情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

제주 스마트그리드 실증단지 보안대책 현황

최 재 덕*, 서 정 택*, 이 철 원*

요 약

지난해 12월 세계 최대·최첨단 스마트그리드 실증단지 조기 구축을 목표로 제주 스마트그리드 실증단지 사업이 시작되었다. 실증단지 사업은 전력재판매, 전기자동차 운행, 무정전 등의 신전력 서비스로 새로운 생활상을 보여주게 될 것으로 기대된다. 그러나 정보통신기술과 융합된 전력망의 사이버 보안위협이 크게 이슈화되면서, 실증단지 사이버 보안대책에 대한 관심이 증대하고 있다. 이에 본 고에서는 실증단지 컨소시엄 추진 현황 및 네트워크 구성을 간략히 살펴보고, 현재 진행되고 있는 보안대책들에 대해서 살펴본다. 실증단지 사업 보안대책은 보안센터 및 보안WG 구성을 통한 총체적인 보안대책 마련 및 지원, 실증단지 보안지침 및 보안가이드라인 제시, 각 운영센터별 보안대책 수립 및 이행 등 다각도로 추진되고 있다.

Ⅰ. 서 론

2030년까지 세계 최초 국가단위 스마트그리드 구축을 목표로 지난해 12월부터 시작된 스마트그리드 실증단지 사업이 지난 5월말로 1차년도 사업을 성공적으로 마무리 하였고, 현재 2차년도 사업이 진행중이다[1]. 실증단지 사업은 2013년 5월까지 신전력서비스 위주의 인프라 구축 및 통합 운영 과정을 거쳐 실증단지 5대 분야에서 새로운 생활상을 보여주게 된다. 예를 들어, 가전제품 전력 사용량에 대한 실시간 전기요금 정보를 통해 시간대별 전력사용량을 조정할 수 있고, 전기자동차가 운행될 수 있도록 가정에서도 충전 설비가 구축된다. 또한, 풍력·태양력 발전 등을 전력망에 안정적으로 연계하고 잉여 전력은 전력망을 통해 실증단지 내 다른 지역으로 전송하기도 한다.

스마트그리드 기술은 발전·송전·배전 및 소비자 단에서 전력 소모 관리를 효율적으로 운영할 수 있도록 해주고, 전력 재판매와 같은 신전력 부가 서비스들을 통해 윤택한 생활을 보장해준다. 그러나 스마트그리드는 전력망에 정보통신기술이 융합되므로 기존 정보통신망에서 발생하는 사이버 보안위협이 스마트그리드 환경에서도 그대로 나타날 수 있으며, 그 파장이 국가 기반 시설인 전력망 장애로 이어져 상상을 초월하는 피해가 발생할 수 있다[2-3]. 미국 사이버 영향분석 기관의 수장인 스콧 보그는 미국 전력망의 1/3이 3개월간 정전된다면 카트리나와 같은 대형 허리케인 40~50개에 달하는 피해를 입게 될 것이라고 밝힌바 있다[4].

이에 제주 스마트그리드 실증단지 사업에서도 보안대책 마련의 중요성을 공감하고 있다[5]. 더욱이 제주 실증단지는 통합운영센터와 제주 전력계통과 연계되기 때문에 사이버 보안위협이 실질적으로 제주 전지역의 장애로 이어질 수 있어 사이버 보안 문제 해결이 필수적이다. 현재 실증단지 사업을 주도하는 스마트그리드사업단에서 한국전자통신연구원 부설연구소를 통해 실증단지 보안대책을 총괄하는 보안센터 및 보안WG을 운영하고 있다. 또한 각 컨소시엄들도 개별적으로 사이버 보안대책을 마련하고 있다. 1차년도 사업을 진행하면서 보안센터와 보안WG에서는 실증단지 보안지침 및 보안가이드라인을 수립하였고, 현재 각 시스템 및 기기의 취약점 분석, 사이버 모의 훈련 기획 등을 통해 실증단지 사이버 보안성 강화 업무를 다각도로 추진하고 있다.

