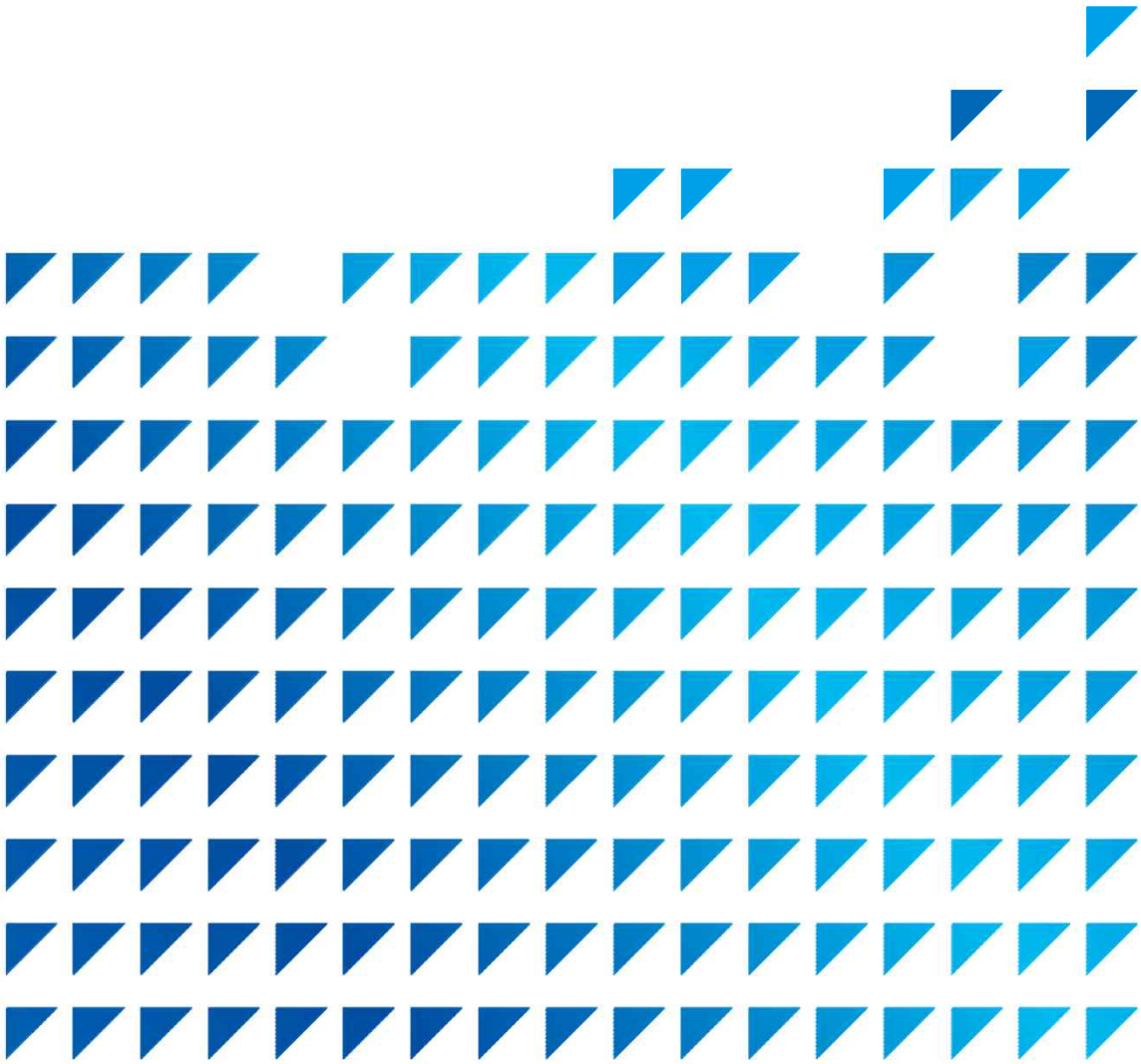
KICI DSR Vol. 26-07

한국정보통신산업연구원

Digital Safety Report 7월호



KICI 한국정보통신 산업연구원

KICI 한국정보통신산업연구원

한국정보통신산업연구원

Digital Safety Report 7월호

Contents

01 전문가 칼럼

㈜케이넷인프라
양철우 대표이사 / 정보통신기술사

AI 시대 해저케이블의 보안 위협과 디지털 재난 대응

들어가며

오늘날 국제 데이터 트래픽의 99% 이상을 전달하는 해저케이블은 글로벌 디지털 경제를 지탱하는 핵심 연결 인프라이자 국가 디지털 안보를 뒷받침하는 필수 기반시설이다. 생성형 AI 확산과 AI 데이터센터(AIDC) 간 초대용량 데이터 전송이 급증하면서 그 중요성은 더욱 커지고 있다. 이제 해저케이블은 단순한 통신시설을 넘어 데이터 보안과 디지털 재난 대응 역량을 좌우하는 전략자산으로 자리매김하고 있다.

그러나 최근 지정학적 갈등과 사이버 위협이 고조되면서 해저케이블을 둘러싼 위험도 커지고 있다. 과거에는 단순히 단선(Cut)과 같은 물리적 훼손이 주된 우려였으나, 이제는 도청, 공급망 공격, 내부자 위협 등 정교한 보안 위협에 직면해 있다. 이에 따라 해저케이블 전 수명주기에 걸친 보안 강화와 디지털 재난 대응 체계 구축이 국가적 과제로 부상하고 있다.

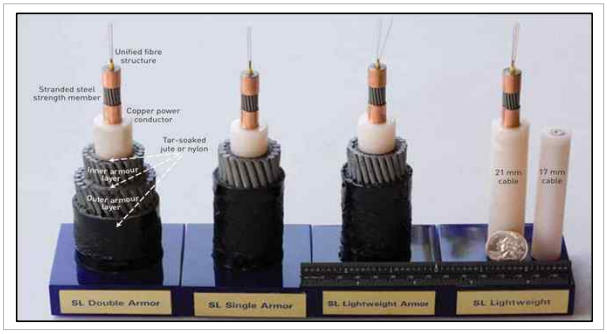
1. 물리적·광학적 접근을 통한 도청 위협과 탐지 기술

1.1 수중 및 육상 구간의 물리적 도청 시나리오

광통신은 전자기파 방사가 거의 없어 외부 검출이 어렵다고 알려져 있지만, 물리적 접근을 통한 도청이 완전히 불가능한 것은 아니다. 대표적으로 광섬유를 미세하게 굽히는 광섬유 굽힘(Macro-bending)이나 두 광섬유를 근접시켜 신호를 유도하는 에바네센트 결합(Evanescent Coupling) 방식이 존재한다. 일각에서는 외부 누설광을 통한 무접촉 도청 우려도 제기하나, 빛이 코어와 클래딩 경계면에서 전반사되는 구조 특성상 자연 누설광을 통한 도청은 현실적으로 매우 어렵다.

