情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

스마트 그리드 보안 표준화 동향

김 미 주*, 윤 미 연*, 정 현 철*, 염 흥 열**

요 약

스마트 그리드는 전력인프라와 정보통신기술이 접목되어 실시간으로 전력공급자와 소비자가 정보를 교환함으로써 전력 사용 및 관리를 최적화하는 기술로, 전 국민의 일상생활과 밀접한 관계를 가지기 때문에 보안 문제 발생 시 심각한 문제를 초래할 수 있다. 우리나라를 비롯하여 미국, 유럽, 일본 등 전 세계 주요 국가들의 스마트 그리드 구축사업이 한창인 지금, 보안에 대한 중요성을 인식하고 스마트 그리드 전 영역에 대한 보안 대책 마련이 필요하다. 이와 관련하여 NIST, IEC, ITU-T 등의 국내외 표준화 기구 및 단체에서 스마트 그리드 보안 표준화의 필요성을 인식하고 표준화 로드맵을 개발하는 등 다양한 표준화 활동을 추진하고 있다. 이에 본 고에서는 스마트 그리드 보안을 위한 국내외 표준화 기구 및 단체들의 표준화 활동 동향에 대한 정보를 제공하고자 한다.

Ⅰ. 서 론

지난 2010년 마이크로소프트 윈도우 취약점을 악용한 '스턱스넷(Stuxnet)' 웜을 이용해 이란 핵시설을 마비시키는 공격이 발생하였다. 이는 국가 및 산업의 주요 기반 시설을 제어하는 스카다(Supervisory Control and Data Acquisition, SCADA) 시스템의 취약점을 이용한 것으로 이 공격에서 사용된 웜은 사이버 미사일로 일컬어지며 컴퓨터 바이러스가 사이버전쟁의 무기로 이용되어 사회 전반에 막대한 피해를 일으킬 수 있다는 경각심을 일깨워 준 계기가 된 사건이기도 하다. 또한 우리나라를 비롯한 미국, 유럽, 일본 등 주요국가에서는 전력인프라와 정보통신기술이 융합되어 사용자에게 실시간 요금정보를 제공하고 에너지 효율을 최적화하는 스마트 그리드 구축사업을 활발히 진행 중에 있다.

미국은 1990년대부터 2000년대 초반까지 전력 인프라 노후화에 따른 대규모 정전사태가 발생한 것을 계기로 노후화된 전력 설비를 교체하고 에너지 안보를 실현한다는 차원에서 스마트 그리드를 추진하고 있다. 미국 의회에서는 2008년부터 2020년까지 스마트 그리드 연구개발과 시범사업을 국책사업으로 한다는 내용을 담은 연방법안을 2007년 통과시켜 제도적 기반을 마련하고, 스마트 그리드 시장에 GE, ABB, 지멘스, 구글, 시스코, 마이크로소프트 등의 업체들이 참여하여 미래 시장 선점을 위해 막대한 투자를 추진하고 있다.

유럽은 탄소배출 절감 및 에너지 효율성 제고를 위해 EU 집행부 내에 스마트 그리드 추진 조직을 만들어 범국가적인 차원에서 스마트 그리드 사업을 추진하고 있다. 이와 관련하여 2030년까지 스마트 그리드 분야에 1조 유로 투자해 2022년까지 회원국의 모든 건물에 스마트 계량기 설치를 계획하고 있으며, 범유럽 연구개발 프로그램(Framework Program 7, FP7)을 통해 IT기반 에너지 효율화 과제를 추진하는 등 스마트 그리드에 대한 막대한 투자를 하고 있다.

일본은 신재생 에너지 개발 및 에너지 안보 측면과 핵심기술 선점을 통한 경제력 제고를 위해 스마트 그리드를 추진하고 있다. 이를 위해 국가차원의 신전력 네트워크 시험 및 시범 단지를 구축하고 분산전원 통합 실증 시험을 추진하고 있고, 도쿄전력, 간사이전력, 미쓰비시전기 등의 전력업체를 중심으로 스마트 그리드 관련 연구를 진행하고 있다[1].

