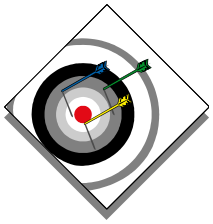


포/커/스

# 일본의 정보보안 분야 정책 동향

김정태* 이현우**

최근 일본은 정보통신 사회로 급속히 전환하는데 성공한 것으로 보인다. 네트워크를 중심으로 한 정보통신 사회에서는 편리함의 이면에 위험성이 뒤따르는 만큼보다 안전한 체계와 구조를 갖추어 많은 이용자들이 네트워크를 안심하고 사용할 수 있도록 환경을 정비하는 것이 중요하다. 일본 정부는 이러한 중요성을 인식하고, 정보보안 분야에서 법제 정비, 사업자와 이용자에 있어서 대책 실시의 촉진, 연구 개발 및 인재 육성의 추진, 보안 대응 기구의 설립 등에서 다양한 정책을 제정하고 추진해 나가며 위험성을 감소시키는 것에 노력을 기울이고 있다.

본 고에서는 'e-Japan 전략'과 근래에 발표된 정책들을 통해 일본의 정보보안 분야에서의 동향을 살펴보도록 한다. ▧

목 차



* ETRI 정보기반연구팀/연구원
** ETRI 정보기반연구팀/책임연구원

## Ⅰ. 서 론

21 세기에 접어들면서 주요 선진국들이 여러 분야를 아우르는 정보통신 환경을 구축한데 비해 상대적으로 뒤쳐진 모습을 보이던 일본에서는 수 년 내 세계 최첨단의 정보통신 국가로 변모하겠다는 계획으로 2001 년 1 월 'e-Japan 전략'을 결정하였다. 또한, 이후의 'e-Japan 중점 계획 2002,' 'e-Japan 전략 Ⅱ,' 'e-Japan 중점 계획 2003' 등을 점진적으로 추진해 나가면서 인터넷 접속 서비스 이용자의 수와 함께 초고속 인터넷 서비스 이용자의 비율이 급증하였고, 자연적으로 사회전반의 정보통신 사회로의 전환이 급속히 진행되었다.

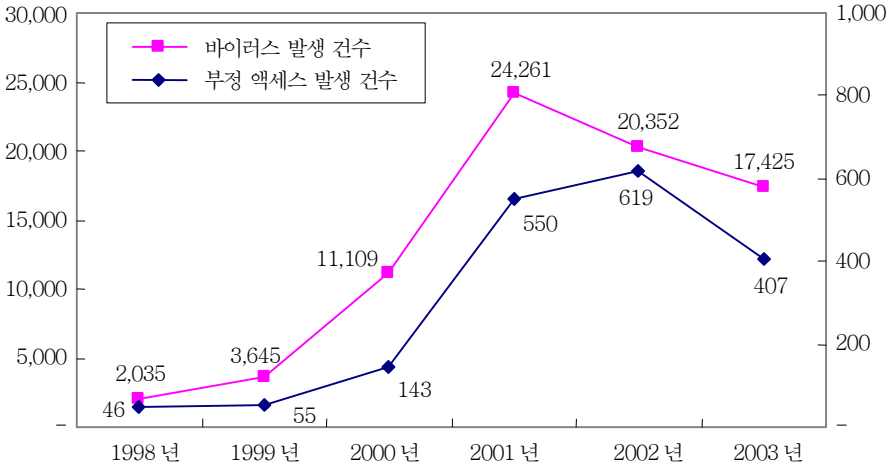
그러나, 이러한 긍정적인 성과와 더불어 정보통신 환경이 구축되기 이전에는 고려 대상이 되지 않았던 문제들이 대두되기 시작하였다. 일본정부가 적

극적으로 추진 중인 전자정부의 실현이나 정보통신 사회로의 전환에 있어서, 기밀 정보의 부정 취득, 정치적 또는 경제적 목적의 사이버 테러리즘, 바이러스나 웜 등의 악성코드에 의한 네트워크 마비, 특정 서버를 목표로 하는 과부하에 의한 업무 방해 등의 위협이 표면화 되고 있다. 이러한 위협에 대응하기 위한 대책의 요구가 증가함에 따라서 일본정부는 다양한 정보보안 정책을 제정하거나 시행해 나가고 있다. 본 고에서는 최근 일본정부가 내놓은 정보보안 분야의 정책과 구체적인 실천 동향에 대해서 살펴보고자 한다.

## II. 정보보안의 필요성

일본은 고도 정보통신 네트워크사회 형성을 위한 정책의 일환으로, 국민의 편리성 향상과 행정운영의 간소화, 효율화 및 투명성을 높이기 위하여 전자정부를 구축해 나가고 있다. 이로 인해, 인터넷을 경유하여 24 시간 행정 업무를 받을 수 있게 되어 국민이나 기업의 편리성이 비약적으로 향상될 것으로 보고 있다. 반면, 네트워크를 통하여 교환되는 행정업무 상의 정보는 개인정보나 기업의 기밀정보, 나아가서는 국가 안전보장에 관한 것도 포함되어 있을 수 있으므로 정보자산의 안전성이 크게 요구되는 부분이다.

