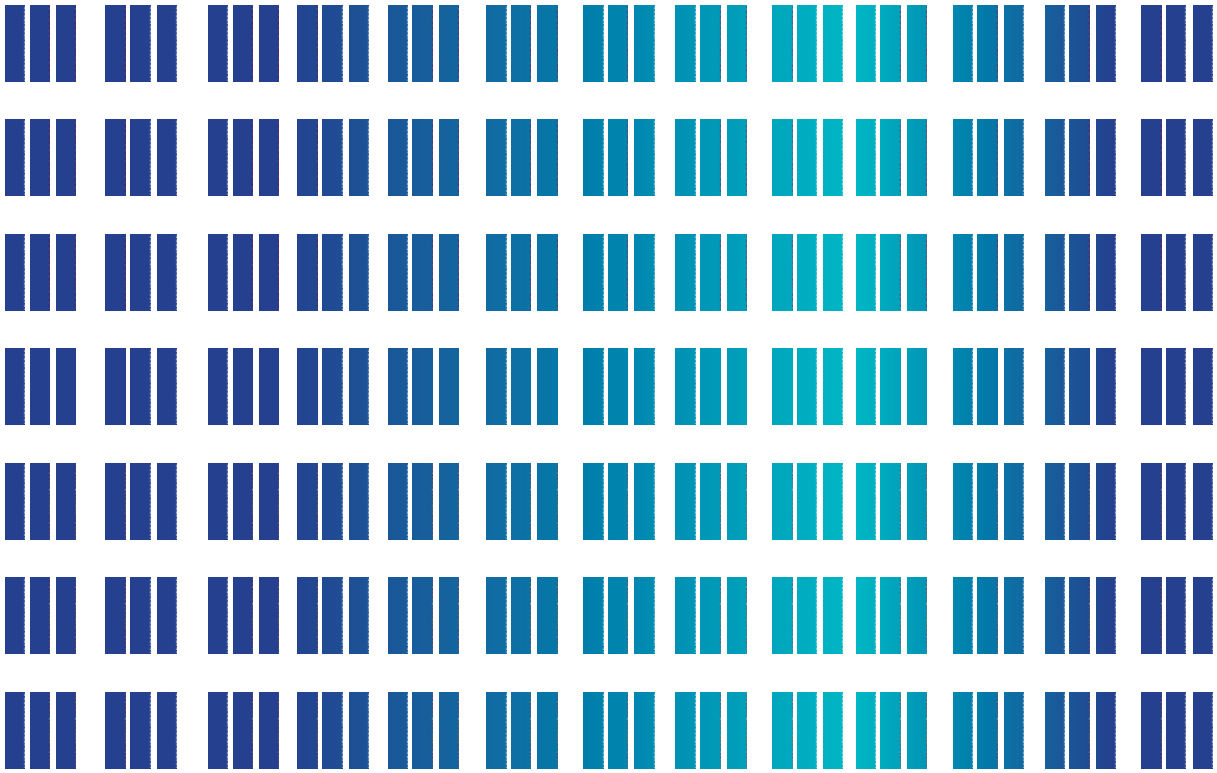
KICI DSR Vol. 25-06

한국정보통신산업연구원

Digital Safety Report

10월호



KICI 한국정보통신 산업연구원

한국정보통신산업연구원

Digital Safety Report

Digital Safety Report Contents

01 건축적 관점에서 바라본 데이터센터의 안전성 확보

㈜ 간삼건축
남영호 소장 (건축사)

들어가며

데이터센터는 4차 산업혁명 시대를 견인하는 핵심 인프라로서, 데이터의 안정적 운영과 보호가 불가결한 요소로 자리매김하고 있다. 일상에서 무한히 생성되는 방대한 데이터를 언제 어디서든 신속하고 손쉽게 활용할 수 있도록 하는 데이터센터는 단순한 저장 공간을 넘어 재난 상황에서도 안정적으로 운영될 수 있는 능동적 대응 체계 구축이 필수적이다. 하지만 최근 국내외에서 발생한 다양한 데이터센터 사고들은 다수 사용자에게 심각한 피해와 일상의 불편을 초래하였으며, 이는 데이터센터의 물리적·구조적·시스템적 안전성을 종합적으로 고려한 건축적 설계의 중요성을 다시 한 번 부각하는 계기가 되었다. 이에 데이터센터의 안전성 확보를 위한 건축적 측면에서 고찰해보고자 한다.

데이터센터의 디지털 재난 사고

최근 데이터센터 사고들은 장비 결함이나 유지관리 부주의와 같은 다양한 요인에 기인하지만, 건축적 측면에서는 주요 시설의 배치 계획과 각종 장비의 통합 구성이 디지털 재난 발생의 핵심 요소 중 하나로 평가된다.

2021년 가산동 내 한 데이터센터에서는 비상 발전기실에 설치된 화재 진압 설비인 이산화탄소 소화가스 누출로 인한 인명사고가 발생한 바 있으며, 이 사건을 계기로 소방법이 개정되어 친환경 소화가스 설비가 추가된 사례가 있다.

2022년 판교의 데이터센터 화재는 인명 피해는 없었으나, 불특정 다수의 서비스 사용 장애를 초래하여 사용자 불편을 야기하였다. 이후 UPS용 축전지에 대한 건축적 세부 설치 기준이 수립되고, 국내 데이터센터 전반에 걸쳐 시설 대응 계획에 반영되고 있는 상황이다.

2025년 발생한 국가 데이터센터 화재는 국가 행정 전산망의 절반 이상을 마비시키고 주요 서비스(정부 24, 국민신문고 등)를 수일간 중단시켜 상당한 불편을 초래하였다. 2022년도 판교 데이터센터 화재 사고와 더불어 주요 원인은 유지관리 이슈 및 노후화된 장비의 결함으로 분석되지만, 건축적 공간 구획 미흡과 화재 확산 방지 구조 결여가 피해 규모를 더욱 키운 것으로 판단된다.

