Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.547

한국형 스마트 그리드의 가용성을 고려한 정보보호 관리체계 평가 기준 제안*

허 옥,† 김 승 주‡
고려대학교 정보보호대학원

Information Security Management System Evaluation Criteria with availability for Korean Smart Grid*

Ok Heo,† Seungjoo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

스마트 그리드는 전력망에 정보통신 기술을 이용하여 에너지 이용 효율을 극대화 하는 것으로 고가용성을 요구한다. 최근 DDos공격 등 서비스중단을 통한 사회적 혼란을 야기하는 공격이 증가되고 있어 가용성에 대한 체계적인 관리가 요구된다. 한국형 스마트 그리드의 정보보호 관리체계 평가에 대해 본 논문은 가용성을 중심으로 하는 국제표준을 비교하여 새로운 평가항목을 제시하여 기존 정보보호 관리체계가 갖는 가용성 평가의 한계를 극복한다.

ABSTRACT

Smart Grid, which maximize the efficiency of energic utilization by applying Information and Communication Technology to Power Grid, requires high availability. Attacks, such as DDoS, which cause suspension of service and lead to social disruptions have recently been increasing so that systematic management over availability becomes more important. In this paper, we presents a new evaluation criteria of Korean Smart Grid by comparing availability assessment items of international standards specified in management system and then overcome the limitations of availability evaluation of existing information security management system.

Keywords: Information Security Management System(ISMS), Information Assurance, Smart Grid, Critical Infrastructure

I. 서 론

최근의 정보보안의 대표적인 사고는 서비스의 가용성을 저해시켜 사회적 혼란을 일으키는데 목적을 두고 있다. 2009년 7월 7일 좀비 PC를 이용하여 금융회사 및 공공사이트 등 국내 주요 사이트에 DDos(Distributed Denial of Service)공격을 가해 서비스 중단을 초래했으며, 3·4DDos공격(2011), 3·20대란(2013)까지 공격이 다발적으로 발생되었고 일부PC의 경우 HDD의 자료가 삭제되는 등 심각한 시스템 가용성의 문제가 발생하였다.

전력·석유·가스 등의 에너지 분야 시설 및 도로·열차·항공·항만 등의 교통시스템, 상수도·하수도·댐 등의 수자원 분야의 기반시설은 정보통신기술이 집약된 제어시스템에 의해 운영 및 관리되고 있다. 제어시스템은 국가운영의 기반이 되는 산업시설의 상태를 실시간으로 모니터링하고 제어함으로써 국가기반시설들이

접수일(2013년 10월 1일), 수정일(1차: 2014년 2월 10일, 2차: 2014년 6월 3일), 게재확정일(2014년 6월 10일)
* 본 연구는 한국산업기술평가관리원의 IT R&D 프로그램 (10043959, 모바일단말의 비인가접근차단 및 운영환경 보장을 위한 EAL 4급 군사용 융합 보안 솔루션 개발) 사업의 연구결과로 수행하였습니다.
† 주저자, ok571@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

Table 1. Combine G-ISMS with ISMS

Division	System	Competent authorities	Legal basis	Target of certification
~2012	Information Security Management System in an E-Government	Ministry of Public Administration and Security	Directive No. 232 of the Ministry of Public Administration and Security	a public institution or administrative agency
2013	Information Security Management System in an E-Government	Ministry of Science, ICT and Future Planning	Directive No. 1 of the Ministry of Security and Public Administration ※ temporary applying on 2013	a public institution or administrative agency
2014~	Information Security Management System	Ministry of Science, ICT and Future Planning	Article 47 of Act on Promotion Of Information And Communications Network Utilization And Information Protection, Etc.	a public institution or administrative agency

안전하게 운영되도록 지원하는 중추신경계로 볼 수 있다. 제어시스템은 별도의 프로토콜을 사용하고 필요시 암호화하여 처리하는 등의 통제가 이루어지고 있으며 국내의 경우 인터넷과 분리된 망을 사용하도록 통제하는 등 강력한 통제를 받고 있으나, 2010년 스턱스넷(Stuxnet)악성코드에 의해 이란의 핵시설이 공격받으면서부터 제어 시스템 또한 안전한 환경이 아니라는 것이 입증되었다.

스마트 그리드는 제어시스템을 비롯하여 정보통신기술의 융합으로 전력사용자와 전력공급자 사이에서 양방향 통신을 하기 때문에 시스템간의 접점이 증가되고 통신망과 통신양이 늘어나는 등 가용성에 대한 위협이 증대되었고 시스템 중단시의 파급력은 더 커지고 있다.

미국의 스마트 그리드의 목표는 노후된 전력설비의 교체로 비롯되었지만, 한국형 스마트 그리드는 에너지 및 환경위기에 대응하고 지식 기반 사회를 견인하기 위함임으로 IT기술을 이용한 악의적인 시스템중단과 재해에 따른 시스템중단 위협을 고려하여 평가기준이 필요하다.

