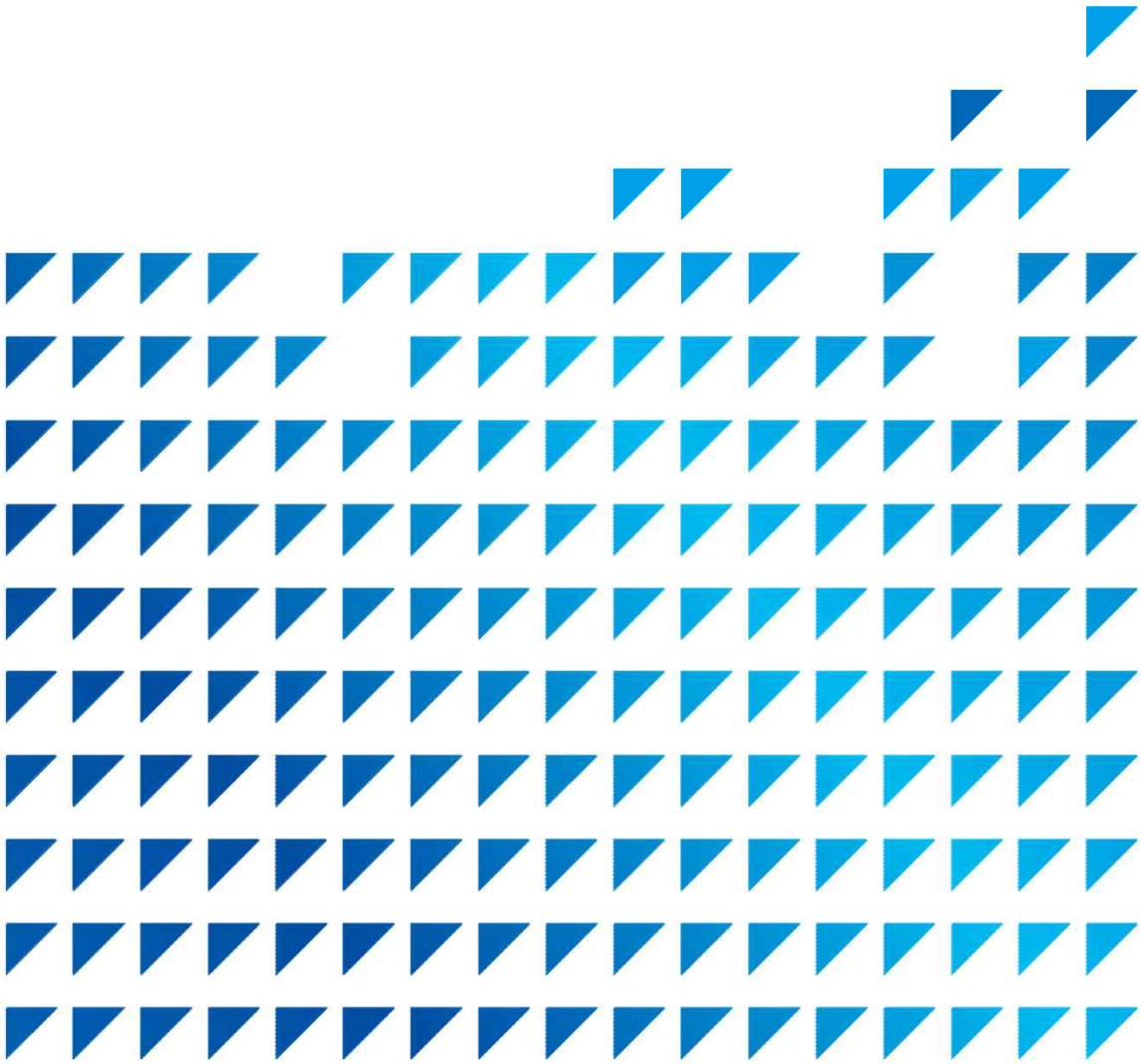
KICI DSR Vol. 26-08

한국정보통신산업연구원

Digital Safety Report

8월호



KICI 한국정보통신 산업연구원

KICI 한국정보통신산업연구원

한국정보통신산업연구원

Digital Safety Report 8월호

Contents

01 전문가 칼럼

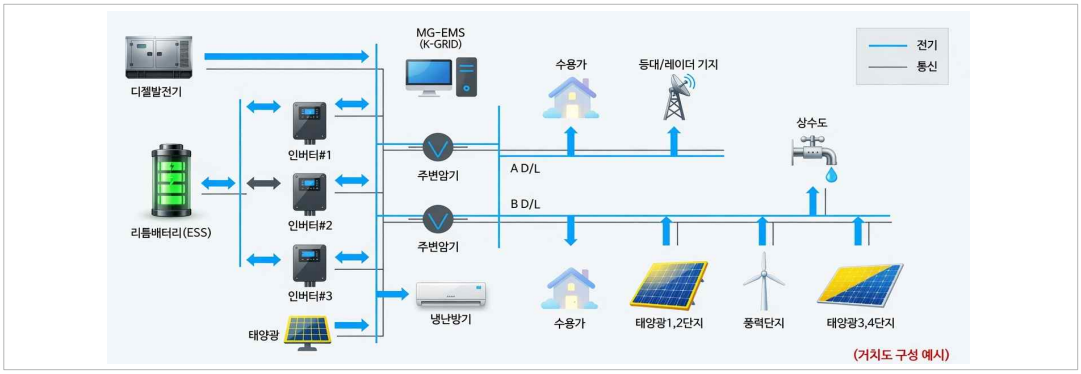
㈜한전KDN
최진대 부장 / 정보통신기술사

디지털 재난이 분산형 에너지 관리시스템에 미치는 영향과 대응방안

들어가며

오늘날 전력산업은 기후위기 대응과 탄소중립 실현이라는 전환적 환경 속에서 태양광 및 풍력 기반의 분산 에너지자원(DER, Distributed Energy Resources)을 중심으로 빠르게 재편되고 있다. 재생에너지는 탄소배출 저감과 송전손실 최소화 측면에서 전력계통의 효율성과 지속가능성에 기여하지만, 기상조건에 따른 출력 변동성이라는 구조적 한계를 내포한다. 이러한 간헐성을 보완하기 위해, 분산형 전원이 집적된 마이크로그리드 환경에서는 인공지능(AI), 빅데이터, 실시간 계측 및 제어 기술을 결합한 에너지관리시스템(EMS)과 SCADA(Supervisory Control And Data Acquisition)의 고도화가 진행되어 왔다. 그러나 고도화된 정보통신기술(ICT)과의 융합은 역설적으로 과거 자연재해에 국한되었던 재난의 범주를 '디지털 재난'이라는 예측 불가능한 영역으로 확장시켰다. 본 기고에서는 디지털 재난이 분산형 에너지관리시스템에 미치는 영향을 분석하고, 이에 대응하기 위한 회복탄력성 강화 방안을 고찰하고자 한다.

