通信情報保護學會論文誌
第 8 卷 第 3 號, 1998. 9

다중보호대책에 대한 보안성 평가모델

오 경희*, 홍 기웅*, 심 주걸*

A Security Evaluation Model on Multiple Protection Countermeasures

KyeongHee Oh*, KiYoong Hong*, JooGeol Sim*

요 약

본 논문에서는 다중보호대책으로 구성된 정보보호시스템의 보호효과를 평가하기 위한 새로운 모델을 제안한다. 제안한 모델은 정보보호시스템이 요구되는 보호수준에 부합하는지 결정할 수 있게 하며, 또한 구축된 정보보호시스템의 위험분석을 위하여 활용될 수 있다.

Abstract

In this paper, a new model is proposed to evaluate the protection effectivieness of security systems that consist of multiple protection countermeasures. The proposed model enables to determine if the security system is appropriate to meet the level of protection. It can be also applied to risk analysis of the installed security system.

Key word : Security Evaluation, Protection Effectiveness, Risk Analysis

1. 서 론

오늘날 점차 증가하고 있는 해킹을 비롯한 각종의 정보화 역기능에 대응하기 위하여 각종의 정보보호시스템이 개발되고 있으며 사용자 측에서는 자신의 조직이나 기관에 적합한 정보보호시스템을 선정하여 활용하고 있다. 존재하는 위협과 그로부터 보호해야 할 자산가치에 적절한 보호기능을 지닌 신뢰할 수 있는 정보보호시스템을 도입하기 위해서는 개발된 정보보호시스템이 실제로 존재하는 위협에 어느 정도 대처할 수 있는지, 그리고 해당 조직

* 한국정보보호센터

의 정보자산의 특성과 가치에 적정한 대책은 어떤 것들이 있는지를 평가할 수 있는 척도나 지침이 필요하다.

정보보호시스템의 보안기능과 신뢰성을 평가하고자 하는 측면에서는 1983년에 미국의 TCSEC[DOD83]으로부터 시작하여 유럽의 ITSEC[HC91] 캐나다의 CTCPEC[CSE93]을 거쳐 1998년 5월에 최종 버전이 발표된 CC[CCIB98]에 이르기까지 정보보호시스템의 평가를 위한 기준을 개발하고 이에 따라 각종의 정보보호시스템을 평가, 인증하는 노력이 진행되고 있다. 국내에서도 1998년 2월에 정보통신망침입차단시스템 평가기준[정통부98]을 고시하여 이에 따라 평가가 진행되고 있으며 한편으로 모든 정보보호시스템에 적용할 수 있는 정보보호시스템 평가기준을 개발하고 있는 중이다. 이러한 평가는 필요한 보안기능 요구사항을 명시할 수 있어 사용자의 요구와 평가 결과를 비교할 수 있고 또한 보증에 필요한 요소도 비교할 수 있어 사용자가 자신의 필요에 적합한 제품을 선정하고자 할 때 도움을 준다. 그러나 평가결과가 평가등급의 형태로 나타나기는 하지만 이러한 정보보호시스템을 사용할 경우와 그렇지 않을 경우의 보호효과의 차이를 정량적으로 보여주지는 못한다.

한편 조직의 보안 위험수준을 평가하고 필요한 보호대책을 선정하기 위한 위험분석 및 위험관리에 관한 연구에서는 정보시스템 및 정보통신망에 대한 위협과 취약성을 식별하고 이들이 자산에 끼치는 위험을 정성적 또는 정량적으로 분석하여 위험을 받아들일 수 있는 수준으로 축소시키기 위한 해결책을 선정하기 위한 방법론을 제시하고 있다. 이 분야는 1970년대부터 꾸준한 연구가 진행되어서 최근에는 ISO/IEC JTC1/SC27/WG1의 정보기술의 보안관리 지침(Guidelines for the Management of IT Security)[ISO97]중에서 위험관리 방법론에 대한 지침이 제시되고 있으며 미국[DOC80], 캐나다[CSE96]의 관련 기관에서는 자체적으로 개발한 위험관리 및 분석에 대한 방법론을 이용하여 조직의 위험분석에 적용하도록 권고하고 있다.

그러나 지금까지 개발된 위험분석의 방법론은 개괄적이며 단계적인 방법론을 제시하는 수준에서 이루어지고 있어 구체적인 분석 단계에서 따를 수 있는 상세한 절차가 부족하다. 또한 조직의 차원에서 위험을 파악하기 때문에 기존의 물리적, 절차적 위협에 대한 측면은 많은 연구가 이루어져 있으나 특히 최근에 급격히 증가하고 앞으로도 계속 비중이 높아질 것으로 예측되고 있는 기술적인 위협에 대한 분석은 상대적으로 부족한 편이다[Clayton97]. 이러한 기술적인 대책을 다룬 연구로는 침입차단시스템의 위험분석을 수행한 것이 있으나[Drake96, Bodeau92] 일반적인 정보보호시스템에 적용하기에는 미비하며 조직의 위험분석 측면에서 접근하였기 때문에 조직에 설치되기 전의 정보보호시스템의 정량적인 보호효과를 측정하기에 적합한 모델은 없다.

따라서 본 논문에서는 기존의 방법으로는 평가할 수 없었던 다중보호대책으로 구성된 정보보호시스템의 보호효과(PE : Protection Effectiveness)를 평가하기 위하여 새로운 모델 PEMM(Protection Effectiveness Measurement Model)을 제안한다. 이러한 모델을 통하여 측정된 보호효과는 정보보호시스템을 선정할 경우 서로 비교하는데 이용할 수 있으며 또한 위험을 최소한의 수준으로 낮추는데 어느 정도 기여할 수 있는지를 측정할 수 있다. 또한 이 보호효과 평가모델을 확장하여 구체적인 운영환경에 설치된 정보보호시스템의 위험분석에도 이용할 수 있다.

