情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

사업연속성을 위한 정보통신 인프라 대비체계의 국제 표준화 동향연구

이 성 일*, 김 정 덕**

요 약

2009년 발생한 DDoS 사태는 정보통신 인프라에 대한 높은 의존도를 나타내는 국내 산업에 있어 보안사고가 심각한 업무 중단 사태를 나타낼 수 있음을 보여주었고 정보통신 인프라 측면에서 사업연속성에 대한 대비체계가 필요함을 시사하고 있다. 국제 표준화 기구인 ISO(International Standard Organization)에서는 보안 사고에 국한된 개념이 아닌 사업연속성을 방해하는 모든 재난 및 재해에 대한 대비체계를 미국, 영국, 호주, 일본 등 재난관리 선진국의 표준을 총망라하여 TC(Technical Committee) 223을 통해 표준(안)으로서 제시하고 있다. TC223 표준(안)의 핵심은 사건, 사고에 대한 대비 및 운영 연속성 관리를 의미하는 IPOCM(Incedent Preparedness and Operational Continuity Management) 프레임워크이며 이러한 IPOCM의 개념은 정보통신 인프라 측면에서 사업 연속성에 대한 가이드라인을 제공하는 SC(Standard Committee) 27의 "ISO/IEC 27031 Guidelines for ICT readiness for business continuity" 표준(안)에 기반을 제공하고 있다. 이러한 국제 표준화 동향을 토대로 본 논문에서는 사업연속성을 위한 국내 정보통신 인프라 대비체계에 포함될 주요 구성요소와 구축 요구사항을 제안하고자 한다.

Ⅰ. 서 론

분산 서비스 거부(Distributed Denial of Service : DDoS) 공격은 해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버로 공격을 하여 특정 시스템 자원을 고갈시킴으로서 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법이다.

2009년 7월 7일부터 만 3일 동안 좀비 PC 11만 5천여 대가 청와대 홈페이지를 포함, 국내·외 주요 홈페이지를 공격하여 접속 장애를 발생시켰다. 정확한 경제·사회적 피해현황은 조사되지 않았지만 최소 363억원에서 최대 544억원의 금전적 피해가 발생한 것으로 추정되며 피해기관의 신뢰도에도 부정적인 영향을 미친 것으로 추정된다[1].

7.7 DDoS 공격은 치밀하게 계획된 공격방법으로 서버에는 처리 지연(혹은 불가능)을 초래하였으며, 치료되지 않은 일부 좀비 PC에서는 주요 문서와 하드디스크를 손상시켰다. 또한, 지금까지 악의적 목적으로 이루어진 해킹과는 다르게 사회적 불특정 공공재를 겨냥한 무차별 테러의 성격을 띠고 있는 것이 특징이다.

7.7 DDoS 공격과 같은 보안사고에 우리나라 대부분의 조직이 제대로 대처하지 못한 핵심 원인으로는 표준화된 보안사고 대비체계의 부재를 들 수 있다. 표준화된 보안사고 대비체계의 부재는 사이버 공격에 대한 훈련 및 국제 공조의 미흡으로 이어져 예방 뿐만 아니라 대처능력에도 심각한 문제점을 나타내고 있다.

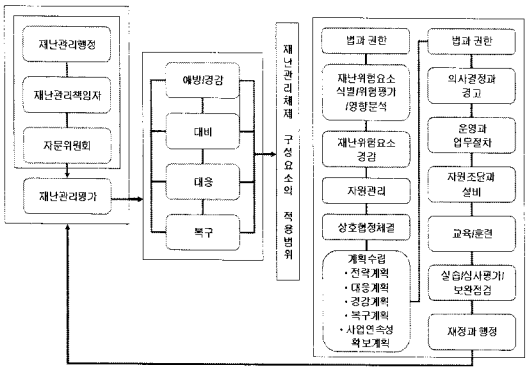
이러한 문제점을 개선하기 위해 본 논문에서는 재난관리 및 업무연속성 관련 국제 표준화 동향과 선진국의 표준을 고찰하여 이와 연계할 수 있는 보안사고 대비체계(사업 연속성을 위한 국내 정보통신 인프라의 대비체계)의 구축 요구사항을 제시하고 한다.

