情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

정보보호 사고관리 국제표준과 해외동향

김 정 덕†, 박 인 범‡, 백 태 석‡, 황 수 하‡

요 약

본 논문에서는 정보보호 사고관리의 중요성과 국가별 정보보호 사고관리체계 및 표준 분석을 통해 사고관리 예방의 중요성과 국제적 협력의 필요성에 대해여 설명하고자 한다. ISO/IEC와 ITU-T의 정보보호 사고관리와 관련한 국제표준 분석과 더불어 한국, 미국, EU, 일본 등의 동향을 분석하여 발전된 형태의 정보보호 사고관리체계를 제시하고자 한다.

Ⅰ. 서 론

일반적으로 정보보호 정책이나 통제의 경우 한가지만으로는 정보, 정보시스템, 서비스, 그리고 네트워크에 대한 총체적인 보호가 어렵다. 통제가 구현된 후 잔여의 취약점은 정보보호를 비효과적으로 만들 뿐만 아니라 정보보호 사고를 유발하게 한다. 이는 잠재적으로 조직의 비즈니스 운영에 있어 직접 혹은 간접적인 악영향을 준다. 조직의 불충분한 대비는 모든 대응을 덜 효과적으로 만들며 잠재적 비즈니스 악영향을 증가시킨다[1].

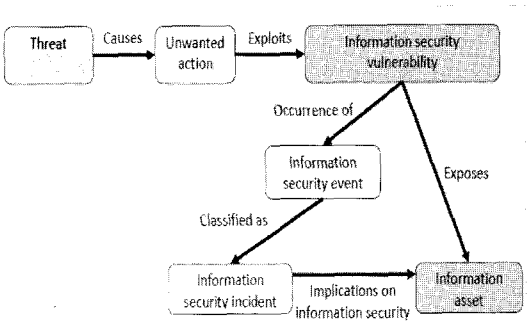
그러므로 어떠한 조직이든 정보보호에 대한 심각성을 인지하여야 하며 탐지, 대응, 보고 및 분석, 그리고 후속조치 순으로 구조 및 계획화에 접근하여야 한다.

ISO 국제표준에서는 다음과 같이 정보보호 사고관리를 정의하고 있다. 정보보호 사건(event)이란 시스템, 서비스 혹은 네트워크 영역에서 발생하는 것으로 정보보호 정책 위반이나 통제 실패, 또는 정보보호와 연관하여 기존에 발생하지 않았던 상황을 지칭한다. 정보보호 사고(incident)란 이러한 정보보호 사건이 비즈니스 운영에 심각한 손상을 가하거나 정보보호를 위협하는 경우를 말한다. 정보보호 사건의 발생만으로 항상 기밀성, 무결성, 가용성에 영향을 주지는 않으며 정보보호 사고로 분류되지 않는다[1].

위협은 원치 않는 방법으로 정보시스템 및 서비스, 네트워크의 취약점을 통하여 나타난다. 이러한 취약점을 통해서 정보보호 사건을 유발하거나 정보보호 사고의 잠재적인 원인이 되기도 한다. 각각의 객체는 [그림 1]과 같은 관계적인 사슬 형태를 가진다[1].

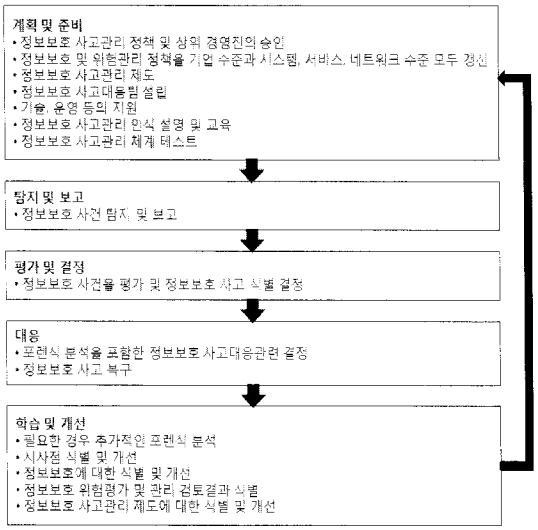
조직 전체를 아우르는 정보보호 전략의 핵심은 정보보호 사고관리를 위해 잘 정립된 통제와 절차를 적절히 구현하는 것이다. 사고가 발생한 경우 직접·간접비용을 줄이기 위하여 정보보호 사고를 회피하거나 영향을 수용하는 것이 비즈니스 관점에서는 주요 목적이라 할 수 있다.

