情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

K-ISMS 기반의 한국형 스마트 그리드 정보보호 관리체계 평가 기준 제안*

김 기 철,[1†] 김 승 주[2‡]
[1]고려대학교 정보보호대학원, [2]고려대학교 사이버국방학과/정보보호대학원

Evaluation Criteria for Korean Smart Grid based on K-ISMS*

Kichul Kim,[1†] Seungjoo Kim[2‡]
[1]Center for Information Security Technologies(CIST), Korea University
[2]Department of Cyber Defense/Center for Information Security Technologies(CIST), Korea University

요 약

스마트 그리드란 전력망에 정보통신기술을 적용하여 에너지 이용 효율을 극대화하는 차세대 지능형 전력망으로 최근 전 세계적으로 관련 기술 및 제도가 개발되고 있다. 정보보호는 스마트 그리드 개발에 필수적인 요소로써 지속적인 관리가 필요하다. 국내에서는 조직의 위험을 관리하기 위해 정보보호 관리체계 인증 제도가 이미 시행 중인 가운데 스마트 그리드에 적용할 수 있는 정보보호 관리체계 기준 마련의 필요성이 제기되고 있으나 구체적인 방법은 제시되지 않고 있다. 본 논문은 미국 스마트 그리드 제도와 비교 분석을 통해 기 시행중인 정보보호 관리체계 기반의 한국형 스마트 그리드를 위한 핵심 평가 기준과 추가적인 평가 기준을 제안한다. 기존의 정보보호 관리체계 인증을 받은 스마트 그리드 관련 사업자는 추가 평가 기준만으로 중복되고 불필요한 인증 평가 작업을 최소화할 수 있다.

ABSTRACT

Smart grid is a next-generation intelligent power grid that applying ICT to power grid to maximize the energy efficiency ratio. Recently, technologies and standards for smart grid are being developed around the world. Information security which is an essential part of smart grid development has to be managed continuously. Information security management system certification for organizational risk management has been implemented in Korea. Although preparation for information security management system certification which is applicable to smart grid is considered, there are no specific methods. This paper is to propose core and added evaluation criteria for Korean smart grid based on K-ISMS through comparative analysis between ISMS operated in Korea and smart grid information security management system developed in the United States. Added evaluation criteria enable smart grid related business that certified existing ISMS to minimize redundant and unnecessary certification assessment work.

Keywords: Information Security Management System, Security Control, Security Evaluation, Smart Grid, Critical Infrastructure

접수일(2012년 7월 25일), 수정일(1차: 2012년 10월 8일), 2차: 2012년 10월 31일), 게재확정일(2012년 10월 31일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT 연구센터육성 지원사업의 연구결과로 수행되었음 (NIPA-2012-H0301-12-3007)

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT 연구센터육성 지원사업의 연구결과로 수행되었음 (NIPA-2012-H301-12-4008)
† 주저자, jeterkim@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr

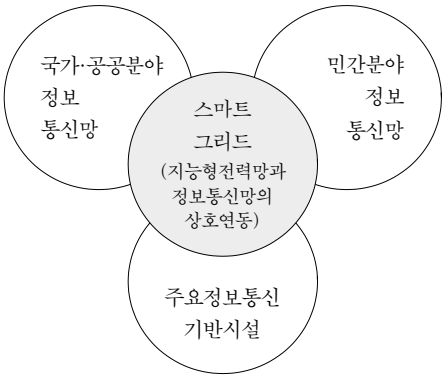
I. 서 론

비즈니스 IT환경이 급속히 발전하고 융·복합화 되어 신규 취약점 및 위협이 등장하고 있다. 기업은 취약점 및 위협에 따른 지속적인 위험을 관리하고 비즈니스의 연속성을 유지하기 위해 정보보호 관리체계를 수립하여 기업의 보안 수준 및 경쟁력을 제고하고자 한다. 최근 국내의 법 개정[1], 국내ISMS(이하 K-ISMS) 및 국제 인증제도인 ISO/IEC 27001(이하 ISO27001)의 인증 건수 증가 추세는 정보보호 관리체계의 필요성을 반영한다. 정보보호 관리체계는 국가·공공기관으로부터 금융, 교육, 의료, 통신 등의 기업, 연구소까지 매우 다양한 분야에서 사업의 안전성과 신뢰성을 보장하므로 최근 주목받고 있는 스마트 그리드 분야에서도 이러한 관리체계가 적용될 수 있다.

스마트 그리드란 전력망에 정보통신기술을 적용하여 에너지 이용 효율을 극대화하는 차세대 지능형 전력망으로 최근 전 세계적으로 스마트 그리드를 위한 기술이 개발되고 있다. 정보보호는 스마트 그리드 개발에 필수적인 요소로써 지속적으로 관리해 주어야 할 필요성이 있다. 하지만 스마트 그리드 시스템은 기존 정보보호 관리체계에서 다루어지고 있는 IT시스템과 구별된다[1][2]. 국내에서는 스마트 그리드 관련된 체계가 미비하여 지속적인 위험을 관리하기 위한 추가적인 정보보호 관리체계 기준 마련의 필요성이 제기되고 있으나 구체적인 방법은 제시되지 않고 있다[3][4].

국내 스마트 그리드 업무 현황을 파악하기 위해서 먼저 정보보호 업무의 현황을 먼저 살펴볼 필요가 있다. 국내 정보보호업무는 2008년 2월 정부조직개편에 따라 방송통신위원회, 지식경제부, 행정안전부로 이관되었으며, 현재 국내에서 시행 중인 정보보호 관련 제도는 시행 주체를 기준으로 크게 국가·공공분야와 민간분야로 나누어진다[5][6]. [표 1]은 스마트 그리드와 관련된 국내 법제 현황을 분류한 것으로 스마트 그리드 업무는 국가·공공분야와 민간분야로 구분하기에 무리가 따른다.

스마트 그리드는 네트워크가 상호 연결되어 있으며 고객과 연결된 접점 및 경로가 증가되어 복잡한 구조로 이루어진다. 지능형전력망과 정보통신망이 상호 연동되는 한국의 스마트 그리드는 [그림 1]과 같이 국가·공공분야 및 민간분야의 정보통신망, 주요정보통신기반시설과 연결되어 있다. 따라서 국가·공공분야와 민간 분야를 모두 포함하는 스마트 그리드 정보보호 관리체계를 개발하여 스마트 그리드 관련 사업자가 다양한 정보보호 정책으로 야기되는 혼란을 최소화해야 한다.



[그림 1] 한국 스마트 그리드의 상호 연동

국내에서 스마트 그리드 정보보호 관리체계 인증제도가 확립·시행되었을 경우 기존의 평가·인증 제도와 중복되는 항목이 발생한다. 예를 들어 국내에서 시행 중인 대표적인 정보보호 관리체계 평가·인증은 K-ISMS(민간), G-ISMS(전자정부)[2], 정보보안 관리실태 평가(국가·공공)[3], IT부문 경영실태 평가(금융)[4] 등으로 조직의 특성에 따라 여러 평가·인증을 받게 되는 경우 다수의 평가 기준이 중복되어 효율성이 저하되고 불필요한 업무가 증가한다. 따라서 한국형 스마트 그리드 정보보호 관리체계 평가 기준을 개발할 경우 기존 ISMS 중심의 비교 연구를 통하여 공통의 핵심 평가 기준과 추가 평가 기준으로 나누어 이미 ISMS 인증을 받은 스마트 그리드 관련 사업자는 추가 평가 기준만으로 간소화된 인증을 시행할 수 있도록 고려해야 한다.

1) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012.2 개정)」은 정보통신서비스 제공자에 대한 기존 정보보호 안전진단 제도를 폐지하고 정보보호 관리체계 인증제도로 일원화

2) 행정안전부 훈령에 의거 전자정부 정보보호 관리체계 인증 제도로 실시

3) 국가정보원 국가사이버안전관리규정에 의거 시행 중인 평가 제도로 인증이 아닌 실태 파악 후 미흡한 부분은 보완 및 보안대책을 지원하는 형식으로 운영

4) 금융감독원은 금융기관 IT부문의 안전성 및 건전성 유지를 위해 일반부문 경영실태평가(CAMELS)를 보완하기 위하여 IT부문 경영실태평가를 별도로 실시

〔표 1〕 스마트 그리드 관련 국내 법제 현황

구분	국가·공공분야	민간분야	국가·공공분야+민간분야	
법·규정	국가사이버안전관리규정	정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신기반보호법	지능형전력망의 구축 및 이용촉진에 관한 법률
적용대상	중앙행정기관, 지방자치단체 및 공공기관의 정보통신망 * 주요정보통신기반시설에 대해서는 적용하지 아니함.	민간분야의 정보통신망	정보통신기반시설(국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 + 정보통신망) 중 국가사회적 중요성 등에 의해 지정된 주요 정보통신기반시설	지능형 전력망(전력망에 정보통신기술을 적용하여 전기의 공급자와 사용자가 실시간으로 정보를 교환하는 등의 방법을 통하여 전기를 공급함으로써 에너지 이용효율을 극대화하는 전력망)

본 논문의 목적은 K-ISMS 기반의 핵심 평가 기준과 미국 NIST 표준 기반으로 통제항목 추가 방법론을 적용하여 도출된 추가 평가 기준을 한국형 스마트 그리드 정보보호 관리체계 평가 기준으로 최종 제안함으로써 중복되고 불필요한 인증 평가 작업을 최소화시키는 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 국내외 정보보호 관리체계 및 미국을 중심으로 한 스마트 그리드 관련 정보보호 관리체계 현황을 살펴보고 3장에서는 정보보호 관리체계 비교 및 통제 항목간의 매핑을 통해 추가적인 평가 기준을 도출하는 미국의 방법론을 살펴본다. 4장에서는 국내에 적용 가능한 평가 기준 도출 방법론을 통해 통제 항목을 상세히 비교 분석하여 핵심 평가 기준 및 추가 평가 기준 후보군을 도출한다. 5장에서는 추가 평가 기준 후보군에 국내 스마트 그리드 특성을 적용하여 K-ISMS 기반의 한국형 스마트 그리드 정보보호 관리체계 평가 기준을 제안한다. 6장에서는 제안된 평가 기준을 검증하고 7장에서 결론을 맺는다.

I. 관련 연구

2.1 K-ISMS, ISO27001

국내에서 가장 잘 알려진 정보보호 관리체계는 K-ISMS와 ISO27001이다. K-ISMS는 ISO-27001과 유사하지만 국내 환경에 맞게 관리과정을 "1.정보보호 정책수립, 2.관리체계 범위설정, 3.위험관리, 4.구현, 5.사후관리" 의 5단계 사이클과 14개 통제 항목으로 관리한다. 또한 문서화와 관련된 3개 통제 항목과 정보보호 대책과 관련된 15개 분야의 120개 통제 항목을 합한 총 137개 통제 항목과 446개의 세부적인 통제 항목을 적용한 국내 정보보호 관리체계이다. ISO27001은 정보보호를 계획-실행-검토-조치 단계의 PDCA (Plan-Do-Check-Act) 사이클에 의해 관리하며 11개 분야의 133개 보안 통제 항목을 적용한 국제 표준의 정보보호 관리체계이다. K-ISMS와 ISO27001는 정보보호 관리체계를 비즈니스, 조직, 장소, 자산과 기술적 특성을 고려하여 수립하고 목적 및 범위를 정의한다. 또한 정보보호 정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해 위험분석 및 평가에 의거 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고 기준에서 제시하는 통제 항목을 선택한다〔7〕〔8〕. K-ISMS는 ISO27001 국제 표준을 모두 포함하고 있으며, 국내 상황에 맞게 침해사고 예방, 암호화, 전자거래 등의 보안요건을 강화하였다. 따라서 ISMS 인증을 받게 되면 ISO27001 인증에서 요구하는 기준을 모두 만족하면서 국내 정보보호 환경에 맞는 정보보호 관리체계가 수립되었음을 보증할 수 있다〔9〕.

2.2 미국 NIST 위험관리 프레임워크

미국은 2002년 전자정부법(e-Government Act) 제3편에 속하는 FISMA(Federal Information Secuirty Management Act,연방정부 보안관리법)를 제정하였다. FISMA에 의해 연방 정부기관은 국가표준기술원(NIST)에서 발간하는 표준, 가이드라인 등에 따라 정보시스템에 대한 적절한 보호조치를 취해야 한다. NIST는 2009년 위험관리 프레임워크인 RMF(Risk Management

Framework)를 개발하여 적용 가이드인 특별간행물(Special Publication) SP800-37을 제시하였다[10]. 구체적으로 "1.정보시스템 분류, 2.통제 항목 선택, 3.통제 항목 실행, 4.통제 항목 평가, 5.정보시스템 승인, 6.정보시스템 모니터" 의 6단계 라이프 사이클로 구성된다. 2, 3, 4단계의 통제 항목은 SP800-53에서 구체적으로 제시된다. SP800-53은 보안 통제 항목을 관리, 운영, 기술의 3개 클래스, 18개의 패밀리로 분류하여 선택할 수 있도록 하는 권고수준의 표준 가이드라인이다. 동 가이드라인은 강제사항은 아니지만 미국의 주요기반시설을 구성하는 주 및 지방 정부, 민간 영역의 조직들도 동 지침을 따라 줄 것을 권고하고 있다. 본 논문에서는 Revision 3을 대상으로 하였으나 2012년 2월 Revision 4의 Draft문서가 작성된 상태이다[11][12].

2.3 스마트 그리드를 위한 정보보호 관리체계

미국은 이미 NIST, 에너지부(DOE), 국토안보부(DHS), 북미전기신뢰성협회(NERC) 등에서 국가주요기반시설인 스마트 그리드 관련 위험관리 프로세스 및 정보보호 관리체계를 개발하였다. NIST는 스마트 그리드 상호운용성 패널(Smart Grid Interoperability Panel, SGIP)을 설립하여 스마트 그리드 사이버보안 가이드라인 NISTIR 7628(이하 NISTIR 7628)[13]을 발표하였고 꾸준한 스마트 그리드 보안 표준을 위한 연구 결과를 통해 스마트 그리드 상호 운용성을 위한 프레임워크 및 로드맵을 구축하여 실현 중이다[14].

[표 2] 국내외 정보보호 관리체계 비교

	K-ISMS	ISO27001	NIST RMF
담당기관	한국인터넷진흥원(KISA)	국제 표준화 기구	미국 국가표준기술원(NIST)
관리절차	1.정보보호정책 수립 2.관리체계 범위 설정 3.위험관리 4.구현 5.사후관리	PDCA모델 1.ISMS 수립 2.ISMS 구현 및 운영 3.ISMS 모니터 및 검토 4.ISMS 유지 및 개선	위험관리 프레임워크(RMF, SP800-37)를 따름 1.정보시스템 분류 2.통제 항목 선택 3.통제 항목 실행 4.통제 항목 평가 5.정보시스템 승인 6.정보시스템 모니터
구조	15개 분야 137개 통제항목 (관리과정 14개, 문서화 3개, 정보보호대책 120개)	11개 도메인	* SP800-53(rev3) 3 클래스 (관리, 운영, 기술) 18 패밀리
통제항목	정보보호 정책 정보보호 조직 외부자 보안 정보자산 분류 정보보호 교육 및 훈련 인적 보안 물리적 보안 시스템 개발 보안 암호 통제 접근 통제 운영 관리 전자거래 보안 보안사고 관리 검토,모니터링 및 감사 업무 연속성 관리	보호 정책 정보보호 조직 자산 관리 인적 자원 보호 물리적/환경적 보호 통신 및 운영 관리 접근 통제 정보시스템 인수,개발 및 유지보수 정보보호 사고 관리 업무 연속성 관리 준거성	접근 통제(AC) 인식 및 훈련(AT) 감사 및 책임 추적성(AU) 보안평가 및 승인(CA) 구성 관리(CM) 비상대응계획(CP) 식별 및 인증(IA) 사고 대응(IR) 유지보수(MA) 매체 보호(MP) 물리적/환경적 보안(PE) 계획(PL) 정보보안 프로그램 관리(PM) 인적 보안(PS) 위험 평가(RA) 시스템 및 서비스 인수(SA) 시스템 및 통신 보호(SC) 시스템 및 정보 무결성(SI)
세부 통제항목	120개	133개	198개
특징	국내 정보보호 관리체계	국제 표준의 정보보호 관리체계	미 연방 정보시스템 및 조직에 대한 보안통제 권고항목
발표년도	2002.4	2005.10	2009.8

