情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

일본 고도정보통신네트워크 안전 · 신뢰성 확보 정책

김 현 수*

요 약

일본은 2001년 확정한 「e-Japan 중점계획」에서 정한 220개의 시책 중 1차년도로 예정된 103개의 시책을 모두 이행하였다. 그리고 2002년 6월 추진성과를 재검토하여 새로이 「e-Japan 중점계획 2002」를 발표하였다. 여기서는 일본의 정보보안 추진전략의 전체상을 살펴보기 위한 방안으로 「e-Japan 중점계획 2002」 중 '고도정보통신 네트워크의 안전성 및 신뢰성 확보방안'을 소개한다.

Ⅰ. 서 론

'일본을 5년이내에 세계 최첨단의 IT국가로 만든다'라고 하는 목표가 2001년 1월 「e-Japan」전략으로 거론된 후, 일본에서는 고도정보통신 네트워크 사회 추진 전략본부(이하 'IT 전략본부')를 중심으로 정부와 민간의 노력이 계속되고 있다. 구체적으로는 2001년 3월 「e-Japan 중점계획」, 2001년 6월 「e-Japan 프로그램」, 2001년 11월 「e-Japan 중점계획, e-Japan 프로그램의 가속」 등 정부가 취할 여러 가지 시책을 정하는 각종 계획을 수립해 왔고, 이와 동시에 「e-Japan 중점계획」에서 정한 220개의 구체적인 시책에 대하여, 1차년도로 예정되었던 103개의 시책을 모두 조치하는 등 이들 계획을 착실하게 실시해 나가고 있다.

이러한 상황에서 2002년 6월 18일 IT전략본부에서는 「e-Japan 중점계획 2002」를 발표하였다. 이는 '고도정보통신 네트워크 사회 형성 기본법'(이하, IT 기본법) 제35조를 근거로 작성된 「e-Japan 중점계획」을 재검토하고, 현재까지의 추진성과에 대한 평가를 통하여, 목표달성을 재확인하고 고도정보통신 네트워크 사회의 형성을 위하여 정부가 신속하고 중점적으로 추진해야 하는 내용을 담은 것이다.

이상과 같이 「e-Japan 중점계획」은 일본의 정보화의 핵심전략을 담은 것이며, 이를 통하여 IT 강국의 달성이라는 목표를 구체적으로 추진해 나가고 있는 것이라고 할 수 있다.

이러한 점을 감안한다면, 「e-Japan 중점계획」에 대한 분석은 일본의 정보화 정책을 종합적으로 판단할 수 있는 자료가 된다고 할 수 있을 것이다.

이하에서는 지난 6월 발표된 「e-Japan 중점계획 2002」에서 채택하고 있는 5가지의 중점정책 중 하나인 '고도정보통신 네트워크의 안전성 및 신뢰성 확보방안'을 살펴봄으로써, 일본의 정보보호정책 전반에 대한 이해를 도모함과 동시에 각각의 시책에 대한 구체적 내용을 분석함으로써 향후 국내 정보보호정책 수립을 위한 자료로 활용되기를 기대한다.

본 논문의 구성은 다음과 같다. 제2장에서는 일본의 정보보안 추진체계 및 「e-Japan 중점계획 2002」의 개요에 대하여 살펴볼 것이다. 그리고 제3장에서는 「e-Japan 중점계획」의 실시 후 이루어진 최근의 추진성과에 대하여 살펴보고, 제4장에서는 「e-Japan 중점계획 2002」에서 다루고 있는 정보보호정책을 개별적으로 고찰한 후, 제5장에서 결론을 내리고자 한다.

Ⅱ. 일본의 정보보호 추진체제[2]

일본은 1994년 총리대신을 본부장으로 하는 고도정보통신사회추진본부를 설치하고, 하이테크 범죄 대책 · 보안 대책 · 프라이버시 대책에 대한 '고도 정보통신사회 추진을 위한 기본 방침(1997년2월 결정, 1998년 11월 개정)'을 발표하였다.

1999년 9월에는 이제까지의 각 성청의 개별적

* 국가보안기술연구소(jura@etri.re.kr)

정보보호 대책에 대한 종합적인 검토와 이에 대한 대책 추진의 필요성으로 내각에 '정보보안 관계성청 국장 등 회의(이후, '정보보안대책 추진회의'로 대체)'를 설치하고, 2000년 1월, 정부 기관의 안전 대책의 추진, 민간 주요 기반시설의 안전 대책의 추진, 국제적인 연대 등을 주요내용으로 하는 '해커 대책 등의 기반 정비에 관한 행동계획'을 마련하였다.