Ⅱ. 선진국의 표준화 현황

2.1 미국의 사업연속성관리 표준 - ANSI/NFPA1600

미국의 NFPA(National Fire Protection Association)

* Ernst&Young Advisory Inc. (seong-il.lee@kr.ey.com)
** 중앙대학교 정보시스템학과 (jdkimsac@cau.ac.kr)



〔그림 1〕 미국의 사업연속성관리 표준 체계

는 공공부문과 민간부문에 종사하는 6만 명의 회원을 보유하고 있으며 이중 25%는 소방업계 종사자로 구성되어 있다. NFPA는 세계적인 비영리규격과 표준기관이며 미국국가표준연구소(ANSI)에 의해서 승인된 표준 개발절차를 준수하고 있다. 또한, NFPA는 다양한 재해 유형에 대처할 수 있는 건축, 생명 안전, 전기 표준을 위한 표준을 개발한다.

ANSI/NFPA 1600은 "재난·응급관리체제 및 사업연속성 확보체제" 표준으로서 공공 부문과 민간 부문을 포함한 모든 단체에 산업표준으로 적용된다[2].

ANSI/NFPA 1600은 아래와 같은 목적을 정의하고 위험과 취약성을 구체화하며 계획수립 가이드를 제공한다.

- 물리적 핵심기반시설의 원활한 복원
- 다양한 재해 유형에 대처 할 수 있는 인력의 건강과 안전 도모
- 경감(예방)/대비/대응/복구 4단계의 업무절차 수립
- 단기 복구 및 장기 사업 연속성 확보를 위한 관리 구조로 수립

재난과 응급상황으로부터 피해를 최소화하기 위하여 ANSI/NFPA 1600은 재난관리체제의 평가, 개발, 수행, 개선과 유지에 대한 범위 등에 관한 의무사항을 정하고 있다([그림 1] 참조).

미국은 다른 선진국들과의 국제표준 추진에 관한 경쟁구도 속에서 ANSI/NFPA1600을 선도 표준으로 제시하기 위한 적극적인 전략을 수립하여 추진 중에 있다.

미국의 국토안보부(DHS), 국방부, 상공부, 주택 및 도시개발부, 중소기업청 등에서는 ANSI/NFPA 1600과 관련 법에 근거한 다수의 사업 연속성 관리 지원 프로그램을 운영하고 있다([표 1] 참조).

〔표 1〕 사업연속성관리 표준에 기반한 민간지원 프로그램

프로그램	목적	수행기관
Hazard Mitigation Grant Program(HMGP)	스탠포드 법에 근거하여 자연재해에 영향을 받을 만한 주택과 사업장의 위험 경감 프로그램	주정부 지방정부
SBA Disaster Mitigation Loan Program	중소기업을 위한 재난 경감 융자 프로그램	중소기업청
The Flood Mitigation Assistance(FMA) Program	주택과 기업주가 소유하고 있는 부동산의 홍수보험 가입시 보험료을 할인	주정부 지방정부
National Flood Insure Program(NFIP)	홍수보험과 홍수범람원 조절 등을 통해 향후 발생될 홍수피해를 줄이기 위해 만들어진 보험 프로그램	FEMA
SBA Disaster Loan Assistance	중소기업을 위한 재난 복구 비용 보조 프로그램	중소기업청
Private Sector Emergency Preparedeness Program	민간부문의 대비 강화를 지원하기 위해 국토안보부의 역할과 책임 명시	국토안보부

2.2 영국의 사업연속성관리 표준 - BS25999-1

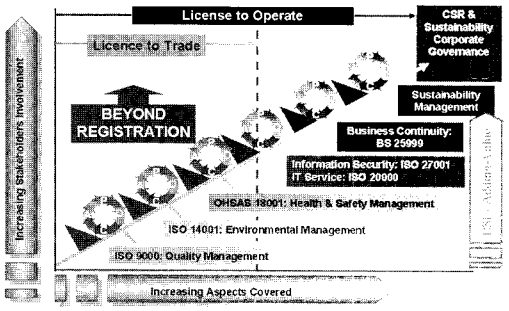
BS 25999-1은 "B2B와 B2C 기반 사업 연속성의 이해, 수립, 집행" 표준으로서 안전관리에 대한 제3자 인증을 전제로 한 시스템 규격이다.

