정보시스템의 효율적인 인적자원 관리를 위한 Cause-Effect Model의 활용

이남훈* · 인 호** · 이도훈*

요 약

최근 정보시스템의 발달에 따라, 다양한 정보시스템과 응용 소프트웨어의 개발이 이루어지고 있다. 하지만 정보시스템의 발달에 따른 역기능으로 많은 침해사고와 사이버해킹이 증가하는 추세이다. 이러한 정보화의 역기능을 차단하기 위해, 많은 기관에서는 정보시스템과 이를 보호하는 정보보호시스템의 운영과 관리를 위하여 많은 정보시스템 운영인력을 투입하고 있으나, 체계적 관리와 각 역할의 특성에 대한 분석부족으로 효율적인 운영에 많은 어려움을 겪고 있다. 본 논문에서는 정보시스템과 정보보호시스템 보안 및 관리 운영과 수행업무의 특성에 따라 정형화된Cause-Effect Model을 제시하도록 한다. 이 모델에서는 정보시스템과 정보시스템 운영자를 하나의 information Component로 간주한다. 본 논문에서 제시된 Cause-Effect Model의 각 단계에서 영향을 미치는 Human Factor의 세부 요소에 대한 영향도 분석을 통하여, 주어진 역할에 따라 최적의human Resource의 관리와 배치가 가능할 것이다. 이러한 분석 및 접근 방법은 각 기관의 제한된 Resource 에 대한 효율적 운영이 가능하도록 하여, 기관의 정보시스템 운영과 악의적 침입에 대한 효율적인 방어를 가능하게 할 수 있다.

A Cause-Effect Model for Human Resource Management

Nam Hoon Lee* · Hoh-In** · Do Hoon Lee*

ABSTRACT

According to the development of information system, many information system and application software are develop. However, cyber attack and incident have more increased to the development of them. To defend from cyber attack and incident, many organizations has run information security systems, such as Intrusion Detection System, Firewall, VPN etc, and employed information Security person till now. But they have many difficulty in operating these information security component because of the lack of organizational management and analysis of each role. In this paper, We propose the formal Cause-Effect Model related with the information security system and administrative mission per each security. In this model, we regard information system and information system operator as one information component. It is possible to compose the most suitable information component, such as information system, human resource etc., according to the analysis of Cause-Effect Model in this paper. These analysis and approaching methodology can make effective operation of each limited resource in organization and effective defense mechanism against many malicious cyber attack and incident.

Key words : Information Security, Cause-Effect Model

* ETRI 부설 국가보안기술연구소
** 고려대학교 컴퓨터학과

1. 서 론

정보시스템의 발달에 따라, 많은 정보시스템이 인터넷 환경과 연결되어 다양한 정보를 주고 받고 있다. 이러한 정보시스템의 발달과 상호 연관성의 복잡도 증가에 따라, 외부에서 나타나는 공격의 형태도 날이 다르게 증가하고 있다. 그리고 이러한 외부의 공격에 적극적으로 대처하기 위해서 다양한 정보시스템 관리도구와 보안도구, 이를 최종적으로 운영하는 정보보호시스템 관리자의 적절한 운영과 소프트웨어간에 유기적인 관계를 이루며 많은 시스템들이 운영되고 있다. 이렇게 다양한 정보보안 시스템이 그 목적을 달성하기 위해서는 시스템 성능뿐 아니라, 관리운영자의 능력 또한 매우 중요한 요소로 간주되고 있다. 근래 연구 개발되는 많은 정보보안 시스템이 많은 부분을 자동화하고 있지만, 여전히 많은 부분을 운영자의 기술과 경험에 의존하고 있다. 이러한 이유로, 정보시스템의 보안관리와 침해사고대응 행위 부분의 많은 연구가 시스템 공학과 인간공학 분야를 응용하여 다양하게 연구되고 있다. 하지만, 이렇게 운영자의 능력이 큰 중요성을 가진다는 점과는 달리, 최근 제한된 정보시스템의 인력과 자원을 효율적으로 운영하기 위한 연구가 제한적인Human-Machine 시스템의 연구에서 이루어질 뿐이고, 그 결과조차도, 추상적인 개념에서 연구의 성과가 멈추고 있다. 본 논문에서는 이러한 시스템과 인간요소의 상호 작용 연관성을 확인하기 위해, 임의의 정보시스템을 목표로 한 공격행위가 정보시스템의 피해정도로 나타나는 프로세스에서 Human Impact Component가 어떠한 영향을 미치는가를 살펴보도록 한다. 또한, 본 논문에서는 시스템과 Human의 상호관계를 모델링하고 각 step에서 Human Factor의 요소가 영향을 미치는 부분에 대한 분석이 용이한 Attack-Incident Cause Model을 제안한다. 그리고 이를 통하여, 제한된 자원을 어떠한 단계에서 적용할 경우 효과적인 대응 단계를 구성할 수 있을지 확인하도록 한다.

