스마트 에너지 개인정보 보호정책에 대한 연구

노 종 호*, 권 헌 영**

요 약

기존의 전력망 중심의 스마트그리드는 최근 들어 스마트에너지로 표현되는 열과 가스 등 신에너지 및 재생에너지 중심으로 빠르게 확산되고 있다. 스마트에너지는 전기에너지와 상호작용을 통해 AI를 활용한 에너지 분석을 기반으로 IoT센서 기반의 유무선 네트워크로 연결되어 다양한 에너지 사업자와 고객들과 생태계를 빠르게 확장시켜 나가고 있다. 그러나, IoT기반의 스마트에너지는 정부와 사업자의 이해관계에 따라 시장 활성화 노력에 비해 보안에 대한 기술적, 제도적 준비가 많이 부족한 것이 현실이다. 본 연구에서는 스마트에너지의 개인정보 보호정책에 대해 융합ICT의 가치체계(CPND) 관점에서 제시해보고자 한다.

A Study on Smart Energy's Privacy Policy

Jong-ho Noh*, Hun-yeong Kwon**

ABSTRACT

The existing smart grid, which is centered on the power grid, is rapidly spreading to new energy and renewable energy such as heat and gas, which are expressed as smart energy. Smart Energy interacts with electric energy and is connected to wired / wireless network based on IoT sensor based on energy analysis using AI to rapidly expand ecosystem with various energy carriers and customers. However, smart energy based on IoT is lacking in technological and institutional preparation for security compared to efforts to activate the market according to the interests of government and business operators. In this study, we will present Smart Energy 's privacy policy in terms of value system(CPND) of convergence ICT.

Key words : Security Convergence, IoT, Enterprise Security Strategy

접수일(2018년 3월 23일), 수정일(1차: 2018년 6월 25일), 게재확정일(2018년 6월 29일)

* 고려대학교 정보보호대학원 박사과정

** 고려대학교 정보보호대학원 정보보호학과(교신저자)

1. 서 론

그 동안 산업혁명의 역사는 에너지의 발전과 함께 하였다. 앞으로 4차 산업혁명 시대에는 신·재생에너지와 IoT기술간 융합으로 지능형전력망(Smart Grid)의 분산화, 지능화가 진행될 것이다.

정부는 2012년 제1차 지능형전력망 기본계획 발표와 더불어, 지능형전력망의 구축 및 이용촉진에 관한 법률을 제정하고, 지능형전력망 정보의 보호조치에 관한 지침을 마련하여 시행하고 있다.

스마트 에너지는 지능형전력망의 서비스 일환으로 에너지 효율화 관리, 에너지 저장장치(ESS), 수요반응 자원거래(DR), 전기 자동차 충천 인프라 등 에서 ICT 융합과 결합으로 시장이 형성되어 가고 있다.

예를 들어, 한전에서는 정부의 지능형 전력망 기본계획과 연계해 2천250만 호(戶)에 지능형 전력계량시스템(AMI)를 구축하는 사업을 추진 중이나 보안모듈이 적용되어 있지 않아 시민단체 및 전문가 그룹에서는 해킹 및 개인정보 침해에 대한 우려를 나타내고 있다.

또한, 스마트 에너지 관리시스템(EMS)분야에 인공지능(AI)의 기술이 접목되기 시작하면서, 지능형 전력계량시스템(AMI)에서 생성되는 다양한 전력사용정보 기반의 빅데이터 정보를 수집, 활용하게 되면 새로운 보안취약점을 생성하게 될 거라는 고민도 존재한다.

이에 본 연구에서는 새롭게 부각되는 인공지능(AI) 기술 적용에 따른 프라이버시 보호 중심으로 스마트 에너지 보안정책 방향에 대해 플랜스만의 CPND (Contents - Platform - Network - Device)의 체계를 토대로 고찰하고자 한다[1].

