정 보 보 호 학 회 지
제27권 제2호, 2017. 4

원자력시설 사이버보안 규제기준 측면의 기술적 보안조치에 대한 이행방안 연구

김 나 영*, 임 현 종**, 김 상 우***, 송 동 훈****, 신 익 현*****

요 약

원자력시설에 대한 사이버보안 위협이 증가됨에 따라 「원자력시설 등의 방호 및 방사능 방재 대책법」에 의거 원자력통제기술원은 사이버보안 이행에 관한 세부 기준을 제시하는 KINAC/RS-015 「원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준」을 마련하고 원자력 사업자로 하여금 사이버보안계획(CSP)을 이행토록 하였다. 따라서 원자력사업자는 사이버공격으로부터 필수디지털자산(CDA)을 보호하기 위해 운영적·관리적·기술적 사이버 보안조치를 적용 및 이행하여야 한다. 본 논문에서는 원자력시설의 최상위 설계요건인 안전성 및 신뢰성 확보를 위해 사이버보안 기술을 적용하는데 많은 어려움이 따르는 기술적 보안조치인 접근통제, 감사 및 책임, 시스템 및 통신의 보호, 식별 및 인증, 시스템 보안강화에 대한 이행방안을 살펴보고자 한다.

Ⅰ. 서 론

디지털 기술의 발전으로 디지털 시스템 도입 및 사용이 확대 되어 원자력시설 뿐만 아니라 산업계 전반에 걸쳐 사용되고 있다. 특히 원자력발전소의 경우 두뇌와 신경망에 해당하는 계측제어시스템 뿐만 아니라 보안시스템, 비상대응시스템 등 많은 디지털 시스템을 사용하고 있으며 운영에 있어 보다 높은 안전성(Safety) 및 신뢰성(Reliability)을 확보 할 수 있도록 지원하고 있다.

반면에 디지털 시스템 도입으로 IT 분야에서 발생하는 각종 사이버위협이 증대되는 단점을 가지게 되었다. 실제 2010년 이란 원자력시설내 우라늄 원심분리기 가동을 중단시킨 스턱스넷(Stuxnet), 2011년 제어시스템 정보 수집 및 유출을 목표로 한 두큐(Duqu), 2012년 이란 등 중동 국가의 전력제어시스템을 손상시킨 플레임(Flame) 등 위협이 현실화되고 있다.[1] 원자력시설을 대상으로 한 사이버공격은 핵물질의 노출 또는 원자력시설의 파괴, 손상으로 인한 공공의 건강, 안전 및 환경을 위태롭게 할 수 있는 심각한 결과를 야기할 수 있으므로 원자력시설을 보호하기 위한 사이버보안 기술 적용은 필수적으로 요구되고 있다.

원자력시설의 보안성 확보를 위해 미국에서는 미연방법 10CFR73.54에 따라 원자력시설의 안전, 보안 및 비상대응(SSEP, Safety, Security, and Emergency Preparedness) 기능 및 지원시스템 기능 수행에 있어 필수디지털자산(CDA, Critical Digital Asset)을 식별하고 설계기준위협(DBT, Design Basis Threat)을 포함한 원자력시설의 디지털 컴퓨터와 통신 시스템 및 네트워크를 사이버공격으로부터 보호 할 것을 요구하고 있다. 이에 따라 미원자력규제위원회(NRC)는 10CFR73.54에서 명시한 사이버보안에 대한 법령을 구체화한 규제지침 RG5.71을 발간하여 미국 전역에 운영 중인 원자력시설에 대해서 사이버보안계획(CSP, Cyber Security Plan)의 수립 및 운영을 요구하고 있다.[2]

RG5.71은 미국립표준기술연구소(NIST)에서 개발한 정보시스템 사이버보안 요구사항인 NIST SP800-53과

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다.
* 원자력통제기술원 사이버보안실 (nykim@kinac.re.kr)
** 원자력통제기술원 사이버보안실 (silltown@kinac.re.kr)
*** 원자력통제기술원 사이버보안실 (kjoey@kinac.re.kr)
**** 원자력통제기술원 사이버보안실 (igiveitashot@kinac.re.kr)
***** 원자력통제기술원 사이버보안실 (ihshin@kinac.re.kr)

SP800-82를 근거로 작성되었으며 이는 연방정부 행정기관을 지원하는 정보시스템에 대한 사이버 보안조치 요건 및 사이버보안 프로그램을 수립하고 유지하기 위한 지침이다.[3][4]

국내의 경우 「원자력시설 등의 방호 및 방사능 방재 대책법」 시행령 및 시행규칙 개정에 따라 원자력통제기술원(KINAC)에서 미원자력규제위원회(NRC) 규제지침 RG5.71을 기반으로 KINAC/RS-015 「원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준」을 마련하였다.[5] 원자력사업자는 기술기준에 따라 사이버보안대책 수립을 위해 사이버보안계획(CSP)을 이행하여야 하며 한국원자력통제기술원에서 이행결과에 대한 적합성 등을 심·검사한다.

사이버보안계획(CSP) 중 보안 조치 활동으로 관리적·운영적·기술적 보안조치를 포함하고 있으며 기술적 보안조치의 경우 하드웨어, 펌웨어, 운영체제, 응용프로그램 내부에 포함된 메커니즘을 통해 수행되는 보안조치로 사이버보안 기술 적용 시 많은 설계 변경 및 비용이 발생할 것으로 우려되고 있다.

따라서 본 논문에서는 기술적 보안조치인 접근통제, 감사 및 책임, 시스템 및 통신의 보호, 식별 및 인증, 시스템 보안강화 5개 통제항목과 62개의 세부항목을 알아보고 원자력시설에 적용 시 고려할 사항과 사이버 위험 요소로부터 필수디지털자산(CDA) 보호를 위한 보안조치 이행방안을 살펴보고자 한다. 다만, 앞으로 서술할 내용은 보안조치로 활용될 수 있도록 고려된 내용이며, 실제 이 이외의 다양한 고려사항과 이행 방안들이 고려되어야 할 것이다.

Ⅱ. 원자력시설 사이버보안

원자력시설의 사이버보안은 핵물질의 불법이전 및 사보타주를 일으킬 수 있는 사이버공격으로부터 원자력시설 등의 컴퓨터 및 정보시스템이 악영향을 받지 않도록 하는 것을 말한다. 이는 원자력시설의 안전, 보안 및 비상대응(SSEP) 기능에 악영향을 미칠 수 있는 시스템이나 데이터의 기밀성, 무결성, 가용성을 유지함으로써 달성된다.

