韓國 컴퓨터情報學會 2007하계학술발표논문집&학회지
第15卷 第1號, 2007. 6.

정량적 침해사고 관리를 위한 Security Ticket 기반의 침해사고 관리시스템(CERT) 설계 및 관리방안 연구

김 선 태*, 박 대 우**, 전 문 석***

A Study and Design on security ticket based CERT system for quantified incident management

Sun-tae Kim*, Dea-Woo Park**, Moon-Seog Jun***

요 약

최근까지의 침해사고 대응에 대한 연구는 국제적 침해사고대응팀(CERT/CC)과 국가 또는 대형기관의 침해사고대응팀(CERT)의 유형을 중심으로 연구되어 일반기업 환경에 적용하기에는 어려움이 있었다. 본 논문에서는 일반기업의 IT 운영환경에 적합한 침해사고 대응절차를 수립하고, 침해사고 관리의 위협요소, 공격요소, 대응요소를 분석하여 Security Ticket을 기반으로 하는 침해사고 관리시스템의 설계 및 관리방안을 연구하였다. 이 방안을 토대로 침해사고 대응실험을 실시하여 제안한 CERT 모델의 유효성과 정량적 침해사고 관리방안의 효과를 확인하였다. 본 연구결과를 통해 일반기업에서는 CERT를 조직하여 체계적으로 관리함으로써 기업의 정보자산을 안전하게 보호할 수 있으며, 이미 CERT를 운영하는 조직에서는 침해사고 대응결과를 계량적으로 측정·분석하여 문제점을 개선함으로써 기업의 정보보호 수준을 높일 수 있다.

Abstract

There's been a difficulty for general corporate to adopt recent incident response study because those studies focus on nation wide CERT Coordination Center or large organization aspect. This study is focus on study and design on security ticket based CERT system through analysis Security management's threat element, attack element, response element and it also help general corporate establish incident response process that is adjusted on IT operation. Confirmed CERT model's effectiveness and effect of quantitative Security incident management way that propose executing Security incident response experiment on the basis of this way. This study which provides general corporate oriented CERT model can be used to improve corporate's capability of responding incident by quantified management technique and select incident response SLA indicator. Already, formation which operate CERT can heighten corporation's information protection level by measure Security incident response result as metrical and analyze and improve problem continuously.

▸ Keyword : CERT, Security Management, Security Ticket, 침해사고

• 제1저자 : 김선태, 교신저자 : 박대우(prof1@paran.com)
* 숭실대학교 대학원 컴퓨터학과, **호서대학교 벤처전문대학원 ***숭실대학교 컴퓨터학부

Ⅰ. 서 론

최근 기업의 모든 업무처리가 컴퓨터를 기반으로 수행되는 방식으로 일반화 되고, 기업의 비즈니스와 관련된 중요정보, 고객정보, 그리고 기업의 핵심 기밀정보 등이 정보시스템으로 처리되고 있어 해킹 등의 사이버 침해 위협이 점차 커지고 있다. 이와 같이 정보시스템에 사이버 침해사고가 발생할 경우 신속하고 정확한 탐지 및 대응 업무를 전담하는 정보보호 전담조직(CERT, Computer Emergency Response Team)을 운영하는 것이 발생한 침해사고의 피해와 영향을 최소화 할 수 있는 가장 실제적인 대책이다.

점차 사이버 보안 위협이 높아짐에 따가 국제 및 범국가적 CERT 조직이외에 민간 기업을 대상으로 정보보호 업무를 전담하는 CERT 조직을 활성화하기 위해 "기업 사이버 보안 전담조직(CERT) 구축 지원계획"을 2003년부터 정보통신부에서 추진하고 있다[1]. 추진 과정 중에 국내 111개 대기업을 대상으로 정보보호 전담조직 운영 현황을 조사한 결과 32%인 36개 기업이 전담조직을 운영 중인 것으로 조사되었다[2]. 그러나 2005년 한국전산원(NCA)에서 조사한 정보화 통계조사에 따르면 중소기업이 포함된 5인 이상의 400,000만 사업장 중 약 94.8%의 사업장이 정보보호 전담조직을 운영하고 있지 않으며, 그중 73.2%는 정보보호업무를 조직적으로 수행하고 있지 않는 것으로 조사되었다[3]. 이 조사 결과의 시사점은 2003년부터 범국가적 차원에서 정보보호 전담조직 구성을 통한 체계적인 정보보호를 권장하기 위해 지속적인 홍보와 지원을 하고 있지만, 일부 대기업과 대표적인 공공기관만이 전담조직(CERT)을 구축하여 운영하고 있으며, 일반 민간기업 등으로 확산되지 않고 있음을 의미한다. 이 문제는 전담인력 확보 및 비용 등과 같은 경제적 요인을 포함한 여러 가지 문제점이 있지만, 그 동안의 침해사고대응팀에 대한 연구와 홍보가 일반기업에 적용하기 어려운 CERT/CC 모델에 대한 개념적인 지식을 중심으로 이루어져 일반기업이 실무에 적용하기 위해서는 많은 수정과 보완이 필요한 문제점이 있다.

본 논문에서는 이러한 문제점을 해결하기 위해 일반기업에서 쉽게 적용할 수 있는 침해사고 대응절차와 Security Ticket을 기반으로 하는 침해사고 관리시스템의 설계 및 관리 방안에 대하여 연구하였다. Security Ticket 기반의 침해사고 관리시스템은 일반 기업의 IT 업무조직 사례를 반영하고, IT 업무 조직과 CERT 조직 간의 침해사고 대응 업무에 대한 책임과 역할을 정의하여 침해사고 대응활동을 보다 효과적으로 수행하고, 대응결과를 계량적으로 측정하여 지속적으로 개선 할 수 있도록 하였다.

Security Ticket은 조직에서 발생하는 침해사고를 인지하는 순간에 부여하는 식별자 이며, 침해사고 대응절차에 따라 대응이 모두 완료된 시점에 Ticket을 종료하는 것으로 정의하여 사용한다. 이와 같이 Security Ticket 기반의 침해사고 관리는 침해사고의 발생부터 완료시점까지 연속적으로 관리할 수 있으며, 침해사고 대응내역을 계량화 하여 측정·분석함으로써 대응 과정의 문제점을 찾아 지속적으로 개선하는 등 사후 평가로도 활용할 수 있다. 그리고 계량화한 관리결과를 서비스수준 관리(SLA)의 보안관리 지표 및 IT 아웃소싱 관련 국제 표준인 ISO 20000 표준에서 권고하는 헬프 데스크와 연계하여 침해사고 대응 관리를 국제 표준과 연계하는 방안으로 확장하여 활용할 수 있다.