본 행동계획에서는 정부부문에서 보안에 관한 신뢰성 높은 정부 시스템의 구축을 요구하고, 방위청, 경찰청 및 각 성청에 대하여 감시·긴급 대처 체제의 정비·강화를 요구하였다. 또한 2000년 7월에 각 성청용의 '정보보안정책에 관한 가이드라인'을 발표하였다. 가이드라인에서는 정부 보안 대책의 기본적인 가치관, 보안정책 책정의 순서를 나타낸 가이드라인 및 각 부처의 정보시스템에 있어서의 필수 대책을 세워 정리한 보안정책의 예 등이 부록으로 구성되어 있다.

민간부문에 있어서는 민간기업이 정보보안대책을 실시하는 경우, 참고가 되는 사항을 수시로 통합하여 공개하기로 하고, 정보통신 네트워크를 통한 사건이 발생한 경우에 국민 생활에 중대한 영향을 줄 가능성이 생각되는 분야를 2000년 4월까지 중요 분야로 선정하여, 2000년 12월의 사이버테러 대책에 관한 특별행동계획으로 통합했다.

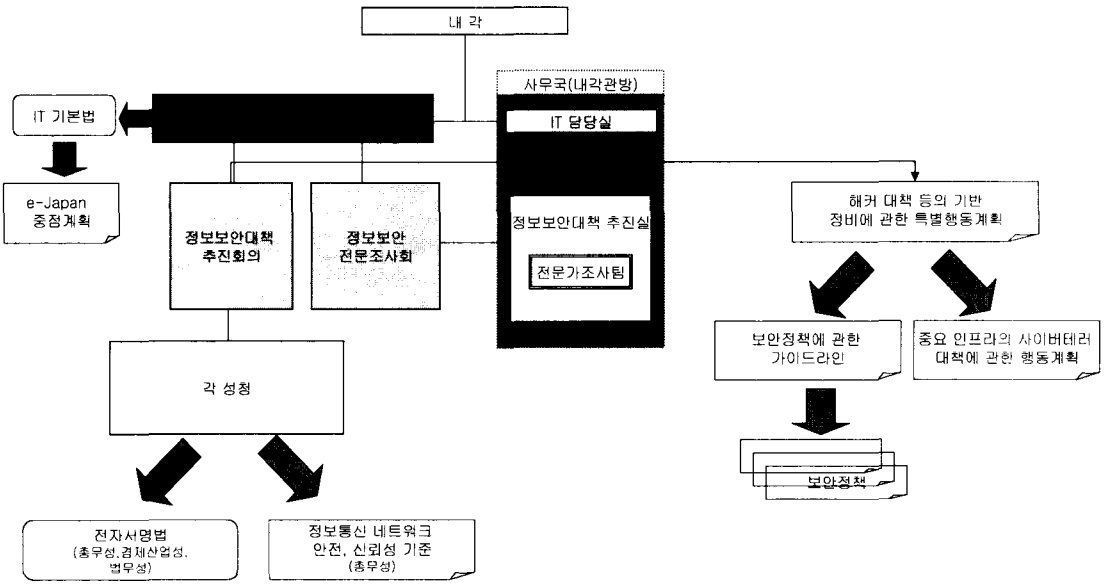
사이버테러 대책에 관한 특별행동계획에서는 정보통신, 금융, 항공, 철도, 전력, 가스, 정부·행정서비스를 주요기반시설로 정하고, 정부와 민간에 있어서의 보안수준의 향상, 정부와 민간의 연락·연대체제의 확립·강화, 정부와 민간의 연대에 의한 사이버 공격의 탐지와 긴급대처, 정보보안기반의 구축 등을 그 내용으로 하고 있다.

한편 일본의 정보보호 관련 조직으로는 정부차원에서 앞서 말한 IT 전략본부하에 전 성청의 국장급 회의(정보보안대책 추진회의)와 학자, 보안 전문가, 주요 민간 기반시설의 대표자 등 민간 전문가에 의해 구성된 정보보안조사회가 설치되어 있으며, 내각관방에 정보보안 대책추진실과 각 성청의 보안 대책에 관한 기술적인 조사, 조언 등을 하는 전문조사팀이 설치·운영되고 있다.

한편 「e-Japan 중점계획 2002」에서는 일본의 정보화와 더불어 앞서 설명한 일본의 정보보호정책을 통합하여 그 내용으로 다루고 있다.

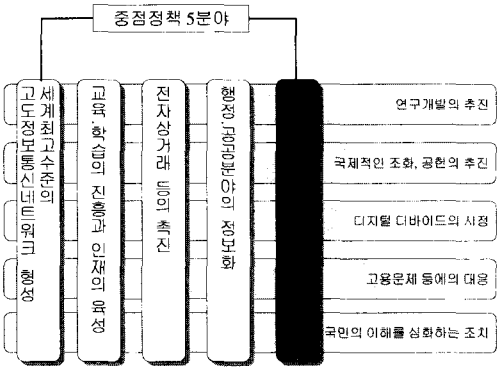
우선 그 구성을 살펴보면 다음과 같다.