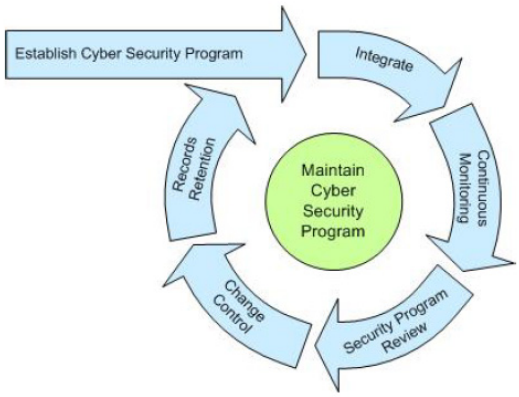
이에 따라 본 장에서는 원자력시설을 사이버공격으로부터 보호하기 위한 사이버보안계획(CSP)을 알아보고, 원자력시설을 포함하고 있는 산업제어시스템(ICS, Industrial Control Systems) 전반에 걸쳐 발생할 수 있는 보안 위협(Threats) 및 취약점(Vulnerabilities)과 이에 따른 사이버공격의 탐지, 예방, 대응, 완화 및 복구 능력을 갖추기 위한 원자력시설의 심층방호(Defense-in-Depth) 전략을 살펴본다.

2.1. 사이버보안 계획

「원자력시설 등의 방호 및 방사능 방재 대책법」 제9조(물리적방호에 대한 원자력사업자의 책임) 및 동법 시행령 제17조(물리적방호규정등 승인신청), 동법 시행규칙 제5조(물리적방호등의 작성), 원자력안전위원회 고시 「물리적방호규정등의 작성내용의 항목별 세부작성기준」에 의거하여 사이버보안계획(CSP)은 사이버 보안의 대상이 되는 필수디지털자산(CDA)을 설계기준위협(DBT)의 사이버공격으로부터 보호하기 위한 세부내용을 기술한다. 보호 대상이 되는 필수디지털자산(CDA)은 SSEP 기능을 수행하거나 그 기능에 영향을 미치는 컴퓨터 및 정보시스템으로서 원자력시설 내·외부의 아날로그 혹은 디지털 기반 시스템을 말하며 원자력시설 시스템, 기기, 통신시스템, 네트워크, 외부통신, 지원시스템 혹은 지원기기를 포함하고 있다.

이에 따라 사이버 공격으로부터 보호할 자산을 식별하고 보호하기 위해 사이버보안계획(CSP)을 수립 및 이행하고 유지해야한다. 사이버보안계획(CSP)는 필수디지털자산(CDA)을 보호하기 위한 보안조치, 심층방호 전략, 사이버보안 훈련, 사이버리스크 평가 및 관리 등을 포함하고 사이버 공격으로부터 악영향을 받지 않음을 보증해야 하고 사이버공격을 탐지, 예방, 지연, 완화 및 복구하기 위한 관리적·운영적·기술적 보안조치 수행 방안을 포함해야 한다.

이에 따라 원자력사업자는 사이버보안계획(CSP)을 마련하고 이를 7단계로 나누어 2018년 10월까지 단계적으로 이행하고 있다. 7단계 이행은 1단계 사이버보안조직 구성, 2단계 필수디지털자산 식별, 3단계 심층방호 및 비상대응, 4단계 매체통제, 5단계 무결성유지, 6단계 운영적·관리적 보안조치, 7단계 기술적 보안조치의 단계로 구성되어 있으며 원자력안전위원회로 부터 심사, 검사, 훈련 및 위협평가 업무를 위탁 받은 한국원자력통제기술원(KINAC)이 각 단계를 순차적으로 이행하도록 규제하고 있다.



〔그림 1〕 원자력시설 사이버보안 생명주기

또한 원자력사업자는 사이버보안계획(CSP)을 수립한 후에는 사이버공격에 대하여 효과적으로 대처가 가능함을 보장하기 위해 [그림 1] 원자력시설 사이버보안 생명주기와 같이 지속적인 감시와 평가 및 변경 통제 활동을 수행하여야 한다.

2.2. 보안 위협(Threats)

원자력시설을 대상으로 발생하는 보안위협은 다양한 공격 행위자 및 공격 유형들이 발생할 수 있으며 원자력시설 뿐만 아니라 산업제어시스템(ICS) 전반에 걸친 보안 위협을 살펴본다.

2.2.1 공격 행위자

원자력시설을 포함한 산업제어시스템을 대상으로 한 공격 행위자는 개인이나 조직이 될 수 있으며 디지털 시스템에 대한 의존도가 높아지면서 사이버 공격에 대한 위험성도 높아지고 있다.

이에 따른 사이버 위협은 국가정부, 테러리스트, 산업스파이 및 범죄단체, 해커, 내부자 등에 의한 악의적인 위협과 시스템 복잡성으로 인해 사람에 의한 실수 및 사고, 장치 고장 및 자연재해와 같은 다양한 위협 인자에 의해 발생할 수 있다.[6] 원자력시설을 대상으로 보안 위협을 수행할 가능성이 있는 악의적인 행위자는 [표 1]과 같이 다양한 목적과 동기를 갖고 있으며 사이버 공격으로 최악의 경우 핵물질의 노출 또는 원자력시설의 파괴 및 손상으로 심각한 결과를 야기할 수 있다.

〔표 1〕 원자력시설 등 제어시스템 대상 보안 위협

위협	위협 내용
국가정부	평시 및 전쟁 수행시 적대국에 대한 시스템 파괴·교란 수행
테러리스트	특정 목적 달성을 위해 인명 피해 및 시설물 파괴 목적으로 사이버테러리즘 수행
산업스파이 및 범죄단체	산업 기밀에 대한 지적자산 및 노하우 취득을 목적으로 대규모 경제 범죄 수행
핵티비스트	정치적 동기를 가지고 시설에 대한 파괴적인 행동 보다는 선전활동 수행
해커	실력과시 등 취약점 도출을 위한 침입 시도, 다양한 해커집단으로 상대적 높은 위협 제기

2.2.2 공격 유형

원자력시설을 포함한 산업제어시스템을 대상으로 한 공격 유형은 다양한 형태로 나타나고 있지만 폐쇄망으로 이루어진 제어시스템 내에 침투하기 위해서는 고도화된 사회공학적 기법 및 피싱 공격과 이동식 미디어 및 외부 하드웨어를 통한 악성코드 침투 공격이 가장 많이 시도되고 있다. 산업제어시스템을 타겟으로 한 공격유형은 최초 공격과 후속 공격으로 구분되어 질 수 있으며 최초 공격은 제어시설 관련자를 타겟으로 인터넷 또는 업무망을 이용해 제어시설 내부 침투를 위해 사용되며 후속 공격은 제어시설내 디지털 시스템을 위협하거나 엑세스하기 위한 공격이 이루어진다.

