전자서명법

「전자서명법(Act on Online Conditions for Electronic signatures)」은 EU에서 1999년 12월에 채택한 전자서명 지침에 따라 제정되었는데 주로 온라인상의 안전성 확보를 위한 인프라 관련 조항이 중심내용으로 되어 있다.

3. EU의 인터넷상에서의 정보보안 안정성 강화 정책

가. 유럽네트워크정보보안청(ENISA)

EU는 정보보안에 대한 유럽 각국의 초국가적 협력을 위해 2004년 유럽네트워크정보보안청(ENISA)을 설립해 공동 대응하고 있다

ENISA는 보안사고 처리를 위한 데이터 수집, 프레임워크 및 신뢰지수 측정방안 개발, 보안정보 공유 및 경고시스템의 실행가능성 검토 등을 수행한다. 또한 ENISA는 유럽 각국에 컴퓨터비상대응팀(CERT) 구축을 지원하고 있는데 2005년 9개국에서 2008년 6월 현재 15개국에 CERT 설립을 지원하였다. 또한 각국의 수준에 맞는 컨설팅을 실시하며 우수 CERT 활동 사례 등도 전파하는 것을 주 임무로 하고 있다.

나. 컴퓨터비상대응팀(CERT)

유럽에도 미국에서 발생한 9. 11 테러와 같은 디지털9/11 테러의 우려가 있다며 2008년부터 3개년 프로그램을 통해 공공부문 전자통신 활성화 및 디지털 9/119/11 위협 완화역량을 갖출 계획을 수립하고 있다.

다. 사이버방어센터

NATO(북대서양조약기구)는 사이버 전쟁에 대한 연구수행 및 대응을 위해 2009년 설립예정으로 에스토니아에 사이버방어센터The Cooperative Cyber Defence Centre of Excellence)를 설립할 계획으로 있는데 독일, 이탈리아, 라트비아, 리투아니아, 슬로바키아, 스페인 등 6개국은 사이버방어센터를 위한 예산과 전문요원을 지원하고 미국은 참관국 자격으로 동참한다. 사이버방어센터는 에스토니아의 수도 탈린에서 30명의 직원으로 운영할 예정이며 사이버테러방어관련연구・협의・훈련 등 프로젝트를 수행한다.

라. 조기경보시스템(EWIS)

EU는 국가사이버테러 발생시 효과적으로 대응하기 위해서 사이버 공격에 대한 조기경보시스템 및 복구시스템 개발이 필요하다는 인식하에 유럽조기경보시스템(EWIS : European Warning and Information System)의 구축을 추진하고 있다.

제5절 정부규제의 한계

정보통신망의 정부규제는 빠르게 변화하는 정보통신기술과 서비스의 특성을 반영하는 데에는 한계가 있을 수밖에 없다. 때문에 과도한 정부규제 및 법적 규제는 인터넷 서비스 기업의 신규 서비스 발굴 및 시장진입을 제한하여 인터넷 산업의 발전을 저해할 소지도 있다.

정부규제는 타율적 책무, 즉 귀책성을 강조한 체계이다. 이용자와 인터넷 기업간의 관계는 유해한 상황에 따른 법률적 보호관계로 한정하고 있으며, 책임과 권

한이 명확하고 신속하다. 그러나 관련주체들 간의 대립적 관계를 전제로 하며, 이용자 간의 관계에서 파생되는 다양한 가치들을 대상으로 하기에 모호한 부분이 많다. 예를 들어, 불법 콘텐츠로부터 이용자 보호 및 피해구제는 명확하지만 이용자 간의 위해성 여부와 수준의 판단이 어려운 경우에는 효율적이지 않다. 따라서 규제비용이 규제 편익보다 높을 수밖에 없으며, 법률적 열거주의를 통해 개별 관계를 규율하지 않는 한, 다양한 가치관계들을 포괄하기 어렵다.[183]

또한, 강제력을 수반하는 법에 의한 통제만을 유지한다면 다른 매체와는 달리 쌍방향성, 탈중앙통제성, 접근용이성, 다양성, 익명성, 복제용이성, 국제성, 초공간성 등 다양한 특성을 가지는 인터넷의 속성 때문에 쉽게 실효성을 확보하기가 어려운 경우가 생긴다. 사실 법적 규제는 무척 효과적이며 반드시 필요한 규제이지만 규제 장치에 변화를 주기 위해서는 여러 가지 절차를 거쳐야 하기에, 인터넷의 변화무쌍한 속성으로 인하여 규제의 수단이 기술이 변화할 때마다 이에 맞추어 대응하지 못할 수 있으며 새로운 인터넷의 유동성을 제어하지 못할 소지도 있다. 그러므로 향후의 법·정책 등 정부규제는 오남용 되는 정보의 유통 자체를 통제하고, 정보서비스 제공자나 데이터 호스트 등의 활동의 규제에는 자율규제 방식을 확산하는 방향으로 변화를 줌으로써 오남용의 폐해를 실효성 있게 차단하는데 중점을 두는 것이 효과적일 것으로 사료된다.[184]

183) 황용석・이동훈・김준교, 미디어 책무성 관점에서의 인터넷 자율규제제도 비교연구, 언론과 사회, 2009년 봄 17권 1호, 성곡언론문화재단, 2009. 111면.
184) 사단법인 한국인터넷기업협회, 인터넷 비즈니스 자율규제시스템 발굴 및 시범적용 방안 연구, 한국전산원, 2005. 10면.

제 4 장 정보통신망의 자율적 활성화 방안

제1절 우리나라 자율규제의 나아갈 방향

1. 이용자 보호 및 권익제고를 위한 자율규제의 활성화

가. 외국의 사례를 통해 본 이용자 보호 및 권익제고 현황

정보통신망의 특성상, 인프라의 급속한 확장과 널리 보급된 망 위에서 이용자들이 이용할 수 있는 서비스도 급속도로 늘어났다. 다만 여태까지는 정보통신망의 특성을 이해하여 정보통신망을 위한 맞춤식 규제는 다소 부족한 측면이 있었다. 그렇기에 앞으로는 이용자 측면에서 보았을 때 나타날 수 있는 부작용 및 역기능 등에 대한 현실적 대응 방안을 마련하는 것이 무엇보다 우선시 되어야 할 것이다. 앞서 검토한 해외의 사례들을 살펴보면 미국의 경우 Industry Consortium for the Advancement of Security on the Internet(ICASI)은 전 세계적으로 사용되고 있는 여러 제품들이 당면하는 보안 위험에 대한 대응을 논의하기 위한 비영리 단체로 선도적인 IT 기업들이 참가하고 있다. ICASI는 회원 회사들이 가지고 있는 기술적 역량을 활용해, 복잡하지만 중요한 보안 문제를 해결하는 노력을 하고 있다. 이러한 활동은 기업용 사용자, 일반사용자, 정보 및 IT 인프라를 보호하는 역할을 한다. ICASI의 대표적인 프로젝트 두 가지로 첫째는 통합보안사고대응전략(USIRP: The Unified Security Incident Response Plan)이며, 둘째는 취약점의 공개 및 대응에 관한 공동 프레임워크(CVRF: Common Frameworks for Vulnerability Disclosure and Response)이다.

통합보안사고대응전략(USIRP)은 인터넷 보안강화를 위한 방법을 논의하는 토론의 장을 열고 회원사들 간의 공조를 통해 신속하고 효율적으로 인터넷보안을 해결하기 위한 절차와 기술적 툴을 제공한다. 또한 USIRP를 통해 회원사들은 보안침해사고 대응센터의 대응절차와 보안담당 직원이 공통적으로 적용해야 할 정식

프레임워크 구축 및 보안위협사례의 해결을 위한 중요한 정보를 공유하게 된다. 이러한 활동으로 인하여 기업뿐만 아니라 일반이용자에게도 정보보호의 역할을 해주게 되어 일반이용자들의 보안에 대한 기여를 하고 있다.

National Cyber Security Alliance (NCSA)도 STAYSAFEONLINE활동을 하고 있는데, NCSA는 이용자들의 안전한 인터넷 사용 및 사이버 인프라 보호를 위하여 2001년에 구성된 민관 공조 단체로써 국토안보부(DHS), 마이크로소프트, 시스코(Cisco), 시만텍(Symantec), SAIC, EMC, McAfee 등 세계적인 IT기업과 비영리 단체가 참여하고 있다. 이 단체는 National Cyber Security Awareness Month를 지정하여 매년 10월에 이용자와 근접한 학교·단체 등을 중심으로 교육과 웹사이트, 소셜미디어 채널을 통하여 보안에 대한 정보를 전달하는 활동을 하고 있다. 이는 6년째 진행되는 행사로 이러한 활동을 통하여 모든 이용자들이 "보안"을 컴퓨터 사용에 필수적인 요소로 생각하도록 하고, 그 외에 NCSA의 활동으로는 2009 National Cyberethics, Cybersecurity Baseline Study 등이 있는데 이러한 활동을 통하여 초·중·고등학생 및 교사들의 사이버윤리·안전·보안에 대한 교육·훈련 등이 이루어지고 있다.

일본의 경우 정보통신망 규제를 위하여 지방자치단체와 기업, 개인 등이 자발적으로 참여하도록 운영하고 있으며 정부가 개입하여 보안 확보를 위한 강제조치를 하는 경우는 거의 없는 것으로 나타났다. 대표적인 정보통신망 자율규제를 위한 협력 체계로는 사이버클린센터(Cyber Clean Center)가 있는데 이곳에서는 가짜 서버인 "honeypots"를 제공해서 감염된 컴퓨터의 IP주소를 얻고 ISP와의 협조를 통해 감염된 컴퓨터의 사용자에게 통보를 한다. 대부분의 사용자에 대한 통보가 이메일로만 행해지는데 비해 사이버클린센터에서는 사용자에게 이메일과 함께 웹사이트 링크를 제공한다. 이러한 방법으로 감염된 컴퓨터의 사용자에게 봇 치료를 할 수 있는 웹사이트의 URL을 함께 보내고 있다. 이렇게 일본의 사이버클린센터는 이용자에 대한 직접적인 통보와 치료방법의 직접적인 제시를 통하여 이용자의 보호와 권익제고에 힘쓰고 있다.

독일의 경우는 온라인상의 자율규제가 청소년보호를 중심으로 이루어지고 있는 것으로 나타나고 있다. 멀티미디어 서비스 제공자의 자율규제 기관(FSM)은 청소

년미디어보호에 관한 주간협약(JMStV)이 체결된 이후 텔레미디어(온라인 내용) 분야에서 유일하게 승인된 자율규제기관으로써 이 기관의 목적은 온라인 미디어에서 청소년미디어보호의 강화, 불법적이고 청소년에게 유해한 온라인 콘텐츠의 척결 및 아동과 청소년들을 위한 미디어 전문지식의 전달에 있다. 현재 이 기관에는 통신, 방송, 온라인 분야에서 망라된 44개의 기업과 단체들이 등록되어 있으며, 지난 11년 동안 FSM은 인터넷상에서의 청소년미디어보호 문제에 관해서 정치적 사회적 담당자로서 확고한 위치를 지켜오고 있다. 특히 사무소는 지속적인 입장표명을 통해서 정치적 의사형성의 과정에서 전문적 지식을 제시하고 있다.

멀티미디어 서비스 제공자의 자율규제기관의 핵심적인 업무로 첫째, 회원들에게 최근의 법률적 기술적 발전에 관한 정보를 제공하고 구체적인 질문에 자문을 하는 것과 지속적으로 회원의 온라인 제공물을 심사하여, 청소년유해적인 내용이 인터넷상에서 호출되지 않도록 확보하는 것 등 적극적으로 회원들을 책임지고 돌보는 것이 있다. 둘째로는, 이의제기부서의 역할이 있다. 모든 인터넷 사용자는 청소년미디어보호의 영역에서 가벌적이고 청소년에게 유해하며 청소년의 성장을 저해하는 온라인 자료에 대해 이의를 제기하고 심사를 하도록 하기 위해서 이 부서를 무료로 이용 가능하다. 셋째, 포괄적인 이용자 계몽과 아동의 미디어능력 촉진에 힘쓰고 있다. 이상에서 살펴본 대로 독일의 경우도 이용자 보호를 위한 계몽활동과 이용자를 위한 적극적인 자문활동과 특히 아동에 대하여 미디어의 위험에 대한 정보를 알려주는 것에 중점을 두고 활동하고 있다.

이상에서 살펴보았듯이 미국, 일본, 독일의 자율규제에 있어서 기업과 정보 및 IT인프라의 정보보안에 관한 노력과 더불어 일반이용자들을 위한 실천적 방안들이 마련되어 있다. 일반이용자들을 위한 교육과 보안에 관한 정보전달, 감염된 컴퓨터의 이용자에게 직접적인 통보와 치료방법의 전달, 적극적으로 이용자에게 최신의 법률과 기술 발전에 관한 정보제공, 구체적 질문에 대한 자문 등으로 이용자들에게 실질적 도움을 주고 있다. 우리나라에서도 해외의 이러한 특징적 활동들을 반영하여 자율규제의 방향성을 만들어 나가야 할 것이다.

나. 이용자 보호 및 권익제고 활성화 방안

정보통신망 자율규제 활성화를 위한 제고사항들을 살펴보면, 먼저 정보통신망 자율규제 기구 및 단체의 운영에 중요한 원칙에 대한 확립이 있어야 한다. 그 원칙으로 첫째, 투명성(transparency)의 확보가 있다. 기존의 기업 간 자율규제에 있어 문제가 되었던 것은 사업자와 이용자 간의 정보 격차 및 활동내용·운영기준·실행규칙의 투명성 확보 문제이다. 또한 정치적 이해관계자 및 이익집단으로부터 자유로울 수 있도록 명확한 절차요건 마련의 필요성이 있다.