본 논문의 구성은 2장에서 CERT의 유형, 업무 및 사례 등을 살펴보고, 3장에서는 Security Ticket 기반의 침해사고 관리시스템과 관리방안을 설계한다. 4장에서는 설계내역을 실험을 통하여 분석하고, 5장에서는 결론과 향후 연구 방향에 대해 기술한다.

Ⅱ. 관련 연구

2.1 침해사고대응팀(CERT)

2.1.1 침해사고대응팀(CERT)의 목적 및 주요업무

침해사고대응팀은 조직 내의 침해사고를 예방하고 복구하는 업무를 수행하는 팀으로 조직의 전산망에 발생하는 침해사고 대응활동을 주관하고 지원하는 업무를 수행하는 정보보호 전담조직이다[4]. 침해사고대응팀의 궁극적인 목적은 조직의 정보자산을 안전하게 보호하는 것이다. 이를 위한 주요업무는 첫째 발생한 침해사고의 피해를 최소화하기 위한 신속한 대응, 둘째 보안 동향 및 취약점 정보의 수집 및 전파를 통한 침해사고 예방, 셋째 침해사고 복구를 위한 기술지원 및 재발방지 계획수립, 넷째 관련 유관기관과의 업무협조 및 침해사고 대응을 위한 단일창구를 운영하는 것이다[5].

2.1.2 침해사고대응팀(CERT) 유형

침해사고대응팀의 유형은 CERT의 구성 목적 및 조직의 특성에 따라 Coordination Center, National Team, Corporation Team, IT Vendor team 등으로 구분된다[5,6]. Coordination Center 즉 CERT/CC는 전 세계 CERT 조직

간의 조정자 역할을 수행하며, 보안 위협에 대한 기술 공유 및 제공 등을 수행하는 최상위의 대표 CERT이다. National Team은 국가 보안 사고에 대한 기술지원 등을 책임지며, 범국가적인 목적으로 취약점 정보제공, 기술지원 등의 업무를 수행하는 조직이다. Corporation Team은 일반기업 등의 조직에서 침해사고 대응 업무를 전담하는 조직으로 CSIRT(Computer Security Incident Response Team)의 역할을 수행하는 조직이다. 마지막으로 IT Vendor Team은 Vendor에서 생산하는 하드웨어나 소프트웨어의 보안 결함을 찾아내고 개선을 위한 패치 및 기술지원을 수행하는 조직이다. 그리고 조직의 규모에 따라 중소규모의 조직에서는 중앙 집중형의 조직을, 대규모 기관에서는 분산형의 CERT 조직을 구성할 수 있다. 그리고 환경에 따라 중앙에 조정(Coordination Center)역할을 수행하는 중안 CERT를 구성하고 각 하부별로 지역 CERT를 구성하는 절충형의 CERT 조직을 구성하여 운영할 수 있다[6].

2.1.3 침해사고대응팀(CERT) 운영업무

CERT의 주요 업무는 침해사고 예방, 대응, 복구 및 재발방지, 그리고 효과적인 침해사고 대응을 위한 대·내외 단일창구 운영 등 이다. 이와 같은 주요 업무 이외에도 각 조직의 CERT 운영 목적 및 특징에 따라 다양한 운영업무를 수행할 수 있다. 2003년에 Carnegie Mellon 대학의 SEI에서는 "Handbook for CSIRT"에서 Reactive service, Proactive service, Security quality management의 영역으로 구분하여 CERT 운영업무를 포괄적으로 정의하여 발표하여, 침해사고의 예방, 대응, 복구 이외에도 다양한 CERT 운영업무를 수행할 수 있도록 권고 하였다[7,8,9,10].

표 1. 침해사고대응팀 운영업무
Table 1. Services of CERT

구분	서비스 내역(
Reactive Service	- 침해사고 전파(Alert and Warning) - 침해사고 대응(Incident Handling) - 보안 취약점 대응(Vulnerability Handling) - 침해사고 분석(Artifact Handling)
Proactive Service	- 보안공지(Announcements) - 보안기술 감시(Technology Watch) - 감사(Security Audit or Assessments) - 예방체계(Configuration of Security tools, App & Infra) - 보안도구 개발(Develop of Security tools) - 침입탐지(Intrusion Detection services) - 보안정보 전파(Security-related Information Dissemination)
Security quality management	- 위험분석(Risk Analysis), 업무연속 및 재난복구(BCP &DR) - 보안자문(Security Consulting), - 인식개선(Awareness building) - 교육/훈련(Education/Training) - 평가 및 인증(Evaluation or Certification)

2.2 침해사고 대응절차

침해사고 대응절차는 실제 발생한 침해사고를 체계적인 방법으로 신속하게 대응할 수 있는 핵심 사항이다. 침해사고 대응절차를 효과적으로 구현하기 위해서는 조직의 정보보호 규정으로 선언하는 것이 중요하다. 규정화 되지 않은 경우 각 담당조직 간의 역할과 책임이 불분명하여 효과적인 침해사고 대응을 어렵게 할 수 있기 때문이다.

2.2.1 국내사례(KISA 침해사고대응팀 구축/운영 교육)

국내 환경 특성을 고려하여 모범사례로 참고 할 수 있는 침해사고 대응절차는 국내 민간부분의 침해사고 대응지원 및 민간 정보보호를 대표하는 한국정보보호진흥원(KISA, Korea Information Security Agency)의 6단계의 대응절차가 대표적인 사례이다[4,5].

