원자력 사이버보안
현안과 정책 제언

2015. 8. 21

한국원자력학회
Korean Nuclear Society

제 출 문

한국원자력학회장 귀하

본 보고서를 **한국원자력학회 원자력이슈위원회**가 수행한 “원자력 사이버보안 현안과 정책 제언” 보고서로 제출합니다.

2015. 8. 21

보고서 발간위원회

위원장: 황주호 (경희대학교)
위원: 황용수 (한국원자력통제기술원)
위원: 이동영 (한국원자력연구원)

보고서 발간회원

회원: 이나영 (한국원자력통제기술원)
회원: 이철권 (한국원자력연구원)

보고서 감수위원

위원: 강현국 (한국과학기술원)
위원: 정재준 (부산대학교)

목 차

표 목차

그림 목차

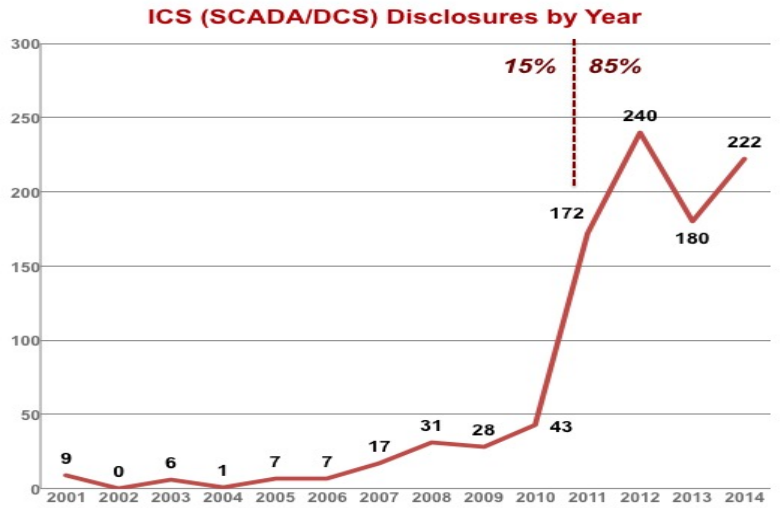
제 1 장 원자력 사이버보안 개요

2014년 12월 9일 '원전반대그룹'을 자처하는 해킹단체에 의한 한수원 정보유출 사건은 국내 전 매스컴의 톱 뉴스를 장식하면서 원전을 포함한 국가 원자력시설에 대한 국민적 불안을 야기한 바 있다. 나아가 원전반대그룹은 지속적으로 원전 관련 정보를 공개하는 방식으로 원전에 대한 신뢰를 실추하기 위한 활동을 진행하고 있다는 점에서 원전뿐만 아니라 관련정보에 대한 보안을 포함한 종합적 대책 마련이 필요하게 되었다.

사이버보안은 사회 각 분야에서 이미 큰 이슈가 되었다. 특히 금융 및 정보산업 등 IT기술 분야에서는 수차례 사이버공격으로 컴퓨터시스템이 해킹당하거나 기능마비를 일으켜 경제적 손실을 초래한 바 있고, 이의 피해자가 다수의 불특정 국민이 됨에 따라 사이버보안은 국가의 중요한 현안으로 부상하였다. 이러한 사이버위협은 전 세계의 국가 주요기반시설에서도 발생하고 있다. [그림 1]은 2001년부터 과거 10년간의 일반 산업제어시스템(ICS, industrial control system)에 대한 사이버 취약점의 증가추이를 나타내고 있으며, 미국국토안보부(Department of Homeland Security)가 운영하는 사이버 비상대응팀(ICS-CERT) 통계자료[표 1]에 따르면 2010년 18건에서 최근에는 연간 150건이 넘어서고 있다.

원자력분야에서도 과거 2001년의 9/11 테러직후 위협의 수준이 달라짐에 따라 원전 시설에서의 각종 위협에 대한 대응방안을 논의하면서 사이버테러에 대한 논의가 있었다. 그러나 당시 기존의 인터넷망과 달리, 원자력 제어망은 일반망과 분리되어 있으므로 사이버침투가 불가능할 것이라 결론짓고 사이버보안 문제에 대해서는 심각하게 고려하지 않았다.

원자력시설에서도 사이버보안 문제가 발생할 수 있음을 확인시킨 사건은 2010년 이란 핵시설에서 발생한 '스턱스넷(Stuxnet)' 사건이다. 당시 일반 컴퓨터가 아닌 제어시스템, 더구나 망이 분리되어 있는 원자력 제어시스템에 USB를 통해 직접적 위해를 가할 수 있다는 사실에 원전 사이버보안에 대한 논의가 다시 수면으로 떠올랐다. 특히 공격대상을 결정하고 이에 대한 테러를 위해 조직적, 체계적으로 제어망 공격용 프로그램을 개발하였다는 사실은 원전 사이버테러가 현실적으로 발생할 수 있음을 인지하는 계기가 되었다.



[그림 1] 제어시스템 사이버 취약점 증가 그래프

출처: "https://www.scadahacker.com"(2015.6.25.)

[표 1] ICS-CERT 통계

ICS-CERT	2010	2011	2012	2013	2014
ICS Related Vulnerabilities	18	139	137	187	159

출처: "ICS-CERT Annual Report 2010~2014"(ICS-CERT)

사이버공격은 언제 어떻게 공격할 지를 예측하기 어렵고 항상 사고가 발생한 후에야 탐지되는 특징이 있다. 국내 원전에 대한 정보유출시도 사건이 그 좋은 사례이다. 이는 사이버테러나 9/11 테러 같은 사건이 우리나라에서는 발생하지 않을 것이란 우리의 인식을 순식간에 바꾸어 우리나라도 사이버테러로부터 자유롭지 못함을 각인시키게 된 대표적인 사례(참고자료 1)가 되었다. 이 사건은 비록 실질적으로 원전 제어망에 침투하지 못한 것으로 확인되었으나 국민적 공포를 조장하는 등 파급효과가 컸다. 이와 같이 예기치 못한 방법으로 공포를 극대화할 수 있다는 사이버보안의 특수성을 감안하여 국내 원자력계도 보다 적극적으로 대응하여야 한다.

