情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

기업 사이버재난 관리를 위한 재해경감활동계획 수립

이 영 재*, 이 성 중**

요 약

2003년 발생한 1.25인터넷 대란을 거쳐 2009년에 발생한 7.7.디도스 공격 등 최근 발생하는 사이버재난의 규모와 피해는 더욱 커지고 있다. 이러한 사이버 재난은 앞으로 스마트폰을 이용한 공격, 클라우드 컴퓨팅의 공격, 스마트그리드에 대한 공격 등으로 새롭게 발전하리라 예상되어지고 있다. 최근 개정된 '재해경감을 위한 기업의 자율활동 지원에 관한 법률'은 자연재난뿐 아니라 사이버재난에 대해서도 재난관리표준 [7] 과 기업재해경감활동계획 수립지침 [8] 의 표준화된 절차와 원칙을 준용할 수 있도록 하고 있다. 따라서 본 논문은 사이버재난과 관련해서 어떻게 기업 재해경감활동 계획을 수립하는가를 보여주고자 한다. 향후 기업 내 사이버재난분야에 대해 동법 제19조~제23조와 제26조에 따른 우수기업 인증제도 도입이 현실화 되면 기업 재난관리 업무에 큰 변곡점이 될 수 있을 것으로 전망한다.

Abstract

Government legislates a private sector preparedness act related to disasters such as natural, technological, and social ones. According to the law, it announces new standard for private sector preparedness. This paper illustrates a mitigation action plan based on the standard in terms of a cyber disaster. This plan includes organization, policy, assessment, impact analysis, strategy, plan, action, evaluation, and feedback. It will also help for business to mitigate a cyber disaster. Private sector accreditation and certification preparedness program which introduces on the law is the realization that enterprise disaster management will be expected as a great tipping-point.

Ⅰ. 서 론

지난 2003년 발생한 1.25 인터넷 대란은 서버 취약점을 이용한 바이러스 공격이 원인으로 밝혀진 바 있다.

당시 공격은 웜바이러스가 마이크로소프트의 SQL 데이터베이스 서버의 취약점을 공격해 확산하며 대량의 네트워크 트래픽을 유발해 인터넷 접속을 마비시킨 사례이다.

슬래머 웜은 불과 수십분 만에 전 세계 7만5000여개 시스템을 감염시켰으며 주요 인터넷망이 마비되는 피해가 발생하였다.

또한 2009년 7월 7일에 발생한 국내 주요사이트 해킹사고는 사전에 특정 사이트를 지정해 트래픽 공격을 퍼붓는 방법에 의한 디도스 공격 방법을 사용한 것으로 디도스 공격은 사전에 공격 사이트를 정해놓고 피해 사이트의 서버들이 서비스 불능이 될 정도로 큰 트래픽을 일으키는 것이다. 이러한 디도스 공격은 특정 사이트의 마비등 피해가 목적이며 이 공격에는 정교한 악성코드에 감염된 PC 내부에 공격대상과 시간이 스케줄링되어 이용된 것으로 분석되었다

상기 두 개의 사고는 이미 잘 알려진 사이버재난으로 각각의 피해액은 1.25 인터넷대란 시 225억원 ~ 1천675억원(한국정보보호진흥원), 2009년 7월 7일 해킹 사고시 363억~544억원(현대경제연구원)으로 추정하고 있으며 제시된 피해액 544억원은 2008년의 풍수해 피해 규모인 580억원에 거의 근접한 수치 [13] 로 심각하게 평가되고 있다.

이 논문은 소방방재청의 2009년도 자연재해저감기술개발사업 중 기업의 재해경감제도 활성화 전략계획과제의 연구성과를 기반으로 하였음.

* 동국대학교 경영대학 경영정보학과 교수, 이학박사 (yjlee@dgu.edu)
** 하나SK카드 감사실 차장, 경영학박사 (dr.infosec@gmail.com)

또한 정국환[10] 등은 최근에 발생하고 있는 사이버 침해 및 사이버테러는 목적 및 대상이 불명확하고 예측 불가능한 결과로 이는 비정상적인 자연현상 또는 인위적인(고의적인) 사고의 원인으로 발생하는 사회적·경제적 피해인 재난과 유사하다고 하였다.

미래에도 해킹, 바이러스, 악성코드, 스파이웨어 등을 이용한 각종 보안위협의 증가로 인해 사이버테러에 의한 통신망의 마비 가능성은 증가추세이다.[2]

이러한 사이버 사고를 재 분석해보면 어떤 공통점이 존재하는데 바로 초동단계와 대응단계에 있어서 체계적인 대응에 미숙하였다는 점이다. 2009년 7월 7일 디도스 사고에서는 최초 18시 40분경 공격이 감지된 이후 웹 접속장애에 대한 판단이 가능했음에도 6-7시간이 지나고 나서야 주의경보가 발령되었다. 또한 홍보 지연으로 대응단계에 진입한 7월 9일에서야 정부기관 및 민간이 참여하는 테스크포스팀을 구성한 공식대책회의가 개최되기도 하였다.

