디지털산업정보학회 논문지 제5권 제4호-2009년 12월

보안 안전성을 위한 자동화 보안진단평가 시스템에 관한 연구

엄 정 호* · 박 선 호** · 정 태 명***

A Study on Automatic Security Diagnostic Evaluation System for Security Assurance

Eom, Jung Ho · Park, Seon Ho · Chung, Tai M.

〈Abstract〉

In the paper, we designed an automatic security diagnostic evaluation System(SeDES) based on a security diagnostic evaluation model(SeDEM) for an organization's security assurance. The SeDEM evaluates a security level of an organization quantitatively by a security evaluation formula which is composed of security variables and security index as applying the statistical CAEL model for evaluate risk level of banks. The SeDES has a good expandability as changing security variables according to an organization scale, characteristics and so on. And it also has a excellent usage because it inputs only numeric data got from statistical technique to security index. We can understand more a security level correctly than the existent risk assessment system because it is possible to assess quantitatively with an security grade as well as score. analysis.

Key Words : Security Evaluation, SeDEM, SeDES

Ⅰ. 서론

지난 7월초에 분산서비스거부공격(DDoS)이 16개국 86개 IP를 통해 국가 주요기관 전산망을 대상으로 발생하여 3일간 전산망이 마비되었고 좀비 시스템으로 이용되었던 PC들은 하드웨어의 데이터가 삭제되는 피해를 입기도 하였다[1]. 이는 조직을 위한 보안정책을 올바르게 수립하지 않았거나 보안 장비를 설치하지 않아서가 아니라 보안에 관련된 요소들에 대한 취약성 분석이나 위험평가, 보안진단평가 등의 보안예방활동을 주기적으로 수행하지 않음으로써 발생하였는지도 모른다.

현대사회에서 산업기술 정보에 대한 가치가 금전적 가치보다 높아짐에 따라 회사나 기관에서 근무하는 내부자가 보다 나은 직장이나 금전적 이익을 위해 정보를 유출시키는 보안사고가 사회에 심각한 보안문제로 대두되고 있다. 이렇게 됨에 따라 기업이나 정부기관의 중요 데이터와 정보자산을 보호하고 보안사고의 피해를 최소화하기 위해 사전에 취약점을 식별하고 보안수준을 측정하는 보안진단평가 방법에 대한 관심이 증가되고 있다[2].

위험평가나 취약성 평가는 조직의 보안과 연관된 요소들을 대상으로 위험분석이나 취약성분석을 통하여 조

* 대한민국 공군 장교
** 성균관대학교 컴퓨터공학과 박사과정
*** 성균관대학교 컴퓨터공학과 교수

직의 위험 및 취약 수준을 평가한 후 그에 맞는 정책이나 대책을 수립하는 것이다[3-5]. 조직의 전체적인 보안진단 평가를 위해서는 보안과 연관된 모든 평가 대상 항목인 보안변수들을 선별하고 이에 포함되는 세부평가 대상 항목인 후보 보안지표들을 선정해야 한다. 그래서 조직의 보안수준을 정확히 파악할 수 있도록 보안변수와 보안지표를 이용해서 보안진단평가를 수행해야 한다. 본 논문에서는 조직의 총체적인 보안진단평가 모델(Security Diagnostic Evaluation Model)을 기반으로 자동화 보안진단평가 시스템(Security Diagnostic Evaluation System)을 개발하였다. 본 논문은 2장에서 관련연구, 3장에서는 SeDES, 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 TR-13335

TR-13335[9]는 조직의 위험분석에 적용될 전략을 기본적으로 4가지 방법으로 분류하고 있으며, 이 중에서 혼합 위험분석 접근법을 많이 사용하고 있다. TR-13335의 주 위험분석 대상은 정보시스템이며, 자동화 도구로 개발이 가능하다. 혼합 위험분석 접근법은 조직의 목표에 치명적일 정도로 높은 수준의 위험에 노출된 정보시스템을 확인하고, 이에 대한 조치를 취하여 이 시스템을 위한 세분화된 위험분석을 수행하고, 그 이외의 정보 시스템에 대해서는 기본통제 방법을 적용시키는 혼합 접근법이다. 일반적으로 위험분석이라는 것은 세분화된 위험분석 방법인 상세 위험분석 방법을 의미한다. 상세 위험분석은 자산분석, 취약성분석, 위협분석, 대응책분석을 수행한 후 위험을 산출하는 것이다. 이 때 위험을 산출하는 방법은 5등급으로 산출하는 Matrix Scaling 방법을 사용한다. 이 후에 대응책을 선정하고 비용효과분석을 통하여 대응책을 적응하였을 때의 비용 대 효과를 분석한다. 마지막으로 잔류 위험평가를 수행하게 된다. 위험 산출 방법인 Matrix Scaling 기법은 1등급에서 5등급까지 분류되며, 평가는 Very Low, Low, Medium, High, Very High로 평가된다.