본 보고서에서는 원자력시설 사이버공격을 예방하고 이에 대응하기 위한 국내 원자력 사이버보안 체제의 현황을 검토하고 개선방안을 제시하고자 한다.

제 2 장 원자력시설 사이버보안의 특징

기존에 아날로그기술 기반으로 구성되었던 원전 계측제어시스템은 2000년대로 접어들면서 디지털기술이 도입됨에 따라 급격히 디지털화 되었고, 현재 국내 대부분의 원전은 디지털기술 기반으로 운용되고 있다. 이에 따라 원자력 사이버보안은 국가의 안정적인 전력공급은 물론 공공의 안전을 보장하기 위한 주요 현안으로 다루어져야 한다.

일반적인 사이버공격이 인터넷망의 마비 또는 정보 탈취의 형태로 이루어지는 것과는 달리, 공업시설에 대한 사이버공격은 그 시설의 오작동을 초래할 수 있다는 특징이 있다. 원자력시설은 방사성물질을 다루고 있다는 점에서 사이버공격이 이루어져 안전관련 핵심시설의 오작동이 초래된다면 큰 문제가 야기될 수 있다. 나아가 사이버공격과 물리적공격이 합쳐진 복합사건이 발생하는 경우에는 더 심각한 사고가 초래될 수 있다 (참고자료 2).

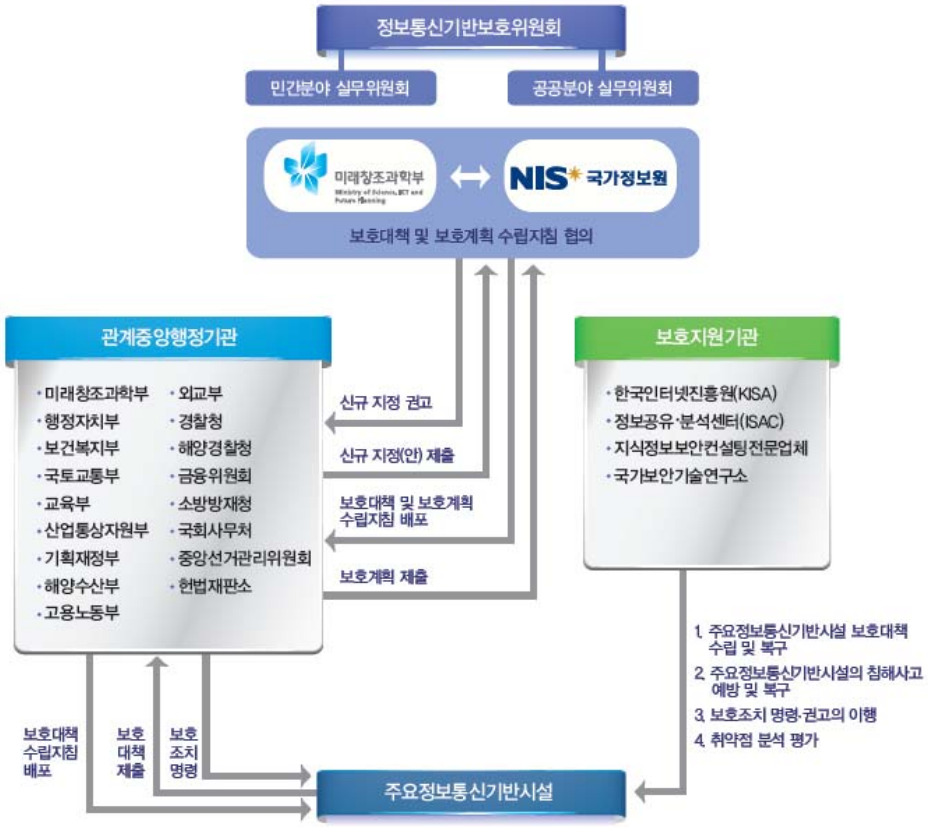
원자력시설 사이버보안은 디지털 기기나 설비를 대상으로 하며, 디지털기술을 적용하는 계측제어시스템, 서버를 사용하는 보안시스템 및 비상방재시스템, 원자력시설 주기기에 사용되는 내장형 디지털장치, 시험 및 분석용 장비 등이 포함된다. 이들은 외형적으로 일반 산업제어시스템과 크게 다르지 않으나, 안전이 중요시되는 원자력 고유한 특성으로 인해 사이버보안 기술 적용시 특히 고려되어야 하는 부분이 많이 있다 (참고자료 3).

통상 원전은 폐쇄망으로 운영되며 인터넷에 연결되지 않는다. 또한 365일 24시간 운영을 원칙으로 하며, 시스템에 적합한 전용의 통신 프로토콜을 사용하고 목적에 맞도록 설계 및 제작된 내장형 운영체제가 사용된다. 이 때문에 범용의 보안솔루션을 설치하기 어렵고 운영체제의 보안패치를 온라인으로 업데이트하는 것이 불가능하다. 백신이나 보안패치를 USB 등 별도의 매체를 사용하여 적용하더라도 운영체제의 업데이트와 보안설정의 활성화를 위한 시스템의 재부팅이 곤란한 경우가 대부분인데, 이는 재부팅이 플랜트 운전 중단을 초래하지 않아야 하기 때문이다. 따라서 원전의 운전 중에는 운영체제의 업데이트와 보안설정들의 설치가 곤란하다.

결론적으로 현재 원자력 시스템이 감염될 경우 시스템 내부 확산 및 전파를 막기 어려우며, 일반적인 IT나 기존 일반 산업제어시스템에 맞게 개발된 대응수단은 원전에 사용할 수 없으므로 원자력 전용의 보안 체계와 보안솔루션이 시급히 개발되어야 한다.

제 3 장 국내 원자력 사이버보안 대응체계 현황

우리나라는 2001년 정보통신기반보호법을 제정하여 전자적 침해행위에 대비하고 주요정보통신기반시설을 보호하기 위한 대책을 수립·시행하였다. 이 법은 주요정보통신기반시설의 안정적인 운용을 통해 국가 및 국민생활의 안정을 가져오는 것을 그 목적으로 한다. 원자력시설은 2011년 2월 주요정보통신기반시설로 지정되었고 [그림 2]와 같은 주요정보통신기반시설 보호체계를 통해 사이버침해 사건에 대응할 수 있는 체계가 마련되었다.



