공공기관 전산보안정책 수립을 위한 지침서 (TTA.KO-10.0089)

이민구
한국전산원 정보화평가분석단 연계표준부 주임연구원

1. 서 론

컴퓨터 전산망과 정보기술의 급격한 발전으로 기존의 문서로 저장되어 오던 자료들이 컴퓨터 파일로 저장되게 되고, 또한 전산망으로 컴퓨터들이 상호 연결됨에 따라 지역과 거리에 무관하게 필요한 서비스를 받을 수 있게 되었다. 또한 인터넷의 빠른 보급으로 전세계의 어떤 자료도 단시간 내에 입수하여 활용하는 등 정보화 사회로의 진입이 빠르게 이루어지고 있다. 그러나, 최근에 그 발생빈도를 더해 가는 일련의 보안사고는 정보화 사회로의 진입에 커다란 장애물이 되고 있을 뿐만 아니라, 개별 조직 및 기관에 막대한 피해를 주고 있다. 이와 같은 보안사고에 각 기관이 체계적으로 대응하기 위해서는 개별조직에 적합한 보안정책 및 보안지침의 수립이 필요해지고 있다.

1, 2차 국가기간전산망사업을 통해 정보화의 토대를 마련한 우리 나라는 각종 보안관련 지침을 제정하여 배포하였으나, 그 내용이 전체적이고 포괄적인 내용을 담고 있어 개별 공공기관의 특성에 적합한 보안대책을 수립하는데 다소 미흡하였다. 또한, 공공기관의 보안에 대한 인식 부족으로 인해 전담 보안담당자를 지정하여 운영하지 않고 타 업무를 수행하면서 보안업무를 수행하고 있어 보안기술의 축적이나 개별기관의 보안대책 수립에는 한계가 있다.

공공기관에서도 최근에 발생하는 보안사고와 이로 인한 피해상황이 심각하다는 것을 인식하고 이에 대한 대책 수립에 고심하고 있지만, 공공기관의 보안대책 수립에 실제적으로 도움이 될 만한 연구자료 및 참고자료가 부족한 형편이다.

이에 따라 본 지침서에서는 공공기관이 구축 및 운영하고 있는 정보시스템의 안전신뢰성 확보를 위해 우선적으로 필요한 보안정책의 수립방법 및 내용을 제시하고 있다. 또한, 보안지침의 세부적인 내용을 제공함으로써 공공기관의 실무담당자들이 손쉽게 개별 공공기관의 전산환경이나 특수한 상황에 적합한 보안지침을 수립할 수 있도록 하였다.

또한, 본 지침서는 개별 공공기관에 적용되고 있는 관련 보안지침(국가전산보안업무기본지침, 행정전산망안전관리지침 등)의 세부적인 내용 및 절차를 보강하여 개별 공공기관의 환경에 적합한 보안정책 및 보안지침을 수립하는데 참고자료로 이용될 수 있으며 만약, 본 지침서에서 기술된 내용이 관련 보안지침

의 내용과 상충될 경우에는 관련 보안지침의 내용을 우선적으로 적용해야 된다.

2. 국내의 관련 지침 및 표준 현황

국내의 정부부처 및 공공기관이 적용받고 있는 전산보안관련 지침은 국가안전기획부의 "국가전산보안업무기본지침"과 "전산망 보안관리 세부지침"이며, 정부부처(국방부, 정보통신부, 재정경제부 등)에서는 "국가전산보안업무기본지침"을 준용하면서 개별 부처에 적합한 보안지침을 운용하고 있다.

'97년 "국가전산보안업무기본지침"이 제정되기 이전에는 각 부처에서 필요에 따라 보안관련 지침 및 기준(행정자치부의 "행정전산망 안전관리지침", 정보통신부의 "전산망안전신뢰성기준"등)을 제정하여 운영해 왔으나, "국가전산보안업무기본지침"이 제정된 이후에는 "국가전산보안업무기본지침"으로 일원화되고 있는 추세이다.

