通信情報保護學會誌
第2卷 第2號, 1992.3

情報保安을 위한 電算網 組織體系 設計†

백인섭* · 김세헌**

일반적으로 정보시스템에서 정보보안을 위한 조직체계 설계의 근본 개념은 직원들간에 담당업무를 적절히 분리함으로써 직원들간의 상호견제효과를 유지하는 것이다. 이는 오류나 부정의 예방 및 신속한 발견을 위해서 필요한 조치이다. 직무를 적절히 분리하면 정보자산의 보호가 향상되며 전문화로 인한 작업능률의 향상, 크로스 체크에 의한 정확성의 향상, 관리통제시스템의 강화등을 기대할 수 있다. 특히 전산망에 있어서 직무 수행상 알 필요에 따른 기준(Need-to-know)의 원칙에 따라 각 직원들의 기능이 분화되어 업무수행에 무관한 정보를 직원들이 습득하는 것을 제한할 수 있도록 조직체계를 설계해야 한다.

1. 일반적인 정보시스템 조직의 구성

그림 1은 정보시스템 조직의 환경을 그림으로 나타낸 것이다. 이 개략적인 조직도와 다음에서 설명될 설계내용은 여러 조직에 따라 차이가 날 수 있다. 중요한 것은 현재의 조직에 대한 취약점과 리스크를 정의하고, 심층분석하여 정보보안시스템을 구축할 수 있는 합리적인 조직설계를 해야 한다는 점이다.

가. 최고 관리층

조직체의 경영방침과 영업전략 등에 관한 의사결정을 행하는 최고관리층은 시큐리티에 대한 대책의 강구여부에 대한 최종적 판단의 책임도 있으므로 시큐리티에 대한 관리층의 인식은 매우 중요하다.

나. 내부감사부문

내부감사부문은 업무감사와 회계감사외에도 조직체 내의 정보시스템 시큐리티감사도 실시한다. 업무분리가 이루어졌다 하더라도 관련업무담당자들이 공모를 하면 정보의 유용, 변조, 사기 등이 이루어질 수 있다. 이러한 것을 방지하기 위해 정기적으로 감사를 수행하여 체크하고 추후 그 성과도 감독할 필요가 있다.

감사부분을 세분화하면, 응용 시스템 감사, 시스템 개발 감사, 일반적 업무 절차에 대한 감사, 안전통제에 관한 감사, 시스템 소프트웨어의 감사, 보수절차의 감사 등이 있는데, 안전 통제에 관한 감사는 매우 중요하며 빈번히 실시되어야 한다.

다. 시큐리티 관리자

조직체에서 시큐리티를 확보하기 위해서는, 모든 부문의 시큐리티를 통괄하고, 조직전체를 대표해서 최고 관리층에 시큐리티 상태를 직접 보고하며, 기업전체의 시큐리티를 확보할 책임을 질 시큐리티 관

† 본 연구는 한국전산원 표준사무부 전산망 안전 및 보안관리 표준화연구회의 '91년도 수행과제인 "국가기간 전산망시스템의 안전관리체계에 관한 연구"에서 요약 발췌한 내용임.
* 정회원, 한국전산원 표준연구본부장
** 정회원, 한국과학기술원 경영과학과 교수

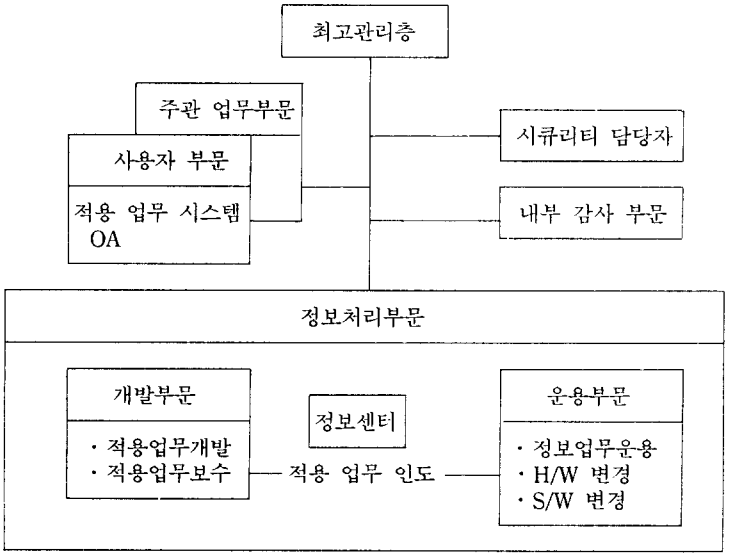


그림 1. 정보 시스템의 개략적인 조직도([17] 일부 수정)

리자를 임명할 필요가 있다.

시큐리티 관리자는 전사적인 시큐리티 문제에 대한 주관 부서가 되며 정보처리 자산의 보호에 관한 규정을 작성하는 것 외에도 다음과 같은 것을 실시할 책임이 있다.

◦ 조직체의 시큐리티 대책의 실시도에 관하여 목표를 설정한다. 예를 들어 전 사원의 시큐리티에 관한 지식을 높이기 위한 대책으로서 시큐리티 교육을 실시한다. 전 사원에 대한 교육을 연간 몇 % 실시할 것인가 하는 것이 대책 실시도의 목표가 된다.

◦ 주관부문과 사용자 등에 대해, 시큐리티에 관한 조언과 컨설팅을 실시한다.

◦ 가이드라인과 각종 규정을 작성한다.

◦ 시큐리티의 평가 수법을 개발한다. 예를 들어, 규정, 기준과 수속의 준수도를 체크 방식으로 채점하여 평가한다.

◦ 각 부서 단위에 시큐리티에 관한 담당자를 배치하도록 추진한다. 시큐리티 관리자와 그 스태프만으로는 전 사원에게 철저할 수가 없으므로 시큐리티 담당자를 배치하여 시큐리티 관리의 집행자 역할을 대행하는 동시에 그 부서의 시큐리티 확보를 위해 노력하도록 한다.

