情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

스마트 그리드 보안 동향

정 영 곤*, 최 현 우*, 염 흥 열**

요 약

세계적으로 그린에너지에 대한 관심이 높아지고 있는 시점에 기존의 전력망에 IT기술을 결합하여 보다 효율적이고 친환경적인 지능형 전력망을 이루는 스마트 그리드 사업이 활발히 전개되고 있다. 우리나라에서도 국가차원의 적극적인 스마트 그리드 구축을 위한 로드맵을 확정하고 이에 기반한 실행계획을 실행하고 있다. 한국의 좁은 국토는 국가단위의 스마트 그리드 구축에 좋은 이점으로 작용하여 세계최초의 스마트 그리드 모델 국가가 될 것으로 예상된다. 한편, 이러한 순기능에 더해 역기능으로 전력망에 IT기술을 적용함에 기인해 다양한 위협 시나리오가 나타날 수 있다. 이 위협을 효과적으로 대응하는 것이 보안 기술이며, 스마트 그리드의 보안 기술은 스마트 그리드 사업의 성패와 직접적으로 연결되는 중요한 요인이 된다. 또한, 이를 제도적으로 지원하는 정보보호관련 법제도도 매우 중요하다. 본 논문에서는 스마트 그리드의 필요성 등을 살펴보고, 스마트 그리드 보안 위협, 위협 대응을 위한 산업체 이니셔티브 등의 국내외 추진 동향을 분석한다.

Ⅰ. 서 론

전 세계가 환경파괴의 심각성을 인식하고 이에 대응하기위하여 국제적으로 회의 및 연구가 활발히 진행되고 있다. 지구의 환경을 침해하는 가장 큰 요인으로 제한된 자원으로 에너지 생산과 소비를 하고 그에 발생되는 환경오염이 꼽히고 있다. 신재생에너지의 개발과 효율적인 사용은 에너지를 절약하고 소비하여 궁극적으로는 환경의 오염과 에너지의 낭비를 감소시키는 역할을 하게 한다. 스마트 그리드는 위와 같은 문제를 해결할 수 있는 기술중 하나이다.

국가단위의 스마트 그리드를 실현시키기 위해 가장 적합한 나라의 요건으로 좁은 국토와 발전된 IT기술이 있다. 그런 면에서 우리나라는 넓지 않은 국토와 그 어느 나라보다도 잘 정비된 IT기반 시설을 가지고 있기 때문에 이런 이점들을 이용한다면 세계 최초로 국가차원의 스마트 그리드의 건설이 가능할 것으로 보인다. 2009년 7월 선진8개국(G8) 확대정상회의에서 한국이 '스마트그리드' 개발을 주도할 선도국가로 선정되었다. 한국은 "저탄소 녹생성장"이라는 비전으로 세계 최초의 국가단위 스마트 그리드를 2030년까지 구축할 계획을 가지고 스마트 그리드의 선도국가로 국제화를 주도할 계획을 가지고 있다. 그 첫 번째 계획으로 세계 최대의 스마트 그리드 실증 사업이 우리나라에서 본격적으로 추진되었다. 제주에 건설될 실증단지는 스마트 그리드의 주요 분야를 모두 포함시켜 세계에서 처음으로 모든 요소들이 구현된 실증단지로 한국의 스마트 그리드 기술을 시험하고 평가할 수 있는 곳이 될 것이다.

어느 IT기술에서나 보안이라는 요소는 배제할 수 없는 가장 큰 부분이다. 더군다나 국가단위의 스마트 그리드에서의 그 중요성은 가히 엄청나다고 볼 수 있다. 한 나라의 전력망이 악의적인 행동이든 예상치 못한 시스템 오류에 의해서든 스마트 그리드로서의 제 기능을 하지 못한다면 개인 및 기업의 재정적 손해 뿐 아니라 한 나라의 막대한 경제적 손실을 가져올 것이다. 이런 보안의 중요성이 대두되고 있지만 현재 국내의 스마트 그리드 보안 기술은 먼저 도입하고 추진하고 있는 미국과 유럽에 비해서는 뒤처져 있는 것이 사실이지만 그 차이는 크지 않아 곧 따라잡을 수 있을 것이라고 예상한다. 스마트 그리드의 기반구조을 기능과 보안을 고려하여 잘 정비하고 운용한다면 그 무엇보다도 안전한 스마트 그리드가 될 수 있을 것이다.

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2010-(C1090-1031-0005))
* 순천향대학교 정보보호학과 석사과정 ({ygjung, zemisolsol}@sch.ac.kr)
** 순천향대학교 정보보호학과 교수 (hyyoum@sch.ac.kr)

본 고에서는 Ⅱ장에서 스마트 그리드의 개요를 소개하고, Ⅲ장에서 스마트 그리드에서 보안의 필요성을 살펴보며, Ⅳ장에서 스마트 그리드와 연관되는 산업체 주요 활동을 제시하며, Ⅴ장에서 국내외 법제도 현황을 살펴보고, Ⅵ장에서 결론을 제시한다.

Ⅱ. 스마트 그리드

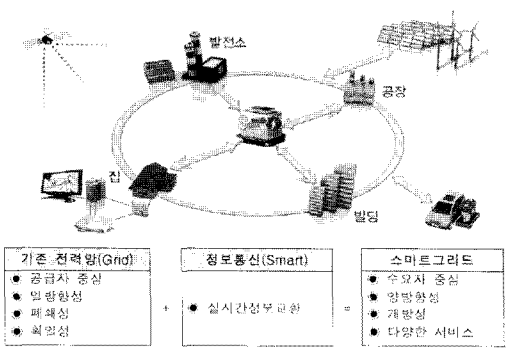
2.1 스마트 그리드의 개념

스마트 그리드의 개념을 보면 각 나라별로 그 정의가 다르지만 그 맥락은 비슷하다. 국내에서는 국가단위의 스마트 그리드를 추진하고 있는 지식경제부에서 완성한 '스마트 그리드 국가 로드맵'에서는 스마트 그리드를 "기존의 전력망(Grid)에 ICT(Information & Communication Technology) 기술(Smart)을 접목하여, 공급자와 소비자가 양방향으로 실시간 전력 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망"으로 정의하고 있다(지식경제부, 2010)[1].

기존의 전력망은 발전소에서 전력을 생산하고 배전 시설을 이용하여 각 가정이나 기업 등의 소비자에게 공급하는 구조를 보이고 있다. 이런 단순한 전력망의 기능에 ICT 기술을 접목하여 전력의 생산과 공급, 소비에 이르기까지 공급자와 소비자 사이에 양방향 통신을 가능하게 함으로서 기존의 전력망에 보다 스마트하고 향상된 가용성, 효율성, 안정성을 보장한다.

2.2 필요성

기존의 노후된 전력망과 비효율적인 전력 시스템으로 인하여 에너지의 낭비가 심하다. 기존의 전력 송·변전 방법을 살펴보면 전력은 교류로 생산하고 송전은 고압으로 변전하며, 다시 소비단계에서는 저압 교류로 변전한다. 송·변전하는 과정에서 손실되는 에너지의 양은 적지 않다. 현재 집중되어있는 대규모 발전 및 송전시설을 소규모로 분산한다면 손실되는 에너지의 양을 줄일 수 있을 것이다. 중앙의 거대한 집중형 전력 시스템으로 인하여 대규모의 정전사고 발생 가능성이 있고 그로인하여 발생 가능한 피해의 규모 또한 커질 수 밖에 없다.



