Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.809

AMI 공격 시나리오에 기반한 스마트그리드 보안피해비용 산정 사례*

전 효 정,† 김 태 성‡
충북대학교

A Case Study of the Impact of a Cybersecurity Breach on a Smart Grid Based on an AMI Attack Scenario*

Hyo-Jung Jun,† Tae-Sung Kim‡
Chungbuk National University

요 약

스마트그리드는 사물인터넷의 핵심 응용서비스이고, 그 중 가장 핵심적인 구성요소인 AMI((Advanced Metering Infrastructure)는 전기사업자와 소비자의 접점에 위치하고 있으며, 스마트 미터는 소비자의 전기사용을 기록하고 사업자에게 전달하는 역할을 한다. 본 논문에서는 스마트그리드에서 소비자와 직접 맞닿아 있는 스마트 미터를 중심으로 AMI에 대한 NESCOR에서 제시하고 있는 사이버공격 및 피해 시나리오를 기반으로 피해비용을 산정한다. 본 연구의 결과는 정책입안자나 전기사업자가 스마트그리드 관련 투자의사결정을 하는데 참고가 될 수 있을 것이다.

ABSTRACT

The smart grid, a new open platform, is a core application for facilitating a creative economy in the era of the Internet of Things (IoT). Advanced Metering Infrastructure (AMI) is one of the components of the smart grid and a two-way communications infrastructure between the main utility operator and customer. The smart meter records consumption of electrical energy and communicates that information back to the utility for monitoring and billing.

This paper investigates the impact of a cybersecurity attack on the smart meter. We analyze the cost to the smart grid in the case of a smart meter attack by authorized users based on a high risk scenario from NESCOR. Our findings could be used by policy makers and utility operators to create investment decision-making models for smart grid security.

Keywords: Smart Grid, Advanced Metering Infrastructure, Cybersecurity Breach, Attack Scenario

I. 서 론

스마트그리드는 기존의 전력망에 정보통신기술(Information Communication Technology, ICT)을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 전력정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력망이다. 기본적으로 지능형 장치, 양방향 통신, 고급제어시스템을 통해 분산형, 지능형 전력망 관리 플랫폼을 갖추고 있으며, 이 플랫폼 위에서 재생에너지통합, 전기자동차 충전방식 지능화, 스마트 계량, 전력망 모니터링, 수요반응(Demand Response, DR)과 같은 애플리케이션을 가동한다[1].

스마트그리드에 대해서는 물리적 공격, 악천후,

Received(03. 07. 2016), Modified(04. 07. 2016), Accepted(04. 07. 2016)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임 (NRF-2011-0025512)
† 주저자, phdhyo@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

사이버공격, 전자기파(Electro Magnetic Pulse, EMP), 지자기폭풍(geomagnetic storm) 등 다양한 차원에서의 위협과 취약점이 존재한다[2]. 그 중에서도 사이버공격에 대한 우려가 가장 높은데, 이는 스마트그리드가 폐쇄망인 기존 전력망과는 달리 개방형 구조를 기반으로 하기 때문이다. 스마트그리드는 전력사용의 효율성을 높이기 위한 수용가와의 정보교환이 증가하고, 고객편의를 위한 수요반응(DR), 지능형검침(AMI) 등 새로운 전력서비스를 제공한다는 장점을 갖지만 동시에 이로 인한 사이버 공격의 위협 가능성도 높아진 것이다. 스마트그리드 확산의 판가름은 ICT기술을 활용해 소비자 댁내 전력소비량을 실시간으로 체크하여 전력수요를 측정해 주는 스마트 미터의 보급이지만, 아이러니하게도 스마트 미터를 기반으로 하는 AMI(Advanced Metering Infrastructure)가 근본적인 스마트그리드 보안취약점으로 우려되고 있다. AMI는 양방향 통신 기반의 스마트 미터와 기타 전기사용 정보 전달 및 제어장치로 구성되어 있는 인프라로서[3], 사용자에게는 실시간으로 전력가격 및 사용정보를 전달해 주고 공급자에게는 더욱 정확한 수요예측과 부하관리를 가능하게 한다. 그러나, 스마트 미터와 HEMS(Home Energy Management System), HEMS와 가전기기 등이 연결됨에 따라 악의를 가진 제3자가 보안이 취약한 가전기기를 통해 사이버공격을 감행할 경우, 계량기를 원격 조정하여 정전을 일으키거나 계량시스템을 공격하여 대규모 정전을 일으킬 소지가 매우 높은 것으로 우려되고 있다[4].

정보보호의 비용과 편익에는 무형적 요소가 다수 존재하며, 정보보호의 성과가 광범위하여 범위설정이 어렵고 성과를 얻기까지 많은 시간이 소요되므로 직·간접적인 편익을 측정하는 데에도 많은 어려움이 존재한다. 그럼에도 불구하고 보다 정확한 정보보호 투자의사결정을 위해서는 투자에 대한 효과를 측정하여 제시하는 것이 필요하다. 더욱이, 사이버 보안은 단순한 일회성의 기술적인 위험이 아니라 비즈니스 전체의 문제이다. 미래인터넷이라고도 불리는 사물인터넷을 위한 많은 기회가 기술 통합과 협업을 통해 발생하기 때문에 사이버 세계의 복잡성은 계속해서 증가할 것이고 이 복잡성은 보다 많은 종류와 범위의 위험을 야기할 수밖에 없다[5]. 이러한 인터넷 환경을 기반으로 구축될 예정인 스마트그리드가 보다 안전하게 구현되도록 하기 위해서는 안전성 및 신뢰성 확보를 위한 보안투자가 필요하며, 보안투자 의사결정을 지원할 수 있는 투자효과 분석이 필요하다.