초고속 인터넷 환경의 발달과 전자정부의 구축과 같은 여러 요인들로 인해 인터넷 이용자의 수가 증가함에 따라, 다양한 악성코드가 빠르게 전파될 수 있는 환경이 갖추어지게 되었고 실제로 이로 인한 피해가 현실화되기 시작하였다. 일본의 정보처리추진기구보안센터(IPA/ISEC)에 신고된 바이러스의 발생 건수를 살펴보면, 신고 건수는 최근 2 년간 소폭 감소하였으나 Nimda,




(그림 1) 바이러스와 부정 접속 신고 건수 추이 - 정보처리추진기구보안센터, 2004 년 1 월

Klez, MS Blaster 등과 같은 네트워크형 바이러스나 웜의 출현으로 인한 피해의 규모나 그 여파는 보다 증가하는 추세에 있다. 악성코드와 더불어 일본 국내에서의 부정 접속, 개인정보의 무단 유출 등의 네트워크를 이용한 범죄도 지속적으로 증가하고 있다[1]. 이에 대응할 수 있는 기술적 지원과 사이버 수사의 경로가 요구되고 있다.

일본 국내에서 사이버 테러라고 공식으로 인정된 사건은 현재까지 발생되지 않고 있다. 일부 정부기관의 서버에 대한 부정침입과 관공서 및 신문사의 홈페이지가 공격 받은 사건이 간혹 발생하였으나, 국민 생활에 영향은 없었기 때문에 사이버 테러라고 규정하기는 힘들다. 일본정부가 가장 우려하고 있는 사항으로는 2001 년부터 시작된 우리나라의 일본에 대한 사이버 데모가 있다. 교과서 개정과 신사참배 등에 항의하는 목적으로 우리나라의 인터넷 이용자들이 일본의 정부기관 홈페이지에 대규모 접속을 시도하여 서비스를 방해하였다. 대부분의 행위는 사전에 예고된 경우가 많아서 목표가 된 서버에 대책을 마련하였음에도 불구하고 서비스 불능 상태가 되어 이러한 방법을 사용하는 공격의 대응에는 어려움이 많다는 것을 인식하고 있다. 나아가, 정부기관이 아닌 전자상거래나 금융기관 등에 동일한 공격이 행해질 경우 피해의 규모는 상당한 수준에 이를 수 있으므로 사이버 테러와 함께 이러한 문제점에 대해서도 정책적인 대응이 필요한 상황이다.

## III. 정보보안에 대한 대응

일본은, ‘e-Japan 전략’의 중점계획 중 하나로, ‘고도 정보통신 네트워크의 안전성 및 신뢰성의 확보’를 통해 보안 체계나 이른바 사이버 테러에 대한 대응 체제의 구축, 민간에 있어서 보안 수준의 향상 등의 사안들을 고려하고 있다. ‘e-Japan 전략 II’나 기타 세부 전략 등에서도 명칭은 조금씩 변경되어 왔으나, 법제 정비, 사업자와 이용자에 있어서 대책 실시의 촉진, 연구 개발의 추진, 인재 육성의 추진, 보안 대응 기구의 설립 등 정책을 다각도로 적용하려는 의도에는 변함이 없다.

### 1. 법제 정비

정보보안 확보를 위해서는 네트워크의 안전성을 위협한 행위를 금지하고 위반 가능성을 억제하기 위한 법제 정비가 우선시된다. 일본정부는 2000 년대에 들어서면서 정보보안과 관련된 구체적인 법률들을 제정하고 시행하기 시작하였다.

### 가. 부정 접속 행위의 금지 등에 관한 법률(2000 년 2 월 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 한다[2].

### 나. 전자 서명 및 인증 업무에 관한 법률(2001 년 4 월 시행)

전자 서명에 일반 문서상의 서명이나 날인과 동일한 법적 근거를 줌과 동시에, 인증 업무에 대한 인정 제도를 도입한 법률이다. 전자 서명에 관하여, 전자적 기록의 성립의 추정, 특정 인증 업무에 관한 인정 제도 및 그 밖에 필요한 사항을 정하고 있다. 전자 서명의 원활한 이용의 확보에 의한 정보의 전자적 방식으로의 유통 및 정보 처리의 촉진을 도모하고, 이를 통해 국민생활의 향상 및 국민 경제가 건전한 발전에 기여하는 것을 목적으로 한다[3].

