스마트 그리드 사용자도메인의 개인정보보호방안 연구

최동민*, 심검*, 정일용*
*조선대학교 컴퓨터공학과
e-mail:cdm1225@gmail.com

A Study of Personal Data Protection Method of Customer Domain on Smart Grid

Dongmin Choi*, Jian Shen*, Ilyong Chung*1)
*Dept of Computer Engineering, Chosun University

요 약

스마트 그리드는 전력망에 정보기술을 접목하여, 전력공급자와 소비자가 양방향으로 정보를 실시간으로 교환하고 에너지효율을 최적화하여 새로운 부가가치를 창출할 수 있는 차세대 전력망이며 기존의 전력 시스템과는 달리 시스템의 개방성이 높아짐으로서 보안위협이 증가하였다. 이러한 보안 위협 중에서 본 연구는 전력망 소비자의 개인정보와 밀접한 관련을 갖는 사용자도메인에서 발생가능한 개인정보 침해 위협을 분석한다.

1. 서론

스마트 그리드는 정보통신 기술의 융합으로 지능화된 전력 시스템으로서 기존의 전력 시스템과는 달리 다른 시스템과의 상호 연계 및 개방성이 높아짐으로서 보안관점에서 볼 때 보안위협이 증가하게 되었다. 따라서 스마트 그리드 시스템 구축에 있어 필수 요건은 보안성의 확보라고 할 수 있으며 이는 전력망이 국가 기간시설로서 전력공급 중단과 같은 위협에 노출시 심각한 피해를 입을 수 있기 때문이다. 이에 스마트그리드 시스템을 구축하고자 하는 여러 국가들은 보안대책 마련을 위해 연구 중에 있다[1]. 또한 개인의 관점에서 볼 때, 시스템의 개방성은 개인정보 및 프라이버시의 보호에 치명적인 위해를 가할 수 있다. 전력망 시스템의 과금체계 또는 전력사용매체의 사용정보와 같은 정보들은 개인의 프라이버시와 밀접하게 관련되어있기 때문이다. 그러나 현재의 스마트그리드에서 적용하는 개인정보에 대한 정의의 한계로 인해 보호받지 못하는 개인정보가 내·외부로부터 침해받을 수 있기 때문에 개인정보에 대한 개념의 정립이 새롭게 필요하며, 이에 따른 영향평가가 이루어져야 한다.

2. 본론

우선, 스마트 그리드 환경에서의 개인정보에 대한 기본 개념을 정립하기 위해 국내·외에서 정의하고 있는 개인정보에 대한 기본적인 정의를 알아야 할 필요성이 있다. 다음은 국내·외에서 정의한 개인정보의 개념을 설명하고 있다[2].

2.1 국제기구가 정한 개인정보의 개념

OECD 이사회가 채택한 1980년「프라이버시보호 및 개인정보의 국가 간 유통에 관한 가이드라인에 관한 이사회 권고」에서는 개인정보를 "식별된 또는 식별될 수 있는 개인에 관한 모든 정보(any information relating to identified or identifiable individual)"라고 정의하고 있다.

EU의 1995년 「개인정보처리에 있어서 개인정보의 보호 및 정보의 자유로운 이동에 관한 유럽의회 및 이사회의 지침」에서는 개인정보를 "자연인을 식별하거나 식별할 수 있는 모든 정보"라고 정의하고 있다.

2.2 우리 법이 정한 개인정보의 개념

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다)에서의 개인정보라 함은 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"이다(동법 제2조제1항제6호).

「개인정보보호법」에서의 개인정보라 함은 "생존하는 개인에 관한 정보로서 성명·주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아 볼 수 없더라도 다른 정보와 쉽게 결합

1) Ilyong Chung is with the Dept. of Computer Engineering, Chosun University (Corresponding Author, e-mail: iyc@chosun.ac.kr)

하여 알아 볼 수 것을 포함한다)를 말한다"이다(동법 제2조제1호).

2.3 개인정보의 성립 요건

국제기구나 우리 법이 정한 개인정보의 성립 요건은 '생존하는 개인에 관한 정보'로서 개인을 알아 볼 수 있는 정보나 해당 정보만으로는 특정 개인을 알아 볼 수 없더라도 다른 정보와 쉽게 결합하여 알아 볼 수 있는 것이라 하겠다.