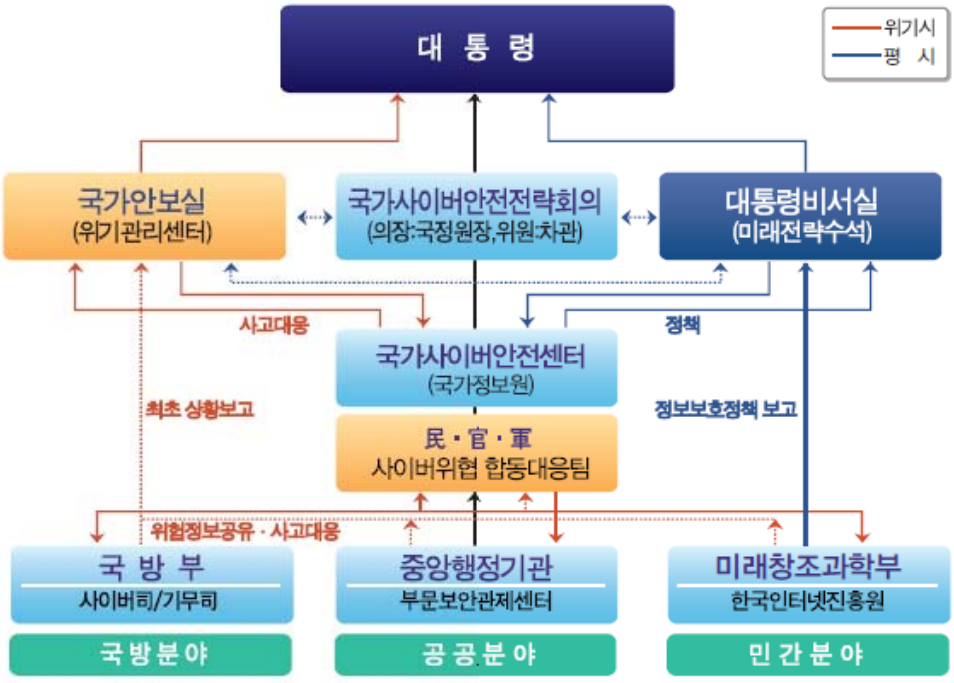
[그림 2] 주요정보통신기반시설 보호체계

출처: 2015 국가정보보호 백서

한편 국내 원자력시설의 방호 및 방재를 포괄하는 방호방재법에서는 2013년 12월 개정을 통해 원자력시설에 발생한 사이버침해 사건은 국정원장에게 보고하도록 되어 있다. 이 법에 의하면 원자력시설에서의 사이버침해 사건 발생시에 원자력시설 운영자는 사이버보안 사건대응팀 (CSIRT, cyber

security incident response team)을 통해 시설의 안전을 유지하며 규제기관(KINAC) 및 국가사이버안전센터에 보고한다. 사건발생을 보고받은 국가사이버비상대응팀(CERT, cyber emergency response or readiness team)은 사이버침해에 대한 위협정보 분석, 사건대응 및 복구 지원, 원인규명(Forensic), 관련기관 간 정보공유 등의 조치를 취한다. 심각한 수준의 사이버침해 사건이 발생한 경우 국가 차원의 사이버 위기 관리체계는 [그림 3]과 같다.

위에서 살펴본 바와 같이 원자력 사이버보안을 성공적으로 수행하기 위해서는 정부부처간 유기적인 협력을 통해 체계적이고 즉각적인 대응이 중요하다. 특히 이러한 대응체계는 침입예방 및 탐지를 전제로 하고 있다는 점에서 원자력 시스템 설계과정에서부터 이를 체계적으로 반영하고 모든 종사자가 평소에 보안의식을 고양하고 주어진 임무수행에 필요한 수준의 교육훈련 프로그램을 이수해야 한다. 참고로 최근까지 국내 원자력 산업계에서는 사이버보안에 관한 규제요건이 없어서 원자력시설에 대한 사이버보안 기술의 적용이 요구되지 않았다.



[그림 3] 국가 사이버위기 관리체계

출처: 2015 국가정보보호 백서

제 4 장 원자력 사이버보안 체제 개선방안

원자력시설 사이버보안에 대해 여러 정부 부처와 원자력산업계가 공동으로 노력함으로써 사이버침해 가능성을 줄이고 사이버사건 발생 시에도 피해를 최소화할 수 있다.

사이버침해를 예방하기 위해서는 먼저 관련 시스템과 위험을 관리하는 법제체제를 정비하고 부처별 업무범위 및 사이버보안 대상기기를 합리적으로 정리하여야 한다. 특히 원자력시설의 전 수명주기 동안 사이버보안 체제가 구축되고 검증이 이루어질 수 있도록 규제업무의 책임이 명확히 정의되어야 하며, 이러한 규제를 수행하는 정부 부처간의 협력 내용도 구체적으로 정의되어야 한다. 이러한 노력에도 불구하고 사이버보안 침해사건이 발생했을 때를 대비하여 범부처적 사건대응 체계가 구축되어야 한다. 이를 통해 원자력시설의 사이버침해를 신속하게 탐지하여 효과적으로 차단하고 완화, 복구 및 보완하는 일련의 과정을 체계적으로 관리할 수 있다.

1) 법제체제 정비

현재 원자력시설에 대한 사이버보안 규제체제는 크게 '정보통신기반보호법', '원자력안전법', '방호방재법'에 의거하여 수행되고 있다. 2011년 2월 '정보통신기반보호법'에 원자력시설을 포함시킴으로써 여러 정부부처로부터 사이버보안 점검이 수행되고 있으며 ([표2]), 2013년 12월 개정된 '방호방재법'이 발표됨으로써 원자력안전위원회가 원자력시설에 대한 사이버보안 규제를 담당하게 되었다. 한편 '정보통신기반보호법'과 '방호방재법' 간에 원자력시설의 규제범위가 매끄럽게 연계되어 있지 않아, 불필요한 중복규제 또는 위험에 대한 규제공백이 발생하지 않도록 제도를 종합적으로 점검할 필요가 있다. 원자력 안전에 관한 규제는 '원자력안전법'에 의거 원자력안전위원회의 전적인 책임하에 규제가 이루어지고 있으므로 규제 체계의 혼란이 없음을 참고할 필요가 있다.

