情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

보안관제 업무에 대한 평가지표 개발 연구

이 현 도,† 이 상 진‡
고려대학교 정보보호대학원

A Study on development of evaluation indicators on the Managed Security Service(MSS)

Hyundo Lee,† Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

현재 많은 중앙행정기관, 지방자차단체 및 공공기관, 포탈 및 일반기업, 금융권 등은 사이버안전센터를 구축하여 운영하고 있다. 기관 입장에서 보안관제 업무는 이제 구축 보다는 효과적인 운영이 중요시되고 있다. 하지만 보안관제 업무를 평가할 수 있는 지표 및 제도가 없는 상황에서 사이버안전센터의 전체적 업무수행 수준을 파악할 수 없고 사이버안전센터별 강점과 약점을 도출하기도 어렵다. 이에 따라 본 논문은 보안관제 업무평가를 위한 지표를 개발함으로서 사이버안전센터의 업무수행 수준파악 및 향후 발전 방향 모색에 기여함을 목적으로 한다. 또한 기관의 정보보안 관리실태 평가를 수행함에 있어 보안관제 업무평가를 반영한다면 기관의 보안수준을 정확히 측정하여 체계적인 보안대책을 수립할 수 있다.

ABSTRACT

Currently, Many Cyber Security Centers(CSC) are established and being operated in our country. But, in the absence of indicators to evaluate activities of the Managed Security Service(MSS), We can't identify the CSC's level of overall job performance. Therefore, we can't derive strengths and weaknesses from the CSC. From these reasons, The purpose of this research is to develop an objective indicator to evaluate activities of the MSS. I studied both international and domestic Information Security Management System(ISMS) as related standards(ISO/IEC 27001, G-ISMS). Moreover, I analysed the NIST Computer Security Incident Handing Guide and the Incident Management Capability Metrics(IMCM) of Carnegie Mellon Software Engineering Institute(SEI). The implications for this analysis and domestic hands-on experience are reflected in the research. So I developed 10 evaluation domains and 62 detail evaluation items. This research will contribute to our understanding the level of the CSC's job performance.

Keywords: Managed Security Service, Evaluation indicators

I. 서 론

사이버공격이 점차 일반 정보시스템(IT) 뿐만 아니라 전력, 원자력, 금융 등 사회기반시설 제어시스템을 대상으로 그 범위가 넓어지고 공격수법 또한 지능화되어 상당한 수준으로 발전되고 있다. 정보시스템의 도움 없이는 국가체제의 원활한 운영, 관리, 통제가 어려운 현실에서 효과적으로 사이버공격에 대응할 수 있도록 국가차원의 보안체계가 필요한 때이다. 이에 따라 정부는 종합적이고 효과적인 사이버공격 방어체제를 구현하기 위해 각 공공분야(에너지, 국방, 교육

접수일(2012년 06월 11일), 게재확정일(2012년 10월 08일)
† 주저자, hdlee@kdn.com
‡ 교신저자, sangjin@korea.ac.kr

등) 대상으로 사이버 보안관제센터를 설치·운영·위탁토록 '국가사이버안전관리규정'에서 정하고 있고, 민간분야도 개인정보유출방지, 산업기밀보호 등 기관의 사업특성에 맞는 정보보안을 강화하고 있다[10][11]. 이렇듯 많은 공공분야 기관 및 중요 민간기관이 보안관제 서비스를 받고 있으나, 기준이 되는 보안관제 업무평가 지표 및 제도가 부재하여 업무 관리실태를 파악할 수 없는 실정이다. 보안관제 업무의 효과적인 발전을 위해서 수행 업무의 평가를 통한 센터의 장·단점 파악은 반드시 필요하다. 또한 기관의 정보보안 관리실태를 평가하면서 각 기관의 사이버안전센터에 대한 업무평가는 수행하지 않는다[4][8]. 대다수 사이버안전센터가 구축·운영되고 있는 상황에서 해당 기관 사이버안전센터의 업무평가가 반영된다면 좀 더 의미있는 평가가 될 것이다. 따라서 본 논문은 보안관제 업무가 체계적으로 진행되고 있는지를 평가할 수 있는 방안을 제시한다.

II. 보안관제 업무현황

2.1 보안관제 업무내역

보안관제 업무란 관제 대상기관의 정보 기술(IT) 자원을 사이버공격으로부터 보호하기 위하여 보안 이벤트 및 로그 등을 중앙 관제 센터에서 실시간으로 감시 및 분석, 대응하는 업무이다. 정보 자산에 대한 보안은 전문 집단이 수행하고, 관제 대상기관은 기관의 핵심 역량에 집중할 수 있는 선진화된 보안 서비스이다. 이것은 정보공유분석센터(ISAC, Information Sharing & Analysis Center)와 같은 의미를 갖고 있다. ISAC은 유사 업무 분야별로 해킹이나 컴퓨터 바이러스 등 사이버테러와 정보 침해사고에 대해 효과적으로 공동 대응하기 위한 서비스 체계로 사이버테러 취약점과 침해요인, 대응방안에 관한 정보를 관제 대상기관에 제공하고 침해사고가 나면 실시간 경보와 분석업무를 수행하게 된다. 아울러 분야별 여건을 고려, 침해사고 대응체계 구성 및 운영, 정보통신기반시설 보호, 정보보호관련 교육과 훈련 서비스 등을 부가적으로 제공한다. 이를 통해 관제 대상기관간 정보보호를 공동대처함으로써 전문조직 별도 운영에 따른 업무 및 비용을 경감할 수 있다. 또한 정보수집 및 적용, 기술 확보, 인력 및 조직 운영 등 모든 요소들에 대한 문제를 줄일 수 있다[3][18]. 국내의 경우, 외국의 경우와 달리 민·관·군을 구별하여 센터를 운용하고 있으며 대다수 중앙부처가 점차 사이버안전센터를 확대하고 있다[1][2]. 보안관제의 정의에 근거해 관제의 주요 역할을 살펴보면 [표 1]과 같다[5].