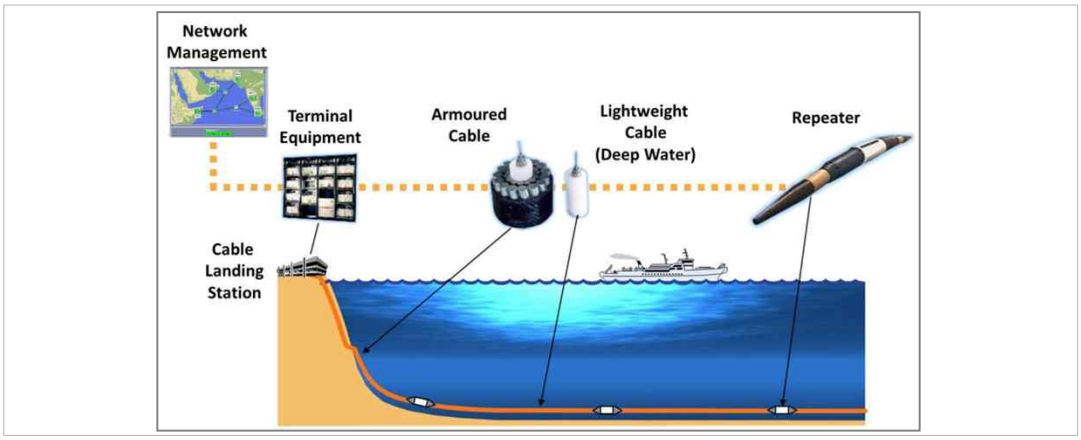
즉, 도청을 위해서는 광섬유에 물리적으로 접촉해야 한다. 특히 심해에 비해 접근성이 높은 육양국(Landing Station)과 육상 관로 구간(광배선반, 맨홀 등)은 이러한 물리적 침입에 취약하다. 침입자가 광분기기(Splitter)를 삽입하거나 케이블에 물리적 변형을 가하는 방식이 시도될 수 있다.

〈그림 1〉 대표적인 해저광케이블(좌에서 우로 천해부용 – 심해부용)



[출처] iCPC-UNEP Report

〈그림 2〉 대표적인 해저 광케이블 시스템의 개략도



[출처] UK Cable Protection Committee and ASN

1.2 광학적 이상 징후 기반의 실시간 탐지 기법

물리적 접근을 통한 모든 도청 시도는 광신호에 반드시 미세한 광학적·기계적 흔적을 남긴다. 광전송망은 이러한 변화를 다중 계층에서 실시간으로 감시한다.

〈표 1〉 광학적 이상 징후 기반의 실시간 탐지 기법

구분	내용
광신호 감쇠(Attenuation)	구조 변형이나 굽힘이 발생하면 광 도파 조건이 변화하면서 일부 광 에너지가 방사되고, 수신단에서는 미세한 삽입 손실로 감지된다.
편광 상태(SOP) 및 위상 변화	압력이나 변형이 가해지면 빛의 편광 특성과 위상, 편광모드분산(PMD) 등의 프로파일이 정상 상태를 벗어난다. 현대 코히어런트(Coherent) 광수신기는 이를 실시간으로 분석해 이상 징후를 조기에 포착한다.
종합 모니터링 및 음향 감지	OTDR/COTDR(광시간영역반사측정기) 기반 광선로 시험과 전송장비 코히런트 수신기의 DSP(디지털 신호처리 프로세서) 분석, OCM(광채널 모니터링 장치)·OSC(광감시 채널)·NMS(네트워크 관리시스템)를 연계한 통합 모니터링을 통해 성능을 실시간 감시한다. 최근에는 분산형 음향 감지(DAS) 기술을 활용해 케이블 주변의 진동, 굴착, 접근 행위 등 물리적 이상 징후를 탐지하는 기술도 적용되고 있다.

2. 수명주기별 보안 취약점과 방어 체계

2.1 유지보수 단계의 내부자 위협 대응

선로 장애 복구나 정기 유지보수 시 발생하는 일시적 통신 중단 시점은 보안 취약 구간이다. 고장 수리 과정에서 악의적으로 광분기기(Splitter)를 삽입하는 시나리오는 대표적인 내부자 위협(Insider Threat)으로 꼽힌다.

이를 방어하기 위해 국제 해저케이블 운영 절차는 철저한 다단계 검증 체계를 운영한다. 작업 완료 후 OTDR/COTDR을 통해 초기 구축 당시 확보한 기준 광학 프로파일(Golden Trace)과 현재의 광학 특성을 정밀 비교하며, 새로운 삽입 손실이나 반사 특성이 발견되면 즉시 원인을 분석한다. 또한 설계 단계에서 엄격하게 산정된 광출력 예산(Optical Power Budget)을 벗어날 경우 시스템이 자동으로 이상을 감지한다. 기술적 검증 외에도 작업 전후 사진 기록, 입회 감독, 이중 확인, 봉인 관리 등 절차적 보안이 필수적으로 병행된다.

2.2 건설 및 공급망 단계의 공격 대응

가장 치명적인 시나리오는 최초 건설 단계에서 비인가 장비나 악성 부품을 은닉하는 공급망 공격(Supply Chain Attack)이다. 이때 삽입된 모듈은 초기 기준 데이터(Golden Trace)로 오인될 수 있어 장기간 탐지를 회피할 위험이 있다.

그러나 실제 프로젝트는 단일 사업자가 전 과정을 독점하기 어려운 구조다. 제조사, 시공사, 독립 검증기관, 발주 컨소시엄이 교차 검증을 수행하며, 공장시험(FAT), 현장시험(SAT), 최종 준공시험(Commissioning)을 거친다. 공장 출하 시 기록된 모든 광코어의 감쇠·반사 특성은 현장 측정 데이터와 엄격히 비교되며, 개통 단계에서 코히어런트 전송장비가 색분산(CD), PMD, 비선형 특성을 자동 분석하므로 비인가 부품 삽입으로 인한 프로파일 불일치는 최종 단계 이전에 대부분 차단된다.

다만, 해저케이블이 특정 국가를 경유하거나 특정 기업(하이퍼스케일러)에 의해 구축·운영되는 경우에는 공급망 위험이나 내부자 위협에 대한 관리 필요성이 더욱 커질 수 있다.

3. 국가 공급망 보안과 제로 트러스트 보안 체계

기술적 방어 체계가 고도화되더라도 제조사, 시공사, 운영사 내부자가 공모하는 형태의 공격은 기술만으로 완벽히 막기 어렵다. 이에 따라 주요 선진국은 해저케이블을 단순한 민간 통신설비가 아닌 '국가안보 자산'으로 지정해 관리를 강화하고 있다.

대표적으로 미국의 'Team Telecom' 제도는 해저케이블 사업의 외국 자본 참여, 운영 구조, 데이터 접근 권한 등에 대한 고강도 국가안보 심사를 수행하며, 위험 요인 발견 시 허가를 제한하거나 보안협약(Security Agreement)을 강제한다. 공급망 전반에서는 핵심 전송장비 제조사 검증, 펌웨어 보안성 확인, 독립적 기술감리, 불시 현장점검이 시행된다.

