情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

제어 시스템에 대한 보안정책 동향 및 보안 취약점 분석

최 명 균*, 이 동 범**, 곽 진***

요 약

제어 시스템은 수도, 오일 등 국가기반시설을 감시 및 제어하는 시스템이다. 최근 이러한 제어 시스템을 공격 목적으로 하는 사이버 공격이 발생하고 있어 제어 시스템에 대한 보안 필요성이 대두되고 있다. 이러한 제어 시스템은 일반적인 IT 시스템과는 달리 상이한 구조적 특성을 갖고 있어 제어 시스템의 특성에 맞는 보안정책을 마련해야 한다. 이를 위해 각 국가에서는 제어 시스템의 보안정책을 재정립하고 있으며 연구기관을 설립하고 프로젝트를 진행하는 등 보안 취약점을 해결하기 위한 노력을 하고 있다. 따라서 본 고에서는 국내·외 제어 시스템에 대한 보안정책 동향 및 보안 취약점을 분석하고자 한다.

Ⅰ. 서 론

정보통신기술의 발전으로 인해 수도, 오일 및 철도, 전력, 발전소 등 국가기반시설이 구축되면서 이러한 시설을 제어하기 위한 시스템의 도입이 증가하고 있다.

제어 시스템은 시스템을 구성하는 장비의 동작을 관리 및 제어하는 시스템으로써 일반적으로 제어시스템은 필드로부터 수집된 데이터와 센서측정 결과를 바탕으로 정보를 표시하고 원격 장비를 순차적으로 제어하는 명령을 수행한다. 이러한 제어 시스템으로 인해서 구축된 국가기반시설을 효율적으로 관리 및 제어할 수 있게 되었다.

하지만 최근 물리적인 공격보다 점차 사이버 공격으로 변화하고 있는 추세이며 제어 시스템이 사이버 공격의 대상이 되고 있다. 제어 시스템을 공격 목적으로 한 사이버 공격의 대표적인 사례인 스턱스넷은 단순히 공격자가 제어 시스템을 공격 목표로 삼은 것이 아니라 악의적인 목적을 가진 인원들이 계획을 세워서 정교하게 만들어진 악성코드이다. 이러한 사이버 공격의 지능화로 인해 제어 시스템 보안의 필요성이 대두되고 있으며 각 나라마다 제어 시스템 보안을 위해 연구기관을 설립하고 보안정책을 확립하는 등 제어 시스템 보안에 대해 노력을 하고 있다.

따라서 본 고에서는 제어 시스템에 대한 국가별 보안정책 동향 및 제어시스템의 보안 취약점을 분석한다.

본 고의 구성은 다음과 같다. 2장에서는 제어 시스템 중에서 일반적으로 널리 사용되는 SCADA 시스템의 구조를 분석하고 3장에서는 국가별 제어 시스템 보안정책을 분석한다. 4장에서는 제어 시스템의 보안 취약점을 분석하고, 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 제어 시스템 정의

제어 시스템은 시스템을 구성하는 장비의 동작을 관리 및 제어하는 장비들을 조작할 수 있도록 하는 시스템이며 센서나 작동장치 등의 필드 장치, 제어용 네트워크, 감시 제어 시스템 등으로 구성된다.

제어 시스템 중에서도 널리 사용되는 시스템인 SCADA(Supervisory Control and Data Acquisition) 시스템은 감시 제어 시스템으로 분산되어 있는 자산을 감시 및 제어하는데 사용된다. 이러한 시스템은 수도 분배와 폐수 수집 시스템, 오일과 천연 가스 파이프라인, 철도 및 다른 교통시스템 등에 사용된다.

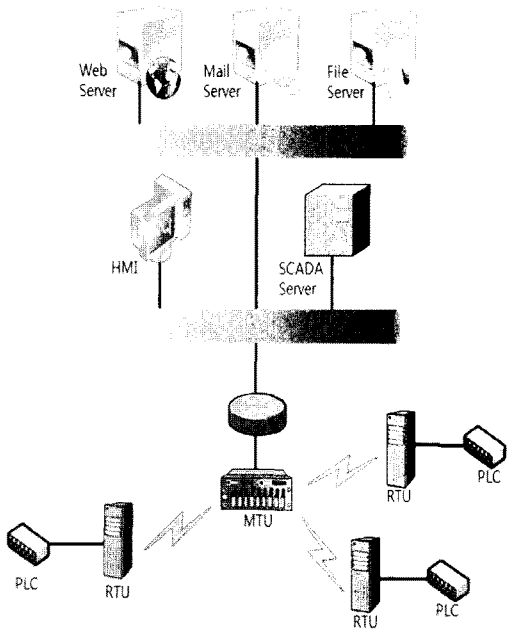
SCADA 시스템은 필드 장비를 통해 필드 정보를 수

* 순천향대학교 정보보호학과 정보보호응용및보증연구실 (mgchoi@sch.ac.kr)
** 순천향대학교 정보보호학과 정보보호응용및보증연구실 (dblee@sch.ac.kr)
*** 순천향대학교 정보보호학과 (jkwak@sch.ac.kr)

집하고 수집된 정보를 중앙 컴퓨터에게 전송하여 관리자가 실시간으로 중앙 위치에서 전체 시스템을 모니터링 하거나 제어할 수 있도록 한다.

