情 報 保 護 學 會 誌
第 13 券 第 3 號, 2003. 6

보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구

최 상 수*, 방 영 환*, 최 성 자*, 이 강 수**

요 약

보안관리, 위험분석 및 PP의 개발 방법(또는 지침, 표준)을 개발하기 위해서는 공통적으로 자산, 위협 및 취약성의 분류체계, 평가기준 및 평가스케일을 정의해야한다. 본 논문에서는 이 분야의 각종 방법들로부터 분류체계, 평가기준 및 평가스케일을 조사연구하였다. 본 결과는 새로운 방법을 개발할 때 활용될 수 있을 것이다.

Ⅰ. 서 론

조직의 정보시스템에서 최소의 비용으로 최대의 보안성을 얻기 위한 체계적인 방법인 보안관리(security management)는 보안정책 수립, 보안대책의 실행 및 위험분석(risk analysis) 과정을 통해 이루어진다. 따라서, 보안관리를 위해서는 보안대책에 의해 보호되어야 하는 자산(asset)을 식별하고 그 가치를 평가하고 자산에 가해지는 위협(threat)과 취약성(vulnerability)을 평가해야한다. 또한, CC(Common Criteria)와 같은 정보보호시스템 평가체계상에서 보안제품의 공통 기능 및 보증 요구사항이라 할 수 있는 PP(Protection Profile)을 개발하기 위해서도 이와 같은 업무를 수행해야한다.

국내외적으로, 보안관리, 위험분석 및 PP개발을 위한 다양한 방법(또는, 지침 및 표준)이 제시 및 사용되고 있지만, 각 방법마다 프로세스, 자산, 위협, 취약성의 분류체계(schema), 평가기준 및 스케일이 서로 다르다. 따라서, 새로운 보안관리, 위험분석 및 PP 개발 방법 및 도구를 개발을 위해서는 다음 사항을 기존의 방법을 고려하여 정의해야 한다.

- 관리 및 평가 프로세스
- 자산의 분류체계, 평가기준 및 스케일
- 위협 및 취약성의 분류체계, 평가기준 및 스케일

이를 위해, 본 연구에서는 기존의 소프트웨어공학 및 품질관리, 보안관리, 위험분석 및 PP 개발 부문의 각종 방법, 지침 및 표준들에서 정의된 프로세스, 자산, 위협 및 취약성의 분류체계와 평가기준 및 평가스케일들을 조사 및 분석하였다.

본 연구의 2장에서는 보안관리, 위험관리 및 위험분석의 개념을 체계적으로 정리하고, 3장에서는 소프트웨어공학, 정보보호시스템평가 및 위험분석에서의 평가 스케일을 비교 및 분석하였다. 4장에서는 위험분석 프로세스를, 5장에서는 자산분류 및 평가방법을, 6장에서는 위협의 분류 방법과 위협과 취약성의 개념차이를 비교 및 분석하였다. 끝으로, 7장에서 결론을 맺는다.

Ⅱ. 보안관리, 위험관리 및 위험분석의 개념

정보보호관리는 위험관리의 상위개념이며 위험관리는 위험 분석의 상위개념이다. 각 개념들의 정의와 관련 표준, 도구 및 기술들은 다음과 같다.

- 정보보호관리(ISM ; information security management) : ISM은 조직의 정보시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를

* 한남대학교 컴퓨터공학과 ({gcss09, bangyh, choisj}@se.hannam.ac.kr)
** 한남대학교 정보통신 · 멀티미디어공학부 교수 (gslee@mail.hannam.ac.kr)

〔표 1〕 보안관리기준의 통제항목 비교

보안관리기준	통제 항목 분류				최상위 클래스명
	클래스	패밀리	컴포넌트	엘리먼트	
BS7799	10	36	127	550	정책, 조직, 자산, 인사, 물리/환경, 통신/운영, 접근통제, 개발/유지보수 연속성 준수
한국기준	12	-	131	-	정책,조직, 아웃소싱/제3자접근, 자산, 인사, 교육/훈련, 접근통제 물리적 운영 개발 연속성 사고대응/복구 준수
GMIT	2	12	63	N/A	관리/정책, 준수, 사건처리, 인사, 운영, 연속성, 식별/인증, 접근통제/감사 악의적 코드 보호 망관리 암호
독일 IT Baseline	6	-	544	N/A	기반구조, 조직, 인사, HW/SW, 통신, 비상계획
SSE-CMM	3	22	128	744	기본, 프로젝트, 조직
Vallabhaneni [9]	7	-	-	58	물리적, 인사, 자료, 응용 SW, 시스템 SW, 통신, 운영

몇 개의 통제분야(클래스)로 나누고 각 통제분야별로 다수의 통제대책(컴포넌트)으로 구성된다. ISO/IEC-13335(GMIT)[1,2], 영국의 BS-7799 (ISO/IEC-17799)[3], 독일 BSI(Bundesamt Fur Sicherheit in der Informarionstechnik)의 BSI IT Baseline Protection Manual[4], 카네기멜론 대학의 SSE-CMM[5], 한국의 「정보보호관리기준」[6]은 ISM을 위한 표준 및 지침들이다[7].

국내외 보안관리 기준들에서는 표 1과 같은 다양한 통제항목이 제시되어 있으며 이러한 통제항목은 보안관리의 수준(또는 보안 위험성)을 상위수준 또는 관리적, 비기술적 수준에서 평가하는데 활용될 수 있다[8].

- 위험관리(IRM : information risk management) : IRM은 ISM시에 최적의 비용으로 최고의 효과를 거두기 위해 통제분야의 우선순위를 결정하고 실제의 통제를 수행하는 방법중의 하나이다. 일반적으로 위험관리는 매우 광범위하며, 소프트웨어 개발시의 위험관리[10] 등은 정보시스템 개발시의 위험관리에 적용할 수 있다. 특히, IRM은 정보보호 차원에서의 위험관리를 의미한다.

