통합전산환경 구축에 따른 보안 관리 아키텍처 설계

홍지범°
고려대학교 컴퓨터과학기술대학원 디지털정보공학과
ziver818@hotmail.com

Security Management Architecture Design for constructing the integrated computing environment

Jiboum Hong°
Dept. of Digital Information Engineering, Korea University

요 약

범정부 통합전산센터 추진에 따라 수많은 공공기관의 통합전산환경 구축이 요구되고 있으며 이에 따른 보안 정책과 관리 대책 수립이 진행되고 있다. 일반적인 보안 개념에 유비쿼터스 개념인 언제 어디서나 제공될 수 있는 서비스에 따른 보안의 개념이 도입됨에 따라 보안 관리 대책은 관리적, 기술적, 물리적인 측면에서 검토되어야 한다. 본 논문에서는 통합전산환경의 보안 요구사항을 파악하여 보안 관리 아키텍처를 관리적, 기술적, 물리적인 측면에서 현재 진행되거나 향후 추진될 공공기관의 통합전산환경 구축의 기본적인 보안 관리 아키텍처로 제안한다.

1. 서 론

IT시대에 정부는 개별 부처의 전산실을 단계적으로 통합 관리하고 운영, 행정기관의 각종 정보의 연계를 가능하도록 하는 한편 정보보안도 집중 강화할 수 있도록 하는 범정부 통합전산환경 기반의 통합전산센터 구축 작업이 본격적으로 추진되고 있다.

범정부적 통합전산환경이 구축될 경우 다음과 같은 효과가 발생된다[1].

- 운영서비스 품질 고도화 및 전문적 운영 인력에 의한 상시 운영체제도입 등을 통해 국민 서비스 만족도 향상 및 전자정부 운영의 효율성을 제고할 수 있다.
- 전산자원의 효율적 관리체계 및 운용체계를 확립하고, 정보시스템의 공동 활용 촉진으로 정보화 예산의 투자 효율성 및 업무 생산성을 제고할 수 있다.
- 개별적·산발적으로 구축하던 정보시스템을 표준화된 기술 구조에 따라 구축할 수 있는 기반을 마련하여 정보시스템간 상호운용성과 신뢰성을 확보할 수 있다.
- 전산환경조사결과는 부처간 정보화 격차 해소 및 고도화된 서비스 체계로의 이행을 위한 정보화 정책 수립 자료로 활용할 수 있다.

본 논문에서는 현재 정부에서 추진하는 통합전산환경 기반의 전산센터 개발에 이어 향후 추진될 공공기관들의 통합전산환경 마련을 위한 보안 관리 아키텍처를 제안한다.

2. 통합전산환경의 보안 요구사항

통합전산환경의 성공적인 구축을 위해서는 통합전산환경의 목표 모형 중 전 영역에 걸쳐 있는 보안 계층이 얼마나 안전하고 신뢰성을 제공하느냐에 달려 있다[2]. 본 논문에서는 통합전산환경의 관리적, 물리적, 기술적 통합 보안관리체계를 구축하고 정보시스템 운영에 대한 안정성 및 신뢰성을 제공하기 위하여 통합전산환경의 보안 관리 아키텍처를 제안한다.

통합전산환경의 보안 요구사항을 바탕으로 통합전산환경에서 제공해야 하는 전체적인 보안모델 아키텍처를 수립하고 통합전산환경의 보안 통제를 적용하게 된다.

통합전산환경의 보안 요구사항은 다음과 같다.

- 정보보호 관리체계의 수립으로 내부 보안성 향상 및 위험 관리 능력 도모
- 도로, 주변 건물 등에서 통합전산환경에 대한 물리적인 시설 접근의 차단 및 탐지
- 웜/바이러스, 유해트래픽, 외부 침입으로부터의 통합전산환경의 네트워크 보호

3. 보안 관리 아키텍처와 설계 원칙

본 장은 통합전산환경에 작용되는 관리적인 측면의 정보보호 아키텍처를 그림 1과 같이 관리적 보안, 기술적 보안, 물리적 보안의 관점으로 정의한다[3].