SCADA 시스템은 하드웨어와 소프트웨어로 구성된다. 일반적으로 하드웨어는 제어 센터에 위치한 제어용 중앙 통제 시스템(MTU : Master Terminal Unit)과 통신장비, 작동을 제어하고 센서를 모니터링 하는 원격 단말 장치(RTU : Remote Terminal Unit) 및 프로그램 가능 로직 제어기(PLC : Programmable Logic Controller)로 구성된다. SCADA 시스템은 집중화된 모니터링과 제어 시스템을 제공하기 위해 데이터 수집 시스템을 데이터 송신 시스템과 기계를 동작시키기 위한 입출력 장치(HMI : Human Machine Interface) 소프트웨어와 융합한다. RTU는 지역 프로세스를 제어하고 MTU는 RTU입력과 출력으로부터 정보를 저장 및 처리한다. PLC는 원래 전자 하드웨어에 의해 실행되는 논리 함수를 실행하기 위해 설계된 작은 산업용 컴퓨터인데 복잡한 프로세스를 제어할 수 있는 제어기로 발전하였고 실질적으로 SCADA 시스템에서 사용된다. PLC는 RTU보다 경제적이고 다목적 및 탄력적으로 사용할 수 있기 때문에 제어 시스템의 필드 장치로서 사용된다.

소프트웨어는 시스템이 언제, 무엇을 모니터링을 하



〔그림 1〕 SCADA 시스템의 구조

〔표 1〕 IT 시스템과 제어 시스템의 비교

구분	IT 시스템	제어 시스템
가용성 요구사항	· 재부팅 가능	· 재부팅 허용되지 않음 · 정전은 미리 일/주일 단위로 계획 하고 실시
위험 관리 요구사항	· 데이터의 기밀성과 무결성을 중시	· 사람의 안전과 프로세스의 보호를 중시
성능 요구사항	· 실시간 아님 · 응답의 신뢰성	· 실시간 · 응답 시간
신뢰성 요구사항	· 고장 및 장애 허용	· 한순간의 운전정지도 허용되지 않음 · 철저한 테스트 필요
정책	· 중요도 순으로 보안성->무결성->가용성	· 중요도 순으로 무결성->가용성->보안성
솔루션	· 중앙 집중적	· 분산
통신	· 표준 통신 프로토콜 및 제한된 무선 능력을 가진 유선 네트워크	· 독점적으로 지정된 유무선을 포함한 복합적인 네트워크
관리 변경	· 소프트웨어의 변경은 뛰어난 보안 정책과 절차로 진행 됨	· 소프트웨어의 변경은 제어 시스템의 무결성이 유지된다는 것을 보증하기 위해서 증진적으로 시험한 후 진행 됨
시스템 수명	· 3~5년의 짧은 수명	· 15~20년의 비교적 긴 수명

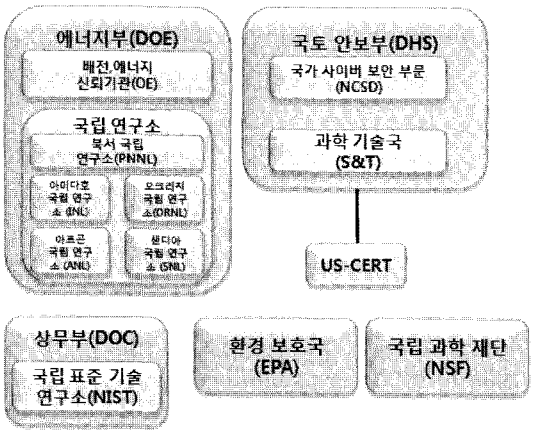
는지, 매개변수의 허용 범위가 무엇이고 허용 범위를 변경할 때 어떤 반응이 생기는지 나타내는 역할을 한다. [그림1]은 SCADA 시스템의 구조를 간략화 하여 나타낸 것이다.

제어 시스템은 일반적인 IT 시스템과는 달리 다양한 성능과 안정성을 요구한다. 제어 시스템은 일반 IT 시스템과는 다른 특성이 있는데 가용성 요구 사항, 통신, 관리 변경, 시스템의 수명, 위험 관리 요구 사항 등 여러 가지 차이점이 있다. [표 1]에서 일반적인 IT 시스템과 제어 시스템과의 차이점을 분석하였다[11].

Ⅲ. 제어 시스템 보안정책 동향

3.1 미국

미국의 에너지부(DOE : Department Of Energy)는 2006년에 에너지 분야의 제어시스템 보안을 위한 로드맵을 발표하였다. 또한 국토안보부(DHS : Department of Homeland Security)에서는 제어시스템의 보안을 위



〔그림 2〕 미국의 제어 시스템 관련 정부 기관

해 정부, 운영기관으로 산업 제어 시스템 협동워킹그룹(ICSJWG : Industrial Control System Joint Working Group)을 설립하였다. 또한, 미국 정부에서는 사이버보안 전략 재검토를 통해 사이버 공격의 위험성을 파악하는 등 제어 시스템 보안에 대해서 많은 관심을 보이고 있다. [그림 2]는 미국의 제어 시스템 관련 정부 기관들을 나타낸 것이다[1].

3.1.1 에너지부(DOE)

DOE에서는 에너지 관련(전력, 가스, 석유 등) 제어 시스템 보안 강화를 지원하기 위한 노력을 하고 있다. 에너지 부문과 관련하여 제어 시스템 특성에 맞는 차세대 제어 시스템, 시스템 취약성 평가, 통합 위험 분석 등의 프로젝트가 진행되고 있으며 2008년에 테스트 베드를 설치하는 등 선행 연구 개발 노력도 진행하고 있다. 테스트 베드는 제어 시스템의 취약점을 파악하고 해결하기 위한 테스트 환경을 사업자 및 정부 기관에 제공하고 있다. 또한 에너지 관련 업계 및 관련 단체의 "에너지 부문의 보안 제어 시스템의 로드맵"을 [표 2]와 같이 개정하여 공개하고 있다. 이 로드맵은 사이버 공격에 대한 핵심 제어 시스템 기능 방어를 위해 10년간의 비전, 노력, 목표를 나타내고 있다[10].