2.2 CSE MG-2 Manual

CSE MG-2[10] 위험분석 매뉴얼은 민감한 시스템 자산을 식별하고 자산들이 위협 에이전트에 의해 어떻게 침해될 수 있는지를 식별하며, 위협 에이전트가 자산에 가져다 줄 수 있는 위험수준을 평가하는 방법론이다. 프로세스는 준비 및 계획, 데이터 수집, 정책 및 표준 이행 여부 분석, 자산 민감도 분석, 위협 분석, 취약성 분석, 위험 분석, 위험수용 확률 평가, 최종 위험평가 보고서 전달로 구성되어 있다. CSE MG-2 매뉴얼도 취약성 심도와 노출 정도를 Matrix Scaling 기법으로 취약성 수준을 산출하고, 취약성 수준과 위협 발생 확률을 가지고 위협수준을 5단계로 구분하여 위험을 평가한다.

기존의 위험분석 방법들은 대부분 Matrix Scaling이나 전문가를 활용한 델파이 기법을 많이 사용하고 있어서 구체적으로 점수제로 결과를 원하는 평가방식에는 적합하지 않다.

2.3 보안진단평가 모델

보안진단평가 모델(SeDEM: Security Diagnosis Evaluation Model)은 기업이나 조직의 총체적인 보안수준을 통계적 CAEL 모델[6-7]을 이용하여 정량적으로 평가할 수 있는 모델이다. 네트워크나 시스템과 같은 정보통신체계 뿐만 아니라 시설, 문서, 구성원 등과 같이 조직에 포함되어 있는 모든 구성요소들에 대하여 부문별 평가 및 종합적인 보안평가 등급과 점수로 보안수준을 측정한다. SeDEM의 수행절차는 <그림 1>과 같다.

① 보안변수 분류

보안변수는 보안진단평가에 필요한 필수 요소로 조

<그림 1> SeDEM의 절차

직의 보안 수준과 위험에 영향을 미칠 수 있는 다양한 요소들을 대상으로 분류한다. 특히, 내·외부로부터 위협에 노출되어 있는 요소들을 식별해야 한다. SeDEM은 국방부가 예하부대를 대상으로 시행하는 정기 보안감사 평가요소[8]을 개선하여 계획, 구성원, 문서, 시설, 정보통신으로 분류한다.

② 보안지표 선정

보안변수별로 보안지표를 선정한다. 우선 주성분 분석을 통해 조직의 보안 상태나 위험수준에 영향을 미칠 수 있는 보안지표를 선별하고, 보안평가 결과에 "+"로 적용되는 지표나 "-"로 적용되는 지표들을 구분해야 한다. 예를 들면, 보안계획에서 보안행사 참여율은 높으면 높을수록 좋으나, 정보통신 분야에서 네트워크 침해율은 낮으면 낮을수록 좋은 요소로 작용한다. <표 1>은 SeDEM의 보안변수별 보안지표의 예를 보여준다.

③ 평가등급 설정

SeDEM은 CAEL 평가방법처럼 통계적 기준에 의한 보안변수별 등급구간을 설정하기 때문에 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.