2. 관련 연구

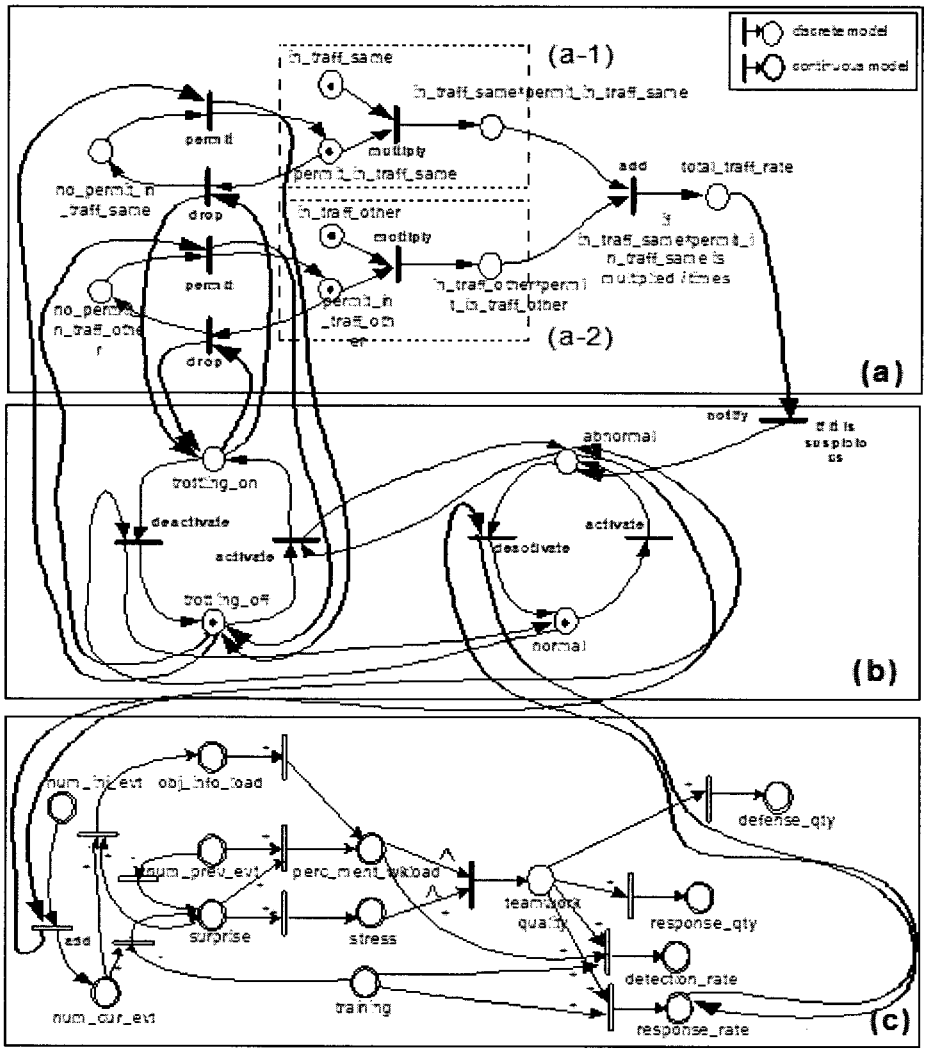
과거 정보시스템의 운영개념에서 인간은 정보시스템을 운영하는 존재로 가정되어, 정보시스템의 주요 요소로 고려되지 않았다. 하지만, 이러한 기존 개념과는 달리, 최근에는 정보시스템과 정보시스템의 운영자가 하나의 요소로 통합된 존재로 인식되고 있다. 또한 개별적인 요소가 아닌 통합요소가 정보시스템의 중요한 요소로 인식이 되면서, 운영자의 능력을 극대화하기 위한 많은 연구가 꾸준히 진행되어 왔다. 이러한 개념에서 시작된 것이 Man-Machine Model에 대한 연구이다. 또한 정보시스템의 보안 수준을 강화하기 위하여, 정보시스템 운영자가 수행하여야 하는 여러 사항이 정보보증이라는 개념으로 연구 발전되어 왔다. 본 장에서는 기 연구된 Man-Machine의 개념과 information assurance 그리고 human factor가 system 운영과 정보시스템의 보안관점에서의 행위의 신뢰성에 영향을 미치는 부분의 연구에 대하여 간단하게 살펴보도록 한다.

