정 보 보 호 학 회 지
제26권 제1호, 2016. 2

국내외 BCP 분석을 통한 우리나라 기업에 효율적인 BCP 적용 방안 연구

김 윤 종*, 김 성 현**, 박 미 혜***, 최 승 우****, 김 학 범*****

요 약

최근 세계적으로 발생하고 있는 사이버 공격, 안전 불감증 등의 인재 및 지진, 태풍 등 자연재해로 인한 피해가 증가하고 있는 상황이나 이에 대한 예방, 대비, 대응 및 복구에 대한 일련의 체계적인 활동은 미흡한 실정이다. 본 논문에서는 업무연속성 계획(BCP : Business Continuity Planning)의 정의 및 필요성에 대해 소개하고, 효율적인 BCP에 대해 알아보기 위해 국내외 BCP 현황에 대해 조사 연구하였다. 미국, 영국, 호주, 일본은 각각 정부기관 차원의 체계적인 관리를 통한 시스템을 마련하고 있는 바 그 효과에 대해 검토하여 우리나라 BCP 현황과 비교 분석한 후 우리나라 기업에 효율적으로 적용할 수 있는 방안을 모색해 보고자 한다.

Ⅰ. 서 론

2014년 4월 16일 세월호 침몰, 2014년 11월 24일 소니픽처스 사이버 테러, 2015년 4월 25일 네팔 지진 등 최근 세계적으로 발생하고 있는 인재 및 자연재해로 인한 피해가 증가하고 있는 추세이다. 이는 예방, 대비, 대응 및 복구의 일련 과정을 체계적으로 관리할 수 있는 정부차원의 관리체계가 잘 갖추어져 운용되었으면 피해를 줄일 수 있었을 것이다.

정부는 2014년 세월호 침몰 사고 시 신속하지 못한 대응과 구조지연, 컨트롤타워의 부재 등으로 수많은 인명 피해를 발생시키고 뒤늦게 국가적 차원에서 총괄할 수 있는 국민안전처를 신설하였다. 이는 단순히 컨트롤타워의 역할만으로 가능한 것이 아닌 국가의 기반이 되는 정부, 공공기관, 지방자치단체, 민간기업의 재난 대비에 대한 인식 변화 필요, 위기대응매뉴얼 작성 및 주기적인 훈련을 통한 기업문화 구축, 여러 조직 간 유기적인 협력이 이루어져야 할 것이다.

우리나라 기업들은 IT라는 특정 분야에 중점을 두고 데이터센터, 재해복구센터, 백업센터 등에 집중하여 관심을 가지고 구축을 하고 있는 현실이며 이마저도 대기업, 금융기관을 제외한 일반기업에서는 인재 및 자연재해 등 각종 위험으로부터 기업의 안정적인 운영을 위한 예방 및 대응에 대한 부분은 전혀 갖추어지지 않고 있다고 할 수 있다.

기업의 존폐를 가져올 수 있는 위험에 대한 관리와 업무 중단 시 핵심업무/프로세스에 대한 복구와 업무연속성 확보를 중점적으로 다루는 것은 9.11 사태 이후 미국과 영국의 기업을 중심으로 핵심 경영 활동으로 인식되어 왔다.[1]

반면 우리나라는 정부를 시작으로 공공기관 및 민간기업에서 BCP의 필요성을 제기하고 계획 수립의 필요성을 느끼고 있는 실정이다.

BCP(Business Continuity Planning)는 대내외적인 위험으로 인해 업무를 정상적으로 운영하는 데 문제가 발생할 경우 이에 체계적으로 대응, 복구하여 업무의 연속성을 유지, 보장하기 위한 관리 체계이다.

BCP 수립을 위해서는 비즈니스 위험 평가, 취약성 분석, 업무영향도 분석, 업무복구전략수립, 세부계획수립, 계획실행, 테스트 및 모니터링의 반복적인 사이클을

* 동국대학교 국제정보대학원 (freemover98@gmail.com)
** 동국대학교 국제정보대학원 (toshi15shkim@gmail.com)
*** 동국대학교 국제정보대학원 (mihyemihye@gmail.com)
**** 동국대학교 국제정보대학원 (seungwoo.choi7@gmail.com)
***** 디지큐코리아㈜/동국대학교 국제정보대학원 (khb0305@dongguk.edu)

구성할 수 있다.

또한, 업무 연속성 계획 확보를 위한 책임 의무사항 제공과 예방, 대비, 대응 및 복구의 재난 관리체계를 구축하고 이러한 관리체계를 평가할 수 있는 평가체계를 갖추어야 한다.

따라서 본 논문에서는 국내외 BCP 현황과 문제점에 대해 살펴보고 이를 바탕으로 우리나라 기업에 효율적으로 적용할 수 있는 방안에 대해 모색해 보고자 한다.

Ⅱ. BCP(Business Continuity Planning)

2.1. BCP 정의

각종 재해 발생 시 비즈니스 연속성을 유지하기 위한 방법론. 자연, 인간, 기술에 관련된 각종 요인으로 인하여 발생하는 위험으로부터 비즈니스 운영상에 문제가 생길 경우, 필수 업무를 중단시키지 않거나 중단되더라도 가능한 한 짧은 시간 안에 업무를 회복하기 위한 계획을 수립하는 프로세스 체계이다.

