情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

스마트그리드 사이버 보안 추진 현황

이 건 희*, 서 정 택*, 이 철 원*

요 약

아날로그 기반의 전력 시스템과 디지털 기반의 IT 기술을 융합한 스마트그리드는 최근 가장 주목받는 분야 중의 하나이며, 이것은 기존의 전력 생산, 소비, 운반 프로세스에 IT 기술을 접목하여 전력 효율의 극대화를 추구한다는 장점이 있다. 하지만 스마트그리드 환경에서는 기존의 아날로그 기반의 전력 시스템에서 문제가 되지 않았던 부분이 디지털 기반의 IT 기술과 융합되면서 새로운 보안 위협들로 발생할 우려가 매우 높다. 따라서 본 고에서는 스마트그리드 환경의 보안 위협을 분석하고, 이러한 보안 위협을 해결할 수 있는 방법으로 암호화된 데이터베이스 검색 기술의 동향을 살펴본다. 암호화된 데이터베이스 검색 기술은 최근 발생한 수많은 데이터베이스 유출 사건을 계기로 활발히 연구되고 있는 분야이며, 암호화된 데이터를 복호화하지 않고도 효과적으로 검색할 수 있는 기술에 대한 연구이다.

Ⅰ. 서 론

에너지 효율성 증대, 그린 에너지 사용 비율 증가, 고품질의 전력 공급 등 에너지 문제와 관련한 현대 사회의 다양한 요구를 반영하기 위해 세계 각국에서는 전력 시스템의 변화를 시도하고 있다. 스마트그리드는 이를 위해 연구되고 있는 차세대 전력망으로 전력시스템과 정보통신 기술을 접목하여 지능화된 전력공급 서비스를 보장하는 지능형 전력망이다.

전기의 생산·공급을 전력사가 일방적으로 계획하고 결정하며, 모든 전력 자원을 전력사에서 제공하던 기존의 전력시스템과 달리 스마트그리드 환경에서는 다양화된 자원과 고객의 수요를 반영하여 실시간으로 전력공급을 조절하며, 자동화된 전력시스템이 전력 공급 과정에서 발생하는 다양한 이벤트에 적시에 대응함으로써 기존의 전력망에 비해 보다 경제적이고, 효율적인 전력 생산 및 공급을 할 수 있도록 지원한다.

이를 위해서 스마트 미터, 스마트 가전, HEMS (Home Energy Management System), 수요반응 기기 등 소비자 영역의 기기가 전력시스템에 연계되어 정보를 상호 교환한다. 또한, 송·배전시스템의 지능화를 위해서 배전망 상황인지를 위한 다양한 센서들이 배전망에 설치되어 송·배전망 운영시스템으로 정보를 제공하게 된다. 더불어 소비자에게 보다 자세한 전력정보(사용량 및 실시간 가격 등)를 제공하고, 사용자의 전력 사용 패턴에 따라 맞춤형 광고, 전기절약 프로그램 등 다양한 서비스를 제공하게 된다. 따라서 제한적인 외부 연계만 허용하던 기존 전력시스템은 스마트그리드 환경이 되면서 많은 외부 기기와 센서 및 서비스 제공 업체 등 다양한 개체와 연계를 허용하는 개방형 시스템이 된다. 이러한 점에 착안해 스마트그리드를 "에너지 인터넷"으로 표현하기도 한다[1].

하지만 현재의 인터넷 환경이 그러하듯 네트워크로 연결된 개방형 시스템에는 언제나 사이버 공격의 위협이 존재한다. 주요 운영시스템으로 접근하기 위한 경로가 기하급수적으로 늘어나는 것은 공격자에게는 다양한 공격 경로를 제공하는 장점이 되지만, 방어자에게는 수많은 연계 지점을 일일이 관리해야 공격자를 막을 수 있다는 어려움을 제공한다.

여기에 주요 사이버 공격 관련 학술대회에서 기반시설에 대한 공격기술이 발표되고[2-5], 주요 언론에서 전력시스템에 대한 사이버 공격 사실을 보도하는 등 사이버 공격의 대상이 기존 정보 시스템에서 주요 기반시설로 옮겨가고 있다는 사실도 스마트그리드의 보안 위협이 증가할 것이라는 사실에 힘을 더한다.

