정 보 보 호 학 회 지
제27권 제2호, 2017. 4

기반시설 침해사고 및 제어시스템 표준 동향

오 준 형*, 유 영 인**, 이 경 호***

요 약

산업 제어 시스템은 사회 기반 시설이나 산업체의 설비를 감시하고 제어하는 시스템을 의미한다. 제어시스템의 효율적 관리를 위해 상용 기술과의 유사성이 증가함에 따라 기존 정보시스템들이 가지는 보안 취약점 또한 수반하게 되었다. 따라서 제어시스템에 대한 침해사고 또한 증가하게 되었으며, 우리나라의 경우 대표적으로 한수원 해킹 사건이 있다. 이렇듯 기반시설에 대한 침해 사고가 늘어나 산업제어시스템 보안에 대한 중요성이 강조되면서 국내외로 제어시스템 보안 표준이 제정·개정되고 있다. 특히, NERC CIP, ISA/IEC 62443, NIST 800 series 와 같은 표준은 매년 또는 격년마다 개정이 되는 등 매우 활발히 변화하는 사이버 위협에 적극적으로 대응하고 있다. 본 논문에서는 2006년부터 현재까지 발생한 주요 침해사고에 대해 알아보고, 동 기간 내 국제 표준 동향 및 국내 정보보호 관리체계를 조사한다. 이를 통해 국내 정보보호 관리체계의 구체적인 문제점을 파악하여 보다 나은 산업제어시스템의 안전성을 확보하고자 한다.

Ⅰ. 서 론

산업 제어 시스템은 산업 분야 및 주요 기반시설에서 사용하는 관리 및 제어시스템이다. 이는 SCADA시스템, DCS, PLC 등과 같은 여러 시스템 유형을 포함하며 전력, 수력, 가스, 교통 등 국가 기반 시설 운용에 핵심적인 역할을 담당한다. 산업 제어 시스템에 첨단 정보통신기술들이 접목됨에 따라 온라인상으로 운용되는 범위가 넓어져 점차 개방화·표준화 되어 가고 있다. 이러한 국가 기반 시설들은 다양한 종류의 사이버 공격에 의해서 침해되는 사례가 늘어나고 있어 정보보호 관리의 필요성이 늘어나는 추세이다.

본 논문에서는 기반시설 침해사고 사례 및 제어시스템 표준 최근 동향에 대해 분석하고자 한다. 2장에서는 2006년부터 2017년까지 발생한 침해사고에 대해 파악하고, 3장에서는 제어시스템과 관련된 보안 표준의 개요 및 파악된 침해사고 동향의 동 기간 내 해당 표준들의 주요 변화 양상을 다룬다. 4장에서는 국내 주요 제어시스템 관련 현황에 대해 설명한다. 결론에서는 국내외 표준 동향에 대해 요약하고 이에 대한 시사점을 도출한다[1,2,3].

Ⅱ. 기반시스템 침해사고 사례

산업제어시스템은 원자력 발전소, 정유 회사, 공항, 은행, 방송사 등 다양한 분야에서 사용된다. 따라서 발생하는 침해사고 또한 다양하다. 본 논문에서는 원자력 발전, 정유, 공항 등 분야별로 대표적인 사건들을 언급하겠다.