최근에는 물리적 선로를 포함한 어떠한 요소도 기본적으로 신뢰하지 않는 '제로 트러스트(Zero Trust)' 개념이 광전송망에도 빠르게 도입되고 있다. 특히 지연시간(Latency) 없이 와이어 스피드(Wire-speed)로 하드웨어 레벨 암호화를 수행하는 L1(물리 계층)의 OTN Security와 L2(데이터링크 계층)의 MACsec 기술이 해저케이블 시스템에 실질적으로 적용되고 있다. 핵심 전송장비 내 ASIC 칩셋에 구현된 강력한 AES-256 기반 회선 암호화를 거치면,

설령 물리적 침입이나 도청으로 광신호의 일부가 유출되더라도 공격자가 무의미한 암호문 외에 실제 데이터를 획득하는 것은 불가능하다. 더 나아가 미래의 양자컴퓨터 위협에 선제적으로 대응하기 위해, 양자내성암호(PQC) 프로토콜과 양자키분배(QKD) 기술을 연계한 차세대 '하이브리드 양자보안 네트워킹' 인프라 구축도 활발히 추진되고 있다.

4. 지정학적 리스크와 글로벌 해저케이블 다변화 전략

최근 해저케이블을 둘러싼 가장 위협적인 시나리오는 공해(公海)상에서 발생하는 하이브리드 위협(Hybrid Threat)이다. 대표적인 사례로 2023년 발트해에서 발생한 통신케이블 절단 사건과 최근 유럽 해역에서 빈발하는 의문의 해저 인프라 훼손 등이 있다. 이러한 공격들은 군사적 전면전이 아닌, 민간 선박의 닻이나 어구(漁具)를 이용한 사고로 위장하거나 귀속을 명확히 밝히기 어려운 '회색지대(Gray Zone)' 전략을 취하기 때문에 국제법적 대응이나 즉각적인 범인 특정에 한계가 있다.

여기에 특정 국가의 영해나 분쟁 소지가 있는 해역, 그리고 육양국과 연결되는 좁은 해협(동중국해, 남중국해, 대만해협, 말라카해협, 호르무즈해협, 홍해)에 해저케이블이 밀집되면서, 물리적 공격이나 인위적인 통제에 따른 취약성도 극대화되고 있다. 만약 핵심 길목의 육양국이나 해저케이블이 하이브리드 공격을 당할 경우, 단 한 번의 사고로도 국가 전체의 국제 연결성이 마비될 수 있다.

이 때문에 글로벌 빅테크 기업들과 선진국들은 보안 위험이 높은 분쟁 해역과 특정 지역을 우회하는 '케이블 노선 다변화(Topology Diversity)' 전략을 가속화하고 있다. 대표적인 추세가 미-중 갈등의 최전선이 된 남중국해를 피해 미국령 괌을 경유해 태평양을 직접 횡단하는 북미-동남아시아 직접 연결 프로젝트(Bifrost, Echo, Apricot 케이블 등)다. 이 프로젝트들은 미국 서부에서 구글, 메타 등이 주도하여 싱가포르, 인도네시아, 필리핀 등을 중국·홍콩 경유 없이 직결함으로써 지연시간을 단축하는 동시에 지정학적 리스크를 원천적으로 회피하는 공급망 분산의 핵심 모델로 자리 잡고 있다.

〈그림 3〉 Bifrost 해저케이블 망도

- 개통일 2025.12.
- 길 이 19,888km
- 소유자 Meta, Keppel T&T, Telin
- 공급사 ASN
- 육양지 Alupang, Guam
  Jakarta, Indonesia
  Manado, Indonesia
  Rosarito, Mexico
  Davao, Philippines
  Tuas, Singapore
  Grover Beach, USA
  Winema, USA

[출처] TeleGeography

이처럼 노선 다변화는 지정학적 위험을 분산하는 전략일 뿐 아니라, 장애 발생 시 국제 데이터 트래픽을 우회시켜 국가 디지털 서비스의 연속성을 확보하는 핵심적인 디지털 재난 대응 및 국가 네트워크 회복탄력성 확보 수단이다.

맺음말

지정학적 갈등과 사이버 위협이 복합화되는 환경에서 우리나라는 해저케이블을 국가 핵심 디지털 인프라이자 전략자산으로 인식하고, 국가 차원의 통합 대응 체계를 구축하기 위해 다음과 같은 정책을 추진해야 한다.

첫째, 해저케이블을 주요정보통신기반시설로 지정·보호하고, 동·서·남해안 육양국 분산과 국제 노선 다변화를 통해 글로벌 디지털 연결망의 보안성과 안정성을 강화해야 한다.

둘째, 민간 통신사업자 중심의 건설·운영 체계에 독립적인 기술감리와 정부 차원의 보안점검 체계를 도입·강화하여 공급망 공격과 내부자 위협에 선제적으로 대응해야 한다.

셋째, 해저케이블을 AI 데이터센터(AIDC)와 인터넷 교환센터(IX) 등 국가 디지털 인프라와 연계한 '국가 해저케이블 종합전략'을 수립하고, 이를 뒷받침할 법·제도와 통합 디지털 안보·재난 대응 체계를 마련해야 한다.

국제 해저케이블은 디지털 경제의 대동맥이자 국가 데이터 주권과 디지털 안보를 지키는 최전선이다. 국가 차원의 선제적·전략적 관리와 체계적인 투자를 통해 기술적·지정학적 위협에 철저히 대비하고, 어떠한 위기 상황에서도 끊김 없는 디지털 연결성을 확고히 확보해 나가야 할 것이다.

[참고문헌]

Carter, Lionel, Douglas Burnett, Stephen Drew, Graham Marle, Lonnie Hagadorn, Deborah Bartlett-McNeil, and Nigel Irvine. 2009.「Submarine Cables and the Oceans: Connecting the World」. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC.

TeleGeography. "Submarine Cable Frequently Asked Questions.