현재 스마트그리드 보안시장은 시장 자체의 범주가 획정적이지 않고(기존의 보안시장의 일부가 될 것인지 별도시장을 형성할 것인지도 불명확), 스마트그리드도 구현 이전 단계이므로 그 하위 시장이라고 할 수 있는 보안시장을 논의하는 것은 매우 시기상조이다. 이러한 상황에서 스마트그리드 구축에 있어 보안에 대한 투자(비용과 편익 측정)를 고려하고 사이버 보안 차원에서의 공격이 발생하였을 경우의 파급효과를 산정해 보는 것은 스마트그리드 구현에 있어서의 보안투자의 필요성을 설득하는 중요한 정보가 될 것이다.

본 논문에서는 스마트그리드 소비자단을 구성하는 AMI를 주요자산(essential assets)으로 분류하고, 이에 대한 사이버보안 위협 및 취약점을 분류하여(잘 알려진 정보 기반), 공격 및 피해 시나리오를 구성한 후 이를 기반으로 사이버보안 위협이 발생하였을 경우를 가정하여 예상되는 피해비용을 산출해 봄으로써, 사이버보안 관점에서의 스마트그리드 보안투자 의사결정 지원을 위한 보안경제성 모델연구의 필요성에 대해 논의해 보고자 한다.

II. 문헌연구

현재, 스마트그리드는 구현되어 있는 시스템이 아니라 개념적으로 그 가능성을 연구하고 있는 단계로서, 우리 정부의 스마트그리드 구현 완료시기는 2030년이다[9]. 국외에서도 스마트 미터기의 보급단계에 있으며, 완전한 개념의 스마트그리드 구현까지는 상당한 시일이 소요될 예정이다. 이로 인해, 스마트그리드를 주제로 한 연구들은 기술적으로 보다 효율적인 스마트그리드 구현을 위한 방법을 찾는데 목적을 두고 있으며, 사이버 보안 차원에서의 위협의 가능성과 그 파급효과에 대한 논의는 아직 초기 단계에 있다. 일부 연구에서 스마트그리드에 대한 사이버 공격의 가능성과 공격 시나리오 개발을 위한 연구가 확인되고는 있지만, 직접적인 피해액 산정이나 그 파급효과 분석을 위한 연구는 아직까지 없는 것으로 파악된다.

정보보호 투자를 위한 의사결정을 지원하기 위해 필요한 자료는 정보보호 예산의 규모, 정보보호 대안의 효과, 정보보호 투자대안 간 비교 및 CEO에 대한 설득, 정보보호 포트폴리오의 가치평가 등으로

요약해 볼 수 있다. 본 연구에서는 대표적으로 정보보안 차원에서의 보안경제성 연구로 자주 인용되고 있는 Gordon&Loeb[6], Cavusoglue 등[7] Bodin 외[8], Kumar 외[9], RAND Corporation[10] 등을 검토하고 스마트그리드에 대한 사이버공격 시나리오에 기반한 피해비용 산정을 위한 산식을 도출하였다.

Gordon&Loeb[6]은 최적의 정보보호 투자량을 결정하는 경제적 모델을 도출하면서, 주어진 정보들로 이용가능한 수학적 모델을 제시하고 이론적 최적 투자량을 계산하였다. 투자의 효율성을 투자 대비 취약성의 감소 정도로 정의하고, 투자의 효율성을 극대화할 수 있는 투자량 계산방법을 제안하였으며, 투자량에 대한 정확한 수치를 제공하지는 못하였지만, 실무자들에게 정보보호 투자에 대한 막연함을 상당히 해소시켜 주었다. Cavusoglu 외[7]는 정보보호 대안들을 평가할 포괄적인 분석모델을 제안하였다. 수동적 모니터링의 최적 빈도(optimal frequency)를 계산하여, 플레이어들이 선택하는 전략의 상호작용에 의해서 각 플레이어의 손익(payoff)이 결정된다는 게임이론을 적용하였다. 또한, 정보보호 기술들의 서로 다른 옵션들의 결과를 탐색하기 위한 what-if 분석과 정보보호 기술의 품질 파라미터들이 기업의 비용에 미치는 영향을 분석하였다. Bodin 외[8]는 AHP를 이용한 정보보호 투자의 평가모델을 제시하였다. 조직의 정보보호를 위한 예산의 최적 배정을 결정하기 위한 각 대안 간 비교방법을 제공하였다. 기준(criteria)과 세부기준(sub-criteria), 강도(intensity level) 등을 AHP 트리에 따라 분류하고, 각각의 가중치를 부여하였다. LBG 사례를 통해 모델의 적용 가능성을 실증하였는데, LBG 사례는 세 곳의 벤더(vendor)들에게 $1million과 $1.3million의 예산 내에서 정보보호 기술공급에 대하여 입찰할 것을 요청하는 시나리오에 기반하고 있다. LBG의 CISO는 각각의 기준(기밀성, 무결성, 가용성)과 가용성의 세부기준(인증, 부인방지, 접근성)에 대한 가중치를 숙고하여 결정하고, 이러한 기준과 세부기준들은 6가지의 강도를 갖는다. Kumar 외[9]는 정보보호 포트폴리오의 편익(benefit)을 평가하고, 포트폴리오를 비교하였다. 위협 환경과 비즈니스 환경, 포트폴리오의 특성들을 파라미터화하여 최적의 포트폴리오를 구성할 수 있도록 하는 방법을 제시하였으며 포트폴리오 간의 상호작용을 고려하였다. 또한, 실험을 통해 유의한 파라미터를 추출하여 4가지 서로 다른 위험환경 시나리오를 이용해 포트폴리오를 비교하고, 포트폴리오의 가치(효과)를 평가하였다.

