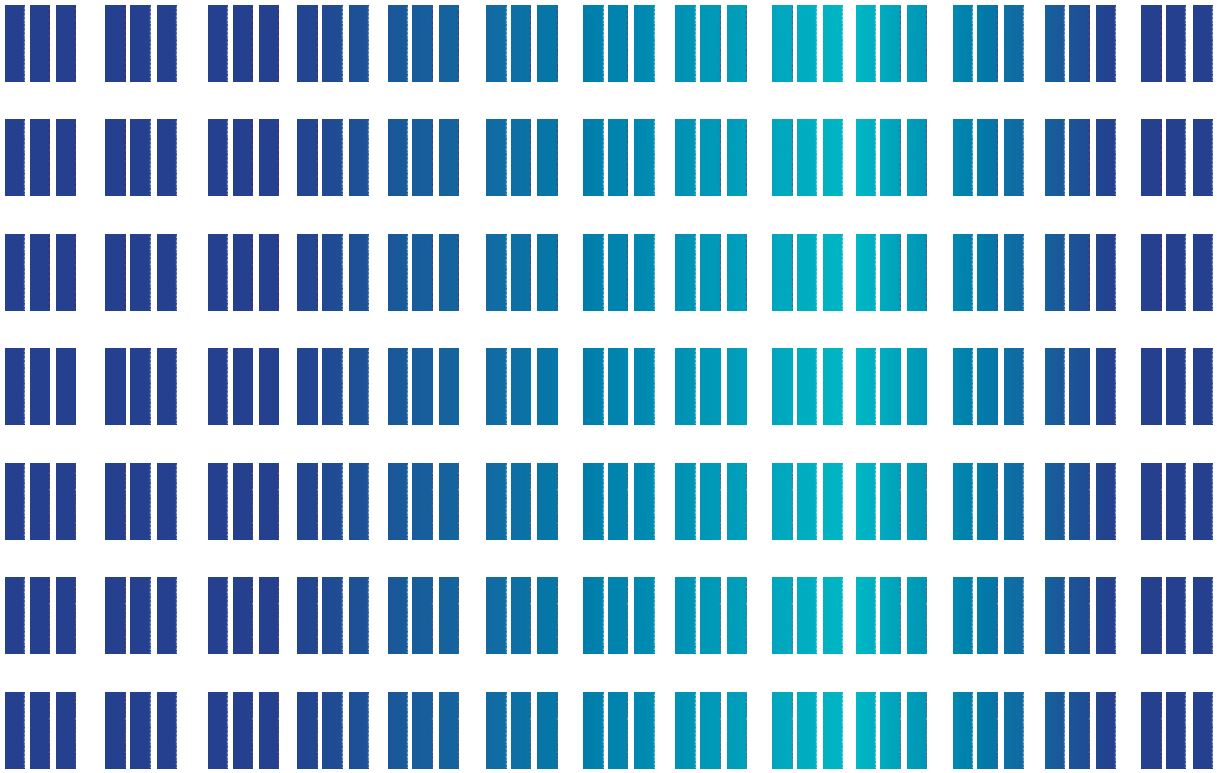
KICI DSR Vol. 25-08

한국정보통신산업연구원

Digital Safety Report

12월호



KICI 한국정보통신 산업연구원

한국정보통신산업연구원

Digital Safety Report

Digital Safety Report Contents

01 AI 데이터센터의 국가핵심기반 보호시설 지정 필요성

동아대학교
이동규 교수

AI 데이터센터, 왜 국가적인 재난관리를 해야 하는가?

인공지능(AI)의 발전 속도가 국가 경쟁력을 좌우하는 시대이다. 그럼에도 우리에게 2025년은 한국의 디지털 인프라 역사상 가장 뼈 아픈 해로 기록될 것이다. 국가정보자원관리원 대전센터 화재로 인한 정부 행정망이 물리적으로 셧다운되었고, 국가 통신 기간망의 주축인 KT와 SKT마저 해킹 공격에 뚫리며 국민의 민감 정보(IMSI, 인증키 등)와 업비트 해킹으로 금융 자산이 탈취당했다. 여기에 GS리테일(GS25, GS샵)에서 발생한 160만 건 규모의 계정 탈취(Credential Stuffing) 사고와 쿠팡 정보유출, 그리고 G마켓 무단결제 사태는 생활 밀착형 플랫폼조차 안전지대가 아님을 보여주고 있다.

위 일련의 사건들은 각기 다른 원인처럼 보이지만, 하나의 공통된 결론을 가리키고 있다. 우리의 디지털 인프라가 물리적 재난과 사이버 공격이라는 '복합적인 위협' 앞에서 속수무책일 수 있다는 점이다. 이러한 사례들의 교훈을 통해 점검해봐야 하는 사례가 바로 현 정부가 중요하게 추진하는 AI 데이터센터(AIDC) 구축이다. 이는 수천억 원짜리 GPU와 국가 기밀급 AI 모델을 다루는 전략 자산을 조성하는 과업이다. 따라서, 기존의 보안 실패를 답습한다면 그 결과는 단순한 불편을 넘어 국가적 재앙이 될 수 있다.