[저자 정보]

본 고의 저자는 육양국 구축, 케이블 시스템 운영·관리, 케이블 선박(세계로호) 확보, 기술 자립화, 국제유지보수협정 가입 등 해저케이블 산업 전반의 실무를 두루 거쳤으며, 북미·동남아·유럽에서 다수의 해저광케이블 프로젝트를 추진한 해저케이블 전문가입니다.(前)

02 이슈 보고서

KICI 디지털안전본부
박민지 선임연구원

AX 전환과 데이터센터 안정성 확보의 패러다임 쉬프트

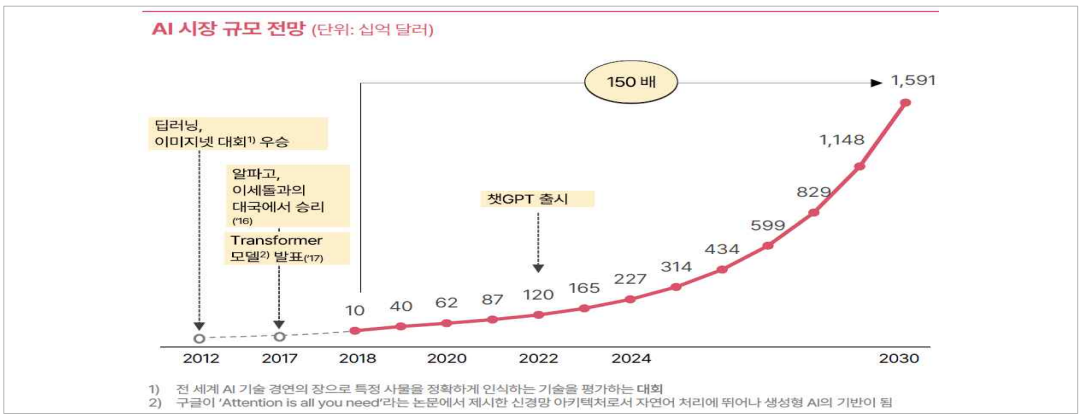
들어가며

인공지능 전환(AX, AI Transformation) 시대에 발맞춰 데이터센터(집적정보통신시설)의 역할이 단순한 정보 저장고를 넘어 대규모 AI 연산을 지원하는 인프라로 확대되고 있다. 생성형 AI의 확산으로 인해 데이터센터는 범용 CPU 중심에서 GPU 및 고대역폭 메모리(HBM, High Bandwidth Memory) 기반의 병렬 연산 구조로 변화하고 있으며, 하이퍼스케일과 엣지 데이터센터로 이원화되는 양상을 보인다. 이러한 고밀도·고전력 환경으로의 변화는 기존의 물리적, 전력망적 운영 방식을 뛰어넘는 새로운 차원의 안정성 확보 방안을 요구한다. 여기서는 AX 전환에 따른 데이터센터의 구조적 변화를 짚어보고, 이에 대응하기 위한 디지털서비스 제공 관점에서의 안정성 확보 방안(냉각 최적화, 전력 다중화 및 무탄소 에너지 연계, LLM 사이버 보안 거버넌스, 사회적 전력망 수용성)의 패러다임 전환 필요성을 논의하고자 한다.

1. 서론

2022년 챗GPT의 등장 이후 생성형 AI가 기업 업무와 개인의 일상에 빠르게 녹아들며 산업 전반에 걸쳐 큰 변화를 일으키고 있다. 전 세계 AI 시장 규모는 2018년 대비 2030년 150배 증가할 것으로 전망되며, 핵심 부품인 데이터센터용 AI 반도체 시장 역시 폭발적인 성장세를 보이고 있다.

〈그림 1〉 AI 시장 규모 전망



[출처] PwC Analysis (25.04.)

AI 기반 서비스는 기존의 디지털 서비스와 비교해 막대한 전력을 소모한다. 예컨대 구글 검색 1회에 0.3Wh의 전력이 소모되는 반면, 챗GPT의 경우 2.9Wh로 약 10배에 가까운 전력이 필요한데, 향후 챗GPT와 같은 AI 검색 기능이 구글 검색에 통합되면 한 번 검색에 필요한 전력량은 6.9~8.9Wh으로, 이는 기존 구글 검색 대비 많게는 30배에 달한다. 이러한 추세에 따라 전 세계 데이터센터 전력 소비량은 2026년 820TWh에 이를 예정이다. 이처럼 대규모 데이터를 실시간으로 처리해야 하는 AX 환경에서 데이터센터는 단순한 정보 저장고를 넘어 문명의 기반이 되는 필수 인프라로 그 역할이 격상되고 있다. 다만 현재 데이터센터의 운영과 관리에 대한 법률상 보호조치는 안정적인 전력공급에 치중되어 있다.

2. AX 전환에 따른 데이터센터의 역할 확대와 변화 양상

2.1 컴퓨터 고사양화 및 이원화

기존 데이터센터는 선형 처리 중심의 CPU 기반이었으나, 대규모 병렬 연산에 특화된 GPU 및 HBM 기반 인프라로 급격히 전환되었다. 이와 함께 대규모 AI 학습을 전담하는 하이퍼스케일 데이터센터와 실시간 저지연 처리를 위한 도심형 엣지 데이터센터로 역할이 이원화되고 있다.

〈그림 2〉 하이퍼스케일과 엣지 데이터센터 비교(재구성)

[출처] PwC Analysis (25.04.)

2.2 전력 밀도 급증과 냉각 시스템의 한계

AI 워크로드 특성상 GPU 서버의 랙(Rack)당 소비 전력은 과거 510kW 수준에서 50,100kW 이상으로 치솟았다. 이로 인해 기존의 공기를 이용한 공랭식(Air Cooling) 시스템은 열 포화점(Thermal Saturation Point)에 도달하여 더 이상 열을 제어할 수 없는 물리적 한계에 직면했다.

3. 디지털서비스 운영 안정성 확보 방안의 패러다임 변화

생성형 AI 시대에 고밀도 디지털서비스를 무중단으로 제공하기 위해서는 단순한 전원 백업을 넘어서는 다차원적인 측면에서 운영 안정성 혁신이 요구된다.

〈그림 3〉 데이터센터 주요구성요소의 변화양상(재구성)

[출처] PwC Analysis (25.04.)

3.1 물리적·환경적 안정성

우선 차세대 냉각 기술 및 AI 지능형 운영을 도입할 필요가 있다. 열 폭주를 막기 위해서는 다이렉트 투 칩(Direct-to-Chip)이나 서버 전체를 비전도성 액체에 담그는 액침냉각(Immersion Cooling)과 같은 차세대 액체냉각 기술의 도입이 필수적이다. 아울러 구글 딥마인드(DeepMind)가 AI 알고리즘을 적용해 실시간으로 반영된 온도와 전력 데이터를 통해 팬, 냉각 시스템, 창문 등 약 120개의 변수를 조정하는 적응형 시스템을 개발해 냉각 에너지를 40% 절감한 사례처럼 실시간으로 워크로드를 최적화하는 AI 기반 지능형 인프라 관리가 동반되어야 한다.

3.2 전력 계통 안정성

고효율 전력 변환과 무탄소 에너지(CFE, Carbon Free Energy)[1] 공급을 확보해야 한다. 데이터센터의 폭발적인 전력 수요를 감당하기 위해 전력 반도체(SiC/GaN) 기반 고효율 UPS와 수소연료전지의 도입을 고려할 필요가 있다. 더 나아가 글로벌 빅테크 기업들이 소형 모듈 원자로(SMR) 및 핵융합 기술에 투자하는 것처럼 상시 CFE 공급망을 선제적으로 확보하여 거시적인 전력 안정성을 꾀해야 한다.