정보보호 사고에 의한 직접적인 악영향을 최소화하기 위해서는 중단, 수용, 근절, 분석 및 보고, 그리고 후속 조치의 절차를 따르며, 잘 정립된 접근법을 통해 정보보호의 목적을 보장받을 수 있다. 이를 위해서 조직은 정보보호 사고가 적절한 분류, 등급, 공유 기준을 통하여 지속적으로 문서화 되어야하며, 통합된 데이터는 정보보호 통제 투자와 관련한 전략적 의사 결정 절차에 도움을 주는 가치 있는 정보가 된다.



[그림 1] 정보보호 사고 관계 사슬

† 중앙대학교 산업과학대학 정보시스템학과 (jdkimsac@cau.ac.kr)
‡ 중앙대학교 일반대학원 정보시스템학과 (infosys@cau.ac.kr)



〔그림 2〕 정보보호 사고관리 단계별 목표

Ⅱ. 정보보호 사고관리 국제표준

2.1 ISO 표준

ISO/IEC 27035 Information Technology - Security Techniques - Information Security Incident Management에서는 앞서 말한 정보보호 사고관리의 목적에 따라 계획 및 준비, 탐지 및 보고, 평가 및 결정, 대응, 학습 및 개선 이렇게 크게 다섯 가지로 구분하였다[1].

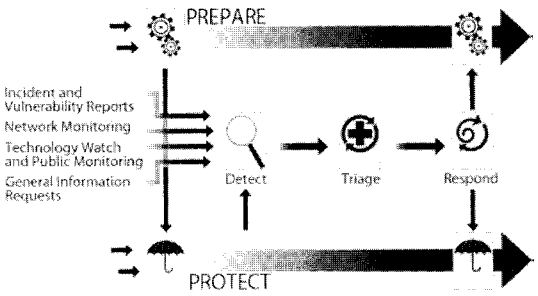
첫 번째 단계에서는 성공적인 정보보호 사고관리를 운영하기위해 필요한 요소들을 획득하는 과정을 포함하고 있으며, 나머지 단계에서는 정보보호 사고관리의 운영적 활용에 대한 부분을 포함하고 있다.

정보보호 사고관리의 단계별 세부 목표는 [그림 2]와 같다[1].

2.2 ITU-T 표준

정보보호 사고관리 분야는 ITU-T Study Group 17에서 연구를 담당하고 있다. Study Group 17은 보안(security) 분야로 사이버보안, 스팸대응 그리고 계정관리와 관련한 보안 사항을 다루고 있으며, 효과적인 정보보호 프로그램 구축의 일환으로 정보보호 사고관리에 대한 연구 활동을 포함하고 있다.

ITU-T Study Group 17에서 설명하는 정보보호 사고관리는 국제적 수준에서의 사이버보안을 위하여 사고



〔그림 3〕 사고관리 과정 5단계

대응 역량 및 탐지, 관리 체계사고와 연계성에 대해 강조하고 있다. 효과적인 사고관리는 자금, 인적 자원, 훈련, 기술적 역량, 공공/민영 부문 간의 관계, 그리고 법적 요구사항에 대한 고려사항이 포함되어야 한다고 하고 있으며 공공, 민영, 학계, 지역 및 다국적 조직 간의 협동에 대해 강조하고 있다. 이는 잠재적인 공격에 대한 인식을 제고 및 개선시킬 수 있다고 하였다.