앞서 언급한 바와 같이 가용성의 중요성은 점점커지고 있어 ISO(International Organization for Standardization)에서는 업무연속성 관리체계인 BCMS(Business Continuity Management System)가 2011년 국제표준으로 채택되었고 ICT에 대한 업무연속성 가이드라인도 2012년 국제표준으로 채택되었고 NIST(National Institute of Standards and Technology)에서는 2010년 5월 800-34(Contingency Planning Guide for Federal Information Systems)를 제정하였다.

우리나라는 대표적인 정보보호 관리체계인 K-ISMS(Information Security Management System)의 경우 기존의 IT시스템에 대한 일반적인 정보보호 평가도구이지만 주로 정보유출을 방지하기 위한 기밀성에 초점을 맞추고 있고, 기밀성에 대한 항목이 추상적인 표현이거나 포괄적인 내용이기 때문에 가용성이 가장 우선시 되는 스마트 그리드에 적용하여 가용성 부분을 보증하는 데에는 한계가 있다.

본 논문의 목적은 국내 정보보호 관리체계인 K-ISMS를 기반으로 하되 다른 국제표준의 가용성 통제항목과의 분석을 통한 도출된 항목을 채용하여 한국형 스마트 그리드에 적용될 정보보호 관리체계를 제안하고자 한다. 공공·행정기관을 대상으로 하는 G-ISMS의 경우 〔Table 1.〕 과 같이 2014년부터 K-ISMS로 통합될 예정이고 스마트 그리드가 공공·행정과 민간으로 나누는데 무리가 따르므로 본 논문에서는 다루지 아니한다.

II. 배경

2.1 K-ISMS

정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의해 한국인터넷진흥원이 개발하고 국내에서 개발,

Table 2. Valuation criteria of K-ISMS

Certification Criteria		Control activities
IS Management Process		12
IT Counterm easures	1. Information security policies	6
	2. Information security organization	4
	3. Security of External Parties	3
	4. Information asset classification	3
	5. Education and training on information security	4
	6. Personnel security	5
	7. Physical security	9
	8. System development security	10
	9. Cryptography control	2
	10. Access control	14
	11. Operation security	22
	12. Intrusion incident handing	7
	13. IT disaster recovery planning	3
	Sub total	92
Total		104

운영하고 있는 대표적인 정보보호 관리체계 인증 제도로써 2012년 2월 17일부터 정보통신서비스제공자 중 법률에서 정한 사업자는 의무적으로 인증을 받도록 하고 있다. 3·20사이버테러 이후 정부종합대책의 일환으로 미래창조과학부에서는 금융, 교육, 의료기관으로 확대할 것을 준비 중에 있다. 정보보호 관리체계 인증 기준은 정보보호관리과정(5단계, 12개 통제항목)과 정보보호대책(13개 분야, 92개 통제항목)의 두 가지로 구성되어 104개의 통제항목으로 평가가 이루어진다. 평가를 받는 조직은 104개의 통제 항목 중 해당되는 영역에 대해 평가를 받는다.

2.2 ISO/IEC 27001

국제표준인 ISO/IEC 27001:2005는 대표적인 정보보호 관리체계(ISMS) 평가기준으로써 11개 분야, 39개 통제목적, 133개의 통제항목으로 구성되어 있으며 정보보호 관리체계가 PDCA(Plan-Do-Check-Act)의 사이클로 관리되고 있는지 평가가 이루어진다. 평가받는 조직은 K-ISMS와 같이 해당되는 업무영역에 한하여 평가가 이루어지게 된다. 현재 ISO/IEC JTC 1/SC 27에서 모바일 텔레워킹 통제항목 추가 및 위험평가 방법의 변경 등 전체적인 통제항목을 수정하는 개정이 진행 중이며 2013년 07월 FDIS(Final Draft Internal Standard)로 통과되었고 문제가 없으면 IS(Internal Standard)로 확정되어 개정될 예정이다. 본 논문에서는 2005버전으로 다룬다.

2.3 ISO22301

ISO22301:2011는 사업연속성관리체계(BCMS)의 국제표준으로 영국표준협회(BSI : British Standards Institution)에서 제정된 BS25999가 발전되어 2012년 5월 TC223(ISO에서 사업연속성 관리 분야를 논의하는 모임)에 의해 국제표준이 되었다. 적용범위는 다른 국제표준과 마찬가지로 민간/공공/비영리 등 광범위하게 적용이 가능하며, 조직의 프로세스가 이해관계자의 요구사항(지원, 파트너관리, 법규준수, IT가용성, 사고복구 등)을 PDCA사이클로 관리되고 있는지에 대해 초점을 맞추고 있다. ISO27031 제정에 영향을 주었고 우리나라에서는 주로 높은 가용성이 요구되는 금융권에서 인증을 추진/획득하고 있다.