「e-Japan 중점계획 2002」에서는 정보통신분야에서 민간이 주도적인 역할을 담당하고, 정부는 자유롭고 공정한 경쟁촉진, 규제의 검토 및 재규정 등 민간부문에서 활력을 충분히 발휘할 수 있도록 하기 위한 환경정비를 내용으로 하는 '정부와 민간의 역할분담'을 기본방침으로 정해놓고 추진하고 있다. 또한 중점시책으로 (1) 세계 최고수준의 고도정보통신네



〔그림 1〕 일본의 정보보호 대책 추진 체제

트워크 형성 (2) 교육·학습의 진흥과 인재의 육성 (3) 전자상거래 등의 촉진 (4) 행정·공공분야의 정보화 그리고 마지막으로 본 논문에서 다루려고 하는 (5) 고도정보통신 네트워크의 안전성과 신뢰성의 확보를 5가지 중점시책으로 선정하였다. 그리고 이들 중점시책의 효율적인 추진을 위하여 횡단적인 접근법으로 5가지 과제를 수행하는 것으로 하였다. (1) 연구개발의 추진 (2) 국제적인 조화·공헌의 추진 (3) 디지털 디바이드의 시정 (4) 고용문제에의 대응 (5) 국민의 이해를 심화하는 조치가 그것이다. 그림 2는 「e-Japan 중점계획 2002」의 구성을 도식화한 것이다.



〔그림 2〕 e-Japan 중점계획 2002의 구성

Ⅲ. e-Japan 중점계획의 추진 성과[3]

앞서 살펴본 것 처럼 일본은 2001년 3월의 「e-Japan 중점계획」에서 언급되었던 여러 가지 시책들을 착실하게 실시하였다. 특히, 주요기반시설의 사이버 테러 대책과 관련되는 정부와 민간의 연락·제휴 체제의 구축, 정부의 긴급 대응 지원팀의 창설 등, 정보보호 사안에 대비한 기본적인 체제를 정비했다.

먼저 전자 정부의 실현에 대응하여 정부부내에서 정부가 취할 조치에 대해서, 「전자 정부의 정보 보안 확보를 위한 액션 플랜」으로서 통합(2001년 10월 10일, 정보보안대책 추진회의 결정)하였고, 긴급대응지원팀(NIRT)을 창설해, 이에 대한 운영 매뉴얼 등을 정비(내각 관방, 2002년 4월 1일)하였다.

그리고 경제산업성 주도로 정보기기 등의 정보 보안 국제 규격(ISO/IEC15408)에 근거한 평가·인증 사업을 개시하였으며, 2002년 2월부터 독립 행정법인인 제품평가기술 기반기구에서 민간 평가기관의 인정 사업을 개시하였다.

사이버테러 대책과 관련해서는 내각관방과 관계부성에 대하여 정보통신, 금융, 항공, 철도, 전력, 가스 등 주요기반시설에 있어서의 연락·제휴 체제를 구축을 위하여 2001년 10월 2일, 정보보안 전문조사회에서 「사이버 테러 대책과 관련된 관민의 제휴·연락 체제」에 관한 대응책을 발표하였다.

또한 경찰청에서는 소위 사이버포스라는 기동기술부대를 정비하였으며, 「사이버 테러 대책 기술실」을 설치하였다(2001년 4월 1일).

그리고 정부부문을 제외한 민간부문에의 정보보안 대책 및 보급계발과 관련하여서, 「컴퓨터·바이러스 감시 장치」의 도입을 실시하는 민간 사업자에 대한 세제상의 우대조치를 실시하였다(총무성, 2001년 8월 13일 고시 개정).

한편 법무성에서는 지불용 카드 위조 등의 범죄에 관한 벌칙을 정비(2001년 6월 26일 「형법의 일부를 개정하는 법률」 성립, 동년 7월 24일 시행)하였으며, 휴대전화 등을 이용한 인터넷 이용 급증에 대처하기 위한 안전성·신뢰성 향상책, 스팸 메일에의 기술적 대책 등에 대해서 기준을 총무성에서 책정(2002년 3월 7일 「정보통신 네트워크의 안전성·신뢰성 기준」 개정)하였다.

그리고 정보 보안 관리에 관한 국제 규격(ISO/IEC17799)을 국내 규격화(경제 산업성, JIS X 5080을 2002년 2월 20일 공시)하여 관련 제도와 기반의 정비를 위한 노력을 하였다.

한편 개인보보호를 위하여 내각관방에서는 개인정보의 보호에 관한 법률안을 제출(2001년 3월 27일)하였으며, 행정 기관이 보유하는 개인정보의 보호에 관한 법률안, 독립 행정법인 등이 보유하는 개인정보의 보호에 관한 법률안, 정보 공개·개인정보 보호 심사회 설치법안, 행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시행에 수반하는 관계법률의 정비 등에 관한 법률안이 총무성에서 제출(2002년 3월 15일)되었다.