1) 발전과정에서 탄소를 배출하지 않는 모든 에너지원으로 풍력, 태양광, 수력, 지열 등 재생에너지뿐만 아니라 탄소를 배출하지 않는 원자력발전, 연료전지 등을 수단에 포함

3.3 사이버 보안 안정성

대규모 언어 모델(LLM) 특화 위협에 대응하기 위해서는 제공되는 디지털서비스 자체의 무결성 확보도 중요하다. LLM은 환각(Hallucination)이나 적대적 공격(Adversarial Risk) 등 독특한 보안 취약점을 지닌다. 이에 대응하여 데이터센터 내 AI 모델에 대한 지속적인 검증(TEVV, Test, Evaluate, Verify, Validate)[2]을 의무화하고, 안전한 AI 거버넌스를 내재화해야 한다.

3.4 사회적 책임

데이터센터 밀집은 지역 전력망의 전압이 10~25% 낮아지는 브라운아웃(Brownout) 위험을 고조시키고 시민의 비용 부담을 가중시킬 수 있다. 이를 극복하기 위해 서버 냉각 시 발생하는 고온의 폐열을 인근 지역난방에 공급하는 폐열 회수 시스템을 구축하고, 데이터센터 내 에너지 저장 시스템(ESS, Energy Storage System)을 지역 전력망과 연계된 가상 발전소(VPP, Virtual Power Plant)[3]로 편입하여 지역사회와 공생하는 수용성을 확보해야 한다.

4. 결론

AX시대를 맞이하여 데이터센터는 단순한 IT 인프라를 넘어 국가와 기업의 AI 경쟁력을 좌우하는 AI 팩토리로 변모하고 있다. 급증하는 전력 소비와 발열을 동반하는 환경 속에서 안정적인 디지털서비스 제공을 위한 데이터센터의 안전관리는 새롭게 정의되어야 한다.

단순히 서버 중단 방지를 위한 정전을 막는 수준을 넘어 ① 액체냉각과 AI 자동화 기반의 물리·열적 안정성, ② 무탄소 에너지 중심의 전력 계통 안정성, ③ LLM 위협을 제어하는 AI 보안 거버넌스, ④ 폐열 회수 등 지역사회와의 공생을 통한 사회적 수용성을 포괄하는 다차원적 체계로 혁신을 고려해야 할 필요가 있다.

[참고문헌]

NIA, 디지털서비스 이슈리포트(2024, Vol.06) AI 시대 데이터 센터 트렌드와 주요이슈
PwC(2025.4), 생성형 AI 시대가 여는 새로운 AI 데이터센터 사업 기회
NIPA(2025.12), AI 인프라 고도화와지속가능한 데이터센터로의 전환

2) 수명 주기 전반에 걸쳐 모델의 성능, 안전성, 신뢰성을 객관적으로 평가하는 과정으로 테스트(Test), 평가(Evaluate), 검증 (Verify), 확인 (Validate)의 4단계로 구성
3) 태양광, 풍력, 에너지 저장장치(ESS), 전기차 등 전국에 흩어져 있는 소규모 분산 에너지 자원들을 정보통신기술(ICT)과 인공지능(AI)으로 통합하여, 마치 하나의 거대한 발전소처럼 관리하고 운영하는 시스템

03 전문가인터뷰

숭실대학교 재난안전관리학과
김덕호 교수

숭실대학교 재난관리학과 김덕호 교수님을 만나다.

Q 우선 김덕호 교수님에 대해 소개 부탁드립니다.

A 안녕하세요. 저는 숭실대학교 일반대학원 재난안전관리학과 김덕호 겸임교수입니다. 저는 기업 부설 연구소에서 R&D IT Infra 관리와 정보보안을 포함한 Risk .Management, 제조현장의 DX 프로젝트를 수행하였습니다. 현재는 대학원에서 재난관리와 BCMS 강의하고 있습니다. 또한 사업연속성 및 재난 분야가 워낙 다양한 분야에서 학술적 논의가 필요한 학문인 만큼 지속적으로 연구하고 있습니다. 특히 사회과학 측면에서 현시대의 특성상 디지털 서비스 관련한 사회적 이슈를 빼놓을 수 없는데, 저는 이 중 디지털 재난과 디지털 서비스 연속성을 주제로 학술활동을 병행하고 있습니다.

Q 디지털 재난·장애의 안전관리와 관련된 업무·연구 경험이 있으시다면 말씀해주시기 바랍니다.

A 저는 24년부터 현재까지 약 3년간 부가통신사업자의 통신재난관리계획 수립과 이행 점검에 외부 전문가로 참여하고 있습니다.

점검에서는 각 기업별 통신재난관리계획에서 부족한 부분을 개선할 수 있는 방안에 대한 제언을 하고 있습니다. 시행이후 연차가 쌓일수록 디지털 서비스 연속성 관점에서 체계가 고도화되며 전년도의 지적사항이 개선되고 있는 점에 대해서는 전문가로서 뿌듯함을 느끼고 있습니다. 다만, 아직 연속성을 위한 RA(Risk Assessment)나 BIA(Business Impact Analysis)등 BCMS의 현장적용 방법론의 이해부족, 디지털 재난 발생 시 디지털 서비스 공급자로서 공공의 역할의식은 아직 한계로서 남아있다고 생각합니다. 이러한 아쉬운 부분에 대해서는 사회과학을 연구하는 연구자로서 책임을 통감하고 디지털 서비스 연속성 관점에서 학술연구를 진행하고 있습니다.

Q 재난안전관리학 관점에서 '디지털 재난'을 어떻게 정의하고 계시는지, 디지털 재난이 기존의 자연재난·사회재난과 비교했을 때 가장 큰 차이는 무엇인지 말씀 부탁드립니다.

A 김현의원 등(2026)이 발의한 「디지털 재난안전 관리법안」이 제안하고 있는 '디지털 재난'의 정의를 보면 '「재난 및 안전관리 기본법」에 따른 재난 또는 「자연재해대책법」에 따른 재해 또는 그 밖에 물리적·기능적 결함, 트래픽 양의 과도한 변동 또는 전송 속도 저하 등 장애·중단에 따라 정보통신서비스의 제공과 집적정보통신시설의 운영·관리가 원활하지 않은 상태'로 규정하고 있습니다.

문헌을 찾아보면 '디지털 재난'의 개념은 IT가 사회전반에 확산되는 1990년대 후반부터 사용되었으며 2000년대부터 디지털 재난이 정의되기 시작합니다. 이 과정에서 디지털 재난을 예측하고 예방하는 의미로 '디지털 위험(Digital Risk) 관리'가 언급됩니다. 초기에는 사이버침해 및 사이버테러, 인터넷 침해 등 외부의 위협을 그 주요 원인으로 보는 경향이 있었으나 점차 다양한 사고의 유형과 광범위한 피해를 경험하며 그 의미가 변화하는 것을 알 수 있습니다. 그리고 디지털 재난의 성격을 국가 핵심 기반 마비나 행정정보시스템 장애 등 디지털 인프라의 중단으로 국민 생활과 국가 기능에 중대한 지장을 초래하는 사회재난으로 보아야 한다는 주장과 자연재난 및 사회재난 위에 겹쳐 나타나는 복합재난으로 보아야 한다는 주장도 확인할 수 있습니다. 그러나 아직 일반화를 위한 학술적 논의가 충분하다고 볼 수 없고 「디지털 재난안전 관리법안」 발의 과정에서도 이러한 디지털 재난을 정의하기 위한 노력이 추가적으로 필요하다고 보여집니다.

