미 국방성의 종심방어전략과 전자정부의 정보보호전략에 관한 비교 연구

송 운 호[†] · 정 욱 재[††] · 김 준 범[††] · 강 한 승[††]

요 약

정보화 시대가 도래함에 따라 세계 각국이 전자정부 구현에 많은 관심을 갖고 있으며, 이미 몇몇 선도 국가들은 다양한 민원서비스 및 행정서비스를 인터넷을 통해 국민들에게 편리하게 제공하고 있다. 본 연구에서는 미 국방성의 종심방어전략(Defense-In-Depth Strategy)과 한국의 전자정부 정보보호전략을 비교·평가함으로써 더욱 안전하고 신뢰할 수 있는 전자정부 구현에 이바지 할 수 있는 기반을 제공하고자 한다.

키워드 : 전자정부, 종심방어전략, 정보보증, 정보보호

A Comparative Study on the Information Security Strategy of Korean E-Government with Defense-in-Depth Strategy of DoD

Woon-ho Song[†] · Wook-jae Jeong[††] · Joon-bum Kim[††] · Han-seung Kang[††]

ABSTRACT

Advanced countries overhaul government workflows using IT, which not only enhances efficiency and productivity, but paves the way to a "e-Government" offering prompt, quality service for citizens. This research analyzes the DiD(Defense-in-Depth Strategy) and compares the information protection strategy of Korean e-Government with DiD for reliable and safe e-Government's build.

Key Word : E-Government, Defense-In-Depth Strategy, Information Assurance, Information Security

1. 서 론

정보기술의 급격한 발전과 인터넷 이용 확산을 기반으로 각국 정부는 경쟁적으로 전자정부를 추진하고 있다. 우리정부도 2002년 11월 전자정부 단일창구를 개통하고 400여 종의 민원안내와 393종의 민원서비스를 인터넷으로 제공[1]하기 시작하여, 현재는 4,000여 종의 민원안내와 400여 종의 민원서비스를 제공하고 있다. 전자정부의 발전은 온라인 민원처리와 네트워크를 통한 비대면의 행정처리를 일반적인 현상으로 만들어 가고 있으며, 국민은 언제 어디서나 행정서비스를 받을 수 있도록 편의성을 제공받고 있다. 그러나 익명성과 비대면성이 상존하는 네트워크를 통한 국가 주요 정보 및 개인정보의 유통이 급증하면서 해킹, 바이러스 유포, 정보유출과 위·변조 등 각종 정보화 역기능에 의한 피해 가능성도 증가하고 있는 것이 사실이다[2, 3].

지난 2000년 초 세계 유명 사이트가 연이어 해커들에 의해 침입을 당하고, 9·11테러까지 발생하면서 많은 정보보호 관계자들이 대응에 고심하고 있으며, 이를 위해 정보보증을 통하여 목표를 달성하고자 많은 관심을 가지고 연구가 진행되고 있다[4, 5].

미국은 사이버 테러를 포함한 각종 테러에 대응하기 위해 최근 국토안보부를 설립하였으며, 민·관·군의 통합된 조직과 최신 기술을 발전시키기 위하여 국가적 차원의 정보보증 프로젝트를 추진하고 있고, 2002년 미국전략사령부(U.S. Strategic Command) 산하에 JTF-CNO(Joint Task Force-Computer Network Operations)를 운용해 공격(CAN) 및 방어(CND)임무를 수행하고 있다[3].

우리나라는 2001년 7월부터 주요 정보통신기반 보호법이 시행되고, 정부기관별로 정보보호를 위한 정책을 개발하고 기술을 발전시키고 있으나, 국가적 통합차원에서의 전략 개발은 미흡하다고 판단된다[4, 7].

이에 본 연구에서는 미 국방성의 정보보증 핵심 전략인 종심방어전략과 우리나라 전자정부 정보보호전략을 비교·평가하여 추후 전자정부 정보보증전략 수립방안을 제안한다.

† 정 회 원 : 서울정보통신대학원대학교 교수
†† 준 회 원 : 서울정보통신대학원대학교 석사
논문접수 : 2005년 2월 1일, 심사완료 : 2005년 7월 14일

2. 미 국방성의 종심방어전략(Defense-in-Depth Strategy)

(그림 1) 종심방어전략

미 국방성에서는 종심방어전략을 효과적인 정보보증을 위한 전략으로 채택하였다. 종심이란 군사용어로써 최전방 초소로부터 최후방 사령부에 이르는 거리를 의미한다. 따라서 종심방어란 전 지역을 방어한다는 것이다. 종심방어전략의 기본 원칙은 조직의 모든 정보시스템과 통신네트워크에 종심방어 전략을 적용하는 것이고, 실용적인 전략으로써 고도화된 응용 프로그램 개발기술과 보안공학을 이용하며, 보호능력의 수준과 비용, 성능, 운영 간의 균형을 잡도록 권고한다.