2.2. BCP 구성요소[1]

BCP는 일반적으로 정보시스템을 중심으로 데이터 백업과 시스템 장애/복구에 초점이 맞추어져 있다. 하지만 비즈니스 관점에서 전반적인 업무에 대해 위험 평가, 상시운영계획, 대응 및 복구 활동, 훈련/학습, 위기전달 등을 포함해야 한다.

BCP의 구성요소는 다음과 같다.

① 위험 평가 (Risk Assessment)

위험들 중에서 조직의 취약한 부분에 영향을 미칠 수 있는 위험들을 분류하고, 그 조직과 관련된 위험의 발생 빈도와 영향의 크기를 예상

② 업무영향력 분석 (Business Impact Analysis)

업무 프로세스를 상실 했을 때 손실의 규모를 평가

③ 위험 관리 (Risk Management)

위험을 최소화 할 수 있는 전략을 수립하고, 최선의 대안을 준비하며, 예방 시스템을 구축

④ 안전/보안 (Safety/Security)

주로 인적, 물적 자원의 안전성과 보안문제를 취급

⑤ 비상 계획 (Contingency Plan)

위험 발생으로 인한 대응, 복구, 계획 그리고 훈련 계획을 세우는 비상운영계획

⑥ 대응/복구 (Response/Recovery)

위험으로 인한 인적, 물적 자원 긴급 조치와 비즈니스 프로세스를 복구

⑦ 위기전달 (Crisis Communication)

조직 내/외부에 위기 상황을 알림으로써 적극적으로 위기상황을 대처

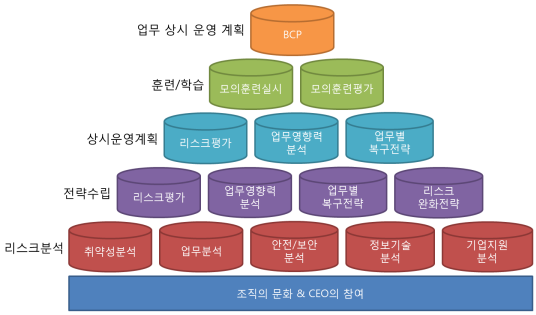
⑧ 훈련/학습 (Exercise / Learning)

평상시 비상운영계획을 수정, 보완

⑨ 조직학습 (Organizational Learning)

경험 또는 다른 사례를 통한 BCP역할의 평가 및 피드백

BCP의 구조는 아래 (그림 1)과 같이 조직의 문화와 경영진의 참여를 기반으로 설계되어야 한다. 상시운영계획은 자원, 업무, 취약성, 정보기술 등 조직의 전체적인 부분의 리스크를 도출하고 이에 따른 리스크평가, 비즈니스 영향력 분석을 바탕으로 전략이 도출되어 이를 가지고 수립되어야 한다. 수립된 상시운영계획은 주기적으로 훈련과 학습을 통해 수정, 보완을 거쳐 위기 상황 발생 시 대응과 복구가 유기적으로 이루어져 정상적인 업무가 유지될 수 있는 BCP 체계를 완성하여야 한다.



〔그림 1〕 BCP 구조

Ⅲ. 국외 BCP 체계 현황

3.1. BCP 국제표준

3.1.1. ISO 22301[2,4]

ISO 22301은 업무 연속성을 확보하기 위해 필수적인 업무의 위험에 대한 보호, 발생가능성의 완화, 대비와 위험 발생 시 복구하기 위한 문서화된 관리 시스템

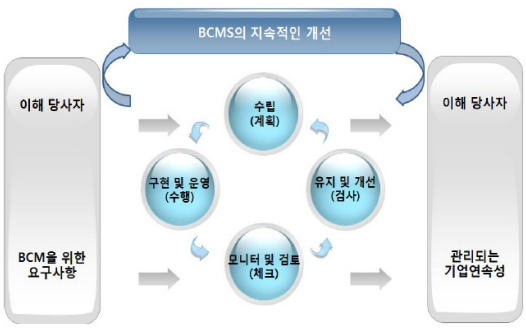
의 기획, 수립, 실행, 운영, 모니터링, 검토, 유지관리 및 지속적 개선을 위한 요건을 명시하고 있다.

ISO 22301의 제정 의도는 BCMS(Business Continuity Management System) 체계에서 획일성을 추구하는 것이 아니라 조직이 조직의 요구사항 및 조직의 이해관계자들의 요구사항에 맞는 BCMS를 설계할 수 있도록 하기 위함이다.

ISO 22301의 주요 내용은 [표 1]과 같다.

조직의 BCMS의 유효성에 대한 기획, 수립, 이행, 운영, 모니터링, 검토, 유지관리 및 지속적 개선과 관련하여 (그림 2)와 같이 PDCA(Plan-Do-Check-Act) 모델을 적용한다.

BCMS는 ① 방침 ② 명시적 책임이 부여된 조직 ③ 관리 프로세스(방침, 계획수립, 이행 및 운영, 성과 측정, 경영진 검토, 개선) ④ 감사 가능한 증거를 제공하는 문서 ⑤ 조직과 관련된 업무연속성관리 프로세스와 같은 요소로 구성된다.