〔표 3〕 스마트 그리드 관련 정보보호 관리체계 비교

	NISTIR 7628	Catalog of Control System Security (ver7)	CIP (ver4)
담당기관	NIST 스마트 그리드 상호운용성 패널(SGIP)	미 국토안보부(DHS)	북미전기신뢰성협회(NERC)
관리절차	1.적용 사례 분석 2.위험 평가 수행 3.상위등급의 보안 요구사항 4.보안 구조 및 스마트 그리드 표준 평가 5.준수 평가	-	통제항목 순서에 따라 관리 절차 수립
구조	3 볼륨 19 패밀리	19 패밀리	8 보호 프로그램
통제항목	접근 통제 인식 및 훈련 감사 및 책임 추적성 보안평가 및 승인 구성 관리 운영 연속성 식별 및 인증 정보 및 문서관리 사고 대응 시스템* 개발 및 유지보수 매체 보호 물리적/환경적 보안 계획 보안 프로그램 관리 인적 보안 위험 평가 시스템* 및 서비스 인수 시스템* 및 통신 보호 시스템* 및 정보 무결성 *스마트 그리드 정보시스템	보호 정책 정보보호 조직 인적 보안 물리적/환경적 보안 시스템 및 서비스 인수 구성 관리 전략 계획 시스템 및 통신 보호 정보 및 문서 관리 시스템 개발 및 유지보수 보안 의식향상 및 훈련 사고 대응 매체 보호 시스템 및 정보 무결성 접근 통제 감사 및 책임 추적성 모니터링 및 제어시스템 정책 검토 위험관리 및 평가 보안 프로그램 관리	주요 자산 식별 보안관리 통제 인사 및 훈련 전자 보안 경계 물리적 보안 시스템 보안 관리 사고기록 및 대응계획 주요 자산 복구 계획
세부 통제항목	197개	250개	42개
특징	스마트 그리드 사이버 보안 가이드라인	제어시스템 보안 목록으로 표준 개발업체용 권고항목	주요기반시설보호(CIP)를 위한 대규모 전력시스템에 의무적으로 적용되는 신뢰성 표준
발표년도	2010.9	2011.4	2011.1

NISTIR 7628은 미국 DHS의 제어시스템 보안 카탈로그와 NERC CIP(Critical Infrastructure Protection) 표준, 그리고 NIST SP800-53을 적용하여 개발되었다. 3개의 볼륨으로 구성되어 볼륨 1에서는 스마트 그리드 사이버 보안 전략, 구조, 상위 등급의 요구사항을, 볼륨 2에서는 프라이버시를 볼륨 3에서는 취약점 클래스, 적용 사례 시나리오 등 분석 및 레퍼런스를 제공한다. 따라서 스마트 그리드와 관련한 보안 권고항목들을 개발하도록 적절한 프레임워크를 제공한다. 관리 절차는 "1.적용사례(Use case) 분석, 2.위험평가 수행, 3.상위 등급의 보안 요구사항, 4.보안 구조 및 스마트 그리드 표준 평가, 5.준수 평가"의 5단계로 이루어진다.

DHS의 제어시스템 보안 카탈로그는 SCADA와 같은 국가 제어시스템의 보안 통제 항목을 선택하도록 공통의 카탈로그를 프레임워크 형식으로 제공한다. DHS 카탈로그는 NIST SP800-53에서 정의된 통제 항목과 비교하여 250개의 추천 통제 항목을 제공한다〔15〕.

NERC의 CIP 표준은 SCADA와 같은 주요기반시설을 보호하기 위해 의무적으로 발전시스템에 적용해야 하는 신뢰성 표준이다. 주요 사이버 자산을 보호하기 위한 프레임워크를 제공하며 "1.주요 자산 식별, 2.보안관리 통제, 3.인사 및 훈련, 4.전자 보안 경계, 5.물리적 보안, 6.시스템 보안 관리, 7.사고기록 및 대응계획, 8.주요 자산 복구 계획"의 CIP-002부터 CIP-009까지 8개 보호 프로그램 순서에 따라 관리 절차가 수립된다〔16〕〔17〕.

II. 비교 연구

3.1 정보보호 관리체계 비교

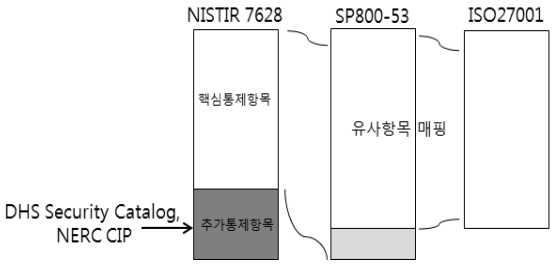
국내·외 정보보호 관리체계는 각각의 관리 절차 및 통제 항목을 가지고 있다. K-ISMS과 ISO27001 그리고 NIST RMF에 적용하고 있는 SP800-53의 통제 항목은 〔표 2〕에서 비교하였고, 스마트 그리드와 관련하여 미국을 중심으로 개발된 NISTIR 7628과 제어시스템 보안 카탈로그 그리고 CIP 표준은 〔표 3〕에서 비교하였다.

3.2 상관 관계

SP800-53의 부록(Appendix H)은 ISO27001의 부록(Annex A)에서 제시하는 통제 항목과 매핑한 테이블을 제공한다. 미국 표준인 SP800-53의 통제 항목은 ISO27001의 통제 항목을 거의 대부분 포함하고 있다[5]. 반대로 ISO27001에는 존재하지 않지만 SP800-53에서만 제시되고 있는 통제 항목은 그 수가 상대적으로 많다[6]. SP800-53은 ISO27001, SP800-53의 통제 항목을 이용하는 조직이 ISO27001의 통제 항목만을 이용하는 조직보다 NIST의 정보보호 표준, 가이드라인을 준수할 가능성이 높음을 매핑 테이블을 통해 입증하였다. NISTIR 7628의 부록(Appendix A)은 SP800-53, DHS의 제어시스템 보안 카탈로그의 추천 통제 항목, NERC CIP의 통제 항목과 매핑한 테이블을 제공하여 NISTIR 7628의 통제 항목이 높은 수준의 보안 요구사항을 제시하고 있음을 보였다. NISTIR 7628의 통제 항목은 SP800-53의 통제 항목 가운데 스마트 그리드와 관련되지 않은 항목은 제외한 후 새로운 통제 항목을 추가하여 개발되어 실제 통제 항목 개수는 큰 차이가 없다.

3.3 상관 관계에 따른 미국의 방법론

미국은 SP800-53의 보안 통제 항목을 적용하여 스마트 그리드, 클라우드 등의 다양한 영역의 보안 통제 항목을 개발 중이다. 2012년 시작된 미국 공공분야 클라우드 인증 프로그램인 FedRAMP (Federal Risk and Authorization Management Program)도 SP800-53에서 제공하는 하급(Low Level) 및 중급(Moderate Level) 통제 항목 패키지 중에서 일부 항목을 추가하거나 삭제하여 통해 클라우드 서비스에 적용하였다[7)][18][19]. 스마트 그리드 사이버보안 가이드라인의 보안 통제 항목 또한 SP800-53을 적용하여 개발되었다. 따라서 미국에서 스마트 그리드와 관련된 보안 통제 항목을 도출하는 방법은 〔그림 2〕와 같이 나타낼 수 있다.

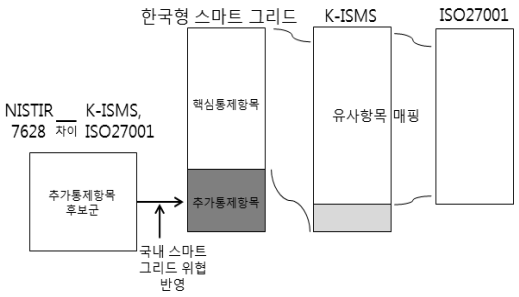


〔그림 2〕 통제 항목 도출 방법

III. 평가 기준 도출

4.1 방법론

본 논문은 한국형 스마트 그리드 정보보호 관리체계와 관련된 통제 항목을 도출하기 위해 미국의 보안 통제 항목 도출 방법과 유사하게 적용한다〔그림 3〕.



