情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

스마트 그리드에서의 소비자 참여와 보안 이슈

이 경 복*, 독고지은*, 유 지 연**, 이 숙 연**, 임 종 인***

요 약

최근 그린 에너지에 대한 관심이 고조되면서, 기존 전력망에 IT 기술이 융합함으로써 보다 지능적으로 전력을 송·배전하고, 에너지를 효율적으로 사용하게 하는 스마트 그리드(지능형 전력망)에 대한 사업 추진이 급속하게 진행되고 있다. 하지만 스마트 그리드는 그 대상이 전력망이라는 주요기반시설의 특성으로 인하여 보안의 고려가 표면적으로 드러나고 있지 못한 상황이다. 이에 스마트 그리드 활성화의 동인으로써 스마트 그리드의 보안에 대한 연구가 지속적으로 진행되도록 하기 위해서, 본 연구에서는 스마트 그리드에서 보안 이슈 가운데 소비자 참여에 한정하여 그 세부 이슈와 더불어 대응 방안을 고찰하도록 한다.

Ⅰ. 서 론 - 연구배경 및 필요성

최근 에너지 고갈 및 지구온난화 등의 환경문제로 인하여 에너지를 효율적으로 사용하고, 오염을 유발하지 않는 에너지를 사용하자는 모토의 '그린 에너지'가 전 세계적인 화두로 떠오르고 있다. '그린 에너지'는 태양열·풍력 발전과 같은 친환경 에너지의 생산부터, 온난화의 원인인 CO_2 배출의 규제, 자전거나 1회용품 등의 친환경 제품 사용 및 전력 에너지의 효율적인 송·배전 등과 같이 에너지와 직간접적으로 관련된 분야에서 광범위하게 논의되고 있는데, 이 가운데 국내에서는 특히 스마트 그리드에 대한 관심이 고조되고 있으며, 현 정부에서도 스마트 그리드 산업과 관련하여 반도체와 조선 산업을 잇는 국가 대표산업으로 육성하려는 계획을 세우고 있다.

스마트 그리드는 에너지의 효율성 향상을 목적으로 기존 전력망에 IT 기술을 도입·융합하여 전력공급자와 소비자 간의 양방향 통신을 구축하고, 실시간으로 데이터를 교환함으로써 지능화된 전력 에너지의 송·배전이 가능하도록 하는 차세대 '지능형 전력망'을 의미한다. 이러한 고효율의 지능화된 전력망은 단순히 전력 공급망 발전의 측면만이 아니라 디지털 사회의 성장하는 수요에 적합한 새로운 전력 인프라의 구축을 위한 것이라 할 수 있으며, 또한 지속가능한 발전을 위한 환경 친화적인 인프라로써 현재의 환경문제를 해결할 것으로 예상되기 때문에 사회 전 분야에서 광범위하게 스마트 그리드에 대한 기대가 일어나고 있다. 이러한 스마트 그리드의 광범위한 중요성은 스마트 그리드가 단기적·지역적인 사업이 아닌 장기적 국가 차원의 사업이 되어야 함을 의미하며, 실제 미국이나 유럽의 스마트 그리드 관련 사업은 정부의 주도 하에서 대략 2020~2030년 정도에 스마트그리드의 완전한 구축을 목표로 추진 중이다.

국내에서는 올해 들어 스마트 그리드에 대한 사업이 가시화되었으며, 이는 미국이나 유럽에 비해 조금 늦은 바가 없지 않다. 하지만 이번 정부의 녹색 성장 정책과 맞물려서, 정부와 산업계의 적극적인 논의로 인하여 사업의 추진이 급속하게 진행되어, 외국에 비해 매우 빠르게 사업화가 진행되고 있다. 스마트 그리드가 단기적인 측면의 사업이 아닌 장기적인 국가적 사업임을 고려할 때, 이러한 급속한 추진은 여러 가지 부작용을 가져올 가능성이 높다. 특히 스마트 그리드가 단순히 차세대 전력망만을 의미하는 것이 아님에도 불구하고 사업의 추

이 연구에 참여한 연구자(의 일부)는 '2단계 BK21 사업'의 지원비를 받았음.
* 고려대학교 정보경영공학전문대학원 석사과정({isnare;ehrrhdms}@korea.ac.kr)
** 고려대학교 정보경영공학전문대학원 박사과정({yooo;chnwolf}@korea.ac.kr)
*** 고려대학교 정보경영공학전문대학원 원장(jilim@korea.ac.kr)

진이 주로 유틸리티 관련 사업자를 중심으로 이루어지고 있기 때문에 잠재적인 부작용의 가능성이 더욱 크다고 할 수 있다. 또한 스마트 그리드가 국가 또는 지역의 정부기관과 더불어 비즈니스 주체들 간의 상이한 이해관계와 밀접하게 결합되어 있기 때문에, 이러한 스마트 그리드의 추진 단계부터 문제가 발생한 경우에 더욱 복잡한 상황으로 발전할 것으로 예상한다.

본 연구는 이러한 스마트 그리드를 둘러싼 문제의 인식으로부터 시작되었으며, 아직 스마트 그리드가 초기 도입 단계에 머물러 있는 상태에서 이러한 문제를 모두 논하는 것은 시기상조이고, 스마트 그리드의 추진에 대한 장애물로 여겨질 수 있다고 판단하기 때문에, 본 연구에서는 스마트 그리드의 동인(動因)의 하나로써 언급되고 있는 소비자 참여와 관련된 부분의 문제에 한정하여 논하고자 한다. 이를 위해 먼저 스마트 그리드의 정의 및 기술 및 정책 동향에 대하여 미국과 유럽을 중심으로 전체적인 내용을 확인하고(II), 이후 스마트 그리드와 관련된 보안 이슈, 특히 소비자와 관련하여 발생 가능한 문제에 초점을 두고 고찰하도록 하겠다(III). 그리고 이에 대한 기술·정책적 대응방안을 모색함으로써, 스마트 그리드에서의 소비자 보안이슈에 대한 대응방안의 방향을 논하도록 하고(IV), 차후 연구 방향에 대하여 언급하도록 한다(V).

Ⅱ. 스마트 그리드 추진 배경과 동향

2.1 스마트 그리드의 정의 및 특징

2.1.1 정의

먼저 본 연구에서 논의하려고 하는 스마트 그리드(Smart Grid)가 과연 무엇을 의미하는가를 확인할 필요가 있다.

스마트 그리드는 기존 전력망에 IT 기술을 도입하여 시스템을 개선함으로써 에너지의 효율성을 높이려는 연구에서 파생되어 시작되었기 때문에, 스마트 그리드에 관한 논의가 먼저 시작된 국외에서도 앞서 살펴본 정의들과 같이 각 국의 전력망에 대한 연구 및 정책에 따라 스마트 그리드의 명칭 및 정의가 각각 조금씩 다르며, 아직까지는 스마트 그리드에 대한 명확한 정의 및 범위에 대해서는 국제적으로는 합의되지 않은 상태이다.[1] 또한 스마트 그리드와 관련하여 각국에서 이제 막 표준을 정하고 있는 상황이기 때문에, 스마트 그리드에 대한 실체적인 정의는 아직까지는 모호하다[4]. 따라서 무엇보다도 스마트 그리드에 대한 명확한 정의, 대상, 목적 등을 실체화할 필요가 있다.

스마트 그리드에 대한 정의를 찾아보면, 미국의 「에너지독립및안보법」[2]에서는 스마트 그리드를 「미래의 증가할 전력 수요를 해결할 수 있으면서도 전력 전송과 분배에 있어 신뢰성과 기반시설보호를 유지할 수 있도록 구조화 된 국가 전력 전송 분배 시스템」으로 정의하고 있다[1]. 또한 EU의 유럽기술플랫폼 스마트그리드[3]에서도 스마트 그리드에 대하여 「지속가능하고, 경제적이며, 안전한 전기 공급을 효율적으로 전송하기 위한, 연결된 모든 사용자의 작업을 지능적으로 통합할 수 있는 전기 네트워크」로 정의하고 있다[2]. 국내에서는 스마트 그리드를 「스마트 그리드를 전력망에 정보기술을 접목하여, 전력공급자와 소비자가 양방향으로 실시간 정보를 교환, 에너지효율을 최적화하고 새로운 부가가치를 창출하는 차세대 전력망」으로 정의[4]하고 있다[3].

이와 같은 스마트 그리드에 대한 여러 가지 정의를 고려하여 정리하면, 스마트 그리드는 IT 기반의 미래형 차세대 전력망으로 센서·통신 네트워크·자동제어 등의 IT 기술을 전력망에 도입함으로써 전력 인프라의 융통성·보안성·신뢰성·효율성·안전성 등을 향상시키고, 유틸리티와 소비자 간의 양방향 통신을 가능하게 하여 소비자의 전력 선택 범위를 넓히고, 이를 통해 에너지 부문의 인터넷으로써 전반적인 전력 인프라 시스템의 효율성을 향상시키는 친환경적인 디지털 시대를 위한 '지능형 전력망'을 의미한다. 특히, IT 기반 기술에서 사용되는 '스마트(Smart)'의 의미가 '여러 가지 기술

1) 국내에서도 처음에는 '지능형 전력망'의 용어를 사용하였으나, 최근에는 스마트 그리드로 영어 명칭을 그대로 사용하고 있으며, 국외에서도 대부분 Smart Grid의 용어가 일반화되고 있다.

