通信情報保護學會誌
第6卷 第1號, 1996. 3

위험분석 도구를 이용한 안전한 시스템 요구사항 분석

A Study on Requirements Analysis for Secure System using Risk Analysis Tool

김 영 길*, 안 금 혁*, 장 청 룡*

요 약

정보통신 자원에 대한 위협이 날로 증가하고 있는 현 상황에서 시스템의 안전성을 보장하기 위해 시스템의 개발 단계에서부터 보다 체계적인 보호기술 적용이 요구되고 있다. 따라서 본 논문에서는 시스템 위험분석의 개념과 그 필요성에 대해 기술하고 자동화된 위험 분석용 도구를 이용하여 특정 전산시스템에 대한 위험분석 작업을 수행하였다. 그리고 이에 대한 대응 방안을 수립하여 이를 안전한 시스템 요구사항으로 제시하므로써 시스템 개발과 운용시에 반영하도록 하였다.

1. 서 론

오늘날과 같이 대량의 데이터가 전산기기를 통하여 처리, 저장, 그리고 통신망을 통하여 전송되는 환경하에서는 정보의 소유자가 곧 힘의 소유자로 인식되기 시작했고, 또한 정보는 조직체를 운영해 나가기 위한 에너지원이며 자산으로 인식되고 있다.

이와같은 정보 자산의 적정한 사용을 도모하고, 정보의 부정당한 파괴, 변조, 노출 등을 막는 수단과 관리 기법을 정보보호 기법이라 한다[1].

이러한 보호되어야 할 대상이 파괴되는 요인에는 천재지변과 같은 자연적인 재해 이외에 인위적인 요인에 의한 경우가 많다. 이에 대한 대책으로는 기술적인 대책으로서 정보보호를 위한 기술을 정보통신 시스템 내에 구현하는 방법이 있으나 그것만으로는 충분하지 못하고 이러한 자원을 운용하는 사람들의 정보보호에 대한 올바른 인식 제고를 위한 교육의 실시와 같은 관리적인 대책, 그리고 법·제도적인 대책 등으로 정보통신 시스템에 대한 보다 체계적인 보호 대책의 적용이 요구된다.

본 논문에서는 정보통신 시스템에 존재하는 여러 위험 요소들을 체계적으로 파악하여 보다 안전한 시스템을 구현하기 위한 과정 중 초기 단계에서 처리하는 위험 분석의 개념과 그 필요성을 설명하고, 개발 중인 특정 시스템에 대해 위험분석용 자동화 도구인 CRAMM(CCTA Risk Analysis and Management Methodology) 패키지를 이용한 위험 분석 작업을 수행하여 그 대응 방안을 제안하였다. 그리고 이를 안전한 시스템 요구사항으로 제시하므로써 시스템 개발과 운용시에 반영하도록 하였다.

* 한국통신 연구개발본부

2. 위험분석의 개념 및 필요성

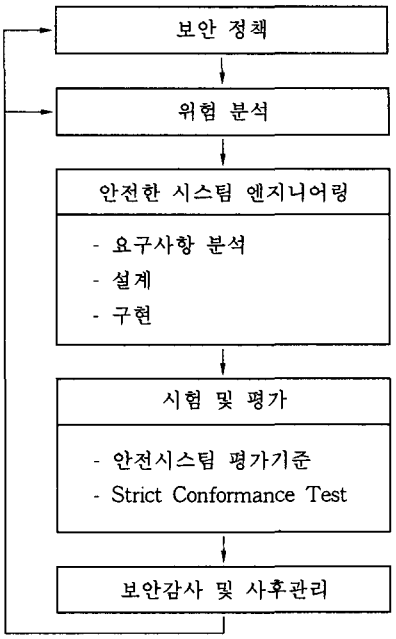
최근 일어나고 있는 정보통신 시스템에서의 각종 보안 사고들은 정보화사회로 나아가는데 있어 큰 걸림돌이 되고있다. 각종 바이러스 프로그램에 의한 정보의 파괴와 통신망을 통한 해커의 시스템에 대한 불법적인 침입등으로 인하여 귀중한 정보가 노출되거나 파괴, 변조되는 경우를 종종 볼 수 있다.

이에대해 각 조직에서는 자체적인 보안 대책을 마련하여 정보 자산을 보호하려는 움직임이 나타나고 있는데, 이러한 보안 대책의 수립시에 이를 보다 효과적이고 경제적으로 실현하기 위한 방안이 필요하다.