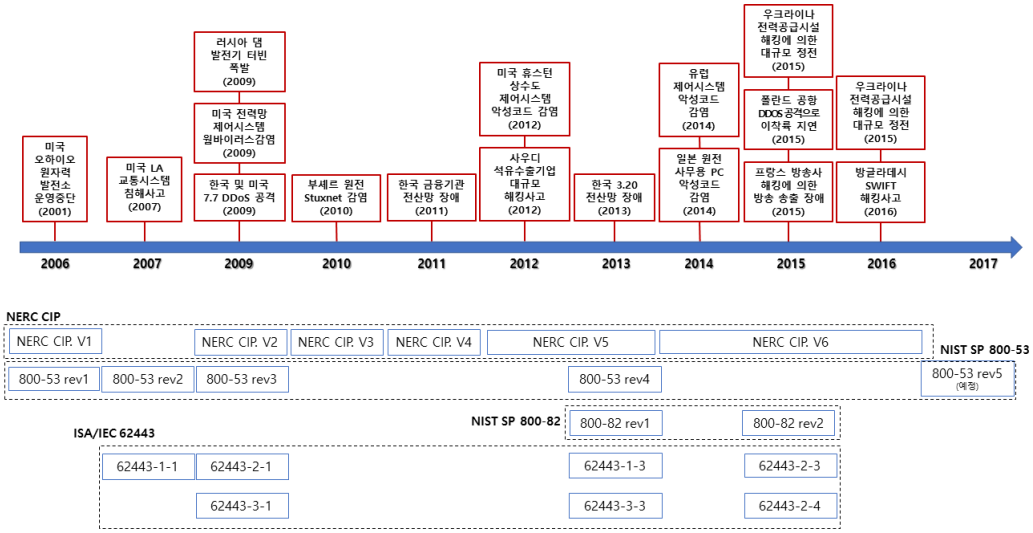
2.1. 부셰르 원전 공격

2010년, 스턱스넷 악성코드가 부셰르의 원자력 발전소를 공격하였다. 이 악성코드는 임의의 컴퓨터에 감염되지만, 지멘스의 SCADA 시스템만을 제어하는 코드가 담겨 있어 타깃이 정해져 있는 악성코드로 추정된다.

2.2. 사우디 아람코 해킹

2012년 8월, 세계 최대 규모의 정유 회사인 사우디 아람코의 컴퓨터 3만 대가 감염되어 손상되는 일이 발생하였다. 보안에 관한 사우디 아람코의 투자는 많이 이루어진 편이었지만 대부분이 생산 시스템에 집중되어 사무 환경 시스템은 취약하였다.

* 고려대학교 정보보호대학원 석·박사 통합과정, 주 저자 (ohjun02@korea.ac.kr)
** 고려대학교 정보보호대학원 박사 과정, 공동저자 (crenius@korea.ac.kr)
*** 고려대학교 정보보호대학원 교수, 교신저자 (kevinlee@korea.ac.kr)



〔그림 1〕 연도별 주요기반시설 침해사고 사례 및 관련 보안표준 개발 동향

2.3. 우크라이나 정전 사태

2015년 12월, 우크라이나의 전력회사들에 대한 사이버 공격이 감행되어 대규모 정전이 일어나 8만 명 이상이 영향을 받았다. 후에 조사된 사항에 따르면 블랙 에너지 악성코드가 이용된 것으로 보이고, 취약점을 이용한 방법이 아니라 매크로 기능을 가진 문서를 이용해 공격이 이루어졌다.

2.4. 폴란드 공항 DDoS 공격

2015년 6월, 폴란드 공항에 대해 DDoS 공격이 일어나 비행기 운항에 지장이 발생하였다. 이 공격으로 인해 폴리시 에어라인의 비행 계획 시스템이 5시간 동안 마비가 되어 약 1400여 명의 승객이 피해를 입었다. 비록 항공기를 해킹한 것은 아니지만, 항공사의 보안망이 뚫렸다는 점에서 중대한 문제가 된다.

2.5. 방글라데시 SWIFT 해킹 사고

2016년 2월, 미국 연방준비은행에 개설되어 있는 방글라데시 중앙은행의 계좌가 해킹되어 1000억 원에 가까운 피해가 발생하였다. 이 사건은 방글라데시 중앙은행에서 사용하는 시스템 중 최소 32개의 은행 서버 컴퓨터가 악성코드에 감염되어 있어서 발생하였다. 방글라데시 중앙은행은 뒤늦게 이체된 금액의 회수를 시도했지만, 대부분은 회수하지 못하였다. 이후, 국제
은행간통신협회(SWIFT)에서 해당 시스템의 보안 취약점을 개선하였다.

2.6. 한국 7.7 DDoS 공격

7.7 DDoS 공격은 2009년 7월 7일부터 3일 동안 DDoS 공격이 일어나 국내외 중요 기관들 및 기업 사이트가 마비된 사건이다. 당시에 정부 부처별로 각각 보도자료를 배포하여 혼선이 있었다. 그리고 악성코드 등 해킹 관련 정보의 공유가 제대로 이루어지지 않았으며 좀비 PC 탐지 체계가 정립되지 않아 DDoS 공격에 피해를 입게 되었다[7]. 이를 통해 정부는 보안 관련 컨트롤타워의 부재를 깨닫고 2010년 1월에 사이버방호사령부를 신설하기로 결정하였다.