인재육성과 관련된 시책으로는 전기통신 주임기술자 시험에 정보보안에 관한 시험 과목이 추가(총무성, 2001년 4월)되었으며, 정보처리 기술자 시험에 정보보안 관리자 시험을 도입(경제산업성, 2001년 10월)하였다. 그리고 방위청에서는 미국 CERT/CC에 전문 기술 요원의 파견(방위청, 2001년 3월-9월)하여 관련 인재 육성에 노력하고 있다.

국제교류를 위한 노력으로는 제2회 G8하이테크 범죄 대책 관민 합동 고위급 회합을 개최(경찰청, 총무성, 외무성, 법무성 및 경제산업성, 2001년 5월 22일-24일, 도쿄)하였으며, 아시아·태평양 하이테크 범죄 대책 담당 실무자 회의를 개최(경찰청, 2002년 2월26일-28일, 도쿄)하였고, 아시아 태평양 지역의 CSIRT(Computer Security Incident Response Team)에 의한 국제회의를 개최(경제산업성 및 방위청, 2002년 3월 24일-26일, 도쿄)하였다.

Ⅳ. 추진 예정된 시책의 구체적 내용

「e-Japan 중점계획 2002」에서는 정보보안정책과 관련하여 1. 정부의 정보보안 확보, 2. 주요기반기설의 사이버테러 대책, 3. 민간부문에서의 정보보안대책 및 보급·계몽, 4. 정보보안 관련 제도·기반의 정비, 5. 개인정보의 보호, 6. 정보보안 관련 연구개발, 7. 정보보안 관련 인재육성으로 나누어 각각의 시책을 추진하고 있다. 이하에서는 각각의 주제에 대하여 향후 일본이 추진하고자 하는 것으로 「e-Japan 중점계획 2002」을 중심으로 살펴본다.

1. 정부내의의 정보보안 확보

정부내의 정보보안확보를 위하여서 일본정부는 각 부성에서 정보보안정책의 계속적인 평가·재검토를 실시해, 그 수준을 한층 향상시키는 것과 동시에 정부의 정보보안 확보를 위한 체제를 정비하려 하고 있다. 또한 정보보안 수준이 높은 제품 등의 이용, 중요 시스템의 백업, 모의공격을 포함한 정보보안 평가의 실시 등 국민에게 신뢰받을 수 있는 체계를 구축하려 하고 있다.

(1) 정보보안정책의 실효성의 확보(내각 관방, 전부성)

2002년중에 내각 관방에서 각 부성의 정보보안정책에 관한 재평가를 실시하여 「정보보안 정책에 관한 가이드라인」(2000년 7월, 정보보안대책 추진회의)의 개정 및 실시 방법에 대한 모범적인 예시를 제시하는 것과, 이에 따른 정보보안 정책의 재검토를 실시한다. 또한 각 부성의 정보보안정책의 실효성을 확보하기 위해, 정책 운용을 철저히 하고, 동시에 정책에 근거하여 안전한 네트워크 설계, 감시·방호대책의 강화, 백업, 외부감사, 훈련의 실시 등 정보보안 확보를 위해서 필요한 조치를 실시해 전자 정부에 대한 적절한 보안 수준을 확보한다.

(2) 전자정부 정보 보안 확보를 위한 체제 정비 (내각 관방)

2003년도까지 훈련 실시 등을 통하여 정부 긴급대응지원팀(NIRT)의 긴급시 대응 능력을 향상시키고, 평시에 있어서의 정보수집·분석능력을 강화하는 한편 해외 관계기관과의 제휴 추진 등을 통하여 긴급대응체제를 강화한다.

그리고 2002년중에 내각 관방을 중심으로 실효성 있는 24시간 감시 체제에 대해서 검토 및 실증 실험을 실시한다.

(3) 지방공공단체 정보보안 확보 지원(총무성)

2002년중에 긴급대응체제의 정비에 대한 지원이나 지방 재정 조치의 실시 등 지방공공단체의 정보보안을 지원한다.

2. 주요기반시설 사이버테러 대책

「주요기반시설 사이버테러 대책 특별 행동 계획」(2000년 12월, 정보보안대책 추진회의결정)을 근거로 하여 주요기반시설의 기간을 이루는 정보시스템에 대해서, 위험평가, 정보보안정책의 책정 및 이에 근거한 정보보안대책을 추진하면서 정부의 긴급 대처 능력을 향상시킨다.

(1) 특별행동계획 강화(내각 관방 및 관계부성)

2002년중에 민간 주요기반시설 사업자 등의 사이버 테러 대책에 관한 노력을 한층 촉진하기 위해, 각 사업자마다 정보보안 대책 상황의 파악이나 실효성 확보 등에 대해서, 구체적 시책을 수립하게 한다.

