□ 研 究 論 文 □

韓國國防經營分析學會誌
第 27 券, 第 1 號, 2001. 7. 2.

BS7799(정보보안관리 표준)를 적용한 국방정보체계 보안감사모델에 관한 연구 (A Study on an Audit Model for the Defense Information System Security using BS7799)

최장욱*, 남길현*

Abstract

Information technology has been made remarkable progress and most of computer systems are connected with internet over the world. We have not only advantages to access them easy, but also disadvantages to misuse information, abuse, crack, and damage privacy. We should have safeguards to preserve confidentiality, integrity and availability for our information system.

Even though the security is very important for the defense information system, we should not over limit users availability. BS7799, a British standard, is an evaluation criteria for information security management.

In this paper we propose an audit model to manage and audit information security using control items of BS7799, which could be useful to manage the defence information system security. We standardize audit items, and classify them by levels, and degrees by using appropriate audit techniques / methods / processes.

* 국방대학교 국방관리대학원
* 국방대학교 국방관리대학원

1. 서 론

전세계가 인터넷이라는 하나의 네트워크로 연결되어 어느 곳에서든지 접근이 가능해 정보공유의 이점이 있는 반면에 자료의 유출·변조·파괴, 전산망 마비, 프라이버시 침해 등의 역기능적 측면이 나타나고 있어 이에 대한 대책이 요구되고 있다.

국방전산망은 논리적으로 분리되어 운영되고 있어 외부적인 접근으로부터는 비교적 안전하지만 내부 불순세력이나 내부자의 실수에 의한 정보 유출의 가능성은 크므로 이에 대한 대책이 필요하다. 그리고 국방전산망이 물리적으로 완전히 독립되어 있지 않으므로 외부해킹에 의한 위협도 상존한다고 볼 수 있다. 군 특성상 보안은 생명과도 같은 것으로 매우 중요하다. 그렇다고 업무효율성 또한 무시해선 안된다. 행정 절차적인 보안을 강조하여 행정업무소요를 가중시키고 있다보니 규정준수보다는 비정상적인 방법으로 업무를 처리하려는 부작용을 낳고 있다. 절차적인 통제수단으로는 근본적인 보안을 달성할 수가 없다. 또한 해킹과 바이러스에 대한 대책과 로그화일에 대한 활용 및 보안대책이 미흡하고 부대 정보보안관리조직의 부재로 체계적인 보안관리가 안되며, 보안대책에 대한 적절한 검토가 이루어지지 않고 있다. 따라서 적절한 보안수준을 유지하고 이를 평가하기 위한 정보체계 보안감사 기준이 정립되어야 한다.

본 논문은 정보보안관리 개념에 의해 적절한 보안대책을 수립하고, 이에 대한 준수여부를 객관적으로 평가할 수 있는 보안감사모델에 관하여 연구하고자 한다.

2. 정보보안관리 표준(BS7799)

정보보안관리는 관리적, 기술적, 물리적 대책 으로 구분하는 정보보안의 분류방식에서 관리적 대책만을 다루는 것이 아니라 보안정책 수립, 위험분석, 보안대책의 선택 / 구현, 정보보안체계 구축, 보안대책 평가를 하나의 과정으로 인식하여 체계적이고 종합적으로 관리하는 활동을 총칭하는 개념이라고 할 수 있다[10]. 즉, 정보와 정보기술서비스로부터 적절한 수준의 비밀성, 무결성, 가용성을 달성하고 유지하기 위한 하나의 과정으로서 조직내 정보보안 환경을 설계, 구축, 운영, 감시하는 활동으로 구성된 생명주기를 기획, 관리하는 과정이다[14]. BS7799[1]는 일련의 정보보안관리방법에 대해 요소별로 해석해 놓은 문서로서 정보보안관리를 위한 국제표준으로 추진중이며, 기업이나 조직의 정보 시스템에 대한 정보보안관리의 평가인증 기준으로 사용되고있다[7][10].

2.1 BS7799의 통제내용

BS7799는 정보의 비밀성, 무결성, 가용성 유지를 위한 요구사항으로서 보안정책, 보안조직, 자산분류 및 통제, 인적 보안, 물리적 / 환경적 보안, 통신 및 운영 관리, 접근통제, 시스템 개발 및 유지보수, 업무연속성 관리, 부합성 등 10개 분류에 대한 127개 통제항목으로 구성되어 있으며 크게 두 부분으로 나누어진다. Part 1은 정보와 관련된 위험을 최소화하고 방지하기 위한 정보보안관리체계를 수행할 수 있도록 하는 최상의 실행지침이며, Part 2는 통제목적

1) 영국표준연구원(BSI)이 '95년 제정, '99년 개정한 정보보안관리 표준 문서

과 선택된 통제를 준수하는지 확인하기 위한 요구사항으로서 정보보안관리에 대한 심사 및 공인인증을 위한 심사기준이다.

2.2 BS7799의 정보보안관리 구조

조직은 정보보안관리에 대해 <그림 1>과 같은 순서로 통제 대상과 통제 방법을 설정하며 이를 문서화하고 유지해야 한다[13][10].