RAND Corporation[10]은 보안위협으로부터 오는 리스크를 줄이는 동시에 효과적인 보안예산 투자방안을 제시하였다. 이 연구에서는 휴리스틱 모델을 개발하였는데, 이 모델은 사이버 보안 리스크 관리에 필요한 종합적인 비용을 체계적으로 보여주고 있다. 외부 공격을 차단하기 위한 보안툴이나 프로그램 성능을 평가하는데 주력했던 기존 모델들과는 달리, Rand Corporation의 휴리스틱 모델은 리스크 관리에 대한 투자수익이나 투자 대비 리스크 감소 등 비즈니스적인 측면에 초점을 맞추고 있다. 이 모델은 기업이나 조직이 최적의 사이버 보안을 구축하기 위해 투자해야 하는 최소한의 비용 규모를 파악하는데 목적이 있으며, 사이버 공격 방지를 위한 조직의 직·간접 비용은 물론 공격으로 인한 잠재적인 손실, 공격 대상이 되는 정보의 가치와 공격 성공 가능성을 종합적으로 파악하였다. 또한, 조직의 사이버 보안 비용에 영향을 미치는 27개의 구체적이고 실질적인 변수를 적용함으로써 10년 동안 발생하는 구체적인 비용을 산출하였다.

본 논문에서는 피해비용 산정을 위해 정보보호 침해사고 피해액을 분석한 Gordon&Loeb[6]의 모델을 기반으로 하였다. 그러나, Gordon&Loeb[6]의 모델도 정보자산에 대해 피해를 입힐 수 있는 위협, 위협시도가 성공할 경우 피해가 발생할 가능성인 취약성, 피해유형 등을 모두 단일 유형만을 가정하였다는 한계는 존재한다.

〈 Gordon&Loeb[6]의 비용-편익분석 〉

§ 직접적인 피해= 시스템복구비용+매출이익손실비용+생산효율저하로인한손실+데이터재생산비용
§ 간접적인 피해 = 예방을 위한 투자비용
§ 잠재적인 비용 = 이미지손상+신뢰도하락+주가하락+법적보상 등

III. AMI 보안 위험분석

스마트그리드 장비는 광범위한 지역에 물리적으로 산재되어 있어 위험 관리 및 보안 관제에 큰 어려움이 있다. 더욱이, 스마트그리드는 국가 기간인프라이기 때문에 기존의 사이버보안 차원에서 발생했던 취약성이나 취약점, 사이버공격 등의 보안사고보다 훨

씬 광범위한 사회·경제적 손실을 야기할 수도 있다. 따라서, 스마트그리드 보안사고의 특징을 분석하고 차별화된 보안대책을 강구하여야 하며, 체계적인 위험분석을 통한 위험관리 프로세스의 정립이 필요하다.

본 연구에서는 위험관리 프로세스에 따라 스마트그리드 사이버 공격 및 피해 시나리오에 기반한 위험분석의 필요성을 제시하고, 잘 알려진 AMI 대상 위협 및 취약점을 분석해 보고 위험분석을 위한 위협 시나리오의 개발 가능성을 검토해 보고자 하였다.

3.1 위험분석의 필요성

위험분석은 자산의 취약점을 식별하고 존재하는 위협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 정도를 결정하는 과정이다[11]. 위험분석 프로세스나 방법론은 매우 다양하나, 미국에너지부(DOE)에서 제시한 위험관리 사이클은 FRAME, ASSESS, RESPOND, MONITOR 등 4단계로 구성된다[12]. 1단계 Risk Framing에서는 위험 기반 의사결정을 위한 제반사항들을 정의하는 단계로서, 전력계통망의 의사결정자들에게 설명 가능한 신뢰성 있는 위험구조를 설정한다(시나리오 기반). 2단계 Risk Assessment에서는 위협(threats), 취약점(vulnerabilities), 영향(impacts; 결과 또는 기회), 가능성(likelihood; 각 이벤트들의 발생확률 또는 빈도) 등을 규명한다. 3단계 Risk Response에서는 각 위험에 대한 대응책 또는 가능한 해결책을 제시하고 각 방안들을 평가하여 구현한다. 4단계 Risk Monitoring에서는 위험에 대한 방안들이 제대로 구현 되었는지, 수정사항은 없는지, 또 다른 위험은 없는지 등을 지속적으로 모니터링 한다.

위험분석은 위험관리의 일부분으로서, 화재, 사고 등의 물리적 위협에 적용되어 위협의 발생가능성에 따른 잠재적인 손실을 계산한다. 위험분석을 통해 적절한 보호대책을 우선순위에 따라 효율적으로 세울 수 있으며, 과도/과소의 투자를 예방하고 효율적이고 효과적인 보안을 실현할 수 있다. 현재, 스마트그리드에 대한 보안위협이나 취약점 등에 대해서는 산발적으로 보고되고 있다. 더욱이, 스마트그리드가 현재 실제적으로 구현되어 있는 시스템이 아니고, 개념모델차원이라는 점에서 발생 가능한 보안 위협이나 취약성은 존재하지만 실질적인 위험도 및 자산중요도(자산가치) 등의 산정은 어렵다. 따라서, 본 논문에서는 문헌연구를 통해 이미 잘 알려진 스마트그리드 특히 소비자 영역에서의 보안 위협 및 취약점들을 정리하였다.

