情 報 保 護 學 會 誌
第20卷 第3號, 2010. 6

스마트 그리드에서의 프라이버시 보호

박 남 제*, 안 길 준**

요 약

최근 그린 IT에 대한 관심이 고조되면서 저탄소 녹색성장의 완성을 위해 지능형 전력망으로 불리는 스마트 그리드(Smart Grid) 기술을 도입하여 빠른 환경 변화에 한발 앞서가고 있다. 스마트 그리드를 통해 전력망이 진화하고 있지만 사이버 공격과 비고의적인 위험노출에 대한 우려도 일각에서 제기되고 있는 상황이다. 전력망이 갈수록 복잡해지고 서로 연결됨에 따라 유틸리티 공급업체의 사이버 보안 위협을 위한 노력이 점차로 중요하게 될 것이다. 이에 본 연구에서는 스마트 그리드의 개인정보보호 필요성과 침해 유형들을 살펴보고, 스마트 그리드에서의 프라이버시 보호에 대한 고려사항과 보호 제공방안을 고찰하도록 한다.

Ⅰ. 서 론

현재 국내외적으로 사회적 이슈 가운데 하나가 녹색성장(Green Growth)이다. 지구온난화의 문제로 이산화탄소(CO_2) 배출을 줄이기 위한 산업적 노력과 이와 관련된 기술 및 산업을 성장 동력의 기회로 만들자는 취지가 녹색성장이다[9]. 오늘날 글로벌 경쟁이 치열해 지는 상황에서 시장 선점의 효과는 어느 때보다 중요해지고 있어 새로운 시장 변화에 대한 인식을 바탕으로 신기술 개발을 통해 경쟁력을 갖추어 나가야 할 때이다. 우리나라는 산업전략 및 '뉴 IT(Information Technology) 전략' 실행계획의 일환으로 IT 분야 녹색성장 전략인 '그린 IT 전략'을 발표했다[16]. 그린 IT 국가전략은 단순한 IT 강국을 넘어 글로벌 그린 IT 선도국으로의 도약을 목표로 하고 있다. 그린 IT는 IT 제품 및 서비스의 라이프 사이클 전반을 녹색화하고, 신성장 동력으로 육성하는 IT부문의 녹색화(Green of IT)와 IT 융합으로 에너지 및 자원의 효율적 이용을 극대화하여 저탄소 사회 전환을 촉진하고, 실시간 환경 감시 및 조기 재난대응 체계를 마련하여 기후 변화에 대한 대응 역량을 강화하는 'IT 융합에 의한 녹색화'를 포괄적으로 의미한다[12].

이러한 그린 IT 실현을 위한 주요 기술의 하나로 스마트 그리드(Smart Grid)가 주목을 받고 있다. 스마트 그리드는 전기 에너지의 효율적 사용을 목적으로 전력망에 IT기술을 도입 및 융합하여 전력의 송·배전을 지능화하는 지능형 전력망을 뜻한다[7,8]. 스마트 그리드 시스템은 공급자, 네트워크, 소비자 간의 에너지 송·배전에 대한 연계, 자동화 및 조정 가능성을 높인다. 스마트 그리드 기술은 소비자의 에너지 사용을 실시간으로 감시하고 비사용 기간 동안(예를 들어 보다 많은 전력자원이 필요한 근무일 동안) 차단 요구에 응답할 가정용 기기와 통신함으로써, 에너지 효율을 가정으로까지 확대해 준다. 이로써 소비자들은 에너지 사용을 보다 효과적으로 조절할 수 있게 된다. 스마트 그리드는 전자통신 분야의 NGN(Next Generation Network, 차세대 통신망)과 다르지 않다. 스마트 그리드는 '단순 파이프(dumb pipe)'의 시대에서 '스마트 파이프(smart pipe)'의 시대로, 그리고 사물 스스로 식별하고 정보를 교환하는 '사물의 인터넷(Internet of things)' 시대로의 근본적인 전환을 의미한다.

스마트 그리드 시스템은 에너지 효율을 크게 높일 수

This work was supported in part by the funds provided by the National Science Foundation(NSF) under Grant NSF-IIS-0242393 and the Department of Energy(DOE) Early Career Principal Investigator Award under Grant DE-FG02-03ER25565.

* Arizona State University, Computer Science and Engineering, Research Scientist (namjepark@asu.edu, namjepark@gmail.com)
** Arizona State University, Computer Science and Engineering, Associate Professor (ahn@asu.edu)

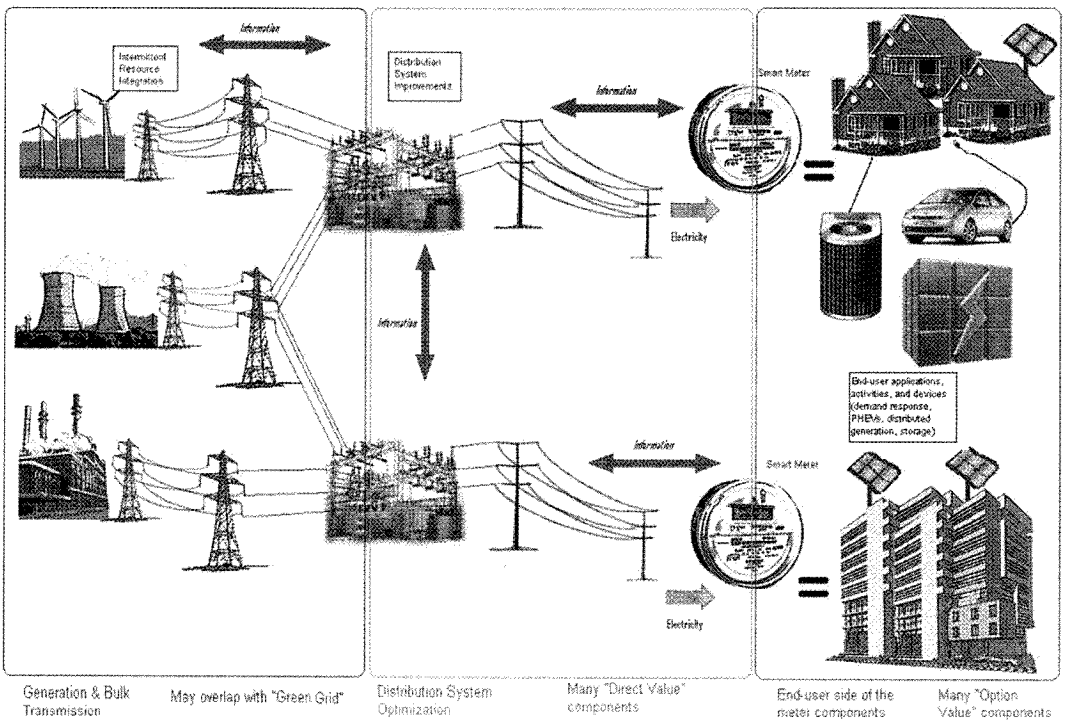
있다. 하지만 스마트 그리드 시스템의 개발에는 여러 기회와 혜택도 존재하지만 동시에 사생활 침해의 우려도 있다. 소비자들의 상세한 전력 사용 내역이 자동 전송됨에 따라 개인 정보의 유출 가능성이 발생되거나 개인의 에너지 사용에 대한 정보가 경찰이나 보험회사 등의 제3자에게 유출될 위험 요소가 존재하는 등의 스마트 그리드의 프라이버시(개인정보 노출) 문제에 대한 논란이 발생할 수 있다. 또한 불법적인 데이터 위·변조 공격 등으로 전력 운영체계와 스마트 미터기(Smart energy meter)를 제어한다거나, 봇(bot)이나 웜(worm) 등의 악성코드를 이용한 분산 서비스 거부(DDoS, Distributed DoS) 공격 가능성 및 전력 제어시스템이 인터넷과 연동될 경우, 외부에서 인터넷의 취약성을 이용하여 제어시스템으로의 침투 가능성이 존재하는 등의 스마트 그리드의 사이버 보안 위협이 발생할 수 있다. 이에, 스마트 그리드의 보안 체계로서 송·배전 보호, AMI (Advanced Metering Infrastructure, 고도화된 검침 기반 시설, 지능형 원격검침)·서비스 보안, 보안관제 기술, 보안기반 기술, 시스템 보안기술 등의 체계화된 보안 프레임워크 기술 연구와 보안에 대한 법, 제도, 조직, 기술 등의 정보보호정책 관점에서의 지원방안이 필요하다.

이에, 본 고에서는 녹색성장을 위하여 정부에서 추진하고 있는 그린 IT 전략 중 스마트 그리드 기술에서 개인정보보호의 요소를 살펴보고, 프라이버시 보호 필요성과 침해의 유형에 대해 분석한다. 그리고, 스마트 그리드의 프라이버시 보호에 대한 고려사항과 보호 제공 방안에 대해 기술한다. 본 연구는 녹색 성장을 위한 전략 수립단계에서 스마트 그리드 보안 및 사용자의 프라이버시 보호에 대한 중요성을 제시하는 것을 목표로 작성되었다.