표 2. KISA 침해사고 단계별 처리 절차
Table 2. Security Incident Processing Step of KISA

단계	설명
사전준비	정보보호 전담조직인 CERT 팀원에 대한 보안전문기술 교육 및 침해사고 대응을 위한 각종 준비물 준비
확인	탐지 또는 신고 되는 이벤트가 실제 침해사고 인지를 결정, 대응을 위한 담당자 통지 등의 침해사고 대응을 준비
확산방지	침해사고의 피해확산 방지를 위한 네트워크 분리 및 주변 시스템으로의 전이여부를 확인 등의 긴급 조치
원인제거	사고원인을 파악하기 위한 시스템 로그 조사 및 공격 흔적조사, 침해사고의 직접적인 원인된 취약점 제거, 재발방지를 위한 방지대책을 수립
원상복구	운영시스템의 서비스를 정상화하기 위해, 사고 이전의 정상 상태로 복구하는 작업들을 수행
보고서 작성	침해사고 경위와 발생원인, 피해, 대응 내역, 결과 및 대책 등을 문서화하여 관련자들에게 통보 및 보고

2.2.2 CERT/CC 모델

CERT/CC(Coordination Center)에서 권고하는 침해사고 대응절차는 보호, 탐지, 구분, 대응의 4단계로 구성된다. 보호(Protect)는 하드웨어와 소프트웨어를 포함한 모든 정보인프라에 잠재적으로 발생할 수 있는 보안 위협을 완화하거나 제거하는 프로세스들로 구성된다. 탐지(Detect)는 보안시스템에서의 침입시도 탐지 및 사고접수를 포함하여 보안사고를 감지하는 프로세스들로 구성된다. 구분(Triage)은 침해사고를 인지한 후에 우선순위를 나누거나 대응을 위한 담당자를 선정하는 등 실제 침해사고 대응을 준비하는 프로세스들로 구성된다. 마지막으로 대응(Respond)은 침해사고 대응조치, 재발방지 등 실제 침해사고 대응과 관련된 프로세스들로 구성된다[7,8,9,10].

2.2.3 NIST/SANS 모델

NIST(National Institute of Standards and Technology) /SANS(SysAdmin, Audit, Network, Security)의 침해사고 대응 모델은 준비(Preparation), 식별(Identification), 확산방지(Containment), 제거(Eradicate), 복구(Recovery), 지원(Follow-up)의 태스크로 구성되어 있다. 그리고 각 태스크를 조합하여 침해사고 대응 준비, 탐지 및 분석, 확산방지/제거/복구, 사후활동의 4단계로 구성하여 침해사고 대응에 대한 Life cycle을 제시하였다[6,8,9].

그림 1. NIST/SANS의 침해사고 대응 Life cycle
Fig. 1. Incident Response Life Cycle of NIST/SNAS Model

2.3. 침해사고대응팀(CERT) 사례

2.3.1 국제 침해사고 대응체계(CERT/CC)

세계 최초의 침해사고대응팀인 CERT/CC는 1988년 Morris worm 사건을 계기로 창설되어 침해사고의 전 세계적인 공동 대응체계 유지를 목적으로 운영하고 있다[11]. 즉 세계 각처에 존재하는 CERT 조직을 폭넓게 포괄하고 조정하는 조정센터(Coordination Center)의 역할을 수행하며, 침해사고와 보안문제에 대한 전문적인 조언과 권고를 제공한다. 그리고 미래의 침해사고의 방향을 식별하며, 미래에 발생 가능한 보안문제들을 방어하기 위한 세계 공동대응 체계를 유지하고 관리하는 역할을 수행한다. 2007년 4월 기준으로 총 38개 국가가 가입되어 있으며, 전 세계 200여 개의 CERT 조직이 활동하고 있다[12].

2.3.2 국내 침해사고대응 조직 체계

국내 정보보호 조직체계는 국가정보원을 중심으로 하는 국가·공공분야, 국방부를 중심으로 하는 국방 분야, 정보통신부를 중심으로 하는 민간분야의 정보보호 체계로 구분되며, 각각 영역별로 역할을 분담하여 수행하고 있다. 그리고 대검찰청(인터넷범죄수사센터), 경찰청(사이버테러대응센터), 국가보안기술연구소, 한국정보보호진흥원 등의 전문기관이 정보보호와 침해사고 대응 업무를 수행하고 있다[3].

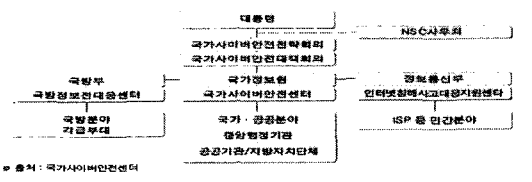


그림 2. 국가 침해사고 대응조직 체계
Fig. 2. Formation System of National Security Incident

2.3.3 국가 대표 침해사고대응팀(KrCERT)

우리나라 대표 CERT는 한국정보보호진흥원내의 인터넷 침해사고대응센터(KrCET)이며, 국내 민간 부문에서 운영되고 있는 전산망의 침해사고 대응활동을 지원하고, 전산망 운용기관 등에 대해 통일된 협조체제를 구축하여 국제적 침해사고 대응을 위한 단일 창구를 제공한다. 주요 업무는 인터넷침해사고대응센터(KrCERT) 운영, 침해사고 분석 및 기술지원, 침해사고 대응 협력체계 구축 및 운영 업무를 수행한다[13].

III. Security Ticket 기반의 침해사고 관리시스템 설계

본 논문에서 설계하는 Security Ticket 기반의 침해사고 관리시스템은 침해사고 대응절차를 핵심요소로 하고, 일반 기업의 IT 운영환경을 반영한 침해사고 대응 조직과 침해사고에 영향을 받는 정보시스템 자산을 추가 요소로 구성하여 설계하였다. 이것은 기존의 침해사고 대응에 대한 연구가 가졌던, 기술 중심의 절차적 대응으로 인한 문제, 대응 담당자들 간의 책임과 역할의 불분명으로 인한 문제, 공격받는 정보시스템과의 연관성 모호의 문제를 해결하기 위한 개선 모델이다.

제안하는 Security Ticket 기반 침해사고 관리시스템의 특징은 첫째, 침해사고가 발생된 시점부터 완료시까지 침해사고를 유일하게 구분하는 Security Ticket에 의해 관리함으로써 침해사고 대응의 연속성과 일관성을 보장하고 침해사고 대응관리의 성숙 수준을 높였다. 둘째, 일반기업 환경에 적합한 체제로 구축하기 위해 일반기업의 IT 운영환경에 맞는 침해사고 대응절차 제시하고, 이를 기반으로 시스템을 설계하여 적용 용이성을 높였다. 셋째, 침해사고의 발생원인과 대응경과, 조직 및 정보자산과의 연관관계를 파악하기 위하여 절차, 조직, 정보자산 인프라를 동시에 고려한 3차원의 침해사고 대응 모델을 제시하였다. 넷째, 침해사고 대응 내역을 관리요소로 계량화하여 측정·분석하여 관리함으로써 침해사고 대응의 문제점과 이슈 사항을 찾아 지속적으로 문제점을 개선할 수 있도록 한 점이다.

아래 그림 3은 해킹, 스캐닝, 웜/바이러스 등의 침해공격 시도에 대한 대응절차, 대응조직, 영향을 미치는 정보 인프라와의 연관관계를 고려한 3차원의 침해사고 대응모델의 구조이다.