이처럼 데이터센터 재난 및 사고를 예방하기 위해서는 건축적 측면에서 주요 시설의 특성과 안전성을 면밀히 고려하여 유사시 피해 확산을 차단할 수 있도록 체계적인 계획과 설계가 필요하며, 아울러 사전 징후 탐지를 통한 조기 대응 시스템 구축도 매우 중요하다.

데이터센터 재난 사고를 대비하는 건축적 고찰

1. 주요 시설의 내화 구조 적용

주요 시설의 내화구조 적용은 [건축물의 피난·방화구조 등의 기준에 관한 규칙]에 근거하여 각 건축물의 규모와 특성에 맞게 반드시 준수되어야 한다. 데이터센터는 내부 화재 위험을 감안하여 법령상 요구하는 내화 성능 기준보다 강화된 내화구조가 요구된다. 주요 구조부(벽, 바닥, 슬래브, 천장 등) 이외에 주요시설의 비구조 요소(칸막이벽, 천장재, 바닥재 등)도 준불연 이상의 내화성을 갖추도록 권장된다. 이는 내부 공간에서의 화재 확산을 방지하고 긴급 상황 시 피난 경로의 안전도를 확보하는 데 중요한 요소이다. 특히 주요시설인 "전산실, 전기실, UPS실, 배터리실, 비상 발전기실" 등은 2시간 이상의 내화 성능을 갖춘 방화구획으로 분리되어야 하며, 데이터센터 운영의 중추인 상황실 또한 동일한 내화 기준에 따라 방화구획을 완비해야 한다. 이러한 내화 구조는 재난 발생 시 확산을 효과적으로 차단하여 인명 피해를 최소화하고, 설비 피해를 제한하는 데 결정적인 역할을 한다.

종합적으로 데이터센터 내 주요 시설에 적용되는 내화구조는 재난 발생 시 피해 확산을 효과적으로 억제하고, 안전한 운영을 보장하는 건축 설계의 핵심 요소이며, 이는 디지털 사회의 기반 인프라로써 데이터센터의 지속 가능성과 신뢰성 확보에 필수적이다.

2. 주요 시설의 구획 및 피해확산 방지

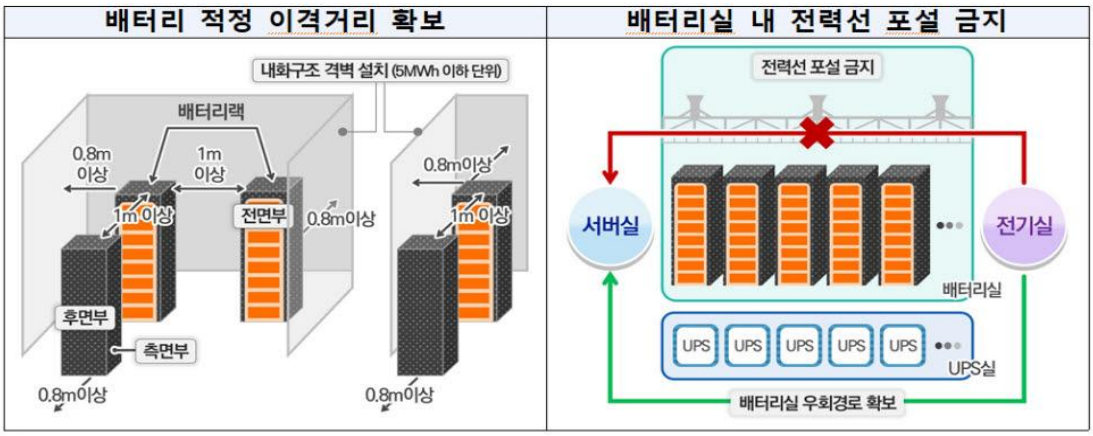
데이터센터 내 주요 공간인 전산실, 무정전전원장치(UPS)실, 배터리실, 발전기실, 통신실, 상황실 등은 각각 독립적인 내화구조로 엄격히 분리되어야 하며, 내화 성능을 충족하는 벽체 및 슬래브로 방화 구획이 이루어져야 한다. 창문 및 출입문은 비차열 기준을 만족하는 내화 인정 제품을 적용해 화재 시 열 차단 및 확산 방지가 가능하도록 설계한다.

특히, 리튬전지 설치 공간은 [한국전기설비규정(KEC)], 집적정보통신시설 보호지침, 산업안전보건법, 소방 관련 법령 및 단체 표준에 근거해 별도 분리 격실로 배치하는 것이 필수적이다. 이를 통해 화재 및 열폭주 위험의 전파를 차단하고 재난 시 피해 확산 최소화 및 데이터 안전성을 확보한다.

최근 데이터센터 설계는 모듈 단위별 세분화된 시스템 구성 방식을 채택하여, 각 모듈 별 독립적 재난 대응 체계를 마련함으로써 다중 장애 시 신속한 격리와 연쇄 피해 방지 기능을 강화하고 있다. 그러나 기존 구축된 데이터센터는 구획과 대응 체계의 부재로 인해 재난 대응에 한계가 있어, 지속적인 관리 및 개선 조치가 요구되며 현실적으로 어려움이 공존한다.

가장 중요한 것은 재난 요소를 선제적으로 탐지·예방하고, 건축 설계를 통해 이후 피해 확산을 사전에 억제하는 것으로, 체계적인 위험 평가와 방화 구획 강화, 조기 경보 및 대응 시스템 통합 구축이 필수적이다. 이는 데이터센터의 물리적 안전성 증대와 운영 연속성 확보를 위한 핵심 전략이다.