Ⅱ. 스마트 그리드 개요 및 주요 특징

2.1 스마트 그리드 개요

스마트 그리드란 IT 기반의 미래형 차세대 전력망으로 센서, 통신 네트워크, 자동제어 등의 IT 기술을 전력망에 도입함으로써 전력 인프라의 융통성, 보안성, 신뢰성, 효율성, 안전성 등을 향상시키고, 전력의 생산 및 소비정보를 유틸리티와 소비자 간의 양방향, 실시간 통신



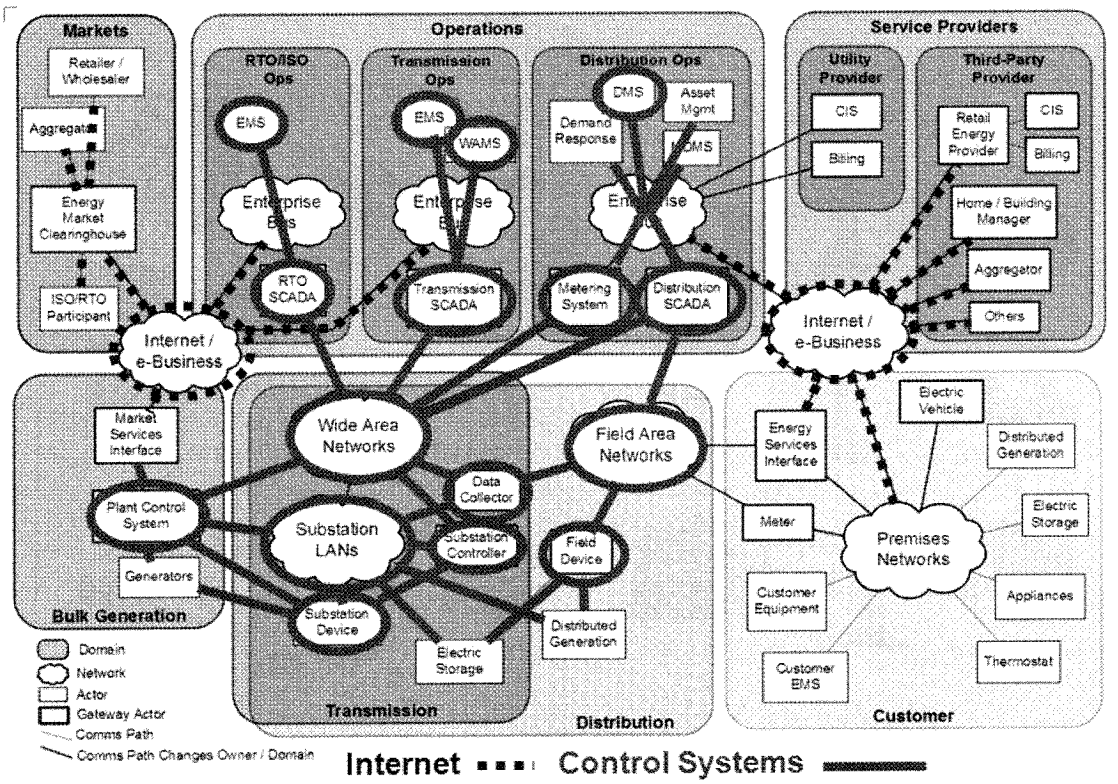
〔그림 1〕 일반적인 스마트 그리드의 구성도[5]

을 가능하게 함으로써 에너지 효율을 최적화하는 차세대 전력망 기술이다[7,8]. 이는 '발전-송전·배전-판매'의 단계로 이루어지던 기존의 단방향 전력망에 정보기술을 접목하여 전력 공급자와 소비자 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 지능형 전력망을 의미한다. 발전소와 송전·배전 시설과 전력 소비자를 정보통신망으로 연결하고 양방향으로 공유하는 정보를 통하여 전력시스템 전체가 하나의 체계 내에서 효율적으로 작동하도록 설계한다[10]. 이 기술을 통하여 전력 낭비를 줄이는 동시에 재생에너지 사용을 활성화하고 이산화탄소 배출도 줄여 지구 온난화 방지에도 효과가 있어 선진국들의 관심과 투자가 이루어지고 있다.

[그림 1]은 전기의 생산과 공급, 제어를 위한 통신 네트워크와 센서 시스템, 각종 지능형 설비, 계측 장비 등을 망라한 통합 네트워크로 구성되는 일반적인 스마트 그리드 구조를 보여주고 있다[5]. 위의 [그림 1]과 같이 스마트 그리드에서는 양방향으로 통합된 통신기술(Communication)이 가장 기반되는 핵심 기반 기술이며, 이러한 통신 기술을 바탕으로 스마트 미터기와 관련된 미터링(Metering) 기술, 전력의 송·배전과 관련되는 고급 제어 기술(Advanced Control), 그리고 정보의 효과적인 전달과 기기간의 호환성을 위한 인터페이스(Interface)가 스마트 그리드를 구성한다고 볼 수 있다. 가정 및 빌딩에 설치된 여러 개의 스마트 미터기에 의해 실시간으로 에너지 사용량이 측정되고 사용자 데이터는 정보 수집 장치에 의해 전력사업자의 서버로 전송되어 수집 및 처리된다. 이렇게 처리된 사용량 정보는 목적에 따라 여러 형태의 정보로 분석 및 가공되어 다시 사용자의 가정 및 빌딩 내부에 있는 단말기로 보내져서 사용자는 이를 통해 자신의 전력 사용량과 요금 정보를 실시간으로 확인할 수 있다.

2.2 IT 기반 스마트 그리드의 주요 특징

스마트 그리드에서 IT는 스마트 그리드의 특징인 자기 복구(Self-healing), 수요반응(Demand Response),



〔그림 2〕 스마트 그리드의 통신 및 제어 시스템들의 구조[28]

〔표 1〕 IT기반 스마트 그리드의 주요 특징

특 징	내 용
자기 복구	• 신뢰도, 보안성, 가용성, 전력품질 및 효율적인 전력망 상태 유지 • 정기적 혹은 자동적으로 전력망의 장치나 네트워크 섹션 탐지 및 분석
능동적인 사용자의 참여	• 사용자는 구성요소로서 능동적인 참여 가능
보안 공격에 대한 대항	• 통합 사이버 보안에 대한 서비스 제시 • 보안을 설계단계에서부터 체계적 구현
21C의 고품질 전력 제공	• 발전 및 송·배전 부하에서 안전한 전력 공급
다양한 발전원 수용	• 분산 전원에서 단순화된 연계과정을 가지며 다양한 발전원을 수용
전력 시장 활성화	• 시장의 개방적인 접근성을 갖도록 설계 • 전력시장을 전력시스템 구조안으로 통합
자산 최적화 및 효율적 운영	• 최소 비용 유지위해 자산 이용률 최적화 관리 운영 • 고정 검출 및 시정조치 시간의 최소화

보안, 전력 품질보장, 그리고 전력 거래 등을 실현시키는 필수 도구이며, 양방향 유·무선 통합 통신망, 센서 네트워크, 알고리즘 기반 관리, 프레임워크 S/W 등의 IT 기술이 전력망의 지능화를 가능하게 한다[19].

[그림 2]는 스마트 그리드의 주요 기능별로 그룹화한 것으로 파란 점선은 다양한 스마트 그리드 요소시스템들과 인터넷 통신을 하는 것을 의미하며[28], 빨간 실선은 통신상의 산업 제어 시스템들이 전력의 생성, 전송 및 배포에 사용되는 다양한 제어 기능으로 운용되는 것을 뜻한다. 스마트 그리드 분야는 전력과 IT 기술을 융합하여 다양한 서비스를 가능하게 하는 AMI 시스템은 물론이고, 발전, 송전 및 배전망의 전력계통 고도화, 신재생 에너지의 활용, 전기자동차 등 에너지 및 환경 관련하여 이슈가 되고 있는 기술들 중 전기와 관련된 모든 것에 직·간접적으로 관계를 맺고 있다[35]. 미국 에너지부 DOE(Department of Energy) 산하의 국립 에너지 기술연구소(National Energy Technology Laboratory, NETL)에서 수행한 전력송전분야에 대한 연구인 MGI (Modern Grid Initiative)에서는 시스템 관점에서 스마트 그리드가 가져야할 기본적인 요소 및 주요 특징을 언급하고 있다[17]. 그 주요 내용은 아래 [표 1]과 같다.

스마트 그리드는 IT 기술의 비중이 매우 높으나 네트워크, IT소자·부품, 네트워크·시스템·사용자 보안 및 소프트웨어 기술 등 IT 기반 인프라 및 기술 연계가 아직은 미흡한 것으로 판단되고 있으며 기존 IT기반 연구의 연계 강화 및 보완 연구를 통한 스마트 그리드 핵심기술 개발이 추진되어야 한다[8]. 미국 상무성 산하의 표준기술연구소(NIST)에서 발표한 '스마트 그리드 상호 운용성을 위한 프레임워크와 로드맵 (2009.10)'[7]에서 우선적으로 표준화 대상이 되는 이슈들인 Priority Action Plans(PAP)의 많은 부분도 IT 인프라의 상호 운용성, 특히, 수용가단 HAN(Home Area Network) 기술에 대한 항목으로 구성되고 있다. 또한, 발전 설비에서 생산된 전력은 송전 설비를 통해 전달되며, 효율적 전달을 위해 변전 설비와 배전 설비를 통해 이용자에게 전달된다. 발전, 송/변전, 배전 설비들은 EMS (Energy Management System), SCADA(Supervisory Control And Data Acquisition), DAS(Distribution Automation System) 등에 의해 운영센터 IT 시스템에서 통제된다. 수용가들의 전력 사용 등에 대한 과금 및 사용자 관리 등은 서비스 제공자에 의해 수행되며, 전력의 도소매 시장 등의 역할로 구분된다. 이처럼 IT 인프라는 스마트 그리드 플랫폼을 구성하는 주요 구성요소이다.

현재까지 전력망은 폐쇄형, 단독망 운영관리로 보안이 크게 문제되지 않았지만, IT가 결합됨에 따라 정보통신 네트워크 기기에서 발생하고 있는 보안 문제가 나타날 수 있는 우려가 높다. 고객의 프라이버시 노출, 정보 도용, 사용요금 조작은 물론, 전력 시스템의 마비까지 기존 전력망에서 나타나지 않았던 새로운 보안 위협의 가능성이 나타난다. 스마트 그리드의 대상이 국가주요기반시설인 전력망이기 때문에, 스마트 그리드의 추진에 있어 주요기반시설보호 등의 보안이 중요한 요소로 고려될 필요가 있으며, 스마트 가전제품 보안, 측정/제어 정보 무결성(integrity), 장치간 상호인증, 크로스 서비스 공격, 분산 서비스 거부 공격(DDoS) 방지, 제어 시스템의 침해사고 탐지/대응/복구 등의 보안 대책이 필요하다. 또한, 스마트 그리드 전반적으로 새로운 국면의 기술적인 보안 대책이 마련되어야 함은 물론, 스마트 그리드 구축과정으로부터 밀착성 있게 구현되어야 한다.

Ⅲ. 개인 정보와 스마트 그리드

3.1 스마트 그리드에서의 개인정보

'개인 정보'란 개인 신상에 관한 모든 기록을 말한다.

개인의 이름, 연락처와 신상 정보뿐만 아니라, 이 개인의 선호, 거래 이력, 활동이나 여행 기록, 또는 프로필이나 점수와 같은 전자에서 파생된 정보, 그리고 가족, 친구, 동료와 같은 개인의 파일에 첨부될 수 있는 기타 관련 정보가 포함될 수 있다. 스마트 그리드의 맥락에서, 에너지 사용과 개인적으로 식별 가능한 정보를 연계하면 개인 정보로서 또 하나의 연계된 정보가 생성된다. 기존 그리드의 현대화는(제3자와 유틸리티 공급자에 의한 개인정보 수집, 사용, 공개를 늘리는 경향이 있는) 최종 사용자와 관련된 요소 및 활동과 관련이 있다[3]. 이러한 요소와 활동의 내용을 살펴보면 다음과 같다.

