情 報 保 護 學 會 誌
第 13 券 第 3 號, 2003. 6

전자정부 정보보호 대응체계 구축 방향에 관한 연구

안 문 석*, 박 성 진**, 맹 보 학***

요 약

본 논문에서는 성공적인 전자정부 구축에 필요한 정보보안 대응체계의 구축 방향을 제시하고자 한다. 이를 위해 현 전자정부 정보보안 대응체계의 현황과 문제점을 분석 한 후 효과적인 정보보안 대응체계 구축을 위한 정책대안을 제시하고자 한다. 즉, 전자정부 정보보안 대응체계의 기본방향을 제시하고, 이를 토대로 전자정부 정보보안 추진체계의 정비와 전자정부 정보보호 추진기반 구축이라는 두 차원에서 관리 및 제도적 정책대안을 제시하고자 한다.

Ⅰ. 서 론

정보통신기술의 발전은 전세계에 걸쳐 급격한 사회변화를 촉진시키고 있다. 컴퓨터와 인터넷이 만들어 낸 새로운 공간 즉, 사이버 공간의 탄생은 인류역사에 있어서 새로운 획을 긋는 문명사적 의미를 지니고 있다고 할 수 있다. 사이버 공간이라는 새로운 공간에서 전세계의 수많은 사람들이 새로운 의사소통 및 생활양식을 창조해가고 있으며, 새로운 공간에 적합한 제도와 질서를 만들어가고 있다.

이러한 변화는 자유로운 정보교환과 경제적 이익, 나아가 일상생활의 유익성과 편리함을 제공하고 있으나, 컴퓨터 해킹, 컴퓨터 바이러스, 프라이버시 침해, 음란·폭력 정보의 범람, 사이버 공간에서의 인권침해 범죄 등 각종 정보화 역기능으로 인한 새로운 사회적 문제도 야기 시키고 있다.

정보화의 역기능은 정보통신기술의 발전으로 나타난 새로운 공간에서 새로운 사람사이의 관계가 형성되면서 나타나는 현상이라 할 수 있다. 즉, 새로운 공간에서 나타난 혼란스러운 관계를 질서와 신뢰가 있는 안정적인 관계로 변화시키는 새로운 제도적·문화적 시스템이 아직 정비되지 않았기 때문에 나타나는 현상이라 할 수 있다. 우리나라는 그 동안 정부의 노력에 의해 물리적 정보인프라 구축면에서는 세계 일류 국가가 되었지만, 정보화 역기능을 제어할 수 있는 새로운 제도적 시스템을 디자인하는 데에는 상대적으로 소홀하였다고 볼 수 있다.

특히 국가의 미래를 걸고 정부가 많은 노력을 기울이고 있는 전자정부의 성공적인 구축을 위한 필수요소 중의 하나가 신뢰성이다. 전자정부의 서비스에 신뢰감이 없다면 아무리 편리한 시스템을 구축하였다 하더라고 국민이나 기업들은 전자정부의 서비스를 이용하려 하지 않을 것이다. 이러한 전자정부 서비스에 대한 국민들의 신뢰감 형성은 철저한 정보보안을 전제로 할 경우에만 가능하다. 해킹과 컴퓨터 바이러스 등을 이용한 전자적 침해행위에 대한 체계적이고 효과적인 대응이 부족하다면 전자정부 구축은 물론 국가안보까지도 위협 받을 수 있다.

미국, 일본, 영국 등 선진국은 이러한 전자적 침해 위협이 전자정부 구축 및 국가안보에 가장 큰 장애요소가 될 것으로 인식하고 제도 및 기술적 측면에서 다양한 정책들을 수립 및 추진하고 있다. 우리나라도 정보통신기반보호법, 정보통신망이용촉진 및 정보보호 등에 관한 법률, 국가정보원법, 전자서명법, 보안업무규정 등 각종 정보보안 관련 법률을 제·개정하여 이러한 정보화의 역기능을 방지하기 위해 노력해 왔다.

그러나 이상과 같은 노력들에도 불구하고 국가 전

* 고려대학교(ahnms@korea.ac.kr)
** 경인여자대학(psj3000@hotmail.com)
*** 경인여자대학(mbohak@kic.ac.kr)

반에 걸친 체계적이고 종합적인 정보보안정책은 아직 부족한 편이라 할 수 있다. 정보시스템은 수 많은 컴퓨터와 네트워크, 그리고 사람들로 구성되어 있기 때문에 어느 한 부분에서 보안의 취약성이 발생한다면 전체 시스템은 외부의 공격에 쉽게 침해당할 수 있다. 정보보안은 어느 시스템 하나 또는 어느 조직 하나만 보안에 철저하다고 해서 항상 안전한 것은 아니다. 따라서 국가의 정보보안정책은 정부와 민간부문, 나아가 세계 각국과의 연계도 고려된 체계적이고 종합적인 정책으로 수립되어질 필요가 있다. 또한 기술적 측면 보다는 제도 및 관리적 차원에서 포괄적인 정보보호정책이 수립되어질 필요가 있으며, 정보보호 기술에 대한 연구개발에 대한 투자, 정보보호 전문인력 양성, 정보보호 인식 제고, 예산 및 법률적 지원 등 지속적이고 적응력 있는 정보보안 노력이 이루어질 수 있는 체계적인 추진전략도 수립되어질 필요가 있다.

따라서 본 논문은 현 전자정부 정보보안 대응체계의 현황과 문제점을 분석 한 후 효과적인 정보보안 대응체계 구축을 위한 정책대안을 제시하고자 한다. 즉, 전자정부 정보보안 대응체계의 기본방향을 제시하고, 이를 토대로 전자정부 정보보안 추진체계의 정비와 전자정부 정보보호 추진기반 구축이라는 두 차원에서 관리 및 제도적 정책대안을 제시하고자 한다.

Ⅱ. 전자정부 정보보안 대응체계의 현황과 문제점

1. 우리나라 정부의 보안침해 현황

인터넷 이용인구가 2002년 6월 기준으로 2,565만 명으로서 전체인구의 약 58%에 이를 정도로 정보화가 급격히 성숙되면서 정부는 물론 민간부문 전 분야에 걸쳐 정보시스템에 대한 의존도가 높아지고 있다.[11] 이러한 추세에 발 맞추어 해킹이나 컴퓨터 바이러스에 대한 피해도 급격하게 증가하고 있다. 2001년 한 해 동안 한국정보보호진흥원에 접수된 해킹 사고건수는 5,333건으로서 2000년 해킹사고 1,943건에 비해 274%나 증가하였다. 2001년 2월부터 12월까지 한국정보보호진흥원과 주요 백신업체에서 접수받은 바이러스 신고건수는 65,033건에 이르고 있다.[9] 인터넷의 전세계적 보급이 가속화되고 정보화가 진전되면서 해킹 및 바이러스로 인한 정보보안 침해사고는 크게 증가하여 왔으며, 앞으로도 계속 증가할 것이다.[3][8]

정부 및 공공기관에서 발생한 보안 침해 추이 또한 급격한 증가 추세를 보이고 있다.[1][4][2] 국가정보원(정보보안119)에서 처리한 국가 및 공공기관에서 발생한 해킹사고를 종합한 통계를 보면, 1998년도에는 8건이었던 침해사고가 2000년에는 102건, 2001년에는 507건으로 급격하게 증가하는 추세를 보이고 있다.

2. 우리나라 정보보안 대응체계의 현황

2.1. 우리나라 정보보안 대응체계 개관

현재 우리나라 정부의 정보보호 체계는 범정부차원의 종합적이고 명확한 체계를 구축하고 있지는 않지만, 대략 3개의 기관을 중심으로 이루어지고 있다. 국가 및 공공분야의 보안업무를 국가정보원이 담당하고 있으며, 행정자치부는 행정부에 대한 보안업무를 담당하고 있다. 정보통신부는 공공 및 민간부문에 대한 정보보호 기능을 수행하고 있으며, 특히 최근에는 정보통신기반에 대한 보호 업무도 관장하고 있다. 국가정보원, 행정자치부, 정보통신부 세 개의 기관을 중심으로 이루어지고 있는 현재의 정보보호체계는 기관간 업무의 중복이나 갈등이 잠재해 있는 상황이다.

현재 우리나라 전자정부 정보보안과 관련된 주요 법령들을 열거하면 다음과 같다.

- 정보통신기반 보호법(법률제6383호 신규제정 2001.01.26.)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률제6360호 전문개정 2001.01.16.)
- 보안업무규정(대통령령 제17116호 일부개정 2001.01.29.)
- 정보화촉진 기본계획법(법률제6360호 일부개정 2001.01.16.)
- 국가정보원법(법률제5681호 일부개정 1999. 01. 21.)
- 정보 및 보안업무 기획조정 규정(대통령령제1 6211호 일부개정 1999.03.31.)
- 행정자치부 보안업무 규정(2000.9.)