영국의 사업연속성관리 표준은 영국의 국가표준 기관으로서 기업과 사회의 요구사항에 기반한 표준과 표준화 솔루션을 개발하고 있는 BSI(British Standards Institution, 영국표준기관)에 의하여 제정되었다.

BSI는 1901년에 설립되었고 현재는 100여국에 걸쳐서 2,100명의 직원을 보유하고 있다. 특히, 재난관리 표준화와 관련하여 독립적인 관리체제와 상품에 대한 인증, 민간/국가/국제표준개발, 표준과 국제무역에 관한 정보수집 기능을 수행하고 있다.

BS 25999코드는 Part 1, 2로 구성되어 있다. BS 25999-1은 조직 내부에서 사업 연속성을 이해, 수립, 진행하는 기초로서 B2B와 B2C를 강조하고 있다.

BS-25999-2는 조직이 직면할 수 있는 모든 위기에 대응하기 위한 사업연속성 관리체계의 수립, 운영, 모니터링, 검토, 유지, 개선 등 구성요소가 가져야 할 필요



〔그림 2〕 BSI Value Positioning

조건을 구체적으로 제시하고 있다.

[그림 2]에서 나타난 바와 같이 BS 25999를 근간으로 보안사고에 대한 대비체계 수립함으로써 보다 적극적이고 능동적인 대응이 가능하며 동시에 국내 대비체계와 선진국 표준의 연계성을 확인하는 부수적인 성과를 확보할 수 있다[3].

영국의 사업연속성관리 표준은 다음과 같은 특징을 가지고 있다.

첫째, 측면에서 지역 중심의 분권화를 통해 사고 대응의 신속성과 현장성을 확보하고 있다는 것이다. 런던의 경우 지방 차원에서 민·관을 아우르는 재난대응 기관들이 참여하는 재난극복 포럼(RRF)에서 전략적 재난관리계획을 수립하고, 이것을 정밀하게 실천할 수 있는 전략적 조정그룹(SCG)을 비롯한 통제기구를 운용하고 있다.

중앙 재난관리 조직의 경우, 국가적 재난의 경우를 제외하고는 지방정부를 지원하는 역할에 주력하고 있다. 아울러 유관기관 간의 공조체계가 원활히 작동되어 재난관리가 전방위적이고 체계적으로 이루어지고 있는 것도 현장 대응 측면의 또 다른 특징이다.

둘째, 사후수습에 있어서 영국의 재난관리 시스템은 구체적인 실행계획을 바탕으로 사고피해자와 유가족에 대한 전문적인 서비스를 장기간에 걸쳐 제공하여 공적 제도에 대한 신뢰를 제고하고 있다.

셋째, 공동체 유지라는 사회적 규범을 존중하는 영국 언론과 이들의 역할을 중요시하는 정부의 정책에 따라 언론이 재난관리 협조자 역할을 수행하고 있다.

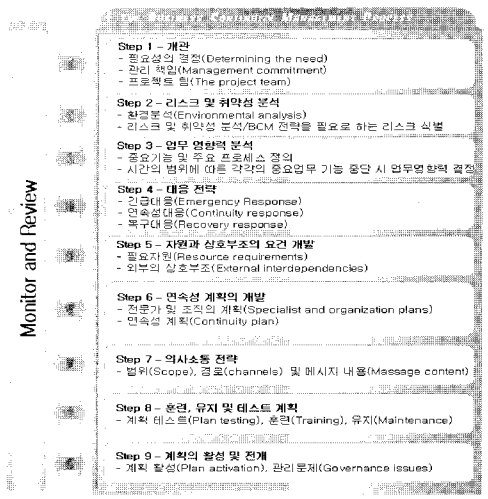
영국은 사업연속성관리 측면에서 놀라울 정도로 신속한 대응력을 갖고 있고, 기업들도 숙달된 재난 대응시스템을 보유하고 있다. 영국의 발전된 재난관리 시스템은 정부와 기업이 수십 년에 걸친 경험, 교육 및 훈련을 되풀이한 산물이다.