이를 위해서 개발중이거나 운용중인 정보통신 자원의 자산에 대한 분석과 분류를 통해 자산을 식별하고, 자산을 위협하는 요소들을 파악해서 시스템의 취약성을 분석하고, 자산이 공격당하였을 때의 영향을 분석하여 조직의 보안 위험을 평가함으로써 그에대한 적절한 보안대책을 마련하여야 한다. 이러한 보안 대책을 안전한 시스템 엔지니어링에 반영시킴으로써 대내외적인 공격으로부터 정보통신 자원의 피해를 최소화하여야 할 것이다.

위험분석(risk analysis)이란 정보통신 자원에 대한 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 영향을 미칠 수 있는 다양한 위협에 대해 해당 시스템의 취약점을 인식하고, 이로 인한 예상 손실을 분석하여 합리적인 비용으로 그 대책을 선정하므로써 정보자산의 보호를 경제적으로 실현하고자 하는 것이다. 즉, 정보통신 시스템 개발자와 관리자는 위험분석을 통해서 정보 자산의 보호를 효과적으로 수행할 수 있다[2].

이와같은 위험분석 단계를 정보보호 서비스 시스템의 개발 측면에서 고려해보면 (그림 1)과 같다[3].



(그림 1) 정보보호 서비스 시스템 개발 과정

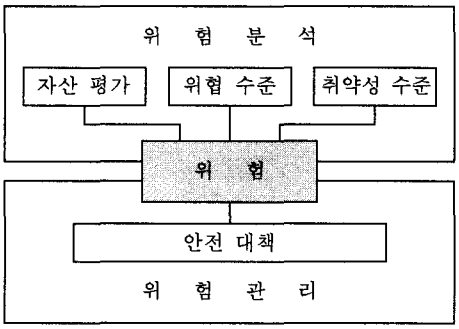
우선 조직에서 적합한 보안 정책을 수립한 후, 보안 정책에 따른 수준으로 위험분석 작업을 수행하고 그 결과를 이용하여 시스템 요구사항 분석을 한 후에 시스템 설계 및 구현에 들어간다. 그리고 개발된 시스템에 대해 시험 및 평가를 행하고 운용에 따른 시스템 감사를 수행한다. 또한 필요시에 보안 정책의 수정이나 시스템에 대한 위험분석 작업을 수행하여 시스템에 대한 계속적인 보호 조치를 취함으로써 시스템에 대한 안전성을 조직에서 목표로 한 수준에 근접시킨다.

2.1 위험분석과 위험관리

운용중인 정보통신 환경에 어떠한 위험이 존재하며, 그에 따른 위협의 정도는 어느 정도인가를 분석 및 진단하는 것, 즉, 보안상태를 분석하는 과정이 위험분석(risk analysis) 단계이다. 그리고 그 결과에 기초해서 어떤 정보보

호 대책을 어느 정도 적용할 것인가를 결정하는 것, 즉, 불확실한 보안 사건의 영향을 식별, 통제 및 최소화 하려는 과정이 위험관리(risk management) 단계이다[4].

(그림 2)에서는 위험분석과 위험관리의 상호 관계를 나타내고 있다.

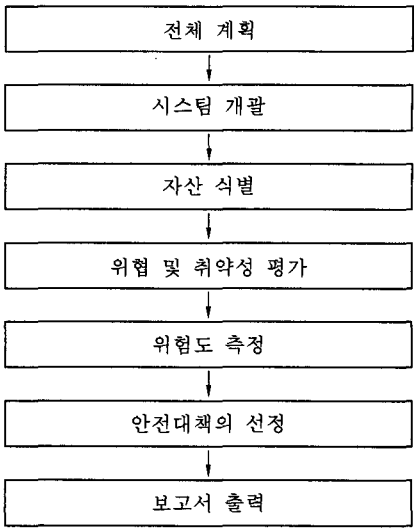


(그림 2) 위험분석과 위험관리의 관계도

위험분석을 위험관리의 한 부분으로 보고 전체 과정을 위험관리로 분류하기도 하는데 (그림 2)에서는 CRAMM에서 정의하는 바와 같이 위험분석과 위험관리를 개별적 단계로 구분하여 나타내었다.