둘째, 책무성(accountability)의 원칙으로 이용자들이 정보통신서비스 제공자 등에게 신고 사항이 있는 경우 이를 신속·정확하게 처리할 수 있는 공개적인 절차가 필요하다. 또한 이러한 처리절차는 공평하고 효율적이며 적절한 수준을 유지해야 하고, 이익집단과 자율규제 기구 간의 명확한 분리를 통하여 순수한 자율규제를 표방할 수 있어야 한다.

셋째, 목표의 명확성(targeting)이 있어야 한다. 명확한 목표 설정을 통하여 업무처리를 함에 있어 우선순위가 확실히 정해져야 한다. 예를 들어, 정보통신망 자율규제의 목표로 될 수 있는 것에는 청소년 유해매체 확산방지 조치, 저작권 보호, 불법게시물에 대한 임시 조치 등이 있을 수 있고 이에 대한 우선순위 결정의 기준이 필요하다 할 것이다. '이용자 보호'(이에는 책임 있는 표현의 자유 보장, 이용자 개인정보의 보호, 이용자의 지적재산권 보호, 이용자의 인격권 침해보호 및 피해구제 절차 등이 포함될 수 있음)는 중요한 목표로 고려될 수 있을 것이다.

넷째, 균형성(proportionality)의 원칙이다. 규제를 준수하는 회원에 대한 보호 메커니즘과 회원사에 대한 보상과 견제의 균형이 마련되어야 한다. 일본의 「Provider 제한법」과 같이 정보통신서비스 제공자가 자율적으로 적절한 수준의 규제 장치를 마련하고 이를 충분히 준수하였지만 사고가 생기는 경우의 면책 방안 등이 제시되어야 한다.

다섯째, 일관성(consistency)의 유지이다. 자율규제의 여러 장치들은 관련된 법령·제도 등과 유기적으로 맞물려야 한다. 유사한 문제 발생시 일관성 있는 규제 방법이 적용 되어야 한다.

정보통신망의 자율규제 기구의 발전을 위하여 고려할 사항으로 이용자 피해구제 절차에 대하여 업계 자율규약이 마련에 대한 문제가 있다. 또한 이용자의 표현의

자유와 책임의 균형을 고려하여야 하고, 정부기관과의 협력이 요구된다. 업계와 공적 규제기구 간의 정보통신망 규제 핫라인 구축 등의 방안이 있어야 할 것이다. 예를 들어 방송통신심의위원회, 혹은 사이버수사대와 정보통신서비스 제공자와의 핫라인 구축을 고려해볼 수 있을 것이다. 핫라인 운영시 업계의 자율적인 대응이 가능한 사안과 정부기구의 개입이 필요한 사안을 구분하여 조치를 취하여야 할 것이다.

그리고 이용자 참여형 규제모델의 개발에 있어 이용자들의 자발적인 'peer review group' 운영을 활성화하고, 이용자의 자율적 모니터링 및 신고체계에 기반을 둔 모니터링 활성화, 현행 제도 개선 요소 연구 및 정책에 대안을 제시하여야 한다.

이용자의 인식제고를 위한 효율적인 방안으로서 다음과 같은 것이 검토될 수 있다. 한국인터넷자율정책기구(KISO)의 활동 중에는 회원사간 게시물 정책공조 및 게시물로 인한 이용자 권익보호 및 피해구조를 위한 공동정책개발 활동이 있다. 이러한 활동의 일환으로 KISO의 주도 하에 이용자 피해구제에 대한 업계의 자율규약을 제정하는 방안을 생각할 수 있다. 이 규약 수립에는 앞서 언급했듯이 이용자의 표현의 자유와 책임에 대한 균형적인 고려가 기반이 되어야 한다. 또한 KISO와 방송통신심의위원회 및 한국인터넷진흥원, 사이버수사대간의 핫라인을 구축하는 것도 좋은 방안으로 사료된다. 핫라인 운영시 명심해야 할 사항은 업계의 자율적인 대응이 가능한 영역과 정부의 개입이 필요한 사안을 구분하고 후자의 경우 어느 정도의 선까지 정부가 개입을 해야 하는 지에 대하여 기준을 정해서 신속한 대처가 가능하도록 하여야 한다.

또한 이용자들이 직접 참여할 수 있는 참여형 규제모델을 개발하여 이용자들의 자율적인 모니터링 및 신고체계에 기반을 둔 모니터링을 활성화 하여야 한다.

인터넷 이용자를 보호하기위한 방안에 대하여 호주의 방송통신규제기구(ACMA: Australian Communication and media Authority) 보고서에서는 인터넷 콘텐츠를 접하면서 많은 위험에 노출되어 있는 소비자 - 그중에서도 특히 미성년자와 아동 - 보호를 위한 필터링 기술 등 인터넷 이용자의 보호를 위한 장치개발에 관한 내용을 담고 있는데 향후 정보통신망 자율규제의 올바른 방향 수립을 위하여 참고

하면 좋을 것으로 생각된다. 동 보고서에는 이용자 인식제고를 위한 방안으로 이용자 교육과 홍보 프로그램에 대하여 소개하고 있다. 이 프로그램은 이용자에게 초점을 맞추어야 할 것이며, 정보통신기술의 발전에 따라 교육·홍보프로그램도 곧바로 업데이트 되어야 함을 명시하고 있다. 보고서에서 소개하는 대표적인 인식제고용 프로그램으로 뉴질랜드의 "Hector's World Limited"가 있는데 이는 기존에 아이들에게 인기를 얻고 있는 Hector라는 돌고래 캐릭터를 이용한 아동용 정보보안 교육 애니메이션이다. 이는 애니메이션 특유의 생동감과 유머를 통하여 지루하지 않게 정보를 전달하며 아동이 직접 문제 상황을 올바르게 해결할 수 있는 선택지를 제시하여 보는 것에 그치지 않고 참여도 할 수 있도록 하였다. 또한 영국의 Child International이 제작한 사이버폭력을 주제로 한 교육용 단편영화도 소개하였다. 이 영화는 사이버폭력을 학생들이 이해하기 쉽도록 평범한 학생의 일상이 폭력으로 인하여 어떻게 변해 가는지를 생동감 있게 보여준다. 또한 영화 제작에 사용된 음악은 유명 가수가 제작하여 아이들에게 흥미를 불러일으키는 요소가 되었다. 그리고 뉴질랜드의 인터넷 보안 교육용 컴퓨터 프로그램인 NetBasics는 게임의 형태로 흥미로운 캐릭터를 등장시키며 이용자에게 생길 수 있는 각종 온라인상의 위험 상황을 제시한 후 여러 가지 선택지 중에서 올바른 답을 고를 수 있도록 유도한 프로그램이다.

이러한 프로그램 개발 사례에서 볼 수 있듯 다양한 분야의 협력으로 이용자들이 쉽고 편하게 접근할 수 있도록 프로그램을 구성하는 것이 중요하다. 이러한 프로그램을 방송통신위원회와 한국인터넷진흥원 및 한국인터넷자율정책기구가 주축이 되어 소프트웨어·비디오·방송콘텐츠 업계뿐만 아니라 시민단체와의 협력을 통하여 개발해나가는 것이 바람직하다고 생각된다.

2. 이해당사자간 갈등조정시스템을 통한 자율규제의 활성화

정보통신망에서의 이해당사자들이라고 한다면 정책을 실시하는 정부와 정보통신 관련 사업자, 그리고 이용자로 나누어 볼 수 있다.

사업자측면에서 보면 분야의 특성상 포털사업자가 대표적이라고 할 수 있겠다.

대부분의 이용자들이 포털을 매개체로 하여 활동을 하고 있기 때문일 것이다. 더불어 포털사이트에서의 활동내용 등이 사회적으로 미치는 영향력이 실제로 크며, 사회적 쟁점들에 대한 논의의 장이 되고 있다.

요즘의 정보통신망에서의 이용자, 특히 인터넷 이용자들의 특성이라면 이용자가 과거에는 단순 이용자의 수준에 머물렀으나, 현재에는 단순 이용자가 아닌 정보생산자로서의 역할과 기능을 하고 있다는 것이다. 이로 인해 이용자가 포털사이트라는 장을 통하여 불법 콘텐츠 생성 및 게시글을 통한 명예훼손 등 범법행위를 저지를 수 있는 개연성이 높다. 그로 인해 정보통신서비스 제공자 등에 대하여 서비스에 대한 직·간접적인 규제와 모니터링 의무부과 등이 나타난 것이다.

그러나 사업자 측에서는 기업의 역량상 그러한 규제사항들을 시행하는 것이 경제적, 기술적 측면에서 상당한 부담을 초래한다. 또한, 이용자측면에서 본다면 이용자들의 이용행위에 있어 상당한 위축효과를 가져올 것이다. 최근 나타난 '사이버 망명'등의 현상으로 대변할 수 있다.

정보통신망의 규제는 정부정책의 목표, 사업자의 경제성 및 기술적 역량과 기업윤리, 그리고 이용자들의 이용행위의 자유 등 각 이해당사자들의 여러 이해가 얽혀있는 문제이다. 그러므로 여러 이해당사자 간의 활동 영역 및 갈등부분을 고려하여 기존의 정부규제와 함께 앞으로는 자율규제적인 측면도 활성화하여 갈등을 조정하는 측면으로 나아가야 할 것이다.

정보통신망의 보안과 관련하여 정부의 정보보안관련 기관과 인터넷서비스 제공자(ISP:Internet Service Provider), 집적정보통신시설(IDC)의 협업과 개별 이용자들의 PC 보안을 위하여 다각적인 대응방안을 모색하여야 한다.

우선 정보보안관련 기관에서는 정부차원의 자율규제에 대한 정책적 지원뿐만 아니라 국제공조에 관한 지원도 반드시 필요하다. 여러 차례의 '분산서비스거부공격'의 실제 사례에서도 경험하였듯이, 분산서비스거부 공격의 문제 중 하나는 공격자 추적의 어려움이다. 국내 규정이 아무리 공격자에 대한 강력한 처벌 조항을 갖추고 있다고 하여도 국외의 공격에 대해서는 국내 수사 체계만으로는 범인을 색출하는 것 자체가 어려운 일이다. 분산서비스거부 공격 범죄를 근절하기 위해서는 기술적인 방어와 더불어 범인을 체포하여 법률이 허용하는 한도 내에서 강력하게

처벌하고, 해외에서 발생하는 공격에 대해서는 외교 경로나 침해사고긴급대응국제포럼(FIRST: Forum for Incident Response and Security Teams) 등과의 협력을 통하여 이를 추적·처벌하는 일이 필요하리라 생각된다.

정보통신망의 보안을 위해서는 정부의 자율규제에 대한 국가 내부적 정책 지원과 외부적인 국제적 공조에 관한 지원이 모두 필요하다. 그리고 각 정보통신망 사업자들 또한 기술적 인프라에 대한 투자와 개발뿐만 아니라 특히 보안과 관련하여서 각 사업자들의 내부적인 기술적 조치를 마련해두어야 하며, 사업자들 간의 유기적 관계가 형성되어 한다. 또한 사업자들과 유관기관과의 협업에 대한 체계가 명확히 마련되어야 한다.

기업들만의 자율규제의 경우 업계의 현실을 반영할 수 있는 장점은 있지만 규율만 정해 놓고 지키지 않는 경우 또는 불법 정보에 대한 처리 방법·절차의 실효성이 확보되지 못할 가능성이 있다. 이러한 점을 보완하기 위하여 기업이 자율규약 위반시 이에 대한 징계를 할 수 있는 법률기관과의 연계 및 이용자의 불만사항을 실효성 있게 해결하기 위한 수사기관 및 정부기관과의 연계가 필요하다. 전체적인 정보통신망 관련 기관과 업계의 유기적 협력체계가 필요한 것이다.

3. 민간 규제 영역의 활성화

자율규제의 모델에 있어서 민간 규제의 영역과 정부 규제의 영역의 활성화를 두고 어떠한 것이 적정하고 합리적인 것인지에 대하여 논의 할 필요가 있다. 과거 우리나라는 정부규제에 집중되어 있었으나, 선진국 등 외국의 사례에서도 보았듯이 정부규제와 함께 자율규제를 활성화 하는 것이 합리적 규제의 방안이 될 것이다. 정보통신망의 특성상 직접규제만으로는 완전한 규제가 어려운 것이 현실이다. 선진국들에서 정보통신망 특히, 인터넷 서비스 업체(OSP)에 대한 규제를 자제하고 자율규제를 내세우는 이유는 크게 세 가지다. 먼저 인터넷 서비스의 중립성에 대한 확신이다. 대부분의 해외국가들은 인터넷 서비스를 두 가지로 분류하고 있다. '내용 중립적 서비스'로서의 검색 서비스와 '공개광장'으로서의 서비스로 포털 등 대개 인터넷 사업자의 두 가지가 있다. 서비스 유형에 따라 법적 책임도 다른

데, 중립 서비스 사업자에 대해 외국은 정보 제공업자로 보지 않고 단순 정보 매개업자로 취급하여, 다양한 면책 규정을 두는 경향이 크다. 플랫폼에서 벌어지는 일에 대해 사업자가 최소의 의무만 다하면 별도 책임을 묻지 않는 것이 일반적이다. 미국, 일본, 프랑스 등이 이런 규제의 대표적인 국가들이다.

두 번째 이유는 지나친 규제는 인터넷 사업의 자율성을 해칠 수도 있다는 우려 때문이다. 해외국가들은 많은 경우 인터넷 산업에서 최소 정부 원칙을 지키고 있다. '사업은 사업자에게'라는 자율 원칙이 우선인 것이다. 물론 이 기조에 맞춰 해외 기업도 기본적인 책임 이행에 대해 적극적이다. 많은 수의 해외 사업자들은 자체 규제에 적극적이며, 다수의 해외 정부는 자율규제를 통한 산업 진흥의 효과에 무척 기대감을 보이고 있다.