  일반적으로, IRM은 위험분석과 보안대책의 선택을 포함한다. 미국 NIST의 FIPS-65[11], FIPS-191[12], SP-800-30[13], NISTIR-4387[14], NISTIR-4325[15], 미국 GAO의 AIMD-00-33[16,17], 카나다의 CSE(Communications Security Establishment)[18] 및 우리나라의 TTA의 TTAS.KO-12.007[19] 등은 정부차원의 IRM 지침이다. 카네기멜론대학의 OCTAVE[20], CRAMM[21], INORSEC-92[22], BDSS[23], RiskWatch[24], Expert[25], 우리나라의 PRAM(국가보안연구소)[26], 팬타(한국과학원)[26] 및 HAWK(한국전산원)[27], CISSP[28], Open Framework[29] 등은 프로토타입 또는 상용화된 IRM 지원도구이다.
- 위험분석(IRA : information risk analysis) : IRA는 보안관련 항목들에 대한 위험파악(RI : risk identification)과 위험평가(RA : risk assessment)로 구성된다. RI는 정보시스템 내에 각 항목의 세부사항을 발견 및 식별하는 것이며 RA는 파악된 항목에 대해 그의 발생가능성과 피해가능성 등을 수치적 또는 등급적으로 부여하는 것이다.

Ⅲ. 평가 스케일의 비교

일반적으로, 측정(measurement)할 수 있는 것만 관리(통제)할 수 있으므로, 관리를 위해서는 관리대상 항목의 척도(metric)를 정의하고 가급적 정량적(수치적)으로 척도 값을 부여해야한다. 척도(예 : 길이의 척도는 ㎝)에 척도값(예 : 1.2㎝)을 매핑하는 과정을 측정(measure) 또는 평가(assessment)라 한다. 예컨대, 정보시스템의 위험 관리를 위해서는 위험의 측정(분석, 평가)이 필요하다.

3.1 소프트웨어공학 부문

소프트웨어제품 평가기준인 ISO/IEC 14598-5 (평가 프로세스)[30], ISO/IEC 14598-6(평가모듈)[31], 소프트웨어 제품 평가기준(품질 특성 및 사용지침)인 ISO/IEC-9126[32], 카네기멜론대학의 소프트웨어 개발조직의 성숙성 평가기준인 CMM[33], 한국 정보통신부의 「소프트웨어사업대가의 기준(2003)」[34],

[표 2] 소프트웨어공학 부문에서의 측정스케일

기준	측정대상 속성	측정스케일	구간수	등급화기준
ISO/IEC 14598-5,6	안전성, 경제성, 보안성, 환경	A, B, C, D	4	서술적
	순응성, 적절성, 정확성, 상호운용성, 보안성	1(poor), 2(fair), 3(good), 4 (excellant)	4	0~1사이의의 구간숫자
CMM	개발환경의 성숙도	1(initial), 2(repeatable), 3(defined), 4(managed), 5(optimizing)	5	서술적
한국 SW사업 대가기준	영향도	0, 1, 2, 3, 4, 5	6	서술적
	품질	상, 중, 하, 불량	4	0~100사이의 구간숫자
	기능점수, 미디어복잡도, 계획	단순, 보통, 복잡	3	서술적
COCOMO-2	스크린, 문서, 복잡도	단순, 보통, 복잡	3	서술적
	경험, 능력, 프로세스, 팀	VL, L, N, H, VH, Extremly High	6	서술적
	고장심각성	None, L, M, H, Critical	5	서술적

B. Boehm이 개발한 소프트웨어 개발비 산정방법인 COCOMO-2[35]에서 측정스케일에 관한 지침들을 조사하였다. 표 2는 소프트웨어공학 부문에서의 측정스케일을 보인다.

각 기준들에서는 측정스케일이 3단계부터 6단계까지 있으며 모든 측정대상속성의 평균 단계 수는 4.26단계이다. 대부분의 평가지침들은 서술적으로 되어있다. 특히, 소프트웨어 품질에 관련된 국제표준은 ISO/IEC 14598에서와 같이 4단계로 분류하고 있다.

[표 3] 정보보호시스템 보안성평가 부문에서의 측정스케일

기준	측정대상속성	측정스케일	구간수	등급화기준
CC	보안기능의 보증수준	EAL0 ~ EAL7	8	서술적
한국정보보호 평가기준	보안기능의 보증수준	K0 ~ K7	8	"
ITSEC	보안기능의 보증수준	E0 ~ E6	7	"
TCSEC	보안기능의 보증수준	D, C1, C2, B1, B2, B3, A1	7	"
CTCPEC	보안기능의 보증수준	T1 ~ T7	7	"
ITSEM	보안강도	Not-basic, Basic, Medium, High	3	서술적, 수치
	전문성	laynam, proficient, expert	3	서술적,수치
	공격시간	minute, day, month	3	수치,
	공격장비	unaided, domestic equipment, special equipment	3	서술적, 수치
	공격기회	결탁, 기회, 발견	3	서술적, 수치
	공모	alone, with user, with adm.	3	서술적, 수치
CEM	보안강도	High, Medium, Basic, No rate	4	서술적, 수치
	보호(저항)강도	H, Moderate, Low, No rate	4	서술적, 수치
	공격경과시간	.5H이하, 1일이하, 1월이하, 1월이상, 기타	5	수치
	전문성	laynam, proficient, expert	3	수치
	TOE 지식	none, public, sensitive	3	수치
	TOE 접근시간	.5H이하, 1일이하, 1월이하, 1월이상, 기타	5	수치
	공격장비	none, standard, specialised, bespoke	4	수치

3.2 정보보호시스템 보안성 평가 부문

국제공통 평가기준인 Common Criteria (CC)[36], CC의 평가지침인 CEM[37], 유럽의 정보보호시스템 평가기준인 ITSEC[38], ITSEC의 평가지침인 ITSEM[39], 미국의 평가기준인 TCSEC[40], 카나다의 평가기준인 CTCPEC[41] 및 한국의 평가기준[42]에서 측정스케일에 관한 지침들을 조사하였다. 표 3은 정보보호시스템 보안성평가 부문에서의 측정스케일을 보인다.