3.1.2 국토안보부(DHS)

DHS는 주요 제어 시스템 보안 대책을 추진하는 기관으로 핵심 제어 시스템의 위험을 감소시키는 것을 목적으로 2004년에 제어 시스템 보안 프로그램(CSSP : Control Systems Security Program)을 설립하였다. CSSP는 DHS의 국가 사이버 보안 부문(NCSD : National Cyber Security Division) 주도하에 민간 협력 및 관련 활동의 진행자를 통한 주요 제어 시스템의 보안 위협 감소를 추진하는 프로그램이다.

〔표 2〕 제어 시스템 보안 로드맵의 주요 내용

목표	내용
보안수준 측정	· 제어시스템 취약점 평가 수행
보안대책 개발	· 차세대 네트워크 및 단말기보안 평가도구 개발
침입탐지·대응전략 수립	· 침입, 오작동, 침해사고대응방안 개발
보안수준 향상	· 보안 포럼 개최 · 보안 인식 교육 실시

CSSP의 주요 대책으로는 보안 관련 문서와 권고 방법 등을 공개하여 교육을 실시하고 있다. CSSP 및 산하 연구 기관에서 나온 연구 결과를 바탕으로 DHS는 제어 시스템의 사이버 자체 평가 도구 개발, 제어 시스템 보안 카탈로그 공개, 참고 사례 소개, 교육 프로그램 제공 등의 대책을 추진하고 있다. 또한 제어 시스템의 보안 대책을 추진하기 위한 프로그램으로 공정 제어 시스템 포럼(PCSF : Process Control Systems Forum)을 2005년부터 시작하여 정부, 제조업체 또는 운영기관 등 제어 시스템 관계자가 참여하는 컨퍼런스를 정기적으로 개최하고 각종 활동을 촉진, 정보 공유를 도모하고 있다. 또한 DHS는 SCADA 시스템 보안과 관련하여 보안 프로그램 개발을 위해 600만 달러를 투자하고 있다.

3.1.3 아이다호 국립 연구소(INL)

아이다호 국립 연구소(INL : Idaho National Laboratory)는 DOE 산하의 10개 연구소 중 하나이며 아이다호 주, 아이다 호 폴즈의 첨단 테스트 원자로 복합시설, 물질 연료 복합시설, 연구 교육 캠퍼스의 주요 3개 시설이 있다. INL은 증식로, 핵 추진 장치를 개발하고 52기의 원자로 설계, 의료 산업용 동위원소생산 등을 실시하고 있다. 제어 시스템의 보안에 대한 연구는 DOE와 DHS의 공동 프로젝트에 의해서 2004년부터 시작했으며 DHS가 추진하는 CSSP에서 중추적인 역할을 담당하고 있다.

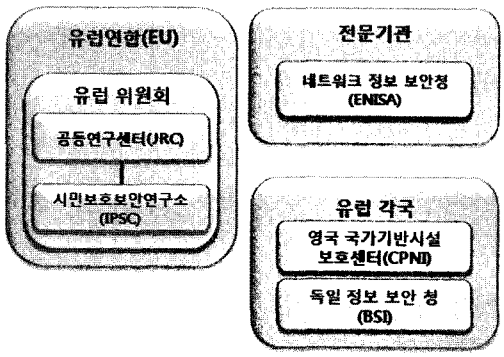
3.1.4 미국국립표준기술연구소(NIST)

미국국립표준기술연구소(NIST : National Institute of Standards and Technology)는 정부를 위한 제어 시스템의 보안 기준으로 산업용 제어 시스템 보안 가이드와 정보 시스템에 대한 보안 제어 권장을 수립하고 있다.

NIST는 제어 시스템의 보안 강화를 촉진하는 프로그램으로 정부기관, 제어기기 공급 업체, 사용자, 보안 업체 등 400개 이상의 조직이 참여하는 프로세스 제어 보안 요구사항 포럼(PCSRF : Process Control Security Requirements Forum)을 추진하고 보안 요구 사항 및 응용 프로그램을 정의하는 등 활발한 활동을 하고 있다. 2008년 이후에는 국제전자기술위원회(IEC : International Electrotechnical Commission)와 국제자동제어협회(ISA : International Sociological Association)에서 표준화 활동에 참여 및 지원하고 있다.

3.2 유럽

[그림 3]에서 보면 유럽위원회는 공동 연구 센터(JRC : Joint Research Center) 산하에 시민보호보안연구소(IPSC : The Institute for the Protection and the Security of the Citizen)를 설치하고 제어 시스템에 대한 일반적인 기술 개발 및 보안정책을 실시하고 있다. 또한 각국의 활동을 지원하고 중개하는 조직으로서 네트워크 정보보안을 담당하는 유럽 네트워크 정보보안청(ENISA : European Network and Information Security Agency)에서 제어 시스템 보안을 담당하고 있다. 제어 시스템 보안정책에 대해 원칙적으로 각국의 정부 주도하에 각 국가별 제어 시스템 정보보안 강화에 노력하고 있다.



