제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

공공기관의 보안 진단을 위한 보안평가모델 설계에 관한 연구

엄정호*, 박선호*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:{jheom, shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

A Study on an Architecture of Security Assessment Model for Security Diagnostics of a Public Institution

Jung-Ho Eom*, Seon-Ho Park* and Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information & Communication Engineering , Sungkyunkwan University

요 약

본 논문에서는 공공기관의 효율적인 보안 진단을 위하여 금융 위험평가 시스템에 사용되는 통계적 CAEL 모델을 적용하여 보안평가 모델(SAM)을 설계하였다. SAM은 통계적 CAEL 모델을 기반으로 조직과 관련된 보안변수와 보안지표를 평가요소로 하여 요소별 평가등급 선정 방식과 최종 종합평점 산출 방법으로 보안평가 결과값을 도출한다. SAM은 조직의 보안수준 결과에 중요하게 영향을 미칠 수 있는 모든 요소들을 평가대상으로 하고 정량적인 방법인 보안평가 모델을 활용하여 결과를 산출한다. SAM은 조직의 규모, 특성 등에 따라 보안변수를 변경할 수 있으며, 각 보안 지표별 통계적 자료값을 수집하여 요구되는 변수만 입력하면 되기 때문에 사용 용이성도 우수하다.

1. 서론

현대사회에서 산업기술 가치가 금전적 가치보다 높아짐에 따라 정보 유출이 심각한 보안문제로 대두되었다. 이렇게 됨에 따라 공공기관에서는 정보시스템과 데이터를 보호하고 피해를 최소화하기 위해 위험분석,보안진단 평가 방법에 대한 관심이 높아지게 되었다.[1,2].

위험 평가나 취약성 평가는 정보통신체계를 대상으로 위험분석이나 취약성분석을 통하여 위험이나 취약 수준을 평가한 후 그에 맞는 정책이나 대책을 수립하는 것이다[3]. 기존의 TR-13335[4], CSE MG-2 Manual[5], NISTIR 4325 RAM[6]과 같은 위험분석 모델은 대상이 대부분 정보통신체계에 국한되어 있다. 즉, 조직 전반에 걸친 위험분석을 수행하지 못한다. 또한, 평가방법이 주로 Matrix Scaling 방법이나 델파이 방법을 사용하여 평가자의 주관에 따라 결과값의 차이가 발생할 수 있다. SAM은 이러한 기존의 위험평가모델들이 가지고 있는 단점을 극복하기 위하여 조직의 보안평가 결과에 영향을 미칠 수 있는 모든 요소들을 식별하여 보안변수들을 선별하고 보안변수에 영향을 미칠 수 있는 세부 보안평가 요소인 후보 보안지표들을 선정하여 통계적 CAEL 모형의 평가공식에 의하여 등급제와 점수로 평가를 수행한다.

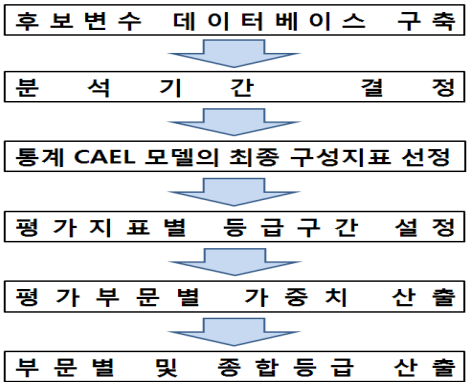
본 논문에서는 조직의 총체적인 보안진단평가를 위해 금융감독원에서 금융회사의 잠재위험에 대한 평가를 수행할 때 이용되는 통계적 CAEL 모형을 활용하여 정량적인 보안수준을 평가할 수 있는 보안평가모델(Security Assessment Model)을 제시하였다. 논문 구성은 2장에서 통계적 CAEL 모델, 3장에서는 SAM 설명, 마지막으로 4장에서는 결론을 맺는다.