2.1 MAN-MACHINE MODEL 관련 연구

정보시스템의 기술이 급격하게 발달하여 기존의 정보시스템만으로는 정보보호관리의 개념을 말하기가 매우 어렵게 되었다. 따라서 최근 많은 정보보호관리 영역에서 시스템 운영자, 즉 인간을 하나의 시스템 Component 인정하고 개별 요소의 연관성을 파악하게 되었다. 이러한 개념에서 도입된 모델이 Man-Machine Model이다. 이러한 Human factor engineering 기법은 Human을 시스템의 한 요소로 간주하고 Man-Machine Model을 통하여 이들 사이의 relationship을 표현하는 일반적인 방법을 제공하고 있다. 일반적으로 man-machine

model의 가장 간단한 모델은 1인 operator가 단일 machine system을 조작하도록 구성되도록 할 수 있으나, 이러한 경우는 극히 예외적인 경우이다. 실제 Man Machine Model에서 표현하는 것은 (C) Human group factor, (A)Machine group factor 그리고 Human과 machine의 연관관계를 구축해주는 (B)Control factor이다. 이러한 3개의 Factor가 연동하여, 하나의 Man-machine Model을 구성하게 된다.

이렇게 연구되는 모델에서 (그림 1)은 인간요소가 시스템에 미치는 영향을 Petri-Net을 이용하여 도식적으로 나타내고 있다. (그림 1)의 모델에서 Human Factor에 영향을 줄 수 있는 세부 요소가 detection rate와 response rate에 영향을 미치는 요소로 작용하는 것을 살펴볼 수 있다. 이때 human factor에 영향을 미칠 수 있는 요소는 operator의



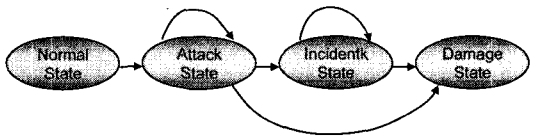
(그림 1) Man-Machine Model의 구성과 흐름

skill과 knowledge, 운영자의 시스템 Training level, operator의 mental state 그리고 operator가 사용하는 software의 성능과 사용된 software의 수 등 다수의 요소가 존재한다. 현재 일부 진행되는 연구의 방향은 Man-Machine Model의 구성 요소 중 Human factor에 중점을 두고 있다. 하지만 Human Factor의 세부 요소가 정량화하기 매우 어려운 부분이기 때문에 관련 연구는 각 세부 요소의 상호관계에 대한 연구를 중심으로 진행되고 있다. Human Factor에서 정량화가 어려운 요소들은 대부분 Ration와 Quality에 영향을 미치는 impact 요소들이며, Human system skill, Human security skill, Knowledge, System training, Security Training 그리고 Human Mental State등의 요소가 있다. 비록 현재 진행중인 연구의 내용에서 정량화가 어려운 부분이 있지만, Human Factor의 요소가 (그림 1) Man-Machine Model의 구성과 흐름과 같이, Man-Machine Model의 Detection Rate과 Response Quality에 영향을 미치는 것은 명확하다. 이러한 Human factor주요 요소의 상호관계에 대해서는 Man-Machine Model에 관한 논문을 참고하도록 한다.