3.1.1 스마트 미터기(Smart meter)

스마트 미터기란 전력 계량기에 수십~수백미터 반경의 근거리 무선 기능을 넣어 다양한 전력기기들을 설치한 가정이나 사무실 내의 설비 기기에 접속함으로써 전력 계량기를 개입시켜 기기의 가동상황 등을 네트워크 공유로 전력회사가 관리할 수 있는 시스템을 말한다. 즉, 전력 소비 정보를 자동으로 기록하고 보고하는 계량기이다. 스마트 미터기는 기존 계량기보다 세밀하게 소비를 식별하고, 모니터링 및 결제 목적으로 다시 그 정보를 전기 유틸리티 업체에 전달한다. 스마트 미터기는 유틸리티 업체와 그리드의 배전 구성요소 사이의 상호작용 측면에서, 매일/매시 또는 실시간으로 정보를 연계한다. 스마트 미터기는 변조나 위조에 강하고, 원격으로 접속 또는 단속이 가능하며, 무단 철거 및 미터기 우회 사용뿐만 아니라 정전 감지가 용이하다. 또한 정보는 유선 또는 무선을 통해 유틸리티 공급자에게 전송될 수 있다. 미국에서는 830만 대 이상의 스마트 미터기가 이미 설치되었고 그 수가 2012년이 되면 5200만에 이를 것으로 예상되고 있다.

3.1.2 스마트 가전제품(Smart appliances)

스마트 가전제품은 효율적이고 보다 생산적인 사용을 위해 최종 사용자가 유틸리티 사업자에게 정보를 직접 전달하도록 구성될 것이다. 스마트 제품장치에 대한 소비자의 투자로 추후 에너지 소비에 대한 비용이 절감될 수 있다. 스마트 기기에는 온도계, 세탁기, 건조기, 전자레인지, 온수 히터, 냉장고가 포함된다. 예를 들어, 스마트 온수기에는 에너지 가격을 기준으로 지정된 한도 내에서 온도를 제어하기 위해 시설의 에너지 관리 시스템과 조율하는 장치가 장착될 수 있다. 이를 동적 요금제(Dynamic Pricing)라고 한다.

다수의 가전제품이 어느 정도의 에너지를 사용하고 있는지 보여주기 위해 이들 가전제품은 전력망과 자주 교신하도록 설계되어 있을 뿐만 아니라, 가격 인센티브를 이해하고 이에 대응하도록 설계되며, 이로써 가전제품의 사용 및 상태에 대한 상세한 정보가 제공되게 된다. 몇몇 주요 가전제품 제조사들은 이미 스마트 그리드에 사용할 수 있는 기기를 개발 중이다. 제너럴 일렉트릭(GE, General Electric) 회사는 2009년 말까지 스마트 온수기를 도입할 예정이고 향후 수년에 걸쳐 각 가전제품의 스마트 버전을 내놓을 예정이다. 또한, 월풀(Whirlpool) 회사는 2011년까지 100만 대의 스마트 건조기를 생산할 예정이다[24].

이러한 가전제품들은 높은 전력이 요구될 때 자동으로 전기를 끌 수 있고, 스마트 미터기와 교신하게 될 소프트웨어도 갖추게 될 것이다. 소비자가 비용 효율적인 방식으로 전력을 사용할 수 있도록 계층별 전기요금 책정 방식과 연계하여 기술이 진보해나갈 것이다.

3.1.3 동적 요금제(Dynamic pricing)

동적 요금제는 일종의 경제적 인센티브로서, 이들 인센티브에 대한 소비자의 반응을 '수요 참여(demand participation)' 또는 '수요 반응(demand response)'이라 부른다. 동적 요금제는 현재 또는 미래의 특정 기간에 대한 요금 정보를 소비자에게 제공하는 기술을 사용하여 고객이 이 요금 정보에 따라 자신의 수요를 수정할 수 있게 한다. 동적 요금제는 다음의 형태를 취할 수 있다.

- 사용시간 요금제(Time-of-use pricing): 에너지 가격은 미리 지정된 피크 시간대에 더 높다.
- 크리티컬 피크 요금제(Critical peak pricing): 가장 큰 피크 시간대가 식별되고 이 시간대에는 훨씬 더 높은 요금 수준이 부과된다. 높은 가격의 총 시간은 사용시간에 비해 적다.
- 실시간 요금제(Real-time pricing): 요금은 에너지 구입을 위한 유틸리티 비용에 의거 시간에 따라 달라진다.

3.1.4 소비자의 에너지 관련 정보 접근(Consumer access)

소비자들은 에너지 요금 정보, 자신의 사용 현황 및 기타 에너지 관련 정보에 대한 접근이 가능해질 것이다. 기업은 소비자들이 비용 절약과 환경에 대한 안목을 가지고 전기 사용량을 모니터링할 수 있도록 에너지 사용 추적 도구와 소프트웨어 프로그램을 개발하고 있다(예: Google의 PowerMeter, MS의 Hohm, GridPoint회사 등). 전기 공급자들은 자신들의 고객 웹 인터페이스도 설정하고 있다.

3.1.5 부하 관리(Load management)

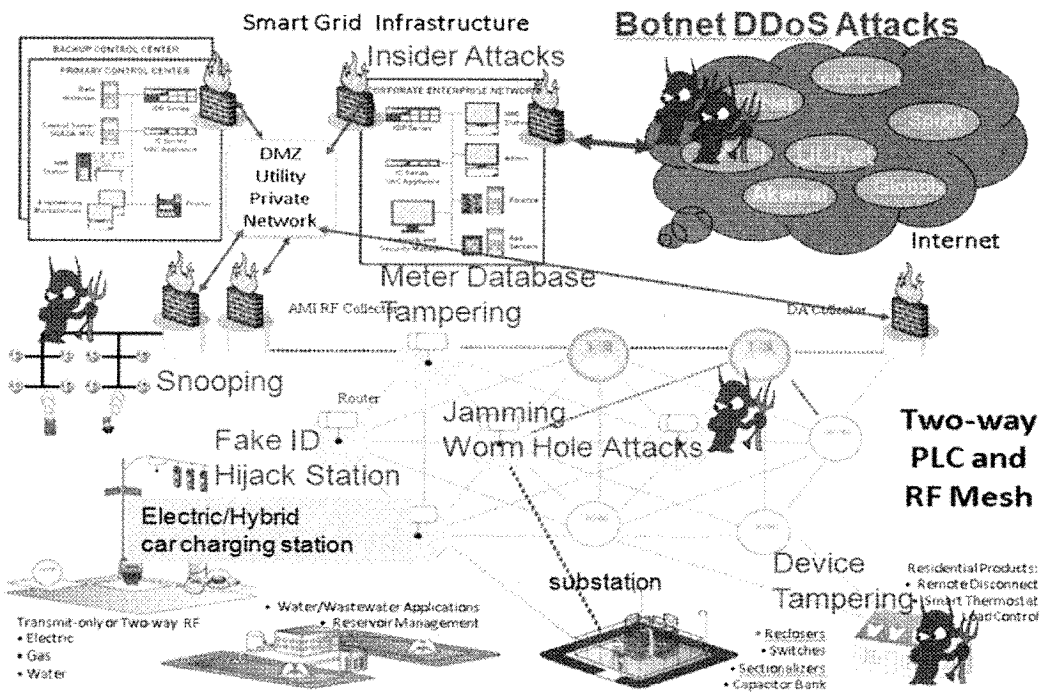
부하 관리를 통해 에어컨, 온수기, 수영장 펌프와 같은 고객 스마트 가전제품의 능동 및 피동 제어가 이루어진다. 그리하여 피크 에너지 수요 기간 중에 전기를 줄이거나 원활화할 수 있을 것이다.

3.2 프라이버시 보호 필요성

정보기술을 접목한 미래의 전력망 기술로 주목받고 있는 스마트 그리드의 취약한 보안성을 종합적으로 진단한 미국의 민관합동보고서가 발표됐다. 미국 표준기술연구소(NIST)는 최근 정보와 업계, 학계 및 사정기관 관계자들로 구성된 사이버보안 합동 태스크포스의 예비보고서를 공개했다[20]. 자국이 추진 중인 스마트 그리드를 보안성과 사생활보호 측면에서 분석한 이 보고서는 공개 열람을 거쳐 올해 2월 스마트 그리드 보안체계와 요건을 종합한 최종판이 나왔다. 예비보고서는 공격자가 스마트 그리드에 침투해 제어 소프트웨어를 접수한 뒤 로드 조건을 변경해 전국적인 전력 대란을 일으킬 수도 있다고 경고하고 있다. 이 보고서는 또 스마트 그리드를 보호하는 사이버 보안 전략은 고의적인 공격뿐만 아니라 사용자 오류, 장비고장 및 소프트웨어 버그에 의한 비고의적인 위험노출도 대처할 수 있게끔 구성되어져야 한다고 권고하고 있다. 특히 스마트 그리드가 사생활에 끼치는 영향을 '프라이버시 영향분석' 항목에 따로 취합해 놓았다.

3.2.1 비고의적인 위험노출의 문제

미국 컨설팅사 아이큐액티브(IQActive)는 2009년 6



[그림 3] 스마트 그리드의 일반적인 보안 취약점 요소[6]

월 스마트 그리드 구성요소의 보안 취약성을 조사한 결과를 발표하고 공격자가 망에 접근해 전력을 차단할 수 있는 스마트 그리드의 허점을 몇 가지로 정리했다. 공격자가 계량기의 결함을 이용해 전력망에 악성코드를 퍼뜨림으로써 원격으로 전력을 끊어버릴 수도 있다고 그 조사보고서는 예시했다[14]. 그리고, 이러한 위험인자를 구체적으로 분석한 것이 위에서 언급한 NIST의 보고서[20]이다. 이 NIST 보고서는 연구소 자체의 산업 제어 시스템에 대한 지침과 OWASP(Open Web Application Security Project)의 취약성 목록을 비롯하여 스마트 그리드의 보안과 관련한 각종 문건들을 토대로 취약성 목록을 총정리해 놓고 있다. 일반적으로 알려진 스마트 그리드 구조상의 보안 취약점을 살펴보면 다음 [그림 3]과 같다[6].