2) 원자력시설의 사이버보안 대상

사이버보안 대상설비가 처음 안전등급 계통으로부터 지속적으로 확대되어 비안전등급인 제어 및 감시 계통은 물론 물리적방호 및 비상방재시스템과 기타 지원시스템, 나아가 주요 설계정보 및 저장장치에 이르기까지 확대되는 것이 현재의 추세이다 ([그림 4]). 그러나 '방호방재법'에 규정된 대상설비는 안전

관련시스템(Safety System), 보안시스템(Security System), 비상방재시스템(Emergency Preparedness System) 및 지원시스템(Support system)으로 규정되어 있어 원자력시설 내에서 이들의 적용범위가 분명치 않다. 또한 지난 한수원 정보유출사건에서 드러난 바와 같이 설계 및 운전정보 보안의 중요성도 높다. 따라서 원자력시설의 사이버보안, 특히 직접적 시설침투가 아닌 정보유출을 포함하도록 책임소재를 규명하고 이를 명확하게 관리할 수 있도록 원자력시설 전체로 규제대상을 확대할 필요가 있다.

[표 2] 정부부처별 사이버보안 점검 근거

구 분	법 적 근 거
국정원	정보통신기반보호법 및 국가 정보보안 기본지침
산업부	공공기관의 운영에 관한 법 제51조 (공기업·준정부 기관에 대한 감독)
감사원	감사원법 제24조 (감찰사항) 및 공공기관의 운영에 관한 법 제52조 (감사원 감사)
행자부 (국민안전처)	재난 및 안전관리 기본법 및 국가위기관리지침 (대통령 훈령)
원안위	방호방재법 및 원자력안전법 시행령, 규칙 및 고시

[그림 4] 원전 사이버보안 규제대상 확대

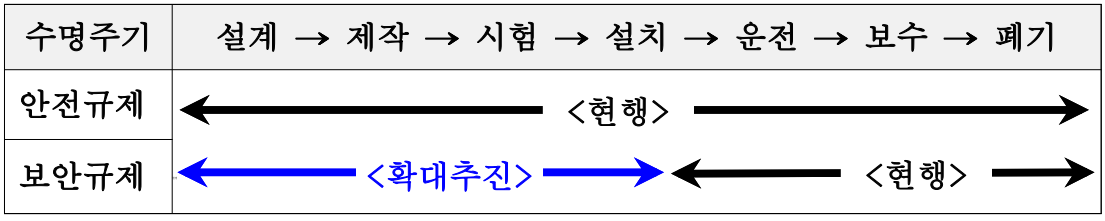
3) 원자력시설 전 수명주기를 고려한 사이버보안기술 적용

'원자력안전법'에 따라 적용되는 사이버보안은 대상시스템에 대하여 전

수명주기 동안 안전성을 보장할 수 있어야 한다. 원자력시설의 전 수명주기 동안의 안전성을 다루는 안전성 분야와는 달리 '방호방재법' 상에서는 핵연료장전 5개월 전부터 규제의 대상이 되므로 실질적으로 신규 원자력시설의 건설단계(설계, 제작, 시험 및 설치 등)에 대한 규제가 이루어지지 않는다([표 3] 참고). 뿐만 아니라 가동중 원자력시설에서 사이버보안 기술을 적용하는 경우에도 기존에 확보된 설비의 안전성을 훼손하지 않음을 보장한다는 전제하에서만 이행이 가능하므로 설비개선이 용이치 않다. 따라서 [그림 5]와 같이 설계단계에서부터 사업자가 사이버보안 대응체제 구축을 고려하고 이를 규제기관에서 설계요건으로 심사할 수 있도록 관련 인허가 심사 법규 및 법령의 개정이 필요하다. 또한 사이버보안 관련설비 및 대응체계가 건설 초기 단계부터 체계적으로 반영될 수 있도록 안전성분석보고서(SAR, safety analysis report)에 사이버보안 관련 내용을 추가하고 필요한 세부 심·검사 요건을 개발해야 한다. 유사하게 가동원전도 사이버보안성 평가, 보안조치의 식별 및 적용이 필요하며, 보안조치 적용시 운영/관리적인 측면 외에도 기술적 보안조치를 최대한 적용할 수 있도록 해야 한다.

[표 3] 원자력시설의 전 수명주기에 대한 규제범위

대상 / 수명단계	Safety(I&C)+supp. sys.		Security+ Supp. Sys.	Empergency Preparedness+ Supp. Sys.
	안전계통	비안전계통		
설계	○	×	×	×
제작	○	×	×	×
시험	○	×	×	×
설치	○	×	×	×
운전	○	○	○	○
보수	○	○	○	○
폐기	○	○	○	○