이상의 법령들을 살펴보면, 국가정보원은 국가 일반 보안업무차원에서 정보통신 분야의 보안업무 기능을 수행하고 있으며, 행정자치부는 행정 각 부처 및 기관의 일반 사무 및 업무 감독 차원에서 보안업

무 기능을 수행하고 있다. 또한 정보통신부는 민간부문을 중심으로 그리고 최근에는 정보통신기반을 중심으로 정보보안업무를 수행하고 있다.

이외에 정보통신부 산하의 한국정보보호진흥원, 한국전자통신연구원 부설 국가보안기술연구소, 경찰청의 사이버테러대응센터, 검찰청의 인터넷 범죄 수사 센터(컴퓨터수사과) 등도 정보보호와 관련되어 있다. 이들 기관의 기능을 간단히 살펴보면 다음과 같다.

한국정보진흥원은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률제6360호 전문개정 2001. 01.16.)이 개정되면서 기존의 한국정보보호센터의 기능이 강화되고 그 명칭이 변경되어 설립된 기관이다. 한국정보진흥원의 주요 기능으로는 정보보호를 위한 정책 및 제도의 조사·연구, 정보화 역기능 분석 및 대책 연구, 정보보호에 관한 홍보 및 교육·훈련, 정보보호시스템의 연구·개발 및 시험·평가, 정보보호시스템의 성능과 신뢰도에 관한 기준제정 및 표준화 지원, 정보보호를 위한 암호기술 개발, 개인정보보호를 위한 대책 연구, 분쟁조정위원회의 운영지원 및 개인정보침해신고센터 운영, 정보시스템 침해사고 처리 및 대응체계 운영, 전자서명법 제25조제1항의 규정에 의한 전자서명 인증관리 등이다.

국가보안기술연구소는 2000년 1월 한국전자통신연구원 부설 연구소로 설립된 기관이다. 국가보안기술연구소는 실질적인 정부 관련 보안 연구개발을 총괄하는 연구개발 중심기관이고, 한국정보진흥원은 업체 인증 기능 등 민간기관 대상 업무를 주축으로 하는 기관이라는 점에서 차이가 있다고 볼 수 있다.

경찰청 사이버테러 대응 센터는 2000년 7월 종전의 사이버범죄수사대가 확대 개편된 기관으로서 단장을 중심으로 협력운영팀, 신고경보팀, 수사팀, 기법개발팀 등 4개팀으로 조직되어 있다. 사이버테러 대응 센터의 주요 임무는 국내외 사이버테러 혐의자 포착 및 동향 관찰, 국내 사이버테러 사건 추적 수사 및 초동 조치, 사이버테러 수사기법 연구개발 및 필요장비 확보, 국제경찰기구 등과의 대 사이버테러 협력체제 유지 등이다.

검찰청 인터넷범죄수사센터는 2001년 2월에 설치된 기관으로서 대검찰청 컴퓨터 수사과(2000년 2월 중앙수사부내 신설)에 의해 운영되고 있다. 또한 서울지검도 인터넷범죄수사센터를 설치되어 있는 데 서울지검 컴퓨터수사부에서 운영하고 있다. 검찰청 인터넷범죄수사센터에서는 해킹, 컴퓨터바이러스 유포와 같은 신종범죄와 전자상거래를 이용한 사기, 개인정보침해 등에 중점을 두고 집중적이고 지속적으로 범죄동향을 파악하고 있으며, 이를 통하여 보다 효율적인 컴퓨터범죄 대책을 수립하고 새로운 수사방법을 개발하여 적극적인 단속활동을 전개하고 있다. 또한 국내외 유관기관과 긴밀하게 협력하면서 수사역량을 극대화하고 있다. 한편 대검찰청 컴퓨터수사과는 주요 기능은 컴퓨터 등 정보처리장치 및 정보통신매체를 사용한 범죄사건에 대한 검찰사무의 지휘감독, 컴퓨터 등 정보처리장치 및 정보통신매체와 관련된 증거자료에 대한 압수수색 및 분석 등의 지원, 위 사건에 규정된 사건에 관한 범죄현상의 분석연구수사 지침수립 및 국내외 중요사건 사례연구집 발간 등이다.

한편, 미국의 9.11 테러 이후 정부는 2001년 11월 6일에 '테러대비 정부 종합대책'을 만들어 정보보호관련 문제를 다루고 있다. 이 대책은 미국의 항공기 테러에 이어 전 세계적으로 발생하고 있는 탄저균 테러 등으로 대표되는 신종 테러로부터 우리나라도 결코 안전할 수 없다는 전제아래 국무조정실 주관하에 관련부처로 구성된 Task Force에서 마련하여 실무협의와 관계차관회의를 거쳐 확정된 것이다. 이 대책에 따르면 새로운 유형의 테러에 체계적·효율적으로 대응하기 위해 국무총리를 의장으로 하는 '국가대테러 대책회의'를 설치하였다.

2.2. 일반 행정부처의 정보보안 대책 : 행자부의'정보통신보안업무규정'

일반 행정부처 및 기관의 정보보안 대책은 국정원의 '보안업무규정'과 행정자치부의 '정보통신보안업무규정(2000.9 제정)'에 의해 영향을 받고 있다. 국정원의 '보안업무규정'은 정보보안 뿐만 아니라 일반 보안 사항을 포괄적으로 다루고 있으며, 특히 국가기밀에 관한 내용을 중심으로 다루어지고 있다. 일반 행정부처 및 기관의 정보보안 대책과 보다 연관성이 높은 지침은 행정자치부의 '정보통신보안업무규정'이기 때문에 아래에서 간략히 살펴보고자 한다.

• 정보통신보안 기본방향

정보통신보안의 기본방향은 해당기관의 정보통신보안에 관한 책임은 해당기관의 장에게 있다는 것이다. 따라서 해당기관은 다음과 같은 정보통신보안의 기본활동을 수행해야 한다. ① 정보통신보안 계획수

립 및 시행, ② 정보통신보안 심사분석 시행, ③ 정보통신보안 관련규정·지침 등 제·개정, ④ 산하기관에 대한 정보통신보안 감사·지도점검 실시, ⑤ 정보통신보안 교육계획 수립 시행, ⑥ 정보통신시스템의 취약성 진단·분석 및 보안대책 수립 시행, ⑦ 정보통신보안 위규적발 강화 및 사고조사 처리, ⑧ 보안시스템 개발 및 운용관리, ⑨ 바이러스·해킹 등 사이버테러 위해요소 제거, ⑩ 도·감청 등 위해요소 제거, ⑪ 기타 정보통신보안 제반 사항 등이다.

• 정보통신보안관리

해당기관의 장은 정보통신실(전산시스템실, 전산센터, 통신실 등)에 대하여 다음과 같은 보호대책을 강구하여야 한다. 즉 ① 천재지변 등 자연재해 방재대책, ② 외부로부터의 위해 방지대책, ③ 항시 이용하는 출입문은 한 곳으로 정하고 이중잠금장치 설치, ④ 출입문 보안장치 설치 및 주야간 감시대책, ⑤ 보조기억매체를 보관할 수 있는 내화금고 등 철제용기 비치, ⑥ 보조기억매체에 대한 안전지출 및 주요자료소산 계획수립, ⑦ 관리책임자 및 자료·장비별 취급자지정 운용 등이다.

• 보안시스템관리

해당기관에서 사용할 보안시스템은 국가정보원장이 개발하거나 제작하여 필요한 기관에 공급한다. 다만 국가정보원장이 필요하다고 인정할 때에는 중앙행정기관 또는 정부출연 연구기관으로 하여금 개발하게 하거나 제작하게 할 수 있다. 이때 중앙행정기관 또는 정부출연 연구기관이 개발하거나 제작한 보안시스템은 보안성 및 신뢰성 등에 대하여 국가정보원장의 평가·인증을 받아야 한다. 보안시스템은 어떠한 경우에도 복제·복사할수 없으며, 다른 기관이나 개인에게 임의 대여할 수 없다. 그리고 암호자재를 취급하는 기관은 등록암호자재 취급기관(행자부 행정정보화계획관실)과 위임암호자재 취급기관(행자부 정부전산정보관리소, 시도 및 경북 울릉군)으로 구분하며, 국가기관의 정보통신시스템에 적용되는 암호프로그램은 국가정보원장이 개발·보급한다.

• 침입차단 시스템(방화벽)

해당기관의 장은 내부 정보통신망을 인터넷 등 외부망과 접속할 때에는 내부망을 보호하기 위하여 침입차단시스템 도입 등 보안대책을 강구하여야 하며, 침입차단시스템을 도입할 경우에는 내부망과 외부망 간의 접속경로를 단일화하도록 하여야 한다. 침입차단시스템을 설치·운용하고자하는 해당기관의 장은 국가정보원장이 인증한 제품을 선정하여야 한다.