2.4 ISO/IEC 27031

ISO/IEC 27031:2012는 ICT환경의 사업연속성 가이드라인(IRBC : Information and communication technology Readiness for Business Continuity)으로써 2011년 3월 ISO/IEC 27001을 제정한 SC(Standard committee)27에 의해 국제표준으로 제정되었다.

IRBC는 사고예방, 사고감지, 대응, 복구, 개선을 원칙으로 하며 인력, 설비, 기술, 데이터, 프로세스, 공급자를 구성요소로 정의하고 있다. 〔Fig.1.〕와 같이 IRBC는 BCMS 프로그램의 일부분으로 구성되어 있으며, ISMS 프로그램을 보완하고 뒷받침하는 관리 시스템이다.

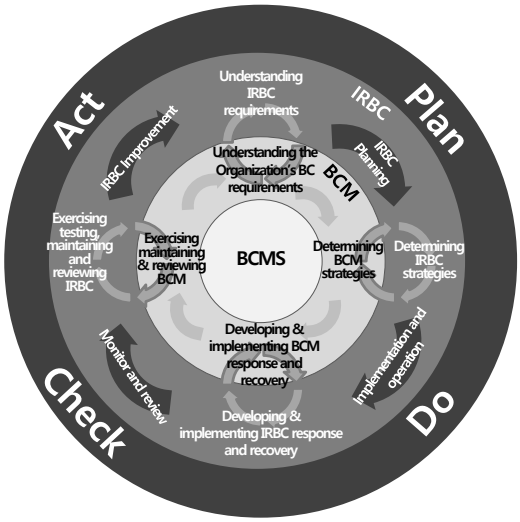

Fig.1. PDCA model of IRBC

III. 가용성 평가항목

3.1 비교분석

2장에서 소개된 국내·외 표준은 각각의 적용대상과 목적에 따라 가용성 평가항목과 내용에 차이가 있다.

K-ISMS를 기반으로 각 표준별 가용성 평가항목의 비교 평가를 위하여 K-ISMS의 통제항목 중 스마트 그리드 환경에서 이행되지 않을 경우 서비스가 중단되는 등 가용성에 직접적인 영향을 미치거나 사업연속성을 위한 계획 및 유지관리에 필요한 항목인 가용성 정책/역할/책임, 사고대응 정책/역할/책임/테스트/조사/분석, 사고예방/처리/모니터링/보고, 백업 및 기타 보안조치 항목을 가용성 통제항목(17개)으로 정하고 다른 표준과 비교를 수행한다.〔Table 3〕

각 통제항목별 내용을 비교하였을 때 완전히 만족할 경우는 '충족'으로, K-ISMS의 통제목표나 통제대상 일부가 부족하였을 경우 '부분충족'으로, 전혀 만족하지 못하였을 경우 '미충족'으로 구분한다.

Table 3. Availability control items of K-ISMS

control area	control no.	control activities
Physical security	7.1.1	Security area
	7.1.2	Securing facilities
System development security	11.2.3	Capacity management
	11.2.4	Fault management
	11.2.9	Backup management
	11.5.1	Malware control
	11.5.2	Patch management
information security incidents procedure	12.1.1	Establish response procedures on information security incidents
	12.1.2	Build response system on information security incidents
information security incidents response	12.2.1	Emergency training
	12.2.2	Emergency report
	12.2.3	Response, recovery on information security incidents
learning from information security incidents	12.3.1	Share the information security incidents analyze result
	12.3.2	Recurrence prevention
IT disaster recovery planning	13.1.1	IT disaster recovery planning
Developing continuity plans	13.2.1	Establish measures by risk assessment
	13.2.2	testing & maintenance

Table 4. Compare ISO27001 with K-ISMS

ISO27001 control activities	vs.	K-ISMS control activities
A.10 Communications and operations management		
A.10.3 System planning and acceptance		
A.10.3.1 Capacity management	O	11.2.3 Capacity management
A.10.5 Back-up		
A.10.5.1 Information back-up	O	11.2.9 Backup management
A.13 Information security incident management		
A.13.2 Management of information security incidents and improvements		
A.13.2.1 Responsibilities and procedures	O	12.2.1 Emergency training
A.13.2.2 Learning from information security incidents	O	12.3.1 Share the information security incidents analyze result
A.13.2.3 Collection of evidence	O	12.2.3 Response, recovery on information security incidents
A.14 Business continuity management		
A.14.1 Information security aspects of business continuity management		
A.14.1.1 Including information security in the business continuity management process	O	13.1.1 Build the IT disaster recovery system
A.14.1.2 Business continuity and risk assessment	O	13.2.1 Establish measures by risk assessment
A.14.1.3 Developing and implementing continuity plans including information security	O	13.2.1 Establish measures by risk assessment
A.14.1.4 Business continuity planning framework	O	13.2.1 Establish measures by risk assessment
A.14.1.5 Testing, maintaining and reassessing business continuity plans	O	13.2.2 Testing & maintenance

3.2 K-ISMS, ISO27001

K-ISMS의 가용성 평가 수준을 평가하기 위하여 정보보호 관리체계의 국제표준인 ISO27001의 가용성 통제항목을 비교분석한 결과 〔Table 4〕와 같이 ISO 27001의 가용성 평가기준 10개 항목 모두 K-ISMS의 평가기준으로 충족(O)되고 있음을 확인하였다.