특히, ITU-T SG17 Working Party 2 Question 7 에서는 2008년 9월 통신조직을 위한 보안사고 관리(security incident management) 과정 및 서비스에 대해 제안 하였다. 특히, 보안사고 관리에 대한 개념 및 관련 이슈들에 대해 중점적으로 설명하였으며, 사고를 단순히 다루는 것에서 나아가 사고재발을 예방하기위한 5단계 과정을 설명하였다. 대비 및 보호 과정은 사고, 취약점 보고 및 네트워크 모니터링 등의 정보를 통하여 탐지, 분류, 대응 단계를 순차적인 과정을 거치게 된다([그림 3] 참고)[2].

또한, ITU-T SG17에서는 2008년 10월 'Encourage the creation of national computer incident response teams, particularly for developing countries'란 이름의 결의안을 발표하였으며 현재관련 구성원들 간의 연구가 활발히 진행되고 있다. 이는 정보보호 사고관리에 대한 다국적 간의 긴밀한 협력을 위하여 표준 작업의 일환으로 개발도상국과 선진개발국과의 차이를 좁히는 것이 목적이라 할 수 있겠다[3].

Ⅲ. 주요국의 동향

미국은 현재 국토안전부(DHS)의 주도하에 NCSD (National Cyber Security Division)에서는 국가 및 민간에서 발생하는 사고 대응을 관리하고 있으며, 유럽은 현재 ENISA(Europe Network and Information Secu-

rity Agency)를 통하여 유럽국가의 전반적인 사고 대응을 관장하고 있다. 또한 일본은 NIRT(국가긴급대응팀), JPCERT/CC(컴퓨터긴급대응센터)의 운영을 통해서 국가 및 민간에서 발생하는 사고 대응을 관리하고 있다. 한국의 사고관리대응체계는 국가정보원의 국가사이버안전센터(NCSC)가 국가 · 공공분야를, 국방부의 국방정보전대응센터가 국방 분야를, 방송통신위원회의 인터넷침해사고대응지원센터(KISC)가 민간분야의 사고 대응을 담당하고 있다. 그리고 국가정보원에서는 이 세 가지 영역을 모두 총괄함으로써 좀 더 유기적이고 효과적인 사고관리대응을 가능하게 한다.

3.1 미국

공공, 민간 및 국제기관과의 공조를 통하여 사이버공간과 자국의 사이버 자산 확보에 힘쓰고 있는 국토안전부 산하의 NCSD(National Cyber Security Division)에서는 정보보호 사고관리에 대비하여 국가 사이버공간 대응 시스템, 사이버위험 관리 프로그램을 운영하고 있다. 이들의 주요 임무는 사이버위협과 취약점 식별, 분석 및 대응을 위한 활동과 위협정보, 위협경보를 제공하며, 침해사고대응관련 업무조정 및 복구활동에 대한 기술적 지원업무를 수행함으로써 주요 인프라를 보호하는 전략적 목표를 이루는 것이다[4].

또한, 미 연방차원에서의 정보보호 사고대응 가이드를 제시하고 있는데 미국 표준기술 연구소인 NIST의 SP 800-61 문서에서는 컴퓨터 정보보호 사고에 대한 조직구성의 방법 및 기능, 사고 취급 방법을 통하여 컴퓨터 정보보호의 사고대응 가이드를 제시하여 주고 있다[5].

한편, 국토안전부는 국가차원에서 사이버 인프라 및 핵심 정보 기술에 대한 위협을 감시하고 대처하기 위해 US-CERT, NCC, NCSC로 이루어진 NCCIC를 구축하였다. 이에 기존 음성통신 및 모뎀통신의 성능을 저해하지 않으면서, 중요 정보기술 기능 및 서비스를 저해 또는 붕괴시킬 수 있는 위협 요인을 억제하는 통합된 사고대응 기능을 제공 할 수 있게 되었다. NCCIC는 음성 및 사이버 통신 기술의 단절을 완화시키기 위하여 탐지, 예방, 대응하는 것을 목표로 하고 있다.