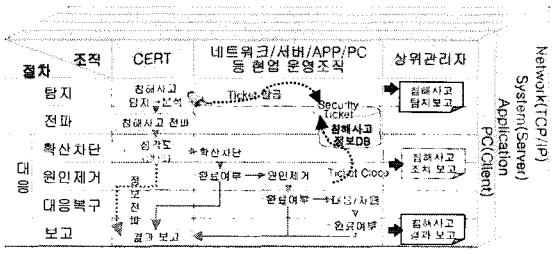


그림 3. 3차원 구조의 침해사고 대응모델

Fig. 3. Security Incident Response model of third dimension structure

3.1. 침해사고 대응체계의 요구사항 분석

3.1.1 위협요소 분석

기존에 연구된 침해사고 대응절차의 위협요소는 침해사고 대응을 단지 기술적인 문제로만 인식하는 1차원적 접근 시도에 근본적인 문제요소가 있다. KISA의 침해사고 대응절차와 CERT/CC의 침해사고 대응 모델 등 대부분의 침해사고 대응체계가 기술적인 대응절차 즉, 프로세스를 중심으로 되어있다[4,5,11,12]. 그러나 실제 침해사고 대응은 네트워크 측면, 시스템 측면, Application 측면, 사용자 PC 측면에서 각 업무 담당자가 책임 있게 조치하거나, CERT 조직과 상호 협조하는 등의 복합적인 대응이 필요하다. 그러나 기존 모델에서 제시하는 기술 중심의 대응절차는 조치를 수행하는 업무 담당자나 대상 시스템의 특성을 고려하지 않았기 때문에 침해사고 대응에 대한 책임과 역할이 불분명하여 책임회피, 지연 등 효과적인 침해사고 대응을 어렵게 하는 위협요소가 되고 있다. 또한 침해사고 대응의 전 과정이 연속성 있게 관리되지 않아 대응의 완전성을 확인하기 어려우며, 침해사고가 대상 정보시스템에 미치는 영향을 파악하기 어려운 점 등의 위협요소가 존재한다.

3.1.2 공격요소 분석

일반적인 침해사고 공격은 피해유형과 공격기법에 따라 해킹, 스캐닝, 웜, 바이러스 및 기타로 분류한다[3]. 이와 같은 분류 기준은 완전하게 정의되어 있거나 고정된 것이 아니다. 사이버 침해공격은 계속해서 새로운 유형으로 발전하고 있기 때문에, 다양한 침해사고 유형 중 가장 빈번히 발생하고 그 피해정도가 큰 유형들을 기준으로 주기적으로 공격요소를 검토하여 개정하는 것이 바람직하다. 공격요소 분석은 국가정보원과 정보통신부에서 발간한 "2006 국가정보보호 백서"를 참조하여 표 3의 유형으로 구분하고, 각 공격요소별로 주요 영향을 받는 정보자산을 추가하여 공격요소를 분석 하였다.

표 3. 침해사고 대응에 대한 공격요소

Table 3. Attack Element about Security Incident Response

공격요소	공격종류	대상 정보자산
해킹	OWASP 10대 취약점 등 해킹공격 패턴명	서버, App
스캐닝	단순 스캐닝, 웹 스캐닝, 취약점 스캐닝	서버, N/W
웜/바이러스	웜, 바이러스, 트로이잔, 악성코드, 애드웨어	PC, N/W
기타	비정상행위 행위탐지 신고 등	-

3.1.3 대응요소 분석

대응요소는 침해사고 대응 및 관리의 핵심사항으로 국내 민간부문에 영향을 미치는 KISA의 침해사고 단계별 처리 절차[4,5]와 NIST/SAN 모델의 침해사고 Life cycle의 요소[6,8,9]를 결합하여 확산차단, 원인제거, 복구/지원으로 대응요소를 세분화하여 구성하였다. 확산차단은 스캐닝 및 해킹공격 시도를 네트워크 단에서 차단하는 것을 포함하여 웜/바이러스의 확산시도 등을 차단하는 1차 대응하는 요소이다. 원인제거는 취약점 제거, 사용하지 않는 서비스 제거, 보안패치 적용 등 침해공격 시도의 직접적인 원인이 되는 취약점을 제거하거나 보완하는 2차 대응 요소이다. 대응/지원은 침해공격으로 인하여 실제 피해나 손실이 발생한 경우로, 피해 영향에 대한 정밀분석과 공격 전이를 목적으로 하는 백도어 설치유무의 확인 등 상세한 분석지원과 조심스러운 서비스 복구를 포함하는 3차 대응요소이다.

3.2 Security Ticket 기반의 침해사고 관리시스템 설계

Security Ticket 기반의 침해사고 관리시스템은 효과적인 침해사고 대응과 Security Ticket을 활용한 침해사고 대응결과의 계량화를 목적으로 침해사고 대응절차를 시스템화한 것이다. Security Ticket은 발생한 침해사고를 유일하게 구분하는 식별자로 본 논문에서 제안하는 요소이다.

3.2.1 침해사고 대응절차 설계

제안하는 Security Ticket 기반 침해사고 대응절차는 탐지, 전파, 대응, 보고의 총 4단계로 구성된다. 첫 번째 탐지는 Firewall[14,15], IDS, IPS 등의 보안시스템에서 탐지하는 이벤트와 네트워크 접속지연, 서버 오동작, PC 이상동작 등 내·외부에서 발생하는 이상 징후에 대한 신고 접수를 포함한다. 두 번째 전파는 탐지된 침해사고에 대한 실제대응을 위해 Application, 네트워크, 서버, PC 등 현업 관리 담당자에게 침해사고 조치를 이관하는 것을 포함한다. 전파는 발생한 침해사고를 전파한다. 침해사고 전파는 침해사고 발생 내역을 6하 원칙에 따라 작성하며, 침해사고 대응을 위한 기술적 조치사항을 포함한 보고서 형태로 전파하여야

한다. 세 번째 대응은 침해사고로 인한 피해와 영향, 공격의 삼각성에 따라서 확산차단, 원인제거, 대응/지원으로 대응요소를 구성하였다. 마지막 보고는 침해사고 발생원인과 대응내역, 그리고 재발방지를 위한 대책수립과 대책적용의 긴급성 등을 포함하며 최종적으로 조치가 완료되었음을 확인하는 것이다.