2. 기존의 관련 연구 조사 분석

2.1 정보보호시스템의 평가

선진 각국은 정보보호 기술을 일반 사용자가 안전하게 사용할 수 있도록 보증하기 위하여 정보보호시스템 보안기능의 성능과 신뢰도에 대한 요구사항들을 평가기준으로 개발하고 이에 따라 각종의 정보보호시스템을 평가하여 평가된 제품의 목록을 유지함으로써 사용자들이 자신들의 요구사항에 적합한 제품을 믿고 사용할 수 있게 제공하고 있다.

미국의 TCSEC[DOD83] 및 FC[NIST92], 캐나다의 CTCPEC[CSE93], 유럽의 ITSEC[HC91], 국제 표준화 중인 CC[CCIB98] 평가기준을 보증측면에서 비교한 것을 다음의 (그림 1)에 보였다. 그림에서 나타나는 바와 같이 등급체계가 다르다 하더라도 요구사항은 비슷한 수준으로 나타나고 있어 이러한 유사성이 CC 개발의 바탕이 되고 있다.

이러한 평가는 필요한 보안기능 요구사항을 명시할 수 있어 사용자의 요구와 평가 결과를 비교할 수 있고 또한 보증에 필요한 요소도 비교할 수 있어 사용자가 자신의 필요에 적합한 제품을 선정하고자 할 때 도움을 준다. 그러나 평가결과가 평가등급의 형태로 나타나기는 하지만 이러한 정보보호시스템을 사용할 경우와 그렇지 않을 경우의 정량적인 보호효과의 차이를 보여주지는 못한다.

미 국				캐나다	유 럽		국 제		한 국
TCSEC		FC		CTCPEC	ITSEC		Common Criteria		침입차단 시스템 평가기준(안)
		PP	보증						
D	최소한의 보호				E0	부적절한 보증	EAL0	부적절한 보증	K0
							EAL1	기능시험	K1(E)
C1	임의적 보호				E1, F-C1	비정형적 기본설계	EAL2	구조시험	K2(E)
C2	통제된 접근보호	CS-1	T1	T1	E2, F-C2	비정형적 상세설계	EAL3	방법론적 시험과 점검	K3(E)
B1	레이블된 보호	LP-1 CS-2 CS-3	T1 T2 T3	T2 T3	E3, F-B1	소스코드와 하드웨어 도면 제공	EAL4	방법론적인 설계, 시험 및 검토	K4(E)
B2	구조적 보호	LP-2	T5	T4	E4, F-B2	준정형적 기능명세서, 기본설계, 상세설계	EAL5	준정형적 설계 및 시험	K5(E)
B3	보안 영역	LP-3	T6	T5	E5, F-B3	보안요소 상호관계	EAL6	준정형적 검증된 설계 및 시험	K6(E)
A1	검증된 설계	LP-4	T7	T6 T7	E6, F-B3	정형적 기능명세서, 상세설계	EAL7	정형적 검증	K7(E)

(그림 1) 국내 외 정보보호시스템 평가기준 비교

$B < P \cdot L$

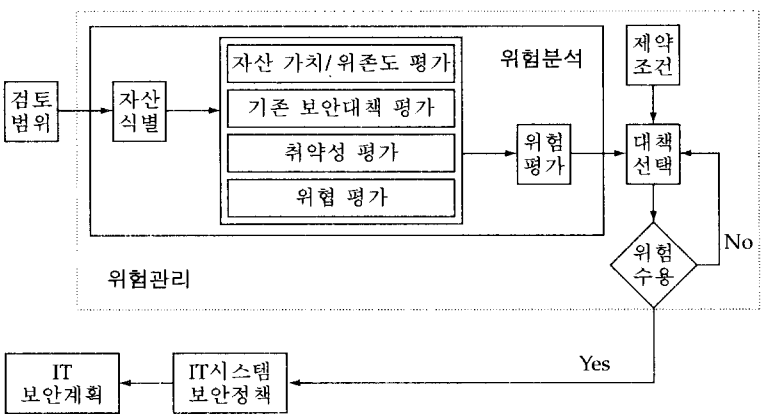
2.2 GMIT의 위험관리

위험분석은 조직의 자산에 대한 위협과 취약성을 정의하고 분석하여 보안에 대한 투자를 최적화하고자 하는 것으로 보안관리의 핵심적인 요소이다. 위험분석 및 이의 결과를 보호대책의 선택에 이용하는 위험관리의 개념은 경영학에서 시작된 것으로 정보시스템에 위험분석의 개념이 도입된 것은 1970년대 후반부터이다.

위험분석을 위하여 요소들 간의 관계를 가장 간단한 형태로 나타낸 기본 모델은 BPL 공식으로서 다음과 같은 식으로 나타낸다[White96].

이때 B는 보호대책을 구현하는데 필요한 비용이며 P는 손실이 일어날 확률이다. L은 특정 사건에 의한 총체적 손실을 나타낸다. $P \cdot L$은 위험을 의미하는 것으로 위의 식은 보호대책의 비용이 보호대책 구현 전·후에 나타나는 기대손실, 즉 위험의 차액 이하가 되는 선에서 선택되어야 한다는 것을 의미한다.