3.2.2 실시간 양방향 통신에 허점

미국표준기술연구소(NIST) 보고서[20]는 스마트 그리드 운용중에 발생할 수 있는 보안 취약성뿐만 아니라 변전소의 사용자 인증, 미터기의 열쇠관리, 발전 장비의 침입방지 등과 같은 문제점들도 함께 살피고 있다. 또한 부적절한 패치, 설정 및 변경관리 프로세스와 허술한 접근제어, 위험성 심사와 감사, 관리 및 사고대책의 부재에 따른 취약성까지 보고서는 고찰하고 있다. 이와 아울러 입력 검증오류와 사용자 인증 오류 등 소프트웨어 코딩의 잘못된 관행 역시 스마트 그리드의 무결성에 흠집을 낼 수 있다고 보고서는 지적하고 있다[14,20]. 보고서는 "지금의 전력망은 요금청구에 필요한 기본적인 내용만 계량기에서 확인하는 체계"라고 전제한 뒤 "스마트 그리드에서는 스마트 미터기에서 다른 데이터까지 수집할 수 있다"며 여기에 포함되는 개인정보가 사생활 보호 측면에서 엄격하게 관리되어야 할 것이라고 결론짓고 있다.

3.3 스마트 그리드의 사생활 침해

3.3.1 개인정보보호에 대한 우려

스마트 그리드의 현대화에 따라 가용한 개인정보의 상세 수준뿐만 아니라 개인정보의 수집 사례, 사용 및 유출의 수준이 높아지고 있다. 각 요금청구 기간 말미에 에너지 사용을 측정하는 대신에 스마트 미터기가 보다 단시간 간격으로 이 정보를 제공할 것이다. 전기 사용이 매분 또는 가전제품 차원에서 기록되지 않더라도, 거주자가 내부에 있을 경우뿐만 아니라 깨어 있을 때 또는 자고 있을 때 대략적인 거주자 수 등의 정보가 전기 소비의 지속적인 모니터링을 통해 수집될 수 있다. 이 문제는 사적인 일상생활은 공개되어서는 안 된다는 '가정의 신성함(sanctity of the home)'과 관련된 문제로 많은 사람들의 공감을 얻게 될 것이다[3].

스마트 그리드의 프라이버시를 다루는 일, 특히 소비자와 유틸리티 정보 교환 영역을 담당하고 있는 사이버 보안 조정 작업그룹 산하 개인정보보호정책 하위 그룹의 프라이버시 영향평가(PIA, Privacy Impact Assessment)에 따르면, 미국의 스마트 그리드와 관련하여 많은 개인정보 누출 대한 우려와 문제가 존재한다고 한다. 프라이버시 영향평가(PIA)에는 다음과 같은 내용이 서술되어 있다[19,20].

- 스마트 그리드의 개인정보 보호와 관련된 사항이 아직 완전히 이해되지 않았다.
- 스마트 그리드 및 정보 수집에 참여하는 업체들의 공식적인 개인정보 보호 정책, 표준, 또는 절차가 부족하다.
- 유틸리티 업계에 개인 식별 정보의 포괄적이고 일관성 있는 정의가 존재하지 않는다.
- 분산된 에너지 자원 및 스마트 미터기로 인해 집안에 거주하는 소비자 및 그의 활동에 대한 정보가 공개될 것이다.
- 친구의 집에서 충전 중인 전기 자동차와 같은 스마트 그리드 기기의 로밍으로 인해, 추가적인 개인 정보가 유출될 수 있다.
- 스마트 미터기 및 스마트 그리드 네트워크가 다양한 방식으로 개인 신상정보를 사용할 수 있을 것이다.
- 개인정보보호 원칙의 채택을 촉구하는 국가전력규제위원협회가 채택한 2000년의 결의안에도 불구하고, 소수의 주 차원의 위원회들이 개인정보보호 문제와 스마트 그리드를 평가하기 시작했다.
- 추가적인 연구가 필요하고 추가적인 PIA를 실시하는 것이 중요하다.

개인적인 습관, 행동 및 주거지 내에서의 개인 생활

양식 등 개인적인 정보를 들추어낼 가능성이 있을 경우 그리고 전기 공급 이외의 이차적 목적으로 정보를 활용하기 위해서, 개인정보 보호 문제가 제기된다. 전기 유틸리티와 기타 공급 업체들은 고객이 무얼 사용하고 있는지, 언제 그것을 사용하고 있는지, 그리고 어느 기기가 그것에 관련되는지에 대한 정보에 접근할 수 있다. 전기 사용 프로필이 세부적으로 고객의 행동 정보에 관한 소스가 될 수 있다. 예를 들어, 최종 사용자 관련 요소의 도입으로 다음과 같은 정보가 수집될 수 있다(이러한 문제는 가전제품과 기기들이 전력망의 일부가 됨에 따라 보다 가시적인 우려가 될 것이다): 사람들이 전자렌지를 이용한 간편 식사를 하는 경향, 사람들이 아침식사를 하는 경향, 사람들이 집에 있는 시간, 집에 경고시스템이 있는지 여부, 어느 정도의 빈도로 이 경고시스템이 울리는지, 거주자가 일반적으로 언제 샤워를 하는지, TV 및 컴퓨터는 언제 켜는지, 가전제품들은 양호한 상태인지, 집에 있는 전기 장치의 개수, 집에 세탁기와 건조기가 있는지 여부 및 어느 정도의 빈도로 사용되고 있는지, 전등과 가전제품들이 한밤중과 같은 일반적인 시간외에 사용되는지, 러닝머신과 같은 운동기구는 어느 정도의 빈도로 사용되는지와 같은 정보. 일하는 장소 및 시간, 자녀가 있는지 여부 등의 다른 정보와 조합하여, 위와 같은 정보로부터 사용자에 대한 추측을 할 수 있게 된다. 예를 들면, 다음과 같은 추측이 가능하다. 집 주인은 술집 문이 닫히면 곧바로 집에 도착하는 경향이 있다. 이 사람은 수면이 불안정하고 수면 부족을 겪고 있다. 거주자는 출근이 늦다. 일하는 동안 자주 가전제품을 켜 둔다. 거주자는 좀처럼 자기 옷을 빨지 않는다. 이 사람은 자신의 아이들을 홀로 집에 둔다. 거주자는 아주 가끔 운동을 한다[21].

원래 수집했던 기본 목적 이외에 정보를 사용할 경우, 개인정보보호의 관점에서 특별한 고려가 필요하다. 이러한 정보를 익명화하여 식별 가능한 고객 수준으로 또는 집계 형태로 에너지 사용량이나 가전제품 정보와 같은 서로 다른 데이터 상품과 그러한 정보를 묶음으로 만들어지는 문제점이 생길 수 있다. 기타 문제점으로는 다른 서비스에 대한 동의를 구하기 위해 정보를 사용하는 유틸리티 업체와 제삼자, 그리고 상업적 이익을 위해 (예를 들어 타깃 광고) 사용자를 참여시키고자 하는 제3자가 있을 수 있다. 비록 우리의 주요 관심사가 개인적으로 식별 가능한 정보에 있지만, 익명화된 정보도 여전히 개인정보 보호와 관련된 문제가 될 수 있다. 행동광고 분야의 경우에서와 마찬가지로, 사용자를 개인 기반으로 다르게 취급하거나 시장에 이용할 수 있게 되면서 강화된 개인정보 보호에 대한 필요성이 제기된다[22]. 또한, 일부 조사자들이 사용자에 대한 비개인적 정보가 최소한이라도 있다면 사용자 식별이 어렵지 않다는 내용을 정리한 바 있다[23].

아직까지 누가 사용자의 개인정보에 접근할 수 있을 것인지, 그리고 전력망의 어느 지점에서 이 접근이 허용될 것인지는 분명치 않다. 일부 유틸리티 업체들은 전력망 관리를 위해 기기 수준의 전기 사용 정보에 대한 필요성이나 바람은 갖고 있지 않다고 표명했다. 일부 현 스마트 그리드 환경에서, 일부 소비자들은 이미 자신의 전기 사용에 대한 정보를 받기 시작했다. 만약 이러한 정보가 더욱 구체화될 경우(즉, 소득, 연령, 가구 규모 등으로 세분화), 더욱 세분화된 정보의 유포가 가지는 혜택과 동시에 위험이 존재한다. 상당수의 미국 주 정부는 이미 유틸리티 업체에 대한 관련 규정을 갖추고 있다. 그러나 아직까지는 이러한 새로운 정보가 현재의 규제 체제 하에서 어떻게 취급되어야 할지는 명확하지 않다. [그림 2]에서 볼 수 있는 바와 같이 스마트 그리드의 방대한 정보 공유 구성요소가 주어진 이 시점에서, 이러한 개인정보의 접근과 취급의 가능성에 대해 앞으로 많은 연구가 필요하다.

스마트 그리드 개인 정보가 개인의 동의 없이 그 개인에 대한 중요한 의사결정을 하는 데 사용될 수 있다는 우려가 있다(보험 리스크 결정 등). 결과적으로, 스마트 그리드로 전력망을 현대화하는 데 있어서 소비자의 신뢰를 얻는 것이 관건이 될 것이다. 미래의 스마트 그리드는 스마트 기술을 사용하고 투자하는 소비자에게 달려 있기 때문에, 스마트 그리드 자체는 소비자들이 그러한 시간과 투자의 가치를 알아보도록 할 수 있느냐에 달려 있다. 만약 스마트 그리드 및 스마트 가전제품들이 개인정보 침해에 계속해서 노출된다면, 스마트 그리드의 미래는 더디거나 어쩌면 아예 미루어지게 될 수 있다. 이에, 스마트 그리드에 대한 구체적인 개인정보보호 방안이 필요하다.

3.3.2 프라이버시 침해 예시

미국 표준기술연구소(NIST)의 스마트 그리드 사이버

보안 전략 및 요구사항의 관계기관 합동보고서(U.S.)[20]에 참여한 한 관계자는 스마트 그리드 기술 표준을 개발할 때 검토해야 할 15가지 프라이버시 침해 우려에 대해서 지적했다[4,40]. 스마트 그리드에서의 정보공개 및 오용과 관련한 프라이버시 침해의 예시는 다음과 같다.

① 신원 도용(**Identity theft**)

개인 신상정보(PII, Personally Identifiable Information)의 특정 조합이 유틸리티 소비자를 사칭하는 데 사용되어, 부정적인 신용 보고, 부정 유틸리티 사용 및 기타 소비자 활동에 해를 입히는 행위 등 심각한 피해를 야기할 수 있다.

② 개인행동의 패턴 식별

가정 내 특정 영역에서 전력 사용의 구체적인 때와 장소를 드러낼 수 있는 정보 사용 프로파일에 대한 접근을 통해서, 소비자 활동의 유형 및 사용한 가전제품들이 무엇인지 알아낼 수 있다. 드러나는 정보로 일종의 감시를 할 수 있는 셈이다. 이러한 정보는 특정 회사가 타깃 마케팅을 하거나, 정부가 특정 활동과 사용에 대한 세금을 부과하거나, 악의적 의도를 가진 개인이 사용(오용)할 수 있다.

