정보보안관리규격(BS7799)을 적용한 국방정보체계 정보보안관리모델에 관한 연구

강행연, 남길현

국방대학교, 전산정보학과

A Study on Information Security Management Model for the Defense Information System using BS7799

Heng-yeon Kang, Kil-hyun Nam

Department of Computer & Information Science, Korea National Defense Univ

요 약

정보기술의 발달과 함께 정보시스템을 보호하기 위한 정보보안관리문제는 모든 기관 및 조직에서 반드시 짚고 가야 하며, 조직 전반에 걸쳐 표준적인 관리지침을 통해 포괄적으로 검토되어야 하는 문제로 대두되고 있다. 그러나, 현행 국방관련조직은 전반적으로 보안관리방법과 관리모델이 정립되지 않은 실정이므로 정보보안관리를 위한 표준관리 지침이 요구된다. 이에 본 논문은 정보시스템을 운영하는 조직 전반의 보안상태를 평가하는 데 유용한 방법론인 정보보안관리규격(BS7799)을 적용함으로서 전사적인 관점에서의 국방정보체계 정보보안관리모델을 제안하고자 한다.

I. 서론

최근 국가 사회 및 공공기관, 민간기관을 포함한 각 분야에서는 정보시스템에 의한 정보처리의 의존도가 날고 증가하고 있다. 그러나 이에 반해 정보시스템에 대한 보안대책은 상대적으로 미비하여 그에 따른 손실도 또한 증가하고 있다. 따라서 각 조직마다 정보시스템 보호와 관련한 정보보안관리의 필요성을 강조하고 있으며, 이는 국제적인 관심사로 떠오르고 있다. 특히, 단순한 정보자산관리의 개념을 떠나 체계적이고 표준적인 관리지침 및 방법을 모색하고자 하는 노력의 결과로서 영국 표준기관(BSI)에서 제정한 BS7799가 대두하게 되었다. 그러나 일반 사회조직들의 정보보안관리에 대한 연구와 관심들에 반해 국방관련조직은 그렇지 못하다. 이에 본 논문은 BS7799를 국방정보체계의 특성에 따라 융통성 있게 적용한 정보보안관리모델을 제안하고자 한다.

II. 정보보안관리

1. 정보보안관리 개념 및 목적

정보보안관리란, 국제적인 용어로는 정보기술보안관리(IT보안관리 : Information Technology and System Security Management)라고 통칭되는데, 이는 정보의 비밀성, 무결성, 인증성, 가용성, 부인봉쇄, 책임 추적성 및 신뢰성을 확보·유지·보장하는 일련의 과정을 말한다[1]. 즉, 관리적, 기술적, 물리적 대책 등의 정보보안의 분류방식에서 관리적 대책만을 다루는 것이 아니라 보안정책 수립, 위험분석, 보안대책의 선택 및 구현, 정보보안체계 구축, 보안대책 평가를 하나의 과정으로 인식하여 체계적이고 종합적으로 관리하는 활동을 총칭한다고 볼 수 있다[2]. 공공기관을 비롯하여 대부분의 조직에서는 정보의 처리를 위한 정보시스템에 대한 의존도가 매우 높으므로 조직의 정보시스템 보안의 필요성은 더욱 중요해지고 있다.

2. 정보보안관리의 일반적 모델

조직이 보안관리를 수행하는 데 있어서 필수적으로 요구되고 가장 기본이 되는 모델은 보안정책, 위험관리, 대응책 구현, 사후관리의 4단계를

거친다. 그 중 위험관리는 위험분석 수행, 보안 대응책 도출, 시스템 보안정책 수립, 보안 대응책 구현계획 수립의 단계를 거친다[3].

3. 정보보안관리규격(BS7799)

BS7799는 1995년에 영국의 표준 연구기관인 BSI(British Standards Institution)에서 제정한 정보보안관리를 위한 지침으로서 1999년에 개정되고, 표준으로 제안되어 ISO/IEC DIS 17799-1이 되었다. 기업이나 조직의 정보보안관리를 위한 방법론과 인증에 주안점을 둔 문서로서, 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조하는 데 유용한 지침이 되고 있다. BS7799는 Part1과 Part2로 구성되어 있다.