산업제어시스템의 경우 과거에 보안을 고려하지 않고 설계를 하였기 때문에 해결되지 않은 기존 취약점에 의해 잠재적인 손상을 줄 수 있는 공격유형이 대다수이며 2016년 가장 많이 발생한 공격유형은 [표 2]와 같다.[7]

〔표 2〕 산업제어시스템을 대상으로 한 공격유형(2016)

순위	공격 유형
1	사회공학기법 및 피싱
2	이동식 미디어 및 외부 하드웨어를 통한 악성코드 침투
3	인터넷망 및 업무망을 통한 악성코드 감염
4	원격 접근경로를 통한 침입
5	휴먼에러 및 사보타주
6	인터넷에 연결된 제어 컴포넌트
7	기능에 대한 잠재적 오류
8	유지보수를 위한 외부 요소 및 익스트라넷의 위험
9	서비스거부 공격
10	작업환경에서의 스마트폰 또는 태블릿PC의 위험

2.3. 보안 취약점(Vulnerabilities)

원자력시설에 사용되고 있는 디지털 시스템은 산업용 컴퓨터, 서버, 네트워크 장비들 뿐만 아니라 임베디드 시스템(Embedded System), PLC(Programmable Logic Controller), DCS(Distributed Control System)를 포함하고 있다. 이는 산업제어시스템에서 발생 할 수 있는 공통 취약점인 소프트웨어 및 제품 보안 취약점, 설정 취약점, 네트워크 보안 취약점을 포함하고 있으며 미국토안보부(DHS)의 제어시스템보안프로그램(CSSP, Control Systems Security Program)와 ICS-CERT의 보안평가를 통해 보고된 취약점 정보를 기반으로 살펴본다.[8]

2.3.1. 소프트웨어 및 제품 보안 취약점

원자력시설을 포함한 산업제어시스템에서는 생산되는 데이터 분석을 위해 원격 관리 및 제어 또는 모니터링을 쉽게 할 수 있도록 웹기반의 응용프로그램과 원격 서비스 등을 지원하고 있다. 이에 따라 소프트웨어 및 제품에 대한 기능 개선 또는 추가로 다양한 취약점들이 도출되고 있으며 웹기반의 응용프로그램 구현에 따라 특정 디지털 시스템에서 디렉토리 트레버셜 및 인증 우회 취약점 등이 발견되고 있다.[9] 산업제어시스템에서 가장 많이 발견되는 소프트웨어 및 제품보안 취약점은 [표 3]과 같다.

〔표 3〕 소프트웨어 및 제품 보안 취약점

구분	취약점
부적절한 코드 사용	• 잠재적으로 위험한 함수 사용 • Null 포인터 역참조
부적절한 입력 검증	• 버퍼오버플로우 • 범위 검사 부족 • 명령어 인젝션 • 크로스사이트스크립트 • 경로 트레버셜
허가, 특권 및 접근 통제	• 부적절한 접근제어 • 불필요한 권한 부여
부적절한 인증	• 인증 우회 • 중요한 기능에 대한 인증 누락 • 클라이언트기반 인증 사용 • 단말간에 접근 가능 채널
데이터 확실성의 불충분한 확인	• CSRF • 무결성 검사에 대한 누락 • 무결성 검사 없는 코드 다운로드
암호화 이슈	• 민감 데이터에 대한 암호화 누락 • 부적절한 암호화 알고리즘 사용
자격 관리	• 불충분하게 보호된 자격증명
보안설정 및 유지관리	• 부적절한 패치 관리 • 부적절한 보안 설정

2.3.2. 설정 취약점

원자력시설을 포함한 산업제어시스템 설정 취약점은 디지털 시스템이 설치되고 유지되는 방식에 따라 취약점이 발생 할 수 있다. 보안 측면에서 디지털 시스템을 안전하게 설정하기 위한 표준 절차 및 지침 부족으로 디지털 시스템을 공급하는 과정에서 도입되는 운영체제 및 응용프로그램의 설치 및 설정에 대한 보안 수준이 다르게 구성된다.

디지털 시스템의 설정으로 발생될 수 있는 일반적인 보안 문제로는 패치되지 않은 운영체제, 응용프로그램 및 서비스 취약점이 존재할 수 있으며 디지털 시스템에서 지원하는 기능을 어떻게 시스템에 설정 하냐에 따라 취약점 존재여부가 달라질 수 있다. 보안 설정은 산업제어시스템의 기존 설계로 제한 될 수 있지만 디지털 시스템을 보안성 있게 설정한다면 사이버 공격에 대한 위험을 최소화 할 수 있다. 산업제어시스템에서 가장 많이 발견되는 설정 취약점은 [표 4]과 같다.

〔표 4〕 설정 취약점

구분	취약점
허가, 특권 및 접근 통제	• 취약한 시스템 접근통제 • ICS 호스트의 공용네트워크 공유 • 부적절한 보안 설정값 설정
부적절한 인증	• 취약한 시스템 식별 및 인증 제어
자격 관리	• 취약한 패스워드 관리 정책 • 불충분하게 보호된 자격증명
보안 설정 및 유지관리	• 취약한 테스트 평가 • 취약한 패치 관리 • 취약한 백업 및 복원 능력
계획/정책/절차	• 부족한 보안 문서 • 취약한 보안 문서 유지관리
감사 및 책임 (모니터링)	• 보안 감사 및 평가 부족 • 로깅용량 부족 및 로깅실행 불량

2.3.3. 네트워크 보안 취약점

산업제어시스템 네트워크는 독립적으로 구성하고 외부 네트워크와 분리한 폐쇄망으로써 사이버보안 경계를 구분해 방어 전략을 수립하도록 권고하고 있다.