마지막으로 체계적으로 정립되어 있는 인터넷에 대한 철학이 자율규제를 이끌어가고 있다. 해외 정부의 규제는 일정 수준의 가이드라인을 제공하며, 이른바 규제보다는 업계의 자체적인 규제를 촉진하며 산업 진흥을 도모하고 있다.[185]

제2절 자율규제 활성화를 위한 업계의 노력

정보통신망 관련 사업자들을 규제하려고 하는 분위기의 저변에는 관련 기업의 사업영역이 국가 사회전체에 미치는 영향력은 광범위한데에 비하여, 기업의 자율정화 활동과 노력이 부족하다는 지적 또한 간과 할 수 없다.

이러한 점에 대한 개선을 위하여 수년 전부터 네이버·다음·네이트 등 주요 포털 기업들은 이용자위원회, 미디어책무위원회 같은 별도 조직을 꾸려 명예훼손, 저작권 침해 등의 피해확산 방지 노력을 벌이고 있다. SK커뮤니케이션즈는 지난 2006년 6월 포털 업계로는 처음으로 자사 서비스에서 제공하는 뉴스의 공정성을 강화하기 위해 외부인사로 구성된 '미디어책무위원회'를 구성하여 편집가이드를 발표하고 있다. 미디어책무위원회의 구성은 학계와 법조계, 시민단체, 네티즌 등으로 다양하며 이들은 정기적으로 SK커뮤니케이션즈의 포털 네이트닷컴과 싸이월드에

185) 전자신문 미래기술연구센터, 인터넷 규제의 패러다임 전환-현행 규제의 문제점과 발전적 대한 -, 2008 신인터넷보고서-02. 79-80면.

서 유통되는 기사들이 자체 규정 및 인터넷선거보도심의위의 규정을 준수하는지 익명성을 지키는지 등을 모니터링하고 이에 대한 보고서를 공개하고 있다. NHN 역시 뉴스 서비스에 한해 이용자위원회를 구성해 운영 중이다.

기업 각자의 노력 외에 협회 차원에서의 공동대응도 진행되고 있다. 한국인터넷기업협회는 2008년 9월 다음커뮤니케이션, SK커뮤니케이션즈, NHN, KTH, 코리아닷컴, 하나로드림(이상 가나다순) 등 6개 포털사가 참여하는 '건강한 인터넷을 위한 포털정책협의회'(이하 '포털정책협의회')를 구성키로 했다. '포털정책협의회'는 인터넷 포털 사이트의 이용자의 권익을 보호하고 피해를 예방하기 위한 핫라인 구축 및 이용자 교육 등 업계 공동의 사업을 발굴해 전개해 나가는 방향으로 진행되고 있다.

이를 위해 우선 포털사들은 업계 핫라인 구축부터 추진키로 했다. 목적은 그 동안 각 포털사들이 개별적으로 처리해 온 이용자 게시물에 대한 처리 상황을 공유함으로써 이용자 피해를 최소화하겠다는 것이다.

'포털정책협의회'는 더 나아가 포털 서비스 이용자의 권익 향상을 위한 쌍방향 커뮤니케이션도 강화할 계획이다. 그 하나로서 이용자들의 인터넷 활용을 돕기 위한 가칭 '인터넷 이용자 아카데미' 설립 안을 구상 중이라고 밝혔다. 학계 및 업계 전문가가 제공하는 교육 서비스에 이용자들이 신청해 수강할 수 있도록 하고 사업체 방문 등의 체험기회를 제공하는 사업이다.

제3절 자율규제 활성화를 위한 정부의 역할과 정책 방향

1. 법체계의 정비

현재 우리나라에서 정보통신망과 관련한 규제를 포함하고 있는 법률로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「전기통신사업법」, 「온라인 디지털 콘텐츠산업 발전법」, 「전자거래기본법」, 「행정법」, 「민법」 등 수 개의 법률이 있다. 이 법들이 포함하고 있는 규제 내용의 대부분은 문제가 발생했을 때 행위자와 동시에 서비스 사업자에게도 책임을 부과하고 있다는 데에 특징이 있다. 그런데 이

러한 특성에도 불구하고 법률 간의 연계성이 부족하여 때로는 그것이 일관적인 집행으로 연결이 되지 않는다는 아쉬운 점도 존재한다.

해외의 경우 미국은 정보보호를 위한 다양한 법과 제도를 시행중이다. 미국에서의 정보보호관련 대표적인 법령으로는 컴퓨터를 통한 국가보안정보, 금융정보, 행정정보 등에 대한 불법적인 접근·취득·사용, 컴퓨터를 이용한 사기, 컴퓨터에 대한 손상 등을 범죄로 규정하고 이에 대한 처벌규정을 수록한 「컴퓨터 사기 및 오용에 관한 법률(Computer Fraud and Abuse Act)」이 있다. 최근에 사이버보안 강화를 위하여 2009년 4월 민주당 상원의원 제이 록펠러(Jay Rockefeller), 빌 넬슨(Bill Nelson)과 공화당 상원의원 올림피아 스노위(Olympia Snowe) 등의 공동발의로 「2009 사이버보안 법률안(Cyber Security Act of 2009)」이 「백악관 내 국가사이버보안자문관실 설립을 위한 법안」과 함께 미국 상원에 제출된 상태이다. 주요 내용으로 사이버보안 자문위원단(Cybersecurity Advisory Panel) 설립, 실시간 사이버보안 경보, 주 및 지역 사이버보안 증진 프로그램, 국립표준기술원(NIST)의 표준개발 및 표준의 준수, 사이버보안 전문가 면허 및 인증, 대통령의 사이버 보안 의무 및 권한의 강화, 상무부의 민관 정보 교환센터(Public-Private Clearinghouse)로서의 역할 담당, 합동 정보위협 평가 실시 등의 내용이 있다.

일본에서는 「고도 정보통신 네트워크사회 형성 기본법(IT기본법)」에서 고도정보통신 네트워크 사회의 형성에 관해 기본이념 및 시책의 책정과 관련되는 기본방침을 정하고 있는데, 국가·지방공공단체와 민간과의 역할 분담과 민간이 주도적 역할을 담당하는 것을 원칙으로 하고, 국가·지방공공단체는 공정한 경쟁의 촉진, 규제의 재검토 등 민간의 활력이 충분히 발휘되기 위한 환경 정비 등을 중심으로 한 시책을 실시하고, '고도 정보통신 네트워크 사회 추진 전략 본부'를 내각에 설치하고, 고도 정보통신 네트워크 사회의 형성에 관한 중점 계획의 작성과 그 실시를 추진하며, 고도 정보통신 네트워크 사회의 형성에 관한 시책으로 중요한 기획에 관해서 심의하거나 그 시책의 실시를 추진하는 것을 그 내용으로 하고 있다. 또한 「부정접속행위의 금지 등에 관한 법률」에서는 부정 접속 행위의 금지 및 처벌에 관하여 규정하고, 시스템에 대해 방어 조치를 실시하도록 하는 의무를 관리자에게 부과한 법률로 재발 방지를 위한 행정기관의 지원 조치 등을 정하고, 전기통신 회

선을 통하여 행해지는 범죄의 방지 및 접근 제어 기능을 통해 전기통신에 관한 질서의 유지를 도모함을 목적으로 하고 있다.

독일의 경우 「정보통신법」에서 온라인 공간의 정보보호를 위한 목적으로 정보기관의 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷서비스 제공자 등 정보통신서비스를 제공하는 모든 책임자에게 고객정보를 정부에서 접근 가능한 상태로 유지할 의무를 규정하고, 정보통신서비스 제공자가 이러한 조치를 실행하지 않을 경우 그 운영을 중지시킬 수 있도록 규정하고 있다. 또한 「통신서비스법」에서 인터넷서비스 제공자의 정보차단의무에 관하여, 일정한 요건 하에서 위법한 정보를 인지한 경우의 인터넷서비스 제공자의 정보차단의무를 규정하고 있다. 「정보통신서비스 정보보호법(TDDSG)」은 정보통신서비스 이용관계에서의 개인정보의 수집·처리에 관하여 규율하며 인터넷 포털사이트 운영자, 이메일서비스 제공자, 온라인 게임서비스 제공자 등의 정보통신서비스 제공자가 고객정보를 이용·처리하는 행위에 직접적으로 적용하고 있다. 주요 내용으로 정보보안의 범위, 서비스 제공자와 이용자의 개념 정의, 정보 보안 원칙, 서비스 제공자의 의무, 보호되는 정보의 내용, 연방정보보안감독관의 역할 등이 있다.

각국의 법률에는 인터넷상의 정보보안에 관하여 이용자에 대한 보호와 서비스 제공자의 보안원칙과 의무에 대한 내용을 담고 있다. 또한 그 특징으로는 법률의 규제내용이 민간부분에서의 규제를 장려하는 경향을 담고 있음을 알 수 있다. 우리나라에서도 규제의 원칙과 기준을 지키면서 규제의 내용의 중복이 없이 민간부분의 규제를 장려하는 방향으로 법률을 정비하여야 할 것이다.

2. 정책의 방향

모든 산업에 있어서 정부와 사용자, 그리고 시장의 개입은 필연적일 것이다. 산업에 있어 그 분야를 관리하고 활성화하기 위한 의무는 정부가 지는 것이다. 정보통신망 관련 산업분야에 있어 규제는 필요하다. 그러나 그 규제는 반드시 적정해야 하고 합리적이어야 한다. 그렇다면 어떠한 규제가 적정하고 합리적이라고 할 수 있는가? 적절한 규제는 역기능을 해결하고 그 분야의 균형을 유지하는 역할을

담당하는 규제라고 할 수 있다.

우리나라에서는 현재 정보통신망의 규제모델에 관하여 민간을 중심으로 한 자율규제에 중점을 둘 것인지 아니면 정부에 의한 강력한 통제모델을 따를 것인지가 논의의 중심이라고 볼 수 있다. 어떠한 모델로 정책을 시행해 나갈 것인지가 정보통신분야의 전체 구조에 큰 영향을 미칠 것이다.

우리나라는 정보통신 분야에 있어 지금까지는 정부규제에 초점이 맞추어져 있다고 평가된다. 정부규제는 사회전체에 있어 미치는 효과는 빠르고 강력하다 할 수 있지만, 정부규제만으로 정보통신망을 규제한다면 때로는 부작용이 생길 수도 있다. 이를 방지하기 위하여 미국·일본·독일 등의 선진국에서는 정부규제와 함께 자율규제를 활성화하여 업계의 자정능력을 키우고자 하는 것이다.

정보통신망에 대한 정부의 정책은 '규제를 위한 규제'가 아닌 규제를 통하여 보다 신뢰할 수 있고 안전한 정보통신 환경을 만드는 것이 목표가 되어야 한다. 개별적이고 산발적인 입법 및 정책 수립을 하는 것보다는 관련 기관과 업계, 그리고 이용자의 목소리를 충분히 반영하여 모두가 합의할 수 있는 규제방식을 도출해내는 것이 옳은 방향일 것이다. 또한 그 실효성을 위해서 현재 시행되는 법·제도와 마찰 및 중복은 없는지를 살펴서 혹시 이미 존재하는 제도인 경우에는 기존의 제도를 적극 활용하는 것이 중요하다. 또한 차후 시행하고 싶은 새로운 규제인 경우는 기존의 관련된 법과 정책들을 충분히 살펴서 조화를 이룰 수 있도록 하여야 한다.

해외의 사례를 살펴보면, 미국의 경우 정보보안의 확보를 위해 다양한 제도를 시행중이다. 또한 최첨단 암호 알고리즘과 프로토콜 개발 등의 정보보호 기술 개발에도 역점을 기울이고 있음을 알 수 있다. 미국의 주요 국가기반 보호계획(National Infrastructure Protection Plan)은 미국 국토안보부(DHS)에서 미국의 주요 국토기반과 자원(CI/KR: Critical Infrastructure and Key Resources) 보호를 위하여 2009는 주요 국가기반 보호계획을 수립하도록 하고 있다. NIPP 2009는 17개 분야를 나누어 각 분야별 보고서에서 연방정부·지방정부·NGO·기업 등이 협력을 통하여 "위험"에 대한 정의를 내리고 위험을 관리하는 절차와 방법을 다루고 있다. 협력관계에 있는 회사들은 정보공유·분석센터, 즉 ISAC을 구성하여 현존하

는 위험 및 미래의 위험, 운영상의 위험을 감소시키고 관리하는 방법을 논의하고 있다. NIPP 2009의 ISAC에는 금융, 교통, 정보기술, 통신 등 여러 분야가 있으며 사이버 위협이나 물리적인 위협이 있을 때 각 네트워크 운영자와 소유자들이 함께 대응방안과 정보를 공유하고 논의하는 취지의 기구이다. 각 분야별로 별도의 ISAC이 존재하는 이유는 네트워크 구성과 성격이 다르고 이를 한 가지 방법으로만 대응하기 어렵기 때문이라고 할 수 있다. 따라서 미국 정부는 기업들의 차이를 인정하여 분야별 ISAC을 구성하여 각 분야별 민관공조를 통하여 사이버 보안을 이루고자 하는 것이다.