디도스 공격 발생초기 혼란은 평소 관련 재난에 대한 대응계획과 상황관리 훈련 부족과 사고원인 분석 대처 미흡 및 유기적인 상호협력 미흡 등이 주요 원인이었다. 당시 각 기업들은 체계적인 사이버재난 대응 능력이 부족하여 해당 위험에 효과적인 대응을 못하고 재난 대응의 한계를 경험하게 되었다. 또한 국가적으로도 관련위원회 또는 사고 대책본부의 가동지연, 관련 대응법령 부재로 인한 상황대응 미흡, 민간에 대한 상황전파 지연현상 등을 경험한 바 있다.

그러므로 본 논문은 기업 사이버 재난관리를 위한 재해경감활동계획 수립 과정을 기업재난관리표준에 따라 체계화하는 내용으로 보이고자 하는 것이다.

Ⅱ. 재난관리표준 연구

재난이라 함은 '재난 및 안전관리기본법' 제3조제1호[5] 에서 국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 것으로 정의하고 있다.

이 정의는 '재해경감을 위한 기업의 자율활동 지원에 관한 법률' 제2조1의2에도 동일하게 정의하고 있다. 2010년 3월부터 개정된 동 법에서는 자연재난만을 재난의 범주로 다루던 틀에서 벗어나 모든 재난의 종류를 포함해 기업의 재해경감활동을 요구하고 있다.

따라서 법에 의해 인터넷대란, 디도스공격, 통신장애와 전자금융 장애, 유무선 통신의 마비, 에너지 인프라의 마비 등의 재난에 대해서 사전에 재해경감활동을 통해 예방하고 기업이 입을 수 있는 피해에 대해 사업의 연속성 유지를 위한 적극적 대비가 가능하게 되었으며 이에 대한 경감활동을 국가로부터 지원받을 수 있도록 하였다.

기업재난관리표준이란 법 제2조 및 제5조에 따른 기업의 재해경감활동계획 수립을 위한 표준화된 절차 및 원칙을 말한다. 표준 내용은 [표 2]와 같다.

기업재해경감활동이란 기업 활동을 안정적으로 유지할 수 있도록 하기 위한 재난관리 체계로써 기업이 재난을 맞더라도 업무연속성(Business Continuity)을 유지할 수 있는 사전, 사후 경감활동을 수행하는 것을 의미한다.

계획에 따라 재해경감활동을 수행하고 별도의 우수기업으로 인증을 받고자 하는 기업은 재난관리표준의 범위에서 대통령령으로 정하는 기준에 따라 정부로부터 인증이 가능하다. 기업재해경감활동은 기업의 재난관리 정책 및 운영, 재해경감활동계획수립, 재해경감활동. 교육과 훈련 그리고 재해경감활동 평가 및 관리로 구성된다([그림 1] 참조).

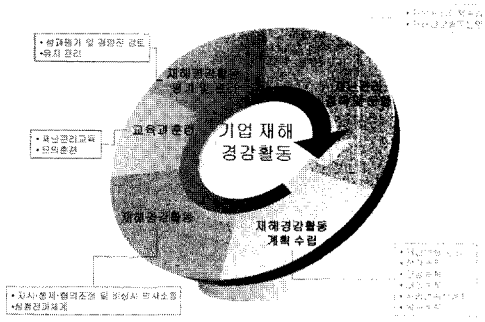
기업재난은 예측치 못한 상황이나 환경급변이 기업이 감내 가능한 수준을 능가하는 피해를 일으키는 경우에 재난의 형태로 나타나게 된다. 그러나 기업에 재난이

〔표 1〕 재난 및 안전관리기본법의 재난

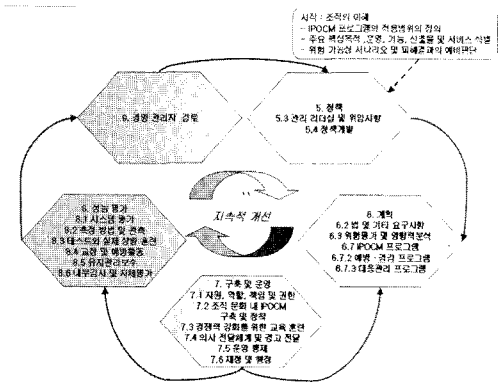
- 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 낙뢰, 가뭄, 지진, 황사(黃砂), 적조(赤潮), 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해
- 화재, 붕괴, 폭발, 교통사고, 화생방사고, 환경오염사고, 그 밖에 이와 유사한 사고로 발생하는 대통령령으로 정하는 규모 이상의 피해
- 에너지, 통신, 교통, 금융, 의료, 수도 등 국가기반체계의 마비와 전염병 확산 등으로 인한 피해

〔표 2〕 기업재난관리표준

- 재해경감활동 조직·체계 등의 구성에 관한 사항
- 재해경감활동 관계법령 준수·절차 및 이행 사항
- 위험요소의 식별, 위험평가, 영향분석 등 재난 위험요소의 경감에 관한 사항
- 자원관리 및 기업과 관련 단체와의 협정에 관한 사항
- 재해경감을 위한 전략계획, 경감계획, 사업연속성확보계획, 대응계획 및 복구계획의 수립에 관한 사항
- 재해경감활동과 관련된 지시·통제·협의조정 등 비상시 의사소통 및 상황전파 체계에 관한 사항
- 재해경감 교육·훈련을 통한 자체평가 및 개선



〔그림 1〕 기업재해경감활동



〔그림 2〕 사회안전-사고대비 및 운영연속성관리 가이드라인(KS A ISO/PAS 22399)

발생하더라도 사전 경감활동을 통해 대처능력을 높이고, 기업 내 인명 및 자산 등을 보호하기 위한 적극적인 대응방안을 준비하였다면 재난발생시 피해규모 최소화가 가능하다.