이러한 미국의 최근 조직 개편에 대한 움직임은 통신기술과 정보 기술의 경계가 모호해 지는 환경변화에 따라 네트워크 위험관리에 주안점을 두고 있다는 것을 알 수 있다[4,6].

3.2 EU

현재 유럽 각국의 CSIRT들은 EGC(European Government CSIRTs)활동을 통해 사고관리에 힘쓰고 있다. 이들은 정책 중심보다는 기술적인 면에 초점을 맞추고 있는 그룹으로서 주요 국가 인프라 그리고 정부관련 이슈 및 자산에 대한 사고의 영향에 관하여 공조 하고 있다[7].

또한, ENISA는 유럽 집행위원회의 산하에서 정보사회미디어총국과 함께 정보보호 사고 대응의 주도적인 역할을 수행하며 CERT를 운영하고 있다. 이러한 사고대응활동에 대한 CSIRT Service를 다음과 같이 구분하여 제공하고 있다[8].

현재 ENISA는 유럽의 정보보호 사고관리에 대한 CSIRT의 구성을 표준[9]으로 개발하였으며, 이 외에도 지속적인 유럽의 사고대응 및 정보보호에 대한 표준화를 진행하고 있다. 금년도는 정보보호 권고 사항에 대한 체제 개선, 데이터 관련 사고에 대한 체제 개선, 정보보호, 취약점, 착취에 대한 체제 개선에 관한 표준화를 진행하고 있다[10].

ENISA는 사고관리에 대한 일회적 대응이 아닌 지속적인 연구를 위하여 정보보호 및 사고대응 등에 관한 정보 공유 및 사고보고 모범사례 가이드, CERT를 위한 보안 역량 서클 및 모범사례 공유 등을 금년도 프로젝트로 초점을 맞추고 있다[11].

3.3 일본

1992년 창설된 JPCERT/CC는 1996년 통상산업성의 지원으로 본격적인 서비스를 시작하였고 현재는 경제산업성 산하에 있다. JPCERT/CC는 현재 일본 국가

〔표 1〕 CSIRT 서비스

실시간 대응 서비스	사전 대응 서비스	위협정보 취급
경보 및 경고 사고 대처 사고 분석 사고대응 지원 사고대응 공조 현장에서의 사고대응 취약성 대처 취약성 분석 취약성 대응 취약성 대응 공조	공표 기술적 관찰 보안 감사 또는 평가 정보보호의 형상관리 및 유지 보안 부서 도구 침입탐지 서비스 보안관련 정보 보급	위협정보 분석 위협정보 대응 위협정보 대응 공조 **보안 관리** 위험분석 사업연속성 및 재난복구 보안 컨설팅 인식 제고 교육/ 훈련 제품 평가 또는 인증

CSIRT(Computer Security Incident Response Teams)의 기능을 수행하고 있고 1998년에 일본 최초로 FIRST(Forum of Incident Response and Security Teams)에 가입하였으며 APCERT의 의장국으로 활동하고 있다.

JPCERT/CC는 2003년 실시간 관제시스템(Internet Scan Data Acquisition System: ISDAS)을 도입하고 2005년에는 조기경보시스템(Security Early Warning Service)을 구축하여 능동적인 사전 대처를 수행하였다. 또한 2006년부터는 사이버공격에 사용된 봇(Bots)과 같은 위협에 대한 분석 및 이에 대처하기 위한 기술에 대해 연구를 하며, 민간 기업에의 침해사고대응팀 수립을 도와주고 있다. 이 밖에도 컴퓨터사고 대응, 국내외 유관조직과의 협력, 컴퓨터 사고사례 및 시스템 취약성 등의 정보를 수집·제공하고 있으며 관련기술 조사·연구 및 보급·교육, 보안권고문, 취약점 등을 메일링 서비스로 제공하고 있다[12].