현대 생활에서 전기는 필수요소로 전력시스템에 사

* 한국전자통신연구원 부설연구소 (icezzoco@ensec.re.kr, seojt@ensec.re.kr, cheolee@ensec.re.kr)

〔표 1〕 국내 산업시설 정전 피해 사례(중앙일보, 2008.5.19)

일시	장소	피해추산액(억원)
'08년 5월	여수 국가산업단지	1,000
'08년 5월	기아자동차 소하리공장	86
'07년 8월	삼성전자 기흥공장	400

고가 발생해 전기 공급이 중단 될 경우 개인 생활 불편은 물론 산업전반에 큰 피해가 발생한다. 실제 국내 전력 공급 중단으로 산업 피해가 종종 발생하고 있다. 이와 관련하여, [표 1]에서 2007년과 2008년에 발생한 사례의 일부를 제시한다.

이에 스마트그리드를 자국에 구축하려는 세계 각국은 사이버 보안 위협을 최소화하기 위한 노력을 촉구하고 있으며, 이에 대한 대응으로 법, 연구 등에서 다양한 움직임이 보이고 있다.

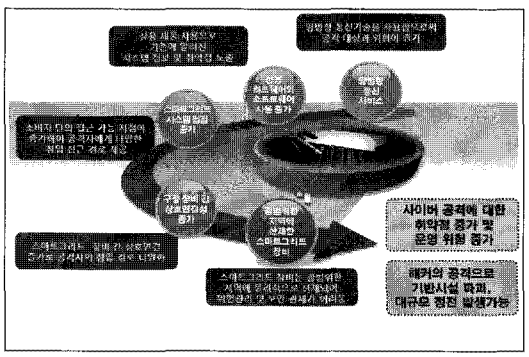
본 고에서는 스마트그리드의 보안 위협을 발생 시키는 환경 변화 및 보안 위협을 알아보고, 미국, 유럽 및 국내에서 이루어지고 있는 스마트그리드의 보안 수준을 제고하기 위한 다양한 활동에 대해 살펴본다.

Ⅱ. 스마트그리드 보안 위협

2.1. 스마트그리드 보안 위협 증가 요인

스마트그리드 환경은 기존 전력시스템과 많은 차이가 있다. [그림 1]은 이러한 차이 중 어떠한 변화가 스마트그리드의 보안 위협을 증가시키는 지를 나타내고 있다.

가장 대표적인 차이는 소비자 망의 시스템과 중앙의 운영 시스템 간 양방향 정보전달이 발생한다는 점이다.



〔그림 1〕 스마트그리드 보안 위협 증가 요소

기존 전력망에서는 소비자 망에서 중앙 전력 운영 시스템으로 정보제공을 위한 인프라가 필요하지 않았지만, 스마트그리드에서는 정보 수집 및 사용자 단의 요구사항 반영을 위해 정보획득이 필요하며, 이를 위한 인프라로 AMI(Advanced Metering Infrastructure) 및 송·배전 센서네트워크 등이 구축된다. 이는 곧 공격자에게 보다 다양한 공격경로를 제공하게 된다.

또한 스마트그리드 환경의 다양한 사용자 기기는 상용 소프트웨어를 많이 사용하게 되고, 통신 기술 역시 기존에는 전력시스템을 위한 전용 통신 프로토콜을 벗어나 WiFi, ZigBee 등의 상용 통신 기술을 많이 사용하게 된다. 이로 인해서 상용 소프트웨어 및 통신 프로토콜이 지니는 보안 취약점을 그대로 상속하게 되는 문제가 발생한다.

더욱이 스마트그리드 환경에서는 기존의 전력시스템과 달리 시스템의 개방성 및 연계성이 급속히 증가한다. 이는 곧 보안성이 취약한 소비자 네트워크의 기기에 대한 공격이 성공하면, 스마트그리드 운영 시스템에도 침투할 수 있는 가능성이 존재한다는 것을 의미한다. 또, 한 곳의 사용자 기기 및 운영시스템에 침투할 경우 다른 네트워크로 쉽게 침입 전이가 발생할 수 있다는 의미이기도 하다.