종심방어전략은 사람(People), 기술(Technology), 운영(Operation)의 세 가지 핵심 요소를 바탕으로 사이버 공격에 대해 방어계층을 형성한다[8].

2.1 사람(People)

정보보증의 성공은 인지된 위협에 대하여 확실한 이해를 통해 상위 수준(일반적으로 최고정보책임자 수준)의 정보관리 수행과 함께 시작된다. 정보관리 수행에 앞서서 효과적인 정보보증 방침 및 절차, 역할 및 책임의 할당, 자원의 할당, 주요 인원(예를 들면, 사용자 및 시스템 관리자)의 훈련 그리고 개인 책무의 시행이 확립되어야 한다.

이 단계는 시설과 IT 환경의 주요 요소에 대한 통제와 접근 제어를 위한 물리적 보안 및 인원 보안의 확립을 포함한다. 따라서 종심방어전략에서 사람이라는 핵심 요소는 좋은 사람을 고용하여 교육과 포상을 하고 권한이 없는 행위는 제재를 한다는 기본을 바탕으로 '방침과 절차', '교육과 인식', '시스템 보안 행정', '물리적 보안', '인원 보안', '시설 보호 대책'으로 구성되어 있다.

2.2 기술(Technology)

기술이라는 핵심 요소에서 취급되는 중요한 영역은 정보보증 아키텍처, 정보보증 평가기준(보안 평가기준, 상호운용성 평가기준, PKI 평가기준), 신뢰할 수 있는 제 3자에 의해 평가된 제품의 획득 및 통합, 시스템의 위험평가 등이 있다. 즉, 계층적 방어전략을 지원하기 위하여 신뢰할 수 있는 제 3자에 의해서 평가된 제품과 솔루션만을 적용해야 한다.

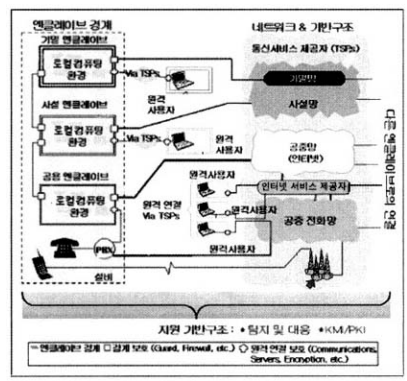
정보기반구조에서 모든 정보시스템은 보안상의 취약점을 가지고 있다. 이러한 취약점에 대처하기 위하여 종심방어전략은 기술이라는 핵심 요소 안에 정보보증기술프레임워크[8]를 포함하고 있다.

2.2.1 정보보증기술프레임워크

정보보증기술프레임워크는 미국 정부의 보안관련 부서와 보안관련 산업 벤더(Vendor)들의 요구에 의하여 NSA(National Security Agency)의 ISSO(Information Systems Security Organization)에 의해 개발된 정보보증기술프레임워크(Information Assurance Technical Framework)를 제시하는 문서로써, 현재 구축되어 운영되고 있는 정보체계 인프라의 약점을 해결하기 위한 일련의 활동인 정보보증에 대한 기술프레임워크이다.

정보보증기술프레임워크는 방어를 필요로 하는 영역을 나누고, 각 영역마다 방어체계를 구성하는 다양한 정보보증기술을 제시하였다. 종심방어전략은 각 영역마다 해당 영역 내의 전 범위에 걸쳐서 동일한 수준의 정보보증 강도를 적용시킬 필요는 없다. 조직은 각 정보 도메인이 필요로 하는 정보보증 수준과 강도에 맞게 정보보증체계를 구성할 수 있다. 즉 정보보증기술프레임워크를 이용하여 조직이 필요로 하는 수준의 정보보증 체계를 융통성 있게 구성 할 수 있다.

이러한 목적을 달성하기 위하여 정보보증기술프레임워크는 (그림 2)와 같이 네 가지 영역(로컬 컴퓨팅 환경, 엔클레이브 경계(Enclave Boundary), 네트워크 기반구조, 지원기반구조)으로 나누어 제시하였다[5].