2. 통계적 CAEL 모델

금융감독원에서 저축은행에 대한 건전성 감독을 강화하기 위해 도입한 경영실태평가제도 방식 중 하나가 CAMEL 모델이다[7]. CAMEL 평가제도는 각 금융회사의 자본적정성(Capital adequacy), 자산건전성(Asset quality), 경영진의 경영관리능력(Management), 수익성(Earnings) 및 유동성(Liquidity) 등 5개 부문에 대한 부문별 및 종합평가를 실시하고, 평가결과를 1~5등급의 평가등급으로 나타낸다. 한편, 금융감독원은 금융회사의 본점에 대한 종합 검사 시 실시되는 CAMEL 평가와 함께 매분기 각 금융회사의 업무보고서를 바탕으로 경영관리부문(M)을 제외한 CAEL 평가를 실시하고 있다. CAEL 평가는 금융회사에 대한 상시감시 및 조기경보시스템의 한 방법으로 은행의 재무건전성을 평가하기 위하여 분기 또는 반기별로 경영실태 평가 시 사용되는 계량지표를 이용하여 평가하는 제도이다. CAEL 평가 모델은 일반적으로 1~3등급에 주로 분포하고 등급의 변화도 크지 않은 단점이 있어 정확한 위험평가가 이루어지지 않는다.

통계적 CAEL 모델(Statistical CAEL Model)[8]은 위에서 설명한 CAEL 평가 방식이 보수적으로 운용되어 등급의 변화가 크지 않은 점을 보완하기 위해 통계적 기법을 사용하여 CAEL 평가등급을 산출하는 위험평가 모델이다. 이 모델은 평가지표의 선정, 평가부문별 가중치의 부여, 평가지표별 등급구간 설정방식 등에 있어 통계적 기법을 활

용함으로써 상대적으로 취약한 개별 금융회사를 식별할 수 있다. 통계적 CAEL 모델의 특징은 첫째, 다양한 재무지표의 유의성을 검증하고 최종 평가지표를 선정함으로써 금융산업의 건전성과 위험도의 변화내용 등을 보다 잘 반영할 수 있게 된다. 둘째, 통계적 기준에 의해서만 지표별 등급구간을 설정함으로써 개별 금융회사의 재무건전성의 변동성을 보다 잘 포착할 수 있다. 마지막으로 종합등급의 산출방식을 부문별 평가등급 정보를 보다 잘 반영할 수 있도록 함으로써 동일 등급을 가지는 두 개의 금융회사에 대한 위험도 비교도 가능하다. 통계적 CAEL 모델의 절차는 (그림 1)과 같다.



(그림 1) 통계적 CAEL 모델의 절차

① 후보변수 데이터베이스 구축 : 은행산업의 후보변수 데이터베이스는 은행산업의 건전성과 위험에 영향을 미치는 다양한 변수들을 대상으로 구축한다.

② 분석기간 결정 : 통계적 CAEL 모델의 분석기간을 결정한다. 분석기간이 짧으면 분석에 필요한 충분한 시계열을 확보할 수 없으며, 길면 은행산업의 구조변화에 따른 가중치의 변화 등을 반영할 수 없다.

③ 최종 구성지표 선정 : 평가지표의 데이터베이스에서 은행산업의 건전성 및 위험수준과 관련성이 높은 변수를 선별한다. 그리고 주성분분석을 통해 부문별로 지표의 기여도를 산출하고 기여도가 낮은 변수를 평가지표에서 제외한다.

④ 평가지표별 등급구간 설정 : CAEL 평가등급을 산출하기 위해서는 평가지표별 평가등급을 산출해야 하며, 이를 위해서는 평가지표별로 등급구간을 설정해야 한다.

⑤ 평가부문별 가중치 산출 : 평가부문별 가중치는 중요도에 따라 각각 10~30%내에서 부여한다.

⑥ 부문별 및 종합등급 산출 : 부문별 평가등급 정보를 나타낼 수 있는 방식으로 종합등급을 산출한다.

3. 보안평가모델(SAM)

보안평가모델(SAM: Security Assessment Model)은 기업이나 조직의 총체적인 보안수준을 통계적 CAEL 모델[8]을 이용하여 정량적으로 평가하는 모델이다. 네트워크나 시스템과 같은 정보통신체계 뿐만 아니라 시설, 문서, 조직원 등과 같이 조직에 포함되어 있는 모든 구성요소들에 대하여 부문별 평가와 종합적인 평가등급과 점수를 산출하여 보안수준을 측정하는 것이다.