재난안전관리학의 근간인 연속성 관점에서 디지털 재난을 논의하자면, 연속성은 재난 발생과 관련한 활동을 예방·대비·대응·복구의 네 단계로 구분하여, 재난 발생의 전주기적 관리(Framework)를 강조하고 있습니다. 이러한 전주기 관점은 물리적 자연재난 및 사회재난뿐 아니라 정보통신 인프라와 디지털 서비스에 기반한 현대적 재난 유형에도 동일하게 적용될 수 있으며, 디지털 재난은 조직의 핵심 업무가 의존하고 있는 정보통신 인프라(네트워크, 데이터센터, 플랫폼 등)와 디지털 서비스(인증, 결제, 메신저, 클라우드 등)에 중대한 장애가 발생한 상황으로 업무가 중단된 상황으로 볼 수 있습니다. 상황에 따라 사전에 설정된 복구목표시간(RTO)과 복구목표시점(RPO)을 위협하고, 다수 핵심 프로세스의 연속성을 동시에 저해하는 재난 유형으로 개념화할 수 있을 것입니다.

따라서 기존의 자연재난과 사회재난과 비교했을 때 자연재난·사회재난은 물리적 자산과 인력, 사회 시스템에 직접적인 피해를 주는 경우로 이해 될 수 있지만, 디지털 재난은 눈에 보이지 않는 네트워크·플랫폼 레이어에서 발생하면서도 BCMS에서 식별한 '핵심 프로세스' 전체를 동시에 중단시키는 특징이 있다고 보고 있습니다. 즉 자연재난은 물리 인프라 중심, 사회재난은 사회·조직 시스템 중심의 충격이라면, 디지털 재난은 '정보·서비스 인프라 재난'으로서 이 둘 위에 겹쳐지는 것이 특징으로 보여집니다.

Q 디지털 서비스 관점에서의 '업무 연속성'에 대한 전반적인 설명을 부탁드립니다.

A 디지털 서비스 관점에서 업무 연속성이란 재난이나 장애가 발생하더라도 조직의 핵심 디지털 서비스가 허용 가능한 수준의 시간과 품질 안에서 유지되거나, 사전에 정의된 목표 시간 내에 복구될 수 있도록 예방-대비-대응-복구 활동을 통해 재난을 관리하는 능력이라고 이해할 수 있습니다. 이를 체계적으로 다루는 관리 프레임이 바로 비즈니스 연속성 경영 시스템, 즉 BCMS(Business Continuity Management System)입니다. BCMS에서는 위험평가(Risk Assessment)를 통해 사이버 공격, 시스템 장애, 데이터센터 사고, 외부 인증·결제 인프라 장애 같은 디지털 재난 요인을 식별하고, 각 요인의 발생 가능성과 영향도를 분석합니다. 또한 비즈니스영향분석(Business Impact Analysis, BIA)을 수행해 위험평가에서 분석된 위험상황에 따라 어떤 서비스가 조직과 사회에 '중요 서비스(Critical Service)'인지, 중단 시 얼마 동안까지 버틸 수 있는지 등을 결정합니다.

이 결과를 바탕으로 복구목표시간(RTO)과 복구목표시점(RPO)을 설정하고, 실제로 장애가 발생했을 때 어떤 순서와 전략으로 서비스를 복구할지 시나리오를 설계합니다. 예를 들어 금융 결제, 대규모 인증·로그인 인프라처럼 사회적 파급력이 큰 서비스는 BIA에서 '우선 복구 대상'으로 분류되고, RTO를 매우 짧게 설정하게 됩니다. 따라서 이들 서비스에 대해서는 데이터센터와 네트워크를 이중화하거나, 다른 인증·결제 수단을 준비해 두는 등 고가용성(High Availability) 구조와 대체 경로를 BCMS 차원에서 설계합니다. 반대로 상대적으로 중요도가 낮고 일시 중단을 허용할 수 있는 내부 관리 시스템은 조금 더 긴 RTO를 설정하고, 비용·효과를 고려해 복구 전략을 차별화할 수 있습니다.

결론적으로 디지털 서비스 업무 연속성은 '장애를 절대 발생시키지 않겠다'는 약속이 아니라 위험을 과학적으로 평가하고(RA), 그 위험이 핵심 서비스와 이용자에게 미치는 영향을 분석한 뒤(BIA), 사회적으로 중요한 서비스가 먼저, 정의된 수준과 시간 안에서 유지·복구될 수 있도록 BCMS를 통해 구조적으로 준비해 두는 활동이라고 볼 수 있겠습니다.

Q 디지털 재난·장애가 발생할 경우, 사회적 파급력이나 이용자에게 미치는 영향력이 큰 서비스에는 어떤 것이 있을까요?

A 제가 부가통신서비스사업자 통신재난관리계획 이행 점검을 하며 느낀 것은 부가통신서비스사업자가 제공하는 디지털 서비스의 공공의 역할이었습니다. 정부가 제공하는 행정서비스와 같은 공공서비스와 마찬가지로 부가통신서비스사업자도 공공의 역할을 하고 있다고 봅니다. 예를 들면 카카오나 네이버가 제공하고 있는 개인인증 시스템, 네이버 페이나 삼성페이가 제공하는 페이 결제 서비스와 그 외 메신저 등은 없어서는 안 될 중요 디지털 서비스입니다. 이러한 여러 영역에서 민간이 제공하는 서비스도 디지털 서비스 중단 사태가 발생하였을 경우 사회적으로 많은 문제가 야기된다고 생각합니다. 이러한 서비스들은 조직·산업·사회 전체의 핵심 업무에 다수 연결되어 있는 '공통 인프라 서비스'로 상호 의존 대상이 될 수 있기 때문에, 장애 발생 시 복수 조직의 업무 연속성을 동시에 위협하기 때문에 그 영향력이 크다고 볼 수 있습니다.

Q 지난 2월 '디지털재난안전관리법 제정을 위한 전문가 간담회'가 개최되었는데요. 방송통신발전기본법·전기통신사업법·정보통신망법 등 디지털 안전3법을 하나로 통합하는 것이 재난관리 실효성 측면에서 어떠한 의미가 있다고 생각하시나요?

A 디지털 안전 3법을 하나의 「디지털 재난안전 관리법」으로 통합하려는 시도는 재난관리 측면, 즉 예방-대비-대응-복구를 법·제도 수준에서 뒷받침하는 공통 프레임을 만든다는 점에서 의미가 크다고 봅니다. BCMS는 조직 차원의 자발적·표준 기반 관리체계이지만, '제2조(정의) 2의 "디지털 안전관리"란 "디지털 재난의 예방·대비·대응 및 복구와 관련된 모든 활동을 말한다.'와 같이 BCMS를 적용해서 디지털 재난관리가 될 수 있다면 국가 차원에서 디지털 재난을 '업무 연속성 관점의 재난'으로 인식하고, 핵심 서비스와 인프라에 최소한의 연속성 요구사항을 제시할 수 있게 된다고 봅니다.