마지막으로 스마트그리드는 인터넷과 같이 전국 규모의 네트워크이며, 소비자 네트워크 역시 전국에 산재하게 되므로 네트워크 전체에 대한 세밀한 보안 관리가 어렵다. 이는 사이버 공격의 징후를 일일이 탐지하기 어렵게 만들고, 결국 사이버 공격의 대응이 늦어져, 그 피해를 증가시키게 될 수 있다.

2.2. 스마트그리드 보안 위협 사례

최근 전력 시스템을 포함한 스마트그리드 보안 위협 사례가 지속적으로 증가하고 있다. 특히 2010년 7월 발생한 스턱스넷(Stuxnet)[4-6]은 국가 기반시설에 대한 공격이 단순한 해커가 아닌 사이버전의 수단으로도 활용될 수 있음을 보여준 중요한 예다. 스턱스넷은 제어시스템을 대상으로 한 최초의 악성코드로 발전 제어시스템에서도 사용하고 있는 WinCC 및 Step7 소프트웨어서 발견되었다. 감염 후 제어시스템 네트워크 구조 및 데이터베이스 정보를 획득하는 시도를 하였으며, 실제 전력공급을 위한 물리적 장치의 동작을 제어하는 PLC(Pro-

grammable Logic Controller)에 접근하여 제어 명령을 내릴 수도 있음이 밝혀졌다. 이는 다른 악성코드와 마찬가지로 자가 복제 및 전파의 기능도 담고 있어, 하나의 시스템에 감염될 경우 스마트그리드 전체 시스템으로도 확산될 수 있으며, 이로 인해 전국규모의 정전도 유발할 수 있다.

이에 앞서 2009년 7월 세계 최대 해킹 컨퍼런스인 BlackHat USA에서는 스마트그리드의 스마트 미터 네트워크에 악성코드가 감염되고, 이 악성코드가 전체 네트워크로 전파될 수 있음을 보인바 있다[2]. 스마트 미터에 감염시켜 공격자가 임의 조작가능토록 하는 악성코드를 만들고, 이를 스마트 미터 소프트웨어 자동 업데이트 기능을 이용해 감염·전파 시킬 수 있음을 보였다. 실제 실험에서는 24시간 내에 이 악성코드를 이용해 15,000~20,000개의 스마트 미터가 감염될 수 있음을 보인바 있다. 스마트 미터에는 원격 전기 차단 기능이 있으므로, 스마트 미터에 악성 코드를 전파하는 것만으로도 특정 지역에 정전을 발생 시킬 수 있다.

또 2010년 BlackHat에서는 스마트그리드에 적용된 무선 통신망을 통해 흐르는 정보를 탈취하여 정보 내용을 파악할 수 있음을 보인 바 있다[3]. 이는 스마트그리드 환경에서 개인정보보호의 필요성을 보인 사례다.

Ⅲ. 국외 스마트그리드 사이버 보안 추진 현황

앞서 살펴본 바와 같이 향후 우리 생활 깊숙한 곳까지 파고들 스마트그리드 시스템은 현재의 인터넷 환경과 같이 다양한 보안 위협에 노출 될 수 있으며, 실제 사례에서 알 수 있듯 해커의 관심 역시 높아짐에 따라 다양한 공격 사례가 향후 지속적으로 발생 할 수 있다.

이에 스마트그리드에 관심이 있는 세계 각국은 자국의 "에너지 인터넷" 스마트그리드 보안성 향상을 위해 많은 노력을 기울이고 있다.

3.1. 미국의 스마트그리드 보안 현황

미국은 현재 스마트그리드 구축에 가장 큰 힘을 쏟고 있는 나라 중 하나다. 특히 2003년 북동부 대정전 이후로 자국의 전력시스템을 최신화하기 위해 많은 연구를 진행했으며, 2007년 에너지 독립 및 안보법(EISA, Energy Independent and Security Act of 2007)에서 스마트그리드의 개발을 법으로 명시한 바 있다.