3.1. 보안평가모델(SAM)의 요구사항

SAM이 기존의 위험분석모델과 차별성을 두고 보다 객관적이고 향상된 결과를 산출하려면 다음과 같은 요구사항을 충족시켜야 한다.

첫째, 보안수준 상태를 구체적으로 알 수 있기 위해 정량적인 평가가 가능해야 한다. 기존의 위험분석 도구[4-6]의 보안수준 평가방법(등급제)으로는 조직의 보안변수나 보안지표에 대한 정확한 보안수준을 측정하기 어렵다. 예를 들어 보안평가 결과가 '보안수준 낮음(4등급)'과 '보안수준 평가 결과가 45점으로 4등급'은 보안 관리자에게 후속조치를 취하는 데 전혀 다른 기준을 제공한다.

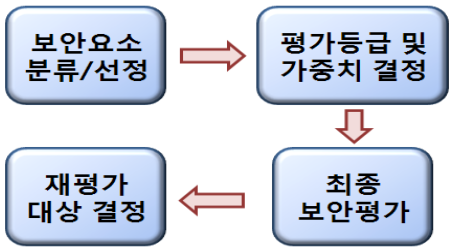
둘째, 보안평가를 위한 보안변수나 지표는 조직의 보안수준에 영향을 미칠 수 있는 모든 요소를 식별하고 포함할 수 있도록 분류하고 선정해야 한다. 특정 보안변수에 치우치거나 제외하지 않고 평가의 주성분 역할을 할 수 있는 변수와 지표를 선정해야만 조직에 대한 총체적인 보안평가를 할 수 있다. 보안지표의 후보지표들 중에서 조직의 기여도가 높거나 보안평가와 연관성이 높은 요소들을 선정해야 한다.

셋째, 평가등급의 구간을 설정할 때 구간의 차이가 실용적이어야 한다. 만약, 등급 구간이 한쪽으로 치중하거나 모든 등급의 구간이 동일하다면 보안지표 중에 취약한 지표를 식별할 수 없다. 그래서 평균과 표준편차를 이용하여 각 평가등급별 구간을 설정하여 결과 오류를 제거한다.

마지막으로, 조직의 주성분 요소로 작용되거나 보안 위협에 노출되어 있는 구성요소에 대해서는 조직내의 비중을 고려하여 보안평가시 가중치를 적용해야 한다. 예를 들면, 예전에는 시설이나 문서에 대한 물리적 보안을 강조하였으나, 최근에는 시스템과 네트워크 기술이 발달함에 따라 정보통신에 의한 업무 의존도가 높고 정보 유출 빈도수도 증가하고 있기 때문에 정보통신 보안지표에 대한 보안평가 비중이 높아지고 있다.

3.2. 보안평가모델 설계

SAM은 (그림 2)와 같이 설계하였으며, 수행절차는 아래와 같다.



(그림 2) 보안평가모델

보안요소 분류 및 선정에는 보안변수 분류와 보안지표 선정으로 구성된다.

① 보안변수 분류

보안평가에 필요한 보안변수는 조직의 보안수준과 위험에 영향을 미칠 수 있는 다양한 요소들을 대상으로 분류한다. 특히, 내·외부로부터 위협에 노출되어 있는 취약점을 가진 요소들을 식별해야 한다. SAM은 공공기관에서 보안평가 요소로 설정할 수 있는 계획, 구성원, 문서, 시설, 정보통신으로 분류한다.

② 보안지표 선정

보안변수별로 보안지표를 선정한다. 우선 조직의 보안상태나 위험수준에 영향을 미칠 수 있는 보안지표를 선별하고 보안수준에 "+"로 적용되는 지표나 "-"로 적용되는 지표들을 식별해야 한다. 예를 들면, 보안계획에서 보안행사 참여율은 높으면 높을수록 좋으나, 보안사고가 낮으면 낮을수록 좋은 요소로 작용한다. <표 1>은 SAM의 보안변수별 보안지표의 예를 보여준다.

<표 1> 보안변수별 보안지표

보안변수	보안지표
보안계획	정기 보안업무 실천율, 보안행사 참여율, 보안사고 현황 등
구성원	보안교육 현황, 보안위규자 현황, 보안책임 임명율, 업무만족도 등
보안시설	사무실 관건율, 폐휴지 처리율, 개인 책상/비품 관건율 등
문서	문서방치건수, 보안시험평균율, 문서분실건수 등
정보통신	네트워크 침해율, 보안프로그램 미설치율, 비인가 저장장치 휴대율, 비밀번호 미설정율 등

평가등급 및 가중치 결정에는 평가등급 설정과 보안변수 가중치 결정으로 구성된다.