◦ 시큐리티에 관하여 교육을 실시한다. 말하자면, 시큐리티란 무엇인가? 왜 시큐리티가 중요한가? 시큐리티 확보의 필요성의 인식, 보호할 만한 자산의 식별 등을 포함한 내용의 교육을 실시한다.

◦ 정보자산의 보호상태에 관해 조직 전체적으로 준수도를 모니터링해서 최고 관리층에 보고한다.

위와 같이 시큐리티를 조직 전반에 걸쳐 추진할 전문 스태프를 채용하자면, 최고 관리층의 후원이 필요하다. 한편 시큐리티를 추진하는 과정에서 반드시 시큐리티 관리자가 부딪치는 문제는 "번기롭기 짝이 없다", "생산성이 없다"등 직원으로부터 나오는 반발이다. 이것은 한 조직이 시큐리티를 확보하는 것이 무엇을 위해서, 누구를 위해서인가에 대한 이해 부족에서 비롯된다. 한 조직이 시큐리티를 확보하는 것은 직원을 모든 문제로부터 보호하기 위해 실시하는 것이다. 또, 조직이 손해를 입는 것은 직원이 손해를 당하는 것이고 그 손해가 크면 조직의 존속이 위태롭게 된다는 것을 인식해야 한다.

라. 주관부문, 사용자 부문, 정보처리 부문

주관부문의 업무가 정보처리 부문에서 컴퓨터로 가동되고 있는 경우에도 업무운영의 책임은 어디까지나 해당업무의 주관부문에 있다. 업무를 기계화한다는 것은 그 운영을 컴퓨터로 처리한다는 것 뿐이기 때문이다. 정보시스템에는 적용업무의 기획 및 개발의 책임을 지는 주관부분, 컴퓨터 시스템을 운영하는 정보처리 부문, 그리고 단말기 등을 이용해서 업무를 수행하는 사용자 부문이 있다. 예를 들면, 인사정보업무의 경우, 주관부문은 인사부문이 되고, 컴퓨터로 그 적용업무를 가동시키는 부문이 정보처리부문이 되고, 가동되고 있는 시스템을 이용하는 부문이 사용자 부문이 된다. 주관 부문이 동시에 사용자 부문이 되기도 한다.

1) 주관부문

주관부문은 적용업무의 책임자가 되며 업무의 처리과정을 숙지하고 있어야 한다. 적용업무의 시큐리티를 확보하기 위해서 주관부문은 정보자산의 가치 및 중요성을 십분 인식하고 다음과 같은 대책을 강구할 의무가 있다.

◦ 정보자산의 취급을 규정대로 운영관리 하기 위해 정보의 기밀도 구분을 한다.

◦ 적용업무의 기획 및 개발 단계에서 각종 사업상의 통제와 필요한 가감사성(Auditability)의 구축을 요구하며, 시스템 시동 전에 요구한 대로 되어 있는지 확인한다.

◦ 적용업무시스템의 사용방법과 오류의 회복과정 등이 사용자에게 충분히 교육되고 있는 지를 확인한다.

◦ 적용업무의 가동상황, 액세스 관리, Recovery의 순서, 기밀도 구분에 합당한 관리가 규정대로 정확히 운영되고 있는지 정기적으로 확인한다.

◦ 운영에 있어서는 리스크분석, 리스크 평가, 대책 선택의 타당성을 확인한다.

◦ 적용업무시스템을 이용해서 업무를 수행하는 사용자에 대해, Need-to know의 원칙에 의하여 액세스 권한을 부여한다. 또 액세스 권한 부여 리스트를 보유한다.

◦ 자연재해 또는 화재 등 예측이 불가능한 사태가 발생해서 장기간에 걸쳐 컴퓨터가 정지할 때의 백업체제, 경우에 따라서는 컴퓨터 시스템이 없는 상태에서의 업무수행을 위한 예측불허사태를 위한 계획에 참여한다.

3) 사용자 부문

사용자는 적용업무 시스템을 이용하여 On-line/Off-line, 개인용 컴퓨터 및 오피스 컴퓨터를 사용해서 일상업무를 수행하는 부서이다. 사용자 부문은 주관부문과 정보처리 부문이 정한 규칙/수속에 따라 다음 항목을 수행할 책임이 있다.

◦ 업무목적 이외에 정보처리기기를 사용해서는 아니된다.

◦ 사용자 측에 설치되어 있는 정보처리 기기를 보호/관리한다.

◦ 정보자산의 액세스에 관해 주관부문의 허가를 받아, 허가된 정보자산에만 액세스한다.

◦ 정해진 방법에 따라 패스워드의 관리 및 갱신을 행한다. 통상 패스워드의 갱신은 정보처리 부문에서 패스워드 발생장치를 이용해서 갱신하지만, 사용자가 패스워드를 지정하는 시스템에서는 타인에게 노출되지 않도록 패스워드를 선정하는 것이 필요하다.

3) 정보처리 부문

정보처리 부문에는 적용업무의 개발 및 보수를 수행할 그룹과 적용업무를 운용하며 사용자의 요구에 합치하도록 하드웨어와 소프트웨어의 변경을 실행하는 운용 그룹이 있다. 또 사용자에 대한 개인용 컴퓨터와 사무자동화의 기술적 지원을 하고 사용자의 의문 및 질문에 답해 줄 Help Desk로서의 정보 센터가 있다. 정보처리 부문은 주관부문의 지시에 따라, 주관부문과 사용자 부문에 대해 서어비스를 제공할 역할이 있으며, 다음을 실행할 책임이 있다.

◦ 모든 정보통신망 시스템의 안전관리를 행한다.

◦ 각 적용업무가 서로 간섭받지 않고 다른 시스템으로부터도 간섭 받지 않음을 확인한다.

◦ 각 정보자산을 주관부문이 규정한 취급방법에 따라 관리한다. 예를 들어 기밀정보는 그 기밀도 구분에 따른 액세스 관리를 실시한다.

◦ 사용자에 대해 가동시간대(적용업무의 서어비

스 시간)등을 알려 놓는다.