더불어 ISO/TC223에서 잠정적으로 모든 재난유형에 대해 사고대비 및 운영연속성관리를 위한 표준을 발표하였다. 표준 내용은 [그림 2]와 같다.

국내 기업재난관리표준은 법을 바탕으로 기업의 사전 재해경감활동에 중점을 두고 있으며, 국제 재난관리 표준은 공공부분부터 모든 민간부분에 이르기까지 재난피해 최소화를 위해 업무연속성계획(BCP) 도입에 초점을 두는 차이점이 있다.

Ⅲ. 사이버재난

최근에 발생하고 있는 사이버침해 및 사이버테러는 예측 불가능하고 사회적·경제적 피해가 커서 이를 디지털재난으로 정의하기도 한다.[10] 이처럼 기업이 직면하는 위기는 시간이 갈수록 하이테크화·대형화·복잡화되고 있다. 따라서 발생하는 재난의 사전예측이 어렵고 파급효과가 큰 위기상황이 증가하고 있다.[9]

사이버재난에도 다양한 발생요인이 존재하는데 바이러스, 해킹, 장애, 기술적 오류 및 화재, 침수 등 다양한 기술적, 비 기술적 요인으로 인해 발생되고 있다. 과거 2003년의 1월 25일에 발생한 인터넷 대란은 바이러스에 의한 공격이었으며 2009년 7월 7일 디도스공격은 해킹공격의 일종이었다. 이 밖에도 통신기업과 정부기관에서 건물, 공동구의 화재로 인한 경우와 단전이나 침수에 의한 경우, 기술적 오류로 인한 경우 등 다양한 사이버 재난이 크고 작은 형태로 발생해오고 있다. 2010년 6월 9일과 11일에도 해외문화홍보원과 법무부 홈페이지가 디도스 공격을 받은바 있다.[전자신문 외, 2010년 6월 12일].

인터넷은 그 구조적 취약점으로 인해 중요한 노드의 1%만 공격하여 마비시켜도 전체 인터넷 기능의 절반이 마비되고 4% 정도를 마비시키면 인터넷은 연결은 완전히 끊기는 것[11]으로 알려져 있다.

또한 경찰청 사이버 테러 대응센터[14] 분석에 의하면 사이버 테러형 범죄 역시 매년 증가하고 있는 것으로 분석되고 있다.([표 3] 참조)

그러나 기업에서도 사이버 영역은 전문화된 영역으로 그 특수성으로 인해 내부의 통제와 견제에서도 벗어나 있어 재난발생시 기업에 중대한 손실을 초래할 가능성은 더욱 높다고 평가되어진다.[9]

최근에는 사이버재난과 사이버테러가 일반 자연재난보다 큰 피해를 일으키는 경우도 증가하고 있다. 이러한 피해발생시 재난의 복구를 위해서는 피해액 1.5배 이상의 비용이 소요[10]되고 있으므로 재난의 사전예방은 점점 강조되고 있다.

그럼 통신이 마비되고 인터넷, 네트워크, 금융, 의료 인프라가 마비되면 기업들이 입는 피해는 무었인가? 사

〔표 3〕 사이버범죄 발생추이

년도	총계	사이버 테러형 범죄	일반 사이버 범죄
2003년	68,445	14,241	54,204
2004년	77,099	15,390	61,709
2005년	88,731	21,389	67,342
2006년	82,186	20,186	62,000
2007년	88,847	17,671	71,176
2008년	136,819	20,077	116,742

이버 재난이 발생하면 먼저 기간통신 사업자가 1차적으로 피해를 보게된다. 그러나 보다 큰 피해는 2차적 피해와 3차적인 피해를 받는 기업에게 더욱 커지는 것으로 예상하고 있다. 특히 사이버 재난이 물리적인 재난과 결합되면 복구시간의 장기화로 인해 피해 규모는 더욱 확산될 수 있다.

오늘날 안정적인 네트워크망이나 사이버 통신망에 대한 기업의 의존도는 더욱 커지고 있다. 따라서 향후 많은 기업들이 사이버 재난의 예방·대비·대응 및 복구를 위한 재난관리 활동을 적극적으로 수행해야 할 것으로 전망된다.

재난 및 안전관리기본법상 재난정의에 따른 사업분야 및 사이버 재난 발생 시 영향도가 높은 위험 분야는 [표 5]와 같다.