[표 1] 보안관제의 주요 역할

항목	역할
보안시스템 통합관리	- 이기종에 대한 Agent를 통한 모니터링 및 관리 ex) 침입탐지/차단시스템, 네트워크, 자원관리 등
일관성 있는 정책구현	- 중앙에서 일관된 정책적용을 통합관리로 보안장비에 대한 위험요소를 최소화
신속한 대응처리	- 침해사고에 대한 사전 예방활동 강화 (모니터링, 사전대응, 효과적인 정책적용 등) - 24X365일 실시간 감시, 장애처리, 업무중단에 대한 위협요소 감소
최적의 보안체계 운영	- 정보자산에 대한 효과적인 방안을 마련할 수 있는 환경 구성

다음으로 보안관제의 구성요소를 살펴보면 크게 3가지로 구분할 수 있다. 첫째로 네트워크나 시스템에 설치된 에이전트이다. 이것은 각종 보안장비 및 서버, 네트워크에 설치하여 해당 시스템에 맞게 설정된 로그정보를 실시간 전송하여 중앙관제센터에서 각종 로그를 쉽게 모니터링하고 분석할 수 있도록 정보를 제공해 주는 것이다. 둘째로는 정보수집 서버가 있다. 정보수집 서버는 각 에이전트에서 보내진 각종 정보를 수집하고 분석 처리하여 DB에 저장하는 역할을 한다. 여기서 에이전트에 대한 Health Check를 통한 모니터링과 분석에 필요한 리포팅 소스를 제공한다. 마지막으로 통합관제용 시스템이다. 여기서 주 역할은 각종 이벤트 로그에 대한 분석을 주로 수행한다. 다양하게 수집되고 분석된 정보를 종합하고 상황을 분석하여 관제요원들이 신속하게 정보를 파악할 수 있도록 최적의 정보를 제공·반영하며, 로그분석에 대한 결과를 주기적으로 저장한다[3][17][18].

2.2 보안관제 업무유형

일반적으로 보안관제 업무유형은 원격관제, 파견관제 및 자체관제로 분류된다. 원격관제는 관제서비스 업체에서 보안관제에 필요한 관제시스템을 구비하고 대상기관의 침입차단시스템 등 보안장비 중심의 보안이벤트를 중점적으로 상시 모니터링하고 침해사고 발생 시 긴급 출동하여 대응 조치하는 서비스이며, 파견

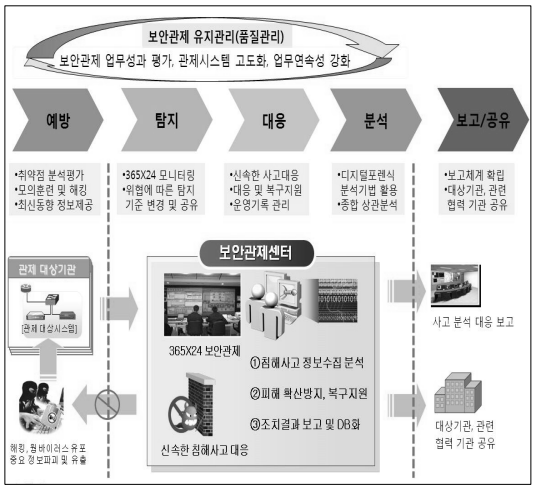
〔표 2〕 보안관제 업무유형

업무유형	주요내용	대상기관
원격관제	- 일부 단위 보안시스템의 운영 및 관리를 위탁하는 방식 - 통합보안 관제시스템 및 관제인력이 원격에 위치함 - 제한적인 범위의 보안 시스템 위탁	일반기업 포탈업체
파견관제	- 자체 구축한 보안관제시스템 운영 및 관리를 위탁하는 방식 - 전문인력이 대상기관에 파견되어 관제업무 수행 - 조직전반 및 산하기관 보안관제 체제 구축 수행	공공분야 금융권
자체관제	- 자체 보안관제시스템의 운영 및 관리를 자체적으로 수행 - 기관 자체 정규직, 계약직 보안인력을 통한 관제업무 수행	국정원, 경찰청 등 대규모 통신사

관제는 관제 대상기관이 자체적으로 보안관제시스템을 구축하고 보안관제 전문업체로부터 전문 인력을 파견 받아 관제업무를 수행하는 형태를 말한다. 주로 정보의 외부 유출 금지, 조직전반 및 산하기관 보안관제 체제를 구축하려는 공공분야 및 금융권 등이 이에 해당한다. 자체관제는 보안관제시스템 및 전문인력을 자체적으로 구축하고 운영하는 형태이다〔12〕〔13〕.

2.3 보안관제 업무프로세스

보안관제 업무에 대한 프로세스는 일반적으로 예방, 탐지, 분석, 대응, 보고 등으로 구분된다. 우선 예방은 세가지로 정의된다. 첫 번째 중요시스템, 네트워크 및 홈페이지 등의 취약점을 사전에 파악하여 침해사고를 예방하는 것이다. 두 번째 예·경보 서비스 부분이다. 사이버위협의 발생정보를 사전에 공지하여 방어토록하며, 최신 위협 및 해킹 등 보안동향 정보를 제공한다. 세 번째로 침입차단시스템, 침입탐지시스템 및 웹 방화벽 등 보안시스템에 대한 보안정책 및 시스템 자원의 최적화를 통해 효율적인 사이버공격 탐지를 지원하는 것이다.



〔그림 1〕 보안관제 업무프로세스

다음 탐지 부분은 보안시스템의 보안이벤트에 대한 24시간 X 365일 보안전문인력에 의한 실시간 감시 탐지를 의미한다. 분석 부분은 보안시스템 로그, 네트워크 패킷 및 다양한 보안이벤트 등을 종합적으로 상관분석하여 재발 방지 및 확산을 방지하기 위한 방안을 강구한다. 대응 부분은 비정상 네트워크 및 시스템에 대한 초기대응, 사이버공격 발생시 신속히 조치 대응하는 것을 의미한다. 보고 부분은 관제일지, 취약점 정보, 침해사고대응 분석보고서 등을 보고 및 관리하는 부분이다. 요약해서 정의하자면 보안관제 프로세스는 주요 관제서비스 대상 시스템에 대한 취약점 분석과 관제 대상기관 경영정책 유형에 따른 보안시스템 탐지 패턴 최적화를 통한 실시간 탐지, 분석, 대응 및 보고 업무를 수행하는 것이다〔13〕〔14〕〔15〕〔16〕.

2.4 보안관제센터 운영관리 보완점

대다수 공공분야 기관 및 중요 민간기관이 사이버안전센터를 구축하여 운영하고 있으나 기준이 되는 보안관제 업무평가 지표 및 제도가 부재하여 업무 관리실태를 파악할 수 없는 실정이다. 따라서 보안관제센터의 지속적인 발전을 위해서는 업무 관리실태 평가를 위한 기준 및 제도가 필요하다. 또한 정보보안 관리실태는 공공기관 대상으로 정보보호 업무에 대한 관리실태를 조사·평가하기 위해서 국정원 및 행정안전부 주관으로 시행되어왔다〔4〕〔8〕. 이것을 통해 기관의 보안수준을 측정하고 향상 대책을 수립할 수 있었다. 하지만 각 중앙행정기관 보안업무의 핵심인 보안관제센터가 대부분 구축된 상황에서 보안관제센터에 대한 업무 관리실태 평가를 실시하지 않고 전체적인 정보보안 관리실태를 측정하는 것은 부족한 측면이 있다.