[그림 5] 원자력시설의 전 수명주기에 대한 규제방안

4) 사이버테러 대응체계

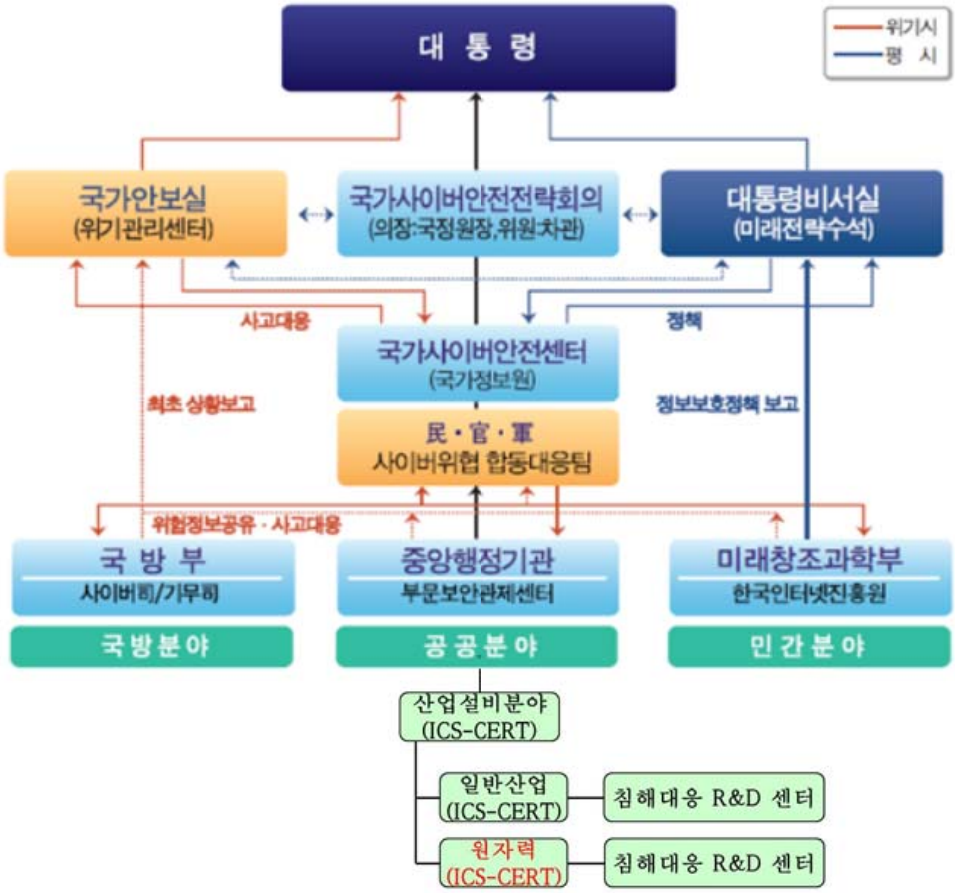
사이버테러 발생시 국가 차원에서 정보통신기반보호법에 근거한 국가 사이버위기 체계에서 국가주요기반시설에 대한 사이버보안은 국정원에서 책임지고 있으므로, 원자력시설의 특수성 및 사고시 파급효과를 고려하여 일반 산업제어시스템 및 원자력설비에 대한 사이버위기 관리체계를 별도로 수립할 필요가 있다. 또한 정보통신기반보호법 관리하에 있는 일반산업과 방호방재법 관리하의 원자력시설에 대한 관리체계를 구분함으로써 효과적인 대응이 가능할 것으로 판단한다 ([그림 6]).

5) 사이버테러 예방 및 대응 기술 개발

사이버보안 체제를 강화하기 위해서는 지속적으로 진화해가는 사이버위협에 대응할 수 있도록 국가 R&D 로드맵에 따른 기술개발이 요구된다. 특히 핵안보 속성상 관련 정보는 대외비로 간주되므로 관련기술의 협력이나 선진기술의 도입에 한계가 있다. 만약 원전 사이버보안 기술을 외국에 의존한다면 국내 상세설계 내용의 유출이 불가피하여 보안유지에 허점이 발생할 가능성이 농후하다. 따라서 일반산업계와 다른 특성을 가진 원자력 특성을 고려한 원자력시설 사이버보안 체제 수립을 위해서는 시험설비를 포함한 관련 기반기술 확보가 선결되어야 한다. 뿐만 아니라 사이버보안 사건 탐지기술의 개발 및 적용을 지속적으로 추진해야 하며, 궁극적으로는 통합 사이버보안 감시 및 관리계통의 개발이 필요하다.

6) 인식제고 및 교육훈련

2014년 12월 9일 원전반대그룹에 의한 한수원 정보유출 사건은 사이버테러가 원자력시설 뿐만 아니라 개인영역의 정보관리 미흡에도 국민 불안을 조성할 수 있음을 확인시킨 바 있다. 따라서 사이버보안이 국민 안심에 심대한 영향을 끼칠 수 있고 물리적 접근이 없이도 원자력시설에 심각한 타격을 미칠 수 있는 중대한 사안이라는 점을 원자력시설 운영자, 관련 규제기관 및 정부 유관부처가 모두 인식해야 하고, 관계시설의 사이버보안팀 뿐만 아니라 원자력시설의 계통 또는 장비 담당자가 사이버보안 첨병으로서 역할을 수행해야 한다. 이러한 의미에서 원자력 관련자 모두에 대해 사이버보안 인식이 확산되어야 하며, 사이버보안 담당업무의 전문성 정도에 따른 수준별 교육 및 훈련이 지속적으로 이루어지도록 프로그램이 개발/운영되어야 한다.



[그림 6] 개정 국가 사이버위기 관리체계(안*)

* 미국 DHS의 NCCIC(national cybersecurity and communications integration center) 산하의 US-CERT(정보보안 담당)와 ICS-CERT(산업제어보안 담당) 체계 참조

제 5 장 결 론

향후 원자력을 포함한 국가 주요시설에서의 디지털기술 사용정도는 더욱 심화되고 무선기술이나 이동기기의 사용이 확산될 것이며, 더불어 이런 시설을 타깃으로 하는 해킹기술도 빠른 속도로 발전할 것이 예상된다. 이제 원자력시설을 보호하기 위해서는 사이버보안은 선택이 아닌 필수로서 기반기술로의 자리매김이 필요한 시점이 되었다. 사이버침해의 예방이 중요한 것은 물론이고, 혹시 발생할지 모를 실제 침해에 차질없는 대응을 위해 원자력 특수성이 반영된 사이버대응체계 및 관리가 필요하다. 공공의 안전과 국가 안보 차원에서 정부 관계 부처는 원자력시설 사이버보안에 대해 산학연과 더불어 종합적인 계획을 마련하고 적극적으로 투자를 할 필요가 있다.

특히 테러의 심리적/물리적 파급효과가 크다는 점에서 원자력이 타깃이 될 가능성이 있으므로 이에 대한 국가적 대응체제 구축이 필요하다. 이를 위해 지금까지 국내에서 다양한 법제체제가 마련되었고 여러 정부부처로부터 사이버보안 검사 등이 수행되었으나, 보다 효율적이고 체계적인 대응이 필요한 시점이다.