보안관리 분야의 표준은 "국가전산보안업무기본지침"이나 "전산망 보안관리 세부지침"에서 다루고 있지 않은 보안관리의 세부적인 내용 및 기술적 내용을 다루고 있다.

〈표 2-1〉 보안관리 분야 표준 I - 한국정보통신표준

표준번호	표준명	제/개정일
KICS.KO-10.0003	국가기간전산망 패스워드 활용 표준	'93
KICS.KO-10.0005	전산망 보안관리를 위한 기술지원서(총론)	'93
KICS.KO-10.0006	전산망 보안관리를 위한 기술지원서(전산센터의 물리적 보안)	'93
KICS.KO-10.0047	전산망 보안관리를 위한 위험관리 지침서	'95
KICS.KO-10.0072	네트워크 보안관리 지침서	'96
KICS.KO-10.0073	소프트웨어 보안관리 지침서	'96
KICS.KO-10.0074	자료 보안관리 지침서	'96
KICS.KO-10.0075	소프트웨어 개발 및 변경에 관한 보안관리 지침서	'96

※ KICS(Korea Information & Communication Standard)

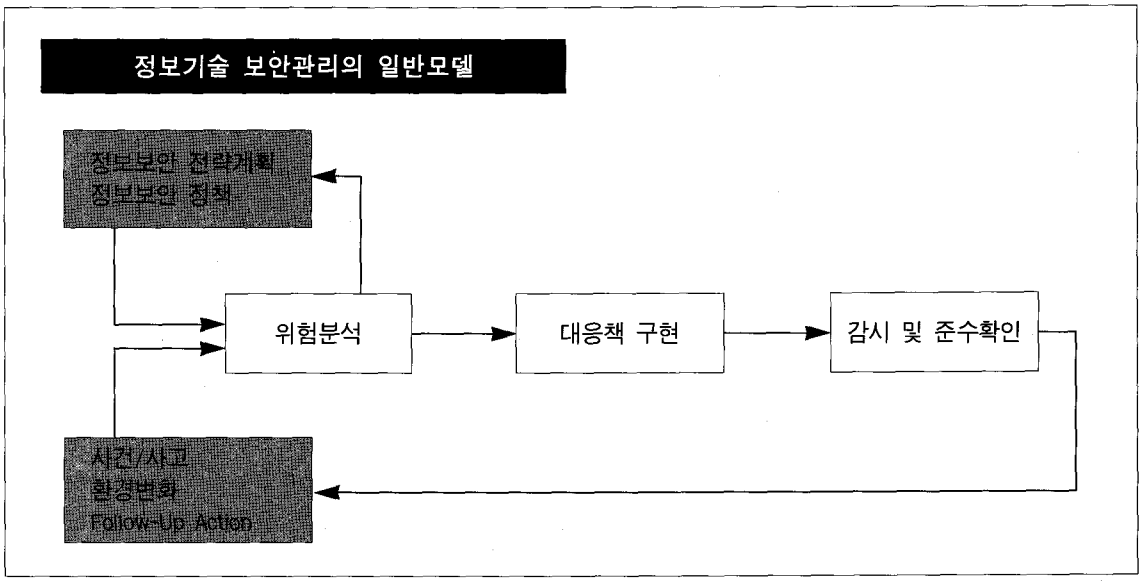
〈표 2-2〉 보안관리 분야 표준 II - TTA 단체표준

표준번호	표준명	제/개정일
TTA.KO-10.0088	공공기관 인트라넷 보안지침서	'98
TTA.KO-10.0089	공공기관 전산보안 정책 수립을 위한 지침서	'98
TTA.IS-TR13335.1	공공정보시스템 보안을 위한 위험분석표준-개념과 모델	'98
TTA.KO-10.0090	웹 환경 구축 및 운영을 위한 보안관리 지침서	'98

3. 공공기관 전산보안정책 수립을 위한 지침서

3.1 보안정책 개요

3.1.1 보안정책 이란



(그림 3-1) 정보기술 보안관리의 일반모델

- 보안정책이란 정보자산을 어떻게 관리하고 보호할 것인가에 대한 지침 및 절차를 문서로 기술해 놓은 것으로, 조직에서 정보자산을 안전하게 보호하고 효율적으로 사용하기 위해서 우선적으로 수립되어야 한다.
- 보안관리의 일반적인 모델은 우선적으로 보안정책을 수립한 후에 보안정책을 근거로 하여 위험분석을 실시함으로써 조직의 보호해야 할 자산, 위협, 취약성 등을 식별하고 이에 대한 대응책을 구현한다.
- 보안정책은 환경의 변화나 새로운 위협이 발생했을 경우, 또는 주기적인 위험분석 실시 과정을 통해 갱신되어 진다.