CPND체계는 융합ICT기반 융합생태계를 설명하는 대표적인 모형으로 스마트 에너지가 지능형전력망의 ICT를 융합한 서비스로 본 연구에 최적이라고 생각하였다. 이를 위해, 지능형전력망 관련 선행연구를 분석하고, CPND체계 기반의 보안위협 및 대책방안을 제시하도록 하겠다.

2. 선행연구 및 시사점

2.1 스마트 에너지의 개념적 이해

기존의 선행연구에서는 스마트 에너지라는 보다는 지능형전력망이라는 인프라 관점에서 많은 연구들이 진행되어 왔다.

지능형전력망법에서는 지능형전력망을 “정보통신기술을 적용하여 전기의 공급자와 사용자가 실시간으로 정보를 교환하는 등의 방법을 통하여 전기를 공급함으로써 에너지 이용효율을 극대화하는 전력망”이라고 정의하고 있다.

지능형전력망에서는 전력 장비들에서부터 수용가의 가전기기, 원격 검침 장치에 이르기까지 광범위하게 데이터의 전송이 이루어지는데, 이러한 데이터 전송들이 기존의 폐쇄된 전력 통신망이 아닌 통합된 광대역 전력 통신망을 통해 이루어지게 된다[2].

지능형전력망은 열, 바이오 연료뿐만 아니라 열병합발전(CHP) 등 에너지 보존 및 효율성 개선과 같은 사업자로 전환되는 재생 가능 에너지의 활용과 조화되어야 하며 지능형전력망은 전체 스마트 에너지 시스템의 일부로 여겨져야 한다는 연구결과도 있다[3].

스마트 에너지는 국가전기기술위원회(IEC)가 기존의 지능형전력망과 에너지를 포괄하는 시스템 수준의 표준화 정보를 제공하는 스마트 에너지 시스템 위원회(SyC - Smart Energy)를 발족시키면서 생겨난 개념으로 기존의 제품, 기능 위주의 접근방식에서 통합적이며 Top-down 방식인 시스템적 접근방식으로 변경하여 표준화에 대한 가이드라인을 제공하고 있다[4].

2.2 스마트 에너지 개인정보 보호

스마트 에너지에 대한 개인정보 보호 관련 연구는 그 동안 지능형 전력계량시스템(AMI), 개인정보보호법 중심으로 진행이 되어왔다.

지능형 전력계량시스템은 고객의 에너지 이용패턴을 분석할 수 있어 프라이버시 침해에 대한 우려가 높아 객관적 신뢰성을 확보할 수 있는 ESCROW 기반의 익명화가 필요하다[5].

특히, IoT기반 지능형전력망 주요 보안 문제점 및 고려사항으로는 지능형 전력계량시스템의 신분위장, 도청, 요금제를 악용한 데이터 손상, 권한부여 및 접근제어 문제, 프라이버시 침해 및 악성코드, 가용성 및 DoS, 스턱스 넷과 같은 사이버 공격에 대비하여 <표 1>과 같이 보안 고려사항을 제시하였다[6].

지능형전력망 개인정보 보호를 위한 정책적 고려사항으로는 개인정보보호의 고지, 공개에 대한 소비자의 허가, 정보공개의 범위 소비가 교육 및 인식, 정보 수집의 최소화, 데이터 품질, 데이터 보안, 위험평가, 데이터 보관 및 폐기, 데이터 침해, 직원교육, 감사 등 NIST의 개인정보보호 실무지침 권고사항을 토대로 연구하였다[7].

또한, 최근 인공지능(AI)의 Data Privacy 관점에서는 모델학습에 사용된 데이터를 추출하는 Inversion Attack과 머신 러닝을 이용한 Data Sanitizing의 취약점을 설명하고, 대응기술이 나와 있지 않기 때문에 이에 대한 적극적인 연구가 필요하다고 하였다[8].

3.3 시사점

스마트 에너지는 융합ICT기반의 에너지 생태계를 포함하므로 지능형전력망 시스템뿐만 아니라, 신·재생에너지 시스템, 정보시스템의 보안위협을 갖고 있다.