왜냐하면 AI 데이터센터는 더 이상 단순한 물리적 건물이나 기업의 IT 운영기지가 아니기 때문이다. 오늘날 AI 데이터센터는 전력, 수자원, 통신, GPU, 반도체가 집중된 초고밀도 국가핵심기반 보호시설이다. 해당 센터들은 그 위험성과 취약성에 대한 구조가 전통적인 인터넷 데이터센터(IDC)와는 차원이 다르다는 점에 주목해야 한다. 랙(Rack) 당 30~120kW에 이르는 전력밀도, 액체냉각 기반의 설비, 고밀도 GPU 클러스터라는 새로운 조합은 '언제든지 단 한 번의 장애가 전국적인 디지털 재난으로 확산될 수 있는 구조'를 의미한다.

AI 모델 학습과 추론 환경은 중단이 허용되지 않으며, 화재와 냉각상실, 그리고 전력 장애는 수 초 내에 AI 팜 전체를 가동 불능 상태로 만들 수 있다. 더욱이 한국은 세계 어느 나라보다 전력망, 통신망, 데이터센터, 금융망이 밀집된 초연결성 국가이기 때문에 AI 데이터센터의 사고는 단순한 기업 문제가 아니라, 국가적 차원의 대규모 재난 대응을 염두해 두고 위기관리 계획을 수립해야 한다.

이러한 위험구조 속에서 AI 데이터센터가 갖추어야 할 물리적인 보호와 기능연속성, 그리고 ESG 등을 통합한 새로운 물리적 및 사이버 보안 융합 안전 프레임워크를 구축해야 한다.

AI 데이터센터를 둘러싼 리스크 식별

1. 전력, 열, 냉각의 초고밀도 리스크

AI 데이터센터의 서버 랙(Rack) 하나가 소모하는 전력은 100kW 이상으로, 이는 일반 가정집 30가구가 동시에 사용하는 전력량과 맞먹는다. 이 막대한 에너지는 좁은 공간에서 고스란히 1,000℃에 육박하는 열로 바뀐다. 만약 냉각 장치가 멈추면 단 3초 만에 GPU는 끓는점까지 치솟아 스스로 녹아내리는 '열 폭주(Thermal Runaway)'를 일으킬 수 있다. 이를 막기 위해 도입된 '액침 냉각(서버를 특수 용액에 담그는 기술)'은 효율적이지만, 화재 발생 시 물을 뿌리면 폭발 반응을 일으킬 수 있어 기존 소방 방식이 무용지물이 된다는 딜레마가 있다. 게다가 '심장'이 멈추면 '뇌'가 죽듯이, UPS 배터리 하나만 고장나도 거대한 GPU 팜 전체가 동시에 심정지(Shutdown) 상태에 빠져 국가 AI 서비스가 '블랙아웃'되는 구조적 취약점을 안고 있다.

2. 군사 및 테러 표적의 리스크 현실화

AI 데이터센터는 단순한 민간 시설이 아닌, 국가의 AI 연산 능력을 좌우하는 전략적 요충지로 볼 수 있다. 따라서 유사시 적군의 미사일 정밀 타격 1순위 목표가 될 뿐 아니라, 자폭형 무인기(UAS)나 상용 드론을 개조한 테러 공격에 상시 노출되어 있다. 또한, 물리적 파괴 없이도 혼란을 야기할 수 있는 전자전의 위협도 존재한다. GPS 스푸핑(Spoofing)으로 데이터센터의 시각 동기화(Time Synchronization)를 교란하거나, 고출력 RF 재밍(Jamming)으로 무선 통신망을 마비시키는 비물리적인 공격이 가능하다.

지상에서는 전기차(EV) 대중화에 따른 새로운 위협이 부상했다. 수 톤에 달하는 배터리를 탑재한 대형 EV 트럭은 그 자체로 강력한 운동 에너지를 가진 무기이며, 고속으로 돌진하여 방호벽을 뚫거나 배터리 폭발을 유도하는 '움직이는 폭탄'이 될 수 있다. 이는 기존의 데이터센터는 고려하지 않았던 새로운 차원의 방호 설계가 요구되고 있는 이유이기도 하다.

3. 수자원과 냉각 인프라에 대한 의존 리스크

AI 데이터센터는 전기를 먹는 하마일 뿐만 아니라, '물을 마시는 거인'이다. 고성능 AI 칩의 열을 식히기 위해 사용되는 물의 양은 상상을 초월하며, 하루에만 수천 톤의 물이 냉각탑에서 증발할 수 있다. 만약 테러로 인해 상수도관이 파괴되거나 취수원에 독극물이 투입되어 급수가 중단된다면 어떻게 될까? 자동차 엔진에 냉각수가 없으면 1분도 못 버티고 눌어붙듯이, 수 조 원짜리 AI 클러스터는 즉시 '뇌사' 상태에 빠진다. 전력선은 눈에 보여 방호가 쉽지만, 땅속 깊은 곳을 지나는 수도관은 어디가 공격받는지조차 알기 힘든 '보이지 않는 아킬레스건'이 될 수 있다.