3.1.2 보안 요구조건

공공기관의 보안정책 및 일련의 보안지침은 다음과 같은 보안요구 조건을 충족해야 한다.

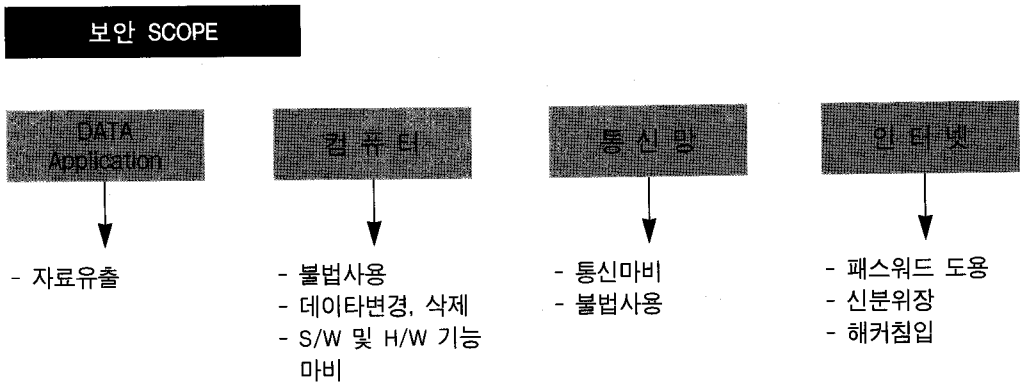
- 무결성
- 기밀성
- 가용성
- 인증성
- 접근제어

3.1.3 보안 기본방침

- 외부에서 내부로의 접근은 원칙적으로 차단한다.
- 모든 자원은 보안등급에 따라 분류, 관리한다.
- 사용자계정 및 패스워드는 개인별로 부여함을 기본으로 한다.
- 주기적인 보안점검을 통해 보안정책 및 보안지침의 준수여부를 확인하고 보안대책을 강구한다.
- 정보자산에 대한 위험분석을 주기적으로

실시하여 그 결과를 보안정책 및 지침에 반영 한다.

3.1.4 적용대상 및 범위



적 용 범 위

자원	보안사고유형	대책
하드웨어	기능파괴	물리적 대책
소프트웨어	자료유출	관리적 대책
데이터베이스	비인가자 사용	기술적 대책
통신네트워크	도청, H/W 도난	

(그림 3-2) 보안 적용범위 및 대상

3.1.5 보안등급 기준

3.1.5.1 보안등급 분류기준

- 정보의 중요도 및 정보의 사용권자
- 정보(시스템)의 절취 및 불법변경시 손실가치
- 정보(시스템)의 파괴시 복구비용

3.1.5.2 정보(시스템) 보안등급

- 정보(시스템) 보안등급은 개별기관의 특성을 반영하여 별도로 유지

※ 본 정책에서 예시로 사용한 보안등급 : PSL (Public-sector Security Level)

〈표 3-1〉 정보(시스템) 보안등급 예시

자원	보안사고유형	대책
PSL1	비밀정보	기밀 정보
PSL2	핵심정보	회계/자산/인사 정보
PSL3	업무정보	전자결재관련정보, 부서별, 업무정보, 폐쇄그룹
PSL4	사내 및 공공기관 공개정보	BBS, 공용문서, 공공기관 공개정보
PSL5	사외 공개자료	Web page/FTP 정보