2) Energy Independence and Security Act of 2007(EISA) (Public Law No. 110-140) TITLE XIII. SMART GRID. Section 1301. Statement of Policy on Modernization of Electricity Grid에서 스마트 그리드에서 요구되는 특징을 명시함으로써 스마트그리드를 정의하고 있다.

3) 정식 명칭은 European Technology Platform for the Electricity Networks of the Future(SmartGrids)이며, 유럽 위원회(European Commission) 산하의 조직이다.

4) 본 정의는 국내 지능형전력망 로드맵 추진위원회의 비전·신비즈니스분과에서 보고한 "한국형 스마트 그리드 비전 초안"에서의 정의(definition)이다.

〔표 1〕 스마트 그리드의 특징

구 분	미 국			EU
	EISA	NETL	DOE	ETP
특 징	정보 및 제어 옵션의 적시 공급	자기복구	발전/저장 옵션	유연성
	전력 그리드에 연결되는 가전제품 및 장비의 상호운영성과 통신의 표준 발전		시스템 침해 예측/대응	
	스마트 가전제품 및 다른 소비자 장치의 통합	소비자 참여	소비자 참여	접근성
	계량, 그리드 운영·상태에 관련된 통신, 배전 자동화 등에 대한 스마트 기술의 배포	시장 활성화	신제품/서비스/시장의 활성화	
	고급전력저장 및 피크 쉐이빙 기술의 배포/통합			
	사이버보안을 완벽 보장하는 그리드 운영	공격에 대한 대항	공격/재해에 대한 탄력 있는 운영	신뢰성
	전력 그리드의 신뢰성, 보안, 효율성 향상을 위한 디지털 정보 및 제어기술 사용	21C의 고품질 전력	디지털 경제의 고품질 전력	
	재생가능자원을 포함한 분산자원의 발전 및 통합	자산최적화 및 효율적 운영	자산최적화 및 효율적 운영	경제성
	수요반응/수요측면자원/에너지효율자원의 발전/결합			
	스마트 그리드 기술, 시행, 서비스 채택에 부당/불필요한 장벽의 식별 및 인하			

이 복합적으로 융합되어 다방향성을 가지게 함'임을 고려하면,[5] 현재 정의된 것보다 스마트 그리드는 그 의미에서 변화가능성을 내포하고 있다고 할 수 있다. 현재 스마트 그리드에 대한 관심이 높고 논의가 활발하게 이루어지고 있기 때문에 이러한 실체적 개념의 정립은 곧 이루어 질것으로 예상한다.

본 연구에서는 스마트 그리드에서 중요한 역할을 담당하는 '소비자 참여'에 초점을 두고 있기 때문에, 소비자와 관련된 문제 논의에서의 스마트 그리드에 대한 실체적 접근을 위해서 스마트 그리드에 대한 구체적인 정의보다 스마트 그리드가 내포할 수 있는 다양한 변화가능성에 초점을 두어, 스마트 그리드를 '소비자가 참여할 수 있는 지능형 전력망'의 측면에서 살펴보도록 하겠다.

2.1.2 특징

스마트 그리드는 전력망 전체의 혁신을 통해 새로운 전력 공급 시스템 체계를 갖추는 것을 목적으로 IT 기술과 전력 기술이 융합되고 있으며, 이러한 융합 부분에서 스마트 그리드의 특징이 구체화된다. 이를 살펴보면, 전력망에서 현재의 아날로그 단방향 통신이 디지털 양방향 통신으로, 유틸리티 중심의 시스템이 소비자 중심으로, 중앙 집중적 발전이 분산 발전 통합제어로, 수동복구 감시가 자가 자동복구로, 제한적인 가격 신호를 가지던 시장에서 수요를 지원하는 시장으로 변화될 것으로 예상하고 있으며, 이러한 특징으로 인하여 스마트 그리드는 기존 전력망에 대한 논의와는 다른 접근을 필요로 한다.

EISA에서는 스마트 그리드의 특징으로 '전력 그리드의 신뢰성, 보안, 효율성을 향상시키기 위한 디지털 정보 및 제어 기술의 증가된 사용', '사이버보안을 완벽하게 보장하는 그리드 운영 및 자원의 동적인 최적화', '재생 가능한 자원을 포함한 분산 자원과 발전의 배포 및 통합', '수요반응, 수요 측면 자원, 에너지 효율 자원의 발전 및 결합', '계량, 그리드 운영·상태에 관련된 통신, 배전 자동화에 대한 스마트 기술의 배포(전자제품의 물리적인 운영 및 소비자 장비를 최적화하는 실시간, 자동화된, 쌍방향 기술)', '스마트 가전제품 및 다른 소비자 장치의 통합', '플러그인 전력 및 하이브리드 전기 자동차, 열저장 냉방장치를 포함하는 고급 전력 저장 및 피크 쉐이빙(peak-shaving) 기술의 배포 및 통합', '소비자에게 정보 및 제어 옵션을 적시에 공급', '그리드를 서비스하는 기반시설을 포함하는 전력 그리드에 연결되는 가전제품 및 장비의 상호운영성과 통신의 표준 발전', '스마트 그리드 기술, 시행, 서비스 채택에 대

5) 스마트카드나 스마트폰에서의 '스마트(Smart)'와 같은 의미로 '복합적인 기능의 구현'을 의미한다.

한 부당하거나 불필요한 장벽의 식별 및 인하'를 명시하고 있다[5].

그리고 미국 에너지부(Department of Energy, DOE) 산하의 국립에너지기술연구소(National Energy Technology Laboratory, NETL)에서 수행한 전력송전분야에 대한 연구인 Modern Grid Initiative에서는 시스템적 관점에서 '자기복구', '소비자 참여 및 동기유발', '공격에 대한 대항', '21세기 디지털경제사회가 요구하는 전력품질의 제공', '전력발전 및 저장기능의 옵션 수용', '시장의 활성화', '자산의 최적화와 효율적 운영'을 스마트 그리드가 가져야할 기본적인 특징으로 언급하고 있다[6]. 이와 유사하게 스마트 그리드에 대한 DOE의 보고서에서 '소비자의 적극적인 참여 활성화', '모든 발전 및 저장 옵션의 수용', '새로운 제품, 서비스, 시장의 활성화', '디지털 경제에 대한 전력품질의 제공', '자산의 최적화와 효율적인 운영', '시스템 침해에 대한 예측 및 대응', '공격 및 자연재해에 대한 탄력 있는 운영'을 스마트 그리드의 특징으로 명시하고 있다[7].

유럽기술플랫폼에서는 스마트 그리드의 특징으로 '변화와 도전에 응함과 동시에 소비자의 요구를 만족시키는 유연성', '재생 가능한 전원(電源)과 고효율 국부발전에 대한 모든 사용자의 연결접근을 가능하게 하는 접근성', '디지털 시대의 수요에 부응하는 공급의 품질과 보안을 보장하고 향상시키는 신뢰성', '혁신과 효율적인 에너지 관리, 그리고 공정한 경쟁과 규제를 통한 최고 가치를 제공하는 경제성'을 명시하고 있다[8]. 이러한 특징을 정리하면 [표 1]과 같다.

2.2 스마트 그리드의 주요 기술

앞서 살펴본 특징을 이끌어 내는 스마트 그리드를 가능하게 하는 주요 핵심기술에 대하여 살펴보면, NETL의 Modern Grid Initiative에서는 통합된 통신(Integrated Communications), 감지 및 측정 기술(Sensing and Measurement), 지능형 컴포넌트(Advanced Components), 고도화된 제어기법(Advanced Control Methods), 향상된 인터페이스와 의사결정 지원(Improved Interfaces and Decision Support)의 5개 분야의 기술을 스마트 그리드의 주요 핵심 기술로 명시하고 있으며[6], 다른 보고서에서도 이와 유사하게 쌍방향 통신 네트워크(Two-way Communication Networks), 미터 데이터 관리 시스템(Meter Data Management Systems), 에너지 관리 및 제어 기술(Energy Management and Control Technology), 송/배전 자동화 기술(Distribution/Substation Automation Technology), 기술 제휴(Technology Alliances)를 스마트 그리드의 주요 기술로 명시하고 있다[9]. 또한 ETP에서도 스마트 그리드의 핵심 기술로 '검증된 기술 솔루션의 툴박스의 개발(Toolbox of Proven Technical Solutions)', '규제와 상업적인 프레임워크의 조화(Harmonizing Regulatory and Commercial Frameworks)', '기술적인 표준과 프로토콜의 공유(Shared Technical Standards and Protocols)', '정보·연산·전화통신 시스템의 개발(Information, Computing and Telecommunication Systems)', '신 설계와 구 설계 사이의 인터페이스 보장(Interfacing of New and Old Designs)'를 내세우고 있다[8].

이를 간단히 정리하면, 스마트 그리드에서는 쌍방향으로 통합된 통신 기술(Communications)이 가장 기저적인 핵심 기반 기술이며, 이러한 통신 기술을 바탕으로 스마트 미터기와 관련된 미터링 기술(Metering), 전력의 송배전과 관련되는 고급 제어 기술(Advanced Control), 그리고 정보의 효과적인 전달과 기기간의 호환성을 위한 인터페이스(Interface)가 스마트 그리드를 구성한다고 볼 수 있다.