3.2 AMI 대상 위협 및 취약점

AMI는 스마트 미터, 전력표시장치, 게이트웨이, 전력정보 수집장치, 스마트 가정 등으로 구성된다. 표준화된 프로토콜을 통해 시스템 간 상호운용성을 확보하여 미터기를 통한 양방향 통신을 지원하고, 수용가와 전력회사 간의 양방향 데이터 통신을 통해 다양한 부가서비스를 제공한다. AMI는 전력의 공급자와 수요자 간의 상호 정보제공 수단이며, 양방향 통신망을 이용하여 전기 등의 에너지 사용에 대한 검침, 사용 정보 수집 뿐만 아니라 개별 에너지 기기에 대한 능동적 제어를 가능하게 하는 기술이다. 특히, 에너지 사용 데이터가 측정되어 실제로 보여지는 부분으로, 스마트그리드 각 이해당사자들에게 다양한 이점을 제공한다[4].

스마트그리드는 폐쇄적인 전력망 구조에서 개방된 구조로 전환되는 시스템이므로 해킹을 통한 교란행위, 데이터 위·변조, 기능마비, 개인정보 유출, 사생활 침해 등과 같은 잠재적인 사이버보안 위협의 발생 가능성이 있다[14]. 더욱이, 스마트그리드 단말기기는 공격자의 접근을 막기 위한 보호 장치가 거의 없고, 외부자가 쉽게 접근할 수 있는 외부에 설치되므로 근본적으로 물리적·논리적 공격에 매우 취약하다. 이 기기들은 전력을 생산·운영하고 공급하는 역할을 수행하고 있어서 이를 대상으로 한 사이버 공격이 발생할 경우 전체 전력 공급에 차질이 생겨 사회적·경제적 피해가 매우 크게 발생할 수 있다. 이외에도, 스마트 미터에 대한 악성코드 제작, 계측된 계량 정보 조작 및 상위 컨트롤 시스템 공격이나 DCU(Data Collecting Unit), MDMS(Meter Data Management System), 유무선 네트워크 통신 프로토콜 공격 등 다양한 취약점과 공격유형이 존재한다[Table 1].

3.3 AMI 대상 위협 시나리오

2013년 발간된 NESCOR[25]의 Electric Sector Failure Scenarios and Impact Analysis 보고서에서는 발전, 송·배전 분야에서 기

밀성, 무결성, 가용성을 유지하기 위해 실제 발생 가능한 이벤트를 공격트리를 활용하여 사이버 보안 실패 시나리오 113개를 제시하였다. 제시된 실패 시나리오의 도메인은 NIST[26]에서 확인된 총 6가지이다: Advanced Metering Infrastructure(AMI), Distributed Energy Resources(DER), Wide Area Monitoring, Protection, and Control(WAMPAC), Electric Transportation(ET), Demand Response(DR), Distribution Grid Management(DGM).

NESCOR[27]에서는 NESCOR[25]에서 제시

Table 1. Smart grid customer domain : Technical vulnerabilities

Vulnerabilities (or Attack Type)	Sub Assets (Criticality*) *H:High, M:Medium, L:Low	References
Brute Force	AMI/Private (M)	[13]
Buffer Overflow	AMI/Public (M)	[13]
Bypass	Battery Management System (M)	[15]
CPU Resource Limit	AMI/Private (M)	[16]
Database Attack	Customer Domain DB (H)	[17]
DDoS	AMI/Private (M)	[14]
DoS	AMI/Private (M)	[18]
	Battery (L)	[16]
DPA *Differential Power Analysis Attack*	AMI Server (H)	[19]
Eavesdropping	AMI/Private (M)	[14]
Error Message Generation	AMI Meter (H)	[16]
Firmware Control	AMI Server (H)	[19]
	Electric Vehicle (M)	[20]
Hacking	AMI Meter (H)	[16]
	Electric Vehicle (M)	[15]
Head-end system	AMI Server (H)	[19]
Hijacking	Supply Management System (M)	[21]
	Demand Response System (H)	
	Electric Vehicle (M)	[15]
Irregular Control Command	Supply Management System (M)	[21]
	Demand Response System (H)	
Injection of Action Error	Electric Vehicle (M)	[20]
Interrupting Data Flow	Electric Vehicle (M)	[20]
Informative or Confidential Data Destruction/Modulation	Customer Domain DB (H)	[16]
Intrusion Transference	AMI/Public (M)	[22]
Leaking of Informative Data	Customer Domain DB (H)	[16]
Malware	AMI/Private (M)	[14]
	Electric Vehicle (M)	[23]
Man in the middle	AMI Meter (H)	[14]
	AMI/Public (M)	[14][22]
Parameter Modulation	AMI Meter (H)	[16]
Pepudiate	AMI/Private (M)	[14]
Privilege Escalation	Emergency Charging Stop (H)	[15]
Programming Logic Control and Code-Reuse Attack	Customer Domain DB (H)	[17]
Replay Attack	AMI/Public (M)	[14]
	Customer Domain DB (H)	[17]
Sniffing	AMI/Private (M)	[16]
Synchronized Multi-point Attack	Electric Vehicle (M)	[20]
Spoofing	AMI/Public (M)	[22][23]
Sensor Network Attack	Battery Management System (L)	[16]
Tamper	Demand Response System (H)	[23]
Wireless Traffic Attack	Energy Storage System (H)	[24]

Table 2. AMI attack scenarios [27]

AMI. 1	Mass Meter Disconnect
AMI. 9	Invalid Disconnect Messages to Meters Impact Customers and Utility
AMI. 12	Improper Firewall Configuration Exposes Customer Data
AMI. 14	Breach of Cellular Provider's Network Exposes AMI Access
AMI. 16	Compromised Head end Allows Impersonation of CA
AMI. 27	Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control
AMI. 29	Unauthorized Device Acquires HAN Access and Steals PII
AMI. 32	Power Stolen by Reconfiguring Meter via Optical Port

한 전력 분야에서 발생 가능한 113개의 시나리오 중 고위험(high risk) 시나리오 12개를 우선적으로 선별하여 보다 상세한 위협과 영향력을 분석하여 제시하였다[Table 2]. 12개의 시나리오 중 상세 시나리오가 개발된 고위험 요소는 3개이며, 본 연구에서는 3개 중 첫 번째 AMI 대상 공격 시나리오를 기반으로 피해비용을 산정하였다.