각 기준들에서는 측정스케일이 3단계부터 8단계까지 있으며 모든 측정대상속성의 평균 단계 수는 4.61단계이다. 정보보호시스템 평가기준들에서 보안기능의 평가 스케일은 7 또는 8단계이며 "0 등급"의 개념(예 : EAL0, K0, E0)을 포함하고 있다. 이 분야의 국제표준인 CC는 0등급(EAL 0)을 포함하여 8단계로 표준화 되어있다. 보안강도에 관련된 측정대상속성들은 3부터 5단계이다. ITSEM의 경우 모두 3단계이며 CEM에서는 "해당 없음"(예: No rate, 기타, none 등)을 포함하므로 단계수가 1개 정도씩 증가하였다.

3.3 위험분석 및 관리 부문

카네기멜론대학의 위험관리 방법론인 OCTAVE2.0, 카네기멜론대학의 보안관리 평가기준인 SSE-CMM, 미국 NIST의 자체보안평가지침인 SP-800-26[43], 영국의 보안관리 기준인 BS-7799, 미국 NIST의 위험관리지침 SP-800-30(2002)[44], 카나다의 위험관리 기준인 CSE, 미국의 CIAO의 취약성평가 골격인 CIAO/VAF[45], 미국 NIST의 FIPS-65, 한국 전산원의 위험관리 도구인 HAWK, 한국의 TTAS 표준 TTAS-KO-12.007, 상용 위험분석도구인 CRAMM, 상용위험분석 도구인 BDSS, ETRI의 위험분석도구인 PRAM, Peeples의 연구[46], M. Timms의 연구(1990년)[47], 미국 NBS의 Risk Scoring Method(1988)[48], S. Vallabhaneni의 전산보안감사 방법(1998), 보안관리표준(GMIT) 중 네트워크보안 관리지침인 ISO-13335-5에서 측정스케일에 관한 지침들을 조사하였다.

각 기준들에서는 측정스케일이 2단계부터 14단계까지 있으며 모든 측정대상속성의 평균 단계수는 4.7단계이다. 각 기준들에서 주요 측정대상속성(즉, 자산, 취약성, 위협 및 위험)별 측정스케일은 그림 1에서 보인다.

- 자산 수준 : 평균 단계 수는 6.25이다. CRAMM에서는 10단계로 세분화하였으며 NIST-65와 HAWK에서는 자산수준을 손실액과 연간기대손실치(ALE)를 통해 평가하고 있다. 또한, ETRI-PRAM에서는 자산가용성, 금전손실 및 법적 책임을 자산 평가시에 고려하고 있다.
- 위협 수준 : 평균 단계 수는 4.27이다. BS-7799에서는 위협 수준과 위협의 빈도를 고려하며, CSE에서는 정보보호시스템 평가기준(CEM, ITSEM)처럼 위협원 능력, 위협원의 동기 및 위협원 등급을 고려하고 있다. 또한, ETRI-PRAM에서는 위협 발생가능성과 위협 심각성을 고려하는 것이 특이하다.
- 취약성 수준 : 대부분이 3단계이다(*표시한 것만 고려함). CSE에서는 취약성의 심각성, 취약성의 노출성 및 취약성 수준을 고려하며, BDSS에서는 취약성값의 획득 비용과 취약성 값의 획득 시간도 고려한다.
- 위험 수준 : "위험"은 자산수준, 취약성수준 및 위협수준의 통합적 속성이며, 이들의 조합에 의해 스케일을 정하므로 단계수가 많다(평균 5.2). CRAMM은 7단계이며 PRAM과 ISO-13335는 9단계로 세분화하고 있지만 OCTAVE, NIST-보안관리, BDSS, NBS-Risk Scoring Method 및 전산보안감사에서는 3단계로 구분하고 있다.

3.4 평가스케일의 분석

조사한 각종 표준, 지침, 도구 및 연구결과들의 측정스케일들은 "다양성"으로 표현한다.

- 단계 명칭의 다양성: 숫자와 단어들을 사용하고 있다. 이는 응용분야의 특성을 반영하려한 시도이지만 궁극적으로는 숫자나 문자는 동일한 의미를 갖는다.
- 단계수의 다양성: 위험분석부문의 경우 각 측정대상속성들은 3단계 또는 5단계가 주류를 이루며 일부 자료에서는 10단계(예: PRAM에서의 자산가치)로 정의한 경우도 있다. 단계수가 많아질수록 인접단계간의 분별력이 적어지며 등급화가 어려워진다. 특히, 자산가치, 위협수준, 취약성수준을 등급화 하는 일은 주관적인(또는 서술적인) 기준에 의존해야한다. 따라서, 단계 수를 세분화하는 것은 평가결과에 대한 신뢰성을 저하시킬 수 있으므로, 3단계 또는 5단계가 적합하다고 판단된다. 문

기준	측정대상속성	구간수
BS-7799	자산가치	5
카나다 CSE	자산민감도	5
NIST-65, HAWK	손실액	8
	연간기대손실치(ALE)	7
한국 TTAS	자산	5
CRAMM	자산가치	10
ETRI-PRAM	자산가용성, 금전손실, 법적책임	5
ISO-13335-5	자산가치	5

(a) 자산

기준	측정대상속성	구간수
BS-7799	위협 수준	3
	위협의 빈도	5
카나다 CSE	위협원 능력, 위협원의 동기	3
	위협원 등급	5
CRAMM	위협수준	5
ETRI-PRAM	위협 발생가능성	5
	위협 심각성	3
	위협 수준(1)	3
	위협 수준(2)	7
Peeples	위협 수준	4
Timms	위협 수준	4