4. EMP와 전자기 리스크

AI 데이터센터의 심장인 GPU와 HBM(고대역폭 메모리)은 나노미터 단위의 초미세 회로로 이루어져 있다. 이는 마치 '유리와 만든 뇌'와 같아서, 아주 미세한 전압 변화에도 산산조각이 날 수 있다.

핵폭발이나 전자기 폭탄(E-Bomb)이 터지면 눈에 보이지 않는 '전기의 쓰나미(EMP)'가 몰려오는데, 일반 건물은 이를 막지 못 한다. 이 충격파가 닿는 순간 수천억 원의 AI 서버들은 겉은 멀쩡해도 속에서는 그 회로가 완전히 타 버려 '고철 덩어리'로 전락할 수 있다. 따라서 데이터센터 건물 전체를 전도성 금속으로 빈틈없이 감싸, 전기가 내부로 들어오지 못 하고 표면으로만 흐르게 하는 '패러데이 케이지(Faraday Cage)' 설계가 필수적으로 고려되어야 한다.

AI 데이터센터와 통신망을 함께 보호해야 하는 이유

과거에 우리는 데이터센터(서버/데이터)와 통신망(네트워크)을 별개의 인프라로 인식하고 관리해 왔다. 그러나 AI 시대의 도래로 이 두 영역의 경계는 완전히 허물어지고 있다. AI 데이터센터는 국가의 '대뇌'로서 판단과 연산을 담당할 것이고, 통신망은 이 판단을 전달하고 '산소(데이터)'를 공급하는 '신경망 및 혈관'이라 할 수 있다. 만약 두 시설이 동시에 타격을 받고 통합 대응에 실패할 경우, 다음과 같은 국가적 재난이 발생할 수 있다.

첫째, 초기 시나리오는 통신망 인증 체계(SMS 등) 마비로 운영자가 데이터센터 관리 시스템(Admin)에 접속조차 하지 못 하는 초기 상황이 발생할 수 있다. 둘째, 물리적 파괴 시나리오는 제어 불능 상태에서 데이터센터 냉각 펌프 정지 → 서버실 고열 발생 → UPS/ESS 배터리 폭발 및 화재로 확산된다. 셋째, 사회 인프라 마비 시나리오다. 금융 결제망 붕괴, 물류 자동화 중단, 행정 서비스 먹통 등 사회 기능이 전부 중단되는 '디지털 블랙아웃'을 초래할 수 있다. 마지막으로, 통신망 두절로 인하여 화재 신고, 피해 상황 공유, 예비 장비 가동 등 재난 대응 매뉴얼이 작동하지 않게 된다.

따라서 예측 불가능한 AI 시대의 재난으로부터 보안의 관점을 '개별 시설 보호'에서 '연결성(Connectivity) 및 기능 연속성 보호'로 전환하여 하나의 안보 자산으로 묶어 통합적으로 보호해야 한다.

정책 시사점

지금까지의 논의를 바탕으로 대한민국은 AI 데이터센터의 리스크를 고려하여 다음 5가지를 시급히 추진해야 한다.

1. 국가 표준 제정

지금의 데이터센터 관련 규정은 10년 전 '인터넷 시대'에 머물러 있다. AI 데이터센터의 물리적인 보호, 사이버 보안, 전력, 냉각, 안전 기준을 아우르는 새로운 국가 표준(KS) 또는 고시를 제정해야 한다. 랙당 5kW를 사용하던 시절의 소방 기준으로는 100kW를 사용하는 AI 서버의 열 폭주를 막을 수 없다. '고밀도 AI 데이터센터 특화 소방 기준'을 신설하여, 물이 아닌 가스나 액침 전용 소화 설치를 의무화해야 한다.

또한 현재는 권고 사항에 불과한 'EMP 차폐'나 '차량 테러 방지(HVM)' 시설을 일정 규모 이상의 AI 데이터센터에는 반드시 설치하도록 법제화해야 한다. 이러한 물리적 보호·방호는 국민의 안전과 직결된 문제이기 때문이다. 친환경 인증처럼 '좋으면 따는' 인증이 아니라, 이 기준을 충족하지 못 하면 AI 데이터센터를 건설할 수 없게 만드는 강력한 '안전 면허(Safety License)' 제도가 필요하다.

2. 부처 공동 거버넌스 구축

AI 데이터센터의 리스크는 한 부처가 감당할 수 있는 범위가 아니다. 가령 화재는 소방청, 재난관리는 행정안전부, 전력은 기후에너지환경부, 산업인공지능은 산업통상부, 데이터는 과기정통부, 해킹은 국정원 소관이다. 이렇게 쪼개진 행정으로는 '복합 재난' 앞에 무력할 수밖에 없다. 따라서 'AI 데이터센터 물리적 및 사이버 보안 융합 안전위원회(가칭)'를 신설하여 범정부 컨트롤 타워를 구축해야 한다.