[그림 1] 스마트그리드 개념[1]

전력을 생산하기 위해서는 자원이 필요하다. 전력 생산에 필요한 자원의 형태는 일반적으로 매장량이 유한한 석유, 석탄, 가스 등 화석연료가 될 수도 있고, 그 양이 무한한 태양열, 지열, 풍력 등 천연자원이 될 수도 있다. 우리나라는 화석연료의 빈국으로 세계적으로 고갈되어가고 있는 원자재와 가격의 상승에 손 놓고 있을 수 없는 상황이다. 이런 유한한 자원의 에너지 화와 온실가스의 배출은 환경을 파괴하는 주요인 이다. 스마트 그리드는 친환경적인 에너지의 생산과 효율적인 에너지 사용으로 기후변화에 대응할 수 있다. 세계적으로 스마트 그리드에 대한 관심과 필요성이 증가함에 따라 그에 따른 관련 시장의 경제규모는 커지고 있다. 이런 상황에 국가차원의 스마트 그리드 건설로 관련산업(통신, 가전, 건설, 자동차, 에너지 등)의 발달은 물론 세계 스마트 그리드 시장에서 경쟁력을 확보함으로서 결과적으로 우리나라의 차세대 국가 수입원이 되어 경제발전의 원동력이 될 것이다.

2.3 기대효과

시작 단계인 스마트 그리드가 20년후인 2030년에 완성을 목표로 연구되고 개발되는데 그에 따른 여러 효과를 예상해 보고 현재의 단순한 전력망을 IT가 결합된 똑똑한 지능망으로 변화하는 과정과 그의 결과에 따른 기대효과를 살펴본다.

▷ 기후변화의 억제 및 보호

화석연료 사용의 감소로 지구 기후변화의 주범이였던 탄소의 배출량을 감소시킨다. 날이 갈수록 고갈되는 화석연료와 그에 따라 증가하는 원자재 가격에 자원이 희박한 우리나라에서는 새로운 대안이 필요했고 그 해결책으로 스마트 그리드가 선택 되었다. 비싼 화석연료 대신 태양열, 풍력 등의 천연자원으로 전기에너지를 생산하고 공급하여 환경보전에 이바지한다.

▷ 효율적인 에너지 사용

공급자와 소비자 간에 실시간 양방향 통신으로 소비자가 실시간으로 전기요금의 정보를 받아 자발적으로 전력수요가 많은 시간대의 전기사용을 줄일 수 있다. 피크타임의 전력 수요로 순간 요구되는 고용량의 전력을 생산하고 송·배전하는데 오버되는 자원을 절약할 수 있다. 또한 소비자로부터 적극적인 에너지 절약 의식을 불러 일으켜 에너지 과소비를 억제한다. 상대적으로 전기요금이 저렴한 저녁이나 새벽시간대의 전기를 이용하여 전기자동차의 충전, 전기온수·난방 등에 사용한다.

▷ 신·재생 에너지의 확산

각 가정마다 태양열이나 풍력의 신에너지를 생산함으로써 전기를 저장하고 소비 할 수 있다. 가정에서 만든 에너지를 1차적으로 소비하고 남은 에너지는 저장해 두거나 거래한다. 풍력, 태양열, 지열 등을 이용한 발전소의 건설로 다양한 품질의 전력이 제공됨에 따라 품질 등급에 적절한 공급을 한다.

▷ 가용성 및 신뢰성의 향상

자능화된 전력망으로 전력을 원격으로 제어하여 고장을 감지하고 치유하는 기능을 제공한다. 자동으로 고장 지점을 찾아내고 대체 경로를 찾아 연결하여 전력공급의 가용성을 향상시킨다. 정전으로 인한 피해가 큰 산업체에서의 전력차단을 미연에 방지하여 물질적 경제적 손해를 줄일 수 있다. 전력 공급에 대한 가용성의 증가로 높은 신뢰도를 가져다 준다.

▷ 신성장동력 창출

정부의 스마트 그리드 사업에 민관 공동으로 27조 5000억원을 투자하여 수출 전략사업으로 육성할 계획을 가지고 있다. 이에 발생되는 효과로 국내 일자리 창출 및 스마트 그리드와 관련된 통신, 자동차, 가전 등의 산업 전반에 걸쳐서 많은 발전이 예상된다. 이에 따라 우리나라는 IT시장에 이어 거대한 세계 스마트 그리드 시장에서 국가 경쟁력을 향상시켜 국내 기업의 이익을 가져와 국가 경제발전의 원동력이 될 것이다.

Ⅲ. 스마트 그리드 보안

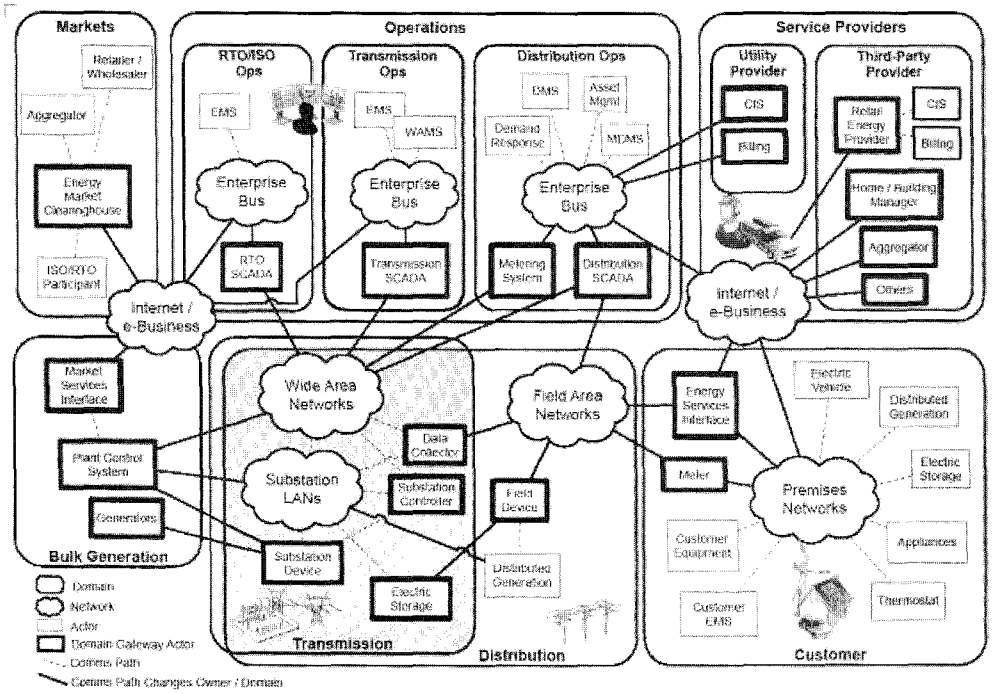
3.1 공격 시나리오

2003년 8월 뉴욕 전체를 단 몇 초 만에 암흑으로 뒤덮은 정전사건은 미국 역사상 ' 최악의 대정전' 사태로 기록되고 있다. 뉴욕을 중심으로 캐나다를 비롯하여 미국 북동부 지역 일대를 25시간동안 무능화 시켰다. 5천만 명이 피해를 입었고 통신, 교통, 의료 등 모든 경제활동이 마비되었고 그에 따른 경제적 손실은 어마하여 손실액으로 약50억 달러를 예상하였다. 이런 과거의 사건들로 보아도 전력망은 그 무엇보다 보안이 중요시 되는 기반시설이다.

많은 언론매체에서 스마트 그리드의 보안에 대하여 언급하고 있지만 보안이라는 것은 경험하지 않고는 피부로 그 중요성을 느끼지 못하는 것이 현실이다. 스마트 그리드는 IT와 연결한 지능형 전력망이다. 기존의 전력망보다 그 위험성은 커진 셈이다. 만약에 국가 차원의 스마트 그리드가 악의를 가진 해커에 의해 장악된다면 끔찍한 결과를 도래할 것이다. 간단히 예상해 보면 교통마비(지하철 운행중단, 교통신호시스템 정지, 항공기 운행중단 등)가 될 것이고 생명과 직접적으로 연관된 병원시설 운영의 한계로 환자의 위험이 증가할 것이다. 금융업계의 시스템 중단에 따라 경제체계가 무너질 것이며 국방·민생치안과 관련된 비상통신 시스템의 마비에 따라 국가 전체가 혼란에 빠져 한나라가 전쟁과 같은 위기를 가져올 것이다. 대부분의 나라에서 전력망은 국가의 기본 인프라로 간주하여 자체적으로 폐쇄적 운영공간에서 관리하였다. 그러나 신재생에너지의 활성화와 스스로 작은 단위의 전력을 생산·소비하고 제어하는 스마트 그리드에서는 폐쇄적 운영이 더 이상 불가능하게 되고 개방적으로 변하여 기본 중요부분만 폐쇄적으로 관리할 것이다. 각 가정, 기업 등 전기를 소비하는 곳마다 스마트 미터기가 설치될 것이고 이 수천만개의 스마트 미터를 사용하는 소비자들 중 작게는 전기요금을 적게 내거나 안내고자 해킹을 시도할 수도 있고 크게는 전력시스템에 접근하여 더 큰 이익을 내려고 해킹하는 경우도 있을 것이다. 지금의 시작단계에서부터 체계적인 계획으로 보안을 고려한 스마트 그리드를 완성해 가야 할 필요성을 가진다.