③ 평가등급 설정

SAM은 통계적 기준에 의한 보안변수별 등급구간을 설정하여 신축성을 보장한다. 3단계에서 선정한 보안변수별 보안지표의 등급구간을 보안지표들의 평균과 표준편차를 이용하여 <표 2>와 같이 부여한다. 이 방식은 보안지표의 값이 평균으로부터 표준편차의 배수(0.5 및 1.5배)에 해당하는 만큼 멀어진 거리에 비례하여 양호 또는 불량한 등급을 받도록 설계되어 있다. 표준편차의 배수의 선정은 이상적인 정규분포를 가정하는 경우 최하위 5등급에 9%, 4등급에 24%, 3등급에 34%, 2등급에 24%, 그리고 최상위 1등급에 9%를 배분함을 의미한다.

<표 2> 보안지표 평가등급 설정

등급	높은 값일수록 양호한 구성요소	낮은 값일수록 양호한 구성요소
1	(평균+1.5×표준편차) 이상	(평균-1.5×표준편차) 이하
2	(평균+0.5×표준편차) 이상	(평균-0.5×표준편차) 이하
3	(평균-0.5×표준편차) 이상	(평균+0.5×표준편차) 이하
4	(평균-1.5×표준편차) 이상	(평균+1.5×표준편차) 이하
5	(평균-1.5×표준편차) 미만	(평균+1.5×표준편차) 초과

④ 보안변수 가중치 결정

SAM에서는 공공기관에서 주로 사용하고 있는 보안감사의 분야별 평가비율을 적용하나, 최근의 보안사고 발생의 주요 원인을 고려한다. 즉, 내부자에 의한 보안사고가 증가[9]하고 정보통신체계에 대한 중요도가 높기 때문에 SAM에서는 구성원과 정보통신 분야에 대한 가중치를 좀 더 높게 적용하였다. 가중치는 보안계획 10%, 구성원 20%, 보안시설 10%, 문서 20%, 정보통신 40%로 적용한다.

⑤ 최종 보안평가

평가등급에 의한 평가는 조직의 보안수준을 추상적으로 제시함으로써 구체적인 보안수준에 대한 세부 결과값을 제시할 수 없는 단점이 있다. 예를 들면 두 개의 조직의 최종 보안평가가 2등급으로 동일하다면, 어떤 분야의 어떤 보안지표가 우수하다거나 미흡하다는 것을 구별할 수 없다. 그래서 SAM은 보안변수별 보안지표의 정량적 평가가 가능하도록 등급별 점수를 부여하였으며, 그 값은 <표 3>과 같다.

<표 3> 등급별 점수 산정

등 급	1등급	2등급	3등급	4등급	5등급
점 수	5점	4점	3점	2점	1점

<표 3>에 의해 보안변수별 보안지표가 4개인 경우는 최고 20점, 5개인 경우에는 25점이 부여된다. 보안지표의 등급별 점수에 따라서 보안변수에 대한 평가등급 기준은 <표 4>와 같이 결정할 수 있다.

<표 4> 보안변수에 대한 평가등급의 예

구 분	등급 기준	총계	등급
구성원 (4/요소, 총 20점)	4.5초과	18점 초과	1
	3.5초과	14점 초과	2
	2.5초과	10점 초과	3
	1.5초과	6점 초과	4
	1.5이하	6점 이하	5

마지막으로 최종 보안평가 등급과 점수를 산출하기 위해서 종합평점 산출기준을 결정해야 한다. 종합평점 산출기준은 보안변수별 평점에 가중치를 감안하여 100점 만점으로 환산하여 결정한다. 보안변수별 가중치를 활용한 종합평점(Total Sum) 산출 공식은 다음과 같다.

$$TS = \sum_{i=1}^{n} [S_i \times (W_i / FS_i)]$$

여기서, n은 보안변수 개수, S는 보안변수별 점수, W는 가중치, FS는 보안변수별 만점을 나타낸다. 위의 표 2, 3, 4를 참조하여 종합평점 산출 공식을 서술하면 다음과 같다.