이에 따라 원격지에서 디지털 시스템 관리 및 모니터링을 수행하고 디지털 시스템에서 발생하는 데이터를 외부 네트워크로 전송하는 경우 사이버보안 경계에서의 데이터 이동 통제를 강화해 네트워크를 안전하게 구현해야한다.[10]

원자력시설은 통신의 신뢰성, 안전성 그리고 실시간 제어능력이 중요시되므로 규제요건을 고려하여 보안성 있게 네트워크가 구현되어야 하며 보안등급이 높은 경계에서 낮은 경계로의 통신은 물리적인 단방향이 되도록 구성하고 낮은 경계에서 높은 경계로의 통신을 금지하고 있다. 하지만 경계 네트워크간의 결함, 잘못된 구성, 또는 허술한 관리로 취약점이 발생 할 수 있다. 산업제어시스템에서 가장 많이 발생한 네트워크 보안 취약점은 [표 5]과 같다.

〔표 5〕 네트워크 보안 취약점

구분	취약점
네트워크 설계 취약점	• 정의 되지 않은 보안경계 • 네트워크 세그먼테이션의 부족 • DMZ의 부족 • 존재하지 않거나 부적절하게 구성된 방화벽 • 방화벽의 통과
네트워크 장비 설정 취약점	• 제대로 설정되지 않은 네트워크 장치 • 네트워크 장비에 구현되지 않은 포트 보안
취약한 방화벽 정책	• 필수 IP 주소로 제한되지 않은 호스트의 특정 포트에 대한 접근 • ICS 트래픽에 맞지 않게 조정된 방화벽 정책
감사 및 책임 (모니터링)	• 잘못 구성된 네트워크 구성 • 원격접근 정책의 취약한 이행 • 미디어에 대한 취약한 통제 • 제어 네트워크 이벤트를 모니터링하기 위한 방법의 불충분함

2.4. 방어 전략 (Defense-in-Depth)

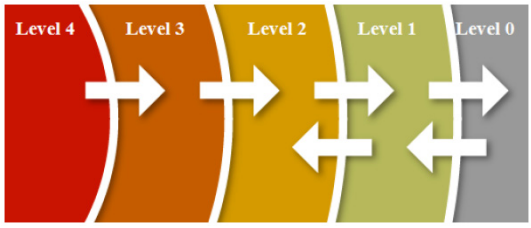
원자력시설의 효과적인 방어 전략은 사이버보안 경계를 구분하여 사이버공격을 탐지 및 예방하고 사이버공격으로 인한 피해 완화 및 복구를 위해 보안조치를 적용한 심층방호(Defense-in-Depth) 구조를 갖는다.

2.4.1. 원자력시설 심층방호 구조

원자력시설의 심층방호(Defense-in-Depth) 전략을 적용하여 필수디지털자산을 설계기준위협에서 정한 사이버 공격으로부터 보호한다. 사이버보안 심층방호 구조는 [그림 2]와 같이 사이버보안 경계로 구분된 5가지의 사이버보안 등급으로 구성되며 각 경계에서의 디지털 통신은 감시 및 통제되며 높은 사이버보안성이 요구되는 시스템일수록 높은 등급의 구역에 배치되고 사이버공격을 탐지, 예방, 지연, 완화 및 복구하기 위한 보안조치들이 적용된다.

일반적인 사이버보안 심층방호 구조는 다음의 특징을 포함한다.

- ⊙ 안전관련 기능 및 보호 기능을 수행하는 필수디지털 자산을 가장 높은 등급에 배치하고 낮은 등급으로부터 보호한다.
- ⊙ 필수디지털자산이 침해를 받을 경우 SSEP 기능에 악영향을 미치는 지원시스템은 최소 3등급 배치한다.
- ⊙ 높은 등급에서 낮은 등급의 통신은 물리적으로 단방향이 되도록 구성하고 낮은 등급에서 높은 등급의 통신이 되는 것을 금지한다.
- ⊙ 등급별 데이터의 이동은 경계보호시스템을 통해서만 가능하다.



〔그림 2〕 원자력시설의 심층방호 전략

Ⅲ. 기술적 보안조치 이행방안

전자적 침해행위에 대한 원자력시설의 컴퓨터 및 정보시스템 보안에 대한 기술기준 KINAC/RS-015의 보안조치로 관리적·운영적·기술적 보안조치를 요구하고 있으며 이중 원자력시설의 최상위 설계요건인 안전성

〔표 6〕 KINAC/RS-015 기술적 보안조치

통제항목	세부항목	설명
접근통제	19	인가된 사용자가 필수디지털자산에 접근하여 인가된 행위만이 수행되도록 보장
감사 및 책임	11	사이버보안계획의 사항들을 감사하기 위해 책임 및 관리되도록 보장
시스템 및 통신 보호	19	시스템 및 통신설비에 악영향을 유발할 수 있는 비인가 접근 위험으로부터 보장
식별 및 인증	8	주요 네트워크 사용자, 호스트, 응용프로그램, 서비스 등에 대한 식별 및 인증 보장
시스템 보안 강화	5	필수디지털자산을 불법 접근 및 불법 사용으로부터 보호하기 위한 기술적 보장

및 신뢰성 확보에 있어 사이버보안 기술을 적용하는데 많은 어려움이 따르는 기술적 보안조치에 대해서 원자력시설에 적용 시 고려사항과 이행방안을 살펴본다. 기술적 보안조치는 [표 6]과 같이 5개 통제항목과 62개 세부항목으로 구분되어 있다.

3.1. 접근통제 기술적 보안조치

접근통제는 오직 인가된 개인 혹은 절차에 따라서만 필수디지털자산에 접근이 가능하고 인가된 행위만이 수행될 수 있도록 아래와 같이 접근 통제 정책을 적용하고 유지하기 위한 절차가 포함되어야 하며 기술적 보안조치로 [표 7]과 같이 19개 세부항목으로 구성되어 있다.

- ⊙ 접근 통제 권한 : 어떤 개인 혹은 프로세스가 특정 자원에 접근할 수 있는지에 관한 사항
- ⊙ 접근 통제 특권 : 어떤 개인 혹은 프로세스가 접근된 자원을 가지고 무엇을 할 수 있는지에 관한 사항
- ⊙ 시스템 강화 : 불필요한 서비스, 데이터 저장 공간 및 안전하지 않은 프로토콜의 식별 및 제거에 관한 사항
- ⊙ 필수디지털자산 감사 : 계정의 생성, 활성화, 변경, 검토, 차단, 폐기 및 제거에 관한 사항
- ⊙ 업무의 분리 : 할당된 접근 권한을 통한 업무 분리에 관한 사항

〔표 7〕 접근통제 기술적 보안조치 세부사항

통제항목	세부항목
1. 접근 통제	계정 관리
	접근통제 이행
	데이터 이동 통제
	기능의 분리
	최소 특권
	접속실패 기록
	시스템 사용 공지
	이전 접속기록 공지
	세션 잠금
	접근통제 감독 및 검토
	식별이나 인증 없이 허가된 활동
	네트워크 접근통제
	안전하지 않은 프로토콜의 제한
	무선연결 금지
	안전하지 않은 연결
	휴대용 매체 및 모바일 기기 접근 통제
	특정 프로토콜 가시성
	제3자 제품 사용
	외부시스템의 사용

3.1.1. 계정 관리 방안

필수디지털자산에 생성 될 수 있는 계정은 관리자계정, 개인계정, 공유계정, 그룹계정, 시스템계정, 게스트 및 익명 계정, 긴급계정, 개발자계정, 제조 및 공급업체 계정, 임시 및 서비스 계정 등이 포함될 수 있으며 해당 계정의 관리 미흡으로 필수디지털자산에 대한 불법적인 사용 및 변경이 될 수 있다.