〔표 4〕 사이버 재난으로 인한 기업피해

- 기간통신 사업자의 직접적인 통신사업 피해
- 기간통신 사업자의 재난으로 인한 부가, 별정통신 사업자의 2차적 피해
- 부가, 별정통신 사업자의 재난으로 인한 데이터센터의 마비, 물류, 유통, 예약, 항공, 항만, 금융, 전력 등 전체 산업군의 3차적 피해

〔표 5〕 사이버 재난 고위험 사업분야

분류	사업분야
정보통신	• 정보통신망법 제46조의3에 해당하는 자로 매년 정보보호 안전진단을 받아야 하는 사업 -. 전기통신사업법 제2조 제1항 제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 사업 -. 집적정보통신시설 사업자 -. 일정규모의 정보통신서비스 제공자 • 모바일 및 스마트폰 인프라를 이용하는 사업 -. 모바일 환경 인프라를 이용으로하는 신사업
금융	• 전자금융업법 제2조 3항에 따른 금융기관 및 해당 기관의 전자금융 사업 -. 금융위원회의 설치 등에 관한 법률 제38조 제1호 내지 제8호 · 제10호 내지 제12호에 규정된 기관 -. 여신전문금융업법에 따른 여신전문금융회사 -. 우체국예금 · 보험에 관한 법률에 따른 체신관서 -. 새마을금고법에 따른 새마을금고 및 연합회 -. 기타 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자로서 대통령령이 정하는 자 • 금융감독원 DDOS 대응체계 구축 권고기관 및 VAN / Payment Gateway 사업 • 신용정보의 조회 기관 및 에스크로 사업 등 온라인 금융 관련 사업
기타	• 교통카드, 하이패스, 지하철 철도 전산시스템 및 교통 예약시스템 등 온라인 통신망을 이용하는 사업 • 의료법 제3조의4에 해당하는 상급종합병원 지정기관 또는 대형병상 의료기관으로 통신을 통한 정보관리 및 결제를 요하는 의료사업 • 에너지 및 전력 발전, 배전, 전력거래 사업 • 스마트그리드 등 신 기술사업

Ⅳ. 사이버재난과 경감계획활동

4.1 재난관리 표준체계

4.1.1 재난관리 정책 수립

기업 사이버 재난관리는 전통적인 재난관리보다 복구 시간 목표(Recovery Time Objective)가 짧고 복구에 필요한 요구기술 수준이 높으며 많은 경우 통신의 장애를 수반하기 때문에 복구의 어려움은 상당이 높은 편이다. 그러므로 기업의 사이버 재난관리를 위해서는 당해 기업의 특성(업무 및 자원)을 정확히 반영한 사전의 경감활동 및 사후의 대응복구활동을 위한 사이버 재난관리 정책이 수립되어야 한다. [12]

가. 정책방향

사이버 재난관리정책 포함 사항은 [표 6]과 같다.

나. 최고경영진 역할과 책임

최고경영진은 기업의 사이버재난 재해경감활동에 대해 적극적으로 지원해 한다. 또한 기업 내의 관리책임을

〔표 6〕 사이버 재난관리 정책 포함 사항

- 기업의 재해경감활동의 목적, 범위, 제약사항
- 재해경감활동 계획에 대한 변경관리, 평가 및 개선활동
- 최고경영진의 재해경감활동 계획의 승인
- 기업의 내외부적으로 기업 재해경감활동에 대한 정책 선언
- 기업재해경감활동을 위한 조직문화의 정착

〔표 7〕 최고 경영진의 역할과 책임

- 사이버재난에 대한 기업재해경감활동 정책 및 계획 승인
- 사이버재난에 대응조직의 승인 및 재난관리담당자 지정
- 사이버재난에 대응에 필요한 예산과 인력계획의 승인
- 지시·통제·협의조정 및 상황전파 의사결정
- 재해경감활동에 필요한 예산과 인력의 확보
- 재해경감활동에 성과평가에 대한 검토

분명히 하기 위해 정책 수립시 최고경영진의 역할과 책임이 명시되어야 한다.

다. 재해경감 단체와의 협정

기업은 사이버 재난발생에 대비하여 관련 기관 및 단체들과 상호협력을 위한 필요사항을 결정하고 문서화를 통해 협약을 체결하여야 한다. 효과적인 사이버 재난대응을 위해서는 반드시 사전에 기업외부 및 내부부서와 사전 협조되어야한다.

4.1.2 재해경감 활동 운영체계

가. 재해경감활동 조직

통상 발생되는 기업내 사이버 재난은 복구목표시간이 매우 짧기 때문에 사전에 내·외부 조직들이 완벽하게 책임과 역할을 정리하도록 해야 한다. 따라서 사이버 재해경감활동은 최고경영진에 의해 공식 임명된 담당조직에 의해 책임있게 구성되는 것이 바람직하다.

나. 재난관리행정과 재무

효과적인 기업 내 사이버 재난관리를 위해서는 경감활동을 수행하기 위한 별도의 업무지원 및 자금집행 절차를 개발·적용하여야 한다. 또한 빠른 시간 내에 복구를 위해서는 재난발생시 별도 승인 없이 즉시 사용이 가능한 예산의 확보도 필요하다.

4.2 재해경감활동 계획수립

사이버 재난에 대한 체계적인 경감활동 계획수립을 위해서 우선, 위험요소를 식별하고 평가하며, 위험발생시 업무에 미치는 영향을 분석하여 재해경감을 위한 전략을 개발한다. 전략계획수립은 경감전략, 대응전략, 사업연속성전략 그리고 복구전략으로 구성된다. 수립된 전략계획을 토대로 경감계획, 대응계획, 사업연속성확보계획, 복구계획을 수립하도록 한다.