이러한 배경하에서 한국원자력학회는 국가적 관심사안인 원자력시설에 대한 사이버보안 체계를 확립하기 위해 원자력 사업자, 연구자, 규제전문가, 정책전문가 의견을 종합 수렴하여 원자력 사이버보안 체제 구축을 위한 개선방안을 아래와 같이 제안하는 바이며, 이를 통해 원자력의 안전과 안보가 확보된 사이버보안 체제 구축에 기여하고자 한다.

1. 규제 체제의 정비: 중복규제나 규제공백이 발생하지 않도록 체제를 정비하고 관련 정부 부처간 유기적인 업무할당이 필요하다. 또한 설계단계에서부터 운영까지 사업자가 사이버보안 대응체제 구축을 고려하여 이행하고 이를 규제기관에서 심사할 수 있도록, 관련 인허가 심사 법규 및 법령이 상세히 제정되어야 한다.
2. 대상 범위의 확대: 안전관련시스템, 보안시스템, 비상방재시스템 및 지원시스템은 물론 설계 및 운전정보를 포함하는 원자력시설 전체로 대상 확대를 통한 보안성강화가 필요하며, 이의 효과적 구현을 위해서는 전 수명주기에 걸친 관리가 요구된다.
3. 사이버 비상대응팀 구축: 국가 원자력시설 사이버테러에 대한 컨트롤타워

로서 역할을 담당하는 비상대응팀(CERT)을 조직하여 사이버침해에 신속, 정확하게 대응하여야 한다.

4. 연구 개발의 강화: 원자력의 특성을 고려한 관련 기술을 로드맵을 가지고 체계적으로 개발하며, 시험시설(Testbed) 등 관련 기반 확충에 노력하여야 한다.
5. 교육훈련 및 인식제고: 많은 사이버보안 이슈가 인적 요인에 의해 발생하므로, 원자력 관련자에 대상으로 한 체계적 교육 및 훈련을 통해 인식 제고 및 사이버보안 문화 정착을 도모하여야 한다.

핵안보 정상회의를 통해 핵안보에 대한 관심이 높아진 가운데, 원자력시설에서의 물리적공격에 대한 대응태세는 이미 상당한 수준으로 강화되었으나, 사이버위협에 대한 대비는 아직 부족한 것으로 드러났다. 우리나라는 국가차원에서 원자력시설 사이버보안의 중요성을 인지하고 2014년 헤이그 핵안보 정상회의에서 '원전시설에 대한 사이버테러 대응방안 강구'를 약속한 바 있으나 같은 해 12월 원전반대그룹의 '사이버테러'를 가장한 위협이 발생한 이후 지속적으로 협박을 받고 있다. 이번 사건을 계기로 규제 체제의 정비 및 관련 연구개발의 심화를 이루어, 향후 사이버위협으로부터 원자력 시설과 국민을 안전하게 보호하는데 충분한 기반을 확보하여야 할 것이다.

참고자료

참고자료 1 : 한수원 사이버위협 사건('14.12.9) 경과 및 대응

1. 사이버위협 사건 경과

□ **스팸메일 발송**

○ 월성원전에서 악성코드 포함된 스팸메일* 최초 인지('14.12.9)

* 악성코드가 포함된 한글파일을 첨부한 상용포털 이메일 다량 수신

□ **원전관련 자료 무단유포**

○ (제1차) 인터넷매체에서 한수원 직원 개인정보* 유출 보도('14.12.17)

* 해커추정자의 블로그에 한수원 직원 개인정보 등 자료 게시(12.15)

○ (제2차) 월성1호기 배관설치 도면 등 유포(블로그, '14.12.18)

○ (제3차) 개량연료 안전성평가 연습용 프로그램 등 유포(트위터, '14.12.19)

○ (제4차) 고리1,2호기 계통요약도 등 유포(트위터, '14.12.21)

○ (제5차) 원전안전해석코드 화면 사진 등 유포(트위터, '14.12.23)

□ **원전 가동중지 협박**

○ 자료 유포와 함께 유포범의 트위터에 협박성 글 게시('14.12.19, '14.12.21)

(참고) 자료 유포범 협박 내용

① 크리스마스부터 고리 1·3호기, 월성 2호기 가동중단 조치
② 미이행시 자료 전부 공개 및 2차 파괴 실행
③ 원하는 것은 원전 해체, 돈도 필요

2. 한수원 대응조치

□ **원전 운전 안전성 확보**

○ 원전 제어시스템의 안전성

○ 사이버 공격 대비 원전 안전운영 점검*

* (**방어계획 시행**) 전산 제어망 방어·복구계획 시행, (**모의훈련 실시**) 사이버 공격 대비 운전원 비상대응 모의훈련 실시

○ 전사적 비상 대응체계 및 물리적방호 조치 시행*

* (**비상 대응체계**) 본사 및 발전소 비상상황반 구성·운영, (**물리적 방호**) 사이버 공격과 병행한 원전 물리적 저해시도 차단

□ **자료 유포 관련 대응**

○ 주요 대응조치*

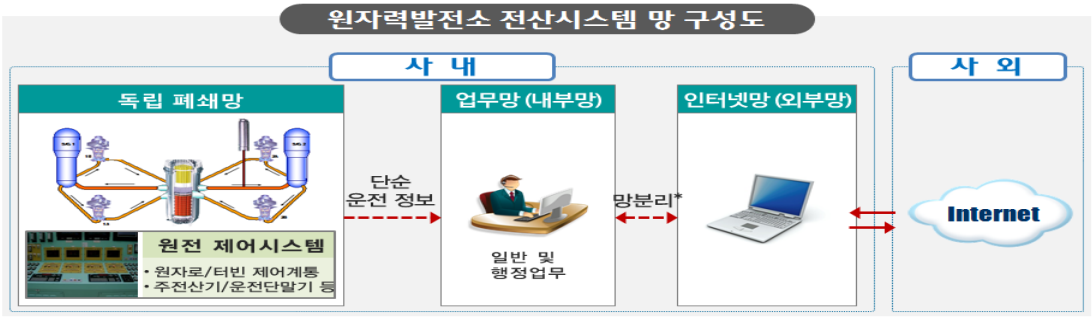
* (**악성코드 차단**) 악성코드 메일 최초감지(12.9) 후, 메일발신 포털계정 차단, 전 PC 정밀점검 등 긴급조치 시행, (**사이버보안 강화**) 사이버보안관제센터 비상근무 조치와 함께 국가 사이버안전센터와 공조하여 추가적 사이버 공격 감시/방어