<표 1> 보안변수별 보안지표

보안변수	보 안 지 표
계획보안	정기 보안업무 계획 수립율, 보안진단평가 시행율, 보안세미나/행사 개최율, 보안규정/규칙 보유현황 등
인원보안	보안교육/회의/행사 참석율, 보안퀴즈 평균점수, 보안위규자수, 보안관련 직책 임명율, 업무만족도, 정기 보안업무 실천율 등
시설보안	CCTV 설치율, 사무실 관건율, 개인 책상/비품 관건율 등
문서보안	문서방치건수, 중요문서 분실건수, 문서보관함 관건율 등
정보통신보안	네트워크 침해율, 비인가 저장장치 적발건수, 보안 프로그램 미설치율, PC비밀번호 미설정율, 전자문서 비밀번호 미설정율, 비인가 시스템 접속율 등

<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

보안등급에 의한 평가는 조직의 보안수준을 추상적으로 제시함으로써 구체적인 보안수준에 대한 세부 결과값을 제시할 수 없는 단점이 있다. 예를 들어 두 개의 조직의 최종 보안평가가 2등급으로 동일하다면, 어떤 분야의 어떤 보안지표가 우수하다거나 미흡하다는 것을 구별할 수 없다. 그래서 SeDES에서는 보안지표의 평가결과가 정량적으로 표현 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 3에 의해 보안변수별 보안지표가 4개인 경우는 최고 20점, 5개인 경우에는 25점이 부여된다. 예를 들어 인원에 대한 보안지표가 3개일 경우, 평가등급 기준은 <표 4>와 같다.

<표 4> 보안변수에 대한 평가등급의 예

구 분	등급판정 기준	구성요소별 총계	등급
인원 (3/요소, 총 15점)	4.5초과	13.5점 초과	1
	3.5초과	10.5점 초과	2
	2.5초과	7.5점 초과	3
	1.5초과	4.5점 초과	4
	1.5이하	4.5점 이하	5

④ 보안변수 가중치 결정

국방부 보안감사에서는 보안계획 10%, 구성원 20%, 보안시설 10%, 문서 20%, 정보통신 40%로 수준으로 가중치를 분류한다. SeDEM에서는 보안변수의 선택에 따라 주성분 평가를 통하여 가중치를 적용한다.

⑤ 최종 보안평가

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.

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

여기서, n은 보안변수 개수, S는 보안변수별 점수, W는 가중치, FS는 보안변수별 만점을 나타낸다.

위의 공식을 이용하여 종합등급 및 평점 기준을 산출하면 <표 5>와 같다.

<표 5> 등급별 종합평점 기준의 예

등 급	1등급	2등급	3등급	4등급	5등급
점 수	90이상	70이상	50이상	30이상	30미만

Ⅲ. 보안진단평가 시스템

본 논문에서 제시한 자동화 보안진단평가 시스템(Security Diagnosis Evaluation System)은 보안진단평가 모델(SeDEM)을 기반으로 수학적 통계 공식을 이용하여 조직의 보안수준을 평가한다. SeDES의 특징은 다음과 같다.

첫째, 보안 수준을 정확하게 알 수 있도록 등급과 점수로 결과가 나타내는 정량적 평가를 수행한다. 기존의 위험분서 도구[9]의 보안수준 평가방법(높음, 보통, 낮음 등)으로는 구체적인 보안수준 평가가 어렵다. 예를 들어 보안평가 결과가 '보안수준 낮음'과 '보안수준이 45점으로 4등급'은 보안 관리자에게 후속조치를 취하는 데 전혀 다른 정보를 제공한다.

둘째, 보안평가 대상의 규모, 특성 등에 따라서 보안변수나 보안지표를 변경할 수 있는 확장성이 우수하다. 부서별 보안평가와 자회사별 보안평가 요소는 전혀 다르다. 예를 들어, 기업내 부서별 보안평가에는 연간 보안업무 수립 현황 등이 포함되어 있는 계획보안 요소는 불필요하기 때문에 평가 보안지표에서 제외할 수 있다.

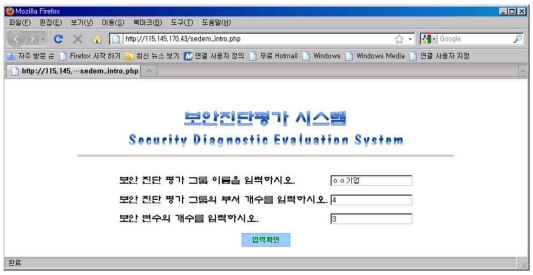
셋째, 보안 감사자가 쉽게 활용할 수 있는 사용 용이성이 우수하다. SeDES는 통계적 산술 공식을 이용한 보안진단평가모델(SeDEM)을 기반으로 하여 입력이 요구되는 수치만 대입하면 보안평가 결과를 쉽게 얻을 수 있다. 예를 들어, 정보통신보안 평가시 보안지표인 비인가 저장장치 적발건수, PC비밀번호 미설정율, 전자문서 비밀번호 미설정율은 보안점검시 식별한 횟수와 비율을 확인하여 입력만 하면 된다.