우리나라는 저탄소 녹색성장 및 기후변화 대응과 에너지 효율 향상 및 신성장동력 창출을 위해 스마트 그리드를 추진하고 있다. 이와 관련하여 2010년 스마트

본 연구는 방송통신위원회의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음.
* 한국인터넷진흥원 인터넷침해대응센터 침해예방단 연구개발팀 ({mijoo.kim, myyoon, hcjung}@kisa.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

그리드 국가로드맵을 확정하여 2030년까지 국가단위의 스마트 그리드 구축완료를 목표로 국가 차원의 종합적 계획을 제시하고, 제주도에 스마트그리드 실증단지를 구축하여 운영하고 있다. 또한 스마트 그리드 구축에 관한 법 및 제도적 기반 마련을 위해 스마트그리드법(지능형전력망의 구축 및 이용촉진에 관한 법률)을 제정하는 등 안정적인 스마트 그리드 구축을 위한 연구개발, 표준화, 사업화 등 다양한 활동을 추진하고 있다.

하지만 스마트 그리드는 전력망뿐만 아니라 정보통신망을 기반으로 사용자 및 사용자의 전력사용 정보를 교환함으로써 서비스를 제공하기 때문에 기존의 IT 환경에서의 보안위협과 함께 스마트 그리드 특징에 기반한 새로운 보안 위협이 추가로 발생 할 수 있으며, 스마트 그리드가 전 국민의 일상생활과 밀접한 관계를 가지기 때문에 보안 문제 발생 시 그 피해 또한 막대할 것으로 예상된다. 따라서 스마트 그리드 인프라 설계 및 구축 시부터 보안에 대한 신중한 고려를 통해 스마트 그리드 전 영역에 대한 보안 대책이 마련되어야 한다. 이와 관련하여 NIST, IEC, ITU-T 등의 국내외 표준화 기구 및 단체에서 스마트 그리드 보안 표준화의 필요성을 인식하고 표준화 추진을 위한 다양한 활동을 진행하고 있다. 이에 본 고에서는 스마트 그리드 보안과 관련하여 국내외 표준화 기구 및 단체들의 표준화 활동 동향을 살펴보고자 한다.

Ⅱ. 스마트 그리드 보안

스마트 그리드 환경에서는 국가 및 산업 기반 시설인 전력인프라와 정보통신망에서의 기존 보안 위협들이 동일하게 발생 할 수 있고, 스마트 그리드 특징에 기반한 신규 및 복합적인 보안 위협들이 추가로 발생 할 수 있다.

스마트그리드를 망 특성 및 기능에 따라 발전소, 송/배전 변전소 등을 통해 수요 기반 전력생산/공급하는 역할을 하는 전력망, 인터넷망을 통해 전력 사용정보 · 과금 등 양방향 통신을 지원하는 역할을 하는 AMI (Advanced Metering Infrastructure), 가정 · 빌딩 · 공장 등에서 전기 및 서비스를 이용하는 소비자 영역으로 나누어 각 영역에 대한 보안 위협은 다음과 같다[2].

- 전력망 : 전력망의 경우 주요 시스템이 보호된 구역 내에서 폐쇄적으로 운영되어 안전하다고 인식되고 있었지만, 2010년 발생한 스턱스넷을 이용한 해킹 사고 등 주요 전력시스템에 대한 다수의 침해사고 발생사례가 존재한다.
- AMI : 기존 IT망에서의 보안위협과 짧은 주기로 전송되는 방대한 데이터 및 스마트 그리드 트래픽 특징에 기반하여 포털, 데이터 관리 서버, 과금 서버 등 주요 시스템을 대상으로 하는 DDoS 공격, 펌웨어 업그레이드 등을 통한 악성코드 감염에 따른 오작동 유도 및 2차 공격, 전력사용정보 위변조에 따른 과금우회 및 전가 등의 보안 위협이 발생할 수 있다.
- 소비자 영역 : 소비자 영역에서는 스마트기기 간에 무선랜, ZigBee, 이더넷 등의 프로토콜을 이용한 유무선 통신을 기반으로 다양한 서비스가 존재하며, 통신 및 서비스 상의 취약점을 이용해 한정된 자원을 가지는 스마트 기기에 대한 서비스거부공격, 소비자 개인정보 노출, 과금정보 노출 및 위변조, 원격제어 정보 노출 및 위변조 등의 보안 위협이 발생할 수 있다.

따라서 이 같은 스마트 그리드 환경에서의 보안 위협을 대응하기 위해서는 전력 및 정보통신 인프라를 기반으로 하는 스마트 그리드 전 영역에 걸친 보안 분석/점검 및 대책 마련이 필요하다.