3.2 NIST에서의 스마트그리드 사이버보안

미국의 NIST는 2010년 2월에 'Smart Grid cyber Security Strategy and Requirements'라는 제목으로 두 번째 드레프트 문서를 발표하였다[2]. 이 문서는 NIST를 중심으로 350개가 넘는 개인이나 학계, 공공기관, 연방관리기구 등이 참여하여 작성되어지고 있다. NIST 스마트 그리드의 개념을 [그림 2]와 같이 스마트 그리



〔그림 2〕 NIST의 컨셉 모델[2]

드는 크게 전력 소비자, 서비스 공급자, 전력 송배전, 전력망 운영 및 제어, 전력 거래시장, 그리고 전력발전 등으로 구성하였다. 종합적인 사이버보안 요구사항 세트는 스마트그리드를 위한 사이버보안 전략을 정의하는 높은 수준의 위험 평가 프로세스를 사용하여 지속적으로 개발하고 있다. 이 문서에는 기능적인 아키텍처 개발, 상향식 평가, 프라이버시, 표준, 연구/개발, 취약점 분석의 내용이 포함되어 있고 대략적인 내용은 다음과 같다. 기능적이고 논리적인 구조를 개발하기 위해서 각종 워크샵의 결과와 로드맵으로부터 유즈케이스와 요구사항을 분석하여 반영한다. 상향식 보안 분석 부분에서는 추가적인 특별하거나 그렇지 않은 사이버 보안 문제/이슈들과 새로운 설계 고려사항 부분에 추가하였다. 프라이버시 부분에서는 어떤 데이터가 수집되어지고 생산되어질 것인지에 초점을 두고, 스마트 그리드의 부분에 컨슈머-유틸리티를 위한 프라이버시 영향 평가를 수행한다. 표준 부분에서는 사이버보안에 적용할 수 있는 표준들과 특징들을 정리하였다. 연구개발 부분에서는 이슈(장치레벨, 새로운 메카니즘, 시스템레벨, 네트워크이슈, 다른 보안이슈) 별로 급하게 요구하는 연구개발 주제를 정리하고 있다.

3.2.1 사이버보안 위험 평가 프로세스

스마트 그리드를 위한 전반적인 사이버보안 전략은 기반구조의 다른 부분을 연결하는 솔루션들의 상호연결성을 보장하기 위한 전략을 개발할 때에 도메인의 특성과 공통의 요구사항들을 검토한다. 가장 주된 목적은 예방에 있다. 그러나 대응 및 복구 전략은 전자 시스템 상에서 사이버공격의 발생 후에 개발되어야 한다[2]. 사이버보안 전략을 수립하는데 있어서 종합적인 사이버보안 위험 평가 프로세스의 정의와 수립이 요구된다. 위험 평가 프로세스는 현재 알려져 있는 취약점과 위협 등으로 구성되어 있기 때문에 항상 새로운 업데이트가 필요하다. NIST에서 보안 요구사항들과 분석을 지원하는 것은 유틸리티들이나, 기업, 기관에서 그들의 위험 평가 프로세스에 적용에 사용되어 질 것이다. 이러한 정보들은 다양한 구성원들의 위험평가와 적절한 보안의 선택이 아닌 필수가 되는 가이드라인으로 제공될 것이다.

3.2.2 가용성, 무결성, 기밀성

기존의 IT에서는 기밀성을 우선시하고 가용성, 무결

성을 고려하였지만 전력망에서는 가용성을 우선으로 하고 그다음으로 무결성, 기밀성 순으로 고려하였다. NIST에서는 전력망에서 요구되는 가용성, 무결성, 비밀성을 다음과 같이 제시하였다[2].

가용성 : 가장 중요한 보안 요소로서 가용성과 관련된 잠재시간이 달라질 수 있다.

- 4ms(보호계전)
- 초단위이하(광대역 상황인식 모니터링 전송)
- 초단위(변전소와 SCADA에 공급하는 데이터)
- 분단위(비교적 중요하지 않은 장치와 시장 가격정보 모니터링)
- 시간단위(검침과 긴 간격의 시장가격정보)
- 일/주/월단위(전력 품질 정보와 같은 긴 간격의 데이터 수집)

무결성 : 전력시스템 운영을 위한 무결성은 다음과 같은 보장을 포함한다.

- 데이터는 권한없이 수정되어지지 않는다.
- 데이터의 자원은 인증된다.
- 데이터와 연관된 타임스템프는 알려져 있고 인증된다.
- 데이터의 질은 알려져 있고 인증된다.

기밀성 : 온라인에서 소비자 정보의 가용성이 증가함에 따라 기밀성이 중요하다.

- 프라이버시, 전력시장정보
- 일반적인 기업정보(payroll, 내부 전략 계획 등)

Ⅳ. 스마트 그리드 산업체 이니셔티브 현황

4.1 시스코(CISCO)

4.1.1 보안환경 및 고려사항

시스코에서는 스마트 그리드를 구성하는데 있어서 생각해볼만한 보안 사항들을 몇 가지 제시하였다[3]. 기업에서 언급하는 스마트 그리드의 특별한 보안 고려사항들을 살펴보면 새로운 기술에 통신망을 적용하는데 있어서 생각할 수 있는 일반적인 사항들이다. 스마트 그리드의 특징을 고려하여 초기에 보안을 고려하여 기반구조를 설계하고 그 후에도 지속적인 보안의 평가와 유지가 필요하다.

규모 확장성 : 넓은 지역에 전력망을 공급하는데 필요한 통신 기반구조는 인터넷보다 커지게 될 가능성이 있다. 그로인하여 대규모 네트워크에서의 보안은 세그멘테이션, 방대한 엔티티들의 신원관리, 데이터의 무결성과 기밀성을 위한 키들의 관리, 다양한 유무선 커뮤니케이션 메카니즘의 결합과 같은 도전 과제들을 제시한다.

기존 장치 고려 : 어떤 단계에서든지 스마트 그리드의 보안을 설계하는데 있어서 기존에 존재하는 시스템들이 기본적으로 가지고 있는 기능 및 특성들과 결합이 가능해야 한다.

필드 로케이션 : 미터기, 변압기, 스위치들과 같은 필드 장치들의 물리적 보안은 하나의 중요한 설계 고려사항이다. 하지만 그것들은 잠재적으로 취약하다. 전력망의 무결성을 위해서 필드 장치들에 의존하지 않은 네트워크 보안 설계가 요구된다.

보안의 문화 : 몇몇 사람들은 만약 스마트 그리드 데이터 통신 네트워크가 독립적이고 라우팅 될 수 없는 프로토콜로 설계되어진다면 안전하게 될 것으로 믿고 있다. 하지만 사실상 공개되어 사용되어지는 보안 시스템들의 취약점들은 긴 시간동안 밝혀지지 않은 채로 남아있을 수 없다. 그렇지만 이렇게 공개적으로 사용되어지는 보안 시스템들을 보면 취약점들은 독점적으로 사용되어지는 시스템보다 더욱 빠르게 발견되고 해결된다.