① 조직의 정보자산에 대한 가치를 분석하고, 어떤 정보가 왜 중요한지를 식별하는 정보보안정책을 정의

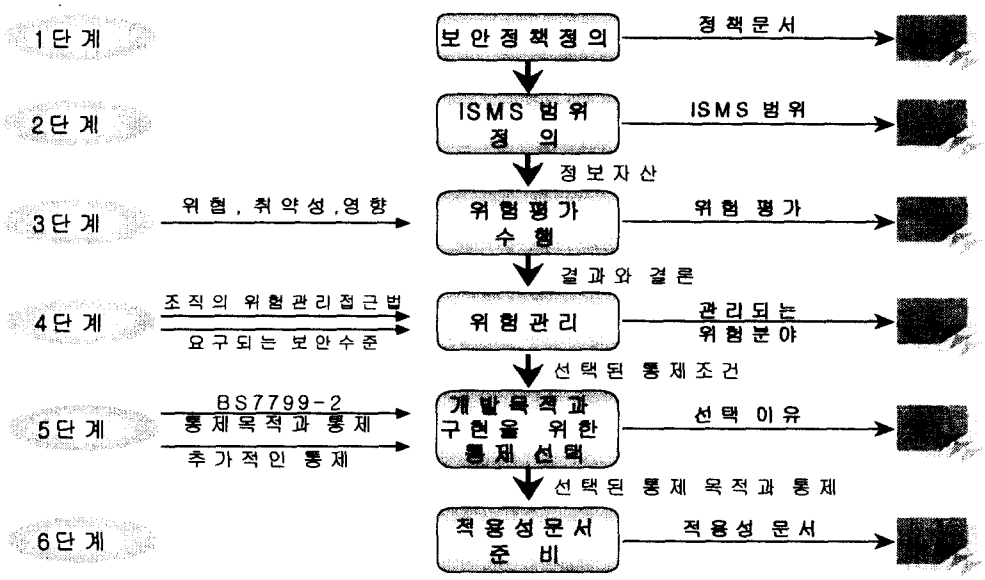
② 조직 및 서비스의 특징, 환경적 요인, 자산 및 기술적인 요소를 근거로 낮은 가치를 가진 정보를 제외하여 관리 대상범위를 설정

③ 자산에 대한 위협, 취약성, 조직 및 서비스의 중요도에 근거하여 가치를 상실하는데 따른 적절한 위험을 평가

④ 물리적, 인적, 절차적인 측면을 고려하여 위험을 어떻게 관리할 것인지 결정

⑤ BS7799-2의 통제항목과 추가통제항목을 선정하여 보안대책을 선정

⑥ 적용성문서(statement of applicability)에 선택된 통제에 대한 설정이유와 제외된 항목이 조직에 관련이 없는 이유를 명시



<그림 1> BS7799의 정보보안관리 구조

2.3 국방정보체계에 적용

BS7799는 민간분야에 적용되는 사항이고 광범위하고 높은 수준의 기준을 제공하기 때문에 국방정보환경에 맞게 조정하여 적용하여야 한다.

첫째, 국방정보체계의 보안 특성상 비밀성 유지가 가장 중요한 요소이므로 비밀성 유지에 대한 보강된 통제항목이 필요하다.

둘째, 정보보안관리조직이 없고 국방 예산, 보안 전문인력, 기술적인 능력면에서 수행하기에 높은 수준에 있는 항목은 능력에 맞게 점진적으로 적용되어

야 한다.

셋째, 국방정보체계 환경에서는 위협이 안되기 때문에 공통적으로 적용이 안 되는 항목은 제외하여야 한다.

넷째, BS7799에서 정의한 정보보안 범주 중 군사보안 범주에 포함되지 않는 부분이 다수 포함되어 있으므로 재검토가 필요하다.

3. 국방정보체계 보안감사 분석

3.1 보안감사 개념 및 목적

보안감사는 규정에 정한 인원, 문서, 자재, 시설, 지역 및 장비 등의 모든 보안관리 상태와 그 적정성 여부를 조사하기 위하여 실시하며 정기적으로 실시하는 정기감사, 보안상태가 불량하거나 기타 필요한 경우에 실시하는 수시감사, 현 보안상태를 확인하기 위해 실시하는 보안점검으로 구분한다. 또한 전산망을 신설 및 증설시에는 보안측정을 실시한다[1]. 정기보안감사는 통상 연 1회 실시한다. 국군기무사령부(이하 기무사) 전문감사팀에 의한 감사는 2년 주기로 사단급이상 부대에 대해 실시하며, 기무사 감사가 없는 해에는 각군본부 주관 전산팀에 의한 감사를 실시한다[1].

국방정보체계 보안감사를 실시하는 주요 목적은 보안사고를 조기에 적발하고 보안사고를 예방하는 것이다.

① 보안사고를 적발하여 해당위반자를 처벌

② 보안정책(규정, 지침, 방침)에 대한 준수 여부를 점검

③ 보안대책에 대한 적절성 여부를 평가

④ 적절한 보안대책을 강구하도록 조언

3.2 보안감사 실태 및 발전방향

국방정보체계 보안감사제도에 대한 문제점을 다음과 같이 분석할 수 있다.