(2) 내각 관방에서의 긴급 대처 체제 정비(내각 관방)

2002년중에 사이버테러 대응 데이타베이스 운용의 개시, 긴급대응지원팀(NIRT)의 사이버테러에의 대응 능력 향상을 위한 연수의 실시 등, 내각 관방에 서의 긴급 대처 체제를 강화한다[4].

(3) 경찰의 긴급 대처 체제 정비(경찰청)[5]

2003년도까지 사이버테러 발생시의 피해를 최소

한으로 억제하기 위한 기동적 기술 부대(사이버 포스)의 대응 능력의 강화, 사이버테러와 관련되는 전자적 공격 수법의 수집·분석 능력의 강화 등 사이버 테러에 대한 긴급 대처 체제를 강화하는 것과 동시에, 2002년중에 주요기반시설 사업자 등에 대해 기술 정보의 제공, 강습회의 개최, 요청에 근거한 취약성 시험의 실시협력이나 긴급 연락 수단의 제공 등 사이버 테러 대책과 관련되는 지원을 실시한다.

또한 2003년도까지 테러 조직 등에 관한 정보 수집 체제의 정비, 경찰과 주요기반시설 관리자와의 제휴 강화, 요원의 기술의 향상을 도모한다.

(4) 방위청의 긴급 대처 체제 등 정비(방위청)

2003년도까지 방위청·자위대가 보유하는 정보시스템에 대해서, 정보보안을 확보하면서 운용하기 위한 운용 가이드라인의 책정 등을 실시한다. 그리고 정보의 중요도에 근거하여 안전한 네트워크를 마련해 이들의 일원적인 감시·통제를 실시하는 조직을 신설함과 동시에, 정보 시스템에 대한 상시감시, 시스템 감사, 긴급사태 대처 등의 각종 기능을 가진 조직(부대)을 구축한다.

3. 민간부문의 정보 보안 대책 및 보급·계몽

정보 보안 대책을 추진하기 위한 세제, 융자 등의 지원을 실시해, 민간 부문의 정보보안 수준을 한층 향상시키면서, 정보 보안 대책과 관련된 상담 업무나 정보교환·발신에 대해서 기능을 충실히 수행한다.

(1) 정보 보안 의식의 향상(경찰청)

2004년도까지 하이테크 범죄[1]에 관한 상담, 홍보 계몽 활동 등에 종사하는 정보보안 자문관을 도도부현 경찰에 배치하여 능력 향상을 위한 연수를 실시한다.

또, 보안 포털 사이트 및 정보 보안 커뮤니티 센터를 활용해, 소비자단체, 학교 관계자 등과 제휴한 홍보 계몽 활동을 추진하면서, 하이테크 범죄 등에 관한 상담에 신속하고 적확하게 대응하기 위한 네트워크 상담 대응 시스템을 구축한다. 또한 하이테크 범죄 등에 관한 상담이나 사건에 관한 정보, 벤더나 관계 기관으로부터의 정보 등을 집약·분석해, 일원적으로 도도부현 경찰에 제공함과 함께, 이들 정보를 도도부현 경찰을 통해서 민간 등에도 제공하는 체제를 확립한다.

(2) 산업계와의 협력 강화(경찰청, 총무성, 경제산업성)

2002년중에 민간 부문에 있어서의 보안 수준의 향상, 하이테크 범죄 대책 등의 정보보안 대책을 효과적으로 추진하기 위해, 정보통신 관련 사업자, 정보보안 전문 사업자, 정보보안 관련 단체, 컴퓨터 전문가 등과 제휴하여 정보보안에 관한 정보를 수집·분석하기 위한 구조를 구축한다.

(3) 신뢰성 향상 시설 등의 도입 지원(총무성)

2002년중에 자연재해 등 비상시에 통신 수단의 확보 와 정보보안을 향상시키기 위하여, 「전기통신기반 충실 임시조치법」상 지원대상이 되는 「신뢰성 향상 시설」에 의해, 이들 시설을 도입하는 민간사업자에 대한 세제 우대 조치를 지원하며, 2003년도까지 법인 또는 개인 사업자가 「방화벽 장치」를 구입했을 경우의 세제 우대 조치를 실시한다.

(4) 정보통신 네트워크에서의 정보 보안 평가 방법 확립 (총무성)

2003년도까지 정보통신 네트워크에 관하여 사업자 규모였던 보안 평가 항목 등의 검토를 실시해, ITU에 대해 국제표준 제안을 하고, 사업자에 있어서의 정보 보안 대책의 수준을 정확하게 판단하기 위한 평가 방법을 확립한다.

(5) 전기 통신사업에서의 정보보안 대책의 인정(총무성)

2002년도중에, 보안대책 실시를 충실히 하고 있는 프로바이더에 관한 민간인정사업의 개시와 관련된 지원을 통하여, 프로바이더의 정보보안 대책의 향상 및 이용자에 의한 프로바이더의 선택에 도움을 준다.