2. 정보처리 부문의 직능별 분화

정보처리 부문은 정보 처리 부장, 시스템분석가, 프로그래머, 컴퓨터 작동 요원, 자료 입력 요원, 라이브러리안 등으로 직무가 분리된다. 또한 무엇보다도 사용자 부서와 조직적으로 독립되어 있어야 함은 물론이다.

정보처리 부문의 기능은 기본적으로

- 전체적인 정보처리 조직 운영
- 시스템 개발과 프로그래밍
- 데이터의 전산 처리

등의 분야를 갖추어야 한다.

가. 정보처리 조직 내의 기본 직무의 분리

정보처리 부문에서 분리해야 할 세가지 주요 직무와 그에 대응하는 직위를 관련 지워 표 1로 나타내었다.

표 1. 정보처리 부문에서 분리해야 할 직무와 직위

정보처리 부문의 직무	직 위
시스템의 개발과 보수 분석 및 설계 프로그래밍	 시스템 분석가 프로그래머
시스템 운영	오퍼레이터
시스템 통제 데이터 처리 통제 화일, 문서류의 보관 및 통제 DB 관리와 통제	 데이터 처리 통제요원 라이브러리언 DB 관리자

정보처리 부문의 조직의 크기가 작을 경우, 시스템 분석과 프로그램을 한 직종으로 보아도 되나 시스템의 개발 작업과 그 운영은 분리시켜야 한다.

또, 다음과 같은 중요한 정보처리업무를 담당하는 요원들은 자신의 책임영역 이외의 정보처리 기능에 대해 자세히 아는 것은 바람직하지 않다.

- 데이터 처리 요원
- 데이타 입력 통제 및 스케쥴링 요원
- 시스템 분석 및 프로그래밍 요원
- 응용시스템 분석 및 프로그래밍 요원
- 미디어 라이브러리언
- 시스템 사용자

직무분리는 물리적인 장애물을 설치하거나 데이터처리, 시스템 접근에 필요한 절차들을 만들어 그 효과를 높인다.

다음은 일반적인 직무분리의 내용이다.

- 프로그래머는 컴퓨터 오퍼레이터가 될수 없다.
- 오퍼레이터는 프로그램을 쓰거나 제공 못한다.
- 오퍼레이터는 미디어 라이브러리에 들어가지 못한다.
- 미디어 라이브러리언은 미디어를 설치하지 못한다.
- 프로그래머는 데이타처리 미디어를 소유할 수 없다.

나. 정보처리 부문의 조직도

정보처리의 조직도는 현재의 권한과 위임 계통을 반영하며 감독 기능의 존재, 직무의 분리를 명확히 나타내어 준다. 조직도를 직원에게 배포하는 것은 직무에 대한 자각과 명령 계통에 대한 이해를 높여 준다.

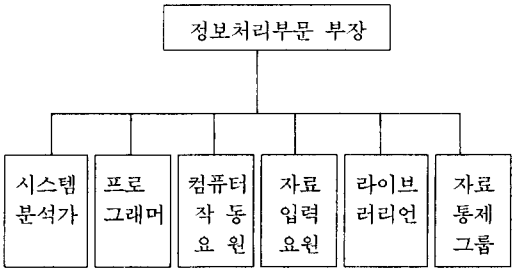


그림 2. 단순화된 정보 처리 부문의 직능별 분화 ([17] 일부수정)

그림 2의 직능별 분화는 단순화된 것이며 조직의 성격 및 규모에 따라 세분화될 수도 있다.

1) 정보처리 부문 부장

부장은 전반적인 통제와 장단기의 계획을 개발하고 시스템을 승인한다. 또한 정보 처리 부문은 주관부문의 지시에 따라 주관부문과 사용자 부문에 대해 서어비스 할 책임이 있으며, 이 모든 것에 대한 감독의 상위 책임자는 부장이 맡는다. 세부적으로 보면, 부장은 정보처리부문 관리자로서 사용자의 정보통신망에 대한 액세스가 적용업무를 주관하는 부문의 관리자가 설정한 액세스 권한의 범위 안에서 이루어질 수 있도록 액세스 컨트롤을 행할 책임을 지고 있다. 따라서 다음 사항을 지휘, 감독할 책임을 진다.

- 송신 및 수신 단말기(또는 마디) 확인
- 사용자 식별 및 인증
- 허가된 루트를 통한 정보의 전송 확인
- 시스템 자원의 불필요한 사용 불허 확인
- 통신 종료시에 확실한 Log-off 확인
- 상황의 모니터 및 기록(여기에는 비상시 경보를 울리게 하거나 통신을 단절시키는 것도 포함된다).

이를 위해 부장은 각 사항에 대해 조직상황에 적절하게 담당자를 두어 그 부문에 책임을 할당할 수 있다. 즉 단말 및 통신회선 관리자를 각각 선정해 그 역할을 명시해서 책임을 지도록 함이 바람직하다. 그리고, 정보처리 부문의 부장은 전 정보시스템의 포괄적인 보안과 정보처리 자산의 보호를 위해 다음과 같은 역할을 수행한다.

- 정보처리 자산 보호에 관한 문제에 관해 부문수준의 중심점이 되어야 한다.
- 정보처리 자산 보호요구를 분석하고, 기업의 정보 시스템과 의사교환을 하고, 부문내의 정보처리 서비스의 공급자와 의사교환을 한다.
- 정보처리 자산 보호의 목표를 부문차원에서 만들고, 조직차원에서 정보처리 자산 보호의 정책, 목표, 방향설정을 부합하여 자체 부문 수준의 정보처리 자산 보호의 정책, 목표, 방향설정을 부합하여 자체 부문수준의 정보처리 자산보호의 정책, 목표, 지침등을 만들고 공표한다.
- 시큐리티 관련 시행세칙, 방향, 지침등을 재검토한다.
- 정보처리 서비스의 공급자가 정보 처리 자산 보호 책임과 요구에 부응하여 효과적인 교육, 방향이 제공되고 있는 지를 확인한다.
- 정보처리 자산 보호의 책임을 가지는 주요 정보시스템 인력의 배치에 관한 상담을 해준다.
- 정보처리 서비스 공급자들이 효과적으로 정보처리 자산 보호의 계획 설립, 프로그램 개발에 지원을 하고 있는 지를 확인해야 한다.
- 정보처리 자산 보호에 대한 자체평가 활동을 지원해주고, 부문수준의 전략적, 시행적 계획으로서의 정보처리 자산 보호를 준비해야 한다.
- 내부 감사자, 사용자, 소유자 시큐리티 스탭들의 교육을 보조해주어야 한다.
- 정보처리 자원 공급자의 정보처리 자산 자체평가를 하고, 정보처리 자산 요구를 준수하고 있는 지를 검사한다.
- 정보처리 자원의 공급자가 전략적 계획, 시행계획, 정보처리 자산 보호 계획, 감사에의 답변, 정보처리 자산 보호등에 효과적으로 참여하고 있는지 검토한다.