마지막으로 보안평가 항목의 중요도를 고려하여 보안변수에 가중치를 적용해야 한다. 예전에는 시설이나 문서에 대한 물리적 보안을 강조하였으나, 최근에는 시스

템과 네트워크 기술이 발달함에 따라 정보통신에 의한 업무 의존도가 높고 정보 유출 빈도수도 증가하고 있기 때문에 정보통신에 해당되는 보안지표에 대한 보안진단 평가에 가중치를 적용하여 평가한다.

3.1 SeDES의 수행절차

기업을 예를 들어 SeDES를 적용하여 평가한다. 우선 기업의 부서는 기획실, 인사부, 개발부 그리고 행정실이며, 주로 기획, 제품 개발, 인사, 행정업무를 다룬다. 본 논문에서 모델의 평가는 한 기업내에 부서간의 보안 평가를 수행하기 때문에 기업의 자회사간의 보안평가를 수행할 때 적용되는 계획보안, 시설보안 항목의 보안변수는 제외한다. <그림 2>는 SeDES의 초기화면을 보여준다.

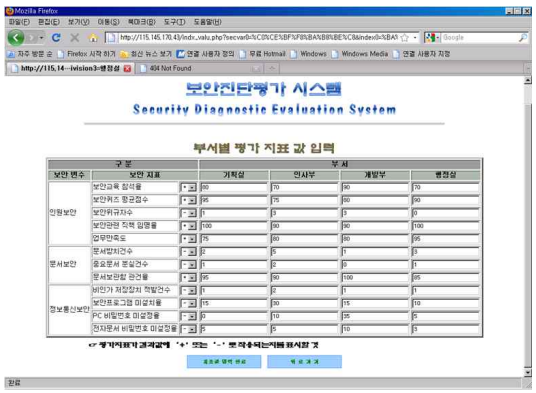


<그림 2> SeDES의 초기화면

<표 6>은 선택된 보안변수와 보안지표를 보여주며, 아래 <그림 3>은 보안지표별 점수 입력 화면이다.

<표 6> 보안변수 및 보안지표 선정

보안변수	보 안 지 표
인원보안	보안교육 참석율, 보안퀴즈 평균점수, 보안위규자수, 보안관련 직책 임명율, 업무만족도
문서보안	문서방치건수, 중요문서 분실건수, 문서보관함 관건율
정보통신 보안	비인가 저장장치 적발건수, 보안프로그램 미설치율, PC비밀번호 미설정율, 전자문서 비밀번호 미설정율



<그림 3> 부서별 보안지표 값 입력

보안지표에서 “+”와 “-” 표시는 보안지표의 값이 높을수록 양호한 구성요소와 낮을수록 양호한 구성요소를 구별시켜 준다.

<그림 4>는 부서별 보안지표 값을 입력시켜 SeDEM 모델의 공식에 의해 부서/보안변수별 결과값을 보여준다. 즉, 평가등급 설정단계에서 보안지표 평가등급 설정기준에 의하여 등급을 설정하고 등급에 따라서 <표 3> 등급별 점수 산정 테이블에 의하여 점수로 환산한다. 그리고 <표 4> 보안변수에 대한 평가등급 테이블에 따라서 보안변수별 등급과 점수를 산출한다.

부서별 평가 등급 및 점수

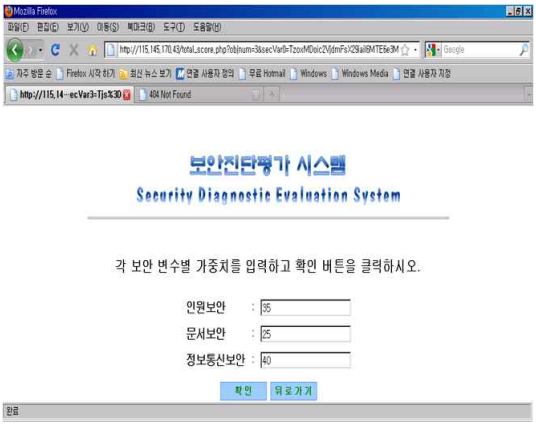
구 분	부서			
	기획실	인사부	개발부	행정실
인원보안	3(17)	4(11)	3(14)	2(19)
문서보안	3(10)	4(6)	2(12)	3(8)
정보통신보안	3(14)	4(8)	4(9)	2(16)