과기정통부(디지털 정책)와 기후에너지환경부(전력 및 에너지)가 머리를 맞대고, 전력 공급과 데이터 안정성을 함께 심사해야 한다. 전기는 공급되는데 통신이 중단되거나, 통신 기능은 작동하나 전기가 공급되지 않는 엇박자를 막아야 한다.

행정안전부(재난 안전)와 국가정보원(국가 안보 및 사이버)이 협력하여, 물리적 테러와 사이버 공격이 동시에 발생하는 '하이브리드 위협'에 대응하는 통합 매뉴얼을 만들어야 한다. 금융위원회는 이러한 안전 기준을 충족하지 못한 AI 데이터센터에는 PF 대출이나 투자를 제한하는 가이드라인을 만들어, 시장 스스로 안전한 시설을 건설할 수 있도록 유도해야 한다. 자본의 흐름이 안전을 강제하는 가장 강력한 수단이 될 것이다.

3. ESG 기반 금융 심사모형 신설

기존의 ESG 평가는 '친환경'에만 치우쳐 있어, AI 데이터센터의 핵심인 '물리적 안전'과 '회복 탄력성'을 담아내지 못 하고 있다. 이제는 K-Taxonomy와 EU Taxonomy에 맞춘 'AI 데이터센터 특화 ESG 평가 모델'이 필요하다.

단순히 전기만 적게 사용한다고 높은 점수를 주어서는 안 된다. 전력효율(PUE)과 물 사용 효율(WUE) 기준을 동시에 충족하면서, 재난 시에도 멈추지 않는 '회복 탄력성'을 갖춘 시설에만 녹색 등급을 부여해야 한다. 또한 사회(S)와 지배구조(G)의 재정의가 필요하다. '사회(S)' 지표에는 사고 예방 능력과 재난 복구(DR) 체계를, '지배구조(G)' 지표에는 공급망 보안(SBOM)과 리스크 투명 공시 여부를 핵심 평가 항목으로 포함해야 한다.

금융기관은 이 평가 모델을 기반으로 프로젝트 파이낸싱(PF) 금리를 차등 적용해야 한다. 안전 기준을 충족한 '요새형 데이터센터'에는 녹색채권(Green Bond) 발행과 저금리 혜택을 주고, 기준 미달 시설에는 투자를 제한함으로써 시장 원리로 안정성을 강제해야 한다.

4. 드론, EMP, 테러 대응 법제화

현행 보안 관련 법령은 10년 전 기준이라, 드론이나 EMP 같은 최신 군사적 위협을 '재난'으로 정의조차 하지 못 하고 있다. '보이지 않는 위협'에 대응할 수 있도록 법의 사각지대를 메워야 한다. 자연재해 중심의 현행법을 개정하여, '지능형 테러'와 '전자전(EMP)'을 명시적인 재난 관리 대상으로 포함해야 한다. 그래야지만 예산을 배정하고 방호 설비를 구축할 법적 근거가 생긴다.

현재 민간 기업이 날아오는 드론을 향해 전파를 쏴서 떨어뜨리면, 오히려 전파법 위반으로 처벌받는다. 국가안보에 직결되는 핵심 AI 데이터센터에 한해서는, 불법 드론을 무력화할 수 있는 '능동적 방어권'을 법적으로 허용해줘야 한다.

5. AI 데이터센터의 국가핵심기반 보호시설 지정 검토

AI 데이터센터는 단순한 민간 건물이 아니다. AI 시대의 '제2의 발전소'이자 '제2의 통신망'이다. 원전이 멈추면 나라가 멈추듯, AI 데이터센터가 멈추면 국가의 모든 연결망이 마비될 수 있다는 가정을 수립해야 한다.

일정 규모 이상의 AI 데이터센터를 '국가핵심기반 보호시설'로 지정하여 국가가 직접 관리해야 한다. 이는 민간의 자율성을 침해하는 것이 아니라, 국가 안보라는 우산을 씌워주는 것이다.

핵심시설로 지정된다면 평시에는 경찰이 순찰을 돌고, 테러의 위협이 있을 시에는 군 병력이 방공망을 제공할 수 있다. 무엇보다 대규모 정전이나 통신 마비 시, 국가의 복구 자원을 최우선으로 투입받을 수 있는 '골든타임 우선권'을 확보하게 된다. 이는 기업 혼자서는 절대 할 수 없는 일이다.

국가 행정망 화재부터 통신 인프라 해킹까지, 최근의 사고들은 우리에게 '설마'가 '국가 차원의 대참사'가 되는 것이 한 순간임을 보여주고 있다. 정부는 국가 안보 차원의 가이드라인을 수립하고, 기업은 보안을 비용이 아닌 최고의 경쟁력으로 인식하는 '패러다임의 대전환(Grand Shift)'이 필요한 시점이다.

02 2025년 통신재난관리 실무협의체 워크숍 개최

2025년 12월 9일, 과학기술정보통신부(부총리 겸 장관 배경훈)가 주최하고 한국정보통신산업연구원(원장 백운일, 이하 KICI)이 주관한 '2025년 통신재난관리 실무협의체 워크숍'이 서울 코엑스에서 개최되었다.