따라서 시스템 개발자나 관리자가 개발 또는 운용중인 정보통신 시스템의 보안 관리를 하기 위해서는 먼저 자원에 대한 식별과 존재하는 위협 요소들을 분석하고 전체 시스템에 대한 위험분석을 하여야 한다. 그리고 그 결과를 근거로 적절한 보안대책을 설정하여 시스템에 대한 위험을 목표 수준으로 관리하여야 한다.

(그림 3)은 위험분석 및 관리를 수행하는 과정을 간략히 도식화한 것이다[5].



(그림 3) 위험분석 및 위험관리 수행 과정

3. CRAMM 패키지

CRAMM은 영국의 CCTA(Central Computer and Telecommunication Agency) 주관의 CEC(Commission of the European Communities) 프로젝트의 일환으로 국가 기밀로는 분류되지 않았지만 공개시 조직에 위해를 미칠 것으로 예상되는 데이터를 처리하는 공공기관의 IT(Information Technology) 시스템을 보호하기 위한 안전대책 수립에 활용할 목적으로 1987년에 개발된 위험분석용 패키지이다[6].

CRAMM은 위험분석과 위험관리의 두가지 측면으로 고려되어 개발되었는데, 위험에 대한 기술(description of risk), 위험의 평가(risk measurement), 그리고 위험의 관리(risk management)의 3 단계로 모델링되었다. 또한 시스템에 대한 위험 요소는 자산(assets), 위협(threats), 그리고 취약성(vulnerabilities)의 3가지 조합으로 구성된다.

3.1 CRAMM의 위험분석 절차

CRAMM에서는 크게 3개의 모듈화된 구조를 가지고서 작업을 수행하는데, 각 단계별 내용은 다음과 같다[7].

가. 제 1 단계 : 평가대상의 자산가치 분석

(1) 자산의 분류
- 위치적 자산, 물리적 자산, 소프트웨어 자산, 데이터 자산

(2) 물리적 자산의 대체 비용 평가

(3) 4가지 영향(파괴, 비가용성, 노출, 변조)에 대한 소프트웨어 자산 및 데이터 자산의 평가

나. 제 2 단계 : 평가대상의 위협 및 취약성 수준 분석

(1) 위험의 평가
- 360 가지의 질문
- 31가지의 일반적인 위협(generic threats) : (T_1 ... T_{31})
- 8가지의 영향(impact) : (I_1 ... I_8)
- 자산/영향의 쌍(pair) 가치 평가 : (A_i I_j)
- 위협(threat) 및 취약성(vulnerability)의 평가 : (Low, Medium, High)
- 위험 측정 : T_i (V_i) I_j A_k 의 조합

다. 제 3 단계 : 평가대상에 대한 안전대책의 설정

(1) 안전대책 제시(53개의 안전대책 그룹)
- 약 1800 가지의 안전대책 지원
- 안전대책의 우선순위 부여

(2) 안전대책의 적용 분야
- 물리적(physical) 보호
- 인적(personnel) 보호
- 절차적(procedural) 보호
- 통신(communications) 보호
- 환경(environmental) 보호
- 하드웨어와 소프트웨어 보호

(3) 안전대책의 내용
- 위협의 발생 확률을 줄인다.
- 특정 위협에 대한 취약성(vulnerability)을 줄인다.
- 위협으로 인한 영향을 줄인다.
- 시스템의 위험 발생(occurence of an impact)을 탐지한다.
- 위험 발생으로부터의 복구를 용이하게 한다.
- 위협 요소의 최소화 대책
- 취약성 요소의 최소화 대책

3.2 CRAMM의 장단점

CRAMM 패키지의 장점으로는 체계화된 위험분석 방법의 제공, 특정 시스템에 국한되지 않는 범용성, 입력 내용의 갱신기능 등과 개발된 시스템의 위험분석 뿐만 아니라 개발 단계에 있는 시스템의 위험분석 작업도 가능하다는 것이다. 한편, 단점은 오랜 작업 시간이 소요되고 산출되는 출력물이 너무 방대하여 결과를 분석하여 종합적인 대응책을 결정하는 일이 그렇게 쉽지 않으며, 입력 내용이 잘못되었을 경우 산출되는 결과물의 신뢰성이 떨어지고 정확한 위험분석을 위해서는 어느정도 숙련된 전문성이 필요하다는 것이다.