표준과 규정의 발전 : 스마트 그리드 개발의 초기단계인 이 시점에 벤더들은 다양한 표준과 독점적인 메카니즘을 사용하여 보안 통제를 개발하려고 한다. 이것은 약한 상호연결성과 관리를 어렵게 만들 수 있다. 이런 이른 활동들은 테스트의 한계와 종종 신뢰하지 않은 결과를 가져오게 된다.

4.1.2 요구사항

위에서 제시한 고려사항들을 바탕으로 시스코에서는 스마트 그리드의 주요 기능을 보호하는 세개의 보안 영역(소비자 운영, 상호 협력, 원격제어시스템)으로 정의하였다. 이 영역을 기반으로 한 모델은 전력망에서 다양한 유틸리티들을 지원하고, 토폴로지나 네트워크 전송에서 독립하여 전력망의 보호를 제공한다[3].

소비자 운영(Customer operations)

소비자 운영 영역에서는 소비자 에너지 관리와 요구

[표 1] JUNIPER NETWORK 스마트그리드 보안 솔루션 요소[4]

Security Solution	Function
방화벽	- 상태기반감시와 지역 네트워크의 세분화로 중요한 데이터 스트림을 독립적으로 보호 - DoS나 DDoS공격으로부터 brute force 예방 - 안티바이러스, 안티스팸, URL필터링 등
침입방지	- 어플리케이션/프로토콜/세션/트레픽 흐름 인식 - 시그니쳐, 프로토콜 변조, 백도어, 트래픽 등의 다양한 탐지방법
사용자 접근통제	- 사용자 역할, 장치, 위치별 비지니스 정책 시행 - IPS와 결합하여 모니터하고 확인
네트워크 이상탐지	- 네트워크/자산 프로파일링과 흐름 분석 - 설계된 네트워크 행위와의 비교로 경보
데이터 가속과 암호	- Site-to-site 최적화와 보호
중앙,역할기반 관리	- 장치 라이프 사이클의 통합된 네트워크 관리와 중앙 자동화 - 전체 보안 포트폴리오 운영 - 유통성과 확장성

반응, 전력 분배, 원격 검침을 위한 정책과 절차가 정의된다. 시스템과 장치 사이에는 소비자 데이터를 수집/처리하고 특별한 보안 요구사항을 가지고 있는 스마트 미터, 소비자 포털, 요구반응 시스템이 존재한다.

- 미터기 부정예방 : 물리적인 미터의 조작을 비롯하여 유틸리티는 미터기들이 거짓장치로 교체되지 않고 데이터가 조작되지 않음을 반드시 보장해야 한다.
- 전력망 무결성 : 필드에 있는 장치가 외부 공격자로부터 타협되었을 경우에 전력망은 인증되지 않은 명령, 네트워크로의 접근, 서비스거부 공격으로부터 상위네트워크를 보호해야 한다.
- 프라이버시 : 소비자의 에너지 사용 정보는 유틸리티로 전송되고 유틸리티의 데이터센터에 저장되는 것을 반드시 보장해야 한다.

인가된 사람과 장치를 제한하기 위해서 소비자 에너지 관리 시스템은 명령과 데이터의 무결성 보장, 인증된 장치, 타협된 장치로부터의 데이터 보호가 반드시 가능해야 한다.

상호협력(Corporate)

위의 '소비자 운영'의 특징과 기능에 더하여 이메일, 인터넷, 전화, 메세지, 다양한 어플리케이션과 같이 비즈니스에 필요한 IT기능을 위한 보안을 포함한다. 이러한 요구사항들을 해결하기 위한 것으로 시스코는 상호운영성을 위해 일관적인 보안 정책과 모든 제품 라이에 걸쳐 네트워크의 검증되고 안전한 IP 아키텍처 집중, 정보교환이 가능한 네트워크과 보안기술에 전념한다.

원격제어시스템(Telemetry and control systems)

탐지와 고장의 수리 기술들은 정전, 침입, 에러 발생으로부터 전력의 재경로를 쉽고 빠르게 만든다. 이 영역에서 가용성, 데이터 무결성, 감사와 기밀을 유지하기 위한 세부사항은 다음과 같다.

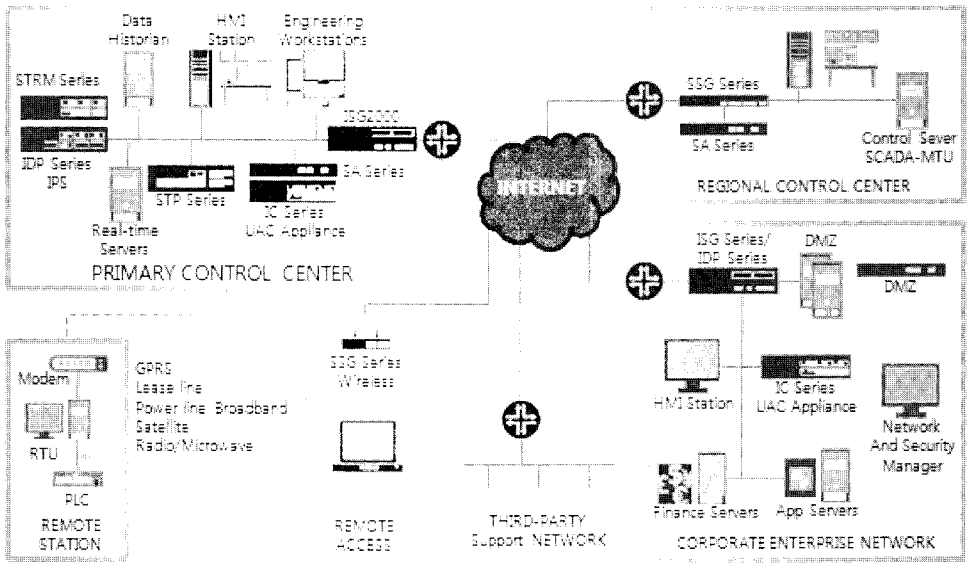
- 가용성 : 기술자와 장치의 인증, 네트워크 서비스와 기능의 접근통제, 사이버 보안 사고에 대한 격리, 재경로 설정, 회복, 서비스거부 공격으로부터의 보호
- 데이터 무결성 : 기술자와 장치의 인가, 원격 데이터와 SCADA(Supervisory Control And Data Acquisition) 명령의 무결성, 컴퓨터 무결성 증명, 잘못된 반응의 보호를 위하여 다른 센서들의 간에 긴급데이터의 상호작용
- 감사와 비밀 : 규제의 준수를 확인하고 포렌식 분석을 가능하게 하고 데이터암호, 침입예방, 침입탐지 적용

4.2 주니퍼 네트워크(JUNIPER NETWORKS)

4.2.1 보안환경 및 고려사항

Juniper Networks에서 생각하는 스마트 그리드의 보안 제품을 적용하는데 있어서 발생하는 보안 문제점을 다음과 같이 정의하였다[4].