• 정보통신보안 측정

정보통신보안측정은 다음의 경우에 실시한다. 즉 ① 정보통신보안사고하여 정보통신망의 취약성 진단이 요구 될 때, ② 국가 주요 기반구조에 대한 불법침해(해킹)나 도청 등으로부터의 보호대책이 필요한 경우, ③ 정보통신수단에 의하여 국가기밀 유출 및 암호체계의 누설 우려가 있는 경우, ④ 정보통신시스템에 대한 보안성검토와 보안시스템 설치 등에 대한 국가정보원장의 보안대책 확인이 요구되는 경우, ⑤ 해당기관의 장이 정보통신망에 관한 취약성 점검 또는 종합진단이 필요하다고 판단하여 요청할 경우, ⑥ 기타 국가보안상 필요하다고 판단하는 경우 등이다. 정보통신보안 위규사항은 ① 불온통신에 관한 사항, ② 군사상 비밀의 누설, ③ 외교상 기밀의 누설, ④ 국가정보활동에 관한 사항, ⑤ 보안시스템에 관한 사항, ⑥ 암호자재에 관한 사항, ⑦ 비인가통신시설 및 통신제원사용에관한 사항, ⑧ 허가목적이외의 방법으로 사용하는 경우 등이다.

2.3. 정보통신기반 보호 대책

우리나라의 중요 기반구조 보호는 2001년 1월 26일에 공표되고 2001년 7월부터 시행되는 '정보통신기반보호법'을 중심으로 이루어지고 있다. 이 법이 제정된 목적은 정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터바이러스 등을 이용한 전자적 침해행위가 21세기 지식기반국가의 건설을 저해하고 국가안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하려는 것이다.[5] 이 법이 재정되기 전에는 주요정보통신기반 사이버 공격에 대한 체계적이고 종합적인 대응을 위한 근거법령이 부족하였다. 전기통신기본법, 정보화촉진기본법, 정보통신망이용촉진 등에 관한 법률, 국가정보원법, 보안업무규정 등에 산재되어 있었던 것이다.

이 법에서 주요 정보통신기반시설로 예시한 것은 국가의 안전과 국민생활의 안정에 중대한 영향을 미

치는 정부(행정), 국방, 금융, 통신, 운송, 에너지 등의 업무와 관련된 정보통신 기반시설(제어·통제 시스템, 정보시스템, 통신시스템 등)이다. 정보통신기반법의 주요 내용을 간략히 정리하면 다음과 같다.

• 정보통신기반보호위원회 설치

주요정보통신기반시설의 보호를 위한 범정부적 대응체제를 구축하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 설치함.

• 해당기관의 장의 책임

- 계획수립: 주요정보통신기반시설을 관리하는 기관의 장은 정기적으로 소관 시설에 대한 취약점을 분석·평가하여 이에 따른 보호대책을 수립·시행하고 주요정보통신기반시설을 관장하는 중앙행정기관의 장은 소관분야별 주요 정보통신기반시설 보호계획을 수립·시행하도록 함.
- 통지 및 조치: 주요정보통신기반시설을 관리하는 기관의 장은 소관 시설이 침해사고로 인하여 교란·마비 또는 파괴된 사실을 인지한 때에는 이를 관계기관등에 통지하고 피해복구 및 피해확산 방지를 위한 조치를 취하도록 함.
- 정보보호책임관 및 정보보호책임자 지정 : 관계 중앙행정기관의 장은 과장급 공무원을 정보보호책임관으로 지정하며, 관리기관의 장은 4·5급 공무원 또는 임원급 관리·운영자를 정보보호책임자로 지정한다.

• 주요정보통신 기반시설의 지정

중앙행정기관의 장은 정보통신기반보호위원회의 심의를 거쳐 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하도록 함.

• 정보보호 전문업체 지정

정보통신부장관은 주요정보통신기반시설을 관리하는 기관의 동 시설에 대한 취약점 분석·평가 및 보호대책의 수립을 지원하기 위하여 정보보호 전문업체를 지정하도록 함.

• 처벌규정

해킹·컴퓨터바이러스 등 전자적 침해행위에 의하여 주요정보통신기반시설을 교란·마비·파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 함.

3. 우리나라 정보보안 대응체계의 문제점

지금까지 우리나라 정부의 정보보안 침해 현황 및 정책 현황에 대해 살펴보았다. 이를 토대로 현재 우리나라가 직면해 있는 정보보안 정책의 문제점을 살펴보고자 한다.

우선적으로 지적될 수 있는 문제점은 최고관리자의 관심과 지원의 부족을 들 수 있다. 아직은 미미하지만 사회전반에 걸쳐 정보보안에 대한 인식이 점차 높아가고 있는 추세이고 정부의 고위 관리자들도 이에 대한 인식의 폭을 넓혀가고 있는 상황이긴 하다. 그러나 국가 전체의 정보보호는 국가의 안보 및 국민의 생명과 재산을 보호하는 필수적인 기반이라는 점을 인식하고 최고지도자가 이를 적극적으로 추진해 나가는 것이 무엇보다도 필요하다. 특히 관련 기관의 이해관계가 충돌하고 민간부문의 기본권 보장과도 마찰이 일어날 수 있기 때문에 최고지도자의 적극적인 관심과 지원 없이는 충분한 효과를 거두기 어려운 것이다.

둘째, 정부는 물론 사회전반에 걸쳐 아직도 정보보안에 대한 인식이 부족하다는 점이다. 예를 들면 "보안이 취약한 인터넷을 내부 전산망에 연결하여 사용할 때에도 비인가자의 침투를 방지하기 위한 기본적인 보안대책도 강구하지 않은 채 내부전산망과 연결하여 사용하는 등 정보보호대책을 소홀히 취급하는 것이 가장 큰 문제"[6]인 것이다. 특히 정부내부에 근무하는 공무원들의 정보보안에 대한 인식부족은 더욱 큰 문제가 된다. 정부 내부의 컴퓨터 시스템에 해커가 침입하더라도 큰 문제는 없다라는 안일한 인식이 더욱 큰 문제라 할 수 있다. 정보보안체계는 수많은 연결 고리로 이루어져 있다. 그 고리들 중 가장 약한 고리가 전체 시스템의 보안상태를 나타내는 것이다. 아무리 많은 자원을 투입하여 보안시스템을 갖추었다 하더라도 가장 약한 고리 즉 인식이 부족한 공무원 개인의 부주의로 공격자의 침투가 방치된다면 전체 시스템은 이미 무방비 상태로 있는 것과 마찬가지 상태가 되는 것이다.

셋째, 전자정부 정보보호 정책을 체계적으로 수립하고 각 관련 기관들의 활동을 총괄적으로 조정할 수 있는 권한과 자원을 가진 최고 정책기구의 부재가 문제점으로 지적될 수 있다.

넷째, 각 기관은 정보보호 전담조직도 없을 뿐만 아니라 정보보호에 필요한 예산 및 전문인력마저 확

보하지 못해 정보보호를 위한 체계적이고 효율적인 대응이 어려운 실정이다. 정보보안 분야에 대한 예산과 조직의 충분한 지원이 없다면 갈수록 고도화되고 지능화되어 가는 공격자의 침투를 막아내고 대응하는 데 많은 어려움을 겪을 수밖에 없다. 각종 침입차단시스템, 침입탐지시스템 등을 설치하고 운영하려고 하여도 막대한 예산을 필요로 하는 것이다. 그리고 이에 대한 정책수립 및 집행, 방어 및 대응, 교육 및 훈련 등을 위해서도 적절한 전문인력과 전담 조직이 필요한 것이다.

다섯째, 체계적인 긴급대응체제 구축이 아직 부족한 편이다. 침해사고가 발생할 경우 이에 대한 적절한 방어, 경고, 복구, 정보공유 등을 수행할 수 있는 체계적인 절차 및 네트워크가 형성되어 있지 않다면, 침해사고 발생으로 인한 피해는 더욱 커질 수밖에 없다. 물론 침해사고시 상담 및 지원을 해주는 기관으로 정보보호진흥원의 118, 국정원의 정보보안 119가 있고, 침입자에 대한 수사를 담당하는 검찰청과 경찰청의 컴퓨터 범죄 담당 부서가 있다. 그러나 이들간의 연계, 그리고 민간기업을 포함한 기타 관련 기관들간의 연계 및 대응절차들이 아직 충분히 수립되어 있지 않은 상태이다.

여섯째, 취약점에 대한 연구 및 분석 부족이다. 공공기관이나 민간조직은 나름대로 정보보안의 취약점에 대한 연구와 분석이 이루어지고, 이에 관한 자료가 축적되어 있어야 한다. 그러나 대부분의 조직들이 인식부족과 전문인력의 부족 등으로 취약점 현황 파악조차 되어 있지 않는 경우가 많다.

일곱째, 정보보안기술에 대한 연구 및 개발 투자가 매우 부족하다. 갈수록 보안침해기술이 발전하고 있는 상황에서 첨단 보안기술에 대한 연구 및 개발 투자가 부족하다면 적절한 대처를 취하기 어려울 것이다. 특히 국가 안보나 국가 기밀에 관한 정보시스템을 보호하기 위하여 외국의 기술에 의존하는 것은 심각한 문제를 초래할 가능성이 있다.

여덟째, 전문인력의 부족이다. 정보보호가 제대로 되기 위해서는 기술적인 전문가가 우선적으로 필요한데, 한국의 경우 정보보안 전문가가 많지 않은 것이 현실이다. 정보통신기반보호법은 공공기관이나 민간기관은 자기조직에 대한 정보보안의 취약점을 발견하고, 분석하고 이에 적절한 대책을 수립할 것을 권고하고 있는데, 실제로 전문가가 많지 않아 어려움이 있을 것으로 예측된다.