〈그림 1〉 마이크로그리드 구성 예시



[출처] 한전KDN

1. 에너지 전환의 두 얼굴과 디지털 의존증

가. 전력 공급 방식의 거대한 변화

과거 대형 발전소에서 지구 온난화를 막고 탄소 배출을 줄이기 위해 초고압선으로 멀리까지 전기를 보내던

방식이 빠르게 사라지고 있다. 대신 전기를 소비하는 지역 근처에서 직접 생산하고 소비하는 태양광 발전, 중소형 풍력발전, 연료전지 같은 '지역별 친환경 발전소(분산형 전원)'가 독립적인 작은 전력망을 이루며 급격히 늘어나는 추세이다. 이러한 방식은 송전 과정에서 버려지는 전기를 획기적으로 줄이고, 전력 자립을 가능하게 만든다.

나. 정보통신기술 융합이 가져온 양날의 검

친환경 에너지가 가진 치명적인 약점은 날씨에 따라 전기 생산량의 변동이 크다는 것이다. 이를 빈틈없이 관리하기 위해 요즘 친환경 발전망은 센서와 인공지능(AI) 기상 예측 프로그램, 그리고 실시간 전기 흐름을 조절하는 '통합 에너지 관리 시스템(EMS)'에 전적으로 의존하고 있다.

하지만 모든 시스템을 컴퓨터와 인터넷을 통해 제어하다 보니, 과거 태풍이나 지진 같은 자연재해에만 취약했던 전력망이 이제는 '인터넷망 마비나 가상 공간에서의 해킹 공격'이라는 완전히 새로운 형태의 위험에 노출되고 있다.

2. 디지털 재난과 가상 해킹이 초래하는 전력망의 타격

통신망 및 컴퓨터 관리 시스템을 겨냥한 디지털 재난은 단순히 모니터 화면이 멈추는 데 그치지 않는다. 가상 공간의 데이터 오류가 실제 현장 설비를 파괴하고, 나아가 도시 전체를 암흑으로 만드는 대규모 정전 사태로 이어질 수 있다.

가. 현장 감시 불능 및 데이터 차단

통신망 인프라 고장이나, 서버 마비, 혹은 고의적인 접속 폭주(DDOS) 공격이 발생하면 본사와 현장 발전소를 잇는 신경망이 즉각 끊어진다. 이로 인해 발전소가 지금 전압을 얼마나 유지하고 있는지, 전류는 얼마나 흐르는지 같은 핵심 정보를 전혀 알 수 없는 이른바 '전력망 깜깜이 상태'에 빠지게 된다.

나. 제어 명령 오류로 인한 설비 고장 및 화재

더 위험한 상황은 해커가 관리자 비밀번호를 훔치거나 정비 업체의 컴퓨터를 통해 관리 시스템 내부로 몰래 침투하는 경우이다.

〈표 1〉 제어 명령 오류로 인한 설비 고장 및 화재

구분	내용
넘치는 전기 차단 실패	대낮에 햇빛이 너무 강해 태양광 전기 생산량이 넘치면 전력망이 버틸 수 있도록 과도한 전기를 차단하라는 명령을 내려야 함. 하지만 통신이 먹통이 되어 이 명령이 전달되지 못 하면 전력망 전체의 균형이 깨져 동네 변전소 설비들이 연쇄적으로 가동이 중단됨
인위적인 설비 파괴	해커가 조작된 명령을 보내 대형 배터리(대용량 에너지저장장치)의 충전과 방전을 강제로 무한반복 시키거나 냉각 장치를 꺼버릴 수 있음. 이는 배터리 과열로 이어져 대형 화재를 일으키고 값비싼 자산을 순식간에 잿더미로 만들 수 있음

다. 전기 거래 정지에 따른 금전적 손실

최근의 친환경 에너지 관리 시스템은 전기만 조절하는 것이 아니라, 실시간 전기 가격을 계산해 시장에 전기를 가장 비싸게 팔 수 있는 최적의 조합을 찾아내고 자동으로 거래까지 처리한다. 디지털 재난으로 데이터가 지워지거나 정산 시스템이 다운되면, 전기를 판 사람들의 과금 내역이 누락되고 대금 지급이 불가능해져 참여 기업과 발전 사업자 모두에게 엄청난 금전적 손해를 입히게 된다.

3. 비상 회복력(Resilience) 확보를 위한 3대 안전 전략

디지털 재난은 100% 완벽하게 막는 것이 불가능하다는 전제 아래, '공격을 받거나 고장이 나더라도 핵심 기능은 멈추지 않고 스스로 빠르게 회복한다'는 기본 원칙 체계를 세워야 한다.

〈표 2〉 비상 회복력(Resilience) 확보를 위한 3대 안전 전략

강화방안	핵심기능	기대효과
구조적	• 스스로 멈추는 자율 조절 기능 탑재 • 재난안전망 및 TV 방송망 비상 연계	• 기기 자체 판단으로 안전 유지 • 비상 제어 통로 확보
기술적	• 철저한 통신망 분리 • 재반입 장비 사전 격리 검사실 운영	• 해커 침입 차단 • 바이러스 감염 예방
관리적	• 정기적인 보안 및 기능 점검 의무화 • 참여 주체 간 유기적 협력 체계 구축	• 예방 및 기록 점검 생활화 • 기획부터 운영 관리 강화

가. 구조적 가용성 방어망 : 멈추지 않는 안전 시스템 구축

현장기기에 자율 조절 기능을 탑재하면 본사의 메인 서버가 다운되더라도, 현장에 있는 태양광 인버터와 배터리들이 직접 통신하며 동네 전압 변화를 스스로 감지하게 만든다. 본사 명령 없이도 현장에서 알아서 전기를 줄이거나 늘리는 자율 조절 기능을 넣어 전력망이 혼자 멈추는 일을 방지한다.

또한 전국의 유선 인터넷망이 통째로 마비되는 최악의 상황을 대비하여, 국가 재난안전망이나 TV·라디오 방송에서 쓰는 특수 비상 주파수를 활용해야 한다. 특히 통신이 중단되어도 최소한의 안전을 위해 '발전기 긴급 정지 명령' 만큼은 무선으로 강제 전달할 수 있는 비상 수신 시스템을 마련하는 등의 강력한 비상 무선 채널을 확보해야 한다.

나. 기술적 가상방역 : 철저한 검문검색과 방화벽 구축

핵심 제어망은 외부 인터넷과의 접속 지점을 물리적으로 완전히 차단하여 데이터가 밖으로 나갈 수는 있어도 안으로 들어올 수 없는 일방향 장치를 설치하고, 시스템에 접속할 때는 아이디·비밀번호 외에도 스마트폰 인증이나 OTP 같은 추가 인증을 반드시 거치도록 의무화한다.

그리고 현장 수리나 점검을 위해 외부로 가지고 나갔던 노트북이나, USB 등은 내부 시스템에 다시 연결하기 전, 바이러스 전파 위험이 없는 별도의 '격리된 검사 컴퓨터'에서 이상 유무를 점검받는 안전 통과 프로세스를 제도화한다.