〔그림 3〕 유럽의 제어 시스템 보안 관련 기관

〔표 3〕 JRC의 보안 정책영역

구분	내용
지식기반 사회	· 지식기반 사회 구현, 리스본전략 분석, 성장 동력 협력 네트워크 구축
천연자원관리	· 친환경, 지속가능 개발(천연자원 관리, 환경, 건강, 기후변화 등)
보안과 자유	· 잠재적 위험관리, 감시, 예방(내부 안보, 재난)
글로벌 파트너	· EU의 외부지원 활동(원조, 개발도상국의 지속적인 개발을 위한 협력, 국제 협력)
원자력공동체 지원	· 핵발전소 안전, 방사능 유출 모니터링

3.2.1 유럽위원회 공동 연구 센터(JRC)와 시민 보호 보안 연구소(IPSC)

IPSC는 유럽 연합의 행정조직이다. 유럽위원회(EC : European Commission)의 38개 시설 중 하나인 JRC 산하의 7개 연구시설 중 하나이며 주요 제어 시스템 방어 기술 개발 및 기술적인 지식을 바탕으로 정책 수립의 지원 및 제어 시스템 보안 연구 및 평가를 실시하고 있다. [표 3]과 같이 JRC는 2007년부터 2013년까지의 7차 프레임워크 프로그램(FP7)에 따라 5개의 정책 영역에서 활동하고 있다[9].

3.2.2 유럽 네트워크 정보보안청(ENISA)

ENISA는 유럽 디지털 사회의 건전한 발전과 정보보안 향상에 기여하기 위해 2004년에 설립된 유럽연합

〔표 4〕 ENISA의 2010년 활동 개요

구분	내용
다년도 테마 프로그램(MTP)	
MTP1	· 유럽 전자통신 네트워크의 장애 내성 향상
MTP2	· 정보보안에 관한 연계 방식의 개발과 유지
MTP3	· 통신 네트워크의 신뢰성·기밀성에 대한 새로운 위협 파악
준비활동(PA)	
PA1	· 향후 인터넷의 이용자 ID, 책임, 신뢰성 확보
PA2	· 유럽연합의 네트워크 보안에 관한 연계 추진과 구조 재작

(EU : European Union)의 전문 기관이다. 주요 역할은 유럽의 각국 정부에 주요 제어 시스템 보안에 대한 조언과 지원을 제공하는 것이다. [표 4]는 ENISA의 2010년 활동 개요를 나타낸 것으로 ENISA의 구체적인 활동이다. 활동 내용은 다년도 테마 프로그램(MTP : Multi-annual Thematic Program)이 있으며, 각종 시험을 통해 새로운 활동을 하는 준비활동(PA : Preparatory Action)이 있다. 활동 기간이 종료된 PA는 MTP로 해야 할 것인가에 대한 여부를 결정한다.

3.2.3 영국 국가기반시설보호센터(CPNI)

영국 국가기반시설보호센터(CPNI : Customer Proprietary Network Information)는 2007년 정보국 보안부의 일부 국가기반시설안전조정국(NISCC : National Infrastructure Security Co-ordination Center), 국가 보안 고문위원회(NSAC : National Security Advice Center)를 합병하여 만들어진 영국 정부의 전문기구이다. 영국의 다양한 정부기관, 기업, 대학의 인력으로 구성되어 있다. CPNI에서는 제어 시스템 안정성을 위한 각종 가이드라인을 제정하여 배포하고 있으며 SCADA와 네트워크를 위한 방화벽 설치 정책 및 사례, SCADA 보안 지침 및 사례 등을 제안하고 있다.

CPNI의 주요 임무는 테러 및 기타 보안 위협으로부터 국가 제어 시스템의 취약성을 감소시키기 위해 주요 제어 시스템 보안에 관한 종합적인 조언을 정부 기관 및 민간 부서에 부여하여 보안 가이드를 작성하여 공개하는 등 다양한 임무를 수행하고 있다. CPNI가 실시하고 있는 연구 프로젝트로는 정보 전자분야와 물리적·인적 보안 분야가 있다. 정보 전자 분야는 프로세스 제어 시스템과 SCADA의 상호 의존성 및 차세대 네트워크에 관한 것이며, 특히 시스템 보안 엔지니어링의 취약점의 발견과 백신, 실시간 악성코드 조사, 상호 의존성 모델링 및 인증이다. 물리적·인적 분야로는 전자 공학 및 제어 시스템(센서 네트워크, SCADA), 물리적 방어 수단 및 스캐닝 검출 기술이 있다.

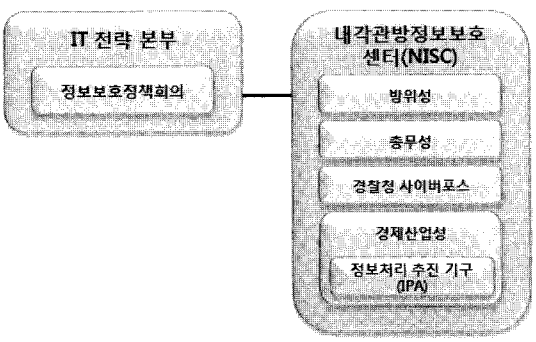
3.2.4 독일 정보보안청(BSI)

BSI(Bundesamt fur Sicherheit in der Informationstechnik)는 1986년 중앙 암호청이 컴퓨터 보안을 담당하는 것을 시작으로 정보보안 요구가 증가함에 따라 1989년 중앙 IT 보안 관청으로 개편 후 1990년대에 이르러서 BSI가 되었다. BSI는 정보보안 관리에 관한 기준을 작성하여 공표하고 네트워크 전반 및 사이버 보안 전반을 관리하고 있으며 주요 제어 시스템에 대한 취약성 분석과 보안에 관여하고 있다. 주요 기반 시설 보호에 대해서는 주요 기반 시설 보호 국가 전략, 국가 기반 시설 보호 계획, 주요 기반 시설 보호 실시 계획이 내무부에 의해 정해져 공개되고 있다. BSI는 독일의 정보보안을 확보하는 일환으로 제어 시스템 보안에 대해 구체적으로 전력, 수력 자원 등에 중점을 두고 있다.