또한, 사이버 정책 검토 보고서(Cyberspace Policy Review)는 2008년 11월 오바마 대통령 인수위원회가 당시 미국 정부의 사이버보안에 대한 현황과 문제점, 개선방안에 대한 내용을 담은 보고서로써, 미국 사이버보안의 문제점을 지적한 사항들을 담고 있다. 그 내용으로는 사이버보안에 대한 책임의 과도한 분산과, 업무의 중복성 문제, 보안문제 해결을 위한 부서의 권한 부족 문제, 정부의 총체적인 접근과 비전을 전제로 한 사이버보안에 대한 경쟁 관계에 있는 이익집단 통일의 필요성, 정보통신 네트워크의 다수가 다국적 기업에 의하여 소유·운영되는 현 상황에서 민관 협조와 국제적인 공조 및 국제적 기준 마련의 필요성 등이 있다. 그리고 미국 정부의 사이버보안과 위협에 대한 사용자 인식 제고를 위한 노력과 동시에 개인정보보호와 헌법에서 보장되는 시민의 자유를 고려한 통합적인 접근의 필요성에 대한 언급과 사이버보안의 취약점 대응 및 미국의 경제적·국가적 보안 요구 충족을 위한 연구에 많은 투자를 촉구하는 내용이 포함되어 있다.

일본의 경우도 정보보안에 관한 정책에 있어 민간이 주도적 역할을 담당하는 것을 원칙으로 정하고 있고, 국가와 지방공공단체는 공정한 경쟁을 촉진하고 규제의 재검토 등 민간의 규제가 충분히 발휘되기 위한 환경 정비 등을 중심으로 한 시책을 실시하고 있다.

EU에서는 정보보안의 인식제고를 위한 지속적 노력 및 투자를 하는 중으로 최근 정보보안 인식 실태조사 및 가이드라인 개발 등 활발한 연구를 지속하고 있다. '정보사회와 미디어 이사회'의 정책으로 "eEurope", "안전한 정보사회를 위한 전략", "미디어 리터러시", "안전한 인터넷 플러스 프로그램" 등이 있다. ENISA는

"ENISA의 역할과 비전" 및 각종 가이드라인을 통해 활발한 정보 보안 인식을 제고하며 활동을 수행 중이다. EU는 정보보안 인식제고 활동의 일환으로 체계화된 정보 보안 인식제고 프로그램을 마련하고 있는데, 정보 보안 인식제고를 위한 프로세스의 마련 및 효과성 측정을 위한 핵심성과지표 개발과 정부와 다양한 분야의 민간기업 간 긴밀한 협조체계를 구축하고, 각종 멀티플라이어(multiplier)를 활용한 대상별, 수준별 정보보호 교육 및 훈련의 중요성을 강조하고 있다.

독일에서도 EU의 적극적 지원과 독일 정부의 승인 하에 자율규제기관이 적극적으로 이용자 보호에 앞장서는 활동을 지속적으로 펼치고 있다.

정보통신망의 기술과 인프라 등에 있어서 우리나라는 어느 나라에 뒤지지 않는 선진국이라 할 수 있다. 그러나 정보통신망에 있어서 규제와 관련하여서는 다른 나라들과 비교해 보았을 때 아직은 선진국이라고 할 수 없을 것이다. 다른 나라의 정보통신망 규제에서 드러나는 특징은 규제에 관하여 일관된 정책적 '규제 철학'이 존재한다는 점이다. 규제의 초점은 사회적 가치에 따라 조금씩 다르지만 경쟁 지지, 이용자 보호, 산업 육성 등 정해놓은 규제의 기본원칙은 흔들리지 않았다. 특히 국가 전체적으로 규제에 대한 시그널이 명확해 어떤 행위들이 바람직한지, 그렇지 않은지에 대한 합의가 이뤄지고 있었다. 또한 사업자 자율규제가 정착된 것도 눈에 띄었다. 자율규제의 정착은 산업 진흥과 예측 가능성의 제고라는 효과를 가져다준다. 그러다보니 기업이든 사용자든 어떤 행동을 해야 하는 지 예측이 가능해져 규제 저항이 상대적으로 적게 나타난다.[186]

정보통신망 관련 분야에 있어 우리나라는 기술적 인프라의 선진성과 정보통신망이 사회에 미치는 영향력의 광범위함에 비하여 규제와 관련하여서는 일관된 기준이 있었다고 보기 어렵다. 정보통신망에의 신뢰성과 안전성을 확보하기 위해서는 하나의 일관된 규제 철학을 가지고 통일성 있는 규제정책(자율규제 확산 중심으로)을 시행해 나가야 할 것이다. 또한 개별적 규제들 간의 상호 관련성을 검토하여 각종 규제간의 불일치를 해소하여야 하며, 규제로 인한 부작용을 최소화할 수 있도록 대응방안도 마련되어야 한다. 또한 자율규제를 활성화 하는 것이 규제에 있어 적정성과 합리성을 확보할 수 있고, 그로 인해 정보통신망에의 신뢰성과 안

186) 전자신문 미래기술연구센터, 인터넷 규제의 패러다임 전환-현행 규제의 문제점과 발전적 대한 -, 2008 신인터넷보고서-02. 99-100면.

전성을 확보할 수 있는 디딤돌이 될 것이다.

전체적인 측면에서 보았을 때 자율규제를 활성화하기 위해서는 어느 한 분야의 노력만으로는 힘들다. 정보통신망의 전체에서 서비스제공자와 콘텐츠 제공자 그리고, 이용자와 정부기관 등 전 단계에서의 노력이 유기적으로 결합되어야 자율규제가 성공적으로 안착될 수 있을 것이다.

제4절 자율규제 활성화를 위한 이용자의 자정활동

최근에 시민단체들은 포털 뉴스를 둘러싼 사회적 이슈들이 등장하자 '포털이용자 운동'을 하게 되었다. 이것은 포털뉴스에 대한 지나친 법적 규제보다는 이용자들의 자발적 참여와 견제를 통해 포털 뉴스가 올바르게 자리매김 할 수 있도록 하자는 취지였다. 포털 이용자 운동의 첫 행보는 네이버, 다음, SK커뮤니케이션즈, 야후 코리아, 엠파스(SK 커뮤니케이션즈와 통합 전), 파란 등 당시 시장 점유율이 가장 높았던 6개 포털사에 공개 질의서를 보낸 일이었다. '미디어 영역', '이용자 권리 영역', '프라이버시 영역' 등 3개 영역에 걸쳐 총 12개의 질의를 담고 있었는데, 이용자의 입장에서 포털에게 개선사항과 제도적 보완장치를 요구하는 내용이었고 이들 12개 질의 중 제일 첫 번째 질의 항목이 바로 지금의 미디어책무위원회와 같은 옴부즈맨 제도의 도입을 권고하는 것이었다.

그 상세내용은 포털사의 뉴스서비스가 이용자와 사회에 대한 책임감을 가진다고 하면 이를 위한 최소한의 장치로서 독자위원회나 옴부즈맨제도가 필요하며, 포털사는 독자위원회나 옴부즈맨들에게 뉴스의 편집 및 유통 등에 관한 정보를 제공하고 이용자들의 의견을 수렴하고 운영에 관한 정보를 정기적으로 공개할 필요가 있다. 이를 통하여 뉴스 유통과 중개의 투명성을 향상시키고 자율적인 모니터 활동을 통해 공정성을 향상시킬 수 있을 것이라는 것이었다.

시민단체의 노력과 이용자들의 적극적인 참여로 인하여 이용자의 권리와 이용자들의 프라이버시에 관한 부분에 있어 각 사업자들도 더욱 적극적으로 자율규제적인 측면에 힘쓰게 되었다.

부 록

부 록

독일

1. <부록1> 통신법(Telekommunikationsgesetz: TKG) 제7장

통신법 제113a조 (데이터 저장 의무) ① 공중이 접근 가능한 전기통신서비스를 이용자를 위해서 제공하는 자는 서비스의 이용에 있어서 그가 생성하거나 처리한 통신데이터를 제2항내지 제5항의 기준에 따라 6개월간 독일 또는 유럽공동체 회원국 안에서 저장할 의무가 있다. 자신이 직접 통신데이터를 생성하거나 처리하지 않고서 이용자를 위해서 공중이 접근 가능한 전기통신망을 제공하는 자는 제1문에 의한 데이터가 확실히 저장되도록 해야 하고, 이 데이터를 저장하는 자를 연방통신망중개소의 요구에 따라 알려야 한다.

② 공중이 접근 가능한 전화서비스를 제공하는 자는 다음 각 호의 사항을 저장한다.

1. 송수신자의 전화번호 또는 다른 표지 및 전환접속 또는 중개접속인 경우 이에 참여한 자의 전화번호 또는 다른 표지

2. 전화접속의 시작과 종료의 표준시간대에서의 날짜와 시간

3. 전화서비스와 관련하여 다른 서비스가 이용될 수 있는 경우에는 이용된 서비스에 대한 정보

4. 이동전화 서비스의 경우에는

a) 이동 가입자의 송수신 접속을 위한 국제적 식별 표지

b) 송수신 단말기의 국제적 표지

c) 송수신 접속을 통해서 접속을 시작하는 경우 이용되는 무선국의 명칭

d) 선불 익명 서비스의 경우에는 서비스의 첫 활성화한 날짜와 시간 그리고 무선국의 명칭

5. 인터넷 전화서비스의 경우에는 송수신 접속의 인터넷프로토콜 주소

제1문은 간단정보, 멀티미디어정보, 이와 유사한 정보(Nachricht)의 중개에도 준용한다. 이 경우에는 제1문 제2호의 정보 대신에 정보의 송신과 발신의 시점을 저장

하여야 한다.

③ 전자우편 서비스 제공자는 다음을 저장한다.

1. 정보(Nachricht) 발신의 경우 전자우편함의 표지와 발신자의 인터넷프로토콜 주소 및 정보수신자의 전자우편함의 표지

2. 정보가 전자우편함으로 도착되는 경우에는 정보의 발신자와 수신자의 전자우편함의 표지 및 발신한 전기통신장치의 인터넷프로토콜 주소

3. 전자사서함에의 접근인 경우에는 그것의 식별부호(Kennung)와 접근한 자의 인터넷프로토콜 주소

4. 제1호 내지 제3호에 언급한 서비스의 시점의 표준시간대에서의 날짜와 시간

④ 인터넷접속서비스 제공자는 다음을 저장한다.

1. 인터넷이용을 위해서 참여자에게 할당된 인터넷프로토콜 주소

2. 인터넷 접속을 하게 하는 연결시설(장치)의 독자적인 표지

3. 할당받은 인터넷프로토콜을 통하여 인터넷을 이용한 시작과 종료의 표준시간대상의 날짜와 시간

⑤ 전화호출에 대한 대답이 없거나 통신망 관리의 침해로 전화호출이 효과가 없는 경우에는 전화서비스 제공자가 본 조에서 언급하고 있는 통신데이터를 제96조 2항에서 언급하고 있는 목적을 위해서 저장하거나 기록하는 한, 그 통신데이터도 이 규정의 기준에 따라서 저장하여야 한다.

⑥ 전기통신서비스를 제공하고 이 경우에 이 규정에 의한 기준에 따라서 저장된 정보(Angaben)를 변경하는 자는 원래의 정보와 새로운 정보 및 이러한 정보의 변경 시점에 대한 표준시간대상의 날짜와 시간을 저장해야 할 책임이 있다.

⑦ 공중을 위해서 이동통신망을 운영하는 자는 다음의 책임이 있다. 이 규정의 기준에 따라서 저장된 무선전화의 통화가능범위의 표시에 대한 데이터도 유지해야 할 책임이 있는데, 그 데이터로부터 각 무선전화의 통화가능범위(Funkzelle)를 관리하고 있는 무선안테나의 지리적 상황 및 이것의 주방사의 방향이 발생한다.

⑧ 통신의 내용과 접근한 인터넷 사이트에 대한 정보는 이 규정을 근거로 해서 저장되어서는 아니된다.

⑨ 제1항내지 제7항에 의한 데이터는 정당한 지위자의 정보요청에 지체 없이 응할 수 있도록 저장되어야 한다.
⑩ 이 규정에 의해서 의무를 지는 자는 저장된 통신데이터의 질과 보호에 대해서 전기통신의 영역에서 필요한 주의를 다해야 한다. 이와 관련하여 의무자는 기술적 조직적 조치를 통하여 그가 특별히 허가한 사람만이 저장된 데이터에 대한 접근이 가능하도록 해야 한다.
⑪ 이 규정에 의해서 의무를 지는 자는 이 규정에 의해서만 저장된 데이터를 제1항에 규정된 기간이 경과한 후 1개월 이내에 소거하거나 소거를 확보해야 한다.

제113b조 (제113a조에 의해 저장된 데이터의 사용) 제113a조에 의한 의무자는 오로지 제113a조의 저장의무를 근거로 하여 저장된 데이터를

1. 범죄의 소추,
2. 공공의 안전을 위한 중요한 위험의 방지,
3. 연방 및 주의 헌법보호청, 연방비밀정보기관, 연방군 안보국의 법적 업무의 수행을 위하여 관할 관청의 요구에 따라 제공할 수 있는데,

이것은 제113a조와 관련하여 각각의 법률에 규정되어 있고 개별적인 사례에서 제공이 명령된 경우에 한한다. 의무자는 제113조에 의한 정보의 제공의 예외로 다른 목적을 위해서는 이러한 데이터를 사용할 수 없다. 제113조 제1항 제4문은 이를 준용한다.

2. <부록2> 형법(Strafrecht) 202a조, 202b조, 202c조, 303b조

제202a조 (데이터 탐지) ① 권한 없이 행위자에게 특정되어 있지 아니하고 부당한 접근에 대하여 특별히 보안이 되어 있는 데이터에 접근보호조치를 침해하여 접근하거나 다른 사람으로 하여금 접근하게 한 자는 3년 이하의 징역 또는 벌금형에 처한다.
② 제1항의 데이터는 전기적, 자기적 또는 그 밖에 직접 인식할 수 없도록 저장되거나 중개되는 것을 말한다.