4. CRAMM을 이용한 위험분석

본 장에서는 응용시스템의 개발과 운용에 따른 보안성을 검토하여 안전대책을 수립하는 사례연구로서 사내에서 유통되는 문서를 전산화하여 처리하는 전자문서시스템에 대한 위험분석을 CRAMM을 이용하여 수행하고 그 결과를 분석하여 안전대책을 수립하므로써 이를 이용하여 안전한 시스템 요구사항 분석에 활용하도록 한다.

4.1 평가대상

전자문서시스템은 문서작성, 결재, 유통, 보관, 검색의 문서처리 전과정을 자동화 및 전산화하여 사내의 사무자동화를 실현하는 시스템으로 그 자산현황을 다음과 같이 분류하였다.

가. 위치적 자산

- 서울, ABC 빌딩, 전산실

나. 물리적 자산

- Multi-user Micro Computer
- Disk Drive 1
- Disk Drive 2
- Personal Computer
- Printer
- Cooler

다. 데이터 자산

- 문서 데이터 (Document data)

라. 소프트웨어 자산

- Application S/W

여기서 위치적 자산 분류에서는 서울이라는 지정학적 위치도 함께 고려대상에 포함시켰고 호스트 시스템은 전산실내에 위치하는데, 시스템의 대내외적 안전성 공격을 고려하여 특정 건물명은 밝히지 않았으며 이하에 시스템 보호가 요구되는 사항들에 대해서는 구체적으로 밝히지 않았다. 그리고 물리적 자산은 호스트 시스템과 문서 데이터를 저장하는 디스크 드라이브, 그리고 각 부서에서 일반 사용자들이 호스트 시스템에 접속해서 사용하는 PC와 출력용 프린터, 그리고 전산실내의 공기조화기 등으로 분류하였다. 또한 데이터 자산으로는 작성한 문서 화일로 분류하고 시스템 운용을 위한 응용 소프트웨어를 소프트웨어 자산으로 분류하였다.

4.2 자산 평가

다음의 〈표 1〉, 〈표 2〉, 〈표 3〉 및 〈표 4〉는 위 4.1절의 자산 현황에 대해 CRAMM을 이용한 평가 결과의 출력 형태를 보여준다.

표 1 PHYSICAL ASSETS에 대한 자산 평가 결과

PHYSICAL ASSETS	PHYSICAL ASSET DESTRUCTION	UNAVAILABILITY OF DATA			DESTRUCTION	DISCLOSURE		MODIFICATION	
		1 day	5 day	10 day		STAFF	OUTSIDERS	ACCIDENTAL	DELIBRATE
CENTRAL PROCESSING UNITS									
Micro Computer	4	2	4	6	6	4	8	4	8
STORAGE DEVICES									
Disk Drive 1	1	2	4	6	6	4	8	4	8
Disk Drive 2	1	2	4	6	6	4	8	4	8
PERSONAL COMPUTER									
PC	5	0	0	0	0	0	0	0	0
INPUT/OUTPUT DEVICES									
Printer	1	0	0	0	0	0	0	0	0
ENVIRONMENTAL									
Cooler	2	0	0	0	0	0	0	0	0

표 2 SOFTWARE GROUP에 대한 자산 평가 결과

SOFTWARE GROUPS	PHYSICAL ASSET DESTRUC-TION	UNAVAILABILITY OF DATA			DESTRUC-TION	DISCLOSURE		MODIFICATION	
		1 day	5 day	10 day		STAFF	OUTSI-DERS	ACCID-ENTAL	DELIB-RATE
APPLICATION SOFTWARE									
All software	3	2	4	6	6	4	8	4	8

표 3 LOCATIONS에 대한 자산 평가 결과

LOCATIONS	PHYSICAL ASSET DESTRUC-TION	UNAVAILABILITY OF DATA			DESTRUC-TION	DISCLOSURE		MODIFICATION	
		1 day	5 day	10 day		STAFF	OUTSI-DERS	ACCID-ENTAL	DELIB-RATE
SEOUL Site	6	2	4	6	6	4	8	4	8
ABC Building	6	2	4	6	6	4	8	4	8
Computer Room	5	2	4	6	6	4	8	4	8

표 4 DATA GROUP에 대한 자산 평가 결과

DATA GROUP	UNAVAILABILITY OF DATA			DESTRUCTION	DISCLOSURE		MODIFICATION	
	1 day	5 day	10 day		STAFF	OUTSID-ERS	ACCID-ENTAL	DELIBR-ATE
Document Data	2	4	6	6	4	8	4	8

