스마트 그리드의 개인정보보호

정영하, 박정규, 이근호
백석대학교 정보통신학부
iwilldono1@gmail.com, sunrise1987@nate.com, root1004@bu.ac.kr,

Private Information Security in Smart Grid

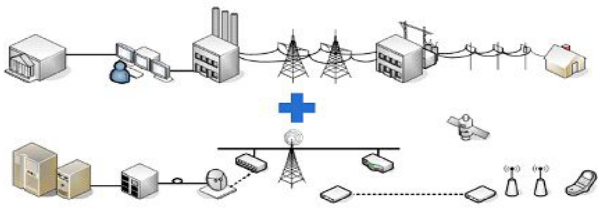
Young-Ha Jung, Jung-Kyu Parkm, Keun-Ho Lee
Dept. of Information Communication, Baekseok University

최근 국내외적 이슈 가운데 하나인 녹색성장(GreenGrowth)은 지구온난화의 문제로 이산화탄소[CO2) 배출을 줄이기 위한 산업적 노력과 이와 관련된 기술 및 산업을 성장 동력의 기회로 만들자는 취지이다. 스마트그리드의 대상이 국가주요기반시설인 전력망이기 때문에 스마트그리드의 추진에 있어 주요기반시설보호 등의 보안은 중요한 요소로 고려 될 필요가 있다. 특히 스마트그리드가 다분히 전력기반시설의 발전을 의미하는 것이 아니라 IT, 통신, 전력 등의 여러 기술이 융합된 디지털 사회의 핵심기반시설로써의 의미가 중요하게 고려되어 논의되고 있기 때문에 더욱 그러하다. 이에 본 연구에서는 스마트 그리드의 개인정보보호의 필요성과 스마트 그리드에서 개인정보보호가 어떻게 이루어져야 할지를 생각해보고 향후 연구의 방향을 제시하고자 한다.

1. 서론

스마트 그리드는 기존 전력망에 IT 기술을 도입하여 시스템을 개선함으로써 에너지의 효율성을 높이려는 연구에서 파생되어 시작되었기 때문에, 스마트그리드에 관한 논의가 먼저 시작된 국외에서도 앞서 살펴본 정의들과 같이 각국의 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. 또한 스마트 그리드와 관련하여 각국에서 이제 막 표준을 정하고 있는 상황이기 때문에, 스마트 그리드에 대한실체적인 정의는 아직까지는 모호하다. 따라서 무엇보다도 스마트 그리드에 대한 명확한 정의, 대상, 목적 등을 실체화할 필요가 있다. 스마트 그리드는 발전소와 송전·배전 시설과 전력 소비자를 정보통신망으로 연결하고 양방향으로 공유하는 정보를 통하여 전력시스템 전체가 하나의 체계 내에서 효율적으로 작동하도록 설계한다[1]. 이 기술을 통하여 전력 낭비를 줄이는 동시에 재생에너지 사용을 활성화하고 이산화탄소 배출도 줄여 지구온난화 방지에도 효과가 있어 선진국들의 관심과 투자가 이루어지고 있다.

<전력망>



<IT망>

[그림 1-1] 일반적인 스마트 그리드의 구성도
출처 : Westar Energy, “Westar Energy Smart Grid,” June 2009

(그림 1-1)은 전기의 생산과 공급, 제어를 위한 통신 네트워크와 센서시스템, 각종 지능형 설비, 계측 장비 등을 망라한 통합 네트워크로 구성되는 일반적인 스마트그리드 구조를 보여주고 있다. 위의 (그림 1-1) 과 같이 스마트 그리드에서는 양방향으로 통합된 통신기술(Communication)이 가장 기반 되는 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 구성한다

고 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 요금정보를 실시간으로 확인할 수 있다.

2. 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[2].