Part 1은 보안관리 실행지침으로 총 10개의 주요 분야 밑에 36개의 세부분야(통제목적), 그리고 127개의 보안통제항목을 정의하고 있다. 그 중 10개의 분야는 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 통신 및 운영관리, 접근통제, 시스템개발 및 유지보수, 업무지속성 관리, 준수(부합성)로 구성된다. Part 1에 수록된 통제항목들은 모두 구현할 필요가 없고 조직의 특성 혹은 상황적 여건에 따라서 유동적일 수 있도록 하고 있다. Part 2는 Part 1에서 설명한 내용에 대한 구체적인 보안관리 프레임워크를 제공하며, 정보보안관리시스템(ISMS)구축과 관련된 절차와 방법을 설명한다[4]. 정보보안 정책 정의, ISMS범위 설정, 위험평가 수행, 위험관리, 통제목적과 구현되는 통제선택, 적용성문서 준비의 6단계를 밟는다[5].

Ⅲ. 국방정보체계 분석

1. 국방정보체계 개요

국방정보체계는 현대전 수행 및 국방운영의 능률화를 위해 국방관련 정보를 컴퓨터, 통신망, 데이터베이스 등의 첨단기술을 활용하여, 원하는 시간과 장소에 제공 및 전달, 활용할 수 있도록 정보기술과 기능을 상호유기적으로 연결하고 통합하는 최적화체계를 말한다. 구성은 정보순환·운영관리·기술기능을 통합하는 국방정보통신운용 및 응용체계로 구성되어 있다. 기반체계는 하드웨어 및 소프트웨어체계로 대변되며, 정보통신망과 컴퓨터체계, 지원체계가 해당된다. 응용체계는 소프트웨어 위주의 운용체계로서 지휘통제체계와 자원관리체계로 나누어진다. 국방정보체계의 정보보안 범위(Security Scope)는 기술적, 물리적, 관리적 보안으로 나눈다.

2. 국방정보체계보안관리현황 및 문제점

보안관리현황 및 문제점은 제도적 측면과 운용·관리적 측면에서 분석된다. 전자의 경우, 정보보안 대책수립 미흡과 정보보안관리체계 및 관리모델의 미 정립, 그리고 정보보안관리 목표에 대한 규정 및 지침 미흡을 들 수 있다. 후자의 경우는 PC 및 디스켓 운용, 패스워드 및 암호장비 운용, 시스템 로그관리 등에 있어서의 취약성을 들 수 있다.

3. 국방정보체계 정보보안 요구사항

국방정보체계의 정보보안 요구사항은 크게 컴퓨터 시스템과 네트워크, 데이터베이스 요구사항으로 나누는데, 공통적인 요구사항으로는 비밀성, 무결성, 가용성을 들 수 있다.

그러나 좀 더 구체적으로 살펴보면, 보안관리현황 및 문제점과 관련하여 다음과 같은 보안요구사항이 제기된다. 즉, 정보자산, 조직, 제도, 시스템 구성 및 네트워크 관리와 컴퓨터매체 취급 및 접근통제, 그리고 통신장비보안과 관련한 물리적인 통제가 필요하며, 기반체계(H/W 및 S/W)내의 보안취약점 제거와 관련한 사용자 식별과 인증, 패스워드 관리시스템 등도 해결되어야 할 사항이다. 이러한 국방정보체계 정보보안 요구사항은 본 논문이 적용하고자 하는 BS7799와 비교해 볼 때, 국방정보체계의 기반체계 범위에서 포함할 필요가 있는 부분과 제외해도 되는 부분으로 나눌 수 있다.

전자의 경우에는 BS7799의 7개 분야인 보안정책, 보안조직, 자산분류 및 통제, 인사보안, 물리적 및 환경적 보안, 통신 및 운영관리, 접근통제가 해당된다. 이는 국방정보체계의 보안요구사항들을 만족하기 위해서는 반드시 적용해서 관리해야 할 분야이다. 각 분야별로 세부적인 지침목록을 작성하고 평가하는 절차가 이루어지게 되면, 그 결과를 토대로 보안요구사항에 따른 보안대책을 수립할 수 있게 된다.

반면, 후자의 경우에 있어서는 국방정보체계의 정보보안 요구사항과 관련이 없으므로 비용효과적인 측면에서 제외시켜도 되는 분야로 선정한 것이다. 여기에는 시스템개발 및 유지보수, 업무연속성관리, 준수(부합성)가 해당된다. 선정한 분야는 응용체계(S/W)와 관련된 부분이 많고, 현재 국방조직에서 실행하고 있는 업무 형태이며, 일반 사조직과 관련한 문제들을 다루고 있다.