III. 보안관제 업무평가 관련 표준 및 모델 연구

3.1 개요

보안관제 업무평가는 크게 두가지 부분으로 분류된다. 첫 번째는 보안관제 업무를 수행하기 위한 정책, 조직, 시스템 및 인력 관리부분인 보안관제 업무관리 부분이다. 이 부분에서는 보안관제 업무를 수행하는 사이버안전센터 같은 조직을 하나의 독립된 조직으로 간주하고 표준화된 정보보호관리체계(ISO/IEC 27001[20], G-ISMS[9])를 참고하여 관제에 필요한 정책과 조직, 시스템 및 인력에 대한 기술수준 관리 등의 평가항목을 살펴본다. 두 번째로 침해사고 관리부분이다. 이 부분은 보안관제 업무의 핵심 업무부분으로 침해사고에 대한 예방, 탐지, 분석, 대응, 보고 등으로 구분한다. 사이버 침해사고의 효율적인 관리를 위해 침해사고관리 문헌(SEI IMCM[21] 및 CSIRTS[17], NIST 문헌[18] 등)을 참고하여 취약점 분석평가 등 예방활동을 비롯하여 침해사고 탐지, 대응, 보안관제 서비스 품질 향상관리 등의 평가항목을 도출한다.

3.2 보안관제 업무관리 부분

국내·외 정보보호관리체계 표준인 ISO/IEC 27001과 G-ISMS(Government-Information Security Management System)를 참조하여 업무관리 부분의 평가항목을 연구한다. 우선 ISO/IEC 27001은 현재 정보보호 분야에서 가장 권위 있는 국제 인증 규격으로서 지난 2005년 10월 영국 표준인 BS7799를 기반으로 만들어진 ISO 17799를 새로운 국제 표준인 ISO 27001로 승격, 위험 관리와 보안 정책 자산 분류 등 11개 분야 133개 항목에 대한 규격을 담고 있다[19][20]. 두 번째로 전자정부 정보보호관리체계(G-ISMS)는 국내 전자정부 서비스의 안전성, 신뢰성 확보를 목표로 하여, 다양한 보안요구사항을 체계적으로 대응하고 지속적인 관리를 통해 정보보안 강화에 기여할 수 있도록 한다. 특히, G-ISMS는 ISO/IEC 27001의 규격에 맞추어 계획(Plan), 시행(Do), 점검(Check), 개선(Act) 등의 관리 사이클을 통해 지속적인 관리, 개선, 수준제고를 요구하고 있다. 또한, G-ISMS의 인증기준에 ISO/IEC 27001의 인증기준을 포함시켜 G-ISMS의 인증과 ISO/IEC 27001의 인증을 동시에 취득할 수 있는 기반도 마련하였다[6][9]. 그러나 이들 표준은 일반적인 기관의 정보보호관리실태에 대한 평가로서 보안관제 업무를 지원하고 관리할 수 있는 지표로 수정해야 된다. 특히, 일반기관과 달리 보안관제 조직 구성에 따른 평가항목이 수립되어야 하고, 인력관리 또한 보안관제 업무를 수행하기에 적합한 보안조치 및 개개인의 기술수준 관리가 포함되어야 된다. 가장 중요한 부분은 침해사고 관리 부분이다. 이 부분은 보안관제 업무 프로세스의 중심을 이룬다. 하지만 국내·외 표준 정보보호관리체계는 기관자체 내에서의 보안사고 관리를 의미하므로 이 부분은 별도의 기준으로 대체해야 된다.

3.3 침해사고 관리부분

보안관제 업무에 대한 핵심부분으로 SEI IM-CM[21]을 중심으로 참고한다. 이 Metrics는 침해사고 예방, 탐지, 대응 등 전반적인 컴퓨터 사고관리

[표 3] 보안관제 업무관리 부분 적용방안

G-ISMS 통제분야	ISO/IEC27001 통제분야	적용방안
정보보호 정책	보안정책	보안관제 정책 및 조직
정보보호 조직	정보보안조직	
자산관리	자산관리	※ '물리적보안'과 통합
인적보안	인원보안	보안관제 인력관리
물리적보안	물리적인 환경 보안	관제시스템 자산관리
통신 및 운영관리	통신과 운영 관리	관제시스템 운영관리
접근통제	접근통제	관제시스템 접근통제
정보시스템 요구사항, 개발 및 유지보수	정보시스템 구매, 개발 및 유지보수	※ 타 평가분야에 일부 포함
보안사고 관리	보안사고 관리	※ 별도 관리체계 적용
업무연속성 관리	사업 연속성 관리	※ 타 평가분야에 포함
준거성	준거성	※ 정부 규정 준수
개인정보보호		※ 기관 자체 개인정보보호를 의미하므로 제외

〔표 4〕 SEI IMCM 적용방안

SEI IMCM 기능 분류	적용방안
예방(Protect)	관제 대상기관에 대한 취약점 점검 등 예방진단 중심으로 적용
탐지(Detect)	보안 이벤트 및 로그에 대한 실시간 탐지정책 등 현재 사이버공격 탐지기술(패턴매칭) 중심으로 적용
대응(Respond)	침해사고의 효과적인 대응 관리체계 적용(침해사고 대응관리)
	침해사고에 대한 과학적인 분석체계 중심으로 '대응'과 별도의 분야로 구성 적용(침해사고 분석관리)
유지관리(Sustain)	보안관제 서비스 품질 및 가용성 강화 분야 적용 ※ 보안관제 업무관리를 위한 내부 활동(인적보안, 운영보안 등)은 앞서 언급한 보안관제 업무관리 부분에서 수용

를 기관이 잘 할 수 있도록 지원하는 활동들을 포함하고 있으며 평가에도 활용할 수 있다. 그리고 침해사고 대응 및 유지관리 등 실 업무에 있어 표준을 제공한다. 따라서 기관이 어떻게 침해사고 관리능력을 정의, 관리 및 측정하고 향상 할지를 이 Metric을 통해 알 수 있어 침해사고관리 서비스를 높은 품질 표준으로 다루고자 하는 보안관제센터에 많은 가이드를 제공한다[12]. 4개의 function categories(Prtect, Detect, Respond, Sustain)로 되어 있으나, 침해사고 정보 및 분석자료가 법적증거물로 활용될 수 있는 상황이 계속 증가되는 등 정확하고 과학적인 분석이 침해사고 관리에 중요한 영향을 미치므로 별도의 분야로 구성한다.