- 취약점과 사이버 사고 : 고의적이나 고의적이지 않은 위협/취약점은 존재



〔그림 3〕 종합적인 네트워크기반 보안(JUNIPER NETWORKS)〔4〕

- 광역네트워크의 한계 : 다양한 유틸리티 운영자는 각기 다른 유틸리티, 소비자끼리 상호 연결
- 운영의 장애 : 네트워크상의 다른 보안체계를 사용하여 접촉하는 포인트 존재
- 소요비용의 증가 : 서로 상이한 보안제품은 각기 다른 운영시스템과 관리툴을 사용
- 중앙집중식 관리와 기록의 어려움 : 전체적인 네트워크, 그에 따른 정책 등의 준수, 각 네트워크간의 연관성, 데이터분석이 어려움

4.2.2 요구사항

위에서 제시한 보안 고려사항을 바탕으로 스마트 그리드 네트워크 기반구조의 요구사항을 기업에서 충족시키기 위하여 보안제품을 설계하였다. 이러한 보안 시스템은 단일 광대역 네트워크의 관점에서 복합적인 공격의 식별, 완화, 보고를 매우 향상시킨 시스템으로 오탐지를 없애고 운영자가 실제 보안 사고에 집중할 수 있게 한다. 어떤 운영자가 네트워크에 접근하던지 지역에 상관없이 일관되고 국부적인 정책 기반 접근통제를 적용한다. 중앙 집중화된 관리로 관리복잡성을 감소시키고 요구사항의 준수를 지원함으로써 소요비용을 감소시킨다. 스마트 그리드를 위한 특정한 보안시스템을 개발하기 보다는 기존에 존재하는 시스템으로 효율적이고 기능적인 보안을 설계하고 있다. [표 1]은 주니퍼에서 제시한 스마트그리드 보안 솔루션에 대한 주요 기능을 나타내고 있다. [그림 3]은 Juniper Networks에서 중앙통제센터, 지역통제센터, 기업의 엔터프라이즈 네트워크, 원격접속 등으로 구분하여 구성하였다. 보안 솔루션과 구성도를 살펴보면 우선적으로 기존의 IT보안 개념을 적용한 것으로 보인다.

4.3 커런트 그룹(CURRENT GROUP)

4.3.1 스마트 그리드 네트워크 전략

통신 취약점을 완화시키기 위해서 이 기업에서는 네트워크를 링크 엔드포인트로 제공되는 각각의 통신장치를 독립적인 링크로 분리시켰다. 네트워크 관리 어플리케이션과 네트워크 요소들 사이에 통신을 위해서 완전한 인증과 암호을 위해 AES-128에 기반을 둔 SNMPv3를 이용한다. 고장의 수리를 위해 장치에 로그인시에 SSH2(Secure Shell 2)를 이용한다. 이런 정책들은 다양한 통신 장치들 사이에 걸쳐 네트워크 장비들의 안전한 상호연결을 가능하게 한다[5].

4.3.2 적용 보안 요소

심층방어 원칙을 지키기 위하여 본 기업은 호스트와 어플리케이션 층의 보안에 다중 접근으로 네트워크 보

안을 증가시켰다. 호스트 및 어플리케이션 계층 보안을 설계하는 보안은 다음을 포함한다.

- 역할기반 접근통제 : 사용자의 타입에 따라 다른 레벨의 접근을 제공하여, LDAP(Lightweight Directory Access Protocol) 사용으로 보다 쉽게 관리하여 중앙집중 방식으로 유지하고 내부자의 공격이나 고의가 아닌 실수를 제한하는데 중요하다.
- 사용하지 않는 서비스 차단 : 사용하지 않는 서비스나 포트를 제한
- 방화벽 호환성 : 다양한 레벨의 IP와 XML 방화벽을 제공, IP와 포트를 제한하고 인증어플리케이션 API에 XML방화벽 제공
- 암호 : AES-128 사용
- 추적성과 감사 : 스마트그리드 요소나 어플리케이션에 관한 모든 활동을 추적하고 감사
- 접근 로깅 : 모든 접근 시도, 명령, 응답을 기록하고 타임스템핑
- 알람 : 보안 침입을 탐지하기위해 모든 로그를 검토 네트워크 장치로부터 오는 모든 알람을 모니터링

4.4 휴렛팩커드(HP)

4.4.1 스마트 그리드 보안

전현직 직원과 계약자, 사이버 테러리스트나 해커로부터 위협의 감지가 현실이다. 스마트 그리드에 대한 중요도가 커지고 여러 국가시설들은 매일같이 개인적으로나 사회적으로 악의적인 공격으로 방해를 받고 있어 보안은 스마트그리드에 필요하다. 각 산업체는 스마트 그리드를 다른 시각으로 보고 있지만 그중 정말 분명한 것은 보안의 중요성 이다. 물리적 기반구조 보안, 정보기술 보안, 금융보안, 전력 신뢰성에 대한 비젼과 현실 사이에는 분명한 차이가 존재한다. 하지만 보안을 나중에 고려되는 설계가 아닌 주요 요소가 되어야 한다. HP에서는 안전한 스마트 그리드를 보장하기 위하여 다음의 주요 고려사항을 말하였다[6].

- 위협과 취약점의 식별
- 네트워크 보호
- 물리적/사이버 공격으로 시스템 취약성 감소나 제거
- 어떤 방해요소에도 최소한의 영향

4.4.2 스마트 그리드의 보안 평가

많은 기업에서 스마트 그리드에서의 보안을 물리적 기반구조, 무결성, 기밀성, 가용성, 암호, 인증 등의 다양한 보안부분을 보고 있지다. 반면에 HP에서는 다른 기업과는 다르게 AMI(Advanced Metering Infrastructure)의 보안 평가라는 특정 분야에 스마트 그리드에 접근하고 있다. HP의 특성을 이용하여 평가라는 새로운 문제에 도전하고 있다.

AMI 제품회사를 선택할 시에 보안은 추후에 보안요소를 추가할 수 있는 사항이 아니기 때문에 중요하게 고려될 사항이다. 과연 제품에 적용된 보안을 어떻게 평가하는 것인가의 문제도 가지고 있다. 몇몇 회사는 제삼자 제품의 IV&V(Independent Verifivation and Valiadtion)를 할 수 있는 능력을 가지고 있다. 하지만 많은 회사는 높은 전문성, 고비용, 관여함 등으로 완료하는데 몇 달이 소요되는게 현실이다[6].

- 보안환경 식별 : 내부 변전소, 변전소간, 센터 대 변전소 통제, 변전소로의 소비자
- 일반 보안 요소 : 인증, 알맞은 정보로의 접근, 통신 접근통제, 메시지 무결성(침입탐지), 스푸프/재생

〔표 2〕 스마트그리드 보안산업 특성 비교

	분야	보안환경 및 고려사항	요구사항
CISCO	Network	기존 장치 고려, 필드 로케이션, 보안의 문화, 표준과 규정의 발전, 규모	Customer Operations(부정예방, 무결성, 프라이버시), Operate, Telematry and control systems(가용성, 무결성, 감사와 비밀)
JUNIPER	Network	취약점, 광역네트워크, 병목현상, 중앙집중관리	방화벽, 침입방지, 접근통제, 네트워크 이상탐지, 데이터가속과 암호, 중앙/역할기반 관리
CURRENT	Network	엔드포인트 네트워크, 인증, 암호모델, 원격접속	역할기반 접근통제, 방화벽의 호환성, 암호, 로깅, 알람
HP	AMI(평가)	위협과 취약점의 식별, 네트워크 보호, 방해요소에 최소한의 영향성	잠재 위험 평가, 침투테스트, 코드분석 등

공격 방지, 비밀성/프라이버시

- 설계의 기본전제 : 보안과 비보안의 프로파일들은 공존 할 수 있고 명백해야 함, 하나의 신분관리 정책 요구(모든 프로파일에 하나의 메카니즘), 주로 IT 방법론 사용을 요구
- 보안 목표 : 폐쇄된 개인 네트워크 안에서도 단 하나의 인가된 접근 보장, 신뢰하지 않은 엔티티로부터의 도청 방지와 캡처된 데이터의 스푸핑/재생공격 방지

이에 HP에서는 효율성, 완성도, 간소화하는 방법으로 이런 문제들에 접근하기 위해 스마트 그리드 보안의 질적 평가를 개발하였다. AMI 보안이 이런 만연하는 문제에 올바르게 평가되고 해결하기위해 HP가 개발하여 증명하는 평가 방법론은 문제들을 만족하는 보안 평가가 될 것이다. 보안 요구사항, 아키텍처, 고레벨 설계에 집중하여 매우 빠르게 높은 보안 평가를 가져와 AMI에 현재 잠재되어있는 위험을 보여주고 어느 지역의 AMI가 초점이 요구되는지 식별하고, 또한 침투테스트, 코드분석 등의 하위레벨의 보안평가를 한다.