2.7. 농협 전산망 사이버테러

2011년 4월 12일, APT 공격으로 인해 농협 내부 전산시스템 수백 개가 파괴되어 그달 말까지 농협 업무의 일부가 마비되었다. 검찰은 악성코드 구조, 공격자 IP 등을 확인하여 북한의 소행이라고 발표하였다. 이 공격으로 인해 외주협력업체의 노트북 관리가 부실하게 이루어지고 있고, 민간 기업에 대한 보안 관제 체계가 잡히지 않아 사이버 공격 예방에 미흡하다는 사실이 드러나게 되었다[8].

2.8. 한수원 해킹 공격

2014년 12월, 범인들은 한국수력원자력 직원들에게 악성코드가 담긴 피싱 메일을 보내 시스템 파괴를 시도하였다. 이 사건은 미리 확보한 원전관련 자료를 미끼로 협박한 최초의 심리전 형태의 사이버 공격이었다[7]. 이 공격은 북한 해커들이 사용하는 것으로 알려진 킴수키 계열의 악성코드와 유사하여 북한의 소행으로 추정된다.

2.9. 한국 3.20 전산망 장애

2013년 3월 20일, 국내 방송사들과 은행 등 금융권의 시스템이 악성코드에 감염되어 수만 대가 파괴되어 9,000억에 가까운 피해가 발생하였다. 당시 방송 및 금융기관은 개인정보 유출과 관련된 신고의무가 없어 상황에 관한 공유가 원활히 이루어지지 않았고, 사고 조사를 위한 업무협조도 피하는 경향을 보였다. 또한, 유관부처와 청와대 간의 보고체계가 명확하지 않아 혼선이 생겨 빠른 대응이 힘들었다[9].

Ⅲ. 해외 보안 표준 동향

미국 국립표준기술연구소(NIST : National Institute of Standards and Technology)에서는 산업 제어 시스템에 대한 보안 가이드와 정보 시스템에 대한 보안 제어 권장 항목들을 수립하여 제공한다[4]. 그렇기에 NIST에서 제정한 표준 중 제어시스템과 관련성이 높은 NIST SP 800-53과 NIST SP 800-82를 다루고자 한다. 그리고 미국 ISA의 표준기구인 ASCI(Automation Standards Compliance Institute)에서 산업 제어 시스템에 관한 보안이슈를 다루기 위해 ISA-99.0X.0X 시리즈를 개발하였다. 이 시리즈가 IEC 표준문서의 토대가 되어 ISA-62443으로 명칭이 변경되었다. 이는 산업 제어 시스템에 적합하도록 보안요구사항 및 위험분석에 따른 보안대책을 강화한 표준으로 의의가 있다[2]. 그리고 NERC(North American Electric Reliability Corporation)는 사이버 및 물리 공격으로 인해 전력 계통이 침해당하는 걸 막기 위해 보안관련 신뢰성 표준인 CIP를 만들어, 전력 계통에서 신뢰받는 표준으로 자리잡았다[5].

3.1. NIST SP 800-53

사이버 공격이 널리 퍼지고 정교한 사이버 공격 방법들이 개발됨에 따라 NIST, 국방부, 정보기관 및 국가안보 시스템위원회에서 NIST SP 800-53을 편찬하였다. NIST SP 800-53은 조직에 정보 보안 및 시스템 운영 환경을 근본적으로 강화시키는 데 필요한 보안 제어 기능을 제공함으로써 시스템에 기여한다. 전체 위험관리 프레임워크 중 NIST SP 800-53은 보안통제 선택 단계와 보안통제 측정 단계에 속해 있다.

NIST SP 800-53은 Revision 3에서 Revision 4로 개편되면서 주요 내용들이 개편되었다. Revision 3에서는 맞춤화 적용을 한 후 위험 평가를 진행하였지만 Revision 4에서는 맞춤화 과정 하나로 통합되었다. 또한, Revision 3에서 Revision 4로 개편되면서 오버레이 개념을 도입하여 개인 정보 제어 기능을 활용하고 정보 시스템을 보호하여 유연성을 높였다. 오버레이는 통제 기준치 맞춤화를 수행할 때 나온 보안 통제들의 모음이다. 오버레이는 통제를 추가하거나 제거할 수 있는 기회를 제공한다. 그렇기 때문에 초기에 기준치를 설정한 후 맞춤화를 진행하였을 때 바뀐 사항이 없다면 오버레이를 만들 필요가 없다. 그리고 특정 정보 기술이나 컴퓨팅 패러다임, 운영 환경, 정보 시스템 유형, 운영 모드, 산업 부문 규제 요건에 대한 보안 제어 적용 및 해석을 제공한다. 또한 보안 통제에서 필요한 매개 변수 값을 설정하고 필요한 경우, 보안 통제를 위한 보충 지침을 확대한다.