〔그림 2〕 BCMS 프로세스에 적용하는 PDCA 모델

〔표 1〕 ISO 22301의 주요 내용

구분	내용
1	조직의 상황 : BCMS 관리를 위한 조직의 역할
2	리더십 : 경영진의 책무 및 방침, 책임 및 역할
3	계획수립
4	지원 : 자원, 수행능력, 인지, 커뮤니케이션, 문서화된 정보
5	운영 : 운영계획수립 및 위험평가, 연습과 테스트 수행
6	성과평가
7	개선

3.2. 미국의 BCP

2001년 9월 미국 세계무역센터 테러 사건 이후로 미국과 영국은 대규모 재해로 마비된 공공인프라의 기능을 요구시간 내에 업무가 가능하도록 하는 연속성 관리가 민간에 까지 정착되어 있다.

3.2.1. FEMA COOP[5]

미국 FEMA(Federal Emergency Management Agency)의 임무는 모든 위험에 대해 방지, 대응, 복구, 완화할 수 있도록 조직의 능력을 향상시키고 시스템을 구축, 유지함으로써 최초 대응을 지원하는 것이다. FEMA는 부처 간 적절한 협력을 도모 및 감독하고 COOP 기능의 상태를 평가한다. 또한 위기상황에 대한 광범위한 부분에서 미국 정부기관들이 가장 최우선되고 기본적으로 수행되어야 하는 기능을 수행할 수 있도록 COOP(Continuity of Operations) 가이드라인을 제시하였다.

COOP 계획의 목적은 비상사태 시 광범위한 부분에 걸쳐 기관의 중요한 기능을 보장하기 위함이며 그 내용은 다음과 같다.

① 비상시 기관의 필수 기능/작업의 지속적인 성능 보장
② 필수시설, 장비, 기록 및 기타자산 보호
③ 축소 또는 운영에 차질 완화
④ 고객에 대한 모든 서비스의 긴급 재개시의 적절한 질서회복

COOP 계획을 수립한다는 것은 어떠한 비상사태가 발생하더라도 필수적인 기능은 유지할 수 있는 능력을 보유하기 위한 것이며 COOP 기능은 아래와 같은 요소들이 포함되어야 한다.

① 필수 기능
② 요구사항 전달
③ 권한 위임
④ 시설에 대한 연속성
⑤ 의사소통의 연속성
⑥ 필수 기록 관리
⑦ 인적 자원
⑧ 평가, 훈련 그리고 연습
⑨ 통제 및 방향 이양

⑩ 재구성

3.2.2. NIST SP 800-34[6]

미국 NIST(National Institute of Standards and Technology)에서는 정보시스템 관점에서 업무 연속성을 보장하기 위한 가이드라인을 제시하고 있다.

가이드라인은 정보시스템 연속성 계획, 다른 보안의 형태, 비상 관리 계획, 조직적인 회복능력, SDLC (System Development Life Cycle) 사이의 연관성을 근거로 하여 제공되고 있다.

정보시스템 연속성 보장은 계획, 절차 그리고 정보시스템, 운영, 데이터가 재해로 인한 기능 상실로부터 복구가 가능하도록 기술적인 의견을 포함하는 전략을 가지고 편성되어야 한다.

서비스가 이루어지지 않고 있는 시스템에 대한 회복을 위해서는 다음과 같은 접근이 필요하다.

① 대체 장비를 이용한 정보시스템 회복
② 일시적인 시스템 마비의 경우 대체 프로세스(수작업 등)을 통한 업무 처리
③ 원격지를 이용한 정보시스템 회복
④ 정보시스템의 보안에 영향을 미치는 레벨(순서)에 기초하여 적절한 연속성 계획 이행

정보시스템의 연속성 계획의 절차는 다음과 같이 7단계의 절차를 통해 이루어진다.

① 연속성 계획의 정책 개발
② 비즈니스 영향 분석 수행
③ 예방 통제 확인
④ 연속성 전략 생성
⑤ 정보시스템 연속성 계획 개발
⑥ 계획 테스트, 훈련 및 연습 운영
⑦ 계획 유지 운영

3.2.3. Gartner BCP[1]

Gartner가 제시한 BCP 구성요소들은 (그림 3)과 같다. BCP 프로젝트를 진행할 때, 비즈니스 영향력 분석(business impact analysis), 위험 분석(risk analysis), 복구 전략(recovery strategy), 조직 구성(create planning organization), 계획서 및 절차(plan and procedures), 리스크 감소(risk reduction), 비상시 교대시설(implement standby facilities), 테스트(testing) 활동이 수행된다. 그리고 BCP 교육 훈련을 통해서 변화관리를 하게 된다.

<table>
<tr><td colspan="4">PROCESS</td></tr>
<tr><td>Change Management</td><td>Education</td><td>Testing</td><td>Review</td></tr>
<tr><td colspan="4">Testing</td></tr>
<tr><td>Group Planning and Procedures</td><td colspan="2">Risk Reduction</td><td>Implement Standby Facilities</td></tr>
<tr><td colspan="4">Create Planning Organization</td></tr>
<tr><td colspan="4">Recovery Stategy</td></tr>
<tr><td colspan="4">Risk Analysis</td></tr>
<tr><td colspan="4">Business Impact Analysis</td></tr>
<tr><td>Policy</td><td>Organization</td><td>Resources</td><td>Scope</td></tr>
<tr><td colspan="4">Business Impact Analysis</td></tr>
</table>

〔그림 3〕 Gartner의 BCP 구성요소

3.2.4. NFPA 1600[7]

NFPA 1600은 미국에서 위기관리를 위한 재난/비상관리와 업무 연속성 확보를 위한 가장 널리 이용되는 표준으로 미국소방방재협회(NFPA : National Fire Protection Association)에서 제공하는 표준이다. 2013년 재난 및 응급관리와 업무연속성 확보의 표준으로 응급관리 및 업무연속성의 기술위원회에서 NFPA 1600 개정판을 출판하였다.