(그림 2) 정보보증기술프레임워크 접근

2.2.2 로컬 컴퓨팅 환경(Local Computing Environment)

로컬 컴퓨팅 환경은 일반적으로 서버, 클라이언트와 이에 설치된 어플리케이션들을 말한다.

로컬 컴퓨팅 환경에서 살펴보면 고객들은 기본적으로 다양한 어플리케이션 분야에 정보보증 솔루션을 필요로 하고 있다. 로컬 컴퓨팅 환경의 보안은 주로 서버와 클라이언트에 설치된 어플리케이션과 호스트 기반 모니터링 능력에 초점이 맞추어져 있다. 일반적으로 정보보증 솔루션을 필요로 하는 어플리케이션은 다음과 같다.

· 메세징(E-mail)
· 운영체제
· 웹 브라우저
· 전자 결재
· 무선 접속
· 공동(collaborative) 컴퓨팅
· 데이터베이스 접근

로컬 컴퓨팅 환경은 엔클레이브와 동일한 의미로 사용된다. 엔클레이브는 근거리통신망(LAN : Local Area Network)을 통해 상호 연결된 로컬 컴퓨팅 장비들의 집합으로 동일한 보안방침에 의해 운영된다.

2.2.3 엔클레이브 경계(Enclave Boundary)

LAN을 통해 상호 연결된 다양한 컴퓨팅 장비들을 울타리처럼 둘러싼 지역이 엔클레이브이고, 엔클레이브 경계는 엔클레이브 내부 또는 외부로부터의 정보가 나가고 들어오는 접점이다. 각 엔클레이브들은 외부의 네트워크를 통해 다양한 연결이 이루어지기 때문에 엔클레이브 경계 보호막을 설치하여 외부 정보의 유입이 조직의 시스템 운용이나 자료에 영향을 미치지 않도록 해야 한다. 엔클레이브 경계보호를 위해 가드, 방화벽 등이 이용되며, 원격접속으로부터의 보호를 위해 암호화를 사용한다.

2.2.4 네트워크 기반구조(Network and Infrastructure)

네트워크 기반구조는 엔클레이브 간의 통신 능력을 제공한다. 네트워크 기반구조에는 사설망(Private Network), 공중데이터망(Public Network, 예를 들면 Internet), 공중전화망(Public Telephone Network) 등이 있다. 또한 네트워크 노드(예, 라우터, 스위치) 간에 정보전송을 위한 매체(유선, 위성, 극초단파, 무선 주파수 등)도 네트워크 기반구조에 포함된다. 네트워크 기반구조의 중요 요소로는 네트워크 관리센터, 도메인 네임 서버 그리고 디렉토리 서비스 등이 있다.

2.2.5 지원기반구조(Supporting Infrastructure)

정보기술 환경에서 지원기반구조의 역할은 시스템 보안관리와 보안서비스를 위해 네트워크, 엔클레이브 경계, 그리고 로컬 컴퓨팅 환경에서 공통적으로 지원되는 정보보증 메커니즘의 기초를 마련하는 것이다. 지원기반구조는 네트워크서비스, 컴퓨터사용자, 웹 서비스, 어플리케이션, 파일, 도메인네임서버와 디렉토리서비스 등에 보안서비스를 제공한다. 지원기반구조는 두 가지 하부 영역을 가지고 있다. 하나는 KMI(Key Management Infrastructure) /PKI(Public Key Infra-structure)이고, 다른 하나는 탐지 및 대응(Detect and Res- pond)이다.

(1) KMI /PKI

KMI는 암호화에 사용되는 키의 생성, 분배 및 분실 시 복구 등 암호키에 대한 관리 업무를 수행하는 하드웨어, 소프트웨어 및 정책 등으로 구성된 기반구조이다. PKI는 전자서명용키 및 인증서 관리를 위한 하드웨어, 소프트웨어 및 정책으로 구성된 기반구조이다.

(2) 탐지 및 대응(Detect and Respond)

탐지 및 대응은 침입에 대한 빠른 탐지와 적절한 대응을 가능하게 한다. 탐지 활동을 통해 수집된 적의 침입유형을 통하여 보안분석가는 적의 활동 패턴을 인식할 수 있다. 탐지 및 대응은 적의 침입에 빠르게 대응하는 기술적 해결책과 침입을 감시할 수 있는 모니터링 소프트웨어를 필요로 하며, 재난에 대비하여 CERT(Computer Emergency Response Team)라 불리는 비상대책 팀을 운영해야 한다.