다. 관리적 거버넌스 : 기획부터 운영까지 상시 감시 체계

관련 법령의 강화 흐름에 맞춰 주기적인 예방 관리와 보안 점검을 수행해야 한다. 친환경 발전소 관리자는 매월 1회 이상 '보안 및 가동 점검표'에 따라 컴퓨터 상태를 점검하고, 접속 기록을 검사하며, 비밀번호를 변경하고, 백업 데이터를 만드는 일을 생활화해야 한다.

또한 발전소의 통합 협력체계를 수립하고, 해당 업무의 전문가를 배치하여 안정적인 운영을 위한 관리체계를 마련해야 한다. 구체적으로 발전소의 기획자, 설계자, 공사업체, 감리사, 그리고 운영자까지 총 5개 주체가 개발 단계마다 보안 서류를 투명하게 넘겨주도록 제도화 한다. 현장에는 현장 책임자로 정보통신 및 보안 자격증을 가진 전문 인력을 상시 배치하여 고도화되는 인터넷 위협에 즉각 대응할 수 있는 환경을 만든다.

4. 결론 및 제언

친환경 에너지를 확대하고 이를 컴퓨터로 스마트하게 관리하는 것은 우리가 가야 할 필수적인 길이다. 하지만 보안과 대비책이 없는 디지털 전력망은 모래 위에 쌓은 성과 같아서, 단 한 번의 해킹이나 통신 마비로도 국가 전체를 멈추게 만드는 부메랑이 되어 돌아올 수 있다. 따라서 정부와 공기업, 그리고 민간 사업자들은 단순히 전기 발전 효율을 높여 돈을 많이 버는 것에만 집중해서는 안 된다. 시스템을 만들 때부터 통신이 끊겨도 현장에서 버틸 수 있는 비상 회복력을 넣고, 강력한 해킹 차단 벽을 세우며, 매달 정기적으로 점검하는 관리 습관을 정착시켜야 한다. 이 삼박자가 맞아야만 우리 미래 세대가 안심하고 쓸 수 있는 안전하고 깨끗한 '친환경 에너지 고속도로'를 완성할 수 있을 것이다.

02 이슈 보고서

KICI 디지털안전본부
장영환 선임연구원

부가통신서비스의 통신재난·장애에 관한 고찰

Ⅰ 서론

디지털 전환이 가속화되면서 부가통신서비스는 국민의 일상생활을 구성하는 핵심 요소로 자리 잡았다. 메신저, 포털, 간편결제, 온라인 동영상서비스(OTT), 모빌리티·배달 플랫폼 등은 통신망 위에서 제공되는 부가서비스의 성격을 넘어, 소통·금융·이동·업무와 같은 일상생활의 기본 동선을 실질적으로 지탱하는 인프라로 변화하였다. 이러한 변화는 부가통신서비스의 장애를 바라보는 시각에도 새로운 고려가 필요함을 시사한다.

부가통신서비스의 장애는 기간통신서비스의 장애와 구조적으로 다른 양상을 보이는 것으로 파악된다. 기간통신서비스는 유·무선망이라는 물리적 인프라에 기반하므로, 장애가 발생하더라도 통상 특정 지역이나 설비 단위로 영향이 제한되는 경우가 많다. 반면 부가통신서비스는 중앙집중형 서버·플랫폼 구조로 운영되는 경우가 많아 장애가 발생하면 지역과 무관하게 전국 단위의 이용자에게 비교적 동시다발적으로 영향을 미치는 특성이 있다. 또한, 서비스의 전면 중단뿐 아니라, 일부 기능 오류나 응답 지연과 같은 부분적 장애 역시 이용자 입장에서는 실질적인 불편으로 이어질 수 있다.

이에 디지털 전환에 따른 부가통신서비스의 중요도 변화를 살펴보고, 기간통신서비스와 구별되는 확산 구조를 정의하며, 일상생활과의 밀접성에서 비롯되는 체감 불편 등을 살펴본다. 또한, 부가통신서비스 의존도 심화에 따른 이용자 요구수준의 변화와 전면 장애뿐 아니라 부분 기능 오류·지연을 함께 고려해야 할 필요성을 살펴보고자 한다.

Ⅱ 디지털 전환과 부가통신서비스의 위상 변화

「전기통신사업법」상 부가통신서비스는 기간통신사업자로부터 회선을 임차하여 콘텐츠·정보·플랫폼을 제공하는 서비스를 의미하며, 초기에는 이메일, 웹하드, 포털 검색과 같이 정보 제공 성격이 강한 서비스가 중심이었으나, 현재는 메신저, 간편결제·간편인증, 클라우드, OTT, 배달·모빌리티 중개 등으로 범위가 지속적으로 확대되고 있다.

특히, 비대면 소비, 재택·원격 근무, 온라인 금융·행정 서비스가 확산되면서 부가통신서비스에 대한 의존도도 함께 높아지고 있다. 결제의 경우, 스마트폰 간편결제를 이용하고, 신원 확인은 민간 플랫폼의 간편인증으로

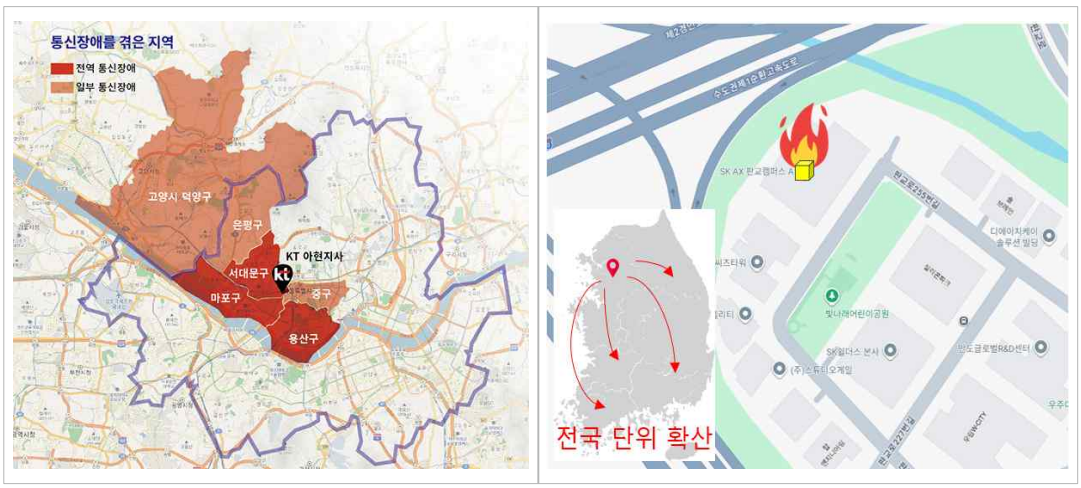
대체되는 경우가 증가하였고, 회의나 협업도 온라인 화상회의 등의 도구를 통해 이루어지는 비중이 증가하고 있다.