이번 행사는 통신재난관리 역량 향상을 위한 우수사례·정보 공유 및 정부-주요 통신사업자 협조체계 강화를 위하여 마련된 자리로, 이성훈 과기정통부 디지털기반안전과장을 비롯해 중앙전파관리소, KICI, 주요 통신사업자(27개사)의 재난관리 전담인력 등 약 95명이 참석하였다.

이 날 행사에서는 기간통신, 부가통신, 데이터센터 분야 별 2026년도 통신재난관리기본계획에 대한 설명, 전문가 발표, 우수사례 발표 등이 진행되었다.

또한 이 날 행사에서는 2025년 통신재난관리 업무 발전에 기여한 유공자 시상식이 진행되어 총 9명이 부총리 겸 과학기술정보통신부 장관 표창을 수상하였다.

※ 자세한 내용은 정보통신신문에서 확인하실 수 있습니다.
https://www.koit.co.kr/news/articleView.html?idxno=204241

03 전문가 인터뷰

- KT 진호섭 센터장님을 만나다 -

KT
진호섭 센터장

Q1. 우선 진호섭 센터장님에 대해서 소개 부탁드립니다.

A1. 저는 2006년 Mobile WiMAX 무선망 전문가로 KT에 입사하여 WiBRO, 3G, 4G 무선망 설계와 구축 업무를 담당하였으며, 현재는 공공안전망운영센터에서 재난 안전통신망(PS-LTE), 해상통신망(LTE-M), 철도통신망(LTE-R) 3개 무선망의 운영관리를 총괄하고 있습니다. 3개 무선망을 공공안전통신망이라고 칭하는데, 공공안전통신망이란 경찰, 소방, 해경, 철도 등 공공기관이 국민 안전, 재해 예방 및 재난 구호를 목적으로 활용하는 무선 통신 인프라입니다.

2016년 재난안전통신망, 해상통신망, 철도통신망 설계 및 구축 책임자로 사업에 참여하여 행정안전부, 해양수산부, 국가철도공사 등 관련 기관과 협력하여 365일 안정적인 네트워크 운영을 책임지고 있습니다.

최근 경북 산불 및 국가정보원 화재와 같은 대형 재난이 발생하였을 때 신속한 대응을 하기 위하여 관련 기관과 실전형 합동훈련을 통해 재난 대응 역량을 강화하고 있습니다. 또한 안정적인 운영과 서비스 고도화를 위하여 정부기관, 이용기관, 공공안전통신망포럼과 함께 기술 연구 및 국내외 표준화 추진에 힘 쓰고 있습니다.

Q2. 센터장님께서는 공공안전통신망을 운영하고 계신다고 하셨는데, 재난·재해 현장에서 재난안전통신망의 서비스 연속성을 유지하는 기술에 대해서 소개 부탁드립니다.

A2. 재난 및 재해 현장에서 재난안전통신망의 서비스 연속성을 확보하기 위해 RAN-Sharing 기술이 도입되었습니다. MOCN(Multi-Operator Core Network) 방식을 적용하여 여러 이동통신사가 동일한 RAN(Radion Access Network)을 공동 사용하면서, 각자의 코어망은 독립적으로 운영하는 방식입니다.

과거에는 경찰, 소방, 철도, 해경 등 각 기관이 독립적으로 통신 인프라를 구축 및 운영해 왔습니다. 이로 인해 재난 발생시 기관 간 상호 연동이 어렵고, 망 장애 발생 시 통신이 단절될 위험성이 매우 높았습니다. 따라서 정부는 재난 관련 기관 간의 통신 단절 문제를 해결하고 국가 차원의 통합 지휘 및 상황 공유를 위해 2021년 전국 단위 재난안전통신망을 구축했습니다. 초기 설계 단계부터 해상무선망 및 철도 무선망과 인접 지역에서 발생할 수 있는 전파 간섭과 서비스 단절을 해소하기 위해 양방향 RAN-Sharing 기술을 도입하여 공공안전통신망의 통신 품질이 개선되고 커버리지가 확장되었습니다.

또한 통신사 기지국과도 RAN Sharing이 적용되어 재난 상황에서 통신망 신뢰성과 안전성이 한층 향상·강화되었습니다. 이러한 구조를 통해 재난안전통신망은 국지적 극한호우에 따른 침수·산사태·도로유실 등으로 통신망이 붕괴되는 경우에도 각 망 간 상호 연동을 통해 서비스 연속성 및 망 생존성을 확보하고 있습니다.

Q3. 최근 몇 년간 발생한 크고 작은 통신 장애나 디지털 재난 사례들을 기술적 관점에서 회고해 보신다면, 과거(음성 중심 시대)와 비교하여 가장 두드러지는 변화나 기술적 취약점은 무엇이라고 생각하시나요?