(괄호 안은 점수를 의미함)

<그림 4> 부서/보안변수별 결과값

최종 보안진단평가 결과를 산출하기 위해서 가중치를 적용하여 결과를 산출한다. 가중치는 조직의 특성과 보안변수의 중요도에 따라서 결정할 수 있으며, 내부자 및

정보통신 위협의 증가에 따라 가중치를 차등 적용하였다. <그림 5>는 가중치 적용을 보여준다.



<그림 5> 보안변수별 가중치 적용

<그림 6>에서는 종합평가등급 기준과 최종 부서별 보안평점과 등급을 보여준다.

<그림 6> 최종 보안진단평가 결과

최종 종합평가 기준은 공식 ①의 $TS = \sum_{i=1}^{n}[S_i \times (W_i / FS_i)]$ 와 표 10을 이용하여 등급기준 점수를 산출한다. 예를 들어 1등급 기준 점수를 구하면 아래와 같이 구할 수 있다. 인원보안 요소는 5개로 1등급은 20점 이상이며, 문서보안은 3개로 13.5점 이상, 정보통신 보안은 4개로 18점 이상이다.

$$\begin{aligned} \textit{1등급 기준} &= [\textit{인원}\times(35/25)]+[\textit{문서}\times(25/15)] \\ &\quad +[\textit{정보통신}\times(40/20)] \\ &= [22.5\times(35/25)]+[13.5\times(25/15)] \\ &\quad +[18\times(40/20)] = 90 \end{aligned}$$

부서별 평가 점수는 공식 ①과 <그림 4>를 이용하여 구하고, 종합평가 기준에 의하여 등급을 산정하면 된다.

최종 보안진단평가 결과로 행정실은 71.93점으로 2등급이며, 인사부는 41.4점으로 4등급이다. 행정실의 최종 보안진단평가는 다음과 같다.

$$\begin{aligned} \textit{행정실 보안평가} &= [19\times(35/25)]+[8\times(25/15)] \\ &\quad +[16\times(40/20)] \\ &= 71.93 \end{aligned}$$

인사부는 각 보안변수별로 보안대응책을 재정비해야 하며, 개발부도 비록 3등급이나 종합평점이 57.6으로 낮기 때문에 다시 한 번 보안정책이나 대책에 대해서 점검할 필요가 있다.

이러한 점수와 등급에 의한 보안평가 방법은 ISO/IEC TR13335[9]이나 BS-7799[11] 등에서 수행하는 위험분석 결과로 5등급(Very High, High, Medium, Low, Very Low)로 산출하는 것에 비해 좀 더 구체적이고 정확하게 조직의 보안수준을 평가할 수 있는 장점이 있다.

3.2 SeDES 평가

ISO/IEC TR13335[9], 캐나다 CSE MG-2[10], BS-7799[11] 등의 위험분석 및 취약성평가 모델은 주로 5등급의 보안 등급과 수준으로 평가하여 정량적인 평가보다는 정성적인 평가에 가깝다. 예를 들어 결과값이 보안

<표 7> 보안평가 모델 및 시스템의 비교

구 분	ISO/IEC TR13335	CSE MG-2 Manual	SeDES
설계 목적	위험분석 표준 제시	위험평가	보안진단/평가
평가 방법	정성	정성	정성/정량
평가 대상	조직/정보시스템	정보시스템	조직/정보시스템
평가대상 선택	델파이 방법	델파이 방법	주성분 분석
평가대상 가중치 선정	자산 종속	자산 종속	보안지표 종속
분석 방법	Matrix Scaling	Matrix Scaling	통계적 CAEL 분석
평가 결과	등급	등급	등급/점수
객관성	위험분석팀에 의존	위험평가팀에 의존	자동화 평가도구에 의존

등급은 '2등급'이며, 보안수준은 'HIGH'라고 한다면, 더 이상 그 부서에 대해서는 보안정책이나 대책을 점검하지 않을 것이다. 그렇게 된다면, 그 부서는 앞으로 평가대상의 요소들 중에서 취약점이 발견되거나 기존의 취약점이 좀 더 약하게 될 것이다. 그러나 SeDES에서는 보안지표, 보안변수별 점수가 산출되고 종합평점을 구할 수 있어서 높은 등급일지라도 정확한 보안수준의 상태를 파악할 수 있고 보안지표별 보안대책을 마련할 수 있게 된다. <표 7>은 SeDES을 TR13335, CSE MG-2와 비교한 것이다.