ISO/IEC JTC1/SG27/WG1에서는 정보기술의 보안관리를 위한 지침인 GMIT(Guidelines for the Management of IT Security)[ISO97]을 개발하여 마무리 단계에 와 있으며 이 지침에서는 다음의 (그림 2)와 같은 위험관리 방법을 제시하고 있다.



(그림 2) GMIT의 위험분석과 위험관리과정

또한 GMIT에서는 위험분석의 전략을 베이스라인 접근법, 비정형 접근법, 상세한 위험분석, 이들을 결합하여 일차적으로는 베이스라인 접근법을 사용하고 특정한 관심사에는 면밀한 정량적 결정을 내리는 결합 접근법 등으로 분류하여 조직의 상황에 따라 이중 하나를 택하여 수행하도록 권고하고 있다.

이러한 위험관리 방법은 전체적인 보안관리의 일부로서 개괄적인 방법론 수립에 도움을 주지만 실제 구체적인 정보보호시스템의 보호효과를 결정하기 위하여 적용하기에는 미비한 측면이 있다.

2.3 위험인덱스(Risk Index)

미 국방성에서는 TCSEC[DOD83]에 따라 평가된 정보보호시스템을 선택하기 위한 지침으로서 위험인덱스[DOD85]를 개발하였다. 위험인덱스는 시스템 사용자의 비밀등급의 최저치와 시스템에서 다루는 비밀정보의 최고치와의 차이값으로 정의되고 이에 따라 특정 등급으로 평가된 정보보호시스템을 사용하도록 권장하였다.

위험인덱스는 다음과 같이 정의된다[DOD85].

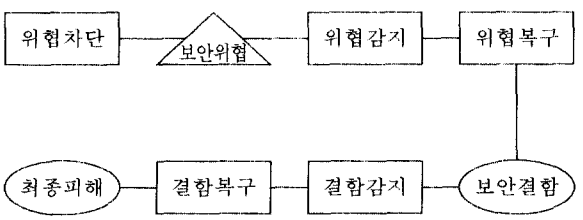
Risk Index = $R_{max} - R_{min}$, if $R_{max} > R_{min}$
= 1, if $R_{min} \geq R_{max}$ and there are categories to which some users are not authorized access
= 0, otherwise
R_{min} = the system's minimum user clearance
R_{max} = the system's maximum data sensitivity

이것은 실제 운영환경의 위험도에 따라 정보보호시스템을 선정하는데 평가 결과를 이용하는 방법을 제시하였다는데 의미가 있다. 그러나 사용자와 정보의 비밀등급만을 요인으로 고려하여 일반적인 위험분석과는 큰 차이가 있다.

미 국방성에서는 이러한 위험인덱스를 이용하여 위험인덱스 값에 따라 정해진 평가등급의 제품을 사용하도록 하였으며 응용시스템의 개발과정의 안전성에 따라 개방보안환경과 폐쇄보안환경으로 나누어 충분한 안전조치가 없이 개발된 응용시스템을 사용하는 개방보안환경에서는 더 높은 등급의 정보보호시스템을 사용하도록 하였다.

2.4 8단계 정보보호 위험분석 모델

1994년 David L. Drake와 Katherine L. Morse[Drake94]는 위협을 일련의 행위로 이루어지는 시나리오로 정의하고 위협이 시스템에 결함을 초래하고 이 결함을 시스템이 감지, 복구하는 단계를 표현한 8단계 모델을 제시하였다. 이 모델을 (그림 3)에서 보였다. 또한 1996년에는 이 모델을 침입차단시스템에 적용하여 위험분석을 수행하였다[Drake96].



(그림 3) 8단계 위험분석 모델

이 모델에서 하나의 위협 시나리오에 대하여 피해를 계산한 예를 [표 1]에서 보였다.

[표 1] 위험평가 매트릭스의 예

단 계	설 명	계 산	값
위협차단	설명, 내장 감사 모듈, 동료	CE_{TO}	.25
위협 시나리오	부패한 사용자가 많은 사본을 출력	PR_T	.05
위협감지	감사, 동료, 감독자	CE_{TR}	.9
위협복구	ISSO 감사, 동료, 감독자	CE_{TR}	.9
보안결함	용지 비용	$ER_B = PR_T \times (1-CE_{TO} \times CE_{TD} \times CE_{TR}))$ PL_B $EL_B = ER_B \times PL_B$	.04 = .05×(1-.25×.9×.9)) $0.25 $0.01 = .14×$0.25
결함감지	감사, 동료, 감독자	CE_{BD}	.9
결함복구	ISSO 감사, 동료, 절차	CE_{BR}	.9
피해	임무수행에 실패, 인적 손실	$ER_H = (M-CEBD \times CEBR))$ PL_H $EL_N = ER_H \times PL_H$ $ER_T = ER_B \times ER_H$ $EL_T = EL_B + (ER_B \times EL_H)$	.19 = (1-.9×.9)) $1,000,000 $190,000 = .19×$1,000,000 .0076 = .04×.19 $.190,000

이 모델에서는 각 공격 시나리오에 대한 전체 예상피해액을 보안 결함의 예상피해액과 최종 피해의 예상피해액의 합으로 나타내었고 이 피해액을 모든 가능한 위협 시나리오에 대하여 총합하여 전체 시스템의 잠재 손실액으로 나타내었다.

이 모델은 의도적인 위협에 대한 정보보호시스템의 보호대책이 작용하는 과정을 모델링하였다는 의의가 있으나 각 단계의 해석 적용에 어려움이 있고 설치된 정보보호시스템의 위험분석에는 사용할 수 있으나 설치되기 이전의 정보보호시스템의 보호효과를 측정하여 비교하기에는 어려움이 있다.