3.3 K-ISMS, ISO22301

K-ISMS의 가용성 평가 수준을 평가하기 위하여 BCMS인 ISO22301의 통제항목에 K-ISMS의 가용성 통제항목을 비교분석한 결과 〔Table 5〕와 같이 충족(O)이 13개, 부분충족이(△) 2개, 미충족(X)이 10개가 발견되어 K-ISMS로 가용성을 평가하는데 한계가 있음을 확인하였다.

Table 5. Compare ISO22301 with K-ISMS

ISO22301 control activities	vs.	K-ISMS control activities
4. Context of the organization(Plan)		
4.1 Understanding of the organization and its context	X	none
4.2 Understanding the needs and expectations of interested parties	X	none
4.3 Determining the scope of the business continuity management system	X	none
4.4 Business continuity management system(BCMS)	O	13.1.1 Build the IT disaster recovery system
5. Leadership(Plan)		
5.1 Leadership and commitment	O	(IS Management Process) 2.1 Executive involvement
5.2 Management commitment	X	none
5.3 Policy	X	none
5.4 Organization roles, responsibilities and authorities	O	13.1.1 Build the IT disaster recovery system
6. Planning(Plan)		
6.1 Actions to address risks and opportunities	O	13.2.1 Establish measures by risk assessment

ISO22301 control activities	vs.	K-ISMS control activities
6.2 Business continuity objectives and plans to achieve them	O	13.2.1 Establish measures by risk assessment
7. Support(Plan)		
7.1 Resources	X	none
7.2 Competence	X	none
7.3 Awareness	X	none
7.4 Communication	X	none
7.5 Documented information	X	none
8. Operation(Do)		
8.1 Operation planning and control	O	13.2.1 Establish measures by risk assessment
8.2 Business impact analysis and risk assessment	O	13.2.1 Establish measures by risk assessment
8.3 Business continuity strategy	O	13.2.1 Establish measures by risk assessment
8.4 Establish and implement business continuity process	O	13.2.2 Testing & maintenance
8.5 Exercising and testing	O	13.2.2 Testing & maintenance
9. Performance evaluation(Check)		
9.1 Monitoring, measurement, analysis and evaluation	O	13.2.2 Testing & maintenance
9.2 Internal audit	△	(IS Management Process)5.3 internal audit
9.3 Management review	△	(IS Management Process) 2.1 Executive involvement
10. Improvement(Act)		
10.1 Nonconformity and corrective action	O	13.2.2 Testing & maintenance
10.2 Continual improvement	O	13.2.2 Testing & maintenance

3.4 K-ISMS, ISO27031

K-ISMS이 IRBC의 가용성 평가의 수준을 파악하기 위하여 ISO27031의 통제항목에 K-ISMS의 가용성 통제항목을 비교분석한 결과 〔Table 6〕과 같이 충족(O)이 10개, 부분충족이(△) 15개, 미충족(X)이 27개가 발견되어 K-ISMS로 가용성을 평가하는데 한계가 있음을 확인하였다.

Table 6. Compare ISO27031 with K-ISMS

ISO27031 control activities	vs.	K-ISMS control activities
5.5 Establishing IRBC	O	13.1.1 Build the IT disaster recovery system
5.6 Using Plan Do Check Act to establish IRBC	O	13.1.1 Build the IT disaster recovery system
5.7 Management Responsibility	-	
5.7.1 Management leadership and commitment	△	(IS Management Process) 2.1 Executive involvement
5.7.2 IRBC Policy	X	none
6. IRBC Planning		
6.1 General	-	
6.2 Resources	-	
6.2.1 General	△	Build the IT disaster recovery system
6.2.2 Competency of IRBC staff	X	none
6.3 Defining requirements	-	
6.3.1 General	O	13.1.1 Build the IT disaster recovery system
6.3.2 Understanding critical ICT services	O	13.2.1 Establish measures by risk assessment
6.3.3 Identifying gaps between ICT Readiness capabilities and business continuity requirements	X	none
6.4 Determining IRBC Strategy Options	-	
6.4.1 General	X	none
6.4.2 IRBC Strategy Options	X	none
6.4.2.1 Skill and Knowledge	X	none
6.4.2.2 Facilities	X	none
6.4.2.3 Technology	X	none
6.4.2.4 Data	X	none
6.4.2.5 Process	X	none