A3. 과거의 경우, 전화 교환기 장애가 발생해도 피해 지역이 한정적이었고, 회선 절체 또는 장비 교체 등을 통해 신속히 복구하여 장애의 사회적 영향이 비교적 적었습니다. 반면 최근의 통신 재난은 단순한 음성 통화 장애가 아니라 복잡한 라우팅 구조와 클라우드 기반의 네트워크로 구축되어, 단일 장애가 네트워크 전체로 파급되고 사회·경제적으로 심각한 영향을 초래합니다.

기술적인 취약점을 살펴보면, 첫째 네트워크 구조의 복잡성 증가와 이기종 시스템의 혼재입니다. 과거 음성 중심 시대에는 유선전화와 2G, 3G 등 비교적 단순한 네트워크 구조가 주를 이루었습니다. 하지만 최근에는 5G, 6G로의 진화와 함께 네트워크 구조가 매우 복잡해졌습니다. 따라서 다양한 장비와 시스템이 혼재되어 운영되면서, 이종 시스템 간의 호환성 검증이 필수적입니다. 특히, 기존 네트워크와 신규 시스템 간의 마이그레이션(Migration) 과정에서 예상치 못한 장애가 발생할 수 있으며, 각 단계별로 발생 가능한 이슈를 신속하게 파악하고 대응하는 체계가 중요해졌습니다.

둘째, 노후 장비와 이중화의 미흡입니다. 여전히 현장에서는 유선전화, 3G 등 노후 장비가 혼재되어 사용되고 있습니다. 이러한 장비의 노후화가 전체 네트워크에 장애를 일으킬 수 있으며, 이중화 및 백업 체계가 미비한 경우 장애 복구가 더욱 어려워집니다.

셋째, 네트워크 진화와 확장에 따른 새로운 취약점 발생입니다. 과거에는 자연재해(지진, 홍수, 대풍 등)으로 인한 물리적 장애가 주를 이루었으나, 최근에는 디지털 재난(사이버 공격, 대규모 DDoS 등)이 빈번하게 발생하고 있습니다. ICT 기반의 재난 대응 체계가 강화되고 있지만, AI·클라우드 등 신기술의 도입으로 인해 새로운 취약점이 계속해서 등장하고 있습니다. 특히, 데이터센터 등 핵심 인프라에 대한 보안 강화와 복구 시나리오 마련이 중요합니다.

마지막으로, 보안에 대한 인식개선이 필요합니다. 네트워크 운용자는 복잡한 환경에서 안정적인 서비스 제공을 위해 체계적 운용과 실시간 모니터링, 자동화된 장애 시스템을 갖추어야 하며, 신기술 도입에 따른 새로운 보안 취약점에 대응하기 위해 보안 인식을 높이고 정책 관리와 교육을 강화해야 합니다.

Q4. 현재 5G, 6G까지 기술이 진화하고 있지만, 현장에는 여전히 유선전화, 3G, LTE 장비가 혼재되어 사용되고 있습니다. 오래된 장비의 노후화가 전체 네트워크에 장애를 일으키지 않도록, '망 진화(Migration)' 과정에서 엔지니어들이 가장 신경 써야 할 부분은 무엇일까요?

A4. 망 진화(Migration) 과정에서는 다각적인 전략과 체계적 접근이 요구됩니다. 첫째, 기존 네트워크와 신규 시스템 간의 호환성 검증을 최우선으로 실시해야 합니다. 현재 운용 장비와 구성 환경이 신규 시스템과 서비스 연속성 유지 및 상호 간 안정적 연동가능한지 사전 점검이 필요합니다. 특히 프로토콜, 인터페이스, 네트워크 구성 요소에 대한 충분한 호환성 검증을 통해 잠재적 이슈를 사전에 파악하고 해소해야 합니다.

둘째, 시스템 단위의 단계적 교체 계획을 수립하여 전체 시스템을 일괄적으로 전환하기보다는 서비스별 소규모 단위의 순차적 전화 방식을 적용함으로써 각 단계에서 발생할 수 있는 문제점을 신속하게 파악하고 즉시 대응할 수 있습니다. 이와 같은 방식은 서비스 중단을 최소화할 뿐 아니라, 장애 발생 시 방식은 서비스 중단을 최소화할 뿐 아니라, 장애 발생 시 신속한 복구를 가능하게 합니다.

셋째, 보안 및 정책 관리의 필수적 점검입니다. 네트워크 및 방화벽 정책을 최신 상태로 유지하고 노후 장비에서 발생할 수 있는 보안 취약점을 철저히 관리해야 합니다. 또한 데이터 무결성 및 접근 제어 강화 또한 망 진화 과정 내내 집중적으로 관리되어야 하며 전환의 모든 단계에서 보안이 내재화되어야 합니다.

넷째, 이해관계자와의 협업 체계 구축이 필요합니다. 프로젝트 주관부서, 외부 벤더사 등 이해관계자 간의 긴밀한 협업을 위한 TF(Task Force)를 구성하고 네트워크 전환 과정에서 발생하는 다양한 이슈를 신속히 공유하고 효과적으로 해결해야 합니다. 각 단계별 진행 상황과 장애 발생 시 체계적인 대응 구조를 공유한다면, 모든 이해관계자가 명확한 정보를 근거로 올바른 의사결정을 할 수 있습니다.