특히, 개인정보보호 차원에서는 기존의 전력망 시스템에 적용되어 있는 물리적 망분리 기반의 보안대책과는 달리 소비자의 에너지 활용패턴과 직접적으로 연결되어 있어 새로운 보안대책 마련이 필요하다고 본다.

추가로, 에너지관리 플랫폼에서 도입되기 시작한 인공지능의 경우 개인정보보호 차원에서 향후 많은 보안정책을 연구해야 할 분야이다.

< 1> IoT 기반 스마트 그리드의 보안 고려사항

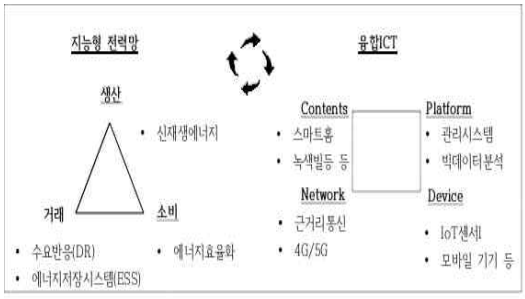
구분	주요내용
확장성	키 관리와 인증 같은 보안 솔루션에 대한 확장성
이동성	이동장치와 객체들에 대하여 인증과 안전한 통신
설치	대규모로 넓게 설치된 객체 및 장치들에 대한 손상 시도 탐지 가능
리거시 시스템	기 설치된 보안 능력이 거의 없거나 전혀 없는 기존 시스템들과 IoT 기반 스마트 그리드의 통합
제한된 자원	제한된 자원 문제로 공개키 암호화와 같은 보안 솔루션의 수용 제한 발생
이질성	스마트 그리드 상의 장치와 객체 자원 그리고 구현된 프로토콜과 통신 스택의 차이로 인하여 안전한 종단간 통신
상호운용성	TCP/IP 스택을 지원하지 않는 전통적 시스템과 장치 및 객체들이 게이트웨이 없이는 IP기반 시스템과 통신이 불가능
부트스트래핑	스마트 그리드 상의 수많은 장치 및 객체들을 암호 키, 암호 함수/알고리즘과 파라미터와 같은 초기 키 정보를 활용한 효율적인 부팅방안
신뢰	대규모 네트워크에서 다른 개체들에 의하여 소유되거나 관리되는 객체/장치들 사이의 신뢰관계
지연/시간 제한	SCADA 시스템은 전류,전압, 주파수 값의 변화와 같은 이벤트와 메시지에 대한 실시간 대응

3. 스마트 에너지의 보안정책

스마트 에너지는 전력의 생산, 거래, 소비의 3가지 서비스 형태를 갖추고 있다.

전력의 생산에는 태양광, 풍력 등 신재생에너지 발전 서비스, 이를 저장하고 방전하는 에너지저장시스템(ESS), 그리고 수요반응거래(DR)사업자를 통한 전력거래 서비스가 있고, 빌딩,아파트 단지의 에너지 소비에 대한 효율화 관리 서비스와 전기차 충전 인프라 서비스가 소비시장을 형성하고 있다.

이러한 스마트 에너지는 지능형전력망 인프라와 연계하여 융합ICT기반으로 <그림 1>과 같은 생태계로 구성되어 있다.



(그림 1) 스마트 에너지 생태계

본 연구에서는 CPND 모델을 기반으로 각 구성요소별 보안위협 및 대책을 살펴보고자 한다.

3.1 서비스(컨텐츠)의 위협 및 대책

스마트 그리드 협회에서는 지능형전력망의 서비스 영역을 에너지 저장(ESS), 재생에너지, 전기차 충전인프라, 녹색빌딩, 스마트 홈 등 5가지로 구분하고 있다. 이중에서 개인정보보호와 상관성이 높은 분야는 <표 2>와 같이 전기차 충전 인프라와 스마트 홈의 영역으로 볼 수 있다.