ISO27031 control activities	vs.	K-ISMS control activities
6.4.2.6 Suppliers	X	none
6.5 Sign Off	X	none
6.6 Enhancing IRBC Capability	-	
6.6.1 Enhancing Resilience	O	13.2.2 Testing & maintenance
6.7 ICT Readiness Performance Criteria	-	
6.7.1 Identification of performance criteria	O	13.2.2 Testing & maintenance
7. Implementation and Operation		
7.1 General	X	none
7.2 Implementing the Elements of the IRBC Strategies	-	
7.2.1 Awareness, Skills and Knowledge	X	none
7.2.2 Facilities	X	none
7.2.3 Technology	X	none
7.2.4 Data	X	none
7.2.5 Process	X	none
7.2.6 Supplier	X	none
7.3 Incident Response	X	none
7.4 IRBC Plan Documents	-	
7.4.1 General	X	none
7.4.2 Content of Plan Documents	△	13.1.1 Build the IT disaster recovery system
7.4.3 The ICT Response and Recovery Plan Documentation	△	13.1.1 Build the IT disaster recovery system
7.5 Awareness, competency and training program	X	none
7.6 Document Control	-	
7.6.1 Control of IRBC records	X	none
7.6.2 Control of IRBC documentation	X	none
8 Monitor and Review		
8.1 Maintaining IRBC	-	
8.1.1 General	X	none
8.1.2 Monitoring, detection and analysis of threats	X	none

ISO27031 control activities	vs.	K-ISMS control activities
8.1.3 Test and exercise	-	
8.1.3.1 General	△	13.2.2 Testing & maintenance
8.1.3.2 Test and exercise program	△	13.2.2 Testing & maintenance
8.1.3.3 The scope of exercises	△	13.2.2 Testing & maintenance
8.1.3.4 Elements of service recovery	△	13.2.2 Testing & maintenance
8.1.3.5 Planing an Exercise	△	13.2.2 Testing & maintenance
8.1.3.6 Managing an Exercise	△	13.2.2 Testing & maintenance
8.1.3.7 Review, Report and Follow-up	△	13.2.2 Testing & maintenance
8.2 IRBC Internal Audit	△	(IS Management Process)5.3 Internal audit
8.3 Management Review	-	
8.3.1 General	△	(IS Management Process) 2.1 Executive involvement
8.3.2 Review Input	△	(IS Management Process) 2.1 Executive involvement
8.3.3 Review Output	△	(IS Management Process) 2.1 Executive involvement
8.4 Measurement of ICT Readiness Performance Criteria	-	
8.4.1 Monitoring and measurement of ICT Readiness	O	13.2.2 Testing & maintenance
8.4.2 Quantitative and Qualitative Performance Criteria	X	none
9 IRBC improvement		
9.1 Continual improvement	O	13.2.2 Testing & maintenance
9.2 Corrective action	O	13.2.2 Testing & maintenance
9.3 Preventive action	O	13.2.2 Testing & maintenance

Table 7. Candidate of additional valuation activities

Control area	Control activities	Contents
Management Responsibility	Management leadership and commitment	To be effective an IRBC program should be a process fully integrated with the organization's management activities, driven from the top of the organization, endorsed and promoted by top management.
	IRBC policy	The organization should have a documented IRBC policy.
IRBC Planning	General	IRBC roles, responsibilities, competencies and authorities should be defined and documented.
	Competency of IRBC staff	The organization should ensure that all personnel who are assigned IRBC responsibilities are competent to perform the required tasks.
	Identifying gaps between ICT Readiness capabilities and business continuity requirements	For each critical ICT service the current ICT Readiness arrangements should be compared with business continuity requirements and any gaps should be documented.
Determining IRBC Strategy Options	General	IRBC strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place.
	IRBC Strategy Options	The organization should consider a range of options for the incident readiness of its critical ICT services include provided externally by one or more third parties.
	Skills and Knowledge	The organization should identify appropriate strategies for maintaining core ICT skills and knowledge.
	Facilities	According to identified risks, the organization should devise strategies for reducing the impact of the unavailability of the normal ICT facilities.
	Technology	The ICT services upon which critical business activities depend should be available in advance of the resumption of their dependent critical business activities.
	Data	Data continuity solutions should be designed to meet the Recovery Point Objectives (RPO) of each critical business activity of the organization as they relate to the critical business activities.
	Processes	In selecting its IRBC strategy, the organization should consider the processes necessary to ensure the viability of that strategy.
	Suppliers	The organization should identify and document external dependencies which support ICT service provision and take adequate steps to ensure that critical equipment and services can be provided by their suppliers within predetermined and agreed timeframes.
Sign Off	Sign Off	IRBC strategy options selected should be presented to top management, with recommendations for a decision based on risk appetite and cost.
Implementation and Operation	General	IRBC strategies should only be implemented after top management approval.
Implementing the Elements of the IRBC Strategies	Awareness, Skills and Knowledge	General awareness of the readiness of the elements of ICT services is a crucial element in ensuring the required support for the business continuity governance and management system, including ICT readiness.