3.3 일본

일본의 주요 기반 시설의 제어 시스템 보안에 대해서는 [그림 4]와 같이 내각관방정보보안센터(NISC : National Information Security Center)가 제어시스템 정보보안 강화를 위한 기본 전략을 수립하고 있다. 그밖에 제어 시스템에 대해서 광범위한 정보보안 대책을 추진하는 독립 행정법인 정보처리진흥사업협회(IPA : Information technology Promotion Agency)는 제어 시스템의 보안 문제와 대책에 대한 연구 활동을 실시하고 있다.

또한 제어 장치 공급 업체인 일본 전기계측공업회(JEMIMA : Japan Electrical Measuring Instruments Manufacturers' Association)와 제어 시스템 보안 과제와 대책에 대한 검토를 실시하고 있다. 주요 기반 시설의 해당 분야에 있어서 연구 및 정보 공유를 실시하고 있지만 해당 분야와의 연계는 서양 국가들에 비해 적기 때문에 앞으로 연계 활동을 지속적으로 실시할 계획이다.



〔그림 4〕 일본의 제어 시스템 보안 관련 기관

3.3.1 내각관방정보보안센터(NISC)

일본에서는 NISC가 중심이 되어 주요 제어 시스템의 정보보안 확보를 위한 정책을 추진하고 있다. 이에 따라 2006년에는 주요 제어 시스템 정보보안 유지에 관한 안전 기준 등을 발표하였다.

NISC는 주요 제어 시스템의 IT화 발전과 상호 의존성의 증대에 따른 정보보안 강화의 필요성을 직감하고 사업자, 정부 기관 등 분야에 따른 안전 기준을 수립하고 스스로 검증하는 것을 요구하고 있다.

또한 2008년 6월에 "Secure JAPAN 2008"에서 지속적인 정보보안 대책의 추진 체제 구축을 위한 기반 정비, 정보 기반의 안전성 확보 등 정책을 발표한 바 있다. 사이버 공격의 지능화된 공격 기법과 제어 시스템 같은 폐쇄적인 구조를 목적으로 한 공격 대상 확대에 대응하기 위해서 공격에 이용되는 기술, 방법 등에 관한 분석 능력의 강화를 추진하고 있다. 또한 사고 대응 지원이나 IT제품시스템 개발자에 대한 보안 제품 개발 기술 및 검증 기술에 관한 정보를 제공하고 사고 대응 기술 개발 등을 통해 정보 처리 환경의 정비를 도모하고 있다.

3.3.2 정보처리진흥사업협회(IPA)

IPA는 IT의 안전성 향상을 위한 정보보안 대책 강화를 목표로 기술 인력의 개발과 공개 소프트웨어를 배포하는 등의 노력을 하고 있다. [표 5]와 같은 IPA의 제어 시스템에 관한 연구 활동을 하는 등 제어 시스템의 보안 대책에 주목하고 있으며 대표적으로 2000년에 "대규모 설비·네트워크 보안"을 시작으로 외국의 선행 사례연구 및 임베디드 소프트웨어의 보안 동향, 2008년에 "주요 기반 시설 제어 시스템 보안" 및 "IT 서비스 연속성에 관한 조사", 2010년에 "제어 시스템에 대한 보안 추진 시책" 등 공통 과제 파악과 문제 제기 대책을 위한 개발 활동을 추진하고 있다[2].

〔표 5〕 IPA의 제어 시스템에 관한 연구 활동

년도	연구 활동
2000년도	· 대규모 설비 및 네트워크 보안
2001년도	· 정보보안 사고에 관한 연구
2003년도	· 전력 주요 기반 시설 보호 운동에 관한 연구
2007년도	· 여러 임베디드 장치 간 보안 연구 보고서
2008년도	· 주요 기반 시설 제어 시스템 보안 및 IT 서비스 연속성에 관한 연구
2010년도	· 제어 시스템에 대한 보안 추진 대책

3.4 국내

2001년 7월부터 구축된 정보통신기반 시설에 대한 국가차원의 보호체계는 주요 정보시스템 제어 네트워크를 주요 정보통신기반 시설로 지정하여 취약점 분석 평가와 보호대책을 수립하여 침해사고를 사전에 예방하고 그에 따른 적절한 대응 및 복구를 할 수 있는 기반을 마련하고 있다.

3.4.1 국가 사이버 안전센터(NCSC)

2002년도에 설립된 국가 사이버 안전센터는 사이버 테러 예방 활동 및 그에 따른 침해 사고를 예방하고 침해사고 발생 시 대응 및 복구지원 등을 수행하고 있다. 2005년에 발간된 국가 사이버 안전 매뉴얼을 개정하여 기관 간에 체계적이고 통일된 대응을 통해 정보통신망의 안전을 확보하고 있으며, 주요 정보통신기반시설 및 제어 시스템과 관련하여 임무를 수행하고 있다[5].

3.4.2 국가보안기술연구소(NSRI)

국가보안기술연구소(NSRI : National Security Research Institute)는 2000년에 설립된 정보보호 전문 연구기관이다. 주요 역할은 주요 정보통신기반시설 등의 보호를 위한 기술 개발 및 지원, 사이버 공격에 효과적으로 대응하기 위한 기술 및 정책을 개발·지원하고 있다. 또한 공공 분야의 사이버 안전 관련 기술 확보를 위한 연구 및 개발을 수행하며 정보보안 기술 개발 및 정책 지원, 관련 기반 구축 및 지원활동 등을 통해 국내 정보보안 기술 발전에 노력하고 있다[7].