제202b조 (데이터 불법 취득) 비공개 데이터 전송으로부터 또는 데이터 처리장치에서 방출되는 전자파로부터 행위자에게 특정되지 아니한 데이터(제202a조 제2항)를 기술적 수단을 사용하여 권한 없이 취득하거나 다른 사람으로 하여금 취득하게 한 자는 그 행위가 다른 규정에 의하여 중한 형벌로 처벌되지 아니하는 한, 2년 이하의 자유형 또는 벌금형에 처한다.

제202c조 (데이터의 탐지 및 취득의 예비) ① 다음 각 호의 1에 해당하는 것을 제작하거나, 취득하거나 타인으로 하여금 취득하게 하거나, 판매하거나, 타인에게 양도하거나, 유포 또는 그 밖에 접근이 가능하도록 함으로써, 제202a조와 제202b조에 의한 범죄행위를 예비한 자는 1년 이하의 자유형 또는 벌금형에 처한다.

1. 데이터의 접근(제202a조 제2항)을 가능하게 하는 패스워드(비밀번호) 또는 그 밖의 보안코드

2. 그러한 범죄를 행할 목적을 가진 컴퓨터 프로그램

② 제149조 제2항과 제3항은 이를 준용한다.

제303b조 (컴퓨터 사보타지) ① 다음 각 호의 행위로써 다른 사람에게 현저히 데이터 처리에 중대 장애를 일으킨 자는 3년 이하의 자유형 또는 벌금형에 처한다.

1. 제303a조 제1항의 범죄행위

2. 타인에게 손해를 줄 의도로 데이터(제202a조 제2항)를 입력하거나 전달하는 행위

3. 데이터처리장치 또는 데이터저장매체를 파괴, 손괴, 사용불능, 소거 또는 변작하는 행위

② 데이터의 처리가 타인의 사업체, 기업 또는 관청에 현저히 중요한 경우에는 5년 이하의 자유형 또는 벌금형에 처한다.

③ 미수범은 처벌한다.

④ 제2항의 특히 중한 경우에는 6월 이상 10년 이하의 자유형에 처한다. 특히 중한 경우란 특별한 사정이 없는 한 다음 각 호의 1에 해당하는 행위를 말한다.

1. 중대한 재산상의 손실을 야기하는 행위

2. 영업적으로 활동하거나 또는 지속적으로 컴퓨터 업무방해행위를 범하기 위해서 조직된 단체의 구성원으로서 활동하는 행위

3. 이 범죄행위를 통하여 국민의 생활필수품의 공급이나 서비스의 공급을 침해하거나 독일연방공화국의 안전을 침해하는 행위

⑤ 제1항에 의한 범죄행위를 예비한 경우에 제202c조를 준용한다.

3. <부록3> 연방정보기술안전청법(BSI-Errichtungsgesetz: BSIG)

제1조 (정보기술의 안전성을 위한 연방행정청) 연방은 상급연방행정청으로서 연방정보기술안전청을 둔다. 이것은 연방내무부장관의 직속으로 한다.

제2조 (정의) ① 이 법률에서 정보기술의 의미는 정보의 이용 또는 전달에 관한 모든 기술적인 수단을 포함한다.

② 이 법률에서 정보기술의 안전성의 의미는 다음 각 호의 안전성보호조치를 통한 정보의 일정한 안전성 상태, 처분 가능성, 불가침성 또는 비공개성의 유지를 의미한다.

1. 정보기술체계 또는 정보기술구성요소에 있어서의 보호조치
2. 정보기술체계 또는 정보기술구성요소의 적용에 있어서의 보호조치

제3조 (연방행정청의 과제) ① 연방행정청은 정보기술안전성의 진흥을 위한 다음의 과제를 수행한다.

1. 연방의 업무수행에 필요한 한에서 정보기술의 적용과 안전대책의 개발, 특히 정보기술안전성을 위한 정보기술절차와 기기의 안전성 위험에 대한 검사

2. 정보기술체계 또는 정보기술구성요소의 안전성 검사와 평가를 위한 기준, 절차, 기기의 개발

3. 정보기술체계 또는 정보기술구성요소의 안전성에 대한 검사와 평가 및 안전성 증명서의 교부

4. 연방 또는 연방의 위탁을 받은 기업의 비공개정보가 제공 또는 전달되어져야 할 경우와 운영을 위하여 허용된 암호화도구를 위하여 비공개데이터가 필요한 경우 이를 위한 정보기술체계 또는 정보기술구성요소의 허용

5. 정보기술안전성을 위한 연방의 권한 있는 기관, 특히 조언 또는 통제를 수행하는 기관에 대한 지원. 이러한 지원은 과제의 수행을 연방데이터보호법에 따라 행하며 이에 대한 지원은 재량에 따르는 데이터보호에 대한 연방수탁기관의 경우보다 우선한다.

6. 다음의 기관에 대한 지원

a) 법률상 과제의 수행에 있는 경찰과 형사소추기관

b) 테러시도에 대한 관찰 또는 연방과 주의 헌법수호법률에 근거한 법률상 권한에 해당하는 정보제공행위를 위한 정보의 활용과 평가를 하는 헌법수호기관

지원은 정보기술의 안전성에 지향된 또는 정보기술의 사용을 연구하는 행위를 방해하거나 행하기 위하여 필요한 경우에 한하여 보장될 수 있다.

7. 결여된 또는 충분하지 않은 안전성의 가능성에 대한 고려하의 정보기술의 안전성에 관한 질문에 대한 제공자, 운영자, 적용자의 자문

② 제1항 제2호의 경우 제4조의 안전성증명서 교부의 근거가 되는 기준과 절차에 대한 결정은 연방경제기술부장관과의 합의로 하여야 한다.

4. <부록4> 연방의 정보기술의 보안 강화를 위한 법률(Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes)

1. 개관

이 법률은 연방정부가 2월 16일 정부법안으로 제출하여 6월 19일 연방하원(Bundestag), 7월 10일 연방상원(Bundesrat)을 각각 통과하여 현재 연방대통령의 서명과 공포를 기다리고 있음.

연방하원은 2009년 6월 19일 대연정(SPD, CDU/CSU)의 동의를 얻어 그 동안 논란이 많았던 연방정부가 제출한 [연방의 정보기술의 보안 강화를 위한 법률안](Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes)을 통과시켰다. 이 법률안은 연방정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)의 권한을 확대하고 있다. 원래 이 법률안에는 연방정부에 의해서 감시권한이 강화되어 있었는데, 연방

상원 내무위원회에 의해서 그러한 감시권한이 완화된 변경안이 수용되어 있다. 이에 대해서 야당은 개인정보보호를 이유로 이 법률안에 반대하였다.
이 법률은 연방의 정보기술 인프라에 대한 공격을 방지하기 위한 여러 가지 수단을 BSI에 부여하고 있다. 악성프로그램을 보다 더 쉽게 찾아낼 수 있기 위해서 BSI는 장래에 IP주소와 같은 개인관련성이 있을 수 있는 이용자정보 뿐만 아니라 시민과 연방의 행정기관 사이에 행해진 온라인 통신의 경우에 발생하는 모든 프로토콜데이터를 제한 없이 저장할 수 있고 자동으로 평가할 수 있다. 다만 사기업이나 주 행정기관의 경우 프로토콜데이터는 이 법률이 적용되지 않는다. 각 주는 이에 대한 개별 법률을 준비 중에 있다.
이 경우에 특히 전자메일은 통신프로파일링의 작성을 피하기 위해서 필터로 걸러져서 익명으로 대체되어야 한다. 실명으로 프로토콜될 경우가 있는데, 이러한 경우로는 가령 악성프로그램과 관련한 혐의사실이 증명된 경우에 이의 처리를 더 하기 위해서 또는 당사자에게 경고를 하기 위해서 필요한 경우이다.

법률초안에 예정되어 있었던 보안기관에게 데이터를 전달하는 일반적인 권한은 형법 제202a조의 해커규정으로 제한되었다. 또한 우연히 발견한 것을 전달하는 경우에도 법관유보를 통하여(법관의 명령을 통하여) 제한을 가하고 있다. 이에 대해서는 사후에 당사자에게 통지해야 할 의무가 있다. 대연정은 허용된 악성프로그램의 수색과 관련하여 사적 생활형성의 핵심영역의 보호를 개선하였다. 어느 정도의 침입이 가능한 최소에 거치도록 하기 위해서 이를 통해서 인식한 내용은 지체 없이 삭제되어야 한다. 증언거부권이 있는 사람들의 연방행정기관과의 통신을 위해서 증거사용금지가 도입되어 있다. 이것은 통신데이터저장지침[187]을 위한 규정들의 경우에 있어서 보다도 더 약하다. 따라서 국회의원, 성직자, 언론인, 의사, 변호사 또는 그 밖의 다른 직무상 비밀유지자들을 위한 특별한 보호는 비례성의 원칙에 의해서 비로소 적용될 수 있다.

좌익정당(Die Linke), 자유민주당(FDP), 녹색당(die Gruenen) 야당은 BSI가 새로운 데이터를 저장한다는 것을 비판적으로 보고 있다. 무엇보다 자유주의자들 또한 많은 비판을 하고 있다. 이 법률은 야간에 연방하원에서 비밀리에 통과되었다. 전

187) 이에 대해서 박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC, 인터넷법률, 법무부, 2008. 7, 통권 제43호, 144-175; - 유럽 공동체 통신데이터 저장 지침과 독일 개정 통신법, 법제처, 법제, 2008. 8, 130-154 참조.

연방의회부의장이었던 부르크하르트 히르쉬는 연방대통령에게 법률안의 서명을 하지 말도록 조언했으며, 연방헌법재판소를 통한 위헌소송도 언급하고 있다.[188]

2. 법률안의 목적 및 주요내용

연방정보기술보안청의 설립에 관한 법률(BSIG)은 1991년 발효 이후 중요한 변경은 없었다.
연방정보기술보안청(BSI)의 법률상 주요한 직무는 다른 기관에 IT 보안문제를 지원하고 보안증명서를 발급하는 것이었다. 보안증명서의 발급만으로는 BSI는 물론 IT 인프라의 형성에 대해서 아무런 중요한 역할을 할 수 없다. 또한 공공에 대한 자문도 연방정보기술보안청의 설립에 관한 법률(BSIG)에는 명백하게 규정하고 있지 않았다. 다른 공공기관의 지원기능은 동 법률에 규정되어 있지만, 상세하게 되어 있지 않다. BSI는 특히 독자적인 권한이 없고, 단지 요구가 있는 경우에 한해서만 활동하였다.
동 법률의 개정을 통하여 BSI에게 다음의 독자적인 권한을 인정하게 되었다. 즉 다른 기관의 공식적인 요청이 없더라도 연방행정에서의 IT보안을 높이고 연방의 정보기술에 대한 위험을 방지하기 위하여 독자적으로 활동하는 권한이다. 이 법률은 보안을 위한 일반적인 기술적 지침에 관한 규정, 개별적으로 정보기술의 설정을 위한 규정, 구체적인 위험의 방지를 위한 조치에 관한 규정 등을 포함하고 있다. BSI는 IT 보안을 위한 중앙기관으로써 취약점과 유해(악성)프로그램에 관한 정보를 수집하고, 이를 평가하여 관련기관에 그 결과를 알리거나 일반 공중에게 경고한다.
이를 통하여 시너지효과를 이용하게 되고 행정비용을 절약할 수 있는 한, 전기통신법(TKG)에 규정된 IT 보안 직무를 BSI에게 이전하게 될 것이다.[189]

3. 법률의 구성

동 법률은 4개의 조로 구성된 항목법률로 되어 있다. 즉 제1조는 연방정보기술보

---

188) http://www.heise.de/newsticker/Bundestag-beschliesst-neues-BSI-Gesetz--/meldung/140769.
189) BT-Drucksache 16/11967, S. 10.

안청에 관한 법률(BSIG), 제2조 전기통신법 개정, 제3조 텔레미디어법 개정, 제4조 효력규정으로 되어 있다. 중요 법률인 BSIG는 전체 12개조로 되어 있다. 연방정보기술보안청의 소속(제1조), 개념규정(제2조), BSI의 직무(제3조), 정보기술보안을 위한 중앙신고소(제4조), 악성프로그램과 연방의 통신기술에 대한 위험의 방지(제5조), 삭제(제6조), 경고(제7조), BSI의 의무(제8조), 인증(제9조), 시행령 제정권한(제10조), 기본권 제한(제11조), 연방정부의 IT 위탁에 대한 자문(제12조)

4. 주요 규정

제2조 개념규정

제1항 이 법에서 말하는 정보기술이란 정보의 처리나 전송을 위한 모든 기술적 수단을 포함한다.

제2항 이 법에서 말하는 정보기술 보안이란
1. 정보기술시스템, 구성요소 또는 처리과정에서 또는
2. 정보기술 시스템, 구성요소, 처리과정의 사용에 있어서
보안장치를 통하여 정보의 가용성, 무결성 및 기밀성과 관련한 특정한 보안기준을 유지하는 것을 의미한다.

제3항 이 법률에서 말하는 연방의 통신기술이란 하나 이상의 연방기관에 의하여 또는 하나 이상의 연방기관의 위탁에 의하여 운영되는 정보기술, 그리고 연방기관 상호간의 통신 또는 데이터교환에 제공되는 정보기술을 말한다. 연방법원의 통신기술은, 이것이 공개적인 법적 행정업무로 인정되지 않는 한, 그리고 연방하원, 연방상원, 연방대통령과 연방회계검사원의 통신기술은 이것이 오로지 독자적인 관할에서 운영되는 경우에는 연방의 통신기술이 아니다.

