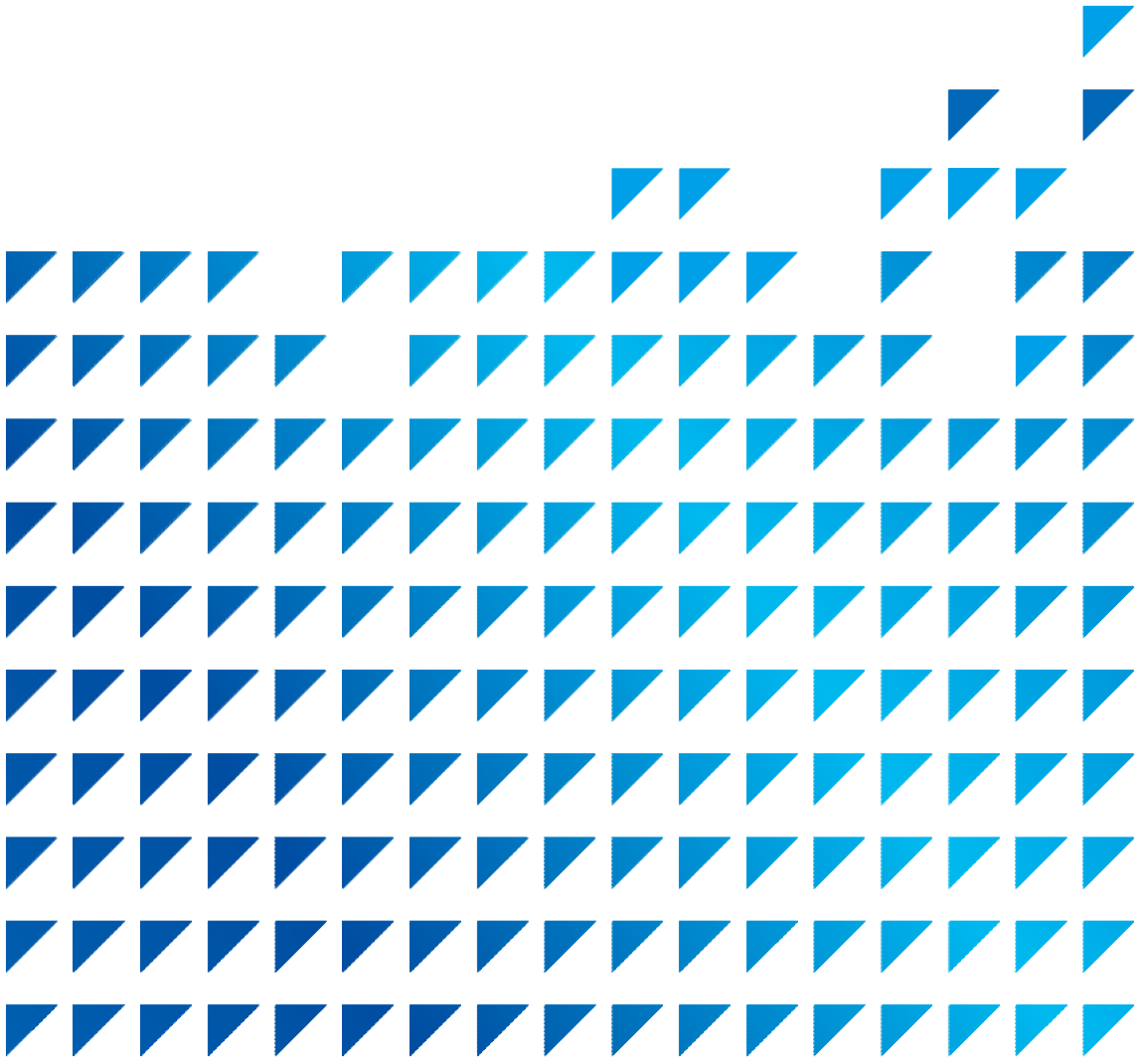
KICI DSR Vol. 26-06

한국정보통신산업연구원

Digital Safety Report

6월호



KICI 한국정보통신산업연구원

KICI 한국정보통신산업연구원

한국정보통신산업연구원

Digital Safety Report 6월호

Contents

01 전문가 칼럼

삼성 SDS
안치준 프로 / 기업재난관리사

디지털 재난에 대비한 데이터센터 회복력, 어떻게 검증할 것인가

I 단일장애점은 설비뿐 아니라 의사결정에도 존재한다

최근 생성형 AI와 클라우드 이용이 확대되고 대규모 데이터 처리 수요가 증가하면서, 데이터센터는 금융거래, 통신, 공공행정, 온라인 유통 등 국민 생활과 밀접한 디지털 서비스를 뒷받침하는 핵심 인프라로 자리 잡았다. 그만큼 데이터센터의 장애는 개별 사업자의 운영 중단에 그치지 않고, 다수 이용자에게 영향을 미치는 광범위한 서비스 장애로 이어질 수 있다.

2022년 판교 데이터센터 화재는 이러한 위험을 보여준 대표적 사례다. 지하 배터리실 화재와 전력 차단으로 다수의 서버가 동시에 정지했고, 핵심 기능과 운영도구의 특정 센터 집중, 미흡한 재해복구 체계는 서비스 복구를 지연시켰다.

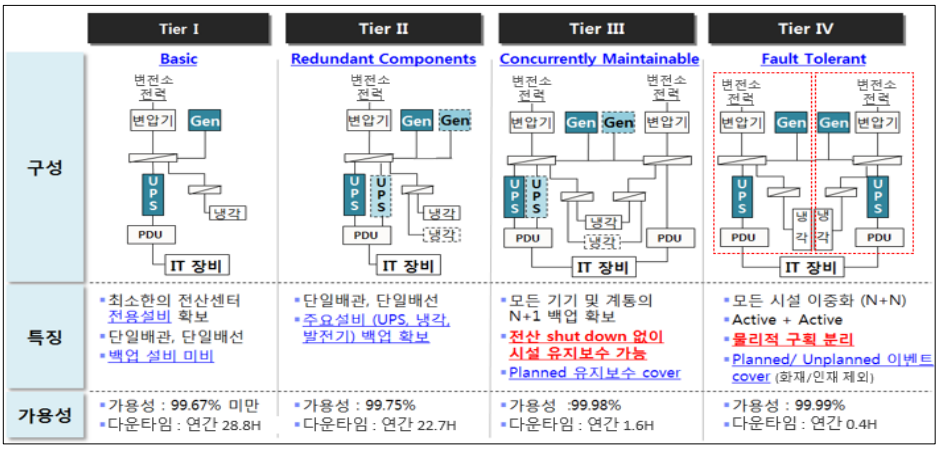
이 사고가 보여준 단일장애점(Single Point of Failure, SPOF)은 설비에만 존재하지 않는다. 재난 선언, 전력 차단 범위, 서비스 전환 등의 권한이 특정 조직이나 인력에 집중되거나, 의사결정 기준과 대체 책임자가 불명확하고 정보공유가 지연되면 이중화 설비와 재해복구(Disaster Recovery, DR) 체계도 제때 작동하기 어렵다. 따라서 데이터센터 재난관리는 인명안전을 최우선으로 하되, 시설 가용성, IT 시스템 복구와 고객 서비스 정상화를 하나의 흐름으로 관리해야 한다. 또한 설비뿐 아니라 조직체계, 의사결정 권한과 절차, 핵심인력, 정보공유 체계에 존재하는 단일장애점까지 사전에 식별하고 보완하는 업무연속성(Business Continuity Management System, BCMS) 기반의 재난관리체계가 필요하다.

II 설비 이중화를 넘어 서비스 전체의 복원력까지

미국 Uptime Institute의 Tier 분류는 전력·냉각 기반시설의 용량 구성요소와 분배경로를 기준으로 예비 용량과 이중화, 동시 유지보수 가능성 및 장애 허용 능력을 평가해 데이터센터를 Tier I부터 Tier IV까지 등급화하는 체계다. 그러나 높은 Tier 등급이 곧 서비스 연속성을 의미하는 것은 아니다.

고객 서비스의 연속성은 전력·냉각설비뿐 아니라 서버와 스토리지, 애플리케이션, 데이터, 통신망, 인증 체계, 운영도구 등 서비스 제공에 필요한 요소가 함께 작동할 때 확보된다. 따라서 이중화 여부도 개별 장비의 수량이 아니라 서비스 전체의 의존관계를 기준으로 판단해야 한다.