### 다. 특정 전자 메일의 송신의 적정화 등에 관한 법률(2002 년 7 월 시행)

이용자의 동의를 얻지 않고 광고, 선전 또는 권유 등을 목적으로 한 전자 메일을 송신할 때에는 '미 승낙 광고※'라고 표시하여야 하며, 수신 거부자에 대해서는 송신을 금하는 법률이다. 다수의 이용자에 대해 동시에 대량의 전자 메일을 송신하는 등에 의한 전자 메일의 송수신상의 지장을 방지하기 위해, 전자 메일 송신의 적정화를 위한 조치 등을 규정하고, 전자 메일의 이용에 관한 양호한 환경의 정비를 도모하는 것을 목적으로 한다[4].

### 라. 개인정보의 보호에 관한 법률(2003 년 5 월 제정, 2005 년 4 월 시행 예정)

고도 정보통신 사회의 진전을 통해 개인정보의 유통, 축적 및 이용이 급속히 증가함에 따라, 개인정보의 적정한 취급에 대해 기본이 되는 사항을 규정하고 개인정보의 유용성을 고려하여 개인의 권리이익 보호를 포함하도록 유도하는 법률이다. 개인정보는 개인의 인격 존중의 이념 하에 신중히 취급되어야 하며, 개인정보를 다루는 자는 개인정보를 취급함에 있어서 다음의 원칙들을 지키도록 권고하고 있다[5].

- 이용 목적에 의한 제한: 개인정보는 그 이용 목적이 명확해짐과 동시에 해당 이용 목적의 달성에 필요한 범위 내에서 취급되어야 함
- 적정한 방법에 의한 취득 및 목적의 통지: 개인정보는 적법 또는 적정한 방법에 의해 취득된 것이어야 하며, 개인정보를 취득한 때에는 이용 목적을 통지 또는 공표하여야 함

- 내용의 정확성의 확보: 개인정보는 그 이용 목적의 달성에 필요한 범위 내에서 정확하고 최신의 내용으로 유지해야 함
- 안전 보호조치의 실시: 개인정보는 적절한 안전 보호조치를 강구한 뒤 취급되어야 함
- 제 3 자 제공의 제한: 본인의 동의 없이 개인 데이터를 제 3 자에게 제공하는 것을 금지함

정부는 2004 년 4 월, 2005 년에 있을 개인정보의 보호에 관한 법률의 완전 시행에 대해 개인정보를 취급하는 민간 사업자나 국가, 지방 자치제가 취해야 할 조치를 규정한 '개인정보의 보호에 관한 기본방침'을 결정하였다. 내부 관계자에 의한 정보 누출 대책을 민간 사업자에게 추구하고, 정부는 각 부처에 불만 상담 창구를 설치하며, 지방자치단체는 개인정보보호조례의 제정이나 재평가를 진행하도록 규정하였다.

기업에 대해서는 정보보호 방침의 명확화, 책임 체제의 확보, 종업원의 계몽 등 3 개를 중요한 항목으로서 지정했다. 먼저, 개인정보 보호에 관한 사고방식이나 개인정보 보호 방침의 책정 및 공표를 시행하도록 했다. 또한 정보 누출 등이 발생한 경우에는 가능한 한 사실관계를 공표하도록 규정하고 있다. 책임 체제에 관해서는 부정 액세스 방지 대책이나 개인정보 보호관리자의 설치, 내부 관계자의 정보 유출 방지 조치 등 책임 체제를 확보하기 위한 구조를 정비하도록 규정하고 있다. 개인정보의 취급을 외부 위탁한 경우에는 계약시에 상호 책임 체제를 명확히 하여 개인정보가 보호받도록 하고 있다. 종업원의 계몽에 관해서는 교육 연수 등을 통해 종업원의 정보 보호 의식을 높이도록 유도하고 있다.

개인정보의 보호에 관한 법률과 함께 발표되었던 '행정기관 등 개인정보 보호법'에서는 정부기관이 취해야 할 사항을 언급하고 있다. 총무성은 보호법과 관련된 지침을 책정하고 국민에게 정보를 제공하며, 기타 부처는 사업 분야의 실정에 따랐던 지침 등의 책정 및 재평가를 조속히 검토하여 작성된 지침을 통해 사업자 단체 등에게 정보 제공이나 조언 등을 행하도록 하고 있다. 그 중에서 의료, 금융, 정보통신 등의 분야에 대해서는 특별히 취급하도록 요구하고 있다[6].

또한, 법무성에서는 이른바 사이버 테러를 포함한 부정 접속, 자료 무단 변조 등과 같은 각종 하이테크 범죄에 대한 벌칙의 정비, 정보통신 네트워크에 관한 수사절차에 관하여 적절한 처벌을 확보하기 위한 법 정비를 2005 년까지 행하기 위해 외국의 법제 조사 및 하이테크 범죄에 관한 국내 사례 조사를 실시하여 대비하고 있다.