2.3 호주의 사업연속성관리 표준
- AS/NZS 4360 HB-221

호주는 사업연속성 관리체계 수립 접근 방법에서 기업의 환경 분석을 언급하고 있으며 다른 국가의 표준과 비교할 때 재무적인 부분과 커뮤니케이션 전략을 분리하여 언급하는 특징이 있다. 전략을 긴급, 연속성, 복구의 세 가지 범주로 분리하여 각각의 단계에서 실행해야 할 행동들을 규정한다. 또한 호주 표준에서는 [그림 3]과 같이 9단계로 세분화하여 단계별로 행동 지침 및 산출물을 제시함으로서 사용자의 용이한 프로그램 적용을 지원하고 있다[4].

이러한 표준에 기반하여 호주에서 가장 광범위하게 사용되고 있는 통합재난관리시스템(ICS: Incident Command System)은 막대한 영향력을 미치는 대규모 사건에 대한 공통적인 관리 문제점을 해결하기 위해 설계되었으며 문제점은 다음과 같다.

- 관리의 비효율적인 범위
- 서로 경쟁하는 조직구조
- 일치하지 않거나 혹은 존재하지 않는 사건 정보
- 호환되지 않는 통신 체계
- 기관들 간의 부조리하고 불합리한 서로 다른 계획
- 불명확한 권한
- 사건을 두고 경쟁하는 기관들
- 일치하지 않는 전문용어



〔그림 3〕 호주의 사업연속성 관리체계

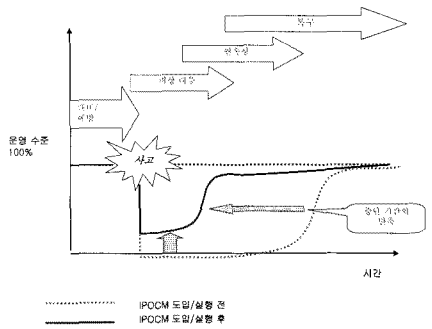
이와 같이 호주 ICS의 체계는 사고 대응에 있어 쟁점화 된 각 기관 간 이슈를 조정할 수 있는 효과적인 방법을 제공한다. 또한 하나의 기관 간 통합사건 지휘 장소에서 개별 관할 대표자들의 통합된 지휘를 확립함으로서 다음과 같은 장점들이 나타난다.

- 단일 사건은 전체 통합재난지휘체계로 전개된다.
- 전략에 기반하여 재난을 해결한다.
- 정보의 순환과 상호 협력은 통합재난 지휘체계 내의 모든 관할대표와 기관들 사이에서 개선되어지고 있다.
- 통합재난지휘체계에 대해 책임이 있는 모든 기관들은 서로 우선적으로 해야 할 일과 할 수 없는 일들이 무엇인지에 대한 분별력을 가진다.
- 기관의 권한 밖의 일이나 비합법적 요구는 조정되어지거나 거절한다.
- 각 기관은 다른 기관의 계획, 역할, 의무에 대해서 완전히 인식한다.
- 모든 기관들의 통합되어진 효과는 하나의 "통합재난대처계획"하에서 각 기관 각각이 담당한 일들을 수행 했을 때 최적화 된다.
- 일에 대한 중복은 회피함으로써 기회 및 비용절감을 할 수 있다.

호주의 ICS 체계는 긴급 재난을 처리하는 통제(Incident Controller), 재난정보의 분석과 수집 및 대처 행동을 수립하는 계획(Planning), 재난 처리를 위한 기관 자원을 관리 및 감독하는 운용(Operations), 재난처리에 필요한 시설, 용역, 재료를 준비하는 물류조달(Logistic)로 구성된다. 이러한 유기적인 체계가 DDoS 사태 같은 보안사고 발생 시 우리나라에서 운영되고 있었다면 혼란을 최소화 한 상태에서 체계적 대응이 이루어질 수 있었을 것으로 판단된다.

Ⅲ. 국제 표준화 기구의 현황

국제 표준화 기구에서 사업연속성관리 분야를 논의하는 모임은 TC223과 SC27이다. TC223은 정보기술에 국한 사업연속성관리를 논의하는 것이 아닌 사회적으로 발생 가능한 모든 재난에 대처할 수 있는 체계를 논의하고 있으며 SC27은 TC223의 회의 결과를 정보보호 분야에 적용한 프레임워크를 제안하고 있다.