Ⅲ. 국제 표준화 동향

국내외 표준화 기구 및 단체에서는 스마트 그리드 보안에 대한 표준화 필요성을 인식하고 안정적인 스마트 그리드 구축을 위한 로드맵을 개발하고 보안기술에 대한 표준화를 추진하는 등 다양한 활동을 진행하고 있다. 이에 본 절에서는 스마트 그리드 보안을 위해 국제표준화기구 및 국외 표준화 단체에서 진행 중인 표준화 활동 동향에 대해 기술하고자 한다.

3.1 NIST(National Institute of Standards and Technology)

미국국립표준기술연구소인 NIST[3]는 스마트그리드에 대한 표준화를 주도하며 스마트 그리드 연구개발 및 표준화를 비롯하여 산업계에 많은 영향을 주고 있다.

NIST에서는 2010년 스마트 그리드 상호운용성을 위한 프레임워크 및 로드맵 1.0을 발표하여 시장, 운영,

서비스 제공자, 발전, 송전, 배전, 소비자 각 도메인에 따른 스마트 그리드 참조 모델을 정의하고 ISO, IEEE, NERC, ISA, OASIS 등 타 표준화기구의 스마트 그리드 표준을 검토함으로써 스마트 그리드 표준화가 필요한 8개의 우선 추진 영역을 [표 1]과 같이 선정하였다.

2012년 2월에는 스마트 그리드 상호운용성을 위한 프레임워크 및 로드맵 2.0[4]을 발표하여 1.0에서 정의한 개념적인 참조 모델에 대한 내용을 [그림 1]과 같이 업데이트하고, 사이버보안과 테스팅 및 인증 분야의 결과물들을 반영하였다.

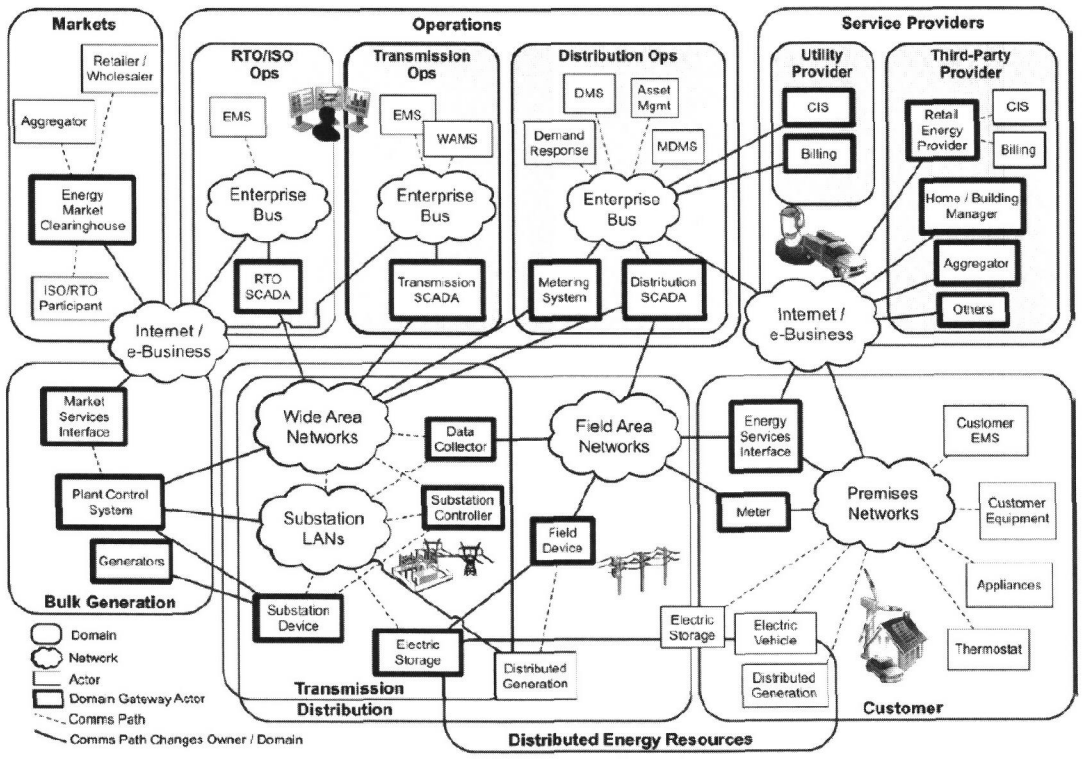
또한 NIST에서는 스마트 그리드 표준들의 조화 및 신속한 표준화 추진을 위해 스마트 그리드 참여자 간의 의견 조정 역할을 수행하는 스마트 그리드 상호운용성 패널(Smart Grid Interoperability Panel, SGIP)을 설립하였고, SGIP에 스마트 그리드 보안을 담당하는 사이버보안 워킹그룹(Cybersecurity Working Group)을 만들어 2010년 스마트 그리드 표준 개발 시 보안성 평가의 기준을 제공하는 스마트 그리드 사이버보안 가이드라인(NISTIR 7628)[5]을 발표하였다. 스마트 그리드 사이버보안 가이드라인은 스마트 그리드 응용분야 및 서비스에 대한 유즈케이스 분석에서 논리적 인터페이스 및 취약점 분석을 통한 보안 위협 평가, 논리적 인터페이스에 따른 상위 수준의 보안 요구사항 도출, 스마트 그리드 보안 구조 개발 및 관련 표준 분석, 보안 요구사항 및 구조에 대한 준수 여부를 검증하기 위한 평가기술 개발까지의 사이버보안 전략과 함께 스마트 그리드 논리적 구조 및 인터페이스, 상위 수준의 보안 요구사항, 암호 및 키 관리 이슈를 기술한다.