③ 사용 가전제품의 식별

앞으로 스마트 미터기의 정보를 활용하여 스마트 미터기와 통신하도록 프로그램된 특정 스마트 가전제품의 사용을 추적할 수 있게 된다. 가전제품 제조업체들은 자사 제품을 누가, 어떻게 그리고 왜 사용하는지를 알기 위해 이러한 정보를 얻으려 할 것이다. 이러한 정보가 가전제품의 보증에 영향을 미칠 수도 있다. 보험사들은 고객의 보험 청구를 승인하거나 거절하는 데 이 정보를 활용하려 할 수도 있다. 게다가 아직은 미처 생각하지 못한 이 정보의 활용 분야는 무수히 많이 존재한다.

④ 실시간 감시 수행

에너지 사용에 대한 실시간 정보에 대한 접근으로, 개인이 주거지에 있는지, 무얼 하고 있는지, 구체적으로 주거지 내 어디에 있는지 등의 정보를 밝힐 수 있다. 이러한 정보는 사유재산을 위협하는 자들에 의해 개인의 재산을 갈취하거나 파괴하는 데 사용될 수 있고, 가정의 에너지 사용 행동을 기반으로 한 타깃 마케팅에 활용될 수도 있다.

⑤ 잔류 정보로 인한 스마트 미터기 소유자의 활동 노출

스마트 미터기의 정보가 효과적으로 또는 완전히 지워지지 않을 경우 이러한 잔류 정보로 인해 차후 이 스마트 미터기를 소유하는 새로운 사용자 또는 회사에게 이전 소유자의 활동 내역이 노출될 수 있다고 경고하는 기사들이 많이 발표되었다. 이것이 사실이라면 앞서 언급한 3가지 유사한 우려 사항이 발생할 수 있다. 또한 행동주의자들이 사회적 책임감 결여라는 자신들의 주장을 피력하는 데 이러한 정보를 활용할 수도 있다. 그러나 과거 정보의 변조를 막고(동일한 물리적 계량기함 내에 보다 많은 기능을 부여함으로써) 신규 계량기의 크기 제약을 해소하기 위해, 스마트 미터기 자체 내에 정보를 저장할 것 같지는 않다. 하지만 스마트 미터기 기능 설계 시 가정용 계량기 내에 정보를 저장할 가능성을 고려하여, 스마트 미터기에 개인 신상정보(PII)를 저장하는 것이 가능해 진다면 개인정보보호 문제를 검토해야 할 것이다

⑥ 특정 가정을 타깃으로 한 침입

특정 소비자의 스마트 미터기 정보를 악의적으로 활용하면 실제로 그 가정에 침입하는 등 여러 가지 문제가 발생할 수 있다. 미터기 정보를 통해 거주자가 언제 집을 비우는지, 경보 시스템이 있는지 등을 침입자 확인할 수 있기 때문이다.

⑦ 의도치 않은 침입

어떤 목적으로 스마트 미터기의 정보를 분석할 때 거주자에 관한 뜻밖의 정보를 공개하게 될 수 있는데 이로써 거주자들이 피해를 입게 될 수 있다.

⑧ 사용자 활동의 검열

스마트 미터기 정보로 거주자의 활동이나 사용 내역이 공개되면, 유틸리티 업체는 거주자의 그러한 활동이나 사용이 적절한 것인지 혹은 이를 금해야 할지를 판단할 수 있게 된다. 또한 이 정보를 아무런 제약 없이 지방정부, 법률기관 또는 공공매체가 공유하게 되면, 주민들은 당혹감이나 모욕감을 느낄 수 있고, 중요한 가전제품의 손실이나 기타 여러 피해를 주는 행위를 겪게 될 수 있다.

⑨ 부정확한 정보에 기초한 결정 및 조치

스마트미터기 정보를 여러 위치에 저장하고 수많은 개인과 회사가 접근하여 다양한 목적으로 사용한다면, 개인 신상정보를 부적절하게 변경할 위험이 존재한다. 가정 에너지의 사용에 대한 스마트 그리드의 자동화된 결정은(자동으로 전력을 제한하거나 자동으로 온도를 위험 수준으로 변경하는 등) 주민에게 해를 입힐 수 있고, 이러한 스마트 그리드 전력 사용 및 활동에 대한 결정도 부정확한 정보에 기초하여 내려질 수 있다.

⑩ 다른 유틸리티 정보와 혼용될 경우의 정보 누출

스마트 미터기의 개인 신상정보가 다른 유틸리티 및 유틸리티 계량기(가스, 수도 등)의 개인 신상정보와 혼용될 경우, 훨씬 더 사적인 활동과 개인 신상정보가 공개될 수 있다.

⑪ 프로파일링(**Profiling**)

이전에는 불가능했던 또는 쉽게 할 수 없었던 방식으로 프로파일링이 가능할 수도 있다. 에너지 소비로부터 얻을 수 있는 정보를 어떻게 활용할 수 있는지 살펴보면 다음과 같다. 예를 들어, 소비자가 일반적 침해자인지? 혹은 테러리스트인지?, 또는 불륜 혹은 그의 불법활동 조사를 위한 정보수집 목적의 정보 접근으로 그 사람을 테러리스트 감시 목록에 올리게 될까?, 정치인들이 소비자의 잠재적인 활동에 세금을 부과하기 위해 정보를 활용하고자 할까? 등의 차이점 분석을 수행하면 관련된 위험과 시나리오를 짚어낼 수 있을 것이다.

⑫ 원치 않는 공개와 당혹감

가전제품 사용 또는 전기 자동차 사용 내역의 무단 유출 및 공개로 인해, 소비자는 당혹감을 느낄 수 있고 기타 부정적인 영향을 받을 수 있다.

⑬ 세입자의 추적 행동

전세, 월세 등의 경우와 같이 집 주인 외의 개인이 유틸리티를 소유하여 결제를 하는 경우, 집 주인이 스마트 미터기 정보에 접근할 수 있고 세입자의 활동을 추적할 수 있다. 결국, 집 주인은 세입자의 과거 전력 사용 내역을 바탕으로 차후 임대를 해줄지를 결정할 수 있다. 전력 사용 프로파일링이 개인을 따라다닐 수도 있고 광범위한 결정에 영향을 줄 수 있다.

⑭ 행동 추적(**Behavior Tracking**)

스마트 그리드 내에 브라우저/문서 쿠키 또는 웹 버그와 유사한 항목이 있을 수 있다. 만약 그렇다면, 쿠키와 웹 버그가 현재 사용(오용)되는 것처럼 이들 항목도 그럴 수 있을 것이다. 어쩌면 RFID(Radio Frequency IDentification) 태그가 어떤 방식으로든 사용 될 것이며, GPS(Global Positioning System) 유형의 기술 또한 그러할 것이다.

⑮ 개별 행동을 드러내는 공공 집계 검색

스마트 그리드 검색 엔진으로는 어떤 유형이 있을까?, 이 가능성을 중심으로 어떤 토론이나 계획이 벌어지고 있는가?, 어떤 정보들이 여기에 관련되는가?, 이러한 검색에 자신들의 정보가 포함되지 않도록 하기 위해 소비자들은 어떠한 장치를 가지고 있는가?, 등 스마트 그리드 개인정보보호 문제는 현재 인터넷 검색엔진의 개인정보보호 문제와 유사할 것이다. 게다가 스마트 그리드 관련 정보는 개인이 의도적으로 인터넷에 올리려고 선택한 것이 아닌 이들의 실제 일상생활 활동을 담은 것이기 때문에 영향력이 더 클 것이다.

Ⅳ. 스마트 그리드에 대한 개인정보보호 방안

4.1 프라이버시 보호에 대한 고려사항

스마트 그리드 기술을 통해서 방대한 양의 소비자 정보를 얻을 수 있다는 것은 분명하다. 유틸리티 회사, 스마트 가전제품 제조사, 추가 소비자 상호작용에 대한 정보를 얻고자 하는 제3자 등, 관련 정보를 사용하고자 하는 잠재된 주체들이 상당수 존재한다. 더욱이, 스마트 미터기, 통합 홈네트워크 및 가전제품을 통해 수집할 수 있는 정보는 상당한 가치를 지닌다[2]. 예를 들어, 스마트 그리드 시스템은 진보된 브로드밴드와 정보 흐름 측정 기능을 통합할 수 있는데 이 기능은 개인의 전기 사용량이 얼마인지, 어느 방에서 가장 많은 전기를 사용하는지, 그리고 언제/얼마나 자주 사용하는지에 관한 정보를 수집할 수 있다. 이 자료를 가지고 있는 유틸리티 회사들은 부하 요구량을 보다 잘 관리할 수 있고 보다 효율적인 배전 시스템을 창출할 수 있을 것이다. 또한, 기기 제조사들은 자신들의 기기가 어떻게 사용되는지에 대해 보다 잘 이해할 수 있게 되어 더 나은 고객 서비스

를 전달할 수 있게 될 것이다. 그러나 이러한 스마트 그리드의 특징은 어느 회사가 개별 사용자 정보에 대한 접근권을 가질지 그리고 개별 기기들의 확인 또는 추적이 가능할 것인지에 대한 의문을 자아낸다.

유틸리티 회사와 기기 제조사를 포함한 잠재적 스마트 그리드 정보 사용자들은 소비자의 신뢰와 믿음을 구축하는 책임있는 정보 관리 관행에 참여해야 한다. 이들은 스스로 소비자와 지속적인 관계를 맺는다는 사실을 인식해야 하고, 이러한 관계를 유지하고 스마트 그리드 에코시스템을 성장시키려면 소비자의 변함없는 믿음이 반드시 필요하다는 사실을 인식해야 한다. 이러한 변함없는 믿음은 소비자들이 자신의 스마트 그리드 개인 정보가 어떻게 사용되는지 충분한 정보를 입수하고 그러한 정보가 통제된 상태에서 사용되고 있다고 느낄 경우에만 얻어질 수 있다. 따라서 스마트 그리드 정보 사용자들은 소비자의 사용 패턴으로부터 얻은 스마트 그리드 정보의 무결성, 기밀성과 보안성을 어떻게 보호할 것인지 신중히 생각해야 하고, 지나치게 많은 정보를 수집하지 않도록 해야 한다. 또한 스마트 그리드 정보를 수집할 때에는 책임감을 가지고 안전하게 그리고 투명성과 소비자 통제에 대한 조치를 갖춘 상태에서 수행해야 한다. 이러한 원칙은(다른 무엇보다도 먼저) RFID 시스템과 사물 인터넷(Internet of things)에 적용될 유럽에서 익히 알려져 있다.