3. Attack-Incident Cause-Effect Model

3.1 Attack-Incident Cause-Effect Model의 개념

정보시스템의 기본요소와 운영관점은 각종 정보기기가 개발 운영되면서 끊임없이 발전하여 왔다. 최근에는, 기존 연구된 정보시스템의 한정된 의미에서 벗어나, Man과 Machine의 상호연관성 파악을 위하여 인간을 정보시스템의 한 요소로 간주하고 종합적인 시스템의 효율을 높이는 연구가 널리 진행되고 있다. 과거 Human factor를 시스템과 별개의 요소로 고려하였던 것과는 달리, 전체 시스템의 요소로 분류하기 시작하였다. 하지만 이 분야의 연구는 여전히 미진하여, 시스템의 개별 요소로서 영향을 미치는 요인을 파악하고 Human factor의 세부 구성요소를 설명하는 분야의 연구는 구체적인 상호연관성 모델을 구성하기에는 부족하다. 하지만 이러한 연간관계를 정보시스템의 피해전이 상태를 고려하여 살펴보면, 정보시스템의 관리 각 단계에서 Human error를 최소화하고, 제한된 자원의 효용성을 극대화 할 수 있는 것을 가정할 수 있다. 또한 이를 하나의 시나리오로 구성하는 것이 가능하다. 이러한 기본 상태전이 개념과 기존 연구된 Man-Machine Model의 이론을 바탕으로 Cause-Effect Model을 생성하여 사이버 공격시의 정보시스템 상태전이를 설명하도록 한다. 이 경우, 정보시스템 자원이 정상 상태로부터 시스템에 피해를 나타내는 damage상태로 전이되는 간단한 상태 전이는 다음의 와 같이 간단하게 나타낼 수 있다.



(그림 2) Simple Cause-Effect Model

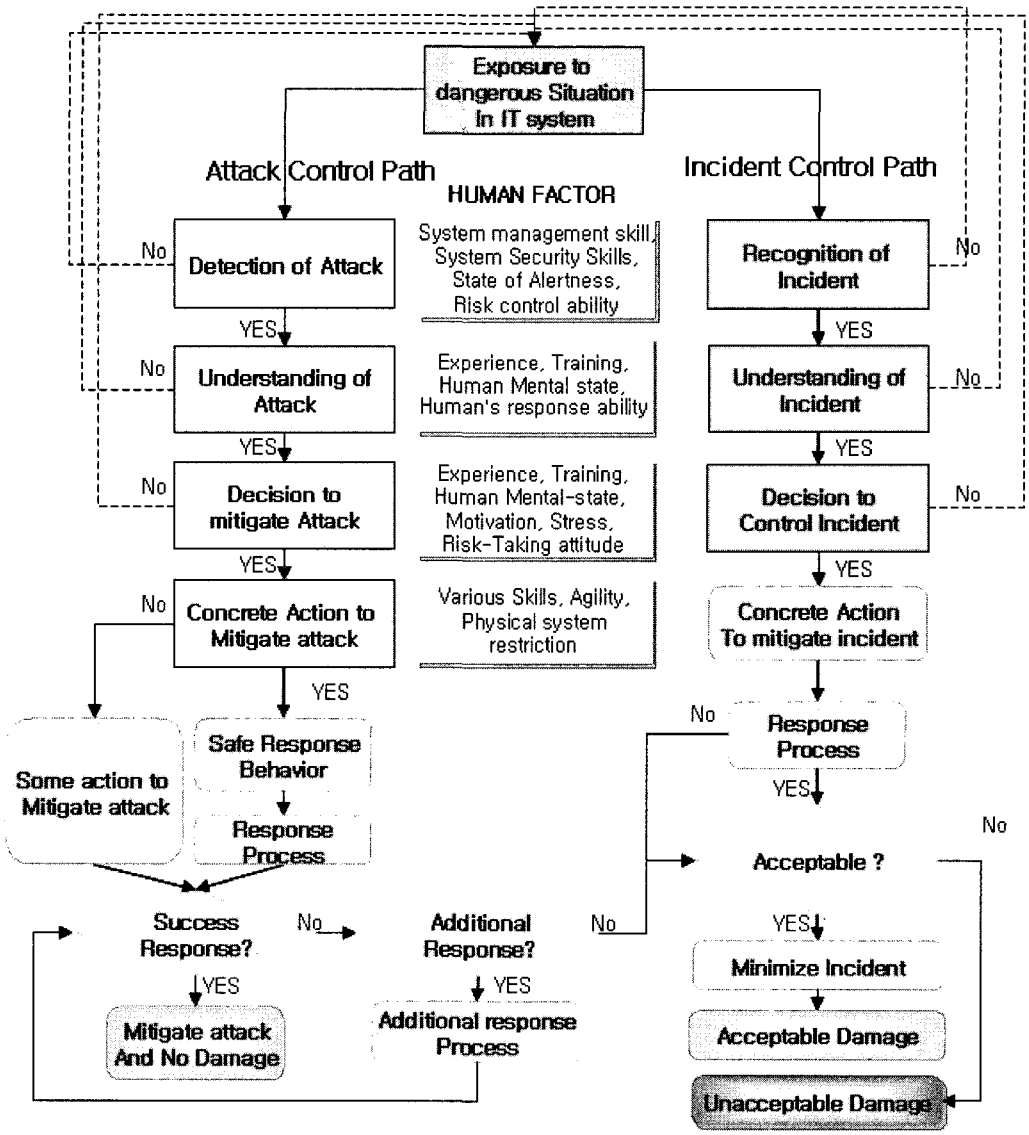
위의 (그림 2)에서 나타난 상태전이를 보다 세부적인 경로로 분류하면, 두 개의 Control Path로 나타낼 수 있다. 또한 정보시스템의 내외부에서 발생이 가능한 공격에 의하여 Incident가 발생하고 최종적으로 시스템 Damage 상태로 전이되는 것을 확인할 수 있다.