2.3 스마트 그리드의 국내·외 동향

국외에서는 미국에서 스마트 그리드에 대한 연구가 가장 활발하게 진행되고 있는데, 1999년에 美 에너지부(Depart of Energy, DOE)와 캘리포니아 에너지 위원회(California Energy Commission, CEC)가 추진한 '전력신뢰도 기술 향상 컨소시엄'[6]과 2001년에 美 전력연구소(Electric Power Research Institute, EPRI)와 전기혁신연구소(Electricity Innovation Institute, E2I)에 의해 구성된 '디지털 사회를 지원하기 위한 전기 인프라 컨소시엄'[7]를 중심으로 미래의 차세대 전력망에 대한 논

6) Consortium for Electric Reliability Technology Solutions, CERTS. CERTS는 실시간 전력망 신뢰성 관리, 신뢰성 및 시장, 분산 에너지 자원(DER) 통합, 자원으로써의 부하, 자산 신뢰성 기술 문제 및 요구 평가의 5가지 영역에서 전력의 신뢰성 연구를 수행하고 있다.

7) Consortium for Electric Infrastructure to Support a Digital Society, CEIDS. 처음 구성될 당시에는 E2I 산하의 컨소시엄이었으나, E2I가 EPRI에 통합됨에 따라 EPRI에서 운영

의가 시작되었으며, 이후 DOE에서 전력망의 첨단화, 고도화를 통한 스마트 그리드(Smart Grid)체계 구축을 위한 「"GRID 2030" A National Vision for Electricity's Second 100 Years」를 발표하고 GridWise Alliance 등을 추진하였다. 이후 2007년에 제정된 EISA에서는 스마트 그리드에 대한 추진과 관련하여 표준 개발의 의무를 NIST에게 부여하는 등의 내용을 규정하였으며, 2009년 미국 오바마 정부가 새로이 들어서면서 내세운 경기부양책(American Recovery and Reinvestment Act of 2009)에 스마트 그리드를 통한 일자리 창출이 포함됨으로써, 점차 스마트 그리드에 대한 추진이 가속화 되고 있다. 미국 외에도 EU, 일본, 중국, 영국 캐나다 등에서도 스마트 그리드에 대한 관심이 높아지면서, 사업이 추진되고 있다.

국내에서는 2009년에 들어서면서, 현 정부의 녹색 성장과 맞물려 스마트 그리드에 대한 적극적인 논의와 함께 추진이 급속하게 진행되어, 2월에 대통령 직속 녹색성장위원회에서 세계 최초의 국가단위 스마트 그리드 구축계획을 발표함으로써, 국내 스마트 그리드 사업이 본격적으로 추진되었다. 이후 지난 4월에 스마트 그리드 구축의 로드맵 마련을 위한 '지능형 전력망 로드맵 수립 추진위원회'가 발대되었고, 5월에는 '한국스마트그리드협회'가 창설되는 등 정부기관 및 산업계의 협력하에 스마트 그리드에 대한 사업의 추진이 급속하게 진행되고 있다.

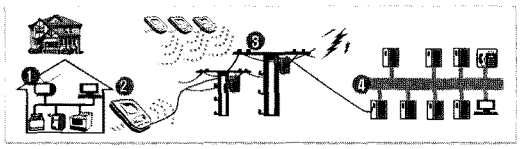
Ⅲ. 스마트 그리드에서의 소비자 참여와 보안이슈

스마트 그리드에서의 소비자 참여는 단순히 소비자단의 검침시스템에 대한 자동화나 검침시스템 기능의 고도화만을 이야기하는 것이 아니라, 수요 관리 시스템(Demand Management System)을 기초로 유틸리티와의 쌍방향 통신을 이용하여, 소비자가 실제로 전력의 발전부터 송·배전에까지 참여함으로써, 전력의 수요와 공급의 균형을 맞추고, 유틸리티의 업무를 개선하며, 다양한 전력 서비스를 창출하고, 소비자 자신의 에너지 소비를 효율적이게 하는 등, 스마트 그리드에서 핵심적인 역할을 담당할 것으로 논의되고 있다.

현재 논의되고 있는 스마트 그리드에서는 소비자로부터 유틸리티에게 전력 사용 내역이나 선호시간 등의 상세한 소비자 데이터가 일방적으로 자동 전송되며, 이를 이용하여 유틸리티가 전력을 통제하는, 상향식(bottom-up) 데이터 흐름 및 하향식(top-down) 통제 흐름의 구조가 나타나고 있는데, 이러한 구조는 스마트 그리드에 대한 소비자 참여와 맞물려서 프라이버시와 측정가능성(scalability) 및 보안 문제를 야기할 것으로 예상한다. 또한 소비자 데이터를 보유하는 유틸리티나 정보 브로커에 의한 소비자 정보의 오·남용 가능성이 존재한다.

따라서 프라이버시에 민감한 소비자들이 스마트 그리드에 참여하지 않을 수 있으며, 이러한 소비자의 불참은 스마트 그리드의 추진에 있어서 가장 큰 장애가 될 수 있기 때문에, 소비자들의 우려를 불식시키고 소비자의 권리를 보장하기 위하여 스마트 그리드의 추진 정책 수립 시 이러한 기술 구조적인 문제에 대한 고려가 필요하다. 이에 스마트 그리드에서의 소비자 참여와 관련된 구체적인 현황과 보안 이슈를 [그림1]과 같이 데이터의 흐름에 따라서 구분하여 살펴보면 다음과 같다.

3.1 소비자의 스마트 제어(Smart Control) 영역



〔그림 1〕 스마트 그리드에서 소비자 데이터 흐름의 구조

먼저, 스마트 그리드에서 소비자 참여가 시작되는 지점은 [그림 1]의 ①에서와 같이, 가정이나 건물 내 설치된 스마트 전자제품에서부터 외부의 스마트 미터기 이전까지의 부분으로, 소비자가 가정이나 건물 내에서 전력을 소비하고, 유틸리티로부터 정보를 받아 확인하는 등의 직접적인 소비자 활동이 이루어진다. 예를 들면, 스마트 칩이 내장된 스마트 전자제품을 사용함으로써, 전력망에 부하가 걸리는 경우 사용을 제한할 수 있고, 또는 전기요금이 저렴할 때만 작동하도록 설정할 수도 있다. 그리고 온수기나 냉난방장치에도 동일하게 응용되어 피크 시의 전력 사용을 줄이고 전력망의 안전성을 높일 수 있다. 또한 스마트 빌딩(Smart Building)의 구축을 통하여 건물 내부의 냉난방, 환기 및 조명 등 에너지 사용을 센서와 자동제어 기술을 이용해 전력망과 연결하여 전력망 상태에 따라 조절할 수 있는, 즉 수요응

중이며, IntelliGrid Consortium으로 불리기도 한다.

답이 필요한 때에 건물의 전력 사용을 줄일 수 있다. 이와 같은 소비자의 스마트 제어는 홈 네트워킹 미들웨어 기술, 상황 인지(context-awareness) 미들웨어 기술, 스마트 컨트롤, 다중 인터페이스 등의 기술이 적용됨으로써 실현이 가능하다.

이 영역에서의 데이터 및 통제의 흐름을 살펴보면, 소비자가 스마트 전자제품을 사용함으로써 각 제품에서 전력소비와 관련된 데이터가 댁내수집장치(Home Concentrator Unit)와 데이터집중장치(Data Service Unit) 등을 통하여 일차적으로 수집되며, 수집된 데이터는 가정이나 건물 내 중앙관리시스템을 통하여 통합되고, 통합된 데이터를 유틸리티로 전송하기 위하여 스마트 미터기에게로 전달된다. 또한 유틸리티로부터 전력 공급과 함께 제공받는 가격 등의 데이터를 소비자가 직접 확인할 수 있도록 하며, 이를 바탕으로 전력 구매를 선택할 수 있게 할 뿐 아니라, 각 제품에서의 전력 통제를 소비자만이 아닌 유틸리티에서도 가능하게 한다.

이와 같은 소비자의 스마트 제어 영역에서는 'ⓐ 인증(authentication)', 'ⓑ 소비자 데이터 수집(collection of consumer data)', 'ⓒ 상호운영성(interoperability)', 'ⓓ 무선 센서의 보안 취약성(vulnerability in wireless sensor)', 'ⓔ 전력 사용에 대한 통제권(control over power usage)'의 보안 이슈가 존재하며, 이들 이슈의 구체적인 내용은 다음과 같다.

먼저, 스마트 제어를 위하여 가정이나 건물 내부의 스마트 전자제품에 대한 제어 신호가 입력된 경우, 이러한 입력이 정당한 사용자에 의한 것인지, 전송된 입력을 받은 제품이 목적 대상이 맞는지 등에 대한 인증이 반드시 요구되기 때문에, 사용자 및 기기의 인증은 스마트 제어의 영역에서 가장 기본적인 보안 요건이라 할 수 있다. 하지만 각 스마트 전자제품에서의 '잘못된 인증'이 단순히 해당 기기의 오작동만을 야기하는 것이 아니라, 타인에 의한 제어 및 다른 기기에 대한 제어권 전이의 가능성을 내포하기 때문에 스마트 제어에서 가장 중요한 보안 이슈라 할 수 있다.