스마트그리드 도입에 따라 소비자는 실시간으로 전력 가격정보를 조회하거나 실시간 가격 변동제에 따른 다양한 방법의 선택 구매, Utility는 고장을 자가 진단하고 설비 점검을 원격수행, 광범위한 제어 가능, 수요,.공급 상호 작용에 따른 양방향 송. 배전 등 여러 가지 장점에도 불구하고 개인정보보호관점에서 여러 취약점을 안고 있다. 소비자의 전기 신청 등 개인정보는 스마트그리드에서도 유사하게 관리되겠지만 시간대별(세부적으로 가전제품 단위까지) 전기 사용 정보와 같이 새로운 영역의 개인 정보가 발생된다. 이러한 개인정보는 실시간으로 자동 수집되어 지는데 수집 시 정보의 동의 문제, 수집과정에서의 유무선 통신기술의 적용에 따른 정보 유출 취약점이 예상된다. 또한 소비자 변경 시 다른 소비자로부터 정보 보호 문제가 이슈가 될 수 있다.

수집된 정보는 Utility로 전송되어지는 과정에서 DAS, SCADA, EMS 많은 영역에 저장되는데 다양한 통신 구간, 분산 저장에 따른 관리적, 기술적 문제로 인해 개인 정보가 노출 될 개연성이 높다. 따라서 스마트그리드에서의 개인정보 수집, 저장 및 관리, 이용 및 제공, 파기 절차별로 예상되는 문제를 파악하고 해결하기 위한 주요 개인정보 흐름 과정에서의 침해요인 및 침해유형을 분석하여 이에 대한 대책이 필요하다고 본다[3].

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 제공하는데 사용될 수도 있다. 그러나 다른 목적으로의 소비자 정보의 사용(정보수집의 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[4].

현재의 전력망은 패쇄형, 단독망 운영관리로 개인정보보호를 포함한 보안이 크게 문제되지 않았지만, IT가 결합됨에 따라 여러 망의 연결, 관련 기기간의 상호 운영성, 개인정보의 여러 단계에서의 저장이 이루어지고 양방향 통신이 되기 때문에 소비자의 개인정보 노출, 정보 도용, 소비요금 조작은 물론, 전력 시스템의 마비까지 기존전력망에서 나타나지 않았던 새로운 보안 위협의 가능성이 나타난다[5].

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 정보사용관행을 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. 미국 연방 통상위원회는 개인정보보호 정책이 영리기관에 의한 개인정보 사용에 대한 공개의 적절치 못한 방법임을 인식해 가고 있다.[6]

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 내부자위협에 대해 특별한 주의를 기울여야한다. 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 이용해내부자 위협의 감지, 감시 및 방지를 위한 방법을 개발하고, 내부자가 취한 위협의 행위 및 범위에 대해 지속적으로 인지하여야 한다.[7]

3. 개인정보보호에 대한 대책

앞서 살펴본 바와 같이 국내 법률은 정보보안에 중심을 둔 법률과 개인정보보호에 중심을 둔 법률로 구분 할 수 있다. 스마트그리드 추진을 위하여 제정된 지능형 전력망의 구축 및 이용에 관한 법률조차도 개인정보에 대한 기본 항목만 언급된 상태고, 최근 입법화되고 시행을 앞둔 개인정보보호법 조차도 스마트그리드의 특성을 수용하지 못하는 상황이라 스마트그리드를 추진함에 있어 적용의 사각지대에 놓여 있는 상황이다. 즉 현재 국내에는 스마트그리드의 개발, 설치, 데이터 수집방법, 정보유출 등에 대한 벌칙 등의 관련 내용을 포괄 할 수 있는 법적 제도가 존재하지 않는다. 따라서 스마트 그리드 보안에 대한 인식의 제고 및 강제성의 부여를 위해, 스마트그리드의 보안을 명시하는 법률 및 이를 뒷받침할 수 있는 정책이 우선적으로 정비되어야 한다. 앞으로의 법률은 미국의 에너지 독립 및 안보법과 같이 IT융·복합 서비스를 제공 하는 스마트그리드에 관한 독립적인 법률의 제정을 통해 스마트그리드의 보안을 현재의 정보보호 관련법과의 관계를 고려해 직접적으로 규정해야 하는 것이다. 이를 위하여 지능형전력망 구축 및 이용촉진에 관한 법률안 안에 목적, 정의 등에 스마트 그리드 내 기반시설 보호 및 이용자 개인정보의 보호를 구체화하여야 한다.