이와 같이 부가통신서비스는 이용자의 편의를 더해주는 보조적 수단을 넘어 일상생활을 뒷받침하는 서비스로 그 위상이 조금씩 이동하고 있는 것으로 보이며, 관련 서비스의 장애가 가지는 사회적 영향력도 이전보다 파급력이 높아지고 있다고 할 수 있다.

Ⅲ 기간통신서비스와 구별되는 확산 구조

기간통신서비스의 장애는 통신국사, 기지국 등 특정 물리적 설비의 문제로 발생하는 경우가 많기 때문에 장애 영향의 범위가 해당 설비가 담당하는 지역에 한정되는 경향이 있다. 실제로 2018년 KT 아현국사 화재의 경우 유선전화·인터넷 장애가 발생하였으나, 그 영향은 서울 서대문구·마포구 일대에 주로 국한되었다.

〈그림 1, 2〉 (좌) KT 아현 국사 화재 시 통신장애 지도, (우) SK C&C 데이터센터 화재로 입주사의 서비스 다운 전국적 확산



[출처] 시사 IN

반면 부가통신서비스는 이용자의 위치와 무관하게 메인 서버·플랫폼을 통해 서비스를 제공하는 구조로 되어 있어 해당 서버나 데이터센터에 문제가 발생하면 지역 구분 없이 전국의 이용자가 비슷한 시점에 영향을 받게 된다. 실제로 2022년 SK C&C 데이터센터 화재 시, 성남시 판교에서 화재가 발생하였으나, 카카오, 네이버 등을 비롯하여 해당 데이터센터에 입주한 모든 서비스들이 전국적으로 서비스 장애를 경험하였다.

이러한 차이는 장애의 심각도를 지역 단위 피해 규모만으로 평가하기보다는, 얼마나 넓은 범위에서 동시에 영향을 미치는지도 함께 확인할 필요가 있음을 의미한다. 또한, 지역별 우회로 확보와 같은 전통적 대응 방식보다 서버·데이터센터 등의 다중화나, 트래픽 분산과 같은 시스템 차원의 대응이 더 유의미한 조치라 할 수 있다.

Ⅳ 이용자 일상생활과 밀접한 영역에서의 체감 불편

부가통신서비스 장애의 영향력은 이용자의 일상생활과 직접적으로 연관된 영역에서 발생한다는 점에서 더 뚜렷하게 나타난다.

〈표 1〉 부가통신서비스 구분별 장애 발생 시 영향 범위

구분	내용
메신저(소통 등)	• 가족·지인 간 연락, 회사·학교에서의 공지, 배달·택배 기사와의 소통 등 • 자영업자·소상공인의 경우 응대 채널 제한으로 신뢰도 저하 및 매출에 영향 발생
결제·금융	• 간편결제·QR결제 등의 의존도가 높은 매장에서는 관련 서비스 장애 시 결제 지연·실패로 매출에 직접적인 영향 발생 • 특정 플랫폼에 로그인·본인인증 의존하는 경우 단일 장애에서 다른 서비스 이용 장애로 확산 가능
이동·물류	• 택시 호출, 내비게이션, 배달 중개 플랫폼 장애의 경우 실제 이동·배송 지연 발생 가능
업무	• 클라우드 협업 툴, 화상회의에 대한 의존도가 높아지면서 관련 서비스 장애가 업무 수행에 영향을 미칠 가능성 증가

이와 같이 부가통신서비스 장애는 단순히 특정 기능 하나 중단에 그치지 않고, 일상을 구성하는 여러 활동으로 확산될 수 있다는 점에서 부가통신서비스의 중요도는 지속적으로 증가하는 추세이다.

Ⅴ 의존도 증가에 따른 이용자 요구수준의 변화

부가통신서비스에 대한 의존도가 증가할수록 이용자가 서비스에 기대하는 안정성의 수준도 함께 높아지는 경향이 나타난다. 과거에는 짧은 서비스 중단을 어느 정도 자연스럽게 받아들이는 분위기가 있었다면, 결제·인증·업무 등 여러 기능을 하나의 플랫폼에 의존하게 된 지금은 비교적 짧은 장애나 사소한 오류에도 이용자들이 불편을 느끼는 경우가 증가하고 있다.

이용자들은 서비스가 항상 안정적으로 제공되기를 바라는 기대와 장애 발생 시 원인과 복구 시점을 신속히 안내받고자 하는 요구, 반복적인 장애에 대해서는 합리적인 설명과 보상을 기대하는 흐름 등으로 나타나고 있다. 결국 의존도의 심화는 이용자 수의 증가뿐 아니라 서비스 안정성에 대한 기대 수준 자체를 함께 끌어올리는 요인으로 작용하고 있다고 볼 수 있다.

Ⅵ 전면 중단을 넘어 부분 기능 오류·지연까지 고려할 필요성

부가통신서비스의 장애를 논의할 때는 서비스를 제공하는 부가통신사업자와 이를 이용하는 이용자 간의 입장 차이가 있을 수 있다. 일반적으로 이용자들의 경우, 서비스가 아예 접속되지 않는 '전면 중단' 상태만 통신장애로 여기지 않고, 특정 기능만 제대로 동작하지 않는 부분 오류(텍스트 메시지 전송은 되지만, 이미지 전송은 되지 않는 경우 등),

접속은 되지만 응답 속도가 눈에 띄게 느려지는 지연 현상 등도 이용자에게는 '장애'로 인식될 수 있다.

〈그림 3〉 부가통신서비스 장애 유형

이러한 시각은 제도적으로도 일부 반영되고 있으며, 「전기통신사업법」 제22조의7 제4항에서는 '전송 속도가 저하되는 등 전기통신서비스 제공에 장애가 발생'한 경우를 서비스 중단과 함께 언급하고 있어, 완전한 중단이 아니더라도 속도 저하나 기능 저하가 장애의 유형 중 하나로 인정될 수 있음을 보여준다.

전면 중단만을 기준으로 삼을 경우, 실제로는 더 자주 발생할 수 있는 부분 장애·지연 사례가 통계 및 점검 과정에서 상대적으로 덜 조명될 가능성이 있으나, 이용자 입장에서는 전면 중단과 부분 오류·지연에 대한 구분 없이 모두 불편으로 받아들이는 경우가 많다는 점을 고려해야 할 필요가 있다.

따라서 부가통신서비스의 장애를 살펴볼 때는 전면 중단뿐 아니라 부분 기능 오류, 응답 지연까지 함께 포함하여 이용자에게 실질적으로 영향을 미치는 여부를 판단해 볼 필요가 있을 것으로 사료된다.