두 번째로, 스마트 전자제품에서 데이터를 수집하는 경우, 소비자의 설정에 의하여 수집하기도 하지만, 대부분 효율성을 위해 상황인지 미들웨어 기술을 이용하여, 소비자의 환경 변화를 자동적으로 인지·해석하고, 개인의 성향을 파악하여 데이터를 수집하도록 설계된다. 이와 같은 자동적인 데이터 수집은 수집단계에서의 프라이버시 침해 뿐 아니라 차후 수집된 데이터의 보관 및 이용단계에서 유출 또는 오용된 경우에도 소비자의 프라이버시를 침해할 수 있기 때문에, 인증과 더불어 스마트 제어에서 중요한 보안이슈라 할 수 있다.

세 번째는 스마트 제어의 과정에서 스마트 전자제품이 서로 상호작용하고, 이를 통하여 각 제품에서 수집된 데이터가 통합되기 때문에, 스마트 전자제품 사이의 상호운영성이 보안 이슈로 존재한다고 할 수 있다. 또한 이런 상호운영성의 문제를 해결하기 위해 사용되는, 각 제품 간 상호 연동을 보장하는 미들웨어 기술은 보안에 있어서 또 하나의 취약점이 될 수 있다. 스마트그리드가 아직 개념 정립 및 기술 개발의 단계이기 때문에, 이러한 상호운영성과 관련된 보안 이슈는 스마트 그리드의 표준이 확정되기 전까지 지속될 것으로 예상한다.

네 번째로, 각 스마트 전자제품에서 사용되는 무선 센서는 하드웨어적 특성상 보안 취약성을 가지고 있기 때문에, 이와 관련된 보안 이슈가 존재한다. 눈에는 보이지 않지만 항상 망이 외부에 노출되어있는 무선의 특성과 함께, 센서가 단순히 데이터 수집 및 전달만을 목적으로 하기 때문에 저처리능력 프로세서(lower processing power processor)로 설계되는 특성은 보안에 있어서 심각한 취약성이라 할 수 있다.

마지막으로 스마트 그리드가 전력의 효율적 사용을 목적으로 하기 때문에, 전체 전력 사용이 큰 시간대에 유틸리티가 소비자의 의사와는 별개로 각 스마트 전자제품의 전력의 사용을 제한하는 등의 소비자의 전력 사용에 대한 통제권 침해의 이슈가 존재한다. 이러한 통제권 침해는 명확하게 보안상의 이슈로 볼 수는 없지만, 적어도 보안과 관련된 사항에서 고려해야할 필요가 있다.

3.2 AMI 영역

[그림 1]의 ②에서는 댁내에서 수집된 소비자의 전력소비 데이터가 스마트 미터 시스템을 통하여 일정시간마다 디지털 방식으로 기록되며, 스마트 그리드의 기반 통신망을 통해 유틸리티 등의 사업자에게 보고된다. 이러한 스마트 미터 시스템의 환경을 AMI(Advanced Metering Infrastructure)라고 하며, AMI 가운데 전력망의 전력 사용량 시간대별 변화에 따라 가격측정을 가능케 하는 스마트 미터기는 수요응답 프로그램의 핵심기술로써 스마트 그리드에서 매우 중요한 역할을 한다.

AMI의 스마트 미터기는 단순히 소비자의 전력 소비 데이터를 유틸리티 사업자에게 보고하는 것만이 아니라 유틸리티로부터 실시간으로 전력 가격의 정보를 전송받아 소비자가 전력 사용에 있어서 고려할 수 있도록 하며, 차후에는 홈 네트워크의 라우터 기능까지 포함하는 가정용 장비의 중앙관리시스템 역할을 수행할 것으로 예상하고 있다.

AMI 영역에서의 데이터 및 통제 흐름을 살펴보면, 유틸리티에서는 스마트 미터기를 원격으로 제어하여 검침을 실시하고, 이러한 통제에 의하여 스마트 미터기에서 실시간으로 댁내의 전력 소비에 대한 검침이 이루어지며, 스마트 미터기의 검침으로 통합된 데이터는 유틸리티 등의 사업자가 사용할 수 있도록 기반시설 통신망을 통하여 전송된다.

이와 같이 스마트 미터기가 기본적으로 소비자와 유틸리티 사이에서 오가는 데이터 및 통제의 게이트웨이 역할을 하고 있음을 고려할 때, AMI에서의 보안이슈는 곧 스마트 미터기에서의 보안 이슈로 볼 수 있으며, 그 중요성 또한 매우 크다고 할 수 있다. 이에 스마트 미터기와 관련된 보안 이슈로 'ⓐ 스마트 미터기의 보안 취약성(vulnerability of smart meter)', 'ⓑ 스마트 미터기에서의 프라이버시(privacy in smart meter)', 'ⓒ 스마트 미터기에 대한 접근통제(access control of smart meter)'가 존재하며, 이들의 구체적인 내용은 다음과 같다.

먼저 스마트 미터기가 우선적으로 전력 검침의 기능에 중점을 두고 설계되었기 때문에, 스마트 미터기의 기기 자체의 보안 취약성이 존재하며, 이는 AMI 영역에서 가장 큰 보안이슈이다. 스마트 미터기는 외부와 직접 연결되는 접점으로, 스마트 미터기에 대한 웜 바이러스나, 서비스 분산 공격 등과 같은 직접적인 공격이 발생할 수 있으며, 실제로 한 보안 업체에서는 스마트 미터기의 보안 취약성을 알리기 위해 스마트 미터기에 감염되어 다른 스마트 기기로 전이되는 웜 바이러스를 개발하기도 하였다[10]. 또한 스마트 미터기가 다기능화됨에 따라 이러한 기기의 보안 취약성의 문제는 더욱 심화되고 있다.

두 번째로 스마트 미터기를 통하여 소비자의 모든 전력 관련 데이터가 집중·통합되기 때문에, 스마트 미터기의 보안 취약성으로 인한 프라이버시의 보안이슈가 존재한다. 현재는 스마트 미터기를 통하여 전송되는 데이터가 단순히 시간별 전력 소비량이나, 부하 수준 등의 기본적인 데이터만을 포함되고 있기 때문에, 개인들이 이에 대하여 프라이버시의 문제로 민감하게 대응하고 있지 않지만, 전력 소비 데이터가 다른 어떤 정보와 결합하여 개인의 프라이버시를 위협할지 모르는 잠재적인 위험성이 존재하기 때문에, 프라이버시에 대한 사전적인 보호의 측면에서 스마트 미터기에서 전송되는 데이터에 대한 보호가 고려되어야 한다. 현재에도 이러한 시스템 센서·스마트 기기·전압 및 전류에 대한 데이터를 정교한 시그널 분석기법을 통하여 분석하거나, 비정상적인 전력소비를 분류함으로써 사용자의 부재 여부, 또는 헤어드라이어 같은 가전제품 사용에 관한 정보를 확인할 수 있으며, 이는 심각한 프라이버시의 문제로 여겨질 수 있다[11]. 실제로 네덜란드에서는 스마트 미터기 강제설치 정책이 프라이버시의 문제로 소비자단체의 반대에 부딪혀 좌절되기도 하였다[12].

마지막으로 스마트 미터기에 대한 통제권이 해커에게 넘어간 경우, 단순히 해당 스마트 미터기를 제어하여 전력 공급을 차단하는 것뿐만 아니라, 다른 스마트 미터기에 대한 공격 수단으로써 사용이 가능한 등의 문제가 발생할 수 있기 때문에 스마트 그리드에 대한 통제권에 대한 보호, 즉 접근제어 역시 중요한 보안 이슈라 할 수 있다[13].

3.3 스마트 그리드의 기반 통신망 영역

[그림 1]의 ③은 스마트 그리드의 기반 통신망을 의미하며, 이 영역에서는 소비자의 직간접적인 활동은 존재하지 않으나, 소비자의 정보가 전송되는 과정에서 이용되기 때문에, 정보의 흐름에 따라 보안 이슈를 고려하도록 하겠다. 스마트 그리드의 이전의 전력망에서는 주로 저속의 전력선통신(PLC) 등과 같은 저속 폐쇄 통신망이 기반 통신망으로써 이용되었으나, 스마트 그리드에서는 고속 양방향 통신이 가능한 광통신이나, 광대역 전력선 통신(Broadband over Powerline Communications, BPL), 이동통신, 위성 통신까지 광범위한 종류의 통신이 적용되고 있다. 이와 같은 스마트 그리드에서의 다양한 통신 기술의 사용은 보다 신속하고 안정적인 통신을 경제적으로 제공함으로써, 스마트 그리드의 다른 기술들이 이용할 수 있는 기본 인프라를 제공한다는 측면에서 스마트 그리드에서의 핵심이라 할 수 있다[14].

기반 통신망 영역에서의 데이터 및 통제 흐름을 살펴

보면, 스마트 미터기와 유틸리티 사이에서 기반 통신망을 거쳐 정보가 교환되며, 통제 신호 역시 기반통신망을 거쳐 유틸리티로부터 스마트 미터기 단으로 전송된다. 즉, 스마트 미터기로부터 얻어지는 소비자 데이터가 기반 통신망을 거쳐 유틸리티에게 전달되며, 유틸리티에서 소비자에게 전송하는, 수집된 소비자 데이터를 분석·처리하여 얻어지는 과금 정보나, 에너지 사용 정보 등의 데이터도 기반 통신망을 거친다. 또한 유틸리티 등의 기반시설에 대한 통제신호 및 정보 역시 기반 통신망을 통하여 전송된다.