본 고에서는 제주 스마트그리드 실증단지 1차년도 추진현황 및 네트워크 구성에 대해서 간략히 살펴보고, 실증단지에서 예상되는 사이버 보안위협들에 대해서 알아본다. 또한, 다각도로 추진되고 있는 실증단지 보안대책들에 대해서 살펴본다.

* 한국전자통신연구원 부설연구소 (cjduck@ensec.re.kr, seojt@ensec.re.kr, cheolee@ensec.re.kr)

Ⅱ. 제주 스마트그리드 실증단지

2.1 5대 컨소시엄 주요 추진현황

제주 스마트그리드 실증단지는 스마트 플레이스, 스마트 트랜스포테이션, 스마트 리뉴어블, 스마트 파워그리드, 스마트 일렉트릭시티 서비스와 같이 5대 분야로 구성된다. 또한 실증단지 마스터 플랜은 실증단지 운영계획 수립 및 상시 관리를 위해 사업특성상 정책 지정돼 스마트그리드사업단에서 맡고 있다. [표 1]은 각 분야별 주요 실증내용과 주관기업을 보여준다. 지난 1차년도 사업성과를 바탕으로 각 컨소시엄들이 수행하고 있는 주요 사업내용을 살펴보면 다음과 같다[1].

스마트 플레이스 분야는 스마트 미터기 사용을 일상화하여 소비자(홈, 빌딩, 공장 등)와 전력 공급자 간 양방향 통신 기반의 수요반응과 전력통신 융합형 신서비스의 구축을 목적으로 하는 실증단지 분야이다. 이 분야는 SK텔레콤, KT, LG전자, 한국전력 4개의 컨소시엄들이 추진하고 있다. SK텔레콤 컨소시엄은 실증가구를 대상으로 태양광 설비를 구축하고, 양방향 원격검침 기기들을 개발하였다. KT 컨소시엄은 스마트박스, 디지털 전력량계, EMS(Energy Management System)들을 연결하는 전력·통신 컨버전스 기술을 개발하였다. LG 전자 컨소시엄은 밀착형 홍보를 통해 스마트그리드 가입자 및 스마트 미터기 고객을 유치하였고, 참여가구에 광통신망을 제공하였다. 한국전력 컨소시엄은 Open Standard 기반 양방향 통신 네트워크, 통합검침 서비스 및 부가서비스 등의 설계를 완료하였고, ZigBee 스마트 에너지 프로파일 인증을 취득하였다.

스마트 트랜스포테이션 분야는 차세대 교통수단인 전기자동차의 운행을 위한 충전 인프라 시범구축 및 전기자동차 운행정보 중앙관제 시스템 구축 등의 신서비스 구축을 목적으로 하는 실증단지 분야이다. 이 분야에는 한국전력, SK에너지, GS칼텍스 3개의 컨소시엄이 참여하고 있다. 한국전력 컨소시엄은 전기자동차와 충전기 간 인터페이스 표준화 및 현대자동차와의 연동 시험 수행 등을 통해 전기자동차 충전 인프라를 구축하였다. SK에너지 컨소시엄은 전기자동차, 배터리, 배터리 관리 시스템을 개발하였고, 충전 스탠드 운영을 통해 운영 시험을 진행하였다. GS칼텍스 컨소시엄은 정보통신 기술을 기반으로 하는 운행정보 실시간 수집장치와 같은 부가서비스 등을 개발하였다.