〔그림4〕 IPOCM의 개념 체계

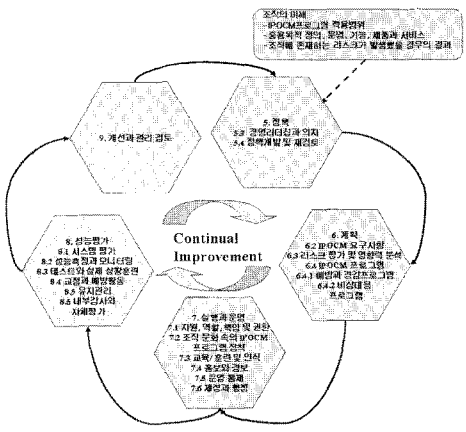
3.1 ISO TC223의 IPOCM 프레임워크

조직의 이해 관계자와 주주들은 조직의 주요 업무와 서비스가 중단되는 것을 피할 수 있도록, 또는 만약 운영과 서비스가 중단되었다면 가능한 빨리 다시 재개될 수 있도록 잠재 사고 및 중단에 대한 능동적 대비를 요구한다([그림 4] 참조).

이러한 관점에서 IPOCM은 조직을 위협하는 잠재적 영향을 확인하고 그 영향을 최소화하기 위한 프레임 워크 제공하는 전반적인 관리 프로세스이다[5].

사고 대비 및 운영 연속성 관리체계의 구축과 지속적인 개선을 위한 프레임워크는 다음의 [그림 5]에 나타나 있다.

그림에 나타난 바와 같이 IPOCM은 변화하는 내부 및 외부 요인에 대응하여 조직의 사고 대비 및 운영 연속성 관리를 위한 효과적인 방향을 제시하고 있다. IPOCM이 제공하고 있는 방안들이 실효성을 나타내기



〔그림 5〕 IPOCM 프레임워크

위해서는 지속적으로 관찰하고 주기적으로 검토해야 하는 관리체계가 필요하다. 이를 위해서는 조직의 모든 레벨에서 사고 대비 및 운영 연속성 개선을 이루기 위한 함께 노력해야 한다. IPOCM 고려 사항들은 모든 조직의 운영 및 사업 의사 결정에 통합될 수 있다.

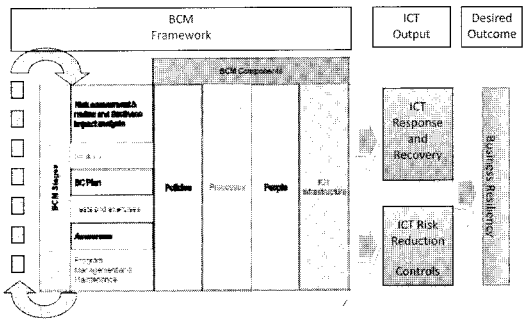
3.2 ISO SC27의 27031

사업 연속성을 위한 정보통신 인프라의 대비체계 표준화를 목적으로 국제 표준화 기구인 ISO 내 SC27에서는 "ISO/FCD 27031 Guidelines for ICT readiness for business continuity" 문서를 준비 중에 있다. 문서 제목에서 "FCD(Final Committee Draft)"의 의미는 최종 협의가 남겨진 버전의 표준(안)을 의미하는 것으로서 연내에 공식 표준으로서 공표될 예정이다.

ISO/FCD27031에서는 정보통신 인프라 (ICT : Information and Communication Technology)의 보안사고 대비체계를 명확히 사업연속성관리체계의 일부로서 정의하고 있으며 정보통신 인프라의 보안사고 대비체계가 사업연속성관리체계의 일부분으로서 통합될 것을 강력히 권고하고 있다. 이러한 개념적 목표에 기반하여 표준(안)에서는 이전 단락에서 언급한 IPOCM의 연속성관리 프레임워크를 적극적으로 참조하고 있으며 핵심 참조 표준으로서 명문화 하였다. 다음 단락은 ISO/FCD27031에서 사업연속성관리의 일부로서 정보통신 인프라의 보안사고 대비체계를 언급한 내용이다.