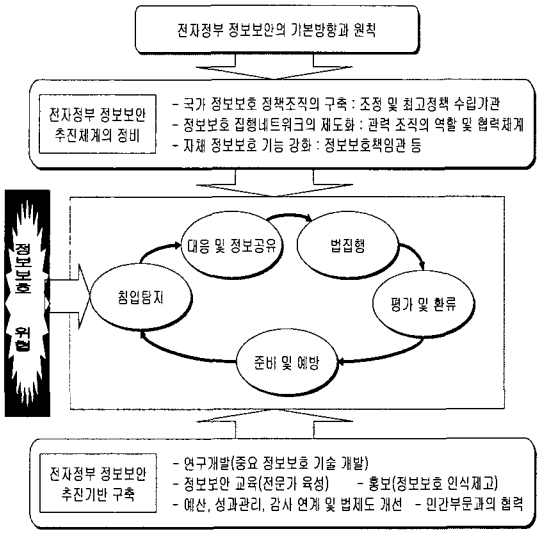
Ⅲ. 전자정부 정보보안 대응체계 구축 방향

1. 전자정부 정보보안의 기본방향

현재 우리가 직면하고 있는 전자정부 정보보안 대응체계의 문제점을 인지하고 이를 극복하기 위한 전략을 수립하기 위해서는 전자정부 정보보안체계의 구조와 과정 전반에 걸쳐 지속적인 혁신작업이 일어나야 한다. 특히 정보통신의 세계는 급속한 변화가 계속해서 일어나고 있기 때문에 시대의 흐름에 따라 보안정책도 지속적인 변화가 뒤따라야 한다.

아래에서는 앞에서 살펴본 우리나라 정보보안정책의 문제점 인식을 바탕으로 전자정부 정보보안 대응체계의 발전방향에 대해 논의하고자 한다. 아래 그림은 정책대안을 모색하기 위한 기본적인 분석틀이다. 우선 전자정부 정보보안의 기본방향을 설정하고, 이를 토대로 전자정부 정보보안 추진체계의 정비, 전자정부 정보보안 추진기반 구축에 대해서 논의하고자 한다.

전자정부 정보보안 대응체계의 기본방향을 제시하기 위해서는 우선적으로 전자정부 정보보안의 주 목적은 무엇인가에 대해서 생각해 볼 필요가 있다. 성공적인 전자정부를 구축하기 위해서 필수적으로 요구되는 조건 중의 하나가 정보보안임을 이미 앞에서 논의하였다. 그리고 전자정부 구축의 목적은 정보통신기술을 활용하여 행정의 효율성과 대국민 서비스 향상을 통해 궁극적으로는 국민의 안전과 복지를 확



〔그림 1〕 전자정부 정보보안 대응체계의 정책대안 모색 틀

보하고 향상시킨다는 것이다. 이와 같이 볼 때 우리가 논의하고자 하는 전자정부 정보보안의 궁극적인 목적은 국민의 안전과 복지를 확보하고 향상시키는 것이다. 따라서 향후 전자정부 정보보안 정책대안을 탐색할 때 이러한 기본적인 목적의식을 기반으로 하여야 할 것이다.

아래에서 전자정부 정보보안의 기본 목적을 바탕으로 보다 나은 정보보안 대응체계를 구축하기 위해 필요한 세 가지 기본방향을 제시하고자 한다.

• 체계적이고 종합적인 정보보안 대응체계기능 강화

정보시스템은 수많은 컴퓨터와 네트워크, 그리고 사람들로 구성되어 있기 때문에 어느 한 부분에서 보안의 취약성이 발생한다면 전체 시스템은 외부의 공격에 쉽게 침해 당할 수 있다. 따라서 정보보안은 어느 시스템 하나 또는 어느 조직 하나만 보안에 철저하다고 해서 항상 안전한 것은 아니다. 갈수록 조직간 네트워크 협력이 증가되고 있는 추세이기 때문에 조직간의 상호의존성으로 인해 발생하는 정보보안의 문제들이 증가할 것이다. 또한 정보보안은 단순히 외부의 공격을 막아내는 것으로 그치는 것이 아니다. 언제든 정보시스템은 다양한 원인으로 인해 침입 당할 수 있기 때문에 침해사고에 대한 탐지, 대응, 복구, 경고 및 정보 공유 등 전반에 걸쳐 체계적인 대응전략이 수립되어질 필요가 있다. 이상과 같은 이유에서 전자정부 정보보안은 국가 전반에 걸친 체계적이고 종합적인 정보보안 대응체계를 수립할 필요가 있는 것이다.

• 민-관 협력 등 다원적 협력체계 구축

전자정부 정보보안은 정부 단독으로 수행하기는 어렵다. 특히 주요 정보통신기반은 정부 이외의 민간 및 공공기관에서 운영하고 있는 경우가 많으며, 일반적인 정부 업무 또한 민간부문과 깊은 연계구조를 가지고 운영되는 경우가 많기 때문에 민간기업, 학계 등 외부의 다양한 기관들과 긴밀한 협력체계를 구축할 필요가 있다.

• 지속성과 적응성을 보장하는 정보보안 대응체계 기반 구축

정보통신기술은 급격하게 변하고 있으며, 이와 함께 해킹 및 바이러스 등 정보시스템에 대한 공격기법도 나날이 변화되고 있다. 따라서 과거의 보호기술로는 새로이 출현하는 공격에 대비할 수 없다. 또한 정보시스템에 대한 침해사고가 갈수록 증가하고 있는 추세이며, 향후에는 국가간의 정보전으로 발전할 수 있는 가능성이 있기 때문에 훈련받은 보안 전문가들에 대한 수요가 급격히 증가할 것이다. 따라서 정보보호 기술에 대한 연구개발에 대한 투자, 전문인력 양성, 국민 전체에 대한 인식 제고, 예산 및 법률적 지원 등 지속적이고 적응력 있는 전자정부 정보보안 체계 구축하기 위한 기반을 마련할 필요가 있다.

2. 전자정부 정보보안 추진체계의 정비

2.1. 국가 정보보안 정책조직의 구축

앞에서 살펴보았듯이 우리나라 정보보안 추진체계는 국가정보원, 행정자치부, 정보통신부 세 기관을 중심으로 이루어져 있으며, 이들 간에 내부적으로 갈등이 발생할 경우 이를 실질적으로 조정할 수 있는 강력한 총괄기구가 없는 것이 문제점으로 지적되고 있다.

물론 정보화와 관련 조정기구로 정보화추진위원회가 있다. 그리고 정보통신기반보호법에 근거한 정보통신기반위원회가 존재한다. 그러나 정보화추진위원회는 정보화 정책 전반에 걸친 문제들을 다루기 때문에 집중적으로 정보보호 문제만을 다루기는 어려운 상황이다. 물론 정보통신기반보호위원회는 국무총리를 위원장으로 한 각료급 위원회로서 정보통신기반보호 정책을 총괄 조정하는 기구라는 점에서 정보보호 문제를 전문적으로 다루는 기구이다. 그러나 간여할 수 있는 정책범위가 주요 정보통신기반시설로만 제한되어 있기 때문에 이에 포함되지 않은 정부 및 공공기관의 정보보호 문제는 조정대상에 제외된다.

따라서 일반적인 정부의 정보보호 업무를 담당하는 행정자치부, 주요정보통신기반의 정보보호 업무를 담당하는 정보통신부, 형식적으로는 국가 보안의 총괄 기구이지만 실질적으로는 국가 안보 및 기밀의 정보보호를 담당하는 국가정보원 간에 책임과 권한을 둘러싼 갈등의 발생소지가 존재하는 것이다. 또한 각 부처 산하의 정보보호 관련 기구들과 법집행을 맡고 있는 검찰과 경찰, 국방관련 정보보호를 담당하는 국방부, 민간 부문의 정보보호 관련 기구들까지도 고려할 때 국가 전체의 정보보호를 총괄적으로 조정하는 보다 강력한 정보보호 총괄기구를 만드는 것이 필요하다.

새로이 설립할 정보보호 총괄 조정기구로 선택될

수 있는 대안들로는 정보화추진위원회의 기능 강화를 통한 정보보호 조정기능 부여, 국무총리를 위원장으로 하는 정보보호 총괄 조정기구 설립, 대통령 직속의 정보보호 총괄 조정기구 설립 등이 제시 될 수 있다.

정보화추진위원회의 기능강화 방안은 정보화추진위원회의가 국가정보화 기능의 일부로 정보보호 업무를 다루기 때문에 상대적으로 그 비중이 약화될 수 있다는 단점이 있다. 그리고 국무총리를 위원장으로 하는 정보보호 총괄 조정기구는 그 성격상 권한과 자원의 동원 면에서 대통령 직속 보다는 상대적으로 약하기 때문에 빠른 시일 내에 전자정부 정보보안체계 및 대책을 수립하고 집행하기에는 미약하다고 볼 수 있다. 미국의 사례에서 보듯이 대통령 직속으로 정보보호위원회를 설치하는 것이 다양한 부처 및 기관, 민간기업 및 민간 분야의 관련 기관들을 총괄적으로 조정하고 지원할 수 있는 강력한 권한과 자원의 동원능력을 갖출 수 있다는 점에서 가장 이상적인 대안으로 판단된다.