4.2.1 재난위험관리

재난위험관리는 기업재해경감활동 계획을 수립하기 위한 기초단계로서 위험요소 식별 및 위험평가, 영향분석, 그리고 재난위험요소 경감으로 구성된다.

위험요소 식별 및 위험평가 결과로 도출된 기업의 중점관리 대상인 사이버 재난이 발생했을 경우, 주요 기업 활동 기능이 상실될 가능성과 이로 인한 예상 손실규모를 예측하는 영향분석을 한다. 이 결과로 기업 활동 우선순위, 복구목표시간 및 최소한의 요구자원이 도출되는데, 이 내용들은 사업연속성 전략 수립을 위한 기본이 된다.

기업은 사이버재난의 경감을 위해서 평상시에 피해경감전략의 개발과 영향분석에서 산출된 주요업무를 보호하기 위한 평상시 주요업무 보호전략을 개발하고, 이 전략에 따라 경감계획을 수립한다. 재난 발생 시 대응하기 위한 대응전략을 개발하고 이를 기반으로 대응계획을 수립한다. 또한 재난 발생 시 주요업무의 연속성을 확보하기 위하여 사업연속성확보 전략을 개발하고, 이 전략에 따라 사업연속성확보 계획을 수립한다. 그리고 재난 발생 후, 기업경영을 정상적 수준으로 복구하기 위해서 기업자산 및 일반업무에 대한 복구 전략을 개발하고, 이 전략에 따라 복구계획을 수립한다.

4.2.2 전략계획

재해경감활동 계획 수립의 두 번째 단계는 전략계획 단계로 경감 · 대응 · 사업연속성확보 · 복구에 관한 세부적인 전략을 수립하는 단계이다. 전략계획은 기업 활동을 안정적으로 유지하기 위한 전반적인 범위를 결정하고, 기본 지침을 수립하는 것이다. [표 8]과 같은 이전의 활동내용을 기초로 하여 사이버재난 전략계획을 수립한다.

가. 경감전략

기업 재난관리 담당자는 평상시 보호대상 자산 및 주요업무의 위험요소를 제거하거나 제거가 불가능한 위험요소에 대해서 위험 경감전략을 개발해야 한다. 사이버재난 경감전략은 위험으로 인한 피경감 전략과 주요업무에 대한 보호전략으로 구분한다. 경감전략에서는 기업이 추진해야 할 하드웨어적인 구조적 대책(예, 물리적보안, 방화벽, 백신 등)과 소프트웨어적인 비구조적

〔표 8〕 전략 수립 시 고려사항

- 재난관리 정책방향, 보호대상 자산, 자원관리
- 사전단계 위험평가와 영향분석 결과
- 정부시책(법, 경감제도 등), 고객, 협력업체, 시장동향, 기술변화 등의 외부환경요소

〔표 9〕 사이버재난 경감전략 구분

• 피해경감 전략 피해경감전략의 목적은 사이버 위험에 대한 기업의 인식을 충분히 향상시키는 것이며 또한 자산피해, 경제적 비용 (수입손실, 재무성과 감소 등) 그리고 재난으로 인한 기업 활동에 관련된 위험을 최소화 하는 것이다. • 주요 업무보호 전략 평상시 기업이 수행하는 업무와 제공하는 서비스를 보호하기 위해 정기적인 업무점검, 관련 장비 및 설비에 대한 실태점검, 보안점검을 실시하기 위한 기본방침을 수립한다. • 비용과 편익 제한된 경감대책들은 대책실행에 따른 비용(cost)과 편익(benefit)을 고려해야 한다.

〔표 10〕 대응전략 고려사항

• 예·경보, 상황전파, 대피 • 현장 상황 정보수집, 분석 및 판단 • 지휘, 명령 체계 및 의사소통 체계 • 자원 수급 및 할당 • 외부기관과의 협력 등 • 시설 인프라에 대한 긴급복구 등

대책(관리 및 제도적 측면)에 관한 경감대책 사항이 포함된다.

나. 대응전략

대응 전략은 원칙적으로 기업의 업무와 서비스, 자산보호 활동을 최우선으로 한다. 그러므로 재난의 원인이 되는 사이버사건(cyber incident) 발생 시 초동 대응부터 이후의 재난대응 활동까지 전반적인 사항을 포괄할 수 있는 기본 방침을 수립한다. 이를 위해 [표 10]과 같

〔표 11〕 사업연속성확보 전략 고려사항

• 장비 및 설비의 연속성 확보를 위한 벤더 및 유지보수 업체와의 협력 • 업무대체 수행 인력의 지정 및 훈련 • 대체공급경로의 확보 • 기업 인프라(수송, 통신 등) 중단 시 대체방안 • 복구목표시점에 따른 정보(데이터)의 백업 • 중요 문서(주요업무관련 서류 등)의 보호 • 주요업무와 관련된 협력업체와의 업무유지 방안 • 원부자재 및 제품의 재고관리 • 고객 서비스 유지 등 • 주요업무 수행을 위한 대체업무 장소 확보 • 주요업무에 대한 복구목표시간과 복구목표시점의 결정 • 주요업무 복구를 위한 최소한의 요구자원 확보

〔표 12〕 복구전략 고려사항

• 기업 자산에 대한 피해평가, 복구계획 및 실행 방침 • 일반 업무 복구에 대한 방침 • 기업의 이해관계자에게 전달 할 복구상황 • 복구일정, 자원 동원 및 예산관리 • 외부기관과의 협력체계 등

은 사항을 고려한다.