〈 배터리실 구조적 안정성 확보 예시 〉



(출처 : 과학기술정보통신부 '디지털서비스 안정성 강화 방안' 일부 발췌) 한국전기설비규정 512.1.6의 다를 준용한 리튬전지 계통의 배터리 설치 시 이격거리 및 상부 주 전력선 포설에 따른 2차 사고방지를 위한 조치 및 규칙을 통해 장비 화재 시 피해 확산 방지 및 2차 피해 방지를 고려

3. 재난의 사전 탐지 및 대응

데이터센터의 재난 대비에 있어 가장 중요한 요소는 재난 발생 요소를 건축 설계 단계에서 철저히 최소화하는 것이다. 이를 위해 건축가는 구조적 내화 성능 강화, 방화 구획의 엄격한 배치, 내진·내풍 설계 등을 적용하여 재난 발생 가능성을 본질적으로 낮춘다. 이와 함께 재난 발생 전 단계에서 선제적 탐지 및 신속 대응을 가능하게 하는 다층적 감지 시스템 구축이 필수적이다. 국내 L 데이터센터 운영사의 경우 자체 기술로 개발한 AI 기반의 영상, 열, 연기, 가스 감지 등을 통합한 감지시스템(AI CCTV)을 도입하여 적용 및 운영하고도 있다. 이를 통해 잠재적 화재 및 이상 신호를 조기에 포착하며, AI 기반의 데이터 분석을 통해 오탐률을 줄이고 실제 위협 상황을 신속하게 인지할 수 있다.

이와 함께, 건축물 내 기계 및 전기 설비 전반에 대해 예방 정비(Preventive Maintenance) 체계를 도입하고, 이를 BMS(Building Management System)와 연동하여 설비 상태 및 이상 징후를 지속적으로 모니터링함으로써 각종 설비의 수명 예측, 고장 예측 및 에너지 효율 최적화에 기여하며, 이상 발견 시 즉각적인 경고 및 자동 제어 기능을 수행할 수 있다.

궁극적으로 건축적 예방 설계와 첨단 ICT 기반 조기 재난 탐지 시스템 융합을 통해 데이터센터의 물리적 안전성 및 운영 연속성을 보장할 수 있을 것이다.

4. DR(Disaster Recovery) 시스템 구축

최근 발생한 데이터센터의 각종 재난에 따른 피해는 중요 데이터의 단일 경로, 단일 시설의 집중화에 따라 그 피해가 컸다. 국내 금융권의 자체 센터는 별도 금융감독원 기준 및 각종 지침에 따라 고객 데이터의 안정적

보관을 위해 DR 구축을 필수로 하고 있다. 다만, 각종 상업형 센터의 입주사는 해당 서비스의 특성 및 중요도에 따라 DR 구축을 하지 않는 경우도 다수이다.

데이터센터의 DR 시스템은 작게는 단일 데이터센터 내의 물리적 이중화(무중단 운영을 위한 기계·전기의 이중화 공급계통 구축)를 통한 전산 장비의 안정성 확보에서부터 크게는 데이터센터 간의 물리적 이중화(적정 이격거리를 확보한 별도의 데이터센터 구축)를 통한 실시간 동기화(백업)이 있다. 이를 통해 장애 발생 시 즉시 DR 시스템을 통해 서비스의 연속성을 확보할 수 있다.

단일 데이터센터의 건축 설계 단계에서부터 DR 시스템을 고려해 구역 별 방화 구획, 인프라 이중화, 신속 복구 절차를 정의하고, 이를 위한 전용 공간·설비 및 AI 감시·복구 자동화 솔루션 통합을 통해 무중단 운영과 업무 연속성 실현이 가능하다.

(출처 : Shutterstock: https://www.shutterstock.com/search/data-center-diagram)

5. 인명피해 방지를 위한 시설

[건축물의 피난·방화구조 등의 기준에 관한 규칙], 데이터센터 방화기준(KFS-1280), [방송통신발전 기본법] 등 관련 법규와 국내외 주요 안전기준에 따르면, 데이터센터는 재난 시 데이터 안전 확보 뿐만 아니라 인명 피해 방지에도 중점을 두어야 한다.

해외 데이터센터 고객사(CSP)들은 재난 상황에서 인명 보호와 화재 진화를 최우선 과제로 삼아, 서버룸 소방 시설을 기존 소화가스가 아닌 중앙소방기술심의를 거쳐 살수소화장치(스프링클러)를 적용하는 경우도 있다. 이는 화재 시 소화 효과는 물론, 인체에 대한 피해 위험을 최소화하기 위함이다.

이렇게 데이터센터는 설계 및 운영 단계에서 반드시 지켜야 할 기본 요건인 비상구, 피난통로, 비상계단, 방화

구획 등 적합한 설치와 유지는 필수사항이며, 더불어 안전 관리 체계 구축을 통해 화재 감지, 대응, 비상 대피, 교육 및 모의 훈련 등 지속적인 기술과 프로세스 업그레이드를 시행해야 인명 피해 리스크를 효과적으로 줄일 수 있다.

결론

지금까지 데이터센터의 재난 시에도 안전성 확보를 위한 방안에 대하여 건축적 관점에서 살펴보았다. 현대 데이터센터는 디지털 사회의 중추적 인프라로써 대규모 데이터의 안정적 운영과 보호를 위해 건축적 안전성 확보가 필수적이다. 데이터센터의 안전성은 재난 발생 요인의 최소화를 위한 건축 설계에서 출발한다. 내화 구조 강화, 엄격한 방화 구획 설치, 구조적 안전성 확보 등이 근본적이며, 주요 시설 별로 내화 성능을 갖춘 별도 방화 구획의 격실 배치가 재난 확산 방지에 결정적인 역할을 한다.

