사이버 위기 시나리오 기반 대응 현황 분석

이대성

부산가톨릭대학교

Analysis of Response Status Based on Cyber Crisis Scenario

Daesung Lee

Catholic University of Pusan

E-mail : dslee@cup.ac.kr

요 약

대형 재난이나 사이버 위기 발생 시에 조기에 대응할 수 있는 효율적인 위기관리체계가 조직 내에서 뿐만 아니라, 협력기관 및 외부와의 관계에서도 필요하다. 본 논문에서는 대형 재난이나 사이버 위기 발생 시에 대처하는 국내외 대응 현황을 살펴보고, ICT 기술발전과 더불어 새롭게 나타나는 위기 대응의 문제점과 앞으로의 전망에 대해 고찰하고자 한다.

ABSTRACT

An effective crisis management system capable of responding early in the event of a major disaster or cyber crisis is needed not only within the organization but also with the partner organizations and the outside. In this paper, we review the domestic and international countermeasures against major disasters and cyber crises, and discuss the emerging crisis responses and future prospects along with the development of ICT technology.

키워드

Cyber crisis, Major disaster, Risk management, Cyber scenario

Ⅰ. 서 론

미국, 영국, 일본 등 해외 주요 국가에서는 대형 재난이나 위기 발생 시에 조기에 대응할 수 있는 효율적인 위기관리체계를 상시 운영하고 있으며, 그 중에서도 중앙정부와 지방정부간의 유기적인 협력과 소통을 강화하여 빈발하는 재난이나 위기 상황에 민관이 신속하게 대처할 수 있는 시스템 구축에 노력하고 있다[1].

미국에서는 1978년에 설립된 연방재난관리청(FEMA; Federal Emergency Management Agency)이 정부 위기관리 소통에서 중심적인 역할을 수행하고 있으며, 대부분의 재난이나 위기가 지역에서 발생하여 중앙정부나 주정부 차원에서 본격 대응하기까지에는 다소의 시간이 소요되므로 지역사회 중심의 위기대응을 중시하고 있는 상황이다.

영국도 위기상황 발생 시에는 내각 브리핑실(COBR; Cabinet Office Briefing)을 즉각 가동하며, 지진, 츠나미, 태풍 등 대형 자연재난이 빈발하는 일본은 지방단치단체의 역할이 중심이 되고, 이를 중앙정부가 지원하는 형태로 운영되고 있다.

이처럼 자연재난이나 질병, 화재 등 사회재난의 경우에는 위기소통관리체계가 일찍부터 정비되어 왔으나, 사이버 재난/위기와 관련된 위기소통관리체계는 발생도나 중요정보통신시설 파괴 등에 따른 사회·경제적 파급효과에도 불구하고 NATO나 체코 등 일부 국가에서만 사이버 보안 전문가를 대상으로 한 미디어 대응훈련이 진행되고 있는 실정이다.

NATO 합동사이버방어센터(CCDCOE; Cooperative Cyber Defence Centre of Excellence)는 매년 1회 락

드실즈(Locked Shields)를 실시하고 있는데, 이는 IT 시스템에 대한 대규모 사이버 공격을 방어하면서 공격상황을 실시간 보고하고, 전략적 방어 결정을 내리며, 포렌식을 진행하고, 법률적 및 대언론 과제들을 해결하는 훈련이며, 정보의 공유 수준, 의사결정자, 가이드라인 준수 등을 신속하고 효율적으로 판단하고 실행하는 보안기술 전문가들의 효율적인 위기소통능력을 강화하는데 중점이 두어지고 있다[2].

CyberCzech에서도 6시간 동안 IT 시스템을 방어하면서 기술적 능력뿐만 아니라 미디어분야, 법자문그룹과의 정보공유, 신속한 커뮤니케이션 능력을 강화하는 훈련을 실시하고 있으나, 국내에서는 아직까지 사이버 재난/위기 시 민·관간에 효율적인 정보공유와 소통을 위한 프로그램체계가 초기단계에 있는 실정이다.