EISA 2007은 미국 국립표준기술원(NIST, National Institute of Standards and Technology)으로 하여금 스마트그리드 상호운용성 및 보안을 위한 표준개발을 주도할 것을 명문화했다. 또한 2009년 4월 CNN 보도에서 미국 전력시스템에 악성코드가 감염된 사고 이후, 하원에서는 전력인프라 보호법을 발의 한 바 있다. 이 법은 전력기반시설을 사이버 공격으로부터 보호하기 위한 대책 마련을 촉구하고 있다. 게다가 2010년 6월에는 전력 신뢰도 및 인프라 보호법(GRID Act, Grid Reliability and Infrastructure Defense Act)이 미국 하원을 통과했다. 이 법은 미국 대통령 및 에너지규제기관(Federal Energy Regulatory Commission)에 미국의 주요 전력시스템에 대한 보안 절차수립, 취약점 분석 등을 수행할 것을 명문화 하고 있으며, 에너지부에 분석된 취약점에 대응하기 위한 보안 시스템 개발 및 도입을 명령하고 있다.

EISA 2007과 관련하여 NIST는 스마트그리드 상호운용성 표준 프로젝트를 수행하고 있다. 이 프로젝트 수행을 위해서 SGIP(Smart Grid Interoperability Panel)을 운영하고 있으며, 2010년 1월 스마트그리드 상호운영성 표준 프레임워크 보고서를 정식 발표했다[7]. 보고서에서 NIST는 스마트그리드 상호운용성 확보를 위해 적용 가능한 75개 표준 목록을 제시했으며, 이 중 25개 표준을 우선 검토해야 할 대상으로 지목했고, 우선 검토 대상 중 [표 2]의 7개 표준이 사이버 보안 표준이다.

3.2. NIST 스마트그리드 사이버 보안 가이드라인

NIST에서는 상호운용성 확보와 함께 스마트그리드 구축에서 가장 중요한 요소로 사이버 보안을 지목하고, 스마트그리드 전반에 걸친 사이버 보안에 대한 검토를 위해 사이버보안 워킹그룹(CSWG, Cyber Security Working Group)을 유일한 상설 워킹그룹으로 운영하고 있다. CSWG는 스마트그리드 보안 아키텍처, 가이드라인, 연구개발 이슈 도출, 상호운용성 표준의 보안관점에서 리뷰 등을 담당하고 있다.

이러한 활동의 결과로 CSWG는 2010년 8월 스마트그리드 사이버 보안 가이드라인을 발표했다. 이 가이드라인은 전력회사, 서비스 제공 업체 등 정부기관 및 산업체가 스마트그리드 구축 시 참조하여 체계적이고 안

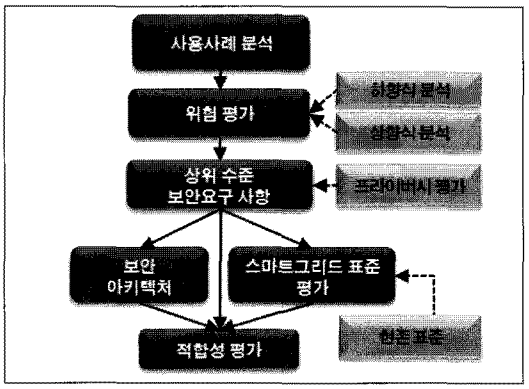
〔표 2〕 NIST에서 선별한 스마트그리드 상호운용성을 위한 우선 검토 표준 중 보안 표준 목록

번호	표준 제목	설명
1	Security Profile for AMI	AMI 솔루션 개발을 위한 보안 가이드라인
2	DHS Catalog of Control System Security : Recommendation for Standards Developers	물리적 공격 및 사이버 공격의 위협으로부터 제어시스템을 보호하기 위한 다양한 기관의 보안관행을 집대성
3	DHS Cyber Security Procurement Language for Control Systems	제어시스템을 위한 사이버보안 기술 조달 절차 수립 가이드라인
4	IEC 62351 Series	전력 시스템 제어 과정에서의 정보보안
5	IEEE 1686-2007	IED, PLC, RTU 등의 제어장치에 대한 보안 권고사항
6	NERC CIP 002-009	대규모 전력 설비에 대한 사이버보안 강화 권고사항
7	NIST SP 800-53, NIST SP 800-82	- 연방 정보시스템 보안 강화를 위한 종합적 보안 통제사항 - 안전한 제어시스템 구축을 위한 보안 가이드라인

전한 사이버 보안 아키텍처를 개발할 수 있도록 돕기 위해 개발되었다.