세부적으로 살펴보면 (그림 3)과 같이 각 state 별로 세부적인 Human factor가 작용하고 있음을 간단하게 확인해 볼 수 있다. 다음의 (그림 3)에서 나타난 각 단계는 정보시스템의 정상적인 운용상태에서 내외부적인 요인에 의하여 발생하는 광의

의 공격으로 인하여 발생하는 각 단계의 전이 상태를 표현한다. 즉 시스템의 정상적인 운영 단계에서 임의의 공격이 발생하였을 경우, 전이되는 Incident와 Damage 상태로 전이될 수 있다.

이렇게 간단한 Attack-Incident Model의 특성상, 상태의 전이와 진행 프로세스로 표현할 수 있고, 아래와 같이 Cause-Effect Model로 표현이 가능하다.

위의 형태와 같이 나타난 Attack-Incident Cause-Effect Model에서 Human factor가 영향을 미치는 경로는 크게 두 가지로 나누어 볼 수 있다. 하나는 외부의 임의적인 행위가 내부 시스템에 영향을 미



(그림 3) Attack-Incident Cause-Effect Model

치는 경로인 Attack-Control Path이고 다른 하나는 임의의 Incident가 발생하였을 경우, 이를 제어하는 Incident-Control Path이다. 이 두 개의 경로에서 정보시스템의 운영자들에 의해 결정되는 Human Factor는 각 단계의 운형행위에 영향을 미치게 된다.

이런 Attack-Incident Cause-Effect Model에서 2개의 Control Path로 정의된 이유는 아래의 2가지로 나누어 볼 수 있다.

첫째, 정보시스템을 대상으로 한 임의의 attack이 모두 정보시스템에 영향을 미치는 것은 아니다. 기본적으로 정보시스템에 대한 Attack은 정보시스템에 대한 악의적인 영향을 발생시켜 비정상적인 행위를 유도하는 것을 목적으로 하고 있다. 하지만 이러한 공격에 대하여, 정보시스템이 시스템적인 안전장치를 충분히 고려하는 경우와, 정보시스템 운영자가 적절한 대응을 하는 경우, 정보시스템에 영향을 미치지 못하고 종료된다. 반대로, 정보시스템을 대상으로 한 공격에 적절히 대응을 하지 못할 경우, 정보시스템에 피해를 입히는 것이다. 따라서 이러한 Attack 진행 상태에 정보시스템 운영자의 Human factor가 영향을 미칠 수 있는 Cause-Effect Path Model을 구성할 수 있다.