(b) 위협

기준	측정대상속성	구간수
OCTAVE 2.0	취약성 수준	*3
BS-7799	취약성 평가	5
	취약성 수준	*3
NIST-보안관리	취약성 수준	*3
카나다 CSE	취약성의 심각성, 취약성의 노출성	3
	취약성 수준	5
CIAO(VAF)	취약성 수준	*3
CRAMM	취약성 수준	*3
BDSS	취약성값 획득 비용	2
	취약성값 획득 시간	14
ETRI-PRAM	취약성 수준	*3
Peeples	취약성 수준	*4
ISO-13335-5	취약성 수준	*3

(c) 취약성

기준	측정대상속성	구간수
OCTAVE 2.0	위험의 영향	3
BS-7799	위험 수준	8
NIST-보안관리	위험 수준	3
CRAMM	위험 수준	7
BDSS	위험 기준	3
ETRI-PRAM	위험 수준	9
Peeples	위험 수준	4
NBS-Risk Scoring Method	위험 수준	3
전산보안감사	위험 수준	3
ISO-13335-5	위험 수준	9

(d) 위험

〔그림 1〕 위험 분석부문의 측정대상 속성별 측정스케일

헌[26]에서는 단계 수에 대한 문제를 고찰하였다.

- 등급화기준의 다양성: 등급화기준은 서술적, 수치적 또는 다른 속성들의 조합(위험 속성의 경우)으로 되어있다. 서술적 기준의 경우, 등급화가 간단하지만 결과의 객관성이 저하된다. 수치적 기준의 경우 위험평가대상 기관의 특징을 반영하기 어렵다. 예컨대, NIST-65나 HAWK처럼 자산가치(피해액)를 금액을 기준으로 하고있는 경우, 10억원의 피해를 입었을 때 피해의 영향은 대기업과 소기업에 있어서 차이는 크지만 이를 항상 최고수준으로 평가하는 것은 문제가 있다.

또한, 단계수의 결정근거와 단계간의 구분근거가 부족하다. 예를 들어, 대부분의 자료에서는 왜 단계 수를 3으로 했는지, 위협수준에서 평균 1년에 1회가 발생하면 왜 "중간"인지(CRAMM의 경우) 등에 대한 근거가 부족하다. 특히, 단계간의 구분근거에 대한 문제는 평가대상기관의 응용, 운영환경, 조직의 특성, 조직의 보안정책 등을 종합적으로 고려하여 결정해야하는 문제이다.

Ⅳ. 위험분석 프로세스

4.1 프로세스, 프로젝트 및 프로덕트의 정의

보안관련 항목은 정보시스템내의 보호가 필요한 자산(asset), 자산에 가해질 수 있는 위협(threat), 공격에 악용될 수 있는 취약성(vulnerability)이며

〔표 4〕 위협과 취약성의 처리 차원에서 위험평가 프로세스의 비교

모델 타입	해당 방법
AVR 타입 : 자산→취약성→위험 (위협 없음)	ISO/IEC TR 13335-3부, OCTAVE
AVTR 타입 : 자산→취약성→위협→ 위험	BDSS, HWAK
ATVR 타입 : 자산→위협→취약성→위험	FIFP-65, FIPS-191, CRAMM, BDSS, 팬타, PRAM, CISSP
ATR 타입 : 자산→위협→위험(취약성 없음)	CSE
TVR 타입 : 위협→취약성→위험(자산 없음)	SP-800-30, SSE-CMM, GAO1, GAO3, 에너지성-SRAG
TR 타입 : 위협→위험(자산과 취약성 없음)	법무성-SRAG
자료 없음	ISO/IEC TR 13335-1부, BS-7799, Open Framework

위험은 이들의 확률적 함수에 의해 수치적으로 계산될 수 있다. 각 IRM 지침과 도구에서는 IRA를 위한 기준이나 척도(예; 등급화 기준)가 제시되어있다.

한편, IRM/IRA의 관점에서 프로세스, 프로젝트 및 프로덕트는 다음과 같이 정의한다.

- 프로세스: IRM/IRA의 타스크들의 업무와 타스간의 수행 순서 및 각 타스크의 입출력을 의미한다. 이를 추상화하고 정형화한 것을 프로세스모델이라 한다. 프로세스 모델의 정의방법, 분석방법 및 시뮬레이션 방법에 대한 연구가 활발하다[49,50]. IRM/IRA는 대부분 지적인 분석업무이므로, 프로세스의 품질이 프로세스의 결과(즉, 프로덕트)의 품질을 좌우한다. 따라서, 우수한 프로세스를 개발하는 것이 매우 중요하다. 프로세스는 학교의 커리큘럼에 비유된다.
- 프로젝트: IRM/IRA은 많은 자원(시간, 인원, 도구)이 소요되는 업무이므로, 효과적인 인원 및 시간관리가 필요하다. 이를 프로젝트 관리라 하며 이 분야에 대한 많은 연구결과가 있다[51]. 프로젝트는 학교의 학사관리 업무에 비유된다.
- 프로덕트: IRM/IRA 수행의 결과물을 의미한다. 자산, 위협, 취약성, 대응책 목록 및 최종 위험평가 결과 등은 프로덕트에 해당한다. 프로덕트는 학교의 졸업생에 비유된다.

본 연구는 기존의 IRM/IRA 표준, 지침 및 도구들에서 사용하는 프로세스를 조사 및 분석한다. NIST, ISO/IED JTC1 SC27, 미 법무성 SRAG, 미 에너지성 DOE, CRAMM에 대한 프로세스 차원의 비교결과는 문헌[52]를 참조한다. 본 논문에서는 비교기준들 중에서 특히, 취약성과 위협의 처리 방법을 기준으로 하고있다.