이를 위한 보안 대책으로는 지능형전력망 정보의보호조치에 대한 지침에 따라, 기술적인 측면에서는 사용자 인증체계 강화, 암호화 통신, 정보의 위변조방지 등에 대한 보안조치와 더불어, 물리적으로 전기차 충전인프라에는 지능형CCTV 연계 및 출입통제를 고려해 볼 수 있다. 또한, 스마트 홈서비스에는 IoT단말, 모바일 앱이나 웹을 통해 불필

요한 개인정보가 수집되거나 해킹을 통해 유출되지 않도록 단위 서비스 설계단계에서부터 구현되어야 한다. 관리적 측면에서는 개인정보 관리를 위한 서비스별 관리계획의 수립하여 시행을 하여야 한다.

스마트 에너지 기반의 다양한 서비스 시장 활성화를 위해서는 서비스 가입단계에서 개인정보 수집목표에 빅데이터 분석을 통해 에너지 관련 서비스 개발 및 부가서비스 제공 등 수집목적을 명확히 하고 계약전력(kW), 요금적용전력(kW), 유효전력(KW), 무효전력(kW) 등 수집항목을 구체적으로 적시해야 한다.

이의 보유 및 이용기간 뿐만 아니라 폐기 등에 관한 절차나 언제든 고객이 요구하면 확인 할 수 있도록 투명하게 진행하여야 한다.

<표 2> 서비스 유형별 보안위협

구분	주요 보안위협	개인정보 상관관계
에너지저장 (ESS)	• 물리적 접근 • 주요정보 위변조 등	낮음
재생에너지	• 연계통신 취약 • 주요정보 변조파괴 등	낮음
전기차 충전인프라	• 물리적 접근 • 웹/앱 서비스 취약점	높음
녹색빌딩	• 물리적 접근 • 주요정보 위변조 등	낮음
스마트 홈	• 웹/앱 서비스 취약점 • 악성코드 등	높음

3.2 플랫폼의 위협 및 대책

현재 시장에서의 에너지 관리 플랫폼은 일별 에너지 사용량 추이분석, 일별 용도별 부하비교, 시간대별 수요패턴 등을 통해 고객의 전력이용 정보에 대한 분석을 하고 고객 맞춤형 에너지 소비 및 예측정보를 <그림 2>와 같이 제공하고 있다.

최근에는 AI알고리즘을 활용하여 전기요금과 전력량 수요예측에 활용하기 시작하였다. 각 IoT디바이스를 통해 들어오는 실시간 빅데이터 전력요금 정보 및 연동되는 xEMS에서 전력분석정보를 활용하고 있다.

그러나, 입력 데이터에서 개인정보가 제대로 보호되지 않은 상태로 입력값으로 들어오고 플랫폼에

(그림 2) KT EMS 관리화면 예시

서 검증되지 않은 지능형 알고리즘을 통해 좀 더 심각한 개인정보를 생성하게 될 수 있는 위협이 존재하게 된다.

비식별화되어 받은 개인정보일지라도 빅데이터 분석과정이나 AI알고리즘을 통해 나온 2차정보가 민감한 정보로써 재식별화 될 가능성이 있다.

이를 해결하기 위해서는 AI알고리즘 적용시 전처리 과정에서 고객정보에 대한 사전검증 및 후처리 과정에서 재검증 절차를 의무화 한다면 가능하다고 생각한다.

일련의 과정에 대한 투명성을 확보하기 위해서는 시스템적인 검증과 더불어, 별도의 전문기관 설립 및 운영을 통해 체계화해야 한다.

추가적으로, 정부에서는 AI기반산업 육성을 위해 가칭 “지능정보사회기본법”,“서비스산업발전기본법”을 입법 준비 중에 있다. 스마트 에너지의 개인정보보호를 위해서는 AI관련 법제에 프라이버시 보호가 반영될 수 있도록 입법동향에 대한 보안전문가들의 지속적인 관심과 참여가 필요하다.