Control area	Control activities	Contents
	Facilities	ICT recovery systems and critical data should, where possible, be physically separated from the operational site to prevent them being affected by the same incident.
	Technology	ICT technology strategies should be implemented.
	Data	The arrangements for the availability of data should be aligned with the requirements identified within the IRBC management strategies.
	Processes	IRBC processes should be documented clearly and in sufficient detail to enable competent staff to execute them (some of these processes may differ from the daily operation).
	Suppliers	The organization should ensure that critical suppliers are able to support the IRBC service capabilities required by the organization.
	Incident Response	The incident response should trigger an appropriate IRBC action.
	Communication	Should to choose the method to inform the security incidents to people concerned.
	General	The organization should have documentation (plans) to manage potential disruption and thereby enable continuity of ICT services and the recovery of critical activities.
	Content of Plan Documents	A small organization may have a single plan document that encompasses all activity to recover the ICT services of its entire operations.
	The ICT Response and Recovery Plan Documentation	The ICT Response and Recovery Plan documentation should be concise, people can use them easily.
	Awareness, competency and training program	A co-ordinated program should be implemented to ensure that processes are in place to regularly promote IRBC awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of IRBC (refer to 7.2.1).
	Control of IRBC records	Controls should be established over IRBC records in order to ensure that they remain legible, readily identifiable and retrievable and provide for their storage, protection and retrieval.
	Control of IRBC documentation	Documents are approved for adequacy prior to issue and their distribution controlled.
Monitor and Review	General	Any change to the ICT services which may affect the IRBC capability should be implemented only after the business continuity implications of the change have been assessed and addressed.
	Monitoring, detection and analysis of threats	The organization should establish a process to continuously monitor and detect the emergence of ICT security threats.
	Test and exercise	The organization should exercise not only the recovery of the ICT service, but also its protection and resilience elements.
	Test and exercise program	The test and exercise program should define how the risk of individual exercise is addressed.
	The scope of exercises	Exercising should apply to the entire ICT environment and all the components that deliver the end-to-end service from the computer room through to the user desktop or any other service delivery channel.

Control area	Control activities	Contents
	Elements of service recovery	The organization should exercise at component level through to full location-based system testing.
	Planning an Exercise	To ensure that an exercise does not cause incidents or undermine the service capability, an exercise should be carefully planned to minimize the risk of an incident occurring as a direct result of the exercise.
	Managing an Exercise	A clear exercise command structure should be developed with roles and responsibilities allocated to appropriate individuals.
	Review, Report and Follow-up	At the end of an exercise its findings should be reviewed and followed up promptly.
	IRBCInternalAudit	The audit plan should also encompass external parties.
	Management Review	Top management should review annually the signed off IRBC requirements.
	Review Input	The inputs should include information on internal service levels, external service providers' ability to maintain appropriate levels of service and etc.
	Review Output	Varying the scope, improving the effectiveness of IRBC management system and etc.
	Quantitative and Qualitative Performance Criteria	Performance criteria for IRBC may be qualitative or quantitative.

IV. 평가기준 도출 및 제안

4.1 방법론

평가기준을 도출하는 방법은 〔Fig.2〕와 같이 ISMS는 국내 K-ISMS와 국제표준인 ISO27001로 구성되어 있고, BCMS와 IRBC가 가용성에 대한 표준으로 제정되어 있으며 서로 파생되거나 지원하는 구조를 갖추고 있으므로 국내 표준인 K-ISMS의 가용성 평가기준에 국제표준인 ①ISO27001의 가용성 평가기준과 비교, ②IRBC의 가용성 평가기준과 비교, ③BCMS의 가용성 평가기준을 비교하여 충족되지 않는 항목들에 대하여 추가 평가 기준 후보군을 도출하고, 한국형 스마트 그리드의 가용성 위협을 식별하여 추가 평가 기준 후보군 가운데 가용성위협에 해당하는 항목을 선별하여 최종 평가 기준으로 도출한다.

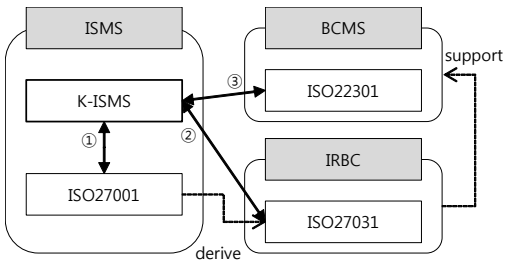

Fig.2. Method for draw a valuation basis

4.2 추가 평가 기준 후보군

K-ISMS의 가용성 평가 기준과 ISO27001의 가용성 평가기준, BCMS, IRBC의 평가기준을 비교하여 추가 평가 기준 후보군으로 하되 중복되는 항목은 제외한다.〔Table 7〕

4.3 가용성 위협 도출

한국형 스마트 그리드의 가용성 위협을 도출하기 위해 〔Table 8〕과 같이 지능형전력망 정보의 보호조치에 관한 지침(지식경제부고시 제2012-129호)과 주요정보통신기반시설 취약점 분석 평가 점검항목(안전행정부고시 제2012-54호)에서 가용성과 관련된 통제항목을 선별하였다.