2) 시스템 분석가

현존 시스템을 평가하고 새로운 시스템을 설계하며 프로그래머를 위한 명세서를 작성한다. 시스템 분석은 현재의 시스템을 분석하여 가능한 해결책을 모색한 후 새로운 또는 개선된 시스템 설계를 하게 되므로 시스템 설계에서 매우 중요한 단계라 할 수 있다.

3) 프로그래머

컴퓨터 프로그램의 논리를 플로차트화 하고 프로그램을 개발하여 문서화하며 프로그램의 에러 관리를 담당한다. 응용 프로그래머는 시스템 프로그램을 수정하거나 접근할 수 있어서는 안되고 응용 프로그램에 대한 인가된 수정만 할 수 있어야 한다. 사전승인된 프로그램 수정을 하고 싶은 프로그래머는 자기 개인 라이브러리에 소스코드를 카피한다. 그리고 이 프로그램을 자신의 라이브러리 안에서 수정보완한다. 작업이 끝나면 소스코드를 컴파일하여 오브젝트코드를 얻은 후 테스트 전용 라이브러리로 카피해 간다. 테스트가 끝나면 프로그래머는 프로

그램 변경신청서를 작성하여 관련 상급자에게 허가를 받는다. 이후 라이브러리안으로 하여금 수정된 마스타 프로그램을 카피해 가도록 한다.

4) 컴퓨터 작동요원

컴퓨터 하드웨어를 작동하며 컴퓨터 작동지시에 따라 프로그램을 집행한다. 이 작동요원 이외에는 기기에 허가없이 액세스할 수 없도록 한다. 그리고 작동요원에게는 작동에 필요한 업무처리나 프로그래밍, 문서화에 관한 지식만을 제공받도록 해야 한다.

5) 자료 입력 요원

자료를 기계가 판독할 수 있는 저장매체로 기록한다. 데이타가 원천자료로부터 컴퓨터가 판독할 수 있는 카드나 테이프로 전환되거나 Teletype 혹은 장거리 터미날같은 수단을 사용하여 직접 입력되기 때문에 이 입력요원의 경우 전산화 자료처리 과정 중 가장 많은 양의 업무처리를 하므로, 안전면에서 매우 취약한 부분이라 할 수 있다. 모든 거래 입력 자료는 일반적 승인 또는 특별 승인절차에 따라 승인된 것이어야 함을 유의한다.

6) 라이브러리안

시스템 문서, 프로그램, 그리고 화일을 관리한다. 라이브러리에 보관되어 있는 것들의 가치를 생각하면 이 라이브러리안의 직무가 매우 중요함을 알 수 있다. 모든 데이타 화일, 프로그램 화일 그리고 문서류는 라이브러리안의 관리하에 보관하도록 해야 한다. 백업용 복사판도 라이브러리에 보관할 수 있지만 전용보관 시설에 보관하는 수가 많다. 라이브러리안은 보관장소에 관계없이 이들 자료에 대한 책임이 있으며 언제라도 특정자료의 소재를 알 수 있도록 체크아웃 절차를 확립해 두어야 한다.

라이브러리안에 관련된 주요 직무 및 유의사항은 다음과 같다.

◦ 모든 화일 및 문서들의 물리적인 위치에 대하여 책임을 진다.

◦ 처리에 사용되지 않은 것, 또는 처리예정에 없는 것은 라이브러리안의 관리하에 두어야 한다. 이들의 대출은 컴퓨터처리 예정표 또는 서명이 되어있는 승인서를 토대로 이루어져야 하며 반납도 같은 컴퓨터 처리 예정표 또는 승인서에 따라 하도록 한다.

◦ 자료를 라이브러리에서 꺼내고 반납하는 권한은 라이브러리안에게만 주어야 한다. 바꾸어 말하면 오퍼레이터, 프로그래머 등이 라이브러리에 출입할 수 없도록 해야 한다. 이를 위해 라이브러리안은 특정화일에 액세스할 수 있도록 승인된 사람의 명단을 보관하고 있어야 하는데 이것은 화일 대출을 승인받은 자에게만 한정시키기 위한 것이다.

위와 같이 라이브러리안의 역할은 매우 중요하며 아주 큰 컴퓨터 센터에는 여러 사람의 라이브러리안을 둘 수 있다. 소규모 컴퓨터 센타인 경우에는 전담 라이브러리안을 둘 필요는 없겠지만, 감사인은 특정인이 라이브러리 담당자로 정해져 중요한 자산에 대한 통제의 책임을 지고 있는가를 확인해야 한다.

7) 자료 통제 그룹

주관부문 및 사용자 부문과 연결을 하며, 처리될 모든 자료를 수령하고 선별하며 모든 입력자료에 대한 일종의 회계처리를 하며, 거래오류를 추적하고, 출력문서의 배포 등을 감시하는 일을 맡는다.

이상에서 우리는 정보처리 부문의 직능별 분화에 대해 간략히 살펴 보았다. 이것은 조직의 성격과 규모에 따라 다를 수 있다. 조직의 특성에 따라 위의 분화 외에도 단말기, 통신회선 관리자를 따로 두어 그 부분에 책임을 지우게 하여, 정보통신망 시스템의 전반적인 경비 관리자를 두는 것이 바람직 하다.