이와 같이 스마트 그리드에서 기반 통신망이 소비자 데이터와 통제 신호의 전송로의 역할을 하기 때문에, 보안 이슈로써 고려해야할 필요가 있다. 사실 통신 네트워크의 기본적인 역할이 데이터 전송에 있기 때문에, 발생 가능한 보안 이슈는 고정되어있다. 즉, 기존 유·무선 통신 네트워크에서의 보안 취약점 및 공격 등이 스마트 그리드에서도 거의 유사하게 전이되어, 보안 이슈를 발생시킬 가능성이 존재한다. 하지만 기존의 통신망에서 요구하는 보안 요구사항과 스마트 그리드의 보안 요구사항에서의 차이점이 존재할 것이므로, 각 통신 기술의 도입 시 스마트 그리드의 기반 통신망 및 시스템의 안전성·신뢰성의 보장과 데이터 보호 등을 위하여, 해당 기술에서의 보안 이슈에 대한 분석을 통해 스마트 그리드에서도 동일한 이슈가 발생할 것인가를 고려할 필요가 있다

이를 고려한 스마트 그리드의 기반 통신망 영역의 보안이슈는 'ⓐ 유·무선 통신 네트워크에서의 취약성(vulnerability of wire/wireless communication network)'과 'ⓑ 전력선 기반 통신에서의 셀 보안 취약성(security vulnerability of cell in powerline-based communication network)'이다.

현재 스마트 그리드의 기반 통신망으로 FTTH, HFC 등의 유선 통신과 WiFi, WiMax, 3G, TDMA, CDMA, VSAT 등의 무선 통신이 논의되고 있다[8][14]. 이러한 통신망은 기본적으로 개방형 네트워크의 형태를 취하고 있기 때문에 여러 가지 보안 취약성을 가지며, 이로 인해 웜이나 바이러스에 의한 해킹이나 서비스거부 공격 등의 잠재적인 위협이 존재하는데, 이러한 위협의 리스크는 스마트 그리드에서도 동일하게 존재할 것으로 예상된다. 물론 기존 전력망의 기반 통신망에서도 이와 같은 위협은 존재하였으나, 기본적으로 폐쇄망을 사용하였기 때문에 이러한 위협이 크게 문제가 되지 않았다. 하지만 개방된 네트워크의 사용으로 인하여 다양한 위협요인의 전달경로가 다원화됨에 따라, 스마트 그리드에서 사용되는 유·무선 통신 네트워크에서의 보안 취약성이 보안 이슈로서 제기되고 있다.

그리고 스마트 그리드의 기반 통신망의 일부 부분에 대해 접근성의 문제나, 비용의 문제 등으로 인하여 기존의 PLC나 BPL와 같은 전력선 기반의 통신 기술을 사용될 것으로 논의되고 있는데, 전력선 기반의 통신 기술에서는 기본적으로 전력선을 통하여 통신이 이루어지기 때문에, 각 장비들은 전력이 항상 연결된 상태로 특정 범위-셀(cell)을 구성하며, 이러한 특성으로 인하여 상시(always-on) 접속조건의 PC처럼 보안 위협에 대하여 노출되는 문제점을 가진다. 그리고 셀 가운데 취약성을 가지는 셀에 대한 공격이 성공하여 한 경우, 연결된 다른 셀에 대해서도 영향력을 미치기 때문에, 악의적인 공격자의 경우 장비 통제권 획득이 더욱 용이하게 되어 심각한 결과를 초래할 수 있으며, 이러한 공격에 대하여 기존의 유·무선 통신 네트워크와 같이 물리적인 차단을 통한 방어가 불가능하기 때문에 더욱 그 위험성이 크다고 할 수 있다. 또한, 항상 전력이 연결되어 있는 PLC상의 장비들이 인터넷 등의 개방형 통신 네트워크와 연결될 경우에는 앞서 언급한 네트워크 환경에서의 보안 취약성처럼 같이 보안에 대한 위험성을 내포하게 되기 때문에, PLC 셀에서의 보안 취약성도 보안 이슈로써 중요하다.

3.4 서비스 제공 사업자 영역

[그림 1]의 ④는 스마트 그리드에서 서비스를 제공하는 사업자의 영역으로, 이 영역에서는 전송받은 소비자의 데이터를 저장·처리·이용함으로써, 서비스 제공 사업자가 소비자에게 여러 가지 서비스를 제공한다. 여기서 서비스는 유틸리티에 의한 전력의 공급뿐만 아니라, 스마트 그리드와 관련된 여러 가지 사업에서 가능한 서비스를 포괄한다.

이러한 서비스에서의 데이터 흐름을 살펴보면, 소비

8) FTTH는 Fiber to the Home의 약어로 댁내광가입자망을 의미하며, HFC는 Hybrid Fiber Coax Architecture 광동축혼합망을, TDMA는 Time Division Multiple Access 시분할 다중접속 통신을, CDMA는 Code Division Multiple Access 코드분할 다중접속 통신을, VSAT는 Very Small Aperture Terminal Satellite 초소형지구국 위성통신을 의미한다.

자로부터 수집되어 전송된 데이터는 일차적으로 과금 산정 시스템에 활용되고, 미터 데이터웨어하우스에서 프로파일이 분석되며, 고객센터에서는 콜센터와 웹 등을 통해서 고객 맞춤형 서비스와 공급 제한 등 상황에 따른 처리가 이루어진다. 이러한 처리를 거쳐 생성된 정보 가운데 일부는 다시 소비자에게 전송되어 스마트 그리드에서 소비자의 참여를 활성화 하는데 이용되며, 일부는 비즈니스의 목적으로 서비스 제공자가 활용한다. 통상적으로 유틸리티는 비용 절감 및 수익 증대의 목적으로 원격검침, 정전관리(outage management), 부하예측(load forecasting), 인력관리, 사업계획 및 최대 부하 비용 산정(peak load billing) 등에서 사용할 수 있는 AMI 정보를 더 많이 수집하려고 노력한다.

이와 같은 활동이 이루어지는 서비스 제공 사업자 영역에서의 보안 이슈로는 'ⓐ 소비자 데이터의 소유권(ownership of comsumer data)', 'ⓑ 소비자 데이터에서의 프라이버시(privacy in comsumer data)', 'ⓒ 소비자의 전력사용에 대한 통제(control over power usage)'가 존재하며, 각각의 구체적인 내용은 다음과 같다.

첫 번째로 소비자 데이터에 대한 소유권이 누구에게 있는지에 대한 보안 이슈가 존재한다. 기존의 전력망에서 전력 데이터의 소유권은 유틸리티에게 귀속되었지만, 스마트 그리드에서의 소비자 데이터는 단순히 전력 사용 정보가 아닌 비즈니스 목적으로 소비자에 대한 분석이 가능한 데이터로 비즈니스 상 핵심 정보가 될 수 있기 때문에, 소비자 데이터의 소유권 관할과 관련하여, 기존 유틸리티 사업자와 신규 통신이나 서비스 사업자 간의 충돌이 예상되고 있다[15][16]. 또한 스마트 그리드에서 전송되는 소비자 데이터가 세밀화되면서 프라이버시까지 확대해석할 수 있는 정보가 포함되고 있기 때문에, 소비자 역시 소비자의 정보자기결정권과 관련하여, 소비자 데이터에 대한 접근권이나 통제권을 가지길 원하게 될 것으로 판단한다.

두 번째로 서비스 제공 사업자에 의한 소비자 데이터의 저장·이용·파기와 관련하여 프라이버시의 보안 이슈가 존재하는데, 이는 기존에 논의되었던 개인정보의 생명주기단계에서의 보안이슈와 거의 유사하다고 할 수 있다. 먼저 저장 단계와 관련하여, 서비스 제공 사업자가 소비자 데이터를 저장하기 때문에, 소비자 데이터 유출이나 임의적인 변조나 조작 등을 통한 프라이버시 침해의 가능성이 존재한다. 그리고 이용 단계와 관련하여, 서비스 제공 사업자가 소비자 데이터를 처리하거나 제3자에게 제공하는 경우에도 프라이버시 침해가 발생 가능하며, 파기 단계와 관련되어 소비자 데이터의 파기가 제대로 이루어지지 않은 경우에도 침해의 가능성이 존재한다.