IV. AMI 사이버보안 공격 피해비용 산정

4.1 위협 시나리오의 개시

NESCOR[27]의 AMI. 1(Mass Meter Disconnect) 시나리오는 전압 및 주파수를 변조하여 고객과의 연결을 차단하고 전력을 손실시키는 상황을 가정한다. 제시된 AMI에 대한 상세 공격 시나리오와 그의 피해범주(영향력) 및 예상되는 피해규모와 복구상황은 다음과 같다.

공격은 인가된 개인(미터기를 원격으로 차단할 수 있는 권한을 합법적으로 가진 개인)이 전력차단 명령을 실행 또는 단시간 내에 대량의 미터기들을 차단할 수 있는 유인이 될 만한 명령을 실행함으로써 시작된다. 호스트 차단 기능을 하는 시스템에 대해 직접적으로 또는 원격 네트워크 접속을 통해 인가된 개인이 시나리오를 개시할 수 있다. 또한, 기본적인 보안조치가 취해졌을 경우 비인가된 소프트웨어는 위협 에이전트가 VPN 액세스 권한을 획득했을 경우 유틸리티 기업 네트워크의 외부로부터 원격으로 직접 설치될 수 있으며, VPN 액세스 권한 획득없이 원격 소스로부터 전송되어 설치된 진보된 악성 소프트웨어(malware)를 통해서도 가능하다.

예상되는 단기적인 피해로는 일시적인 전압이나 주파수 변동 가능, 미터기가 차단된 고객들에 대한 전력손실과 고객응대 불가능 상황 초래, 전력이 차단된 지역 내에서 범죄자들이나 테러리스트들이 음모를 꾸밀 수 있는 것 등이다. 만약 이러한 상황이 비인가된 소프트웨어의 설치로 인해 발생한 것이라면, 비인가된 소프트웨어를 식별해서 삭제하고 정상작동하는 소프트웨어를 재설치하기까지 많은 비용이 발생할 수 있다는 것도 단기적인 피해의 하나이다. 복구는 전력차단 후에 나타나는 모든 전압과 주파수 파동에 대한 어드레싱(전압과 주파수 파동을 어드레싱하기까지의 시간은 이러한 파동의 수준에 따라 달라지며 이는 차단된 미터기의 수와도 직결됨)과 서비스 재개를 위해 차단된 미터기들의 복구(미터기들의 재연결은 빠른 시간 이내로 복구되어야 함)로 구성된다. 가능한 한 정확한 소프트웨어를 빨리 회복시켜야 한다. 일단 비인가된 소프트웨어가 있음이 밝혀지면 수시간내로 복구작업이 진행되어야 하지만, 승인된 소프트웨어를 다운로드 하는데 시간이 걸릴 경우에는 이보다 많은 시간이 소요될 수 있다.

복구를 위해서는 비용차단 명령어의 전송을 위한 유틸리티 운영자, 유틸리티 필드 서비스 제공업체, 또는 제3의 운영자가 개입되어야 한다. 복구 단계에서 소프트웨어 설치 또는 재설치를 위해 다수의 IT 제품 및 기술이 도입되어야 하며, 시스템 로드의 재균등화 작동을 위한 분배작업이 진행되어야 한다. 또한, 전력차단으로 영향을 받은 고객들의 인터페이스에 대한 고객 서비스가 제공되어야 한다.

4.2 AMI 구축 비용

AMI 구축비용은 스마트 미터기가 전체 비용의 30%, 통신 인터페이스가 25%, MDMS가 5%, 모듈·시스템 통합 등 기타 비용이 40% 등으로 구성된다[28]. AMI 구축을 위한 요소기술별 비용 이외에

도 초기 설치비용(업그레이드, 교체 등을 위한 인력 방문 필요)이 소요되며, 운영이 시작되면 금전적 가치를 지닌 고객정보도 발생하기 때문에 이의 저장·관리 등에도 비용이 소요된다.

2015년 이후에는 대규모 AMI 설치로 인해 가격 인하가 빠르게 진행될 것으로 예상되고 있으며 가격 경쟁력이 입찰 과정에서 더욱 강화될 것으로 예상됨에 따라 스마트 미터기의 보급가격은 점차적으로 내려갈 것으로 예상되고 있다. 현재 한국에서의 스마트 미터기 보급은 2011년 75만 호에 추가 보급되었고, 2012년 100만 호, 2013년 200만 호 등 2020년까지 1,700만 대가 보급될 예정이며, 총 1조 1,367억 원이 투자될 계획이다[29].

4.3 피해비용 산정

본 논문에서는 NESCOR[27]의 AMI. 1(Mass Meter Disconnect) 시나리오와 AMI 구축 비용 등을 기본가정으로 하여 피해비용을 산정하였다[Table 3].