종합평점 = [보안계획×(10/15)]+[구성원×(20/20)]+[보안시설×(10/15)]+[문서×(20/15)]+[정보통신×(40/25)]

만약 종합등급 1등급을 부여할 수 있는 종합평점 기준을 산출하면 아래와 같으며, 이러한 방식으로 2~5등급의 종합평점 기준을 구할 수 있다. 등급별 종합평점은 <표 5>와 같다.

1등급 종합평점 기준 =
[14×(10/15)]+[18×(20/20)]+[14×(10/15)]+[14×(20/15)]+[23×(40/25)]
= 9.3+18+9.3+18.7+36.8 = 92.1이상

<표 5> 등급별 종합평점 기준

등 급	1등급	2등급	3등급	4등급	5등급
점 수	92.1이상	73.7이상	52.1이상	32.2이상	32.2미만

재평가 대상 결정은 등급별 종합평점 기준으로 조직의 특성과 보안수준을 감안하여 재평가 기준을 설정한 후 결정한다. 통상적으로 4등급 이하는 재평가를 실시한다.

4. 결론

SAM은 조직에서 보안평가 결과값에 영향을 줄 수 있는 보안변수들을 선별하고 보안변수를 구성하는 보안지표들을 선택한다. 보안변수와 보안지표는 조직에서 주성분 요소로 작용하고 보안수준과 밀접한 관련이 있는 구성요소들로 선별한다. 각 보안지표들은 평가등급 선정 방식에 의하여 등급과 점수가 부여되고 보안지표들의 결과값을 종합하여 보안변수의 등급과 점수를 산출한다. 여기서 보안지표의 종합등급은 평균과 표준편차를 이용하여 산출하며, 평균으로부터 표준편차의 배수(0.5 및 1.5배)에 해당하는 만큼 멀어진 거리에 비례하여 양호 또는 불량한 등급을 받도록 설계하였다. 보안변수들에 가중치 선정은 현재 공공기관에서 수행하고 있는 보안감사의 분야별 점수를 비례하여 산출한 것으로 가중치에 대한 객관성을 보장해 준다. 최종 종합점수는 종합평점 산출 공식에 의해서 산출되며, 그 점수로 보안등급을 평가받는다.

SAM은 보안지표의 선정, 보안변수별 가중치의 부여, 보안지표별 등급구간 설정방식 등에 있어 통계적 기법을 활용함으로써 비교적 객관성 있는 결과를 유도한다. 아울러 조직의 규모와 특성에 따라 보안변수와 보안지표를 조정할 수 있기 때문에 확장성이 좋으며, 입력변수에 통계적 방법과 설문지기법을 활용하여 얻는 지표별 수치만 대입하면 되기 때문에 사용 용이성도 우수하다.

참고문헌

[1] 엄정호 외 3명, “사이버 공격과 보안 기술” 홍릉과학출판사, pp.3-9, 2009.

[2] 엄정호 “국방 정보통신기반체계의 보안관리를 위한 효율적인 위험분석 모델에 관한 연구” 석사학위논문, 성균관대학교, 컴퓨터공학과, 2003.

[3] 엄정호 외 3명, “정보시스템의 체계적인 위험관리를 위한 실용적인 위험감소 방법론에 관한 연구”, 정보처리학회 논문지 C 제10-C권 제2호, 2003.

[4] ISO/IEC SC 27/WG2, “Information Technology-Security techniques-Guidelines for the management of IT security-Part1:Concepts and models of IT Security”, TR 13335-1, 1996.

[5] “A Guide to Security Risk Management for Information Technology Systems″, MG-2, CSE Manual, 1996.

[6] Edward Rarkely, “Risk Assessment Methodology NISTIR 4325″, NIST, 1990.

[7] 김영기, 정신동, “SCOR 모형을 활용한 상호저축은행의 조기경보시스템 연구” 한국금융연구, 제19호 제1호, pp.35-71 Jan, 2005.

[8] 정신동, “금융감독원 조기경보시스템의 발전방향”, 한국경제학회지 제2008권 단일호, pp.1-32, Jan, 2008.

[9] “*2007 E-Crime Watch Survey-Survey Results*”, CSO magazine, The U.S Secret Service and CERT, 2008.