2.3 운영(Operation)

종심방어 전략의 마지막 핵심 요소는 운영이다. 운영은 조직의 보안 태세를 유지하기 위해 요구되는 모든 활동에 초점이 맞춰져 있다. 운영에는 보안방침, 검증 및 인정, 정보보증 준비태세 평가, 보안관리, 키관리, 공격 탐지와 경보 및 대응, 복구와 재구성으로 구성된다.

3. 전자정부의 정보보호전략

전자정부의 정보보호전략은 (그림 3)에서 보는바와 같이 정보보호 방법에 따라 기술적 측면, 보안관리 측면, 법·제도적 측면의 정보보호 대책으로 나누어 고려하고 있다[9].

(그림 3) 안전하고 신뢰할 수 있는 전자정부 구현 도식도

법·제도적 측면에서의 정보보호 대책은 정보보호에 관련한 법·제도적인 지원대책을 의미하며 정보보호 관련 법률, 정보보호 관련 규정, 세부지침, 보안교육 및 홍보 등이 있다.

보안관리 측면의 정보보호 대책은 정보보호 정책 시행, 행정전자서명 인증기반(GPKI), 통합 보안관리, 키관리(Key Management) 등이 있다.

기술적 측면의 정보보호 대책은 조직의 특성에 맞는 정보보호시스템을 구축하기 위하여 필요한 서버보안, 네트워크보안, PC보안, DB보안, 바이러스 방역, Data 백업 등과 같은 정보보호 응용기술을 의미한다. 기술적 측면의 정보보호 대책은 다시 보호 대상을 기준으로 정보보호 시스템에 대한 정보보호 대책과 정보통신망에 대한 정보보호 대책으로 구분하여 제시하고 있다.

본 연구에서는 우리나라의 전자정부 정보보호전략이라고

명시된 문건이 없기 때문에 행정자치백서에 제시된 (그림 3)이 우리나라의 전자정부 정보보호전략에 가장 유사하다고 판단하고, 최근 검토되고 있는 행정자치부의 「정보보호지침(안)」에 대해 살펴보았다. 「정보보호지침(안)」은 (그림 3)을 골격으로 작성된 문건이라 할 수 있고, 그 세부 내용은 <표 1>에 간략히 나타나 있다[10].

〈표 1〉 행정자치부의 전자정부통합망 관리운영 지침

지침	내용
정보보호 관리 지침	행정자치부 정보시스템 및 관련 중요 자산을 다양한 침해행위로부터 보호하기 위하여 적정한 운영과 관리에 필요한 기준, 방안을 제시한다.
보호구역 관리 지침	행정자치부 보호구역의 정보시스템 및 관련 중요 자산을 물리적으로 보호하기 위해 필요한 기준, 방안을 제시한다.
네트워크 보안운영 지침	행정자치부의 안정적인 지방행정정보망 및 정부고속망 운영, 보안관리에 필요한 기준, 방안을 제시한다.
서버 보안 운영 지침	행정자치부의 안정적인 서버 운영 및 보안관리에 필요한 기준 및 방안을 제시한다.
데이터베이스 보안운영 지침	행정자치부의 안정적인 데이터베이스 운영 및 보안관리에 필요한 기준 및 방안을 제시한다.
응용시스템 보안운영 지침	행정자치부의 응용시스템 개발 및 운영시, 보안관리에 필요한 기준 및 방안을 제시한다.
보안시스템 운영 지침	행정자치부의 안정적인 보안시스템 운영 및 관리에 필요한 기준 및 방안을 제시한다.

행정자치부의 전자정부통합망 관리운영 지침에는 <표 1>의 지침 외에도 UNIX 서버보안운영가이드, Windows 서버보안운영가이드, PC 보안운영가이드가 첨부되어 있다.

4. 상호비교를 통한 고찰

미국의 종심방어전략은 "사람이 기술의 지원을 받아 운영한다."는 평범한 진리를 종심방어전략의 핵심 개념으로 삼은 것이다. 따라서 세 가지 핵심 요소는 사람, 기술, 운영이다.

반면에 전자정부의 정보보호전략은 여섯 개의 핵심 요소로 구축되어 있다. 즉, 종심방어전략과 같은 평범한 핵심 개념을 발굴하지 못하고 기술적인 솔루션과 방어대상을 중심으로 핵심 요소를 분류하였다. 그래서 여섯 가지 핵심 요소는 서버보안, 네트워크보안, PC보안, DB보안, 바이러스 방역, 데이터 백업이다. 이에 본 연구에서는 주요 사실을 파악하기 위하여 미국 종심방어전략의 세 가지 핵심 요소인 사람, 기술, 운영 측면에서 전자정부 정보보호전략을 상호 비교하였다.