〔표 1〕 스마트 그리드 표준화 우선 추진 분야

주요 추진 분야
Energy Storage
Demand Response & Consumer Energy Efficiency
Wide-Area Situational Awareness
Electric Transportation
Advanced Metering Infrastructure
Distribution Grid Management
Cyber Security
Network Communications

스마트 그리드 사이버보안 가이드라인에서 정의하는 19개의 상위 수준의 보안 요구사항은 다음과 같다.

- 접근 제어



〔그림 1〕 NIST 스마트 그리드 참조 모델

- 인식 및 훈련
- 감사 및 책임
- 보안성 평가 및 허가
- 설정 관리
- 운영의 지속성 보장
- 식별 및 인증
- 정보 및 문서 관리
- 침해 대응
- 스마트 그리드 정보 시스템 개발 및 유지
- 미디어 보호
- 물리적 보호
- 계획
- 보안 프로그램 관리
- 인적 보안
- 위험 관리 및 평가
- 스마트 그리드 정보 시스템 및 서비스 인수
- 스마트 그리드 정보 시스템 및 통신 보호
- 스마트 그리드 정보 시스템 및 정보 무결성 보장

3.2 IEC(International Electrotechnical Commission)

IEC는 전기 및 전자분야 국제 표준화 기구로 SG3 (Strategic Group 3)[6]에서 스마트 그리드에 대한 표준화를 추진하고 있다. IEC SG3에서는 2010년 6월 IEC 스마트 그리드 표준화 로드맵[7]을 개발하여 통신, 보안, 스마트 그리드 계획 등 3개의 공통영역과 전송 시스템, 정전방지/EMS(Energy Management System), 배전 관리, 배전 자동화, 변전소 자동화, 분산 에너지 자원, 미터링, 수요반응/로드관리, 홈 및 빌딩 자동화, 전력저장, 전기자동차, 상태 모니터링, 재생 에너지 발전 등 13개의 응용영역에 대한 설명, 요구사항 분석, 기존 표준들에 대한 식별, 격차 분석, 표준 개발을 위한 권고사항을 정의하고 있다.

로드맵에서 정의한 스마트 그리드 관련 기존 보안 표준들은 다음과 같다.