1) '생존하는 개인'의 정보

개인정보의 주체는 자연인이어야 하며, 법인 또는 단체의 정보는 해당되지 않는다. 따라서 법인의 상호, 영업소재지, 대표이사의 성명, 이사, 감사 등 임원정보, 자산, 영업실적 등의 정보는「정보통신망법」과「개인정보보호법」에서 규정하고 있는 개인정보의 범위에 해당된다고 볼 수 없다. 하지만 법인이나 단체의 정보에 포함하는 것일지라도 개인을 식별할 수 있는 경우에는 개인정보에 해당될 수 있다.

'생존하는 자연인'에 관한 정보이기 때문에, 이미 사망하였거나, 실종신고 등 관계 법령에 의하여 사망한 것으로 간주되는 자에 대한 정보는 개인정보로서 보호되기 어렵다. 다만, 사자에 관한 정보가 생존하는 유족 등 후손과 관련 있는 경우에는 유족 등 후손의 개인정보로서 적용대상이 될 수 있다.

2) '개인에 관한' 정보

개인정보는 당해 개인에 대한 사실, 판단, 평가 등 특정 개인과 관련된 일체의 정보가 모두 해당된다. 따라서 개인정보는 객관적 사실 정보(예: 이름, 주민등록번호, 직업 등)뿐만 아니라, 타인이 특정인에 대해 가지고 있는 의견, 견해, 평가 등과 같은 주관적인 정보 (예: 개인의 신용평가정보, 코멘트, 사회적 지위 등)도 개인정보로 인정될 수 있다.

3) '식별하거나 식별 가능한' 정보

어떤 정보가 개인정보로 인정되기 위해서는 해당 정보가 '특정 개인을 식별하거나, 식별 가능'해야 한다. 따라서 이미 통계적으로 변환되어 개인을 식별할 수 없는 상태라면, 이는 개인정보로 인정되기 어렵다.

수만 명의 이름, 주민등록번호, 거주 지역, 학력, 결혼여부, 자녀의 수 등의 개인정보를 수집한 후에, 개인을 식별할 수 있는 정보항목을 제외한 후 거주 지역과 결혼 여부에 대한 통계를 작성할 경우, 이미 통계화된 해당 결과값을 통하여 역으로 개인을 추적하기 어렵기 때문에 이를 개인정보로 인정하기 어렵다. 하지만 인적 데이터가 적어 통계화된 결과값으로 개인이 추적될 수 있다면 개인정보로 인정될 수 있는 것이다.

한편, 해당 정보만으로 개인을 식별할 수 있는 정보뿐 아니라 '다른 정보와 용이하게 결합'해서 개인 식별이 가능한 경우도 개인정보로 정의하고 있다. 예를 들면 주민등록번호는 개개인마다 고유하므로 주민등록번호를 활용하면 개인을 손쉽게 식별할 수 있다. 하지만 혈액형 정보는 개인마다 고유하지 않고 동일한 혈액형을 가진 사람이 많기 때문에 혈액형만 있는 경우에는 개인정보로 보기 어렵다.

하지만, 혈액형이 주민번호나 주소 등의 정보와 결합하는 경우에는 개인 식별이 가능해지므로 개인정보로 볼 수 있게 된다. 따라서 사업자들은 개인과 관련된 일반적인 정보들이 다른 정보와 결합하는 경우 대부분이 용이하게 개인 식별이 가능해지므로 이용자와 관련된 정보 일체를 개인정보로 간주하고 개인정보 보호를 위해 각별한 주의를 기울려야 할 것이다.

다른 정보와 '쉽게' 결합하여 알아 볼 수 있다는 대목에서의 '쉽게'의 의미는 결합이 가능한 환경, 맥락 등을 종합적으로 고려해서 판단해야 할 것이다. 예를 들면, 이름정보와 주소정보의 결합함에 있어서 주소가 상세할수록 특정 개인을 식별할 수 있는 것이다.

특정 정보들이 조합되어 개인을 식별할 수 있는 경우는 획일적으로 구분될 수 있는 것이 아니라 문맥적(Contextual)으로 이해될 때만이 가능하며, 이러한 문맥은 시대적 상황. 기술의 발전, 정보 보유의 형태 등에 따라 다양하게 해석이 가능하기 때문에 특정 정보들의 조합에 의한 개인 식별의 문제는 때로 법률적 판단을 필요로 하기도 한다.

결국 개인정보란 생존하는 자연인의 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 평가에 관하여 식별되거나 식별할 수 있는 모든 정보를 의미한다고 할 수 있다.