더불어, 향후 해외 스마트 에너지 사업 확장을 위해서는 EU의 개인정보보호규정(GDPR)의 자동적 의사결정으로부터의 보호책(22조)에서 명시한대로 정부고 정부주체에 대항 중대한 영향을 미치는 의사결정에 인간이 반드시 참여해야 한다는 규제에 대해서도 대응할 수 있도록 반영 하여야 한다.

3.3 네트워크의 위협 및 대책

스마트 에너지 네트워크는 전송속도, 통신방식 등에 따라 <표 3>과 같이 구분할 수 있다.

네트워크 연결은 다양한 xEMS와 이기종 장치간 시리얼 통신(RS485, RS232)과 TCP/IP 등 복잡하게 구성되어 운영하고 있다.

무엇보다도 에너지 단말과 플랫폼간 다양한 이기종 연동을 위해서는 시스템간 상호운용성(IEC 61850)의 보안표준을 제시하고 있는 IEC 65351를 따르는 스마트 에너지 네트워크 구성 및 운영이 뒷받침 되어야 한다.

그러나, NW보안 장비 등 도입으로 인해 실시간 데이터 처리가 중요한 에너지 서비스의 특성을 고려하여 각 장치들 간의 특성을 고려하여 설계되어야 할 것이다.

<표 3> 스마트 에너지 네트워크 보안위협

구분	주요 보안위협	개인정보 상관관계
근거리 통신(NFC, 블루투스, WIFI 등)	기밀성, 무결성 필요	낮음
저전력 장거리 통신 (TVWS, Weightless 등)		
트래픽 분산 (D2D통신 등)		
이동통신(4G, 5G)	모바일 기기 활용증가로 인한 개인정보, 단말정보 유출, DDos 공격 등	높음

3.4 디바이스의 위협 및 대책

스마트 에너지 서비스는 다양한 디바이스로 구성되어 있다.

최근 이슈가 되고 있는 디바이스는 지능형 전력계량시스템(AMI)과 전기차 충전카드, 모바일, 센서 등을 들 수 있다.

지능형전력계량시스템은 <그림 3>과 같이 고객이 댁내에서 언제 무슨 일을 했는지 전력량의 추이를 통해 확인 할 수 있다고 한다[5].

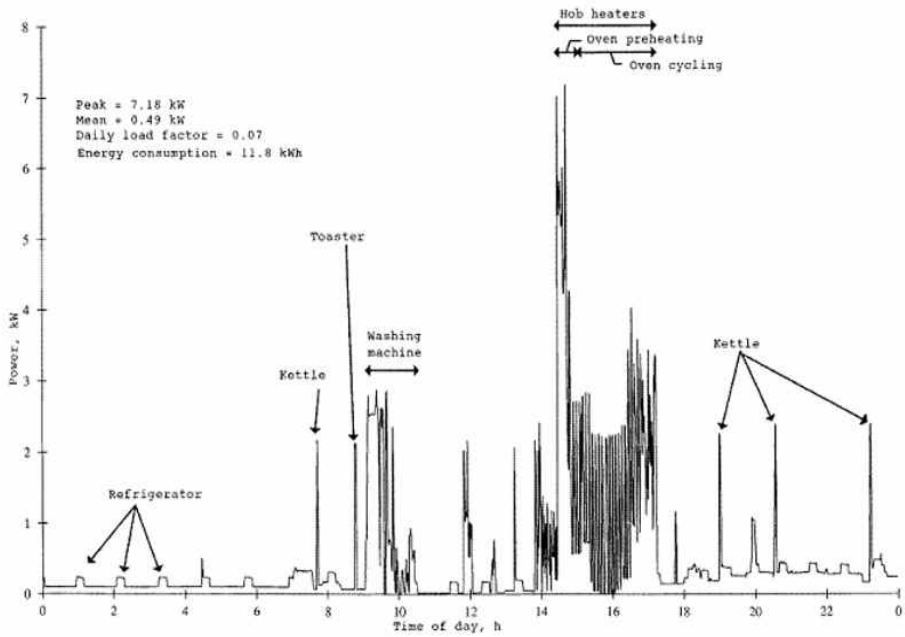
예를 들어, 고객이 전기를 사용하는 제품별 이용시간분석을 통해 고객의 생활패턴 분석이 가능하여 고객의 카드이용 정보유출과 비슷한 위험성을 지니고 있다.