8) 대규모의 정보처리 조직

그림 3은 대규모 정보처리 조직의 한 예이며, 위에서 살펴본 단순화된 정보처리 조직에 데이터베이스 관리자, 품질보증담당관리자, 데이터 보안 담당자, 네트워크 관리자 등을 두고 있다.

정보처리의 기능에 대해 직무를 명확히 정해 둘 필요가 있다. 직무는 각 부문의 관리자가 결정하지만, 내용은 정보처리 시설의 규모와 복잡함을 반영하여야 한다. 직무의 명확한 분리를 위해서 직무기술서의 작성이 필요하며, 직무 기술서는 직무의 분

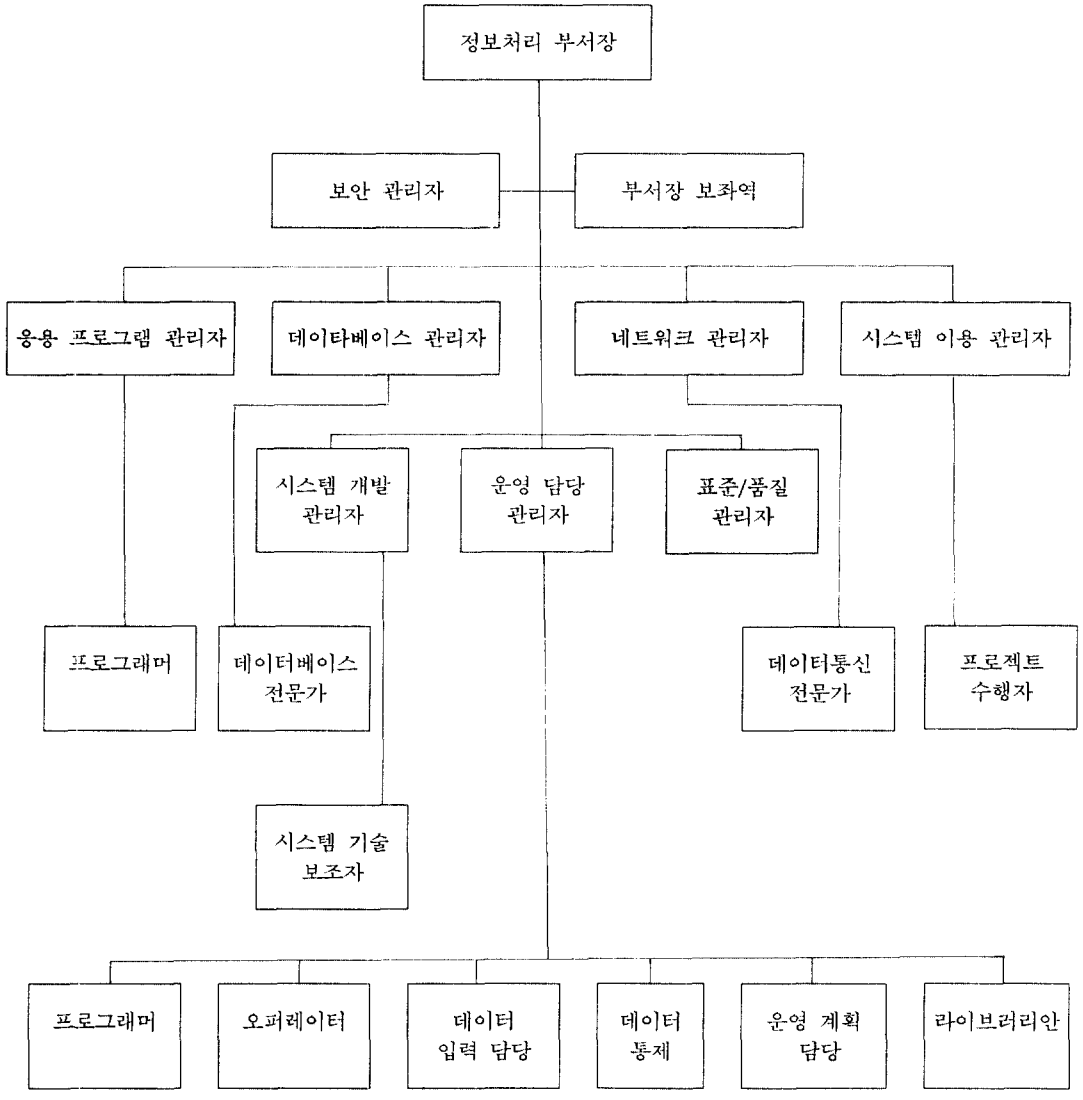


그림 3. 대규모 데이터 처리 조직의 예([19] 일부수정)

담, 책임, 보고의무의 소재등을 명확히 하고 각 직원의 업무 내용을 담고 있어야 한다. 그리고 직원에 대해서 주어진 모든 내용에 대한 교육을 시행하여야 한다.

3. 시큐리티 담당부서의 조직설계

시큐리티 담당부서의 조직설계는 부서의 역할을 명확히 하고 정보시스템 조직 전체 내에서 어떤 위치에 부서를 위치 시키는가가 중요한 고려 사항이 된다.

가. 시큐리티 담당부서의 기본 기능

조직 내의 보안을 위한 시큐리티 기능을 갖기 위해 시큐리티 담당부서는 조직 내에서 다음과 같은 기본 기능을 행하여야 한다.

- 시큐리티 통제에 관한 제안
- 시큐리티 자체 평가
- 통제의 시행에 있어서의 보조
- 사용자, 관리자에게의 시큐리티 교육
- 시큐리티 정책, 기준, 가이드라인의 제공
- 시스템 개발에의 참가
- 컨틴전시 계획 : 예상되는 각각의 긴급상황에 대응할 수 있는 방안들에 대해 구체적인 계획을 수립한다.
- 시큐리티 경영(예 : ID, Passward관리)
- 불법적행위, 횡령들의 발견과 사전대비
- 시큐리티에 관한 책임과 직무를 설정, 유지, 변경
- 대상이 되는 시큐리티 환경의 체크
- 조직 시큐리티와 관련된 제품, 용역의 선정과 평가

나. 조직 내의 위치 선정 기준

1) 수직적 위치 기준

일반적으로 시큐리티 부서의 레포팅 대상을 의미하며, 최고 관리자를 대상으로 하거나, 중간관리자를 대상으로 하거나, 또는 일선 관리자에게 할 수 있다.