가이드라인은 스마트그리드 논리적 아키텍처 분석, 스마트그리드의 인터페이스에 적용 가능한 사이버 보안 통제사항, 암호 및 키관리 문제, 프라이버시 보호, 스마트그리드 보안 연구개발 이슈 등을 정리했다. 이를 위해 [그림 2]와 같은 사이버 보안 전략을 수립했다.

사이버 보안 아키텍처 수립을 위해 CSWG에서는 우선 Intelligrid 프로젝트, EPRI, SCE(Southern California Edison), UCAIug 등에서 제시한 스마트그리드 사용사례(Use Case)를 스마트그리드 중요 응용 분야를 중심으로 분석하였다. 여기서 중요 응용 분야는 AMI, 수요반응, 고객영역, 전력시장, 배전자동화, 전기자동차, 분산전원, 송전운영, 설비자산관리 등이다.



〔그림 2〕 NIST 스마트그리드 사이버 보안 수립 전략

둘째로 앞서 분석한 사용사례에 근거하여 스마트그리드 시스템의 위험분석을 수행했다. 이 때, CSWG는 AMI, 배전관리, 전력저장, 전기자동차, 수요반응, 광역 상황인식 등의 6대 우선 분야를 지정하여 위험분석을 수행했다. 위험분석 수행을 위해 6대 분야 서비스에 필요한 각 시스템을 정의하고, 시스템 간 정보교환을 위한 인터페이스를 명시하였다. 이렇게 도출된 130여개의 인터페이스를 보안 특성에 따라 22개 유형으로 분류하였고, 각각에 대한 특성, 취약점, 위협, 3대 보안요소(기밀성, 무결성, 가용성) 침해 시 피해수준을 분석하는 하향식 분석을 수행했다. 이와 더불어 AMI, 배전관리 등 그 구조가 명확한 시스템에 대해서는 시스템 단위로 취약점을 분석하는 상향식 분석도 수행하였다.

셋째, 위험평가 결과에 따라 각 시스템에 필요한 보안 통제사항을 제시하였다. 이 통제사항은 NIST Special Publication 800-53, NERC CIP(Critical Infrastructure Protection), DHS Catalog of Control System Security 등을 참조하여, 스마트그리드 시스템의 특성에 맞게 수정, 추가 하였다.

넷째, 상기 식별된 스마트그리드 논리적 인터페이스와 보안 통제사항을 활용하여, 스마트그리드 시스템을 구축하는 기관별 보안 아키텍처를 수립할 수 있도록, 인터페이스 유형과 보안 통제사항 사이의 맵핑 테이블을 제시하였다. 향후 AMI 시스템 구축 예정에 있는 기관에서는 구축 예정인 AMI 시스템이 가진 논리적 인터페이스를 정의하고, 이를 22개 유형에 맵핑시킨 후, 보안 통제사항 맵핑 테이블에 따라 보안 대책을 마련할 수 있도록 정책을 정의하면 될 것이다. 또, 이 과정에서 다양한 표준 중 보안에 안전한 표준을 적용할 수 있도록 CSWG에서는 현재 제시된 스마트그리드 표준이 적절한 보안 수준을 지니고 있는지 평가하고 있는 중이다.

마지막으로 2010년 하반기를 기점으로 적합성 평가 프로그램을 개발할 예정이다. 즉, 구축될 스마트그리드 시스템이 제시된 보안 가이드라인에 따라 안전하게 구성되었는지를 평가할 수 있는 프로그램을 개발하고, 이를 운영할 수 있는 체계를 제시할 예정이다.

NIST 스마트그리드 보안 가이드라인에서는 프라이버시 문제도 다루고 있다. 스마트그리드에서는 사용자의 에너지 소비 정보가 운영센터로 실시간 취합되어, 수요반응, 실시간 가격 결정 등 에너지 효율을 높이기 위한 서비스에 사용된다. 하지만 사용자의 에너지 소비 정보의 교환이 안전하게 이루어지지 않거나, 정보가 남용될 경우 개인 프라이버시 침해 가능성이 존재한다. 전력 소비 패턴을 분석하면, 시간대별 주로 사용하는 가전제품이 파악 가능하고, 개인의 생활 패턴도 파악 가능해지는 등 심각한 프라이버시 침해 문제가 발생한다.