첫째, 비밀성 유지에 대한 감사에 치중하고 있다. 국방정보체계 보안감사는 전시가 아닌 평시에 문서보안 위주의 전통적 관점에서 비밀성, 무결성, 가용성 등의 정보보안 목표중 비밀성 유지에 치중한다. 무결성 및 가용성 유지는 정보의 비밀성을 유지하는데 필요한 경우에만 적용한다. 그러나 국방정보체계에서 다루는 정보는 비밀성 유지뿐만 아니라 무결성과 가용성도 똑같이 중요하게 취급되어야 한다.

둘째, 표준화된 감사 기준이 없다. 표준화된 감사기준이 없어 매년 실시되는 외부 보안감사나 내부 보안감사시에 일시적인 점검표를 만들어 감사관에 의한 비교적 주관적인 감사 점검표와 기준에 의해 감사를 실시하여 일관성이 없고 보안대책에 대한 객관적인 평가가 되지 못하고 있다. 또한 기무사 검검표 자체를 대외비로 분류하여 실무부대에서는 자체 보안점검시 활용이 불가능하여 부대보안대책의 적절성 여부를 평가할 수 있는 기준이 없다. 따라서 부대 임무 및 특성에 따라 표준화된 감사기준이 필요하다.

셋째, 기술적 보안에 대한 감사가 미흡하다. 정보환경의 급격한 발전에도 불구하고 보안감사는 행정절차적인 보안을 강조하고 물리적, 인적보안에 치중하여 체계적인 보안감사가 이루어지지 못하고 있다. 보안규정에도 기술적인 보안에 대해 명확하게 규정하지 않아 기술적인 보안감사가 이루어지지 않으며 실무부대에서도 소홀히 다루고 있다. 따라서 정보체계 사용에 대한 기술적인 감시 / 통제 수단이 필요하며 이에 대한 감사기술이 필요하다.

3.3 보안관리 실태 및 문제점

3.3.1 제도적 측면

점차 정보화 의존도가 높아지고 역기능적 현상이 심화됨에 따라 체계적인 보안관리의 필요성이 증대되고 있는 사회현상에 비해 군은 아직 정보보안관리 체계 정립이 미흡하다. 각급부대는 정보보안를 위해 부대보안 정책을 수립하고 방향성을 제공할 수 있는 정보보안조직이나 정보보안전문인력의 부재로 부대보안관리 및 부대 보안발전에 대한 의사결정기구도 없다. 따라서 전산운영조직과 분리된 정보보안을 전담할 수 있는 정보보안관리조직이 필요하며, 부대실정에 맞는 보안정책에 따라 위협 분석 및 평가를 실시하고 그 결과에 따라 보안대책을 수립, 시행하며 관리하는 체계적인 정보보안관리가 필요하다.

사용자가 정보체계를 사용하기 위해서는 행정서류작성, 행정절차 수행 등 추가적인 많은 행정업무가 요구되기 때문에 업무효율을 크게 떨어뜨린다. 결국 규정을 준수하려하기보다는 비정상적인 방법으로 업무를 처리하려하기 때문에 더 큰 제 3의 사고발생 위험이 있다. 따라서 감시 / 통제 기능을 강화하고 기술적인 보안대책을 강구할 수 있도록 규정화해야 한다.

정보기술, 해킹 공격기술, 공격대응기술은 하루가 다르게 급변하는데 비해 보안감사기준이 되는 보안정책, 보안규정은 수정/보완 시기가 너무 늦다. 따라서 이 기준에 의해 감사를 하다보니 보안대책의 적절성 여부에 대한 평가 자체가 무의미할 수 있다. 실제 군사보안업무시행규칙은 '92년 개정판 발간이후 '99년에 재개정되는 등 보통 6~7년 주기로 개정되고 있다. 따라서 정보보안관리에 대한 규정은 현행 군사보안업무시행규칙에서 분리하여 최소 2~3년 주기로 개정해야 한다.

과거 문서보안 위주의 전통적인 관점에서 국방정보체계 보안은 비밀성 유지에 중점을 두고 있다. 국방분야에서 보안은 비밀성유지가 매우 중요한 요소이다. 그러나 국방업무의 정보화 확대로 정보체계에 대한 의존도가 높아져 무결성 및 가용성에 대한 침해가 있을 때 정보로서의 가치를 상실해 국가안보에 커다란 위협이 될 수 있다. 따라서 무결성 및 가용성에 대한 보안 규정을 함께 강화해야 한다.

3.3.2 관리적 측면

정보보안, 장비관리 및 비밀관리에 대해 개인에게 책임을 부여하는 개인보안책임제를 실시해 책임있는 관리가 이루어지는 반면에 조직 전체적인 보안관리와 보안대책 검토 등 지휘관 및 관리자의 관심은 소홀하다. 또한, 사용자 편의성을 배제한 관리자 위주의 비효율적인 행정 절차적인 보안을 강조한다. 따라서 개인 보안책임제를 보완해 보안에 대한 지휘관 심도를 높일 수 있는 방안을 강구해야 한다.