3.1.5.3 사용자 보안등급

- 사용자 보안등급은 개별기관의 특성을 반영하여 별도의 보안등급 유지

〈표 3-2〉 사용자 보안등급 예시

보안등급	사용자	정보이용범위	
		해당부문	타 부문
PSL1	기관장/비밀취급인가자 PSL1 자원관리책임자	PSL1	PSL2
PSL2	단위부서장/PSL2 자원관리책임자	PSL2	PSL4
PSL3	팀장/실무자/PSL3 자원관리팀장	PSL3	PSL4
PSL4	전직원	PSL4	PSL4
PSL5	외부인/임시직원	PSL5	PSL5

3.1.6 책임 및 권한

- 사용자는 허가된 보안등급내의 정보자산을 이용할 권한을 가지며, 불법사용에 대한 최종 책임은 사용자에게 있다.
- 사용자가 허가된 범위 이외의 정보자산을 불법 사용하여 재산상의 손실을 입히거나 이미지를 훼손했을 경우 징계 조치를 취할 수 있다.
- 기타의 경우는 전산시스템 사용지침에 따른다.

3.1.7 전산시스템의 사용

3.1.7.1 사용자 정의

- 공공기관의 직원
- 해당 공공기관의 시스템을 사용하는 최종 사용자
- 기타, 기관의 장이 규정에 의거 사용을 인정한 자

3.1.7.2 사용의 부 적절성

전산시스템을 이용할 수 있는 사용자라도, 전산시스템 사용에 있어 적절성을 보장받아야 한다. 다음의 경우는 부적절한 사용으로 간주한다.

- 타 사용자의 사용자 계정 및 패스워드를 허가 없이 사용한 경우
- 타 사용자의 서비스 사용을 방해한 경우
- 타 사용자의 자료를 허가 없이 유출, 또는 읽고 쓰는 행위
  - 일반사용자가 루트 패스워드 또는 타 사용자의 패스워드를 이용해 자료를 읽고 쓰는 행위
  - 시스템 관리자가 일반사용자의 허락없이 메일사서함을 열람하거나 폐쇄그룹으로 운영되고 있는 게시판 자료를 읽는 행위
- 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
- 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
- 사용자 계정 및 패스워드를 상호 공유하는 행위
  - 시스템관리자가 특별한 사유 없이 루트 패스워드를 일반사용자와 공유한 경우
- 허가된 보안등급 이상의 자료를 유출, 또는 읽고 쓰는 행위

3.1.7.3 사용의 제한

- 전산시스템을 적절히 사용하지 않을 경우, 전산시스템의 사용을 제한한다.
- 특히, 전산시스템의 불법사용으로 해당 기관에 해를 끼치거나 이미지를 훼손시켰을 경우 별도의 징계 조치를 취할 수 있다.

3.2 분야별 보안관리 지침

분야별 보안관리 지침의 구성내용은 아래와 같으며 자세한 내용은 표준을 참조하기 바란다.

- 네트워크 보안관리 지침
- 서버 보안관리 지침
- 자료 및 데이터베이스 보안관리 지침
- 어플리케이션 보안관리 지침
- 인터넷 보안관리 지침
- 개인용 컴퓨터 보안관리 지침

3.3 전산센터 운영관리

전산센터 운영관리의 구성내용은 아래와 같으며 전산센터의 운영과 관련된 보안지침을 다루고 있으며 자세한 내용은 표준을 참조하기 바란다.

- 시설 기준
- 전산실 운영 지침
- 백업 및 자료보관 지침
- 비상대책 및 재해복구 대책

3.4 보안관리 절차 및 점검지침

3.4.1 보안관리 절차

가. 개 요

정보시스템 보안관리가 필요한 대상에 대해 업무처리 절차를 규정하여 체계적이고 일관된 보안정책을 구현한다.

나. 대 상

(1) 사용자 계정절차(등록, 변경, 폐기)

- 사용자계정은 사용자등록/변경/폐기 신청서를 작성 후 시스템관리자에게 통보한다. 특히 외부사용자는 사용기간, 사용목적 등의 사유를 명확히 해야한다.
- 시스템관리자는 내용검토 후 사용자 계

정을 등록/변경/폐기하고 사용자에게 통보한다.

