한국위기관리논집 제6권 제4호 2010. 12 157~174쪽

교육행정기관의 사이버 위기관리 활동에 대한 상대적 중요도 분석

류영은*, 이재은**

본 연구에서는 교육행정기관의 정보보안 전문가를 대상으로 사이버 위기관리 활동의 상대적 중요도를 측정하고 우선순위를 제시하는데 목적이 있다. 이를 토대로 본 연구와 관련하여 사이버 위기관리의 효과성 제고를 위한 개선방안은 다음과 같다. 첫째, 사이버 위기 및 대응에 대한 교육 및 세미나를 강화하며 사이버보안 전문 인력을 양성해야 한다. 둘째, 사이버 위기에 대응하기 위한 인력은 정보통신분야에서의 기술적이고 전문적인 지식과 보안 분야에서의 전문적인 이해를 갖추어야 하므로 사이버 위기관리 활동을 전담할 수 있는 정보보호 전문인력을 확보해야 한다. 셋째, 정보보호 투자를 확대하여 최신기술이 적용된 전문장비를 확보하고 주기적인 업데이트 및 보완을 통해 빠르게 지능화고도화되고 있는 사이버 위기에 맞추어 신속하게 대응할 수 있는 체계를 갖추어야 한다. 넷째, 사이버 위기 발생 시 각 부서의 업무 처리 절차나 역할체계를 명확히 규정하는 것이 필요하다. 다섯째, 사이버 위기를 총괄적으로 관리하고 대응할 수 있는 책임과 권한을 지닌 총괄 전담기관을 구성해야 한다. 여섯째, 국가에서 교육을 전담하고 있는 교육행정기관의 정보인프라를 주요정보통신기반시설로 지정·관리하여 피해 확산을 방지하고 국가 핵심 기반시설에 대한 사이버 위기 대응 능력을 제고하여야 한다.

주제어: 사이버 위기관리, 사이버 위험, 교육행정기관, AHP

Ⅰ. 서론

교육행정 조직은 편리한 교육 행정서비스 및 민원서비스를 원스톱으로 제공하기 위하여 각각의 행정기관과 사이버공간에서 상호 연계되는 시스템으로 구성되어 있으며, 전체 교직원과 학생, 학부모를 아우르는 전 국민적인 개인정보와 교육 관련 중요 정보를 시스템으로 관리하고 있다. 그러나 정보화가 진행됨에 따라 역기능 또한 커지고 있다. 정보화의 역기능은 인터넷의 일반적 특성인 비대면성, 익명성, 시공초월성 등과 더불어 해킹과 같은 사이버 공격기술의 대중화, 인터넷 자체의 취약성 등과 결합하여 사이버 활동의 실질적인 위협요소가 되고 있다. 특히, 인터넷 자체의 취약성인 공개 프로그램 소스의 사용, 인터넷 접속의 용이성 증대, 손쉬운 공격 툴의 개발, 인터넷 자체의 공개 지향적 속성, 수 많은 버그(bug)의 존재, 사용자의 보안의식 부재 등의 문제가 서로 맞물리며 정보화 시대의 난제

* 제1저자, **교신저자.

로 등장하게 되었으며(김정규, 2007: 42), 사이버 위협은 지금까지 적용되어 오던 사회 전반의 법과 질서에 변화를 요구하고 있다(정정일, 2005: 323).

또한, 정보통신 기술이 빠르게 발전하면서 사이버 공간에 대한 의존성이 커지게 됨에 따라 국가위기도 기존의 전통적인 군사적 안보 위협에서 점차 사이버 공격 기술을 기반으로 한 사이버 위협으로 전환되고 있다. 물리적·공간적 특성을 초월한 사이버공간에서 국가 운영과 관련된 주요 핵심 기반시설과 정보가 시스템으로 관리·운영되는 정보화시대에서 갈수록 고도화·지능화되고 있는 각종 사이버 위협은 그 파괴력과 피해도 점점 커지고 있어, 사이버 위기에 대한 관리가 시급한 실정이다. 또한, 사이버 공간이 제2의 국민 생활공간으로 변화하면서 사이버 공간에 존재하는 개인정보와 활동전반에 대한 위협이 커지고 있어 국민의 정보인권과 정보자산 보호에 대한 필요성도 증대되고 있다. 인터넷이라는 거대한 네트워크로 전 세계가 그물망처럼 묶여 있는 사이버공간에서는 일부에서 발생한 사이버위협에 적절히 대응하지 못하는 경우, 전국가적인 위기상황으로 확대될 수 있기 때문이다.

사이버 위기는 조직에 소속된 전체 구성원들의 인식과 수준에 따라 대응이 달라지기 때문에 특정 전담조직에 의해 관리되는 것이 아니라 총괄적으로 관리되어야 한다. 조직 구성원의 공감대가 필요하며 담당 조직의 편제와 함께 전문 인력의 확보와 양성도 추진되어야 하고 적정 규모의 예산도 지원되어야 하는 등 조직 내 사이버 위기를 효율적으로 관리하기 위해서는 여러 고려사항들이 존재한다(박상서, 2009: 8). 특히, 교육행정 조직은 기관 자체가 교육청, 학교, 직속기관 등 이 한곳에 집중되어 있는 것이 아니라 여러곳에 산재하여 있고, 조직 구성원도 교원 및 공무원, 학생 등 다원화된 체제로 구성되어 있어 사이버 위협에 체계적으로 대응하기 어려운 조직 구조를 지니고 있으며, 도 단위를 제외한 시·군 단위 지역의 학교 및 교육행정조직의 사이버 보안 업무를 전문적으로 담당하는 전문 인력은 지역교육청의 경우 1~2명으로 산하기관 및 학교에 대한 사이버위기 관리 및 대응에 많은 어려움이 있다.

최근 상대적으로 보안에 취약한 학교 홈페이지가 해외에서 시도되는 해킹의 경유지로 사용되는 사례가 급증하고 있으며, 컴퓨터실의 PC가 악성코드에 감염되어 DDoS 공격을 유발하거나 주요 자료가 유출되고 악성 및 유해정보가 학생들에게 노출되는 등 사이버 침해 사고가 급격히 증가하고 있어 교육행정기관의 사이버 보안에 대한 문제가 심각한 실정이다.

이에 본 연구에서는 교육행정기관의 정보보안 전문가를 대상으로 사이버 위기관리 활동의 상대적 중요도를 측정하고 우선순위를 제시하는데 목적이 있다. 이를 위하여 사이버위기에 대한 이론적 논의와 선행연구 검토, 그리고 교육행정기관에서의 전산 및 정보보안 담당 공무원의 사이버 위기관리 활동의 상대적 중요도를 측정하고 우선순위를 제시한다.

II. 이론적 논의

1. 사이버 위기의 개념

국가사이버안전센터에서는 사이버테러를 '특정한 정치·사회적 목적을 가진 개인·테러집단이나 적성국 등이 해킹·컴퓨터 바이러스의 유포 등 전자적 공격을 통해 주요 정보기반시설을 파괴하거나 마비시킴으로써 사회혼란 및 국가안보를 위협하는 행위'로 정의한다. 그리고 사이버 공격은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위라고 정의할 수 있고, 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 '사이버 안전'이라고 말할 수 있다(국가사이버안전관리규정, 제2조). 또한, 전자적 침해행위에 대비하여 주요 정보 통신 기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것을 목적으로 제정된 정보통신기반보호법에서는 정보통신기반시설을 '국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망이용촉진및정보보호등에관한법률 제2조 제1항 제1호의 규정에 의한 정보통신망'을 말하는 것으로, 중앙 행정기관의 장이 전자적 침해로부터 보호가 필요하다는 판단에 따라 지정한 정보 통신 시설로 주요 정부 기관의 정보시스템을 포함한다. 그리고 사이버 관련 국가 핵심기반 마비는 해킹, 바이러스 등으로 인한 전자정보 수집, 국가 전산망의 파괴 및 마비/교란과 이로 인한 서비스 중단을 의미하는 것으로 이해할 수 있다(국가위기관리기본지침, 2004).