위의 〈표 1〉, 〈표 2〉, 〈표 3〉 및 〈표 4〉는 자산을 PHYSICAL ASSETS, SOFTWARE GROUP, LOCATIONS, DATA GROUP별로 나누어 평가한 결과인데, 각 항목의 수치는 1에서 10까지의 범위내에서 담당자와의 인터뷰를 통해 수집한 값으로 수치가 클수록 위험도가 크다. 즉, 〈표 1〉에서 보면 정보가 노출되었을 경우 내부자 보다도 외부자에게 노출된 경우가 더 큰 값으로 나타나고 있다. 또한, 특히

데이터의 비가용성 항목은 1일, 5일, 10일의 각 기간별로 그 자산이 사용되지 못할 경우의 비가용성 정도를 정량화 한 값이다. 입출력 장치나 공기 정화기 같은 경우는 그 자산내에 의미있는 정보가 존재하지 않으므로 대체 비용의 물리적 자산 가치만 평가하고 나머지 항목에 대해서는 모두 0값으로 채워졌다. PC의 경우에도 각 연구실에 위치하며 일종의 단말기능으로 다른 PC로 대체 작업이 가능하므로 물리적 자산 가치만 평가하였다.

4.3 위협 및 취약성 분석

CRAMM에서는 모두 31 가지의 위협에 대해 작업을 수행하는데 그 중에서 특히 위험도가 상대적으로 높게 나타난 내부자와 외부자에 의한 시스팀으로의 침입에 대한 위협 및 취약성 분석결과를 보면 다음의 〈표 5〉와 같다.

표 5 시스템의 내외부자 침입 위협 및 시스템 취약성 분석 결과

KIND OF THREAT	THRT	VULN	ASSET VALUE									SECURITY REQUIREMENT								
			PHY.	UNAV'T			DEST	DISCL.		MOD'N		PHY.	UNAV'T			DEST	DISCL.		MOD'N	
				T1	T2	T3		STAF	O/SD	ACC'	DELI		T1	T2	T3		STAF	O/SD	ACC'	DELI
System Infiltration by OUTSIDERS	M	H	6	2	4	6	6	0	8	0	8	4	1	3	4	4	0	5	0	5
System Infiltration by STAFF	M	L	6	2	4	6	6	4	0	0	8	3	1	2	3	3	2	0	0	4

주) THRT : Threat, VULN : Vulnerability, PHY. : Physical, UNAV'T : Unavailability, DEST : Destruction, DISCL. : Disclosure, MOD'N : Modification, STAF : Staff, O/SD : Outsiders, ACC' : Accidental, DELI : Deliberate, T1 : 1 day, T2 : 5 days, T3 : 10days, H : High, M : Medium, L : Low

위의 〈표 5〉에서는 앞절의 자산 평가 결과를 고려한 위협과 취약성의 정도를 Low, Medium, High로 표시하고 있으며, 그에 대한 보안 요구사항을 각 항목별로 정량화한 값으로 나타내고 있는데, 1에서 5까지의 범위내에서 고려하여 조치해야 할 정도가 클수록 수치가 높다. 〈표 5〉에서 시스팀이 전산망으로 연결되어 운용됨으로써 외부의 침입자에 의한 위협과 취약성이 높고 내부자에 의한 의도적인 시스팀 불법침입의 위험도 상대적으로 높음을 알 수 있다. 따라서 안전대책을 수립할 때 이점을 특히 고려하여야 할 것이다.

4.4 제안된 안전대책

CRAMM에서는 위험분석 결과로서 모두 41개의 안전대책 그룹별로 세부적인 안전대책을 제안하는데 그 중에서 우선 순위가 높게 나타난 13개 안전대책 그룹에 대해 다시 각 그룹별로 우선 순위를 두어서 상위 3가지 정도의 세부 안전대책을 정리하면 〈표 6〉과 같다.

표 6 제안된 안전대책

안 전 대 책 그 룹	안 전 대 책
ROOM ACCESS CONTROL	1. 비인가된 출입자들을 통제한다. 2. 외부인의 방문시 관계 직원이 항시 동행한다. 3. 출입문이나 창문에 침입자 경보 장치를 설치한다.
HARDCOPY OUTPUT CONTROL	1. 출력물을 인가된 수신자에게 전달할 수 있는 공식적인 절차를 세운다. 2. 출력물에 연속된 페이지 번호를 매긴다.
MISUSE OF RESOURCES PROTECTION	1. 각 실에서 운용되는 PC에 대해 적절한 수준의 감독관리를 한다. 2. 민감한 데이터를 취급하는 경우 사용자 접근제어와 데이터에 대한 암호화를 수행한다. 3. 데이터나 소프트웨어에 대해 안전한 접근제어를 위해 물리적인 잠금장치나 인증 토큰을 사용한다.