일반적으로, 위험분석시에 다루어야할 개념인 자산(A), 위협(T), 취약성(V)중에서 위협과 취약성은 그 구분이 애매하므로, 위험분석자들은 취약성과 위협을 처리하는데 어려움이 있다. 본 조사에서는 특히, 위험분석시 위협과 취약성의 처리순서를 기준으로 하여 기존의 프로세스를 비교하였다(표 4 참조).

AVR, AVTR, ATVR 및 ATR타입은 "자산기반" 위험분석 방법이라 할 수 있으며, AVR과 ATR은 위협과 취약성간의 애매성을 배제하기 위해 한가지만을 택하고 있다. 특히, 위험분석 방법중 지명도가 높은 카나다의 CSE와 SEI의 OCTAVE는 이 부류에 속한다. 또한, AVTR과 ATVR타입의 경우에도 위협과 취약성중 한가지만을 집중적으로 분석하고있다.

4.2 기존 프로세스의 문제점

첫째, 대부분의 방법(특히, 도구)들은 위험분석 프로젝트의 관리에 대한 지원기능이 부족하다. 위험분석은 평가대상조직의 내부자, 조직의 외부자(예: 사용자) 및 위험분석자들이 다수 참여하며 많은 미팅이 진행되며 많은 문서들이 적시 적소로 이동해야하며 평가기간도 수개월에 이른다. 이를 위해서는 평가 프로세스 내에 프로젝트 관리활동과 그룹웨어 기능이 필요하다.

둘째, Top-down 위험분석을 실시하지 않고 있다. Top-down 위험분석이란 위험분석을 상위수준과 하위수준으로 구분하여 실시하는 것이며 상위수준에서는 ISO/IEC 13335나 BS-7799와 같은 보안관리 표준의 준수여부를 분석 및 평가하는 것이다. 하위수준은 각 자산별 위협, 취약성을 바탕으로 위험을 분석하는 것이다. 상위수준은 Black-box 분석방법이며 하위수준은 White-box 분석방법이라 할 수 있다. ISO/IEC -13335의 보안관리와 이를 토대로 한 한국의 TTA표준에서는 "상위수준" 위험

분석 단계가 있지만 "상세수준" 위험분석 단계가 없으므로, 진정한 Top-down 위험분석이라 할 수는 없다.

V. 자산분류 및 평가방법

5.1 자산분류체계

표 5는 기존의 자산분류체계들을 보인다. 대부분의 기준에서는 유사한 분류체계를 택하고 있지만 카나다 CSE의 경우 5수준으로 세분화하고있으며 OCTAVE에서는 주로 IT자산만을 대상으로 하고 있다.

5.2 자산평가 방법

각 자산클래스의 평가방법은 다음과 같다.

- HW 자산: HAWK, CRAMM에서 적용한 방법은 자산에 대한 성능 대비 가격변동에 따른 자산 교체비용을 적용하였으나 시세차액을 고려한 교체비용을 산정하는데 시간이 많이 걸리며, TTA-KO-12.00과 BS-7799에서 적용한 감가상각비는 운영시 시간경과에 의한 해당 자산의 평가절하를 고려하여 "감가상각 비용" 속성에 해당하는 자산의 취득비용과 사용연수와 사용연한만을 입력한 결과를 HW 자산가액으로 한다.
- 상용 SW자산: TTA-KO-12.00과 BS-7799에서는 "상용 SW"는 구매비용에 무료 보상이 가능한 보증 정보의 합으로 산정하고 있다. 정비료(구입가의 9~11%)와 운영비는 자산의 가치라 볼 수 없으므로, 이를 제외할 수 있다.(예, 자동차의 운영비는 자동차의 가치와 무관하다). 또한, 감가삼각 비용은 적용하지 않으며, 상용 SW의 가치는 최초 구매비용과 업그레이드비용의 합으로 계산한다.
- 개발 SW 자산: TTA-KO-12.00과 BS-7799에서는 "개발 SW"는 재 개발비에 기회비용을 합산하고 있다.
- 자료와 무형자산: HAWK에서는 자료와 무형자산에 대한 가치산정을 위해 복구비용과 손실비용을 이용한 간접적 산정을 적용하였고, TTA-KO-12.00과 BS-7799는 자료에 대해선 복구비용을, 무형자산에 대해서는 중요도에 따른 정성적 평가로 자산가액을 산정하였다.

5.3 기존의 자산분류체계의 문제점

자산분류스키마는 자산 파악 및 분류업무에 직결되므로, 자산파악의 용이성과 결정성(determinism)을 제고하도록 자산을 분류해야한다. "결정성"이란 자산의 분류결과가 분류자에 무관하게 일정한가를 나타내는 성질이다.

- 정보보호시스템평가 부문(CC와 기존 PP)에서는 "자료"만을 기준으로 하고 있으므로, 조직전체의 자산평가에는 부적합하다. OCTAVE에서는 "장비"를 기준으로 분류함으로서, 평가대상기관내의 데이터나 소프트웨어 및 응용들을 분류하기가 어렵다.
- 모든 경우에, 평가대상기관의 "응용"을 고려하지 않고 있다. 또한, "자료"나 "정보"를 최상위 단계에서 분류하고 있으며, 평가대상기관내의 자료와 정보는 매우 추상적이며 응용과 결부되어야만 가치가 있으므로, 자료와 정보를 하위수준으로 분류하는 것이 좋다.
- KISA와 PRAM에서는 "하드웨어"와 "소프트웨어"를 최상위 단계에서 분류함으로서 자산파악시의 결정성이 저하된다. 예컨대, 웹서버의 경우 HW와 SW를 구분하기가 어렵다. 특히, 서버를 구할