2) 수평적 위치 기준

주된 레포팅 책임 영역을 말한다. 수직적인 위치는 단순히 레포팅의 수준을 나타내는 반면, 수평적 위치란 보고대상의 구체적인 조직 부문을 나타낸다. 예를 들어 정보처리부장에게 보고를 한다든지, 감사부장에게 보고를 한다든지 하는 것이다.

전통적으로 시큐리티 기능은 기존의 정보처리 부문에 깊게 내재되어 있었다. 그러나 시큐리티 문제는 정보처리 부문에서 사소히 다루어졌다. 왜냐하면 정보시스템의 성과는 단순히 생산성으로 평가되어 졌기 때문이다. 예를 들면 컴퓨터 시스템으로의 접근의 신속성, 용이성, 효율성등이 주된 성과평가의 측면이 되어 왔다. 위와 같이 정보처리 부문과 시큐리티 기능의 성과평가의 측면이 다르므로, 시큐리티 부서의 독립적인 운영이 요구된다. 또한 시큐리티 부서의 수직적 위치는 높은 위치를 필요로 한다. 낮은 위치에 있다면 시큐리티의 감사역할이 하급자 역할로 왜곡될 수 있기 때문이다.

다. 시큐리티 담당부서의 조직상의 독립성의 정도와 내부직무 분리

조직내 관리자들이나 관리대상들과 독립적일수록, 실질적이고 장기적인 이익을 가져다주는 편향되지 않는 시큐리티 관리를 가능하게 한다. 예를 들어 만약 암호 시스템의 설계자가 암호키 관리도 수행한다면 관심(목적)의 갈등현상이 발생하거나, 전문화가 어렵게 되므로, 직무 분리의 기본원리를 고려하여 시큐리티 부서내의 하부그룹들을 적절히 분리하는 것이 필요하다.

시큐리티 담당부서는 컴퓨터, 데이타통신 기법 등에 대해 기본적인 지식을 가지고 있는 상부관리자나, 주요 정보처리 부서장등에게 직접적인 보고를 해야 한다. 이들 보고대상자들은 충분한 지식을 가지고 최고경영자와 시큐리티 관리에 대해 의논할 수 있어야 한다.

다음은 그림 4에 나타난 각 구성요소들에 관한 논의이다.

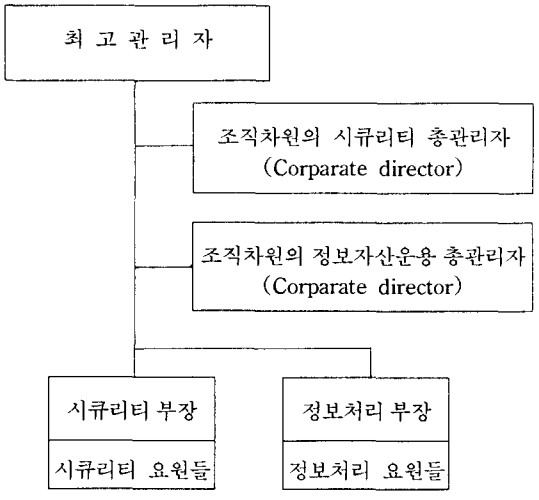


그림 4. 시큐리티 관련 부서([8] 수정)

1) 조직차원의 시큐리티 총관리자의 역할

◦ 조직 시큐리티의 목표를 설정한다.

◦ 조직 시큐리티 시행세칙, 명령, 표준, 지침을 만들고 시큐리티 정책을 시행한다.

◦ 제안된 정보처리 자산 보호의 시행세칙, 명령, 지침을 검토한다.

◦ 정보처리 서어비스의 사용자, 정보처리 자산의 소유자, 시큐리티 부문의 스탶에 대해 상담을 하고 충고 방향 등을 제시한다.

◦ 사업 시행계획과 전략적 계획에서 시큐리티에 관련된 사항을 검토하고, 직면한 시큐리티 잇슈들을 해결한다.

◦ 조직 전체의 시큐리티 문제에 관해 조직수준의 중심점이 되는 역할을 한다.

◦ 정보처리 자산 보호에 관한 안전사건들을 감시한다.

◦ 시큐리티 적용을 위한 정보처리 시스템을 만들고, 평가, 추천한다.

◦ 시큐리티 스탶, 정보처리 서어비스의 사용자, 정보처리 자산의 소유자들이 효과적으로 정보처리 자산 보호 책임과 요구들에 관한 교육과 방향이 제공되는 지를 확인한다.

◦ 시큐리티 시스템의 효과를 평가할 수 있는 기법을 개발한다.

◦ 조직전체를 통해 정보처리 자산 보호가 제대로 수행되는 지를 검토한다.

2) 조직차원의 정보자산 운용 총관리자의 역할

◦ 정보처리 자산 보호의 문제들에 관해 조직수준의 중심점이 된다.

◦ 필요하고 가능하다면 정보처리 자산 보호 능력을 키우기 위하여 내부적 노력을 한다.

◦ 조직 시큐리티 정책, 목표, 방향을 지원하는 차원에서 정보처리 자산 보호의 목표를 설정하고 정책을 추천한다.

◦ 조직 시큐리티 정책, 목표, 방향을 보완하는 차원에서 정보처리 자산 보호의 시행세칙, 방향, 지침을 설정, 공표해야 한다.

◦ 조직 시큐리티 관련 시행세칙, 방향, 지침을 검토한다.

◦ 정보처리 자산 보호에 관하여 조직수준의 방향을 제공한다.

◦ 정보처리 자산 보호 책임을 가지는 인력의 조직부문에 배치하는 것을 상담한다.