Ⅳ. 국방정보체계 정보보안관리모델

1. 정보보안관리모델 제안

본 논문은 전사적인 관점에서 BS7799를 적용한 국방정보체계 정보보안관리모델을 제안한다. 특히, 기반체계(H/W 및 S/W)와 응용체계(S/W) 중 기반체계 위주의 연구에 중점을 둔다. 국방정보체계 정보보안관리모델은 각 단계마다 구체적인 산출물이 도출될 수 있다. 또한 각 단계는 주기적으로 검토되고 관리되어야 한다.

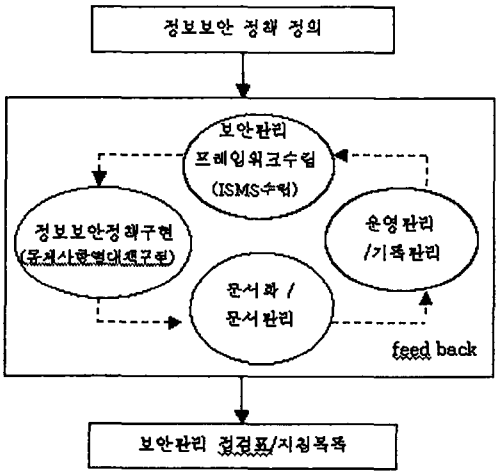

그림 1: 국방정보체계 정보보안관리모델

1) 정보보안 정책 정의

조직이 선택하는 정보보안관리 방향을 제시하기 위한 상위개념의 정보보안정책을 수립하는 단계로서, 정보시스템의 역할에 기반을 두는 활동이다. 조직의 정보보안실태와 보안요구사항 및 해당 정보자산이나 기술에 대한 환경을 분석하게 된다.

2) 보안관리 프레임워크 수립

① ISMS 범위 설정

정보보안관리시스템(ISMS)의 범위 설정단계는 낮은 가치의 정보를 제외함으로서 관리대상의 범위, 즉, 체계의 범위를 정의한다. 본 논문은 그 범위를 국방정보체계의 기반체계에 두고 범위 내에 포함되는 자산들은 통제항목과 통제대책을 통해 관리될 수 있도록 하는데 중점을 둔다.

② 위험분석

관리대상에서 제외된 범위 내의 자산들에 대해서는 위험분석을 실시하게 된다. 그 활동은 자산 및 취약성 분석, 위협분석의 과정을 거친다. 위험분석의 목적은 위험관리를 위한 보안대책을 선정할 때 참고로 하기 위해서이다.

③ 위험관리

위험관리 단계는 정보시스템에 영향을 줄 수 있는 위험을 통제하고 관리하며 최소화 또는 제거하는 과정으로 이루어진다. 즉, 조직에서 채택한 정보보안정책에 근거하여 조직이 보유하고 있는 예산, 현실성 등을 고려한 후, 조직에서 받아들이기 어려운 통제항목과 조직에 미치는 영향이 비용 효과성 측면에서 무시하여도 되는 통제항목으로 분리한다. 본 논문은 10개의 분야 중 7개의 분야로 제한한다.

④ 통제목적과 구현되는 통제수립

선택된 통제항목의 선정이유와 제외된 항목이 국방정보체계에 관련이 없는 이유를 명시하는 단계이다.

3) 정보보안 정책 구현(통제별 대책의 구현)

전 단계에서 선정한 통제목표 및 방안을 정보보안정책과 기술적 수준의 검토에 따라 구현하고 검증하는 단계로서, 조직적, 기술적 측면까지 세부적으로 구현하게 된다.(세부내용 부록 참조)

4) 문서화 및 문서관리

조직의 정책 또는 통제사항을 구현하는 과정에서 필요하다고 인정한 사항에 대해서는 문서화 및 문서관리의 과정을 거치게 된다. 정보보안관리시스템의 전반적인 관리절차와 관련한 활동을 기술한 절차서로서 체계화 할 수 있다.

5) 운영관리 및 기록관리

운영관리는 조직의 보안관리 절차들을 모니터링하고 내·외부로부터의 각종 사고들에 대응하는 과정으로서, 모니터링과 업무지속성 관리, 변화관리의 업무를 수행한다. 다음으로 조직은 운영관리 절차를 준수할 수 있는 기록을 식별하거나 유지 및 보관, 폐기하는 절차를 수립 및 관리하는 기록관리의 활동을 준수해야 한다.

6) 보안관리점검표/지침목록

정보보안관리모델의 최종산출물로서 통제의 분류는 대·중·소분류를 하였다. BS7799가 10개 분야 밑에 36개의 세부분야(통제목적), 127개의 보안통제항목을 정의하고 있는데 반하여, 본 논문은 7개 분야(대분류)밑에 30개의 세부분야(중분류), 116개의 보안통제항목(소분류)을 정의했다.