〈그림 1〉 데이터센터 가용성 수준(Tier Classification)



예를 들어 메인센터의 데이터를 백업센터에 복제했더라도 두 센터가 동일한 통신망이나 인증체계, 운영도구에 의존한다면 하나의 장애가 양쪽 센터에 동시에 영향을 줄 수도 있다.

이중화를 무력화하는 대표적인 위험은 공통원인고장(Common Cause Failure, CCF)이다. 이는 하나의 원인으로 서로 독립돼 있다고 여겨진 복수의 설비나 시스템이 동시에 기능을 상실하는 것을 말한다. 예를 들어 A·B 전원 계통이 동일한 방화구획이나 케이블 경로를 공유하면 화재나 침수로 두 계통이 동시에 영향을 받을 수 있다. 메인 센터와 백업 센터가 동일한 소프트웨어, 통신망 또는 제어체계에 의존하는 경우에도 하나의 장애가 양쪽으로 확산될 수 있다. 따라서 실질적인 이중화를 확보하려면 장비를 추가하는 데 그치지 않고, 서비스 전 과정에 남아 있는 공통 의존요소를 식별해 물리적·논리적으로 분리해야 한다.

최근 고밀도 AI 서버의 확산은 데이터센터 냉각계통의 구성과 운영을 더욱 복잡하게 만들고 있다. 직접 액체냉각(Direct Liquid Cooling, DLC)의 도입이 확대되면서 냉각수 분배장치(Coolant Distribution Units ,CDU), 매니폴드, 펌프, 열교환기, 배관, 누수감지장치 및 제어전원 등 새로운 설비와 의존요소가 늘어나고 있다. 이들 설비가 동일한 전원이나 제어계통에 의존할 경우 냉각계통 자체가 새로운 단일장애점이 될 수 있다. 따라서 기존 공랭식 설비와 새롭게 도입되는 액체냉각 설비를 하나의 냉각체계로 보고, 새로운 장애시나리오를 구축하고 비상운전 가능시간과 설비 전환·복구시간을 재산정해야 한다. 또한 그 결과를 IT 시스템의 안전한 종료·전환 시간과 고객 서비스의 목표복구시간에 연계하여 설계하고, 실제 장애 시나리오에 따른 테스트를 통해 검증해야 한다.

결론적으로 데이터센터의 이중화와 복구체계는 개별 설비가 아니라 서비스 전체의 복구 가능성을 기준으로 설계하고 검증해야 한다.

III 복구의 출발점은 현황 파악과 의사결정 권한

앞서 살펴본 판교 데이터센터 화재는 운영도구와 서비스 전환체계의 취약성이 복구를 지연시킬 수 있음을 보여줬다. 2025년 국가정보자원관리원 대전 본원 화재에서도 재난 초기에는 장애 시스템이 647개로 집계됐으나, 통합운영관리시스템의 데이터가 복구되고 전체 목록을 다시 확인한 뒤 709개로 정정됐다. 복구해야 할 시스템의 범위와 수량을 초기 단계에서 정확히 확인하지 못한 것이다. 전체 시스템을 복구하기까지 무려 95일이 소요되었다.

이 사례는 복구 대상과 우선순위, 시스템 간 의존관계 및 담당 책임을 파악할 수 있는 정보가 단순한 관리 자료가 아니라 복구계획을 수립하고 실행하는 핵심 자원임을 보여준다. 이러한 정보가 정확하지 않으면 필요한 장비와 인력, 대체센터의 수용 용량을 산정하기 어렵고, 복구 순서와 예상 복구시점도 신뢰성 있게 결정할 수 없다.

백업 데이터가 존재하더라도 어떤 서비스와 시스템이 영향을 받았으며, 다른 시스템과 어떻게 연결돼 있는지 파악하지 못하면 실제 서비스 복구로 이어지기 어렵다. 따라서 서비스·시스템 목록, 중요도, 의존관계, 담당 부서와 책임자, 복구목표 및 진행현황을 통합적으로 관리해야 한다. 이 정보는 주 운영시스템과 동일한 장애 영역에만 저장하지 말고, 재난 상황에서도 독립적으로 조회하고 최신성을 검증할 수 있도록 별도의 시스템이나 대체 수단으로 확보해야 한다.

정확한 현황이 확보된 뒤에는 이를 바탕으로 의사결정 권한이 작동해야 한다. 재난 선언, 전력 차단 범위, 서비스 전환과 복구 우선순위를 결정할 권한 및 대체 의사결정자를 사전에 지정하고 반복적으로 훈련해야 한다. 핵심 정보와 의사결정 권한, 대체 인력이 하나의 사고로 동시에 기능을 잃지 않도록 분리하는 것은 설비 이중화와 함께 갖춰야 할 운영체계 차원의 이중화다.

IV 준비를 성과로 연결하는 조직 대응 역량

재난에 대비해 지침·매뉴얼, 협력체계, 자원과 교육훈련을 갖추는 것은 중요하다. 그러나 이러한 요소가 실제 대응과 성과로 이어지려면 재난 발생 시 조직간 정보를 공유하고 역할과 자원을 조정하며, 공통된 기준에 따라 판단하고 행동할 수 있어야 한다. 필자는 이러한 능력을 '조직대응역량'으로 보고, 재난안전인식과 재난관리시스템이 조직의 성과로 이어지는 과정에서 어떤 역할을 하는지 실증적으로 분석했다.

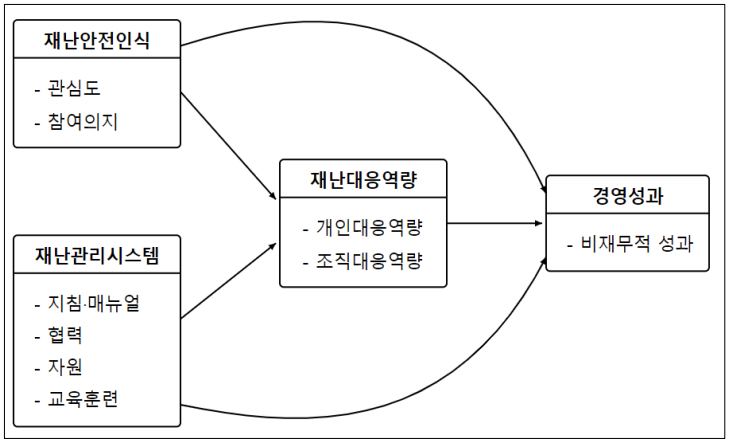
본 연구는 국내 IT서비스 기업이 보유·운영하는 5개 데이터센터 종사자 328명을 대상으로 진행했다. 재난안전인식은 관심도와 참여의지로, 재난관리시스템은 지침·매뉴얼, 협력, 자원, 교육훈련으로 구분했다. 이를 바탕으로 재난안전인식과 재난관리시스템이 비재무적 경영성과에 미치는 영향과, 그 과정에서 개인 및 조직의 대응역량이 어떤 역할을 하는지를 검증했다. 비재무적 경영성과는 경쟁우위 확보, 품질향상, 기업이미지 향상과 고객만족으로 측정하였다. 분석 결과, 조직대응역량은 관심도, 참여의지, 지침·매뉴얼, 자원, 교육훈련과 비재무적

경영성과의 관계를 매개하는 것으로 나타났다. 이는 이러한 요인들이 조직의 공동 대응능력으로 전환될 때 성과로 이어질 수 있음을 보여준다. 반면 협력은 조직대응역량을 통한 간접효과보다 비재무적 경영성과에 대한 직접효과가 유의하게 나타났으며, 개인대응역량을 통한 간접효과는 통계적으로 유의하지 않았다.

이 결과를 개인의 지식과 숙련이 중요하지 않다는 의미로 해석해서는 안 된다. 다만 개인이 보유한 역량만으로는 조직 전체의 성과로 연결되기 어려우며, 이를 공통된 판단기준과 역할분담, 정보공유, 자원동원 및 협업절차 속에서 작동하게 하는 조직 차원의 대응역량이 중요하다는 점을 시사한다. 특히 교육훈련은 조직대응역량을 통한 간접효과가 가장 크게 나타났다.

따라서 교육훈련은 단순한 지식 전달이나 매뉴얼 숙지에 머물러서는 안 된다. 누가 재난을 선언하고, 어떤 기준으로 설비를 차단하거나 서비스를 전환하며, 누가 복구 우선순위를 결정하는지를 실제 상황과 유사한 조건에서 반복적으로 확인해야 한다. 재난안전인식과 지침·매뉴얼, 자원, 교육훈련 등의 관리요소가 조직의 일관된 판단과 행동으로 전환될 때 비재무적 경영성과로 이어질 수 있다고 판단된다.