다. 사업연속성확보 전략

사업연속성확보 전략은 사이버재난 발생시 주요업무의 연속성 확보를 위해 [표 11]과 같은 사항을 고려하여 기본방침 수립해야 한다.

라. 복구전략

사이버재난으로 인한 긴급복구 이후 기업 경영을 정상적인 수준으로 복구하기 위한 기본방침을 수립하기 위해 [표 12] 사항을 고려하여 수립한다.

4.2.3 사이버 재해경감활동 계획의 수립

마지막 단계인 재해경감활동 계획수립 단계는 기업의 전략계획을 바탕으로 경감·대응·사업연속성확보·복구 계획을 수립하는 것을 의미한다.

가. 경감 계획

사이버재난에 대한 경감계획은 경감전략에서 선정된 구조적·비구조적 경감대책에 대한 구체적인 실행계획을 수립하는 단계이다. 경감계획에는 [표 13]과 같은 사항이 포함되어야 한다.

나. 대응 계획

사이버재난 대응계획은 기업의 업무와 자산보호를 최우선으로 고려하여 수립하며, 대응전략을 토대로 초동대응과 사건 확산 방지를 목적으로 수립한다.

특히 사이버재난 대응의 성패는 신속한 초동대처를 통한 확산 방지에 있으므로 초기 발견 및 전파 시간 최

〔표 13〕 사이버재난 경감계획 포함사항

• 경감대책 수행조직 구성에 관한 사항 • 경감대책 수행일정 및 예산에 관한 사항 • 경감대책 수행의 구체적인 방법 • 경감대책 점검 및 평가에 관한 사항 등

소화, 사건을 통제할 수 있는 초동 대응태세의 확립, 초동 대응방법에 대한 신속한 의사결정은 매우 중요하다.

대응계획은 사이버재난 발생 시 기업 활동에 전반적인 대응체계를 정의하는 비상운영계획과 기업 활동 구성원들의 구체적인 활동 절차를 정의하는 표준행동절차로 구성된다.

다. 사업연속성확보 계획

사이버재난 발생 시 기업 활동에 관련된 주요업무를 지속하기 위해 사업연속성확보 계획을 수립한다. 본 계획은 기업이 비상시에도 유연하게 상황에 대처할 수 있도록 포괄적인 방식으로 개발되어야 한다. 이 계획도 사이버재난 발생 시 주요업무를 지속하기 위한 체계를 정의하는 비상운영계획과 주요업무를 담당하는 구성원들의 구체적인 업무절차를 정의하는 표준행동절차로 구성된다.

라. 복구 계획

복구계획은 피해 발생 이후 기업 활동을 정상적인 수준 또는 그 이상의 개선된 상태로 복구할 수 있도록 하는 계획을 말한다. 사이버재난 대응에서는 기반시설과 업무부분으로 분리된 복구계획을 수립해야하며, 실효성 있는 계획수립을 위해 사전에 명확한 복구목표와 절차가 포함되어야 한다.

4.3 재해경감활동

재해경감 활동은 평상시 경감계획에서 제시된 일정에 따라 배정된 예산을 투입하여 구체적인 경감대책을 시행하고 경감활동 결과를 점검하는 것이다.

비상시 대응활동은 사이버재난으로 인한 피해를 최소하기 위한 대응계획과 사이버재난 발생시 주요업무의 지속적인 유지를 위한 사업연속성확보계획, 그리고 사이버재난 발생으로 피해를 입은 기반시설과 일반업무의 복구를 위한 복구계획에 따라 활동하는 것을 의미한다.

4.3.1 지시통제

기업은 비상시 효과적인 대응활동을 전개하기 위하여 사이버재난 발생의 원인에 대한 정확한 정보를 신속하게 수집할 수 있는 체계를 마련하여야 한다. 지시·통제·협의조정은 사이버재난 발생 시 수립된 대응 및 사업연속성확보 계획에 근거하여 재난 및 주요업무를 효과적이고 효율적으로 통제할 수 있도록 설계된 체계이다. 지시·통제·협의조정은 초동대응, 재난상황관리 운영, 현장수습 및 관리, 주요업무의 연속성 활동으로 구성된다.

가. 초동 대응

사이버 재난발생시 초기에 사건 확산을 방지하기 위한 목적으로 수행하는 초동대응은 피해확대를 최소화할 수 있으며 다음과 같은 사항이 중요하다. 특히 7일월 7일 디도스 사고에서 경험한 바와 같이 일부사이버재난은 재난의 상황판단에 어려움이 있기 때문에 사전에 명확한 의사결정 기준이 수립되어야 한다,

- 사건 신고, 접수 및 전파
- 초기 사건 진압을 위한 지시·통제
- 초동대응 수행 방법에 대한 의사결정

나. 재난상황관리 운영

사이버재난 상황관리에서 특정분야에 대한 전문적이고 기술적인 능력이 요구될 수 있다. 예를 들면 디도스 공격, 해킹 공격, 새로운 형태의 사고 등이 그러한데 사고별·유형별 계획된 관리가 중요하다 하겠다.