둘째, 정보시스템에서 발생할 수 있는 임의의 incident에 대하여 시스템적으로 혹은 운영자가 적절한 대응을 할 수 있을 경우, 정보시스템에 영향을 최소화하여 줄일 수 있다. 하지만 이러한 대응이 적절하게 이루어지지 않을 경우, 최종적으로 시스템이 감내할 수 없는 영향을 미치는 경우로 종료될 있다. 따라서 이러한 Incident의 발생시, 정보시스템 운영자의 Human Factor가 영향을 미칠 수 있는 Cause-Effect Path Model을 구성할 수 있다.

이렇게 구성된 Cause-Effect Model은 기존의 Petri-Net을 이용한 시나리오 및 이벤트 기반의 Model에 비하여 두 가지 장점을 지닌다.

첫째, 기존 Petri-Net을 이용한 Model의 경우에는 시나리오 기반으로 특별하게 제작된 형태의 공격과 Incident에 대한 기술이 용이하다. 이러한 기술에는 각 시나리오의 흐름에서 Machine과 Man의 요소가 영향을 미치는 부분에 대한 내용이 명확하게 분리될 수 있으며, 연속적인 흐름으로 표현이 가능하다. 하지만, 제한된 정보보안 관리 인력의 효율적 운영을 위해서는 Attack과 Incident의 경우, 각 단계가 명확해야하며, Machine의 관점보다 Man의 관점에서 분리되어야 한다. 기존의 Petri-Net을 이용한 모델은 Control Layer Component가 Man과 Machine을 연결하는 역할을 수행하고 있었으나, 특정 영역에서 Human 요소 중, Impact 요소가 중복되어 표현되어 있고, 특정 시나리오에 제한되는 영역이 존재하였다. 하지만 Cause-Effect Model의 경우, Attack과 Incident Control Path의 단계 구분이 명확하고 각 단계에서 영향을 미치는 Human Factor가 정의될 수 있다. 또한 기존 Man Machine Model에 비하여 상대적으로 범용적 모델이기 때문에, 일반 정보시스템 보안 관리에서 범용적으로 적용될 수 있다. 이를 이용하여 정보시스템의 2가지 Control Path를 기본으로 Cause-Effect Model을 구성하여 Human Factor가 정보시스템에 미치는 영향을 파악할 수 있다.

둘째, 기존 모델의 경우에는 시나리오 기반이 대부분이기 때문에, 각 시나리오의 흐름에서 Human Factor가 Model의 내부에서 고정적인 요소로 영향을 미치기 때문에, 정성적 및 정량적 요소에 대하여 주관적 관점으로 평가된 요소에 의하여 모델 전체의 신뢰도에 영향을 줄 수 있다. 하지만, Cause-Effect Model의 경우, Cause-Effect Model과 각 단계에서 영향을 미치는 Human 요소에 대한 분리를 통하여, 모델의 신뢰도와 Human 요소를 이용하여 모델의 수행영역 적용후의 영향평가가 분리되도록 설계되었다. 따라서 Human Factor 중 정량화가 명확한 인자들을 선별하여 Attack-Incident Cause-Effect Model을 구성하여 적용할 경우, 기존의 영향평가에 비하여 객관적인 Human Resource Management가 가능하다.

3.2 Attack-Incident Cause-Effect Model과 Human factor의 특성 분석

Attack-Incident Cause-Effect Model에서는 앞서 언급된 두 개의 경로(Attack Control Path와 Incident Control Path)에서 Human factor의 개별적 요소가 영향을 미치는 것을 가정하고 있다. 이 Human factor가 영향을 미칠 수 있는 세부적인 기준과 요소들은 각 운영자의 기술적 경험적 개별 요소에 의존하고 있다. 그리고 이들 세부 요소는 기존 사용자의 경험적 요소와 일정부분의 정량적인 요소로 판단할 수 있는 부분으로 나누어 볼 수 있다. 전자에 해당하는 부분은 sensory training, perception skill, Human memory ability, Attitude, motivation 등이 있고 그 외의 요소는 부분적 정량화가 가능한 요소로 분류할 수 있다. 각 Attack-Control Path와 Incident-Control Path의 각 단계에서 영향을 미치는 요소를 정량적 혹은 정성적 특징에 따라 분류하면 다음의 <표 1>과 같이 나타낼 수 있다.