4.1 사람(People)

종심방어전략에 있어서 중요한 축을 차지하는 핵심 요소 중 하나는 사람이다. 기술의 지원을 받아 운영하는 주체가 사람인만큼 정보보증에 있어서 사람은 가장 먼저 고려되어야 할 요소인 것이다. 즉 좋은 사람을 고용하여 교육과 포상을 하고 권한이 없는 행위는 제재를 한다는 개념이 사람이라는 핵심 요소의 기본 철학이다.

그러나 전자정부 정보보호전략에서는 사람에 대한 직접적인 언급은 없다. 대신 사람이 지켜야 할 법·제도를 중요한 영역으로 부각시키고 있다. 법·제도는 '정보보호 관련 법률', '정보보호 관련 규정', '세부 지침', '보안교육 및 홍보'로 구성되어 있다. 사람에 대한 종심방어전략과 전자정부 정보보호전략을 비교해 보면 <표 2>와 같다.

〈표 2〉 사람에 대한 종심방어전략과 전자정부 정보보호전략 비교

종심방어전략	전자정부 정보보호전략
방침과 절차	- 정보보호 관련 법률 - 정보보호 관련 규정 - 세부 지침
교육과 인식	보안교육 및 홍보
시스템 보안 행정	-
물리적 보안	-
인원 보안	-
시설 보호 대책	-

<표 2>에서 보듯이 전자정부 정보보호전략에서는 '시스템 보안 행정', '물리적 보안', '인원 보안', '시설 보호 대책' 등 종심방어전략에서 언급한 요소들은 존재하지 않는다. 그렇다고 해서 이 요소들이 전자정부 정보보호 전 분야에서 다루지 않고 있는 것은 아니다. 예를 들면, 종심방어전략의 '시스템 보안 행정', '인원 보안' 및 '교육과 인식 분야'는 「정보보호지침(안)」 내의 「정보보호 관리지침」에서 관련 사항을 다루고 있고, 종심방어전략의 '물리적 보안' 및 '시설 보호 대책' 또한 「정보보호지침(안)」 내의 「보호구역 관리지침」에서 관련 사항을 다루고 있기는 하지만, 전자정부 정보보호전략에서 관련 사항 전체를 체계적으로 제시하고 있지 않다. 즉, 종심방어전략의 사람에 해당하는 일부 항목이 전자정부 정보보호전략에 나타나 있을 뿐, 하위 관련 지침에서 사람에 대한 대부분의 정보보호 지침을 다루고 있으며, 전자정부 정보보호전략에서는 이를 명확하게 제시하고 있지 않다.

거시적인 전략 측면에서 전자정부 정보보호전략의 가장 큰 문제점은 사람에 대한 중요성을 인식하여 나타내지 않고, 하부 지침 수준의 중요도로 사람을 인식하고 있다는 것이다. 앞서 언급했듯이 기술의 지원을 받아 운영하는 것이 사람이다. 그런데 이를 서버나 PC 등과 같은 수준으로 인식하여 정보보호 지침이 만들어져 있다. 따라서 전자정부 정보보호전략에서 사람은 시스템과 분명히 구분을 해야 할 것이고, 또한 시스템보다 상위 수준에서 사람에 대한 정보보증 방안을 수립해야 할 것이다.

4.2 기술(Technology)

우리나라의 인터넷 활용 기술은 높은 수준의 인프라를 갖추고 있다. 그러나 정보보호 시스템의 구축전략 측면에 있어서 물리적 인프라의 확장에 치중한 나머지 체계적인 전략은 제시하고 있지 못하다. 이에 미국의 종심방어전략 핵심기술 네 개 영역과 전자정부 정보보호전략의 여섯 개 핵심 요소를 비교해 봄으로써 정보보증 기술의 나아갈 방향을 전망해 보고자 한다.

<표 3>에서 종심방어전략과 정보보호전략의 차이점은 크게 다섯 가지로 도출할 수 있다.

첫째, 미국의 종심방어전략에서 기술이라는 핵심 요소의 개념은 평가된 제품과 솔루션을 채택하고 계층화 된 방어전략을 지원하는 것이다. 이를 위해 정보보증 아키텍처, 정보보

증 기준, 평가된 제품의 획득 및 통합, 시스템 위험평가 요소가 기술이라는 핵심 요소에 포함되어 있다. 반면 전자정부의 정보보호전략에서는 기술에 대한 핵심 개념과 주요 요소에 대한 정의가 없다.