더불어 모듈 단위 설계와 AI 기반 다층 감지 시스템을 통한 조기 재난 탐지, BMS와 연계된 예방 정비 체계의 구축은 재난의 선제적 대응이 가능한 요소이다. 이는 장비의 이상 징후를 실시간으로 모니터링하고, 재난 발생 가능성을 사전에 예측하여 신속한 대응을 가능하게 한다. 이러한 건축적 대비와 첨단 ICT 시스템의 융합은 데이터센터의 물리적 안전성과 운영 연속성을 극대화하여, 재난 시에도 데이터의 무결성과 시스템 가용성을 확보할 수 있다고 판단한다.

따라서 데이터센터는 건축 설계 단계 구조적 안전과 첨단 기술 기반의 통합 감지 및 관리 시스템이 서로 조화롭게 작동하는 통합 전략으로 접근해야 하며, 이를 통해 지속 가능하고 신뢰성 있는 데이터 인프라를 구현할 수 있다. 이와 같은 균형 잡힌 접근만이 미래 디지털 사회에서 데이터센터가 안정적이고 안전하게 제 역할을 수행할 수 있는 토대가 될 것이다.

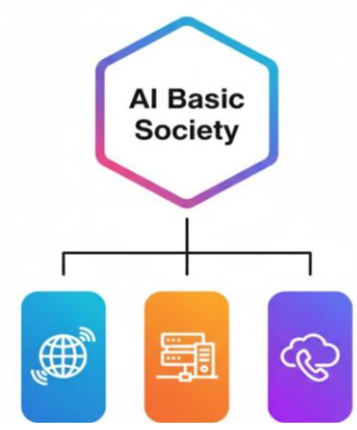
02 AI 기본사회를 위한 디지털 재난 안전 고도화 방향

KICI 디지털안전본부
신현철 디지털안전관제센터장

AI 기본사회의 전제 조건

우리 사회는 인공지능(AI) 기술이 사회 전반의 운영 시스템과 결합하는 'AI 기본사회'로 빠르게 전환하고 있다. AI는 특정 산업 분야를 넘어 경제, 행정, 문화 등 사회 전반의 핵심 기능을 수행하는 보편적 기술로 자리 잡고 있다.

이러한 AI 기술의 광범위한 적용과 확산은 반드시 안정적인 디지털 인프라의 뒷받침을 전제로 한다. AI 기본사회를 구성하는 핵심 디지털 인프라는 ①데이터를 전송하는 '기간통신망', ②데이터를 저장하고 연산하는 '데이터센터(IDC)', 그리고 ③서비스를 제공하는 '부가통신서비스(클라우드 및 플랫폼)'로 구성된다.



AI 기본사회에서 디지털 인프라의 안정성은 과거 산업 사회의 전력, 수도, 교통망과 같은 국가 기간시설과 동등하거나 그 이상의 중요성을 갖는다. AI 시스템이 정교하게 설계되더라도 네트워크 중단, IDC 정전, 플랫폼 서비스가 마비된다면, AI 기반의 사회 시스템은 즉각적으로 기능 부전에 빠지게 된다. 2018년 통신구 화재, 2021년 네트워크 장애, 2022년 판교 데이터센터 화재, 2025년 국가정보자원관리원 화재 등 대규모 인프라 및 플랫폼 장애는, 특정 서비스의 중단이 단순한 불편을 넘어 사회 재난 수준의 파급력을 가질 수 있음을 명확히 보여주었다.

이처럼 AI 기본사회로의 성공적인 이행은 AI 모델의 기술적 진보 뿐만 아니라, 이 모든 서비스의 기반이 되는 디지털 인프라의 '안정적이고 지속적인 운용'을 어떻게 보장할 것인가의 문제와 직결된다.

AI 기본사회에서의 인프라 역할

AI 기본사회 이전에 현대사회에서 디지털 인프라는 선택적 서비스가 아닌, 사회 시스템 유지를 위한 필수 서비스로서의 성격을 갖고 있다. 이는 데이터의 수집-전송-저장-연산-활용의 모든 단계에서 중단이 곧 사회적·경제적으로 큰 파장을 야기할 수 있음을 의미한다.

기간통신망은 오랫동안 초고속 인터넷과 모바일 통신을 제공하며 디지털 경제의 기반이 되어왔다. 과거 통신망의 핵심 성능이 '광대역성(Bandwidth)'이었다면, AI 시대에는 '초저지연성(Ultra-low Latency)'과

'초연결성(Massive Connectivity)'이 핵심 요구사항으로 추가된다. 예를 들어, 자율주행차가 도로 정보를 0.1초 지연하여 수신하거나 원격 수술 로봇의 반응이 지연된다면, 이는 단순한 서비스 품질 저하가 아닌 물리적 사고 및 재난으로 직결된다. 즉, AI 서비스의 실시간 판단과 제어를 위해 통신망은 한 치의 오차나 지연도 허용되지 않는 수준의 무중단 운영이 요구된다.

데이터센터(IDC)는 과거 웹사이트와 기업 데이터를 '저장(Storage)'하는 역할에서, 이미 클라우드 시대를 거치며 애플리케이션을 '운영(Operation)'하는 핵심 시설로 기능해왔다. AI 시대는 여기서 더 나아가 IDC를 '고성능 연산(Compute) 시설'로 변모시키고 있다. AI 모델 학습은 수천 개의 GPU를 동시에 가동하며 막대한 전력을 소모하는 작업이다. 이 과정에서 발생하는 순간적인 전력 불안정이나 냉각 시스템 오류는 수개월간의 학습 성과와 막대한 비용을 무위로 돌릴 수 있다. 데이터센터의 기능 상실은 화재, 정전 등의 물리적 재난 뿐만 아니라 사이버 공격, 작업자의 오류 등을 통해서도 발생할 수 있다.