- IEC 62351-1~6[9] : 전력시스템 관리 및 관련 정보 교환 데이터 및 통신 보안 상의 이슈, 용어, 통신 네트워크 및 시스템 보안, 프로파일, 변전소 시스템 보안 등 정의(로드맵 개발 이후 네트워크 및 시스템 관리 데이터 객체 모델을 정의한 IEC 62351-7 표준이 제정되었으며, 역할 기반 접근 제어 기술을 정의하는 IEC 62351-8에 대한 표준화가 진행 중에 있음)
- NERC CIP-002, CIP-003~CIP009[10] : 대량 전기 시스템에서의 사이버보안을 위한 주요 자산에 대한 식별, 보안 관리 통제, 훈련, 전자적 보안 영역, 물리 보안, 시스템 보안 관리, 침해 처리 및 복구 계획 등 정의
- IEEE 1686-2007[11] : 지능형 전자장치에 대한 사이버보안 요구사항 정의
- ISO/IEC 27001[12] : 정보보호 관리체계
- ANSI/ISA-99[13] : 산업 자동화 및 제어 시스템 보안
- NIST Special Publication 800-82[14] : 산업 제어 시스템 보안 가이드

3.3 IEEE(Institute of Electrical and Electronics Engineers)

IEEE에서는 스마트 그리드에서의 상호운용성에 대한 지침인 IEEE Std 2030[8]을 발표하였으며, 스마트 그리드 보안과 관련된 다음의 표준들을 개발하였다.

- IEEE 1402-2000[15] : 변전소에 대한 물리적 전자적 보안 가이드 정의
- IEEE 1686-2007 : 변전소의 지능형 전자 장치(Intelligent Electronic Devices, IEDs)에 대한 사이버보안 요구사항을 정의
- IEEE 1711-2010[16] : 변전소 직렬 링크의 사이버 보안을 위한 암호 프로토콜 정의

또한, C37.240WG(Working Group)에서는 변전소 자동화 · 보호 · 제어 시스템을 위한 사이버보안 요구사항을 정의하는 표준을 개발하는 PC37.240[17] 프로젝트를 진행 중에 있다.

3.4 ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)

ITU-T[18]에서는 스마트 그리드에 대한 표준화 중요성을 인식하고 통신/ICT 관점에서 스마트 그리드 권고안 개발에 도움이 될 수 있는 정보와 개념들을 수집하고 문서화하는 목적으로 2010년 2월 스마트 그리드 포커스 그룹(Focus Group on Smart Grid, FG Smart)[19]을 설립하였다. FG Smart는 2011년 12월까지 총 9차례

에 걸친 회의를 통하여 스마트 그리드 개요, 유즈케이스, 구조, 통신 요구사항, 용어에 대한 5개의 결과문서를 도출하였고, 활동 종료 후 각 SG(Study Group)로 보내 추가 연구를 진행하기로 하였다.

또한 2012년 1월 개최된 스마트 그리드과 클라우드 컴퓨팅 워크숍 및 TSAG(Telecommunication Standardization Advisory Group)회의를 통해 기존 JCA on HN (Joint Coordination Activity on Home Networking)그룹을 JCA on SG&HN(Joint Coordination Activity on Smart Grid and Home Networking)[20]으로 변경하고 ITU-T 안팎의 스마트 그리드 활동에 대한 조정 역할을 수행하기로 하였다.

ITU-T 내에서 정보통신 보안 선도그룹인 SG17[21]에서는 스마트 그리드 홈 영역에서 활용될 수 있는 홈 네트워크 보안 표준을 다음과 같이 개발한 바 있다.

- X.1111[22] : 홈 네트워크 보안 기술 프레임워크
- X.1112[23] : 홈 네트워크 디바이스 인증서 프로파일
- X.1113[24] : 홈 네트워크 서비스를 위한 사용자 인증 메커니즘 가이드라인
- X.1114[25] : 홈 네트워크 인가 프레임워크