스마트 리뉴어블 분야는 신재생발전원의 안정적 계통연계, 전력시장 운영체계와의 연계 등 관련 신서비스의 구축을 목적으로 하는 실증단지 분야이며, 한국전력, 현대중공업, 포스코ICT 컨소시엄이 참여하고 있다. 1차

〔표 1〕 5대 컨소시엄 및 실증단지 마스터 플랜 주요내용 및 구성 현황

분야	주요 실증내용	컨소시엄
스마트 플레이스 (공모) (Smart Place)	(소비자 중심의 에너지 효율화 체계 구축) 소비자·공급자 간 양방향 통신 기반의 효율적 에너지 수요·공급 체계 구축	SK텔레콤, KT, LG전자, 한국전력
스마트 트랜스포테이션 (공모) (Smart Transportation)	(전기 운송 수단 확대 기반 구축) 전기자동차의 운행 핵심기술 확보 및 중앙관제 시스템 구축	한국전력, SK에너지, GS칼텍스
스마트 리뉴어블 (공모) (Smart Renewable)	(녹색에너지 활용 기반 구축) 신재생에너지원의 전력계통 연계 및 마이크로그리드 운영 플랫폼 구축	한국전력, 현대중공업, 포스코ICT
스마트 파워그리드 (정책지정) (Smart PowerGrid)	(지능형 송·배전망 구축) 전력망의 지능화 및 자동복구 체계 구축	한국전력
스마트 일렉트릭시티 서비스 (정책지정) (Smart Electricity Service)	(신전력서비스 활성화) 통합운영센터 구축 및 신전력서비스 설계	한국전력, 전력거래소
실증단지 마스터 플랜 (정책지정) (Master Plan)	(실증단지 운영계획 수립·상시 관리) 5대 추진분야 통합운영 및 상시관리, 실증단지 보안대책 마련, 실증단지 상호운용성 확보방안 마련	스마트그리드사업단

년도 사업기간 동안 한국전력 컨소시엄은 신재생에너지 출력안정화 기술 등의 모델 수립, 행원실증단지 구성 기본계획 수립, 13종의 실증기기 설계를 완료하였다. 현대중공업 컨소시엄은 실증단지 네트워크 구성 및 설비들의 설계와 함께 스마트그리드 전력시장 입찰전략과 EMS 구성 및 풍력발전예측 시스템 기본 방안을 수립하였다. 포스코ICT 컨소시엄은 풍력발전 출력 안정화와 마이크로그리드 망의 효율적인 운영을 위한 설계를 진행하였다.

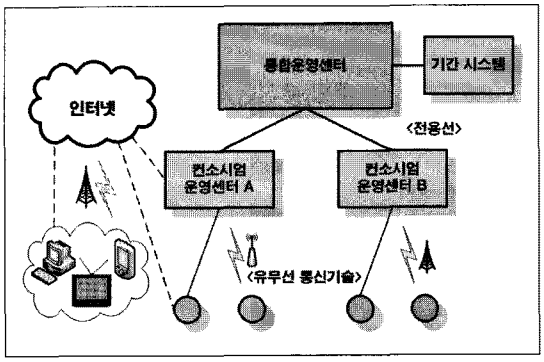
스마트 파워그리드는 한국전력 컨소시엄이 단독 참여하고 있는 분야로 전력망을 지능화하여 전력망 감시, 제어, 예방 등의 기술을 구현하는 실증단지 분야이다. 한국전력은 전력IT 통합실증기술 플랜트 및 실시간 요금제도 설계와 함께 이를 주택용 및 고압 고객에 시범 적용하였다.

스마트 일렉트릭시티 서비스는 스마트그리드 환경에 적합한 새로운 전력 서비스 등의 촉진을 위한 인프라 및 시스템 구축을 목적으로 하는 실증단지 분야이다. 컨소시엄 주관기업은 한국전력과 전력거래소로 구성되어 있다. 한국전력 컨소시엄은 각 컨소시엄 운영센터들의 운영상태 및 파워그리드 기반 계통운영 상태를 실시간으로 통합 모니터링 할 수 있는 종합상황판 구현계획을 수립하였다. 또한 통합운영센터 기반시스템 구축을 위해 컨소시엄 운영센터 간 데이터 연계분석 및 세부속성들을 정의하였다. 전력거래소 컨소시엄은 30분 단위 전일 사전입찰 및 5분 단위 당일 실시간 거래 가능한 전력시장설계, 시장규칙 개발을 완료하였고, 시장운영의 핵심기능에 해당하는 입찰·발전 계획과 가격결정 프로세스도 구현하였다.