3. 평가 모델

3.1 평가개념 및 용어 정의

본 장에서는 상태 전이도를 이용하여 정보보호시스템의 보호효과를 측정하기 위한 새로운 평가 모델(Protection Effectiveness Measurement Model, PEMM)을 제안한다.

정보보호시스템의 개발에서 사용되는 다중의 보호대책에는 식별 및 인증, 접근통제, 암호화, 부인봉쇄 등이 있다. 최근에는 강력한 보안이 필요할 경우 패스워드와 생체인증을 동시에 사용하는 것처럼 같은 목적의 보호대책을 복수로 채택하기도 한다.

한편 이렇게 위협이 자원에 접근하는 것을 막기 위한 대책 뿐 아니라 무결성 검사, 감사기록, 침입탐지, 백업 등 취약성이 이용되는 것을 감시하고 복구하여 피해를 제한하기 위한 보호대책도 다양하게 개발되어 사용되고 있다. 본 모델은 이러한 다중의 보호대책을 갖춘 정보보호시스템이 대상 위협에 대하여 어느 정도의 보호를 제공하는지를 평가하고자 한다.

PEMM 모델을 설명하기 위하여 먼저 몇 가지의 용어를 정의한다.

CM_i : 어떤 정보보호시스템에서 자원에 접근하기 위하여 i 번째로 거쳐야 하는 정보보호대책

$T_i = \{t_i \mid t_i$는 보호대책 CM_i에 대한 위협 사건$\}$

T = {t | t는 위협사건} $\supseteq \bigcup_i T_i$

λ_i : t_i가 발생할 확률

$\delta(t_i)$ = 1 : t_i가 CM_i를 공격하여 성공한 경우
0 : t_i가 CM_i를 공격하는데 실패할 경우 (즉, CM_i가 t_i를 차단하는 경우)

$P_{CM_i}(t_i) = Pr(\delta(t_i) = 0)$: CM_i가 임의의 t_i를 막을 확률

$\tau = (t_1, t_2, \ldots t_n), t_1 \in T_1, t_2 \in T_2, \ldots t_n \in T_n$: 위협 트랜잭션

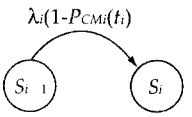
$f(\tau) = k$: τ를 구성하는 t_i에 대하여 $\prod_1^k \delta(t_i) = 1$인 최대 k, $1 \le k \le n$

$Z\{\tau\} = S_k, k = MAX(f(\tau))$: 발생한 위협 트랜잭션의 집합 $\{\tau\}$에 대한 정보보호시스템의 상태

정보보호시스템은 여러 가지 보호대책을 탑재하고 있으며 이러한 각각의 보호대책은 특정 유형의 위협에 대응하기 위한 것이다. 정보보호시스템에 식별 및 인증 기능이 설치되어 있다면 먼저 이 기능을 통과하여야만 자원에 도달할 수 있다. 이 경우, 그 보호대책에 효과가 없는 위협은 발생하여도 의미가 없다. 즉 어떤 보호대책을 CM_i로 나타냈을 때 이 CM_i를 통과하기 위한 위협사건을 t_i라 하고 이러한 위협을 모아놓은 집합을 T_i로 정의한다. 일반적으로 정보보호대책은 일련의 순서로 배치되어 자원에 대한 인가되지 않은 접근을 차단하게 된다. 이에 따라 n개의 보호대책으로 구성된 정보보호시스템은 CM_1, CM_2, .. CM_n으로 배치되어 이러한 순서로 모든 보호대책을 거쳐야 최종적으로 자원에 접근할 수 있다고 가정한다.

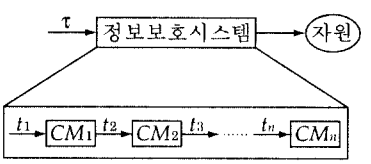
$\delta(t_i)$는 위협 t_i가 CM_i를 통과하면 1, 위협 t_i가 보호대책 CM_i에 의해 차단되면 0의 값을 갖는 함수이다. 위협 t_i는 λ의 확률로 발생하며 보호대책 CM_i는 확률 PCM_i로 위협 t_i에 대응한다. 이 PCM_i는 발생한 특정 유형의 위협 중 효과적으로 보호대책 CM_i에 의하여 차단되는 위협의 비율로 정의한다.

t_i가 발생하여 CM_i를 공격하여 성공하게 되면 이때 CM_i가 설치된 정보보호시스템은 $S_i - 1$ 상태에서 S_i상태로 전이한다. 이때 상태 전이 확률은 해당 위협 사건 t_i가 발생할 확률 λ에 해당 보호대책 CM_i가 그 위협을 차단하지 못할 확률 $(1 - P_{CM_i}(t_i))$의 곱이 된다. $i \neq j$ 일 경우 $P_{CM_i}(t_j)$는 0으로 정의한다. 이러한 상태의 전이를 (그림 5)에 보였다.



(그림 5) 상태 S_{i-1}에서 S_i으로 전이

n개의 보호대책이 있는 정보보호시스템의 경우 시스템의 상태는 보호대책에 대하여 의미 있는 일련의 위협사건으로 이루어진 위협 트랜잭션 $\tau = (t_1, t_2, \ldots t_n)$에 의하여 결정된다. t_1이 CM_1의 공격에 성공하고 t_2가 CM_2의 공격에 성공하고 뒤이은 모든 공격이 성공하여 tn이 CM_n의 공격에 성공하였을 때 가 정보보호시스템의 공격에 성공한 것으로 정의한다. 위협 트랜잭션과 정보보호시스템의 관계를 (그림 6)에서 나타내었다.