〈그림 2〉 재난안전인식과 재난관리시스템이 비재무적 경영성과에 미치는 영향에 관한 연구모형



V 회복력은 문서가 아니라 실행으로 검증

앞서 살펴본 사례와 연구결과는 설비와 시스템을 이중화하고 계획을 마련하는 것만으로 서비스 연속성이 확보되는 것은 아니라는 점을 보여준다. 업무연속성관리의 핵심은 조직이 정한 복구목표와 대응체계가 실제 재난 상황에서도 작동하는지를 반복 검증하고 개선하는 데 있다.

우선 업무영향분석(Business Impact Analysis, BIA)을 통해 중단 시 영향이 큰 핵심 서비스와 업무를 식별하고, 업무 중단을 감내할 수 있는 최대 허용 중단기간(Maximum Tolerable Period of Disruption, MTPD)을 정해야 한다.

이를 기준으로 업무와 서비스를 복구해야 하는 목표복구시간(Recovery Time Objective, RTO)과 허용 가능한 데이터 손실의 시점을 나타내는 목표복구시점(Recovery Point Objective, RPO)을 설정해야 한다. 위험평가(Risk Assessment, RA)에서는 개별 설비의 고장뿐 아니라 전력·냉각·통신·운영도구의 공통원인고장, 정보와 의사결정 권한의 집중, 핵심인력과 협력사에 대한 과도한 의존 등 서비스 중단을 확대할 수 있는 단일장애점을 함께 식별해야 한다. 그 결과는 대체시설 확보, 시스템 전환, 비상운영, 핵심인력과 공급망 확보 등을 포함한 업무 연속성 전략과 대응계획에 반영돼야 한다.

계획의 실효성은 복합적인 장애 상황을 가정한 훈련을 통해 확인해야 한다. 주 센터 상실, 통신망 단절, 운영도구와 인증체계 장애, 핵심 협력사 연락 두절, 주요 의사결정자의 부재가 동시에 발생하는 상황에서도 조직이 현황을 파악하고 권한을 대체하며 서비스를 전환할 수 있는지 검증할 필요가 있다. 훈련은 정해진 절차를 따라 읽는 방식이 아니라, 불완전한 정보와 시간 제약 속에서 실제로 판단하고 행동하도록 설계해야 한다.

성과지표 역시 매뉴얼 보유 여부나 교육시간과 같은 투입 중심 지표에서 벗어나야 한다. 재난 인지와 선언에 걸린 시간, 정보공유와 의사결정 지연, 서비스 전환 및 복구 소요시간, 목표복구시간 달성 여부, 훈련에서 확인된 미해결 과제와 공통 의존성의 해소 정도를 중심으로 관리해야 한다. 사고와 훈련에서 드러난 문제를 계획과 설비, 조직과 절차에 다시 반영하는 PDCA가 지속적으로 작동할 때 대응체계는 실제 조직역량으로 축적될 수 있다.

최종적인 복구 기준은 전력·냉각설비나 서버의 정상화에 머물러서는 안 된다. 애플리케이션과 데이터, 통신망과 인증체계가 정상적으로 작동하고, 고객이 서비스에 접속해 중단된 업무를 다시 수행할 수 있어야 비로소 복구가 완료됐다고 볼 수 있다. 데이터센터의 회복력도 계획서의 완성도나 설비의 개수와 이중화 정도로만으로 판단해서는 안 된다. 위기 상황에서 정보와 권한, 인력과 기술이 함께 작동해 고객 서비스를 정해진 시간 안에 실제로 회복할 수 있는지를 기준으로 검증해야 한다.

[참고문헌]

과학기술정보통신부·방송통신위원회·소방청, 「SK C&C 판교 데이터센터 화재 및 카카오·네이버 등 부가통신서비스 장애 조사결과 발표」, 2022.
행정안전부 중앙재난안전대책본부, 「국가정보자원관리원 행정정보시스템 화재 관련 대처상황 보고」, 2025.
안치준·정종수, 「데이터센터 근로자의 재난안전인식 및 재난관리시스템이 비재무적 경영성과에 미치는 영향: 재난대응역량의 매개효과를 중심으로」, 『한국IT정책경영학회 논문지』, 2026.
Uptime Institute, Data Center Site Infrastructure Tier Standard: Topology, Uptime Institute, LLC, 2018.
ISO, *ISO 22301:2019, Business continuity management systems — Requirements*, 2019.
행정안전부, 「기업재난관리표준」(전부개정), 행정안전부고시 제2025-42호, 2025.6.16.

본 고에 수록된 내용은 집필자의 개인적인 견해이며, 한국정보통신산업연구원의 공식적인 입장과 다를 수 있습니다.

02 이슈 보고서

KICI 디지털안전본부
신현철 디지털안전관제센터장

집중호우 대비 중요통신시설 침수방지 동향 및 방향

기후위기 심화와 통신 인프라 회복탄력성의 중요성

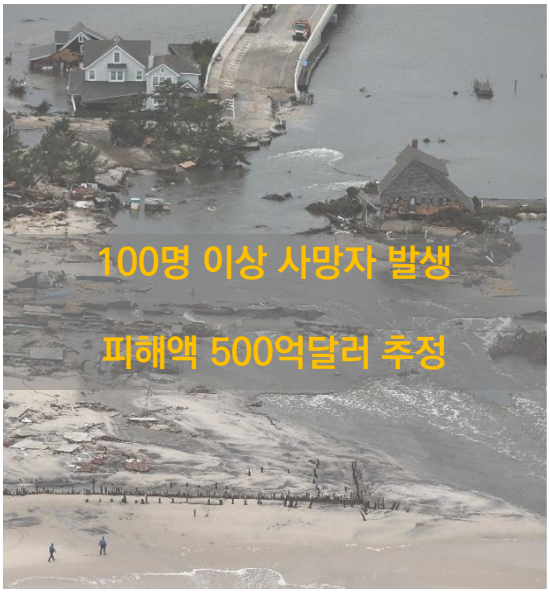
최근 글로벌 기후변화로 인한 국지성 집중호우와 대규모 홍수는 예측 불가능한 패턴으로 발생하며 도시 기능의 전반적인 마비를 초래하고 있다. 특히 전력이나 교통과 함께 사회적 핵심 인프라의 축을 담당하는 통신국사, 데이터센터와 같은 중요통신시설 및 중계기, 기지국 등 주요시설은 침수 피해가 발생할 경우 단순히 개별 시설의 파손을 넘어 사회 전체의 재난 대응 체계를 무력화하는 디지털 블랙아웃으로 이어지게 된다. 통신 인프라의 마비는 금융, 물류, 긴급 구조 요청 등의 전면 중단을 야기하며 재난 발생 시 골든타임을 놓치게 만드는 치명적인 취약점으로 작용한다. 실제로 최근의 침수 피해는 과거 지표면 중심의 범람을 넘어 장비가 밀집된 지하공간으로 우수가 급격히 유입되는 양상을 보이고 있다. 이에 따라 주요시설의 침수 피해 사례와 방지 기술 동향을 분석하고, 국내 중요통신시설의 침수 예방 및 신속 복구를 위한 제도적, 기술적 고도화 방향을 살펴보고자 한다.

국내외 통신시설 침수피해 사례

① 2012년 미국 뉴욕에서는 허리케인 샌디로 인해 맨해튼 하부의 주요 통신 국사와 데이터센터 지하 전력실이 침수되면서 백업 발전기 가동이 중단되어 수일간 통신이 마비되었다.

미 연방통신위원회(FCC)에 따르면 태풍 영향은 15개주이며, 이중 피해가 심한 10개주의 통신케이블 및 기지국의 1/4이 손상된 것으로 나타났다.

이 사건은 슈나이더 일렉트릭 등 글로벌 인프라 전문가들을 중심으로 데이터센터 내 배전반, 전력 스위치 기어, 연료 이송 펌프 등 핵심 지원 설비를 지하가 아닌 지상 상부 층으로 이전 배치해야 한다는 강력한 기술적 교훈을 남겼다.



Juliana Jiménez Jaramillo(2012), Hurricane Sansy's Aftermath, SLATE

BBC(2017), Hull telecoms firm KCOM fined over 999 call failures

② 2015년 영국에서는 겨울철 폭우(Storm Eva)로 인해 요크주 스톤보우에 위치한 BT 통신 교환국이 전면 침수되었다. 이로 인해 해당 인프라와 연계된 KCOM 등의 통신사에서 약 18만 가구의 통신선이 마비되면서 약 4시간 동안 해당 지역의 999 또는 112 긴급구조 호출 서비스가 중단됨에 따라 규제기관(Ofcom)으로부터 90만 파운드의 벌금을 부과 받았다.