IV. 보안관제 업무평가 지표개발

4.1 개요

보안관제 업무 평가분야 및 항목이 정부에서 고시하는 법률 및 규정 등에 위배되지 않도록 고려했다. 또한 보안관제 조직부분과 관제시스템 관리부분은 국내·외 표준인 정보보호관리체계를 참조하고 침해사고 예방·탐지·대응·관리 부분은 카네기멜론대학의 SEI(Software Engineering Institute) IMCM (Incident Management Capability Metrics) 등을 중심으로 참조하였으며 실제 보안관제 업무 환경을 반영하여 수립하였다. 그리고 보안관제 센터 핵심 업무인 침해사고 관리부분인 침해사고 예방, 탐지, 대응, 분석, 관리 분야만을 별도로 평가에 활용 할 수 있도록 구성하였다.

4.2 평가분야 수립기준

4.2.1 보안관제 업무관리 부분

보안관제센터를 별도의 조직으로 간주하고 센터 자체의 관리적 정보보안에 초점을 맞추어 표준화된 정보보안관리체계를 참조하여, 실제 업무환경을 반영한 보안관제 조직부분과 관제시스템 관리부분으로 정책, 조직, 인력 및 관제시스템 보안관리를 제시한다.

첫 번째, 보안관제 정책 및 조직 분야이다. 관제업무를 효과적으로 수행하기 위하여 정책 및 지침, 규정을 수립하고 이에 대해 중장기 계획을 수립하고 연도별 실행 및 자체평가를 통해 보안관제센터의 발전방향을 제

〔표 5〕 보안관제 평가부분별 평가분야 및 주요내역

평가부분(평가분야 개수)	평가분야(평가항목 개수)	주요내역
보안관제 조직부분(2)	보안관제 정책 및 조직(5)	보안관제 업무절차 및 규정, 조직 구성
	보안관제 인력관리(5)	인력 정보보호 기술수준 및 적격심사
관제시스템 관리부분(3)	관제시스템 자산관리(8)	자산에 대한 위험평가 및 보호구역 지정·관리
	관제시스템 운영관리(7)	운영절차 규정 및 변경 통제방안 수립·시행
	관제시스템 접근통제(6)	접속 사용자 권한 및 특수권한 통제
침해사고 관리부분(5)	침해사고 예방관리(8)	취약점 분석평가 등 예방진단 활동
	침해사고 탐지관리(4)	보안 이벤트의 실시간 모니터닝 실시
	침해사고 대응관리(8)	침해사고 대응체계 수립·시행
	침해사고 분석관리(5)	침해사고 분석체계 수립·시행
	보안관제 서비스 관리(6)	서비스의 품질 및 가용성 강화

시하며 보안관제, 침해사고대응 및 취약점 분석평가 등 효율적인 조직을 고려하여 관제업무에 대한 기본적인 역할을 정의한다. 【보안관제 업무절차 및 규정(지침, 시행세칙 등) 제·개정 / 보안관제 조직구성, 책임자 지정, 명확한 역할 지정 및 활동여부】 두 번째, 보안관제 인력관리 분야이다. 수행인력에 대한 보안관리, 즉 담당 업무 범위 내에서의 시스템 및 정보 접근제어 등 취급관리 뿐만아니라 더욱 중요한 것은 보안관제 전문인력에 대한 기술수준을 심사하고 관제업무의 전문성을 유지시키기 위한 절차를 마련하고 수행하는지 점검한다. 【보안관제 인력에 대한 전문성 및 적격심사 기준 등 관리계획 수립 운용 / 보안관제 인력에 대한 업무별 취급정보에 대한 접근권한 규정 / 보안관제 인력에 대한 보안교육 수행】 세 번째, 관제시스템 자산관리 분야이다. 대부분 보안관제센터는 자체가 보호구역으로 지정·운용되고 있어 센터 내 관제시스템 및 정보 등 자산에 대한 관리는 물리적 보안이 포함된 관리가 수반되어야 한다. 이에 따라 물리적 보안과 자산관리를 통합하여 보호구역 내의 자산관리를 진단한다. 【관제시스템이 설치·운영되는 장소가 보호구역으로 지정·관리 / 관제시스템이 전원 및 공조시설, 통신망 등의 장애에 따른 중단으로부터 보호 여부 / 관제시스템에 대한 지속적인 가용성과 무결성 보장】 네 번째, 관제시스템 운영관리 분야이다. 보안관제 업무를 수행함에 있어 관제시스템을 보안의 관점에서 효과적으로 운영하는지 정의한다. 웜바이러스 등 악성코드를 자주 다뤄야 하는 업무를 수행하기 위한 보안 환경구성 및 운영관리를 진단한다. 【시스템 운영 절차 규정, 변경에 대한 통제방안 수립·시행 / 해킹기술 시험 및 악성코드 분석 등을 위한 절차를 수립하고 안전하게 수행 / 관제 데이터(사이버공격 탐지 로그, 보안장비 로그 등) 등 중요정보 및 소프트웨어 백업】 다섯 번째, 관제시스템 접근통제 분야이다. 관제시스템 및 민감정보(관제 대상기관 침해사고 관련정보 및 취약점 등)에 대한 접근권한을 인가된 사용자에 한하여 명확히 구분하고 이에 따른 통제여부 사항을 비롯하여 네트워크 및 통신설비에 대한 접근제어가 정확히 수행되는지 점검한다. 【관제시스템에 대한 접속 사용자 권한 및 특수권한 등 승인·변경·해지 관리규정 수립 시행 / 관제시스템의 접속을 통제하기 위한 적절한 로그온 절차 사용 / 민감 정보를 관리하기 위한 격리 및 통제 수행】

4.2.2 침해사고 관리 부분

침해사고 관리 부분은 SEI IMCM를 중심으로 기관의 정보자원 보호 및 유지를 위한 컴퓨터 침해사고 관리를 잘 할 수 있도록 하는 활동들을 정의한다. 국내 상황에 맞게 실제 업무환경을 고려하여 침해사고를 5가지 분야(예방, 탐지, 대응, 분석, 유지관리 등)로 분류하여 제시한다.