〔그림 3〕 한국형 스마트 그리드 보안 통제 항목 도출 방법

5) 「A.11.5.6 연결시간 제한」, 「A.11.6.2 중요시스템 분리」, 「A.12.2.4 출력 데이터 검증」 3개 항목 제외

6) 「AC-22 공개적으로 접근가능한 내용」 등 38개 항목

7) FedRAMP의 보안 통제 항목 개수

등급	NIST Baseline (SP800-53)	추가	계
Low	115	1	116
Moderate	252	45	297

〔표 4〕 ISO27001 「통신 및 운영관리」 항목의 비교 분석

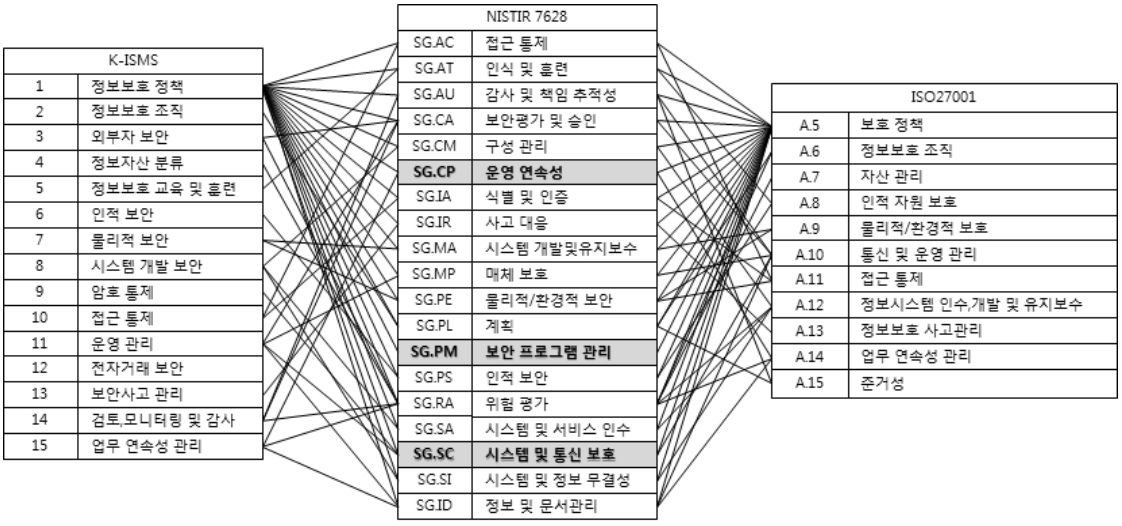
K-ISMS		NIST SP800-53		NISTIR 7628		ISO27001	
11. 운영 관리						A.10 통신 및 운영 관리	
11.1 운영 절차와 책임						A.10.1운영 절차 및 책임	
11.1.1	운영절차의 문서화	XX-1 control sCM-9	각 항목의 정책과 절차 구성 관리 계획	XX-1 controls SG.CM-11	각 항목의 정책과 절차 구성 관리 계획	A.10.1.1	문서화된 운영 절차
11.1.2	정보자산의 변경관리	CM-1 CM-3 CM-4 CM-5 CM-9	구성관리 정책과 절차 구성 변경 통제 보안 영향 분석 변경을 위한 접근제한 구성 관리 계획	SG.CM-1 SG.CM-3 SG.CM-4 SG.CM-5 SG.CM-11	구성관리 정책과 절차 구성 변경 통제 구성 변경 모니터링 구성 변경을 위한 접근 제한 구성 관리 계획	A.10.1.2	변경 관리
11.1.3	직무 분리	AC-5	직무 분리	SG.AC-6	직무 분리	A.10.1.3	직무 분리
11.1.4	개발과 운영 환경의 분리	CM-2	기준선(Baseline) 구성	SG.CM-2	기준선 구성	A.10.1.4	개발, 테스트, 운영설비의 분리
11.1.5	외부 운영 설비의 관리						

하지만 국내는 SP800-53과 같은 체계적인 통제 항목 리스트가 존재하지 않기 때문에 K-ISMS 통제 항목을 근거로 하여 통제 항목을 도출할 수 있다. 먼저 한국형 스마트 그리드 정보보호 관리체계의 핵심 평가 기준을 도출하기 위해 K-ISMS와 ISO27001의 보안 통제 항목을 비교 분석한다. 그리고 NISTIR 7628과 K-ISMS, ISO27001의 통제 항목을 비교 분석하여 중복되지 않은 통제 항목을 추가 평가 기준 후보군으로 도출한다. 이와 같은 비교 분석 방법은 4.2장에서 다룬다.

4.2 비교 분석

보안 통제 항목의 비교 분석은 〔표 4〕과 같이 상세한 매핑 테이블을 통해 수행 되었다. 본 논문에서는 매핑 테이블을 모두 나열할 수 없으므로 분석 결과만을 제시한다.

NISTIR 7628의 19개 패밀리로 구성된 통제 분



〔그림 4〕 NISTIR 7628 과 ISMS 통제 분야 매핑도

야는 적게는 5개에서 많게는 30개의 세부 통제 항목을 포함하고 있다. 이 세부 통제 항목을 K-ISMS, ISO27001과 상세히 매핑하여 매핑도로 나타낸 결과는 〔그림 4〕와 같다. 매핑율로 나타낸 결과 운영 연속성, 보안 프로그램 관리, 스마트 그리드 정보시스템 및 통신 보호의 3개 통제 분야는 60% 이하로 상대적으로 낮은 수준이었다〔표 5〕. 세부 통제 항목을 모두 비교한 결과 K-ISMS는 NISTIR 7628과 79.7% 매핑되었고 ISO27001은 NISTIR 7628과 78.2% 매핑되었다. 매핑율이 서로 비슷한 것은 K-ISMS와 ISO27001이 많은 유사성을 가지고 있다는 것을 나타낸다.

NISTIR 7628을 기준으로 보았을 때 K-ISMS와 ISO27001의 통제 항목 매핑 결과는 약 80%를 밑도는 수준이다. 이것은 20% 이상 통제 항목이 부족함을 의미한다. 따라서 기존 K-ISMS 및 ISO27001 인증을 받은 기업이라 할지라도 스마트 그리드 정보보호 관리를 위해서는 추가적인 평가 기준이 고려되어져야 한다.

NISTIR 7628의 "운영 연속성, 보안 프로그램 관리, 시스템 및 통신보호와 기타" 의 항목은 한국형 스마트 그리드 정보보호 관리체계를 위한 평가 기준을 개발할 때 고려해야 할 후보군으로 분류할 수 있다. 기타 항목에는 NISTIR 7628의 19개 통제 분야 중 "운영 연속성, 보안 프로그램 관리, 시스템 및 통신보호" 를 제외한 나머지 16개 분야에서 매핑되지 않은 세부 통제 항목이 포함된다.

4.3 평가 기준 도출

4.3.1 핵심 평가 기준 도출

핵심 평가 기준은 K-ISMS의 15개 보안 통제 항목을 모두 선정한다. 통제 항목 「12.전자거래 보안」의 경우 NISTIR 7628의 통제 항목과 매핑되지는 않지만 국내 상황을 고려하여 보안요건이 강화된 항목이고 ISO27001에서 다루지 않는 영역을 추가한 항목이므로 핵심 평가 기준에 반영한다. 이미 국내에서는 K-ISMS 인증 제도가 정보통신서비스 사업자를 대상으로 의무화되었기 때문에 K-ISMS 인증을 받은 기업의 경우 추가적인 평가 기준만을 고려할 수 있도록 개발하기 위해서라도 K-ISMS의 15개 항목은 한국형 스마트 그리드 정보보호 관리체계를 위한 핵심 평가 기준이 된다.

〔표 5〕 세부 통제 항목 매핑율

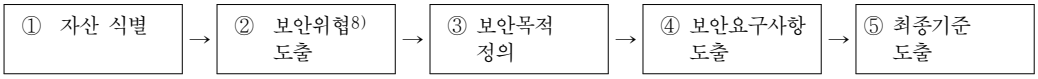
구 분		K-ISMS		ISO27001	
NISTIR 7628 통제 분야 (세부 통제 항목 개수)		매핑수	비율(%)	매핑수	비율(%)
SG.AC	접근 통제 (21)	19	90.5	19	90.5
SG.AT	인식 및 훈련 (7)	6	85.7	5	71.4
SG.AU	감사 및 책임 추적성 (16)	15	93.8	13	81.3
SG.CA	보안평가 및 승인 (6)	6	100.0	6	100.0
SG.CM	구성 관리 (11)	9	81.8	9	81.8
SG.CP	운영 연속성 (11)	6	54.5	5	45.4
SG.IA	식별 및 인증 (6)	4	66.7	4	66.7
SG.ID	정보 및 문서 관리 (5)	5	100.0	5	100.0
SG.IR	사고 대응 (11)	10	90.9	10	90.9
SG.MA	시스템 개발 및 유지보수 (7)	6	85.7	6	85.7
SG.MP	매체 보호 (6)	6	100.0	6	100.0
SG.PE	물리적/환경적 보안 (12)	11	91.7	11	91.7
SG.PL	계획 (5)	4	80.0	5	100.0
SG.PM	보안 프로그램 관리 (8)	3	37.5	3	37.5
SG.PS	인적 보안 (9)	9	100.0	9	100.0
SG.RA	위험 평가 (6)	6	100.0	6	100.0
SG.SA	시스템 및 서비스 인수 (11)	9	81.8	10	90.9
SG.SC	시스템 및 통신 보호 (30)	15	50.0	14	46.7
SG.SI	시스템 및 정보 무결성 (9)	8	88.9	8	88.9
전 체 (197)		157	79.7	154	78.2

4.3.2 추가 평가 기준 후보군 도출

4.2장의 비교 분석 결과를 토대로 4개 통제 분야에 대한 38개 세부 통제 항목을 〔표 6〕과 같이 도출하였다. 본 논문에서는 도출된 세부 통제 항목을 한국형 스마트 그리드 정보보호 관리체계를 위한 평가 기준 후보군으로 놓는다. 평가 기준 후보군에서 한국형 스마트 그리드의 특성을 반영한 최종 평가 기준 도출은 5장에서 다룬다.