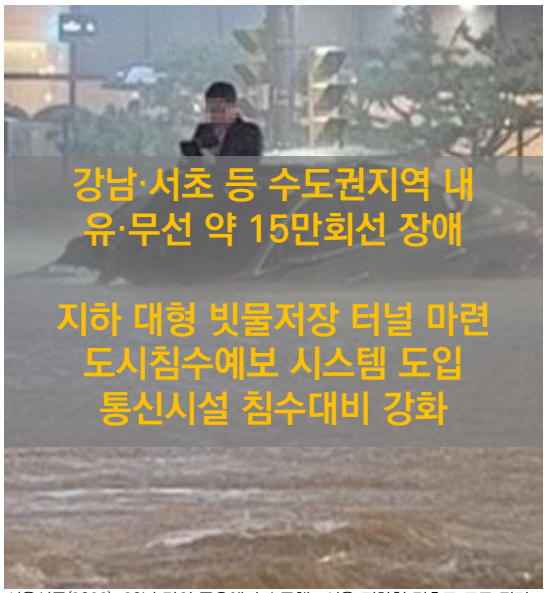
현장 조사 결과 지하 관로를 타고 우수가 유입된 것이 원인으로 밝혀지면서, 주요 관통부인 케이블과 파이프에 대한 가스 및 수밀성 복합 실링 자재 도입의 중요성과 단일 국사 마비에 대비한 자동 우회(Back-up) 경로 다중화의 중요성이 강조되었다.

③ 2021년 서유럽에 100년만의 기록적인 폭우가 발생하면서 독일 서부, 벨기에, 네덜란드에 한 달 치 강수량이 24시간 만에 쏟아졌다. 이로 인해 유선망 분배국과 기지국이 대거 침수되며 현지 유무선 통신 네트워크가 마비되었고, 재난 경보망 전송이 실패하면서 인명 피해가 확대되었다.

특히 사고 당시 독일 라인란트팔츠주 바트노이에나르 아르바일러 마을에서는 1,300명의 생사가 확인되지 않고 있다고 밝혔으며, 당국자는 생사 미확인의 원인을 통신 두절이라고 설명하기도 했다. 이후 독일에서는 기지국의 무정전전원장치의 용량을 확대하고 비상 발전기를 추가로 확보, 긴급통신을 위한 로밍 협력 체계 강화 등 대규모 정전을 대비하고 있다.

또한 해당 사고로 인하여 통신망의 물리적 분산과 더불어 위성 백업망을 연계하는 다원화된 인프라 구축의 필요성이 대두되었다.

경향신문(2022), '상상밖' 대홍수가 주고 간 교훈….필수적으로 '기후위기' 고려해 복구해야



서울신문(2022), 80년 만의 폭우에 속수무책…서울 지하철 멈추고 도로 잠겨

④ 2022년 서울 남부지역에 시간당 100mm 이상의 폭우로 하수관로의 배수 용량이 한계에 도달, 도로 위 폐기물이 지상 빗물받이를 막으며 저지대 빌딩 지하로 대량의 우수가 유입되었다.

이로 인해 빌딩 내 전력실과 기계실이 침수되고, 건물 정전에 따른 유무선 통신장애가 동시다발적으로 발생하였다.

과학기술정보통신부는 중요통신시설 내 지하공간에 주요시설*이 있는 경우 물막이판과 배수시설을 병행 설치하여 통신국사 피해를 예방할 수 있도록 조치를 취하였다.

* 중앙감시실, 항온항습시설, 전산실, 전력감시실, 전력관련 시설 (축전지설비, 자가발전설비, 수변전설비), 통신장비실 및 방재센터

국내 침수방지 기준 동향

「방송통신발전기본법」 제35조에 따라 중요통신시설은 주요시설이 지하공간에 있는 경우 침수방지를 위한 조치를 이행하여야 하며 침수방지를 위한 구체적인 사항은 행정안전부 고시 「지하공간 침수 방지를 위한 수방기준」을 참고하고 있다.

특히, 과학기술정보통신부는 “제4차 정보통신 진흥 및 융합 활성화 기본계획” 및 “제8차 지능정보사회 종합계획”에서 디지털 안전관리 강화를 위한 풍수해, 화재 등 재난대비 강화를 중점사항으로 담았으며, 중요통신시설의 차수시설의 높이 기준을 추가하고 배수시설을 병행 설치하도록 풍수해 대비 방안을 강화하고 있다.

현재 시행 중인 행정안전부 고시 「지하공간 침수 방지를 위한 수방기준」은 자연재해위험개선지구 등 침수우려 지역 내 지하공간의 인명과 시설물 피해를 방지하기 위한 지침을 제공하고 있으며, 지방자치단체 또한 고시를 바탕으로 조례를 통해 지하공간의 침수방지를 조치하고 있다.

지하공간 침수 방지를 위한 수방기준

제4조(예상 침수 높이의 결정) ① 예상 침수 높이는 다음 각 호에 따라 결정하여야 한다.
1. 과거의 태풍, 호우, 해일 등으로 인한 침수피해나 침수 흔적에 따른 침수 높이
2. 침수흔적도에 의한 침수 높이
3. 하천 범람 모의, 해일 범람 모의 등의 침수 높이 분석 결과
4. 지역별 방재성능목표를 적용한 내수 침수 모의 등의 침수 높이 분석 결과
5. 「자연재해대책법」 제16조에 따라 수립하는 자연재해저감 종합계획의 전 지역단위 침수 높이 분석 결과
6. 침수예상도(홍수범람, 내수침수, 해안침수)가 작성된 지역에서 침수 높이

② 제1항의 자료 활용이 불가능할 경우 과거의 강우 기록과 침수피해, 인근 주민들의 탐문조사 결과 등을 고려하여 예상 침수 높이를 추정하되 과대 · 과소 추정되지 않도록 유의하여야 한다.

집중호우 대비 통신 인프라 수방 고도화 방향

집중호우로 인한 통신시설 침수피해는 지표면 중심의 범람을 넘어 장비가 밀집된 지하공간으로 우수가 급격히 유입되는 양상을 띄고 있다. 향후 집중호우의 강도와 빈도가 변동성을 키우며 증가할 것으로 예상됨에 따라 중요통신시설의 침수 방지 대책은 단순한 법적 최저 기준 만족을 넘어 비즈니스 연속성 및 공공 안전 확보 차원에서 다각도로 고도화되어야 한다. 이를 위해서는 다음과 같은 방향으로 검토할 필요가 있다.

① (시설물 위치의 수직적 배치) 신축 국사 및 데이터센터 설계 시 배전반, UPS, 백업 발전기, 통신장비실 등 핵심 설비의 지하 배치를 지양하고 지상층 배치를 원칙으로 정립해야 한다. 기존 지하 차수벽을 최소 예상 침수 높이보다 여유고를 두어 높게 설치하는 것이 바람직하다.

② (관로 진입로의 수밀화) 케이블 인입 구간이 우수의 이동 통로가 되지 않도록 건물 인입동의 관로 개구부에 가스 및 물 결합 차단 씰링을 적용하고 주기적으로 밀폐성 실측이 필요할 것으로 판단된다.

③ (배수 인프라 다중화) 단일 배수펌프 고장에 대비해 예비 배수펌프를 1대 이상 추가 설치하고 비상발전기 전원과 연계하여 상용전원 차단 시에도 배수 기능이 유지되도록 하여 긴급한 상황에서 활용할 수 있도록 배치한다면 긴급한 상황에서의 대응이 가능할 것이다.

④ (민관 합동 재난 대응체계 강화) 특정 국사의 완벽한 침수 방지가 불가능한 극한 재난 상황을 가정하여 사전에 대비하고 즉시 대응할 수 있도록 다양한 시나리오를 바탕으로 정기적인 모의훈련을 통해 극한 호우와 같은 비정상적인 재난 상황에 대한 일상적인 대응능력을 갖출 수 있도록 노력해야 한다.

통신 인프라와 서비스는 재난 상황에서 국민의 생명과 직결되고 있으며, 현행 수방기준의 기술적 가이드라인을 철저히 준수하면서 해외의 실패 사례를 거울삼아 인프라 전반의 물리적, 소프트웨어적 회복탄력성을 지속적으로 강화해 나가야 할 것이다.

[참고문헌]

BBC(2017), Hull telecoms firm KCOM fined over 999 call failures
Juliana Jiménez Jaramillo(2012), Hurricane Sansy's Aftermath, SLATE
경향신문(2022), '상상밖'대홍수가 주고 간 교훈….필수적으로 '기후위기 ' 고려해 복구해야
서울신문(2022), 80년 만의 폭우에 속수무책…서울 지하철 멈추고 도로 잠겨

03 전문가인터뷰

법무법인 광장
조대근 전문위원

법무법인 광장 조대근 전문위원님을 만나다.