AMI 대상 사이버공격으로 인한 피해규모 산정을 위한 기본가정은 다음과 같다. 첫째, 현재 전국에 보급된 스마트 미터는 200만 개이며[29], 이 중 금번 공격으로 인해 피해를 입은 스마트 미터는 전체의 10%이다. 둘째, 피해를 입은 스마트 미터에 대해 전체 교체 없이 SW 수정만으로 재사용이 가능할 수도 있지만, 본 연구에서는 피해를 입은 스마트 미터 전량을 교체한다고 가정하였다. SW 수정을 할 경우, 수정에 필요한 인력비용 등이 산정되어야 하는데, 이는 DCU에 대한 수정비용에 기반하여 추정할 수 있다. AMI 설치 및 수정을 위한 인력비용은 알려져 있지 않지만, 한국전력이 2010년도 AMI 구축 사업에 투입한 DCU는 1만 7,000대인데, DCU 1대당 교체/유지보수를 위해 투입된 인건비는 56만원 정도로 알려져 있기 때문이다[30]. 또한, 스마트 미터에 대한 reprogram 비용은 34만원 수준으로 알려져 있다[31]. 셋째, 1가구당 1일 전력요금(한국전력 입장에서 판매수입)은 평균 4,748원으로 가정하였는데, 이는 한국전력의 1일 전력 판매수입을 기반으로 도출하였다[32]. 넷째, 전력공급 중단에 따른 피해보상금액은 1가구당 3.5만원으로 추산하였는데, 이는 상수도공급중단에 대한 피해보상사례를 기반으로 도출하였다[33]. 다섯째, 전력은 국가자원이며 한국의 경우 민간기업들이 경쟁하는 미국시장과는 달리 한국전력 단독시장으로 볼 수 있어 사이버공격에 따른 일시적인 기업손실액은 발생하지 않는다고 가정

Table 3. Equation for estimating costs of cybersecurity breach for AMI

Category		Equation
First Tier Costs (direct costs)	Costs for replacing or fixing equipment or machinery in position again	$C_1 = \sum_{i=1}^{l} \alpha_i$ *(a_i=market price of ith equipment replacing, l =amount of replaced equipment)*
Second Tier Costs (direct costs)	Costs for business loss	$C_2 = \sum_{j=1}^{m} \beta_j + P$ *(β_j=electricity sales cost of jth subscriber, m =amount of subscriber, P=compensation costs for service recovery)*
Third Tier Costs (indirect costs)	Costs for prevention, Costs for cybersecurity breach	$C_3 = \sum_{k=1}^{n} \gamma_k + \sum_{i=1}^{m} \delta_i + Q$ *(γ_k=legal compensation costs for private information breach of kth subscriber, n=amount of subscriber, δ_i=notice costs for ith subscriber, m=number of subscriber, Q=preparation cost for legal suits (legal counsel, forensic, etc.))*
$Total\,cost = \sum_{i=1}^{l} \alpha_i + (\sum_{j=1}^{m} \beta_j + P) + (\sum_{k=1}^{n} \gamma_k + \sum_{i=1}^{m} \delta_i + Q)$		

하였다. 또한, 사이버공격과 기업매출액과의 관계에 대한 기존 연구에서도 보안사고 발생으로 인해 단기적인 매출손실은 기록할 수 있으나 장기적인 영향은 미미한 수준으로 나타난 것을 감안하였다[34][35]. 여섯째, 법정비용의 경우 개인정보 유출로 인한 1가구당(4인가구 기준) 배상금액은 20만원으로 추정하였다. 이는 A은행 개인정보유출 관련 소송 사례를 준용하였다(1인당 5만원, [36]).

이를 기반으로 도출한 피해비용 산정 결과[Table 4], 1회손실비용(Single Loss Expectancy, SLE)은 총 371.9억 원으로 추정되었다. 1차 피해비용 약 274.4억 원, 2차 피해비용 89억 원, 3차 피해비용 8.5억 원 등이다. 1차 피해비용은 피해를 입은 스마트 미터기 전량을 교체하는 비용을 포함하였다. 금번 사고로 인해 스마트 미터기는 전체의 10%가 피해를 입었지만 스마트 미터기들을 관장하는 DCU에 대해서는 피해가 없었다고 가정하였다. 2차 피해비용은 비즈니스 손실로서 사고가 발생하고 복구하기까지의 2일간 한국전력 입장에서 각 가구당 전력사용량 체크가 불가능하였다고 가정하여 이를 손실로 잡았다(DCU에서 가구당 전력사용량을 지속적으로 업데이트하여 저장하지만, 고객 입장에서의 전력사용불가로 인한 피해배상비용 차원에서 한국전력에서 요금감면을 시행하였음을 가정). 이와 함께, 전력사용불가로 인해 발생하였을 수 있는 가구당 피해(냉장고 등의 사용불가로 인한 2차적인 피해)에 대한 배상비용으로 1일 35,000원씩 20만가구에 지급함을 가정하였다. 3차 피해비용은 간접비용으로서 각종 법정비용 및 추가적인 투자비용이다. 여기서는 아직까지 고객정보유출은 확인되지 않았기 때문에 개인정보유출로 인한 피해배상금액은 산정하지 않았지만, 사고조사와 포렌식이 진행중임을 가정하여 해당 비용을 포함하였다. 또한, 추가적인 보안컨설팅 비용도 포함하였다. 이와 함께 사고공지비용(사고발생공

Table 4. Single Loss Expectancy (Assumption: 10% of total subscribers are damaged by AMI attack scenario)

		Amount of Damaged	Basic Parameters (won)	Total Costs
First Tier Costs	smart meter replacement or reprogram	Smart Meters 200,000	HW replacement : 50,000 SW reprogram : 0 M/P for replacement/day : 348,900 Recovery Hours/HW : 0.25days	27,445,000,000
	DCU replacement or reprogram	No Impacted		
Second Teir Costs	electricity sales loss	Electricity Subscribers 200,000	4,748/subscriber (accident occurs 2 days)	1,899,200,000
	compensation costs for service recovery	Electricity Subscribers 200,000	35,000/day	7,000,000,000
Third Tier Costs	legal compensation costs for private information breach	Electricity Subscribers 200,000	no customer private information breach (accident investigation is on-going)	
	notice costs for each subscribers	Electricity Subscribers 200,000	500/subscriber (total 3 times notice)	300,000,000
	costs for accident investigation (Forensics)			50,000,000
	costs for legal counsel			5,000,000
	added ISMS consulting			500,000,000
Total Costs (First Tier Costs + Second Tier Costs + Third Tier Costs)				37,199,200,000

지, 사고진행상황공지, 사과문발송 등을 감안하여 3회)도 포함시켰다.