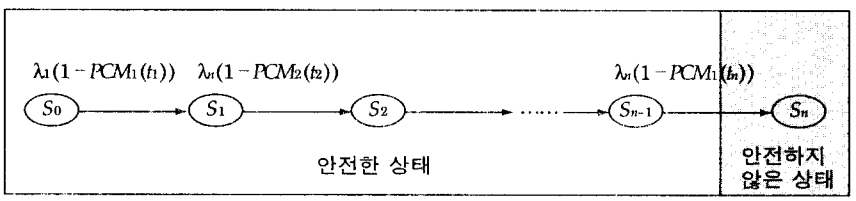
(그림 6) 위협 트랜잭션과 정보보호시스템

시스템의 상태는 최초의 안전한 상태 S_0에서 시작하여 t_1이 CM_1을 통과하면 시스템의 상태는 S_1로 변화하고 그렇지 않으면 S_0에 그대로 남아 있게 된다. S_1에서 t_2가 발생하여 CM_2를 통과하면 시스템의 상태는 S_2로 바뀐다. 이때 다른 t_i이 발생하여 CM_i을 통과하였는가 아닌가는 시스템의 상태에 영향을 미치지 않

고 $1 \le i \le k$인 모든 i에 대하여 $\delta(t_i)=1$ 이 되는 일련의 $t_1, t_2, ..t_k$ 로 구성된 τ가 있을 경우 이 때의 k가 시스템의 상태를 결정한다. 또 어떤 t_j에 대하여 $\delta(t_j)=1$이라 하더라도 τ에서 $\delta(t_i)=0$인 $i<j$가 있다면 이것 역시 시스템의 상태에 영향을 미치지 못한다. 즉, 각각의 에 대하여 $f(\tau)=k$ 일 때 k는 $\prod_{i}^{k}\delta(t_i)=1$인 최대 k를 말하며 시스템의 상태는 발생한 모든 위협 $\{\tau\}$에 대하여 $S_{Z_{(\tau)}}$가 된다.

3.2 단순 모델(Simple PEMM, sPEMM)

위협 트랜잭션 가 성공하였다는 것은 τ를 구성하는 각각의 t_i가 각각의 CM_i를 통과하여 최종적으로 자원에 피해를 발생시킨 것을 말한다. 즉 $f(\tau)=n$일 경우 정보보호시스템의 모든 보호대책을 통과하여 위협행위자가 자원에 대하여 원하는 접근을 수행할 수 있는 상황이 된다. 이러한 상태를 '안전하지 않은 상태'로 정의한다. 이 외의 상태는 자원에 피해를 주지 않는 상황이므로 안전한 상태이다. 즉, 위협이 나타나지 않거나 발생한 위협이 보호대책에 의하여 보호하여야 할 자원으로부터 차단된 상태를 안전한 상태로 정의하는 것이다. 따라서 여러 개의 보호대책이 존재할 때 일부의 보호대책은 통과하였으나 자원에 접근하기 위하여 통과하여야 할 보호대책이 남아있는 상태는 안전한 상태에 포함된다. (그림 7)에서 이를 보이고 있다. 이때 현재의 상태에 머무를 확률은 $1-\lambda_i(1-P_{CMi})$가 된다.



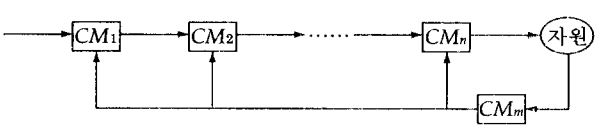
(그림 7) 시스템의 상태 전이도

이러한 모델에 따른 정보보호시스템의 보호 효과를 PE_{sPEMM}이라 하고 다음과 같이 정의한다.

$$PE_{sPEMM} = 1 - \prod_i \lambda_i \times (1 - P_{CMi}(t_i)) \quad \text{..... (1)}$$

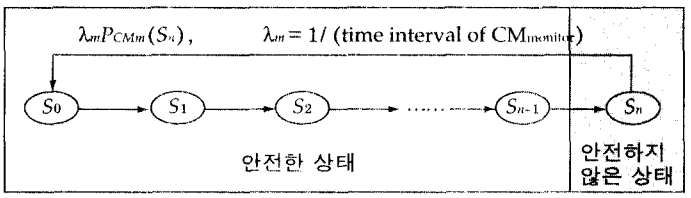
3.3 궤환 모델(Feedback PEMM, fPEMM)

한편, 만일 위협이 자원에 도달하여 자원에 대한 불법적인 접근이 이루어졌음을 판단할 수 있는 감시 또는 감사대책이 있어 이를 통하여 시스템을 복구하고 각 보호대책을 재 설정하여 안전하지 않은 상태에서 다시 안전한 상태로 되돌아갈 수 있다. 이러한 기능을 가진 정보보호시스템을 (그림 8)에 보였다.



(그림 8) 감시 및 복구 대책이 존재하는 정보보호시스템

이렇게 안전하지 않은 상태 S_n에서 안전한 상태 S_0으로 상태 전이할 경우의 확률은 감시 또는 감사대책 CM_m이 작용할 확률과 그 기능이 이러한 상태를 감지할 수 있는 확률 $P_{CMm}(S_n)$의 곱으로 나타낼 수 있다. 감시 또는 감사대책이 주기적으로 작동한다면 그 대책이 작용할 확률은 작동 주기의 역수로 나타낼 수 있다. 이러한 상태 전이를 (그림 9)에 나타내었고 이때의 시스템의 전이확률행렬을 [표 2]에서 보였다. 여기에서는 감시 또는 감사대책을 하나만 있는 것으로 설정하였으나 여러 개가 있을 경우도 모델링이 가능하다.