NFPA 1600에서는 종합적인 리스크 평가란 조직, 주변지역 또는 조직을 지원하고 있는 주요 인프라에 충격을 주는 일련의 발생 가능한 위험, 위협 또는 재난을 식별하는 것이라고 기술하고 있으며 공공부문과 민간부문 모두를 포함하고 있다. 또한, 공공과 민간 사이의 협력의 중요성이 증가하고 있는 바 공공기관, 단체, 민간 기업을 포함하는 협력체계를 다루고 있다.

NFPA 1600의 목적은 예방, 완화, 준비, 대응, 연속성, 복구에 관한 프로그램 개발, 이행, 평가 그리고 유지보수에 대해 근본적인 기준을 제공하는 것이다.

NFPA 1600은 위험과 취약점을 구체화하여 계획수립 시 안내지침을 제공한다. [3]

① 물리적 핵심 기반시설의 안정적인 복원
② 인력의 건강과 안전보호
③ 재난 전달체계의 업무절차
④ 단기복구와 장기간 계속되어야 하는 업무 연속성 모두를 위한 관리구조

3.2.5. GAP for Business Continuity Practitioners[8,9]

민간협회인 DRII(Disaster Recovery Institute International)과 DRJ(Disaster Recovery Journal)이 공동으로 위원회를 구성하여 비즈니스 연속성 실행 가이드라인을 제공하고 있다.

비즈니스 연속성 연습 주제는 10개의 DRII Professional Practice Subject Area로 구성되어 있다.

① 프로젝트 개시 및 관리
② 위험 평가 및 통제
③ 비즈니스 영향 분석
④ 비즈니스 연속성 전략수립 개발
⑤ 비상 대응과 운영
⑥ 비즈니스 연속성 계획 개발 및 구현
⑦ 인식 및 훈련 프로그램
⑧ 비즈니스 연속성 계획 연습 및 유지
⑨ 홍보 및 위기 협력
⑩ 공공단체와의 협력

그리고 각 주제별로 무엇을 해야 하는지(What), 그리고 어떤 방법으로 이를 수행해야 하는지(How)를 구체적으로 기술하고 있고, 마지막으로 기존 문서나 자료 등 수행에 참고할 수 있는 참고문헌(Points of Reference)을 통해 실제 도움이 되도록 하고 있다.

3.3. 영국의 BCP

지난 2005년 런던 지하철 폭탄테러에서의 신속성과 현장성을 확보하기 위한 지역 중심의 위기관리 시스템 운용, 체계적인 전 방위 대응을 위한 유관기관의 공조체계 구축, 사후 수습에 대한 구체적 실행계획, 언론기관의 협조 등은 위기관리의 모범 사례로 남아있다. 이러한 영국에는 정부 내각 산하 비상대비 전담 국가기관인 국가비상대응사무처(CCS : Civil Contingencies Secretariat)가 있다. 이 기관은 영국 내에서 발생하는 모든 재해는 물론 외부에서 영향을 미치는 위험요소에 대응하기 위한 위기관리평가 및 재해복구를 수행하고 있다. 또한, NSCWIP(National Steering Committee on Warning & Informing the Public)라고 하는 비상대응서비스 제공기관, 지방정부, 정부규제기관, 공공시설, 미디어, 산업계의 전문가 집단으로 구성되어 있는 최고 자문기관이 있다.

3.3.1. British Standards 25999, Part 1 and 2[3]

영국에서는 비즈니스 연속성 협회(BCI)와 영국 표준협회(BSI)가 공동으로 지난 2002년에 BCM에 대한 공공 표준인 PA S56을 제정하였으며 이를 기반으로 새로운 국가 표준인 BS 25999를 제정하였다.

BS 25999는 Part 1과 Part 2로 구성되어 있으며 Part 1에서는 BCM에 권장되는 프로세스, 원칙과 용어에 대한 일반적인 지침을 정의하고 있으며 Part 2에서는 BCM을 구현, 운영 및 개선하기 위한 일련의 요구사항을 정의하고 있다. BS 25999 Part 2는 2012년 11월 ISO 22301에 의해 대체되었다.

BS 25999는 Part 1의 내용은 다음과 같다.

① 범위와 적용
② 용어 및 정의
③ 비즈니스 연속성 관리의 요약
④ 비즈니스 연속성 관리 정책
⑤ BCM 프로그램 관리
⑥ 조직의 이해
⑦ BCM 전략 고려
⑧ BCM 대응 개발 및 구현
⑨ BCM 연습, 유지관리, 검토
⑩ 조직의 문화에 BCM 내장

BS 25999는 Part 2의 내용은 다음과 같다.

① 범위 및 요구사항 정의
② 용어 및 정의
③ 비즈니스 연속성 관리 계획
④ 구현 및 운영
⑤ 모니터링
⑥ 유지보수

3.3.2. Good Practice Guidelines 2013[10]

ISO와 함께 국제 표준 중에서 공신력을 가지고 있는 BCI(Business Continuity Institute)는 1994년을 시작으로 2013년까지 가이드라인을 보완하여 왔다. 이 가이드라인은 실무 담당자가 참고할 가이드라인으로 손색이 없을 정도로 구체적으로 작성되어 배포되고 있다. GPG

〔그림 4〕 GPG 2013의 BCM Life cycle

2013은 [그림 4]와 같이 6개의 Chapter로 구성되어 있다.