Ⅳ. 보안 취약점 분석

제어 시스템 및 프로토콜은 자체 프로토콜 기술 및 기반 제어 시스템이며 기존 제어 시스템 동작에 대한 공개 정보가 없었기 때문에 초기부터 해커의 침입은 있을 수 없다는 것을 전제로 보안 대책을 고려하지 않고 구현 되었다. 그리고 외부와 통신하지 않거나, 전용망 및 사설망을 사용하여 두 지점 간의 통신만을 사용하는

폐쇄적인 구조이기 때문에 기존에는 보안을 고려하지 않는 경향이 있었다[3].

하지만 최근에는 실제 운영 상황이 다르고 공격 기법의 발달과 점차 드러나는 취약점으로 인해 보안 위협 및 침해사고가 증가하고 있기 때문에 제어시스템의 취약점을 분석하고 대처하는 방안이 필요하다.

따라서 본 장에서는 제어 시스템에 대한 보안 취약점에 대해서 분석한다.

4.1 정책적 취약점 분석

현재, 제어 시스템 보안에 있어서 필요한 보안정책이 미흡하다. 보통 구체적인 보안정책이 마련되어 있지 않고 긴급 상황 시에 언급되고 있기 때문에 꾸준한 보안 정책 활동이 필요하다.

제어 시스템의 보안 교육 및 프로그램은 해당 기업의 보안정책 뿐 만 아니라 보안 요구사항 및 표준화 등 최신 정보까지 포함하여 설계되어야 하는데 이러한 보안 교육 및 프로그램의 부재가 안전한 제어 시스템 환경을 구축하는데 있어서 문제가 되고 있다. 또한 보안정책을 위한 보안 절차가 문서화되어 있지 않고 장비의 구현 지침, 보안 감사, 사고 발생 시 대응 및 복구 계획의 부재가 제어 시스템의 취약점을 야기시키고 있다. 또한 제어 시스템 관련 정보보호 인력 부분에서 국내 정보보호 전문가는 다수 있지만 제어 시스템과 관련한 정보보호 전문가는 부족하며 제어 시스템 보안에 관한 연구실적 및 관련 보안 솔루션이 미흡하다. 따라서 보안 인식 교육이나 보안 포럼을 개최하는 노력이 필요하다.

4.2 악성코드로 인한 취약점 분석

악성코드는 제어 시스템의 성능 저하, 가용성 손실 및 데이터 수집, 데이터의 수정 및 삭제와 같은 결과를 일으킬 수 있다. 그렇기 때문에 제어 시스템의 악성코드 감염은 치명적이다.

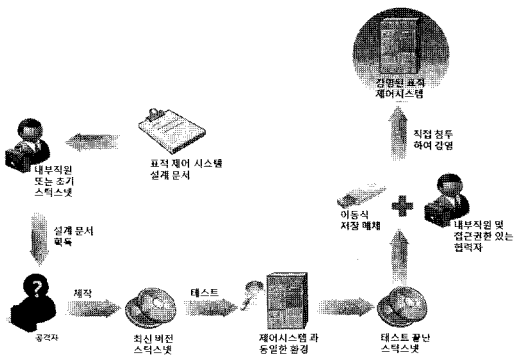
나날이 개발되고 발전되는 악성코드에 반해, 현재 제어 시스템에서 사용되고 있는 백신은 주기적인 업데이트가 이루어지지 않고 있다. 백신의 버전이 최신이 아닐 경우에는 신규 악성코드에 감염될 가능성이 있다. 백신의 버전이 업데이트가 안 되는 이유는 제어 네트워크와 외부와의 통신이 차단되어 있기 때문이다. 백신뿐만 아니라 OS에 대한 보안패치도 네트워크를 이용하여 실시간으로 이루어지지 않고 있다. 따라서 관리자가 이동식 저장매체로 업데이트를 직접 실시하게 되는데 관리자가 주기적으로 업데이트를 실시하지 않거나 허가받지 않은 이동식 저장매체를 이용하여 실시할 경우 악성코드로 인한 취약점이 발생한다. 또한 충분한 테스트를 수행하지 않고 구현된 백신을 사용할 경우 악성코드를 제대로 잡아내지 못하여 정상적인 운영에 문제가 발생할 수 있다.

4.2.1 스턱스넷 분석

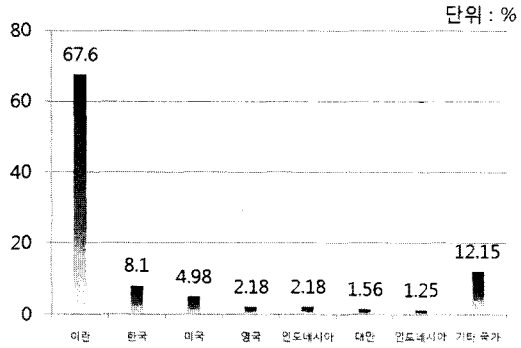
스턱스넷은 주요 산업 기반 시설의 제어 시스템에 침투하여 시스템을 정상적으로 동작하지 못하게 하는 악의적인 공격자에 의해 배포된 악성코드이다. 스턱스넷의 주요 공격 목표는 발전소 등에서 사용하고 있는 산업용 제어 시스템 및 유사한 시스템이며 최종 목표는 PLC(Programmable Logic Controller) 운영자가 변경 사항을 알지 못하도록 PLC 코드를 수정하여 제어 시스템을 재설계하는 것이다.