사업연속성관리는 조직의 일상적 비즈니스 활동을 위협하는 모든 요소를 식별하고 이들에 대한 안전하고 효과적인 대응 역량을 고취시키기 위한 전사 단위의 경영프로세스이다. 이러한 사업 연속성 관리체계의 일부로서 정보통신 인프라의 보안사고 대비체계는 조직의 사업연속성관리 및 정보보호관리체계 같은 경영시스템을 지원하고 연계할 수 있어야 한다([그림 6] 참조).

정보통신 인프라가 조직의 핵심 비즈니스를 지속적으로 지원하고 있음을 입증하기 위해서 정보통신 인프라의 가동 중단을 야기할 수 있는 다양한 보안사고에 대한 예방, 대비, 대응 및 복구체계를 수립하여야 하며 이러한 대비체계를 표준(안)에서는 IRBC(ICT Readiness for Business Continuity)의 개념으로 설명하고 있다[6].



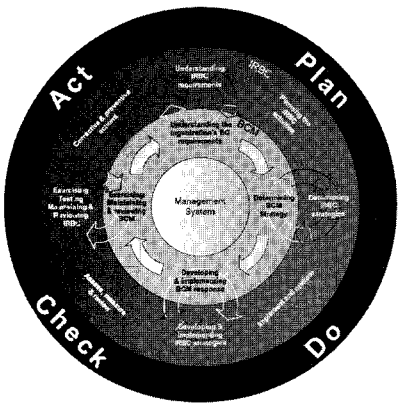
[그림 6] 사업연속성관리체계 내에서 보안사고 대비체계의 위상

ISO/FCD 27031에서는 정보통신 인프라의 보안사고 대비체계가 사업연속성 관리체계의 일부로서 정의되기 위해서는 계획-실행-평가-개선의 생명주기가 필요함을 언급하고 있으며 다음의 그림과 같이 최종 목표 이미지를 제시하고 있다.

정보통신 인프라 보안사고 대비체계가 계획, 실행, 평가, 개선의 생명주기를 내재하기 위해서는 계획의 수립 뿐만 아니라 다양한 상황 시나리오에 기반한 모의훈련이 활성화되어야 하며 이에 따른 계획의 갱신과 현실화가 지속적으로 수행되어야 한다.

Ⅳ. 국제 표준화 동향에 따른 시사점

이번 단락에서는 ISO에서 제시한 국제 표준과 선진국(미국, 영국, 호주) 표준의 비교 분석을 통해 정보통신 인프라의 보안사고 대비체계가 수용해야 할 요건을 식별해보고자 한다. DDoS 같은 전 세계적인 공격에 대



[그림 7] 정보통신 인프라 보안사고 대비체계의 목표 이미지

해 전 세계가 협력하여 대응체계를 실행하고자 할 경우 우리나라의 대비체계와 국제 표준 대비체계의 연계성은 매우 중요한 요소이므로 본 논문에서 제시하는 요건을 최소한의 요구사항으로 결정하여 보다 발전적인 대비체계가 개발되어야 한다.

ISO/TC223에서 공표한 IPOCM의 개념은 선진국 표준의 통합된 형태로 구성되어 있고 ISO/FCD27031은 이러한 IPOCM의 개념을 100% 수용하고 있다. 이러한 연관관계에 기초하여 본 논문에서는 [표 2] 와 같이 정보통신 인프라 보안사고 대비체계의 필요 요건을 도출하였다.