## 2. 사업자와 이용자에 있어서 대책 실시의 촉진

e-Japan 전략에서는 총무성과 경제산업성은 정보보안과 관련된 기관들과 함께 민간에의 정

보 제공 및 지도 조언 기능을 강화해 나가며, 정보보안에 관한 보급 계몽 활동을 행함과 동시에 고도의 정보보안 설비의 도입이나 정보보안 관련 서비스의 구입 등을 계획하는 민간기업 등에 대해 지원하도록 규정하고 있다. 또한, 경찰청은 민간에서의 상담 접수 업무의 충실 및 하이테크 범죄 대책을 위한 체제의 강화를 행하도록 하고 있다.

인터넷 보안을 확보하기 위해서는 네트워크 기반구조를 제공하고 운용중인 통신사업자에 대해 Δ 정보통신 네트워크 안전 및 신뢰성에 대한 가이드 라인 제시Δ 인터넷접속 서비스 안전・안심 마크 제도Δ 정보통신 투자 촉진 세제 지원 등의 적절한 보안 대책을 실시하는 것이 중요하다.

동 전략에서는 정보통신 네트워크에 있어서 안전성 및 신뢰성에 대한 기본적이면서 총괄적인 가이드 라인을 제시한다. 정보 시스템의 안전한 운용을 가능하게 하고, 운용에 관련되는 사람의 관리나 컴퓨터가 설치되어 있는 건물 등 물리적인 관리를 행하기 위한 보안 관리 대책, 정보 시스템의 신뢰성을 확보하기 위해서, 위협에의 대항 조치로서 보안 기능이나 품질을 확보하기 위한 보안 기술 대책, 네트워크상에 있어서의 클라이언트와 서버간이나 정보 시스템 사이를 오가는 데이터의 안전성을 확보하기 위한 안전한 데이터 처리 기술 등을 마련하려는 목적이다.

2002 년 6 월부터 보안 대책이나 사용자 대책 등으로 일정한 수준을 충족시키는 인터넷 접속 서비스 사업자에게 총무성의 조언을 받고 있는 인터넷접속 서비스 안전・안심 마크 추진 협의회(텔레콤 서비스 협회, 일본 인터넷 제공자 협회에서 구성)는 마크를 부여하고 있다. 이 '안전・안심 마크'는 일반 이용자가 서비스 제공자를 선택함에 있어, 사용자 대책이나 보안 대책 등이 일정 기준을 만족한다는 정보를 제공하는 것이다.

2003 년도에 일본정부는 기업의 사업 효율화나 고부가가치화 등을 촉진하기 위해 기업의 정보통신 네트워크 투자에 대해 세제 지원 조치를 실시하는 '정보통신 투자 촉진 세제'를 창설하였다. 이 세제는 일정한 정보통신 관련 설비 등을 취득했을 경우에, 취득가격의 50%의 특별상각 또는 10%의 세액공제를 선택할 수 있다. 그러나 문제는 '부정 접속, 바이러스 대책 소프트웨어'가 일정한 정보통신 관련 설비에 해당하는지 명확하게 규정되어 있지 않지만 기업의 시스템 신뢰성 향상 대책에 사용되고 있다는 것이다[7].

통신사업자뿐만 아니라 네트워크에 접속하고 있는 개별적인 이용자에게 있어서도 정보보안과 관련된 정보와 다양한 세제 혜택 등을 제공하는 등의 적절한 정보보안 대책을 실시하는 것이 중요하다.

일반 국민을 대상으로 정보보안에 대한 주지 계몽을 도모하기 위한 목적으로, 2003 년 3 월부터 총무성 홈페이지 내에 정보보안 홈페이지가 개설되었다. 이 홈페이지에는 인터넷과 정보보

안의 기초지식, 사고・피해의 사례, 보안 용어 등의 정보보안에 대한 지식과 이용방법에 따른 정보보안 대책을 강구하기 위한 기본 지식이 수록되어 있다.

네트워크 이용자에게 컴퓨터 바이러스 예방 대책이나 정보를 제공하기 위해서 1998 년 6 월부터 일본 데이터 통신 협회 및 멀티미디어 진흥 센터가 공동으로 바이러스 컨설팅 센터를 개설하여 바이러스의 기초지식이나 백신 소프트웨어 사이트로의 링크, 감염 사례를 소개하고 있다.

총무성은 인터넷에 접속하는 법인 또는 개인 사업자가 부정 접속 대책으로서 적절한 조치를 강구했을 경우에 지방세를 경감하는 '부정 접속 대책 촉진 세제'를 실시하고 있다. 대상 설비는 방화벽 한 종류로 한정하였고, 고정 자산세의 과세표준을 취득 가격의 5 분의 4 로 경감할 수 있도록 하였으며, 2002 년 4 월부터 2004 년 3 월까지 적용되었다[8]. 2004 년 4 월부터는 부정 접속 대책 촉진 세제를 대체하여 2 년간 새롭게 적용되는 '네트워크 보안 유지 세제'에서는 부정 접속이나 컴퓨터 바이러스 등으로부터 정보 시스템을 보호하려면 방화벽뿐만 아니라 침입 탐지 시스템이나 스팸 메일 제거 시스템과 같은 다양한 장비가 필요하다는 판단에 따라, 세제의 대상이 되는 장비를 보안관련 복합기로 확대하고 과세표준은 6 분의 5 로 소폭 변경되었다[9].