마지막으로, 망 전환 후 네트워크 성능 및 관리 지표 관리가 필요합니다. 망 전환 이후 네트워크 성능 및 관리 지표를 마련하여 실시간 모니터링과 데이터 분석을 통해 개선 작업을 병행해야 합니다. 이를 통해 시스템의 안정성과 효율성을 지속적으로 유지할 수 있습니다.

Q5. 지하 통신구 및 지하 시설물의 이상징후를 정밀 감시할 수 있는 최신 기술 트랜드가 있을까요?

A5. 최근 지하통신구의 관리에는 AIoT, 로봇, 3D 레이더 기반 정밀 탐사 등 첨단 기술이 도입되고 있습니다.

AI와 IoT가 결합된 AIoT 시스템은 센서, 카메라, 로봇 등 다양한 기기로부터 실시간 데이터를 수집·분석하여 이상징후를 감지하고 신속한 상황 전파를 가능하게 합니다.

지하통신구 시설물 감시로는 스마트플랫폼이 대표적입니다. AIoT 기반의 실시간 모니터링, 자동 경보 등 다양한 서비스를 제공하며 4G, 5G 네트워크와 연계되어 실시간 데이터 전송 및 분석이 이루어지고 있습니다.

스마트 모니터링 시스템은 지하 공간에 AI 기반의 IoT 센서와 결합해 온도, 습도, 가스 농도 등 데이터를

실시간으로 수집 및 분석하여 위험 발생 시 자동으로 관제센터 및 현장 담당자에게 즉시 알림으로써, 현장에서의 안전사고 발생률을 크게 낮추고 있습니다. 이러한 기술 도입은 기존의 단순 감시 체계를 넘어 실시간 데이터 수집 및 분석으로 자동화된 이상 감지를 통해 선제적 유지관리 및 안전관리 중심으로 진화하고 있습니다.

Q6. 지진이나 전쟁 등으로 지상 케이블(가공 및 지중)이 물리적으로 소손되었을 때, 저궤도 위성(Starlink 등)을 활용한 백홀(Backhaul) 연결이 대안으로 떠오르고 있습니다. 실제 국내 통신 환경에서 위성 통신을 '긴급 복구 백업망'이나 일반적인 통신수단으로 활용할 수 있을까요?

A6. 2025년 5월, 과기정통부가 해외 저궤도 위성 사업자(SpaceX)의 국내 서비스 공급계약을 승인했고, 단말기 적합성 평가 후 12월부터 일반 소비자 대상 서비스(B2C)와 산업체(B2B) 분야에서 해상, 조선, 항공 등 위성 인터넷 서비스를 공식적으로 시작하였습니다.

저궤도 위성은 여러 장점을 가지고 있으나, 동시에 기술적·구조적 문제점과 한계를 가지고 있습니다.

첫째, 우회경로로 인한 보안 문제입니다. 저궤도 위성은 공중망을 기반으로 하여 국내에는 지상국이 없고 일본 지상국을 경유하여 해저망을 통한 우회 경로를 거쳐 사용자에게 도달합니다. 때문에 일반 전용회선 대비 지연 증가 및 품질 예측이 어렵다는 문제가 있습니다.

둘째, IPv6 호환성 논란입니다. 저궤도 위성은 IPv4 기반으로, 접속 단말이 IPv6 기반일 경우 Dual Stack, 터널링 등이 필요합니다.

마지막으로, NAT(Network Address Translation) 환경 이슈입니다. 저궤도위성은 고정 공인 IP 미제공으로, VPN 안정성 확보를 위한 추가 장비 VPN Router가 필요합니다.

국내 시장에서는 이미 전국 단위 광 코어, 5G 등 초고속 통신 인프라가 충분히 구축되어 있어 위성 인터넷의 활용도는 다소 적을 것으로 보이며, 이에 따라 실질적인 수요는 해상 및 도서 산악지역 등으로 제한적일 것으로 생각합니다.


이미지 : flaticon.com

Q7. 통신망 재난 대응 발전 방향과 시사점은 무엇일까요?

A7. 네트워크 인프라 측면에서는 대규모 재난 발생 시 능동적인 통신망 로밍 전환과 광케이블 지중화, 난연 케이블 적용, 통신3사 통합 이동기지국 등 물리적, 기술적 보강이 필요하며, 이기종 네트워크와 저궤도 위성통신(LEO) 등 다양한 네트워크와 연계 가능한 솔루션 확보가 필요합니다. 이를 통해 어떠한 재난 상황에서도 통신망의 생존성을 보장하고, 서비스 단절을 최소화할 수 있습니다.

정부는 통신사업자 간의 협력체계와 합동훈련을 통해 재난 대응역량을 지속적으로 강화해야 하며, 경찰·소방 등 재난 대응 기관 단위의 긴급 통신망 솔루션 개발과 운영도 필요해 보입니다.