이에 대해 조호대(2006: 3)에서는 사이버 테러를 '해킹, 바이러스 유포, 논리폭탄 전송, 대량정보 전송, 서비스거부 공격, 고출력 전자총 등을 통신망에서 사용하는 "컴퓨터 시스템 운영 방해 행위" 내지는 "정보통신망 침해 행위", 또는 전자적 침해행위에 의하여 "국가적·사회적으로 공포심 내지 불안감을 조성하는 행위"'라고 정의하고, "컴퓨터시스템 운영 방해 행위" 또는 "정보통신망 위협 및 침해 행위"와 "테러리즘"의 결합이 사이버 테러의 개념요소라고 하였다. 이러한 사이버 테러는 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있다(조호대, 2006: 3).

<표 1> 테러 주체에 따른 테러 위협

구분	개인적 침해	조직적 침해	국가적 침해
주체	해커, 컴퓨터 범죄자	산업스파이, 테러리스트, 조직화된 범죄 집단	국가 정보기관, 사이버전 전사
목적	금전획득, 영웅심, 명성 등	범죄조직의 이익, 정치적 목적, 사회·경제적 혼란야기	국가기능 마비, 국가방위능력 마비
대상	민간사설망, 공중 통신망, 개인용 컴퓨터	기업망, 금융·항공교통 등 정보통신망	국방, 외교, 공인망 등

자료: 조호대(2006: 3)에서 재구성.

한편, 정보화 사회의 발전에 따라 악성 댓글, 스팸메일, 개인정보 유출, 금전적인 목적의 피싱

(Phishing)등에 따른 다른 개인적인 피해와 불건전 정보 유통, 개인 사생활 침해 등과 같은 부작용(국가정보보호백서, 2009: 6)도 사이버 위기로 볼 수 있다. 이와 함께 디지털 위험의 영향 범위에 따라 경제적 차원, 사회문화적 차원, 개인적 차원으로 구분하는 동시에 물리적 기반인 컴퓨터 및 통신기기 등에 직접 관련된 위험으로 유형화 할 수 있다(최흥석, 2009: 34).

<표 2> 디지털 위험의 유형

구 분	내 용
경제적 차원	저작권 침해, 인터넷 사기, 개인정보 유출 등
사회문화적 차원	생활감시, 언어파괴, 정보격차, 사이버폭력, 유해사이트, 잘못된 정보 유포 및 확산
개인적 차원	인터넷 중독
컴퓨터 등 디지털매체에 직접 관련된 차원	해킹 및 사이버 테러, 바이러스 유포, 스팸문자 및 스팸메일

자료 : 최흥석(2009: 34).

이와 같이 다양한 관점에서 사이버 범죄, 사이버 테러(또는 테러리즘), 사이버 위협, 사이버 공격, 디지털 위험 등이 논의되고 있는데, 본 연구에서는 이들 사이버와 연관된 위기의 의미를 포괄하여 '사이버 위기'로 본다. 즉 사이버 위기는 그 연구기관(연구자)이나 규정에 따라 다르게 정의 내릴 수 있으나, 사이버 공간을 이용한 일반적인 불법행위로서, 생활감시, 사이버 폭력, 불법 유해 사이트(음란, 도박, 폭발물, 자살), 잘못된 정보의 유포 및 확산, 저작권 침해, 불법복제, 명예훼손, 사이버 스토킹, 사이버 성폭력, 인터넷 사기 등의 일반 사이버 범죄를 포함하여 사이버 공간에 위치한 국가정보통신망이나 시스템 등에서 주요 국가정보나 개인정보유출, 훼손 등의 악의적인 목적으로 공격·마비시키는 테러 행위와 개인적인 측면으로 볼 수 있는 인터넷 중독, 도박, 자살, 음란 등 유해사이트나 악성 댓글 등에 의해 발생할 수 있는 위기를 총칭한다고 볼 수 있다.

특히, 사이버위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 사회 및 국가 전체의 위기로 발전할 수 있고, 개인에 대한 사이버공격이라고 할지라도 그 개인이 대통령 등 국가기관을 구성할 경우에는 국가기관에 대한 공격으로 볼 수밖에 없는 특징을 보유한다는 점에 주목해야 한다(김도승, 2009).

2. 사이버 위기의 특징

정보통신 기술의 고도화와 인터넷 환경의 대중적인 보급에 따라 사이버 위기에 대한 대응체계 마련이 시급해지고 있다. 한 번의 클릭으로 전 세계가 하나의 네트워크로 연결되는 사이버 공간의 특성으로 인하여 사이버 위기는 매우 빠르고 광범위하게 전개될 수 있기 때문이다.

또한, 사이버 위기는 언제 어디에서 발생할지 예측하기 어렵고, 인터넷의 개방성과 익명성의 특징으

로 인해 공격 대상자에 대한 정보를 얻기 어려우며, 그 유형도 더욱 다양화·지능화되고 있어 사이버 위기에 대한 예방과 대비 또한 매우 어려운 실정이다. 지식 정보화 사회에서 정보통신 기술의 발전 및 변화 속도가 빠르면 빠를수록 사이버 위험 요소 및 유형도 더욱 다양화·고도화되고 있다. 또한, 사이버 공간에서 여러 정보시스템 및 네트워크가 복잡하게 구성되어 유기적으로 상호 연계·운영되고 있는 대부분의 핵심기반 시설은 그 관리가 어려울 뿐만 아니라 일부 특정 분야가 사이버 위협에 노출될 경우 연속적 파급효과를 통해 타 분야뿐만 아니라 전체 핵심기반이 광범위하게 피해를 입을 수 있는 취약점을 안고 있어 개인적인 피해뿐만 아니라 국가적인 위기를 초래할 수 있으므로 민·관의 구분 없는 범정부적인 사이버 위기관리가 필요하다.

현대사회는 '고도화된 정보위험사회'로 웜 바이러스와 해킹 기능의 결합으로 복합화, 악성화된 사이버 공격이 증가하고 있으며, 비윤리적·반사회적·정보침해 내용의 콘텐츠들이 개방된 네트워크를 통해 급속히 전파되면서 사이버공간의 심각한 사회·문화적 부작용을 야기한다. 즉 고도화되고 복잡해진 정보기술이 사회시스템의 핵심기반으로 자리 잡게 되고 디지털 컨버전스가 확대되면서 특정 기술의 약한 고리에서 발생한 위험이 도미노 현상을 일으켜 전 사회의 위기로 몰아 갈 수 있는 잠재적 가능성이 상존하고 있는 것이다(황중연, 2008: 44-45).

이러한 사이버 위기의 특징은(이진수, 2000: 34; 조호대, 2008: 3; 이재은, 2008: 3), 첫째, 공격자가 목표로 정한 공격지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수 있는 광역성과 다양성의 특징을 갖고 있다. 둘째, 컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술만 있으면 최대의 피해를 줄 수 있는 가능성의 특징을 갖고 있다. 셋째, 사이버 위기는 반복 가능성, 영속성의 속성이 있으므로 한 번의 범죄행위는 그 규모나 피해가 작을 지라도 계속적으로 자동적인 프로그램의 실행, 확산을 통해 피해가 계속 증가한다는 특징이 있다. 넷째, 물리적 제약 공간이 아닌 사이버 공간의 특수성을 활용하여 증거를 변조하거나 삭제할 수 있는 은닉성과 정보가 눈에 직접적으로 보이지 않는 비가시성을 동시에 지니고 있다. 다섯째, 사이버 위기는 위기 상황 발생 가능성에 대한 징후를 포착하기 어려우며 파급효과가 급속하여 시간적인 압박이 크다. 익명성으로 인하여 상대방에 대해 확인할 수 있는 정보가 제한적이며 위기 상황에 대한 정보도 부족한 실정이다(정일석, 2004: 14-15).