또한, 현재 Revision 5로 개편될 예정이고 2017년 3월 말에 DRAFT 버전이 나오는 것으로 공지되었다. Revision 5에서는 Revision 4에 비해 보안 통제의 내용을 강화하는 데 초점을 맞추고, 통제의 목적에 중점을 두어 의도된 결과를 보다 잘 반영할 수 있도록 내용이 추가될 예정이다.

3.2. NIST SP 800-82

NIST SP 800-82는 산업 제어 시스템(ICS, Industrial Control Systems)을 안전하게 수립하기 위한 공식적인 지침서이다. 산업 제어 시스템에는 감시 제어 및 데이터 수집 시스템(SCADA, Supervisory Control And Data Acquisition), 분산 제어 시스템(DCS,

Distributed Control System) 및 프로그래머블 로직 컨트롤러(PLC, Programmable Logic controller) 등이 포함된다. 이러한 산업 제어 시스템들에는 기존 IT 시스템과 다른 다양한 종류의 위험이 존재하기 때문에 NIST SP 800-82에는 NIST SP 800-83을 참고하여 산업 제어 시스템을 보호하기 위한 목록들을 제공한다. 이를 위해 산업제어시스템에 대한 일반적인 구성과 개념을 제시하고 산업제어시스템의 관리적, 운영적, 기술적 보안 통제를 분류한다. 또한, IT시스템과 비교하여 산업제어시스템이 가지고 있는 취약성과 위험요소를 도출하여 산업제어시스템을 보호하기 위한 기술과 대응책을 제공한다.

NIST 800-82 Rev 1에서 NIST 800-82 Rev 2로 개편되면서 ICS에 대한 잠재적 위험에 대한 대응 방법과 ICS를 보호하기 위한 기술들의 목록을 제공하고 있다[6]. 주요 업데이트 내용은 ICS 위협 및 취약점에 대한 업데이트, ICS 위험 관리, 권장 사례 및 아키텍처에 대한 업데이트, ICS 보안의 현재 활동 업데이트, ICS의 보안 기능 및 도구에 대한 업데이트와 관련된 사항들이다. 또한, NIST SP 800-52의 오버레이를 포함하여 보안 및 개인 정보 제어에 대한 맞춤 지침이 추가되었다.