상급자가 권한을 악용하여 업무이외의 자료나 개인프라이버시 관련 자료의 열람을 요구하는 사례가 자주 발생한다. 특히 권력을 악용한 비절차적인 업무관행이 지속될 경우 그 위험성은 더욱 크다. 따라서 공식적인 절차에 의해 자료를 열람하도록 명확하게 규정화해서 통제해야 한다.

컴퓨터 활용능력에 비교적 능통한 20~30대 초급간부 및 병사에 비해 지휘관 및 참모들의 전산에 대한 마인드가 부족하고 전산기술에 대한 지식이 부족하여 사용자 편의위주의 전산기술 활용에 대한 보안감독 및 지도 능력이 부족하여 사고발생 위험이 크다[5]. 따라서 이에 대한 감시 수단과 보안관리 조직이 요구된다.

3.3.3 운용적 측면

멀티미디어 파일이 포함된 문서파일의 대용량화

와 디스켓의 잦은 오류발생으로 디스켓 사용을 기피하고 암호장비 또한 잦은 오류로 사용을 기피하여 음성적으로 비밀 자료를 하드디스크에 저장한다. 또한 저장파일을 제대로 삭제하지 않아 비밀자료가 하드디스크에 남아있거나, 삭제하였다고 해도 복구프로그램을 이용하면 쉽게 복구가 가능하다. 따라서 하드웨어의 도난, 분실 또는 리스만료후 반납시 삭제된 자료를 복구하여 비밀자료에 대한 의도적, 비의도적 유출가능성이 크다. 또한 PC를 네트워크로 연결 운용함에 따라 윈도우 운영체제하에서 다른 사용자가 쉽게 접근이 가능하고, '백오리피스'와 같은 해킹도구를 이용하면 상대방 PC로부터 정보유출은 물론 상대방PC에 대한 제어도 가능하다. 이런 해킹도구는 인터넷 상에서 구하기 쉽고 설치가 용이하기 때문에 더 큰 위협이 된다. 또한 PC는 운영체제상 완전한 패스워드시스템 및 로그파일 시스템의 부재로 PC의 불법 사용 및 정보유출 가능성이 높으며 자료무단이용에 대한 추적이 불가능하다. 암호화하지 않고 하드디스크에 중요 정보자료를 보관하는 것은 위험하다. 따라서 안정적인 군사용 암호장비를 개발하여 군 내부에서 사용하는 모든 문서파일은 자동으로 암호화되어 저장되도록 하며 외부 전산망과는 논리적으로 분리하는 것과 같은 기술적인 보안대책이 요구된다.

패스워드를 암기하기 쉽게 짧게 제정하거나, 단어나 생일, 기타 숫자로만 제정하는 등의 문제가 있다. 또한 월 1회이상 교체해야 하는 패스워드를 바꾸지 않고 사용하거나 반복해서 사용하는 사례가 많으며, 영숫자, 기호를 혼합하여 수시로 변경하여 사용하다보니 숙지가 곤란하여 키보드 밑이나 모니터의 빈 공간에 메모해서 사용하는 사례가 빈번하여 패스워드누출로 인한 시스템에 대한 비인가자의 접근 가능성이 높다.

시스템관리의 중요성을 인식하지 못하거나 전산직위 간부의 부족으로 시스템 관리자를 특별히 임명하지 않고 병사에게 일임하여 시스템관리에 허점이 노출되고 있다. 또한 시스템 관리인원과 감시 능력이 부족하여 시스템 침입감시와 감사가 제대로 이루어지지 않고 있으며 또한 관리 소홀로 인해 루트권한의 시스템파일을 일반 사용자가 쓰기가 가능한 모드로 설정되어 시스템설정을 일반사용자가 변경 가능한 경우와 사용자 홈디렉토리를 다른 사용자가 변경 가능한 경우가 자주 발생한다

로그파일은 시스템 사용자의 모든 활동내역을 자동 기록하여 사후 확인이 가능한 기록내용이다. 따라서 침입자의 흔적을 확인하고 어떤 경로로 침입을 했는지, 침입자가 어떤 작업을 수행했는지 파악하여 사후조치를 할 수 있는 수단을 제공한다. 따라서 로그 파일의 보호는 매우 중요하다. 그런데 로그파일에 대한 지식과 로그파일의 중요성에 대한 인식이 부족하여 로그파일 관리가 미흡하다. 일반적으로 로그파일 관리는 취약성이 있다. 로그파일 종류가 많고 복잡하며 슈퍼유저 권한만 있으면 어떤 로그 파일도 삭제할 수 있다. 어떤 클라이언트에서든 루트권한으로만 접속하면 로그 파일의 수정, 삭제가 가능하여 해킹위협으로부터 안전하지 못하다. 특히, 백도어(backdoor)프로그램은 침입자가 슈퍼유저 권한으로 로그인할 수 있도록 허용하고, 로그아웃하면 침입자의 모든 사용 내역을 로그 파일로부터 삭제한다. 따라서 특정 호스트 및 콘솔에서만 접근이 가능하도록 설정하여 불법침입으로부터 보호해야 한다. 그리고 로그 관리 및 분석도구를 운용해 로그의 보호와 보안기능을 강화해야 한다.