3.4 한국

국가사이버안전센터는 2004년 개소하였으며 2005년 1월 제정된 국가사이버안전관리규정(대통령훈령 제14호)에 의거하여 국가차원의 종합적이고 체계적인 사이버공격 대응을 위해 국가사이버안전 정책수립, 전략회의 및 대책회의를 운영하며, 정보보안수준평가, 사이버전 모의훈련 실시 등을 통하여 사이버안전 예방활동을 수행하고 있다. 또한 24시간 주요기관 대상 보안 관제를 실시하여 위협 수준별 경보(5단계)를 발령하고, 침해사고 발생 시 사고조사 및 대책을 강구하며, 피해확산 방지 및 복구지원을 수행하고 있다. 이 밖에도 국내외 사이버위협정보 공유 및 공조대응을 위해 국내 사이버안전전문기구와 협의체를 운영하고 미국, 영국, 프랑스, 독일, 일본 등과 협력체계를 구축 및 운영하고 있다[13,14].

국방정보전대응센터는 국군기무사령부에서 2003년 1·25 인터넷 마비사고 이후 범국가적 대응시스템 사이버테러 대응체제 구축 시 기존 조직인 대정보전팀을 확대하여 설립한 것으로 국방 주요 정보체계에 대한 취약성 진단 · 탐지 · 분석의 임무와 국방전산망에 대한 침해사고 예방 및 사고조사 · 수사 임무 등을 수행하고 있다[13,14]. 그리고 국방전산망에 대한 24시간 침해정보 탐지 · 분석 · 각급부대 CERT에 대한 조정통제는 물론 예방 및 조사활동, 원격 · 현장 피해복구 지원, 국내외 정보전관련 정보 분석 등의 임무를 수행한다. 또한 합참 주관 정보작전방호태세(INFOCON)훈련에 동참하여 사이버전 대응훈련을 실시하고 있다[15].

KrCERT는 2003년 12월부터 한국인터넷진흥원(당시 한국정보보호진흥원)의 인터넷침해대응지원센터(KISC)에서 운영하는 것으로 국내 민간분야에서 운영되고 있는 전산망의 침해사고 대응활동을 지원하고 전산망 운용기관 등에 대해 통일된 협조체제를 구축하여 국내 및 국제적 침해사고 대응 창구 역할을 하고 있다. 특히 FIRST(국제침해사고대응협의회), APCERT(아시아·태평양지역 침해사고대응팀협의체) 등 국제기구에 참여를 통하여 국내외 전문기관과 정보교류 및 협력체계를 구축하고 있다[13,14].

KrCERT에서는 올해부터 사전예방 중심의 사이버침해대응체계를 강화시키기 위해 국내 주요 웹사이트를 대상으로 매일 수행하는 악성코드 은닉 점검 대상을 대폭 확대하고, 광범위한 이용자PC의 사이버방역체계를 구축할 예정이다. 그리고 DDoS 등 사이버 공격 근원을 제거하기 위해 통신서비스사업자들과 사이버치료체계를 운영하여 사용자가 인터넷 접속 시 PC의 상태를 진단해 감염된 경우 이를 공고하고 전용백신을 보급해 치료할 수 있는 서비스를 제공할 예정이다[16].

3.5 국제 협력단체

오늘날 국경을 초월한 사이버공격에 효과적으로 대응하기 위해서는 국제협력체계 강화 및 국제사회의 이슈 해결에 적극적인 참여가 반드시 필요하다. 그래서 점점 다자간 협의체라던가 범국가적인 단체들이 생겨나는데 IMPACT, FIRST, APCERT 등을 예로 들 수 있다. 따라서 각각의 협의체에 대해 간단히 알아보고자 한다.

IMPACT(International Multilateral Partnership Against Cyber Threats: 사이버 위협에 대비한 국제 다자간 협의체)는 2008년 5월 말레이시아 쿠알라룸푸르에서 개최된 월드 사이버보안 정상회의(World Cyber Security Summit)에 참석한 26개 국가의 합의하에 창설한 것으로 현재 191개 국가와 11개 업체, 26개의 대학 및 3개의 국제기관이 참여하고 있다[17].