둘째, 전자정부 정보보호전략에서는 엔클레이브 경계 개념이 고려되고 있지 않다는 것이다. 종심방어전략에서 엔클레이브 경계를 기술의 네 영역 중 하나의 핵심 영역으로 제시한 것은 엔클레이브 경계가 공격의 최초 관문이 되기 때문이다. 최종 방어선인 엔클레이브를 방어하기 위한 전방 방어선인 엔클레이브 경계에 정보보증기술을 접목함으로써 계층화된 방어 시스템을 성공적으로 구축하고자 하는 것이 종심방어전략의 궁극적인 목적이다.

이에 반해 전자정부의 행정정보보호체계 강화를 위한 핵심 분야는 정보보호를 위한 응용 솔루션 및 보호 대상을 근거로 하여 여섯 개 핵심 요소로 분류하였다. 이렇듯 전자정부의 정보보호전략은 경계방어 개념을 반영치 않음으로써 계층적 방어전략이라는 개념을 지원하지 못하고 있다.

셋째, 전자정부의 정보보호전략은 방어대상과 정보보호 솔루션을 축으로 정보보호전략의 핵심 요소를 도출하였다는 것이다. 이로 인해 정보보호 6대 핵심 요소에 DB보안, 바이러스 방역과 데이터 백업 분야가 포함 되었으며, 이 세 개의 요소(DB보안, 바이러스 방역, 데이터 백업)는 다른 세 개의 요소(서버보안, 네트워크보안, PC보안)에 하위 영역으로 다시 포함되는 오류를 범하고 있다.

이에 반해 종심방어전략에서는 4대 핵심 영역(로컬 컴퓨팅 환경, 엔클레이브 경계, 네트워크 기반구조, 지원기반구조) 별로 해당 영역 특성에 맞는 정보보증기술을 적용함으로써 전체 시스템의 가용성을 고려한 정보보증 시스템 구현에 초점을 맞추고 있다.

넷째, 전자정부 정보보호전략에서는 보안관리라는 하위 영역 안에 행정전자서명인증기반(GPKI)이라는 기술적인 요소와 정보보호정책 시행, 통합 보안관리, 키관리(Key Management)라는 운영적인 요소가 혼재되어 있다. 따라서 기술적인 요소와 운영적인 요소를 분리하여 표시하는 것이 바람직하다. 키관리 요소는 기술적인 요소인 키관리기반구조(Key Management Infrastructure)와 운영적인 요소인 키관리로 구분하여 명시하는 것이 바람직하다.

미국의 종심방어전략에서는 KMI/PKI가 로컬 컴퓨팅 환경, 엔클레이브 경계, 네트워크 기반구조를 공통적으로 지원하기 때문에 지원기반구조라는 기술 영역에 포함되어 있다. 따라서 전자정부 정보보호전략에서도 GPKI와 키관리기반구조(KMI)는 세 개의 핵심 요소인 서버 보안, 네트워크 보안, PC 보안에 공통적으로 적용되는 기술인 만큼, 보안관리라는 하위 영역에 둘 것이 아니라 핵심 요소의 하나로 격상시키는 것이 바람직한 방향이라고 판단된다.

다섯째, 전자정부의 정보보호전략에서는 종심방어전략의 지원기반구조 내의 한 영역인 탐지 및 대응이 전략적인 측면에서 전혀 다루어지지 않고 있다는 점이다. 다만 하위 지침 수준에서 탐지 및 대응관련 솔루션인 방화벽(Firewall)과 침입탐지시스템(IDS)이 언급되고 있다. 따라서 전자정부 정보보호전략에서도 탐지 및 대응 영역을 전략적인 차원에서 명시함으로써 공격 유형에 따른 탐지전략을 세우고, 이에 적절히 대응할 수 있는 방안을 마련할 수 있도록 하여야 한다.