전송자료 보안을 위해 영외구간 연결시에는 자료전송용 암호장비를 연결하여 사용하도록 규정하고 있다. 그러나 보안장비 보급률이 부족하고, 보급되어 있더라도 암호장비 연결시 잦은 에러발생으로 실제

연결을 하지 않는 사례가 많다. 인터넷망과 같은 일반 공중망과는 논리적으로 분리되어 있어 안전하다고 인식하고 있어 보안을 소홀히 하고 있으나 한국통신망과 같은 상용망을 임대하여 사용하므로 물리적으로 완전히 독립되지 않아 외부 도청에 대한 위협이 상존하고 있다. 또한 자료보관용 암호장비는 사용자들의 보안에 대한 인식과 장비에 대한 신뢰성 부족, 사용의 불편함 등으로 인하여 사용하지 않고 장비를 방치하는 사례가 많다. 따라서 국방전산망의 보안 취약성에 대한 올바른 인식과 안전성 높은 암호장비의 개발이 요구된다.

공중망을 이용해 영내에 설치운용중인 인터넷은 기술적인 통제수단이 마련되어 있지 않은 상태에서 운용되고 있다. 비밀정보에 대한 유출뿐아니라 바이러스유포, 해킹프로그램 및 음란/오락물 유통, 불건전 싸이트 접속 등 역기능적 현상의 위험이 크므로 대책이 필요하다[4].

인터넷의 활성화로 영내에 운용되고 있는 인트라넷과 인터넷에서 E-mail을 통한 비밀자료의 무단 송수신의 가능성이 높다. E-mail은 보안성 검토 후에 보내도록 통제하고 있으나 보안성 검토후 중간에 내용을 변경한 경우나 절차를 무시한 경우에 어떤 자료를 보냈는지 확인하고 통제하는 것이 어렵다. 따라서 기술적인 감시 / 통제 수단과 전자서명(digital signature)같은 부인방지서비스가 필요하다.

국방인트라넷, 인터넷, 사무자동화시스템 등의 전자게시판에 익명성 허용으로 군비하, 음란물, 불평불만, 갈등조장, 유언비어, 상행위 등 불건전한 내용을 게시하고 무분별하게 운용하는 사례가 많다[3]. 이는 개인 명예훼손뿐만 아니라 사기저하 요인이 되며, 나아가 부대 및 군 전체의 단결과 전투력발전을 저해하는 위해요소다. 따라서 통제장치가 마련되지 않으면 사용을 금지해야 한다.

4. 국방정보체계 보안감사모델 제안

4.1 감사 고려사항

국방정보체계에서 안전한 정보보안을 위해서는 다음과 같은 보안 요구사항[6]을 고려해서 감사하여야 한다.

첫째, 비밀성(confidentiality)을 유지한다. 정보체계내의 정보는 인가된 자에게만 접근을 허용함으로써 자료의 비밀성이 노출되지 않도록 한다. 이러한 비밀성을 유지하기 위한 메카니즘으로는 접근제어와 파일의 암호화가 있으며, 어떤 정보의 존재 사실 자체도 노출되지 않아야 한다. 국방정보체계에서 요구하는 가장 기본적인 요구사항이다.

둘째, 무결성(integrity)을 유지한다. 정보는 오직 인가된 자만이 내용을 수정할 수 있도록 보장되어야 한다. 수정에는 파일에 대한 기록, 삭제, 생성, 변경 등이 포함되며, 무결성을 보장하기 위한 메카니즘에는 물리적인 통제, 접근제어, 고장에 대한 회복 메카니즘이 있다. 정보가 변조된 경우에는 이를 탐지해내고 경고하는 것 또한 정보의 무결성을 유지하기 위한 중요한 기능이다.

셋째, 가용성(availability)을 유지한다. 정보자산은 오직 인가를 받은 자만이 사용할 수 있도록 하고 필요시 언제나 사용이 가능하도록 보장되어야 한다. 가용성을 보장하기 위해서는 자료 백업, 중복성(redundancy) 유지, 물리적 위협요소로부터의 보호가 유지되어야 한다.

넷째, 인증성(authenticity)을 제공한다. 비밀성과 무결성을 보장하기 위해서 정보시스템에 접근하는

사용자가 정당한 실체인지 여부를 확인할 수 있어야 한다. 인증은 데이터 발신지를 증명하는 것과 원격지의 상대를 서로 인증하는 것 등이 있다.

다섯째, 책임추적성(accountability)을 유지한다. 시스템은 대부분 로그파일을 이용하여 시스템 사용에 대한 사용자 ID와 시간, 주소, 사용형태, 파일명 등에 대한 기록을 유지하여 시스템 사용에 대한 통계자료로 활용하거나 시스템 오류 발생시 복구를 위한 자료로 사용한다. 특히 시스템의 침입탐지와 추적에 필수적인 자료가 된다.

여섯째, 효율성(efficiency)을 제고한다. 정보체계를 사용하는데 있어서 보안기능이 너무 많으면 시스템의 효율성이 떨어지고 사용자도 사용을 기피하게 된다. 따라서 시스템의 효율성 저하를 최소화하고 사용자의 편의성을 높여야 한다.