제4항 연방의 통신기술 중개소(Schnittstellen der Kommunikationstechnik)란 연방의 통신기술 내에서 또는 이들 사이에서 그리고 개별 연방기관, 연방기관의 그룹 또는 제삼자의 정보기술 사이에서 보안상 중요한 네트워크를 중개하는 곳이다.

제5항 악성프로그램(Schadprogramme)이란 권한 없이 데이터를 사용하거나 삭제

할 목적으로 기여하거나 권한 없이 그 밖의 정보기술적 과정에 영향을 미치는 목적으로 기여하는 프로그램과 그 밖의 정보기술적 과정과 절차를 말한다.

제6항 보안상 하자란 프로그램이나 그 밖의 정보기술 시스템의 특성을 말하는데, 제삼자가 이를 이용하여 권리자의 의사에 반해서 타인의 정보기술 시스템에 접근을 취득하거나 그 정보기술 시스템의 기능에 영향을 미칠 수 있게 한다.

제7항 인증기관을 통하여 제품, 처리, 시스템, 보호프로필(보안인증), 사람(인정인증) 또는 IT 보안서비스제공자가 특정한 요구를 충족하는 것을 확정하는 것이다.

제8항 이 법에서 의미하는 프로토콜데이터란 데이터 전송을 위한 정보기술 프로토콜의 조종데이터를 말하는데, 이것은 통신과정의 내용과는 상관없이 전송되거나 통신과정에 참여하는 서버에 저장되고 수신자와 송신자 사이의 통신의 보장을 위해서 필요한 데이터이다. 프로토콜데이터는 전기통신법 제3조 30호에 의한 통신데이터(Verkehrsdaten)와 제15조 1항에 의한 이용데이터(Nutzungsdaten)를 포함할 수 있다.
제9항 데이터 교환이란 기술적 프로토콜을 통하여 전송되는 데이터이다. 데이터교환은 전기통신법 제88조 1항에 의한 전기통신의 내용과 동법 제15조 1항에 의한 이용데이터를 포함한다.

제3조 BSI의 직무
제1항 BSI는 정보기술보안을 촉진한다. 이 외에 다음의 직무를 인정한다:
1. 연방의 정보기술의 보안에 대한 위험의 방지;
2. BSI의 직무 수행을 위하거나 보안이익을 위해서 필요한 경우에는 보안위험과 보안조치에 관한 정보의 수집과 평가 그리고 다른 기관을 위해서 획득한 인식내용의 사용.
이 외에 15호까지 직무가 있음.

제2항 BSI는 정보기술의 확보에 있어서 각 주의 요청에 지원할 수 있다.

제4조 정보기술보안을 위한 중앙 신고소

제5조 악성프로그램과 연방의 통신기술에 대한 위험의 방지

제1항 BSI는 연방의 통신기술에 대한 위험방지를 위해서,
1. 연방의 통신기술의 운영에 있어서 발생하는 프로토콜데이터를, 이것이 연방의 통신기술의 방해 또는 하자(흠결)의 인식, 제한, 제거를 위해서 또는 연방의 정보기술에 대한 공격의 인식, 제한, 제거를 위해서 필요한 경우에는, 수집하고 자동으로 평가한다.
2. 악성프로그램의 인식과 방지를 위해서 필요한 경우에는, 연방의 통신기술의 편집기관에 해당하는 데이터를 자동으로 평가한다.
다음의 각 항은 이 밖의 사용이 허용되지 않는 한, 이러한 데이터의 자동 평가는 지체없이 수행되어져야 하고 이것은 비교를 행한 뒤 지체 없이 흔적 없이 삭제되어야 한다. 사용제한은 프로토콜을 위해서는 적용되지 않는다. 이것이 개인관련 데이터(개인정보)나 통신의 비밀에도 해당되지 않는 한. 기관내부의 프로토콜데이터는 단지 각 해당 기관과의 합의하에서만 수집될 수 있다.

제2항 제1항 1문 1호에 의한 프로토콜데이터는 제1항 1문 1호에 의한 자동평가를 위해서 필요한 기간을 초과해하여 길어도 3개월 동안 저장될 수 있다. 이것이 발견된 악성프로그램으로부터 오는 위험의 방지를 위해서 또는 다른 악성프로그램의 인식과 방지를 위해서 제3항 2문에 의한 혐의의 증명이 있는 사례를 위해서 필요할 수 있는 사실상의 준거점이 있는 경우에는. 조직적 그리고 기술적 조치를 통하여 이 항에 의해 저장된 데이터의 평가는 단지 자동으로 행해진다는 것이 확보되어야 한다. 자동화되지 아니한 평가나 개인관련 데이터의 사용은 단지 다음 각 항의 기준에 따라서 허용된다.

제3항 제1항과 제2항을 초과하여 사용한 개인관련 데이터는 다만 다음의 경우에 한해서만 허용된다. 특정한 사실이
1. 이것이 악성프로그램을 포함하고 있거나,
2. 이것이 악성프로그램을 통하여 전달되었거나
3. 이것으로부터 악성프로그램의 징표를 나타낼 수 있는 혐의의 근거를 가지고 있고, 혐의를 증명하거나 반박하기 위해서 데이터처리가 필요한 경우. 이에 대한 증명이 있는 경우에는 개인관련 데이터의 더 이상의 처리는 다음의 경우에 허용된다. 이것이

1. 악성프로그램의 방지를 위해서,
2. 발견된 악성프로그램으로부터 발생하는 위험의 방지를 위해서 또는
3. 다른 악성프로그램의 인식과 방지를 위해서 필요한 경우에 한해서
악성프로그램은 제거되거나 그것의 작동방식에 방해가 되도록 할 수 있다. 제1항과 제2항에 의한 자동화되지 아니한 데이터의 사용은 오로지 법원으로부터 자격이 부여된 BSI의 공무원을 통해서만이 명령 될 수 있다. 통신진행과정에의 참여자는 늦어도 악성프로그램과 이로부터 발생한 위험의 인식과 방지 이후에 보고(통지)하여야 한다. 그것들이 알려지거나 그것의 실체가 지나치게 그 밖의 조사 없이도 가능하고 무엇보다도 제삼자의 보호 이익에 반하지 아니한 경우에는. 보고는, 그 자가 단지 사소하게 관련되어 있었고 그 자가 보고에 관심이 없다고 인정되는 경우에는, 중지될 수 있다. 제4항과 제5항의 사례에서의 통지는 이 기관을 위해서 적용되는 규정을 준용하여 거기에 언급된 기관을 통하여 수행된다. 이것이 통지의무에 대한 아무런 규정을 포함하고 있지 아니한 경우에는, 형사소송법의 규정이 이에 상응하게 적용될 수 있다.

제4항 BSI는 제3항에 의해 사용되는 개인관련 데이터를 형사소추기관에 중요한 의미를 가지는 범죄의 소추를 위해서 또는 전기통신 수단을 사용해서 범해진 범죄의 소추를 위해서 전달할 수 있다. BSI는 또한 이 데이터를
1. 악성프로그램으로부터 직정 발생하는 공공의 안전에 대한 위험방지를 위해서 연방과 주 경찰관서에,
2. 다른 권력을 위해서 안전을 위협하거나 비밀정보기관의 활동을 인식하게 하는 활동에 대한 보고를 위해서 연방헌법보호(수호)에 전달할 수도 있다.

제5항 그 밖의 목적을 위하여 BSI는 데이터를 전달할 수 있다.
1. 연방과 주의 경찰관서에 국가의 존립이나 안전에 대한 위협 또는 개인의 생명, 신체, 자유 또는 이것의 유지가 공공의 이익에 제공되는 의미를 가지는 물건에 위험을 방지하기 위해서,
2. 연방과 주의 헌법보호기관에게대한 폭력을 행사하거나 이를 목적으로 하는 예비행위를 통하여 연방헌법보호법 제3조 1항에 언급된 보호법익에 반하는 독일연방공화국내에서의 기도행위에 대한 사실상의 준거점이 있는 경우에.
1문 1호에 의한 전달은 법원의 동의가 필요하다. 1문 1호에 의한 절차를 위해서는 비송사건절차법의 규정이 준용된다. 관할은 BSI의 소재지를 관할하는 구법원이다.

1문 2호에 의한 전달은 연방내무부장관의 동의에 의해서 수행된다; 편지.우편.통신비밀의 제한에 관한법률(Artikel 10-Gesetzes) 제9조 내지 제16조가 준용된다.

제6항 앞의 각 항을 벗어나는 다른 목적을 위한 내용평가와 제3자에 대한 개인관련 데이터의 전달은 허용되지 않는다. 제1항내지 제3항의 조치를 근거로 사적 생활형성의 핵심영역에 대한 인식내용이나 연방데이터보호법 제3조 9항의 데이터가 획득되는 경우에는, 이것은 사용되어서는 아니된다. 사적 생활형성의 핵심영역에 대한 인식내용은 지체 없이 삭제되어야 한다. 사적 생활형성의 핵심영역에 속하는지가 의심이 있는 경우에는 이것을 경우에 따라서는 삭제하거나 지체 없이 이에 대한 사용이나 삭제데 대한 결정을 위해서 연방내부장관에게 지체 없이 제출해야 한다. 이것의 획득과 삭제의 사실은 문서로 작성되어야 한다. 이 문서는 오로지 데이터보호통제의 목적을 위해서만 사용되어야 한다. 이러한 목적을 위해서 이것이 더 이상 필요하지 않는 경우에는, 늦어도 서류가 작성된 년도의 말까지 삭제되어야 한다.

제7항 BSI는 데이터의 수집과 사용을 개시하기 이전에 데이터 수집과 사용개념을 설정하고 연방 데이터보호수탁자를 통한 통제를 위해서 준비해야 한다. 그 개념에는 연방정부와 통신의 특별한 보호필요성이 고려되어야 한다. 연방 데이터보호수탁자는 그의 통제결과를 연방데이터보호법 제24조에 의해서 또한 연방정부의 IT 수탁자 위원회에 통보해야 한다.

제6조 삭제

BSI는 자기의 권한과 관련하여 개인관련 데이터를 수집한 경우에는, 직무수행을 위해서 수집된 데이터가 더 이상 직무수행을 위해서 또는 예상되는 법원의 심사를 위해서 더 이상 이용되지 않는 즉시 이것은 지체 없이 삭제해야 한다. 그 삭제가 오로지 예상되는 법원의 심사를 위해서만 제5조 3항에 의한 조치로부터 보류되는 한, 그 데이터는 당사자의 동의 없이 이러한 목적을 위해서만 사용될 수 있다; 이것은 다른 목적을 위해서는 차단되어야 한다, 제5조 6항은 아무런 영양을 받지 않는다.

제7조 경고

제1항 제3항 1항 2문 14호에 의한 직무를 수행하기 위해서 BSI는 정보기술 제품과 서비스의 보안상의 하자에 대한 경고와 관련 당사자의 범위 또는 공중에게 악성프로그램에 대한 경고를 배포하거나 보안조치 및 특정한 보안제품의 설치를 추천할 수 있다. 발견한 보안상의 하자나 악성프로그램이 일반적으로 알려지지 아니하는 경우에는, 더 이상의 유포나 불법한 이용을 방지하기 위해서 또는 BSI가 제삼자에 대해서 기밀을 지켜야 하는 의무가 있기 때문에, 그것은 경고될 사람의 범위를 사물상의 기준에 따라서 제한할 수 있다; 사물상의 제한은 특히 특정한 시설의 특별한 위험 또는 특별한 수신자의 허용이 될 수 있다.

제2항 제3항 1항 2문 14호에 의한 직무를 수행을 위해서 BSI는 공중에게 관련제품의 제작자와 표지에 이름을 붙여서 정보기술 제품이나 서비스의 보안상의 하자와 악성프로그램을 경고하거나 보안조치 및 특정한 보안제품의 설치를 추천할 수 있는데, 이로부터 정보기술의 안정에 대한 위험이 발생한다는 것에 대한 충분한 준거점이 있는 경우에 한한다. 공중에게 배포된 정보가 차후에 거짓으로 되거나 또는 근거가 되는 상황이 불충분한 것으로 재배포된 것으로 드러나는 경우에는 이것은 지체 없이 공중에게 알려야 한다.

5. <부록5> 통신망에서 아동포르노의 척결을 위한 법률안 (Entwurf eines Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen)

1. 개관

이 법률은 전체 4개의 Artikel로 구성된 항목법률이다. 4개의 Artikel은 통신망에서 아동포르노에의 접근을 어렵게 하는 법률(Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz - ZugErschwG)(Artikel 1), 전기통신법 관련 규정의 개정(Artikel 2), 연방정부의 연방의회에의 보고의무(Artikel 3), 발효 및 실효(Artikel 4). 이 중에서 Artikel 1이 중요하다.

이 법률안은 CSU/CDU와 SPD의 대연정에서 격렬한 공개토론이 있은 후 합의를 도출했다. 2009년 6월 18일 찬성289표, 반대 128표, 기권 18표로 연방하원, 2009년 7월 10일 연방하원의 동의를 얻어 통과되었다. 아직 발효되지 않고 있으며, 2012년 말까지 한시적 효력을 가진다(한시법).

[통신망에서 아동포르노에의 접근을 어렵게 하는 법률]은 WWW에서의 아동포르노 웹사이트에의 접근을 어렵게 하는 것이다. 하지만 동법 제5조에서 차단된 웹사이트나 도메인의 호출로 인한 형사소추는 부정된다.