① 정책과 프로그램 관리 : 업무 연속성의 구현, 통제 그리고 검증과 관련하여 조직의 정책을 정의
② 업무 연속성 내장 : 업무의 활동과 조직의 문화 내에 업무 연속성을 통합하기 위한 방법 모색
③ 분석 : 조직의 목표, 기능 그리고 운영에 관련된 환경은 어떻게 되어 있는지 검토와 평가
④ 디자인 : 적절한 전략과 전술에 대한 식별 및 선택
⑤ 구현 : 업무 연속성 계획 개발 과정의 전략과 전술 실행
⑥ 검증 : 조직의 목표와 업무 연속성 정책 및 목적과 일관성 검증

3.4. 호주/뉴질랜드의 BCP

2006년 기업재난 관리표준인 HB 292-2006을 호주와 뉴질랜드 표준협회에서 공동으로 발간하였으며, 2010년 6월 28일에 호주 업무 연속성 표준(AS/NZS 5050)이 미국 NFPA 1600과 BS 25999과 함께 국제 업무 연속성 관리 표준 중의 하나로 지정되었다.

3.4.1 AS/NZS 5050[11]

AS/NZS 5050 표준은 위험과 연계된 중단으로부터 AS/NZS ISO 31000:2009(Australian and New Zealand risk management standard)에 어떻게 적용할 것인가에 대해 기술하고 있다. 여러 위험의 특징과 위험 관리를 위한 위험 관리 프레임워크에 대한 자세한 가이드라인을 포함하고 있다. 조직의 업무 연속성을 보장하기 위한 방법론을 [표 2]와 같이 제시하고 있다.

〔표 2〕 AS/NZS 5050 방법론

원칙	BS 25999의 목적과 내용에 유사한 원칙 설정
프레임워크	상호 의존성과 의사 결정 프로세스의 모듈화
프로세스	초기 위험 분석
	비즈니스 영향 분석
	중단 관련 위험의 처리
	유지 관리 및 복구 계획 테스트
검증	연속성 문서 및 대처, 책임에 대한 체크리스트 검증

3.4.2. HB 292-2006[1]

호주의 기업재난 관리표준인 HB 292-2006(A Practitioners Guide to Business Continuity Management)는 2004년 판 BCM 지침서 HB 221:2004를 근간으로 하여 개정한 표준문서이다.

① BCM 개념정의 및 개요에 있어 BCM 구현의 기대효과와 전반적인 BCM 프로세스에 대한 설명
② 경영진의 지원과 참여의 중요성 및 업무분담, 자원분배, 수행을 위한 원칙 등을 정의
③ BCM 리스크의 인식, 분석, 평가, 관리, 대응과 모니터링에 중점
④ 비즈니스 영향분석 수행
⑤ 재해 및 위기 시 긴급대응과 복구 단계별 비즈니스 연속성 확보 전략 수립에 대한 가이드
⑥ 대응, 복구를 위한 필요자원 평가 및 확보에 있어 BCM을 위한 조직의 역량 평가 방법
⑦ 일반적 수준과 실무, 구체적 수준으로 구분하여 계획서에 포함되어야 하는 내용의 지침화
⑧ 대내외 위기관리커뮤니케이션과 효과적인 커뮤니케이션 수행방안
⑨ BCM 유지보수(교육, 훈련, 테스트, 주기적인 검토)에 있어 직원에 대한 훈련 및 인식 교육
⑩ BCM 체계의 시동, 배치 가이드를 통해 사고 발생 시 적용된 계획서들에 대한 통제와 조정 작업을

중심으로 구현을 위한 고려사항을 중점적 기술

3.5. 일본의 BCP[2]

일본의 경우 1959년의 이세완 태풍을 계기로 종합적이고 계획적인 방재체제의 정비를 도모하기 위해 1961년 재해대책 기본법이 제정되었다. 일본은 예방, 응급, 복구, 부흥 등 모든 부분을 중앙정부와 지방공공단체에게 권한과 책임이 명확히 정해져 있으며 정부와 민간의 관련 주체가 연계되면서 대책을 강구하고 있다.

3.5.1. Government of Japan BCP Guideline

일본의 BCP 가이드라인은 2005년 8월 제1차 가이드라인을 책정하였고 그 후 2차례 개정판을 공표 하였다. BCP가이드라인의 내용은 모든 위기현상을 극복하기 위한 전략과 대응을 목표로 하여 2013년 8월 3차 개정판을 발표하였으며 내용은 다음과 같다.

① 개념의 정의
② 업무 연속성 관리의 필요성
③ 경영자에게 요구되는 사항
④ 방침의 책정
⑤ 업무 연속성 관리 실시체제 구축
⑥ 분석 및 검토
⑦ 업무 연속성 전략 대책의 검토와 결정
⑧ 계획수립
⑨ 사전대책 및 교육, 훈련 실시
⑩ 검토 및 개선
⑪ 경영자 및 경제사회에 대한 제언

3.5.2. Japanese Corporate Code - BCP

일본의 동경 상공회의소에서 기업의 편의를 위해 BCP 매뉴얼을 제작, 배포하였으며 BCP 홍보 안내, 본편, 매뉴얼 등으로 구성되어 있다. BCP 매뉴얼의 업무 연속성 전략 가이드는 다음과 같다.