부가통신서비스(Cloud/Platform)는 모바일 메신저, 결제, 포털 서비스 등을 통해 국민 대다수가 의존하는 사회 기반 서비스가 되었다. 2022년 카카오 장애 사례는 특정 플랫폼 기업의 서비스 중단이 사회 전체를 마비시킬 수 있음을 보여주었다. AI 시대는 이러한 '소수 플랫폼으로의 집중 및 종속' 현상이 더욱 심화될 것으로 예상된다. 천문학적인 비용이 드는 파운데이션 모델 개발 및 운영 인프라를 모든 기업이 갖출 수 없으므로, 대부분의 AI 서비스는 AWS, MS Azure, Google Cloud, Naver Cloud 등 소수의 CSP(클라우드 서비스 제공자)가 제공하는 AI API에 의존하게 된다. 이는 해당 CSP의 장애가 곧 그 위에 구축된 수만 개의 AI 서비스 전체의 동시 중단으로 이어지는 '연쇄 장애(Cascading Failure)'의 위험을 극대화한다.

이처럼, 기간통신, 데이터센터, 부가통신서비스는 AI 기본사회 시스템 전반에 영향을 미칠 수 있는 단일 장애점(Single Point od Failure)으로 작용할 잠재적인 위험성을 내포하고 있다. 이들 인프라 중 하나의 기능 장애가 전체 시스템의 안정성을 저해하는 구조적 취약점이 존재한다.

해외사례로 본 인프라 유형별 회복탄력성 확보 방향

디지털 인프라는 '절대 장애가 발생하지 않아야 한다'는 전통적인 안정성(Stability)의 개념을 넘어, '장애가 발생할 수 있음'을 전제로 구축되어야 한다. 즉, 장애 발생 시에도 핵심 기능을 유지하고 신속하게 정상 상태로 복구되는 '회복탄력성(Resilience)'의 확보가 중요하다.

AI 기본사회로의 전환에 있어 글로벌 데이터 전송은 지리적 분산을 통한 '물리적 경로 다각화'를 전제로 해야 한다. 2006년 12월 대만 남부 해역의 지진으로 인해 6개 해저케이블이 절단됨에 따라 한국을 포함한 아시아 전역(대만과 홍콩, 중국 등)의 인터넷 속도가 급감하고 일부 서비스가 마비되는 등 대규모 피해가 발생했다. 이는 단순 유무선 통신사업자의 주요시설 이중화를 넘어, 해저케이블 육양국 및 포설 경로를 지리적으로 분산시켜야 할 필요성을 시사한다. 특히 한국은 국제 트래픽에 대한 해저케이블 의존도가 높고, 남해안에 집중되어 있어 지리적 리스크가 크기 때문에 더욱 유의해야 할 필요가 있다.

데이터센터의 회복탄력성은 동일한 건물을 두 개 짓는 고전적인 이중화 재해복구(DR) 개념을 넘어, 건물 내부의 설계에서부터 시작되어야 한다. 첫째, '전력 계통의 완벽한 분리'가 필요하다. 2022년 SK C&C 화재 이후 UPS와 배터리실의 공간분리, 예비전력설비 이중화 등 정부의 대책마련이 있었다. 이를 통해 주/예비 전력의 UPS, 배터리실, 배전반이 각각 물리적으로 분리된 공간에 배치되어 상호 화재나 침수로부터 영향을 받지 않도록 안정성을 확보하도록 하고 있다. 둘째, '독립적 가용 영역(Availability Zone, AZ) 구조'가 필요하다. 아마존(AWS) 등 글로벌 CSP들이 적용하는 방식처럼, 대형 IDC는 건물 자체를 '하나의 장애가 다른 곳으로 전파되지 않는' 복수의 독립 구역(AZ)으로 분할해야 한다. 각 AZ는 독립적인 전력, 냉각, 네트워크 장비를 가지며, 한 AZ의 장애가 다른 AZ로 확산되지 않아야 한다. 데이터센터의 장애는 연쇄적인 서비스 장애를 야기함에 따라, 특정 데이터센터가 단일 장애점이 되는 것을 구조적으로 차단하여 데이터센터 회복탄력성을 확보하고 있는 것으로 나타난다.

부가통신서비스의 회복탄력성은 시스템적 오류에 대한 복구가 주요 과제이다. '24년 크라우드스트라이크社의 보안SW 업데이트에 따른 마이크로소프트 서비스 장애로 글로벌 IT대란이 발생하여 항공편 취소, 금융 서비스 지연, 생산공장 중단 등 블루스크린으로 인한 대규모 피해가 있었다. 이 외 '22년 카카오 장애 등 부가통신서비스의 '논리적·운영적' 회복탄력성의 중요성을 보여주는 사례는 흔하게 일어나고 있으며, 부가통신서비스의 회복탄력성 확보는 소프트웨어 운영 취약성을 어떻게 관리하는지가 중요하다. 이를 위해서는 핵심 기능에 대한 논리적 분리(Decoupling)를 통한 장애전파 차단이 필요하고, 핵심 시스템에 적용되는 모든 소프트웨어 업데이트는 일부 사용자에게 선적용하고 문제 발생 시 즉시 자동 롤백하는 안전한 배포 파이프라인을 갖춰야 한다. 또한, 넷플릭스의 '카오스 몽키'와 같이 선제적으로 장애 복구를 테스트할 수 있도록 반복적인 훈련이 필요하다.