4.4 최종 평가 기준 도출

4.2장의 추가 평가 기준 후보군에서 4.3에서 도출된 스마트 그리드의 가용성 위협 항목을 그룹핑 하여 정리하면 K-ISMS의 구성요소 이외에 추가적으로 평

Table 8. Threat of Korean Smart Grid in Availability

Division	Contents	Possible threats
Guidelines for protection of information on Smart Grid	OS patch is not applied	Hinder availability using OS vulnerability
	Check the server security	Hinder availability using Server security vulnerability
	Prevent, response and recovery measures on information security incidents	Incident response delay
	Establish and enforce response procedures on information security incidents by type	Incident response delay
	Establish and enforce emergency contact system for information security incidents	Incident response delay
	Simulation training for information security incidents	Incident response delay
	Establish and enforce emergency contact system of the smart grid service provider	Incident response delay
	Written policy, guidelines, manual of Information security system	User mistake
	Approval to the establish or change of Information security system	Abusing privileges
Vulnerability Analysis and Evaluation on Major information and communication infrastructure	Establish business continuity strategy	Delay in recovery
	Test business continuity management by simulation training	Delay in recovery
	Duplex configuration for high important system	Spread of system stop
	Backup cycle and storage	Failure in recovery
	Documentation for reporting procedure on information security incidents	Delay in recovery
	Build DDoS response system and training	Delay in recovery
	Manage the analysis record of security incidents	Delay in recovery
	Working process in information security incidents	Delay in recovery
	Establish and enforce a measure to prevent a repeat of information security incidents	Hinder availability
	Documentation for information security incidents coping plan	User mistake
	Organize information security incidents response team	Delay in recovery
	Build the coordinated response system with external agency for information security incidents	Delay in recovery
	Educate on the respond process of security incidents	User mistake
	Establish DDoS respond method by attack level	Delay in recovery
	Countermeasure against DDoS attack (Green DDoS Zone)	Delay in recovery

가받아야 할 가용성 평가 항목이 도출된다.〔Table 9〕

기존 ISMS평가 기준에 최종 평가 추가 항목을 추가하면 최종 평가 기준이 된다. 각 항목의 세부 평가 기준과 방법은 각각의 표준에서 정의하는 것을 따른다.

도출된 최종 평가 기준은 스마트미터, Concentrator, 각종 송배전 시설, EMS, EV, 과금 등 스마트 그리드와 관련된 모든 시스템에 적용하여 평가할 수 있다. 관련하여 자산의 한 종류로 스마트미터를 대상으로 하였을 경우 스마트 미터의 가용성 사고 발생시 커뮤니케이션의 부재여부, 복구대응 계획에 스마트 미터를 문서화 하여 반영여부, 관련자에게 인식교육을 하였는지 등을 확인 할 수 있다.

V. 평가 기준 검증

4장에서 도출된 최종 평가 기준은 지능형전력망 정보의 보호조치에 관한 지침(지식경제부고시 제2012-129호)과 주요정보통신기반시설 취약점 분석 평가

점검항목(안전행정부고시 제2012-54호)의 가용성 관련된 기준을 〔Table 10〕과 같이 모두 충족하므로 정당성이 입증된다.

VI. 결론

본 연구는 국가기반시설인 스마트 그리드를 대상으로 스마트 그리드의 가용성 측면의 위협을 고려한 정보보호 평가방법을 제시한 것으로 기존 정보보호 평가제도인 K-ISMS와 ISO27001의 평가항목의 한계를 극복한다.

본 연구는 발전사, 거래소, 제어망 사업자 등 스마트 그리드와 관련된 모든 사업자에게 적용시킬 수 있으며, ISMS 인증을 취득한 후 가용성 확보를 목적으로한 BCMS 혹은 IRBC의 인증을 추가로 취득할 필요가 없도록 설계되어 있어 중복에 따른 업무 불편을 최소화 할 수 있다.