◦ 정보처리 서어비스의 제공자들에게 정보처리 자산 보호의 책임과 요구에 관해 효과적인 교육과 방향이 제시되는지를 확인한다.

◦ 정보처리 자산 보호에 관해 정보처리 서어비스의 운용, 정보처리 서어비스의 공급자들이 제대로 부응하고 있는 지 확인한다.

◦ 정책, 시행계획 등의 정보처리 자산 보호의 요소들을 검토하고, 정보처리 공급자에 대한 계획의 참여성과를 검토한다.

◦ 감사나, 사용자, 소유자, 시큐리티 스탶들의 교육을 후원해야 한다.

3) 시큐리티부장

◦ 조직 전체의 시큐리티 목표에 준하여 부문수준의 시큐리티 목표를 선정한다.

◦ 조직차원의 명령, 회사 정책을 기반으로 시큐리티 부문의 시큐리티 시행 세칙, 명령, 지침 등을 만든다.

◦ 제안된 시큐리티 부문의 정보처리 자산 보호에 관한 기준, 명령, 지침의 시행안을 검토한다.

◦ 조직 시큐리티 문제에 관해 부문수준의 중심점 역할을 한다.

◦ 정보처리 자산 보호에 관해 감사를 한다.

◦ 시큐리티의 실행을 위해 사용될 정보처리 시스템을 추천한다.

◦ 정보처리 자산 보호의 책임, 요구에 관해 시큐리티 스탶, 정보처리 서어비스 사용자, 정보처리 자산 소유자들이 효과적인 교육과 방향을 공급받는 지를 확인한다.

◦ 시행되는 시큐리티 시스템의 효율성을 검토한다.

4. 전산망 관리 조직도

그림 5의 조직도는 앞에서 부분적으로 언급된 내용들을 전체의 전산망을 구성하기 위해 통합한 것

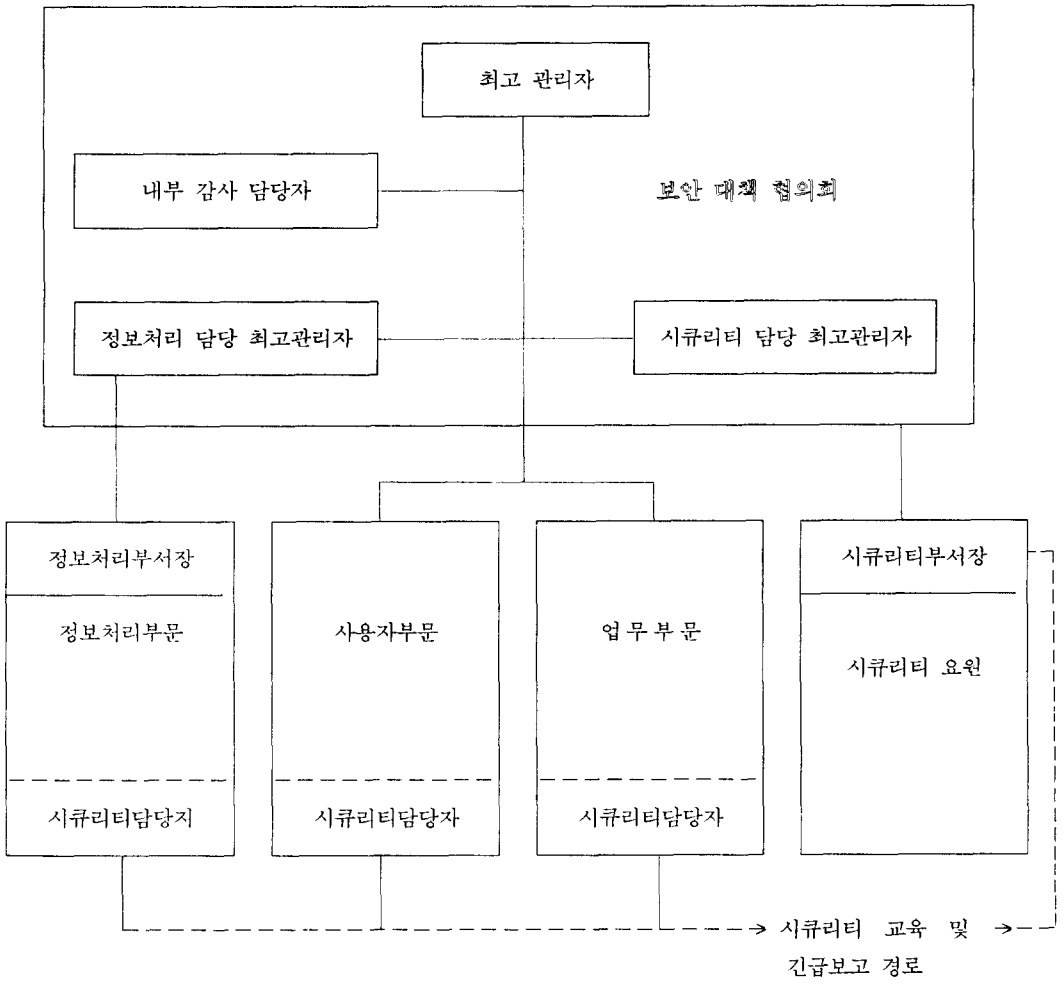


그림 5. 전산망 시큐리티 관리의 조직도

이다.

제안된 전산망의 조직도는 정보처리 부서장과 시큐리티 부서장을 독립시켜 역할의 분담을 통한 상호 견제 위치에 있게 하였다. 정보처리 부서장과 시큐리티 부서장은 최고 관리자의 통제 영역안에 있음은 물론, 각부문의 최고관리자에게 보고의 의무를 진다.

정보처리 부문에서 추구하는 효율성과 시큐리티 부문의 목적인 안전성은 상호 배치되므로 그로부터 야기되는 갈등은 최고 관리자, 내부 감사 담당자, 정보처리 부문 최고 관리자, 시큐리티 최고관리자 등에 의해 구성되는 보안 대책 협의회에서 해소하게 된다. 이는 정보처리 부문과 시큐리티 부문의 실무적인 독립성의 보장을 더욱 공고히 하기 위함이다.