Q 우선 조대근 전문위원님에 대해 소개 부탁드립니다.

A 저는 법무법인(유) 광장의 TMT(방송정보통신) 전문위원으로 AI 인프라, IT·방송통신, 기업 자문 분야를 담당하고 있고, 서강대학교 공공정책대학원 겸임교수로서 후학 양성과 연구도 병행하고 있는 조대근이라고 합니다. 저는 상호접속이나 설비제공 같은 통신시장 공정경쟁 규제정책 및 망중립성, 온라인플랫폼, IP Interconnection, 네트워크 안정성 그리고 최근에는 AI 데이터센터(AIDC), 해저케이블, 전력, 6G, 저궤도위성과 같은 AI 및 관련 인프라 정책에 이르기까지 방송통신 정책과 디지털 인프라 전반을 연구하고 자문하고 있습니다. 아울러 우리나라의 ICT 정책과 제도를 해외에 소개하고, 개발도상국과 저개발국 정부에 정보통신정책 자문을 제공하는 등 국내·외를 아우르는 지식 공유 활동에도 힘을 쏟고 있습니다.

Q ICT 규제정책 분야에서 오랫동안 경력을 쌓아오신 만큼, 디지털 재난·장애 사례도 많이 접해보셨을텐데요. 위원님께서 생각하시기에 가장 인상 깊었던 사건이나 사례가 있으시다면 말씀 부탁드립니다.

A 제가 인상 깊게 본 세 사건은 공교롭게도 디지털 재난의 서로 다른 발생 메커니즘을 하나씩 대표합니다. 인적 오류의 증폭, 안전성의 역설, 그리고 지정학과 제도의 변화입니다.

첫째는 2021년 KT 네트워크 장애 사고입니다. 부산국사에서 라우터 교체 작업 중 작업자가 'exit' 명령어 한 줄을 누락한 것이 발단이었는데, 잘못된 경로정보가 IS-IS(Intermediate System to Intermediate System) 라우터들끼리 자동으로 주고받는 구조를 타고 전국으로 번지면서 약 89분간 유·무선 인터넷이 마비됐습니다. 네 글자 누락이 전국의 결제·인증·물류를 동시에 멈춰 세운 것이죠. 저는 이 사건이 효율을 위한 연결성과 자동화가 곧 단일장애점의 전국적 증폭 경로가 된다는 역설을 가장 압축적으로 보여준다고 봅니다. 결국 인재(人災)의 본질은 개인의 실수가 아니라, 사전 시뮬레이션과 확산 차단 장치가 없었던 시스템에 있다는 것입니다.

둘째는 2024년 CrowdStrike 사태입니다. 보안업체가 배포한 업데이트의 논리 오류 하나로 Windows 약 850만 대가 다운됐고, 전 세계 항공·의료·미디어가 마비되며 추정 손실이 최소 100억 달러에 달했습니다. 시스템을 지키려고 만든 보안 소프트웨어가 어떤 해커보다 광범위한 다운을 일으켰다는 점이 핵심입니다. 보안 프로그램은 커널 깊숙이 최고 권한으로 작동하기 때문에, 바로 그 권한 때문에 결함이 생기면 OS 전체를

무너뜨립니다. KT가 국내 통신망 내부의 자동 확산이었다면, 이건 글로벌 소프트웨어 공급망의 자동 확산이었습니다.

셋째는 발트해 해저케이블 절단입니다. 2023년 이후 이른바 '그림자 함대'가 최소 11개 케이블을 손상시킨 것으로 집계되는데, 정작 고의 여부 입증이 어렵다는 점이 이 위협의 특징입니다. 제가 이 사례를 가장 인상 깊게 본 이유는 '위협 인식 → 고립 우려 → 제도 정비'라는 규제 변화의 동학을 선명하게 보여주기 때문입니다. EU가 우려한 것은 단순한 통신 장애가 아니라 유럽의 전략적 고립이었습니다. 결국 2025년 2월 EU 집행위는 예방·탐지·대응·억지 4개 축의 해저케이블 보안 액션플랜을 내놓았습니다. 이러한 사례는 제도가 평시의 합리적 설계보다 충격적 사고를 계기로 사후 정비되는 경우가 많다는 것을 잘 보여줍니다.

세 사례를 관통하는 메시지는 디지털 재난이 더 이상 기술 부서의 사고가 아니라 사회 전체의 시스템 리스크이며, 그 원인이 복잡성·신뢰·지정학이라는 비기술적 층위에 있다는 점입니다. 따라서 디지털 재난 대응도 기술적 복구를 넘어 제도와 거버넌스, 국제협력의 문제로 다뤄야 한다고 생각합니다.

Q 2018년 KT 아현지사 화재부터 2022년 SK C&C 판교 데이터센터 화재, 그리고 최근의 디지털 인프라 장애를 거치며 '디지털 재난'이라는 개념이 사회적으로 부각되었는데요. ICT 규제 정책 전문가의 시각에서는 디지털 재난을 어떻게 정의하시나요?

A 먼저 말씀드리면, '디지털 재난'은 아직 국제적으로 합의된 단일 법적 정의가 없습니다. 국제기구들은 이를 두 갈래로 다뤄 왔습니다. ITU는 전통적으로 디지털 인프라를 '재난 대응의 수단'으로, 즉 재난 발생 시 통신을 어떻게 유지하느냐의 관점에서 봤습니다. 반면 EU의 NIS2(Network and Information Security 2, 네트워크 및 정보보안 지침 2)나 미국 CISA(Cybersecurity Information Sharing Act, 사이버정보공유보안법)는 통신·데이터센터·클라우드를 '재난의 대상'으로 보고, 그 붕괴 자체를 재난으로 규율합니다. 음성 중심 시대에는 전자의 관점이 지배적이었다면, 데이터 중심 시대로 오면서 후자가 부상하고 있는 것이죠.

우리나라도 별도의 디지털 재난 정의 없이, 「방송통신발전기본법」의 방송통신재난과 「재난 및 안전관리 기본법」상 사회재난으로 나누어 규율하고 있습니다. 2018년 KT 아현지사 화재 사고 이후에는 통신설비 중심으로, 2022년 SK C&C 판교 데이터센터 화재 이후에는 부가통신서비스·데이터센터가 국가 재난관리 체계에 포함되는 등 그 객체는 지속적으로 확장되고 있습니다.

제가 정책학자로서 강조하고 싶은 가장 중요한 변화는, 디지털 재난의 판단 기준이 '물리적 피해의 크기'에서 '사회적 기능 마비의 크기'로 이동했다는 점입니다. "exit" 명령어 한 줄, 채널 파일 하나가 전국과 전 세계를 멈추는 시대에는 재난의 크기를 원인이 아닌 사회적 결과로 측정해야 합니다.

그래서 제가 제안하는 정의는 이렇습니다. 디지털 재난이란 네트워크·데이터센터·클라우드·핵심 디지털 서비스의 가용성·무결성·기밀성이 자연적·기술적·인위적 원인으로 침해되어, 그 물리적 피해 규모와 무관하게 국민의 일상과 경제활동, 그리고 금융·교통·의료·행정 등 국가기반체계 기능에 중대한 마비를 초래하거나 초래할 급박한 우려가 있는 상태를 말합니다.

행정학적으로 보면, 정의는 곧 관할과 예산을 결정합니다. 디지털 재난을 독립 개념으로 규정하는 것은 단순한 용어 정리가 아니라 책임 주체와 권한을 명확히 하는 거버넌스 설계의 출발점이라는 점을 강조하고 싶습니다.

Q 방송통신발전기본법상 재난관리 체계나 전기통신사업법상 안정성 의무 등 현행 통신 재난 관련 법제도가 실제 위험에 비추어 보았을 때 충분하다고 생각하시는지, 보완이 필요한 부분이 있다고 생각하시는지 답변 부탁드립니다.

A 외형상 우리나라의 규율 체계는 해외 사례와 비교해도 촘촘한 편입니다. 다만 저는 그것이 '사고 발생 → 사후 입법'의 반복으로 만들어진 체계, 즉 위험 기반이 아니라 사건 기반 법제라는 점에 구조적 한계가 있다고 봅니다. 실제로 KT 아현지사 화재 사고가 통신설비 이원화를, SK C&C 판교 데이터센터 화재가 부가통신서비스와 데이터센터에 대한 규율을 한 칸씩 뒤따라가며 만들었습니다. 각 개정은 직전 사고에 최적화돼 있지만, 위험 포트폴리오 전체를 평가해 자원을 배분하는 사전적 위험평가 메커니즘은 법률 차원에 없습니다.