Table 9. Additional valuation basis

Control area	Control activities	Contents
Management Responsibility	IRBC policy	The organization should have a documented IRBC policy
Determining IRBC Strategy Options	Skills and Knowledge	The organization should identify appropriate strategies for maintaining core ICT skills and knowledge
	Data	Data continuity solutions should be designed to meet the Recovery Point Objectives (RPO) of each critical business activity of the organization as they relate to the critical business activities
	Suppliers	The organization should identify and document external dependencies which support ICT service provision and take adequate steps to ensure that critical equipment and services can be provided by their suppliers within predetermined and agreed timeframes
Sign Off	Sign Off	IRBC strategy options selected should be presented to top management, with recommendations for a decision based on risk appetite and cost
Implementing the Elements of the IRBC Strategies	Incident Response	The incident response should trigger an appropriate IRBC action
	Communication	Should to choose the method to inform the security incidents to people concerned
	Content of Plan Documents	A small organization may have a single plan document that encompasses all activity to recover the ICT services of its entire operations
	The ICT Response and Recovery Plan Documentation	The ICT Response and Recovery Plan documentation should be concise, people can use them easily
	Awareness, competency and training program	A co-ordinated program should be implemented to ensure that processes are in place to regularly promote IRBC awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of IRBC (refer to 7.2.1)
	Control of IRBC records	Controls should be established over IRBC records in order to ensure that they remain legible, readily identifiable and retrievable and provide for their storage, protection and retrieval
	Control of IRBC documentation	documents are approved for adequacy prior to issue and their distribution controlled

Table 10. Valuation basis mapping table

Division	Threats	Satisfied	Control
guidelines for protection of information on Smart Grid	OS patch is not applied	O	ISMS 11.5.2
	Check the server security	O	ISMS 10.4.2
	Prevent, response and recovery measures on information security incidents	O	ISMS 12.1.2, IRBC Policy Incident Response
	Establish and enforce response procedures on information security incidents by type	O	ISMS 12.1.2, IRBC Policy Incident Response
	Establish and enforce emergency contact system for information security incidents	O	Communication
	Simulation training for information security incidents	O	ISMS 13.2.1
	Establish and enforce emergency contact system of the smart grid service provider	O	Communication
	Written policy, guidelines, manual of Information security system	O	IRBC Policy Content of Plan Documents
	Approval to the establish or change of Information security system	O	Sign Off Document Control
Vulnerability Analysis and Evaluation on Major information and communication infrastructure	Establish business continuity strategy	O	IRBC Policy
	Test business continuity management by simulation training	O	ISMS 13.2.1
	Duplex configuration for high important system	O	Skill and Knowledge ISMS 7.1.2
	Backup cycle and storage	O	ISMS 11.2.9
	Documentation for reporting procedure on information security incidents	O	ISMS 12.2.2
	Build DDoS response system and training	O	ISMS 12.1.2, ISMS 12.2.1
	Manage the analysis record of security incidents	O	ISMS 12.3.1, Control of IRBC records
	Working process in information security incidents	O	Process
	Establish and enforce a measure to prevent a repeat of information security incidents	O	ISMS12.3.2
	Documentation for information security incidents coping plan	O	ISMS 12.1.1, The ICT Response and Recovery Plan Documentation
	Organize information security incidents response team	O	Incident Response
	Build the coordinated response system with external agency for information security incidents	O	Supplier
	Educate on the respond process of security incidents	O	Awareness, competency and training program
	Establish DDoS respond method by attack level	O	ISMS 12.1.2
	Countermeasure against DDoS attack (Green DDoS Zone)	O	ISMS 12.1.2

References

〔1〕 Kichul Kim, Seungjoo Kim, "Evaluation Criteria for Korean Smart Grid based on K-ISMS," Journal of The Korea Institute of Information Security & Cryptology, 22(6), pp.1375-1392, Dec. 2012.

〔2〕 Kyung-bok Lee, Tae Hyoung Park, Jong-in Lim, "A Study on the Security Policy of Smart Grid," Journal of Information Policy, 16(4), pp.73-96, Dec. 2009.

〔3〕 Seongil lee, Jungduk Kim, "Information and communication infrastructure for business continuity of the system compared to trends in international standardization research," Journal of The Korea Institute of Information Security & Cryptology, 20(4), pp.34-41, Aug. 2010.

〔4〕 NIST Special Publication 800-34 Rev. 1, "Contingency Planning Guide for Federal Information Systems," May. 2010.

〔5〕 Kichul Kim, Ok Heo, Seungjoo Kim, "A Security Evaluation Criteria for Korean Cloud Computing Service," Journal of The Korea Institute of Information Security & Cryptology, 23(2), pp.251-265, Mar. 2013.

〔6〕 Sang-Keun Lee, "A Study on Smart Grid and Cyber Security Strategy," Journal of The Korea Institute of Information Security & Cryptology, 21(5), pp.95-108, Oct. 2011.

〈저자소개〉

허 옥 (Ok Heo) 학생회원
2007년 8월: 단국대학교 경영학과 학사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2010년 1월~현재: 엔씨소프트 재직 중
〈관심분야〉 IT감사, 개인정보보호, 정보보호관리체계, 보안성 평가

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security