- 사용자 계정등록/변경/폐기시 일반적인 사항은 월 단위로 부서장에게 사후 보고하고, 특별한 상황이 발생할 경우 부서장의 허가를 득한 후에 작업을 실시한다.
  - 일반적인 상황 : 직원의 입/퇴사, 직원의 장기출장 등
  - 특별한 상황 : 외부사용자의 계정 등록 요청 등

(2) 보안점검 절차

- 시스템관리자는 보안점검 체크리스트에 의거 주, 월 단위로 점검내용을 체크한다.
  - 보안사고의 징후가 보이는 시스템관리자는 필요시 일 단위로 점검 내용을 체크한다.
- 공공기관 전체 시스템에 대한 보안점검은 보안점검 지침에 따른다.

(3) 시스템사용 신청절차

- 시스템 장애복구 및 점검을 위해 루트권한 위임 시에는 시스템 작업계획서를 작성하여 해당 부서장의 허가를 득한 후에 시스템관리자 입회하에 작업을 실시한다.
- 작업종료 후 시스템관리자는 보안점검 체크리스트에 준하여 시스템 점검 후 사용자 계정 절차에 의해 패스워드를 변경한다.

3.4.2 보안점검 지침

가. 개 요

공공기관의 네트워크 및 시스템을 외부의 불법침입으로부터 안전하게 보호하기 위해 보안점검을 실시한다.

나. 보안점검 구분

- 시스템 및 네트워크별 보안점검
  - 시스템관리자가 서버운영관리지침에 따라 개별 점검
- 공공기관 전체 시스템에 대한 보안점검
  - 내부 망에 존재하는 모든 시스템 자원은 보안 관리자에 의해 중앙 집중식으로 점검하고
  - 그 결과를 각 시스템 관리자에게 통보해준 뒤 관리자로부터 보완계획을 보고받고 계획된 일정 하에 단계적으로 수정해간다.
  - 시스템 관리자는 수정된 결과를 정리하여 보고하고 보안 관리자는 전 내부망 시스템을 다시 점검하여 전반적인 보안상황을 체크한다.

다. 보안점검 지침

(1) 적용대상

- 공공기관이 보유하고 있거나 관리하고 있는 정보자산

(2) 점검시기

- 보안담당 부서에서 년 2회 이상 정기점검과 필요시 수시 점검 실시
  - 작성된 보안점검 세부사항에 따라 구분하여 정기적으로 점검한다.
  - 변동사항이 많거나 사용자의 접근이 많은 부분(네트워크 서비스, 사용자 계정, 시스템 파일 속성 등)에 대해서는 매일

또는 수일 간격으로 반복 점검하고
- 비교적 접근이 많지 않은 부분(운영체제 버그, 사용자 파일 속성 등)에 대해서는 주 또는 월 간격으로 반복 점검한다.

(3) 점검절차

- 보안담당 부서에서는 보안점검반을 구성한 후 보안점검 대상 및 분야를 해당 부서에 통보한다.
- 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비한다.
- 보안담당부서에서 보안점검을 실시하여 그 결과를 기관의 장에게 보고한 후 해당 부서에 통보한다.
- 해당 부서에서는 지적사항을 보완하고 그 결과를 보안담당 부서에 통보한다.
- 보안담당부서는 필요시 보안점검 지적사항에 대한 조치 여부를 확인한다.

라. 책임 소재

보안점검을 실시하여 다음과 같은 사항이 발견될 경우 규정에 의거 징계 할 수 있다.

- 허가받지 않은 정보자산에 접근하여 불법사용 및 정보 유출시
- 타인의 사용자 계정 및 패스워드를 허가없이 사용한 경우
- 이전 보안점검의 지적사항에 대해 조치를 취하지 않은 경우
- 기타, 정보자산 사용지침을 위반했을 경우

3.4.3 보안사고처리 지침

가. 개 요

전산망을 통해 외부의 불법침입자가 원내의 전산시스템에 침투했을 때 이에 효율적으로 대처할 수 있는 일련의 방법 및 절차를 정의한다.