〔표 3〕 분야별 컨소시엄 참여기업 현황

공모분야	주도기업	참여기업
지능형 소비자 (96개사)	SK텔레콤	삼성전자, 일진전기, 안철수연구소, EN테크 등 29개사
	KT	삼성SDS, 삼성물산, 루택, 옴니시스템, 가인정보기술 등 14개사
	LG전자	LG파워콤, GS건설, GS EPS, 이글루시큐리티, 제노텔 등 15개사
	한전	대한전선, 누리텔레콤, 넥스첼, 우암 등 38개사
지능형 배 송 (43개사)	한전	삼성SDI, 롯데정보통신, 피엔이솔루션, KAIST, LG텔레콤 등 22개사
	SK에너지	SK네트웍스, 르노삼성, 일진전기, 벽산파워 등 14개사
	GS칼텍스	LG CNS, ABB 코리아, 넥스콘테크놀로지, GS퓨어셀 등 7개사
지능형 신재생 에너지 (29개사)	한전	남부발전, 효성, LS산전, 인텍FA, 램피스 등 16개사
	현대중공업	맥스컴, 아이셀시스템즈코리아, 전력품질기술 등 6개사
	포스코	LG화학, 포스데이타, 우진산전, 대경엔지니어링 등 7개사
지능형 전력망	한전	-
지능형 전력시장	한전/ 전력거래소	-

4.5 한국 제주실증단지

국내의 경우, 제주도의 구좌읍에는 세계 최대·최첨단의 스마트그리드 실증단지가 구축 중이다. 올해 한국에서 열리는 G20회의에 한국의 스마트그리드 기술을 홍보하기 위해 먼저 홍보관을 건설하여 한국의 스마트그리드를 세계에 선보일 수 있는 좋은 기회의 장이 될 것이다. 또한 국가단위의 스마트그리드의 테스트베드로써 관련 기술의 상용화 및 검증을 한다. 위와 같은 목적으로 총 2,395억원을 투자하여 2011년 5월까지 인프라를 구축하고 2013년 5월까지 통합운영을 계획하고 있다. 제주 스마트그리드 실증단지에는 국가로드맵에 따라 5개의 분야에 전력·통신·자동차·가전 등 스마트그리드 유관 기업들이 참여하여 각 컨소시엄별 추진 전략에 맞추어 실증단지의 구축이 진행되고 있다[1]. 제주에 건설되는 실증단지는 현재 운영중인 미국, 네덜란드의 실증단지보다 첨단의 기술이 투입된 세계 제일의 실증단지가 될 것으로 기대된다.

실증단지의 건설에 참여하는 기업들 중 보안을 전략으로 하는 기업들이 존재한다. 안철수연구소, 이글루시큐리티, 넥스지 등의 보안회사를 비롯하여 롯데정보통신과 같은 대기업에서 보안을 고려한 실증을 할 것이다. 스마트그리드에서의 보안 위협을 해결하려 노력하고 있지만 아직까지는 초기단계에 있다. 예상되는 보안 위험요소 및 취약점을 파악하고 그에 대응하는 보안 프로토콜을 연구하고 표준화하는 단계이다. 국가보안연구소에서는 안전한 스마트그리드의 구축을 위한 보안가이드라인을 2010년까지 마련할 계획이다. 제주실증단지에 실증된 보안 시스템들은 국가단위의 스마트그리드의 테스트베드인만큼 계획적이고 확인된 보안시스템의 연구와 개발이 필요하다.

4.6 ITU-T 스마트그리드 보안 표준화 현황

국제전기통신연합(ITU-T) 연구반 17은 2009년 9월 스마트 그리드 보안 표준화의 중요성을 인식하고, 산하에 보안 전문가그룹(CG)을 설립한바 있으며, 이번 회의에서 전문가그룹의 활동 결과 보고서가 발표되었다[10]. 한편, 최근 ITU-T TSAG 산하에 스마트 그리드 포커스그룹(FG)이 2월 TSAG 회의에서 ToR 신설이 결정되어, 금년 4월 16일까지 국가별 의견 수렴 후 최종 ToR(Terms of Reference)이 확정되었으며, 금년 6월

14일에서 16일에 첫 포커스 그룹 회의를 시작할 예정이다[11]. 이에 따라 연구반 17회의에서는 스마트 그리드 보안의 경우, 포커스그룹 활동에 적극 참여해 보안 표준화 활동을 주도적으로 추진하기로 했으며, 그 결과를 포커스그룹의 활동이 완료되는 시점에 연구반 17로 가져와 표준화를 완성하기로 결정했다. 따라서 1년 정도의 활동 수명을 갖는 포커스그룹 활동이 완료되고 나면, 구체적인 표준화를 위한 구체적인 로드맵과 표준화 아이템이 도출되어 본격적인 글로벌 표준화가 추진될 전망이다.

V 국내·외 스마트그리드 보안관련 법·제도

5.1 국내의 법·제도 현황

5.1.1 지능형전력망 구축 및 지원에 관한 특별법(가칭)

'스마트그리드 국가 로드맵'이 발표되고 법·제도의 정비중의 일환으로 스마트 그리드만을 위한 특별법을 제정할 계획이다. '지능형전력망 구축 및 지원에 관한 특별법(가칭)'이라는 제목으로 법제처에 7월까지 제출하고 9월 15일까지 국회에 제출할 예정이다. 지능형 전력망의 조기 구축 및 효율적인 운영을 위해 재원을 조달하고 세제지원 등으로 스마트그리드의 종합적·안정적 추진을 위한 사업추진 체계를 확립하는 의의를 가진다. 그 주요내용으로는 다음과 같다.

- 산업육성 계획 수립 및 위원회 구성·운영
- 인프라 구축, 인센티브 지원
- 시범도시 운영
- 정보보호 및 보안, 인증제도
- 핵심 기술개발 및 신제품 시장 창출 지원
- 재원 조달방법 등

미국 에너지부에서는 스마트그리드 투자 프로그램에 사이버 보안과제를 의무적으로 반영하고 있고 유럽연합에서는 스마트 그리드 공격 대응방안과 송배전 시스템 복구능력 향상을 위한 방법론을 연구하고 있다. 이런 상황에 국내에서도 스마트 그리드 보안의 중요성이 부각되고 있어 '지능형 전력망 구축 및 지원에 관한 특별법(가칭)'에서도 보안 규정을 명확히 한다는 계획이다. 보안을 더욱 강조하기 위해서는 법의 명칭을 '지능형 전력망 구축 지원 및 정보보호에 관한 특별법'으로 바꿔야 한다는 일각의 의견도 있다[12].

5.1.2 정보통신기반 보호법

현재 추진중에 있는 스마트 그리드가 국가중요기반시설로 지정될 것이 기정 사실화 되고 있다. 주요정보통신기반시설인 전력망과 IT망이 결합하여 에너지와 통신을 제어·관리하는 시스템으로 국가단위의 스마트 그리드이기 때문에 국방 안보와 직결될 수 있어 주요정보통신기반시설에 포함할 수 있다. 스마트 그리드에서의 송변전 SCADA시스템, 배전자동화시스템, 전력계통운영시스템 등이 현재 '정보통신기반보호법'에서 기반시설로 지정, 관리되고있는 시스템이다. '정보통신기반 보호법'은 정보통신기반시설을 대상으로 해킹, 바이러스, 서비스거부 등에 의하여 전자적 침해행위에 대비하여 보호대책을 수립하고 실행함으로써 국가의 안전과 국민의 안전을 목적으로 제정된 법이다. 본 법은 현재 제정된 법률중에서 스마트 그리드와 관련할 수 있는 법에 있어서 가장 근접한 내용과 의미를 가지고 있는 법이다. 하지만 새로운 개념의 전력망인 스마트그리드를 다루는데 에는 한계가 따를 것으로 보이기 때문에 그 특성에 맞는 법의 개정이나 스마트그리드를 전적으로 포괄할 수 있는 새로운 법의 제정이 필요하다는 일각의 주장이 있다.