표 1에서 보듯이 7개 분야(대분류)는 BS7799에서 시스템개발 및 유지보수, 업무지속성 관리, 준수(부합성)을 제외한 항목으로 세부분야(중분류)가 3개, 통제항목(소분류)은 23개 추가되었다. 표 1의 통제항목에서 괄호부분은 BS7799의 통제항목의 개수를 나타낸다. 이러한 보안관리지침은 평가를 통해 효율적인

보안점검 및 관리가 될 수 있다.

표 1: 보안관리지침목록의 분야와 통제항목

분야(대분류)	세부분야(중분류)	통제항목(소분류)
보안정책	프로그램 정책	3(2)
	개별 점검 정책 (추가)	3
	개별 시스템 정책 (추가)	3
보안조직	정보보안 기반구조	6(7)
	제3자 접근 보안	3(2)
	외주보안	2(1)
자산분류 및 통제	자산에 대한 책임	1
	정보분류	2
인사보안	직무(업무)정의 및 자원배정 보안	6(4)
	사용자 교육 및 훈련	6(1)
	보안사고및오류(기능장애)의 대응	4(5)
물리적 및 환경적 보안	통제구역(보안지역)	5
	장비보안(통신장비보안)	6
	일반적인 통제수단	2
	자연재해 대책 (추가)	5
통신 및 운영관리	운영절차 및 책임	7(6)
	시스템 계획수립 및 승인	3(2)
	악성 소프트웨어에 대한 보호	2(1)
	운영관리	4(3)
	네트워크 관리	1
	매체의 취급 및 보안	5(4)
	정보 및 소프트웨어의 교환	9(7)
접근통제	접근통제 업무 요건(요구사항)	2(1)
	사용자 접근 관리	4
	사용자의 책무(책임)	2
	네트워크 접근통제	9
	운영체계 접근통제	8
	어플리케이션 접근통제	2
	시스템 접근과 사용의 감시	5(3)
	이동 컴퓨팅 및 텔레워킹	2

① 평가기준

평가받고자 하는 지침목록은 용이성, 효과성, 위험성, 비밀성 등을 고려하여 시행 우선순위 및 중요도에 따라 표 2와 같이 낮은수준,(L:Low), 중간수준(M:Medium), 높은수준(H:High)의 3개수준으로 구분하여 단계화 한다. 기타 전산운영조직과 관련이 없는 단순한 사용자에 대한 통제는 기본(U:Usual)항목으로서 Lu, Mu 2개 수준으로 분류, 적용한다.

표 2: 평가항목 단계화

			위험성	High		Low	
			비밀성	Yes	No	Yes	No
용이성	Easy	효과성	High	1	2	3	4
			Low	2	3	4	5
	Hard	효과성	High	3	4	5	6
			Low	4	5	6	7

※ L : 1~3 M : 4 H : 5~7

② 평가방법

보안평가등급에 대한 지침목록의 이행여부를 '이행(O)', '부분이행(△)', '불이행(X)'으로 구분하여 평가한다.

③ 평가등급

전산실 편성부대와 미편성부대로 나누어 실시한다.

표 3: 보안 평가등급

점검요소 / 등 급		L/Lu	M/Mu	H	비 고
"수" (높은 수준)	1	완 전	완 전	완 전	
	2	완 전	완 전	대부분	
"우" (중간 수준)	1	완 전	완 전		군사급이상 부대
	2	완 전	대부분		
"미" (낮은 수준)	1	완 전			군단급이하 부대 및 학교기관
	2	대부분			
"양" 중간 수준	1	완 전	완 전		전산실 미편성 부대
	2	완 전	대부분		
낮은 수준	3	완 전			
	4	대부분			
"가" (아주낮은수준)		미이행			불합격 수준

* [illegible]

전산실 편성부대는 지침목록 L/Lu, M/Mu, H등에 대해 '수', '우', '미' 3개수준, 6개 등급을 부여하며, 전산실 미편성부대는 지침목록 Lu, Mu에 대해 '양', 1개수준, 4개 등급을 부여한다. 하위수준의 지침목록 요소에 대해서는 모두 '이행(O)' 평가를 받아야 다음 수준의 평가등급을 부여하며, 해당등급 지침목록에 대해 '불이행(X)'요소가 하나라도 발생하면 하위등급으로 평가한다. 다음 페이지의 표 4는 이상과 같은 평가기준과 등급, 방법 등을 적용하여 실무적인 보안관리 점검시 활용할 수 있는 점검표 양식이다.