Ⅶ 결론

부가통신서비스는 디지털 전환의 흐름 속에서 일상생활과 밀접한 서비스로 자리 잡았으며, 부가통신서비스 장애는 기간통신서비스와 달리 비교적 넓은 범위에서 동시에 영향을 미치는 구조적 특성을 가지고 있다. 메신저 등을 통한 소통, 결제, 이동, 업무 등 다양한 생활 영역과 연관되어 있다는 점에서 단순하게만 볼 수는 없으며, 서비스 의존도가 높아질수록 이용자들이 서비스에 기대하는 안정성의 수준도 함께 증가하고 있다. 또한, 서비스 전면 중단에만 포커스를 맞출 경우, 이용자들이 실제로 자주 겪는 부분 기능 오류나 지연은 상대적으로 관심에서 벗어날 수 있다는 점도 함께 고려해야 할 필요가 있다.

이를 종합하면, 부가통신서비스의 통신재난·장애를 이해하기 위해서는 확산 범위, 생활 밀착도, 장애의 형태(전면 중단·부분 오류·지연)를 함께 살펴보는 균형 잡힌 시각이 도움이 될 것으로 보인다. 이러한 관점의 확장이 향후 부가통신서비스의 안정성 향상에 도움이 될 것으로 사료된다.

03 전문가인터뷰

KT cloud
김승희 매니저/정보통신기술사

KT cloud 김승희 매니저님을 만나다.

Q 우선 김승희 매니저님에 대해 소개 부탁드립니다.

A 안녕하세요. KT cloud DBO사업팀의 김승희입니다. 저는 데이터센터의 구축과 관련된 프로젝트를 담당하고 있습니다. 데이터센터는 건축·전기·기계·소방·통신 등 여러 전문 영역이 하나의 시스템으로 맞물려야 완성되는 복합 시설이기 때문에, 데이터센터 개발과 운영 과정에서 각 영역의 전문가 그룹을 포함한 다양한 분야의 전문가들과 협업하며 업무를 진행하고 있습니다. 다소 낯선 용어인 DBO는 Design(설계), Build(시공), Operate(운영)의 약자로 데이터센터의 설계부터 시공, 그리고 준공 후 운영까지 전 생애주기를 일괄 수행하는 사업 방식입니다. 설계 단계부터 운영 관점을 반영할 수 있고, 구축과 운영의 책임이 하나로 이어진다는 것이 DBO의 가장 큰 강점입니다. 최근에는 AI데이터센터(AIDC) 관련 업무가 주를 이루고 있습니다. 고밀도 랙과 수냉식 냉각 등 AIDC로의 전환은 데이터센터의 설계·시공·운영 방식 전반을 바꾸고 있으며, 이러한 패러다임 변화에 맞춰 신뢰성과 안정성을 갖춘 경쟁력 있는 데이터센터를 공급할 수 있도록, 설계 컨설팅부터 사업관리까지 빈틈없이 힘을 쏟겠습니다.

Q 정보통신 전문가의 입장에서 “디지털 재난”은 무엇이라고 생각하시나요?

A 저는 시민이 우회할 방법 없이 불편을 겪고, 그 시간이 사회가 감내할 수 있는 한계를 넘어서는 순간, 단순 장애가 아니라 디지털 재난이 되는 것이라고 생각합니다. 특정 IT 장비나 플랫폼 하나의 문제냐 아니냐가 아니라, 시민의 삶이 멈추느냐가 기준입니다.

시민의 입장에서 디지털 재난은 결국 ‘일상의 정지’입니다. 통신망이나 시스템이라는 기술적 개념은 보이지 않습니다. 당장 메신저가 안 되고, 택시가 안 잡히고, 결제가 안 되고, 은행 앱이 열리지 않는 순간으로 다가옵니다. 원인이 화재인지 해킹인지는 중요하지 않습니다. ‘불편하다, 불안하다’는 사실만 남습니다.

정보통신의 시각에서 이런 재난의 원인 구조를 본다면, OSI 7계층에서 장애는 아래에서 위로 전파됩니다. 하위 계층 하나가 무너지면 상위 계층이 아무리 정상이어도 서비스는 멈춥니다. 그리고 1계층 밑에는 전력·UPS·냉각 등 이른바 ‘0계층’이라 부르는 시설 인프라가 존재합니다. 굴착기 한 번에 광케이블이 끊기고, 배터리 셀 하나에서 시작된 불이 국가 행정을 멈추게 합니다. 2022년 판교와 2025년 국가정보자원관리원 화재는 0계층 설비 장애가 상위의 전 계층으로 번진 대표적인 사례였습니다. 따라서 디지털 재난의 범위에는

IT 장애와 보안 사고뿐만 아니라 시설(Facility) 영역까지 반드시 포함되어야 합니다.

그러므로 대비의 전제 또한 변해야 합니다. 모든 것이 연결된 초연결 환경에서 장애 제로는 현실적으로 불가능합니다. 장애는 반드시 발생한다는 전제 위에서 회선과 시스템의 이중화로 우회 경로를 확보하고, 장애를 조기에 격리해 연쇄 확산을 차단하며, 신속한 복구 절차와 함께 시민에게 상황을 정확히 알리는 소통 체계까지 갖추어야 합니다. 장애가 시민에게 닿기 전에 그 연쇄적인 확산을 끊어내는 회복 역량, 그것이 결국 재난 여부를 가른다고 저는 생각됩니다.

Q 국내 데이터센터 환경에서 화재·정전·침수·통신 장애 등 가장 현실적인 위협은 무엇이라고 생각하시나요?

A 화재·정전·침수·통신 장애도 현실적인 위협이지만 저는 가장 큰 위협은 보안사고, 그 중에서도 AI에 의한 보안 위협이라고 생각합니다. 물리적 재해는 발생 확률과 대응 체계가 어느 정도 정형화되어 있는 반면, AI 기반 공격은 발생 가능성이 빠르게 커지고 있음에도 대응 체계가 아직 정립되지 않았기 때문입니다.

수십 년 묵은 취약점들을 스스로 엮어 실제 공격 경로를 구성해냈다는 미토스 사례*처럼, 공격의 주체가 사람에서 AI로 넘어가고 있습니다. Zero-Day Attack 시대가 아니라, AI가 탐색·분석·공격에 이르는 전 과정을 실시간·자동으로 수행하는 Machine-Speed 시대입니다. 사람의 속도로는 따라갈 수 없는 속도 비대칭이 핵심 리스크입니다.

특히 AI 데이터센터는 수냉식 냉각, 수·배전 설비, UPS 등 IT보다 유틸리티, 즉 UT(Utility Technology)의 중요성이 더 커진 환경입니다. 만약 AI 기반 공격이 DCIM과 유틸리티 제어권을 침해한다면, 냉각 정지에 의한 서버 과열과 셧다운, 전원 차단에 의한 전면 서비스 중단, 나아가 설비 파손까지 이어질 수 있습니다. 즉 사이버 침해가 곧 화재·정전과 같은 물리적 재해로 이어지는, 데이터센터의 새로운 위협 시나리오입니다.

* 앤트로픽(Anthropic)의 최신 AI 모델인 '미토스(Claude Mythos)'가 강력한 취약점 탐지·공격 자동화 가능성으로 보안 리스크를 키우고, 동시에 미국 정부의 수출통제·접근 제한으로 글로벌 이용이 중단되며 촉발된 사건

Q 최근 발생한 국내외 디지털 재난 사례 중에서 주목할 만한 사례는 무엇이 있을까요?