사이버 공간은 정보통신기술의 비약적인 발전과 더불어 정보기기와 컴퓨터 그리고 인터넷 등의 네트워크로 연결된 가상의 공간으로 이미 국민 생활의 보편적인 영역으로 자리매김했고 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있다. 이러한 특수성으로 말미암아 복잡·고도화되며 시·공간의 제약을 벗어나 발생하는 모든 사이버 공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있다. 게다가 사이버공격으로 초래되는 사이버위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 국가전체의 위기로 확대될 수 있다(보안뉴스, 2008. 12. 12자).

시·공간을 초월하여 국내의 발전된 인프라가 해킹과 바이러스의 유포를 위한 중간 경유지로 사용

되고 있으며, 더욱이 국외에 거주하는 사이버범죄자에 대해서는 법적인 조치조차 취하기가 어렵다. 더욱 심각한 것은 주요 기반 시설이 점차 정보통신 네트워크에 의해 관리·통제됨에 따라 정보통신 인프라의 위협이 주요 기반시설의 위협으로까지 확장되어 있어 국가 안보적인 측면에서도 위험이 될 수 있다[1].

집집마다 하나의 초고속 인터넷으로 연결된 우리나라의 현재 정보통신 수준은 매우 높은 편이지만, 그에 비해 국민 개개인의 보안 의식 수준 및 대비(방어) 능력은 낮은 편이다. 지난 2009. 7. 7. 우리나라에서 발생한 인터넷 대란 때 각 개인의 PC가 사이버 공격의 대상 및 숙주로 사용되어 국민 개개인이 국가정보원의 지침에 의해 사이버 공격에 대해 대응하고 피해를 복구했던 예처럼 개인의 사이버 공격에 대한 의식 수준 및 능력을 높여야 할 필요가 있으며, 개인은 물론 각 관련기관(조직)들이 유기적인 협조체제를 구성하여 사이버 위기를 대응하여야 한다.

3. 사이버 위기관리 활동

사이버 위기관리 활동은 크게 예방, 대비, 대응, 복구 활동으로 구분할 수 있는데 우선, 예방활동은 예상 위협을 식별하고 운영의 지속성 보장을 위한 보호, 보안 대책을 강구하며 사이버 보안기술의 개발 및 취약점 발굴, 개선, 정보보호를 위한 전문 인력 양성 등「위기관리계획」을 수립한다. 대비 활동은 경보체계를 구축·운영하고 위기요인에 대한 감시태세를 유지하며,「위기상황 대응 매뉴얼」을 작성하고 이에 대한 교육 및 연습/훈련을 통하여 각종 위협에 대한 대응능력 및 대비 태세를 확립한다. 대응활동은 상황관리 및 보고체계를 운용하고「합동조사팀」을 구성하여 사고원인과 의도를 분석하며 긴급 대응 조치를 통해 피해 확산을 방지한다. 또한 대국민 교육 및 홍보를 강화하여 국민 불안을 해소시킨다. 복구활동은「복구지원팀」을 구성하여 조기에 피해를 복구하고 재발방지를 위하여 제도적 장치를 마련하거나 운영 체계를 보완하는 등 보다 항구적인 대책을 마련한다(국가위기관리기본지침, 2004).

본 연구에서의 사이버 위기관리 단계 중 예방단계의 활동은 다음과 같다. 첫째, 사이버 위기를 예방하기 위한 활동 전반에 대한 예방 계획의 수립이다. 둘째, ESM(Enterprise Security Management) 등 사이버 위기와 관련된 경보 및 모니터링을 제공하는 경보시스템의 구축이다. 셋째, 보안 취약성에 대한 분석 결과와 최신 보안 정보에 대한 공유 활동이다. 넷째, 조직구성원을 대상으로 사이버 위기와 관련된 교육 및 홍보를 주기적으로 실시하여 조직 구성원의 사이버 위기에 대한 인식 수준과 능력을 높이는 활동이다.

다음으로, 대비활동은 다음과 같다. 첫째, 비상대비 대책 등 사이버 위기와 관련된 대응 매뉴얼을 작성·비치하는 활동이다. 둘째, 사이버 위기관리 대응 팀을 구성하고 전담인력을 확보하여 사이버 위

1) 2008년 7월 그루지야의 인터넷 기반시설에 대한 사이버 공격이 바로 그러한 예가 될 수 있다(국가정보보호백서, 2009).

기와 관련된 업무분장을 명확히 명시하는 활동이다. 셋째, 사이버 위기관리 매뉴얼에 의거하여 주기적으로 사이버 위기 발생 대비 훈련 및 연습을 실시하여 대응 능력을 높이고 대응 체계를 개발하는 활동이다. 넷째, 최신기술이 적용된 전문장비와 시스템을 확보·구축하는 활동이다.

셋째, 대응활동으로는 첫째, 사이버 위기 발생 시 신속하게 진단할 수 있는 대응체계 구축 및 사이버 위기관리 매뉴얼에 의해 구성되어 있던 비상 연락 체계를 통해 경보를 확산하는 활동이다. 둘째, 사이버 위기가 실제 발생했을 때 사이버 위기관리 매뉴얼을 실행하는 활동이다. 셋째, 사이버 위기가 발생했을 경우 피해상황을 공개하고 관련조직과 유기적으로 대응하는 활동이다.

마지막으로, 복구활동은 다음과 같다. 첫째, 사이버 위기가 발생한 원인을 분석하고 평가하는 활동이다. 둘째, 발생한 사이버 위기에 대한 개선안을 발굴하고 보안시스템에 보안정책을 정비하고 최신기술을 도입하는 등 유사위기가 발생하지 않도록 방지하는 일련의 활동이다. 셋째, 원인분석과 평가 결과를 예방단계로 환류하여 사이버 위기관리 매뉴얼 등을 재정비하고 제도적 장치에 대한 미비점을 보완하고 운영체계를 개선하는 활동이다.

4. 선행연구 검토

사이버 위기에 관한 대표적인 선행연구로는 조호대(2008), 김영환(2009), 김민식 외(2009), 김정규(2009), 권소화·안성진(2004), 정관진(2004), 황중연(2008), 이재은 외(2008), 김귀남(2006), 김영진 외(2009), 권문택(2005) 등이 있는데, 이들 선행연구는 일반적인 사이버 위기관리의 법·제도적 측면과 정책적 측면에서 논의하고 있으며, 사이버 위기와 관련하여 기존에 수행되었던 연구는 대부분 정보통신 분야의 관점에서 기술적으로 사이버 위기 대응 체계 및 기 발생한 사이버위기 유형을 현상별로 파악하고 대처 방안을 수립하는 것과 사회과학분야에서의 이론적인 사이버 위기관리, 국가 안보위주의 전략과 사이버 심리전 대응방안 등에 대해서 이루어졌다. 또한, 범조직적인 참여가 필수적인 사이버 위기 분야에서 사이버 위기 대응을 위한 보안 전략의 조직에 관한 연구는 보안 조직 체계의 배치나 운영에만 초점이 맞추어져 있는 실정이며, 조직 구성원에 대한 설문이나 인터뷰를 통한 실증적 연구는 거의 이루어지지 않은 한계가 있다.