그러나 대통령 직속으로 설치하는 것은 장기적으로 대통령의 관심 여하에 따라 형식적인 기구로 전락할 가능성이 높으며, 대통령에게 너무 많은 책임을 집중시키고 있다는 점에서 문제점이 지적될 수 있다.

따라서 정보보호에 대한 사안의 시급성 면에서, 그리고 초기 단계에서 강력한 권한과 자원동원을 통해 정보보호 대책을 수립하고 집행하여야 한다는 점에서 단기적으로는 대통령 직속으로 정보보호 관련 총괄조정기구를 설치하는 것이 바람직하다. 그리고 초기 단계의 정보보호정책이 패도에 오르게 되면, 안정적으로 정보보호 관련 정책에 대한 총괄 조정을 할 수 있는 국무총리를 위원장으로 하는 기구를 설립하는 것이 바람직하다고 본다.

신설되는 대통령 직속 (가칭)정보보호위원회는 각료급 위원회로 구성하되, 그 위원장은 대통령에게 직접 자문이 가능한 정보보호 전문가가 선임될 필요가 있다. 그리고 위원회 산하에 실무위원회를 설치하고 (신설이 필요한)정보보호 담당 대통령 특별 비서관이 그 위원장을 겸임하도록 함으로서 정책결정 및 조정, 그리고 그 집행에 있어 강력한 권한과 자원 동원을 가능하게 할 필요가 있다.

또한 신설되는 대통령 직속 정보보호위원회는 그 기능이 국가안보 및 대테러 정책과 밀접한 연관이 있기 때문에, 국가안전보장회의 및 '국가대테러 대책회의'와의 긴밀한 협조관계를 유지할 필요가 있다. 그리고 실무위원회 산하에는 정보보호 관련 세부 분야별로 상임위원회 및 특별 위원회를 설치하여 구체적인 쟁점 사항에 대하여 실무적인 논의와 조정 작업을 수행할 필요가 있다.

2.2. 정보보안 정책네트워크의 제도화

본 연구는 정보보호 정책 총괄기구인 대통령 직속 정보보호위원회의 신설을 전재로 정보보호 기관간 다원적 협력체계를 강화하기 위한 방안을 논의하고자 한다. 즉, 새로운 정책네트워크의 구심점 역할을 하는 신설기구를 축으로 한 정부내 정보보호기관간 정책네트워크의 강화, 정부와 민간부문의 정보보호 네트워크 및 국가간 정보보호 협력네트워크의 발전 방향에 대해 논의하고자 한다.

2.2.1. 정부내 정책네트워크의 강화 : 정보보호 기관간 연계관계 강화

정보보호정책의 성공적이고 안정적인 추진을 위해서는 우선적으로 산재해 있는 정부내 정보보호기관간 연계를 강화할 수 있는 네트워크를 구축할 필요가 있다. 이를 위해서는 먼저 각 정보보호 기관의 역할을 명확히 정립할 필요가 있으며, 이를 토대로 이들 기관간의 연계 및 협조 체제를 공고히 할 수 있는 대안을 마련할 필요가 있다.

현재 정보보호 관련 주요 기관들로는 국가정보원, 행정자치부, 정보통신부, 한국정보진흥원, 국가보안기술연구소, 검찰 및 경찰의 사이버범죄수사센터 등이 있으며, 범정부기관으로 정보통신기반보호위원회와 국가대테러 대책회의 등이 있다. 우리나라 정보보호 정책의 문제점으로 지적되었듯이 이들 각 관련 기관간 이해관계가 충돌하여 실질적인 협력이 부족할 수 있다. 또한 이들 기관간 업무의 관할 영역이 중복됨으로써 갈등 및 정책혼선 등의 문제점이 발생할 수 있다.

따라서 국가 전체의 정보보호를 확보 및 향상시킬 수 있는 차원에서 이 들 기관간의 업무영역을 명확히 재정립하고, 이를 토대로 한 연계관계를 설정할 필요가 있다.

국가적 차원에서 보호되어야 할 정보 및 시스템(시설 포함)은 정부 및 공공기관의 정보시스템과 민간부문의 주요 정보시스템으로 구분될 수 있다. 또한 정부 및 공공기관의 정보시스템은 국가 안보 및 기밀 관련 정보시스템과 일반 정부 정보시스템으로

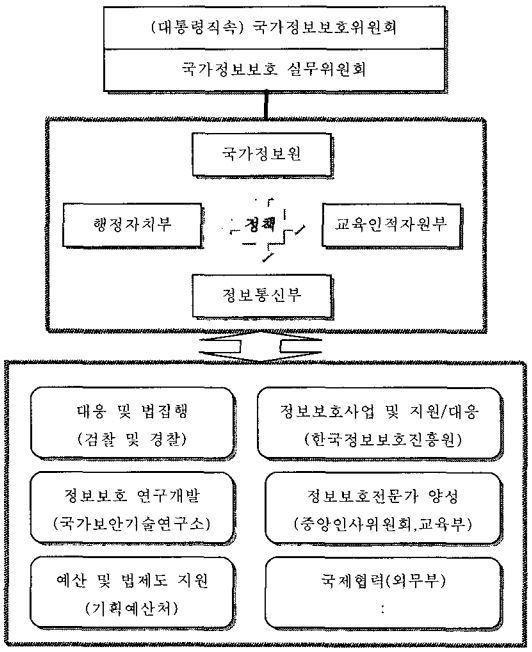
구별될 수 있다. 현재 국가정보원은 정부 및 공공기관의 정보보안 관련 총괄기구로서 역할을 수행하고 있으며, 행정자치부도 중앙부처 및 지방자치단체의 정보보안 관련 업무를 수행하고 있다. 다만, 정보통신부는 주로 민간과 정부의 영역이 만나는 부문과 주요 정보통신기반시설에 대한 정보보호 업무를 수행하고 있으며, 점차 정부 및 공공기관에도 그 영역을 확장하고 있다. 이러한 과정에서 부처간 갈등이 나타나고 있으며, 상호간의 협력도 적극적으로 진행되고 있는 것 같지는 않다.

본 연구에서는 이러한 세 기관의 업무영역을 구체적으로 정립하기는 어렵지만, 그 기본방향과 조정방안을 제시하고자 한다. 우선적으로 국가 전체의 정보보호관련 총괄 및 조정기구는 신설되는 대통령 직속 정보보호위원회가 수행하며, 정보보호 관련 기관의 업무영역에 대한 갈등이 있을 경우에는 이를 조정하는 역할을 수행하여야 한다. 국가정보원은 정부 및 공공기관에 대한 정보보안 총괄기구이기는 하지만, 그 핵심역량을 국가안보 및 국가 기밀 관련 정보시스템에 대한 보호로 집중하여 그 효과성과 능률성을 향상시키는 것이 바람직할 것이다. 그리고 일반적인 정부 및 공공기관에 대한 정보보호 문제에 관하여는 행정자치부와 협의하여 자문 및 기술지원을 수행할 필요가 있다. 다만, 국가안보 관련 업무 중 국방관련 정보보호 문제는 현재 국방부에서 담당하고 있다. 국방관련 정보보호 대책은 본 연구에서는 논외로 하고자 한다.

국가안보 및 기밀 관련 정보시스템을 제외한 일반적인 정부 정보시스템에 대한정보보호정책은 국가정보원의 협조하에 행정자치부에서 관리할 필요가 있다. 특히 상대적으로 보안이 취약한 지방자치단체에 대한 정보보호에 대해 좀 더 많은 관심을 기울일 필요가 있다. 또한 가장 취약한 공공기관으로 나타난 교육기관에 대한 정보보호정책은 교육인적자원부에서 국가정보원의 협조하에 관리할 필요가 있다.

정보통신부는 정부와 민간부문이 만나는 부문, 특히 주요 정보통신기반시설에 대한 보호정책을 관리한다. 다만, 이 과정에서 행정자치부 및 국가정보원과의 긴밀한 협조관계를 필요로 한다. 이러한 협조 및 조정을 '정보보호위원회'에서 주관하여 합리적인 결론을 도출할 필요가 있다. 정보통신부는 특히 정보보호위원회와 협조하여 민간부문에 대한 정보보호 지원 및 상담업무도 수행할 필요가 있다.

이제까지 국가정보보호 관련 정책 및 지침 개발 및 집행관리에 대한 주요 관련 기관의 책임 영역과 그 연계를 위한 조정방안에 대해 논의하였다. 이를 그림으로 간단히 표현하면 〔그림 2〕와 같다.