통합전산환경의 관리적 보호 대책을 수립하기 위해서는 통합전산환경에 맞는 정보보호관리체계의 구축이 필요하다. 정보보호관리체계 구축은 통합전산환경의 위협 및 취약점을 분석하고, 보안 통제를 구축하며 정보보호 정책, 지침, 절차 및 보안 가이드라인을 설정한다. 영국의 정보보호관리분야의 표준인 BS7799[4]와 정보통신부의 정보보호관리체계를 중점으로 비교(표 1)하여 통합전산환경의 정보보호관리체계를 구성한다.

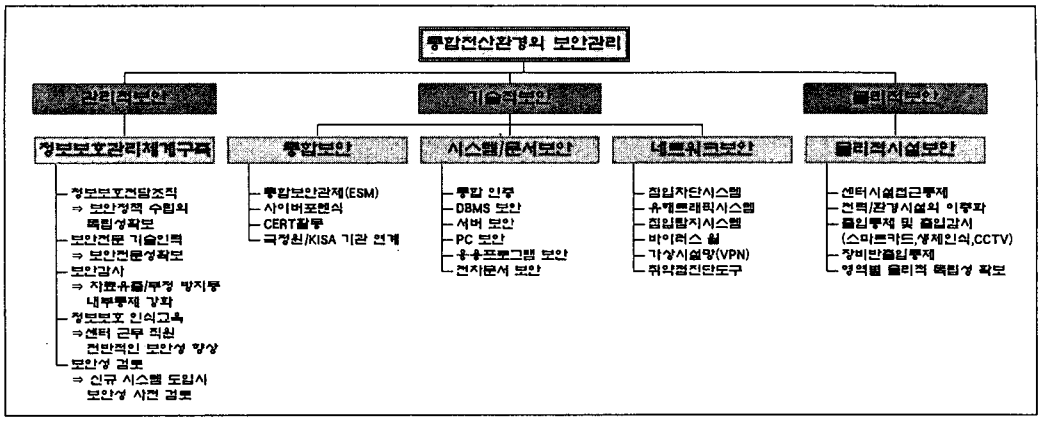

그림 1. 통합전산환경의 보안 관리 아키텍처

BS7799	정보통신부	제안사항
보안조직	정보보호조직	정보보호관리자 역할 부족
자산분류 및 통제	정보자산분류	아웃소싱, 서드파티 인력 관리 항목 필요
물리적/환경적보안	물리적보안	전산센터 보안항목 필요
부합성	검토,모니터링 및 감사	기술적 점검 항목필요

표 1. BS7799와 정통부 정보보호관리체계 비교

정보보호관리체계는 조직의 정보보호 목표와 중요성을 선언하는 정책과 정책을 준수하기 위한 세부 지침과 절차, 그리고 정보보호의 준수 여부를 확인하기 위한 점검으로 구성(표 2)된다.

구분	세부사항	구분	세부사항
정책	·개념 확립 ·지침수립의 근간 ·정보보호관리기준	점검	·일반보안 점검리스트 ·UNIX점검리스트 ·네트워크장비점검리스트 ·Windows 점검리스트 ·보안장비 점검리스트
지침	·정보보호 지침서 ·정보보호조직운영지침 ·보안사고 대응지침 ·보안성 검토지침 ·사용자 관리지침 ·네트워크 보안지침 ·시스템 보안지침 ·응용프로그램보안지침 ·시스템 운영지침	절차	·보안절차 ·문서관리절차 ·사고처리절차 ·신규도입절차 ·변경통제절차 ·비밀정보반출절차 ·보안점검절차 ·보안관제절차 ·사용자관리절차 ·교육/홍보절차

표 2. 통합전산환경의 정보보호관리체계 구성

통합전산환경의 물리적 보호 대책은 정보를 처리하는 컴퓨터, 통신기기 등과 같은 시설 및 장비들 또는 이러한 시설이나 장비로 처리된 자료나 정보를 보관하는 매체나 장소를 여러 위협으로부터 보호하는 보안 관리 대책(그림 2)이다. 환경적 위험 및 통제, 물리적 시설 보호, 통제구역 설정은 상호 보완 관계에 있다.