〈표 3〉 기술에 대한 종심방어전략과 전자정부 정보보호전략 비교

<table>
<tr><td colspan="2">미국의 종심방어전략</td><td colspan="2">전자정부 정보보호전략</td></tr>
<tr><td colspan="2" rowspan="4">로컬 컴퓨팅 환경</td><td colspan="2">서버 보안</td></tr>
<tr><td colspan="2">PC 보안</td></tr>
<tr><td colspan="2">DB 보안</td></tr>
<tr><td colspan="2">데이터 백업</td></tr>
<tr><td colspan="2">엔클레이브 경계</td><td colspan="2">-</td></tr>
<tr><td colspan="2">네트워크 기반구조</td><td colspan="2">네트워크 보안</td></tr>
<tr><td colspan="2">-</td><td colspan="2">바이러스 방역</td></tr>
<tr><td rowspan="2">지원기반구조</td><td>KMI/PKI</td><td rowspan="2">보안관리</td><td>GPKI</td></tr>
<tr><td>탐지 및 대응</td><td>-</td></tr>
</table>

4.3 운영(Operation)

미국의 종심방어전략에서는 운영이라는 핵심 요소 하에 보안방침을 집행하고 침입에 대응하며 주요 서비스를 복구한다는 개념이 명시적으로 나타나 있지만 전자정부의 정보보호전략에서는 묵시적으로 표현되어 있다.

전자정부 정보보호전략에서 보안관리(Security Management)가 운영을 나타냈다고 볼 수 있다. 보안관리에는 정보보호 정책 시행, 통합 보안관리, 행정전자서명 인증기반(GPKI), 키관리(Key Management)가 있으며, 이 중 행정전자서명 인증기반은 종심방어전략의 지원기반구조에서 KMI/PKI에 해당되는 기술적인 요소이고 운영을 나타내는 것은 정보보호정책 시행, 통합 보안관리, 키관리 뿐이다.

〈표 4〉 운영에 대한 종심방어전략과 전자정부 정보보호전략의 비교

미국의 종심방어전략(운영)	전자정부 정보보호전략(보안관리)
보안방침	정보보호 정책 시행
검증 및 인정	-
보안관리	통합 보안관리
키관리	키관리
정보보증 준비태세 평가	-
공격 탐지와 경보 및 대응	-
복구와 재구성	-

<표 4>에서 보듯이 전자정부 정보보호전략에서의 문제점은 다음과 같다.

첫째, 종심방어전략에 비해 운영적인 요소에 대한 고려가 부족하다는 것이다. 즉, 전자정부 정보보호전략에는 종심방어전략의 검증 및 인정, 정보보증 준비태세 평가, 공격 탐지와 경보 및 대응, 복구와 재구성에 대한 요소가 존재하지 않는다.

둘째, 우리나라에서 정보보증 시스템의 검증은 한국정보보호진흥원에서 하고 있으며, 인정은 국가정보원에서 하고 있다. 이미 검증 및 인정에 대한 체계는 갖춰 있지만 전자정부 정보보호전략에는 명시되어 있지 않기 때문에 검증 및 인정 요소도 운영 전략에 포함시켜야 할 것이다.

셋째, 위협으로부터 얼마나 정보보증이 잘 이루어져 있는가에 대한 정보보증 준비태세 평가가 필요하다. 취약점 분석,

위험 분석을 통해 현재의 정보보증 수준을 평가해 봄으로써 위협에 대한 철저한 대비를 할 수 있도록 정보보증 준비태세 평가에 대한 요소를 포함시켜야 할 것이다.

넷째, 공격 시 이를 탐지하고 빠르게 대응할 수 있는 공격 탐지와 경보 및 대응 요소는 종심방어전략의 탐지 및 대응 기술과 매우 밀접한 관계가 있다. 종심방어전략에서는 탐지 및 대응에 대해 기술 분야와 운영 분야 모두에서 다루고 있지만, 전자정부 정보보호전략은 탐지 및 대응에 대한 요소가 핵심 요소의 하나로 명시되어 있지 않으며, 그렇기 때문에 이에 대한 운영 요소도 포함되어 있지 않다.

다섯째, 공격이나 사고로 인해 전자정부 시스템에 문제가 발생했을 시, 이에 대한 복구와 재구성 요소도 포함되어 있지 않다. 이는 국가사이버안전센터에서 발행한 '국가사이버안전 메뉴얼'에 절차 및 보고 체계가 명시되어 있지만, 전자정부 정보보호전략에는 아직 명확하게 명시하고 있지 않다. 그러므로 전자정부 정보보호전략에도 '탐지 및 대응'과 '복구와 재구성'에 대한 운영 전략을 포함해야 할 것이다.

여섯째, 종심방어전략에서는 보안관리를 운영이라는 핵심 요소의 한 영역으로 보고 있지만, 전자정부 정보보호전략에서는 보안관리를 별도의 영역으로 인식하고 있다. 이는 운영 전체의 중요성을 인식하지 못하고 운영의 일부 요소인 보안관리에 대해서만 치중하고 있다. 그러므로 전자정부 정보보호전략에서는 사람, 기술, 운영에 대한 명확한 핵심 요소에 대한 정의가 선행되어야 할 것이다.