지능형 전력계량시스템(AMI) 수집정보로부터 개인정보를 보호하기 위해서는 세부항목에 대한 이용정보는 비식별화 처리해서 보낼 수 있는 통신모듈을 정착하고 서비스사업자에게 사전 동의하는 고객에 한해 이 기능을 우회할 수 있게 하는 방법을 제시해 본다.

또한, 전기 자동차 시장에서 구축 운용중인 전기차 충전카드는 단순 교통카드 형태를 띄고 있어 사용자 인증 및 정보 위변조에 대한 취약성을 갖고 있어 현재의 신용카드 수준으로 보안성을 확보해야 하며 회원카드와 결재카드를 통합해서 관리하여야 한다.

모바일 단말은 다양한 바이러스 프로그램을 통해 계정정보를 탈취하여 개인정보를 유출할 수 있다.

스마트 에너지 서비스 이용자들의 바이오와 결



(그림 3) 가정집의 에너지 사용분석 그래프

합한 멀티팩트 인증과 더불어, 서비스 앱/웹 이용 시 보안 프로그램 설치운용 및 문제 발생시 원격에서 단말 초기화 하는 등 기능보완이 필요하다.

무엇보다도 무선통신기기들이 확산되고 이기종 센서들이 초연결화 되고 있는 스마트 에너지 시장에서는 디바이스 보안 인증제 도입을 통해 인증받은 기기 기반으로 안정적인 서비스를 제공해야 사회전반적인 리스크를 최소화 할 수 있을 것이다.

4. 결론 및 연구의 한계

지금까지 CPND관점에서 스마트 에너지에 대한 보안위협 및 대책에 대해 살펴보았다.

서비스(컨텐츠) 측면에서는 서비스별 Life Cycle에 대한 개인정보 보안대책을 수립하여야 한다.

플랫폼 측면에서는 에너지관리시스템(xEMS)에 대한 개인정보의 비식별화 처리 및 AI알고리즘 적용시 알고리즘의 투명성을 반영하고 개인정보보호규정(GDPR)에 명시한 자동적 의사결정으로부터 보호대책을 마련해야 한다.

네트워크 측면에서는 시스템간 상호운용성 확보 및 보안표준 이행을 통해 정보의 위변조가 발생하지 않도록 해야 한다.

디바이스 측면에서는 지능형전력계량시스템(AMI)은 개인정보 비식별화 모듈정착 의무화 및 센서 등에 대한 보안디바이스 인증제 도입을 제시하였다.

프라이버시 보호는 수집단계에서부터 철저한 개인정보 비식별화가 전제가 되어야 하며, Opt-out도입을 통한 실질적 행사를 할 수 있도록 하여야 한다. 특히, 스마트 에너지 플랫폼의 AI 알고리즘 적용에 대해서는 시스템 개발자와 정책 참여자간 협업 및 투명성 심의를 위한 전문기관 신설이 필요하다.

이번 연구에서는 아직 스마트 에너지 시장이 초기이며 관련 법제도적인 한계로 인해 실증적인 검증을 다루지 못한 한계점이 존재한다.

이를 위해 후속연구를 통해 스마트 에너지 진화방향을 고려하여 서비스별 보안정책에 대해 실증적인 연구를 진행하여 위협요소 및 적절한 대책을 제시 할 계획이다.

참고문헌

[1] Martin Fransman, The New ICT Ecosystem : Implications for Policy and Regulation, Cambridge University Press, 2010.