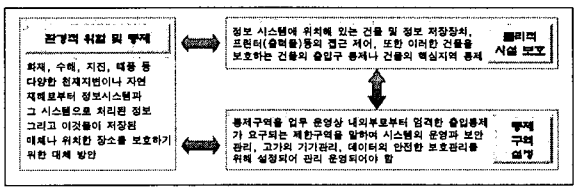

그림 2. 통합전산환경의 물리적보호대책

민간 분야에서 활용되고 있는 IDC(Internet Data Center)의 시설 안전·신뢰성 기준을 연구하여 최상등급기준을 통합전산환경의 구축에 반영한다. IDC는 최상등급의 시설관리, 인적, 제도적 운영에 대한 내부운영지침서와 시설, 인원에 대해 재난 발생시부터 사후복구까지의 모든 행동지침을 포함한 비상계획서와 보안계획을 담은 보안계획서를 작성한다. 물리적 보호 대책은 접근제어 및 감시, 가용성, 방호성, 방재성을 갖추어야 한다. 출입 통제 및 감시는 내외부인 모두를 대상으로 하며 대응방안은 1단계(건물출입통제), 2단계(주요지역 입·퇴실 통제), 3단계(로그 기록)의 단계로 나눠진다. 시설방호체계는 출입카드관리, 야간출입통제, 정보자산 반출관리, 정보자산 반입관리, 통제구역 설정 및 관리가 이뤄져야 한다.

통합전산환경의 기술적 보호 대책은 네트워크 보안과 정부 인증관리체계를 기반으로 그 위에 서버 보안, 응용시스템 보안, DBMS 보안, 관리자 PC보안, 전자문서 보안 등 요소 보안이 이루어지며, 기술적 보안을 통합하여 관리하는 통합보안 관제를 수행한다. 통합전산환경의 기본적인 보안 모델은 Web Server 영역 - Application Server 영역 - DB Server 영역의 3단계 보안 심화 모델이다. 고도의 보안의 요구되는 시스템의 경우는 독립 시스템 영역을 별도 제공한다. 통합전산환경의 인증 보안은 암호기술을 이용한 송수신기관 및 사용자의 신원확인, 유통문서의 비밀성 확보 등 전자문서의 보안성 확보를 위해 각 기관 및 사용자에 부여되는 디지털 정보이다. 인증 보안을 위해 인증관리센터를 설치하며 PKI를 이용하여 전

자서명, 암호키관리, 접근권한통합관리, 사용자전자카드 등에 적용하고 통합전산환경의 보안성을 향상시킨다(표 3).

구분	세 부 사 항
전자서명	·전자문서를 작성한 사람의 신원과 전자문서의 변경여부를 확인할 수 있는 고유정보 ·행정전자서명을 통한 본인 확인, 유효성 검증, 시점 확인서비스 제공
암호키 관리	·정보통신망을 이용하여 전자문서를 전달하는 과정에서 문서에 대한 기밀성 서비스를 제공하기 위하여 사용하는 암호키에 대한 검증 업무를 제공하는 것 ·안전한 전자문서 관리를 위한 기반
접근권한 통합관리	·접근권한통합관리는 사용자 권한, 지위, 업무 등의 사용자 Attribute를 정의하여 사용자의 신원 확인 후 사용자의 권한을 정의 ·현재 구축된 전자서명을 이용한 시스템 접근권한 통합관리체계를 통합전산환경으로 확대, 적용함
사용자 전자카드	·사용자의 IC칩이 내장된 전자카드로 전환하여 사용자의 인증서를 저장함 ·인증서가 저장된 전자카드는 전자서명, PC접근제어, 출입통제 등에 활용이 가능하며, 통합전산환경에서는 사용자 전자카드를 적극 활용함

표 3. 통합전산환경 기술적 보안 대책의 인증 보안

통합전산환경에 통합보안관제가 요구되는 필요성과 대응방안은 그림 3과 같다.

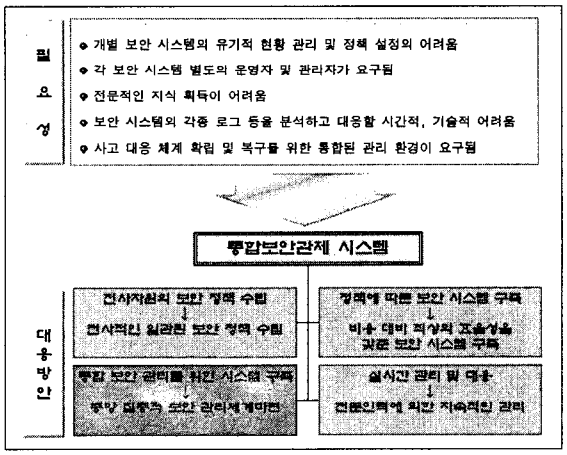

그림 3. 통합보안관제의 필요성과 대응방안

통합보안관제 시스템의 구축 목표는 안전한 네트워크와 시스템으로 보안이벤트 통합분석(ESM), 취약점/위협정보 관리, 유해트래픽 분석(MTA)이 필요하다.