3.3. ISA/IEC 62443

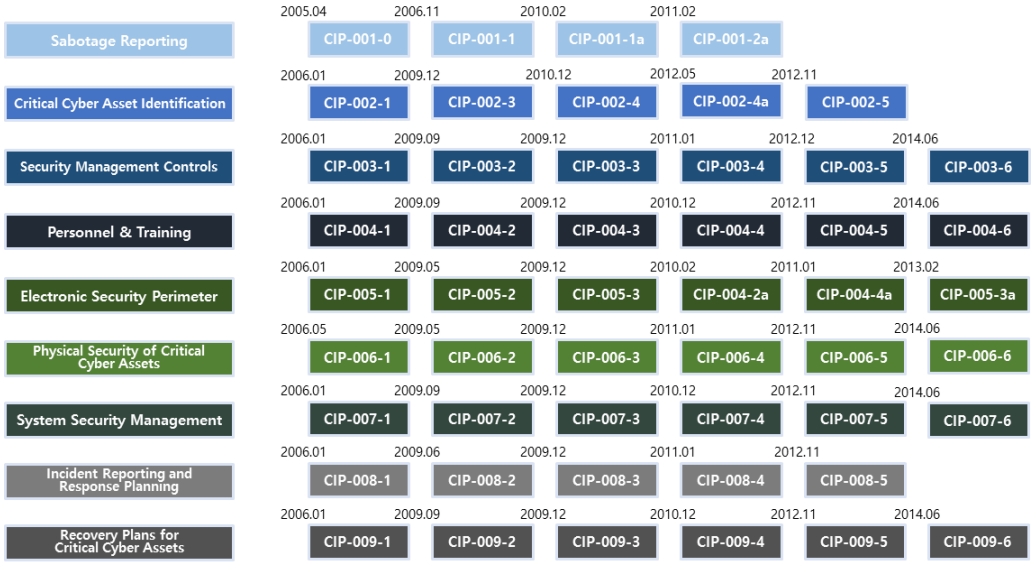
ISA/IEC 62443은 미국 ISA(International Society of Automation)가 산업제어시스템(ICS)에 대한 보안이슈를 다루기 위해 제정한 표준이다. ISO/IEC 62443 시리즈의 보안요구사항 및 보안대책은 산업제어시스템 환경에 적합하도록 특성화하여 제정되었으며 ISA/IEC 62443 시리즈는 일반, 정책 및 절차, 시스템, 컴포넌트의 4가지 범주로 나누어져 있다. 특히 중점을 두고 있는 대상은 주요 기반시설에서 다루고 있는 SCADA 시스템이다. IACS(Industrial Automation and Control System) 보안에 대한 정의 및 개념, 모델 등을 포괄하며 자산 소유자와 시스템 통합 관리자, 제품 공급자가 각자 지켜야 할 표준들이 제정되어 있다. 또한, 동일한 보안 요구사항을 준수하는 논리적, 물리적 자산들을 임계성과 중요성에 의해 나눈 Zone과 Zone들 사이에서의 네트워킹과 보안 레벨의 차이를 경감시키며 안전한 통신을 보장하는 Conduit이라는 개념을 포괄한다. 또한 ISA/IEC 62443은 보안 정책 및 절차와 기술적 보안 이행을 통해 제어시스템 내 보호 등급(Protection Level)을 제정할 예정이다. 보호 등급(Protection Level) 내 정책 및 절차에 대한 평가는 성숙도 수준(Maturity Level)을 통해 이루어지며, 기술적 보안 이행에 대한 평가는 보안 등급(Security Level)을 통해 이루어진다. 이를 통해 도출된 성숙도 수준과 보안 등급을 통합하여 최종 보호 등급(Protection Level)이 제정된다.

ISA/IEC 62443-1시리즈는 개념 및 모델과 용어의 정의, 시스템 보안 적합성과 보안 생명주기 등을 규정하며 ISA/IEC 62443-2시리즈는 제어시스템을 보유한 조직이 갖추어야 하는 보안정책과 관리 시스템에 관하여 규정한다. ISA/IEC 62443-3시리즈는 보안 기술, 보안 위험평가 및 시스템 디자인, 보안 등급 및 보안 요구사항을 규정하며 ISA/IEC 62443-4시리즈는 제품개발단계 보안요구사항과 기술적 보안요구사항을 규정한다. 또한 ISA/IEC 62443에는 자산 소유자와 시스템 통합 관리자, 제품 공급자가 각자 지켜야할 표준들이 제정되어 있다.

2007년도에는 62443-1-1이 정립되었다. 이는 용어, 컨셉 모델을 정리한 부분이다. 2009년에는 62443-2-1과 62443-3-1이 추가되었다. 이는 IACS 보안 프로그램 구축과 IACS에 적용 가능한 보안 기술에 관한 내용이다. 2013년에는 62443-1-3과 62443-3-3이 추가되었다. 이는 시스템 보안 준수여부 측정 방법과 보안 보증 수준 및 시스템 보안 요구사항이 포함된 내용이다. 그리고 2015년에는 62443-2-4 가 추가되었다. 이는 IACS 공급자 보안 정책 요구사항으로서 WIB의 표준을 ISA 62443 시리즈에 포함한 것이다.

3.4. NERC CIP

NERC는 2006년 FERC에 의해 세워진 미국 전기 신뢰성기구(ERO: Electronic Reliability Organization)이고, CIP는 준수하지 않으면 하루에 수천~수백만 달러에 이르기까지 상당한 재정적 처벌이 발생할 수 있는 주요 표준 중에 하나이다. 따라서 NERC CIP는 자율 규제에 있어서 가장 영향력을 갖는 보안 표준이 되었다. NERC CIP에서는 사이버 보안 자산 식별 및 보호에 관한 사이버 보안 프레임워크를 제공하여 대형 에너지 시스템(Bulk Electric System)을 안전하게 조작할 수 있도록 지원하고 있다. NERC CIP는 매년 또는 격년으로 개정



〔그림 2〕 NERC CIP 세부 항목별 개정 동향

되고 있고, 가장 최근의 변화인 버전 5에서 버전 6으로의 변화 양상에 대해 보고자 한다. 버전 5, 6의 주요 변화 양상은 아래와 같다.