소비자들이 자신의 정보가 어떻게 사용되는가에 대한 확신을 갖게 될 경우에만 스마트 그리드 기술이 결정적으로 성장할 수 있을 것이다. 소비자의 행동 습관에 관한 정보가 안전할 것이며 오직 소비자의 이해와 동의를 얻은 목적에만 사용된다는 사실을 소비자에게 보증해 주어야 한다. 아울러 소비자는 정보가 어떻게 사용되는지 충분히 알아야 하고, 정보의 부적절한 사용이나 유포가 방지된다는 확신이 있어야 한다. 만약 이러한 요구조건이 충족된다면 소비자들은 진보된 스마트 그리드 기술을 수용할 가능성이 더 클 것이다. 이러한 책임있는 정보관리 관행 없이는 스마트 그리드 기술에 대한 소비자의 저항과 스마트 그리드 구축 노력을 저해할 수 있는 소비자의 신뢰 상실이 있을 수 있으며, 결국 신상품에 대한 낮은 수요와 혁신 감소로 이어져 기기 제조사들도 스마트 그리드 에코시스템을 떠나게 될 것이다.

지금까지, 규제기관과 기기 제조사들은 스마트 그리드 기술에서 전파될 정보의 소유권이 소비자에게 있다는 점과, 그래서 예상치 않은 정보의 사용이나 공유가 있으면 소비자들에게 승인을 요청해야 한다는 점을 분명히 하고 있다. 사실, ePrivacy 지침의 특별 규정을 따르게 될 정보통신 네트워크의 트래픽 정보와 전기 사용 정보 간에는 몇 가지 유사점을 찾아 볼 수 있다. 그러나 정보사용에 대한 승인 요청을 하기가 어렵고 심지어 사용자에게 정보관리 정책을 전달하는 것조차 힘든 일일 수 있다. 소비자들이 스마트 그리드 기술을 자신의 가정과 삶에 도입하는 것과 관련하여, 이러한 개인정보 문제에 관한 의사결정을 내리는 것에 대한 정보를 소비자에게 전달하는 최선의 방법을 조사하는 연구가 필요하며, 스마트 그리드 기술의 'opt-in'과 'opt-out' 간에 적절한 균형이 이루어질 필요가 있다. 유틸리티 사와 제조업체들은 프라이버시 친화 설계의 원칙들을 정보 인프라 구축 시 통합시켜야 한다. 이러한 원칙들로 인해, 수백만 달러가 지출되기 전에 그리고 스마트 그리드 기술이 보급되기 전에 개인정보 보호정책의 핵심 우려사항이 고려될 수 있다.

규제기관은 스마트 정보사용에 대한 강력한 개인정보 보호정책 요구사항에 대한 필요성을 부각시킴으로써 긍정적인 실천이 이루어지도록 장려해야 한다. 또한 규제기관은 유틸리티 업체, 기기 제조업체, 소비자 단체, 개인정보 보호 옹호자를 포함한 모든 스마트 그리드 이해관계자들로 하여금 적절한 개인정보 보호정책과 정보보안 관리를 유지하기 위한 그리고 소비자에게 스마트 그리드 정보의 수집 및 사용의 충분한 통제와 투명성을 부여하기 위한 모범사례를 개발하도록 격려해야 한다.

모든 스마트 그리드 정보의 사용은 개인정보 보호정책 및 보안 원칙을 확고히 한 상태에서 실시되어야 한다. 스마트 그리드 정보와 정보통신 네트워크의 트래픽 정보 취급이 얼마나 달라야 하는지 혹은 반대로 얼마나 조화를 이루어야 하는지에 대한 고찰이 필요하며, 일련의 일관된 원칙을 세우기 위해 노력해야 한다.

4.2 프라이버시 보호 해결 접근 방안

요즈음 전력망에 지능적으로 연결된 온라인 탄소 계산기가 어떻게 모든 사회문제의 해결책이 되는지에 관해 많은 관심들을 갖고 있다. 심지어 GE 회사는 TV에서도 스마트 그리드를 광고하고 있다. 그러나 우리의 정보가 담긴 데이터가 큰 서비스 프레임워크에서 어떻게

통합되어야 하는지, 얼마나 많은 정보를 전력망에 보내야 하는지에 대해 의문이 제기되고 있다. 비즈니스위크의 게스트 컬럼, "What the Smart Grid Can Learn From Facebook Connect"의 저자인 Celeste LeCompte는 스마트 그리드와 사업이 연결되는 방식과 사람들이 소셜 마케팅(social marketing) 툴을 사용하는 방식 간에는 같은 성질이 있다고 주장하였다[26,27].

소셜 마케팅 웹 툴을 고려할 때 갖게 되는 질문은 그 웹 툴이 연합(federation)에 의존하느냐 혹은 집합(aggregation)에 의존하느냐이다. 다시 말해, 웹 툴이 우리의 개인적 데이터에 선별적으로 연결되는가 혹은 그 웹 툴이 모든 정보를 한데 모아 다루는가이다. LeCompte는 스마트 그리드에서는 Facebook Connect와 같은 연방적 접근법(federated approach)이 보다 프라이버시를 보호하는데 도움이 된다고 말한다. 페이스북은 Facebook Connect에서 콘텐츠를 연방화시킴으로써 프라이버시 문제를 완화시키고 있다. Facebook Connect를 이용하게 되면 사용자가 공개된 웹을 서핑하면서, 그의 프라이버시 설정이 항상 그를 따라다닌다. 그리고 사용자의 정보와 프라이버시 규칙이 항상 업데이트된다. 예를 들어 한 사용자가 자신의 프로파일 사진을 바꾸거나 친구 연결을 삭제한다면 외부 사이트에도 자동으로 업데이트된다. 그리고 사용자는 누가 그들 정보의 어떤 부분을 봤는지도 알 수 있다.

LeCompte는 한 월풀(Whirlpool)회사의 스마트 가전기기를 예로 들며, 그 기기가 어떻게 전력망에서 나오는 정보에 기반하여 의사결정을 하는지 지적하였다. 여기에는 전력망이 그 기기를 통제하지 않고, 소비자가 그 기기에 관련해 어떤 의사결정을 하였는지도 누설하지 않는다. LeCompte는 그런 연방적 접근방식 하에 전력서비스업체, 장비제조업체, 소비자 모두 민감한 정보를 공유하지 않고, 그들 스스로 필요한 특정 정보만을 접속할 수 있다고 말한다. 유사하게 한 회사가 전력망에 연결되어 있다면, 그 회사는 자사에 해를 끼치지 않는 정보만을 노출하고 싶어 할 것이다.

4.3 스마트 그리드의 개인정보보호 기준

우리는 우리가 따라야 할 스마트 그리드의 일부가 되는 조직을 위한 몇 가지 실제 개인정보보호 기준을 만들 필요성에 대해 토론하고 설명해 왔다. NIST에서 검토한 스마트 그리드의 개인정보보호 기준[20]과 Rebecca Herold가 제시한 개인정보보호의 기준[4]을 살펴보면 다음과 같다.

① 동의 및 선택(**Consent & Choice**)

조직은 개인정보의 수집, 사용 및 공개에 대해, 개인이 채택 가능한 선택을 기술하고 가능할 경우 명시적인 동의 또는 이것이 타당하지 않을 경우엔 묵시적인 동의를 구해야 한다.

② 통지 **&** 목적 사양

조직은 개인정보의 수집 시점 또는 그 이전에 수집되는 항목을 나열하는 한편 이 개인정보의 수집, 사용, 공유의 목적을 기술함으로써 명확한 말로 된 통지서를 제공해야 한다.

③ 개인의 참여 **&** 접근

조직은 해당 개인정보를 알아보기 위해 물어 볼 수 있도록 개인 및 가구에 대한 프로세스를 제공해야 한다. 또 조직은 개인 및 가구의 부정확한 내용에 대한 정정 요청이 각 조직에 의해 제공된 해당 개인정보 안에서 가능하도록 프로세스를 제공해야 한다. 개인 및 가구는 또 해당 개인 정보를 공유한 다른 모든 당사자에 대해 공지되어야 한다. 개인정보 사용에 대한 개인 정책(Policy)의 설정, 개인정보보호의 설정 및 제어 기능들이 제공되어져야 한다.

④ 정보의 품질/무결성/정확성

조직은 개인정보와 스마트 미터기로부터 수집한 기타 정보의 정확성, 완전성, 통지에서 식별된 목적에 적합성, 그리고 조직의 통제 안에서 정보의 일생동안 정확성을 기하기 위해 문서화한 정책, 절차, 기준 및 진행중인 훈련 및 인식 소통을 동원하여 모든 노력을 해야 한다. 정책 및 절차는 개인 정보의 수정이 이루어질 때 그들만의 것인 해당 정보를 적절히 수정할 수 있도록 다른 모든 기관에 통지할 수 있게 적소에 있어야 한다.

⑤ 사용 제한(**Use limitation**)

스마트 그리드 네트워크와 시스템 내에서의 정보는 수집된 목적으로만 사용되고 공개되어야 하며, 이 정보를 받을 권한이 부여된 자들에 한해서 공개되어야 한다.