연방범죄수사청은 형법 제184b조(아동포르노는 아동에 대한 성적남용행위로써 아동포르노를 유포, 취득 또는 소지하는 경우에 형법 제184b조에 의하여 처벌됨)에 의한 아동포르노 웹사이트 및 아동포르노를 링크한 사이트의 도메인네임, IP주소, URL를 나타내는 차단리스트를 작성하여 서비스제공자에게 배포하여 이들이 차단될 수 있도록 하고 있다. 다만 이들 사이트는 삭제될 수 없거나 적정한 시간 내에 삭제될 수 없는 경우에 한한다.
범죄가 되는 웹사이트의 내용제공자와 호스트제공자는 이의 지정에 대해서 통지를 받아야 한다. 10.000명 이상의 고객을 가진 접속제공자는 법률적으로 차단리스트에 표시된 음란정보에 대한 접근을 최소한 DNS-차원에서 차단하고, BKA가 설치한 정지 표지(Stopp-Schield) 우회하여 접속토록 하고, BKA에게 익명의 접근통계를 전달해야 할 의무가 있다. BKA는 차단의 근거를 실제의 아동포르노를 통하여 차단의 근거를 문서로 기록해야 하고 연방 데이터보호수탁자에 의해서 임명된 전문가위원회의 한 사람(5명으로 구성되어 있으며 이 중 과반수는 법관의 자격을 요한다) 매분기마다 표본조사의 방법으로 통제를 받아야 한다.

이 법률이 통과된 이후 SPD의 Jörg Tauss 의원은 연방헌법재판소에 이 법률에 대해서 기관쟁송을 제기했다. 그 이유는 법률안의 중요한 변경이 있음에도 불구하고 연방하원이 입법과정에서 새로운 제1독회의 날짜를 정하지도 않았기 때문이다. 처음 제출된 법률안에는 Artikel 1이 텔레미디어법(Teledienstgesetz, TMG)의 개

정이었는데, 이후에 [통신망에서 아동포르노 내용의 접근을 어렵게 하는 법률]이란 단행법률로 제정되었기 때문이다.

이 법률 통과 이전에 이 법률안에 대한 찬반논쟁이 치열하였다. 반대하는 입장에서 기본권침해와 관련하여 많은 비판이 제기되었다. 즉 통신비밀, 정보자기결정권, 정보의 자유, 서비스제공자의 직업의 자유를 침해한다고 주장하였다(Telemedicus, Netzsperren: Der neue Entwurf und seine Rechtsmäßigkeit. 24. April 2009.).
뿐만 아니라 이 법률안에 대한 반대시위를 비롯하여 온라인 청원(Petition: Kinder- und Jugendhilfe - Kinderpornografie im Internet vom 17.03.2009, https://epetitionen.bundestag.de/index.php?action=petition;sa=details;petition=3293)도 있었다. 그 외에 미디어관련 입법권과 경찰의 예방적 입법권은 연방관할이 아니라 각 주 관할이라는 비판, 인터넷검열이라는 비판, 아동음란물의 척결이 아니라 사전선거운동이라는 등 많은 비판이 제기되었다.

이에 대하여 독일 아동원조단체는 2009년 5월 연방정부의 입법안을 지지하기 위해서 여론조사를 실시하였는데, 그 결과는 응답자의 92%가 이 법률안에 찬성하는 것으로 나왔다. 이에 대해서 인터넷차단 남용 피해자 단체(Der Verein MissbrauchsOpfer Gegen InternetSperren)로 부터 설문 조항이 조작되었다는 비판이 제기되기도 하였다.

2. 주요 내용

통신망에서 아동포르노 내용의 접근을 어렵게 하는 법률(Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz - ZugErschwG)

제1조 차단리스트

제1항 연방범죄수사청(BKA)은 형법 제184b조에 의한 아동포르노를 포함하고 있거나 이러한 텔레미디어 제공을 링크하는 데에 그 목적이 있는 도메인네임, IP 주소, URL의 대한 리스트를 작성한다(차단리스트). 연방범죄수사청은 제2조에 의한 서비스제공자에게 매일 통지해야 할 시점에 최신의 차단리스트를 제공한다.

제2항 텔레미디어제공물의 삭제를 목적으로 하는 허용된 조치가 가망이 없거나 적절한 시간 내에도 가망이 없는 경우에 한해서만 차단리스트에 등재된다. 유럽연합 전자상거래지침(der Richtlinie 2000/31/EG)의 적용영역에 있는 다른 국가에서 개업한 서비스제공자의 텔레미디어 제공물이 차단리스트에 등재되기 이전에 텔레미디어법 제3조 5항 2문에 의한 절차가 수행되어야 한다. 이 지침의 적용영역 바깥에 있는 국가에서 해당 국가에서 다른 조치들, 특히 경찰상의 정보교류를 위한 관할 관청에의 통지가, 텔레미디어 제공물을 삭제할 가망이 없거나 적절한 시간 내에도 가망이 없다고 연방범죄수사청의 평가(사정)에 의해서 도출되는 경우에 그 텔레미디어는 즉시 차단리스트에 등재될 수 있다.

제3항 텔레미디어 제공물이 처음 또는 새로이 차단리스트에 등재되는 경우에는, 연방범죄수사청은 일반적으로 텔레미디어법 제7조 1항의 독자적인 정보로써 이러한 텔레미디어 제공물의 이용에 제공하는 서비스제공자에게 또는 텔레미디어법 제10조에 의한 이러한 텔레미디어 제공물을 이용자를 위해서 저장하는 서비스제공자에게, 서비스제공자가 적당한 비용이 산출되는 경우에는 차단리스트에의 등재와 그 이유를 알려야 한다. 그러한 서비스 제공자가 독일연방공화국의 통치권 바깥에서 자신의 소재지를 가지고 있는 경우에는 연방범죄수사청은 제2항에 의해서 통지가 이미 발생하지 않는 경우에는 해당 국가의 다른 국가와 경찰상의 정보교류를 위한 관할 관청에 알린다.

제2조 접근을 어렵게 함

제1항 텔레미디어법 제8조에 의한 서비스 제공자는 그가 최소한 10.000 참여자

또는 그 밖의 이용권자를 위해서 통신망에 정보의 이용을 위해 접근을 가능하게 하는 경우에는 차단리스트에 열거되는 텔레미디어 제공물에의 접근을 어렵게 하기 위해서 적합하고 적절한 조치를 강구해야 한다. 1문에 의한 조치들이 이미 다른 제공자에 의해서 수행되고 있는 그러한 접근만을 제공하는 서비스제공자 또는 공중을 위해서 인터넷 접속을 제공하지 아니하는 서비스제공자가 스스로 동일하게 효과가 있는 차단조치를 설치하는 경우에는 이것은 적용되지 아니한다.

제2항 차단을 위해서는 텔레미디어 제공의 도메인네임, IP주소, URL이 사용될 수 있다. 그 차단은 최소한 도메인네임의 단계에서 이루어진다. 그것의 폐기는 이에 속하는 IP주소에서 중지된다.

제3항 서비스제공자는 연방범죄수사청이 최신의 차단리스트를 제공한 이후 지체없이 하지만 늦어도 6시간 이내에 조치를 취해야 한다.

제3조 차단리스트의 확보

제2조의 서비스제공자는 차단의 전환에 참여하지 않는 제삼자를 통한 인식에 대하여 적절한 조치를 통하여 차단리스트를 확보해야 한다.

제4조 정지표시

제2조에 의한 서비스제공자는 차단리스트에 등재된 텔레미디어 제공물이 호출될 수 있도록 한 이용자 질문을 연방범죄수사청이 운영하는 텔레미디어 제공물(정지표시)로 우회하도록 하는데, 이것은 이용자에게 차단의 근거 및 접속가능성에 대해서 연방범죄수사청으로 문의하도록 한다.

제5조 통신데이터와 이용데이터

접속을 어렵게 한 근거로써 정지표시로 우회하는 경우에 발생하는 통신데이터와 이용데이터는 형사소추를 목적으로 사용되어서는 아니된다.

제6조 접근시도의 회수 익명 작성 제공

제2조의 서비스제공자는 연방범죄수사청에게 매주 차단리스트에 등재된 텔레미디어제공물에 대한 매시간당 접근시도의 회수를 익명으로 작성하여 제공한다.

제7조 민사상의 청구권

제1항 제2조의 서비스제공자는 그가 제2조 내지 제4조에 의한 조치를 통해서 차단리스트를 최소한 과실없이 규정에 따르지 아니하고 전환한 경우에 한해서 책임을 진다.

제2항 이 법률의 전환을 위해서 만들어지는 기술적 차단 조치와 함께 제2조의 서비스제공자에 대한 민사상 청구권을 요구하는 것은 불가능하다.

제8조 연방범죄수사청의 문서기록의무 및 정보제공의무

제1항 연방범죄수사청은 차단리스트에 등재된 기록들이 연방범죄수사청에 의해서 평가되는 시점에 제1항에 의한 조건을 충족하였다는 증명이 될 만한 서류를 구비해야 할 의무가 있다.

제2항 연방범죄수사청은 정당한 이익을 설명하는 동 법률의 서비스제공자들에게 텔레미디어 제공물이 차단리스트에 포함되어있는지 또는 있었는지 그리고 어떤 기간 동안 그랬는지에 대한 문의에 대하여 정보를 제공한다.

제9조 전문가위원회

연방 데이터보호 위탁자는 5인으로 구성되는 독립적인 전문가위원회를 선출한다. 구성원은 2012년 12월 31일까지 임명된다. 구성원의 과반수는 법관의 자격이 있어야 한다. 연방범죄수사청에게 차단리스트를 언제나 열람할 권리가 있다. 위원회는 최소한 상당한 수의 표본을 기초로 하여 리스트에 기록된 것들이 동법 제1조 1항의 조건을 갖추고 있는지에 대하여 매분기마다 심사한다. 열거된 텔레미디어 제공물이 이러한 조건을 충족하지 못했다고 확정되면, 연방범죄수사청은 이 텔레미디어 제공물을 가장 최근 목록에서 삭제해야 한다.

제10조 기술적 지침

차단리스트와 제6조에 의한 기록을 어떠한 형식과 어떠한 절차에 의해서 할 것인가는 연방범죄수사청은 서비스제공자의 참여하에 기술적 지침에서 정한다.

제11조 기본권의 제한

통신비밀의 기본권(기본법 제10조)은 동 법률 제2조 내지 제4조에 의해서 제한된다. 이를 통하여 전기통신법 제88조 제3항 3문에 의한 전기통신과정이 관련된다.

제12조 행정법적 소송방법

차단리스트에 텔레미디어의 수용에 관한 논쟁에는 행정법적 소송방법이 있다.

제13조 질서위반행위

제1항 고의 또는 과실로
1. 동 법률 제2조 1항 1문 또는 4문에 반하여 조치를 하지 않거나 적시에 취하지 아니한 자

2. 제3조에 반하여 차단리스트를 확보하지 않거나 적시에 또는 불완전하게 확보한 자는 질서위반행의에 해당한다.

Artikel 2 전기통신법 개정

Artikel 3 연방정부는 연방하원에 이 법률의 발효 이후 2년 이내에 이 법률의 적용에 관한 보고서를 제출해야 한다. 여기에는 접근을 어렵게 한 법률 제9조에 의한 전문가위원회의 경험이 포함되어야 한다.

Artikel 4 발효 및 실효

(1) 동 법률은 제2항을 유보하여 공포한 날로부터 발효된다.

(2) Artikel 1 제13조는 동 법률의 발효 후 6개월이 되어야 효력이 있다.

(3) 동 법률의 Artikel 1은 2012년 12월 31일이 경과하면 실효된다.

미국

1. <부록6> 「컴퓨터 사기 및 오용에 관한 법률(CFAA : Computer Fraud and Abuse Act)」

Computer Fraud and Abuse Act : CFAA

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or

of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)

(i) knowingly causes the transmission of a program, information, code,

or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or

national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [1]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an

attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or

both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)

(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure

for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a

manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) [2] of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may

be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

「컴퓨터 사기 및 오용에 관한 법률」

§ 1030. 컴퓨터에 관한 사기 및 이에 관련된 행위[190]

(a) 다음에 열거된 자는

(1) 정당한 권한 없이 또는 허가된 접근 범위를 넘어 고의로 컴퓨터에 접근함으로써 미국 정부가 행정명령이나 법률에 의거 국방 또는 국제 관계의 견지에서 무단 공개되지 않도록 보호하기로 한 정보 및 1954년의 원자력법 제 11조 (y)항에서 규정한 것과 같은 제한된 자료를 취득한 뒤, 이렇게 하여 취득한 정보가 미국을 해치고 어느 외국을 이롭게 하는데 쓰일 수 있다고 믿을 이유를 가지고, 이를 받을 자격이 없는 사람에게 함부로 통지, 배달, 전송하거나 통지, 배달, 전송되게 하거나, 통지, 배달, 전송할 것을 기도하거나, 통지, 배달, 전송되게 하도록 기도하거나, 이러한 정보를 정당하게 받을 자격이 있는 미국 정부 공무원이나 고용원에게 고의로 제대로 배달하지 않는 자;

(2) 정당한 권한 없이 또는 허가된 접근 범위를 넘어 고의로 컴퓨터에 접근함으로써 다음과 같은 정보를 취득하는 자

(A) 금융기관이나 15U.S.C.1602(n)에서 규정한 카드 발급자의 금융기록에 포함된 정보 또는 공정신용보고법(Fair Credit Reporting Act) (15U.S.C.1681 참조)에서 정의된 용어에 따른 소비자보고기관의 파일에 들어있는 정보;

(B) 미국의 각 정부부처 또는 행정기관으로부터 나온 정보; 또는

---

190) 18U.S.C.§1030 Fraud and related activity in connection with computers에 대한 동 번역문은 프로그램심의조정위원회, 「미국 IT법제자료 번역연구」, 2002. 12. pp31-37. 국가 정보 기반시설 보호법(National Information Infrastructure Protection Act of 1996)에 따라 개정된 번역문을 토대로 그 이후에 여러 차례 개정되고 최종적으로는 2008년의 신분 절취 강화 및 회복법(Identity theft Enforcement and Restitution Act of 2008)에 따라 개정되어 2008. 9. 26일부터 시행되고 있는 조문을 번역한 것이다.