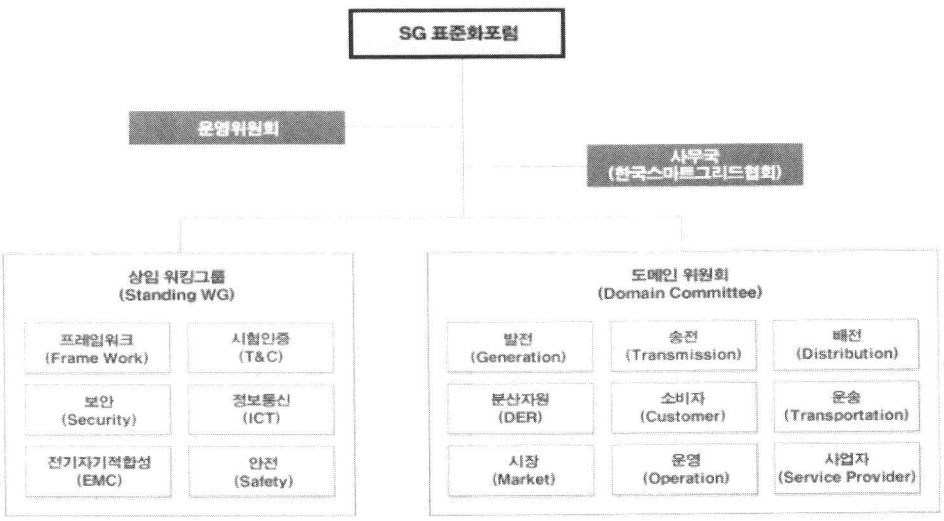
또한 ITU-T SG17 내 Q.6(유비쿼터스 보안)에서는 지난 2012년 3월 개최된 정기회의에서 ITU-T 내에서 스마트 그리드 보안에 대한 첫 표준화 아이템으로 정보통신망을 기반으로 하는 스마트 그리드 서비스에서의 보안 기능 구조(X.sgsec-1, Security functional architecture for smart grid services using telecommunication network)가 신규 표준화 아이템으로 제안되어 채택된 바 있다. 본 표준화 아이템에서는 FG Smart에서 정의한 스마트 그리드 기능 모델을 기반으로 정보통신망을 사용하는 스마트 그리드 서비스 구간에서의 보안 위협, 보안 요구사항, 보안 기능 구조에 대한 표준화를 진행하게 될 예정이다.

3.5 기타

그 밖에도 Zigbee Alliance[26]에서는 홈 영역에서 스마트 에너지 기기 연결 및 상호운용성을 위한 프로토콜인 스마트 에너지 프로파일 2.0(Smart Energy Profile 2.0)을 개발 중에 있으며, 유럽연합의 표준화기구인 CEN, CENELEC, ETSI는 스마트 그리드 표준개발을 위한 공동작업반(Joint Working Group)[27]을 결성해 유럽의 스마트 그리드 표준화 현황을 조사하는 활동을 진행하였다. 특히 ETSI[28]에서는 스마트미터에 M2M기술을 활용하는 방안 등 기존 M2M기술에 대한 스마트 그리드 활용성에 대한 논의를 진행하고 있다.

Ⅳ. 국내 표준화 동향

국내에서는 지식경제부에서 발표한 '스마트 그리드 국가 로드맵'[29]에 따라 스마트 그리드 핵심기술 개발



〔그림 2〕 스마트 그리드 표준화 포럼 구성

지원 및 조기 국제 표준화 지원을 위한 표준화 가이드라인을 설정한 바 있으며, 스마트 그리드 단계별 보안 표준 개발 계획을 [표 2]와 같이 수립하였다.

〔표 2〕 스마트 그리드 단계별 보안 표준 개발 계획

단 계	분 야	세 부 기 술
1단계 (2010~2011)	AMI, 기기 보안 등 표준개발이 시급한 분야(장치·시스템 보안 기술)	○ 스마트 미터 및 가전기기 보안모듈 표준 ○ AMI 암호/인증 및 접근제어 기술 표준
2단계 (2012~2013)	실증단지 수요 표준 개발(전력망 보안 표준화)	○ 배전망 감시센서 보호 기술 및 통신보호 기술 표준 ○ 전력망 제어 프로토콜 보안 및 보안관제 기술 표준
3단계 (2014~)	광역망 운영 표준 개발(서비스 보안기술 표준화)	○ 개인정보보호기술 및 네트워크 접근제어 기술 표준 ○ 전력거래서비스 보안 기술 및 보안관제 기술 표준

또한 우리나라에서 중점 추진 중인 5대 주요 영역(지능형전력망, 지능형소비자, 지능형운송, 지능형재생, 지능형서비스)에 대한 효과적인 표준화 추진을 위하여 '스마트 그리드 표준화 포럼'[30]을 출범하였다.

스마트 그리드 표준화 포럼은 프레임워크, 시험인증, 보안, 정보통신, 전기자기적합성, 안정 측면에서의 표준 검토를 수행하는 6개 상임워킹그룹과 스마트 그리드 도메인에 따른 기술 표준을 개발하는 9개의 도메인 위원회로 구성되며, 제주스마트그리드실증단지 기술 등 국내 스마트그리드 기술에 대한 국내외 표준 개발 및 국외 표준 기술에 대해서 국내 환경에 적합한 형태로 수용하여 단체 및 국가 표준으로 개발하는 역할을 수행한다.