(그림 9) 감시 및 복구 대책이 존재할 경우의 상태 전이도

[표 2] 상태전이확률표

From \ To	S_0	S_1	S_2	....	S_n
S_0	$1-\lambda_1(1-P_{CM1}(t_1))$	$\lambda_1(1-P_{CM1}(t_1))$	-		-
S_1	-	$1-\lambda_2(1-P_{CM2}(t_2))$	$\lambda_2(1-P_{CM2}(t_2))$		-
S_2	-	-	$1-\lambda_3(1-P_{CM3}(t_3))$		-
...					
S_n	$\lambda_m P_{CMm}(S_n)$	-	-		$1-\lambda_m P_{CMm}(S_n)$

이렇게 안전한 초기 상태 S_0으로 다시 되돌아 갈 수 있을 경우 모든 상태가 서로 왕래 가능하고 상태의 갯수가 유한하므로 각 상태에 대하여 극한확률(limiting probability) πS_i가 존재한다[이호우96]. 이때 안전하지 않은 상태 S_n의 극한확률 πS_n은 오랜 시간 이러한 상태 전이가 이루어질 동안 안전하지 않은 상태가 차지할 시간의 비율, 즉 시간평균확률(time-average probability)로 해석될 수 있다. 따라서 이렇게 정보보호시스템의 상태전이를 모델링하였을 때 식 (2)와 같이 정보보호시스템의 보호효과 PE_{ifPEMM}을 전체 시간 중 안전한 상태에 머무를 시간의 비율로 정의한다.

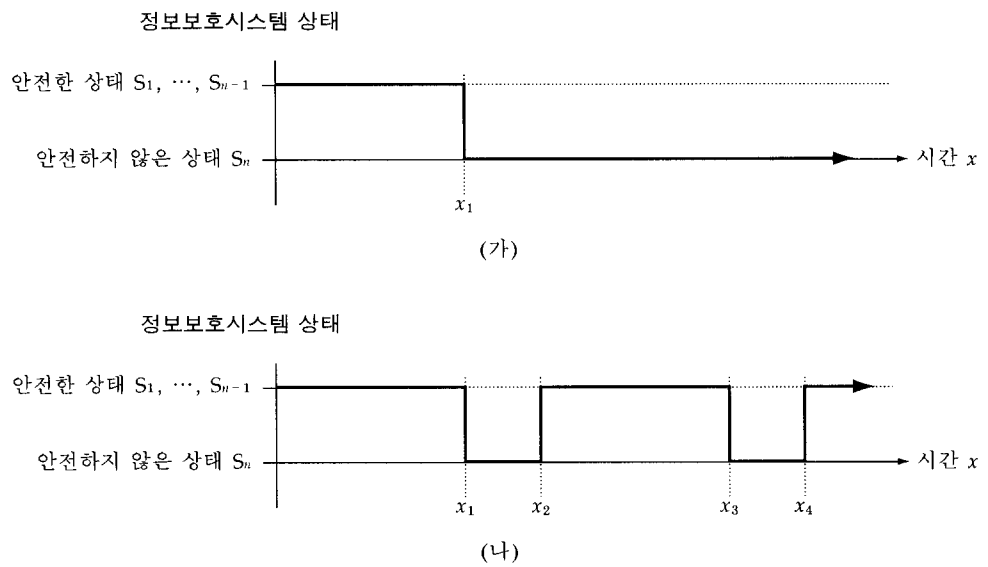
$$PE_{ifPEMM} = 1 - \pi_{Sn} \quad \cdots\cdots (2)$$

이때 식(1)과 식(2)의 의미의 차이는 시간의 관점에서 보면 더욱 분명해진다. 식(1)의 경우 이 정보보호시스템은 확률 $1-PE_{sfPEMM}$으로 보호에 실패하고 한번 실패한 후에는 계속 실패한 상태로 있게 된다. 물론 이 경우에도 피해의 내용에 따라 관리자에게 알려질 수도 있고 복구가 가능하지만 이것은 정보보호시스템의 운영환경에 의하여 결정될 문제이다. 실패할 때까지의 평균시간을 E(T)라 하면 E(T) = 단위시간/$(1-PE_{sfPEMM})$이 된다. 따라서 이 정보보호시

스템은 작동을 시작한 후 E(T) 시간 동안 정보를 안전하게 보호할 것이라고 기대할 수 있다. 관리자는 이 정보를 이용하여 정보보호시스템의 관리적인 점검기간을 정할 수 있다. 한편 식(2)에서는 전체 관찰시간 중 정보보호시스템이 자원을 보호할 기간의 비율이 PE_{fPEMM}이 된다. 이 관계를 (그림 10)에서 보였다.

(그림 10)의 (가)는 식 (1)로 나타나는 시스템의 상태를 시간에 따라 나타낸 것이다. 시스템은 안전한 상태에서 시작하여 시간 x_1에서 어떤 위협 트랜잭션 가 성공하여 안전하지 않은 상태로 동작하게 되며 외부의 감사 및 감지를 통한 복구가 없을 경우 계속 이러한 상태로 동작하게 된다. (그림 10)의 (나)에서는 정보보호시스템 내부에 감시 및 복구 기능이 있어 시간 x_1에서 정보보호시스템이 안전하지 않은 상태로 전이하더라도 시간 x_2에서 감시 및 복구 기능이 이러한 상태를 감지하여 복구하게 되면 시스템은 다시 안전한 상태로 돌아온다. 이때 시스템이 안전하지 않은 상태에 머무르는 시간 간격 $|x_2-x_1|$이 $|x_4-x_3|$와 항상 같다고 말할 수는 없으나 이 시스템이 오랜 시간 동안 작동할 경우 안전하지 않은 상태에 머무르는 시간의 비율은 π_{S_n}이 된다.