[2] 홍석원, 이명호, 이철환. “한국형 스마트 그리드에서의 보안 위협 및 보안 요구사항”. 정보과학회지, 30(1), pp. 66-74, 2012,

[3] Henrik Lund, Anders N. Andersen, Poul Alberg Østergaard, Brian Vad Mathiesen, David Connolly, “From electricity smart grids to smart energy systems e A market operation based approach and understanding”, Elsevier, Vol. 42, Issue 1, pp. 96-10, 2012.

[4] 김정욱, “스마트 시티와 스마트 에너지”, 한국건축환경설비학회, 9(2), pp. 6-13, 2015.

[5] Costas Efthymiou and Georgios Kalogridis, “Smart Grid Privacy via Anonymization of Smart Metering Data”, IEEE, 2000.

[6] Chakib BEKARA, “Security Issues and Challenges for the IoT-based Smart Grid”, Procedia Computer Science 34, pp.532-537, 2014.

[7] 이동혁, 박남제 (2016). “스마트그리드 개인정보보호를 위한 정책적 고려사항”. 정보보호학회지, Vol 26, No.1, pp. 99-104, 2016.

[8] 박소희, 최대선, “인공지능 보안 이슈”. 정보보호학회지, 27(3), pp. 27-32, 2017.

[9] Patrick McDaniel and Stephen McLaughlin, “Security and Privacy Challenges in the Smart Grid”, IEEE Security &Privacy, Vol. 7, No. 3, 2009.

[10] E. L. Quinn, “Privacy and the New Energy Infrastructure”, Social Science Research Network (SSRN), February 2009.

[11] Kaile Zhou, Chao Fu, Shanlin Yang,“Big da

ta driven smart energy management: From big data to big insights", Elsevier, Vol. 56, pp. 215 - 225, 2016.

[12] 이경복, 박태영, 임종인, "정보보호정책 관점에서의 한국형 스마트 그리드 추진 방안에 관한 연구- 미국과의 비교연구를 중심으로-", 한국정보화진흥원, 정보화정책 Vol.16, No.4, pp. 73-96, 2009.

[13] 윤종완, 박태준. "CPS 및 IoT 기술을 통한 제조혁신 동향 및 전망". 한국통신학회지(정보와통신), 33(11), pp. 23-28, 2016.

[14] 양일권, 정남준, 최승환, 이상호. "AMI시스템 구현을 위한 보안 요구사항 분석 및 추진 방향제안". 대한전기학회 학술대회 논문집, pp. 1898-1899, 2010.

[15] 김지희, 서인용, "가상발전소(VPP) 사업자 관점에서의 분산자원 최적배분 기초 연구", 대한전기학회 학술대회논문집, PP. 463-464, 2017.

[16] 정구형, 박만근, 허돈, "스마트그리드 하에서 가상발전소의 전력시장참여를 위한 제도적 선결요건에 관한 제언", 전기학회논문지, 64권 3호, PP. 375-383, 2015.

[17] 박훤일, 윤덕찬, "스마트그리드 사업과 개인정보보호 : 스마트그리드 거버넌스의 제안, 기업법연구, 26권 2호. PP. 257-281, 2012.

[18] 이일우, 김현, "스마트 에너지 서비스 기술", 한국전자통신연구원, 30권 5호, PP. 69-79, 2015.

[19] 김천기, "신재생에너지 시스템 환경에서의 보안 취약점에 대한 연구", 고려대학교 정보보호대학원,석사학위, 2014.

[20] 김지소, 문형돈. "지능정보기술을 활용한 '에너지 한계비용 제로사회' 실현방안에 관한 고찰". 한국통신학회 학술대회논문집, pp. 677-678, 2016.

〔저자소개〕

노 종 호

1994년 8월 전남대학교 전산통계학과 학사
2009년 2월 연세대학교 정보대학원 IT 경영전략 석사
2016년 9월 ~ 고려대학교 정보보호대학원 정보보호학과 박사과정
email : parker.noh@gmail.com

권 헌 영

2008년 3월 ~ 2015년 8월 광운대학교 법과대학 교수
2015년 9월 ~ 고려대학교 정보보호대학원 교수
email : khy0@korea.ac.kr