〔표 6〕 스마트 그리드 평가 기준 후보군

분야	세부 통제 항목	내용
운영 연속성	운영 연속성 훈련	스마트 그리드 시스템과 관련한 운영 연속성의 역할과 책임 훈련 및 연수 실시
	운영 연속성 계획 갱신	스마트 그리드 시스템에 대한 운영 연속성 계획을 실시함으로 인해 발생되는 문제점 및 변경사항을 주기적으로 갱신
	예비의 제어 센터	주 센터를 운영할 수 없을 때를 대비한 협약, 회선 등 예비의 통제 센터에서 필요한 제반사항 확인
	스마트 그리드 정보시스템 복구 및 재구성	보안에 치명적인 패치, 보안과 관련된 구성 설정 등이 보안이 유지된 상태에서 복구 및 재구성
	자동 안전장치 응답	통신 중의 손실, 스마트 그리드 정보시스템 자체 손실시에 대비한 적절한 자동 안전장치 절차 보유
보안 프로그램 관리	보안 프로그램 계획	전사적인 보안 프로그램 계획, 검토 및 변경, 문제점 발생시 계획 수정
	보안 아키텍처	조직의 자산, 조직원, 타 조직의 위험 결과를 고려한 보안 아키텍처 개발
	운영을 위한 보안 승인 절차	보안 승인 절차를 통한 조직 정보시스템의 보안 상태 관리
	미션/비즈니스 절차 정의	위험을 고려한 보안 목적과 비즈니스 절차를 정의
	관리 책임 추적성	사이버 보안 정책 승인을 위해 역할과 책임을 명시하고 관리 책임 추적성의 프레임워크를 정의
시스템 및 통신 보호	통신 채널 분할	원격 측정/데이터 인수 서비스 및 관리 기능성을 위한 통신 채널 분할
	잔여 정보	공유된 스마트 그리드 시스템 자원을 경유한 승인되지 않은 정보 전송 금지
	서비스 거부 공격 보호	서비스 거부 공격에 대한 방어 체계
	신뢰 경로	사용자와 스마트 그리드 시스템 사이의 신뢰선 통신 경로 설치
	협업 컴퓨팅	협업 컴퓨팅 정책 개발, 배포 그리고 주기적인 검토 및 갱신
	VoIP	VoIP를 사용하여 스마트 그리드 시스템을 모니터링하고 제어 시 가이드라인 구현 및 제한된 사용
	안전한 이름/주소 변환 서비스	스마트 그리드 시스템 구성시 이름/주소 변환을 통해 계층적이고 분산된 운영 지원
	알려진 상태 고장	스마트 그리드 시스템은 고장 시 이미 알려진 상태 유지 필요
	최소 노드	컴포넌트를 프로세싱할 때 최소한의 기능성과 데이터 저장을 포함
	허니팟	스마트 그리드 시스템을 표적으로 하는 공격을 탐지하기 위해 허니팟 운영
	운영체제와 독립적인 애플리케이션	스마트 그리드 시스템은 운영체제에 종속되지 않은 애플리케이션을 포함
	미사용 정보의 기밀성	스마트 그리드 시스템은 모든 주요 보안 속성에 암호화 매커니즘을 사용하여 정보 노출 방지
	이질성	스마트 그리드 시스템의 구현시 동질적이지 않은 다양한 기술 사용
	가상화 기술	서로 다른 구성의 컴포넌트와 컴포넌트의 다른 형식 사용하기 위해 가상화 기술 사용
기타	외부 정보 제어 시스템의 사용	인가된 사용자만이 외부의 정보 시스템을 제어
	공개적으로 접근 가능한 내용	공개적으로 접근 가능한 정보 시스템에 정보를 추가하는 인가된 사용자 지정
	보안 책임 테스트	역할과 책임을 근거로한 보안 정책과 절차의 지식을 테스트
	부인 방지	스마트 그리드 정보 시스템의 부인 방지 기능
	기준선 구성	스마트 그리드 현재 기본 설정을 개발, 문서화, 유지
	구성 관리 계획	스마트 그리드 시스템의 구성 항목 및 절차 정의
	장치 식별 및 인증	스마트 그리드 시스템은 연결 전 조직에 기 정의된 장치리스트를 유일하게 식별 및 인증
	인증자 피드백	스마트 그리드의 인증 매커니즘은 비인가된 개인에 의해서 사용되는 것을 보호하기 위한 피드백 관찰
	사고 대응 테스트 및 연습	조직에서 기 정의된 테스트 절차를 사용하여 사고 대응 테스트 및 연습
	구형 스마트 그리드 정보시스템 업그레이드	구형의 스마트 그리드 정보시스템을 업그레이드하기 위한 정책과 절차 개발
	백업 작업 공간	주 작업 공간이 없어도 제대로 운영될 수 있는 백업의 작업 공간 마련
	개인정보 영향평가	스마트 그리드 시스템에 대한 개인정보 영향평가를 수행
	생명주기 지원	시스템 개발 생명주기 방법론을 사용하여 스마트 그리드 시스템 관리
	보안 기능성 검증	스마트 그리드 정보시스템내 보안 기능의 정확한 작동을 검증



〔그림 5〕 한국형 스마트 그리드 정보보호 관리체계 평가 기준 제안 절차

IV. 평가 기준 제안

본 장에서는 4장에서 도출한 평가 기준 후보군에 국내 스마트 그리드 업무 환경을 적용하여 5단계의 절차〔그림 5〕를 거쳐 한국형 스마트 그리드 정보보호 관리체계를 위한 평가 기준을 제안한다. 제안 절차는 정보보호시스템 공통평가기준(Common Criteria)을 통해 보호 프로파일(Protection Profile) 개발 시 보안 요구사항을 도출하는 방법론[9]을 준용한다〔20〕.

5.1 자산 식별

최근 지식경제부가 제정·시행한 「지능형전력망 정보의 보호조치에 관한 지침」〔21〕은 지능형전력망 정보의 신뢰성과 안전성을 확보하기 위해 지능형전력망 사업자가 준수해야 할 보호조치를 제공하고 관련 용어를 정의한다. 지능형전력망 사업자란 "지능형전력망 사업자", "지능형전력망 기반구축사업자", "지능형전력망 서비스제공사업자" 를 의미하며 〔표 7〕과 같이 정의한다. 지능형전력망 사업자는 기반구축사업자와 서비스제공사업자를 포함하는 보다 넓은 범위의 사업자를 의미한다. 지능형전력망 사업자가 보호해야 할 자산은 "지능형전력망 통신망", "지능형전력망 시스템", "지능형전력망 기기" 의 세 가지로 분류할 수 있으며, 본 논문에서는 이 세 가지를 한국형 스마트 그리드 자산으로 정의한다〔표 8〕.