※ 악성코드 분석결과, 컴퓨터 하드파괴 기능외의 자료반출 기능 없음

○ 유출자료 분석 결과*

* 5회에 걸쳐 유포된 자료는 문서, 도면, 사진, 프로그램 등 총 24건으로 원전 안전운전에 영향이 없는 일반 기술자료임

(참고) 원자력발전소 전산시스템



※ 원전 제어망은 운전 정보를 전송하는 단방향 통신만 가능하도록 되어있어 인터넷망으로부터 네트워크를 통한 접속은 불가능

참고자료 2 : 해외 원자력 사이버테러 사례

사이버보안 관련 사건의 발생 주기를 살펴보면 원자력발전소 계측제어시스템에 대한 사이버보안 위협이 지속적으로 증가하는 것을 알 수 있다. 2003년 9월 인터넷망을 통해 제어시스템에 침투한 슬래머 웜이 미국 Davis-Besse 원전을 감염시켰으며[그림 7], 2006년 8월 미국 Browns Ferry 원전에 새로 설치된 PLC[1]가 대량의 broadcast traffic을 발생시켜 냉각수 드라이버가 동작하지 않아 원자로 가동이 중단되었다. 원자력 시설과 관련된 사이버보안 사례를 [표 4]에 정리하였다.

[표 4] 원자력시설 관련 사이버보안 위협 사례

시설	일시	원인	피해 및 결과	비고
Davis-Besse원전 (미국)	'03.1	원전 사설 컴퓨터 네트워크에 슬래머웜 침투	안전감시시스템 5시간동안 정지	889MW
Brown Ferry원전 (미국)	'06.8	원전 네트워크에 과다한 컴퓨터 트래픽 발생	펌프제어기 미동작으로 원전 정지	1100MW
Hatch 원전 (미국)	'08.5	업무PC가 업데이트 후 재부팅되면서 연동된 제어시스템 데이터 리셋	안전시스템이 냉각수 부족으로 오인 48시간동안 원전 비상정지	924MW
EFH 전력사 (미국)	'09.3	전직 직원이 에너지수요 예측시스템 조작을 통해 원전을 공격하려다 발각	에너지수요예측시스템이 1일간 마비되어 26,000달러 피해 발생	-
Bushehr 원전 등 (이란)	'10.6	악성코드(Stuxnet)가 이동저장매체를 통해 원전 네트워크에 전파	원전제어시스템 및 원자력시설 원심분리기 파괴	1000MW
몬주 원전 (일본)	'14.1	제어실PC에서 작업자가 프로그램 업데이트 수행 중 악성코드 감염	감염PC를 통해 42,000개 이상의 관련 문서 도난	280MW

1) PLC: Programmable Logic Controller, 디지털 또는 아날로그 입출력에 대한 기능을 수행하기 위하여 프로그램 가능한 메모리를 사용하고 여러 종류의 기계나 프로세스를 제어하는 디지털 동작의 전자장치

NRC NEWS

U.S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs Telephone: 301/415-8200

Washington, DC 20555-001 E-mail: opa@nrc.gov

Web Site: http://www.nrc.gov/OPA

No. 03-108 September 2, 2003

NRC ISSUES INFORMATION NOTICE ON POTENTIAL OF NUCLEAR POWER PLANT NETWORK TO WORM INFECTION

The Nuclear Regulatory Commission staff has issued an Information Notice to alert nuclear power plant operators to a potential vulnerability of their computer network server to infection by the Microsoft SQL Server worm.

The vulnerability was demonstrated by a January event at the shutdown Davis-Besse nuclear power plant. The worm infection increased data traffic in the site's network, resulting in the plant's Safety Parameter Display System and plant process computer being unavailable for several hours. Neither of those systems, however, affects the safe operation of a nuclear plant. NRC regulations require safety-related systems to be isolated or have send-only communication with other systems. Public health and safety were never impacted during the incident.

FirstEnergy Nuclear, the licensee at Davis-Besse, investigated the incident and found a contractor established an unprotected computer connection to its corporate network, through which the worm reached the plant network. The investigation also found plant computer engineering personnel were unaware of a security patch that prevented the worm from working. Corrective actions include requiring documentation of all external connections to the internal network, installing an additional layer of security software, and ensuring computer personnel review new security patches and install them promptly.

[그림 7] Davis-Besse 원전 웜 감염 관련 NRC 공식 보도

미국 국토안보부와 아이다호국립연구소(INL)는 이러한 사이버보안의 중요성을 인식하고 Aurora 취약성[2]에 대한 연구를 착수하였다. 2007년 수행된 실험에서 사이버공격만으로 발전기 자체 보호메커니즘을 무력화시켜 디젤발전기를 파괴할 수 있다는 것을 보여주었다. [그림 8]

2010년 9월, 최초의 제어시스템 사이버 공격무기인 스턱스넷(Stuxnet)이 이란의 우라늄 원심분리기를 파괴하여 가동을 중단시켰다. 스턱스넷은 제로데이 취약점[3]을 이용하여 제어시스템을 공격한 최초의 악성프로그램이다. 스턱스넷은 2008년부터 활동하기 시작하였으나, 2010년에 이란 부세르 원전 시스템 및 나탄즈 농축시설 내 제어시스템 공급사인 독일 Siemens社의 WinCC[4]을 대상으로 실질적인 악성행위를 시작했을 때 감지되었다. 공격대상이 폐쇄망

2) 발전기를 보호하는 보호계전기는 차단기가 Open된 후 일정시간(10~15사이클)이 경과 후 작동하는데, 일정시간 경과 전에 차단기가 Close되면 보호 계전기가 동작하지 않음. 이런 특성을 이용하여 일정시간 경과 이전에 차단기의 Open/Close 반복으로 발전기 파괴가 가능한 것을 Aurora 취약성이라 한다.
출처 : "Myth or Reality - Does the Aurora Vulnerability Pose a Risk to My Generator?" (IEEE 2011 64th Annual Conference for Protective Relay Engineers, '11.04.)