- 기술적 정보수집 및 분석
- 상황예측 및 평가
- 비상대응을 위한 구체적 의사결정 및 공유
- 수립한 결정사항의 실행

다. 현장수습 및 관리

사이버재난은 신속한 상황예측 및 판단을 통해 짧은 복구목표시간 내에 주요업무를 재개해야 하는데 이를 위해서는 재난 발생 시 지시통제에 따른 사고처리와 외부기관과의 협력 조정도 중요하다.

라. 주요업무의 사업연속성 확보활동

사이버재난 발생 시 주요업무 현황의 지속적인 모니터링에 의한 상황을 예측하고 판단하여 목구목표시간 내에 주요업무 재개를 위한 지시통제를 해야 하며 아울러 주요업무 재개상황을 전달해야 한다.

4.3.2 상황전파체계

기업은 재산피해를 최소화할 수 있도록 사이버위험

〔표 14〕 사이버재난 예·경보 계획 포함사항

- 동원할 수 있는 모든 자원
- 재난 상황실 가동 여부 판단 등
- 예·경보 대상 파악 (기업조직 내부, 고객, 이해관계자 등)
- 사이버재난의 유형과 규모에 따른 발령 및 해제
- 사이버재난의 유형과 규모에 따른 행동요령의 전파

자료들을 수집·분석하고 사이버재난 발생 가능성 등 위험정보를 고객 및 이해관계자에게 먼저 예·경보할 수 있도록 구축·운영하여야 한다. 사이버재난은 일반적으로 통신단절을 수반할 수 있기 때문에 예·경보 대처가 쉽지 않다. 이를 위해 통신망 단절을 고려한 별도 예·경보 방안이 마련되어야 한다.

상황전파는 사이버재난 발생에 대한 정보를 기업 내외부에 전달하며 상황에 따라 필요한 재해경감활동을 실행하는 것이다.

4.4 교육과 훈련

사이버재난 관리를 위한 사전교육 프로그램은 재난발생 가능성을 줄이고, 발생 시 복구시간을 최소화 하기 위한 방향으로 시행되어야 한다. 사이버재난 관리를 위한 교육과 훈련에 사이버 기술을 사용할 수 있으나, 실제 재난상황에서는 사용이 불가할 수 있으므로 그 가능성을 고려해야 한다.

4.4.1 재난관리 교육

사이버재난 관리 교육은 기업 사이버 재해경감활동

〔표 15〕 교육 프로그램 포함사항

- 재난관리 정책
- 재해경감활동 운영체계
- 재난위험 관리
- 재해경감활동 계획
  - 전략 계획
  - 경감 계획
  - 대응 계획
  - 사업연속성확보 계획
  - 복구 계획
- 전문 기술교육
  - 대응 기술
  - 복구 기술
- 재해경감 활동
- 모의 훈련
- 재해경감활동 평가 및 관리

〔표 16〕 모의훈련 포함사항

- 사이버재난 관리를 위한 모의훈련 목표
- 사이버재난 관리 모의훈련 방법, 범위, 평가, 참여 대상 등
- 사이버재난 관리를 위한 모의훈련 시나리오
- 사이버재난 관리를 위한 모의훈련 주요 성공 요인
- 사이버재난 관리를 위한 모의훈련 상세 점검표
- 사이버재난 관리를 위한 모의훈련 수행 결과의 평가

의 개발, 실행 및 유지를 위해 필요한 역량 강화를 목적으로 수행한다. 사이버재난 관리 교육 프로그램은 필요 인원에 대한 전문적 기술교육을 포함해야 한다.

4.4.2 모의 훈련

기업은 사이버재난에 대한 모의훈련을 통해 실제 상황의 대응 및 복구 능력을 확인·향상할 수 있다. 모의훈련은 재난 대응을 위한 조직 내·외간의 협력 및 대응 능력 제고와 사이버재난 발생 시 최소 복구목표시간을 이해하는데 효과적이다.

사이버재난 관리를 위한 모의훈련은 훈련목적에 따라 적용 범위, 훈련 방법, 참가 대상, 훈련 빈도를 결정하여 일관성 있게 진행되어야 하며, 세부적으로 달성 여부를 확인할 수 있어야 한다.

4.5 재해경감활동 평가 및 관리

성과평가는 기업의 사이버재난 관리 체계가 관계법령, 기준, 전략, 재해경감활동계획, 교육과 훈련 등에 따라 원활하게 운영되는지 여부를 다시 확인하는 것이다. 이러한 평가는 기업 사이버재난 관리 체계의 전반적인 개선방향을 제시하고 향상관리를 하기위한 기본자료가 된다.