이상의 피해비용 산정은 AMI 구축에 소요되는 비용과 위협, 위협으로 인한 피해범위 등에 대한 다양한 기관의 조사자료 및 신문기사, 연구문헌 등에 기반하여 추정한 것이다. 따라서, 실제 운영상황과는 많이 다를 수 있다. 이에 대해서는 한국전력 등 실제 스마트그리드를 운영하는데 참여하는 사업자들을 대상으로 한 설문조사 또는 공개된 시스템 운영자료 등이 필요하지만, 보안상의 문제로 확보에 어려움이 있다.

위험이란 조직에 악영향을 미치는 불확실한 사건들의 발생으로 인해 조직이 평균적으로 받을 것으로 예상되는 충격의 양에 대한 측정치이다. 위험을 결정하기 위해서는 발생하는 불확실한 사건들의 유형, 발생빈도, 발생으로 인한 예상 손실액 등을 알아야 하는데 이들을 결정하기 위해서는 여러 가지 복잡한 요소들이 인식되고 측정되어야 한다. 일반적으로 위험은 일정기간 동안 평균적으로 잃게 되는 금액으로 표현되는데, 일반적으로 측정치가 연간 예상 손실액($ALE = SLE \times ARO$, Annualized Loss Expectancy)이다[37]. SLE(Sisngle Loss Expectancy)는 어떤 위협이 발생하였을 때의 예상되는 손실이며, ARO(Annualized Rate of Occurance)는 일년 동안의 예상 발생 횟수이다. 따라서, 본 논문에서 산정한 SLE를 기준으로 평균 이러한 규모의 보안사고가 1년에 3회 발생함을 가정하여(실제 사고빈도에 대한 다년간의 추적조사 필요) ALE(연간 예상 손실액)을 산정하면 대략 1,116.7억 원이다. 이는 한국전력[31]의 2014년 영업이익 5.7조원의 2.0%에 상응하는 규모로서, 절대 무시될 수 없는 규모의 비용이다.

V. 연구의 결론 및 향후 연구방향

2010년부터 2015년 동안 AMI 보안기술개발(스마트 미터/가전 보안모듈 기술, AMI 암호/인증 모듈 개발)에 투자된 금액은 138억 원이다(R&D 투자계획 기반). 이와 함께, 향후 장기적으로 AMI 해킹방지 기술, AMI 접근제어 기술, 전기차 보안 기술, 개인정보 보호 기술 등의 보안기술 개발이 계획되어 있다[4]. 2015년부터는 미래창조과학부 주관으로 사물인터넷 실증사업으로서 스마트그리드 보안 실증사업이 진행되고 있으며, 2017년 완료될 예정이다. 이 사업은 신규 보안기술의 개발이 아니라 기존에 개발된 기술을 적용하여 실증하고 개선하는데 그 목적이 있다[39]. 이와 같이, 스마트그리드의 보안성 확보를 위한 기술개발 및 실증사업이 진행되고 있는 상황에서 본 논문에서 도출한 보안피해비용 산정 사례는 향후 스마트그리드 보안투자 관련 의사결정을 지원하는 기반이 될 수 있을 것으로 기대된다.

본 논문에서 산정한 피해비용은 초안단계의 결과로서, 연구의 목적은 추정된 피해규모를 기반으로 스마트그리드 구현에 필요한 보안투자의 범주를 가늠해 보는데 있다. 따라서, 본 논문의 결과는 많은 가정과 예상되는 상황설정만으로 도출한 것으로서, 보안사고가 발생한 이후의 실제 상황을 분석하여 피해규모를 산정하는 기존 연구들의 결과와는 달리, 단지 피해의 가능성과 규모를 짐작해 보는 데에 목적이 있다.

향후, 스마트그리드의 본격적인 구현과 함께 사이버보안 차원에서의 보안성과 신뢰성 향상을 위해서는 다음과 같은 추가적인 연구가 필요하다. 첫째, 본 논문에서는 미국 NESCOR 보고서[27]를 기반으로 위험분석을 위한 위협/공격 시나리오를 구성하였는데, 한국의 전력시장환경 분석에 기반한 별도의 시나리오 개발이 필요하다. 둘째, 많은 전제조건을 기반으로 한정된 피해비용 산정을 하였는데, 향후에는 피해비용 산정을 위한 보다 세분화된 기반데이터의 확보를 위한 조사가 필요하며 실제적인 보안사고 발생 횟수에 대한 추정도 필요하다. 현재에는 1차 피해비용을 중심으로 구성하였는데, 향후에는 2차 및 3차(이미지 손상 및 주가하락 비용 등) 피해에 대해서도 충분히 고려함으로써 보다 현실성을 높여 나가야 할 것이다. 셋째, 시장현황에 대한 실측데이터의 확보가 필요하다. 시장 참여자들에 대한 심층인터뷰 등을 통해 시장상황에 대한 보다 현실적인 분석이 필요하며, 스마트그리드 관련 시스템의 보급현황 등에 대한 실제 데이터를 활용하는 현실적인 모델개발이 필요하다. 이러한 과정을 통해 현재에는 비용만을 산정하였는데, 향후에는 편익까지도 포함함으로써 실질적인 스마트그리드 보안 경제성 분석을 위한 모델의 개발이 가능할 것으로 기대된다. 넷째, 무엇보다도 국내 스마트그리드 시장 자체와 스마트그리드로 인해 추가적으로 수요가 발생할 것을 고려한 스마트그리드 보안 실태조사가 필요하다. 이를 통해 전반적인 스마트그리드 관련 보안시장을 획정하고 투자가 필요한 부분과 효과가 나타날 부분에 대한 전망도 가능할 것이다.