보완이 필요한 부분을 세가지로 말씀드리겠습니다.

첫째, 절차 중심 규제라 결과 검증이 약합니다. 이중화가 서류상 존재하는 것과 실제 자동 failover(장애극복)가 복구 목표 시간 내에 작동하는 것은 전혀 다른 문제입니다. 국가정보자원관리원 화재가 공공 부문에서 이를 입증했죠. 정기 failover 훈련과 복구시간 측정을 법정 의무로 둘 필요가 있습니다. 제재 수준도 비대칭적입니다. 개인정보 유출에는 매출액 기준 과징금이 가능한 반면, 통신재난 의무 위반은 시정명령·과태료 중심이어서 가용성 의무를 어기는 기대비용이 더 낮은 규제 차익이 존재합니다.

둘째, 의무 대상 지정이 이용자 수나 면적 같은 외형 기준이지, 서비스의 사회적 필수성이나 대체 불가능성을 반영한 기능 기반 지정이 아닙니다. 간편인증이나 모바일 결제가 멈출 때의 연쇄효과가 기준에 들어가야 합니다.

셋째, 신종·구조적 위험이 미반영되어 있습니다. KT 아현지사 화재 사고, SK C&C 판교 데이터센터 화재, 국가정보자원관리원 화재 세 건 모두 본질은 전원 사고였는데도 백업전원 기준이 미약하고, 해저케이블 육양국 같은 국제 관문 인프라가 국내 국사와 동일 평면에서 다뤄집니다. 특정 클라우드나 데이터센터 권역에 대한 의존도를 측정하고 임계치를 관리하는 장치도 없기 때문에 '2개 이상 클라우드 다중화'가 여전히 권고에 머물러 있습니다.

요약하면, 현체계는 '지난 전쟁에 대비하는 법'에 가깝습니다. 앞으로는 사후 대응에서 사전적 위험평가로, 절차 의무에서 결과 검증으로, 외형 기준에서 기능 기준으로 무게중심을 옮겨야 한다고 봅니다.

Q 해외 주요국의 통신 규제 정책 관련 자문을 해오신 것으로 아는데, 통신 재난 예방·대비 측면에서 우리나라가 참고할 만한 해외 제도나 사례가 있다면 소개해주실 수 있을까요?

A 네 가지를 말씀드리고 싶습니다. 영국, 일본, 미국, EU인데요. 이들을 관통하는 공통 키워드는 "계획 제출"에서 "검증 가능한 결과 의무와 사업자 간 상호 백업"으로의 전환입니다.

먼저 영국입니다. 영국은 2021년 통신보안법으로 사이버 보안과 물리적 복원력을 'security compromise(보안침해)'라는 단일 의무 체계로 통합했습니다. 특히 인상적인 것은 규제 방식인데요. 법률에서 원칙을 정하고, 시행규정과 사업자 규모별 차등 기대 수준을 담은 실행규범, 그리고 Ofcom의 기술 가이던스로 이어지는 4층 구조로 의무의 구체성과 비례성을 동시에 확보했습니다. Ofcom은 2024년 핵심 인프라에 자동 failover를 갖추라는 아키텍처 수준의 기대치까지 명문화했고, 실제로 복원력 의무 위반에 제재금을 부과한 집행 실적도 있습니다. '계획 미제출'이 아니라 '복원력 결과 미달'을 직접 제재한 것입니다. 우리나라 「방송통신발전 기본법」의 '방송통신재난관리기본계획 수립' 의무를 이런 결과 의무와 등급별 가이던스, 결과 기반 제재로 재설계하는 모델로 참고할 만합니다.

일본은 비상시 사업자 간 로밍을 의무적으로 제도화한 과정이 참고됩니다. 2022년 KDDI의 약 86시간 대규모 장애가 계기가 되어, 지금은 'JAPAN 로밍'으로 통신 4사가 참여하는 체계가 상용화됐습니다. 긴급통보만 가능한 단계와 음성·SMS·데이터까지 가능한 풀로밍 2단계로 운영됩니다. 사실 우리나라가 2018년 아현 화재 이후 재난로밍을 선제적으로 구축한, 시기적으로는 일본보다 앞선 사례입니다. 다만 단일사 전체 가입자가 마비되는 시나리오에 대비한 수용 용량, 발동 요건의 법정화 수준, 데이터 통신 포함 여부와 정기 실전 훈련 측면에서는 일본의 최신 설계가 앞서는 부분이 있어 '재난로밍 2.0'의 벤치마크로 삼을 만합니다.

미국은 FCC가 업계 자율 협약을 의무 패키지로 법제화한 점이 핵심입니다. 재난 시 로밍 협정, 사업자 간 상호 지원, 소비자 소통 등을 자율 MOU가 아니라 법정 의무에 사전 시험과 성과 보고를 묶어 운영하고, NORS(Network Outage Reporting System, 네트워크 장애 보고 시스템)·DIRS(Disaster Information Reporting System, 재난 정보 보고 시스템) 같은 장애 보고 인프라로 데이터를 주·연방 기관과 공유합니다. 우리도 사업자 간 상호 지원을 법정 의무로 묶고, 장애 데이터를 지자체·소방·행안부와 실시간 공유하는 한국판 DIRS를 제도화할 필요가 있습니다. 캘리포니아가 산불 지역 기지국에 72시간 백업전원을 의무화한 것도 백업전원 기준 논의에 참고가 됩니다.

마지막으로 EU는 분절 해소의 입법 모델입니다. NIS2 지침은 통신사업자를 데이터센터·클라우드와 함께 '필수 주체'로 묶어 단일 사이버 복원력 체계에 편입하면서 전위험 접근과 경영진의 직접 책임, 단계적 사고 보고를 골자로 합니다. 여기에 물리적 위협을 다루는 CER 지침(Critical Entities Resilience Directive 2022, 핵심주체 복원력 지침)을 짝으로 설계했는데, 우리 식으로 말하면 「정보통신기반 보호법」과 「방송통신발전 기본법」의 재난관리를 의도적으로 정합화한 쌍둥이 입법입니다. 2026년 제안된 Digital Networks Act는 해저케이블 보호까지 단일시장 규제로 끌어들이고 있어, 통신 재난 규율이 국사 화재 대응을 넘어 지정학적 인프라 보호로 확장되는 추세를 보여줍니다.

Q 통신 기술이 빠르게 변화하고 있는데 비하여 관련 규제나 정책은 사후적·경직적이기 쉬운데요. 규제 정책 전문가로서 기술 변화 속도를 따라가면서도 안정성을 확보하는 '유연한 재난 규제'를 위해서는 어떠한 노력이 필요할까요?

A 제 생각의 출발점은 이렇습니다. 규제는 정부의 고유 권한이지만 행사하려면 법적 근거가 필요하고, 그러다 보니 경직된 규정 아래 이루어질 수밖에 없습니다. 그런데 기술 발전이 빠르고 사안이 다양하며 신속한 대응이 필요한 재난 영역에서는 통신망을 직접 운용하는 사업자에게 대응 권한을 충분히 부여하고 정부는 방향성만 제시하는 방식이 바람직하다고 봅니다. 대신 자율규제를 성실히 수행하는 사업자에게는 합당한 제도적 유인을 주고, 그러지 못해 재난을 유발한 사업자에게는 상응하는 충분한 책임을 묻는 구조여야 합니다. 재난의 원인과 주체가 워낙 다양하기 때문에 이를 모두 통제하려 하기보다 정부가 정책목표를 담은 가이드라인을 제시하고 사업자가 스스로 책임을 다하되, 기술 발전에 따라 그 가이드라인을 지속적으로 업데이트하는 것입니다.

이 구상은 국제 규제학의 최신 흐름과도 정확히 맞닿아 있습니다. OECD가 정식화한 '민첩 규제'는 규제를 일회성 입법이 아니라 반복적 학습 과정으로 보고, EU의 Better Regulation은 자율·공동규제를 공식 원칙으로 인정합니다. 제가 말씀드린 '정부는 방향성만, 방법은 사업자에게'라는 구조는 학술적으로 결과 기반·위험 기반 규제라고 부릅니다. 흥미롭게도 이 방식은 안정성이 중요한 유틸리티나 헬스케어에서 오래 검증된 모델이고, 잘 설계되면 오히려 안정성과 예측가능성을 높입니다. '유연함'이 곧 '불안정'은 아니라는 것을 보여주는 것입니다.