권소화·안성진(2004)은 교육기관에 피해를 주는 사고에 초점을 두고 초·중·고등학교 정보시스템을 대상으로 연구하였다. 즉 권소화·안성진(2004)은 정보화의 진전으로 인한 정보화 역기능 현상의 확산으로 해킹, 바이러스로 인해 교육기관에 피해를 주는 사고가 빈번하게 발생하면서 초·중·고등학교 정보시스템의 보안 취약점 강화와 구성원의 보안 인식 제고가 시급하게 해결해야 할 과제로 대두되고 있다고 지적하였다. 이를 위한 대책으로 학교에서 교육정보화 업무를 담당하고 있는 교육정보담당교사의 정보통신 윤리 및 정보통신 보안 능력을 강화할 필요가 있다고 하였다. 이를 위해 현재 교원 정보화 활용 능력을 종합적이고 체계적으로 진단하고 평가할 수 있도록 정보화에 대한 이해, 불건전 정보유통 방지, 지적재산권 보호, 네티켓 준수의 정보통신 윤리영역과 접근통제 관리, 악성코드

관리, 위험대비 관리의 정보보안영역으로 구분한 평가기준과 내용을 제시하였다.

조호대(2008)에서는 사이버테러리즘이 광역성 및 다양성, 최소 인원으로 최대 피해를 줄 수 있는 가능성, 물리적 공간이 아닌 사이버 공간의 특수성을 활용하여 증거를 변조하거나 삭제할 수 있는 증거의 은닉성과 비가시성을 특징으로 제시하면서, 사이버테러리즘의 대응방안으로 대테러방지법 제정 등의 법제도 정비와 공공부문과 민간부문을 아우르는 대응조직 구축, 보안분야에서 전문적인 이해를 갖추고 있는 전문인력 양성·확충, 국제적인 정보교류와 공조체제를 구축 등을 제시하였다.

김영환(2009)은 사이버 테러 대응체계 분석에서, 정보기술의 발전 속도는 법과 제도가 따라가기에 너무 빠르고, 대응체계의 낮은 탄력성이 위협의 증대요인이라고 하였으며, 이를 위한 대응으로 법적·제도적 기반의 확보, 범정부 차원의 대응체제 구축과 대응체계의 기술적 능력 확보, 정보보호시스템 구축 및 보안관리 강화, 군의 사이버전 대응체계 구축, 그리고 사이버테러리즘에 대한 국가 간 국제협력의 강화 등을 위한 범국가적인 적극적 대응전략 방안을 제시하였다.

<표 3> 세계 각국의 사이버테러 대응체계

국 가	사이버테러 대응체계
미 국	사이버안보국, 국가정보체계국 등
영 국	M-15:국가기반시설 보안조정 기구 등
독 일	컴퓨터긴급대응팀-DFN-CERT 등
유럽연합	유럽네트워크정보보안청 등
일 본	정보보안부회, 방위청-사이버부대 등
*우리나라	국가사이버안전센터, 국방정보전대응센터, 경찰청 사이버테러대응센터 등

자료: 김영환(2009: 168).

김민식 외(2009)에서는 사이버 위기관리체계의 대표적인 모델인 미국의 사이버 위기관리 체계의 동향을 분석한 후, 한국의 사이버 위기관리체계의 발전방향을 제시하였다. 미국의 사이버 위기관리 체계는 관리예산처와 연방정보보안관리법, 국토안보법, 사이버 보안연구개발법과 사이버 위기관리 관련 대통령령(국토안보경보시스템, 국내 사고관리, 주요기반 식별 및 우선순위 설정/보호, 국가준비 규정, 국가 사이버 안전센터 설립) 등과 사이버 위기관리 관련 전략으로 국가 사이버보안 종합전략이 있다. 한편, 일원화된 미국의 사이버 위기 관리체계와 다르게 공공분야와 민간분야, 또는 주요 정보통신기반시설 여부에 따라 적용 법령 및 주관기관이 달라지는 형태를 갖는 우리나라의 사이버 위기 관리체계를 문제점으로 지적하였으며, 그 해결방안으로 단일화된 법률과 제도 및 정책을 중심으로 하나의 기관으로 일원화된 관리체계의 설립을 발전방향으로 제시하였다.

김정규(2009)는 사이버 테러리즘의 위협을 전통적 테러리즘의 도구로서 활용되는 측면과 시스템 파괴형태로 구분하여 고찰하였으며 불법유해정보의 차단, 파괴적 사이버 테러리즘에 대한 기술 및 관리적 대응방안, 북한의 사이버 테러리즘에 대한 군사적 대응방안으로 테러리즘과 관련된 불법·유해정보의 차단을 위한 국제공조 강화와 인터넷 사용자의 자발적인 차단 활성화를 제시하고, 기술적 측면

에서 통제 프로그램의 개발을 위한 정부의 지원 등을 강조하였다.

정관진(2004)은 정보기술 발전에 따른 사이버위협의 재정립에 대한 연구에서 현대사회 사이버위협을 증대시키는 요소로 빠르게 발전하고 있는 컴퓨팅 파워의 증대, 초고속인터넷의 보급과 전세계적인 네트워크 형성, 시스템과 네트워크의 의존도가 증가함에 따라 구성의 복잡성과 관리의 어려움을 들었으며, 사이버공격의 발전 요소로 위협대상의 범위의 다각화, 인프라의 발전, 정보 접근의 용이성을 들었다. 또한, 그에 대한 대응체계로는 개인, 기업 그리고 국가가 함께 활동하는 협력대응체계를 통하여 공동목표 가치인 위협으로부터 안전을 달성하고 이러한 협력을 위해서는 공통 전략적인 체계와 표준이 필요함을 강조하였다.

이재은 외(2008)에서는 국내·외 사이버 위기관리 체계 분석을 통해 변화하는 국내 실정에 적합한 국가 사이버 위기관리 체계 강화 방안을 모색하기 위해 미국, 영국, 독일, 일본의 사이버 위기관리체계를 분석하였으며, 한국의 사이버 위기관리체계 강화방안으로 첫째, 국가 사이버 위기관리는 개인, 조직, 기업, 공공기관, 정부기관 등이 각각의 수준에 맞는 사이버 위기관리 체계 확립 둘째, 국가 사이버 위기의 개념을 국가위기의 개념과 연계 셋째, 국가 사이버 위기관리의 개념과 국가 위기관리개념을 연계, 넷째, 국가 사이버 위기관리 기관을 책임 정도에 따라 국가 사이버 위기관리 주관기관, 실무기관, 협력기관 등으로 체계화하여 관리 다섯째, 국가 사이버 위기관리 법체계 정비 여섯째, 국가 사이버 위기관리 조직체계 강화 일곱째, 국가 사이버 위기관리의 전문성 확보 여덟째, 국가 사이버 위기경보 체계 구축 아홉째, 국가 사이버 위기관리 평가체계 구축 열번째, 국가 사이버 위기관리는 공공과 민간 분야에서의 전문 인력 확보와 전문성 향상, 열한번째, 국가는 국가 사이버 위기관리의 지속적인 발전을 이룩하기 위하여 학술적 발전에도 노력해야 함을 강조하였다.

김귀남(2006)은 사이버 위협을 국제적 사이버정보전의 입장에서 연구하였는데, 미국, 영국, 중국 등에서 운영하고 있는 사이버전부대나 해커부대의 미양성, 사이버 범죄 및 사이버 테러 행위에 대한 공동대응체계 구축의 미흡함을 지적하며, 사이버 공격으로부터 국가 핵심체계를 보호하기 위한 대응 방안으로 현행 개별법을 통합한 가칭 '사이버안전기본법'의 제정, 청와대 사이버안보보좌관 신설 또는 국가정보원 주관의 대응 시스템 구축, 기술개발을 위한 안정적 예산 확보 및 지원의 필요성을 주장하였다.