## 3. 연구 개발의 추진

부정 접속 기술, 바이러스나 웜 등의 악성코드의 위력, 암호 해독 기술 등은 끊임없이 진화되고 있고, 이에 대응하기 위해서는 부단의 연구 개발이 불가결하다. 산업계가 추진하기 어려운 연구나 비용이 큰 연구 등에 대해서는 국가가 직・간접적으로 연구 개발을 추진할 필요가 있다. 이에 따라, 암호 기술, 정보보안 평가 기술 등의 기반 기술의 개발과 국방・치안 관련 기술에 관하여는 지장이 없는 범위 내에서 정부의 기타 기관 또는 민간에도 공개한다는 방침을 가지고 있다. e-Japan 전략을 통해 정보보안과 관련된 기반 기술의 개발을 담당하는 기관으로는 총무성, 경제산업성, 방위청, 경찰청, 문부과학성 등이 있다.

총무성은 2004 년도 예산의 5 가지 중점 추진안 중에서 '일본발의 신 IT 사회의 구축'을 통

<표 1> 총무성의 정보보안 분야 연구 개발 예산(2003~2004 년) (단위: 억 엔)

| 연구 분야 | 2003 년 | 2004 년 |
|---|---|---|
| 네트워크 보안 기반 기술의 추진(2001 년부터) | 26.0 | 24.7 |
| 고도 네트워크 인증 기반 기술에 관한 연구 개발(2004 년부터) | - | 10.4 |
| 컴퓨터 바이러스 등에 관한 연구 기반의 구축(2003 년부터) | 1.8 | 1.8 |
| 타임 스탬프 플랫폼 기술의 연구 개발(2003 년부터) | 2.7 | 1.7 |
| 합계 | 30.5 | 38.1 |

해 정보보호 전략의 종합적 추진을 꾀하고 있다. 이에 신설된 '정보통신 보안 인재육성센터 개설 지원사업' 분야에 2 억 4 천 엔, 2003 년 30 억 5 천 엔이 배정되었던 '보안 기술기반의 형성' 분야에 38 억 1 천 엔을 책정하여 연구 개발에 투자하고 있다[10].

경제 산업성에서는, 컴퓨터 바이러스나 부정 접속 등에 의해 정보 처리 시스템이 받는 위협의 상황이나 그것에 대한 방어 조치에 관한 기술 개발을 추진해 오고 있으며, 2004 년 연구개발 예산으로 '정보보호 문제에 대한 대응' 분야에 24.8 억 엔의 예산을 배정하였다[11].

<표 2> 경제산업성의 정보보안 분야 연구 개발 예산(2001~2004 년) (단위: 억 엔)

| 연구 분야 | | 2001 년 | 2002 년 | 2003 년 | 2004 년 |
|---|---|---|---|---|---|
| 전자정부의 보안기술 개발 | | 14.1 | 10.0 | 5.0 | 6.0 |
| 정보보안 대책추진 | 정보보안 평가·인증기반 정비사업 | 5.5 | 2.1 | 2.3 | - |
| | 정보보안 대책연구 개발 평가사업 | | 3.5 | 3.5 | 5.0 |
| EC 기반의 상호운용성에 관한 조사연구 | | 1.0 | 2.7 | 2.4 | 1.8 |
| 정보보안 매니지먼트 이용 촉진사업 | | - | - | 0.8 | 1.5 |
| 전자서명・인증제도 이용 촉진사업 | | 1.0 | 0.9 | 0.8 | 0.8 |
| 부정접속행위 등 대책 업무 | | - | 1.5 | 6.5 | 6.7 |
| 전력 분야의 사이버 테러 대책 촉진사업 | | - | - | - | 3.0 |
| 합계 | | 21.6 | 20.7 | 21.3 | 24.8 |

방위청에서는 사이버 공격에 대한 대처 수법의 실증적 연구 및 컴퓨터 시스템 등의 안전성 확립을 위한 운용 지침에 관한 조사 연구를 추진 중이다. 사이버 공격의 위협에 정확하게 대응하기 위해서는 정보보안의 기반을 정비함과 동시에 사이버 공격에 대한 방어・대처 능력이나 체제를 확보하는 것이 필요하다. 이 때문에 정보보안 방침의 개선, 사이버 공격에 대한 대처 수법의 연구, 보안 시스템의 운용 평가 등의 정책을 진행하고 있다. 경찰청은 네트워크상의 부정 접속 자동 검지에 관한 조사 연구, 고도의 보전 기술에 대응하는 요소 기술의 연구 등을 실시하고 있다.