다만 한 가지 단서를 더하고 싶습니다. 재난 규제는 안전이 걸린 고위험 영역이므로, 순수한 자율규제가 아니라 '정부가 결과와 책임의 골격을 법으로 정하고 이행 방법은 사업자에게 위임하는 공동규제'가 글로벌 정답입니다. 실제로 미국 FCC는 통신 재난 대응을 처음에 업계 자율 협약으로 시작했지만, 한계가 드러나 2022년 의무 규제로 전환했습니다. 그래서 핵심은 '자율이냐 규제냐'의 양자택일이 아니라, '무엇을 법으로 고정하고 무엇을 위임할 것인가'의 정교한 설계입니다.

Q 많은 국가에서 해저 통신케이블은 단순한 통신 설비를 넘어 안보 자산으로 다뤄지고 있는데요. 해외 주요국은 해저 통신케이블을 어떻게 관리·보호하고 있으며, 우리나라가 통신재난 예방과 국가안보를 함께 고려해 참고할 만한 접근 방식이 있다면 소개해주실 수 있을까요?

A 제가 최근 가장 집중해서 연구하는 분야인데요. 해저케이블 규율의 글로벌 패러다임은 '통신설비'에서 '안보 자산'으로 명확히 이동했고, 크게 세 가지 축으로 수렴하고 있습니다. 누가 깔고 운영하느냐를 통제하는 미국형 공급망 통제, 누가 지키느냐에 집중하는 EU·NATO형 감시·억지, 그리고 끊겨도 살아남느냐를 보는 일본형 복원력입니다.

먼저 미국은 '소유·공급망 통제' 모델입니다. FCC의 육양면허 권한은 1921년 케이블육양면허법에 뿌리를 두는데, 핵심은 'Team Telecom'이라 불리는 부처 간 안보심사 위원회입니다. FCC라는 통신규제기관과 법무·국방·국토안보 같은 안보기관이 케이블 면허를 공동으로 심사하는 구조입니다.

특히 주목할 것은 2024년부터 25년 만에 규칙을 전면 개정한 점입니다. 중국 연계 Salt Typhoon 첩보 사건을 배경으로, 적성국 소유·통제 주체의 육양면허 취득을 배제하고, 적성국 장비·서비스를 쓰지 않는다는 인증을 요구하며, 반대로 고수준 보안기준을 충족하면 심사를 면제해 주는 비대칭 유인을 도입했습니다.

EU와 NATO는 발트해 해저케이블 절단 사태가 촉발한 '감시·억지·복원력 통합' 모델입니다. 우크라이나 전쟁 이후 그림자 함대에 의한 케이블 손상이 잇따르면서, EU가 우려한 것은 단순한 통신 장애가 아니라 '유럽의 고립'이었습니다. EU는 2025년 2월 예방·탐지·대응·복구·억지의 전 주기를 포괄하는 해저케이블 보안 액션플랜을 채택했고, 2026년 1월 제안한 Digital Networks Act에서는 케이블을 '필수 인프라'로 격상했습니다. NATO는 2025년 1월 '발틱 센트리(Baltic Sentry)'를 발족해 프리깃·초계기·드론으로 핵심 인프라를 감시하고 있죠. 여기서 인상적인 것은 민관 협력의 강조입니다. 이상 징후를 가장 먼저 탐지하는 것은 대개 민간 운영자이므로, 민간이 당국에 경보하고 법집행·군사 대응으로 연계하는 구조가 핵심입니다.

일본은 우리와 조건이 가장 유사합니다. 국제통신의 99%를 해저케이블에 의존하는 섬나라인데, 동일본 대지진 때 한 반도의 육양 중계국이 거의 전부 파손된 경험이 분산 정책의 원점이 됐습니다. 그래서 일본은 육양국 분산, 경로 다변화, 즉 다루트화를 핵심으로 삼고, 디지털인프라 정비기금으로 데이터센터와 케이블 정비를 재정 지원합니다. 중국 영향이 작은 알래스카 경유 북극해 루트를 기대하는 등 육양국의 지정학적 성격까지 고려한 경로 설계가 특징이고요. 여기에 경제안전보장추진법으로 기간 인프라를 사전 심사하고, EEZ까지 방호구역을 확대하는 방안도 검토 중입니다. 즉 자연재해 복원력과 경제안보 법제를 함께 묶은 모델입니다.

우리나라에 대한 제언은 이 세 모델을 선택적으로 결합하자는 것입니다. 우리는 부산·거제·태안에 육양이 집중된 단일장애점 구조를 가지고 있으면서도, 해저케이블을 일반 중요통신시설 등급 체계 안에서 국내 국사와 같은 평면으로 다루고 있습니다.

그래서 첫째, 일본형 복원력을 기본 골격으로 삼아 육양지점 분산과 경로 다양화에 법정 유인을 제공하고 동·서해 측 신규 육양을 검토해야 합니다. 둘째, 미국형 공급망 심사를 안보 차원에서 도입해, 과기정통부와 국정원·국방부가 케이블의 육양·운영·정비를 공동 심사하는 절차를 제도화해야 합니다. 셋째, EU·NATO형 복구역량과 민관 협력으로, 국내 수리선과 예비 부품을 확보하고 민간 운영자와 해경·해군 간 정보공유 체계를 갖춰야 합니다.

결국 가장 중요한 것은, 해저케이블을 통신설비로만 다루는 현행 접근을 넘어 통신재난과 국가안보를 함께 고려하는 별도 규율로 격상하는 것입니다. 미국이 25년 만에 규칙을 고치고, EU가 케이블을 필수 인프라로 끌어올리며, 일본이 새 법 정비에 착수한 것은 모두 '통신설비 규율로는 안보를 담을 수 없다'는 같은 인식의 산물입니다. 무기화된 상호의존의 관점에서 보면 육양 지점과 경로는 곧 지정학적 레버리지의 지점이고, 한국이 미·중 데이터 중계 허브로서 갖는 위치는 기회이자 취약점입니다. 그래서 복원력·공급망·억지를 한데 묶는 통합 거버넌스가 필요하다고 봅니다.

Q 해저 통신케이블은 영해, 배타적 경제수역, 공해를 넘나들며 설치되어 있어 관할권과 보호 책임이 복잡하게 얽혀 있는데요. 해저 통신케이블을 통신 재난 관점에서 보호하기 위한 법 체계의 공백이 있다면 무엇이 필요하다고 생각하십니까?

A 말씀하신 대로 해저케이블은 영해, 즉 주권이 미치는 영역부터 제한적 관할만 있는 EEZ, 그리고 자유가 보장되는 공해를 넘나들기 때문에 보호 책임이 관할권별로 파편화되어 있습니다. 문제의 근원은 국제법인 UNCLOS(United Nations Convention on the Law of the Sea) 자체에 있습니다. UNCLOS는 '사후 처벌'만 요구할 뿐 '사전 보호 의무'를 부과하지 않고, 공해상 관할을 기국, 즉 선박의 국적국에 의존하다 보니 실효성이 약합니다.

구조적 한계를 세 가지로 정리할 수 있습니다.

첫째는 기국주의('선박이 게양한 깃발의 국가가 관할권을 갖는다'는 원칙)의 한계입니다. UNCLOS 제113조가 케이블 손괴를 범죄화하도록 요구하지만 관할이 기국에 한정되어, 편의치적 선박이 케이블을 끊어도 무력합니다. 발트해 사건이 이를 그대로 노출했죠.

둘째는 사전 보호 의무의 부재입니다. 제113조는 손괴를 막는 법을 제정하라고만 할 뿐 적극적으로 보호할 의무를 지우지 않아서, 각국이 국내법으로 입법하지 않으면 공백이 생깁니다.

셋째는 EEZ 보호에 대한 침묵입니다. 정작 손괴의 다수가 EEZ에서 일어나는데 UNCLOS는 여기에 대해 거의 규정하지 않습니다. 게다가 1884년 파리협약이나 1982년 UNCLOS 모두 물리적 절단만 상정했을 뿐, 도감청이나 사이버, 그레이존 사보타주 같은 진화한 위협을 포섭하지 못합니다.