Ⅳ. 결론

본 논문은 조직에 대한 총체적인 보안수준을 평가할 수 있는 보안진단평가 모델(SeDEM)을 기반으로 설계한 자동화 보안진단평가 시스템에 대해 설명하였다.

SeDES는 조직에서 보안관련 주성분 요소로 작용하는 보안변수들을 보안평가 대상 항목을 선별하고, 보안변수를 구성하는 세부 항목을 보안지표로 선택하여 요소별 평가할 수 있다. 각 보안지표들의 평가는 SeDEM에 의해서 등급과 점수가 부여되고, 보안지표들의 결과값을 종합하여 보안변수의 종합등급과 점수를 산출한다.

SeDES는 보안지표의 선정, 보안변수별 가중치의 부여, 보안지표별 등급구간 설정방식 등에 있어 통계적 기법을 활용하여 정량적이고 구체적인 결과를 산출한다. 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] http://www.hani.co.kr/arti/society/society_general/364809. html, 2009.

[2] 엄정호 외 3명, "사이버 공격과 보안 기술," 홍릉과학출판사, 2009, pp. 3-9.

[3] 엄정호 "국방 정보통신기반체계의 보안관리를 위한 효율적인 위험분석 모델에 관한 연구," 석사학위논문, 성균관대학교, 컴퓨터공학과, 2003.

[4] 김신원, "정보시스템 보안 위험분석 모델에 관한 연구," 서강대학교, 정보통신대학원, 석사학위논문, 2001.

[5] "Risk Analysis and Management Standards for Public Information Systems Security-Risk Analysis Methodology Model," 한국정보통신기술협회(TTA), 2000. Richard Fairley, "Risk management for software projects," IEEE Software, Vol. 11, No. 3, 1994, pp. 57-67.

[6] 김영기, 정신동, "SCOR 모형을 활용한 상호저축은

행의 조기경보시스템 연구," 한국금융연구, 제19호 제1호, Jan, 2005, pp. 35-71.

[7] 정신동, "금융감독원 조기경보시스템의 발전방향," 한국경제학회지 제2008권 단일호, Jan, 2008, pp. 1-32.

[8] 국방부, "군사보안시행규칙," 국군 인쇄창, 2009.

[9] 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.

[10] "*A Guide to Security Risk Management for Information Technology Systems,*" MG-2, CSE Manual, 1996.

[11] "*BS 7799-Guide to Risk Assessment and Risk management,*" BSI, 1998.

■ 저자소개 ■

엄 정 호
Eom, Jung Ho

1994년~현재
대한민국 공군
2008년 성균관대학교 컴퓨터공학과(박사)
2003년 성균관대학교 컴퓨터공학과(석사)
1994년 공군사관학교 항공공학과(학사)

관심분야 : 사이버전, 사이버보안, 접근제어, 위험분석
E-mail : eomhun@gmail.com

박 선 호
Park, Seon Ho

2007년~현재
성균관대 전자전기 컴퓨터공학과 박사과정
2007년 성균관대학교 컴퓨터공학(석사)
2005년 성균관대학교 정보통신 공학부(학사)

관심분야 : 접근제어, 네트워크 보안
E-mail : shpark@imtl.skku.ac.kr

정 태 명
Chung, Tai M.

1995년~현재
성균관대학교 컴퓨터공학과 교수
1995년 Purdue University W. Lafayette, IN, U. S. A. 컴퓨터공학 졸업(박사)
1987년 University of Illinois Chicago IL, U. S. A. 컴퓨터공학과 졸업(석사)
1984년 University of Illinois Chicago IL, U. S. A. 전자계산학과 졸업(학사)
1981년 연세대학교 전기공학과 졸업(학사)

관심분야 : 통합보안관리, 네트워크, 무선망
E-mail : tmchung@ece.skku.ac.kr

논문접수일 : 2009년 10월 19일
수 정 일 : 2009년 11월 10일
게재확정일 : 2009년 11월 19일