## 4. 인재 육성의 추진

정보보안의 확보에는 보안 관리 기술자의 양성이 불가결하다. 보안 기술자의 육성은 긴급한 사안이지만, 교육을 위한 기기, 교재 개발 등 초기 비용이 커서 육성이 진행되기 어려움이 많기 때문에 정책적 차원의 접근이 필요하다. 일본은 보안관리 기술자가 절대적으로 부족한 상황임을 인지하고, e-Japan 전략을 통해 각 분야의 요구에 입각한 인재 육성 프로그램을 지원하고 있다. 정보통신 분야에서는 총무성, 경제산업성, 방위청, 문부과학성 등을 중심으로 인재 육성을 추진

중에 있다.

총무성은 다양한 자격 제도를 통한 인재 육성을 꾀하기 위해, 2001 년 7 월 전기통신사업법에 근거한 '전기통신 주임기술자 시험'에 정보 보안에 관한 과목을 추가하였다. 또한, 통신 사업자 단체가 정보 보안 분야의 인재 육성을 추진하기 위한 협의회를 설립하고, 전기통신 사업자 협회 등 7 단체에 의하여 2001 년 4 월에 정보보안에 관한 민간 자격으로서 '네트워크 정보보안 매니저(NISM)' 제도를 창설하였다.

NISM 은 해커, 부정 접속, 컴퓨터 바이러스 등으로부터 정보통신 네트워크와 그 이용자를 방어하기 위한 전문 지식을 갖는 기술자를 육성하고, 정보통신 서비스를 제공한 사업자에게 배치하기 위한 목적으로 창설되었다. 또한, 총무성은 '정보통신 네트워크 안전・신뢰성 기준'을 개정하고, 정보보안에 관한 자격의 보유자 등 일정 이상의 지식이나 기능을 갖는 자의 배치를 단계적으로 실시하도록 규정하였다. NISM 자격은 업계 단체의 자격에 의한 민간 자격이나 총무성의 고시 개정에 합쳐서 창설된 공공성을 지니고 있다[12].

경제산업성은 2001 년도에 '정보보안 관리자 시험'을 창설하고, 정보보안 평가 기술자 및 정보보안 설계 기술자의 육성 사업을 추진하고 있다. 향후 보안 분야 인재 육성에 관해 보안 기술의 지식을 갖춘 인재 육성에서 머무르지 않고, 보안의 전체적인 향상을 꾀할 수 있도록 경영이나 법률적인 지식을 습득하도록 유도하고 있다. 또한, 경찰청과 방위청에서는 미국 등의 정부 기관이나 정보 보안 관련 단체 등에 인력을 파견하여 연수 및 정보교환 등을 실시하고 있다.

## 5. 보안 대응 기구의 정비

e-Japan 전략에서는 사이버 테러 대책의 강화를 위해 사이버 테러에 관계된 정보의 집약, 전달, 축적 및 관민으로의 공유 등을 행하기 위한 조직의 구축 또는 기능 강화를 언급하고 있다. 이를 위해 기관 뿐만 아니라 민간 단체 차원에서의 보안 대응 기구의 결성도 이루어지고 있으며, 관계 기관들간의 연계를 강화하기 위해 협의회와 같은 자리를 통해 공조해 나가고 있다.

### 가. 정보보안 대책 추진실

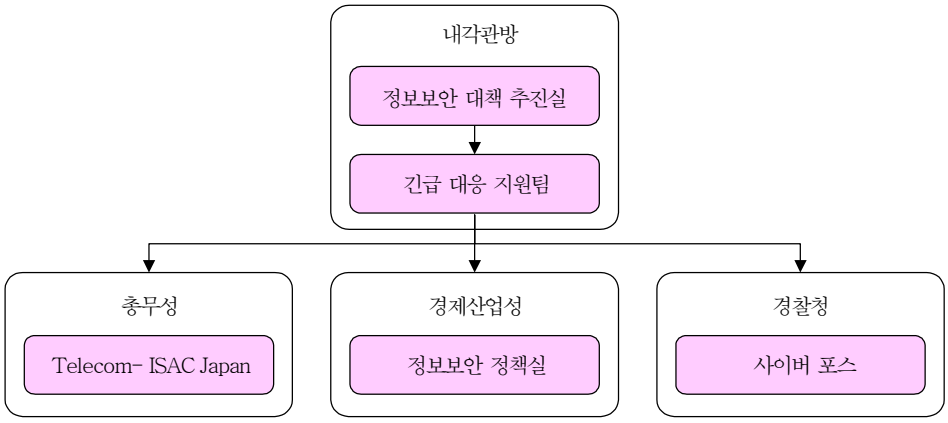
2000 년 내각관방 산하에 설립된 정보보안 대책 추진실은 관계 각 부처와의 연휴・협력과 동시에 관민의 정보보안 전문가로 구성된 비상근 팀의 조언을 얻으면서, 전자 정부의 정보보안 확보나 중요한 기반시설에 대한 사이버 테러 대책 등 관민에 있어서 정보보안 확보를 위한 정책 추진에 몰두하고 있다. 또한 고도 정보통신 네트워크 사회 추진 전략 본부의 하에 설치되어 있는 정보보안 대책추진 회의 및 정보보안 전문 조사회의 사무국을 담당하고, 각 부처와의 종합

조정 등을 행하고 있다[13].