2015년, FERC의 Order 822로 인해 NERC CIP 버전 6이 승인되었다.

CIP-004-6, CIP-007-6, CIP-009-6, CIP-011-2에서는 크게 2가지가 바뀌었다. 첫 번째는, 결함을 식별하고 평가하고 수정하는 방식으로 특정 언어 비트를 제거하는 것이다. 이는 여러 가지 CIP 요구 사항에 나타나지만, FERC는 Order 791에서 "너무 모호하여 감사를 받을 수 없다"고 결정했다. 두 번째는, 임시 사이버 자산과 이동식 미디어에 관한 업데이트 지침이 포함된 것이다.

CIP-003-6에서는 BES 사이버 자산의 처리에 관한 항목이 바뀌었다. '높음 및 중간'의 평가를 받는 것으로는 최상위 레벨에 속하지 못하도록 바꾸었다. 그리고 이를 위한 기본 요구 사항을 '높음 및 중간'에 대한 부분과 '영향이 적은 자산'에 대한 별도 부분으로 나누어 평가한다.

CIP-006-6에서는 R1.10을 추가하여 물리적 보안 경계 외부에 있는 '케이블링 및 기타 프로그래밍 할 수 없는 통신 구성 요소'의 물리적 보안을 해결한다. 이러한 요소를 물리적으로 적절하게 보호할 수 없는 경우, 해당 구성 요소를 통과하는 데이터의 암호화 시스템, 모니터링 시스템, 네트워크 경보 시스템 등을 포함한 일련의 논리적 제어를 구현해야 한다.

Ⅳ. 국내 정보보호 관리체계 현황

4.1. 주요정보통신기반시설 취약점 분석·평가

정보통신기반보호법은 2001년에 제정되었는데, 이에 따르면 정보통신기반시설이란 국가 안전 보장·국방·금융·운송·에너지 등의 업무와 관련된 전자적 제어관리 시스템 및 정보통신망을 의미한다. 동법에서는 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 '주요정보통신기반시설'로 지정할 수 있도록 하였다[6].

주요정보통신기반시설 취약점 분석·평가는 스턱스넷 등 새로운 유형의 침해사고를 예방하기 위해 기존에 있던 취약점 분석평가 기본항목 외에도 제어·DB·PC 분야별로 분석항목을 새로 만들었다. 그리고 특수한 정보시스템에 관한 정보통신기반시설 취약점 분석·평가 기준은 일차적으로 2001년부터 2004년까지 수립 및 배포되었다. 이를 통해 기본적인 기준이 수립되었다. 그리고 이차적으로 2004년부터 2011년까지 수립 및 배포되었는데, 이때는 취약점 분석·평가 절차의 단계별 상호 연계성을 강화하였다. 3차적으로 2012년 12월에 신규 취약점 적극 대응을 위하여 매년 진행하는 취약점 분석평

가 및 취약점 분석항목의 신설을 확대하였다. 그리고 이를 2013년 8월에 시행하여 계속 이어져 오고 있다.

4.2. 정보보안 관리실태 평가

정보보안 관리실태는 각급 기관이 체계적으로 정보보안 업무를 수행할 수 있도록 지원하고 관련 기관 종사자의 보안의식을 함양함으로써 국가기관 정보보안 수준을 높이고, 국가의 사이버 안전을 확보하기 위해서 만들어졌다.

정보보안 관리실태 평가는 정보보안 정책, 정보자산 보안관리, 인적 보안, 사이버 위기 관리, 전자정보보안, 정보시스템 보안 이렇게 5가지 항목에 대해 각각 평가를 진행한다. 그리고 각각의 항목에 대해 세부 항목의 점수를 합산하여 우수(90점 이상), 양호(80점 이상), 보통(70점 이상), 미흡(60점 이상), 불량(60점 미만)의 5단계로 관리 수준에 대한 평가결과를 산출한다.

정보보안 관리실태 평가는 2004년에 도입되었으며 2006년에 50개 국가기관을 대상으로 시범평가를 실시하였다. 2007년에는 교육청 및 99개 공공기관 대상으로 수행하고, 2008년에는 정부출연 연구기관, 2009년에는 공기업으로까지 대상을 확대하였다. 2011년에는 사이버안전센터에서 정보보안 관리실태에 대해 직접 평가하고, 감독부처를 통해 산하기관 간접평가를 진행하였다. 2012년 준정부기관으로 대상을 확대하고 2013년에는 120개 공공기관에 대한 평가를 수행하였다[10].