[표 2] 스마트 그리드의 개인정보보호 제공 방안

구 분	내 용
지능적 (Intelligent)	만약의 단전 사태를 방지 또는 최소화하기 위해 시스템 과부하를 감지할 수 있고 전원을 대체할 수 있다. 유틸리티 회사, 소비자 그리고 규제자의 목표에 맞추어 협조적으로 그리고 사람이 대응할 수 있는 것 이상으로 빠른 문제해결이 요구될 경우 자발적으로 가동할 수 있다.
	(방안) 제공되는 서비스의 품질과 범위를 감쇄시키지 않으면서 필요한 소비자 개인정보를 최소한으로 수집할 수 있다. 소비자 개인정보의 수집, 사용, 유출 측면에서 정보 소통을 위해 소비자와 투명하게 움직인다. 개인정보 보호와 보안을 어떻게 할 것인가를 사전에 계획하고 활용에 앞서 시스템으로 구축한다.
효율성 (Efficient)	추가적인 인프라 없이도 증대하는 소비자의 요구를 만족시킬 수 있다.
	(방안) 개인정보의 보호 및 보안에 대한 어떤 절충 없이도 증대되는 소비자의 요구를 만족시킬 수 있다. 개인정보가 원래 수집될 당시의 목적으로 더 이상 필요치 않을 경우 개인정보를 안전하게 폐기한다.
수용성 (Accommodating)	석탄과 천연 가스와 마찬가지로 투명하고 쉽게 태양에너지와 풍력에너지와 같은 거의 모든 연료원으로부터의 에너지를 수용한다. 모든 더 나은 아이디어와 기술(예를 들면, 에너지 저장 기술)이 시장에서 검증되고 온라인으로 현실화되고 있기 때문에 이들을 통합할 수 있다.
	(방안) 개인정보의 사용, 보관, 그리고 유출에 대한 다양한 소비자 선호도의 수용으로 인해, 개인들이 쉽게 선호하는 옵션에 접근할 수 있다.
동기 부여 (Motivating)	소비자와 유틸리티 업체 간의 실시간 의사소통을 가능하게 함으로써 소비자들은 요금 및 환경 문제와 같이 자신의 에너지 소비를 개인의 선호에 따라 직접 조정할 수 있다.
	(방안) 소비자와 유틸리티 업체 간의 실시간 의사소통과 통지를 가능하게 함으로써 소비자들은 자신의 개인정보 옵션을 개인의 선호도에 따라 자기만의 것으로 만들 수 있다. 개인정보를 제삼자에게 공개하기 전에 적극적으로 동의를 얻는다.
기회 (Opportunistic)	언제 어디서나 플러그 앤 플레이 혁신을 이용하는 능력을 통해서 새로운 기회와 시장을 창출한다.
	(방안) 언제 어디서나 프라이버시 강화 기술을 이용하는 능력을 통해서 새로운 기회와 시장을 창출한다.
품질 중심 (Quality)	필요한 전력 품질(전압강하, 스파이크, 장애, 중단 등이 없음)을 점차 커지는 디지털 경제와 정보 센터, 컴퓨터 그리고 전자제품 등에 전력을 공급함으로써 이들이 작동할 수 있도록 한다.
	(방안) 정확한 정보만을 제공하고, 개인들에게 자신의 개인정보에 접근해 필요한 수정을 가할 수 있도록 한다.
탄력성 (Resilient)	스마트 그리드 보안 프로토콜로 더욱 분산되고 강화됨에 따라, 특정 공격과 자연재해에 점점 더 저항력이 커진다.
	(방안) 기본 및 위반 통보 프로토콜에 의한 개인정보보호 정책 등과 같은 개인 정보 및 보안 프로토콜로 강화되어, 정보 유출과 개인정보 침해에 대한 저항력이 갈수록 커진다.
그린 (Green)	지구 기후 변화를 둔화시키고 현저한 환경 개선을 향한 진정한 통로를 제공한다.
	(방안) 환경 개선으로 이어지는 개개인의 더 많은 참여를 도모하고, 그리드에서 소비자의 신뢰와 관련된 기술을 확보함으로써 환경에 이바지한다.

개인 정보는 기록을 컴퓨터 매칭 및 정보 마이닝에 대한 가능성을 제한하기 위해 가능한 한 어디서나 집합화 또는 익명화되어야 한다.

⑥ 보존 및 폐기 정책/관행

스마트 미터기의 정보와 해당 개인 정보는 수집 목적을 완수하기 위해 그것을 필요로 하는 기간 동안만 보관해야 한다. 명시된 수집 목적을 위해 더 이상 필요치 않을 때, 최소한 NIST의 폐기 기준에 부합하는 처리 방법을 사용하여 돌이킬 수 없도록 삭제/파괴해야 한다.

⑦ 투명성 & 개방성(Transparency & Openness)

문서화된 개인정보보호 정책은 스마트 그리드 시스템과 네트워크의 일부인 개인 및 가구가 사용할 수 있어야 한다. 개인 및 가구에게는 명시된 개인 정보 보호 정책뿐만 아니라 실제 개인 정보 보호 관행을 조직이 준수할 것을 요구하는 능력과 프로세스가 주어져야 한다.

⑧ 수집 제한(Collection limitation)

명시된 목적을 완수하는 데 필요한 정보만이 개인과 가구로부터 수집되어야 한다. 정보를 수집하는 조직은 공정한 정보처리 관행을 따라야 한다. 왜 불가하다는 승

인되고 문서화된 이유가 없는 한, 개인정보는 가구에 대한 각 개인, 이들의 해당 스마트 미터기 또는 인가된 이동식 스마트 미터기 정보 수집 장비로부터 직접 수집되어야 한다.

⑨ 보안/안전장치(Security/Safeguards)

스마트 미터기 네트워크의 일원인 조직은 도난, 손실로부터 모든 형태로 개인 정보를 보호해야 하고, 무단 접근, 공개, 복사, 사용 또는 수정을 막아야 한다.

⑩ 회계 & 관리(Accountability & Management)

각 조직은 공식적으로 지위, 팀, 부서 또는 개인을 지정해서 정보 보안과 개인정보보호 정책 및 관행이 존재하고 따르게 되도록 보장해야 한다. 정기적인 교육과 지속적인 인식 활동을 위한 문서화 요구 사항이 존재해야 하고 일관되게 따라야 한다.

⑪ 공개 및 공유 제한

개인정보는 그것이 수집된 목적으로만 사용되어야 한다. 개인정보는 그 통지에서 식별된 자, 또는 해당 개인 또는 적절한 가구 대표의 명시적인 동의가 있는 자들을 제외한 어떤 자에게도 공개되어서는 안 된다.

⑫ 감시 및 강화(Monitoring & Enforcement)

스마트 그리드는 네트워크 및 시스템의 일원인 각 조직은 그 조직의 개인정보보호 정책 및 절차 준수 여부를 모니터링해야 하며, 개인정보보호 관련 문의 사항 및 분쟁을 다루기 위한 절차를 가지고 있어야 한다. 모든 스마트 그리드 정보와 개인정보를 사용, 공유 및 수정을 감시하기 위해 감사기능이 있어야 한다.

4.4 프라이버시 보호 제공 방안

유틸리티 공급자에 의한 서비스 제공, 가격 통지, 원격 전원 접속 및 단속, 기기의 도난 감지 등, 스마트 그리드의 서비스에서 개인정보 사용이 꼭 필요한 경우가 존재한다. 또한, 이러한 개인정보가 에너지 효율 분석과 모니터링 및 부하 관리와 같은 소비자에게 유익한 정보를 제공하는 데 사용될 수도 있다. 그러나 다른 목적으로의 소비자 정보의 사용(정보 수집의 기본 목적이 아닌 사용)은 개인으로부터의 동의가 없을 경우 사생활 또는 개인정보 침해 문제가 제기될 수 있다. 스마트 그리드의 혜택을 줄이지 않고서, 시스템의 모든 물리적, 관리적 그리고 기술적 측면에서 개인정보 보호를 그 기본으로 하면서 스마트 그리드 서비스를 설계해야 한다[3]. 스마트 그리드에서 제공되어지는 주요 기능을 기본으로 하여, 스마트 개인정보보호 제공방안을 살펴보면 [표 2]와 같다.

구체적으로 개인의 분명한 동의하에 개인 정보를 제3자에게 제공하는 유틸리티 업체의 경우, 보다 강력한 개인정보 보호를 실현하는 스마트 개인정보보호의 사례는 다음과 같다[3].

- 서비스의 본질이 적절할 경우, 최소한의 정보만을 제3자에게 제공한다. 예를 들어, 우편 번호 앞부분 몇 자리와 같은 부분 정보만으로도, 이웃의 평균 사용량이나 기상 통계와 같은 비교를 수행하는 데 충분할 수 있다.
- 가능하면 신원을 익명화한다. 제삼자와 정보를 공유할 경우, 고유 번호(개인이 언제든 재설정하는 것이 가능)와 같은 익명의 사용을 고려한다.
- 제3자는 유틸리티 업체로부터 소비자 정보를 요구해서는 안 되고, 오히려 소비자가 유틸리티 업체에 의한 제3자에게로의 정보 유출의 유형에 대해 지속적으로 제어할 수 있어야 한다.
- 정보를 전송할 때 정보를 가로챌 위험이 발생한다. 집 내부 네트워크, 통신 시스템, 인터넷 프로토콜과 같은 통신에 다중 채널이 있다는 것을 우리는 알고 있다. 적절할 경우, 스마트 그리드와 함께 강력한 개인정보 보호를 보장하기 위해 전달되는 정보의 유형에 맞는 전송 보안 채널이 필요하다.
- 제3자는 개인의 동의 없이는 특정 정보를 다른 소스나 그 사람으로부터 얻은 정보와 연관지어서는 안 된다.

스마트한 개인정보 보호의 전체론적 접근 방식에서는 개인 및 관련 산업으로 하여금 설계에 의한 개인정보 보호를 보장하는 방법을 알게 하는 것이 필요하다. 정기적인 개인정보 보호 교육과 스마트 그리드를 통한 관리 책임이 있는 다른 업체 및 모든 유틸리티 협력 업체에 대한 지속적인 인식 활동이 있어야 한다. 그러나

정보사용과 공개에 대한 통보가 주어진다 해도, 정책을 소비자에게 전달하는 것이 쉽지는 않다. 신흥 스마트 그리드 에코시스템에서는, 영리기관들이 자신의 정보사용 관행을 소비자에게 전달하여 소비자가 자신의 정보를 사용하는 것에 대해 충분히 설명을 받아 의사결정을 할 수 있도록 하는 방법을 활용할 수 있다.

대중 또한 자신의 에너지 소비에 대해 접근하게 될 제3자가 스마트 그리드 서비스에 참여할 경우, 자신의 개인정보 보호에 대한 필요성에 대해 교육을 받을 필요가 있다. 유틸리티 공급업체 및 협력업체는 각 개인들이 자신의 개인정보를 어떻게 보호하는지 이미 알고 있을 것으로 가정해서는 안 된다. 예를 들어, 페이스북에는 2억 5000만여 명의 활동 중인 사용자가 있으나, 그들 중 다수가 활용할 수 있는 개인정보보호 설정을 이용하지 않는다. 그 이유는 이들이 그 활용 가능성에 대해 알지 못하기 때문이다. 연방 통상위원회는 개인정보보호 정책이 영리기관에 의한 개인정보 사용에 대한 공개의 적절치 못한 방법임을 인식해 가고 있다. 유틸리티 업체와 제3자 서비스 제공 업체들은 로그인과 비밀번호와 같이 제공되는 개인정보 안전장치의 사용 방법뿐만 아니라. 탈퇴와 자신의 개인정보를 삭제하는 방법에 대한 분명한 지침을 제공해야 한다.