SYSTEM ACCESS CONTROL	1. 사용자 신분확인을 위한 장치를 설치한다. 2. 패스워드 시스팀 사용시 그 길이와 형태, 변경주기, 그리고 패스워드 보호를 위한 절차를 세운다. 3. 민감한 데이터 처리시에 전자서명 기법을 사용한다.
RESOURCE ACCESS CONTROL	1. 하드웨어 장비에 유일한 식별자를 부여한다. 2. 보안 담당자에 대한 에러 로그 화일이나 일지에 대한 화일 접근을 읽기 전용으로 한다. 3. 화일에 대한 접근 허용을 단계화 한다.
SYSTEM ARCHITECTURE	1. 접근제어나 감사증적 요구사항에 의거 시스팀을 보호한다. 2. 보호되어야 할 프로세스를 특정 데이타 영역에 둘 수 있는 기능을 제공한다.
INPUT/OUTPUT CONTROL	1. 입출력작업은 운영체제를 통해서만 수행되게 한다. 2. 입력과 출력 장치의 불법 사용에 대비한 대책을 세운다. 3. 입력과 출력 장치를 물리적으로 안전한 장소에 위치시킨다.
LAN PROTECTION	1. 불법적인 액세스 시도에 대해 추적할 수 있는 절차를 세운다. 2. 다이얼업라인 사용시 정규 시간이외에는 접속을 끊는다. 3. 회선 및 통신장비에 대한 물리적 보호장치를 설치한다.
SECURITY ADMINISTRATION	1. 보안관리자에 의해 수행되는 모든 작업은 감사증적 화일에 기록되도록 한다. 2. 감사증적 화일을 점검하고 관리하는 절차를 세운다. 3. 시스팀 운용자와 보안 관리자의 역할 분담을 한다.
SECURITY EDUCATION & TRAINING	1. 보안 담당자에 대한 보안 교육을 실시한다. 2. 신규 직원을 포함한 전직원에 대한 보안 의식 교육을 실시한다.
USER CONTROL	1. 보안 담당자에 의해 일반 사용자들은 단말 환경만을 이용하여 작업하도록 통제되어야 한다. 2. 일반 사용자들은 프로그래밍이나 컴파일 작업등을 하지 못하게 조치한다.
SECURITY TESTING	1. 감사증적 화일이나 인증 데이터에 대한 비인가된 접속을 허용하는 소프트웨어 버그가 존재하는지를 시험한다.
BACK-UP	1. 시스팀 복구 후에 화일이나 데이타베이스의 내용이 일치되도록 하는 자동화된 절차가 필요하다. 2. 단말 사용자에게 시스팀 복구작업 완료시 통보해 준다.

즉, 예를들면 자원의 오용을 방지하기 위한 대책으로 운용 PC에 대한 필요한 수준의 감독 관리와, 민감한 데이터의 보호를 위해 접근제어와 데이터에 대한 암호화를 하도록 하고, 사용자 확인을 위한 인증토큰의 사용과 물리적인 잠금장치의 설치 등의 안전대책이 제안되었다.

한편, 안전대책 그룹은 동일한 위협에 대한 여러 안전대책들로 구성되는데 이것은 한가지 위협에 하나의 안전대책만을 지원할 경우, 안전대책의 선정 요인인 비용대 효과 측면에서 수용이 곤란할 경우에 시스팀은 계속 위험에 노출되게 된다. 따라서 복수개의 안전대책들을 제안하므로써 대응 방안의 폭을 넓히고 또 그러한 안전대책들은 상호 보완 효과를 가져오므로 항상 여러 안전대책들을 함께 고려 대상에 포함시켜야 한다.

5. 안전한 시스팀 설계 요구사항

안전대책의 수립에는 기술적, 관리적 및 법·제도적인 대책 등으로 나누어 수행할 수 있는데, 여기서는 그 중에서 우선순위가 높은 항목들에 대해 기술적인 측면만을 제안하도록 한다.