(6) 부정 액세스 대책·바이러스 대책 등에 관한 정보 제공 체제의 강화(경제 산업성)[6]

2003년도까지 부정 액세스, 바이러스 등에 관한 정보 수집·분석을 실시하고 있는 정보처리진흥사업

1) 일본에서 말하는 하이테크 범죄는 컴퓨터 기술 및 전기통신기술을 악용한 범죄로, 전자계산기사용사기, 네트워크를 이용한 음란물 배포, 부정액세스금지법위반 등을 들 수 있다.

협회(IPA) 및 컴퓨터 긴급대응센터(JPCERT/CC)에 대해, 내적 충실을 강화하고 상호 제휴 및 해외 관계 기관과의 제휴에 대한 지원을 실시해, 정보보안 정보 제공 기능을 향상시켜 폭 넓게 일반 이용자가 이들 정보 제공을 향수할 수 있는 환경을 정비한다.

(7) 정보보안 관리 규격의 보급·계몽(경제산업성)

2002년중에 정보보안 관리규격(ISO/IEC17799, JISX 5080)에 근거한 관리 실시를 위한 가이드라인을 정비해 보급·홍보한다.

4. 정보보안 관련 제도·기반의 정비

형사 기본법제, 정보보안에 관한 객관적인 판단기준 등 정보 보안 대책에 있어서의 제도·기반의 정비를 추진한다.

(1) 형사 기본법제 등의 정비(경찰청, 총무성, 법무성, 외무성, 경제 산업성)

고도 정보통신 네트워크 사회의 안전성 및 신뢰성 확보에 이바지하기 위해, 2005년까지 가능한 한 빨리 각종 하이테크 범죄에 대한 벌칙, 정보통신 네트워크에 관한 수사절차에 대해서, 적절한 처벌을 확보하기 위하여 필요한 법제정비를 실시한다.

(2) 전기 통신사업에서의 안전·신뢰성 대책(총무성)

2003년도까지 전기통신사업에 있어서의 정보보안에 관해서 진행되고 있는 국제 규격의 책정에 대응하여 일본 국내에서의 전기통신사업용 네트워크의 안전·신뢰성 대책 기준에 대해서 필요한 제도 정비를 실시하며, 2002년중에 관계부성과 협력해, 비상시의 다수 사업자간의 제휴 강화나 중요통신을 효과적으로 확보하기 위한 시스템의 상태에 대하여 검토하여, 구체적인 방향을 확립하도록 한다.

(3) 암호 기술 표준화의 추진(총무성 및 경제산업성)

객관적으로 그 안전성이 평가되고 실용성이 뛰어난 암호 기술을 채용하기 위하여, 2002년중에 ISO, ITU 등에서의 암호 기술 국제 표준화 상황에 따라, 전문가에 의한 검토회의 개최 등을 통해서 전자정부 이용에 도움이 되는 암호 기술의 평가 및 표준화를 행한다.[2)]

(4) 정보보안 평가·인증 사업의 국제상호승인(경제산업성)

2003년도까지 일본 국내의 정보기기 등의 정보보안 관련 국제규격(ISO/IEC15408)에 근거한 평가·인증 사업에 대해서, 정부 차원에서의 인증결과에 관한 국제상호승인스킴에의 참가를 목표로 한다.

5. 개인정보의 보호

고도정보통신 네트워크 사회의 진전에 따라 개인정보의 이용이 현저하게 확대되고 있는 것을 감안하여, 정부와 민간을 통한 개인정보의 적정한 취급을 확보함으로써, 개인정보의 유용성을 배려하면서 개인의 권리 이익을 보호한다.

(1) 개인정보의 적정한 취급에 관한 기본법제의 정비(내각 관방, 내각부 및 전 부성)

개인정보의 적정한 취급에 관해, 기본원칙 및 정부에 의한 기본방침의 작성 기타 시책의 기본이 되는 사항을 정해, 국가 및 지방공공단체의 책무 등을 명확히 하는 동시에, 개인정보를 취급하는 사업자가 준수해야할 의무 등을 정하는 「개인정보 보호에 관한 법률(안)」의 공포 후 2년 이내의 시행을 위해 노력한다.

또, 모든 분야를 포괄적 대상으로 하는 「개인정보의 보호에 관한 법률(안)」의 동향을 감안하여, 법 공포후 2년 이내에 개별 분야에서의 개인정보의 적정한 취급이 담보되도록 필요한 조치를 강구해, 법의 적절하고 유효한 시행을 도모한다.