현재 각 컨소시엄들은 1차년도에 수행된 설계, 모델 수립 등을 바탕으로 2차년도부터 연구에 박차를 가해 주요기능의 개발 및 실증을 진행하고 있다.

2.2 실증단지 네트워크 구성

실증단지 네트워크는 크게 통합운영센터, 각 컨소시엄 운영센터, 기간시스템 네트워크, 기기 네트워크, 인터넷과 같은 외부 네트워크 등으로 구성되며, 이들 간에 상호 연계구간이 존재한다. [그림 1]은 실증단지 네트워크 구성 개요도를 보여준다. 통합운영센터와 연계된 모든 네트워크는 전용선으로 연결되며, 각 컨소시엄 운영



〔그림 1〕 실증단지 네트워크 구성 개요도

센터와 기기 네트워크 간에는 FTTH, PLC, ZigBee, WiFi, WiBro, WCDMA, Binary-CDMA, D-TRS 등 다양한 유·무선 통신 기술이 사용된다. 또한 컨소시엄별로 개발될 다양한 스마트그리드 서비스를 적용하기 위해 외부 인터넷과 연계, 스마트폰, PC, IPTV 등 IT 기기와의 접목도 예상된다.

Ⅲ. 실증단지 사이버 보안위협

앞서 살펴본 것과 같이 제주 스마트그리드 실증단지는 통합운영센터, 컨소시엄 운영센터, 기간시스템, 실증단지 내에 설치된 기기, 인터넷 등과의 다양한 연계 때문에 기존 전력제어 시스템뿐만 아니라 실증단지 운영센터 내부 인프라 시스템 및 네트워크에서 발생할 수 있는 사이버 위협 가능성이 매우 높아지고 있다. 사이버 공격이 발생할 경우, 제주 실증단지 및 제주 전력에 전력사용 불가, 실시간 전력 거래 불가, 실증단지 주민 개인정보 침해 등의 피해를 초래할 수 있다. 본 절에서는 운영센터와 기기 측면에서 예상되는 보안위협들에 대해서 간략히 살펴본다.

3.1 운영센터 보안위협

실증단지 운영센터는 내·외부적으로 다양한 보안 위협들이 존재한다. 먼저, 운영센터 내부 보안위협으로는 최근 스턱스넷 (Worm.Win32.Stuxnet) 악성코드가 USB를 통해 산업제어시스템 네트워크 내부에 전파된 것처럼 운영센터 내에서 USB 저장매체 사용에 따른 악성코드 감염으로 주요 시스템 및 네트워크 장애를 유발할 수 있다. 내부 정보유출 측면에서는 스마트 미터기로

부터 수신되는 소비자 에너지 정보 등이 각종 마케팅을 위한 목적으로 제3자에게 유출되어 실증단지 소재지 주민들의 개인 프라이버시 침해 문제가 발생할 수 있다. 운영센터 외부 보안위협으로는 웹 서비스를 통한 전력 운영 정보 제공시 웹 서비스 취약점을 악용하여 운영센터 내부로의 침입이 예상된다. 또한, 운영센터 시스템들의 원격 패치 및 업데이트 서비스 경로를 통해 운영센터 외부에서 내부로의 침입도 가능하다.