4.2 감사항목의 수준평가

감사의 객관성과 보안관리의 효율성을 높이기 위하여 감사항목을 표준화한다. 정보의 비밀성, 무결성, 가용성을 유지하고 정보보안관리 개념에 의한 보안정책 수립, 위험분석, 보안대책 선정 및 구현, 보안대책 평가 등 체계적이고 종합적인 보안관리와 보안감사를 위해 BS7799를 적용하며 기타 통제사항을 추가하여 군 실정에 맞게 감사항목을 표준화한다. 실무부대는 부대 위험분석 및 평가 결과에 따라 표준화된 세부감사항목에 대한 적용여부를 결정한다.

또한 감사항목은 용이성, 위험성, 효과성, 비밀성 등을 고려하여 시행 우선순위에 따라 <표 1>과 같이 낮은 수준(Ll : Low Level), 중간 수준(Lm : Medium Level), 높은 수준(Lh : High Level) 등 3개 수준으로 구분하여 단계화한다.

① 용이성은 통제를 구현하는데 소요되는 예산, 인력, 기술수준 등을 고려하여 예산, 인력, 기술수준이 적게 소요되는 것에 우선순위를 부여한다.

② 위험성은 국방정보체계 자산에 보편적으로 예상되는 위협 및 취약성과 발생에 따른 영향 등을 고려하여 위협, 취약성, 영향이 큰 것에 우선순위를 부여한다.

③ 효과성은 정보자산의 자산가치가 크고 통제구현에 따른 대응효과가 큰 것에 우선순위를 부여한다.

③ 비밀성은 군사보안 특성상 비밀성 유지가 중요한 요소이므로 비밀성을 유지하는 것이 가용성, 무결성을 유지하는 것보다 우선순위를 부여할 수도 있다.

전산운영조직과 관련없이 단순한 사용자에 대한 통제는 기본(P : primary)항목으로 Llp, Lmp 2개 수준으로 분류하며 전산실이 편성되지 않은 부대 및 부서에 적용한다.

<표 1> 감사항목 단계화

			위험성	High		Low	
			비밀성	Yes	No	Yes	No
용이성	Easy	효과성	High	1	2	3	4
			Low	2	3	4	
	Hard	효과성	High	3	4		
			Low	4			

※ Ll : 1~3 Lm : 4 : 5~7

같은 목적을 가진 보안대책에 대해서 낮은 수준 즉, 정보에 대한 위험성이 크고 비밀성을 유지하며 구현이 용이하고 구현에 따른 효과가 큰 항목을 최우선적으로 시행하고 이것이 완성된 후에 다음 수준의 항목을 시행하도록 한다.

4.3 감사방법

보안감사 방법은 수작업에 의한 감사와 자동화도구에 의한 감사로 구분하여 실시한다. 수작업에 의한 감사는 감사관에 의해 (그림1)과 같은 점검표를 활용하여 현장에서 관찰, 관계자 면담, 증빙자료 검증 등을 통해 규정준수 여부 및 보안대책 적절성 등을 확인하여 평가한다. 자동화 도구에 의한 감사는 수작업으로 감사할 때는 효율성이 떨어지고 실질적인 준수여부에 대한 적절한 평가가 이루어지지 않는 분야 즉, 접근통제 분야와 같은 경우는 침투시험을 통해 취약성을 평가한다. 현재 자동화도구를 위한 시스템이 마련되어 있지 않은 경우는 ISS, SATAN, SecureDr 등과 같은 시스템안전진단도구를 이용해서 평가한다.

피감사부대는 표준화된 감사목록에 대한 자체감사를 통해 분석한 결과를 토대로 감사 희망등급을 요구한다. 감사관은 희망 등급에 대한 통제항목의 이행여부를 '완전이행(Y)', '부분이행(P)', '불이행(N)'으로 구분하여 평가한다. 감사항목에 대한 점검요소를 만족할 때 '완전이행', 일부사항에 대한 불이행요소가 있을 때 '부분이행', 해당항목에 대한 이행이 전혀 이루어지지 않을 때 '불이행'으로 평가한다. '불이행'이나 '부분이행'에 대한 이유를 위험 미판단, 예산·기술·인력 부족, 관리자 과실 / 태만, 사용자 과실 / 태만, 기타사유 등으로 분석하여 관리자가 보안관리와 미비점 보완에 도움이 되도록 한다. 또한 '의견'란에는 위반 내용을 구체적으로 기술하고, 법, 지침, 표준 등 관련근거를 제시하며, 위반에 따른 예상 위험 및 손실 등의 영향을 분석하고, 피감사부대의 능력면에서 실행가능하고 구체적인 해결책이나 대안을 제시한다.

4.4 보안평가등급 인증

부대 보안수준을 평가하기 위해 부대별 보안평가등급을 부여하여 부대 보안수준에 대한 객관적인 비교가 가능하도록 한다. 부대 보안평가등급 부여는 <표 2>와 같이 전산실 편성부대와 미편성부대로 나누어 실시한다. 전산실이 편성된 부대는 감사항목 Ll/Llp, Lm/Lmp, Lh 등에 대해 평가하여 A, B, C 3개 수준, 6개 등급을 부여하며, 미편성부대는 평가항목중 Llp, Lmp 2개 수준에 대해서만 평가하여 S 1개 수준, 4개 등급을 부여한다. 또한 부대 임무 및 전산업무 규모를 고려하여 군사급 이상부대는 최소 요구수준을 B등급으로 차등화하여 적용하여 C등급을 받으면 불합격으로 평가한다.