① 이중화
② 대기를 갖춘 대체 시설 준비
③ 건물에 대한 대체 시설 부지 준비
④ 아웃소싱
⑤ 경영 통합, 합병
⑥ 현지 복구
⑦ 새로운 사업에 관여
⑧ 재택근무

3.5.3. 일본 중소기업청의 BCP

일본 중소기업청에서는 BCP 보급, 촉진을 목적으로 중소기업의 특성과 실제 상황에 맞도록 기본코스, 중간코스, 고급코스로 구성하여 BCP 매뉴얼을 제공하고 있다.

3.6. 국외 BCP 체계 비교

국외 BCP 체계는 (그림 5)와 같이 정부와 민간의 상호 유기적인 협력 하에 체계가 갖추어져 있다.

미국은 공공, 민간 사이의 협력의 중요성을 바탕으로 정부기관과 협회 등 단체가 그 성격(특정 분야)에 맞는 가이드라인을 제공하고 있으며, 영국의 경우 지역 중심의 위기관리 시스템을 운용, 정부와 함께 체계적인 전방위 대응을 위한 공조체계가 구축되어 국제적 공신력을 지니고 있다.

호주는 표준협회의 기업재난 관리표준과 함께 ISO31000을 기반으로 국가 표준을 제작하여 국제 표준의 하나로 지정되는 수준으로 체계를 갖추고 있으며, 일본의 경우 지역적 특성을 바탕으로 자연재해에 대비하여 중앙정부와 지방자치단체의 명확한 역할을 가지고 상호 연계하여 운영되고 있다.

또한, 국제 표준인 ISO 22301은 BS 25999를 바탕으로 획일적이지 않고 조직의 특성과 요구사항에 맞는

미국	정부	FEMA COOP NIST SP 800-34
	민간	NFPA 1600 Gartner BCP GAP BCP
영국	정부	BS 25999
	민간	GPG 2013
호주	정부	AS/NZS 5050
	민간	HB 292-2006
일본	정부	내각부 BCP Guide line 중소기업청 BCP Manual
	민간	상공회의소 BCP Manual

〔그림 5〕 국외 BCP 체계 비교

BCP를 설계할 수 있도록 되어 있다.

Ⅳ. 국내 BCP 체계 현황

우리나라에는 기업을 위한 업무연속성 가이드라인 및 매뉴얼 뿐 아니라 정부/지자체/공공기관의 업무중단 시 이를 연속화하기 위한 절차나 프로세스가 일부 존재 하나 BCP에 대한 활동은 아직 미흡하다. 국내에서는 2008년도에 대한민국 재해경감을 위한 기업의 자율 활동 지원에 관한 법률을 시행하고, 재난관리표준을 고시, 기업 재해경감협회를 설립하여, BCP 활동을 지원하고 있다.

4.1. 대한민국 재해경감을 위한 기업의 자율 활동 지원에 관한 법률[12]

이 법은 소방방재청 소관으로 2008년에 시행되어 2011년에 개정을 실시하였으며, 태풍, 지진 등 자연재난이 발생하는 경우 기업 활동이 중단되지 아니하고 안정적으로 유지될 수 있도록 하기 위하여 기업의 재해경감 활동을 지원함으로써 국가의 재난관리 능력을 증진함을 목적으로 하며, 내용은 다음과 같다.

① 총칙
② 재난관리표준
③ 재해경감 우수기업의 인증 및 업무대행
④ 우수기업에 대한 지원
⑤ 재해경감활동 기반조성
⑥ 보칙

4.2. 기업재난관리 표준

재난관리 표준에는 다음 사항이 포함되어 있다.

① 재해경감활동 조직·체계 등의 구성에 관한 사항
② 재해경감활동 관계 법령 준수·절차 및 이행에 관한 사항
③ 위험요소의 식별, 위험평가, 영향분석 등 재난 위험요소의 경감에 관한 사항
④ 자원관리 및 기업과 재해경감 관련 단체와의 협정에 관한 사항
⑤ 재해경감을 위한 전략계획, 경감계획, 사업연속성확보계획, 대응계획 및 복구계획의 수립에 관한 사항
⑥ 재해경감활동과 관련된 지시·통제·협의조정 등 비상시 의사소통 및 상황전파 체계에 관한 사항
⑦ 교육·훈련을 통한 자체평가 및 개선에 관한 사항

「재해경감을 위한 기업의 자율 활동 지원에 관한 법률」 제5조에 따라 기업의 재해경감활동계획 수립을 위한 재해경감활동 관리체계 구축, 운영 및 실행, 교육과 훈련, 감시 및 검토, 유지관리 및 지속적 개선 등의 표준화된 절차와 원칙을 규정한다.

4.2.1. 재해경감활동 관리체계 모델[13]

기업재난 관리표준은 재해경감활동 관리체계의 수립, 운영 및 실행, 교육과 훈련, 감시 및 검토, 유지관리 및 지속적 개선 등을 위한 프로세스 접근방법은 (그림 6)과 같이 P(Plan)-D(Do)-C(Check)- A(Act) 모델을 적용하며 PDCA 모델의 주요 내용은 [표 3]과 같다.

재해경감활동 관리체계를 확립하기 위한 기업재난 관리표준의 주요 구성 체계는 [표 4] 및 (그림 7)과 같다.