(2) 행정기관 및 독립 행정법인 등이 보유하는 개인정보의 적정한 취급에 관한 법제의 정비(총무성 및 전부성)

국가의 행정기관, 독립 행정법인 등에 관하여 개인정보의 보호에 관한 법률안에 따라 공적 부문에 어울리는 개인정보의 적정한 취급을 정하는 「행정기관이 보유하는 개인정보 보호에 관한 법률(안)」 및 「독립 행정법인 등이 보유하는 개인정보의 보호

2) 암호기술검토와 관련된 자세한 사항은 아래 참조.
http://www.meti.go.jp/policy/netsecurity/cryptpress2001.htm

에 관한 법률(안)」, 기타 관련법의 공포 후 2년 이내의 시행을 위해 행정 기관이 보유하는 개인정보의 대강을 기재한 개인정보 파일을 작성하는 등으로, 행정의 적정하고도 원활한 운영을 도모하면서 개인의 권리 이익을 보호한다.

6. 정보 보안과 관련되는 연구개발

(1) 국방·치안과 관련 정보보안 기술 연구개발 추진

2002년 중에 강력한 방화벽의 연구개발을 실시하여, 경찰이 보유하는 네트워크의 정보 보안을 강화한다. 또, 2004년도까지 사법절차를 위한 전자적 기록의 해석 기술에 관한 계통적인 조사 연구 등을 실시해, 「컴퓨터 법과학」 분야의 확립을 목표로 한다(경찰청). 그리고 2003년도까지 사이버 공격에 대한 대처 수법의 실증적 연구 등을 실시하여, 방위청이 보유하는 네트워크의 정보보안을 강화한다(방위청).

(2) 정보보안에 관한 기반기술 연구개발의 추진(경찰청, 총무성 및 경제산업성)

2005년도까지 세계 최첨단 IT국가에 상응하는 기술 수준을 확보하기 위해, 현재 상정되고 있는 모든 위협에 대한 정보보안 기술의 연구개발을 추진해, 아래 2가지의 연구개발에 대해서 2005년도까지 실용화를 목표로 한다.

i) 부정 액세스나 사이버 테러의 예방, 탐지 등에 관한 연구개발

부정액세스나 이른바 사이버 테러 등의 위협으로부터 정보통신 네트워크를 보호하기 위하여, 이들 위협을 탐지하여 신속하고 적절한 대처를 가능케 하기 위하여 필요한 기술을 개발한다.

ii) 정보통신 네트워크의 안전성 및 신뢰성의 확보에 관한 연구개발

정보의 자유로운 유통을 확보하기 위해 암호기술, 전자서명 등의 인증기술, 보안 평가·인증기술, 자연재해 등의 비상시 통신기구 등의 정보통신 네트워크의 안전성 및 신뢰성 확보에 필요한 기술을 개발한다.

7. 정보 보안과 관련된 인재육성

연구개발, 연수사업, 자격제도 도입 등을 통하여 높은 수준의 정보보안 기술을 가진 인재를 충분히 확보하기 위한 다각적인 육성책을 실시한다.

(1) 하이테크 범죄 대책 관련 인적 기반의 정비(경찰청)

2004년까지 하이테크 범죄 수사관의 배치, 사이버 패트롤 모니터의 위촉, 하이테크 범죄 수사에 종사하는 전국의 경찰직원에 대하여 부내외의 연수 실시 등 하이테크 범죄 대책에 필요한 인재의 확보나 민간과의 협력 체제 정비를 실시한다.

(2) 방위청에 있어서의 정보보안 등 관련 인재 교육(방위청)

2003년까지 방위청 직원을 미국 등에 파견해 긴급사태 대처 등 고도의 정보보안 기술 등을 습득한 핵심적인 기술 전문 요원을 확보하여, 부내에서의 기술요원의 교육 및 작전 정보 등 은닉성이 높은 정보를 취급하는 방위청 네트워크의 정보보안을 확보한다.

(3) IT보안 기능 표준의 책정·보급(경제 산업성)

2004년까지 고도의 IT보안 기술자의 육성·활용을 추진하기 위해 IT보안 관련 업무에 필요로 하게 되는 기능에 관한 표준을 책정함과 함께 해당 표준에 근거하는 인재육성 프로그램 작성을 지원한다.

(4) 정보보안 평가 기술자의 육성(경제 산업성)

2004년까지 정보보안 평가기준(ISO/IEC15408, JIS X 5070)에 근거한 평가를 실시할 정보 보안 평가 기술자 및 정보 보안 설계 기술자를 육성하기 위해 연수 사업에 대한 조성을 실시한다.

8. 정보 보안과 관련되는 국제 제휴

정보보안에 관한 국제적인 노력의 추진과 더불어, 개발 도상 지역에의 지원 등 국제적인 노력에 적극적으로 공헌한다.

(1) 하이테크 범죄 대책과 관련되는 국제 제휴의 강화(경찰청, 총무성, 외무성, 법무성 및 경제산업성)

2002년중에 G8의 구조에서 하이테크 범죄에 관한 신속한 수사 협력을 위한 규정작성 등에 관해 협의한다.