첫 번째, 침해사고 예방관리 분야이다. 침해사고를 사전에 예방할 수 있는 활동들을 말한다. 기술적인 부분과 관리적인 부분으로 구분되는데, 기술적인 부분으로는 취약점 진단 및 예방점검, 모의 훈련 및 해킹 등을 통하여 시스템의 보안 허점을 제거하는 것이다. 그리고 관리적인 부분으로는 주기적인 정보보안 교육시행 또는 최신 보안이슈를 수집하여 전파하는 정보공유 활동 등을 의미한다. 【주기적인 취약점 분석평가 등 예방진단 활동계획 수립 시행 / 취약점 분석결과, 모의훈련 또는 관제정보를 통한 동향분석 정보 제공 / 관제 대상시스템 및 자료 등의 중요도 식별, 목록 관리】 두 번째, 침해사고 탐지관리 분야이다. 보안관제센터는 침입차단·탐지·예방시스템 및 중요 시스템의 보안 이벤트를 수집하고, 24시간 관제요원이 지속적으로 침해사고 이상 여부를 모니터링 하고 있다. 현재 사용되고 있는 공격탐지 방법은 패턴 매칭에 의한 방법으로 새로운 사이버공격 및 자주 발생하는 공격에 대한 정교한 사이버공격 탐지패턴을 개발하여 전파하는 것이 중요하다. 또한 침해사고가 발생할 경우 해당 기관에서는 이를 은폐하기 쉽기 때문에 신속히 신고할 수 있도록 신고절차를 마련하고 시스템화 되어야 한다. 이와 같이 시스템적인 자동화된 침해사고 탐지와 체계적인 신고 시스템을 점검한다. 【모든 관제 대상시스템을 대상으로 보안 이벤트의 실시간 모니터닝 및 분석 실시 / 외부 위협환경 변화에 따른 보안장비의 보안정책 및 탐지기준 등 변경 및 공유】 세 번째, 침해사고 대응관리 분야이다. 침해사고 관리부분에서 매우 중요한 부분으로 침해사고가 발생 하였을 경우 신속하고 정확한 대응으로 피해를 경감시키는 것이 목적이다. 침해사고의 경·중 및 위급상황에 따라 어떻게 대응하는지 절차를 마련하고 대응 및 복구지원 등을 통한 피해확산 방지 활동을 정의한다. 【침해사고 위급상황에 따른 보고체계 수립 시행 / 침해사고 및 보안이벤트 처리 정책 및 절차 수립, 수행 능력 보유 / 침해사고에 대한 탐지결과 및 로그, 운영기록 일별 관리】 네 번째, 침해사고 분석관리 분야이다. SEI IMCM에서는 구분하지 않았지만 정확하고 과학적인 분석이 침해사고 관리에 대단히 중요한 영향을 미치기 때문에 별도의 분야로 구분한다. 침해사고 정보 및 분

석자료가 법적 증거물로 활용될 수 있도록 디지털 포렌식 분석기법 활용 및 보안 이벤트간 종합적인 상관분석에 대한 활동을 점검한다.【침해사고분석을 위한 디지털 포렌식 분석기법 활용 / 침해사고 분석 시 보안 이벤트간의 관계를 이용하여 상관분석 실시】 다섯번째, 보안관제 서비스 관리 분야이다. 보안관제 서비스에 대한 품질향상을 위해 보안관제 업무성과 평가활동 및 관제 업무의 기술적 향상을 위해 관제시스템 고도화 등 서비스 품질관리를 위한 활동을 정의한다. 또한, 장애 또는 천재지변으로 인한 업무 중단 복구에 따른 업무연속성 강화를 위한 활동을 진단하다.【보안관제 업무성과 평가절차 수립 시행 / 관제시스템에 대한 연도별 고도화 계획 수립 시행 / 관제업무의 중단 또는 장애 후에 요구된 수준만큼 유지 및 복구할 수 있도록 업무연속성 계획 수립】

4.3 평가점수 산정

단지 보안관제 주요업무인 침해사고의 효과적 관리만을 평가대상으로 한다면 보안관제 업무관리(보안관제 조직부분 및 관제시스템 관리부분)를 제외하고 침해사고 관리부분만을 평가에 활용할 수 있다.

따라서 침해사고 관리를 위한 정책 및 조직의 지원체계인 보안관제 업무관리를 분리하여 평가할 수 있다. 그러나 보안관제센터를 하나의 독립된 조직으로 전체적인 보안관리, 침해사고 지원체계 및 관리실태를 평가하고자 한다면 전체 10개의 평가분야를 적용하여 평가해야 한다. 보안관제센터 별 보안관제 업무관리는 표준화된 관리실태 평가로 가중치를 적용하지 않지만, 침해사고 관리부분 5개 분야는 센터가 추구하는 업무 방향에 따라 중요도가 달라질 수 있으므로 자체적으로 우선순위를 결정하고, 가중치를 평가에 반영할 수 있다[7].

〔표 6〕 평가항목 답변에 따른 점수

평가항목 답변 수		답변에 따른 점수
4개	①	100
	②	67
	③	33
	④	0
3개	①	100
	②	50
	③	0

평가분야 별 점수 = (($\sum_{i=1}^{n} T_i$) / n) × 가중치

※ T_i : 평가항목 별 평가점수, n : 평가항목 개수
종합점수 = 평가분야 별 점수 / 10

V. 사이버안전센터 적용사례

5.1 개요

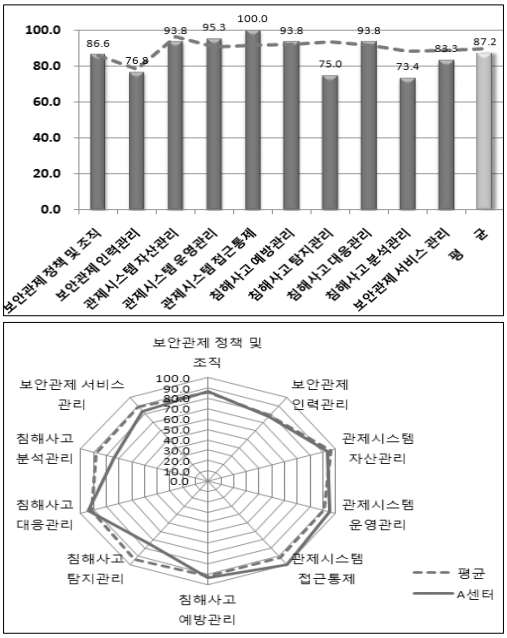
민간분야 보다 상대적으로 잘 구축되어 있는 중앙부처 사이버안전센터(부문관제센터) 4곳을 대상으로 개발한 '보안관제 업무평가 지표'를 적용하여 보았다. 분석 대상 중앙부처 사이버안전센터는 사회기반시설 제어시스템을 운영하고 있는 에너지, 산업, 금융, 지자체 등의 관련 기관을 대상으로 관제업무를 수행하고 있으며, 운영인원은 약 16명에서 32명 수준이고 관제대상 기관은 약 3개 기관에서 많게는 2백여개 기관으로 다양하다. 주요업무로는 실시간 보안관제, 침해사고대응 및 분석, 취약점분석 및 평가를 수행하고 있으며 규모를 계속해서 확장하고 있다.