스턱스넷은 USB나 기타 이동식 저장매체의 자동실행 기능을 이용한 자기복제, MS사의 윈도우 바로가기 파일인 LNK 자동 실행 취약점, LAN상에서 P2P방식으로 스스로 업데이트, 바이너리가 숨겨진 윈도우 루트킷, 기존에 나와 있던 백신 소프트웨어 회피를 시도하는 특징을 갖고 있다.

스턱스넷의 공격 시나리오를 간단히 살펴보면 [그림 5]와 같다. 먼저 대상인 제어 시스템의 설계문서를 획득한다. 설계문서는 내부 직원 또는 스턱스넷의 초기버전 및 다른 악성 바이너리를 통해 입수한다. 입수한 설계문서를 바탕으로 최신 스턱스넷 버전을 개발한 후에 표적



〔그림 5〕 스턱스넷의 공격 시나리오



〔그림 6〕 스턱스넷에 감염된 국가별 호스트 비율

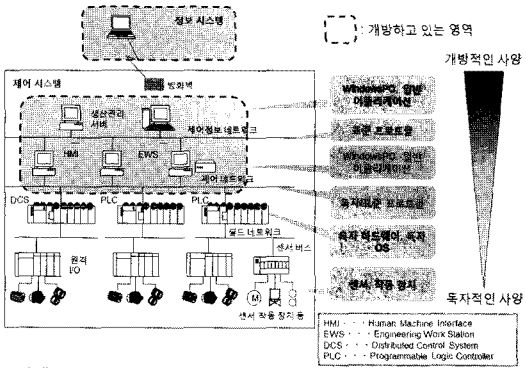
제어시스템과 동일한 환경을 구축하여 테스트를 실시한다. 테스트가 완료되면 접근권한이 있는 내부 직원들을 이용하여 직접 감염을 시도한다. 표적인 제어 시스템 파괴를 위한 모든 기능은 스턱스넷의 실행파일에 이미 구현되어 있으며 감염된 컴퓨터의 PLC코드를 변경하여 PLC 시스템을 파괴한 후에 코드 변경사항을 숨긴다.

이러한 공격 시나리오를 가진 스턱스넷은 2010년 7월경에 바로가기 파일 취약점을 이용한 악성코드로 처음 감염사례가 확인되었으며 이란 부셰르 원자력 핵발전소와 중국의 주요 산업 시설 1천여 개가 감염되면서 이슈화되었다[8]. 이미 전 세계의 PC 수십만 대가 감염되었다고 밝혀진 스턱스넷은 지멘스사의 STEP 7 소프트웨어가 설치된 호스트를 목적으로 하기 때문에 일반 PC에서는 감염만 되고 피해를 받지는 않는다. [그림 6]은 감염된 호스트 중 지멘스사의 STEP 7 소프트웨어가 설치된 호스트의 국가별 비중을 나타내고 있다[12].

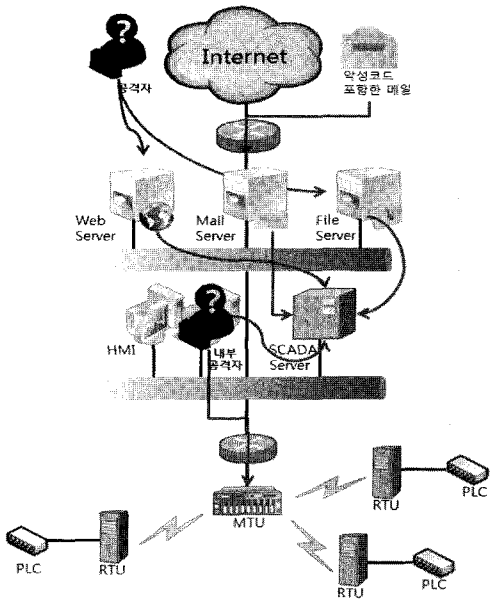
스턱스넷이 출현하기 전에는 일반 제품 또는 표준 프로토콜로 구성된 정보 시스템만이 공격의 대상이었지만 최근 공격의 대상이 제어 시스템으로 변화하고 있는 추세이다. 이에 대한 배경은 독립적으로 운영되고 있던 제어 시스템의 환경이 [그림 7]과 같이 점차 개방적인 환경으로 변화되고 있기 때문인데 일본 경제 산업성이 설비에 대해서 234개사에 설문 조사를 실시한 결과 서버와 단말기의 10%이상이 윈도우 시스템을 사용하고 있었다. 외부 저장장치에 대해서는 서버·단말기에서 USB 메모리가 7%, CD/DVD 리더기가 5%정도 보유하고 있었다. 또한 서버 네트워크 연결 포트의 6%가 이더넷을 보유하고 있었다. 그리고 외부 네트워크와는 4%연결되어 있으며 사내 정보 시스템은 절반 이상이 접속되어 있었다. 이러한 설비의 제어 시스템이 예전과는 달리 독립적으로 운영되지 않고 개방적인 환경으로 변화되고 있다[4].

4.3 기술적 · 구조적 취약점 분석

대부분의 제어 시스템은 업무상의 필요성을 이유로 내부 업무용 네트워크나 외부 기관 네트워크와 연동하여 사용하고 있기 때문에 내부 및 외부의 모든 보안위협에 노출되어 있다. 인터넷을 통해서 제어 시스템 운영을 위한 서버나 터미널 장치 등을 이용해서 다양한 형



〔그림 7〕 제어시스템의 개방적인 환경



〔그림 8〕 제어시스템의 기술적 · 구조적 취약점

태의 공격이 가능하며 e-메일을 통한 악성코드 감염 가능성도 있다. 또한 악의적인 내부 공격자가 제어 시스템의 권한을 획득하여 악의적으로 시스템을 제어 할 수 있다. [그림 8]은 제어시스템의 기술적·구조적 취약점으로 인한 공격자들의 공격 시나리오를 보여주고 있다[6].