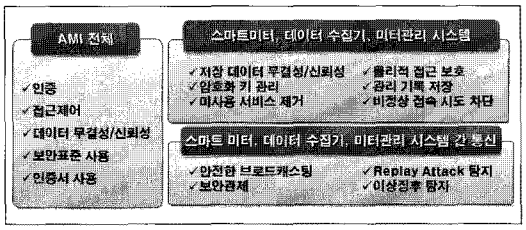
프라이버시 침해 문제가 발생할 경우 스마트그리드 구축에 반대하는 소비자의 움직임이 발생해 기술 도입이 늦어지게 될 것이다. 실제 2009년 네덜란드에서는 스마트 미터 설치를 의무화하고, 설치 거부 시 17,000 유로의 벌금을 부과하는 법을 제정하고자 했으나, 소비자 단체가 프라이버시 침해 문제를 제기하여 의무화 조항이 삭제된 사례가 있다.

이러한 프라이버시 침해 문제를 막기 위한 대책으로 가이드라인에서는 OECD 프라이버시 원칙에 따른 개인정보 정책을 수립할 것을 권고하고, 프라이버시영향평가 수행을 통해 프라이버시 침해 여지를 미리 분석하고, 이에 대한 대비책을 세울 것을 주장하며, 소비자에게 개인정보 위협과 완화 방안에 대한 지속적인 교육을 실시할 것을 제시하고 있다.

3.3. 스마트그리드 보안 가속화 프로젝트(ASAP-SG)

스마트그리드 사이버 보안을 강화하기 위해 시스템 수준의 스마트그리드 보안 요구사항 개발을 위한 민관합동 연구 프로젝트가 진행되고 있다. ASAP-SG (Advanced Security Acceleration Project - Smart Grid)로 명명된 이 프로젝트는 NIST 스마트그리드 보안 가이드라인의 틀 내에서 스마트그리드 세부 기술 별 보안 요구사항을 제시한다.

현재 1단계 과제가 완료되었으며, 현재 그 결과물로 AMI 구축 및 운영을 위한 보안 프로파일[8], 전력사업자와 서비스 제공 업체 및 전력 재판매 업체 간 정보 교환 과정을 위한 보안 프로파일[9], 배전 자동화 시스템 구축 및 운영을 위한 보안 프로파일[10] 등 3개의 보안 프로파일이 발표되었다.



〔그림 3〕 OPENmeter 프로젝트의 AMI 보안 요구사항

3.4. 유럽 스마트그리드 보안 추진 현황

유럽연합도 신재생 에너지 사용 및 국가간 에너지 거래를 위한 스마트그리드 구축에 관심이 높으며, 스마트그리드 사이버 보안 확보에 대한 중요성 역시 인식하고 있다. 따라서 유럽집행위원회에서 2011년 입법예정인 스마트그리드 프레임워크에는 사생활 정보와 데이터 보호 조항이 포함되었다.

또한 2009년 발표된 '유럽연합 명령 441'에 의거해 유럽전기통신표준협회(ETSI), 유럽표준화위원회(CEN), 유럽전기기술표준화위원회(CENELEC) 등 3개 표준화 단체가 나서서 진행 중인 유럽 스마트 미터 표준 개발 프로젝트인 OPENmeter에서는 보안 요구사항을 포함하는 스마트 미터 요구사항을 2009년 발표했다. 해당 프로젝트에서는 인가되지 않은 자의 정보 접근 및 수정, 권한을 획득한 해커에 의하여 전기, 수도, 가스 등의 차단, 스마트 미터와 미터 데이터 수집기 및 관리 시스템 등에 대한 DDoS공격 등을 AMI 보안 위협으로 정의하였고, 이를 차단하기 위한 보안 요구사항을 [그림 3]과 같이 제시하였다.