김영진 외(2009)에서는 사이버 공격에 대한 실시간 탐지, 분석·대응의 보안관제의 중요성을 지적하고 현재 우리나라에서 실시하고 있는 보안관제 업무의 수행체계·방법 등을 분석하였다. 그 결과 국가 전체 전산망의 안전성을 높이기 위해서는 모든 국가·공공기관 및 지방자치단체의 정보통신망에 대하여 보안관제를 의무적으로 실시하도록 국가차원의 보안관제대책(구축·운영기준 및 실무매뉴얼 등)을 마련하고 그 이행여부를 확인 감독할 수 있는 장치를 강구하며, 보안관제 정보를 실시간으로 교류할 수 있는 공동대응체제를 갖추는 것이 시급하다고 보았다.

권문택(2005)은 사이버 테러에 대응함에 있어 경쟁력 있는 전문 인재 개발과 육성의 중요성을 강조하였으며, 정보보호 인력 육성체계의 미비, 특기분야 위주의 인력운영 및 관리체계 부족에 문제의식을

갖고 정보보호 조직 구성 및 인력현황, 정보보호 교육 현황을 분석하였다. 전문인력 양성을 위한 발전 방향으로는 획득-양성-활용의 세 가지 차원으로 구분하여 제시하였는데, 전문인력 획득을 위해서는 정부 조직에서 정보보호 분야 인력에 대한 특기별 인사 실시 및 전문성 분야 반복 보직으로 정보보호 전문기술을 지속적으로 함양 할 수 있도록 관리하여야 하며, 양성을 위해 전문 교육과정 체계화 및 신기술 습득을 위한 지속적인 보수교육을 실시하고, 활용을 위하여 직무분석을 통한 적재적소 배치, 수당 및 승진 등의 보상체계 개선을 위해 노력하여야 한다고 하였다.

<표 4> 선행연구 결과 요약

연구자	연도	주요 내용
조호대	2008	◦사이버 테러리즘의 특징 분석 - 광역성, 다양성, 은닉성, 비가시성 등 ◦사이버 테러리즘 대응 방안 제시 - 대테러방지법 제정 등의 법제도 정비 - 공공/민간부문을 아우르는 대응 조직 구축 - 전문인력 양성 및 확충, 국제적인 정보교류와 공조체제 구축
김영환	2009	◦세계 각국의 사이버테러 대응체계 분석 ◦분석결과에 따른 대응전략 방안 제시 - 법적·제도적 기반 확보, 국가 간 국제협력 강화 - 범정부 차원의 대응체제 구축, 기술적 능력 확보 - 정보보호시스템 구축 및 보안관리 강화
김민식 외	2009	◦미국의 사이버 위기관리 체계 동향 파악 ◦우리나라의 사이버 위기관리 체계 문제점 지적 : 공공/민간분야, 주요정보통신기반시설 여부에 따라 적용 법령 및 주관기관이 다름 ◦하나의 기관으로 일원화된 관리체계 설립 제시 : 단일화된 법률과 제도 및 정책
김정규	2009	◦전통적 테러리즘의 도구로서 활용되는 측면과 시스템 파괴형태로 구분하여 고찰 ◦군사적, 관리적, 기술적 대응방안 제시 - 불법·유해정보 차단을 위해 국제공조 강화 - 인터넷 사용자의 자발적인 차단 활성화 및 통제 프로그램의 개발을 위한 정부의 지원
권소화 안성진	2004	◦초·중고등학교 정보시스템의 보안취약점 강화 및 구성원의 보안인식 제고 필요 ◦교육정보화담당 교사의 정보통신 보안 능력 및 윤리 강화 - 교원정보화 활용능력평가의 기준 및 내용 도출
정관진	2004	◦구성의 복잡성과 관리의 어려움으로 사이버 위협 증대 - 컴퓨터 파워 증대, 시스템과 네트워크 의존도 증가 - 위협대상 범위 다각화, 정보접근 용이성 ◦개인, 기업, 국가의 협력대응체계 구축 강조 : 공동목표 가치 창출, 전략적 체계와 표준 필요
이재은 외	2008	◦미국, 영국, 독일, 일본의 사이버 위기관리체계 분석 ◦한국의 사이버위기관리 체계 강화방안 - 국가사이버위기의 개념을 국가위기의 개념과 연계 - 국가사이버 위기관리 주관, 실무, 협력기관으로 체계화 - 법체계 정비, 조직체계 강화 및 전문성 확보 - 국가 사이버 위기 경보 및 평가체계 구축 - 전문인력 확보 및 학술적 발전에도 노력
김귀남	2006	◦사이버범죄 및 사이버테러의 공동대응체계 구축 - 가칭 '사이버안전기본법'제정 필요 - 청와대 사이버안보보좌관 신설 또는 국가정보원 주관 대응시스템 구축 - 기술개발을 위한 안정적 예산 확보 및 지원

<표 4> 선행연구 결과 요약(계속)

연구자	연도	주요 내용
김영진 외	2009	◦사이버공격 실시간 탐지, 분석·대응을 위한 보안관제 강조 ◦국가차원의 보안관제대책 마련 및 공동대응체계 구축 : 국가공공기관 및 지방자치단체의 정보통신망에 대한 보안관제 의무 실시
권문택	2005	◦정보보호 조직, 인력, 교육현황 분석 ◦전문인력 양성을 위한 발전방향 : 3가지 차원 - 획득 : 특기별 인사 실시 및 전문성 분야 반복 보직 - 양성 : 전문 교육과정 체계화 및 보수교육 실시 - 활용 : 직무분석을 통한 적재적소 배치, 보상체계 개선

III. 사이버 위기관리 활동에 대한 상대적 중요도 분석

1. AHP 분석

1) 측정지표 및 측정요인의 선정

본 연구에 있어 AHP 분석[2]은 교육행정기관의 사이버 위기관리 활동에 있어 중요하게 인식해야 할 요인들에 대한 상대적 중요도를 우선 측정하여 교육행정기관이 사이버 위기관리 활동에 대한 효과성 확보를 위한 개선방안을 사전에 모색하는 것에 목적이 있다. 이에 따라 AHP 분석에서는 교육행정기관의 사이버 위기관리 활동 영역을 논리적 일관성을 유지하여 Petak(1985)의 위기관리 4단계 모델을 적용하여 '예방활동', '대비활동', '대응활동', '복구활동'으로 설정하였다.

<표 5> 교육행정기관의 사이버위기관리 측정영역

구분	영역	내 용
위기 관리 활동	예방	장기적 관점에서 미래에 발생할 수 있는 사이버 위기를 극복할 수 있도록 능력을 증진시키고 위기 발생 요인을 제거 및 억제하는 활동
	대비	사이버 위기 발생 전 사전대책을 수립하고 위기관리 능력을 유지하는 활동
	대응	사이버 위기가 현실로 나타날 경우 이미 수립된 대책을 시행하고 정상상태로 돌아오도록 대응하는 활동
	복구	피해를 복구하고 사이버 위기 발생원인 및 활동 전반에 대한 내용을 평가하고 학습하여 문제점을 분석하고 개선방안을 도출하는 활동

한편, 측정영역을 구성하는 측정지표는 각 영역에서 시행되는 주요 사이버 위기관리활동 3-4개를 측정지표로 선정하였으며, 각 활동의 측정지표는 동일 영역 내에서 쌍대비교를 실시하는 것으로 하였