〔표 5〕 기존의 자산분류 체계

기 준	대 분 류	분 류 수 준
HAWK	7종 (H/W, 운영체제, 네트워크, 자료, 응용, 사용자, 환경)	없음
KAIST 펜타	5종 (S/W 및 자료(업무 프로세스에 직접적으로 연관), OS, HW, 네트워크, 인원, 환경	없음
ETRI PRAM	5종 (SW, HW, 네트워크, 물리적, 기타)	없음(응용 및 공통자산)
카나다 CSE	8종 (정보, 프로세스, 플랫폼, 인터페이스, 인사, 환경, 기타 유형자산, 무형 자산)	5
OCTAVE	9종 (서버, 네트워크 장비, 보안장비, 워크스테이션, PC, 랩탑, 저장장치, 무선장비, 기타	없음

[표 6] 기존방법에서의 위협과 취약성의 정의

방법	위협정의	취약성정의
TTAS	• 자산에 피해를 가할 수 있는 잠재적인 요소	• 자산이 지닌 잠재적인 약점 • 이 약점 자체가 직접적인 위험을 초래하지는 않지만, 위협에 의해 이용되어 위험을 발생시킬 환경 제공
GMITS, BS-7799	• 시스템, 조직, 조직의 자산에 피해를 주는 원치 않는 사고를 일으킬 잠재성 가짐 • 피해는 비 인가된 파괴, 공개, 변경, 훼손, 불 가용성, 손실 등 IT 시스템에 의해 처리되는 정보 또는 서비스에 대한 직간접의 공격으로부터 발생 • 자산에 피해를 입히기 위하여 위협은 자산의 취약점을 파고듦	• IT 시스템이나 사업목표에 유해한 위협이 침투하는 경로 • 취약성 자체는 피해를 일으키지 않음 • 단지 하나의 조건 즉, 위협에 의해 자산이 피해를 입게 되는 일련의 조건 • 악용의 소지가 있고 바람직하지 않은 결과를 초래할 수 있는 시스템상의 약점이 포함 • 위협이 피해를 일으키는 기회 • 특정 시스템이나 조직내의 모든 취약성이 위협으로 직결되는 것은 아님 • 취약성에 대응하는 위협이 존재하는 경우가 관심의 대상 • 취약성 분석은 식별된 위협이 침투할 수 있는 약점을 점검하는 것
CSE	• 임계 정보, 자산 또는 서비스에 대하여 인가되지 않은 폭로, 파괴, 제거, 변경, 방해중 하나 이상이 발생하도록 원인이 되는 잠재적인 사건 또는 활동	• 그것이 작용하고 있는 시스템 경계나 환경내의 어떠한 자산의 계량적인 위협-독립적 특성 또는 속성. 그것은 기밀성, 가용성 및 무결성에 대한 피해 원인과 위협 이벤트 발생 확률을 늘리거나 발생하는 위협 이벤트의 영향 강도를 늘린다.
HAWK	• 위협과 취약성의 개념에 대해서는 언급하고 있지 않음 • 각각의 의미를 혼용해서 사용	
OCTAVE	• 위협과 취약성을 혼용해서 사용 • 행위자는 위협원과 취약성이며 위협원은 취약성을 이용	
PRAM	• 정의 불분명	• 특정 자산 항목이 특정 위협의 공격에 대해 얼마나 많이 노출되어 있는지, 즉 위협(액터)에 의해 얼마나 쉽게 이용될 수 있는지에 의해서 평가 • 특정 자산이 위협에 대한 대항력(보안대책) 수준으로 이해 • 취약성 평가에서도 취약성 자체의 심각성과 취약성이 위협에 의하여 현실화되었을 때 나타나는 영향의 두 측면을 동시에 고려 • 취약성이 현실화되어 나타나는 피해의 정도는 자산의 평가에서 이미 반영됨으로 취약성의 심각성, 즉 위협 인자에 얼마나 많이 노출되어 있는가를 평가
BDSS	• 정의 불분명	없 음
NIST	• 특정 취약성을 성공적으로 발생시키는 특정 위협원의 잠재성 • 위협원은 발생될 수 있는 취약성이 없을 때 위험을 발생시키지 않음	• 취약성은 우발적인 발생 또는 의도적인 악용이 될 수 있는 약점 • 수행(우발적 발생 또는 고의적 악용)될 수 있는 시스템 보안 절차, 설계, 구현 또는 내부 제어 상의 틈이나 약점과 보안 불이행 또는 시스템 보안 정책의 위반 결과

때 HW와 SW(OS등)을 별도로 구입하지는 않으며 HW와 시스템 SW를 하나의 플랫폼으로 간주하므로, 자산평가시에는 하나의 시스템으로 보는 것이 유리하다.

- PRAM의 경우, "인간"을 고려하지 않고 있다. 따라서, 인간은 평가대상기관의 주체이며 위험의 근원이므로 반드시 분류되야 한다. 참고로, 평가대상기관의 위험은 주로 인간 때문에 발생하며 정보시스템은 인간의 도구에 지나지 않는다.
- KISA 및 HWAK의 경우, "네트워크"와 "환경"을 최상위 단계에서 분류하고 있다. 최근의 평가대상기관의 정보시스템에서는 네트워크와 서버(HW, OS 등)를 구분하기가 어렵다. 따라서, 네트워크를 하위수준으로 분류하는 것이 유리하다. 또한, "OS"를 최상위 단계에서 분류하고 있다. 일반적으로 OS는 HW와 별도로 구입하지는 않으므로 "OS"만을 최상위 수준으로 분류하는 것은 불합리하다.
- BS7799와 CSE에서는 "서비스" 또는 "프로세스"를 최상위에서 분류하고 있다. 서비스나 프로세스

개념은 자산평가대상기관의 "응용"으로 처리하는 것이 유리하다.

Ⅵ. 위협의 분류

6.1 위협의 분류방법

위협원에 대한 분류는 위협원이 인간인 경우와 비인간인 경우로 분류할 수 있다. 위협원이 인간(해커, 사용자 개발자, 시스템관리자)인 경우는 ITSEM의 보안강도 계산규칙을 5단계로 확장하여 적용하고, 비인간(자연재해, 고장 등)인 경우는 PRAM이나 CRAMM에서 사용한 5단계의 발생빈도별 기준을 사용하는 것이 바람직하다.