세 번째로 유틸리티가 소비자 데이터의 분석을 통해 얻은 정보를 가지고, 소비자의 전력 사용에 대하여 통제하는 경우에 대한 보안 이슈가 존재하는데, 이는 앞서 스마트 제어의 영역에서와 거의 유사하게 보이지만 차이가 있다. 스마트 제어에서는 유틸리티의 통제권 침해에 대한 부분이 중점적인 이슈라면, 서비스 제공 사업장

〔표 2〕 스마트 그리드에서의 소비자 보안 이슈

구 분		보 안 이 슈
소비자정보의 흐름	스마트제어	• 소비자 및 스마트 전자제품의 인증 • 스마트 전자 제품에서의 소비자 데이터 수집 • 스마트 전자제품 간의 상호운영성 • 스마트 그리드에서 사용되는 무선 센서의 보안 취약성 • 소비자의 전력 사용에 대한 통제권
	AMI	• 스마트 미터기 기기 자체의 보안 취약성 • 스마트 미터기에서의 프라이버시 유·노출 • 스마트 미터기에 대한 접근통제
	기반통신	• 스마트 그리드에 도입되는 유·무선 통신 기술에 내재된 취약성 • 전력선 기반 통신 기술에서의 셀 보안 취약성
	서비스제공자	• 소비자 데이터의 수집, 이용, 처리 권한 (소유권, 관할권 등) • 소비자 데이터에서의 프라이버시 유·노출 • 저장된 소비자 데이터에 대한 접근통제 • 소비자 데이터의 처리 및 제3자 제공 등의 이용에 대한 고지 및 동의 • 소비자 데이터 파기의 보장 • 소비자의 전력사용 통제의 적법 근거
기 타		• 계약 상 소비자 보호의 사각지대

영역에서는 유틸리티의 통제 근거가 되는 데이터의 처리 과정의 적법성과 관련하여 보안 이슈로써 고려할 필요가 있다. 또한 해당 통제에 대한 접근제어 및 인증의 부분도 고려해야한다.

3.5 이외의 소비자 보안 이슈

스마트 그리드에서 소비자 참여의 비중이 크기 때문에, 앞서 살펴본 소비자 데이터 흐름에 따른 보안 이슈 외에도, 여러 가지 보안 이슈가 존재한다. 이를 간단히 살펴보면, 먼저 소비자와 서비스 제공 사업자간의 계약상의 보안 이슈가 존재한다. 이는 기존의 전력망에서는 소비자와 유틸리티간의 계약이 유틸리티는 전력을 제공하고, 소비자는 전력 이용에 대한 비용을 지불하는 단순한 형태를 취하였던 것과는 달리, 스마트 그리드에서는 소비자가 전력을 생산·판매하고, 유틸리티만이 아닌 통신이나 인터넷 서비스 제공 사업자 등이 복잡하게 얽혀 계약이 이루어지기 때문에, 소비자 보호의 측면에서 계약상 사각지대가 발생할 수 있다.

지금까지 살펴본 소비자의 보안 이슈는 기본적으로 소비자 프라이버시와 관련되며, 이를 표로 정리하면 다음 [표 2]와 같다.

Ⅳ. 스마트 그리드의 소비자 보안 이슈에 대한 기술·정책적 대응방안

앞서 살펴본 것과 같이 스마트 그리드에서의 소비자의 보안 이슈는 소비자의 전력 데이터에 대한 침해와 직·간접적으로 연결되며, 본 연구에서는 이러한 소비자에 대한 전력 데이터의 침해가 개인정보나 프라이버시의 침해로써 문제가 됨을 전제로 한다. 따라서 본 연구에서 스마트 그리드에서의 소비자 보안 이슈에 대한 대응방안을 논하기에 앞서 전력 데이터의 개인정보의 개념에 포함될 수 있는가를 확인하고, 이를 바탕으로 대응방안을 논의하도록 한다.

먼저 개인정보가 무엇을 의미하는 가를 국내법에서 찾아보면, 「공공기관의 개인정보보호에 관한 법률」에서 「생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)」라고 정의하고 있으며,[9] 이와 유사하게 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서는 「생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함)」로 정의하고 있다.[10] 즉, 개인정보는 특정 개인을 식별할 수 있는 정보와 더불어 다른 정보와 결합되어 개인의 식별이 가능한 정보를 의미하며, 이는 전통적인 프라이버시의 개념을 넘어 적극적인 정보 프라이버시의 개념까지 포괄함을 알 수 있다.

스마트 그리드에서 소비자의 전력 데이터는 기본적으로 과금을 위한 소비자 식별정보를 포함하는데, 이는 개인정보의 특징인 식별가능성을 가지고 있다고 볼 수 있으며, 전력 데이터만으로 특정 개인을 식별하지 못한다고 가정하더라도 다른 정보와 결합하여 개인을 식별하는데 이용될 수 있는 가능성을 가지고 있기 때문에 소비자의 전력 데이터는 포괄적인 의미에서 개인정보에 포함된다. 또한 본 연구에서 다루는 소비자의 전력 데이터에 대한 보안 이슈가 정보의 흐름에 따라 논의되고 있으며, 정보 프라이버시는 정보의 생산자와 소비자 간의 유통을 중요시하는 특성이 존재함을 고려하면, 소비자 전력 데이터가 정보 프라이버시의 개념에 포함될 수 있다고 판단한다. 따라서 [표 2]의 소비자 보안 이슈와 관련하여 발생하는 소비자 전력 데이터에 대한 침해를 곧 개인정보의 침해로써 확장하여, 이에 대한 대응방안을 기술적·정책적 대응방안을 고려하면 다음과 같다.

4.1 기술적 대응방안

스마트 그리드에서의 소비자 관련 보안 이슈가 전력 데이터와 관련된 각 기술에서의 보안 취약점으로 인해 존재하는 경우, 이에 대한 대응방안으로써 기술적인 보안 조치를 고려해야한다. 하지만 현재 스마트 그리드에서 사용되는 기술에 대한 명확한 세부사항이 정해지지 않았기 때문에, 본 연구에서는 구체적인 기술적 대응방

9) 「공공기관의 개인정보보호에 관한 법률」[법률 제8871호, 2008.2.29, 타법개정] 제2조 제2항에서 개인정보를 정의하고 있다.

10) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」[법률 제9244호, 2008.12.26, 일부개정] 제2장 제6항에서 개인정보를 정의하고 있다.

안보다 각 보안 이슈에서 요구되는 보안 요구사항을 바탕으로 현재 이러한 보안요구사항을 만족시킬 수 있는 기술적 보안조치를 제안함으로써, 차후 고려해야할 기술적 대응방안의 방향을 제시하도록 하겠다.

먼저, '소비자와 스마트 전자제품 간의 인증'의 보안 이슈와 관련하여, 상호인증기술 및 인증서시스템을 사용함으로써 스마트 그리드 내에 존재하는 스마트 전자제품에 대한 가용성을 보장할 수 있으며, '스마트 전자제품에서의 소비자 데이터 수집'과 관련하여, 데이터를 자동으로 수집하는 경우에 필터링이나 암호화 또는 개인화 설정을 통하여 수집되는 소비자 데이터를 최소화함으로써 소비자 데이터의 기밀성을 보장할 수 있다.

그리고 '스마트 전자제품 간의 상호운영성'을 위해 상호운영성과 관련된 표준과 상호운영성을 가능하게 하는 미들웨어 기술에 추가 가능한 보안 모듈을 개발함으로써 스마트 그리드의 가용성을 보장할 수 있으며, '스마트 그리드에서 사용되는 무선 센서의 보안 취약성'에 대해서는 센서에서도 암호화를 사용할 수 있도록 하는 경량 암호 및 센서 보안 네트워크를 개발함으로써 센서의 무결성 및 가용성을 보장할 수 있다.

또한 통제 신호에 대한 인증 및 로그 관리 시스템을 사용하여, 무결성 및 가용성을 보장할 수 있는데, 이는 '소비자의 전력 사용에 대한 통제권'의 이슈를 일부분 해결할 것으로 예상되며, 외부 공격에 강인한 스마트 미터기의 개발 및 스마트 미터기에 대한 안티 바이러스 등의 연구를 통해 '스마트 미터기 기기 자체의 보안 취약성'과 관련하여, 가용성을 보장할 수 있다.

'스마트 미터기에서의 프라이버시 유·노출'의 보안 이슈에서는 기밀성을 보장할 수 있도록 스마트 미터기에서 통합, 전송되는 정보에 대한 암호화 및 처리에 대한 보안조치가 요구되며, '스마트 미터기에 대한 접근통제'에서는 스마트 미터기에 대한 인증이나 로그 관리 등의 기술을 사용함으로써, 무결성 및 책임설명성을 보장할 수 있다.

'스마트 그리드에 도입되는 유·무선 통신 기술에 내재된 취약성'의 보안 이슈에서는 기존 통신망에서의 보안조치 -암호화, 인증, 전자서명 등이 그대로 사용되어, 기밀성·무결성·가용성·부인방지가 보장 가능하며, '전력선 기반 통신 기술에서의 셀 보안 취약성'에서는 셀 간의 위협 차단을 위한 기술 개발을 통해 가용성 및 무결성을 보장할 수 있다.

'소비자 데이터에서의 프라이버시 유·노출'의 보안 이슈에서는 소비자 데이터의 저장·처리·제공·파기와 관련하여, 무결성 및 기밀성의 보장을 위한 저장 매체의 암호화 및 장비에 대한 접근 통제와 접근에 대한 로그 관리, 침해를 최소화하는 데이터 처리 및 제공 메커니즘, 완전한 데이터 파기를 제공하는 메커니즘 등이 요구된다.