정보보안 대책 추진실에서는 '해커 대책 등의 기반 정비에 관계된 행동 계획'을 기초로 주로 두 가지의 정책을 민간 전문가, 기업, 각 정부 부서 등의 협력을 통해 진행해 왔다. 그 중 하나는 전자 정부 및 자치단체의 보안 확보에 있고, 또 다른 하나는 사이버 테러로부터 금융, 전력, 철도 등 중요한 기반시설을 보호하는 대책이다. 최근 조사 및 연구 활동으로 보안 강화 소프트웨어의 조사와 오픈 소스 소프트웨어의 평가 연구도 중요한 대상이 되고 있다.

### 나. 긴급 대응 지원 팀

2002 년 3 월의 정보보안 대책 추진회의에서의 결정사항으로, 전자 정부나 민간에 중요한 기반시설을 대상으로 하는 사이버 테러 등에의 대책 입안에 필요한 조사・조언 등을 행하는 기구의 설립을 결정하였다. 이에 따라 2002 년 4 월 내각관방 정보보안 대책 추진실에 '긴급 대응 지원팀(NIRT, National Incident Response Team)'이 설치되었다. 사이버 공격 등에 의한 전자 정부나 민간의 중요한 정보통신 사업자 등의 정보 시스템에 관계된 장애의 발생에 대해 정부차원의 위기 관리 대응이 필요한 사안을 활동 대상으로 삼고 있다. 이를 위해, Δ 사안의 정확한 파악 Δ 피해 확대 방지, 복구, 재발 방지하기 위한 기술적 대응책의 검토 Δ 대책의 실시에 관계된 지원 등의 활동을 담당한다.




(그림 2) 각 성청의 정보보안 대응 기구

### 다. Telecom-ISAC Japan

'Telecom-ISAC Japan'은 정보통신 사업자들이 제공중인 네트워크와 같은 기반시설의 보호를 위해 전기통신사업자협회, 일본 인터넷 제공자 협회, 텔레콤서비스협회, 전기통신 사업자 등

이 2002 년 7 월에 설립한 조직이다. 사업자들이 제공 중인 통신 서비스의 보안 수준을 평가하고, 다른 중요한 기반시설에 대한 정보보안 상의 영향이 예상되는 보안 침해 사안에 관한 대처 및 예방조치를 취하는 것을 상호 연계를 통해 수행하려는 목적을 지니고 있다.

또한, Δ 인터넷 서비스 제공자를 중심으로 하는 네트워크의 각 거점에 보안 정보를 수집하기 위한 기기 배치 Δ 집중 센터에 보안 정보를 신속하게 수집・분석 Δ 각 거점에 있어서 사이버 테러에 의한 오염 상황・피해 상황을 실시간으로 파악 Δ 상호 정보의 공유를 할 수 있는 연구 개발의 기반 정비 등의 역할을 담당하고 있다.

### 라. 사이버 포스

경찰의 수사는 본래 사건이 일어나고 나서 수사를 시작하는 사후 수사의 성격이 강하지만, 사이버 테러는 사회에 대한 영향이 크기 때문에 사전에 전조를 파악해 미리 예방하는 것이 요구된다. 따라서, 경찰청은 2001 년 4 월에, 시스템의 취약성의 검사나 사이버 공격에의 대처 기술의 연구를 담당할 기관으로 사이버 포스(Cyber Force)를 설립하였다. 경찰청의 정보통신 기술자로부터 선발된 60 명이 도쿄 내의 민간 빌딩에 있는 '사이버 포스 센터' 등 전국 57 개소의 거점으로부터 경찰 네트워크에의 해킹 행위를 24 시간 체제로 감시하며, 정보통신이나 은행・증권거래소 등 금융 관계, 철도・항공, 전력・가스 등의 사회의 중요 기반시설에 대해서도 방호를 수행하고 있다. 네트워크를 사용한 범죄에 대한 각급 경찰의 수사를 기술 측면에서 지원하는 것도 중요한 임무이다.

사이버 포스는 사이버 공격 또는 그 징조가 파악되면 대책 요원이 현장에 출동하고 피해 확대의 방지, 범인의 추적 등을 행하며, 광범위하게 수집된 정보로부터 보안에 관한 정보를 제공하고 있다. 또한, 공격 수법에 관한 연구, 사이버 테러의 대책의 연구・개발 등도 수행하고, 향후 점점 고도화한 공격 수법에의 대응책을 준비하고 있다.