'서비스 연속성'을 위한 아키텍처 중심의 접근

AI 기본사회의 편의와 효율성은 '디지털 인프라'의 안정성이 보장될 때만 지속될 수 있다. 기간통신망, 데이터센터, 그리고 클라우드 및 플랫폼으로 대표되는 부가통신서비스는 개별 기업의 사적인 상용 서비스를 넘어, 사회 전체가 의존하는 공공적 성격의 인프라가 되었다. 이러한 필수 인프라의 안정성을 확보하는 것은 실제 장애 사례들이 증명하듯, 시스템은 언제든 실패할 수 있다는 가능성을 인정하고, 장애 발생 시에도 즉시 복구하여 서비스 연속성을 보장하는 '기술적 회복탄력성'을 시스템에 내재화하는 것이 무엇보다 중요하다. 결국 AI 시대의 진정한 인프라 경쟁력은 어떠한 재난 상황에서도 '중단 없는' 서비스를 제공할 수 있도록 인프라를 설계하고 운영하는 구체적인 기술 역량에 달려있을 것이다.

03 전문가 인터뷰

- ICT폴리텍대학 김영철 교수를 만나다 -

ICT폴리텍대학
김영철 교수

Q1. 우선 김영철 교수님에 대해서 소개 부탁드립니다.

A1. 현재, ICT 폴리텍 대학 정보보안학과에서 근무하며, 주로 방송통신과 네트워크 보안 그리고 재난 분야를 연구하고 있습니다.
2004년도 대학에 임용되기 전에 주로 통신 분야를 연구하였기 때문에 이러한 경험을 바탕으로 한국항공대학교에서 공학박사를 취득하였습니다. 그리고 현 대학에서는 방송통신설비학과로 임용되어 통신을 기반으로 방송을 하게 되었고, 유선케이블과 IPTV 및 공중파 사업자들과 교류하였습니다. 그러나 방송이 디지털로 전환되면서 미래에 다가올 새로운 분야를 탐구해야겠다는 생각으로 재난과 주 전공인 통신이 접목된 방송통신재난 분야를 개척하게 되었습니다.

Q2. 교수님께서는 디지털 재난·장애의 안전관리에 관한 업무 경험이 있으실까요?

A2. 2007년도 재난관리지도사를 취득하였을 시점에는 통신재난에 대한 개념 자체가 없었다고 생각합니다. 그 당시에는 정보통신부(現 과학기술정보통신부)에서 정보통신 분야의 위기관리표준 및 위기대응실무 매뉴얼에 대한 체계를 준비하고 있던 시점이기 때문에 담당 주무관님들과 매뉴얼 검토 및 체계화에 일조하였습니다. 2011년도 우면산 산사태로 EBS 침수가 발생하였을 때 해당 매뉴얼을 바탕으로 비상기획관에서 빠르게 대응하여 EBS 정상화가 조속히 이루어질 수 있었던 것으로 알고 있습니다.
특히 기억에 남았던 것은 2018년도 KT 아현통신국사 화재에 과학기술정보통신부(이하 과기정통부)의 TF팀에 민간위원으로 참여하여, 여러 문제점을 발견하고 해결하고자 노력하면서 민관의 연결고리 역할을 했었던 것이 가장 기억에 남습니다.

Q3. 교수님께서 한국디지털콘텐츠학회 회장직을 맡고 계신 것으로 아는데, 디지털 콘텐츠 산업에서도 디지털 재난·장애의 안전관리가 중요하다고 생각하실까요?

A3. 최근 학회 논문 투고를 보게 되면, 디지털콘텐츠라는 학문적 범위가 IT를 아우르고 있는 듯 합니다. 당연히 디지털 재난 및 장애와 관련된 다양한 논문(메타버스, 디지털 트윈 등)이 제출되고 있고, 저 역시 디지털 안전관리에 대한 중요성을 인식하고 있습니다. 따라서 이와 관련된 분야의 전문가 분들을 초청하여 모시고 하계 학술대회에서 발표 등을 통하여 학회 회원 분들에게 학문적으로 더 넓은 시야를 가질 수 있도록 기회를 제공하고 있습니다.

Q4. 최근 발생한 국내외 데이터센터 장애 사례 중 주목할 만한 사례는 어떤 것이 있을까요? 또 해당 사례를 보았을 때, 한국의 데이터센터 사업자들이 교훈 삼아야 할 점은 무엇이라고 생각하시나요?

A4. 가장 최근에 발생한 국내 사례는 국가정보자원관리원 리튬이온 배터리 폭발 사고(25.09.26.)이고, 해외 사례로는 미국 오리건주의 X(前 트위터)의 데이터센터 화재(25.05.22.)가 있습니다. 국가정보자원관리원 사고의 경우에는 국가적 피해 심각성이 상당한데, 과거 SK C&C 화재 사고를 거울 삼지 못한 것이 이번 사고를 크게 키웠다고 생각합니다. 다음으로 X의 데이터센터 화재 사고는 철저한 비밀 유지로 어떠한 피해가 있었는지 정확히 가늠이 되지는 않으나, 대규모 서비스 중단 등의 피해는 없었던 것으로 보여집니다. 이 부분은 모순적이라고 생각될 수도 있지만, 미국만의 자율적 기업 문화가 가지고 있는 특색을 바탕으로 자체적인 위기관리 능력을 갖추고 있었기 때문이라고 생각합니다.

국내의 경우 데이터의 이중화에 관한 이야기가 나오는 상황으로, 데이터 백업이 문제가 되는 것이 아니라 운용 중인 응용 소프트웨어의 백업이 문제가 되고 있다고 봅니다. 이를 백업해 놓지 않음으로써 전환이 지연되는 문제가 발생하는 것이죠.

Q5. 최근 데이터센터 장애 원인은 주로 전력 계통(정전, UPS 고장), 냉각(냉각탑 문제), 화재 등 물리적 요소가 많습니다. 교수님께서 보시기에 국내 데이터센터는 어떤 위험에 가장 취약하다고 생각하시나요?