A 많은 분들이 2022년 카카오 사태, 즉 판교 데이터센터 화재를 먼저 꼽으실 것입니다. 이 사건의 의미는 단순한 서비스 장애가 아니라, 전문가뿐 아니라 전 국민이 디지털 재난, 이른바 '디지털 블랙아웃'의 불편함과 무서움을 몸으로 직접 겪었다는 데 있습니다. 책으로 배우는 이론이 아니라, 디지털 세상의 이면을 사회 전체가 체험한 최초의 사례였습니다.

또 하나 기억할 것은, 같은 데이터센터 화재였지만 금융 서비스와 택시 호출 서비스의 복구 시간이 달랐다는 점입니다. 이를 통해 기술력의 차이가 아니라 거버넌스의 차이가 서비스 복구 속도를 결정한다는 것을 확인하게 되었습니다. 그리고 이 사건을 계기로 디지털 안전 3법 같은 제도적 대응이 잇따랐습니다.

조금 더 과거로 가면, 2001년 9.11 테러로 세계무역센터가 붕괴하면서 트레이딩을 비롯한 수많은 금융·무역 기업의 서비스가 건물과 함께 일제히 멈췄습니다. 그러나 BCP 정책과 거버넌스를 갖춘 기업은 즉시

대체 사이트에서 서비스를 재가동한 반면, 그렇지 못한 기업은 복구 불능을 넘어 존폐 자체가 갈렸습니다. 9.11 이후 미국에서는 의회 보고서를 비롯한 방대한 자료와 연구논문이 공개되었고, 이것이 후속 거버넌스의 근거가 되었으며, 그 성과가 각국의 BCP 표준을 거쳐 ISO 22301이라는 국제 인증 체계로 결실을 맺었습니다. 9.11이 ISO 22301과 우리나라 공공·민간의 BCP 인식 전환으로 이어졌듯이, 카카오 사태는 한국판 디지털 재난 거버넌스의 출발점이 되었고 그 연장선은 지금도 진행 중입니다.

Q AI 데이터센터로의 변화가 정보통신 산업 및 데이터센터 운영이나 안전관리에 실질적으로 어떠한 영향을 미칠까요?

A 공동주택이나 일반 건축물의 통신 담당자에게 통신 전용 공간은 통상 TPS실과 집중구내통신실, 즉 MDF실 정도로 인식됩니다. 그러나 데이터센터의 통신 공간 구성은 이와 다릅니다. TPS실도 IT 서비스용과 건축물 설비용으로 경로 자체를 분리하는 사례가 있고, MDF실 외에 통신사업자 중립 접속 공간인 MMR(Meet-Me Room), 그리고 백본 집선을 위한 별도 공간도 존재합니다. 네트워크 연결 또한 XC(Cross Connect), IX(Internet eXchange), DCI(Data Center Interconnect) 등 서로 다른 기술 기반 위에서 다양한 방식으로 운영됩니다.

AIDC에서는 이 구조가 다시 한번 변합니다. 네트워크는 GPU 패브릭 중심의 스케일업·스케일아웃 계층 구조로 재편되고, 구축 방식도 모듈형·스키드, Pod형 일체형 랙으로 바뀌고 있습니다. 그 결과 전력·냉각 설비 비중이 급증하면서 전체 공사비에서 통신공사가 차지하는 비중은 레거시 데이터센터에 비해 절반에서 3분의 1 수준으로 줄어드는 추세입니다. AIDC 열풍 속에서 통신 영역만 그 흐름에서 비켜나 있는 것처럼 보이는 이유입니다.

하지만 실상은 반대입니다. DLC(Direct Liquid Cooling) 누수탐지 센서, 모니터링용 지능형 IR 카메라, 컨테인먼트 열관리 등 AIDC의 모든 운영관리·안전관리가 통신망 위에서 작동합니다. 통신망은 시공 물량은 줄었어도 데이터센터의 '신경망'으로서 중요성이 더욱 높아지고 있고, 그 결과 기계설비·전기설비 담당자에게 통신 업무가 계속 부가되고 있습니다. 즉 AIDC에서는 IT와 UT, 다시 말해 정보기술과 전력·냉각 같은 기반 설비 사이의 경계가 무너지고 있는 것입니다.

따라서 세 가지 대응이 필요합니다. 첫째, IT·통신·기계·전기로 나뉜 직무 경계와 조직·책임 체계를 융합형으로 재정의하는 것입니다. 둘째, 설비 담당자가 통신을, 통신 담당자가 유틸리티를 이해할 수 있도록 하는 크로스 도메인 융합 교육입니다. 셋째, 변화하는 데이터센터의 특성을 반영하지 못하는 기존 구내통신 설계 기준과 운영·안전관리 제도의 개선입니다.공사비 비중은 줄었지만, AIDC 시대의 통신은 물량이 아니라 신경망으로써의 역할로 평가되어야 합니다.

Q 최근 AI 서버의 도입으로 수냉식(리퀴드 쿨링) 랙 도입이 늘고 있는데, 기존 공랭식 대비 누수 등 새로운 리스크가 발생할 것으로 보입니다. 가장 우려되는 지점이 있다면 무엇인가요?

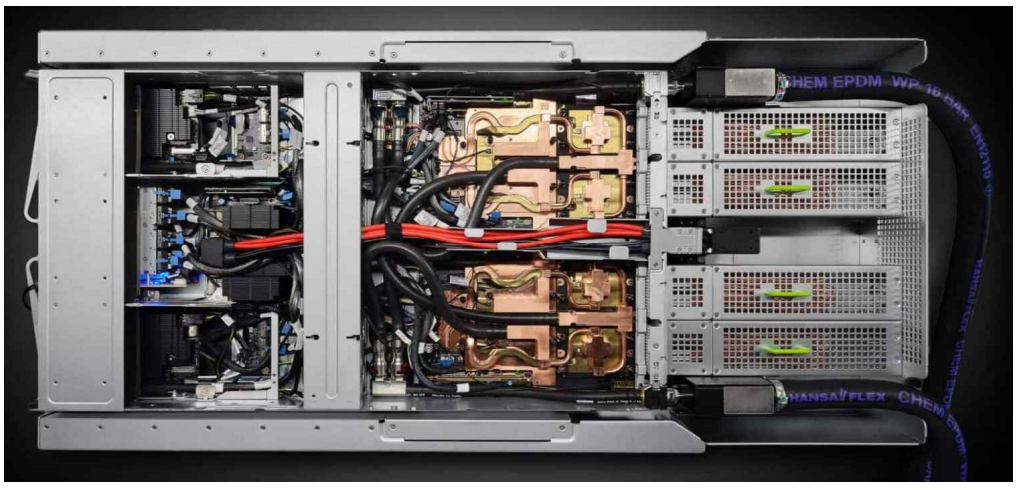
A 가장 우려되는 것은 단연 누수, 리키지(Leakage)입니다.수냉식 시스템의 주요 설비별로 나누어 보면 누수 피해 양상이 다릅니다. 첫째, GPU 칩에 직접 부착되는 콜드 플레이트에서 누수가 발생하면, 냉각수, 즉 부동액에 의한 쇼트로 GPU 칩과 메인보드가 물리적 손상을 입는 국지적 직접 손상이 발생합니다.