II. 국내 사이버 위기 대응의 문제점

ICT 기술과 뉴미디어의 급속한 발전에 따라 신문, 방송 등 기존 미디어 외에 트위터, 페이스북, 밴드, 카톡 등 SNS가 현대 시민들의 핵심 소통미디어로 사용됨에 따라 국가 재난이나 위기 시에 신속하게 대응하지 못하면 '가짜뉴스' 등 유언비어를 통제할 수 없게 된다.

이를 위해, 정부에서도 2014년에 위기관리 커뮤니케이션을 위한 기본 매뉴얼을 제정하고, 대응과정에서 드러난 취약점들을 개선하여 반영하고 있으나, 부처별, 재난별 특성이 매우 다양하며, 사이버 재난과 같이 자연재난이나 사회재난에 비해 기술적 이해가 필요한 분야에 대해서는 독자적인 위기소통 매뉴얼에 의한 보안전문가의 미디어 대응 역량강화 훈련이 필요하다.

즉, 사이버 재난/위기와 같이 고도의 정보기술적 배경을 갖는 경우, 보안 전문기관간의 유기적인 소통이나 협력 뿐 아니라, 국민과의 투명한 정보공유가 주기적으로 이루어져야 하므로, 보안전문가들도 일관된 위기상황정보를 일반인들에게 알기 쉽게 전달할 수 있는 위기상황 시의 커뮤니케이션 대응역량이 요구된다.

III. 앞으로의 전망

이제까지 정부는 사회·경제적 파급효과가 엄청난 중요정보통신시설 보호에만 중점을 두어 왔으나, 4차 산업혁명시대에 진입하면서 스마트시티, 스마트 팩토리, 스마트 팜 등 사회 전분야로 CPS(Cyber Physical System)가 확산됨에 따라 국가 사이버 재난/위기 시에 보안기술 전문가들의 위기소통 범위가 일반시민으로까지 빠르게 확산될 전망이다.

따라서 기술/연구자들이 일반적으로 취약한 소통능력을 증진시키고, 특히 정보전파 속도가 매우 빠른 SNS에 대한 이해와 활용방법에 대해 숙달된 지식과 경험이 더욱 필요하게 될 것으로 전망된다.

IV. 결 론

정부는 다변화된 미디어 환경에 대응하여 국가 재난위기 발생 시에 국민의 심리적 안정과 신뢰를 확보하기 위해 2014년부터 위기 단계별 미디어 소통 표준 매뉴얼을 제정하여 시행하고 있으나, 실행단계에서 부처별·재난별 특성에 보다 적합한 업그레이드된 실용 매뉴얼의 개발이 요구되고 있다.

사이버 재난분야의 경우, NATO CCDCOE의 locked shields 훈련, 체코의 CyberCzech 훈련 등에서는 미디어대응 훈련을 실시하여 사이버 위기소통 역량을 강화하고 있으나, 국내에서는 아직 이에 대한 대응훈련 프로그램이 이루어지지 않고 있어 이와 관련된 기초연구가 시급히 이루어져야 한다. 특히, 미디어 다양화 시대에 사이버보안 실무 담당자의 경우, 기술적 대응뿐만 아니라, 효과적인 사이버 위기 소통을 통해 국민의 알권리를 효과적으로 충족시켜야 하는 위기소통능력이 요구되므로, 방송, 신문, SNS 등 여러 미디어들의 언론동향을 파악하고, 미디어 당사자들의 직접적인 질의 등에 대한 답변활동이 포함된 미디어 대응 훈련프로그램을 조속하게 개발하여 사이버 위기 발생 시 커뮤니케이션 역량을 강화시켜야 한다.

References

[1] Eunsung Kim, Hyukkeun Ahn, "Study on effective cooperation of disaster safety management for central and local governments," Seoul, Korea, KIPA research report, 2009

[2] NATO Cooperative Cyber Defence Center. [Internet]. Available : https://ccdcoe.org.