외부로부터의 침입차단과 네트워크 각 영역에서의 논리적인 보호를 위하여 침입차단시스템(방화벽)을 구성해야 한다. 방화벽을 우회한 침투, 정상적 경로를 통한 침해사고 탐지를 위해서 침입탐지시스템(IDS)을 설치하여야 한다. 공공 기관에서 통합전산환경으로 접근하고자 하는 경우는 가상사설망(VPN)을 통한 사용자 인증과 터널링을 통한 전송 데이터의 노출을 보호한다. 유해트래픽 차단시스템은 방화벽, IDS가 방어할 수 없었던 유해트래픽을 지능적으로 탐지/차단하여 네트워크를 보호한다. 악성코드가 통합전산환경의 내부 네트워크에 진입하기 전에 발견하고 제거하기 위하여 바이러스 월을 설치한다.

취약점 진단 도구는 공격에 취약한 점을 발견하고 보안정책에 반영한다. 전체 네트워크에 대하여 주기적으로 상호 취약점 진단을 시행하며 지속적인 공격에 대하여 시스템 취약점에 대한 대처와 네트워크 장비, 시스템, 사용자 PC에 대하여 보안 취약성을 주기적으로 진단, 조치함으로써 정보보호 마인드를 향상한다. 관리자 및 일반사용자의 취약점을 별도 진단/분석함으로 취약점 분석시 발생할 수 있는 사용자별 충돌을 막을 수 있다. 또한 공격에 취약한 대상 시스템 분석시 타시스템의 침입시도를 동시에 진단/분석하여 네트워크 전체의 보안 관리 체계를 유지할 수 있다. 이동성을 보장하여 취약점 DB의 실시간 업그레이드와 보안 취약점의 자동 점검 및 레포팅을 한다. 취약성에 대한 원인, 중요도, 영향 범위, 조치 방법, 관련 사이트 등의 DB도 제공한다. 진단/분석 결과를 중요도별로 분류하고 침입 및 권한탈취 시도의 결과, 보안 취약점, 결함을 교정하고 ESM Main Server에 전송하여 보안 관리 정책에 반영한다.

이상의 관리적, 물리적, 기술적 보안 관리 대책들은 통합전산환경 구축에 반드시 필요한 요소들로 그림 1의 보안 관리 아키텍처는 시스템 설계에 기본이 된다.

4. 결론 및 향후 과제

범정부에 추진 중인 통합전산환경의 전산센터는 보안관리 대책이 매우 미흡하다. 본 논문에서는 관리적, 물리적, 기술적 보안 관리 아키텍처를 수립하여 통합전산환경 설계에 기본 모델로 반영한다. 계층화된 보안, 접근제어, 역할기반 정보보호, 사용자 인식 재고, 모니터링, 시스템 패치, 대응 팀의 보안 관리 아키텍처는 네트워크에서 가장 크게 발생하는 서비스거부, 악성코드, 비인가접근 등의 공격을 방지하고 관리할 수 있다. 앞으로 보안관리 방안을 관리적, 물리적, 기술적 보안 관리 아키텍처에 따라 실제 모델을 설계하고 침해사고 대응체계를 제시한다면 보안관리대책의 일관성이 유지되고 체계적인 보안관리대책이 수립될 것이다. 향후 이러한 보안관리대책을 기반으로 관련 법규 및 지침을 만들어야 한다.

참고문헌

[1] 전자정부특별위원회, "전자정부백서", 2003.01
[2] 서용원외, "공공부문 전산환경의 통합 방안에 관한 연구", 2002.10
[3] 조영훈외, "CC기반의 정보보호체계 인증평가모델에 관한 연구", 2003.07
[4] BSI, "Information security management - Part 1 : Code of Practices for Information Security Management", BS7799-1:1999, 1999.
[5] 정태명외, "통합전산환경의 추진방향 ", 2004.11
[6] 행정자치부, http://www.mogaha.go.kr
[7] 정보통신부, http://www.mic.go.kr