즉, $\dfrac{\sum_{i=1}^{\infty}|x_{2i}-x_{2i-1}|}{x_\infty}=\pi_{S_n}$이다.



(그림 10) 정보보호시스템의 운영시간에 따른 상태의 변화

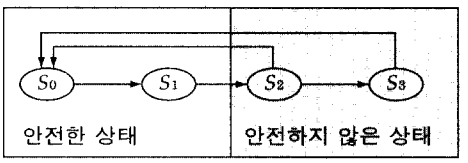
3.4 궤환 모델(fPEMM)을 이용한 위험분석

이렇게 감시 또는 감사 대책을 사용하였을 경우, 안전하지 않은 상태에서 나타나는 자산의 피해는 안전하지 않은 상태에 머무르는 시간과 자산의 민감성(sensitivity)에 따라 변한다. 즉, 민감한 정보자산은 짧은 시간의 노출에도 큰 피해가 나타나고 덜 민감한 정보자산은 같은 기간의 노출에 대해 상대적으로 피해가 적다고 볼 수 있다. 이러한 민감성에 대한 결정은 정보자산을 평가하는 위험분석의 초기

단계에서 이루어지며 본 논문의 범위를 벗어난다. 특히 시간에 따른 정보자산의 피해액의 변동을 추정하는 것은 매우 복잡한 문제이지만 정성적 분석을 통한 개략적인 형태라 하더라도 그러한 경향을 파악할 수 있다면 위험을 파악하는데 매우 도움이 될 것이다.

정보보호시스템을 평가하는 경우는 해당 정보보호시스템의 최대 보호효과를 평가하기 위하여 모든 보안대책을 거쳐 최후에 자원에 도달하는 것으로 모델링하였다. 그러나 일반적으로 정보보호시스템을 사용할 경우 모든 자원을 보호하기 위해 모든 보호대책을 다 거치도록 설정하지는 않는다. 일반적인 경우 하나의 정보보호시스템에 다양한 정보를 저장하는데 이 정보들은 그 특성이나 중요도에 따라 분류하여 중요도가 낮은 정보는 보호대책의 일부만을 거쳐 접근할 수 있도록 하고, 중요도가 높은 정보는 추가의 보호대책으로 보호하도록 할 수 있다.

예를 들어 어떤 정보보호시스템에 두 종류의 정보 자산이 있어 하나는 기본적인 보호대책 CM1, CM2를 거치면 접근이 가능하고 다른 하나는 추가적인 보호대책 CM3으로 보호될 경우 이 시스템은 다음 (그림 11)과 같이 모델링할 수 있다. 시스템의 각 상태는 그 상태에서 접근할 수 있는 자산에 따라 안전하거나 안전하지 않은 상태로 나뉜다. 일부의 자산이라 하더라도 자산에 접근이 가능한 상태는 안전하지 않은 상태로 정의한다.



(그림 11) 예제 시스템에 대한 모델링

시스템 상태 S_0은 위협이 발생하지 않았거나 발생한 위협이 첫번째 보호대책 CM_1에 의하여 성공적으로 차단된 상태를 나타낸다. S_1의 상태에서는 위협이 CM_1을 통과하였으나 자원은 아직 CM_2 의하여 보호되고 있다. 위협이 CM_2를 통과하게 되면 첫번째 종류의 정보자산에 접근이 가능하게 되어 피해가 발생하는 S_2 상태로 전이하게 된다. 이 상태에서 위협이 CM_3을 통과하게 되면 두번째 종류의 정보자산까지 접근이 가능하게 되어 피해가 더 커진다. 이 예제에서의 상태전이확률은 S_2의 경우를 제외하고는 3.1절의 모델과 동일하다. S_2의 경우에는 S_3으로 전이하는 것 외에 S_0으로 전이할 수 있고 이때의 전이확률은 $\lambda_m P_{CMm}(S_2)$가 되며 따라서 S_2에 그대로 남아있을 확률은 $1-(\lambda_m P_{CMm}(S_2)+\lambda_3(1-P_{CM3}(t_3)))$이 된다.

[표 3]에서 이 예제의 상태전이 확률을 보였다.

안전한 상태에서는 자산에 접근할 수 없으므로 이때의 자산 손실은 0이다. 안전하지 않은 상태에서는 자산의 손실이 일어나므로 각 상태에 관련된 단위시간당 자산 손실액과 안

[표 3] 예제 시스템의 상태전이확률

From \ To	S_0	S_1	S_2	S_3
S_0	$1-\lambda_1(1-P_{CM1}(t_1))$	$\lambda_1(1-P_{CM1}(t_1))$	-	-
S_1	-	$1-\lambda_2(1-P_{CM2}(t_2))$	$\lambda_2(1-P_{CM2}(t_2))$	-
S_2	$\lambda_m P_{CMm}(S_2)$	-	$1-\lambda_3(1-P_{CM3}(t_3))$ $-\lambda_m(1-P_{CMm}(S_2))$	$\lambda_3(1-P_{CM3}(t_3))$
S_3	$\lambda_m P_{CMm}(S_3)$	-	-	$1-\lambda_m P_{CMm}(S_3)$

전하지 않은 상태의 시간평균확률을 계산함으로써 일반적으로 잘 알려진 위험 척도인 연간 예상 손실액 ALE(Annual Loss Expectancy)을 구할 수 있다[DOC80].