Ⅴ. 결 론

본 논문에서는 제어시스템에 대한 국내외 주요 침해사고 및 표준에 대해 조사하였다. 국외 제어시스템 관련 표준으로 NIST SP 800-53, NIST SP 800-82, ISA/IEC 62443, NERC CIP 와 국내 정보보호 관리체계 현황으로 주요정보통신기반시설 취약점 분석·평가, 정보보안 관리실태 평가에 대해 알아보았다. 동 기간 내 침해사고 발생 및 국제표준 개정 양상을 개괄적으로 살펴보았을 때, 공격 흐름에 따라 지속적으로 국제 표준이 개정 또는 새로 발간되고 있다. 반면, 국내 정보보호 관리체계는 수행되는 분석 및 평가 대비 지속적인 제정·개정은 상대적으로 이루어지고 있지 않은 것으로 보인다. 따라서 빠르게 변화하는 사이버환경에 적합한 정보보호 관리체계가 요구된다. 이를 위한 향후 연구로써 침해사고와 보안 표준 개정 및 제정의 직접적인 연관관계를 찾고, 국내 정보보호 관리체계 문제점에 대한 해결 방안에 대하여 논의해봐야 할 것이다.

참 고 문 헌

[1] 김인중, 정윤정, 고재영, 원동호, “중요핵심기반시설에 대한 보안 관리 연구”, 한국통신학회논문지, 30(8C), 2005.

[2] 이철원, “국가 기반시설 사이버 보안기술 동향”, 한국위기관리논문집, 2008.

[3] 손경호, “산업시스템 보안성 평가·인증 동향 분석”, 정보보호학회지, 24(5), pp. 15-25, 2014.

[4] 최명균, 이동범, 곽진, “제어 시스템에 대한 보안 정책 동향 및 보안 취약점 분석”, 정보보호학회지, 21(5), pp. 55-64, 2011.

[5] 김성호, 김신규, 서정택, “전력신뢰도 관리기구의 사이버보안 활동 동향 및 국내 적용방안 고찰”, 정보보호학회지, 24(1), pp. 59-64, 2014.

[6] 박소현, 이용주, 이경호, “위험관리 측면에서의 제어시스템 보안 표준 동향”, 정보보호학회지, 25(5), pp. 45-52, 2015.

[7] 윤오준, 배광용, 김재홍, 서형준, 신용태, “사이버 공격 대응 분석을 통한 사이버안보 강화 방안 연구, 한국융합보안학회, 15(5), pp. 71-78, 2015.

[8] 윤오준, 한복동, 박정근, 서형준, 신용태, “침해사고 분석을 통한 기반시설 보호 강화 모델 연구”, 한국융합보안학회, 15(6), PP. 29-36, 2015.

[9] 신영웅, 전상훈, 임채호, 김명철, “국가 사이버보안 피해금액 분석과 대안”, 국가정보연구, 6(1), pp. 129-173, 2013.

[10] 국가사이버안전센터, “정보보안 관리실태 평가 소개”, 한국정보보호학회지, 23(5), pp. 9-11, 2013.

〈저 자 소 개〉

오 준 형 (Jun Hyoung Oh)
정회원

2017년 2월 : 고려대학교 전기전자전파공학부 졸업
2017년 3월~현재 : 고려대학교 정보보호대학원 석·박사 통합과정
관심분야 : 정보보호, 위험관리, 정보보호컨설팅

유 영 인 (Young in You)
정회원

2013년 8월 : 서울시립대학교 수학과 졸업
2013년 9월~2015년 8월 : 고려대학교 정보보호대학원 석사 졸업
2015년 9월~현재 : 고려대학교 정보보호대학원 박사 과정
관심분야 : 정보보호, 위험관리, ISMS

이 경 호 (Kyung Ho Lee)
종신회원

1989년 8월 : 서강대학교 수학과 학사
1997년 8월 : 서강대학교 정보통신대학원 석사 졸업
2009년 8월 : 고려대학교 정보보호대학원 박사 졸업
1994년 2월~현재 : 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재 : 고려대학교 정보보호대학원 부교수
관심분야 : 정보보호, 위험관리, 정보보호컨설팅, 개인정보보호 정책