〔그림 2〕 국가정보보호 관련 체계도

정보보호 침해사고가 발생할 경우 이에 대한 대응업무는 현재 국가정보원의 정보보안119와 한국정보진흥원의 해킹바이러스상담지원센터에서 주로 담당하고 있다. 국가정보원의 정보보안119는 정부 및 공공기관(교육기관 포함)의 침해사고에 대한 대응업무를 수행하고 있으며, 정보통신부의 한국정보진흥원은 개인 및 기업 등 민간부문의 해킹 및 바이러스 대응업무를 수행하고 있다. 이러한 역할 분담은 현 시스템에서 당분간 유지되는 것이 바람직하다고 본다.

다만, 두 기관간의 정보공유 및 협조는 국가기밀과 관련되지 않는 한 적극적인 관계로 발전될 필요가 있다고 본다. 이 두 기관간의 정보공유 및 협조 차원에서 국가정보보호위원회의 조정을 통해 긴밀한 네트워크 관계를 형성할 필요가 있다.

검찰 및 경찰의 사이버 범죄 센터는 침해사고에 대한 신속한 수사 및 법집행을 더욱 향상시킬 필요가 있다. 이를 위해서는 컴퓨터 관련 범죄 수사를 전담할 전문인력과 첨단 수사장비를 갖추기 위한 예산을 확보할 필요가 있다. 국가정보보호위원회의 조정 및 기획예산처의 협의를 거쳐 우선적으로 이 분야에 대한 적절한 예산확보가 우선될 필요가 있다.

또한 전문수사인력을 확보하기 위한 적극적인 인사 및 교육 대책을 마련하여야 한다. 그리고 효과적인 수사를 위해 접속기록의무화 등 개인의 사생활을 과도하게 침해하지 않는 범위에서 효율적인 수사를 할 수 있는 법적·제도적 장치를 마련할 필요가 있다.

기타 정보보호기술 연구개발 총괄 기구로서의 국가보안기술연구소, 정보보호전문가 양성 업무를 주관하는 중앙인사위원회 및 교육인적자원부, 정보보호 관련 예산 및 법제도 지원을 담당하는 기획예산처, 정보보호 관련 국제협력을 지원하는 외무부 등 각 관련 기관들은 정보보호를 위한 굳건한 기반구축을 위한 역할을 효과적으로 수행할 필요가 있다. 이들 기관의 역할에 대해서는 아래에서 보다 구체적으로 다루기로 한다.

2.2.2. 정부-민간 부문간의 정보보호 네트워크

국가 정보보호는 정부 단독으로 수행하는 일이 아닌 기업, 개인, NGO 등 모든 국가 구성원의 적극적인 동참을 필요로 하는 일이다. 따라서 모든 국가 구성원의 협력을 유도해 낼 수 있는 대안을 마련할 필요가 있다. 우선적으로 정보보호 중요성에 대한 대국민 홍보 및 인식 제고를 위한 노력을 기울일 필요가 있다. 이에 대해서는 뒤에서 자세히 논의하기로 한다.

다음으로 주의를 기울여야 할 부문은 정보보호 과정에서 발생할 수 있는 개인의 권리(자유권, 사생활 보호권, 사유데이터보호 등)를 보호하기 위한 제도적 장치를 마련할 필요가 있다. 이는 개인의 권리침해에 대한 우려로 인해 정보보호정책에 대한 반발 및 비협력이라는 저항에 부딪힌 다면, 정보보호정책 목표의 효과적인 달성이 어렵게 될 가능성이 높기 때문이다.

따라서 국가정보보호위원회는 매년 정보보안과 시민권에 대한 토론회 개최, 시민단체와 공동으로 '정보보호백서' 발간 등 정보보호에 대한 인식제고 및 진지한 토론의 장을 마련할 필요가 있다. 그리고 시민단체, 산업계, 학계 등의 인사들로 구성된 위원회를 구성하여 시민의 자유, 사생활 보호, 사유데이터 보호 등의 관점에서 정보보호정책을 검토할 수 있는 제도적 장치도 마련할 필요가 있다.

2.2.3. 초국가 정보보호 네트워크 강화 : 국제 협력 강화

정보보안 침해사고 즉, 해킹이나 사이버 공격은 인터넷을 타고 국경을 초월하여 행해지고 있으며, 그 추세는 갈수록 증가하고 있는 추세이다. 특히 초고속망 등 국내 인터넷 이용환경의 편리성이 증가하면서 국외로부터 침입되는 사례가 증가하고 있다. 실제 국내 정보시스템 침해사고의 상당부문이 국외 해커에 의해 이루어지고 있다.

따라서 국경을 넘어 행해지고 있는 공격에 적절히 대처하기 위한 국제적인 제휴를 추진하는 것이 필요하다. 우선적으로 침해사고, 취약점 등 정보보안 관련 정보를 국외의 정보보안 관련 기관들로부터 체계적이고 지속적으로 수집할 수 있는 시스템을 구축하고 이를 위한 여러 나라 관계기관의 제휴 강화를 추진할 필요가 있다. 또한 사이버 테러 대책과 관련된 국제적인 노력에 적극 동참할 필요가 있다. 예를 들면, 정보보안의 선진국이라 할 수 있는 미국의 정보보호기관(NSA, NIPC 등) 및 CERT/CC 등과 같은 국제적인 기구들과 제휴관계를 맺어 신속한 정보수집, 분석, 제공(공유), 대응, 정책수립 등을 향상시킬 필요가 있다.

한편으로는 해커 등 컴퓨터 범죄자에 대한 국제적인 공조 수사체제가 이루어질 필요가 있다. 관련되는 법규와 범죄자 인도법 등이 상호 체결되어 국제적인 사이버 범죄에 적절히 대응할 필요가 있다. 그리고 국제컴퓨터침해사고대응협의회(FIRST)와 긴밀한 협조체계를 구축하여 각 나라별로 암호 기술 및 해킹 기술 등의 정보를 교환함은 물론, 이러한 협력을 통해 국제적인 해커를 끝까지 추적하여 퇴치할 수 있도록 하여야 한다.

2.3. 자체 정보보호 기능 강화 : 중앙부처를 중심으로

전자정부 정보보호를 성공적으로 수행하기 위해서는 우선적으로 각 부처 및 기관 자체 차원에서 정보보호 기능을 강화할 수 있는 대책을 수립할 필요가 있다. 정보보호는 정보화추진 즉, 전자정부 구현을 위한 필수적인 요소임을 인식하고 이에 대한 조직적, 제도적, 예산적 차원에서 적극적인 관심과 노력을 기울일 필요가 있다.

이를 위해서는 각 부처 및 기관은 우선적으로 자체 정보보호정책을 수립할 필요가 있다. 각 기관별 세부 정보보호정책을 수립할 경우에 국가정보보호위원회는 관련 기관 및 전문가의 협조를 얻어 각 기관의 정보보호정책 수립을 지원하고 이에 대한 검토작업을 수행할 필요가 있다. 또한 영국에서 정보보호 관리 국제 표준인 ISO17799(BS7799)를 모든 정

부 부처에서 도입하도록 촉진하는 정책을 수행하고 있듯이 우리나라 정부에 맞는 적절한 정보보호관리 표준을 제정하여 각 부처 및 기관이 이를 인증 받도록 권고할 필요가 있다.

다음으로 정보통신기반보호법에서 요구하고 있는 정보보호책임관 및 정보보호책임자를 실질적인 전문가로 채용할 필요가 있다. 또한 단순히 주요정보통신기반시설의 보호에 관한 업무만 총괄 할 것이 아니라, 기관 전체의 정보보호업무를 총괄하고 그 기관과 긴밀한 연계관계를 맺고 있는 민간부문에 대한 지원 및 협력 업무도 수행하게 할 필요가 있다. 이를 위해서는 정보보호책임관은 실질적인 권한과 기관장의 적극적인 지원이 필요하다. 현재 법에서 4·5급 공무원 또는 임원급 관리·운영자를 정보보호책임자로 지정하도록 되어 있는 데, 그 중요성에 비추어 볼 때 이들의 직급을 격상할 필요가 있다. 또한 현재 부처 내에는 이러한 직무를 수행할 수 있는 전문가가 매우 부족하기 때문에 외부에서 특별채용 하거나, 단기적으로 신뢰할 수 있는 민간업체에게 아웃소싱을 주는 방안도 고려할 필요가 있다.

또한 정보보호책임자는 정보화 추진을 맡고 있는 각 기관의 CIO와 긴밀한 협력관계를 유지하여야 하며, 정보보호 추진 실태에 대한 보고를 기관장 및 국가정보보호위원회에 함으로써 국가 전체차원의 정보보호 정책과 조율을 맞출 필요가 있다. 한편, 각 기관의 정보보호에 대한 감사를 각 기관의 감사담당관이 매년 주기적으로 수행하여 이의 결과를 국회 및 기획예산처, 국가정보보호위원회에 보고토록 함으로써 실질적인 통제장치를 마련할 필요가 있다. 또한 이의 결과를 기관평가 및 예산에 반영토록 함으로써 각 기관이 자체적으로 최선의 노력을 기울일 수 있도록 하여야 할 것이다.