3) 제로데이 취약점: Zero-day Vulnerability, 알려지지 않은 또는 해결책이 제시되지 않은 취약점

4) WinCC: Siemens社 PLC 내부 구동논리를 프로그래밍하는 소프트웨어

으로 되어있어 해커가 직접적으로 침투하기가 매우 어렵기 때문에 이동저장 매체 및 네트워크로 우회하여 감염 및 전파되었다. 스턱스넷은 국가기반시설로 사이버 공격 대상이 확장된 것을 반증하는 대표적인 사례로 평가되고 있으며 이후 지속적으로 목표지향적인(targeting) 공격들이 빈번히 발생하고 있으며 [표 5], 이들은 더욱 지능화되고 공격회수와 피해규모도 증가하는 추세이다.

[그림 8] CNN 방송 : 모의 사이버공격에 의한 발전기 파괴

[표 5] 원자력시설 및 기반시설을 타깃으로 하는 악성코드 사례

악성코드명	발견일자	기능
Flame	'11.05	원전 제어정보 유출
Shamoon	'12.08	석유기업 일반 전산망 마비
Energetic Bear	'13.05	제어시스템에 원격접속 가능
Black Energy	'14.10	원전 모니터링 시스템 공격

참고자료 3 : IT, SCADA(ICS), 원자력 I&C 특징

사이버보안 관점에서 비교한 IT 시스템, SCADA 및 ICS, 원자력 계측제어시스템의 차이점은 다음과 같다.

구분	IT 시스템	SCADA 및 ICS	원자력 계측제어시스템
성능 요건	- 비실시간 - 일관적인 응답 - 고성능 처리량 - 시간지연 수용가능	- 실시간 - 시간이 중요한 응답 - 적정한 처리량 - 시간지연 수용곤란	- 좌동
가용성 요건	- 재부팅 수용가능 - 시스템 작동 요건에 따라 가용성 결함 허용	- 공정 가용성 요건 때문에 재부팅 수용불가 - 정지는 수일/수주전 미리 계획 - 철저한 사전 시험으로 높은 가용성 요구	- 재부팅 수용불가 - 연차보수 적용 - 최고 수준의 가용성, 기능성, 내환경 시험 요구
위험 관리 요건	- 데이터 기밀성 및 무결성이 최대 목표 - 상대적으로 덜 중요한 내고장성, 순간적 정지는 중요하지 않음 - 중요한 위험은 사업 운영의 지연임	- 인명안전이 최우선, 다음으로 시설 보호 - 내고장성 필수, 순간적 정지 수용불가 - 중요한 위험은 규제 불만족, 인명, 장비, 생산의 손실임	- 좌동 - 원자로 안전성 및 핵물질 방호를 추가적으로 고려해야 함
시스템 구조 보안의 초점	- IT 자산 및 정보(저장된 혹은 전송되는)의 보호 - 중앙 서버는 더욱 보호가 요구됨	- 말단 클라이언트(예, 공정 제어기기와 같은 필드 기기)의 보호가 최우선 - 중앙서버의 보호도 중요	- 안전등급 순위를 고려한 보안 등급 설정 필요 - 보안 위협의 안전성 위해도 평가 필수
의도되지 않은 결과	- 보안 솔루션들은 대표적 IT 시스템 중심으로 설계됨	- 보안 도구들은 ICS 동작을 방해하지 않는지 시험해야 함	- 보안 기능이 시설의 안전성 및 성능에 악영향이 없도록 철저히 검증
상호작용의 시간 중요도	- 상대적으로 덜 중요한 긴급 상호작용 - 필요에 따라 엄격한 접근 통제가 구현 가능함	- 사람에 대한 응답과 기타 긴급 상호작용이 중요함 - ICS에 대한 접근이 엄격히 통제되어야 하나 인간-기계 상호작용을 방해하지 않아야 함	- 좌동 - 안전계통 및 비안전계통 감시 및 제어수단의 신호적 및 물리적 분리
시스템 운영	- 시스템이 대표적 OS에 맞게 설계됨 - 업그레이드는 자동화된 툴이 있어 손쉽게 이루어짐	- 보안 기능이 없는 변종 및 주문 제작형 OS 사용 - 소프트웨어 변경은 신중히 이루어짐. 특수한 제어 알고리듬, 하드웨어 및 소프트웨어 변경이 수반되므로 일반적으로 판매자에	- 좌동 - 안전성/신뢰성 관련 업무 추가 - 규제기관의 심사/검사 필수

		의해 이루어짐	
자원 제약	- 보안 솔루션과 같은 제3자 어플리케이션 추가를 지원할 수 있도록 시스템 자원이 충분함	- 시스템이 산업공정에 맞게 설계되어 보안 솔루션을 추가하기에 최소한의 메모리와 연산 능력 보유	- 좌동 - 다중화/다양성 설계에 대한 고려 필요
통신	- 표준 통신 프로토콜 - 국지적 무선 통신 기능을 가진 유선 통신 기반 - 대표적 IT 네트워크 사용	- 많은 독점적 및 표준 프로토콜 - 전용 유선 및 무선(radio 및 위성)을 포함한 여러 유형의 통신 매체 사용 - 복잡한 네트워크 사용, 때로는 제어 엔지니어가 필요함	- 좌동 - 무선 통신은 일반적으로 허용치 않음
변경 관리	- 소프트웨어 변경은 좋은 보안 정책과 절차 하에 시기 적절히 이루어짐. 절차는 종종 자동화됨	- 제어시스템의 무결성 유지를 보장하도록 소프트웨어의 변경은 철저히 시험되고 시스템에 점진적으로 이행됨. ICS 정지는 수일/수주전 계획되어야 함	- 좌동 - 안전성/신뢰성 평가 추가 - 변경에 대한 인허가 심사/검사 필요 - 핵연료 교체주기에 맞춘 연차보수 시 변경
지원 관리	- 다양한 유형의 지원이 가능함	- 일반적으로 단일 판매자에 의해 지원됨	- 좌동
기기 수명	- 3-5년	- 15-20년	- 좌동
기기 접속	- 기기들이 보통 근거리에 위치하고 접근이 용이함	- 기기들이 고립되고 원격에 위치하며 접근하기에 과도한 물리적 노력이 요구될 수 있음	- 좌동