이에 따라 필수디지털자산에 사용되는 계정은 관리(승인, 사용, 변경, 불용 및 삭제)되어야 하며 아래와 같이 주어진 업무를 수행하는데 필요한 만큼의 제한된 접근권한을 각 계정에 부여하고 관리되어져야 한다.

- ⊙ 관리자계정 : 관리자 권한이 요구되는 사용자는 보안 책임자에 의해 계정 및 권한이 부여되고 주기적으로 관리 및 감독한다.

⊙ 임시 및 게스트 계정 : 단기간 임시로 사용 할 계정으로 필요시 활성화 및 비활성화 한다.
⊙ 비상계정 : 비상 상황에서 식별과 인증 없이 사용할 수 있는 상황을 구분하고 SSEP 기능에 악영향을 미치지 않는 범위내 권한을 부여한다.
⊙ 개발자계정 및 제조, 공급업체 계정 : 유지보수 및 작업 요구사항 등을 고려하여 주어진 업무를 수행하는데 필요한 만큼의 제한된 접근권한을 부여한다.

3.1.2. 데이터 이동 통제 방안

심층방호 전략에 따라 필수디지털자산 간 데이터의 이동을 준실시간으로 통제하고 필수디지털자산 간 데이터 이동이 필요한 경우 사이버 보안등급 경계에서의 경계보호시스템을 정의하고 제한적 데이터 이동을 허용한다. 이때 데이터 이동 통제를 위해 경계보호시스템으로써 방화벽 또는 단방향 데이터 전송 장치가 사용 될 수 있다.

⊙ 방화벽 : 네트워크 경계에서 트래픽 흐름을 제어하는 시스템으로 설정된 정책에 따라 허용 또는 거부를 결정하여 필수디지털의 불법 접근을 차단 할 수 있으며 방화벽 기술은 [표 8]과 같다.
⊙ 단방향 전송장치 : 정보 전달이 필요한 두 시스템 사이에 단방향으로만 정보가 전달 될 수 있도록 송·수신 회선의 한쪽을 물리적으로 차단한 전용 하드웨어 기반의 전송장치로 단방향 보안 게이트웨이 또는 데이터 다이오드라고 불린다.

〔표 8〕 방화벽 기술

구분	설명
패킷필터 기반	MAC 주소와 IP 주소, Port 주소를 기반으로 한 트래픽 제어 수행
상태 기반	네트워크 트래픽과 관련된 모든 통신 채널의 상태목록을 유지하고 서비스에 대한 특성 및 통신상태 관리를 통한 제어 수행
프록시 기반	FTP, HTTP 등과 같이 특정 응용프로그램 및 프로토콜 제어 수행

3.1.3. 네트워크 접근통제 방안

제어 네트워크에서 발생할 수 있는 중간자 공격(Man-in-the-Middle Attack)과 같은 위협으로부터 보호하기 위하여 아래와 같은 네트워크 접근 통제를 적용할 수 있다.

⊙ MAC 주소 잠금 : 네트워크 스위치 포트에 필수디지털자산에 부여된 MAC 주소를 고정시킴으로써 MAC 주소가 불일치 할 경우 통신 링크가 비활성화 됨에 따라 로컬 네트워크를 보호할 수 있다.
⊙ 정적 테이블 유지 : 대부분의 운영체제는 MAC 주소를 ARP 테이블에 동적으로 캐싱하고 있다. ARP 테이블을 정적으로 설정함에 따라 ARP 캐쉬감염 공격으로 부터 보호할 수 있다.
⊙ 물리적/논리적 네트워크 분리 : 동일 네트워크를 단일 브로드 캐스트 영역으로 나누기 위해서 물리적 스위치 또는 VLAN 기술이 사용된다. 이는 이더넷 계층에서 트래픽을 분리함으로써 브로드캐스트 영역에서 발생할 수 있는 위협으로부터 보호 할 수 있다.
⊙ 중요정보 암호화 : 제어 데이터에 대한 위·변조를 예방하기 위해서 장기적으로 시스템간 암호화를 포함하도록 설계하여야 하며 암호화와 더불어 인증 메커니즘을 통해 중간자 공격으로부터 보호 할 수 있다.

3.1.4. 휴대용 매체 및 모바일 기기 접근 통제 방안

휴대용 매체 및 모바일 기기에 대한 사용 제한을 위해 필수디지털자산에 접근 가능한 휴대용 매체 및 모바일 기기를 별도로 확보하고 사용 통제 및 모니터링을 수행하여야 한다. 또한 휴대용 매체 및 모바일 기기가 하나의 보안등급 내에서만 사용되어지고 다른 보안등급으로 이동되지 못하도록 적용해야한다.

⊙ 휴대용 매체 통제 : 플로피디스크, CD, DVD, 마그네틱테이프, USB, 노트북 등 디지털 저장장치에 대해서 접근 권한이 있는 사용자만 사용하여야 하며 매체에 대한 저장, 이동, 삭제, 파괴 및 처리뿐만 아니라 라벨링을 통해 관리되어져야 한다.
⊙ 모바일 기기 통제 : 개인용 모바일 기기의 경우 조직에서 구현한 보안 정책이 구현되지 않기 때문에 많은 위험요소를 가지고 있다 이에 따라 모바일 기기에 대한 구성관리, 식별 및 인증, 악의적인 코드 탐지, 보안 소프트웨어 구현, 안티바이러스 및 소프트

웨어 업데이트, 운영체제 무결성 확보, 불필요한 하드웨어(무선 등) 비활성 등 수행하고 이는 모바일장치관리(MDM)와 같은 시스템을 통해 관리 되어질 수 있다.