(C) 주간(州間) 또는 외국과의 통신에 포함되어 보호되는 컴퓨터로부터 나온 정보;

(3) 고의로, 미국의 각 정부부처 또는 행정기관의 비공개 컴퓨터에 접근할 권한이 없이, 미국정부가 전용하는 정부기관 또는 대행기관 컴퓨터에 접근하는 자; 또는 그 컴퓨터가 미국 정부의 전용이 아니라 하더라도 그것이 미국 정부에 의하여 또는 미국 정부를 위하여 사용될 경우, 이러한 정부에 의한 또는 정부를 위한 사용에 영향을 미치는 자;

(4) 고의로, 사취할 목적으로, 정당한 권한 없이 또는 허가된 접근 범위를 넘어 보호되는 컴퓨터에 접근하고 이렇게 함으로써 의도된 사취를 더 진행시키고 이득을 취하는 자. 다만, 사기의 목적과 얻은 이익이 단지 컴퓨터를 사용하는데 그치거나 사용의 가치가 1년간 $5,000 이하인 경우에는 제외한다;

(5)

(A)

(i) 고의로 프로그램, 정보, 부호, 또는 명령을 전송하게 하여, 보호되는 컴퓨터에 정당한 권한 없이 손상을 입히게 하고;

(ii) 정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 무모하게 손상을 입히게 하고; 또는

(iii) 정당한 권한 없이 보호되는 컴퓨터에 고의로 접근함으로써 손상을 초래하는 자; 그리고

(B) 전 호 (A)의 (i), (ii), (iii)에서 열거된 행위로 인해 다음과 같은 결과를 초래하는 자 (또한, 범죄 기도의 경우에는 만일 그 것이 실제로 이루어 졌다면 발생했을 경우를 추정한다)

(i) 1년간 1인 또는 그 이상에게(수사, 기소, 또는 미국 정부에 의해서 행해지는 다른 절차를 위한 경우에는 행위로부터 유발되는 손실을 말한다) 총 $5,000 이상의 손실;

(ii) 1인 이상에게 의료 처리나 진단, 치료, 간호 중에 발생하는 수정 또는 손상, 잠재적인 수정 또는 손상;

(iii) 개인에 대한 신체적 손상;

(iv) 공공 보건이나 안전에 대한 위협; 또는

(v) 정부조직체가 운영하는 또는 정부조직체를 위하여 운영되는 컴퓨터 시스템에 영향을 미치는 손상(특히 법무 행정, 국가방위, 국가보안의 경우;

(6) 고의로 그리고 사취할 목적으로 암호 또는 이와 유사한 정보를 거래(제1029조에서 규정한 바와 같이) 함으로써 정당한 권한 없이 컴퓨터에 접근하는 자. 다만, 다음의 경우가 전제된다.

(A) 이런 거래가 주간(州間) 또는 외국과의 통상에 영향을 미치는 경우; 또는

(B) 접근한 컴퓨터가 미국 정부에 의하여 또는 미국 정부를 위하여 쓰이는 경우;

(7) 어떤 자(any person)로부터 금전이나 기타 가치 있는 물건을 강제로 탈취하

기 위하여 주간(州間) 또는 외국과의 통상에서 보호되는 컴퓨터에 손상을 입힐 것을 위협하는 통신문을 전송하는 자;

제 1030조 (c)항에서 정하는 바에 따라 처벌한다.

(b) 제 1030조 (a)항에서 정한 범죄를 기도한 자는 제 1030조 (c)항에서 정하는 바에 따라 처벌한다.

(c) 제 1030조의 (a)항 또는 (b)항에서 정한 범죄에 대한 처벌은 다음과 같다.

(1)

(A) 본 조의 (a)항 (1)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이 아니면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 10년 이하의 징역에 처하거나 이 두 가지를 병과한다; 그리고

(B) 본 조의 (a)항 (1)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 다른 유죄판결이 있은 후에 저질러진 것이면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 20년 이하의 징역에 처하거나 이 두 가지를 병과한다;

(2)

(A) (B)에서 따로 규정한 경우를 제외하고는 본 조의 (a)항의 (2)호, (3)호, (a)항의 (5)호(A)(iii), 또는 (a)항의 (6)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이 아니면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 1년

이하의 징역에 처하거나 이 두 가지를 병과한다;

(B) (a)항의 (2)호에서 정하는 범죄가 아래의 경우에 해당할 때에는 본 편(title)에서 정하는 벌금이나 5년 이하의 징역에 처하거나 이 두 가지를 병과한다.

(i) 상업적인 이익이나 사적 금융이익을 위하여 죄를 범한 때;

(ii) 이러한 범죄가 헌법이나 미국 또는 어느 주의 법률에 위배하여 범죄적인 또는 불법행위적인 행위를 진행시키기 위하여 저질러졌을 때; 또는

(iii) 취득한 정보의 가치가 $5,000을 넘을 때; 그리고

(C) 본 조의 (a)항의 (2)호, (3)호, (6)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 1년 이하의 징역에 처하거나 이 두 가지를 병과한다.

(3)

(A) 본 조의 (a)항의 (4)호, (7)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이 아니면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 5년 이하의 징역에 처하거나 이 두 가지를 병과한다; 그리고

(B) 본 조의 (a)항의 (4)호, (a)항의 (5)호(A)(iii), (a)항의 (7)호에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이면, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 10년 이하의 징역에 처하거나 이 두 가지를 병과한다;

(4)

(A) (5)항에서 따로 규정한 경우를 제외하고는 (a)항의 (5)호(A)(i)에서 정한 범죄를 저지르거나, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 10년 이하의 징역에 처하거나 이 두 가지를 병과한다;

(B) (a)항의 (5)호(A)(ii)에서 정한 범죄를 저지르거나, 또는 본 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 5년 이하의 징역에 처하거나 이 두 가지를 병과한다;

(C) (5)항에서 따로 규정한 경우를 제외하고는 (a)항의 (5)호(A)(i) 또는 (5)호(A)(ii)에서 정한 범죄가 본 조에서 정한 다른 범죄에 대한 유죄판결이 있은 후에 저질러진 것이면, 또는 그 두개 항에 의하여 처벌될 수 있는 범죄를 기도했을 경우에는, 본 편(title)에서 정하는 벌금이나 20년 이하의 징역에 처하거나 이 두가지를 병과한다; 그리고

(5)

(A) 만일 범죄자가 (a)항의 (5)호(A)(i)을 위반하여 고의로 또는 무모하게 심각한 신체적 손상을 입히거나 이를 기도했을 경우에는 본 편(title)에서 정하는 벌금이나 20년 이하의 징역에 처하거나 이 두 가지를 병과한다; 그리고

(B) 만일 범죄자가 (a)항의 (5)호(A)(i)을 위반하여 고의로 또는 무모하게 사망에 이르거나 살인을 기도했을 경우에는 본 편(title)에서 정하는 벌금이나 최고 종신형에 처하거나 이 두 가지를 병과한다;

(d)

(1) 미국 비밀검찰국은 동일한 권한을 갖는 다른 기관과 더불어 본 조에서 규정된 범죄를 수사할 권한을 갖는다.

(2) 미국 연방수사국(FBI)은 스파이 행위, 해외 방첩, 국방, 외교 등을 이유로 허가받지 않은 자에 대한 노출로부터 보호되는 정보, 또는 1954년의 원자력법 제11조 y항(42U.S.C.2014(y))에서 규정한 것과 같은 제한된 자료를 포함하여 (a)항의 (1)호에서 규정된 범죄에 대하여 우선적인 수사권을 갖는다. 다만 본 편(title)의 3056조 (a)호에 따른 미국 비밀검찰국의 직무에 영향을 미치는 범죄를 제외한다.

(3) 그러한 수사권은 재무부장관과 법무부장관에 의한 동의에 따라 행사된다.

(e) 본 조에서

(1) "컴퓨터"라 함은 전자적, 전기적, 광학적, 전기화학적, 또는 기타 고속처리장치로서 논리적, 산술적, 또는 저장의 기능을 수행하는 것을 의미하며, 이런 장치에 직접 관련되어 있거나, 이런 장치와 맞물려 작동하는 자료 저장 장치나, 통신 장치를 말한다. 그러나 자동화된 타자기나 식자기, 휴대용 소형 계산기 또는 이와 유사한 장치들은 포함되지 않는다;

(2) "보호되는 컴퓨터"라 함은

(A) 금융기관 또는 미국 정부가 전용하는 컴퓨터를 의미하며, 그렇게 전용하지 않는 경우에는, 금융기관이나 미국 정부에 의하여 사용되거나 금융기관이나 미국 정부를 위하여 사용되는 컴퓨터로서, 범죄를 구성하는 행위가 금융기관이나 미국정부에 의한, 또는 금융기관이나 미국정부를 위한 사용에 영향을 미치는 경우; 또는

(B) 이러한 컴퓨터가 주간(州間) 또는 외국과의 통상이나 통신에 사용되는 경우를 말하는데, 미국과의 주간(州間) 또는 외국과의 통상이나 통신에 영향을 미치는 방식으로 사용되는 경우 미국 외에 있는 컴퓨터를 포함한다.

(3) "주(州)"에는 콜롬비아 특별구, 프에르토리코 특별주와 기타 미국의 특별주, 속령 또는 해외 영토가 포함된다;

(4) "금융기관"은 다음을 의미한다.

(A) 연방예금보험공사에 의하여 그 예금이 보증되어진 기관;

(B) 연방지불준비국 및 연방준비은행을 포함한 연방준비금 기구의 회원;

(C) 전국소비자신용조합본부에 의하여 그 계좌가 보증된 신용조합;

(D) 연방주택융자은행의 회원 및 주택융자은행;

(E) 농가신용대부법(Farm Credit Act of 1971)에 의하여 설립된 농가신용 대출기관;

(F) 증권거래법(Securities Exchange Act of 1934) 제 15조에 의거 증권거래위원회에 등록된 중개 거래인;

(G) 증권투자자보호공사;

(H) 국제은행업법(International Banking Act of 1978) 제 1조 (b)항 (1)호 및 (3)호에서 규정한 외국은행의 지점 또는 대리인; 그리고

(I) 연방준비금법(Federal Reserve Act) 제 25조 또는 제 25조 (a)항에 의거 운영되는 기관;

(5) "금융기록"이라 함은 금융기관이 고객과의 관계에 관하여 유지하고 있는 기록으로부터 나온 정보를 의미한다;

(6) "허가된 접근범위를 넘어(exceeds authorized access)"라 함은 허가를 받아 컴퓨터에 접근하는 자가 그 컴퓨터 안에 있는 정보를 취득하거나 변경할 자격이 없는데도 불구하고 그렇게 하는 것을 의미한다;

(7) "미국 정부기관(department of the United States)"이라 함은 정부의 입법부와 사법부 또는 미국법전 제 5편 제 101조에 열거된 행정부 기관을 의미한다;

(8) "손상(damage)"이라 함은 자료, 프로그램, 시스템, 또는 정보의 완전성과 이용 가능성을 다음 중 어느 하나와 같이 해치는 것을 의미한다;

(9) "정부조직체(government entity)"라 함은 미국 정부나 주, 주의 정치적 하위단위, 외국, 외국의 주, 도, 지방자치단체, 또는 외국의 정치적 하위단위를 포함한다;

(10) "유죄판결(conviction)"이라 함은 범죄 구성요소가 컴퓨터에 대한 권한 없는 접근, 또는 허가된 접근 범위를 넘은 접근 등으로 어느 주법 하에서 1년 이상 징역에 처해질 수 있는 범죄에 따른 유죄판결을 포함한다;

(11) "손실(loss)"이라 함은 범죄행위에 수반되는 비용, 손상을 평가하는 비용, 범죄행위 이전 상태로 자료, 프로그램, 시스템, 또는 정보를 복구하는 비용과 서비스 방해로 인해 발생된 다른 손실 수익, 비용, 또는 결과적 비용을 포함하는 희생

자가 부담하는 합리적 비용을 의미한다;

(12) "자(者, person)"라 함은 자연인, 회사, 협회, 교육기관, 금융기관, 정부조직체, 기타 법인을 의미한다.

(f) 본 조의 규정은 미국, 주, 주의 정치적 하위조직의 사법기관 또는 비밀 정보기관의 합법적으로 승인된 수사 활동, 보호활동 또는 정보활동은 금지하지 않는다.

(g) 본 조의 규정을 위반한 행위로 손상이나 손실을 입은 자는 그 행위자에 대하여 민사상 보전적 손해배상과 금지명령, 기타 형평법상의 구제조치를 청구할 수 있다. 본 조 규정 위반 행위에 대한 민사상 대응은 그 위반행위가 (a)항의 (5)호(B)의 (i), (ii), (iii), (iv), (v) 중 어느 하나에 해당될 경우에만 가능하다. (a)항의 (5)호(B)의 (i)에서 규정된 행위만을 포함하는 손상은 경제적 손상에만 제한적으로 적용된다. 본 조 규정 위반 행위에 대한 민사상 대응은 손상을 발견한 날로부터 2년 이내에 또는 고소한 날로부터 2년 이내에 취해지지 않으면 효력이 없다. 또한 과실로 인한 컴퓨터 하드웨어, 소프트웨어, 또는 펌웨어의 제작 또는 제조 행위에 대해서는 본 조 규정 위반 행위에 대한 민사상 대응을 할 수 없다.

(h) 법무부장관과 재무부장관은 본 항이 제정된 날로부터 3년 동안에는 해마다 (a)항의 (5)호에 의한 수사와 기소 사항에 관하여 의회에 보고하여야 한다.