5.1.1 A 기관 사이버안전센터

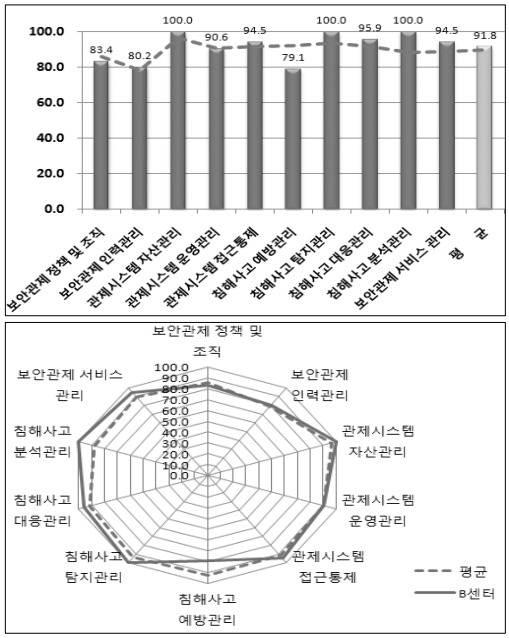
A 사이버안전센터는 가장 많은 관제대상 기관을 보유하고 있지만 평가된 4개의 중앙부처 사이버안전센터 중에서 가장 적절하지 못한 결과가 나왔다. 보안관제 업무관리에서는 보안관제 조직부분이 관제시스템 관리부분 보다 낮게 평가되었으며 특히 인력관리 분야가 가장 낮게 평가되었다. 침해사고 관리에서는 침해사고 탐지와 분석관리가 침해사고 예방, 대응, 보안관제 서비스 관리 보다 낮게 평가되었으며 특히 침해사고 분석관리가 가장 점수가 낮게 평가됨에 따라 효과적인 분석을 위한 절차 및 디지털 포렌식 기법 활용 등이 요구된다. 평균 점수를 기준으로 전체적으로 살펴보면 침해사고 관리 보다는 보안관제 업무관리가 더 우수하다는 것을 알 수 있다. 사이버안전센터의 중심업무는 침해사고 관리이다. 따라서 다른 업무보다 상대적으로 더 많은 노력을 해야 할 것이다. 특히 침해사고 탐지 및 분석 분야에서 홈페이지에 대한 실시간 위변조 모니터링 및 디지털 포렌직을 통한 분석기술을 강화해야 된다.

5.1.2 B 기관 사이버안전센터

관제대상 기관은 적지만 평가결과가 가장 높게 나타났다. 〔그림 3〕에서 보듯이 평균 점수보다 침해사고 예방관리를 제외한 전분야가 동등하거나 더 높게 나타



〔그림 2〕 A 기관 사이버안전센터 평가결과



〔그림 3〕 B 기관 사이버안전센터 평가결과

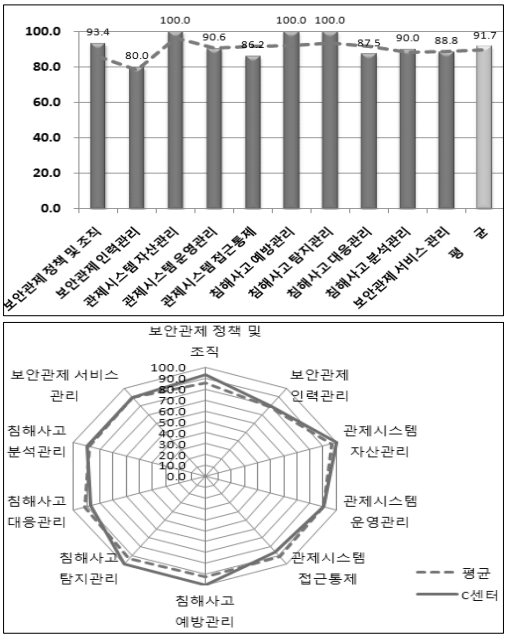
났다. 특히 침해사고 관리에서 평균 점수보다 더 높게 평가되어 평가한 4개의 중앙부처 사이버안전센터 중에서 가장 적절한 보안관제 업무를 수행하고 있다고 판단된다. 보안관제 업무관리에서는 평균과 비슷한 수준을 유지했다. 보안관제 인력관리 분야의 평균 점수가 가장 낮고 또한 B 기관 사이버안전센터의 보안관제 인력관리 분야의 점수도 낮다. 이것은 대부분 사이버안전센터가 보안관제 인력의 기술수준 및 보안관리 강화에 노력하고 있지 않다는 것을 나타낸다. 침해사고 관리에서는 예방관리를 제외한 탐지관리, 대응관리, 분석관리, 보안관제 서비스 관리가 평균 점수보다 우수하게 평가되었다. 이는 보안관제 핵심 업무인 침해사고 관리가 우수하다고 평가된다. 그러나 침해사고 예방관리 분야에 있어 모의 해킹 등 관제대상 기관 임직원을 위한 정보보안 교육부분이 미흡하게 평가되어 향후 보완이 필요하다. 전체적으로 보안관제 업무관리보다 침해사고 관리에 중점을 둔 적절한 업무수행 행태를 보이고 있다.