〔표 7〕 지능형 전력망 사업자

지능형전력망 사업자	지능형전력망의 구축 및 이용에 관한 재화 또는 지능형전력망을 이용한 서비스를 제공하는 사업으로서 다음 어느 하나에 해당하는 사업을 영위하는 자 - 지능형전력망 기반 구축사업 - 지능형전력망 기기 및 제품 제조사업 (지침의 적용대상에서 제외) - 지능형전력망 서비스 제공사업
지능형전력망 기반구축 사업자	지능형전력망을 이용하여 전기를 공급하거나 전력계통의 운영에 관한 사업을 수행하는 「전기사업법」 제7조에 따라 허가받은 송전사업자, 배전사업자, 구역전기사업자 또는 같은 법 제35조에 따라 설립된 한국전력거래소
지능형전력망 서비스제공 사업자	지능형전력망을 이용한 서비스를 제공하는 수요반응 관리서비스 제공사업, 전기차 충전 서비스 제공사업 또는 기타 서비스 제공사업을 수행하는 자

〔표 8〕 한국형 스마트 그리드 자산

지능형전력망 통신망	지능형전력망을 운용하기 위해 사용되는 정보통신망
지능형전력망 시스템	지능형전력망을 운용하기 위해 사용되는 정보시스템
지능형전력망 기기	지능형전력량계, 데이터수집장치, 센서, 충전기, 신재생 발전원, 소규모 발전기 등 지능형전력망에 연결되는 기기 또는 설비

5.2 보안 위협 도출

스마트 그리드 환경에서 발생할 수 있는 모든 위협을 도출하기 위해 우선 공개된 취약점 데이터베이스 웹사이트 및 위협 관리 웹사이트[10]를 통해 스마트 그리드 관련 취약점 및 위협을 분류할 수 있다. NISTIR 7628에서 제공하는 스마트 그리드 관련 취약점은 미국 에너지부 산하 아이다호 국립연구소 및 NERC에서 발표한 취약점 등을 모두 포함하고 있다〔22〕〔23〕. 이 가운데 스마트 그리드의 보안 위

8) 보호 프로파일 개발 시 위협, 조직의 보안정책, 가정사항의 3가지 보안 문제 중 본 논문에서 위협만을 고려하는 이유는 정보보호시스템 개발 시 실제 운영 환경을 고려하여 보안 문제를 정의해야 하지만 정보보호 관리체계는 실제 운영 중인 조직의 위험을 관리하므로 위협에 운영 환경, 조직의 정책 등이 모두 포함된다.

9) 보호 프로파일 개발 시 정보보호시스템의 자산 정의(TOE)후에 위협, 조직의 보안정책, 가정 사항으로부터 보안목적을 도출한다. 도출된 보안목적으로부터 CC 2부의 보안기능 요구사항에서 나열된 컴포넌트들을 선택한다. 최종 선택된 컴포넌트는 이론적 근거를 바탕으로 추적이 가능하고 정당성이 입증된다.

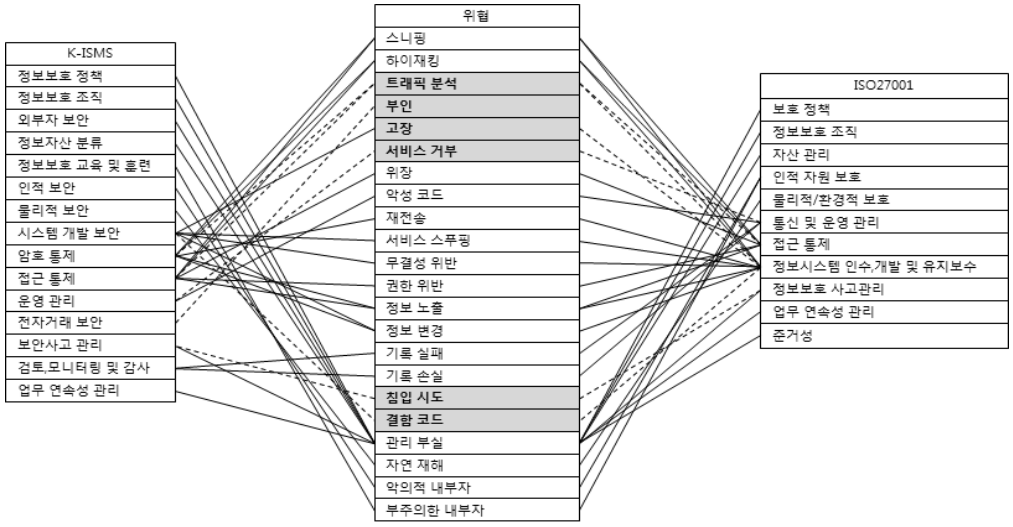
10) MITRE(http://cve.mitre.org), SANS ISC(https://isc.sans.edu), CERTCC(http://www.cert.org), Symantec DeepSight Threat Management System(https://tms.symantec.com) 등 다수

협은 기존 네트워크 환경의 보안 위협으로 대응할 수 있는 현존하는 스마트 그리드 시스템 및 네트워크 영역으로 제한한다[24][25][26].

현존하는 스마트 그리드 환경의 모든 위협 가운데 국내 특성을 반영한 한국형 스마트 그리드 환경에서 발생할 수 있는 모든 위협을 도출하기 위해 본 논문에서는 「지능형전력망 정보의 보호조치에 관한 지침」을 근거로 하여 보호 조치가 제대로 구현되지 않았을 경우 발생할 수 있는 위협을 [표 9]와 같이 재구성하여 분류하였다.

[표 9] 한국형 스마트 그리드 환경에서 발생 가능한 위협

구분	보호 조치 항목	내용	발생 가능한 위협
기술적 보호 조치	지능형전력망 시스템 보안관리	시스템의 효율적인 보안관리를 위한 관리책임자 지정 및 패치 등의 보안관리	관리부실, 위장, 정보노출, 악성코드, 침입시도, 악의적 내부자
	시스템 계정 관리	시스템 계정의 비인가자 도용 및 불법접속 방지를 위한 계정의 등록·변경·폐기	위장, 권한위반, 관리부실
	비밀번호 관리	비밀번호의 암호화 보관 및 주기적 변경	위장, 정보노출, 기록실패, 기록손실
	무선통신망 보안	무선통신망 이용의 최소화 및 통신내용 암호화	스니핑, 하이재킹, 위장, 권한위반
	정보보호시스템 운용	침입차단시스템, 침입탐지 기능의 정보보호시스템 설치·운용	서비스거부, 침입시도
	악성코드 방지	악성코드 감염을 방지하기 위한 예방대책 수립·시행 및 조치	악성코드
	암호모듈	국정원 검증필 암호모듈 사용 및 128비트 이상의 보안 강도 만족	정보노출, 정보변경
	암호키 관리	암호키의 재사용을 할 수 없도록 관리 정책 수립·시행	재전송, 관리부실
	지능형전력망 시스템 인증	중간자공격, 스니핑 공격을 차단하기 위한 상호인증	스니핑, 하이재킹, 부인
	지능형전력망 기기 통신보안	통신내용 위·변조 및 도·감청 방지 및 부인방지 기능 제공	스니핑, 하이재킹, 트래픽분석, 부인, 서비스 스푸핑, 무결성위반
	지능형전력망 기기 데이터보안	최소 정보를 필요한 기간만 기기에 저장하고 중요 정보 암호화	무결성위반, 정보노출, 정보변경
물리적 보호 조치	출입자 출입통제	신원확인이 가능한 출입통제장치 설치 및 출입에 관한 정책과 절차 수립·시행	악의적내부자
	출입자 감시통제	CCTV 설치 및 출입자 감시, 출입기록의 보관	악의적내부자, 기록실패, 기록손실
	시설물 접근통제	지능형전력망 시스템·통신망·기기를 물리적인 보호장치로 보호	악의적내부자, 관리부실, 고장
관리적 보호 조치	정보보호계획 수립	지능형전력망 시스템·통신망·기기의 보호대책 등 정보보호 계획 수립·시행	관리부실
	정보보호 전담조직	정보보호계획을 계획·실행·검토하는 전담조직 구성 및 담당자 지정	관리부실
	정보보호 교육 실시	시스템 운용자 및 정보보호담당자에 대한 정보보호 교육	부주의한내부자
	침해사고 대응체계 구축	해킹·바이러스 등 사이버공격의 신속한 대응 및 복구를 위한 대응체계 구축	서비스거부,악성코드,침입시도
	취약성 분석	지능형전력망 시스템 및 통신망에 대해 취약점 분석 수행 및 발견된 취약점 조치	악성코드,침입시도,결함코드
	정보보호시스템 정책관리	정보보호시스템 지침·가이드·매뉴얼을 근거로 정책 관리 수행	관리부실
	휴대용저장매체 관리	휴대용 저장매체 사용의 최소화 및 사용기록 저장	관리부실,기록실패,기록손실
	중요정보 보안	중요정보가 외부로 노출되지 않도록 관리	정보노출,정보변경,관리부실
	보안위해물품 관리	운영실과 정보통신실에 반·출입되는 보안위해물품에 대해 보안검색 수행 및 기록	관리부실,기록실패,기록손실
	외부자 보안	외부유지보수직원 및 외부용역자 등 3자의 접근 내역 기록·보관	위장,관리부실,기록실패,기록손실



〔그림 6〕 위협과 K-ISMS, ISO27001의 매핑도

22가지의 위협 가운데 기존의 정보보호 관리체계에서 관리되어지지 않는 스마트 그리드와 관련된 위협을 도출하기 위해 기존 K-ISMS, ISO27001의 통제 항목으로 모두 관리되어 매핑되는 위협은 실선으로, 부분적으로 관리되어지는 위협은 점선으로 표시하였다〔그림 6〕. 이 가운데 점선으로 표시된 위협과 매핑되지 않는 위협을 기존 K-ISMS, ISO27001 인증을 받은 지능형 전력망 사업자가 추가적으로 고려해야 할 6가지 보안 위협으로 선정하였다〔표 10〕. 위협원은 스마트 그리드 자산을 손상시킬 수 있으며 외부의 범죄 집단, 스파이, 해커 등의 인적 위협원과 홍수, 지진, 화재 등의 자연 위협원으로 구분할 수 있다. 단, 내부 직원, 외부 협력업체 등은 훈련, 교육 등으로 정보보호 측면에서 관리되어질 수 있으므로 위협원에 포함시키지 않는다.