또한 파편화된 규제를 통합하면, 사업자 입장에서는 디지털 재난 관련 요구사항을 BCMS에 일괄 반영할 수 있어 효율성이 높아질 것으로 보여집니다. 예를 들어, 재난 관리 의무 대상 여부, 보고·복구 계획 수립 의무, 비상대응 조직 구성 요구 등을 통합 법에서 제시하면, 조직은 이를 기준으로 BCMS 내 위험평가와 비즈니스영향분석을 수행하고, 정책·절차·훈련을 표준화할 수 있어 효과적인 디지털 재난관리를 수행 할 수 있을 것으로 기대됩니다.

Q 카카오톡 인증 기능처럼 하나의 서비스 장애가 다른 다수의 서비스에 연쇄적으로 영향을 미치는 사례가 반복되고 있습니다. 이러한 '디지털 인프라의 연쇄성'을 재난관리 체계에서 어떻게 다뤄야 할까요?

A 카카오톡의 인증 장애는 하나의 서비스 장애가 다수의 서비스에 연쇄적으로 영향을 미치는 현상으로, BCMS에서 말하는 '상호의존성(Interdependency)' 문제의 전형적인 예로 볼 수 있습니다. 재난관리 체계에서는 이런 디지털 인프라의 연쇄성을 파악하기 위해, 서비스 간 의존 관계를 '업무 연속성 다이어그램'이나 '서비스 맵' 형태로 시각화하는 작업이 필요하다고 하겠습니다. 업무 영향 분석(BIA) 시, 업무간 상호의존성, 시스템/인프라 의존성 고려하여 내부 시스템뿐만 아니라 외부 디지털 인프라에 대한 의존도를 전수 조사하고 시각화(Mapping)해야 합니다. 이를 통해 하나의 링크가 끊어졌을 때의 영향을 받는 파급 범위를 미리 인지할 수 있어야 합니다. 그리고 상호의존성을 시각화 하는 작업에 머무르지 않고 넷플릭스에서 시행하고 있는 '카오스 엔지니어링' 기법처럼 의도적으로 카카오 인증 API 연결을 끊어버리는 재난 시뮬레이션 수행을 통해 상호의존성을 점검하고 시스템이 자동으로 우회 경로를 찾는지, 사용자에게 올바른 에러 메시지를 띄우는지 실전처럼 검증하는 모의훈련의 체계를 갖추는 것도 필요하다고 보여집니다.

Q 당월 7일부터 정보통신망법 개정안이 시행되면서 업계에도 혼란이 예상되는데요. 이번 정보통신망법 개정안이 디지털 재난 관리 체계에 어떤 영향을 미칠 것으로 예상하시는지 궁금합니다.

A 정책브리핑에서 정부는 개정 정보통신망법을 통해 "대규모 정보통신서비스 제공자의 신고접수 의무화 및 사업자 책임 강화"를 명시하며, 불법·허위조작정보 신고·접수·조치·통지 체계를 갖추도록 요구하고 있습니다. 디지털 재난 체계에서 보면 기존의 "서비스 중단·물리 인프라 장애" 뿐 아니라 "허위조작·혐오·선동 정보로 인한 사회적 혼란, 평판 붕괴, 집단 행동 왜곡" 또한 디지털 재난의 한 범주로 보고 대응해야 할 것으로 보여집니다. 사회혼란을 야기하는 정보의 생성자 뿐만 아니라 정보를 제공하는 상호의존성 관점에서 어떠한 부분에 영향을 미치는지를 파악하는 것이 중요하다고 생각되며 이러한 것들이 디지털 재난 관리 체계에 예방-대비-대응-복구 측면에서도 고려되어야 한다고 봅니다.

Q 마지막으로, 앞으로의 디지털 재난관리 체계는 어떤 방향으로 나아가야 할지 말씀 부탁드립니다.

A 디지털 재난관리 체계를 위해 두 가지 축을 강화하는 방향으로 나아가야 한다고 생각합니다.

첫 번째 축은 재난관리 측면에서 예방·대비·대응·복구의 전주기 관점을 디지털 재난에 본격적으로 적용하고, 이를 BCMS와 연계하는 것입니다. 지금까지는 자연재난·사회재난에 비해 디지털 재난을 상대적으로 '기술 장애' 수준으로 보는 경향이 있었지만, 디지털 재난이 조직의 핵심 프로세스와 사회 시스템의 연속성을 직접 위협하는 만큼 국가와 조직 차원에서 디지털 재난을 전주기적으로 관리하는 프레임을 분명히 할 필요가 있습니다.

두 번째 축은 법·제도와 BCMS의 정합성을 높이는 것입니다. 「디지털 재난안전 관리법」 제정 논의나 「정보통신망법」 개정처럼, 디지털 안전 3법을 통합하고 재난관리 의무를 명확히 하는 입법 흐름은 분명 긍정적인 방향이라고 봅니다. 다만 법·제도에서 요구하는 디지털 재난 예방·대비·대응·복구 활동이 실제 현장의 BCMS와 어떻게 연결될 것인지, RA와 BIA, RTO/RPO 설정, 비상조직 운영, 모의훈련 체계 등과 구체적으로 어떻게 매핑될 것인지까지 같이 논의되어야 제도와 실무 간 괴리가 발생하지 않습니다. 이러한 관점에서 국가가 제시하는 기준과 가이드라인을 토대로, 각 조직이 BCMS를 통해 자율성과 책임을 함께 확보하는 구조가 중요합니다.

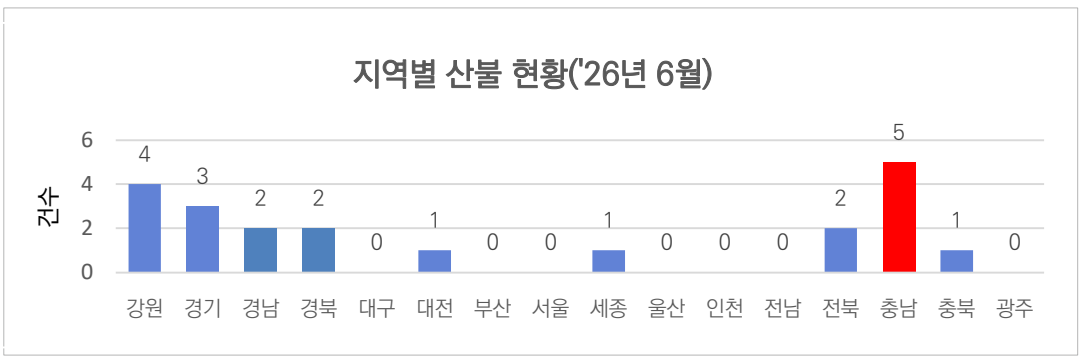
이러한 축을 통해 기술적인 고가용성과 인프라 복원력을 확보하고 중단없는 공공서비스 제공을 수행하여 디지털 재난시 회복탄력성을 높이는 방향으로 디지털 재난 체계를 구축해야한다고 생각합니다.