TTA 정보통신표준화위원회[31] TC2(전송통신 기술위원회) 산하 디지털홈 프로젝트 그룹(PG214)에서는 스마트 그리드 소비자 영역인 홈 네트워크 관련 표준개발을 진행하고 있으며, TC5(정보보호 기술위원회) 산하 응용보안 및 평가인증 프로젝트그룹(PG504)에서는 스마트 그리드 응용 보안 관련 표준 개발 임무에 따라 표준화를 추진하고 있다.

또한 TTA에서 발간한 ICT 표준화전략맵 2012[32]에서는 표준화 필요성, 시급성, 파급효과 등을 고려하여 스마트 그리드 보안 분야의 중점표준화항목으로 스마트 그리드 보안 프레임워크, 스마트 그리드에서의 개인정보보호, 스마트 미터 보안 프로토콜 등을 도출한 바 있으며, 제주 스마트그리드 실증단지와 같은 시범사업 경험을 토대로 스마트 그리드 및 정보보호 산·학·연 전문가들의 협력을 통해 스마트 그리드 보안 기술들에 대한 표준을 개발하고 적극적으로 국내외 표준화를 추진할 필요가 있다고 언급하고 있다.

V. 결 론

전 세계적으로 에너지 효율 및 환경 문제로 스마트그리드에 대한 관심이 증가하고 있으며, 세계 각국에서는 스마트 그리드 사업을 적극적으로 추진함으로써 전력망의 지능화에 연구 개발 및 사업화에 많은 투자를 하고 있다. 하지만 스마트 그리드의 특성상 전력망 및 서비스 등에서의 보안 문제 발생은 심각한 사회 문제를 초래할 수 있기 때문에, 스마트 그리드 인프라 구축 시 보안은 필수 고려 요소로 인식되고 있으며, 스마트 그리드 보안을 위한 정부, 산업계, 연구소, 학계 차원의 다양한 활동이 진행되고 있다.

또한, 국내외 표준화 기구 및 단체에서는 스마트 그리드의 안전한 구축을 위해 스마트 그리드 표준화 로드맵 개발 및 보안 기술에 대한 표준화 추진 등의 활동을 진행하고 있고, 우리나라는 제주 스마트그리드 실증단지 구축 및 연구개발을 통해 도출된 기술들에 대한 국내외 표준 개발을 추진하고자 하고 있다.

이에 본 논문에서는 스마트 그리드 보안을 위한 국내외 표준화 기구 및 단체의 표준화 추진 활동 동향에 대해서 살펴보았다. 본 논문에서 다뤄진 스마트 그리드 보안 표준화 활동이 좋은 결실을 이뤄 스마트 그리드의 안정적인 구축 및 활성화에 기여해 안전하고 편리한 스마트 그리드 서비스를 제공받고 더 나아가 국내의 보안 기술들이 국제 표준에 반영되어 세계적으로 활약할 수 있기를 기대해본다.

참고문헌

[1] KSGI, KOTRA, "주요국 Smart Grid 정책/시장 조사", 2010.

[2] 홍석원, 이명호, 이철환, "한국형 스마트 그리드에서의 보안 위협 및 보안 요구사항", 정보과학회지, 제30권 제1호, pp. 66-74, 2012. 1.

[3] NIST smart grid, http://www.nist.gov/smartgrid/

[4] NIST Special Publication 1108R2, "NIST Framework and Roadmap for Smart Grid Interoperability

Standards, Release 2.0", 2012. 2.

[5] NISTIR 7628, "Guidelines for Smart Grid Cyber Security", 2010. 8.

[6] IEC SG3, http://www.iec.ch/smartgrid/development/

[7] IEC, "IEC Smart Grid Standardization Roadmap", 2010. 6.

[8] IEEE 2030, "Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads", 2011. 9.

[9] IEC 62351, Power systems management and associated information exchange - Data and communications security, Part 1: Communication network and system security - Introduction to security issue,s Part 2: Glossary of terms, Part 3: Communication network and system security - Profiles including TCP/IP, Part 4: Profiles including MMS, Part 5: Security for IEC 60870-5 and derivatives, Part 6: Security for IEC 61850, Part 7: Network and system management (NSM) data object models, Part 8: Role-based access control.