## IV. 결 론

9・11 테러 이후 미국이 물리적 테러뿐만 아니라 생화학 테러나 사이버 테러에도 대처하기 위한 여러 정책을 발표함에 따라, 일본 정부도 자국에 대한 사이버 테러에 대해서 국가적인 수준에서 대책을 마련하기 시작하였다. 또한, 앞으로 전자 정부가 확대 적용된다면 그 시스템이 피해를 받을 가능성도 있기 때문에 전체적인 정보보안 의식을 고취하고자 다양한 정책을 준비하거나 시행하고 있다. 그러나 일본의 정보보안 의식이나 정보보안 정책의 수준은 인터넷 대중화 초

기의 정보기술 분야의 발전 추이를 따라가지 못했던 우리나라의 전철을 따르고 있다. 근래 발표된 법률에서는 표현의 모호함으로 인해 해석의 융통성에 따라서 적용 범위가 크게 달라질 수 있으며, 이러한 법률들의 강제성의 부족과 유도 요인의 빈약함으로 인해 실효성에 의문이 제기되고 있다.

개인정보 보호법 등 일부 법률에서는 정보 보안에 대한 방침을 제정한 의식은 확실하게 나타나고 있지만, 실제로 실행해 나가야 하는지에 대해 명확하게 기술되어 있지 않다는 것이 약점으로 나타난다. 또한, 총무성의 투자 촉진 세제들을 살펴보면 여타 분야의 감세 정책과는 달리 정보보안 제품을 구비할 경우 큰 이익이 발생할 것이라는 매력적인 요소는 없다. 정보통신 업계에서도 이 세제를 이용한 정보보안 제품의 적극적인 프로모션은 행해지지 않고 있다는 점에서도 대폭적인 세제 감면 조치를 취해야 할 필요가 있다고 생각된다.

한편으로, 각 전략의 구체적 추진을 위해서나 정보의 공유와 긴급 대처를 위해서는 여러 기관의 영역을 초월한 협조가 필수적이나 아직 정부 기관과 민간이 공동으로 대응한 사례는 드물다는 점에서 전환점을 제공할 대책이 요구된다. 보안 대책을 세우고 관리하기 위해서는 고도의 전문성이 필요하며 동시에 운용 부담이 크므로 지방 자치 단체나 소규모 민간 업체의 경우에 재정적인 부담이나 인재의 부족이 우선 해결해야 할 과제이다. 이를 위해 국가적 차원에서 연계체제의 구축을 통해 공동의 자원을 관리하거나 아웃소싱을 조율하여야 할 것이다.

인재의 육성의 측면에서도 서버, 네트워크, 시스템 통합 등 다양한 분야에서 요구되고 있는 보안 기술자를 위한 통일된 보안 방침이 확실히 세워지지 않았다는 문제를 지니고 있다. 여러 영역을 포괄하는 전체적인 발상으로 관리자와 사용자 모두의 입장에 서서 생각할 수 있는 기술자를 육성하여야 한다. 기업에 있어서는 사원이 정보보안과 관련된 기술을 습득하는 것을 무엇보다도 중요하게 여겨야 한다. 사원이 교육을 받는 것으로 끝을 맺는 것이 아니라 교육을 받았던 것에 대해 현재의 기술과 격차가 발생하지 않았는가에 대해 지속적으로 확인하는 것이 중요하다. 이는 상당한 비용이 소요되기 때문에 기업의 경영 상황이 나쁜 상황에서 교육을 실시한 것은 의문시 될 수 있다. 그러나 인재를 육성을 하지 않는다면 기업의 존속 그 자체가 위험하다는 인식을 가지도록 유도하거나 정부차원의 교육 지원정책이 마련될 필요가 있다.

## <참 고 문 헌>

[1] 정보처리추진기구 보안센터, 컴퓨터 바이러스・부정 액세스의 신고 상황에 관하여, 2004 년 1 월
[2] 총무성, 부정 접속 행위의 금지 등에 관한 법률, 2000 년 2 월
[3] 총무성, 전자 서명 및 인증 업무에 관한 법률, 2001 년 4 월

[4] 총무성, 특정 전자 메일의 송신의 적정화 등에 관한 법률, 2002 년 4 월
[5] 수상관저, 개인정보의 보호에 관한 법률, 2003 년 5 월
[6] 총무성, 행정기관 등 개인정보 보호법, 2003 년 5 월
[7] 총무성, 정보통신 투자 촉진 세제, 2003 년 1 월
[8] 총무성, 부정 액세스 대책 촉진 세제, 2002 년 4 월
[9] 총무성, 네트워크 보안 유지 세제의 안내, 2004 년 3 월
[10] 총무성, 2004 년 '정보보안 관련 예산', 2004 년 1 월
[11] 경제산업성, 2004 년 '정보보안 정부예산안 경제산업성분 개요' 등, 2003 년 12 월
[12] NISM 추진협회, NISM 자격의 2003 년 7 월~9 월 신규 수강자의 모집 개시 및 갱신 제도의 신설에 관하여, 2003 년 6 월
[13] 내각총리대신, 정보보안 대책 추진실의 설치에 관한 규칙, 2000 년 2 월