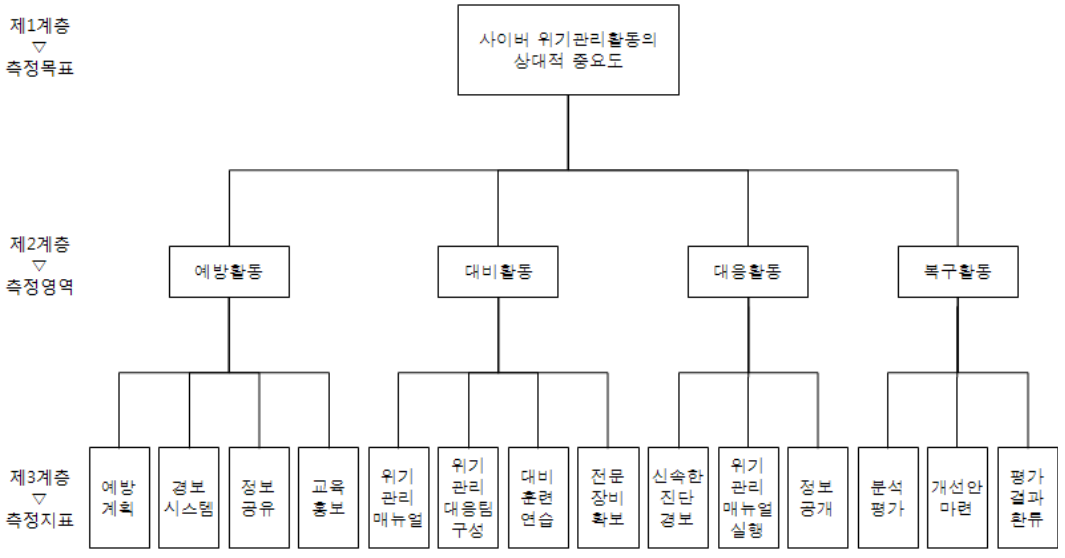
2) AHP 분석의 측정 방법에 관한 내용은 이재은(2002)을 참조할 것.

다.

<표 6> 교육행정기관 사이버위기관리 활동의 측정영역별 측정지표

측정영역	측정지표	내 용
예 방	예방 계획	사이버 위기를 예방하기 위한 활동 전반에 대한 계획 수립
	경보시스템	ESM 등 사이버 위기와 관련된 경보 및 모니터링을 제공하는 시스템
	정보공유	보안 취약성 분석결과 및 최신보안정보 공유
	교육·홍보	조직구성원을 대상으로 사이버 위기와 관련된 교육 및 홍보를 주기적으로 실시
대 비	위기관리 매뉴얼	사이버 위기관리 매뉴얼의 작성·비치
	위기관리대응팀 구성	사이버 위기관리대응팀의 구성 및 업무의 명확화
	대비 훈련 및 연습	주기적인 사이버 위기 대비 훈련 및 연습
대 응	전문 장비 확보	최신기술이 적용된 전문장비·시스템 구축
	신속한 진단·경보	사이버 위기 발생 시 신속한 진단 및 비상연락체제를 통한 경보의 확산
	위기관리 매뉴얼 실행	사이버 위기가 실제 발생할 경우 위기관리 매뉴얼의 절차에 따라 가장 먼저 대응
복 구	정보 공개	피해상황 공개 및 관련조직과 공통 대응
	분석·평가	사이버 위기 발생 원인 분석 및 평가
	개선안 마련	발생한 사이버 위기에 대한 개선안 발굴 및 보안시스템에 유사위기 방지 조치
	평가결과 환류	평가결과를 예방단계로 환류 및 사이버 위기관리 매뉴얼 등의 재정비

전문가를 대상으로 한 교육행정기관에서의 사이버 위기관리 활동의 상대적 중요성 및 우선순위 분석은 각 측정영역내에서 측정지표 간의 상대적 중요성을 각각 두 개씩 상호 비교하는 상대비교(pair comparison)방법을 수용하였으며 측정 요소 및 모형은 측정목표>측정영역>측정요소의 계층화 구조로 구성하고 AHP 기법을 이용한 Expert Choice 2000을 이용하여 분석하였다.



<그림 1> 교육행정기관에서 사이버 위기관리활동의 상대적 중요도 측정 구조

2) 자료수집 및 표본구성

교육행정기관의 사이버 위기관리 활동에 있어 측정영역과 요소의 상대적 심각과 우선순위 측정을 위해 전국 16대 시·도교육청의 사이버 위기관리 전담팀(CERT 등)에서 사이버 위기관리 활동을 주요 업무로 맡고 있는 정보보안 실무전문가집단을 모집단으로 설정하였다. 자료 수집은 2010년 5월 18부터 5월 21일까지 우편 및 메일을 통해 실시하였으며, 조사기간 중 교육행정기관이나 국가 정보시스템에 대한 침해사고가 발생하지 않아 실험설계의 내적타당성과 외적타당성이 비교적 확보되었다고 판단된다. 설문지는 전국 16개 시·도교육청에 배부한 16부 중에서 14부(회수율 87.5%)를 회수하였으며, 전체 설문지에 대한 일관성 검증 결과 일관성 비율이 0.1 이내로 유의미한 설문지 8부를 대상으로 계층분석절차(AHP)기법을 이용하여 분석하였다. 분석에 이용된 설문조사 응답자의 인구통계학적 특성은 다음의 <표 7>과 같다.

<표 7> 응답자의 인구통계학적 특성

(N=8)

구분		빈도	유효 퍼센트
성별	남성	6	75
	여성	2	25
직급	8-9급	1	12.5
	7급	3	37.5
	6급	4	50
현 업무경력 (현재보직)	6개월-1년미만	2	25
	1년-2년 미만	2	25
	2년 이상	4	50
소지 자격증	CISA	1	12.5
	없음	7	87.5
학력	대학 졸	6	75
	대학원(석사과정)	2	25

2. 측정영역 분석 결과

교육행정기관에서 사이버 위기관리 업무를 전담하고 있는 전문가를 대상으로 AHP 계층 모형에 속한 개별 요인들을 쌍대 비교하여 각 요인별 가중치(중요도)를 계산하고 그 결과를 분석한 결과 '예방활동', '대비활동', '대응활동', '복구활동'에 대한 상대적 중요도와 우선순위는 '예방활동' > '대비활동' > '대응활동)' > '복구활동'인 순으로 '예방활동'을 다른 세 요소에 비해서 중요하게 인식하고 있다. 즉 사이버 위기가 발생하기 전 예방계획을 수립하거나 위기 발생 가능성에 대한 모니터링 수행, 취약점등을 분석하고 조직 구성원들에게 사이버 위기가 발생하지 않도록 지속적으로 교육과 홍보를

실시하여 사이버 위기 발생을 적극 예방하는 것이 사이버 위기를 효과적으로 관리 할 수 있다고 인식하는 것으로 나타났다. 일관성 비율은 0.00으로써 설문에 대한 응답의 일관성이 지극히 양호한 것으로 나타났다.

<표 8> 측정영역별 상대적 중요도와 우선순위

측정영역	상대적 중요성	우선순위
예방활동	0.414	1위
대비활동	0.226	2위
대응활동	0.204	3위
복구활동	0.157	4위

CR = 0.00 / N=8

3. 측정요소 및 복합가중치 분석 결과

교육행정기관에서 사이버 위기관리 업무를 전담하고 있는 정보보안 전문가를 대상으로 교육행정기관에서 사이버 위기관리 활동에 있어 각 측정요소 간의 상대적 중요도 및 우선순위를 측정한 결과는 <표 9>와 같다.