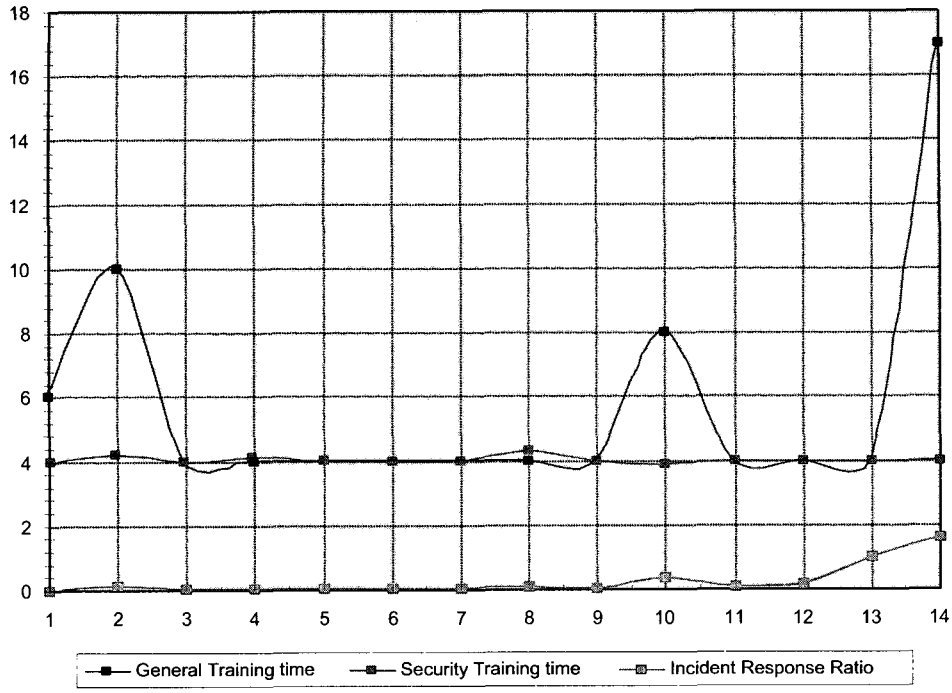
〈표 1〉 The Impact Human Factor in the Accident and Damage Path

Impact Factor Candidate	(Somewhat) Quantitative Element	Qualitative Element
System Skill		○
Security Skill		○
Risk Control Ability		○
System Experience	○	
Security Experience	○	
System Management Training	○	
Security Training	○	
Human Mental Stress		○
Number of Used Security Tool	○	
Quality of Used Security Tool	○	
Motivation		○

본 논문에서는 <표 1>과 같이 분류된 각 개별 요소 중, 일정부분 정량적으로 나타낼 수 있는 요소를 고려의 대상으로 제한하도록 한다. 또한 Attack-Incident Cause-Effect Model에서 Attack-Control Path를 제외한 Incident-Control Path에 미치는 상호관계를 분석하도록 한다. 논문에서는 이러한 상호관계의 분석을 위해, 제한된 Human factor로 Human General Training 요소와 Human Security Training 요소의 가정하도록 한다. 이 두 가지 요소를 가정한 이유는 일정기간동안 수집된 정량화된 신뢰도를 가진 요소이고, Human factor 중 수준 정량화가 가장 용이하기 때문이다. 이 두 요소가 Incident Control Path에서 평가되는 Incident Response Ratio에 미치는 영향도 분석결과에 대하여 고찰해보도록 한다.

아래의 (그림 4)는 앞서 언급된 Attack-Incident Cause-Effect Model을 기반으로 Human factor의 요소 중, 정량화가 가능한 Human General Training Time과 Security Training Time과 Incident Response Ratio의 상호관계를 파악한 것이다. 직관적으로 판단할 경우, Security Incident Response의 경우, Security Training Time이 더 높은 영향을 미치는 것으로 생각될 수 있으나, 실질적으로는 어느 한 요소만으로는 Incident Response Ratio의 증가를 기대하기가 어려웠다. 실험결과 오히려 Incident Response Ratio에는 일반 System Training 요소가 상대적인 특정 요소에 비하여 상대적으로 더 큰 영향을 미치는 것으로 판단되었다.