3.2. 감사 및 책임 기술적 보안조치

감사 및 책임은 원자력시설의 사이버보안계획(CSP)의 사항들을 감사하기 위한 목적, 범위, 역할, 책임 및 관리적 이행 의지에 대하여 기술적으로 구현해야하며 [표 9]와 같이 11개 세부항목으로 구성되어 있으며 최소한 아래의 내용을 포함하여 감사 수행을 보장해야한다.

⊙ 모든 필수디지털자산 통신연결 구성
⊙ 사용자 로그인, 로그아웃 기록
⊙ 설정, 로그, 소프트웨어, 펌웨어 변경
⊙ 관리자 접속 기록 및 관리자 명령어 사용 기록
⊙ 필수디지털자산에 적용된 보아요소의 변경 사항
⊙ 특정 관리자 기능의 불법적인 실행 여부

〔표 9〕 감사 및 책임 기술적 보안조치

통제항목	세부항목
2. 감사 및 책임	감사 대상 비상사건
	감사 기록의 대상
	로그 저장 용량
	로그 저장용량 초과 시의 대응
	감사대상 기록의 검토, 분석 및 보고
	감사대상 기록의 축약 및 생성
	타임스탬프
	감사 정보의 보호
	부인방지(Non-repudiation)
	감사기록의 보존
	감사기록의 생성

3.2.1. 감사 로그 관리 방안

보안 감사 로그는 로그인 활동, 자원 사용, 파일 수정 및 기타 보안 관련 정보를 제공해야한다. 감사 및 로그 관리를 적절히 구성하고 유지 관리 하지 않는다면 사이버 공격과 같은 비상사건 발생 시 분석 및 추적을 의한 처리과정(탐지, 분석, 격리, 제거 및 복구)에 영향을 받을 수 있기 때문에 아래와 같이 로그 생성, 보호 및 분석을 수행해야 한다.

⊙ 로그 생성 : 필수디지털자산에서 발생하는 다양한 로그를 생성하고 저장하기 위해서는 어떤 비상사건이 언제, 어디서 발생했으며 근원지 및 결과를 분석할 수 있도록 로그 컨텐츠를 구성해야한다. 또한 로그 분석시 추적성을 위한 타임스탬프 동기화, 대용량 로그 분석 등 자동화 분석을 위해 로그 표준형식을 사용하여 로그를 생성하고 저장해야한다.
⊙ 로그 보호 : 필수디지털자산에서 생성된 로그에는 중요 레코드가 포함되어 있으므로 로그를 침해로부터 보호해야한다. 로그의 고의적 또는 의도하지 않은 변경 및 삭제 등의 영향을 최소화하기 위해 가용성을 보장해야하며 로그 관리 정책에 따라 로그 저장 용량을 확보해야 한다. 이에 따라 스케줄에 의해 로그를 저장하고 일정 기간 후 발생한 사건의 분석과 추적을 위해 감사기록을 보존해야 한다.
⊙ 로그 분석 : 효율적인 로그 분석을 위해서는 분석 시간을 단축하고 가치 있는 결과를 생성하는 것이다. 이에 따라 필수디지털자산에서 발생되는 이벤트에 대한 상세 정보 및 메시지나 코드 등에 대한 로그 항목에 대한 이해도가 필요하다. 또한 이벤트에 대한 심각도 및 중요도를 구분하여 로그 항목 우선순위를 결정하여 분석을 진행하여야 한다. 또한 분석 시간 단축 및 다양한 분석 기법을 적용해 로그를 분석하기 위해 자동화된 로그분석 소프트웨어 등을 고려할 수 있으며 정기적 로그 검토 및 분석을 해야 한다.

3.2.2. 감사 로그 분석 방안

다양한 필수디지털자산에서 발생하는 비정형화된 로그와 축적된 대용량 로그 분석을 위해 SIEM (Security Information and Event Management)과 같은 로그 분석 소프트웨어가 고려될 수 있다. SIEM은 다양한 로그 정보를 수집 기록하고 다양한 분석 기법 등을 제공한다. SIEM 기술은 분석 데이터의 장비 정보, 장비 용량 및 장애 지점을 예측하고 보안 정보를 제공하는데 도움을 줄 수 있으며 잠재적인 보안 침입이 발생했을 때 경고를 제공할 수 있다. 또한 누적된 로그 데이터 수집 및 분석을 통하여 가시성을 제공함으로써 로그 분석 시간

을 최소활 할 수 있다.

SIEM은 제어시스템과 같은 복잡한 환경에서 네트워크 장치, 운영체제, 응용프로그램 및 데이터베이스에서 생성되는 로그를 중앙 집중식으로 관리할 수 있다. 하지만 제어시스템의 안전하고 효율적인 작업을 위해 신뢰성과 가용성을 보장해야하기 때문에 보안의 중앙 집중식 분석에 대한 필요성을 인식하고 기능을 통합하는 것은 아직 초기 단계이다.

3.3. 시스템 및 통신의 보호 기술적 보안조치

시스템 및 통신설비에 악영향을 유발할 수 있는 비인가 접근 위험성을 최소화하기 위해서 시스템 및 통신 보호에 관한 정책을 이행하고 유지하기 위한 절차로 [표 10]과 같이 19개 세부항목에 대한 기술적 보안조치를 요구하고 있다.

〔표 10〕 시스템 및 통신의 보호 기술적 보안조치

통제항목	세부항목
3. 시스템 및 통신의 보호	응용프로그램 보안기능의 분리
	공유 자원
	서비스거부 공격으로부터의 보호
	자원사용 우선권
	전송 무결성
	전송 기밀성
	신뢰 경로(Trusted Path)
	비승인 원격 서비스 기동
	보안 매개변수의 전송
	공개키 구조(PKI)
	모바일 코드
	안전한 DNS(재귀적 혹은 캐싱 변환)
	안전한 DNS(신뢰된 소스)
	DNS 구조
	세션의 보호
	씬 노드(Thin Nodes)
	휴면 정보의 기밀성
	이질성 및 다양성
	필수디지털자산 장애

3.3.1. 전송 무결성/기밀성 방안

필수디지털자산에서 전송된 정보가 수신측에서 전송도중 변경이 없음에 대한 무결성을 보장하고, 정보의 불법적인 열람을 예방하기 위해 암호화 설정을 통해 기밀성을 보장해야한다. 하지만 제어시스템 환경에서 암호화를 사용하려면 메시지 암호화, 복호화 및 인증을 하는데 추가적인 컴퓨터 자원이 필요하기 때문에 통신 지연이 발생 할 수 있다. 이는 제어시스템 환경의 가용성을 침해할 수 있음으로 컴퓨터 자원의 최소화 및 안전성을 고려해 OSI 2계층의 암호화를 구현할 수 있다.