<표 9> 측정요소간 상대적 중요도와 우선순위

측정 영역	측정요소	상대적 중요성	측정요소의 우선순위	복합 가중치	전체 측정요소의 우선순위	일관성 비율
예방 활동	예방계획	0.217	3순위	0.090	5순위	0.00
	경보시스템	0.271	2순위	0.112	3순위	
	정보공유	0.180	4순위	0.075	6순위	
	교육홍보	0.332	1순위	0.137	1순위	
대비 활동	위기관리매뉴얼	0.135	4위	0.031	13순위	0.01
	위기관리대응팀 구성	0.239	2위	0.054	9순위	
	대비훈련 및 연습	0.205	3위	0.046	11순위	
	전문장비 확보	0.420	1위	0.095	4순위	
대응 활동	신속한 진단경보	0.651	1위	0.133	2순위	0.08
	위기관리매뉴얼실행	0.248	2위	0.051	10순위	
	정보공개	0.102	3위	0.021	14순위	
복구 활동	분석평가	0.389	1위	0.061	7순위	0.00
	개선안마련	0.356	2위	0.056	8순위	
	평가결과환류	0.255	3위	0.040	12순위	

예방활동 영역에 대한 측정결과 시·도교육청 정보보안 전문가 집단은 교육·홍보를 가장 중요하게 인식하고 있는 것으로 나타났으며, 경보시스템, 예방계획, 정보공유 순으로 중요성을 인식하고 있는 것으로 측정되었다. 즉 사이버 위기관리 예방활동을 위해서는 조직구성원을 대상으로 사이버 위기와 관련된 교육 및 홍보를 주기적으로 실시하는 것을 가장 중요하게 인식하고 있으며, 다음으로 ESM 등

사이버 위기와 관련된 경보 및 모니터링을 제공하는 시스템을 구축하여 운영하는 것을 중요하게 생각하고 있다고 볼 수 있다.

대비활동 영역에서는 전문장비 확보를 가장 중요하게 인식하고 있는 것으로 나타났으며, 위기관리 대응팀 구성, 대비훈련 및 연습, 위기관리 매뉴얼의 순으로 나타났다. 이는 교육행정기관 내에서 전문적으로 사이버 보안 관련 업무를 담당하는 전산 공무원 집단은 사이버 위기관리 매뉴얼의 작성·비치보다는 실제 업무적으로 최신 기술이 적용된 전문장비와 시스템을 구축하는 것이 대비활동에서 가장 중요하게 인식하고 있다는 것을 알 수 있다.

대응활동 영역에 대해 시·도교육청 정보보안 전문가 집단은 신속한 진단경보를 매우 중요하게 인식하고 있는 것으로 나타났으며, 다음으로 위기관리매뉴얼의 실행, 정보공개의 순이었다. 즉 대응활동 영역에 있어서는 사이버 위기 발생 시 다른 무엇보다도 신속하게 위기상황을 진단하고 비상연락체제를 통해 경보를 확산하여 긴급하게 위기에 대처하는 것이 사이버 위기 대응 활동에 있어 가장 중요하게 인식하고 있는 것으로 나타났다.

한편, 복구활동 영역에 대한 중요도 측정에서는 분석·평가, 개선안 마련, 평가결과 환류의 순으로 나타났는데, 사이버 위기 발생 원인을 분석하고 평가하는 것을 가장 중요한 요소로 인식하고 있으며, 발생한 사이버 위기에 대한 개선안을 발굴하고 보안시스템에 유사위기가 발생하지 않도록 정책 등을 보완하는 조치를 2순위로, 그에 대한 평가 결과를 다음 순으로 중요하게 인식하고 있음을 보여준다.

전체 측정요소의 우선순위를 살펴보면 교육홍보가 1순위, 신속한 진단경보가 2순위, 경보시스템이 3순위, 전문장비 확보가 4순위로 나타났다. 이는 교육행정조직의 정보보안 전문가 집단은 사이버 위기관리 활동에 있어 조직 구성원들에 대해서 사이버 위기에 대한 심각성에 대한 교육을 실시하고 홍보를 강화하여 전반적인 정보보호 인식 수준을 높이는 것에 대해 가장 중요하게 생각하고 있으며, 위기가 발생한 이후에는 발생한 위기에 대하여 신속하게 진단하고 경보를 발령하여 연쇄적인 피해를 막고 즉각적인 대응을 실시하는 것을 두 번째로 중요하게 인식하고 있는 것으로 나타났다.

한편, 예방단계의 경보시스템에 대해서 교육행정조직의 정보보안 전문가 집단은 전체 측정요소의 3순위로 인식을 하고 있었는데, 경보시스템의 구축은 이미 2순위로 인식하고 있던 신속한 진단 및 경보 발령을 체계적으로 관리할 수 있게 하는 예방단계에서의 활동으로 유기적으로 연계되는 사이버 위기관리 활동에 있어 교육행정기관내의 정보시스템 및 네트워크 등에 대하여 보안 관제를 체계적으로 위기 발생을 사전에 예측하고 모니터링을 실시하며 위기를 즉각 진단하고 경보를 발령하는 것에 대해 매우 중요하게 인식하고 있음을 보여준다.

Ⅳ. 결론

본 연구에서는 사이버 위기관리 단계별 활동에 대하여 정보보안 전문가를 대상으로 상대적 중요도

를 측정하는데 목적이 있다. AHP 분석결과에서는 측정영별로 예방활동, 대비활동, 대응활동, 복구활동에 대한 상대적 중요도와 우선순위는 예방활동 > 대비활동 > 대응활동 > 복구활동 순으로, 예방활동을 다른 세 요소에 비해서 중요하게 인식하고 있는 것으로 나타났으며, 측정요소별로는 예방활동 영역에 대한 측정결과에서는 시·도교육청 정보보안 전문가 집단은 교육·홍보를 가장 중요하게 인식하고 있는 것으로 나타났으며, 경보시스템, 예방계획, 정보공유 순으로 중요성을 인식하고 있는 것으로 측정되었다. 대비활동 영역에서는 전문장비 확보를 가장 중요하게 인식하고 있는 것으로 나타났으며, 위기관리대응팀 구성, 대비훈련 및 연습, 위기관리 매뉴얼의 순으로 나타났다. 대응활동 영역에 대해서 시·도교육청 정보보안 전문가 집단은 신속한 진단경보를 매우 중요하게 인식하고 있는 것으로 나타났으며, 다음으로 위기관리매뉴얼의 실행, 정보공개의 순이었다. 한편, 복구활동 영역에 대한 중요도 측정에서는 분석·평가, 개선안 마련, 평가결과 환류 순으로 나타났다.

전체 측정 요소의 우선순위로는 교육·홍보, 신속한 진단경보, 경보시스템, 전문장비 확보 순으로 나타났다. 즉 교육행정조직의 정보보안 전문가 집단은 사이버 위기에 대한 교육 실시 및 홍보 강화를 통해 전반적인 정보보호 인식 수준을 높이는 것을 가장 중요하게 생각하고 있으며, 발생한 위기에 대하여 신속하게 진단하고 경보를 발령하여 연쇄적인 피해를 막고 즉각적인 대응을 하며, 교육행정기관 내의 정보시스템 및 네트워크 등에 대하여 보안관제를 체계적으로 실시하여 위기를 즉각 진단하고 경보를 발령할 수 있는 예방단계의 '경보시스템' 구축과 최신 기술이 적용된 전문장비와 시스템을 구축하는 것을 중요하게 인식하고 있음을 알 수 있다.