5.1.3 C 기관 사이버안전센터

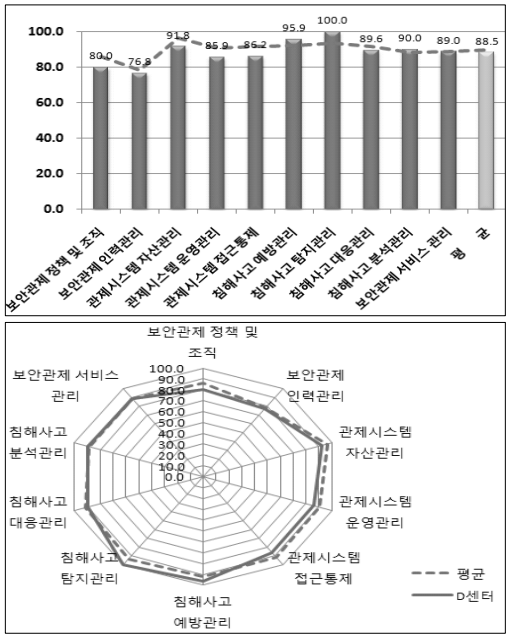
이 사이버안전센터는 평균 점수와 유사한 평가 점수를 기록하고 있다. 〔그림 4〕에서 보듯이 보안관제 업무관리에서는 A 기관, B 기관 사이버안전센터의 경우와 유사하게 보안관제 인력관리 분야가 다른 분야보다 낮게 평가되었다. 이는 보안관제 인력에 대한 보안관리와 관제기술 향상을 위한 교육의 강화가 필요함을 나타낸다. 그러나 보안관제 정책 및 조직 분야 즉, 관제업무 규정 및 절차, 조직 구성 및 역할 등이 상대적으로 우수하게 평가되었다. 침해사고 관리에서는 침해사고 탐지관리와 예방관리가 다른 4개 중앙부처 사이버안전센터 보다 우수하게 평가되었다. 이것은 침해사고가 발생한 후의 대응관리, 분석관리 분야 보다 사이버공격 사전예방을 위해 탐지관리와 예방관리를 강화한 것으로 설명할 수 있다. 보안관제 정책 및 조직 분야가 잘 정비되어 있고, 또한 침해사고 탐지관리와 예방관리도 상대적으로 훌륭히 수행되고 있다고 판단된다. 향후 관제업무의 중요요소인 침해사고 관리 즉, 대응관리, 분석관리, 보안관제 서비스 관리 분야에 좀 더 중점을 두어야 할 것이다.

5.1.4 D 기관 사이버안전센터

이 사이버안전센터 또한 C 기관 사이버안전센터와 같이 평균 점수와 유사한 평가 점수를 기록하고 있지만 〔그림 5〕에서 보듯이 보안관제 업무관리에서 약간 평균 점수 보다 낮고 침해사고 관리에서는 같거나 조금 높게 평가되었다. 보안관제 업무관리 보다 침해사



〔그림 4〕 C 기관 사이버안전센터 평가결과



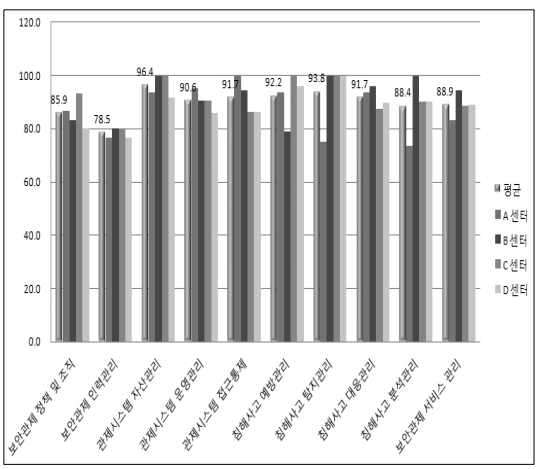
〔그림 5〕 D 기관 사이버안전센터 평가결과

고 관리를 좀 더 강화한 것으로 나타났다. 보안관제 업무관리에서는 전반적으로 모든 분야를 향상시킬 필요가 있으며 특히 보안관제 인력에 대한 기술수준 향상 등 관리계획을 수립하고 보안관리를 강화해야 한다. 침해사고 관리에서는 전반적으로 모든 분야에서 평균 점수 보다 동등하거나 근소하게 높게 평가되어 사이버안전센터로서 주요 역할수행에 노력하고 있음을 알 수 있다. 특히 사이버공격에 대한 실시간 모니터링, 홈페이지 위변조 감시 등 침해사고 탐지관리가 상대적으로 높게 평가되었다. 보안관제 인력관리는 A · B · C 기관 사이버안전센터와 유사하게 인력에 대한 관제기술 강화 및 보안관리가 필요하지만 침해사고 관리가 비교적 원활히 수행되고 있다. 다만 보안관제 정책 및 조직, 관제시스템 관리 등이 전체적으로 좀 더 강화되어야 한다.

5.2 사례비교

〔그림 6〕을 참조하여 4개의 중앙부처 사이버안전센터의 평가 점수를 비교하여 분석한다. 우선 보안관제 업무관리 즉, 보안관제 정책 및 조직, 인력관리, 관제시스템 관리 등에서는 공통적으로 인력관리 분야가 가장 약점으로 나타났다. 관제인력에 대한 기술향상을 위한 계획수립과 시행이 필요하며 중요 자료에 대한 접근통제 및 유출 등을 강화해야 된다. 다음은 전체적으로 4개 기관별 사이버안전센터의 강점과 약점이다.

- A 기관 : 자체 보안관리 및 관제시스템 관리가 강점이지만, 상대적으로 침해사고 관리가 미흡한 부분이 약점이다. 평가된 4개 기관 중에서 가장 적절하지 못한 업무형태이다.
- B 기관 : 자체 보안관리 및 관제시스템 관리는 평균을 유지 했지만, 침해사고 관리가 비교적 강점으로 나타났다. 다만 침해사고 예방관리 분야



〔그림 6〕 기관별 사이버안전센터 평가결과 비교

가 미흡한 것이 약점으로 판단된다. 평가된 4개 기관 중에서 가장 적절한 업무형태이다.

- C, D 기관 : 자체 보안관리 및 관제시스템 관리는 평균을 유지 했고, 침해사고 관리 또한 평균보다 동등하거나 약간 우세했다. 평가된 4개 기관 중에서 평균적인 업무형태이다.

VI. 결론 및 향후 연구 방향

점차 사이버공격이 지능화 고도화됨에 따라 많은 기관들은 보안관제센터, 즉 사이버안전센터를 구축 운영하고 있지만 이에 대한 업무평가가 시행되지 않아 발전모델을 파악할 수 없고, 정보보안관리실태를 평가하는데 있어 보안관제센터 업무수준을 반영하지 않고 있다. 따라서 본 논문에서는 보안관제 업무에 대한 평가지표를 개발하고 시뮬레이션함으로서 사이버안전센터의 장점과 약점을 파악하여 향후 발전 방향 모색에 기여하고 있다. 4개의 중앙부처 사이버안전센터를 대상으로 개발된 평가지표를 적용하여 평가함으로서 다음과 같은 사항을 알 수 있었다. 첫 번째 사이버안전센터의 전반적인 업무실태 현황을 알 수 있었다. 두 번째 사이버안전센터별 강점과 약점을 파악하여 발전방향을 모색할 수 있었다. 세 번째 사이버안전센터의 업무내역과 역할을 정의할 수 있었다.