〔표 10〕 보안 위협 도출

위협	내 용
트래픽 분석	위협원은 전송되는 정보의 패턴을 조사하고 정보의 내용을 추측할 수 있다.
부인	위협원은 데이터의 송수신 여부를 부인할 수 있다.
고장	스마트 그리드 자산의 고장으로 사용자에게 정상적인 서비스를 제공하지 못할 수 있다.
서비스 거부	위협원은 스마트 그리드 자산의 서비스 자원을 모두 사용하여 사용자의 서비스를 방해할 수 있다.
침입 시도	위협원은 스마트 그리드 자산 내 메모리 정보에 직접 접근할 수 있다.
결함 코드	스마트 그리드 자산 내 개발자에 의해 결함이 있는 코드가 삽입되어 오작동이 발생할 수 있다.

5.3 보안 목적 정의

보안 목적은 K-ISMS, ISO27001 인증을 받은 지능형 전력망 사업자가 추가적으로 고려해야할 6가지 보안 위협에 대응하기 위한 의도를 서술한 것으로 〔표 11〕과 같이 정의할 수 있으며 위협과 보안 목적

〔표 11〕 위협을 해결하기 위한 보안 목적

보안 목적	내용
가용성	스마트그리드 자산은 고장 또는 공격 발생 시 최소한의 보안 기능을 유지하여 정상적인 서비스를 제공해야 한다.
식별 및 인증	스마트그리드 자산은 접근을 허용하기 전 사용자의 신원을 인증해야 한다.
사고 대응	스마트그리드 자산의 물리적인 공격 침해공격에 대응 수단을 마련해야 한다.
관리	스마트그리드 자산은 인가된 관리자가 안전하게 관리할 수 있는 수단을 제공해야 한다.
결함코드 검사	스마트그리드 자산 내 개발자가 생성한 결함코드가 존재하는지 검사되어야 한다.
전송데이터 보호	스마트그리드 자산과 사용자 간 통신되는 전송 정보를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.

〔표 12〕 위협과 보안목적의 대응 상관관계

보안목적 / 위협	가용성	식별 및 인증	사고 대응	관리	결함 코드 검사	전송 데이터 보호
트래픽 분석						×
부인		×				
고장				×	×	
서비스 거부	×					
침입 시도			×			
결함 코드				×	×	

의 대응 상관관계는 〔표 12〕에서 제시하였다.

5.4 보안 요구사항 도출

보안목적을 충족하는 보안 요구사항을 보안기능 요구사항과 환경적 요구사항으로 나누어 서술한다. 4장에서 도출한 평가 기준 후보군은 기술, 운영, 관리의 3개 클래스로 구분되어 이 가운데 기술 클래스는 보안기능 요구사항으로 운영과 관리 클래스는 환경적 요구사항으로 나눌 수 있다. 이와 같은 과정을 통해 18개의 보안 요구사항이 도출되었다. 〔표 13〕은 보안 요구사항을 나열하였으며 〔표 14〕는 〔표 13〕에서 도출한 보안 요구사항이 보안목적을 충족하는지 이론적 근거를 제시한다.

〔표 13〕 보안 요구사항 도출

구분	보안 요구사항	클래스
보안기능 요구사항	부인 방지	기술
	인증자 피드백	
	통신 채널 분할	
	신뢰 경로	
	서비스 거부 공격 보호	
	허니팟	
환경적 요구사항	운영 연속성 훈련	운영
	운영 연속성 계획 갱신	
	예비의 제어 센터	
	스마트 그리드 정보시스템 복구 및 재구성	
	자동 안전장치 응답	
	구형 스마트 그리드 정보시스템 업그레이드	
	사고 대응 테스트 및 연습	
	백업 작업 공간	
	보안 기능성 검증	
	보안 프로그램 계획	관리
	보안 아키텍처	
	생명주기 지원	

5.5 최종 평가 기준 도출

4장의 평가 기준 후보군 가운데 5.4장에서 도출된 18개의 보안 요구사항을 대상으로 유사 항목 그룹핑을 통해 〔표 15〕와 같이 추가 평가 기준을 도출하였다. 도출된 평가 기준은 기존 K-ISMS, ISO27001 인증을 받은 지능형 전력망 사업자가 추가적으로 고려해야할 정보보호 관리체계 평가 기준이 된다.

추가로 도출된 "인증체계 관리, 운영 연속성 훈련, 테스트 베드 운영, 망 분리, 생명주기 관리" 의 5개 분야와 기존 K-ISMS의 15개 통제 분야를 합하여 ISMS기반의 한국형 스마트 그리드 정보보호 관리체계 최종 평가 기준을 〔표 16〕과 같이 제안한다.

V. 평가 기준 검증

5장에서 최종 도출된 K-ISMS기반의 한국형 스마트 그리드 정보보호 관리체계 최종 평가 기준과 「지능형전력망 정보의 보호조치에 관한 지침」의 대응 상관 관계를 나타낸 결과 〔표 17〕과 같이 모두 만족하므로 제안한 기준의 정당성이 입증된다.

〔표 14〕 보안 요구사항의 이론적 근거

보안 목적 / 보안 요구사항	가용성	식별 및 인증	사고 대응	관리	결함 코드 검사	전송 데이터 보호
부인 방지		×				
인증자 피드백		×				
통신 채널 분할						×
신뢰 경로						×
서비스 거부 공격 보호	×		×			
허니팟			×			
운영 연속성 훈련	×					
운영 연속성 계획 갱신	×					
예비의 제어 센터	×					
스마트 그리드 정보 시스템 복구 및 재구성	×					
자동 안전장치 응답	×				×	
구형 스마트 그리드 정보시스템 업그레이드				×		
사고 대응 테스트 및 연습			×			
백업 작업 공간	×				×	
보안 기능성 검증					×	
보안 프로그램 계획				×		
보안 아키텍처				×		
생명주기 지원				×		

〔표 15〕 추가 평가기준

평가 기준	보안 요구사항	내용
인증 체계 관리	부인 방지	보안이 강화된 상위 수준의 인증 매커니즘 사용
	인증자 피드백	
운영 연속성 훈련	운영 연속성 훈련	운영의 연속성을 위한 실제 훈련 실시 및 서비스 거부 공격 대응체계 구축·운영
	운영 연속성 계획 갱신	
	예비의 제어 센터	
	스마트 그리드 정보시스템 복구 및 재구성	
	자동 안전장치 응답	
	서비스 거부 공격 보호	
테스트 베드 운영	허니팟	테스트 베드 및 허니팟 시스템 구축·운영
	사고 대응 테스트 및 연습	
	백업 작업 공간	
망 분리	통신 채널 분할	제어망은 인터넷망과 분리되어야 하고 신뢰된 경로를 통해서 제어
	신뢰 경로	
생명 주기 관리	보안 프로그램 관리	스마트 그리드 기기의 취약점 진단, 업그레이드, 기능성 검증 등 생명주기 관리
	보안 아키텍쳐	
	보안 기능성 검증	
	생명주기 지원	
	구형 스마트 그리드 정보시스템 업그레이드	