04 디지털 안전 관제 이슈

6월 발생 이슈

화재	• 2026.06.01. SK 하이닉스 청주공장 화재	
	• 2026.06.01. 대전 한화 에어로스페이스 폭발 사고	
	• 2026.06.13. 경기 용인 처인구 원삼면 고당리 185-3 공장 화재 * 소방대응 1단계 발령	
	• 2026.06.13. 경북 고령군 운수면 팔산리 499-2 전신주 화재	
	• 2026.06.15. 서울 도봉구 도봉로 618 화재	
	• 2026.06.21. 광주 광산구 송촌동 290 공장 화재 * 소방대응 1단계 발령	
	• 2026.06.27. 경기 시흥시 대야동 253-1번지 화재	
지진	• 2026.06.08. 경남 통영시 해역 2.9 지진	
정전	• 2026.06.08. 대전 대덕산업단지 정전	
	• 2026.06.11. 충북 청주시 청원구 내덕2동 일대 정전	
	• 2026.06.19. 경기 연천읍 옥상리 인근 정전	
	• 2026.06.25. 경기 안산시 선부동 131-1, 원곡동 993-7 일대 등 정전	
가스 유출	• 2026.06.16. 지하철 6호선 안암역 이산화탄소 가스 유출	
대규모 인파	• 2026.06.19.	광화문 월드컵 응원 대규모 인파 밀집 및 6/29(금) 광화문 일대 도로 통제
	• 2026.06.25.	

재난유형	일시	주요내용 (과기정통부 보고)
산불	6월 中 21건 보고 (기간통신 재난대응 보고)	• 산불대비·피해상황 보고 • 통신사 피해 없음 확인 • 통신마비 대비 상황보고 • 정부-사업자간 허브 역할 수행 • 지속 모니터링 실시



04 디지털 안전 관제 이슈

기간 / 부가 / IDC 부문 장애 대응

01 2026.06.04., 2026.06.12.

- 네이버 일부 안드로이드 유저 네이버페이 이용 불가 오류

02 2026.06.12.

- 인스타그램 및 페이스북 서비스(게시글, 로그인 등) 오류

03 2026.06.22.

- 트위터(X) 검색 오류장애

04 2026.06.26.

- 토스 포스(POS) 결제 장애 오류

05 2026.06.30.

- 카카오페이증권 서비스 접속 오류

05 Digital Safety Inside

2026년도 통화량 급증 예상 달력 (8~9월)

8월(August)

일	월	화	수	목	금	토
특이사항						1 o 싸이흠뻑쇼-수원 (수원, 8/1~8/2) o 스트레이키즈 콘서트 (서울, 8/1~8/2) o 2026 인천펜타포트 락 페스티벌(8/1~8/2) o 보이넥스트도어 콘서트 (부산, 8/1~8/2)
2	3	4	5 o 홍천강 별빛음악 맥주 축제(홍천, 8/5~8/9)	6	7 o 밀양 수퍼 페스티벌 (밀양, 8/7~8/9) o 에스파 콘서트 (서울, 8/7~8/8)	8 o 싸이흠뻑쇼-광주 o 워터밤 부산 o 오피셜히게단디즘 콘서트(서울, 8/8~8/9)
9	10	11	12 o 통영한산대첩축제 (통영, 8/12~8/16)	13	14 o 강릉 국가유산 야행 (강릉, 8/14~8/16) o 김천포도축제 (김천, 8/14~8/16)	15 광복절 o 싸이흠뻑쇼-부산 (부산, 8/15~8/16)
16	17 대체공휴일	18	19	20 o K-일러스트레이션페어 (마곡, 8/20~8/23)	21 o 빅뱅 콘서트 (고양, 8/21~8/23)	22 o 싸이흠뻑쇼-대전 (대전, 8/22~8/23) o 카스쿨 페스티벌 (과천, 8/22)
23	24	25	26	27	28	29 o Sustainable Wave Festival (인천, 8/29~8/30)
30	31					

9월(September)

일	월	화	수	목	금	토
		1 o 2학기 개학식	2	3	4 o 평창효석문화제 (평창, 9/4~9/13) o 무주반딧불축제 (무주, 9/4~9/12) o 임영웅 콘서트 (고양, 9/4~9/6)	5
5	7	8 o 오피셜히게단디즘 콘서트(서울, 8/8~8/9)	9	10 o 장수한우랑사과랑축제 (장수군, 9/10~9/13)	11	12 o 플레이브 콘서트 (인천, 9/12~9/13)
13	14	15	16	17	18 o 진안홍삼축제 (진안, 9/18~9/20) o 시흥갯골축제 (시흥, 9/18~9/20) o 부천국제만화축제 (부천, 9/18~9/20) o 영광불갑산상사화축제 (영광, 9/18~9/27)	19 o 2026 아시아 탑 아티스트 페스티벌(서울 9/19-9/20)
20	21	22 o 경남고성공룡세계엑스포(고성 9/22~11/1)	23	24 추석연휴 o 안동국제탈춤페스티벌 (안동, 9/24~10/4)	25 추석	26 추석연휴
27	28	29	30	특이사항 o 세계 불꽃축제 예상 (서울, 9월말) o 서리풀뮤직페스티벌 예상 (서울, 9월말)		

KICI Digital Safety Report 원고 공모

한국정보통신산업연구원에서는 'KICI Digital Safety Report'에 게재할 디지털 재난·장애 관련 원고를 모집하고 있습니다. 해당 분야의 전문가 분들의 많은 관심과 참여 바랍니다.

01 원고 주제

- **디지털(통신) 재난·장애(기간통신, 부가통신, 데이터센터 등)**
  ※ 제목, 목차 등은 자율 기재

02 제출 자격

- **원고 모집 분야의 전문가**

03 접수 기간

- **수시 접수**

04 원고 양식 및 분량

- **한글 파일 4장 내외 분량**
  (글자크기 12, 줄간격 160%, 그림, 표 등 출처 포함)

05 기타

- **게재된 원고에 대하여 소정의 원고료 지급(최대 40만 원)**
- **게재된 원고로 인하여 지적재산권 침해문제 등이 발생할 경우, 원고저자는 원고료 반환, 게시물 삭제 및 한국정보통신산업연구원이 입게 될 손실 및 비용에 대한 배상 등 불이익을 받을 수 있습니다.**

06 제출 및 문의처

- **한국정보통신산업연구원 디지털안전본부 KICI Digital Safeyt Report 담당**
- **Tel : 070-4149-3469 / E-mail : jjdaeun29@kici.re.kr**

KICI 한국정보통신산업연구원

경기도 수원시 장안구 하률로 12번길80(천천동)

TEL.031-231-3400 FAX.031-269-5210

www.kici.re.kr