부족했던 부분은 보안관제 전문인력에 대한 기술수준을 실질적으로 파악하지 못하고 다소 형식적인 기준으로 판단해야 한다는 것과 사이버안전센터의 정보보안 때문에 많은 센터를 대상으로 평가를 수행하지 못하여 전체적인 업무실태를 정확히 파악하는데 미흡한 부분이다. 평가지표에 대한 정보를 외부인에게 노출하지 않으려고 했고 검증자료 또한 확인하지 못했다.

향후 계속 연구되어야 될 방향은 첫 번째 이러한 보안관제 업무평가가 원활히 전 사이버안전센터를 대상으로 수행될 수 있도록 체계적인 제도를 마련하는 것이다. 제도와 환경이 뒷받침되지 않는다면 아무리 좋은 평가지표도 무용지물일 것이다. 두 번째 관제대상 시스템 특징에 따라 평가지표 또한 전문화하는 것이다. 전력 · 가스 · 석유 등 제어시스템을 위한 보안관제 업무형태가 전문화될 경우, 이에 따라 평가지표 또한 전문화되어야 한다. 국가적으로 매우 중요한 시스템은 특별히 차별화된 관제방법으로 관제되어야 하기 때문이다. 세 번째 보안관제 전문인력에 대한 실질적인 기술수준을 파악하기 위한 세부적인 절차 및 검증 방법론이 연구되어야 한다.

우리나라의 사이버안전센터가 본격적으로 구축 · 운영된 기간이 오래되지 않았지만 현재 많은 중앙부처 및 공공기관이 정보보안의 중요성을 인식하고 사이버안전센터 운용을 강화하고 있다[1]. 갈수록 고도화되는 사이버전쟁 환경에서 사이버공격 대응력 강화를 위한 노력이 이처럼 활발히 진행되는 것은 정말 다행스러운 일이다. 사이버안전센터를 구축하는 것도 중요하지만 이제 부터는 어떻게 효율적으로 발전시키고 운영할 것인지 고민해야 된다. 이 같은 취지에서 본 논문이 도움이 되길 바란다.

참고문헌

[1] 김영진, "국가정보통신망에 대한 체계적인 보안관제수행을 위한 모델 연구," 박사학위논문, 고려대학교, pp. 27-51, 2010년 6월.

[2] 이연수, 이수연, 윤석구, 전재성, "주요국의 사이버안전관련 법 · 조직체계 비교 및 발전방안 연구, "국가정보연구, 1(2), pp. 30-56, 2008년 12월.

[3] 박민수, "공공기관의 사이버안전센터 모델에 관한 실증적 연구," 박사학위논문, 숭실대학교, pp. 3-58, 2011년 6월.

[4] 방송통신위원회 · 행정안전부 · 지식경제부, 2011 국가정보보호백서, pp. 112-128, 2011년 5월.

[5] 한국인터넷진흥원 · 한국침해사고대응팀협의회, 침해사고대응팀(CERT) 구축/운영 안내서, pp. 71, 2010년 1월.

[6] 한국인터넷진흥원, 2011 ISMS 구축 및 운영교육자료, pp. 15-58, 2011년.

[7] 국가사이버안전센터, 국가사이버안전매뉴얼, pp. 92-99, 2005년 10월.

[8] 국가사이버안전센터, 2011년도 중앙행정기관 · 광역지자체 정보보안 관리실태 평가 해설, pp. 3-7, 2011년.

[9] 행정안전부 · 한국인터넷진흥원, 전자정부 정보보호관리체계(G-ISMS) 인증안내서, pp. 3-12, 2011년.

[10] 지식경제부, 보안관제 전문업체 지정 등에 관한 공고, 2010년 12년 21월.

[11] 국가사이버안전관리규정, 대통령훈령 제267호, 일부개정 2010년 4월16일.

[12] 홍진기, "침해사고관리 평가지표 개발에 관한 연구 - 보안관제업무 평가 중심으로," 석사학위논문,

동국대학교, pp. 9-11 32-35, 2009년 6월.
〔13〕 http://www.skinfosec.com/05_control/5_02_01.php, SK인포섹(주).
〔14〕 http://www.ahnlab.com/kr/site/product/controlInfo.do?svccode=aa1001&contentscode=432, (주)안랩.
〔15〕 http://sniper.wins21.co.kr/, 윈스테크넷.
〔16〕 http://www.igloosec.co.kr/p/husky, 이글루씨큐리티.
〔17〕 Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek, Handbook for Computer Security Incident Response Teams(CSIRTS): Carnegie Mellon Software Engineering Institute, Second Edition, pp. 76-91, Apr. 2003.
〔18〕 Karen Scarfone, Tim Grance, and Kelly Masone, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology: NIST Special Publication 800-61 Revision 1, March. 2008.
〔19〕 http://www.iso27001certificates.com/, the site of the International Register of ISMS Certificates.
〔20〕 John Snare and Eva Kuiper, "Text for ISO/IEC Final DIS 27001 Information technology - Security techniques - Information security management systems - Requirements," ISO/IEC FDIS 27001: 2005(E), pp. 1-29, Apr. 2005.
〔21〕 Audrey Dorofee, Georgia Killcrece, Robin Ruefle and Mark Zajicek, Incident Management Capability Metrics: Carnegie Mellon Software Engineering Institute, Version 0.1, pp. 23-207, Apr. 2007.

〈著者紹介〉

이 현 도 (Hyundo Lee) 학생회원
2012년 8월: 고려대학교 정보보호대학원 사이버보안학과 석사
1995년 1월~현재: 한전케이디엔(주) 근무
2008년 6월~현재: 지식경제 사이버안전센터 보안진단팀 차장
〈관심분야〉 주요정보통신기반시설 보안, ISMS, 침해사고대응, 정보보호 등

이 상 진 (Sangjin Lee) 종신회원
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: 한국전자통신연구원 선임연구원
2006년 2월~2011년 12월: 암호연구회 위원장
2008년 3월~현재: 고려대학교 정보보호연구원 디지털포렌식센터장
2006년 1월~현재: 한국디지털포렌식학회 이사
現 고려대학교 정보보호대학원 교수
〈관심분야〉 암호이론, 디지털포렌식