암호화 기술은 국가·공공기관에서 사용되는 정보보호제품에 중요 자료를 저장·소통하기 위한 암호 기능이 포함될 경우는 반드시 검증필 암호모듈을 탑재해야 한다. 검증대상 암호알고리즘은 블록암호, 해시함수, 메시지인증코드, 난수발생기, 공개키 암호, 전자서명, 키 설정 방식 등으로 분류되며, 112비트 이상의 보안강도를 만족하는 알고리즘으로 구성된다.[11]

3.3.2. 세션의 보호 방안

제어시스템에 접근하는 계정에 따라 동시 세션 수와 세션에 대한 기밀성 및 무결성을 보장해야 한다. 따라서 동일 계정에 의해 동시 세션을 처리하지 못하도록 제한하고 여러 계정에 의한 동시 세션의 최대 수를 정의해 제어시스템을 설정해야 한다. 제어시스템에 연결된 세션의 기밀성 및 무결성을 보장받기 위해 아래와 같은 기술을 사용 할 수 있다.

- ⊙ IPSec(Internet Protocol Security) : IP 계층에서 통신을 보호하는 기술로 다양한 운영체제에서 지원하고 있으며 패킷의 데이터 영역을 암호화 하는 전송(Transport) 모드와 패킷의 모든 영역을 암호화하는 터널(Tunnel) 모드를 지원한다.
- ⊙ SSL(Secure Sockets Layer) : HTTP, FTP, SMTP 등과 같은 응용프로그램을 보호하기 위한 기술로 상호인증, 데이터 암호화 및 무결성 기능을 지원하고 다양한 응용프로그램에 적용 할 수 있다.
- ⊙ SSH(Secure Shell) : 원격 터미널 통신에 대한 인터페이스로 원격에서 디지털 시스템을 안전하게 제어하기 위해 사용된다. 일반적으로 텔넷 프로그램에

대한 안전한 대안으로 사용된다.

3.4. 식별 및 인증 기술적 보안조치

주요 네트워크 사용자, 호스트, 응용프로그램, 서비스 및 자원을 식별하고 인증하기 위해 [표 11]와 같이 9개 세부항목에 대한 기술적 보안조치를 요구하고 있다.

〔표 11〕 식별 및 인증 기술적 보안조치

통제항목	세부항목
3. 식별 및 인증	사용자 식별 및 인증
	패스워드 요건
	인증 불가한 HMI 보안
	기기 식별 및 인증
	식별자 관리
	인증자 관리
	인증자 피드백
	암호화 모듈 인증에 따랄 암호화 수행

3.4.1. 식별 및 인증 방안

식별과 인증을 통해 필수디지털자산에 사용자가 자원에 접근하는 것을 승인하거나 비승인 한다. 아래와 같은 인증 기술을 통해 필수디지털자산에 접근하는 사용자에 대한 식별 및 인증이 가능하다.

⊙ 암호 인증 : 일반적으로 인증을 위해 사용되는 기술로 PIN번호 및 암호를 통해 접근을 요청한다. 암호 인증은 유추하기 쉬운 암호 사용 또는 키로거 등을 통해 쉽게 노출될 수 있기 때문에 엄격한 패스워드 관리가 필요하다.

⊙ 시도/응답 인증 : 응용 프로그램 기반의 인증 기술로 서버에서 사용자에게 비밀번호 요구를 시도하고 사용자로부터 응답을 받아 비밀번호가 정확하면 인증을 수행한다.

⊙ 물리토큰 인증 : 물리적 토큰 인증 기술은 암호 인증과 유사하지만 접근을 요청한 사용자가 가지고 있는 장치 및 토큰으로부터 생성된 비밀 코드 또는 키를 통해 인증을 수행한다.

⊙ 생체 인증 : 생체 인증은 접근을 요청하는 사용자의 고유한 생체적 특징을 확인함으로서 인증을 수행 하며 물리적 접근제어를 위해 주로 사용된다.

3.4.2 패스워드 관리 방안

패스워드의 길이, 강도 및 복잡성은 보안과 운영 용이성 사이에서 균형을 맞춰야 한다. 제어시스템 운영 중 긴급상황 발생 시 운영자가 암호를 기억하지 못하거나 입력하지 못한다면 긴급 대응이 지연될 수 있다. 따라서 패스워드의 보안정책에 부합하는 길이 및 복잡성을 갖추어야한다.

방송통신위원회의 “개인정보의 기술적 관리적 보호조치 기준” 고시에 따르면 패스워드는 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하고 연속적인 숫자나 개인정보 및 아이디와 비슷하거나 유추하기 쉬운 패스워드를 사용하지 않아야 하면 패스워드 유효기간을 설정하여 반기별 1회 이상 변경하는 것을 권고 하고 있다.[12]

3.5. 시스템 보안강화 기술적 보안조치

필수디지털자산에 불법 접근 및 불법 사용으로부터 보호하기 위해 시스템 보안강화 정책을 이행하고 유지하기 위해 [표 12]와 같이 5개 세부항목에 대한 기술적 보안조치를 요구한다.

〔표 12〕 시스템 보안강화 기술적 보안조치

통제항목	세부항목
4. 시스템 보안강화	불필요 서비스 및 프로그램의 제거
	호스트기반 침입탐지시스템
	파일시스템 및 운영체제 변경 승인
	하드웨어 구성
	운영체제, 응용프로그램 및 제3자 소프트웨어 설치 및 업데이트

3.5.1. 패치 및 취약점 관리 방안

원자력시설을 구성하고 있는 제어시스템에 패치를 적용시 의도하지 않은 결과로 제어시스템의 기능을 방해 할 수 있기 때문에 시스템 관리자는 패치 적용에 큰 어려움이 있다. 이에 따라 시스템 관리자는 동일한 모델

및 제어시스템 유형이 포함된 테스트 환경에서 패치가 의도하지 않은 결과를 초래하지 여부를 판단하기 위해 오프라인 상태에서 모든 패치를 테스트해야 한다. 또한 패치 적용 시 제어시스템의 계획된 중단 중에만 수행되어 져야 하고 응용 프로그램 업데이트가 적용되기 전 프로그램 공급 업체와 사용자에게 철저하게 검사되어야 한다.