본 법에는 주요정보통신기반시설의 보호체계, 지정 및 취약점 분석, 보호 및 침해사고의 대응, 기술지원 및 민간협력 등의 내용이 포함되어 있다. 스마트그리드 보안관 연관되는 주요 관련 조항들을 보면 다음과 같다. 제3조(정보통신기반보호위원회), 제5조(주요정보통신기반시설보호대책의 수립 등), 제6조(주요정보통신기반시설보호계획의 수립 등), 제8조(주요정보통신기반시설의 지정 등), 제9조(취약점의 분석·평가), 제10조(보호지침), 제11조(보호조치 명령 등), 제12조(주요정보통신기반시설 침해행위 등의 금지), 제13조(침해사고의 통지), 제14조(복구조치), 제15조(대책본부의 구성 등), 제16조(정보공유·분석센터), 제24조(기술개발 등), 제26조(국제협력) 등이다.

5.1.3 정보통신망 이용촉진 및 정보보호에 관한 법률

정보통신망을 이용하는 자의 개인정보를 보호하고 건전하고 안전하게 이용하여 국민생활의 향상과 공공복리의 증진을 도모하는 목적으로 제정 되었다. 정보보호라는 것을 법제에 명시함으로써 정보통신망이란 특정한

분야에서의 정보보호 중요성을 반영한 제정으로 볼 수 있다. 그 중 스마트 그리드 보안과 연관되는 조항은 다음과 같다. 제4장 개인정보의 보호(제1절 개인정보의 수집 이용 및 제공 등, 제2절 개인정보의 관리 및 파기 등, 제3절 이용자의 권리, 제4절 개인정보분쟁조정위원회)는 스마트 그리드에서 소비자 전력 사용정보(패턴, 사용량, 시간대 등)의 관리가 필요한 상황에서 관련지어볼 수 있는 장이 된다. 그 중에 유심히 살펴볼 조항들은 다음과 같다.

제23조(개인정보의 수집 제한 등)
제24조(개인정보의 이용 제한)
제28조(개인정보의 보호조치)

위 조항들은 스마트그리드에서 개인정보가 전력 공급량의 관리나 실시간 요금의 책정에 사용되는 등으로 공급자에게나 제3자에게 불법적으로 이용될 우려가 있어 새로운 스마트그리드법의 제정에 참고해 보아야 할 조항들이다.

제45조(정보통신망의 안정성 확보 등)
제46조(집적된 정보통신시설의 보호)
제46조의2(집적정보통신시설 사업자의 긴급대응)
제46조의3(정보보호 안전진단)
제47조(정보보호 관리체계의 인증)
제47조의3(이용자의 정보보호)
제48조(정보통신망 침해행위 등의 금지)
제48조의2(침해사고의 대응 등)
제49조(비밀 등의 보호)

위의 조항들은 전력망을 고려하지 않은 기존의 정보통신망만을 고려하여 제정된 법률이기 때문에 스마트그리드에서의 스스로 고장을 탐지하고 스스로 치유하는 시스템이나 분산된 전력 생산과 공급으로 안정성 확보나 인증 등에는 보다 구체적이고 알맞은 법의 개정이나 새로운 법의 제정에 고려해야 할 것으로 보인다. 따라서 위에서 제시한 여러 조항을 고려하고 기반보호법에서 제시한 규정을 특화한 법 조항도 특별법에 반영할 필요가 있다.

5.1.4 그 외 법률

'국가정보화 기본법'과 '전자거래 기본법'에 있는 일부 조항들이 스마트 그리드 보안과 연관될 수 있는 정보이용과 전자거래의 보호에 관한 조항을 포함하고 있다. '국가정보화 기본법' 제4장(국가정보화의 역기능 방지) 제2절(정보이용의 안전성 및 신뢰성 보장) 제37조(정보보호 시책의 마련), 제38조(정보보호시스템에 관한 기준 고시 등), 제39조(개인정보 보호 시책의 마련) 등과 같은 조항들은 전력의 소비와 판매에 따른 개인이나 기업의 정보가 전자적 시스템에서 사용되어 보호가 필요하다. '전자거래 기본법' 제3장(전자거래의 안전성 확보 및 소비자보호) 제12조(개인정보보호), 제13조(영업비밀보호), 제14조(암호제품의 사용), 제15조(소비자보호시책의 수립·시행 등), 제16조(소비자 피해의 예방과 구제), 제17조(전자거래사업자의 일반적 준수사항)의 조항들은 전자문서에 의해 처리되는 전자거래가 기존에 전력망에서 사람에 의해서 전력을 거래하였지만 스마트 그리드에서는 전자적인 통신망을 이용하여 거래가 이루어지기 때문에 전자거래의 안전성을 고려해 볼 수 있는 법률이다.

5.2 미국의 법·제도 현황

5.2.1 주요 전력기반시설 보호법(안)

주요 전력기반시설을 보호하는 연방에너지규제위원회를 구성하여 취약점·위협을 연구하고 일정의 권한을 부여하여 주요 전력기반시설에 포함되는 스마트그리드를 보호할 '주요 전력기반시설 보호법(Critical Electric Infrastructure Protection Act)'을 2009년 4월에 제안하여 현재 수정 및 검토 중에 있다. 미국 내 전력기반시설에 대한 공격이 증가함에 따라 오바마 정부는 전력기반시설의 중요성을 인식하고 법을 제정하는 단계에까지 이르렀다.

제안하는 주요 법안의 내용으로 다음을 포함한다. 국토안보부는 다른 국가 안보·정보 기관과 협력으로 주요 전력기반시설의 운영에 필수적인 연방 소유의 전기 장치와 커뮤니케이션 네트워크(하드웨어, 소프트웨어, 데이터) 침해에 대응하는 연구를 실시한다. 연방전력법을 개정하여 주요한 전력기반시설과 향상된 전력 미터링 기반시설의 사이버 취약점과 사이버 위협을 지속적으로 평가하고 신뢰할 수 있는 리포트를 제공한다. 연방 에너지 규제위원회(FERC)에 주요 전력기반시설의 운영에 대하여 미국에서 잘 알려진 사이버 취약점이나 위협에 대응하여 보호하기 위해 임시적으로 법적 권한을 부여한다[7].

5.2.2 국토안보법

2002년 7월, 미국 정부는 국가안보를 보완하기 위해 '국토안보법(Homeland Security Act, HR 5005)'을 발표하고, 2002년 11월 19일에 통과되었다. 이 법률에 의해 국토안보부(Department of Homeland Security)가 설립되어 중요한 국가 기반시설의 보호를 담당하고 있던 기존의 여러 보안 연관 조직들이 국토안보부에 통합되었다[8].

국토안보부의 주요 임무는 미국에 대한 테러공격을 예방하고 자국민을 보호하는 것이다. 이를 위해 △정보분석과 기반시설 보호 △화학·생물·방사능·핵 등에 대한 대응조치 △국경 및 수송부문 보안 △비상시 대처 및 대응조치 △연방 주 지방 정부 부서 및 민간부문과 공조 등 5가지 기능을 수행한다. 다음과 같은 구체적 조항이 국토안보법에 포함되어 있다[4].

- 정보기술, 금융 네트워크, 위성 등을 포함한 미국의 중요 자원 및 기반시설을 보호하기 위한 포괄적인 국가 계획을 작성함
- 중앙정보국(CIA), 국방부(DoD), 국가 안전 보장국(NSA)을 포함한 모든 정부기관에 대해, 미국의 기반시설의 취약성에 관한 정보를 국토안보부에 제공하는 것을 의무화함
- 시스템 및 위약성 분석, 전화망이나 인터넷 등의 기반시설의 취약성에 대해 시뮬레이션과 모델링을 수행하는 국토보안연구소(Homeland Security Institute)를 설치함
- 국토안보부는 중요한 정보 시스템을 운영하는 기업에 대해 기술 지원을 제공하여 취약성에 대해 경고함

본 법을 보면 미국의 강력한 테러방지 의지를 엿볼 수 있다. 국가의 주요 기반시설을 보호함에 따라서 국민의 안전을 보장하는 목적을 둔다. 미국도 우리와 같이 기존에 스마트그리드와 관련된 법률이 존재하지만 포괄적으로 국토의 안보만을 고려한 것으로 스마트그리드라는 새로운 전력망을 다루기에는 부족하여 새로 주요 전력기반시설 보호법을 제안하였다.