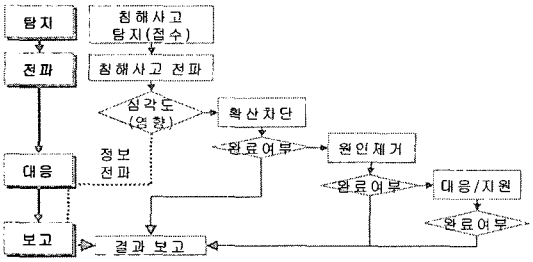


그림 4 침해사고 대응절차

Fig. 4. Procedure of Security Incident Response

침해사고 대응절차의 효율적인 운영과 침해사고에 대한 효과적인 대응을 위해서는 체계적으로 정립된 침해사고 대응절차 이외에 실제 업무를 수행하는 조직 간의 역할과 책임을 분명하게 정의하는 것이 중요하다. 침해사고에 대한 총괄적인 책임은 CERT 조직에 있지만, 침해사고 대응에 대한 책임은 정보시스템의 관리 권한을 가지고 있는 현업 운영조직에서 책임을 가져야 한다. CERT는 발생한 침해사고에 대한 내용, 피해, 대응방법 등의 필요한 정보를 현업 운영조직에 제공해야 하며, 원활한 조치를 위한 기술지원과 자문을 수행해야 한다. 침해사고 대응에 대한 1차 보고는 현업 조직의 책임이며, CERT는 대응의 완전성과 재발방지 대책 등을 포함한 최종 보고에 대한 책임을 갖는다.

표 4. 침해사고 대응의 역할과 책임

Table 4. Role and Responsibility for Security Incident Response

단계	담당조직	역할과 책임
탐지	CERT	침해사고 탐지에 대한 모든 Ownership
전파	CERT	침해사고 전파에 대한 모든 Ownership
대응	현업/CERT	침해사고 조치/CERT는 대응지원
보고	현업/CERT	초지결과 보고/전체 침해사고 대응결과 보고

3.2.2 침해사고 관리시스템 구성도

Security Ticket 기반의 침해사고 관리시스템 구성은 기존에 조직에서 운영하고 있는 Firewall, IDS, IPS 등의 보안시스템을 기반으로 구성한다. 통합보안관리시스템(ESM)은 필수요소가 아니라 효율적 관리를 위한 지원요소이다. 그리고 내/외부로부터 신고 되는 침해사고는 CERT 담당자가 수동으로 입력하는 것으로 구성한다. 침해사고 관리시스템 구성의 핵심요소는 단위 보안시스템의 완벽한 구성이 아니라 조직의 운영환경에 맞는 침해사고 대응절차와 대응조직 간의 역할과 책임이 명확하게 정의되어 관리할 수 있는가가 중요한 요소이다.

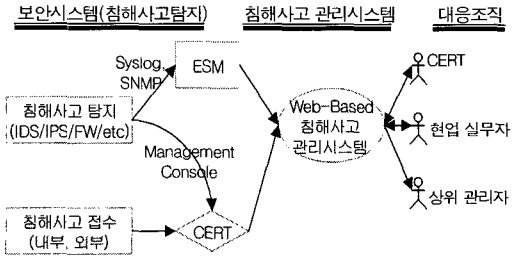


그림 5. 침해사고관리시스템 구성 개념도

Fig. 5. Schematic diagram for CERT Management System

그리고 침해사고 관리시스템의 구현은 제한 없는 접근성을 보장하기 위하여 표준 Web 환경으로 구현한다. 침해사고 관리시스템 자체의 보안 문제는 CERT, 현업 실무자, 상위 관리자의 역할에 따라 역할기반 접근통제(Role based Access control) 메커니즘에 따른 통제를 적용하여[16], CERT는 Administrator 권한을 가지며, 그 외는 사용자는 User 권한을 갖는다. 인증 수단은 ID/Password 기반 또는 인증서 기반의 PKI 인증체계로 구현할 수 있다. 향후에는 기타 보안정보를 콘텐츠를 추가하여 일반사용자와 보안정보를 공유하는 보안정보 공유시스템으로 확장할 수 있다.

3.2.3 Security Ticket 기반의 침해사고 관리시스템 설계

본 논문에서 제안하는 Security Ticket 기반의 침해사고 관리시스템은 탐지, 전파, 대응, 보고로 구성된 4단계 침해사고 대응절차와 침해사고를 유일하게 식별하여 침해사고 대응의 연속성을 보장하고 대응결과를 계량화하여 측정할 수 있는 Security Ticket을 시스템화하는 방식으로 설계하였다. Security Ticket은 침해사고를 탐지한 시점에 생성되며, 대응이 완료되는 시점에 Ticket이 종료된다. 또한 모든 침해사고 대응정보는 Security Ticket을 기준으로 관리된다. 침해사고 대응단계별 Security Ticket과 침해사고 정보의 흐름은 아래 그림 6과 같다.

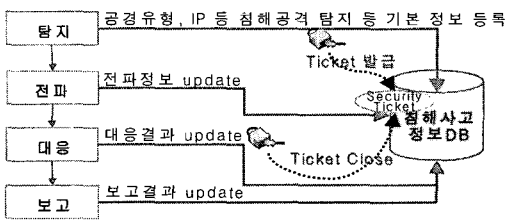


그림 6. Security Ticket과 침해사고 정보의 흐름

Fig. 6. Flowchart of Security Ticket & Security Incident Information

Security Ticket 기반의 침해사고 관리시스템의 설계요소는 Ticket Number를 Primary Key로 하는 탐지요소와 침해사고 대응절차의 각 단계별 Activity 들을 관리요소로 정의하여 설계하였다. 탐지요소는 침해사고 탐지 일자와 시간, 그리고 Security Ticket 번호와 발행시간으로 구성된다.