그리고 각 주요 부처 및 기관별로 침해사고대응팀(CERT)을 편성·운영하면서, 각 기관이 자체적으로 정보시스템에 대해 정기적인 보안진단을 실시하고 침해사고 발생에 따른 세부적인 대응절차 지침서를 마련하여 시행할 필요가 있다. 특히 기관 내부 네트워크와 인터넷의 연계점에 대한 보안대책 뿐만 아니라 정부기관간 네트워크 연계점에 대한 보안대책도 수립할 필요가 있다. 취약한 기관을 경유지로 하여 정부 전체 기관에 대한 침해공격도 가능하기 때문이다. 예를 들면, 현재 대부분의 정부 및 공공기관은 내부 네트워크를 인터넷에 연결할 때 침입차단 및 탐지시스템을 설치하는 등 보안대책을 마련하여 운영하고 있으나, 기관간 네트워크 또는 정부고속전산망에 연결할 때에는 보안이 취약한 기관을 경유지로 하여 타 기관의 네트워크 및 정부고속전산망에 침입할 가능성이 있는 것이다. 따라서 각 기관간 네트워크 및 정부고속전산망이 연결되는 지점에 침입차단 및 탐지시스템 등을 설치하는 등 보안대책을 마련할 필요가 있다.

3. 전자정부 정보보안 추진기반 구축

3.1. 연구개발 투자 강화

전자정부 정보보안을 위해서는 정책적·관리적 대책도 중요하지만, 중요 핵심기술의 연구개발 능력이 보다 우선시 될 필요가 있다. 특히 정보전 등 국가간의 관계에서 국가 기밀정보 보호를 위해서, 나아가 정보보호산업의 양성 차원에서 국가 자체적으로 정보보안 기술을 보유하는 것이 매우 중요하다고 할 수 있다.

현재 우리나라가 보유하고 있는 정보보안 기술로는 급격하게 발전하고 있는 보안침해에 대해 실질적이고 효과적으로 대처하는 데에는 많은 한계를 가지고 있다. 이러한 점은 선진국인 미국도 예외는 아니다. 따라서 미국의 경우도 정보보안 대책을 집행하는 데 필요한 보안기술 개발에 대한 막대한 노력을 진행 중에 있다.

미국에 비해 어느 정도 뒤 떨어져 있는 우리나라 보안기술의 현 주소를 고려할 때, 보안기술에 대한 적극적인 지원과 관심, 노력을 기울일 필요가 있다. 이를 위해서는 우선적으로 국가정보보호위원회는 국가보안기술연구소와 협의하여 전자정부 정보보호에 필요한 정보보호기술 들을 정의하고, 이 들의 우선순위를 결정할 필요가 있다. 이를 토대로 기획예산처의 협조를 얻어 예산 및 기금을 마련하여 적극적인 투자를 할 필요가 있다.

또한 제도적으로는 체계적이고 효과적인 연구개발 투자를 위해 보안기술 연구 총괄기구를 지정할 필요가 있다. 현재 우리나라는 정보보호 연구개발능력이 분산되어 있으며, 전략적 차원에서 체계적인 연구개발이 이루어지고 있지 않은 실정이다. 따라서 국가보안기술연구소와 같은 기관이 보안기술연구 총괄기구로서의 역할을 수행하여 전략적이고 체계적인 연구개발투자가 이루어지도록 하는 것이 바람직하다. 기존에 수행하고 있던 국가 및 공공기관의 정보시스템 보호에 필요한 연구개발 및 국가기밀 관련 연구

개발을 지속적으로 수행할 뿐만 아니라, 국가에서 수행할 필요가 있는 즉, 민간분야에서는 할 수 없으나 꼭 필요한 정보보호관련 연구에 대한 총괄 조정 및 자금 배분 기능을 수행하도록 할 필요가 있다. 현재 각 부처별로 산발적으로 진행되고 있는 정보보호 관련 연구개발 투자를 국가보안기술연구소에서 일괄적으로 통제하여 국가 정보보호라는 전략적 차원에서 체계적으로 연구개발이 이루어 질 수 있도록 하여야 할 것이다.

향후 사이버 테러는 물론 국가간 정보전의 형태로 발전할 가능성이 높기 때문에, 특히 북한과의 적대적 관계에 있는 현 상황에서 국가안전보장(국방 및 기밀) 관련 정보보호 대책은 매우 심각하게 고려될 필요가 있다. 현재 국가안전보장 관련 정보보호 업무는 국가정보원과 국방부가 수행하고 있으나, 이들에 대한 전문적 기술지원이 상대적으로 부족한 것으로 판단된다. 특히 미국의 NSA, 영국의 GCHQ와 같이 국가안전을 위한 암호해독 및 암호화를 통한 정보수집, 분석, 보호능력을 지원하는 기관이 우선적으로 필요하다. 예를 들면 미국과 영국 등은 '에셜론' 프로젝트를 통해 국가안전보장과 관련된 정보를 인터넷 등 정보통신망을 통해 지속적으로 수집 및 분석하고 있는 것으로 보도되고 있다.

이러한 측면에서 우리나라는 기술과제도, 예산 차원에서 상대적인 열세에 있는 것으로 보인다. 따라서, 장기적 관점에서 국가보안기술연구소를 미국의 NSA, 영국의 GCHQ와 같은 기관으로 발전시킬 필요가 있다. 이를 위해서는 전문가 양성, 관련 기술 개발, 슈퍼컴퓨터와 같은 첨단 장비 도입 등 막대한 예산과 국가차원의 지원이 요구된다고 볼 수 있다. 또한 미국의 NSA 등과 같은 기관과 국제적인 제휴를 맺어 선진기술 및 정보를 습득하고 발전시켜 나갈 필요가 있다. 이를 위해서는 장기적인 전략을 수립하여 지속적이고 체계적으로 발전시켜 나감은 물론, 국가정보원, 국방부, 기획예산처 등의 적극적인 협조와 지원, 활용이 요구된다고 본다.

3.2. 정보보안전문가 양성 : 정보보안 교육 및 훈련

전자정부 정보보호를 위해서 가장 시급히 해결해야 할 문제점으로 떠오르는 것이 정보보호전문가 충원 문제이다. 정부는 물론 민간부문에도 이들 정보보호전문가의 인력이 절대적으로 부족한 상황이기 때문에, 정보보호에 대한 강한 의지를 가지고 있다 하더라도 이를 제대로 수행할 수 없는 것이 현실이다. 전자정부 정보보호를 위해서는 무엇보다도 잘 훈련된 정보보호 전문인력 필수적이다.

따라서 정보보호 전문가를 시급히 양성하기 위해서는 몇 가지 차원에서 대책을 세울 필요가 있다. 우선 단기적으로는 정부에 있는 기존 IT인력에 대한 훈련에 집중할 필요가 있다. 기존 IT.기술자 들 중에 정보보호에 자질이 있는 자들을 선발하여 집중적인 교육과 훈련을 통해 정보보호 전문가로 양성할 필요가 있다. 국가정보보호위원회는 중앙인사위원회의 협조 및 한국정보보호진흥원/국가보안기술연구소의 지원을 받아 선발된 인력에 대한 단기간의 집중적인 교육훈련을 통해 정보보호전문가로 변신시킬 수 있는 계획을 수립하여야 할 것이다. 이와 더불어 모든 공무원들에게 사이버 위협을 인지하고 대처할 능력을 배양하는 정보보호 인식제고 사업을 전개함으로써 인력기반을 공고히 할 필요가 있다. 이를 위해 CD-ROM, 비디오, 워크샵, 시연회, 온라인 교육 등 각종 시청각 교육재료와 프로그램을 활용하여 공무원들에 대한 정보보호 훈련을 수행할 필요가 있다. 그리고 정보보호자격증을 소지하고 있는 자에게는 승진시 가산점을 부여하는 방안 등을 마련하는 것도 대안으로 고려해 볼 만 하다.

한편, 중앙인사위원회는 정부에서 필요한 정보보안 전문가의 수요와 필요 기술을 분석하여 인력을 모집, 선발, 배치, 훈련하는 데 기본적인 정책자료로 활용할 필요가 있다. 또한 기존 IT 관련 공무원에 대한 훈련으로도 필요한 전문 인력을 충원할 수 없을 경우에는 외부에서 이들 전문가를 특채할 수 있는 방안을 마련할 필요가 있다. 경우에 따라서는 아웃소싱 형태로 외부 인력을 활용할 필요가 있다.

장기적으로는 우수 정보보호 전문가 양성 및 현직 정부기관 정보보호 전문인력의 훈련을 위하여 각 대학의 우수 정보보호교육센터를 지정하여 지원하고, 지정된 센터에서는 정보보호를 위한 전문교육을 시행토록 할 필요가 있다. 이러한 맥락에서 대학 및 대학원 과정에 정보보호 관련 과목 또는 학과를 개설함으로써 향후 정보기반시스템 침해대응에 필요한 전문인력을 단계적으로 양성할 수 있도록 지원하여야 하며, 추가적으로 산·학·관이 공동으로 필요한 정보보호 교육프로그램도 개발할 필요가 있다.