(그림 4)에서는 General Training Time과 Security Training Time의 변화와 Incident Response Ratio의 변화를 표현하고 있다. 위 그래프에서는 Incident Response Ratio의 비율이 General Training Time과 Security Training Time의 종합적인 변화와 연관되고, 어느 한 요소의 변화만으로는 효율적인 Incident Response가 곤란함을 확인할 수 있었다. 이러한 결과는 General information과 Security Information을 통합한 종합적 Training이 이루어져야,



(그림 4) System Training 기간과 Security Training 기간의 변화에 따른 Security Incident 발생시 Incident Response Action Ratio의 변화

제한된 Human Resource를 Incident Response 단계에서 효율적으로 운용할 수 있음을 보여준다.

4. 결 론

지금까지 기 연구된 Man-Machine Model을 바탕으로 순차적 프로세스의 개념을 강화한 Accident-Incident Cause-Effect Model과 세부 요소에 대하여 살펴보았다. Accident-Incident Cause-Effect Model의 Incident-Control Path를 중심으로 정량화된 Human Factor와 Incident Response Ratio에 미치는 영향을 관찰하여 보았다. Human factor의 세부 요소 중 많은 부분이 정량적으로 표현되기 어려운 부분으로 구성되어 있으나, 상대적 비율로 정량화 할 수 있는 요소에 대하여 정량화하여 Incident Recognition의 단계에서 영향을 미칠 수 있는 Human factor의 세부 종류에 대하여 상호연관성을 파악하였다. 이 결과는 정보시스템에 Security 요소를 강화할 경우, 필요한 수행 업무와 단계에 따라 중요도가 다른 Human factor가 다수 존재한다는 것을 반증하고 있다. 현재의 결과는 Human factor의 세부 요소에 대한 개략적인 내용만이 전반적으로 표현되고 있으나, Human factor의 세부 요소에 대한 세밀한 분석과 분석된 요소의 정량화에 대한 보다 깊이 있는 연구가 필요하다. 이러한 연구는 Human factor가 전체 Security Mechanism에 미치는 영향을 구체적으로 파악할 수 있게 할 뿐 아니라, 효율적인 보안관리 Mechanism의 구성을 가능하게 할 것이다. 이를 달성하기 위해서는 기 연구된 Man-Machine Model의 구체적인 개념확립과 많은 실험 데이터를 이용하

여 현실에 가까운 Man-Machine Model과 Attack-Incident에 기반한 Cause-Effect Model의 수립 및 검증을 통해 가능할 것이다.

참 고 문 헌

[1] H. P. In, S. Liu, and S. Jung : A Spiral/Reverse Spiral Life Cycle Model for Information Systems Risk Assessment, The 2rd Annual IEEE SMC Information Assurance Workship, 2001.

[2] H. P. In, S. Jung, S. Poole, and S.Liu, Modeling Man and Machine Interactions for Virtual Vulnerability Defense, The 3rd IEEE SMC Information Assurance Workshop, West Point, NY, 2002.

[3] M. Bishop. Vulnerabilities Analysis, Proceedings of the Recent Advances in Intrusion Detection, Septmber 1999.

[4] Kenneth R. van Wyk and Richard Forno. Incident Response, O'Reilly & Associates, Inc. July 2001.

[5] IT Security Guidelines : IT BaseLine Protection in Brief, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf

[6] W. Stallings. Network Security Essentials : Applications and Standards, Prentices-Hall, 2000.

이 남 훈

1999년 홍익대학교 컴퓨터공학과(공학사)
2001년 홍익대학교 전자계산학과(공학석사)
2001년~현재 국가보안기술연구소 연구원

인 호

1990년 고려대학교 컴퓨터학과(공학사)
1992년 고려대학교 컴퓨터학과(공학석사)
1998년 Ph.D University of Southern California (USC)
현재 고려대학교 컴퓨터학과 조교수

이 도 훈

1989년 한양대학교 전자계산학과(공학사)
1991년 한양대학교 전자계산학과(공학석사)
1991년~2000년 국방과학연구소
2000년~현재 국가보안기술연구소