나. 보안사고 처리 지침

보안사고처리 지침은 침입자 침입예방, 침입자 발견징후 파악, 침입자 발견시 처리, 침입후 사후처리로 나누어진다.

(1) 침입자 침입예방 단계

시스템에 침입자가 침입할 가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다

- 불필요한 계정이나 패스워드가 없는 계정에 대한 조치를 취한다.
- 크랙(Crack) 등의 패스워드 검출 프로그램을 이용하여 침투 가능한 패스워드에 대한 조치를 취한다.
- 보안 진단도구(COPS, SATAN) 등을 이용하여 시스템을 수시로 점검한다.
- 접근통제도구(TCPwrapper, TIS Toolkit)를 설치하여 불법 침입자의 접근을 차단한다.
- 시스템의 로그를 주기적으로 분석하여 시스템의 침입 징후가 있는지 확인한다.
- 최근의 해킹방법 및 대처방안에 대한 자료를 입수하여 즉각적으로 대처한다.

(2) 침입자 발견 징후 파악

시스템관리자는 자신의 시스템에 다음과 같은 비정상적인 활동이나 징후가 보이면 시스템에 불법 침입자가 침투했을 가능성이 있으

므로 점검해야 한다.

- 한 사용자가 둘 이상 로그인 한 경우
- 일반사용자가 컴파일러, 디버거를 사용하고 있는 경우
- 네트워크에 로드를 걸고 이상한 프로그램을 실행한 경우
- 일반 모뎀 사용자가 아닌데 모뎀으로 로그인 한 경우
- 관리자가 아닌데 관리자 명령을 실행하는 경우
- 휴가이거나 근무시간이 아닌데 사용하는 경우
- 일반사용자의 홈 디렉토리에 시스템 파일이 존재하는 경우
- 일반적이지 않은 감추어진 파일(hidden file) 또는 디렉토리가 존재할 경우
- 계정 관련 시스템 파일(/etc/passwd,/etc/shadow 등)에 관리자이외의 접근이 발견된 경우(중복UID, 계정추가 등)

(3) 침입자 발견시 조치방법

침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 다음과 같은 조치를 취한다.

- 접속을 추적한다
  - 내부 단말기에서 침투한 경우에는 현재의 단말 위치를 확인 후 조치를 취한다.
  - 네트워크를 통해 침투한 경우는 침입시스템의 관리자에 연락해 로그를 유지하도록 요청하고 공동으로 대응하도록 한다.
- 대화를 시도한다
  - 역추적을 통해 상대방 시스템을 알아낸 후 talk(1), write(1) 등을 이용하여 침입자의 의도나 요구사항을 알아본다.
  - 역추적을 하기전에 대화를 시도할 수 있으나, 이 경우 침입자가 접속을 끊기 때문에 추적이 불가능 할 수 있다.
- 접속을 차단한다.
  - 침입자를 추적할 자신이 없거나, 해킹으로부터 시스템의 보호가 우선되는 경우에는 접속을 차단한다.

(4) 침입후 사후처리

침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 보안진단도구나 체크리스트를 이용하여 다음과 같은 사항을 점검한다.

- 새로운 계정이 만들어져 있는지를 확인한다.
- 패스워드 파일이 변경되었거나 모드가 변경되어 있는지를 확인한다.
- .rhost 등 외부에서 허가없이 접속 가능한 파일들의 변경유무를 확인한다.
- 특권프로그램(suid, sgid)이 새로 만들어져 있는지를 확인한다.
- 특정파일의 접근모드가 변경되어 있는지를 확인한다.
- 시스템 유틸리티의 변경 및 수정여부를 확인한다.
- 기타, 해킹 스크립터를 이용한 경우 변경될 수 있는 부분을 확인한다.

3.5 보안교육

가. 개 요

공공기관에 근무하는 일반사용자 및 시스템 관리자를 대상으로 전산보안교육을 실시함으로써 보안에 대한 인식을 제고하고 사용자나 시스템 관리자의 부주의나 고의에 의한 보안

사고를 최소화한다.