그 밖에, 시큐리티 부서장은 업무 지휘 계통의 조직 밖에 시큐리티의 지휘계통 조직을 업무조직에 밀착시켜 구축한다. 그 조직의 시큐리티 담당자는 각 부서의 장이 임명한다. 지명된 부서의 시큐리티 담당자는 통상업무외에 통상업무와 동일한 레벨로

시큐리티 확보에 대한 업무를 맡는다.

각 부서의 시큐리티 담당자의 수는 조직과 장소에 따라 차이가 있으나, 20~30명에 1인 정도로 지명한다. 일반적으로 업무의 조직단위에 따라서 시큐리티 부서장이 임명된다. 이렇게 해서 지휘계통이 구축되면 시큐리티에 관한 모든 지시는 이 지휘계통을 따라서 이루어지게 한다. 예를 들어, 전 사원에 시큐리티 교육을 실시하도록 요청받는 경우, 각 부서에 임명되어 있는 시큐리티 담당자에 대한 시큐리티 교육은 시큐리티 부서장이 실시한다. 교육을 받는 각 부서의 시큐리티 담당자는 그 부서에 소속되어 있는 모든 사원에게 시큐리티 교육을 실시할 책임이 있다. 그러나 교육을 포함해 시큐리티 확보의 최종책임자는 라인 관리자임을 잊어서는 아니된다. 시큐리티에 관한 보고서는 라인 관리자가 통상업무 지휘계통을 통하여 상부의 라인 관리자에게 보고하게 된다. 그러나, 긴급의 경우 시큐리티 부서장에게 직접 보고할 수 있다.

여기에 제시된 전산망 관리의 조직도는 하나의 방향이며, 완전한 시스템이 한번에 구축될 수는 없는 것이다. 따라서, 전산망의 종류에 따라 다르겠지만 항상 자체적인 감사 및 외부의 감사를 통하여 리스크를 식별하고, 그에 대한 대책을 수립해 나가는 과정에서 보다 안전한 시스템이 구축될 것이다. 조직설계에 대한 표준의 방법이 없음은 각 전산망의 내용과 상황이 상이할 것이기에 너무나 당연하다. 그러나 분명한 것은 적절한 업무 분담을 통한 상호 견제 및 보완을 유지하도록 설계되어야 하며, 그것보다 더 중요한 것은 최고 관리층 및 직원들의 인식으로서, 항상 조직의 리스크에 대한 식별과 이에 대한 보다 개선된 안전통제의 조직체계 및 그 규범에 적응하려는 자세이다.

참 고 문 헌

1. 김세헌, 컴퓨터범죄와 프라이버시 침해, 희성출판사, 1989.

2. 김세헌, 정보통신망의 정보보안체계 설계에 대한 종합적 연구, '89전기통신학술연구과제, 한국과학기술원 경영과학과, 1990.

3. R.L. Daft, *Origanization Theory and Design*, 1986.

4. D. Davies and W. Price, *Security for Computer Networks*, John Wiley Sons, Reading, 1984.

5. D.E. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, 1983.

6. W. Diffie and M. Hellman, "Privacy and Authentication : An Introduction to Cryptography," Proc. IEEE, Vol.67, No.3, 1979.

7. A. Ditri, J.C. Slaw and W. Atkins, *Managing the EDP Function*,

8. R.P. Fisher, *Information System Security*, 1984.

9. J. Lobel, *Foiling the System Breakers*, McGraw-Hill, New York, 1986.

10. I.C. Palmer and G.A. Potter, *Computer Security Risk Management*, Van Nostrand Reinhold, New York, 1990.

11. W. Price, *Progress Towards Data Security Standards*, System Security Online Publication, Pinner, UK, 1985.

12. J.A. Schweitzer, *Protecting Information in the Electronic Workplace - A Guide for Managers*, Reston, 1983.

13. D.W. Straub, "Organizational structuring of the computer security function," Computer Security, Vol.7, pp.185-195, 1988.

14. R. Sugarman, "On foiling computer crime," IEEE spectrum, 1979.

15. M.M. Wofsey, *Advanced in Computer Security Management : Vol 2*,

16. C.C. Wood, "Information system security : Management sucess factors," Computers and Security, Vol.6, pp.314-320, 1987.

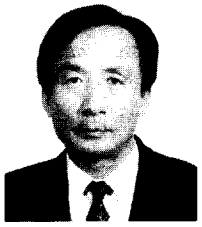
17. 上園忠弘, 小林孝夫, 山本明知, 情報システムのセキユリテイコソトロール, オ-ム社1988.

18. 情報化白書 1988, 日本情報處理開發協會, 1988.

19. 會計監査とユソヒユ-タ, 日本公認會計士協會電子計算機會計委員會, PMC出版, 1988.

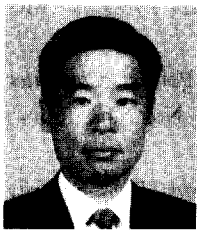
□ 著者紹介

백 인 섭



1963년~1969년 서울 대학교 공과대학 전기공학과(학사)
1973년~1975년 한국과학기술원 전산학과(석사)
1976년~1981년 프랑스 ENSIMAG 대학 컴퓨터 공학(박사)
1970년~1976년 한국과학기술원 부설 전산개발센터 전산기술과장
1982년~1983년 프랑스 국립 컴퓨터 연구소(INRIA) 선임연구원
1983년~1989년 한국데이타통신(주) 정보통신연구소장
1989년~ 현재 한국전산원 표준연구본부장

金 世 憲



서울文理大 物理學科 卒業
美 Standford大(經營科學 碩士 및 博士)
美 System Control, Inc 社 勤務
現 韓國科學技術院 經營科學科 教授, 本 學會 論文誌 編輯委員長
關心分野 : 컴퓨터 犯罪와 프라이버시 侵害 防止 對策, 情報시스템 保安, 暗號學