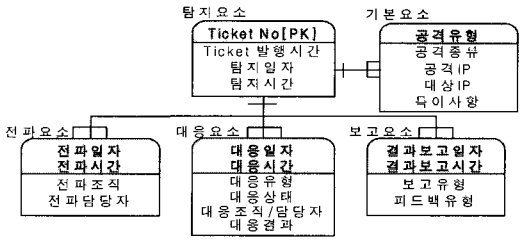


그림 7. 침해사고 관리시스템 설계 요소

Fig. 7. Design Element for CERT Management System

기본요소는 Security Ticket과 직접 관련되지 않는 일반적인 침해사고 관리요소로 발생한 침해사고에 대한 일반정보로 침해사고 공격유형, 공격종류, 공격자 및 공격대상 IP, 심각도, 침해사고에 대한 특이사항을 구성요소로 한다. 공격유형은 3.1,2 절에서 기술한 공격요소이며, 공격종류는 실제 공격코드 명칭이다. 전파요소는 실제조치를 위해 현업조직에 전파한 전파일자와 시간, 전파조직과 담당자, 조치를 위한 기술적 조치방안을 포함한다. 대응요소는 침해사고 대응 유형 및 상태, 대응조직, 대응일자와 시간, 그리고 대응결과로 구성된다. 대응유형은 확산차단, 원인제거, 복구/지원으로 구분하며, 대응상태는 차단완료, 조치완료, 자연소멸로 구분한다. 보고요소는 침해사고 대응이 완료된 일자와 시간, 침해사고 재발방지를 위한 추가대책, 담당 조직 간의 피드백 및 사례학습 등을 포함한다. 침해사고 대응절차별 대응조직, 대응 업무, 시스템 요소는 그림8과 같다.

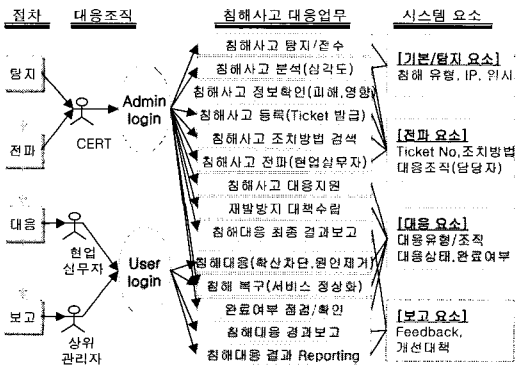


그림 8. 침해사고 관리시스템 기능 및 요소간의 연관성

Fig. 8. Function and relation between element for CERT Management System

3.3 Security Ticket기반의 침해사고 관리방안설계

3.3.1 Security Ticket 기반의 침해사고 관리요소

침해사고 관리요소는 침해사고 대응절차 및 침해사고 관리시스템에 따라 수행된 침해사고 대응결과를 측정하여 관리하기 위한 보안관리 지표이다. 관리요소의 구성은 침해사고 대응절차의 각 단계별 시스템 요소를 조합하여 관리요소를 도출하였다.

표 5. 침해사고 관리 요소

Table 5. Element for Security Incident Management

단계	시스템 요소	관리방안 및 보안관리 지표
기본	공격유형, 공격종류 공격 IP, 대상 IP, 심각도,	월별/분기별/연도별 발생빈도 통계 (침해사고 발생 건수, 유형 공격대상, 공격자, 심각도 등)
탐지	탐지일자, 탐지시간, Security Ticket No, 발생시간	탐지소요시간 (탐지의 신속성 및 정확성)
전파	전파일자, 전파시간 전파조직, 전파담당자	전파소요시간, 전파자별 통계 침해 유형별 탐지 소요시간
대응	대응 일자/시간/유형/형태 대응 조직/담당자, 대응결과, 대응내역	대응 소요시간(조직, 유형, 등) 대응조직 업무량 및 대응수준 대응결과 및 내역 통계
보고	결과보고 일자/시간 보고내역, 보고유형	피드백, 사례학습 등

3.3.2 Security Ticket 기반의 침해사고 관리방안

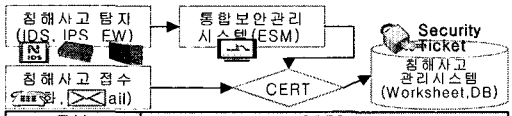
조직의 프로세스 능력성숙도를 나타내는 능력 성숙도 모델(CMM, Capability Maturity Model)은 초기단계, 반복단계, 정의단계, 관리단계, 최적화단계의 총 5단계로 구성된다[17]. 초기 CERT 조직은 일반적으로 반복단계에 해당하며, 체계화된 절차에 따라 정형화된 프로세스로 침해사고를 관리하는 조직은 정의단계에 해당한다. 본 논문에서 제안하는 Security Ticket 기반의 침해사고 관리방안은 CMM 4단계인 관리단계의 프로세스 요구사항인 "수행결과의 계량화를 통한 지속적인 개선"을 목표로, 침해사고 대응절차의 각 단계별로 실행결과를 계량화하여 관리할 수 있다.

기본요소는 Security Ticket과 직접 관련되지 않지만 일반적인 관리내역으로 침해사고 유형, 공격대상, 공격자, 발생 건 수 등에 대한 빈도를 관리하여 침해사고의 일반현황을 관리한다. Security Ticket으로 관리하는 탐지/전파/대응요소의 시간을 이용하여 각 단계별 소요시간을 관리함으로써 침해사고 대응의 신속성과 정확성을 관리한다. 그리고 침해사고 발생건수와 소요시간을 비교하여 대응조직의 능력수준과 업무량을 파악할 수 도 있다. 보고요소는 재발방지 대책의 유효성을 검증하기 위해 유사/동일 유형의 침해사고 발생빈도를 관리하는 것으로 관리방안을 설계하였다.

Ⅳ. Security Ticket 기반의 침해사고 관리시스템 실험 및 결과

4.1. 침해사고 관리시스템 실험 환경

본 논문에서 제안하는 Security Ticket 기반의 침해사고 관리시스템의 실험환경은 Firewall, IDS, IPS와 같은 단위시스템에서 탐지한 보안 로그와 이를 통합 관리하는 통합보안관리시스템(ESM)에서 전송된 보안 이벤트들 중 CERT 담당자가 침해사고로 인지하여 대응하는 침해사고 대응내역을 실험 환경으로 구성 하였다. 실험 환경의 구성과 실험 시스템 내역은 그림 9와 같다.



구분	SPEC
IDS/IPS	ISS Real Secure7.0/ISS Proventia G200
Firewall	Absolute Firewall
ESM	ISS社 Site-Protector
관리시스템	Win 2000, LG-IBM x-Series 360

그림 9. 침해사고 관리시스템 실험환경

Fig. 9. Experiment environment for CERT Management System

4.2 Security Ticket기반의 침해사고 공격실험

Security Ticket 기반의 침해사고 공격실험에 사용된 침해사고 대응절차의 운영사례는 그림 10과 같다. 모든 대응절차의 Activity들이 Security Ticket에 의해 관리되며, 침해사고 대응과 관련된 IT 운영조직 및 담당자와 연계되어 있는 것이 특징이다. 또한 각각의 침해사고가 Network, Application, Server, PC 등의 정보자산에 미치는 영향을 파악하기 위한 영향 관계를 가지고 있다.