위의 정의에 의하면 스마트그리드 환경에서 발생하는 소비자의 개인정보(HAN에서 수집하는 개인정보, AMI 미터기에서 수집하는 정보 등)는 기존 전력망의 '개인식별정보'라는 협의의 관점에서 벗어나 다양한 조건에서 검토되어야 함을 알 수 있다.

2.4 사용자도메인에서의 개인정보보호 문제

사이버 보안 조정 작업그룹 산하 개인정보보호정책 하위 그룹의 개인정보영향평가에 의하면 미국의 스마트그리드와 관련한 많은 개인정보 누출에 대한 우려와 문제가 있으며 다음과 같이 서술되어 있다.[3]

· 스마트그리드의 개인정보보호에 관련된 사항이 아직 완전히 이해되지 않았다.

· 스마트그리드 및 정보수집에 참여하는 업체들의 공식적인 개인정보보호 정책, 표준, 절차가 부족하다.

· 유틸리티업계에 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 스마트그리드 기기의 로밍으로 인해, 추가적인 개인 정보가 유출될 수 있다.

· 스마트 미터기 및 스마트그리드 네트워크가 다양한 방식으로 개인 신상정보를 사용할 수 있을 것이다.

· 개인정보보호원칙의 채택을 촉구하는 국가전력규제위원협회가 채택한 2000년의 결의안에도 불구하고, 소수의 주 차원의 위원회들이 개인정보보호 문제와 스마트 그리드를 평가하기 시작했다.

· 추가적인 연구가 필요하고 추가적인 개인정보 영향평가를 실시하는 것이 중요하다.

이와 같이 사용자 도메인(HAN과 AMI)에서 사생활 침해의 소지가 다분하기 때문에 다른 관점에서 개인정보보호 접근이 필요하며 스마트그리드 설계단계에서 개인정보 영향평가의 필요성이 강력히 요구된다.

3. 결론

우리 법이 정한 개인정보의 개념에 따르면,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다)에서의 개인정보라 함은 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다" 라고 명시하고 있으며(동법 제2조제1항제6호), 「개인정보보호법」에서의 개인정보는 "생존하는 개인에 관한 정보로서 성명·주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아 볼 수 없더라도 다른 정보와 쉽게 결합하여 알아 볼 수 것을 포함한다)를 말한다" 로 명시되어 있다 (동법 제2조제1호). 그러나 스마트그리드에서 취급하는 데이터는 정보의 조합을 통해 개인정보를 생성해 낼 수 있는 환경이다. 예를 들어 HAN 내의 스마트 디바이스들이 AMI 미터, EMI와 연계하여 동작할 때 자신의 에너지 사용량 및 시간대가 기록이 된다. 이러한 기록은 상위 시스템에 보고가 되며, 이러한 자료들은 적응적 전력제어를 위한 자료로 활용될 수 있다. 그러나 이런 자료들은 개인의 사생활과 관련된 자료로서, 이러한 자료들의 조합을 통해 특정 개인의 일상생활 패턴을 읽어낼 수 있는 치명적인 개인정보보호 침해 자료로 활용이 될 수 있다. 따라서 스마트 그리드 환경에서는 기존의 전력망에서 정의하였던 협의의 개인정보의 개념에서 벗어나 보다 넓은 의미를 가지고 다른 관점에서 접근해야 한다.

그러나 현재 세계 어느 나라에서도 이러한 부분이 명확히 규명되지는 않았다. 따라서 현재 진행 중인 외국의 개인정보영향평가와 관련된 보고서와 스마트그리드 연구의 진행 상황과 문제점을 통하여 국내 스마트그리드환경에서 적용하여야 할 개인정보의 개념과 범위를 명확히 규명해야 한다.

이후, 명확히 정의된 개인정보의 개념을 통해 개인정보 영향평가를 실시하고 우리의 스마트그리드 환경 즉, 사용자 도메인에서 발생하는 개인정보의 흐름을 파악하는 것이 우선 과제이며, 개인정보 라이프사이클의 각 단계에 해당하는 침해 유형에 대한 분석 및 개인정보 업무흐름도와 개인정보 흐름표를 토대로 하여 개인정보 흐름도와 시스템 구조도를 작성하여 개인정보 침해요인을 분석하며 이에 따른 개선방안을 도출해야 한다.

참고문헌

[1] Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid, U.S. DoC NIST(National Institute of Standards and Technology), NISTIR 7628 Vol.2, August 2010.

[2] 한상열, 최동민, "개인정보보호사(PIP)", (사)벤처기업협회검정평가원, pp.10-12, 2012.

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