둘째, 랙에 냉각수를 공급하는 매니폴드에서 누수가 발생하면 GPU 서버들과 네트워크 스위치의 동시 다발적 직접 손상에 더해, 냉각 상실로 인한 랙 전체의 과열 다운이라는 2차 피해까지 이어집니다. 즉 누수는 발생 지점이 콜드 플레이트에서 매니폴드, 나아가 CDU 같은 상위 설비로 올라갈수록, 피해 범위가 서버 한 대에서 랙, 클러스터 전체로 확대되는 재해가 될 수 있습니다.

그런데 현재 많은 AIDC에서 GPU 서버 소유자와 데이터센터 운영 주체가 다릅니다. 그 결과 콜드 플레이트는 GPU 서버 소유자가, 매니폴드는 DC 운영자가 관리하는 이원화 구조가 됩니다. 예를 들어 NIPA가 발주한 2026년 'AI컴퓨팅자원 활용기반 강화사업'의 경우, GPU 서버와 부대장비는 NIPA 소유이지만 전력·냉각·항온항습은 사업참여사 또는 DC 운영사가 관리합니다. 하나로 연결된 냉각수 배관 위에 관리 책임의 경계선이 그어져 있는 것입니다. 이 때문에 누수 사고 시 원인 규명과 책임 소재가 모호해질 수 있습니다.

우리나라는 올해가 수냉식, DLC 상업 운영의 원년이라 할 수 있습니다. 이제는 AI 클러스터뿐 아니라 CDU를 비롯한 리퀴드 쿨링 핵심 설비의 운영 노하우와 전문 인력 보유 여부가, AIDC의 성능을 보장하는 핵심 요소가 될 것입니다. 누수 감지·차단 체계를 갖추는 것과 함께, 소유자와 운영자 간 책임 경계와 대응 절차를 사전에 정의하고 모의 훈련으로 검증하는 것이 새로운 과제일 것입니다.

〈그림 1〉 수랭식 NVIDIA Blackwell 컴퓨팅 트레이



[출처] NVIDIA

Q 데이터센터의 디지털 재난 대응 능력을 높이기 위해서 가장 우선적으로 갖춰야 할 역량이나 체계는 무엇이라고 생각하시나요?

A 디지털 재난 대응 능력은 두 개의 범위, 즉 센터 '내부의 결단 역량'과 산업 전체의 '연계 대응 체계'에서 봐야 한다고 생각합니다.

첫째, 데이터센터에는 전기안전관리자, 소방안전관리자, 정보통신설비 유지관리자 등 법적 선임자가 규모에 따라 10명 안팎에 이르러, 평시의 안정적 운영은 확보됩니다. 그러나 판교 데이터센터 화재나 국가정보자원관리원 대전 화재 같은 상황에서 전체 셧다운을 담당자 개인이 과감히 결단할 수 있는가는 별개의 문제입니다. 디지털 안전 3법의 영향으로 구역별 격리가 적용되어 피해 확산은 늦출 수 있어도, 셧다운 결정 자체는 여전히 사람의 몫입니다. 평시 관리 역량도 중요하지만, 관건은 재난 시 '결단 역량'입니다. 그리고 이것은 개인의 용기가 아니라, 사전에 정의된 권한 위임과 면책이라는 제도적 뒷받침이 있어야 가능할 것입니다.

둘째, 산업 전체의 연계 대응 체계입니다. 디지털 세상은 케이블과 API 등으로 모두 연결되어 있어, 내가 복구되어도 상대가 복구되지 못하면 소용없다는 것을 카카오 사태 때 경험했습니다. 부분적·분야별 훈련은 존재하지만, 통신망·데이터센터·인증을 관통하는 기관 간 연계 훈련은 아직 제도화되어 있지 않습니다. 특히 모든 연결이 물리적·논리적으로 집중되는 AIDC는 기존과 다른 새로운 영역의 재난을 낳을 수 있습니다. 따라서 AIDC 시대에는 내부적으로는 권한·절차·면책을 사전에 정의한 의사결정 체계가, 산업적으로는 생태계 전체가 함께 검증하는 연계 대응 체계가 우선적으로 필요하다고 생각합니다.

Q 현재 국내에서 진행되고 있는 AI데이터센터의 재난 관리에 보완이 필요하다고 느끼시는 부분이 있다면 무엇인가요?

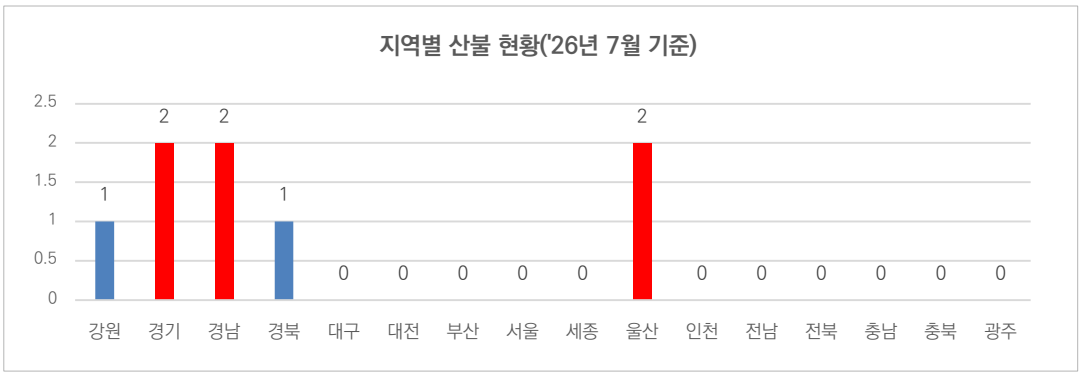
A 현재 신규 AI 데이터센터의 최대 관건은 전력수급입니다. '전력계통영향평가'라는 채찍과, 올해 제정된 '인공지능 데이터센터 산업 진흥에 관한 특별법'(AIDC 특별법)이라는 당근이 함께 작동하면서, 지금 계획되는 대부분의 AIDC는 비수도권에 들어설 예정입니다. 이러한 지방 분산은 국가 차원의 재난 리스크를 나누는 효과가 있습니다. 하지만 통신망이 뒷받침되지 않으면 그 효과는 반쪽에 그칩니다. 백본 통신망 역시 전력망과 마찬가지로 수도권 중심으로 구성되어 왔기 때문입니다. 전북, 전남, 경남 등에 새로 들어서는 AIDC를 잇는 백본 회선이 단일 경로라면, 재난으로 그 경로 하나만 끊겨도 센터가 멀쩡해도 서비스는 마비됩니다. 데이터센터는 분산해 놓고, 통신에서 새로운 단일 장애점을 만드는 셈입니다. 전력은 발전 및 송전 제약으로 완벽한 경로 이중화가 어렵지만, 통신은 다릅니다. 비수도권에 대규모 AI 데이터센터가 속속 건설되는 지금이야말로, "어떤 단일 재난에도 주센터와 DR센터가 동시에 멈추지 않는다"는 원칙으로 통신망을 구축할 유일한 기회입니다. 거대한 자본이 AI 인프라에 투입될 때, 이를 뒷받침할 AIDC 전용 DCI 구성, 백본망 이중화, 경로 다양화 등 미래 네트워크 전략이 반드시 함께 담겨야 합니다.