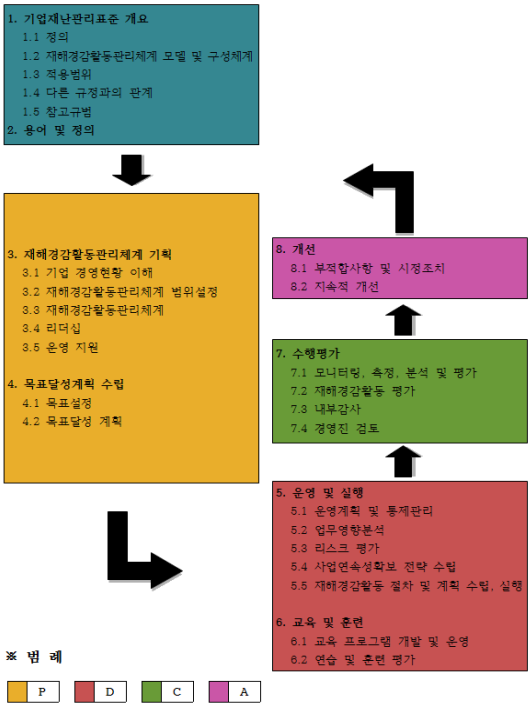
〔그림 6〕 재해경감활동 관리체계 적용 모델

〔표 3〕 PDCA 모델의 주요내용

구분	주요내용
Plan (계획수립)	기업의 정책 및 목표, 이해관계자의 요구사항에 따라 결과를 도출하는데 필요한 재해경감활동 목표 및 프로세스의 절차 수립
Do (운영 및 실행)	재해경감활동 목표 및 프로세스 절차의 실행
Check (감시 및 검토)	재해경감활동 정책 및 목표의 성과를 평가하고 검토하여 관리자에게 시정 및 개선 활동사항을 결정하도록 권한 위임
Act (유지관리 및 개선)	관리자 검토, 재해경감활동 관리체계의 범위, 정책 및 목표에 대한 재검토와 시정조치를 통한 지속적인 개선

〔표 4〕 기업재난관리표준 구성 체계

구분		주요내용
1절. 개요		계획 수립에 관한 일반적인 사항
2절. 용어의 정의		용어에 대한 설명
Plan	3절. 재해경감 활동관리 체계 기획	재해경감활동 관리체계 기획을 위한 기업 경영현황 분석, 요구사항 및 범위, 최고 경영진 및 관리자의 역할, 운영 지원 등에 대한 사항
	4절. 목표달성 계획 수립	재해경감활동 관리체계의 목표 및 목표달성 계획 수립 등에 대한 사항
Do	5절 운영 및 실행	재해경감활동 실행 과정으로서 업무영향분석 및 리스크 평가, 사업연속성 전략 수립, 재해경감활동 절차 수립 및 실행 등에 대한 사항
	6절 교육 및 훈련	재해경감활동 관리체계를 효과적으로 실행하기 위한 교육프로그램 개발, 운영 및 연습에 관한 사항
Check	7절 수행평가	재해경감활동 관리체계 수행평가와 유효성 검증을 위한 절차와 프로세스
Act	8절 개선	감사 및 검토를 통해 시정사항을 식별하고 지속적인 개선을 위한 요구사항



〔그림 7〕 기업재난 관리표준 구성체계도

4.2.2. 재해경감활동 관리체계 모델 적용범위

기업재난 관리표준은 재난의 예방, 대비, 대응 및 복구 각 활동에 있어, 계획 수립, 운영 및 실행, 감시 및 검토, 유지관리 및 지속적 개선을 수행하는데 필요한 요구사항들에 대하여 문서화된 관리체계를 규정한다. 다만, 기업의 특성에 따라 재난의 범주에 포함되지 아니하는 업무중단 사고의 경우에도 준용할 수 있다.

본 표준은 영리를 목적으로 「상법」 제172조에 따라 법인설립등기를 마친 기업 또는 「소득세법」 제168조 및 「부가가치세법」 제5조에 따라 사업자등록을 한 기업에 적용된다.

4.3. 국내 BCP 체계의 발전 방향

국내에서는 2008년도에 재해경감을 위한 기업의 자율 활동 지원에 관한 법률을 시행하고 있으며 업무 연속성 계획의 절차나 프로세스가 일부 존재 하나 그에 따른 실제 훈련 등의 활동은 미흡한 실정이다.

국외 정부와 민간에서 상호협력 하에 갖추고 있는 업무 연속성 계획 체계 및 표준을 통해 우리나라의 체계 및 표준과 정부, 공공기관, 지방자치단체, 민간기업 등 여러 조직 간 유기적인 협력이 원활하게 이루어지지 않고 있음을 되짚어 볼 수 있었으며, 우리나라에 보다 수준 높고 실현 가능한 체계를 구축하는데 도움이 될 것으로 생각한다.

2014년 세월호 침몰 사고 시 신속하지 못한 대응과 구조지연, 컨트롤타워의 부재로 인한 체계적인 지원 활동 미비, 인식 및 훈련의 문제점을 보였다. 이러한 문제점을 해결해 보고자 국가적 차원의 컨트롤타워인 국민안전처를 신설하였다.