기존의 제어 시스템들에 대한 잘못된 생각들이 많다. 제어 시스템은 외부와 통신하지 않고 전용망 또는 사설망을 사용하여 통신 하는 폐쇄형 구조이며 패치의 적용이 필요가 없고 완벽하게 통제가 되는 외부 연결이 없는 안전한 환경에서 돌아가는 시스템이라고 생각하는 경향이 있다. 하지만 실제로는 운영 상황이 다른데, 기본적으로 SCADA 프로토콜은 개방형이며 구하고자 한다면 인터넷으로 구할 수가 있다. 또한 운영체제는 Windows와 Linux 및 그 외 프로그램으로 동작을 하며 데이터 전송은 인터넷 프로토콜을 사용한다. 따라서 기존에 있는 OS와 프로토콜의 취약점이 제어 시스템에도 그대로 적용된다. 그 밖에 공격자들이 제어 시스템 침입에 대한 관심이 커지고 있고 폐쇄적인 구조라는 인식 때문에 관리자가 주기적으로 암호 변경 및 보안 패치를 하지 않는 경우가 많다.

V. 결 론

제어 시스템은 시스템을 구성하는 장비의 동작을 관리하거나 조작하기 위하여 많은 국가기반시설에서 사용되고 있다. 기존의 제어 시스템에 대한 보안대책은 물리적 공격에 대한 대책을 중심으로 이루어졌다. 하지만 제어 시스템을 목적으로 한 사이버 공격이 증가하면서 보안정책의 재정립이 요구되었다. 이에 따라 미국, 유럽, 일본을 비롯한 각국에서는 제어 시스템 보안에 대한 보안정책 및 기술 개발에 노력 하고 있다.

따라서 본 고에서는 제어 시스템의 각 국가별 보안대책과 제어 시스템에서 존재하는 취약점에 대해서 집중적으로 분석하였다. 이러한 취약점들이 존재하는 이유는 보안 인식의 문제점에서 비롯되었다. 제어 시스템에 대한 잘못된 인식이 취약점을 야기시키고 있는데 이러한 취약점들을 보완해 나가기 위해서는 제어시스템에 대한 보안 인식을 재정립해야 한다.

앞으로 제어 시스템의 보안을 위해서 전문 교육을 통한 인재 양성과 그에 밑받침되는 철저한 보안정책 수립이 필요하다.

참고문헌

[1] *重要インフラの制御システムセキュリティとIT サービス継續に關する調査*, IPA, March 2009

[2] *制御システムセキュリティの推進施策に關する調査報告書*, IPA, May 2010

[3] Eric Luiijf, *上水道分野用のSCADA (監視制御システム) セキュリティグッド・プラクティス*, IPA, December 2007

[4] *IPAテクニカルウォッチ『新しいタイプの攻撃』に關するレポート : Stuxnet (スタックスネット) 等の新しいサイバー攻撃手法の出現*, IPA, December 2010

[5] *국가 사이버 안전 매뉴얼*, 국가 사이버 안전 센터, 2005년 10월.

[6] 김영진, 이정현, 임종인, "SCADA 시스템의 안전성 확보방안에 관한 연구," 한국정보보호학회논문지, 19권 6호, pp. 146-149, 2009년 12월

[7] *2010 국가정보보호백서*, 방송통신위원회, 행정안전부, 지식경제부, 2010년 4월.

[8] 김홍석, "사이버 테러와 국가안보," 한국법학원 저스티스 통권 제121호, 2010년 12월.

[9] *유럽연합 프레임워크 프로그램 참여전략II*, 한국과학기술연구원 유럽연구소, 2010년 6월.

[10] *Roadmap to Secure Contorl Systems in the Energy Sector*, Department of Energy, Department of Homeland Security, January 2006

[11] Keith Stouffer, Joe Falco, and Karen Scarfone, *Guide to Industrial Control Systems(ICS) Security*, NIST, September 2008

[12] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, symantec, September 2010

〈著者紹介〉

최 명 균 (Myeonggyun Choi)

학생회원

2006년 3월~현재 : 순천향대학교 정보보호학과

<관심분야> : 정보보호, 스마트폰, 제어 시스템 보안 등

이 동 범 (Dongbum Lee)

학생회원

2008년 2월 : 순천향대학교 정보보호학과 학사 졸업

2008년 3월~2010년 2월 : 순천향대학교 정보보호학과 석사 졸업

2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정

<관심분야> 정보보호, 보안성 평가, 전자여권 보안 등

곽 진 (Jin Kwak)

종신회원

1994~2006년 : 성균관대학교 전자공학과(공학사 공학석사, 공학박사)

2006~2006 : 일본 큐슈대학교 방문연구원

2006~2006 : 일본 큐슈시스템 정보기술연구소 특별연구원

2006~2007 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관

2007~2009 : 정보통신연구진흥원 집필위원

2009~2009 : 순천향대학교 공과대학 교학부장

현재 : 순천향대학교 정보보호학과 교수, 정보통신산업진흥원 기술평가위원, 디지털아이디관리포럼 기술평가위원, 한국정보통신기술협회 JTC/SC27 분과 기술위원, 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원, 순천향BIT 창업보육센터 소장, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원, 교육과학기술부 국가기술 수준 평가 전문위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향대학교 중소기업산학협력센터 소장

<관심분야> 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등