ITSEM에서 정보시스템의 "보안강도" 개념은 "위협수준"의 반대 개념이며 보안강도가 높을수록 위협수준은 낮으며 위협개념은 "공격" 개념을 포함한다고 가정하였다. 즉, 위협수준은 공격시간, 공모여부, 위협원의 전문성 및 위협원이 가용한 공격장비의 수준의 함수로 정한다. CSE나 OCTAVE에서도 위협원의 동기, 능력을 고려하였다.

6.2 위협과 취약성의 구분

위협과 취약성간의 구분문제는 논란이 많으며 표 6과 표 7은 기존 방법들에서 위협과 취약성의 개념상의 구분결과를 보인다. TTAS에서는 위협과 취약성이 동일한 분류체계를 가지므로, 이는 위협과 취약성을 유사한 개념으로 보는 것이다. 특히, GMITS, BS-7799, HAWK, PRAM, CRAMM, NIST-CVE, OCTAVE에서는 취약성을 별도로 분류하지 않고 있다. 따라서, 취약성과 위협간의 구분에는 논란의 여지가 많다.

예컨대, NIST의 취약성 데이터베이스인 Common Vulnerability and Exposure(CVE)[53]에서 취약성 번호가 CVE-1999-0002인 "NFS의 mountd 프로그램에서, 오버플로우 때문에, 주로 Linux 시스템에서 원격의 공격자가 루트에 접근함"(http://www.cve.mitre.org/cve/ 참조)이라는 취약성은 시각에 따라 위협으로도 볼 수 있다. 즉, "Linux 시스템에서 원격의 공격자는 NFS의 mountd 프로그램을 악용하여 루트에 접근함"으로 해석할 때는 위협이 된다. 이런 문제 때문에 위험분석자들은 취약성과 위협을 처리하는데 어려움이 있다.

Ⅶ. 결 론

본 조사연구에서는 정보시스템의 보안관리, 위험분석 및 PP개발을 위한 방법(또는 지침, 표준)들에서의 프로세스, 분류체계, 평가기준 및 평가스케일들을 조사 분석하였다.

특히, 정보시스템의 보안관리, 위험분석 및 PP개발 부문은 정보보호 컨설팅 분야에서 필수적인 부문이며 본 결과는 새로운 보안관리방법 및 기준을 개발하고, 위험분석 및 평가방법을 개발하며, 또한, PP

[표 7] 위협과 취약성 처리 방법

비교항목 / 방법	위협분류 수준 및 종수	위협분류 기준	취약성분류 수준 및 종수	취약성 분류기준	중복여부
TTAS	1수준, 7종	자산기반	1수준, 7종	자산기반	분류 중복
GMITS, BS-7799	3조합, 47종	위협원 (계획적-우연-자연적의 조합)	분류 없음 (보안영역별 예 만 보임)	없음	-
CSE	5수준, 72종	위협원	4수준, 166종	위협원	-
HAWK	3수준, 133종	자산 기반	1수준, 31종	없음	-
PRAM	3수준, 14종이상	위협원	없음	없음	-
BDSS	3수준, 60종	위협원	4수준, 93종	취약원	-
CRAMM	3수준, 32종	위협원	-	없음	-
NIST- CVE	3수준, 42종	위협원	4조합, 864종 (취약원-결과-형태-노출자산의 조합)	없음	-
OCTAVE	4조합, 70종	접근-행위자-동기-결과의 조합	없음	없음	-

의 개발방법을 연구 및 개발하는데 필요한 문헌조사 결과로써 활용될 수 있을 것이다.

참 고 문 헌

[1] ISO/IEC TR 13335, 1부, "IT보안 개념 및 모델"(1996), 2부 "보안관리 및 계획"(1997).

[2] ISO/IEC TR 13335, 3부, "IT 보안관리 지침"(1998), 5부, "네트워크 연결관리 지침" (2000).

[3] British Standards Institution(BSI), "BS-7799", 1999.

[4] Bundesamt fur Sicherheit in der Informationstechnik), "IT Baseline Protect Manual", - Standard security safeguards, http://www.bsi.bund.de/gshb/english/menue.htm

[5] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document", V.2, http://www.sse-cmm.org, 1999. 4. 1.

[6] 정보통신부, "전산망 보안을 위한 위험관리 지침서", KICO.KO-10.0047, 1995.12.

[7] 이강수, "선진국 정보보호시스템의 평가제도에 관한 연구", KISA 보고서, 1998. 3.

[8] 이강신, 김학범, 이홍섭, "국내외 정보보호 모델에 관한 연구", 정보보호학회지, 11-3, 2001.6

[9] S. Vallabhaneni, "Auditing Computer Security-A Manual with Case Studies", 1989.

[10] ISO/IEC 14598-1, "IT-Software product evaluation, Part 1. General overview", 1997. 3.

[11] FIPS-65, "Guidelines for Automatic Data Processing Risk Analysis", NIST, 1975 (Aug. 1995에 폐지됨).

[12] FIPS-191, "Specifications for Guideline for The Analysis Local Area Network Security", NIST, Nov. 1994.

[13] NIST, "Risk Management Guide for Information Technology Systems", NIST-SP-800-30, 2001.10.

[14] NISTIR-4387, "Simplified Risk Analysis Guideline", NIST, 1990.

[15] NISTIR-4325, "Simplified Risk Analysis Guideline", NIST, 1990.

[16] GAO, "Information Security Risk Assessment - Practices of Leading Organizations", - Case Study 1, GAO/AIMD-00-33, 1999. 11.

[17] GAO, "Information Security Risk Assessment - Practices of Leading Organizations", - Case Study 3, GAO/AIMD-00-33, 1999. 11.

[18] CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment(CSE)", 1996.

[19] TTAS, "공공정보시스템 보안을 위한 위험분석 표준 - 개념과 모델", TTAS.KO-12.007, 1998. 11.