이를 토대로 본 연구와 관련하여 사이버 위기관리의 효과성 제고를 위하여 다음과 같은 개선방안을 제시하고자 한다. 첫째, 사이버 위기 및 대응에 대한 교육 및 세미나를 강화하며 사이버보안 전문 인력을 양성하는 한편, 보안 의식 수준을 높이기 위해 지속적으로 사이버 위기 대응 방법을 홍보해야 한다. 둘째, 사이버 위기에 대응하기 위한 인력은 정보통신분야에서의 기술적이고 전문적인 지식과 보안 분야에서의 전문적인 이해를 갖추어야 하므로 사이버 위기관리 활동을 전담할 수 있는 정보보호 전문 인력을 충분히 확보하고 전문가 양성을 위한 정보보안 전문 기술 교육을 실시하여 사이버 위기 대응능력을 강화시켜야 할 것이다. 셋째, 정보보호 투자를 확대하여 최신기술이 적용된 전문장비를 확보하고 주기적인 업데이트 및 보완, 유지보수를 통해 빠르게 지능화·고도화되고 있는 사이버 위기에 맞추어 신속하게 대응할 수 있는 체계를 갖추어야 한다. 넷째, 사이버 위기 발생 시 각 부서의 업무처리 절차나 역할체계를 명확히 규정하고 상호간의 토론을 통하여 유기적인 업무 협의문화를 조성하여 보안 업무 및 역할에 대한 인식차이로 인해 발생할 수 있는 갈등을 완화하기 위해 조직 구조 및 문화를 개선하여야 한다. 다섯째, 개별적으로 관리되고 있는 관련법들과 업무 기능이 분산 수행되고 있는 조직체계를 정비하여 사이버 위기를 총괄적으로 관리하고 대응할 수 있는 책임과 권한을 지닌 총괄 전담기관을 구성하고 통합법을 제정하여 위기 발생 시 신속히 대응할 수 있도록 법적 근거를 마련하여야 한다. 여섯째, 국민생활에 영향을 미치는 사회의 한 분야로서 국가에서 교육을 전담하고 있는 교육행정기관의 정보인프라를 주요정보통신기반시설로 지정·관리하여 피해 확산을 방지하고 국가

핵심 기반시설에 대한 사이버 위기 대응 능력을 제고하여야 한다.

참고문헌

권문택. 2008. 국가사이버안전관리 조직의 통합적 체계구축에 관한 연구. 정보·보안논문지. 9(3): 61-70.

김귀남. 2006. 국가 사이버전 대비방안 연구. 정보·보안논문지. 6(4): 141-151.

김도승. 2009. 사이버위기 대응을 위한 법적 과제: 미국의 사이버위기 대응체계 현황과 시사점을 중심으로. 방송통신정책. 21(17): 21-56.

김민식·박상돈·권헌영·김일환·임종인 2009. 통합적 사이버 위기관리 체계의 필요성에 관한 연구: 미국과 한국의 제도 및 정책 비교를 중심으로. 정보·보안논문지. 9(1): 29-37.

김영진·이수연·권헌영·임종인. 2009. 국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구. 한국정보보호학회논문지. 19(1): 103-111.

김영환. 2009. 사이버범죄에 대한 국가적 대응체계 구축의 이론적 함의: 사이버테러형 범죄를 중심으로. 한국컴퓨터정보학회논문지. 14(6): 165-171.

김원기. 2008. Fuzzy AHP 기법을 이용한 NEIS의 효과적 활용 방안에 관한 연구. 상명대학교 대학원 박사학위논문: 64-73.

김정규. 2007. 사이버 테러리즘의 위험성 증가에 따른 국가위기관리 차원의 대처방안. 국가위기관리연구. 1: 41-74.

류상일. 2010. 한국의 지방자치단체 재난대응체계: 정책네트워크 이론의 호혜성과 확장성을 중심으로. 충북대학교 대학원 행정학박사학위논문: 121.

박상서. 2009. 조직 정보 시스템 보안을 위한 총괄 전략 프레임워크. 정보·보안논문지. 9(2): 7-21.

이재은. 2002. 지방자치단체의 자연재해관리정책과 인위재난관리정책 비교 연구: AHP기법을 이용한 상대적 중요도 및 우선순위 측정을 중심으로. 한국행정학보. 36(2): 160-180.

이재은·김영평·정윤수·김태진. 2007. 발전원별 사회적 위험도에 대한 상대적 심각성 분석: AHP 기법을 활용하여. 한국행정학보. 41(1): 113-132.

이재은·양기근·류상일. 2008. 국가 사이버 위기관리체계 강화 방안에 관한 연구, 한국위기관리논집. 4(2): 69-93.

이철원. 2008. 국가 기반시설 사이버 보안기술 동향. 한국위기관리논집. 4(1): 11-22.

정관진. 2004. 정보기술 발전에 따른 사이버위협의 재조명. 제1회 한국사이버테러정보전학회 춘계학술발표대회: 207-218.

정정일. 2005. 사이버범죄에 대한 국제적 대응방안. 경호경비연구. 10: 323-354.

조성봉. 2009. 온라인 협업을 통한 제조업의 혁신: i-Manufacturing사례. 한국기술교육대학교 대학원 석사학위논문: 44.

조호대. 2006. 사이버 테러 대응 방안에 관한 연구. 한국위기관리논집. 2(1): 14-29.

조호대. 2008. 사이버 테러리즘 현황과 정책적 대응. 한국위기관리논집. 4(1): 1-10.

황중연. 2008. 유비쿼터스 환경변화에 따른 정보보호의 주요 현황과 대응전략. 정보와 통신. 25(1): 44-51.

McLoughlin, David. 1985. A Framework for Integrated Emergency Management. *Public Administration Review*. 45(Special Issue, Jan.): 165-172.

Petak, William J. 1985. Emergency Management: A Challenge for Public Administration. *Public Administration Review*. 45(Special Issue, Jan.): 3-7.

Saaty, Thomas L. & Kevin P. Kearns. 1985. *Analytical Planning: The Organization of Systems*. New York: Pergamon Press, Inc.

Saaty, Thomas L. 1982. *Decision Making for Leader: The AHP for Decisions in a Complex World*. CA: Wadsworth.

柳玲恩: 충북대학교에서 행정학석사학위(논문: 교육행정기관의 사이버위기관리에 관한 실증분석, 2010)를 취득하였으며, 주요 관심분야로는 사이버 위기관리, 조직이론, 재난관리 등으로 현재 충청북도교육청에 재직하고 있다(yesryu@cbe.go.kr).

李在恩: 연세대학교에서 행정학 박사학위(논문 : 한국의 위기관리정책에 관한 연구: 집행구조의 다조직적 관계 분석을 중심으로, 2000), 현재 충북대학교 행정학과 부교수로 재직중이다. 주요 관심분야는 위기관리, 조직이론, 정책집행 등이며, 시민참여와 거버넌스(공저, 2009) 등의 저서와 “국가갈등관리의 효율화 방안”(2009), “지방정부 재난관리 기관의 반응 분석”(2008), “국가위기관리의 새로운 영역 설정과 추진 전략: 국민생활안전 위기 영역의 분류와 운영 방안 모색”(2007), “국가 위기관리 정책의 영역별 상대적 중요도 분석: AHP 기법을 이용한 우선순위 측정을 중심으로”(2007) 등이 있다(jeunlee@chungbuk.ac.kr).

투 고 일: 2010년 7월 30일
수 정 일: 2010년 8월 24일
게재확정일: 2010년 9월 15일

Relative Importance of the Cyber Crisis Management Activities of Educational Administrative Institutions in Korea

Yeong Eun Ryu, Jae Eun Lee

The purpose of this article is to analyze the perception of the information officers who are in charge of computer and cyber security jobs in educational administrative institutions on the cyber crisis management activities in order to perform the cyber crisis management effectively in educational administrative institutions. Relative importance perception of the experts on the cyber crisis management activities has been analyzed through AHP design. Based on this analysis, the major findings for improving the effectiveness of the cyber crisis management are as follows; First, we need to introduce the education and workshop regarding cyber crisis and countermeasures. Second, we must educate the experts and perform the technical training for the experts. Third, we need to expand investment in information protection. Fourth, we need to specify the roles and responsibilities of each department in cyber crisis. Fifth, we have to restructure the organizations which individually manage related laws and regulations and business functions so that we can establish a dedicated organization with the authority and responsibility and legislate the integrated law for the legal ground of quick response. Sixth, it is needed that we appoint and manage information infra of educational administrative institution that is in charge of education as major information communication infra.

Key words: cyber crisis management, cyber emergency, educational administrative institutions, AHP