이러한 IMPACT는 사이버공격에 대한 조기 경보 시스템(early-warning system)을 통해 정보시스템 침해에 대한 정부 차원의 대응을 가능하게 하고 사이버공격으

로 인한 피해를 신속히 파악하여 이에 대한 유용한 정보의 회원국 정부 간 공유에 주안점을 두고 있다. 아울러 IMPACT는 인터넷 위협에 대해 선제적으로 모니터링하고, 위기 상황에 직면 시 정부가 신속한 정보를 입수할 수 있도록 하며, 정책 및 국제협력 센터(Centre for Policy and International Co-operation)를 통해 사이버 범죄 대응 정책수립을 추진하고, 훈련기술개발센터(Centre for Training and Skills Development)를 통해 회원국 정부의 해당 요원을 교육시키고 있다[18].

FIRST(Forum of Incident Response and Security Teams: 국제침해사고대응팀협의회)는 1990년 설립된 다국적 침해사고대응팀 및 보안 전문가로 구성된 협의체로 현재 약 200여개 기관 및 기업들이 회원으로 되어 있으며 정보보호관련 국제 공동 협의체로서는 가장 높은 신뢰도를 가진다. FIRST는 주로 국제적인 침해사고에 대한 경보, 예보 활동 및 이상 징후에 대한 상호 회의와, 해킹바이러스 동향 및 기술적 분석에 대한 토론을 수행한다[14,19,20].

APCERT(Asia-Pacific Computer Emergency Response Team)는 2003년 2월 설립된 것으로 아시아 태평양 지역의 16개국 23개의 침해사고대응팀으로 구성되어있고, 한국과 일본이 현재 공동 사무국으로서의 역할을 하고 있다. APCERT는 주로 아시아 태평양지역 이외의 국가와의 국제적인 협력을 증진시키고, 보안사고 대응에 대한 예방책의 협력개발, 정보공유 촉진 및 기술 교류, 상호 공동연구 및 개발 촉진을 수행한다[2,4]. 또한 2004년 한·중·일 공동대응 훈련을 시작으로 2005년부터는 공동대응 국가 수를 늘려 APCERT 차원으로 확대 진행하여 2010년도에는 총 14개 국가의 16개 침해사고대응팀이 참여한 공동훈련을 무사히 마쳤고, 2011년 APCERT 총회를 한국에서 개최하기로 하였다[21].

Ⅳ. 결 론

에스토니아의 Cyber war, 국내의 7.7 DDos 대란 이 두 가지 사건의 공통점은 두 국가 모두 IT 기술이 고도화 되어있다는 것이다. 그리고 사고 대응 및 정보보호에 대하여 항상 대비를 하여왔다. 하지만 점점 고도화되고, 지능화 되는 공격 방식에 따라 국가들은 피해를 보고 있는 상황이다. 이러한 사건은 비록 한 국가에 부정적인 영향을 미쳤지만, 해당 국가에만 생긴다고 단언할 수는 없는 것이다. 오늘날의 사이버 공격은 국경을 초월한 말 그대로 세계화를 따르기 때문이다.

따라서 각 국가들은 국가기밀 유출의 위협과 중요 인프라를 공격하는 사이버전쟁에 대처하기 위한 국제공제체계 구축에 적극적인 참여와 주도적 역할을 담당하고, 국제 공조체제 그룹에 활발한 참여를 통하여 폭 넓은 연구를 해야 할 것이다. 또한, 사고 대응에 있어 사고 발생 후에 대처하는 사후관리도 중요하지만 이를 예방할 수 있는 사전예방이 이슈가 되고 있는 만큼 국제 협의체 간의 유기적인 공조가 필요하고 이를 위해 전 세계적인 사이버침해대응 훈련 프로그램이 필요하다.