A5. 국내 데이터센터의 취약점은 절차적 공정이 부족함에 있다고 생각합니다. 철저하게 위험 요소가 있는 부분을 절차에 맞추어 관리하였다면 문제가 발생하지 않았을 수 있는데, 안일한 생각으로 위험 요소들을 놓치고 있는 것 같습니다. 이와 관련하여 이번 국가정보자원관리원을 예시로 보면 전문성을 갖춘 업체를 선정하였음에도 불구하고 실제 작업자는 숙련된 자원이 아니었다는 것이 문제라 볼 수 있습니다. 그렇기 때문에 철저한 교육 및 지속적 반복 훈련이 함께 이루어져야 이러한 위험 요소들을 극복할 수 있다고 생각합니다.

Q6. IT 및 네트워크 구조의 복잡성 심화로 인하여 IT 및 네트워크 관련 장애가 증가하고 있다는 조사 결과가 있습니다. 이러한 장애 원인에 대해서는 어떻게 대비할 수 있을까요?

A6. IT는 당연하게도 발전하고, 그 과정에서 새로운 문제들 또한 야기합니다. 아무리 좋은 자원이 있다 하더라도 틈새가 생길 수 밖에 없는 상황이라는 것입니다. 그렇기 때문에 앞서 거론한 바와 같이 새로운 문제를 탐구하고 이를 해결하기 위한 노력으로 교육과 훈련이 반복적으로 이루어져야 한다고 봅니다. 어떻게 보면 네트워크도 하나의 유기체처럼 살아서 움직인다고 표현하는데요. 예기치 못한 장애나 고장, 복잡하고 심화된 네트워크 장애 등은 숙력자의 경험과 대응 능력과 이를 도와줄 수 있는 최신 기술(AI 등)이 함께 적용되어야만 해결할 수 있다고 생각합니다.

Q7. 데이터센터 장애 발생 원인 중 인적 오류는 데이터센터 운영에서 지속적인 과제로 꼽히고 있습니다. 인적 오류를 최소화하기 위한 교육 체계나 전문 인력 양성은 어떤 방향으로 이루어져야 한다고 생각하시나요?

A7. 최근 안전에 대한 경각심은 많이 커지고 있는 것 같습니다. 그렇지만 정보통신분야의 안전에 대한 교육은 여전히 부족하다고 느껴집니다. 당연히 기술에 대한 고장이나 장애 처리 등에 관련된 교육을 실시하겠지만, 위기를 의식화하고 조직적으로 대응할 수 있는 교육은 많이 부족한 실정입니다. 실제로 관련 전문 교육기관 등이 없다는 것만 봐도 알 수 있는데요. 따라서 정보통신 분야도 안전과 재난을 교육할 수 있는 체계를 갖출 수 있도록 제도화가 필요하지 않을까 생각합니다. 한 가지 예로써, 디지털 재난 관련 대학원 과정과 같은 전문 교육이 개설된다면 더 많은 인적 자원을 성장시킬 수 있다고 생각하는데요. 자신의 핵심 업무와 프로세스가 중단되었을 경우 그 영향이 얼마나 지대한지 볼 수 있는 업무영향분석(BIA)을 할 수 있는 역량을 갖출 수 있다면 기업에게도 큰 도움이 될 수 있을 것 같습니다.

Q8. 국내 데이터센터가 수도권에 집중되어 있어 지진과 같은 국지적인 재난 및 재해 등에 취약하다는 우려가 있습니다. 재난 관리 차원에서 데이터센터 지역 분산에 대하여 어떻게 생각하시나요?

이미지 : flaticon.com

A8. 지리적으로 수도권에 IT기업이 집중되고 있기 때문에 그러한 우려가 발생하는 것 같습니다. 재난 관리 차원이 아니더라도 데이터센터의 지역 분산은 필요하다고 생각합니다만, 이를 제도적으로 분산할 수 있도록 데이터센터 유치 지역에 세금 감면 혜택을 주고 적극적 홍보를 하는 등 지역 분산을 유도하는 것이 바람직하다고 봅니다. 특히 데이터센터 건설과 관련하여 많은 민원이 들어오고, 유치를 반대하는 지역이 발생하고 있으므로 정부 차원에서 주민들과의 소통, 인프라 확충 등 적극적인 대처가 필요하다고 생각합니다.

Q9. 전 세계적으로 이상기후가 발생하면서 폭염으로 인한 냉각장치 고장 등으로 데이터센터 장애가 발생하고 있는데요. 기후 변화로 인하여 발생할 수 있는 장애를 대비하기 위해서 어떤 노력이 필요할까요?

A9. 이미 우리는 국지적 호우나 폭염 등과 같은 예기치 못한 큰 자연재난을 경험하고 있습니다. 따라서 폭염 등과 같은 열로 인한 냉각 장치의 이상보다는 데이터센터의 지리적 위치 관리나 자체 기후 현황 파악 등의 모니터링을 강화하고, 문제 발생 시 원인에 따른 대응 방안(이중화 및 분산화 등)이나 체계를 마련하는 것이 필요하다고 생각합니다.

Q10. 생성형 AI의 확산으로 고성능 데이터센터에 대한 수요가 급증하여 데이터센터가 단순한 IT 인프라를 넘어 AI 시대의 핵심 동력으로 부상하였는데요. AI 기술의 발달로 인하여 늘어나는 트래픽 양에 대비하여 데이터센터는 어떠한 대비가 필요할까요?