[10] NERC CIP(Critical Infrastructure Protection) 002 Cyber Security - Critical Cyber Asset Identification, 003 Cyber Security - Security Management Controls, 004 Cyber Security - Personnel & Training, 005 Cyber Security - Electronic Security Perimeter(s), 006 Cyber Security - Physical Security of Critical Cyber Assets, 007 Cyber Security - Systems Security Management, 008 Cyber Security - Incident Reporting and Response Planning, 009 Cyber Security - Recovery Plans for Critical Cyber Assets.

[11] IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.

[12] ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements.

[13] ANSI/ISA-99, Security for Industrial Automation and Control Systems.

[14] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security.

[15] IEEE 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security.

[16] IEEE 1711-2010 - IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

[17] IEEE PC37.240, Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems.

[18] ITU-T, http://www.itu.int/en/.

[19] ITU-T FG Smart, http://www.itu.int/en/ITU-T/focusgroups/smart/.

[20] ITU-T JCA SG&HN, http://www.itu.int/en/ITU-T/jca/SGHN/.

[21] ITU-T SG17, http://www.itu.int/ITU-T/studygroups/com17/.

[22] ITU-T X.1111, Framework of security technologies for home network.

[23] ITU-T X.1112, Device certificate profile for the home network.

[24] ITU-T X.1113, Guideline on user authentication mechanisms for home network services.

[25] ITU-T X.1114, Authorization framework for home networks.

[26] ZigBee Alliance Smart Energy, http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx.

[27] CEN, CENELEC, ETSI, "Final Report of the CEN/CENELEC/ETSI Joint Working Group on standards for smart grids".

[28] ETSI Smart Grid, http://www.etsi.org/website/Technologies/SmartGrids.aspx.

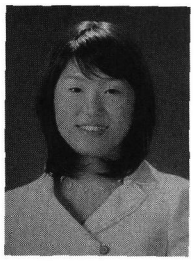
[29] 지식경제부, "스마트그리드 국가 로드맵".

[30] 스마트그리드표준화포럼, http://www.sgstandard.org/.

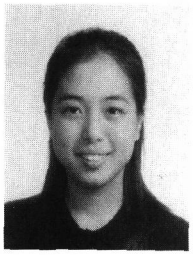
[31] TTA 정보통신표준화위원회, http://committee.tta.or.kr/.

[32] TTA, "ICT 표준화전략맵 Ver.2012 - 종합보고서 6 정보보호".

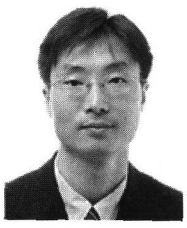
〈著者紹介〉



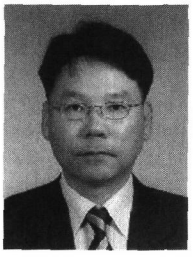
김 미 주 (Mijoo Kim)
정회원
2006년 2월: 순천향대학교 정보보호학과 졸업(학사)
2008년 2월: 순천향대학교 정보보호학과 졸업(석사)
2008년 9월~현재: 순천향대학교 정보보호학과 박사과정
2008년 4월~현재: 한국인터넷진흥원 연구개발팀 주임연구원
<관심분야> 스마트그리드 보안, 스마트폰 보안, 사이버보안



윤 미 연 (Mi Yeon Yoon)
정회원
2000년 2월: 가톨릭대학교 수학과/컴퓨터학과 졸업(학사)
2002년 2월: 숭실대학교 컴퓨터공학과 졸업(석사)
2005년 8월: 숭실대학교 컴퓨터공학과 졸업(박사)
2005년 6월~현재: 한국인터넷진흥원 연구개발팀 책임연구원
<관심분야> 스마트그리드 보안, 스마트폰 보안, 멀티캐스트 보안



정 현 철 (Hyun Chul Jung)
정회원
1996년 2월: 서울시립대학교 전산통계학과 졸업(학사)
1999년 8월: 광운대학교 전자계산학과 졸업(석사)
2006년 9월~현재: 고려대학교 정보보호대학원 박사과정
1996년 7월~현재: 한국인터넷진흥원 연구개발팀 팀장
<관심분야> 침해사고대응, 융합서비스보안, 네트워크보안, 컴퓨터포렌식



염 흥 열 (Heung Youl Youm)
종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장, 학회장(역)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