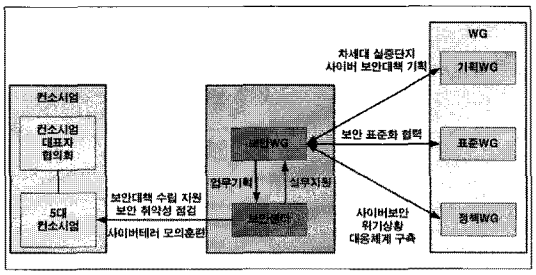
3.2 실증단지 기기 보안위협

실증단지 기기들은 지역적으로 다양하게 분포되어 있어 물리적인 접근 용이성 때문에 악의적인 공격자에 의해 손쉽게 공격 대상이 될 수 있다. 이렇게 불법 점령된 기기들을 대상으로 공격자는 기기 내부에 저장된 개인전력정보 등을 유출할 수 있고, 전력사용량에 대한 조작도 수행할 수 있다. 한편, 스마트그리드 기기에 기기 자원제약이나 비용문제 등의 이유로 보안강도가 약한 암호 알고리즘 모듈을 적용할 경우, 악의적인 공격자들은 해당 기기의 암호 모듈 취약점을 통해 기기를 불법 점령할 수 있고, 나아가 해킹된 기기를 거점으로 전체 실증단지 네트워크로 침투할 수도 있다.

ZigBee, Wi-Fi, WCDMA 등 무선 통신 기술이 사용되는 경우, 송·수신 데이터의 스니핑이 쉽게 이루어질 수 있기 때문에 전력관련 정보 등의 노출이 우려된다. 특히 무선 통신 환경에서는 AP와 같은 무선 접속 포인트의 보안설정 등이 기본설정 등으로 이루어지는 경우가 많아 이를 악용한 2차 사이버 공격도 가능하다. 또한, 댁내에서 정보통신 및 가전제품 사용시 실시간 에너지 사용량과 시간대별 전력 가격을 알 수 있는 스마트그리드 서비스들을 제공하기 위해 스마트폰·PC·IPTV 등 IT 기기들이 접목되기 때문에 이들 IT 기기들을 통한 운영센터로의 침입도 예상된다.

Ⅳ. 실증단지 사이버 보안대책

스마트그리드 실증단지 보안대책은 그 중요성이 충분히 인식되고 있으며, 스마트그리드사업단을 통한 보안센터 및 보안WG 구성, 보안지침 및 보안가이드라인 제시, 각 운영센터별 보안대책 수립 및 이행 등 다각도로 추진되고 있다.



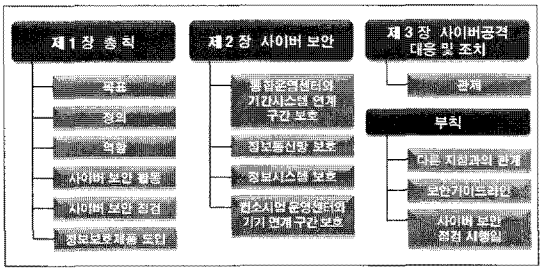
〔그림 2〕 실증단지 보안대책 구성 및 체계

4.1 실증단지 보안대책 구성 및 체계

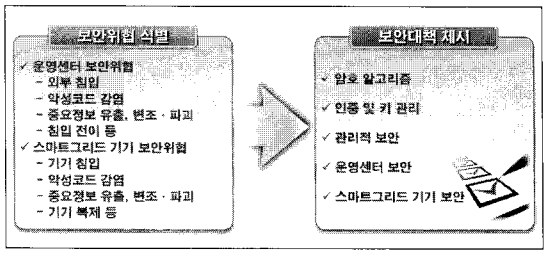
실증단지 보안대책은 보안업무를 기획하는 보안WG과 실무 추진을 위한 보안센터로 구성되며 추진체계는 [그림 2]와 같다. 먼저, 보안WG은 사이버 보안을 고려한 실증단지의 안전한 네트워크 구성방안, 사이버 테러 모의훈련, 시스템 및 네트워크 보안 취약점 분석 업무 등을 기획한다. 또한 기획WG과 연계한 차세대 실증단지 사이버 보안대책 기획, 표준WG과 연계한 보안 표준화 협력 방안 모색, 정책WG과 연계한 사이버 보안 위기상황 대응 체계 구축 등을 조정한다. 보안센터는 실증단지 보안지침 및 보안가이드라인 수립, 사이버보안 위기상황 대응체계 구축, 각 컨소시엄 보안대책 수립 지원, 사이버테러 모의훈련, 보안 취약점 분석 업무 등의 실무업무를 추진한다.