앞장에서 제안된 안전대책들을 대상 시스팀인 전자문서시스팀에 적용하여 구현하기 위해서는 먼저 개방형 환경에서 적용될 수 있는 개방형 통신시스팀에 대한 안전성 구조를 고려하여야 한다[8]. 이 안전성 구조에서는 개방형 통신시스팀 환경에 적용될 수 있는 일반적인 안전성 구조의 요소들을 정의하고 안전성 서비스와 관련된 보호메카니즘에 대한 규정과 이들의 OSI 각 계층에서의 위치가 규정되어 있다.

따라서, 제안된 안전대책에 대한 기술적 대책 중 우선순위가 높은 항목들을 중심으로 한 안전대책 그룹과 개방형 통신시스팀 안전성 구조의 안전성 서비스를 〈표 7〉과 같이 상호 연계시킬 수 있다.

표 7 안전대책 그룹과 안전성 서비스의 관계

안전대책 그룹	안전성 서비스
MISUSE OF RESOURCES PROTECTION	접근제어, 기밀성
SYSTEM ACCESS CONTROL	인증, 무결성
RESOURCE ACCESS CONTROL	감사증적, 접근제어
SYSTEM ARCHITECTURE	접근제어, 감사증적
LAN PROTECTION	감사증적

이를 요약하면 시스팀에 대한 접근제어, 사용자 인증, 데이터 무결성 및 기밀성, 그리고 감사증적 등으로 나누어진다. 〈표 8〉은 우선순위가 높은 항목들을 중심으로 안전대책 지원을 위한 안전성 서비스와 보호 메카니즘과의 관계이다.

표 8 안전성 서비스와 보호 메카니즘과의 관계

안전성 서비스	보호 메카니즘
사용자 인증	단순인증(패스워드), 강력인증(인증교환)
무결성	전자서명

기밀성	암호화 알고리즘
감사 증적	로그 화일 관리, 침입탐지
접근제어	접근제어

따라서, 전자문서시스템에서는 시스템 접속시 사용자 확인을 위해 인증교환 방법을 채택하고, 전자결재를 위해서는 전자서명 메카니즘을 선정하였다. 또한 민감한 데이터에 대하여는 화일을 암호화하여 저장하도록 하므로써 비인가자에게 데이터 내용을 노출되지 않게하고 비인자로부터 자원의 사용을 막기위해 접근제어 메카니즘을 선정하였다. 그리고 추후 문제가 발생했을 때 참조하기 위하여 분석에

필요한 감사증적을 위한 로그 화일 관리와 대내외적인 불법적 접근 시도를 탐지해 내기 위한 침입탐지 시스템도 필요하다.

그외에도 시스템 운용자들에 대한 보안 교육 및 훈련의 실시와 같은 관리적 대책과 법·제도적인 대책을 함께 수립하므로써 보다 안전한 시스템을 개발, 운용할 수 있을 것이다.

그리고 이러한 위험분석 결과로 선정된 안전대책들을 개발중인 시스템의 분석과 설계 단계에 시스템 요구사항으로 반영하여 개발 단계에서부터 보호 메카니즘을 적용하므로써 시스템의 안전성을 강화할 수 있을 것이다.

6. 결 론

날로 개방화, 국제화 되어가는 정보통신 환경으로 말미암아 정보통신 자원에 대한 위험요소가 증가하고 있다. 이러한 위험으로부터 정보 자산을 보호하기 위하여 정보통신 시스템의 개발자 또는 관리자는 기술적, 관리적 및 법·제도적인 방법으로 자산을 보호할 수 있게 하여야 한다.

본 논문에서는 특정 전산 시스템의 자산을 식별하고 존재하는 위협 요소의 분류 및 취약성 분석을 하여, 위험의 정도를 분석 및 진단하기 위하여 위험분석 도구인 CRAMM 패키지를 이용하였으며, 그 결과에 기초해서 대상 시스템의 안전대책을 제안하였다. 그리고 이러한 대책을 해당 시스템을 보다 안전하게 개발하고 관리하기 위한 시스템 요구사항으로 제시하므로써 시스템 개발단계에서 부터 고려하여 반영되도록 하였다.