미국의 경우 정부가 필요로 하는 정보보호 전문인력을 양성·유치하기 위해서 정보보호를 전공하는

대학생과 대학원생들에게 장학금을 수여하는 장학금 제도를 시행하고 있다. 장학생으로 선발된 학생들은 2년간의 등록금 등 학비 일체와 생활비를 장학금으로 수여 받지만, 졸업 후에 2년간 연방정부 기관에서 정보보호 전문가로 근무할 것을 조건으로 하고 있다.[10] 우리나라도 미국의 이러한 제도를 참고하여 각 대학의 우수 정보보호교육센터 재학생 등을 대상으로 장학금을 수여하고 이를 토대로 우수 인력을 유치하는 계획을 세울 필요가 있다.

한편, 정보보호 전문 인력을 초기부터 발굴·육성하기 위하여 중·고등학교 학생들과 교사들을 대상으로 한 정보보호 교육 및 인식제고 활동을 전개할 필요가 있다. 국가정보보호위원회는 교육인적자원부와 협의하여 중·고등 학생을 대상으로 한 정보보호 교육과 홍보 계획을 수립하고 이를 지원하기 위한 방안을 마련할 필요가 있다. 더 나아가 대국민 홍보 및 정보보호 마인드 확산 차원에서 관련 학회나 연구기관을 통한 심포지엄을 개최하는 등 정보보호 관련 저변인구를 확대할 필요가 있다.

3.3. 정보보안 홍보를 통한 대국민 인식 제고

전자정부 정보보호를 위한 정책이 지속적으로 효과를 산출하기 위해서는 공무원이나 일반 시민들을 대상으로 한 정보보호 교육·홍보활동이 전제되어야 한다. 이러한 정보보호 교육·홍보활동은 공무원들이나 일반 국민들에게 정보보호가 지니는 중요성을 분명하게 전달하는 수단이기 때문이다.

교육·홍보의 활성화를 유도하는 구체적 대안으로, 우선 공무원들을 대상으로 한 교육·홍보기능의 강화방안을 생각해 볼 수 있다. 우수 정보보호 전문가 및 정보보호 우수 사례를 발굴하여 특별 포상 및 승진 혜택을 부여하는 제도를 실시하고, 아울러 전 공직자를 대상으로 정보보호 교육을 체계적으로 실시하여 정보보호 마인드를 심어줄 필요가 있다.

다음으로 일반 국민들을 대상으로 한 교육·홍보기능의 강화방안으로는 정보보호 관련 세미나의 개최, 정보보호 광고 및 홍보책자 발간, 정보보호 백서 발간, 인터넷이나 PC통신을 통한 정보보호 정보 제공, 중·고등학교 교과과정에 정보보호 관련 내용의 추가 등을 들 수 있다. 또한 미국의 사이버 시티즌 운동에서 시사 받을 수 있듯이, 청소년 및 일반 네티즌들을 대상으로 사이버 공간에서 건전한 시민의식을 함양시키는 운동을 전개할 필요가 있다.

3.4. 예산 및 법제도적 지원

정부에서 어떤 정책을 수립하고 집행하는 데 있어서 필수적으로 확보되어야할 것이 예산과 법제도적 지원이다. 기본적으로 예산이 지원되지 않거나, 법률적으로 근거하지 않은 정책은 현실적으로 그 효과를 거두기는 거의 어렵다. 더군다나 기존의 법률이 새로운 정책을 시행하는 데 장애가 된다면 그 정책의 성공가능성은 매우 희박하다고 볼 수 있다.

전자정부 정보보호 정책도 예외일 수는 없다. 특히 정보보호 정책은 그 성격상 막대한 예산을 필요로 하는 정책이기 때문에 예산 당국의 적극적인 지원이 없이는 정책의 실효를 거두기는 매우 어렵다고 볼 수 있다. 따라서 국가정보보호위원회는 기획예산처와의 긴밀한 협의를 통해 정보보호 관련 예산을 적절히 확보할 수 있는 권한을 보유해야 함은 물론 예산 확보를 위해 많은 노력을 기울일 필요가 있다.

또한 정보화의 급격한 발전과 더불어 그 침해기술도 급속히 발전하고 변화하고 있는 추세이다. 따라서 시기 적절한 법률 제정 및 개정이 없이는 정보보호를 위한 효율적인 정책집행을 하기가 어렵다. 국가정보위원회는 이러한 법률문제를 전담하는 상임위원회를 설치하여 지속적으로 정보보호 관련 법률들을 검토하고 시기적절한 법률 제정 및 개정작업에 노력을 기울일 필요가 있다.

Ⅳ. 결 론

우리는 그 동안 급격히 변화하는 정보통신기술을 적극적으로 받아들여 정보 인프라 구축 및 인터넷 사용자 수에 있어서 세계 일류국가 수준에 이르렀다. 그러나 이러한 정보 인프라 수준에 맞는 전자정부 구축은 아직도 많은 노력을 필요로 하고 있다.

"최고수준의 對국민서비스 제공", "최적의 기업환경 제공", "생산성·투명성이 높은 정부 구현"이라는 전자정부의 비전[7]을 성공적으로 달성하기 위해서는 다양한 각도에서 많은 노력을 기울여야 하겠지만, 무엇보다도 철저한 정보보안을 바탕으로 한 전자정부 서비스의 신뢰성을 확보할 필요가 있다.

본 연구는 전자정부의 정보보안을 확보하기 위한 차원에서 국가 전반에 걸친 체계적이고 종합적인 정보보안 대응체계를 제시하고자 하였다. 전자정부 정보보안 대응체계의 기본방향을 제시하고, 이를 토대로 전자정부 정보보안 추진체계의 정비와 전자정부 정보보호 추진기반 구축이라는 두 차원에서 제도적

정책대안을 제시하였다.

정책은 제도와 사람 그리고 기술이 조화롭게 운영되어야만 성공할 수 있다. 아무리 좋은 제도가 있어도 이를 운영하는 사람이나 이에 적합한 기술이 받쳐주지 않는다면 그 제도의 효과는 크게 나타나지 않을 것이다. 특히 중요한 것은 제도를 운영하는 사람들의 마인드가 변하지 않으면 그 제도의 효과가 반감될 수 있을 뿐만 아니라 극단적으로는 정책의 실패로 이어질 수 있다. 따라서 정부조직을 구성하고 있는 구성원들이 정보보안에 대한 필요성을 깊이 인식하고, 이에 필요한 지식 및 기술을 습득함은 물론 이를 습관화할 수 있도록 하여야 할 것이다.

참 고 문 헌

[1] 국가정보원, "2000년도 국가·공공기관 해킹사고 5.7배 급증", *http://www.nis.go.kr/119*, 2001.

[2] 국가정보원, "2001년도 국가·공공기관 해킹사고 현황 및 통계". *http://www.nis.go.kr/119*, 2002.

[3] 박정현, "국내 해킹사고 분석 및 대응기술", *제6회 정보보호 심포지엄*, 2001.

[4] 신영진, "국가·공공기관 해킹사고 현황 및 지원", *제6회 정보보호 심포지엄*, 2001.

[5] 안성일, "정보통신기반보호법 주요내용 및 시행방안", *제6회 정보보호 심포지엄*, 2001.

[6] 이진수, "국가·공공분야 사이버테러 대응 종합대책", *제6회 정보보호 심포지엄*, 2001.

[7] 전자정부특별위원회, *세계일류국가 도약을 위한 전자정부구현 전략*, 2001.

[8] 정보보호산업협회, *국내·외 해킹 등 사이버테러 사례분석 및 피해규모 분석에 관한 연구*. 한국정보보호센터, 2000.

[9] 정현철, "2001년 해킹·바이러스 사고를 돌아보며", *정보보호뉴스*, 통권54호, 2002.

[10] 정휴붕, "미국 정보보호 인력양성 정책동향", *제6회 정보보호 심포지엄*, 2001.

[11] 한국인터넷정보센터, *한국인터넷통계집*, 2002.

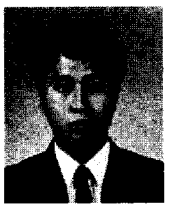
〈著 者 紹 介〉

안 문 석 (Ahn, Moon Suk)

서울대학교 경제학과(경제학사)
서울대학교 행정대학원(행정학 석사)
University of Hawaii(컴퓨터학 석사)
University of Hawaii(자원경제학 박사, 시스템분석전공)
한국과학기술연구원(KIST) 전산시스템개발실장 역임
한국정책학회 회장 및 한국행정학회 부회장 역임
고려대학교 행정문제연구소 소장, 기획처장, 정책대학원장 역임
미국 Syracuse University, Maxwell School of Citizenship and Public Affairs, 객원교수 역임
전자정부 특별위원회 위원장 역임
현재 고려대학교 행정학과 교수
현재 규제개혁위원회 위원장 역임
현재 고려대학교 교무부총장

박 성 진 (Park, Sung Jin)

고려대학교 학사,석사,박사
현재 경인여자대학 컴퓨터정보기술학부 부교수
관심분야 : 정보체계, 정보정책



맹 보 학 (Maeng, Bo Hak)

고려대학교 박사수료
현재 경인여자대학 조교수
관심분야 : 전자정부, 조직간 네트워크