5. 결 론

우리나라는 지금까지 전자정부의 구축과 관련된 공식문서에서 "정보보호"라는 용어를 사용하여 왔다. 그러나 미국에서는 "정보보호"라는 개념에 가용성을 추가하여 "정보보호"는 물론이고 필요한 정보와 정보서비스를 중단 없이 제공해야 한다는 새로운 개념인 "정보보증"으로 발전시켰다[5]. 이에 전자정부에서도 "정보보호"의 개념을 뛰어넘어 "정보보증"이라는 개념으로 가야할 것이다.

"최고 수준의 대국민서비스 제공", "최적의 기업환경 제공", "생산성·투명성이 높은 정부 구현"이라는 전자정부의 비전을 달성하기 위해서는 다양한 각도에서 많은 노력을 기울여야 하겠지만, 무엇보다도 정보보증전략의 수립이 최우선 과제라 할 수 있다.

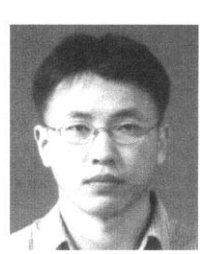
체계화되고 일관된 정보보증전략을 따르는 정보시스템 구축 및 운영을 통해 성공적인 전자정부를 이룰 수 있을 것이며, 이는 곧 국가 경쟁력 향상이라는 부가적인 열매를 우리에게 안겨 줄 것이다.

참 고 문 헌

[1] 전자정부특별위원회, "전자정부 백서", pp.20-23. Jan., 2003.
[2] 김삼교, "정보전 대비 정보보증 발전방향", 국방정보통신, pp.3~9, May, 2003.
[3] WWW.STRATCOM.MIL
[4] 안문석, 박성진, 맹보학, "전자정부 정보보호 대응체계 구축 방향에 관한 연구", 정보보호논문지, 2001.
[5] 국가기술보안연구소, "정보보증 프레임워크에 관한 연구", Nov., 2003.
[6] 이철원, "주요 정보통신망기반구조 보호를 위한 정보보증 기술", 제6회 정보보호 심포지엄, pp.1~5, April, 2003.
[7] 송운호, 선우종성, 정욱재, 김준범, 강한승, "IATF와 전자정부의 정보보증요구사항에 관한 비교연구", WISC 학술대회 논문집, pp.762~789, 2004.
[8] U.S. National Security Agency(Information System Security Organization), "Information Assurance Technical Framework", Sep., 2002.
[9] 행정자치부, "행정자치백서", pp.35~39, June, 2003.
[10] 행정자치부, "정보보호지침(안)", June, 2004.
[11] WWW.IATF.NET

송 운 호

e-mail : woonhosong@dreamwiz.com
1969년 육군사관학교 일반공학(이학사)
1974년 Univ. of California Berkeley Computer Science M.S.
1981년 Univ. of Virginia Computer Science Ph.D.
1981년 Virginia Tech Economics M.A.
1982년~1997년 국방정보체계연구소 부소장
1983년~1990년 한국과학기술원 전산학과 겸임교수
1992년~1993년 미국 IBM WATSON 연구소 객원연구원
1997년~1998년 한국전산원 연구위원
1999년~2001년 한국 유니시스 Information Service 그룹 상무
2001년~2004년 숭실대학교 정보과학대학 컴퓨터학부 객원교수
2004년~현재 서울정보통신대학원대학교 교수
관심분야 : 정보보증기술프레임워크, 정보보증, 전자정부 등



정 욱 재

e-mail : wjjung11@yahoo.co.kr
2002년 한국항공대학교 항공통신정보공학과(학사)
2005년 서울정보통신대학교대학원 정보통신공학과(석사)
관심분야 : 정보보증, 네트워크, 임베디드 시스템 등

김 준 범

e-mail : hisecure@paran.com
2003년 호서전산대 정보보호학과(학사)
2005년 서울정보통신대학교대학원 정보통신공학과(석사)
관심분야 : 네트워크/시스템 보안, 정보보증 등

강 한 승

e-mail : dimakang@paran.com
1998년 광주대학교 경영학과 졸업(학사)
2005년 서울정보통신대학교대학원 정보통신공학과(석사)
관심분야 : 네트워크보안, 정보보증, 정보시스템 감리 등