〔표 2〕 정보통신 인프라의 보안사고 대비체계 수립을 위한 필요요건 도출

필요 요건	ISO 표준	각 국 표준		
목차	내 용	미국	영국	호주
프로그램 재정	IPOCM의 정의	○	○	○
	IPOCM의 목적	○	○	
IPOCM 프로그램 적용 범위	IPOCM의 범위	○	○	○
	IPOCM의 문서화	○	○	
	조직의 이해관계자 구성	○	○	○
정책				
정책	정책수립	○	○	○
	정책문서화		○	
	정책 검토			
경영리더십과 의지	위원회 구성	○		○
	실무조직 구성	○	○	○
정책 재검토	정책 재검토			
	최고경영진의 정책검토			○
	실무조직의 정책검토			○
수행을 위한 조직상 구조	IPOCM 프로그램 위원회 조직화		○	
	IPOCM 전문가 구성		○	
계획				
일반사항	리스크 분석, 평가, 계획 수립의 전체적인 프레임 워크 소개	○	○	○
합법적인 다른 요건	관련법규	○		
재해, 위험 및 위협의 식별	재해, 위험, 위협의 지속적인 확인	○	○	
	발생 가능한 리스크 식별	○	○	○
위험분석	식별된 리스크에 대한 우선순위 결정	○		○
	취약성 유발요소 선정	○	○	○
	정량적/정성적 방법을 통한 리스크 산정			
영향력 분석	프로세스 상실로 인한 업무 영향력 측정	○	○	○
	복구우선순위	○	○	○
	최소요구자원	○	○	○
	조직핵심 업무프로세스 식별		○	○
영향력 분석 절차	영향력 평가	○	○	○
	-복구우선순위 절차	○	○	
	-업무 손실의 측정	○		
	-목표복구시간	○	○	
	-복구자원 추출		○	○
IPCOM 프로그램	IPOCM의 지속적 개선		○	
	IPOCM의 구조		○	
제지 및 완화 프로그램들	리스크 대응 구조의 재배치, 개선 또는 제거	○		
	리스크 요인의 제거	○		
	리스크로 인한 비용감소의 노력	○		
	리스크 요인 발생률의 통제	○		
	전자적, 물리적 리스크 대응을 위한 방어 시스템 및 장비의 설치	○	○	
	핵심인원 및 중요 시스템, 장비, 정보, 운영체계, 원자재 등의 이중화	○	○	○
응답관리 프로그램	긴급응답		○	○
	연속응답			○
	회복응답			○
비상대응관리 프로그램	현장의 상황관리		○	
	지시 명령	○	○	
	조직 내외부의 인적, 물적 자원 수 급 및 할당 방법	○	○	
	응급조치와 응급복구를 위한 우선 순위 지정		○	
	소방서, 경찰서, 병원, 정부기관 등 외부기관과의 협력	○	○	
	이해관계자에게 상황전달		○	○
실행과 운영				
자원, 역할, 책임 및 권한	조직화(역할, 책임, 권한)	○	○	
	-일반 조직도 상의 직무에 비상사태를 대비한 일상점검 등 역할, 책임, 권한 반영	○	○	
	비상조직의 구성	○	○	
	유관기관 협조체계	○	○	○
	자원수급	○	○	○
	-비상시 필요한 물품	○	○	○
	-비상설비	○	○	
	-비상 대응 활동 별 전문가 확보 방안 수립	○	○	
	지휘, 명령 계통	○	○	
	-평상시 역할 수행을 위한 지휘, 명령 및 보고	○	○	

	체계 정의			
	-비상조직을 기준으로 지휘, 명령 계통을 설계하여 문서화	○	○	
조직 문화속의 IPOCM 수립과 배치	인식제고 프로그램의 개발		○	
	IPOCM 프로그램의 인식		○	○
교육, 훈련 및 인식	교육 목적 정의	○	○	○
	교육대상자 분류	○	○	
	훈련의 필요성 평가		○	
	교육활동의 계획 및 개발		○	○
	훈련의 목적	○	○	○
	교육, 훈련을 통한 개선		○	○
홍보와 경보	홍보의 목적 정의	○		
	사고 발생 시 미디어와의 의사소통전략 수립	○		○
	사고 발생 초기 단계에서 미디어에 제공할 문서 초안에 대한 가이드라인 작성	○		○
	적절한 통신 전략 개발	○		○
	홍보 및 경보 시스템의 정기적인 점검	○		
	홍보활동 실행을 위한 방법 제시	○	○	
운영 통제	문서화된 내부 절차의 수립		○	
	내부 위험을 이해관계자에게 전달		○	○
	효율적인 계획, 운영, 통제를 위한 절차 수립		○	
재정과 행정	비상시 IPOCM실행을 지원하는 자금집행 및 행정지원 업무절차 개발	○	○	
	-IPOCM 관리자와의 협의 및 보고체계 수립	○	○	
	-자금집행 권한 및 의무 명시	○		
	-비용 산정 시 전산화와 문서화 비용이 포함된 회계시스템	○		
	-비상시 급여 지급 기준			
성능평가				
시스템 평가	전체적인 프로세스의 모의실전을 통한 평가	○	○	○
	주기적인 평가에 의한 절차 수립 및 이행	○		○
성능 측정과 모니터링	적합성 유효성 체크를 위한 모니터링		○	○
	모니터링을 위한 절차 제정 및 유지		○	○
테스트와 연습	시나리오를 기초로 한 테스트 실행	○		
	테스트 실행 후 보고서 작성		○	
교정과 예방 행동	교정 절차 제정, 실행, 유지		○	○
	교정의 목적		○	
	예방활동의 정의		○	
유지관리	최고경영자의 IPOCM 개정 내역 승 인	○	○	
	지속적인 모니터링 실시		○	○
	전체 구성원에게 문서화된 변경사항 배포	○	○	
	문서 갱신에 관한 지침 수립		○	
내부 감사와 자체 평가	계획된 간격에 의한 IPOCM 내부 감사와 자체 평가 실시	○	○	
	감사 및 평가 시 객관성 및 공정성 이행		○	
	감사기준과 범위, 빈도에 따른 자료 문서화		○	○
개선과 관리 검토	최고경영진의 주기적인 검토		○	○
	관리검토 기록의 유지		○	