<표 2> 보안 평가등급

점검요소 / 등급			Ll/Llp	Lm/Lmp	Lh	비 고
"A" (높은수준)		1	완전	완전	완전	
		2	완전	완전	대부분	
"B" (중간수준)		1	완전	완전		군사급이상 부대
		2	완전	대부분		
"C" (낮은수준)		1	완전			군단급이하 / 학교기관
		2	대부분			
"S"	중간 수준	1	완전	완전		전산실 미편성 부대
		2	완전	대부분		
	낮은 수준	3	완전			
		4	대부분			
"F"			미이행			불합격 수준

※ C2<C1<B<A2<A1, S4<S3<S2<S1

평가등급은 하위 수준의 감사항목요소에 대해서는 모두 '완전이행(Y)' 평가를 받아야 다음 수준의

감 사 점검표(작성 예)

6. 통신 및 운영 관리 감사항목 분류
6.1 운영절차와 책임 감사항목 소분류

점검. 감사항목의 등급요소에 대한 이행여부를 완전이행(Y), 부분이행(P), 불이행(N) 등으로 표시하거나 해당 없음에 V표시

감 사 항 목	Ll	Lm	Lh	해당 없음
6..1.1 정보처리설비와 시스템 변경을 통제한다. (Ll) *a. 시스템 변경이 일어났을 때 로그가 유지되어야 한다.* *b. 중요 시스템에 대한 변경이 일어나면 관리자에게 경보를 발생해야 한다.(Lm)*	*Y*	*P*		
6.1.2 보안사고에 대하여 신속하고, 효과적이며, 순차적인 대응절차와 사고관리 책임이 확립되어야 한다. (Ll)	*Y*			
6.1.3 관리책임자는 전산자료 관리, 백업, 바이러스 감염방지 등 보안대책을 강구한다. (Llp)	*P*			
6.1.4 주요 업무영역에서 관리와 운용에 대한 직무를 분리하여야 한다.(Lh).			*N*	*V*
6.1.5 주요 시스템 자원은 항상 모니터링하고 가용성을 확보해야 한다. (Lm)		*N*		

사유. 부분이행(P)이나 불이행(N)에 대한 이유 분석(다수 선택)

감 사 항 목	위 험 없 음	위 험 미판단	예 산	기 술	인 력	관리자 태 만	관리자 과 실	사용자 태 만	사용자 과 실	기 타
6.1.1.a *6.1.1.b*					*V*					
6.1.2										
6.1.3								*V*		
6.1.4			*V*		*V*					
6.1.5				*V*	*V*					

의견. 구체적인 위반내용 및 법률, 지침, 표준 등 관련근거, 위반에 따른 예상 위험 및 손실 등 영향, 실현가능한 해결책이나 대안 등을 포함 구체적으로 기술

(그림1) 감사 점검표(예)

평가등급을 부여한다. 즉, B등급은 모든 C등급 요소(Ll/Llp)에 대해서 '완전이행(Y)' 평가를 받아야 한다. 또한 해당등급 감사항목에 대해 '불이행(N)'요소가 하나라도 발생하면 하위등급으로 평가한다. 즉, B등급 요소(Lm/Lmp)에 대해 대부분 '완전이행(Y)'이나 '부분이행(P)'의 평가를 받더라도 감사항목에 대해서 한 개라도 '불이행(N)'요소가 발생하면 C등급을 부여한다.

부대 보안평가등급은 감사 결과보고를 위한 1회용이 아니고 다음 감사에서 재평가될 때까지 해당부대 보안수준으로 인정하고 부대 보안평가등급 인증서를 부여한다. 그렇게 함으로써 부대보안에 대한 목표를 제공하고 부대보안에 대한 지휘관심을 고취시킬 수 있다.

4.5 감사절차

국방정보체계 보안감사는 5단계로 나누어 실시한다. 먼저 피감사부대를 이해하고 감사범위를 설정하기 위한 자료수집 단계와 이 단계에서 얻어진 자료를 기초로 존재하는 감사항목의 적용성을 결정하는 통제평가 단계, 감사항목에 대한 준거성을 점검하고 보고서를 작성하는 조사 및 보고서 작성 단계, 추가조사 및 입증단계, 종합 평가보고서 작성 단계로 나눈다.

① 자료수집 단계

사전준비단계로서 피감사부대 및 부서에 대한 과거 감사자료, 정보자산, 임무 및 특성 등을 분석하여 피감사부대 및 부서의 정보 자산 및 설비를 이해하고 감사범위를 설정한다.

② 통제 평가

피감사부대에서 작성한 위험분석결과보고서에 대한 적절성 여부를 검토 및 평가하고 필요시 위험분석을 다시 실시하며, 위험분석 결과와 피감사부대에서 요구한 감사희망 등급을 근거로 감사항목에 대한 적용 여부를 결정한다.