$ALE = \sum_i [L_i \times \pi_{Si}]$. 여기에서 L_i는 S_i에서의 단위시간당 손실

이 예제에서는 $L_0 = L_1 = 0$이므로 $ALE = L_2 \times \pi_{S2} + L_3 \times \pi_{S3}$가 된다.

4. 결 론

본 논문에서는 기존의 정보보호시스템 평가방법이나 위험분석방법으로는 해결할 수 없는 정보보호시스템의 보호효과를 평가하기 위하여 상태전이도를 사용한 정보보호시스템의 평가모델 PEMM (Protection Effectiveness Measurement Model)을 제안하였으며 이 모델에 따라 보호효과 PE(Protection Effectiveness)를 산출하는 방법을 제시하였다. PE는 정보보호시스템에 포함된 다중 보안대책의 종류와 효과에 따라 자산을 안전하게 보호할 확률 또는 전체 시간 중에 안전한 운영 시간의 비율로 나타난다. 또한 이 모델을 확장하여 위험분석에 적용하는 방법을 제시하였다. 이 모델은 의도적인 위협과 그에 대응하기 위한 다중의 보호대책을 탑재한 정보보호시스템을 평가하기에 매우 적합하며, 평가된 결과는 곧바로 조직의 위험분석에 적용할 수 있다.

본 논문에서 제안한 PEMM에서 실제 각 t_i가 발생할 확률 λ나 보호대책의 효과 P_{CMi}, 또는 각 상태에서의 자원의 가치와 그 손실액, 시간에 따른 손실액 함수 등을 구체적으로 계산하는 것은 또 다른 차원의 어려운 문제이나 이는 향후 수행되어야 할 연구분야이다.

5. 참고문헌

[Bodeau92] Bodeau, A Conceptual Model for Computer Security Risk Analysis, IEEE 1992, pp.56-63.

[CCIB98] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, CCIB-98-028, May 1998, Version 2.0.

[Clayton97] John F. Clayton, Threat Assessments Addressing the Unknown in Risk Management, 9th Annual Canadian Information Technology Security Symposium, 1997, pp301-321.

[CSE93] Canadian System Security Centre, The Canadian Trusted Computer Product Evaluation Criteria, Communications Security Establishment, January 1993, Version 3.0e.

[CSE96] Communications Security Establishment, A Guide to Risk Management Framework for Information Technology Systems, 1996, 38pages.

[DOC80] FIPS Pub 65, Guidelines for Automated Data Processing Risk Analysis, U.S. Department of Commerce/NBS, Jun. 1980.

[DOD83] Department of Defense Standard, Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 1983.

[DOD85] Department of Defense, Technical rationale behind CSC-STD-003-85: Computer security requirements, Guidance for applying the DOD TCSEC in specific environments, CSC-STD-004-85, 25 June 1985.

[Drake94] Drake, Morse, The Security-Specific

Eight Stage Risk Assessment Methodology, Proceedings of the 17th National Computer Security Conference, 1994.

[HC91] Harmonised Criteria of France, Germany, the Netherlands, and the United Kingdom, Information Technology Security Evaluation Criteria(ITSEC), June 1991, Version 1.2 (Provisional).

[ISO97] ISO/IEC JTC1, Guidelines for the Management of IT Security, TR 13335, 1997. 5.

[NIST92] National Institute of Standards and Technology and National Security Agency, Federal Criteria for Information Technology Security, Version 1.0 December 1992.

[White96] White, Fisch and Pooch, Computer System & Network Security, CRC press, 1996.

[정통부98] 정보통신부, 정보통신망침입차단시스템평가기준, 1998.

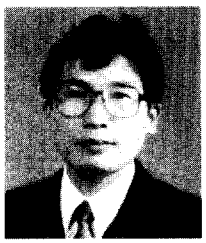
[이호우96] 이호우, 대기행렬이론, 도서출판 기술, 1996.

□ 著者紹介

오 경 희

1988년 2월 서강대학교 전자계산학과(학사)
1992년 2월 한국과학기술원 전자계산학과(석사)
1995년 11월 CISA
1992년 10월 - 1996년 12월 한국통신 멀티미디어연구소 전임연구원
1996년 12월 - 현재 한국정보보호센터 주임연구원

※ 주관심분야 : 정보보호시스템 평가체계, 정보시스템 감사, 위험분석 및 관리



홍 기 웅

1985년 2월 전남대학교 전자계산학과(학사)
1990년 2월 중앙대학교 대학원 전자계산과(석사)
1994년 4월 정보처리기술사
1996년 2월 아주대학교 컴퓨터공학과(박사)
1985년 9월 - 1995년 10월 한국전자통신연구소 선임연구원
1992년 - 1993년 이태리, Alenia Spazio사 Senior Researcher
1995년 10월 - 1996년 4월 한국전산원 선임연구원
1996년 4월 - 현재 한국정보보호센터 책임연구원, 평가체계팀장/기술표준팀장

※ 주관심분야 : 컴퓨터 · 네트워크 보안, 정보시스템 위험분석 · 평가, 정보보호 표준화

심 주 걸

1957년생
중앙대학교 전자공학과(학사)
건국대학교 대학원 전자공학과(석사)
성균관대학교 정보공학과 박사과정재학중
현재 한국정보보호센터 기준평가부장

※ 주관심분야 : 정보보호시스템 기준 · 평가 암호이론