[표 2]에서 어둡게 표시된 영역은 2개국 이상의 선진국에서 자국 표준의 항목으로 채택한 영역을 의미하고 있으며 우리나라의 보안사고 대비체계에서도 필수 항목으로서 고려되어야 할 요소이다.

V. 결 론

우리나라의 보안사고 대응체계는 활동 중심으로 볼 때 예방, 대비에 초점을 두고 있으며 대응, 복구가 미흡한 수준이다. 이와 반대로 국제 표준화가 활성화되어 있는 사업연속성관리 분야는 사고에 대한 예방, 대비, 대응, 복구의 균형을 강조하고 있고 사고대응을 위한 이해관계자의 협조체계 등은 오히려 대응 복구에 강력한 영향력을 발휘하고 있다. 이러한 동향을 고려할 때 우리나라 정보통신 인프라의 보안사고 대비체계는 국제적인 흐름에 상당히 동떨어져 있으며 실제 대형 보안사고 발생 시 막대한 피해와 사회적 혼란이 가중되는 심각한 사태를 나타내고 있다. 이러한 문제점을 개선하고자 본 논문에서는 국제 표준 및 선진국 표준에서 채택된 정보통신 인프라 보안사고 대비체계의 구성요소를 고찰하였고 이러한 흐름과 연계하기 위해 우리나라에 적용할 수 있는 필요 요건을 제시하였다.

본 논문에서 제시한 정보통신 인프라 보안사고 대비체계의 요건과 국제 표준 요구사항에 대한 보다 심도

깊은 분석을 통해 실제 보안사고 발생 시 강력한 내구성을 나타낼 수 있는 표준화된 체계가 향후 개발될 수 있기를 기대한다.

참 고 문 헌

[1] 배성훈, "'7.7 DDoS 사고' 대응의 문제점과 재발방지 방안," 현안보고서 Vol. 48, 국회입법조사처, 2009.

[2] Lloyd W. Bokman, "Standard on Disaster/Emergency Management and BusinessContinuity Programs" NFPA 1600, Jan. 2007.

[3] British Standard Institution, "BS 25999-1:2006 Business Continuity Management. Code of Practice" BS25999-1, Dec. 2006.

[4] Carl Gibson, "Business Continuity Management" AS/NZS HB221, Jan. 2004.

[5] International Standard Organization, "Societal security - Guideline for incident preparedness and operational continuity management" ISO/PAS 22399, Nov. 2007.

[6] International Standard Organization, "Information technology - Security techniques - Guidelines for ICT readiness for business continuity" ISO/FCD 27031, Aug. 2010.

[7] 동국대학교 위기관리연구센터, "재난관리시스템 표준화 및 표준의 활용방안 연구," 기술표준원 연구보고서, 2007년 12월.

〈著者紹介〉

이 성 일 (Seongil, lee)

1998년 2월 : 중앙대학교 산업정보학과 졸업
2002년 2월 : 중앙대학교 산업정보학과 석사
2008년 8월 : 동국대학교 경영정보학과 박사수료
2009년 12월~현재 : Ernst&Young Advisory
<관심분야> 정보보호 거버넌스, 정보보호관리체계, 사업연속성관리

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