③ 조사 및 보고서 작성

감사항목에 대한 준수여부를 관계자 면담, 현장에서 관찰, 문서를 통한 각종자료 검증, 자동화감사도구를 이용한 결과 등을 통해 증거를 확보한다. 감사항목에 대한 준거성 검사를 토대로 요구사항에 대한 위반사항, 위반사유, 위반결과 나타나는 위험 및 손실, 실현 가능하고 구체적인 해결책이나 대안 등을 포함해서 평가보고서를 구체적으로 작성한다.

④ 추가 조사 및 입증

조사단계에서 발견된 개인에게 불리한 주요 위반사항 즉, 보안사고에 대하여 재조사하고 재검증하여 확실한 증거를 확보하고 본인의 과실 및 고의성 여부를 평가한다. 개인신상에 불리한 영향을 미치는 중요한 사항이므로 억울한 피해가 발생하지 않도록 신중을 기해서 조사한다.

⑤ 종합 평가보고서 작성

종합평가보고서에는 보안평가등급, 주요 위반 및 모범사례, 개인에 대한 처벌 및 표창사항을 포함하여 작성한다. 또한 감사항목에 대한 이행실태를 종합적으로 평가하여 부대 보안수준에 대한 평가등급을 부여하며 감사항목중 주요 위반사항, 위반사유, 위반결과 나타나는 예상 위험 및 손실, 해결책이나 대안 등을 포함하여 포괄적으로 작성한다.

5. 결 론

국방정보체계를 안정적으로 운용하기 위해서는 보안정책을 수립하고, 위험분석 및 평가를 통해 적절한 보안대책을 수립하고 구현하며, 보안정책 및

보안대책에 대한 적절성과 준수 여부에 대해 평가하는 정보보안관리절차가 이루어져야 한다. 국방정보체계 보안감사는 이런 정보보안관리 개념하에서 보안정책 및 대책에 대한 적절성과 준수여부를 평가해야 한다.

본 논문에서는 국방정보체계 관리실태와 문제점을 분석하고, 현 보안감사의 한계성을 분석하였다. 이에 따른 해결방안으로 정보보안관리 개념을 적용하여 국방정보체계 환경에 적합한 새로운 보안감사 모델을 제안하였다. 부대보안관리에 대한 지휘관심을 고취시키기 위해 부대 보안평가등급제를 제안하고, 외부감사에 대한 객관성 증대와 내부감사의 질적 향상을 도모하고 부대보안관리조직이 없는 현 상황에서 보안관리에 대한 방향을 제공하기 위해 감사항목을 보안수준별로 단계화하여 구분하였으며, 행정 절차적인 보안보다 기술적인 보안을 강조하여 사용자의 업무효율성을 제고하였다. 또한 소홀히 다루어 온 무결성 및 가용성에 대한 보안대책의 제고를 제안하였다. 감사효과를 증대시키기 위해 자동화 분석도구에 의해 국방전산망 해킹 취약성을 감사하며, 위반사항에 대한 원인과 위반결과 나타나는 영향을 분석하고 구체적인 해결책이나 대안을 제시해 의사결정 참고자료를 제공하도록 제안하였다.

참고 문헌

[1] 국방부, 군사보안업무 시행규칙, 국방부, 1999

[2] 국가정보원, 국가정보통신보안 기본지침, 국가정보원, 2000

[3] 국군기무사령부, 군사보안 지휘참고, 국군기무사령부, 2000.2

[4] 국군기무사령부, 군사보안 지휘참고, 국군기무사령부, 2000.4

[5] 국군기무사령부, 군사보안 지휘참고, 국군기무사령부, 2000.5

[6] 남길현, "정보사회에서의 정보보안," 정보보안대책연구 및 토론회('96 제9회 정보의 달 기념 심포지움), 한국정보시스템 감사인협회, 1996

[7] 시큐리티정보, "정보보호관리체계 인증규격," 정보보호 21C, 시큐리티정보, 2000.8

[8] 오경희, "정보시스템 보안감사," http://www.kisa.or.kr/edu/edu99/index.html, 1999

[9] 최장욱, BS7799를 적용한 국방정보체계 보안감사 모델에 관한 연구, 국방대, 2000

[10] 한국정보보호센타, 정보보호 뉴스, 한국정보보호센타, 2000.11

[11] 한국전산원, 정보시스템 보안 / 통제 감리지침 연구, 한국전산원, 1999

[12] BS7799-1:1999, "Code of practice for information security management," Information Security Management, BSI, 1999

[13] BS7799-2:1999, "Specification for information security management systems," Information Security Management, BSI, 1999

[14] ISO/IEC TR1335-1:1996, "Concepts and models for IT Security," Guidelines for the management of IT Security, ISO/IEC, 1996

[15] ISO/IEC TR1335-2:1997, "Managing and planning IT Security," Guidelines for the management of IT Security, ISO/IEC, 1997

[16] ISO/IEC TR1335-3:1998, "Techniques for the management of IT Security," Guidelines for the management of IT Security, ISO/IEC, 1998