따라서 관리자는 제어시스템에 대한 체계적인 패치 및 취약성 관리 접근법을 개발하고 제어시스템의 가용성을 보장하면서 시스템 취약점에 대한 노출을 줄이도록 해야 한다.

3.5.2 호스트기반 침입탐지시스템

호스트기반 침입탐지시스템은 통신 트래픽은 물론 시스템 로그, 파일 접근과 같은 시스템 이벤트를 모니터링 한다. 이를 통해 불법 침입자가 시스템에 접근하거나 접근을 시도하는 것을 [표 13]와 같은 탐지기술을 이용하여 탐지한다. 제어시스템의 정상 작동 범위 밖의 모든 트래픽에 대한 경보를 모니터링 하고 생성 할 수 있으며 출발지 및 목적지IP, 프로토콜, 제어데이터 등의 분석을 통해 간단한 탐지규칙을 작성 할 수 있다.

한 예로 OSSEC(Open Source Security)과 같은 오픈소스 기반의 호스트기반 침입탐지시스템은 응용프로그램 레벨의 로그 분석, 파일 무결성 검사, 감사정책 모니터링, 루트킷 탐지, 실시간 경보 등을 지원한다.[13]

〔표 13〕 침입탐지시스템 탐지기술

구분	내용
시그니처기반 탐지	• 알려진 패턴에 대해서만 검사 • 자신의 호스트 영역에서만 탐지 • 동일 트래픽의 양방향 검사가 가능 • 사후 대응 및 트래픽 차단 지원(IPS모드) • 트래픽을 구별하지 않음
행위기반 탐지	• 정상적인 트래픽에 대한 학습기간 필요 • 정상적인 트래픽 이외의 편차를 감시한다. • 공격 시그니처에 대한 설정이 필요없음 • 비정상행위를 탐지 하나 오탐 증가 • 동적 환경에서 구현하기 어려움

Ⅳ. 결 론

본 논문에서는 KINAC/RS-015 기술기준의 보안 조치 활동으로 기술적 보안조치의 5개 통제항목과 62개 세부항목을 소개하고 이를 원자력시설에 적용하기 위한 고려사항 및 이행방안을 살펴보았다.

원자력시설에 기술적 보안조치를 적용하기 위해서는 보안성 적용으로 인해 안전성 및 신뢰성을 최우선시 하는 설계 요건에 영향을 미칠 수 있는 여러 요인을 정확히 이해하고 분석이 이루어져야한다. 또한 실제 적용 시 철저하게 검증되고 테스트된 범위 내에서 기술적 보안조치를 적용한다면 원자력시설의 설계, 제작, 설치, 운전, 유지보수 및 폐기 단계까지의 전주기에 걸쳐 안전성 및 보안성을 확보할 수 있을 것으로 사료된다.

아울러 본 연구를 통해 원자력시설에 기술적 보안조치를 적용하고 이행하는데 활용 될 수 있을 것으로 기대한다. 다만, 앞서 분석한 사항들은 연구를 통한 고려사항에 대한 내용이므로, 이러한 사항이외의 여러 고려사항들에 대해서도 대처 및 조치를 취해야 함을 당부한다.

참 고 문 헌

[1] Candid Wueest, "Targeted Attacks Against the Energy Sector Ver 1.0", Symantec, Jan. 2014.

[2] NRC, "Cyber Security Programs For Nuclear Facilities", Regulatory Guide 5.71, 2009

[3] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations" SP 800-53 Rev.4, Apr. 2013.

[4] NIST, "Guide to Industrial Control Systems(ICS) Security" SP 800-82 Rev2, Aug. 2015.

[5] 한국원자력통제기술원, “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”, KINAC/RS-015, 2016.

[6] ICS-CERT, Cyber Threat Source Descriptions, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

[7] BSI, "Industrial Control System Security Top10 Threats and Countermeasures 2016", Jan. 2016.

[8] DHS, "Common Cybersecurity Vulnerabilities in Industrial Control Systems", May. 2011.

[9] KasperskyLab, "Industrial Control Systems Vulnerabilities Statistics", Jul. 2016.

[10] DHS, "Recommended Practice: Improving

Industrial Control System Cybersecurity with Defense-in-Depth Strategies", Sep. 2016.
[11] NCSC, “정보보호제품 평가인증 수행규정“, Nov. 2015.
[12] 방송통신위원회, “개인정보보호 기술적·관리적 보호조치 기준 및 해설서“, Sep. 2012.
[13] Kieran McLaughlin, Sakir Sezer, “Cyber attack Detection and Response for Industrial Control Systems, ICS-CSR, Sep. 2014.

〈저 자 소 개〉

김 나 영 (KIM NA YOUNG)
2006년 8월 : 국가평생교육진흥원, 컴퓨터공학과 졸업
2010년 2월 : 충남대학교 정보통신공학과 석사 졸업
2016년 8월~현재 : 한국원자력통제기술원 사이버보안실 전문연구원
관심분야 : 제어시스템 보안, 네트워크 보안, 침해사고 분석

임 현 종 (LIM HYUN JONG)
정회원
2014년 8월 : 고려대학교 방사선학과 졸업
2016년 8월 : 고려대학교 바이오융합공학과 석사
2016년 7월~현재 한국원자력통제기술원 사이버보안실 전문연구원
관심분야 : 제어시스템 보안, 네트워크 보안, 기반시설 보안

김 상 우 (KIM SANG WOO)
2013년 2월 : 충남대학교 컴퓨터공학과 졸업
2015년 2월 : 충남대학교 컴퓨터공학과 석사 졸업
2015년 2월~현재 : 한국원자력통제기술원 사이버보안실 연구원
관심분야 : 사이버보안, 제어시스템 보안, 네트워크 인증

송 동 훈 (SONG DONG HOON)
2012년 2월 : 부산대학교 전자전기공학부 졸업
2012년 1월~2015년 8월 : 한국전력기술 기술원
2015년 8월~현재 : 한국원자력통제기술원 사이버보안실 연구원
관심분야 : 사이버보안, 전기공학, 전자공학

신 익 현 (SHIN ICK HYUN)
2004년 8월 : 뉴욕 시립대학교 컴퓨터 사이언스학과 졸업
2014년 8월 : KAIST 정보보호대학원 석사 졸업
2005년 8월~현재 : 한국원자력통제기술원 사이버보안실 선임연구원
관심분야 : 제어시스템 보안, 기반보호 정책, 사이버보안 전략