5.2.3 에너지독립보안법

2007년 2월에 통과된 에너지독립보안법(Energy Independence and Security Act of 2007, EISA 2007)은 'SMART GRID'라는 단어가 언급된 최초의 법률이다. 본 법의 제13장이 스마트 그리드로 제정되고 각 부문별로 전력망의 현대화 정책 기술, 스마트그리드 시스템 보고, 스마트그리드 자문위원회와 스마트그리드 테스크포스, 스마트그리드 기술 연구, 개발, 실증, 스마트그리드 상호운용성 프레임워크, 스마트그리드 투자금을 위한 연방 매칭펀드, 스마트그리드에의 주 고려사항 등 9개의 부문에 걸쳐 언급되었다.

본 법에서 스마트그리드 보안에 관한 주요 내용을 보면 다음과 같다. 제13장 제1조에서 '안전한 사이버보안과 함께 전력망의 운영과 자원의 동적인 최적화'라고 스마트그리드의 특징을 기술하고 있다. 제6조 스마트그리드의 기능으로 디지털 정보, 미디어, 장치들을 이용하여 사이버보안 위협과 테러리즘을 포함하여 시스템 보안 위협으로부터 탐지, 보호, 통신에 관한 것이나 응답하거나 회복하는 능력이라 한다. 제7조의 경우, 각 주에서는 스마트그리드에 투자하는데 있어 보안의 요소를 고려해야 한다. 제9조의 경우, DOE(Department of Energy)는 스마트그리드에서의 보안 속성을 보고 한다[9].

스마트그리드에 대한 직접적으로 언급하고 그에 대한 규정이 나타나 있는 법률이다. 게다가 보안이라는 특정한 부분을 명시하고 있다. 스마트그리드에서 보안의 필요성을 인식하고 일부 보안을 규정하여 스마트그리드의 확산에 기반을 두고 제정된 법률로 볼 수 있다. 스마트그리드만을 위하여 제정된 법이 아니고 또한 보안이라는 것을 제13장에서만 다루어서 부족한 면이 보인다. 하지만 스마트그리드를 건설하는 초기에는 아주 유효한 법률이었을 것으로 보인다.

Ⅵ 결 론

본 고에서는 스마트 그리드의 취약점을 살펴보고, 이에 대한 기술적 대응방안을 살펴보았으며, 국내와 미국의 스마트 그리드에 관한 법률을 알아보았다. 세부적으로는 세계 주요 산업체들의 스마트 그리드에 대한 보안 기술 이니셔티브 등의 동향을 살펴보았다. 또한, 선도적인 스마트 그리드에 대한 국내 법률 및 정책 구축, 기술적 대응 등을 구축하기 위한 활동도 소개했다.

세계의 주요 IT 기업들은 스마트 그리드의 보안에 대한 문제점과 그에 따른 각 기업들의 대응책을 다각적으로 제시하고 있다. 스마트 그리드 보안에서 해결해야할

문제점들은 기존의 IT기술에서 가지고 있는 위협이나 취약점에 더한 다양한 신규 문제점을 포함할 것으로 예상하고 있다. 보안 측면에서 보면, 스마트 그리드는 기존의 IT 기술의 위협/취약점에 더해 신규 취약점에 대해서도 효과적으로 대응하도록 설계되어야 한다. 이런 보안기술을 연구하고 검증할 수 있는 제주실증단지 테스트베드는 이를 위한 중요한 테스트베드로 활용가능하다. 그리고 글로벌 차원에서 국가단위의 스마트 그리드가 건설되는 만큼 그에 발맞추어 보안을 고려한 설계가 필요하겠다.

미국에서도 9.11테러를 기점으로 테러에 대한 법률이 많이 제정되었다. 전력망도 하나의 국가 중요 시설로 지정하여 전력망에 대한 테러를 예방하는 차원의 법률들이 존재한다. 하지만 IT와 결합하는 전력망의 특성을 모두 포함할 수 없기에 정보보호 규제를 강화한 새로운 법의 제정을 추진하고 있다. 스마트 그리드와 관련된 한국의 법률들을 보면 역시나 새로운 개념의 전력망을 바로 기존 정보보호 유관 법에 적용해 규제하는 것은 본래의 목적을 달성하지 못할 것으로 판단된다. 따라서 보안을 고려한 스마트 그리드만을 위한 특별법의 제정이 필요하다.

세계 최초의 국가단위 스마트그리드를 위해서는 잘 정비되고 정리된 안전한 법제도적 뒷받침에 선도적인 기술적 보안 대책을 적용해야 세계 최초의 최고의 스마트그리드 구축이 가능할 것이다. 이에 대한 지속적인 연구가 필요하다.

참 고 문 헌

[1] 대한민국정부, 관보 제17185호, 2010년 1월

[2] U.S. Department of Commerce, "(DRAFT) NISTIR 7628, Smart Grid Cyber Security Strategy and Requirement, Feb. 2010.

[3] CISCO, "Securing the Smart Grid," Oct. 2009.

[4] JUNIPER Networks, "Juniper Networks smart grid security solution," Dec. 2009.

[5] CURRENT Group, "U.S. Smart Grid Security," Oct. 2009.

[6] HP, "Security－-Vital to the Smart Grid," Nov. 2009.

[7] GPO, "Critical Electric Infrastructure Protection Act of 2009," Apr. 2009.

[8] Homeland Protection Institute, "Key CBR Technology-Related Provisions of House Bill HR5005," 2002.

[9] GPO, "Energy independence and Security Act of 2007," Dec. 2007.

[10] ITU-T, CG on Smart Grid Security, SG17, http://www.itu.int/ITU-T/studygroups/com17/past-meetings.html

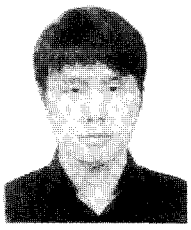
[11] ITU-T, Focus Group on Smart Grid, TSAG, http://www.itu.int/ITU-T/focusgroups/smart/

[12] 임종인, "지능형 전력망, 보안 구축이 생명이다," 동아닷컴 기고문, http://news.donga.com/3/all/20100219/26277713/1

〈著者紹介〉

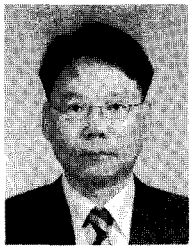
정 영 곤 (Young-Gon Jung)
학생회원

2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 스마트그리드 보안, IPTV 보안, 역추적



최 현 우 (Hyun-Woo Choi)
학생회원

2009년 2월 : 순천향대학교 정보보호학과 졸업
2009년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> : IPTV 보안, 스마트그리드 보안, USN 보안, 역추적



염 흥 열 (Heung-Youl Youm)
종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 9월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월 ~ 1990년9월 : 한국전자통신연구소 선임연구원
1990년9월 ~ 현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년3월 ~ 2000년 3월: 순천향대학교 산업기술연구소 소장
2000년4월 ~ 2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년3월 ~ 현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, 총무이사(역), 논문지편집위원회 위원장(현), 상임부회장
2010년 1월 ~ 현재: 한국정보보호학회 수석부회장
2005년 ~ 2008년 : ITU-T SG17/Q.9 Rapporteur
2006년11월 ~ 2009년 2월 : 정보통신연구진흥원 정보보호전문위원((구) 정보통신부 정보보호PM)
2008년 8월 ~ 현재 : 디지털아이디관리포럼 의장
2009년 ~ 현재 : ITU-T SG17 부의장 /SG17 WP2 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호프로토콜