(2) 각국 경찰 관계 기관과의 제휴 강화(경찰청)

2002년중에 아시아·태평양 하이테크 범죄 대책 담당 실무자 회의의 개최, 아시아 각국 경찰 기관과의 연락을 위한 24시간 컨택포인트 시스템의 확장 등을 통

해, 각국 경찰 기관과의 제휴를 강화함과 함께, 하이테크 범죄 대책과 관련되는 기술적 지도 등을 실시한다.

(3) 미국 국방부와의 제휴 강화(방위청)

2003년까지 미 국방부와 정책 협의, 의견교환(IT포럼 등) 등을 통해서 방위청에서의 정보보증[3] 을 확립하는 것과 동시에, 이들 노하우·기술 등에 대해서 국방상 지장이 없는 한 부외에 공표한다.

(4) 정보 보안에 관한 글로벌 정보 교환 네트워크의 구축 (경제산업성)

2003년까지 부정액세스·바이러스 등의 발생 상황·분석 등 정보보안에 관한 정보집적을 행하고 있는 CERT/CC등 여러 나라의 정부와 민간 관계기관과의 정보 교환을 위하여, JPCERT/CC에서의 관계 제기관과의 제휴 강화, 민간 각층에 있어서의 네트워크 구축의 지원 등을 실시하여 정보보안에 관한 신속하고 정확한 정보 제공, 대응 및 시책에의 반영을 할 수 있는 환경을 정비한다.

V. 결 론

이상으로 「e-Japan 중점계획 2002」 중 고도정보통신네트워크 안전·신뢰성 확보방안에 대하여 살펴보았다.

앞서 살펴본 바와 같이 일본은 국가차원의 정보화 전략으로 「e-Japan 전략」을 선택하였고, 이를 구체화하는 방안으로 중점계획을 작성, 시행하고 있다.

한편 정보화정책 중 고도정보통신네트워크 안전·신뢰성 확보방안이 차지하고 있는 것은 5대 중점과제 중 하나로서 그 중요성이 부각되어 있다.

또한 지난 9.11테러 이후 미국은 자국의 테러대응태세와 관련하여 종전의 테러대응이 각 부처별로 별도로 추진되어 종합적이고 효율적인 대응이 불가능하다고 판단하여, 범국가적 차원에서 정비를 시도하고 있다. 이러한 상황은 정보보안부문에서도 마찬가지여서, 이전의 정보보안관련 정책 및 국가계획을 대체할 종합적 대응체제정비를 내용으로 하는 새로운 국가전략(National Strategy to Secure Cyberspace)을 수립하고 있다.

현재 국내의 경우도 정보보안 또는 정보보호부문의 업무 수행에 있어 범국가차원의 종합적·체계적 전략이 부재한 것으로 생각된다. 정보화추진을 위하여 그간 많은 노력을 기울인 결과 우리는 상당한 정보화의 진전을 거두었다. 이는 국가·사회적으로 주요한 기반시설의 정보시스템에 대한 의존성의 심화라는 결과를 가져오게 되었고, 이러한 정보시스템에 대한 위협은 국가 경쟁력의 손실과도 직결되는 문제로 인식될 수 있다.

이러한 상황인식을 바탕으로 빠른 시일내에 범국가적·범부처적 차원에서의 정보보안 부문에서의 국가전략을 수립하여 시행하는 것이 필요하다고 판단된다.

참 고 문 헌

[1] 김현수, 박소현, *"9.11테러 이후 미국·일본의 대응동향"*, Security Focus 2002-2, 국가보안기술연구소, pp. 21-28, 2002. 6.

[2] 박영우, 김현수, *"정보통신기반보호 관련 해외동향과 법률시행에 따른 정보보호산업계의 변화"*, 월간 정보보호21c, pp. 84-88, 2001. 1.

[3] IT 戦略本部, e-Japan 重点計劃-2002, 2002. 6.

[4] 内閣官房 情報セキュリティ 対策推進室, "緊急対応支援チームの設置について", 2002. 3. 28.

[5] 警察庁, ハイテク犯罪対策, http://www.npa.go.jp/hightech/index.htm

[6] 經濟産業省, 情報セキュリティ政策, 署名認証, http://www.meti.go.jp/policy/netsecurity/index.html

〈著 者 紹 介〉

김 현 수 (Hyun-soo Kim)
정회원

1997년 2월 : 부산대학교 사법학과 졸업
1999년 2월 : 부산대학교 일반대학원 법학과 석사
2000년 2월~2002년 3월 : 한국정보보호진흥원 정책연구팀 연구원
2001년 3월~현재 : 한국전자통신연구원 부설 국가보안기술연구소 정책팀 연구원
관심분야 : 국가 정보보호 정책, 전자거래법, 지적재산권법

3) 정보보증: 여기서는 현재 미 국방부가 실시하고 있는 컴퓨터 시스템 등의 안전에 관한 각종 시책의 총칭(Information Assurance).