나. 보안교육 구분

- 시스템관리자 교육
- 일반사용자 교육

다. 교육시기

- 시스템관리자 : 년 1회의 정기교육 및 수시 교육
- 일반사용자 : 년 1회

라. 교육 분야

(1) 시스템관리자

- 전산망 보안일반
- 위험관리 및 위험분석 소개 및 적용
- 보안정책 및 세부보안지침 소개 및 적용
- 해킹방지 도구 및 보안프로그램 소개 및 적용
- 방화벽시스템 소개 및 적용
- 기타 보안관련 내용

(2) 일반사용자

- 전산망 보안일반
- 원내 보안정책 소개
- 관련 지침 및 법령 소개
- 보안취약성 및 대책(사용자 관점)
- 기타 보안관련 내용

3.6 보안관리 조직

가. 조직구성

- 보안총괄 : 보안관련 부서
  - 보안정책 수립 및 보안점검 실시
  - 보안관리를 자동화 할 수 있는 기술개발 및 보급
  - 보안관련 자료 및 기술 제공
  - 보안교육의 실시
- 전산부서(전산실)
  - 전산장비 운영 및 관리
  - 보안기술 적용
  - 보안장비 운영
  - 운영관련 개별 부서 지원
- 개별 부서 : 각 부서의 보안업무담당자 및 시스템관리자

4. 결 론

공공기관은 업무의 성격 및 보유 정보의 형태에 따라 다양한 형태의 보안관리가 필요하다. 따라서 광범위하고 일반적인 형태의 보안지침으로는 개별 공공기관의 특성에 적합한 보안정책이나 세부적인 보안지침을 수립하기 곤란하다. 또한, 개별 공공기관의 보안정책이나 세부적인 보안지침을 수립하기 위해 참고할 수 있는 자료 및 지침은 주로 절차나 방법론 등을 기술하고 있어 개별 공공기관의 실무담당자들이 접근하기가 매우 어려운 실정이다.

아울러, 공공기관의 보안에 대한 인식부족으로 인해 몇몇 기관을 제외하고는 보안관리만을 전담하고 있는 실무담당자가 없을 뿐만 아니라, 전담 실무담당자가 있는 경우에도 전산이나 전산보안에 대한 축적된 기술이 부족해 개별 공공기관의 보안정책 및 세부 보안지침을 수립하기는 역부족인 경우가 많다.

보안정책 및 보안지침 수립에 대한 절차 및 체계적인 방법론은 학술적으로 연구하는 사람

에게는 도움을 줄 수 있지만 우리 나라 공공기관의 현실에 비추어 볼 때 공공기관의 관련 실무담당자에게는 많은 도움을 줄 수 없다고 판단되며, 최선의 방법이 되지는 못하지만 공공기관의 실무담당자들이 손쉽게 개별 공공기관의 보안정책을 수립할 수 있도록 잘 정리된 보안정책 및 보안지침을 제시하는 것도 시급히 필요하다고 생각된다.

공공기관 보안정책 수립을 위한 보안지침서는 크게 보안정책 개요, 분야별 보안지침, 전산센터 운영, 보안관리 절차 및 방법에 대해서 기술하고 있어, 기존의 각종 보안지침에서 언급되지 않은 사항이나 세부적인 보안관리 절차 등에 대해서는 기존의 보안지침을 보강하는 자료로 이용될 수 있다. 그러나 본 지침에서 기술된 내용중에 개별 공공기관에서 적용 받고 있는 기존의 보안지침(국가전산보안업무기본지침 등)과 상충되는 내용에 대해서는 개별 공공기관에서 독자적으로 수용해서는 곤란하며, 수용이 필요한 경우에는 관련기관과의 사전협의가 필요하다.

본 지침서를 통해 공공기관 보안관리 체계 구축에 일조 할 수 있다고 판단되며, 보안정책 및 보안지침 수립에 관한 절차 및 방법론 분야는 향후에도 지속적인 연구가 필요한 분야이다. TTA