이러한 보안대책 계획을 기반으로 1차년도 사업 수행기간 동안 보안센터는 실증단지 보안지침 및 보안가이드라인을 수립하였고, 동 지침 및 가이드라인은 보안WG의 의견을 수렴하였다. 실증단지 보안지침 구성은 [그림 3]과 같다. 보안지침은 실증단지 구축 및 운영에 있어 최소한의 보안요구사항들을 규정한다.

실증단지 보안가이드라인은 [그림 4]와 같이 실증단지 사이버 보안위협을 식별하고, 이에 대한 보안 대책을



〔그림 3〕 실증단지 보안지침 구성



〔그림 4〕 실증단지 보안가이드라인 구성

제시한다. 보안위협은 운영센터 측면에서 발생 가능한 외부 침입, 악성코드 감염, 중요정보 유출·변조·파괴, 침입 전이 등을 식별하고 있으며, 스마트그리드 기기 측면에서는 기기침입, 악성코드 감염, 중요정보 유출·변조·파괴, 기기복제 등을 위협으로 고려하고 있다. 이에 대해 제시된 보안대책으로는 실증단지 내에서 사용할 수 있는 권장 암호 알고리즘 목록, 인증 및 키 관리에 대한 보안 요구사항, 운영센터에서 사이버 보안을 위해 관리적으로 수행해야 하는 보안대책, 운영센터의 안전한 구축과 네트워크 연계구간 보안대책, 스마트그리드 기기 보안대책이 있다.

현재 실증단지의 보안센터는 각 컨소시엄에서 개발하는 스마트그리드 서비스, 유·무선 네트워크, 기기 및 시스템들의 특성들을 고려하여 보다 구체적이고 실질적인 보안가이드라인 수립, 사이버보안 위기상황 대응체계 구축, 각 컨소시엄 보안대책 수립 지원, 사이버테러 모의훈련, 보안 취약점 점검 등을 추진하고 있다.

4.2 운영센터별 보안대책

실증단지 운영센터들의 정보보호 기본방향은 통합운영센터에서 통합운영센터와 연계 구간에 대한 사이버 보안대책을 수립하고, 각 컨소시엄 운영센터에서 자체 사이버 보안대책을 수립하는 것이다. 또한 국가 및 한국전력 정보보호 기본지침 및 실증단지 운영규정을 (보안지침 및 보안가이드라인) 준수하는 것이다. 통합운영센터와 각 컨소시엄 운영센터 간 연동분야 정보보호체계는 실증단지 네트워크 간 연동은 DMZ를 경유하도록 하고, 네트워크 간 통신라인은 전용선 및 암호화를 적용하는 것이다. 실증단지 통합보안관제체계를 위하여 통합운영센터와 각 컨소시엄 운영센터 간 보안관제 연동체계 구축 마련도 기본 보안대책이다.

통합운영센터에서는 스마트그리드가 보안에 취약할 수 있다는 지적에 따라 접근보안, 물리적 보안, 네트워크 보안, 시스템 보안, 운영관리 등 5대 보안대책을 마련하여 추진하고 있다[6]. 접근보안은 아이디, 패스워드 등 사용자 인증을 통해 수행하고, 물리적 보안은 출입자 모니터링, 주요시스템 및 설비보호 등 접근통제를 통해 수행하고, 네트워크 보안은 시스템과 시스템 간 상호인증과 암호화를 통해 수행할 방침이다. 시스템 보안은 인증정보를 통한 비인가자의 접근 차단을 통해 시스템을 보호하는 것이며, 운영관리는 운영절차 문서화, 백신설치, 백업서버 구축 등 보안절차를 수립하는 것이다.