A10. 대표적 국제 기업인 메타의 페이스북은 하루 수백 TB(테라바이트)나 수 PB(페타바이트)로 트래픽 양이 증가한다고 합니다. 이는 단순한 수치로 보여질 수 있으나 실제로 초빅데이터나 고성능의 NPU가 작동하게 되면, 데이터센터가 감당할 수 있는 능력의 한계치에 도달할 수 있다고 봅니다. 따라서 초기 설계 시 수용 가능한 데이터 용량을 산정하고, 관련된 전력 및 트래픽 양을 단계별로 조정할 수 있도록 설계가 필요할 것으로 생각합니다. 특히나, 재난 관리 차원에서 체계적인 재해복구(Disaster Recovery: DR)와 업무연속성계획(Business Continuity Planning: BCP)은 중요한 요소이며, AI 기반의 트래픽 예측과 최적화 기술이 필요할 것으로 보입니다.

04 디지털 안전 관제 이슈

pay 증권

2025.09.01
카카오페이증권 입출금 서비스 장애

인터넷우체국 ePOST kr

2025.09.02
우체국 웹/앱 접속불가 및 서비스 장애

2025.09.04
티맵 네트워크 관련 서비스 장애

NAVER

2025.09.07 MS Edge 브라우저 내 네이버 메인 홈페이지 접속 서비스 장애
2025.09.24 모바일 웹 내 네이버 카페 검색 서비스 동작 오류

Google Play

2025.09.12
구글 플레이스토어 접속 장애

coupang play

2025.09.17
쿠팡 플레이 결제 서비스 장애

Samsung Account

2025.09.18
삼성어카운트 웹페이지 로그인 서비스 장애

홈택스 Hometax.

2025.09.25
국세청 홈택스 접속 관련 장애 발생

하나카드

2025.09.25
하나카드 앱 접속 관련 장애 발생

05 Digital Safety Inside

국가정보자원관리원 화재

사고 개요

2025년 9월 26일 오후 8시 15분경 대전광역시 유성구에 위치한 국가정보자원관리원 대전 본원에서 화재가 발생하였다. 화재는 무정전전원장치(UPS) 점검 및 교체 과정 중 리튬이온배터리 과열 또는 단락(합선)으로 인하여 발생한 것으로 추정되고 있으나, 정확한 발화 원인은 현재 국립과학수사연구원에서 감식 중이다.

화재는 약 3시간 만에 진화되었고, 작업자 한 명이 경상을 입었으나 사망자는 발생하지 않았다.

이번 화재 사고로 인하여 국가 주요 행정 전산망이 광범위하게 마비되었다. 행정안전부는 사고 다음날인 27일 1차 브리핑을 통하여 화재로 인하여 총 647개 전산시스템이 중단되었다고 발표하였으나, 이후 연동기관 및 지원시스템을 포함한 추가 분석 결과 피해 범위가 확대되어 10월 9일 기준 총 709개의 시스템이 중단된 것으로 정정 발표하였다. 이에 따라 주민등록, 세금 등 전국 단위의 행정서비스가 중단 또는 지연되는 등 광범위한 행정 혼란이 발생하였다.

[출처] 국정자원 장애시스템 8개 추가 정상화 … 복구율 71.7% (NEWS1, 2025. 10. 24., https://www.news1.kr/local/moi/5953106

복구 현황

정부는 사고 다음날인 27일부터 중앙재난안전대책본부를 가동하여 복구작업에 착수하였다. 행정안전부는 관계부처 및 민가 IT전문인력 약 900명을 투입하여 24시간 체계의 복구 작업을 진행하였다. 복구는 우선순위에 따라 핵심 1등급 업무, 대민서비스, 내부 행정업무 순으로 추진되었다. 그 결과 9월 27일 기준 약 5% 수준이던 복구율은 10월 9일 기준으로 27%, 10월 26일 기준으로는 72% 수준으로 전체 709개 시스템 중 514개가 복구 완료되었다. 정부는 11월 초까지 90% 복구, 11월 말까지 완전 복구를 목표로 하여 작업을 이어가고 있다.

〈 시점별 주요 복구 현황 〉

일자	기준 시스템 수 (개)	복구 시스템 수 (개)	복구율 (%)	주요 내용
9.27.	647	30	5	초기 진화 후 전원 복구 작업 개시
10.01.	647	98	15.1	1등급 시스템 21개 복구
10.04.	647	134	20.7	1등급 시스템 22개 복구
10.09.	709	193	27.2	피해범위 재산정, 1등급 62.5% 복구
10.17.	709	357	50.4	전체 복구율 50% 돌파
10.22.	709	453	63.9	1등급 시스템 80% 복구
10.26.	709	514	72.5	정부디렉터리·모바일 신분증 등 복구

국민 불편 최소화를 위한 조치

한편, 정부는 화재로 인한 행정서비스 중단으로 증명서·서류 발급이 불가능한 주민센터에는 오프라인 임시 발급 창구를 운영하고, 신고 및 납부 기한이 도래한 세금 및 행정 절차는 기한을 연장하는 등 국민 불편을 최소화하기 위한 긴급 조치를 시행하고 있다. 또한 정부 24, 국민신문고 등 주요 포털 서비스는 10월 중순 이후 단계적으로 정상화되었다.

재발 방지 대책

이번 사고는 단일 데이터센터 장애로 행정망 전체가 마비되는 초유의 사태로, 국가 전산 인프라의 중앙집중적 구조의 한계를 드러냈다는 평가를 받고 있다. 행정안전부는 이를 계기로 국가 전산망의 이중화 및 분산 백업체계 도입, 민간 클라우드 활용 확대, UPS 등 전원설비 관리기준 강화 등 종합적인 재발방지 대책 마련에 착수하였다. 또한 전국의 공공기관 전산시설을 대상으로 하여 전기 및 소방 설비 긴급 점검을 시행하고, 재해복구센터의 실효성을 재검토하고 있다.

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