[20] OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute(2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http://www.sei.cmu.edu/publications/ pubweb.html.

[21] CRAMM, "A Practitioner's View of CRAMM", http://www.gammassl.co.uk/.

[22] 김기윤, 나관식, 김종석, "보안관리를 위한 위협, 자산, 취약성의 분류 체계", 정보보호학회지, 6권 1호, 1995. 6.

[23] Will Ozier, "Risk Analysis and Assessment", Information Security Management Handbook (4'th Ed.), CRC Press, 2000.

[24] C. Hamilton, "Data-driven Security: How to Target, Focus and Justify the Security Program", 28'th Annual Computer Security Conference & Exhibition, 2001.

[25] "시만텍사의 Expert 4.1 소개", 1회 서울정보보안기술 국제컨퍼런스, 2000년 11월.

[26] 김정덕 (외), "위험 분석 도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.

[27] 송관호(외), "정보시스템 보안을 위한 위험분석 소프트웨어 개발" 한국전산원 연구보고서, 1997. 12.

[28] J. Freeman, et al., "Risk Assessment for Large Heterogeneous Systems", 13'rd Computer Application Conference, 1997.
[29] R. Craft, et al., "An Open Framework for Risk Management", 21'st National Information System Security Conference, 1998.
[30] ISO/IEC 14598-5, "IT-Software product evaluation, Part 5. Process for evaluation", 1997. 12.
[31] ISO/IEC 14598-6, "IT-Software product evaluation, Part 6. Documentation for evaluation modules, 1997. 3.
[32] ISO/IEC-9126 "IT-Software product evaluation - Quality characteristics and guidelines for their use, 1991. 12. 15.
[33] B. Boehm, "Software Engineering Economics", Prentice-Hall, 1981.
[34] 「소프트웨어사업대가의 기준(2003)」, 정보통신부, 2003.
[35] Barry Boehm, et al., "COCOMO 2.0 Software Cost Estimation Model", International Society of Parametric Analysts, May 1995, http://sunset.usc.edu/research/COCOMOII /index.html.
[36] CC, "Common Criteria for Information Technology Security Evaluation", Version 2.1, CCIMB-99-031, August 1999, http://www.commoncriteria.org/site_index.html.
[37] CEM, "Common Evaluation Methodology", Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site_index.html
[38] European Community, "Information Tech nology Security Evaluation Criteria (ITSEC)", Ver. 1.2, June 1991. http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm
[39] European Community, "Information Technology Security Evaluation Criteria (ITSEM)", Ver. 1.0, 1993. http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm
[40] DoD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)", Dec. 1985.
[41] Canadian System Security Centre, "The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)", Ver.3e, Jan. 1993.
[42] "정보통신망 침입차단시스템 평가기준·평가지침서", 정보통신부고시 1998-19호, 정보통신부, 1998.
[43] M. Swanson, "Security Self-Assessment Guide for Information Technology Systems", NIST- SP-800-26, NIST, IT 보안평가, 2001.11.
[44] G. Stonebumer, et al., "Risk Management Guide for Information Technology System", NIST-SP-800-30,NIST, 2002.1.
[45] CIAO/VAF, "Vulnerability Assessment Framework 1.1", Critical Infrastructure Assurance Office(CIAO), 1999.10.
[46] D. Peeples, "The Foundations of Risk Management", 20'th National Information Security Conference, 1997.5.
[47] M. Timms, "A Practical Approach to Risk Assessment", Compsec Computer Security Conference'90, 1990. 10.
[48] Z. Ruthber et al., "Guide to Auditing for Controls and Security: A System Development Lifecycle Approach", NBS Special Publication 500-153, 1998.4.
[49] A. Finkelstein et al. (ed.), "Software Process Modeling and Technology", John Wiley&Sons, 1994.
[50] A. Furretta, A. Wolf, (ed.), "Software Process", John Wiley&Sons, 1996.
[51] W. Royce, "Software Project Management - Unified Framework", Addison Wesley, 1998.
[52] 이병만, 윤정원, 박승규, "정보시스템 위험분석 모델에 관한 연구", WISC-97, 1997.
[53] CVE, "Common Vulnerability and Exposure", NIST, http://www.cve.mitre.org/cve/.

〈著 者 紹 介〉

최 상 수 (Sang-Soo Choi)
학생회원

2001년 2월 : 한남대학교 컴퓨터공학과 졸업 (학사)
2003년 2월 : 한남대학교 대학원 컴퓨터공학과 졸업 (석사)
2003년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 소프트웨어공학, 웹공학, 보안공학, 정보보호 컨설팅 및 위험분석

방 영 환 (Young-Hwan Bang)
학생회원

1997년 2월 : 한남대학교 컴퓨터공학과 졸업 (학사)
2002년 2월 : 대전대학교 대학원 컴퓨터공학과 졸업 (석사)
2002년 3월~현재 : 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사
2002년 8월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학

최 성 자 (Sung-Ja Choi)

1991년 2월 : 한남대학교 컴퓨터공학과 졸업 (학사)
1997년 2월 : 한남대학교 대학원 컴퓨터공학과 졸업 (석사)
2002년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 소프트웨어공학, 웹공학, 보안공학

이 강 수 (Gang-Soo Lee)
종신회원

1981년 : 홍익대학교 컴퓨터공학과 졸업 (학사)
1983년 : 서울대학교 대학원 전산학과 졸업 (이학석사)
1989년 : 서울대학교 대학원 전산학과 졸업 (이학박사)
1985년~1987년 : 국립대전산업대학교 전자계산학과 전임강사
1992년~1993년 : 미국일리노이대학교 객원교수
1995년 : 한국전자통신연구원 초빙연구원
1998년~1999년 : 한남대학교 멀티미디어학부장
1987년~현재 : 한남대학교 컴퓨터공학과 정교수
관심분야 : 소프트웨어공학, 병행시스템 모형화 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