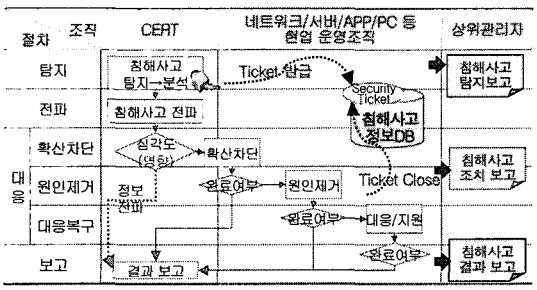


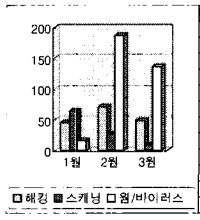
그림 10. Security Ticket 기반의 침해사고 대응 관리 운영사례

Fig. 10. Experiment example about CERT Management based Security Ticket

4.3. Security Ticket기반의 침해사고 대응결과

침해사고 대응에 대한 실험결과는 본 논문에서 설계한 침해사고 대응절차와 관리시스템의 설계요소와 관리요소를 조합하여 일반관리, 대응시간 관리, 조직별 대응능력 관리, 정보자산 영향관리로 나누어 실험결과를 기술한다.

침해사고에 대한 일반관리 대응결과는 Security Ticket을 적용하지 않아도 관리할 수 있는 일반적인 침해사고 관리 요소이지만, 침해사고 발생내역에 대한 통계분석을 위해 공격유형, 공격종류, 공격자(해커), 공격을 받는 대상시스템 등에 대한 통계분석을 위해 사용한다. 이를 통해 조직에 발생하는 침해사고의 유형, 종류 등에 대한 빈도를 분석할 수 있으나, 예측과 개선을 목적으로 정량화하기에는 한계를 가지고 있다.

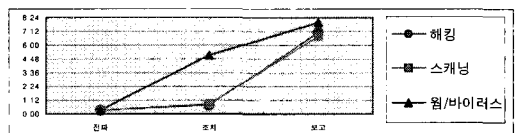


공격 종류	1	2	3	계
악성코드 유포도메인 탐지	1	5	7	13
FTP Brute force	16	18	5	39
SQL Brute force	25	37	23	85
SQL Injection	4	7	5	16
SSH Brute force	0	4	3	7
Telnet 관련 취약점 공격탐지	0	0	4	4
Telnet Brute force	0	0	2	2
Spammer	1	0	0	1
Web 취약점 Scanning 탐지	15	27	10	52
Email 웜	9	19	4	31
IPC 웜	55	170	132	357
계	126	286	195	607

그림 11. 일반관리 요소에 대한 실험결과

Fig. 11. Experiment result about general Management Element

Security Ticket을 적용한 침해사고 관리를 통해 각 대응단계별 소요시간을 측정함으로써, 침해사고 대응의 신속성과 정확성을 분석할 수 있다. 실험결과는 3단계(전파→대응)에 해킹, 스캐닝에 대한 대응보다 웜/바이러스의 대응에 평균 5기간이 소요되는 이슈를 발견하였다. 이에 대한 문제점을 대응절차 즉 프로세스 측면, 조직측면, 담당자 측면, 솔루션 또는 기술 측면에서의 분석을 통해 이슈화된 보안 문제점에 대한 개선 계획을 수립하고, 개선 후의 결과를 예측할 수 있다. 이것은 대응 결과를 정량적으로 측정하여 관리하며, 그 결과를 예측하여 관리하는 CMM 레벨4인 관리단계의 특징을 반영할 수 있는 실행결과 이다.



공격유형	대응조직/자산	전파	조치	보고	계
해킹	Network, System, App	0:19	0:45	7:03	2:42
스캐닝	Network, System	0:18	0:54	6:43	2:38
웜/바이러스	PC	0:19	5:07	7:58	4:28
전체 평균 시간		0:18	2:15	7:15	3:16

그림 12 대응시간 측정결과

Fig. 11. Experiment Result about Response time of Security Incident Responding Step

침해사고에 대한 신속한 대응뿐 아니라 정확한 대응에 대한 결과 측정은 전파, 대응, 보고 단계의 소요시간을 분석함으로써 침해사고 대응 단계별 정확성을 분석할 수 있다. 그리고 각 단계별 소요시간은 침해사고 대응과 관련된 각 조직의 업무량, 업무수행 능력 등을 측정하는 자료로도 활용이 가능하다.

또한 실제 공격에 사용되는 공격 종류별로 공격빈도와 대응시간을 측정·비교함으로써, 공격받는 정보시스템의 취약점 유무와 취약점 보안 대책 적용의 문제점을 도출하고 이에 대한 보안개선 계획을 수립할 수 있다.

공격 유형	공격 종류	1	2	3	평
해킹	악성코드 유포도메인 탐지	0: 13	0: 39	0: 23	0: 25
	FTP Brut ef or ce	0: 55	0: 43	0: 50	0: 49
	SQL Brut ef or ce	0: 37	0: 54	0: 43	0: 44
	SQL Inj ect i on	1: 07	0: 36	0: 19	0: 40
	SSH Brut ef or ce	0: 00	0: 24	1: 46	1: 05
	Tel net 취약점 공격탐지	0: 00	0: 00	0: 58	0: 58
	Tel net Brut ef or ce	0: 00	0: 00	1: 11	1: 11
스캐닝	Spammer	1: 27	0: 00	0: 00	1: 27
	Web 취약점 Scanni ng 탐지	1: 29	0: 44	0: 36	0: 56
웜/바이러스	Email 웜	2: 02	2: 42	2: 35	2: 26
	I RC 웜	3: 46	5: 08	7: 04	5: 19

그림 13 공격 종류별 대응시간 분석

Fig. 13. Experiment Result about Response Time of Attack Pattern

침해사고가 정보자산에 미치는 영향도는 각 대상 시스템별 발생 빈도를 기준으로 분석하였다. 실험결과 사용자 PC에 매월 웜/바이러스 감염이 다수 발생하였고, 백신은 적용되어 있지만 패치 적용률이 낮은 문제점을 찾을 수 있었다. 또한 한번 감염 후 치료 이후에도 재차 감염되는 동일 감염 PC가 다수 존재하여 사용자의 의식개선이 필요한 것으로 분석되었다. 따라서 패치관련 솔루션의 도입과 사용자의 보안인식을 위한 보안교육의 필요성을 찾아내었다. 그러나 정보자산 영향도는 정보자산의 중요도(자산 가치), 피해영향 등에 대한 추가 정보가 필요하며, 단순 발생 빈도이외에 위협동향을 반영하여 분석하여야 한다.