〔표 16〕 최종 평가 기준 도출

한국형 스마트 그리드 정보보호 관리체계 평가 기준			
핵심 평가 기준	1	정보보호 정책	K-ISMS 기반
	2	정보보호 조직	
	3	외부자 보안	
	4	정보자산 분류	
	5	정보보호 교육 및 훈련	
	6	인적 보안	
	7	물리적 보안	
	8	시스템 개발 보안	
	9	암호 통제	
	10	접근 통제	
	11	운영 관리	
	12	전자거래 보안	
	13	보안사고 관리	
	14	검토,모니터링 및 감사	
	15	업무 연속성 관리	
추가 평가 기준	16	인증체계 관리	-
	17	운영 연속성 훈련	
	18	테스트 베드 운영	
	19	망 분리	
	20	생명주기 관리	

VI. 결 론

K-ISMS, ISO27001 등은 대다수의 기업에 적용하여 위험을 관리할 수 있는 범용적이고 일반적인 통제 항목을 적용한 정보보호 관리체계 인증 제도로써 스마트 그리드와 관련된 사업자가 고려해야 하는 최소 요구수준의 보안 대책이라 할 수 있다. 미국은 이미 스마트 그리드와 관련하여 보다 높은 수준의 통제 항목을 적용하기 위해 NISTIR 7628을 개발하였다. 국내 스마트 그리드 환경에서도 국가주요기반시설을 관리하고 통제하기 위해 보다 상위 수준의 평가 기준을 추가적으로 개발하여야 한다. 스마트 그리드 사업자와 같이 보다 높은 수준의 정보보호 수준을 고려해야 하는 조직을 위한 국내용 권고 수준의 통제 항목 리스트가 체계적으로 개발되어진다면 K-ISMS, G-ISMS, 정보보안 관리실태 평가, IT 부문 경영실태 평가 등의 평가·인증 시 평가 기준을 추가할 때 중복되지 않는 상호 독립적인 항목을 각 영역별로 개발할 수 있다.

본 논문은 국내 스마트 그리드 특성을 고려한 한국형 스마트 그리드 정보보호 관리체계를 위한 평가 기준을 핵심 평가 기준과 추가 평가 기준으로 나누어 제안하였다. 한국형 스마트 그리드 정보보호 관리체계 인증제도가 확립·시행되었을 경우 기존 K-ISMS, ISO27001 인증을 받은 스마트 그리드 사업자는 추가 평가 기준만으로 평가·인증을 수행하여 중복되고 불필요한 업무를 최소화할 수 있다.

본 논문을 통해 국가·공공 분야, 민간 분야를 모두 포함하고 상위 수준의 통제 항목을 적용한 지속적인 정보보호 관리 제도가 마련되어 한국형 스마트 그리드가 새로운 부가가치를 창출하는 차세대 지능형 전력망으로 정착되길 기대한다.

〔표 17〕 평가 기준과 지침의 대응 상관 관계

관리체계 평가 기준 / 지침 항목	한국형 스마트 그리드 정보보호 관리체계																		
	정보보호정책	정보보호조직	외부자보안	정보자산분류	정보보호교육및훈련	인적보안	물리적보안	시스템개발보안	암호통제	접근통제	운영관리	전자거래보안	보안사고관리	검토·모니터링및감사	업무연속성관리	인증체계관리	운영연속성훈련	테스트베드운영	망분리	생명주기관리
지능형전력망 시스템 보안관리						×	×	×			×									×
시스템 계정 관리										×										
비밀번호 관리										×										
무선통신망 보안										×	×									
정보보호시스템 운용											×									×
악성코드 방지											×									
암호모듈									×							×				
암호키 관리									×											
지능형전력망 시스템 인증																×				
지능형전력망 기기 통신보안																×				
지능형전력망 기기 데이터보안																			×	
출입자 출입통제							×													
출입자 감시통제							×													
시설물 접근통제							×													
정보보호계획 수립	×														×					
정보보호 전담조직		×																		
정보보호 교육 실시					×															
침해사고 대응체계 구축													×				×			
취약성 분석																		×		
정보보호시스템 정책 관리	×													×						
휴대용저장매체 관리											×									
중요정보 보안				×								×							×	
보안위해물품 관리							×													
외부자 보안			×																	

참 고 문 헌

〔1〕 E. Richard Brown, "Impact of Smart Grid on distribution system design," Industry Applications Conference, Oct. 2008.

〔2〕 David Dolezilek, "Requirements or Recommendation? Sorting Out NERC CIP, NIST, and DOE Cybersecurity," IEEE 64th Annual Conference, pp. 328-333, Apr. 2011.

〔3〕 이경복,박태형,임종인, "정보보호정책 관점에서의 한국형 스마트 그리드 추진 방안에 관한 연구-미국과의 비교연구를 중심으로," 정보화정책 저널, 16(4), pp. 73-96, 2009년.

〔4〕 이철환,홍석원,이명호,이태진, "한국형 스마트

그리드를 위한 정보보호 체계 및 대책," Internet & Information Security, 2(1), pp. 71-89, 2011년 5월.
〔5〕 방송통신위원회, "국제표준 사이버 보안지수 개발 및 방법론 연구," 2010년 11월.
〔6〕 김지숙, 이수연, 임종인, "민간기업과 공공기관의 정보보호 관리체계 차이 비교," 정보보호학회논문지, 20(2), 2010년 4월.
〔7〕 E. Humphreys, "Implementing the ISO/IEC 27001 information security management system standard," Artech House, 2006.
〔8〕 한국인터넷진흥원, "정보보호관리체계(ISMS) 구축 및 운영 안내서," 2010년 7월.
〔9〕 한국인터넷진흥원, "정보보호관리체계 안내서," KISA 안내·해설, 제 2010-21호, 2010년 1월.
〔10〕 NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," Feb. 2010.
〔11〕 NIST SP 800-53 Rev3, "Recommended Security Controls for Federal Information Systems and Organizations," Aug. 2009.
〔12〕 NIST SP 800-53 Rev4, "Security and Privacy Controls for Federal Information Systems and Organizations," Feb. 2012.
〔13〕 NISTIR 7628, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," Sep. 2010.
〔14〕 NIST SP 1108R2, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0," Feb. 2012.
〔15〕 U.S. Department of Homeland Security, "Catalog of Control Systems Security: Recommendations for Standards Developers," Apr. 2011.
〔16〕 North America Electronic Reliability Corporation (NERC), "Critical Infrastructure Protection Series (CIP-001~CIP-009)," Jan. 2011.
〔17〕 Wipul Jayawickrama, "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001," Springer-Verlag Berlin Heidelberg, vol. 4277, pp. 565-574, 2006.
〔18〕 U. Lang and R. Schreiner, "Analysis of recommended cloud security controls to validate OpenPMF 'policy as a service'," Information Security Tech. Report, vol. 16, pp. 131-141, Aug. 2011.
〔19〕 박춘식, "미국 클라우드 컴퓨팅 보안인증제도 FedRAMP 소개," 정보통신산업진흥원 주간기술동향 pp. 13-24, 2012년 4월.
〔20〕 CCMB-2009-07-001, "정보보호시스템 공통평가기준," 개정3판, 2009년 7월.
〔21〕 지식경제부, "지능형전력망 정보의 보호조치에 관한 지침," 지식경제부 고시 제2012-129호, 2012년 6월.
〔22〕 Idaho National Laboratory, "Vulnerability Analysis of Energy Delivery Control Systems," Sep. 2011.
〔23〕 North America Electronic Reliability Corporation (NERC), "TOP 10 Vulnerabilities of control systems and their associated mitigations - 2007," Dec. 2006.
〔24〕 F. M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," IEEE T&D Conference, Apr. 2008.
〔25〕 한국인터넷진흥원, "클라우드 기반 스마트 그리드를 위한 보안기술 연구," 2010년 12월.
〔26〕 Tony Flick, Justin Morehouse, "Securing the Smart Grid: Next Generation Power Grid Security," Syngress, Sep. 2010.

〈著者紹介〉

김 기 철 (Kichul Kim) 학생회원
2001년 2월: 동국대학교 컴퓨터공학과 졸업
2002년 4월~현재: 금융결제원 재직 중
2011년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융IT보안, 정보보호관리체계, 정보보증, 정보보호제품 보안성 평가, 기반시설보호

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: KISA(舊한국정보보호진흥원) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 정보보호대학원 정교수
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~현재: 대검찰청 디지털수사 자문위원
2007년~2009년: 전자정부 서비스 보안위원회 사이버 침해사고대응 실무위원회 위원
2010년~현재: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: SK커뮤니케이션즈 보안강화 특별자문위원
2012년: 중앙선거관리위원회와 서울시장후보 홈페이지 사이버테러 특별검사 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security