Ⅳ. 국내 스마트그리드 사이버 보안 추진 현황

국내에서도 스마트그리드 구축에 있어 사이버 보안의 중요성을 서서히 인식하고 있다. 따라서 스마트그리드 구축 촉진을 위한 법, 스마트그리드 국가 로드맵, 스마트그리드 실증사업, 연구개발 과제 등 다양한 분야에서 스마트그리드 보안성 강화를 위해 노력하고 있다.

우선 정부에서는 2010년 7월 '지능형 전력망 구축 및 이용 촉진에 관한 법률'을 입법예고하면서, 향후 안전하고 체계적인 스마트그리드 구축을 위한 법·제도 기반을 조성했다. 동 법에서는 스마트그리드를 위한 보안 대책이 필요함을 명시하면서, 개인정보 관리방안, 스마트그리드 보호대책 수립 및 시행, 스마트그리드 정보

보호 대책 수립 및 시행, 스마트그리드 침해행위 금지 등의 조항을 포함하고 있다. 이에 앞서 지식경제부에서는 2009년 기존의 '전력계통 신뢰도 및 전기품질 유지 기준'을 갱신하면서, 제 45조에서 전력망을 사이버 공격으로부터 보호하기 위해 전력IT 설비에 대한 정보보안 대책 수립 및 이행을 의무화 한 바도 있다.

또한 정부는 2010년 1월 국내 스마트그리드 추진의 청사진인 스마트그리드 국가 로드맵을 발표하면서 스마트그리드 보안을 주요 이슈로 다루고, 관련 기술 개발에 대한 로드맵을 발표했다. [그림 4]와 같이 동 로드맵에서는 안전하고 성공적인 스마트그리드 구축을 위해 5대 추진 분야에서 기술개발, 사업화, 표준 및 보안, 제도 등에 대한 실행 로드맵을 제시했다. 특히 '안전한 스마트그리드 구축 및 운용을 위한 보안 체계 구축'을 정부의 정책과제로 선정하고, 보안 인프라 구축을 위해서 올해까지 스마트그리드의 안전한 구축을 위한 보안 가이드라인을 마련하며, 향후 국가단위 스마트그리드에 적합한 보안 체계를 구축 지원하고, 스마트그리드 보안성 유지를 위한 보안 표준 마련 및 보안 인증제도 운영 등의 내용이 포함되어 있다.

더불어 현재 제주도에 구축되고 있는 스마트그리드 실증단지 보안대책 역시 그 중요성이 충분히 인식되고 있으며, 스마트그리드사업단을 통한 보안센터 및 보안 WG 구성, 보안지침 및 보안가이드라인 제시, 각 운영센터별 보안대책 수립 및 이행 등 다각도로 추진되고 있다. 특히 보안센터에서는 실증단지 구축이 완료되는 시점에 맞추어 각 컨소시엄의 스마트그리드 시스템에 대해 취약성 분석을 수행할 예정이며, 이를 통해 발견된 취약점을 개선토록 함으로써 보다 안전한 실증단지를 구축할 계획이다. 또한 실증단지 보안 침해 대응 매뉴얼 개발 및 보안 침해 대응 훈련을 통해 사고 발생 시 각 컨소시엄이 신속히 대응하여 피해를 최소화 할 수 있도록 체계를 구축할 예정이다.

〔그림 4〕 스마트그리드 국가로드맵에 제시된 보안 기술

마지막으로 스마트그리드 보안성 강화를 위한 보안 기술을 개발하기 위한 "국가 스마트그리드 보안 체계 연구"가 수행될 예정이다. 동 과제에서는 향후 구축될 국가단위 스마트그리드에 적합한 보안체계를 개발하는 것을 목표로, 스마트그리드 보안모델을 연구하고, 스마트그리드 보안체계를 개발한다. 이를 통해 국가 스마트그리드에 필요한 보안체계를 수립하고, 새롭게 연구개발이 필요한 스마트그리드 보안 기술을 식별하는 등 안전한 국가 스마트그리드 구축과 운영에 기여할 것으로 예상된다.