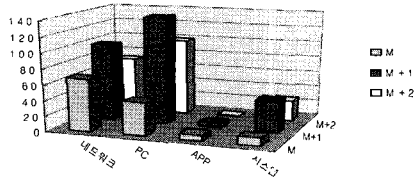


그림 14 대상 시스템별 측정결과

Fig. 14. Experiment Result of Target Information System

4.4. 일반적인 침해사고대응 관리와 Security Ticket 기반의 침해사고 관리에 대한 비교

본 논문에서 제안한 Security Ticket 기반의 침해사고 관리와 기존의 일반적인 침해사고 관리에 대한 비교 결과는 아래 표 6과 같다. Security Ticket을 적용한 정량적 침해사고 관리의 주요 개선결과는 대응 소요시간 관리를 통해 신속한 침해사고 대응을 통제할 수 있으며, 각 단계별 소요시간 관리를 통해 침해사고 대응의 정확성을 분석할 수 있다. 또한 침해사고 대응 조직의 대응능력과 정보자산의 영향을 추가로 고려하여 문제점을 분석하여 개선대책을 수립할 수 있다.

표 6. 일반대응과 Security Ticket 기반의 공격대응 비교결과

Table 6. Comparison Result of Security Ticket base CERT Management and General Security Incident Response

침해사고 구분	일반적인 침해사고 관리	Security Ticket 기반의 침해사고 관리	비교
일반현황 관리	- 침해유형별/종류별 발생현황 - 침해공격자/대상별 Top list - 월별/분기별 발생 빈도	동일	동일
대응시간 관리	없음	단계별 대응소요 시간관리 공격유형별/종류별 시간관리	개선
관련조직 대응능력	없음	단계별 대응소요 시간관리 (단계별 대응조직 R&R)	개선
정보자산 영향도	없음	공격받는 자산 유형별 빈도 (네트워크, 서버, App, PC)	개선

V. 결론 및 향후 연구

본 논문에서는 Security Ticket 기반의 침해사고 관리시스템과 관리방안을 설계하여 실험을 수행하였다.

실험결과 일반기업 환경에 적합한 침해사고 대응절차의 유효성을 확인하였고, 정보보호 업무를 전담하는 CERT 조직 이외에도 IT 운영부서의 중요성을 도출하여 침해사고 대응절차에 반영하였다. 그리고 침해사고 대응결과를 계량화하여 측정·분석함으로써 문제점을 찾아 지속적으로 개선함으로써 조직의 정보보호 수준을 높일 수 있다. 그리고 계량화를 통한 정량적 관리는 프로세스 성숙도 모델에서 제시하는 CMM 레벨4의 요구사항을 준용 할 수 있도록 설계함으로써 기존 CERT를 운영하는 조직에서는 침해사고 대응 서비스의 품질을 향상할 수 있는 방안을 제시하였다.

향후 연구과제는 침해사고 대응활동이 예측 가능한 수준으로 정량화 할 수 있는 CMM 레벨 4의 요구사항을 충족할 수 있는 관리방안에 대한 세부 연구를 통해, 보안서비스 수준관리(SLA), IT 아웃소싱 표준(ISO20000) 및 정보보호 관리 표준(ISO27001) 등 국제 표준과 연계할 수 있는 보안관리 방법에 대한 추가 연구가 필요하다.

참고문헌

[1] 기업사이버보안 전담조직(CERT) 구축 활성화 방안, 정보통신부, 2003.

[2] 기업정보보호체계 구축 지원계획, 정보통신부, 2004.

[3] 국가정보보호백서, 국가정보원/정보통신부, 2006.

[4] 정태명, 침해사고대응팀의 기능과 역할, 침해사고대응팀(CERT) 구축·운영 과정 교육(KISA), 2002.

[5] 윤승노, CERT 구축요소 및 제공서비스, 한국정보보호진흥원 대응협력팀, 2004.

[6] NIST, Computer Security Incident Handling Guide(NIST Special Publication 800-61), 2004.

[7] Moira J. West-Brown, Handbook for Computer Security Incident Response Teams(CSIRTs), CMU/SEI, SEI-2003-HB-002, 2003

[8] Ajoy Kumar, CSIRT Framework and Models, <http://www.securitydocs. com/library/2964>, 2005 .

[9] FIRST, "Forum of Incident Response and Security Teams(FIRST) Operational Framework." <http:// ww w.first.org/about/policies/op-framework/>, 2006

[10] Brownlee, N. & Guttman, E. Expectations for CSIRT(IETF RTC 2350, Best Current Practice). <http://www.faqs.org/rfcs/rfc2350.html>, 1998.

[11] CERT/Coordination Center, "CSIRT Frequently Asked Questions." Pittsburgh, Pa.: CMU/SEI, 2007.

[12] CERT/CC, http://www.certcc.org, 2007.

[13] 인터넷침해사고대응지원센터, http://www.krcert.or.kr, 2007.

[14] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[15] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, pp1-10, 2006. 9. 30.

[16] 김정재, 이경석, 전문석, "시큐리티 에이전트를 이용한 사용자 인증과 DRM 보안 시스템 설계," 정보처리학회논문지, p.973-980, 2005.

[17] 양해술, 안유환, "프로세스 성숙도 모델 CMM의 적용 평가 방법", 한국정보처리학회 학술발표논문집(추계), p.653-658, 1997.

저 자 소 개

김 선 태

2001년 숭실대학교 정보과학대학원 정보통신학과(공학석사)

2007년 숭실대학교 컴퓨터학과(박사과정수료)

1999년 ~ 2003년 Securesoft 컨설팅사업본부 책임컨설턴트

2003년 ~ 현재 인포섹(주) 전략 컨설팅사업본부 수석컨설턴트

〈관심분야〉 CERT, Forensics, SLA, CoBIT ERM(Enterprise Risk Management)

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)

2004년 숭실대학교 컴퓨터학과(공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

2007년 호서대학교 벤처전문대학원 조교수

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, VoIP보안, 이동통신 및 WiBro 보안, Cyber Reality

전 문 석

1981년 숭실대학교 전자계산학과(공학사)

1986년 University of Maryland Computer Science(공학석사)

1989년 University of Maryland Computer Science(공학박사)

1989년 Morgan State University 조교수

현 재 숭실대학교 정교수

〈관심 분야〉 전자상거래 보안, 인터넷 보안, 멀티미디어 보안