한편, CRAMM은 위험분석과 위험관리 전체 과정에서, 위험분석 수행 및 그 결과로 위험관리 과정에서 고려해야 할 모든 안전대책들을 제시해 주는데, 어떠한 안전대책을 수용할 것인가는 그 시스템의 관리자가 결정해야 할 사항이다. 또한 안전대책을 선정할 때에는 비용대 효과 측면의 고려가 함께 있어야 한다. 즉, 예산의 제약과 같은 요인에 의해 실제 적용에 제약을 받게 된다. 그러므로 어떠한 안전대책을 채택하여 설치할 것인가를 결정하는 것은 위험분석 작업을 수행한 사람의 조언에 의한 관리의 기법이다. 하지만 CRAMM은 많은 위험 요인들에 근거한 안전대책들에 우선순위를 부여함으로써 이러한 과정의 수행을 용이하게 한다.

따라서 본 논문의 사례연구에서 위험분석 도구를 이용하므로써 보다 체계적인 위험분석 작업을 수행할 수 있었을 뿐만 아니라 효율적인 대책 설정도 할 수 있게 하였고, 시스템의 위험도를 정량화된 데이터로 나타내 줌으로써 보안 담당자들이 실제로 가장 어려움을 겪고 있는 시스템의 위험도를 파악할 수 있는 자료를 일선 경영자에게 제시해 줄 수 있게 하였

다는 데에 큰 의의가 있다.

그러나 시스템 개발자나 관리자가 반드시 고려해야 할 사항으로 위험분석 작업이 특정 정보통신 환경에 존재하는 위험을 받아들일 수 있는 수준으로 줄이는 것이지 위험을 완전히 없앨 수 있는 안전대책을 설정하는 것은 어렵다는 것을 염두에 두어야 할 것이다.

또한 이러한 일련의 과정들이 시스템 개발자와 관리자, 그리고 사용자간에 정보보호의 필요성에 대한 올바른 인식과 공감대가 우선적으로 형성되지 않고는 만족할 만한 효과를 기대하기가 어렵다는 점을 인식해야 한다.

참 고 문 헌

[1] 辻井 重男, 笠原 正雄 編著, *暗號と情報セキュリティ*, Chap. 9, 昭晃堂, 1990.

[2] Charles P. Pfleeger, *Security in Computing*, Prentice-Hall, 1989.

[3] Edward Amoroso, W.E.Kleppinger, David Majette, "*An Engineering Approach to Secure System Analysis, Design, and Integration*", AT&T Technical Journal, pp.40-51, SEPTEMBER / OCTOBER, 1994.

[4] 한국전산원, 전산망 보안을 위한 위험관리 지침서, 1994.

[5] I. C. Palmer, G. A. Potter, *Computer Security Risk Management*, Chap. 16, Jessica Kingsley Publishers Ltd., 1989.

[6] CCTA, *Guidelines for Directing Information Technology Security*, IT Security Library, 1991.

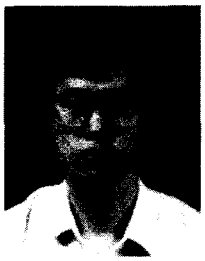
[7] BIS Informations Systems, *CRAMM User Guide (Ver 2.1)*, 1993.

[8] CCITT Recommendation X.800, "*Data Communication Networks : Open Systems Interconnection (OSI) ; Security, Structure and Applications*", 1991.

□ 筈者紹介

김 영 길

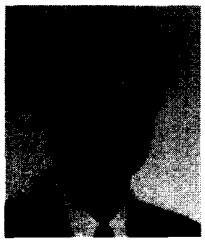
1990년 한양대학교 전자계산학과 졸업 (학사)
1992년 숭실대학교 대학원 전자계산학과 졸업 (석사)
1992년 ~ 현재 한국통신 연구개발본부 연구원



안 금 혁

1988년 2월 숭실대학교 전자계산학과 졸업(학사)
1991년 2월 한국과학기술원 전산학과 졸업(석사)
1991년 3월 ~ 현재 한국통신 연구개발본부 연구원

※ 관심 분야 : 정보보호, 위험분석



장 청 룡

1957년생
1980년 성균관대학교 전자공학과 졸업(공학사)
1986년 연세대학교 대학원 전자공학과 졸업(공학석사)
1995년 성균관대학교 대학원 정보공학과 졸업(공학박사)
1979년 ~ 1983년 한국전기통신연구소 연구원
1984년 ~ 현재 한국통신 연구개발본부 선임연구원
※ 관심 분야 : 정보보호, 시험평가