참 고 문 헌

[1] ISO/IEC 27035, "Information technology - Security techniques - Information security incident management" Final Committee Draft, Jun. 2010.

[2] ITU-T SG17, "6th Draft of X.sim: Security incident management guidelines for telecommunications," Sep. 2008.

[3] ITU-T WTSA Resolution 58, "Encourage the creation of national computer incident response teams, particularly for developing countries," Oct. 2008.

[4] DHS, http://www.dhs.gov/xabout/structure/editorial_0839.shtm

[5] Karen Scarfone, Tim Grance, and Kelly Masone, "Computer Security Incident Handling Guide," NIST, pp. ES-1-ES-4, Mar. 2008.

[6] 한국인터넷진흥원, "인터넷 & 시큐리티 이슈," pp. 101-102, 2009년 12월.

[7] European Government CERTs Group, "EGC Fact sheet," pp. 1-2, Dec. 2008.

[8] ENISA, "CERT cooperation and its further facilitation by relevant stakeholders," pp. 8, Jun. 2006.

[9] ENSIA, "A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT," pp. 2-5, Dec. 2006.

[10] ENISA, "Inventory of CERT activities in Europe," pp. 59-61 Nov. 2010.

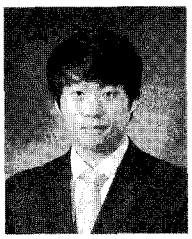
[11] ENISA, "WORK PROGRAMME 2010," pp. 2-44, 2010.

[12] JPCERT/CC, "About JPCERT/CC," Jun. 2009.
[13] 국가사이버안전센터, "국가정보보호백서," pp. 16-33, 2009년 4월.
[14] 국가사이버안전센터, "2006년 사이버 침해사고 사례집," pp. 97-101, 2007년 4월.
[15] 국군기무사령부, http://www.dsc.mil.kr/security.do?setForward=securityCenter&topSeq=04&leftSeq=04
[16] 디지털데일리, http://www.ddaily.co.kr/news/news_view.php?uid=64677
[17] IMPACT, http://www.impact-alliance.org/countries.html, http://www.impact-alliance.org/partners.html
[18] ZDNet, http://www.zdnet.co.uk/news/security-threats/2008/05/21/global-group-to-provide-cyber attack-early-warnings-39421618/
[19] 허창열, "국내외 침해사고대응 협력 현황," KrCERT/CC, pp.18-19, 2008년 9월.
[20] FIRST, http://www.first.org/members/teams/index.html
[21] 한국인터넷진흥원, http://www.kisa.or.kr/notice/pressView.jsp?mode=view&p_No=8&b_No=8&d_No=407&ST=T&SV=평화유지군

〈著者紹介〉

김 정 덕 (Kim Jungduk)
종신회원
1979년 2월: 연세대학교 정치외교학과 학사
1981년 8월: 연세대학교 경제학과 석사
1986년 5월: University of South Carolina, MBA
1990년 12월: Texas A&M University, Ph. D. in MIS
1995년 3월: 중앙대학교 정보시스템학과 교수
<관심분야> 정보보호관리/거버넌스, 시스템감리, IT 전략/관리

박 인 범 (Park Inbum)
학생회원
2010년 2월: 중앙대학교 정보시스템학과 학사
2010년 3월: 중앙대학교 정보시스템학과 석사과정
<관심분야> 정보보호 거버넌스, 시스템감사



백 태 석 (Baek Taesuk)
학생회원
2010년 2월: 중앙대학교 정보시스템학과 학사
2010년 3월: 중앙대학교 정보시스템학과 석사과정
<관심분야> 정보보호 거버넌스, 시스템감사

황 수 하 (Hwang Sooha)
학생회원
2010년 2월: 중앙대학교 정보시스템학과 학사
2010년 3월: 중앙대학교 정보시스템학과 석사과정
<관심분야> 정보보호 거버넌스, 시스템감사