이를 위해 목적, 정의 규정에서의 보호에 관한 사항을 추가해야 하며 보호에 대한 구체적인 명시 및 이용자 , 시설보호에 대한 시책·계획 수립을 반영하고 지능형 전력망의 보호와 관련하여 타법(정보통신망 이용촉진 및 정보보호에 관한 법률)등 과의 관계가 명시되어야 한다. 지능형전력망 보호를 위한 법적 권한을 가지는 기구의 규정, 지능형전력망 보호 기술 개발의 추진 및 지원의 규정, 위협 및 취약성에 대한 평가 및 보고의 의무화, 정보보호의 대상 중복되거나, 사각지대가 발생하지 않도록 명시, 타법이 적용되지 않는 부분에 대한 규정은 다른 규정에서 명시, 국가의 시책 및 계획 수립에서 정보보호가 포함, 전기사용자의 보호 외 시설 보호 등에 대한 항목, 침해사고 대응에 대한 항목 추가 필요, 지능형전력망 보호에 대한 기술 개발의 항목이 추가 필요하다.

4. 시사점 및 향후 연구 방향

본 논문에서는 스마트 그리드에서의 개인정보보호의 요소를 살펴보고, 개인정보보호의필요성과 프라이버시 침해의 유형에 대해 분석하였다. 그리고, 스마트 그리드의 개인정보보호에 대한 고려사항과 보호 제공방안 및 기술적 대응방안을 제시하였다. 특히, 서비스 환경에서의 개인정보 정의 및 개인정보 흐름을 분석 하였으므로 개인정보보호에 대한 접근의 단초가 될 수 있을 것으로 판단한다[8].

스마트그리드 도입에 따른 개인정보보호를 위해 관리적, 기술적, 정책적 대책이 잘 조화될 필요성에 대하여 강조하고자 하였다. 스마트 그리드 기술이 실질적인 소비자 혜택 및 에너지 효율성 혜택을 가져다 줄 수 있지만, 동시에 다수의 개인정보보호 및 정보보안 문제를 자아낸다. 기존의 IT 기술에서 가지고 있는 위협이나 취약점에 더한 신규 문제점을 포함 할 것으로 예상하고 있다. 보안측면에서 보면, 스마트그리드는 기존의 IT 기술의 위협/취약점에 더해 신규 취약점에 대해서도 효과적으로 대응 하도록 설계되어야 한다. 또한 기존에 존재하는 법률이 IT와 결합하는 전력망의 특성을 모두 포함 할 수 없기에 정보보호규제를 강화한 새로운 법의 제정이 필요하다. 스마트그리드와 관련된 국내 법률들을 보면 역시나 새로운 개념의 전력망을 바로 기존 정보보호 유관법에 적용해 규제하는 것은 본래의 목적을 달성하지 못할 것으로 판단된다. 따라서 보안의 특성을 고려한 특별법의 제정이 필요하다. 세계 최초의 국가단위 스마트그리드를 위해서는 잘 정비되고 정리된 안전한 법 제도적 뒷받침에 선도적인 기술적 보안 대책을 적용해야 세계 최초의 최고의 스마트그리드 구축이 가능 할 것이다. 이에 대한 지속적인 연구가 필요하다.

"이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2011-0010457)"

참고문헌

[1] U.S. Department of Commerce,"NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)," September2009.

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

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

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

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

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

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

[8] 이연섭, "스마트 그리드에서의 개인정보보호에 관한 연구", 동국대학교 국제정보대학원 석사학위논문, 2011