보안관리 점검표 양식은 선정한 분야의 세부적인 통제항목의 이행여부를 평가하게 된다. 이러한 활동의 결과는 종합, 분석 및 대응책 제시를 통해 향후 계속적인 정보보안대책수립에 참고가 된다.

④ 보안관리 지침목록

보안관리 지침목록은 별도의 부록으로 작성하여 참조할 수 있도록 한다.

표 4: 보안관리 점검표 양식

보안관리 점검표 양식

[대분류 5. 물리적·환경적 보안]

중분류 1 통제구역 (소분류 5개, 통제항목 53개)

2 장비보안 (소분류 6개, 통제항목 53개)

3 일반적인 통제수단 (소분류 2개, 통제항목 15개)

4 자원지배대책 (소분류 5개, 통제항목 21개)

점검. 각각의 통제항목에 대한 이행 여부를 이행(O), 부분이행(△), 불이행(X)으로 구분하여 평가

(※ 통제대책은 지면 관계상 기재하지 않음)

중분류	소분류	통제항목	L	Lu	M	Mu	H
1 통제 구역	1.1 물리적 보안 구역	1.1.2 정보처리설비지역을 보호하기 위한 보안구역이 지정되어 있는가?(Mu)				△	
		1.1.11 군사보안구역은 인가된 부대원만이 출입하도록 통제되고 있는가?(H)					△

종합. 중분류별 비율과 등급을 산출한 후, 각각을 종합하여 최종등급을 최정

평가. 부분이행이나 불이행의 경우, 아래 표와 같은 원인분석을 실시하고 불이행에 따른 예상 위험과 손실을 평가하여, 대응책과 해결방안 및 관리지침을 제안함 (원인분석은 V표시)

분류	Risk	Budget	Environment	Technology	Culture	Time	Not-Applic.	Other
1.1.2		V						
1.1.11						V		
1.2.2								

2. 제안모델 평가 및 향후전망

제안한 모델은 기존에 없던 국방정보체계의 정보보안관리모델을 국제표준의 성격에 따라 새로이 제안함으로서 정보보안관리모델의 틀을 제시했다는 데 의의가 있다. 아울러, 조직간 또는 부서간의 업무활동에 있어 공동의 이해관계를 도모하고, 표준화된 보안지침목록을 통한 평가 및 분석, 대책수립을 지원하고자 했다. 특히, 아직은 미흡한 점이 많지만, 관리의 일원화 및 효율성, 그리고 관리의 표준화를 위한 노력 과정에서 본 논문은 하나의 방향을 제시했다고 볼 수 있다. 이후로도 보다 적실성 있고 발전된 양상의 보안관리지침 수립을 위한 연구활동이 적용범위를 확대화하여 지속적으로 이루어질 것으로 판단된다.

V. 결 론

본 논문의 목적은 BS7799에 대한 이해와 방법론을 적용함으로서 국방정보체계의 효과적인 보안관리방법이나 절차, 응용에 대한 이해를 돕고, 실무에 적용하기 위한 참조기준을 제시하는 데 있다. 본 논문은 이러한 목적을 달성하기 위한 접근방법으로서 BS7799를 적용했고, 국방정보체계의 환경적 또는 기술적 제약조건 등을 고려하여 국방조직에 맞게 선택하여 재구성했다. 본 논문에서 제시한 국방정보체계 정보보안관리모델은 조직 전반적인 차원에서의 모델이므로, 차후 각 부서별, 혹은 분야별 적용이 가능하다. 특히, 최종적인 산출물인 보안지침목록은 기반체계의 보안상태를 파악하고 관리하는 데 유용한 지침이 될 것으로 판단된다. 아울러, 정보보안이 국제사회에서 경쟁우위를 제공하는 핵심 전략이 될 수 있다고 인식하고 있는 현 시점에서 표준적이고 종합적인 정보시스템 보안지침목록의 도출은 의미 있는 결과라 할 수 있겠다.

참고문헌

[1] ISO/IEC JTC1/SC27, "Guideline for the Management for IT Security", ISC/IEC, 1996

[2] 한국정보보호진흥원, 정보보호뉴스, 한국정보보호진흥원, 2000.11

[3] 한국정보통신기술협회, 공공기관전산보안정책수립을 위한 지침서, 한국정보통신기술협회, 1998

[4] 이철원 외 3인, "정보보안관리 평가방법론 고찰", 정보보호논문지 제11권 제3호, 한국정보보호학회, 2001.6

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