04 디지털 안전 관제 이슈

7월 발생 이슈

화재	• 2026.07.07. 10:50경 경기 파주시 와동동 아파트 화재 * 소방대응 1단계 발령, 소방대원 1명 탈진, 주민 3명 연기흡입으로 인한 경상
	• 2026.07.09. 경기도 파주시 맥금동 480-1 공장 화재
	• 2026.07.13. 10:27경 국회 인근 오피스텔 화재 발생, 도로 통제 * 부상자 1명 발생
	• 2026.07.18. 인천시 서구 석남동 224-8(쿠팡물류센터) 화재 * 소방대응 1, 2단계 발령 및 국가소방동원령 발령
	• 2026.07.21. 서울 강남구 압구정동 한양아파트 화재
	• 2026.07.23. 강원 동해시 구호동 세진산업(플라스틱 제조공장) 화재 * 소방대응 1단계 발령
지진	• 2026.07.06. 경북 김천시 북동쪽 13km 지역 규모 2.1 지진 발생
	• 2026.07.23. 03:47경 경북 예천 북쪽서 규모 2.6 지진 발생
	• 2026.07.28. 일본 구마모토서 규모 7.1 지진 발생 * 진도3 흔들림 전달 : 전남 광주, 경남, 부산, 제주도 * 진도2 흔들림 전달 : 울산, 경북, 전북, 충북, 대구, 충남, 강원, 경기
정전	• 2026.07.13. 인천광역시 영종구 중산동 영종하늘도시 인근 정전
	• 2026.07.19. 인천광역시 당하동 청마로 일대 변압기 고장으로 인한 정전
대규모 인파	• 2026.07.11. 서울 반포한강공원 포켓몬 GO 행사 인파 밀집
호우	• 2026.07.07. 집중호우 대비 평시보고 확대

재난유형	일시	주요내용 (과기정통부 보고)
산불	7월 中 8건 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 2026.07.01.

- 위택스 시스템 통합 작업으로 인한 접속 장애

02 2026.07.06., 26.07.23.

- 2026.07.06. 쿠팡 마이페이지 일부 안드로이드 이용자 오류
- 2026.07.23. 토큰 에러로 인한 쿠팡이츠 결제 불가 장애 발생

03 2026.07.15., 2026.07.25.

- 2026.07.15. ChatGPT 접속 오류
- 2026.07.25. ChatGPT(PC, APP&for KaKao) 서비스 이용 불가

04 2026.07.19., 2026.07.22.

- 2026.07.19. 페이스북, 메신저, 인스타그램 서비스 이용자 접속 장애
- 2026.07.22. 페이스북, 인스타그램 일부 이용자 장애 발생

05 2026.07.23.

- 인스타그램 DM 장애 발생

05 Digital Safety Inside

2026년도 통화량 급증 예상 달력 (9~10월)

9월(September)

일	월	화	수	목	금	토
		1 o 2학기 개학식	2	3 o 괴산 고추축제 (9/3~9/6)	4 o 서울세계불꽃축제 -전야제(서울) o 평창효석문화제 (평창, 9/4~9/13) o 무주반딧불축제 (무주, 9/4~9/12) o 임영웅 콘서트 (고양, 9/4~9/6)	5 o 성시경 콘서트 (서울, 9/5~9/6) o 서울세계불꽃축제 -불꽃쇼(서울)
5	7	8 o 오피셜히게단디즘 콘서트(서울, 8/8~8/9)	9	10 o 장수한우랑사과랑축제 (장수군, 9/10~9/13)	11 o 거제맥주축제 (거제, 9/11~9/12)	12 o 플레이브 콘서트 (인천, 9/12~9/13) o 이슬라이브 페스티벌 (인천) o 옥토버페스트 서울2026 (서울, 9/12~9/21)
13	14	15	16 o 서리풀 뮤직페스티벌 (서울, 9/19~9/20)	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 페스티벌서울 9/19-9/20
20	21	22 o 경남고성공룡세계 엑스포(고성 9/22~11/1)	23	24 추석연휴 o 안동국제탈춤페스티벌 (안동, 9/24~10/4)	25 추석	26 추석연휴 o 실리카겔 콘서트 (서울, 9/26~9/27)
27	28	29	30	특이사항		

10월(October)

일	월	화	수	목	금	토
특이사항 o 대학 가을축제 (전국, 10월 중)				1 o 천안 흥타령춤축제 (천안, 10/1~10/5) o 정선아리랑제 (정선, 10/1~10/4) o 김제 지평선축제 (김제, 10/1~10/5)	2 o 포스트말론 내한공연 (고양) o 금산세계인삼축제 (금산, 10/2~10/11) o 부평풍물대축제 (부평, 10/2~10/4) o 산청한방약초축제 (산청, 10/2~10/11) o 남사당 바우덕이 축제 (안성, 10/2~10/5)	3 개천절 o 경북영주 풍기인삼축제 (영주, 10/3~10/11) o 렛츠락 페스티벌 (10/3~10/4)
4 o 수원화성문화제 (수원, 10/4~10/11)	5 대체공휴일	6	7 o 광주 추억의 충장축제 (광주, 10/7~10/11) o 현대카드 슈퍼콘서트 28위켄드 (고양 10/7~10/8)	8 o 임실N치즈축제 (임실, 10/8~10/11)	9 한글날 o 세종한글축제 (세종, 10/9~10/11) o GHOST 페스티벌 (파주, 10/9~10/11) o 악동뮤지션 콘서트 (서울, 10/9~10/11)	10
11 o 찰리 푸스 내한공연 (고양)	12	13	14	15	16 o 목포항구축제 (목포, 10/16~10/18) o 순창장류축제 (순창, 10/16~10/18)	17 o 그랜드 민트 페스티벌 (서울, 10/17~10/18) o 대전 빵축제 (대전, 10/17~10/18)
18	19	20	21 o 강릉커피축제 (강릉, 10/21~10/25)	22 o 사천에어쇼 (사천, 10/22~10/25)	23 o 김천 김밥축제 (김천, 10/23~10/25)	24
25	26 o 밴슨 분 내한공연(고양) o 실리카겔 콘서트 (서울, 9/26~9/27)	27	28	29	30 o 할로윈 o 세종보헤미안 뮤직페스 티벌(세종 10/13~11/1)	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