Q8. 마지막으로 정보통신 엔지니어로서 지속가능한 디지털 인프라는 무엇이라고 생각하시나요?

A8. 먼저 디지털 인프라의 안정적인 운영을 위해 장애 발생 시 빠른 복구와 함께 백업 구조의 네트워크 구성이 필요합니다. 특히 이중화 및 분산된 구조에서 장애의 신속한 탐지와 대응 체계를 갖춰야 합니다.

둘째, 대규모 데이터센터, 네트워크 장비의 저전력을 설계하고 가상화, 클라우드 기반으로 자원 운영 효율을 높여야 합니다.

셋째, 사이버 공격 등 데이터 유출을 대비하여 암호화, 제로 트러스트(Zero Trust) 모델, 보안 모니터링 강화가 필요합니다.

넷째, 상대적으로 취약한 농어촌, 도서지역 등도 안정적인 네트워크 제공이 되도록 보편적인 서비스 제공이 이루어져야 합니다.

즉, 지속가능한 디지털 인프라는 단순히 네트워크와 데이터센터를 구축하는 것을 넘어 환경, 사회, 경제적 책임을 고려하여 안정적이고 효율적으로 운영할 수 있는 ICT 생태계를 구성하는 인프라 구축을 의미한다고 생각합니다.

04 디지털 안전 관제 이슈

coupang

2025.11.14., 2025.11.29.

('25.11.14.) 쿠팡 검색서비스 장애

('25.11.29.) 쿠팡, 쿠팡이츠 결제 서비스 오류 장애

CLOUDFLARE

2025.11.18.

클라우드 플레어 DNS 접속 장애로 인한 X, Chat GPT 서비스 장애

2025년 가을철 산불조심기간

산림청 공고 제2025 - 338호

「산림보호법」 제31조 제3항에 따라 2025년 가을철 「산불조심기간」을 다음과 같이 공고합니다.

2025년 10월 14일
산 림 청 장

2025년 가을철 「산불조심기간」 설정·운영

1. 가을철 「산불조심기간」 설정

○ 산불조심기간 : 2025. 10. 20. ~ 12. 15(57일)

* 지자체는 기상상태 및 지역여건을 고려하여 산불조심기간을 탄력적으로 조정·운영

(출처: 2025년 가을철 「산불조심기간」 공고, 산림청, 2025. 10. 14.)

2025.10.20. ~ 12.15. 가을철 산불조심기간

산불로 인한 디지털 재난·장애 대비 모니터링 강화

2025.11.20. 강원 인제 산불

통신마비 대비 상황 보고

2025.11.22. 강원 양양 산불

통신마비 대비 상황 보고

2025.11.29. 전북 순창 산불

통신마비 대비 상황 보고

05 Digital Safety Inside

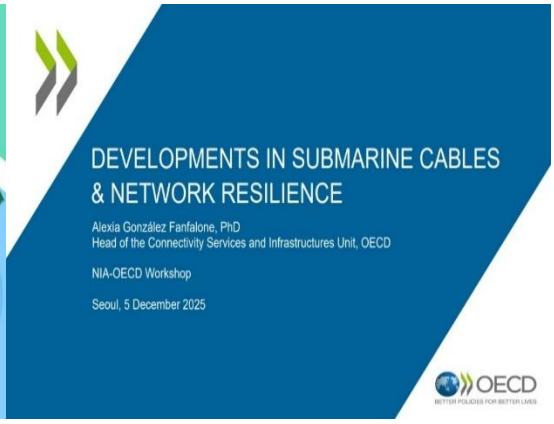
글로벌 디지털 재난 및 해저 통신케이블 동향 세미나

2025년 12월 5일(금), 한국지능정보사회진흥원(이하, NIA)이 디지털 재난 상황에서의 통신 인프라 복원력을 강화하고, 국가 핵심 자산인 해저 통신케이블의 글로벌 전략을 논의하기 위한 자리를 마련하였다.

이번 세미나는 최근 발생한 산불, 집중호우 등 복합재난 증가에 따른 통신망 안정성 확보와 더불어, 전략적 중요성이 커지고 있는 해저 통신케이블에 대한 국제적 기술·정책 동향을 파악하기 위해 기획되었다.

이날 행사에는 NIA 나성욱 단장과 한국정보통신산업연구원(이하, KICI) 최지은 본부장 등 국내 통신 전문가를 비롯하여 OECD 알렉시아 곤잘레스 판팔로네(Alexia González Fanfalone) 실장 등 약 20명의 주요 관계자가 참석하였다.

세미나는 KICI 신현철 디지털안전관제센터장의 '디지털 재난 사업 소개' 발표로 시작되었고, 이어 OECD 알렉시아 곤잘레스 판팔로네 실장의 '해저케이블 글로벌 동향 발표'가 진행되었다.



KICI 한국정보통신
산업연구원

경기도 수원시 장안구 하률로 12번길80(천천동)
TEL.031-231-3400 FAX.031-269-5210
www.kici.re.kr

편집 : KICI 디지털안전본부 김성용, 한갑운, 용경진, 김다은