그래서 실질적 보호는 각국 국내법이 메우고 있는데, 주요국을 비교해 보면 나라마다 결이 다릅니다. 미국은 면허와 적성국 배제 인증으로 공급망을 통제하고, EU는 케이블을 필수 인프라로 격상하며 수리모듈 사전 배치까지 투자합니다. 일본은 다루트화와 영해 방호구역을 두고 EEZ 확대를 검토 중이고요. 가장 정교한 운영 모델은 싱가포르입니다. 신규 케이블을 지정 육양지에만 부설하게 하고, 해저 매설을 의무화하며, 손괴 시 즉시 보고하고 해사항만청과 협력해 수리계획을 제출하도록 표준 프로토콜을 갖췄습니다. 반대로 홍콩은 가장 자유주의적인 개방 면허제여서 투자 유치에는 유리하지만 안보심사는 약합니다. 자국 선적 화물선이 타국 케이블을 손괴한 사건이 개방성과 안보 책임 사이의 긴장을 보여줍니다. 호주의 해저케이블 보호구역은 사실상 글로벌 모범 사례로 꼽힙니다. 이러한 비교를 통해 드러나는 국내법 차원의 공백은 대부분의 국가가 공유하지만 우리나라에서 특히 심각합니다.

문제점을 여섯 가지로 짚어 보겠습니다.

첫째, 가용성을 다루는 통신재난 규율과 소유·도감청을 다루는 안보 규율이 별도 법, 별도 기관에 흩어져 있어 해저케이블이라는 단일 객체를 통합적으로 다루지 못합니다.

둘째, 보호구역이 영해에만 설정되어 정작 손괴가 많이 일어나는 EEZ에서는 실효성이 낮습니다.

셋째, 케이블을 핵심기반시설로 명시 지정하지 않아 보호·예산·책임의 법적 근거가 모호합니다. 싱가포르조차 이건 권고 단계에 머물러 있습니다.

넷째, 수리선이나 예비부품 확보 의무, 복구목표시간 기준 같은 복구역량 규율이 없습니다.

다섯째, 육양지 집중이라는 단일장애점을 완화할 법정 장치가 미흡합니다.

여섯째, 해저케이블 사업자와 통신규제기관, 해경·해군을 잇는 표준 보고·정보공유 체계가 약합니다.

그래서 한국에 필요한 과제를 정리하면, 해저케이블을 통신재난과 국가안보를 함께 고려하는 별도 규율 대상으로 격상하고, UNCLOS와 합치하는 범위에서 EEZ까지 보호구역을 확대하며, 케이블과 육양국을 핵심기반시설로 명시 지정하고, 국내 수리역량과 복구목표시간을 법정화하는 것입니다. 여기에 부산·거제·태안 집중을 완화하는 육양지 분산 유인, 통신·안보·해양 기관과 민간을 잇는 통합 거버넌스, 그리고 UNCLOS 국내 이행 점검과 한미일 정보공유 협력이 더해져야 합니다.

마지막으로 강조하고 싶은 것은, 세계 어느 나라도 해저케이블 보호를 '완성'하지 못했다는 점입니다.

미국은 25년 만에 규칙을 고쳤고, EU는 격상 중이며, 일본은 신법을 검토하고, 싱가포르도 아직 명시 지정 권고 단계입니다. 그대로 베낄 정답은 없습니다. 결국 통신재난 예방과 안보를 통합하는 거버넌스를 지진과 육양 집중, 미·중 중계 위치라는 한국의 고유 조건에 맞게 설계하는 것이 우리의 과제라고 생각합니다.

04 디지털 안전 관제 이슈

5월 발생 이슈

01 2026.05.12., 2026.05.23.

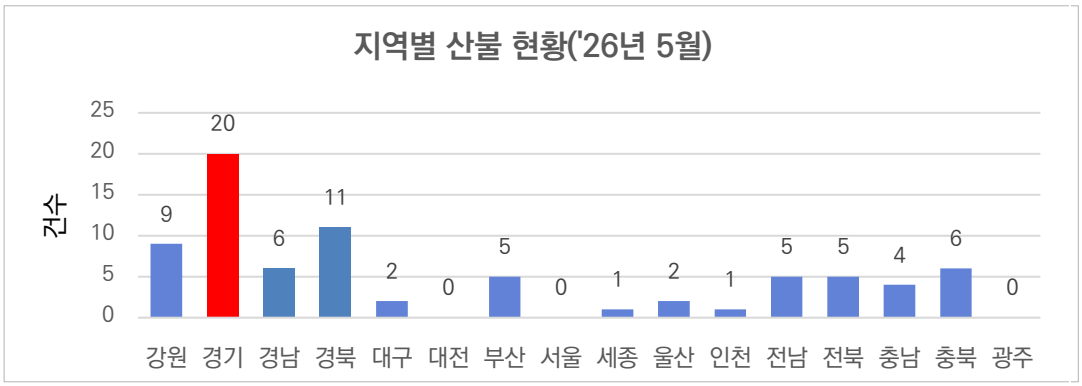
- 2026.05.12. 구글 웹/앱 검색 기능 서비스 오류
- 2026.05.23. 구글 플레이스토어 접속 불가 오류

02 2026.05.13.

- 삼성월렛 내 신한카드 지문인증 결제 오류

사회·자연재난 대응 실적(산불)

재난유형	일시	주요내용 (과기정통부 보고)
산불	5월 中 77건 보고 (기간통신 재난대응 보고)	• 산불대비·피해상황 보고 • 통신사 피해 없음 확인 • 통신마비 대비 상황보고 • 정부-사업자간 허브 역할 수행 • 지속 모니터링 실시



05 Digital Safety Inside

스마트테크 코리아 2026 참관

AI와 로봇, 양자, 보안 등 미래 산업 전반을 아우르는 '스마트테크 코리아 2026(STK 2026)'이 6월 10일부터 12일까지 서울 코엑스에서 개최되었다. 이번 행사는 'The Tech Nexus : 산업 전 과정을 연결하는 기술 생태계'를 주제로 16개국 620개사가 참가해 약 2,000개 부스 규모로 진행됐다.

피지컬 AI와 고성능 연산 수요가 급증하면서 IT 장비의 발열 문제가 업계 전반의 과제로 떠오르고 있는 만큼, 이번 전시에서도 그 해법으로 주목받는 수냉식 냉각 장비를 다수 확인할 수 있었다.

전시에서는 베이퍼챔버와 리퀴드쿨러를 활용한 액체냉각 방식의 발열 처리 설비, 발열이 가장 극심한 CPU·GPU에 직접 냉각수를 순환시키는 직접액체냉각(DLC) 방식, 히트싱크와 송풍기를 최소화한 액침냉각 서버 등을 살펴볼 수 있었다. 대형 사업자 중심이었던 과거와 달리, 엣지 데이터센터에 적용 가능한 중소 규모용 수냉식 인프라 솔루션도 눈에 띄었다.이러한 흐름은 데이터센터 업계가 공랭식의 물리적 한계를 인정하고 수냉식으로의 전환을 본격화하고 있음을 보여준다.

다만, 냉각 방식의 전환은 냉각수 누수, 배관 결함 등 기존 공랭식에는 없던 새로운 장애 유형을 수반할 수 있다는 점에서 디지털 재난 관점의 별도 검토가 필요할 것으로 보인다.

05 Digital Safety Inside

2026년도 통화량 급증 예상일 달력 (7~8월)

7월(July)

일	월	화	수	목	금	토
특이사항			1 o 대구치맥페스티벌 (대구, 7/1~7/5)	2	3 o 부여서동연꽃축제 (부여, 7/3~7/5) o 데이식스 콘서트 (서울, 7/3~7/5)	4 o 양평수박축제 (양평, 7/4~7/5) o 싸이흠뻑쇼-대구 (대구, 7/4~7/5) o 2026 Palette Festival (고양, 7/4~7/5)
5	6	7	8	9	10 o 금산 삼계탕축제 (금산, 7/10~7/12)	11 o 칠곡 꿀맥페스티벌 (칠곡, 7/11~7/12) o 르세라핌 콘서트 (인천, 7/11~7/12) o 싸이흠뻑쇼-인천
12	13	14	15	16	17 제헌절 o 싸이흠뻑쇼-서울대공원 (경기, 7/17~7/18)	18 o 코르티스 콘서트 (인천, 7/18~7/19)
19	20	21	22	23	24 o K-일러스트레이션페어 (부산, 7/24~7/26) o 워터밤 서울 2026 (경기, 7/24~7/26) o 보령머드축제 (보령, 7/24~8/9)	25 o 정남진 장흥 물축제 (장흥, 7/25~8/2) o 싸이흠뻑쇼-원주
26	27	28	29	30	31 o 2026 인천펜타포트 락 페스티벌(인천 7/31~8/2)	

8월(August)

일	월	화	수	목	금	토
특이사항						1 o 싸이흠뻑쇼-수원 (수원, 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)	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	22 o 싸이흠뻑쇼-대전 (대전, 8/22~8/23)
23	24	25	26	27	28	29 o Sustainable Wave Festival (인천, 8/29~8/30)
30	31					

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