이러한 기술적 보안 조치 및 보안 요구사항을 통합·정리하면, 스마트 그리드에서 발생하는 소비자 보안 이슈는 일반적인 IT 보안 요구사항과 같이, '① 기밀성', '② 무결성', '③ 가용성', '④ 부인방지'가 요구되며, 인증, 암호화, 접근통제관리, 로그 관리 등과 같은 기존 보안 기술의 사용으로 이들 요구사항을 일정 부분 보장할 수 있다. 하지만 이러한 기존의 보안 기술이 그대로 스마트 그리드에 적용될 수 있는가가 문제이기 때문에, 스마트 그리드의 사업 추진에 따라 사용되는 기술이 명확하게 될 때까지는 특정 보안 기술의 개발보다는 스마트 그리드에 도입 가능한 보안 기술을 선별하여, 일차적인 문제 해결을 위한 대응방안으로써 사용하는 것이 바람직할 것으로 판단한다.

4.2 정책적 대응방안

다시 언급하지만 스마트 그리드의 사업이 초기 단계이기 때문에, 기술의 부분만 아니라 관련법이나 지침과 같은 정책적인 부분에서도 구체적인 대응방안을 언급하는 것은 시기상조일지 모른다. 하지만 스마트 그리드의 추진에서 관련법의 제정이나, 지침의 수립 시 사전적으로 대응방안을 고려함으로써, 보안 이슈와 관련된 문제를 사전에 예방할 수 있기 때문에, 이러한 법과 컴플라이언스의 측면에서 각 보안 이슈에 대한 정책적 대응방안을 제안하도록 하겠다.

4.2.1 스마트 그리드 관련법의 제정

먼저 스마트 그리드에서 발생 가능한 보안 이슈의 해결을 위해서 미국의 EISA와 같이 스마트 그리드와 관련된 법의 제정이 우선시 될 필요가 있다. 현재 국내에서도 '지능형 전력망 구축 추진위원회'에서 「지능형전력망촉진법(가칭)」을 준비 중이지만, 그 내용에서 아직까지는 보안과 관련된 규정이 없는 것으로 알려져 있다

[17]. 따라서 이러한 법의 제정 시 보안 관련 규정을 추가해야할 필요가 있으며, 이를 위해 [표 2]의 보안 이슈에서 요구되는 규정 사항을 나열하면 다음과 같다.

4.2.1.1 소비자 및 스마트 전자제품의 인증

먼저 앞서 기술적 대응방안에서 언급한 기술적 보안 조치를 뒷받침 할 수 있도록 법에서 근거를 규정해야한다. 이를 보안이슈와 연관하여 구체적으로 살펴보면, '소비자 및 스마트 전자제품의 인증'에서는 인증서 시스템 및 상호인증 기술의 도입을 추진할 수 있도록 인증이 필요한 대상 범위 및 그 근거를 규정할 필요가 있다.

4.2.1.2 소비자 데이터 보호 모델

개인의 식별이 가능한 소비자 데이터는 개인정보에 포함되고, 한국전력공사가 스마트 그리드의 사업자가 될 경우 「공공기관의 개인정보보호에 관한 법률」에 의하여,[11] 민간 기업이 운영자가 될 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의하여,[12] 사업자는 개인정보보호의 의무를 부담하게 된다. 한편, 제17대 국회에 이어 제18대 국회에서도 공공부문과 민간부문으로 나뉘어 규율되던 개인정보 보호 법제를 통합하자는 논의가 진행 중이어서, 멀지 않은 장래에 공공부문 및 민간부문을 아우르는 개인정보보호 입법이 탄생할 것으로 예상된다. 그러나 스마트 그리드에서 발생한 소비자 전력 데이터는 민감한 정보와는 거리가 있으며 이를 분석하는 등 특별한 가공을 거치기 전에는 프라이버시를 침해한다고 보기 어려운 반면, 시행착오를 줄이고 사업방향을 신속히 잡아가기 위해서는 피드백이 이루어져야 하므로, 소비자 데이터를 '개인정보 보호'의 원칙에 따라 보호할 경우 태동기에 있는 사업의 발전에 걸림돌로 작용할 것이 우려된다. 따라서 별도의 입법에 의하여 스마트 그리드에서의 소비자 데이터는 종래 개인정보 보호에 관한 기존의 법률의 적용을 받지 아니함을 명시하고, 그 수집, 처리, 이용절차에 관한 규정을 둘 필요가 있다.

이와 같은 측면에서 스마트 그리드 법에서는 원칙적으로 사업자는 소비자의 동의 없이 소비자 데이터를 수집, 처리, 이용할 수 있도록 하되, 이를 제3자에게 제공할 경우에만 소비자의 동의를 얻도록 하는, 다른 개인정보 보호법제와는 차별화된 정보보호 모델을 수립할 것이 요구된다. 이와 같은 경우에도 '소비자 데이터에서의 프라이버시 유·노출'과 관련하여 소비자 데이터의 취급 시 요구되는 기밀성 조건과 정보보호조치의무의 규율이 필요하다.

한편, '소비자의 정보 접근권 보장'에 대한 규정 및 소비자 데이터의 파기조건 및 기간, 파기의 예외 조건, 소비자의 파기 확인 방법 등이 규정되어야 할 것이다.

4.2.1.3 보안 및 접근통제

'스마트 미터기 기기 자체의 보안 취약성'에서는 스마트 미터기의 기능에 대한 제한 및 관련 사업자에 대한 규제를 위하여 규제 대상을 규정해야 하며, 그리고 '스마트 미터기에 대한 접근통제'에서는 스마트 미터기에 대한 임의적인 접근, 즉 공격에 대한 처벌을 규정할 필요가 있다.

4.2.1.4 소비자의 전력 사용 통제

'소비자의 전력 사용 통제'에 대해서는 전력 통제가 허용되는 경우 및 이에 대한 고지 및 동의 획득, 통제에 대한 협상과 보상, 통제가 감시 등에 이용되지 않음에 대한 보장 등에 대하여 규정이 요구된다. 또한 '계약 상 소비자 보호의 사각지대'와 관련하여, 소비자의 참여가 기본적으로 전기 사용과 관련된 계약 상 약관에 의거하는 바, 약관에 대한 규정이 요구된다. 특히, 스마트 그리드가 현재 법상에서 「전기사업법」이나 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등에 중복 적용되

---

11) 「공공기관의 개인정보보호에 관한 법률」
제1조 (목적) 이 법은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다.
제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "공공기관"이라 함은 국가행정기관·지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관을 말한다.
「공공기관의 개인정보보호에 관한 법률 시행령」
제2조 (적용대상) 「공공기관의 개인정보보호에 관한 법률」 제2조제1호에서 "대통령령이 정하는 기관"이라 함은 다음 각 호의 기관을 말한다. (1~2, 4생략)
3. 특별법에 의하여 설립된 특수법인
현재 국내 스마트 그리드에서 전력 공급 사업자인 한국전력공사는 특별법인 「한국전력공사법」에 의하여 설립된 특수법인이다.

12) 다만, 스마트 그리드가 전력공급 사업을 주된 내용으로 할 경우 정보통신망법의 적용대상인 정보통신서비스 제공자 혹은 준용사업자(동법 제67조)에 해당한다고 보기 어렵다.

는 바가 적지 않기 때문에, 이를 통합할 수 있는 규정이 요구된다고 할 수 있다.

4.2.1.5 소결론

이와 같이 법에서 규정되어야 할 것으로 도출된 내용은 「전기사업법」에서의 사용자 보호 조항[13]이나, 「소비자기본법」과 「전자상거래 등에서의 소비자 보호에 관한 법률」에서의 소비자 보호 조항[14]과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「공공기관의 개인정보보호에 관한 법률」의 개인정보 보호 조항[15]과 거의 유사하다. 기존의 법률에서 이러한 내용이 존재함에도 불구하고 스마트 그리드 관련 법률 제정으로 규정의 명시가 요구되는 이유는 스마트 그리드가 광범위에 걸쳐 추진되고 있기 때문이다. 즉, 여러 사업자가 동시에 참여하고 있기 때문에, 각각의 법에 의거하여 규제하는 것이 어렵고, 또한 규제의 사각지대가 발생할 수 있기 때문에, 이를 미연에 방지하기 위해서 스마트 그리드 관련 법률의 제정이 요구된다고 할 수 있다. 그리고 이러한 스마트 그리드 관련법의 제정에 있어서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 같이, 법률명에서 '정보보호'와 같이 보안의 의미를 넣음으로써, 스마트 그리드에서의 보안의 중요성을 강조할 필요가 있다.

13) 「전기사업법」[법률 제9244호, 2008.12.26, 일부개정]에서는 전기 사용자 보호와 관련하여 제4조 (전기사용자의 보호), 제21조 (금지행위) 등이 규정되어있으며, 전기 사용과 관련하여 제16조 (전기의 공급약관), 제18조 (전기품질의 유지), 제20조 (전기설비의 이용제공) 등에서 전기 이용의 보호에 대하여 규정하고 있다.

14) 「소비자기본법」에서는 소비자 보호와 관련하여 제4조 (소비자의 기본적 권리), 제8조 (위해의 방지), 제13조 (소비자에의 정보제공), 제19조 (사업자의 책무), 제20조 (소비자의 권익증진 관련기준의 준수), 제45조 (취약계층의 보호) 등이 규정되어 있으며, 특히 제15조 (개인정보의 보호)에서 소비자의 개인정보보호에 대하여 규정하고 있다. 「전자상거래 등에서의 소비자 보호에 관한 법률」에서는 제6조 (거래기록의 보존 등), 제7조 (조작실수 등의 방지), 제11조 (소비자에 관한 정보의 이용 등), 제21조 (금지행위) 등에서 소비자 보호를 규정하고 있다.

15) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 개인정보보호에 대한 조항으로 제24조 (개인정보의 이용제한), 제24조의2 (개인정보의 제공 동의 등), 제28조 (개인정보의 보호조치), 제29조 (개인정보의 파기), 제47조의3 (이용자의 정보보호) 등이 규정되어 있으며, 「공공기관의 개인정보보호에 관한 법률」에서는 제3조의2 (개인정보보호의 원칙), 제4조 (개인정보의 수집), 제7조의2 (개인정보보호방침), 제9조 (개인정보의 안전성확보등), 제10조 (처리정보의 이용 및 제공의 제한), 제10조의2 (개인정보파일의 파기) 등에서 개인정보의 보호에 대하여 규정하고 있다.

4.2.2 자율 규제를 위한 컴플라이언스의 수립

그리고 스마트 그리드와 관련된 사업자가 여러 분야에 걸쳐 존재하기 때문에 법에 의해 규제할 수 있는 대상의 한계가 존재한다. 따라서 앞서 고려한 스마트 그리드에 대한 관련법에서의 보안 규정 외에, 스마트 그리드 관련 사업자가 자율규제를 통하여 소비자의 보안 이슈를 해결할 수 있도록 사업자가 준수해야할 사항에 대한 컴플라이언스를 수립할 필요가 있다. 컴플라이언스에는 기본적으로 스마트 그리드 사업자가 컴플라이언스 준수를 위한 관련 시스템의 구축과 데이터 보관체계 등을 의무적으로 갖출 것과 함께, 관련된 모든 기록의 보유와 파기에 대해 비즈니스 라이프사이클에 따라 체계적으로 관리할 것을 포함하고 있어야 한다. 특히 본 연구에서는 소비자 보호에 초점을 두고 있기 때문에, 자율 규제를 위한 소비자 보호 지침에 포함되어야할 내용은 다음과 같다.

먼저, 스마트 그리드 관련 사업자의 의무와 관련하여 보유하고 있는 소비자 데이터의 통제를 명시해야한다. 세부적으로 ① 사업자가 보유하는 소비자 데이터 별 보유 근거 및 목적과 이용범위를 고지해야함, ② 사업자가 데이터 수집 시 소비자의 동의나 법률근거에 따라 수집해야함, ③ 소비자가 자신의 데이터 수집에 대한 세부 내용을 확인할 수 있도록 조치해야함, ④ 사업자가 업무 수행에 필요한 범위 및 기간에 한하여 소비자 데이터를 보유해야함, ⑤ 소비자 데이터 처리나 송·수신시 안전성 확보를 위한 조치를 마련해야함, ⑥ 처리정보 이용·제공시 최소한 범위로 제한하고, 정보주체의 동의 없이 제 3자에게 제공하지 못하도록 해야 함, ⑦ 다른 기관에 제공하는 개인정보가 존재하는 경우 그 현황과, 소비자 데이터의 처리에 관한 사무를 위탁한 경우 그 위탁 사항, 그리고 보유목적 달성 및 보유가 불필요한 경우 파기 및 파기 내용을 명시해야함 등의 내용이 소비자 보호 지침으로서 컴플라이언스가 수립되어야 한다.

4.2 결 론

스마트 그리드에서의 소비자 참여와 관련된 보안 이

슈를 해결하기 위해서는 앞서 논의한 바와 같이 기술적·정책적 대응방안이 요구된다. 스마트 그리드가 아직 기술적인 측면에서 많은 발전이 이루어 질 것으로 예상되기 때문에, 기술적 대응방안은 기술의 발전에 따라 지속적으로 연구가 요구된다. 따라서 현 상황에서는 기술적인 대응방안보다는 정책적 대응방안이 시급하며, 이 가운데에서도 가장 중요한 것은 스마트 그리드 관련 법의 제정이라 할 수 있다.

V. 향후 연구방향

스마트 그리드가 가능하기 위해서는 무엇보다도 보안이 보장되어야 함에도 불구하고, 아직까지는 스마트 그리드에 대한 관심에 비해 보안의 고려가 미흡한 상태이다. 아직 스마트 그리드가 실체적인 모습을 갖추는 초기 단계이고, 스마트 그리드에서 사용될 기술들 또한 한창 논의·개발 중임을 고려하면, 아직 스마트 그리드에서 요구되는 보안 요구사항 등을 논의하는 것은 시기상조일지 모르지만, 보안의 고려가 초기에부터 동반되지 않는다면, 차후 문제 상황이 발생하였을 때 피해의 복구가 어려울 수 있기 때문에, 본 연구와 같은 보안의 논의가 스마트 그리드의 개발과 더불어 동반되어야 한다고 생각한다.

본 연구에서는 스마트 그리드에서의 소비자 참여와 관련된 보안 이슈에 대한 고찰과 더불어 기술적·정책적 대응방안에 대한 방향을 제시함으로써, 스마트 그리드의 보안에 대한 접근의 단초가 될 수 있을 것으로 판단한다. 향후에는 스마트 그리드에서 논의되고 있는 기술들에서의 보안 요구사항을 분석하고, 이를 실제 연구개발에 적용할 수 있기 위한 정책 방안에 대하여 연구함으로써, 스마트 그리드에서의 보안을 보다 실체적으로 보장하고, 이를 통해 스마트 그리드의 추진에 있어서 보안이 장애물이 아니라, 활성화의 동인으로써 중요성이 강조될 수 있도록 할 필요가 있다.

참고문헌

[1] Fred Sissine, "Energy Independence and Security Act of 2007: A Summary of Major Provisions", *CRS Report for Congress*, RL34294, December 2007.

[2] European Technology Platform, "SmartGrids: Strategic Deployment Document for Europe's Electricity Networks of the Future", September 2008.

[3] 지식경제부, "세계최초 Smart Grid(지능형 전력망) 구축을 위한 상세 로드맵 수립착수", 지식경제부 전력산업과 보도자료, 2009년 3월 31일.

[4] 정해춘, "전력IT 전문 요원 양성이 Smart Grid 성공의 열쇠", 디지털파워 뉴스 글로벌 해외동향, 2009년 5월 1일. http://www.dpn21.com/news/articleView.html?idxno=1855.

[5] Amy Abel, "Smart Grid Provisions in H.R. 6, 110th Congress", *CRS Report for Congress*, RL34288, February 2008.

[6] National Energy Technology Laboratory, "A Systems View of the Modern Grid", January 2007.

[7] Department of Energy, "The SMART GRID: An Introduction.", April 2009.

[8] European Technology Platform, "Strategic Research Agenda for Europe's Electricity Networks of the Future", 2007.

[9] Research Reports International, *The Technology of the Smart Grid*, Research Reports International, January 2008.

[10] IOActive, "IOActive verifies critical flaws in Next-Generation Energy Infrastructure", March 2009. http://www.ioactive.com/pdfs/AMIPressRelease032309.pdf.

[11] Mark F. Foley, "The Dangers of Meter Data", SmartGridNews, June 2008. http://www.smartgridnews.com/artman/publish/industry/The_Dangers_of_Meter_Data_Part_1.html.

[12] Wilmer Heck, "Smart energy meter will not be compulsory", April 2009. http://www.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory.

[13] Jeanne Meserve, "'Smart Grid' may be vulnerable to hackers", CNN News, March 2009. http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/.

[14] National Energy Technology Laboratory, "Appendix B1: Integrated Communications", February 2007.

[15] Jeff St. John, "Utilities Brief California Energy Commission on Smart Grid Efforts", May 2009. http://www.greentechmedia.com/articles/read/utilities-brief-california-energy-commission-on-smart-grid-efforts-4672/.

[16] Katie Fehrenbacher, "Will the Microsoft-Google Battle Move to Energy Data?", May 2009. http://earth2tech.com/2009/05/21/will-the-microsoft-google-battle-move-to-energy-data/.

[17] 지식경제부, "한국형 스마트 그리드 비전(Smart Energy Green Revolution) 논의", 지식경제부 전력산업과 보도자료, 2009년 6월 4일.

〈著者紹介〉

이 경 복 (Kyungbok Lee)

2008년 2월: 고려대학교 산업시스템정보공학과 졸업
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 개인정보보호, 스마트 그리드 보안, e-Discovery

독고지은 (JiEuin Dokko)

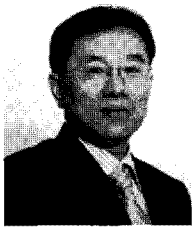
1996년: 동아대학교 사학과 졸업
2008년 9월~현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 개인정보보호, 디지털 포렌식

유 지 연 (Jiyeon Yoo)

1995년 2월: 상명대학교 일어교육과 졸업
1999년 2월: 상명대학교 정보통신학과 석사
2008년 2월~현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 방송통신정책, 방송통신융합, 정보보호

이 숙 연 (Sook-Yeon Lee)

1991년 2월: 포항공과대학교 산업공학과 졸업
1995년 2월: 고려대학교 법학과 졸업
1998년 2월: 고려대학교 법학과 석사
2007년 9월~현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 정보보호, 정보보안, 저작권, 특허, 사이버법률



임 종 인 (Jong-in Lim)

종신회원

1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장 (고려대학교 정보보호연구원 원장 겸임), 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원 등
<관심분야> 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등