이는 단순히 정부 부처의 신설에서 그치는 것이 아닌 재해 대비에 대한 인식 변화, BCP 체계 표준 개발, 매뉴얼 및 가이드라인 작성, 주기적인 훈련을 통한 보완 및 갱신, 경영진의 참여를 바탕으로 한 기업문화 구축, 여러 조직 간 유기적인 협력이 이루어질 수 있도록 유도, 지원에 만전을 기해야 한다.

Ⅴ. 결 론

최근 세계적으로 자연재해 및 인재로 인한 피해가 증

가하고 있는 상황이나 이에 대한 인식 및 대비에 대한 활동은 미흡한 실정이다. 이는 아직까지 정부기관 등 주체의 제도적 장치 및 상호 협력 등의 부재로 인해 기업의 업무에 있어 재난 대비에 큰 의미를 부여하지 않고 있기 때문이다. 하지만 업무 연속성 계획은 단지 논의의 대상이 아니라 국가와 조직 및 기업들의 필수 당면 과제로 대두되고 있다.

지금까지의 재해에 대한 복구 계획은 IT라는 특정 분야에 중점을 맞춘 데이터센터, 재해복구센터, 백업센터 구축 등을 중심으로 진행되어 왔으나, 이제는 업무 연속성 계획 수립을 통해 기업의 전사적인 관점에 초점을 맞추어야 한다. 즉, 업무 연속성 계획은 더 넓은 범위에서 조직의 문화와 구조 및 경영진의 적극적인 참여를 바탕으로 전략적인 차원에서 다루어져야 한다는 것이다. 기업에서의 인재 및 자연재해 등 각종 위험으로 인한 업무 및 서비스 중단은 단순히 기업의 문제만으로 돌릴 수 없으며, 이는 그 규모에 따라 관련된 고객과 이해 당사자들의 문제 일 뿐 아니라 나아가 그 조직이 국가 조직 일 경우 대규모의 사회적인 문제로까지 확장 될 것은 당연한 일이다.〔14〕

업무 연속성 계획의 목적은 각종 위험으로 인한 비상사태 발생 시 우선순위에 따라 조직의 필수 업무를 지속하고, 적정시간 안에 순차적으로 업무를 회복 하는데 있다. 이러한 목적 자체는 언제 어디서나 변함이 없지만, 그 운영 방안 및 구성 내용은 조직의 문화와 업무환경 그리고 조직 간 상호 협력이 원활하게 이루어질 수 있도록 적절하게 구성되어야 한다.

본 연구에서는 업무 연속성 계획의 중요성을 고찰하고 우리나라 보다 선진화된 국외의 동향을 소개 및 연구, 분석하여 보다 향상된 업무 연속성 계획의 방안을 모색해 보고자 했다.

본 연구에서는 미국, 일본, 영국, 호주의 정부 및 민간의 업무 연속성 계획에 대하여 소개하고, 국내 현황에 대해서 조사 하였다.

이를 통해, 보다 나은 업무 연속성 계획을 수립하여 불의의 사고나 위험으로부터 업무의 중단을 해소하고, 중요 시설 및 정보시스템 등의 중요 자산의 장애 또는 위험의 영향으로부터 핵심 업무 프로세스를 보호하며 예방과 복구 통제의 일련의 과정을 거쳐 수용할 만한 수준으로 업무 연속성 활동을 지원 할 수 있어야 한다,

향후, 연구에서는 최신 국내외 업무 연속성 계획 동향을 분석하여 전사적인 관리체계 조직 구성 및 조직의 문화 개선, 가이드라인 및 매뉴얼 구축, 더불어 평가체계에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] 우종협, “자연재해 대비를 위한 기업의 BCP 도입 방안에 관한 연구”, *서울산업대학교 산업대학원 석사학위* 논문, 2009.

[2] “ISO 22320,22300,22301에 관한 사회안전 분야 국제표준의 효율적인 국내 도입방안”. 소방방재청. 2012.

[3] 권영택, “일본의 기업 BCP(사업연속성계획) 제도 분석 및 한국의 정책적 시사점에 관한 연구”, *서울시립대학교 일반대학원 박사학위* 논문, 2014

[4] ISO 22301 *http://www.pecb.org/iso22301*

[5] https://www.fema.gov/

[6] NIST SP 800-34 rev 1 (Nov 2010)

[7] NFPA 1600 2013 Edition http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600

[8] www.drj.com/GAP/gap.pdf

[9] www.drii.org/docs/professionprac.pdf

[10] www.bcifiles.com/GPG2013PresentationforBCAW.pdf

[11] https://complispace.wordpress.com/tag/asnzs-505 02010/

[12] 대한민국 재해경감을 위한 기업의 자율활동 지원에 관한 법률 “소방방재청”

[13] 기업재난관리표준 “소방방재청”

[14] 강희조, “업무연속성계획(BCP)관점에서 위기관리 통합체계 구축” 목원대학교.

〈저 자 소 개〉

김 윤 종 (Yun-Jong KIM)
정회원
2013년 9월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 정보보호, 거버넌스

김 성 현 (Sung-Hyun KIM)
2013년 9월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 정보보호, 클라우드 보안

박 미 혜(Mi-Hye Park)
2013년 9월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 정보보호, 소프트웨어 공학

최 승 우(Seung-Woo Choi)
2013년 9월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 정보보호, ISMS

김 학 범 (Hak-Beom KIM)
정회원
1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2015년 5월~현재 : 디지큐코리아(주) 부사장
관심분야 : ISO 27001, PIMS, ISMS, 클라우드컴퓨팅 보안, 개인정보보호