컨소시엄 운영센터별 보안대책 및 기술은 각 컨소시엄이 운영하는 필드에 설치된 기기들 간 통신보안, 기기 침입을 통한 운영센터 내부 침투 방지 등에 주력하고 있다. 기본적인 보안대책은 기존에 유·무선 통신 네트워크 환경에서 사용되는 보안기술들을 적용하는 것이며, 실증단지 네트워크 환경에 적합한 보다 구체적인 보안기술 개발은 각 컨소시엄별 실증단지 인프라 구축 및 기술 개발이 진행되면서 함께 진행될 예정이다.

V. 결 론

본 고에서는 실증단지 사이버 보안대책 현황에 대해서 살펴보았다. 현재 제주 스마트그리드 실증단지 사이버 보안에 대한 인식을 크게 공감하고 있으며, 이를 위해 실증단지 사이버 보안 문제 해결을 다각도로 추진하고 있다. 기본 보안대책 및 기술들이 실증단지 인프라 구축 단계에서부터 고려되고 있고, 스마트그리드 서비스, 네트워크, 기기 개발 등이 진행되면서 구체적이고 스마트그리드에 적합한 보안대책 및 기술들이 개발될 예정이다. 향후 한국형 스마트그리드 모델이 이 사업에서 결정될 가능성이 높으므로, 구축 초기부터 사업기간 전반에 거쳐 사이버 보안에 대한 고려가 반드시 이루어져야 한다.

참 고 문 헌

[1] 스마트그리드 1차년도 제주 실증사업 '합격점', 신소재경제신문, 2009년 9월.

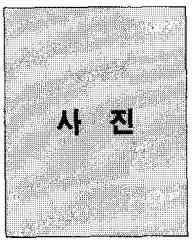
[2] 이건희, 서정택, 이철원, "스마트그리드와 사이버 보안", 한국통신학회지(정보와통신), 27(4), pp. 23-30, March 2010.

[3] 서정택, 이철원, "스마트그리드 사이버 보안 동향", 정보처리학회지, 17(2), pp. 37-45, March 2010.
[4] Staged Cyber Attack Reveals Vulnerability in Power Grid, CNN News, 2007.
[5] 필요한 스마트그리드...선결과제는 보안!, 보안뉴스, 2010년 9월.
[6] 세계 최초 국가 단위 스마트그리드 구축 및 첫 시험 무대, 전기신문, 2009년 9월.

〈著者紹介〉

최 재 덕 (Jaeduck Choi)
정회원

2002년 2월 : 숭실대학교 정보통신전자공학부 졸업
2004년 2월 : 숭실대학교 정보통신공학과 석사
2009년 2월 : 숭실대학교 전자공학공학박사
2004년 1월~12월 : (주)애드팍테크 놀러지 S/W 연구원
2009년 3월~2010년 1월 : 숭실대학교 전자공학과 박사후 연구원
2010년 2월~현재 : 한국전자통신연구원 부설연구소 연구원
관심분야 : 스마트그리드 보안, 제어시스템 보안, 유무선 네트워크 인증 및 키 교환



서 정 택 (Jung-Taek Seo)
정회원

1999년 2월 : 충주대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2007년 2월 : 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년~현재 : 한국전자통신연구원 부설연구소 선임연구원/과제책임자
관심분야 : 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응

이 철 원 (Cheol-Won Lee)
정회원

1987년 2월 : 충남대학교 수학과 졸업
1989년 2월 : 중앙대학교 전자계산학과 석사
2009년 8월 : 아주대학교 컴퓨터공학공학박사
1989년~1994년 : 한국전자통신연구원 선임연구원
1994년~2000년 : 한국정보보호진흥원 선임연구원/과제책임자
2003년~2004년 : Texas A&M University 방문연구원
2001년~현재 : 한국전자통신연구원 부설연구소 책임연구원/본부장
관심분야 : 사이버 안전, 정보보호시스템 평가, S/W 안전성 분석, 산업보안 등