4.5.1 성과 평과 및 경영진 검토

기업은 주기적으로 재해경감활동 성과를 모니터링

〔표 17〕 성과 모니터링 및 측정 절차

- 기업의 필요에 맞는 재해경감활동 평가
- 사이버재해 경감활동의 목표 달성 범위
- 기업 사이버재해 경감활동 계획과 운영기준, 해당 법규 및 규제 요구사항에 대한 부합여부 관찰
- 모니터링 및 평가 결과의 기록

하고 측정하여야 한다. 모니터링 및 측정 절차에는 [표 17]과 같은 사항이 포함된다.

또한 최고경영진은 기업재해경감활동 계획의 지속적인 적합성, 타당성, 그리고 효과를 확실히 하기 위해 성과평과 결과를 주기적으로 검토해야 한다.

4.5.2 유지관리

모의훈련, 성과평가, 정책변경 및 위험관리, 경영진 검토 등에 의한 유지관리를 통해 기업 사이버재해 경감활동 계획이 변경 및 개선되었다면, 기업은 모든 구성원에게 문서화된 변경사항을 배포해야 한다.

V. 결론

기업들은 지금까지 사이버재난 관리를 정보시스템 보안(IT Security) 관점과 IT업무 연속성계획(BCP) 관점으로 대응하여 왔다. 그러나 이러한 대응은 기업 내 전사적인 지원을 만들거나 전체 직원들의 참여와 예산 지원을 받기에는 충분하지 못하였다.

'재해경감을 위한 기업의 자율활동 지원에 관한 법률'은 재난이 발생하는 경우, 기업활동이 안정적으로 유지될 수 있도록 정부에서 기업의 재해경감활동을 지원하고 국가의 재난관리 능력을 증진하기 위한 방안으로 시행되었다.

본 논문은 사이버재난의 관점에서 기업재난관리표준에 따라 재난관리정책 및 운영, 재해경감활동계획수립, 재해경감활동, 교육과 훈련, 재해경감활동 평가 및 관리에 관한 내용을 기술하였다.

사이버재난 발생 시 피해가 큰 기업들은 이번에 개정된 법 조항의 선제적 적용을 통해 전사적 관심을 제고할 수 있을 것이다. 또한 사전에 우수한 경감활동계획을 수립하여 사이버 재해경감활동에 노력한 기업들은 1.25 인터넷 대란이나 7.7 디도스 같은 사고가 반복되더라도 보다 안정적인 기업 활동이 가능할 것이다.

또한 우리나라 '재해경감을 위한 기업의 자율활동 지원에 관한 법률'은 국제적 재난관리의 표준 공식문서로 인증(세계일보 2010.6.21)되어 추진기업의 사이버재난 관리 책임자들에게는 다양한 우수기업 지원혜택 등을 통해 지금까지의 수행해온 사이버 재난관리 업무수행에 있어서 새로운 변곡점(tipping-point)을 경험하게 할 것으로 전망하고 있다.

참고문헌

[1] 이영재, 이성중, 이성일, "IT 리스크 평가사례-국내 건설사 적용사례," 한국재난관리 표준학회 논문지 Vol. 2, No. 1, pp. 47-56, 2009년 3월.

[2] "2010 국가안전관리집행계획," 행안부, 2009년 10월.

[3] "재난관리기준 제정" 행정안전부 고시, 10(17), pp. 11-21, 2010년 3월.

[4] "재해경감을 위한 기업의 자율활동 지원에 관한 법률," 법률 제10225호

[5] "재난 및 안전관리기본법," 법률 제10347호

[6] "정보통신망 이용촉진 및 정보보호 등에 관한 법률," 법률 제10138호

[7] "기업재난관리표준," 소방방재청 고시 제2010-22호, 2010년 4월.

[8] "기업재해경감활동계획 수립지침 (안)" 소방방재청, 2010년 6월.

[9] 한창수, "돌발사태와 기업의 위기대응," 삼성경제연구소 CEO Information(제315호), pp.16, 2001년 9월.

[10] 정환국, 유지현, "디지탈재난 그 의미와 새로운 패러다임," 정보통신정책연구원, 2009년 9월.

[11] R.Albert, H.Jeong, and A.L.Barabasi, "The large-scale organization of metabolic network," Nature 407, pp. 651-654, Oct. 2000.

[12] 이영재, "위기관리," 생능출판사, 2006년 3월

[13] 이장균, "사이버테러의 상시 감시체계를 구축하자," 현대경제연구원, 2009년 7월.

[14] 경찰청 사이버테러 대응센터 www.ctrc.go.kr/ cyber/graph01.jsp

[15] 이철수, "침해사고 국가 대응 체계," 정보보호학회지, 제15권 제1호, pp. 33-40, 2005년 2월

[16] 안문석, 박성진, 맹보학, "전자정부 정보보호 대응체계 구축 방향에 관한 연구," 정보보호학회지, 제13권 제3호, pp. 1~14, 2003년 6월

〈著者紹介〉

이 영 재 (Lee Young Jai)
동국대학교 경영정보학과
정교수, 이학박사
(특)기업재해경감협회 회장.
주요관심분야:
의사결정, BCP,재난관리표준

이 성 중 (Lee Sung Joong)
정회원
동국대학교 경영학박사
하나SK카드 감사실
주요관심분야:
재난관리, IT감사, 위험관리
개인정보보호, 정보보안