V. 결론

본 고에서는 국내·외의 스마트그리드 보안 추진 현황에 대해서 살펴보았다. 스마트그리드는 기존의 전력망과 달리 양방향 서비스가 증가하고, 개방화 및 네트워크화 되므로 기존의 인터넷과 같이 사이버 공격에 노출될 가능성이 매우 높다. 이에 미국을 중심으로 유럽 등의 스마트그리드 구축에 관심이 높은 선진국에서는 스마트그리드 보안의 중요성과 필요성에 대해 깊이 공감하고 있으며, 이를 위해 법, 제도, 표준제정, 연구개발과제 수행 등 다각도의 노력을 수행하고 있다. 국내에서도 이러한 세계의 움직임에 발맞추어 스마트그리드 보안 위협의 심각성을 인지하고, 법 제정, 보안체계 연구 수행, 실증단지 내 보안대책 마련 등 스마트그리드 보안성 강화를 위한 노력에 최선을 다하고 있다.

스마트그리드 구축 초기부터 사이버 보안을 고려한 연구개발을 수행하여, 인터넷이 겪고 있는 어려움을 다시 겪지 않도록 해야 할 것이다. 이는 곧 한국이 세계 스마트그리드 선도 국가로 나서기 위한 또 하나의 도전과제라 할 수 있다.

참 고 문 헌

[1] T. L. *Friedman, Hot, flat, and crowded: Why We Need a Green Revolution - And How It Can Renew America*, Large Print Press, 2009.

[2] M. Davis, "Smart Grid Device Security: Adventures in a new medium", BlackHat USA 2009.

[3] S. Moyer, N. Keltner, "Wardriving the Smart

Grid: Practical Approaches to Attacking Utility Packet Radios", BlackHat USA 2010.

[4] L. O'Murchu, "Stuxnet - Infecting Industrial Control Systems", Proceedings from Virus Bulletin Conference, 2010.

[5] A. Gostev, C. G. Raiu, "Unravellling Stuxnet", Proceedings from Virus Bulletin Conference, 2010.

[6] N. Falliere, L. O'Murchu, E. Chien, *W32.Stuxnet Dossier*, Semantec Security Response, 2010.

[7] Office of the National Coordinator for Smart Grid Interoperability, *Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, NIST Special Publication 1108, NIST, Jan. 2010.

[8] The Advanced Security Acceleration Project (ASAP-SG), *Security Profile for Advanced Metering Infrastructure*, UCA International Users Group, Jun. 2010.

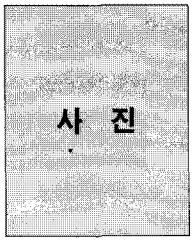
[9] The Advanced Security Acceleration Project (ASAP-SG), *Security Profile for Third Party Data Access*, UCA International Users Group, Jan. 2010.

[10] The Advanced Security Acceleration Project (ASAP-SG), *Security Profile for Distribution Management*, UCA International Users Group, Aug. 2010.

〈著者紹介〉

이 건 희 (Gunhee Lee)
정회원

2001년 2월 : 아주대학교 정보및컴퓨터공학부 졸업
2003년 2월 : 아주대학교 정보통신전문대학원 정보통신공학과 석사
2009년 2월 : 아주대학교 정보통신전문대학원 정보통신공학 공박사학
2009년 3월~현재 : 한국전자통신연구원 부설연구소 연구원
관심분야 : 스마트그리드 보안, 제어시스템 보안, 유무선 네트워크 인증 및 키 관리



서 정 택 (Jung-Taek Seo)
정회원

1999년 2월 : 충주대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2007년 2월 : 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년~현재 : 한국전자통신연구원 부설연구소 선임연구원/과제책임자
관심분야 : 스마트그리드 시스템 및 통신 보안, 제어시스템 보안, 제어시스템 통신 프로토콜 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응

이 철 원 (Cheol-Won Lee)
정회원

1987년 2월 : 충남대학교 수학과 졸업
1989년 2월 : 중앙대학교 전자계산학과 석사
2009년 8월 : 아주대학교 컴퓨터공학 공학박사
1989년~1994년 : 한국전자통신연구원 선임연구원
1994년~2000년 : 한국정보보호진흥원 선임연구원/과제책임자
2003년~2004년 : Texas A&M University 방문연구원
2001년~현재 : 한국전자통신연구원 부설연구소 책임연구원/본부장
관심분야 : 사이버 안전, 정보보호시스템 평가, S/W 안전성 분석, 산업보안 등