References

[1] MOEIA, Smart grid national roadmap, Jan. 2010.

[2] CSPC, Securing the U.S. electrical grid, July 2014.

[3] KSGA, Smart grid AMI technology trend report, Sep. 2012.

[4] KSGA, Smart grid security technology trend report, Sep. 2012.

[5] Ernst&Young, Cybersecurity and the Internet of Things, Mar. 2015

[6] L.A. Gordon, and M.P Loeb, Managing cybersecurity resources: A cost-benefit analysis, New York: McGraw-Hill, Sep. 2005.

[7] H. Cavusoglu, B. Mishra and S. Raghunathan, "A model for evaluating IT security investments," Communications of the ACM, 47(7), pp.87-92, July. 2004.

[8] L.D. Bodin, L.A. Gordon and M.P. Loeb, "Evaluating information security investments using the analytic hierarchy process," Communications of the ACM, 48(2), pp.78-83, Feb. 2005.

[9] R.L. Kumar, S. Park and C. Subramaniam, "Understanding the value of countermeasure portfolios in information systems security," Journal of Management Information Systems, 25(2), pp.241-280, Sep. 2008.

[10] RAND Corporation, The defender's dilemma: Charting a course toward cybersecurity, June 2015.

[11] Jang SangSoo, "Information security management system development and application", Life and Power Press, June 2015.

[12] DOE, Electricity subsector cybersecurity risk management process, May 2012.

[13] KATS and KSA, R&D roadmap based on technology standards: Smart grid, Apr. 2014.

[14] D. Grochocki, J.H. Huh, R. Berthier, R, Bobba, W.H. Sanders, A. Cardenas and J.G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp.395-400, Nov. 2012.

[15] Kang Seong-ku and Seo Jung-Taek, "An analysis of the security threats and security requirements for electric vehicle charging infrastructure," Journal of the Korea Institute of Information Security and Cryptology, 22(5), pp.1027-1037, Oct. 2012.

[16] H. Suleiman and D. Svetinovic, D., "Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: a case study using smart grid advanced metering infrastructure," Requirements Engineering, 18(3), pp.251-279, Sep. 2013.

[17] F. Aloul, A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," International Journal of Smart Grid and Clean Energy, 1(1), pp.1-6, Sep. 2012.

[18] G. Kalogridis, C. Efthymiou, S.Z. Denic, T. Lewis and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.232-237, Oct. 2010.

[19] R.C. Parks, "Advanced metering infrastructure security considerations," SANDIA REPORT: Sandia National Laboratories, Oct. 2007.

[20] H. Chaudhry and T. Bohn, "Security concerns of a plug-in vehicle," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Jan. 2012.

[21] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid,"

2012 IEEE Power and Energy Society General Meeting, July 2012.
〔22〕 S. McLaughlin, D. Podkuiko and P. McDaniel, "Energy theft in the advanced metering infrastructure," Critical Information Infrastructures Security, pp.176-187, Aug. 2010.
〔23〕 V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," IEEE Power and Energy Society General Meeting, pp.1-8, July 2011.
〔24〕 W. Su, H. Eichi, W. Zeng and M.Y. Chow, "A survey on the electrification of transportation in a smart grid environment," IEEE Transactions on Industrial Informatics, 8(1), pp.1-10, Jan. 2012.
〔25〕 NESCOR, Analysis of Selected Electric Sector High Risk Failure Scenarios, Sep. 2013.
〔26〕 NIST, NIST framework and roadmap for smart grid interoperability standards, Release 1.0, Jan. 2010.
〔27〕 NESCOR, Attack trees for selected electric sector high risk failure scenarios, Sep. 2013.
〔28〕 KETEP, The market report for 2013-2014 energy technology, Jan. 2014.
〔29〕 MOTIE, Plan smart meter and ESS supply, June 2013.
〔30〕 http://www.etnews.com/201402100504 (Feb. 2014)
〔31〕 http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ (Apr. 2012)
〔32〕 http://home.kepco.co.kr/kepco/KE/E/htmlView/KEEBPP0010101.do?menuCd=FN270101 (Sep. 2015)
〔33〕 http://www.cj-ilbo.com/news/articleView.html?idxno=903155 (Aug. 2015)
〔34〕 A. Acquisti, A. Friedman and R. Telang, "Is there cost privacy breaches? An event study," The 5th Workshop on the Economics of Information Security(WEIS), June 2006.
〔35〕 M. Ishiguro, H. Tanaka, K. Matsuura and I. Murase, "The effect of information security incidents on corporate values in the japanese stock market," Workshop on the Economics of Securing the Information Infrastructure(WESII), Aug. 2006.
〔36〕 MOI, Understanding privacy act, Dec. 2012.
〔37〕 Kim Sehun, "Information Security Management and Policy", Life and Power Press, Nov. 2002.
〔38〕 KIET, "Making secure net for Internet of Things: Convergence security industry", e-KIET Industry Economics Information, 586, pp.1-12, Apr. 2014.
〔39〕 http://www.msip.go.kr/webzine/posts.do?postIdx=149 (Dec. 2015)

〈저자소개〉

전 효 정 (Hyo-Jung Jun) 정회원
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 기획본부 기술원
2014년 2월: 충북대학교 경영정보학과 박사
2014년 3월~현재: 충북대학교 정보보호경영학과 박사후연수원
〈관심분야〉 정보보호 인력정책, 보안경제성

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수 및 학과장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정