그리고, 소비자들의 에너지 소비 정보를 사용하는 서비스를 제공하는 유틸리티 업체와 이들 조직의 내부자 위협에 대해 특별한 주의를 기울여야 한다. 이러한 위협들은 조직이 이들의 발생을 방지하고, 감지하고, 줄이는 방법에 대해 고유성을 띠고 있다. 왜냐하면 이 위협을 저지르는 내부자는 개인정보에 접근할 수 있는(그러나 승인되지 않은 목적으로) 합법적인 권한과 특권을 행사하고 있기 때문이다. 이렇게 악성 내부자는 직원, 협력업체, 사업 파트너, 감사, 심지어 동창 등 조직의 어느 급에서나 있을 수 있다. 다중 전문분야 접근법을 이용해 내부자 위협의 감지, 감시 및 방지를 위한 방법을 개발하고, 내부자가 취한 위협의 행위 및 범위에 대해 지속적으로 인지하여야 한다.

V. 결 론

오바마 미국 대통령은 "미국의 21세기 경제적 번영은 사이버 보안에 달려있다"라고 말했다. 이와 같이 전력망이 갈수록 복잡해지고 서로 연결됨에 따라 유틸리티 공급업체의 사이버 보안 위협을 위한 노력이 점차로 중요하게 될 것이다. 암호화 또는 인증 프로세스의 결여 외에도, 스마트 그리드 메쉬 네트워크의 대다수가 성능, 관리, 그리고 특히 보안에서 결정적인 취약점을 보이고 있다. 개방형 표준이 부족한 탓으로, 메쉬 네트워크는 스마트 그리드에서의 대형 설치 준비가 아직 되어 있지 않다.

본 고에서는 특히 스마트 그리드 기술의 도입에 따른 프라이버시 보호를 위해 개인정보보호 기술의 필요성에 대하여 강조하고자 하였다. 미국 표준기술연구소(NIST)에서 설명하다시피 개인정보보호는 스마트 그리드의 '아킬레스건'이다. 스마트 그리드 기술이 실질적인 소비자 혜택 및 에너지 효율성 혜택을 가져다 줄 수 있지만, 동시에 다수의 개인정보보호 및 정보보안 문제를 자아낸다. 결과적으로, 스마트 그리드 에코시스템에 관련된 모든 이해 당사자가 책임있는 정보 관리를 실시하는 것이 필수적이라 생각한다. 스마트 그리드도 기회가 열려있는 만큼 우리가 먼저 선도를 하게 되면 세계의 표준이 되고 세계 시장을 선점할 수 있기 때문에 국민적 역량을 결집하여 대표 산업으로 자리 매김할 수 있게 해야 할 것이다. 기회는 열려있고 미개척 시장들이 다가오고 있으므로 위기와 기회가 혼조된 이 시기에 세계를 주도하고 리드할 역량과 전략이 필요한 때라고 사료된다.

참고문헌

[1] Patrick McDaniel & Stephen McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security and Privacy*, 7(3), pp. 75-77, 2009.

[2] Christopher Wolf, Winston Maxwell, "Smart Grids And Privacy," *Communications & Strategies,* No.76, pp. 127-130, 2009.

[3] Ann Cavoukian, Jules Polonetsky, Christopher Wolf, "SmartPrivacy for the Smart Grid: Embedding Privacy in the Design of Electricity Conservation," *The Future of Privacy Forum*, November 2009.

[4] Rebecca Herold, "15 Smart Grid Privacy Concerns +Other Smart Grid Thoughts," *Realtime Communities,* November 2009.

[5] Westar Energy, "Westar Energy Smart Grid," June 2009.

[6] Edward Chow, "Secure Smart Grids, University of Colorado at Colorado Springs," *Freshmen Welcome '09,* 2009.

[7] U.S. Department of Commerce, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)," September 2009.

[8] 이일우, 한동원, "IT기반의 스마트 그리드 기술", *한국정보기술학회지,* 7(1), pp. 25-30, 2009.

[9] 박신정, "녹색성장과 스마트그리드 동향", *전자정보센터 산업동향분석,* 2010.

[10] (주)유오씨, "Smart Grid 관련 해외 산업 동향", *전자정보센터 산업동향분석,* 2010.

[11] 박찬국, "전력인프라 사이버보안 이슈와 정책 대응", *주간기술동향,* no.1398, pp. 1-10, 2009.

[12] 전용희, 장종수, "그린 IT 보안 기술", *한국통신학회지(정보와통신),* 26(9), pp. 34-41, 2009.

[13] 이경복, 독고지은, 유지연, 이숙연, 임종인, "그리드에서의 소비자 참여와 보안 이슈", *정보보호학회지, 19(4),* pp. 21-35, 2009.

[14] "*스마트 그리드 사생활보호 대책 시급*", 하이테크정보, 2009년 12월호, 제429호, pp. 100, 2009.

[15] 박남제, "스마트 그리드와 개인 프라이버시", *디지털타임즈,* DT발언대(2010.4.14), 2010.

[16] 제3차 녹색성장위원회, *그린 IT 국가 전략(안)-(2009.5.13),* 지식경제부, 2009.

[17] Office of Electricity Delivery and Energy Reliability, "A System view of the modern Grid," *NETL,* 2007.

[18] 이명훈, 김창섭, 손성용, "미국 스마트 그리드 사이버보안 동향분석", 주간기술동향, 통권 1429호, pp. 32-44, 2010.

[19] 이일우, 박완기, 박광로, 손승원, "스마트 그리드 기술 동향", *한국통신학회지(정보와통신),* 26(9), pp. 24-33, 2009.

[20] U.S. Department of Commerce, "(Draft) NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements," February 2010.

[21] E. L. Quinn, "Privacy and the New Energy Infrastructure," *Working Paper Series,* 2009

[22] FTC Press Release, "FTC Staff Revises Online Behavioral Advertising Principles," Feb. 2009.

[23] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *Legal Studies Research Paper* No.09-12, University of Colorado Law, 2009.

[24] R Smith, "Stimulus Funds Speed Transformation Toward 'Smart Grid'," *The Wall Street Journal,* September 2009.

[25] Cisco White paper, "Security for the smart grid," 2009.

[26] "The Smart Grid Faces Off Against Privacy Rights," *Environmental Leader*, http://www. environmentalleader.com/.

[27] "What the Smart Grid Can Learn From Facebook Connect," http://www.business week.com/.

[28] Andrew Wright, "Cyber Security for the Power Grid:Cyber Security Issues & Securing Control Systems," *ACM CCS Tutorial*, Nov. 2009.

[29] AMI-SEC-ASAP, "AMI System Security Requi -rements," v1.01, December 2008.

[30] AMI-SEC-ASAP, "AMI Security Implementation Guide," v0.4, February 2009.

[31] Frances M. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure, Beyond Simple Encryption," *IEEE PES Transmission and Distribution Conference and Exhibition*, 2006.

[32] Chee-Wooi Ten, Chen-Ching Liu & Manimaran Govindarasu, "Cyber-vulnerability of Power Grid Monitoring and Control Systems," *CSIIRW '08 Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research,* 2008.

[33] Frances M. Cleveland, "Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System," *IEEE Power Engineering Society General Meeting*, 2007.

[34] Frances M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," *IEEE Power Engineering Society General Meeting. Helen Cheung, Alexander Hamlyn,*

Todd Mander, 2008.

[35] 도윤미, 김선진, 허태욱, 박노성, 김현학, 홍승기, 서정애, 전종암, "스마트그리드 기술동향:전력망과 정보통신의 융합기술", *전자통신동향분석*, 24(5), pp. 74-86, 2009.

[36] 윤인하, "최근 미국 동부지역의 정전사태와 미국 전력산업의 문제점", *Asia-Pacific Review*, 2003.

[37] 전용희, "지능형 전력망과 정보보호", *정보보호학회지*, 19(4), 2009.

[38] 임종인, "지능형 전력망, 보안구축이 생명이다", *동아일보 기고문*(2010.2.19), 2010.

[39] 박남제, "스마트 그리드 환경에서의 개인정보 취약점 분석과 보호 방안", *한국정보기술학회 논문지*, 제8권, 2010.

[40] Rebecca Herold, "Smart Grid Privacy Concerns," October 2009.

[41] P. Tsang and S.W. Smith, "Yasir: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems," *Proc. IFIP TC 11 23rd Int'l Information Security Conf. (SEC 08)*, Springer, pp. 445-459, 2008.

[42] H. Khurana et al., "Design Principles for Power Grid Cyber-infrastructure Authentication Protocols," *Proc. 43rd Ann. Hawaii Int'l Conf. System Sciences (HICSS 10)*, IEEE Press, 2010.

[43] R. Bobba et al., "PBES: A Policy Based Encryp -tion System with Application to Data Sharing in the Power Grid," *Proc. 4th Int'l Symp. Informat -ion, Computer, and Communications Security (ASIACCS 09)*, ACM Press, pp. 262-275, 2009.

[44] Ray Belf, "Safe smart grid design," *SC Magazine*, Feb. 2010.

[45] Wikipedia encyclopedia, "Smart Gird," May 2009.

[46] John Steven, Gunnar Peterson, Deborah A. Frincke, "Smart-Grid Security Issue," *IEEE Security and Privacy*, 8(1), pp. 81-85, 2010.

〈著者紹介〉

박 남 제 (Namje Park)

종신회원

2000년 8월: 동국대학교 정보산업학과 졸업

2003년 8월: 성균관대학교 정보보호학과 석사

2008년 2월: 성균관대학교 컴퓨터공학과 박사

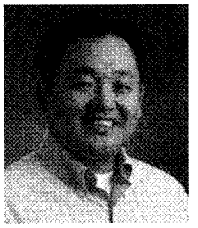
2003년 4월~2008년 12월: 한국전자통신연구원 정보보호연구단 선임연구원

2009년 1월~2009년 12월: University of California, Los Angeles (UCLA) 공과대학 Post-Doc.

2009년 3월~2009년 12월: University of California, Los Angeles (UCLA) WINMEC 연구센터 Staff Researcher

2010년 1월~현재: Arizona State university(ASU) 컴퓨터공학과 Research Scientist

<관심분야> 암호이론, 융합기술보안, 모바일컴퓨팅, 스마트 그리드, RFID/USN 등



안 길 준 (Gail-Joon Ahn)

1994년 2월: Soong-Sil University, Computer Science, B.S.

1997년 5월: George Mason University, Computer Science, M.S.

2000년 5월: George Mason University, Information Technology, Ph.D.

2000년 7월~2008년 7월: University of North Carolina at Charlotte, Software and Information Systems, Associate Professor

2008년 7월~현재: Arizona State University, Computer Science and Engineering, Associate Professor

<관심분야> Authentication and access control, Vulnerability and risk assessment, Network and distributed systems security, Digital identity management, Cyber crime analysis, Computer and network forensics.