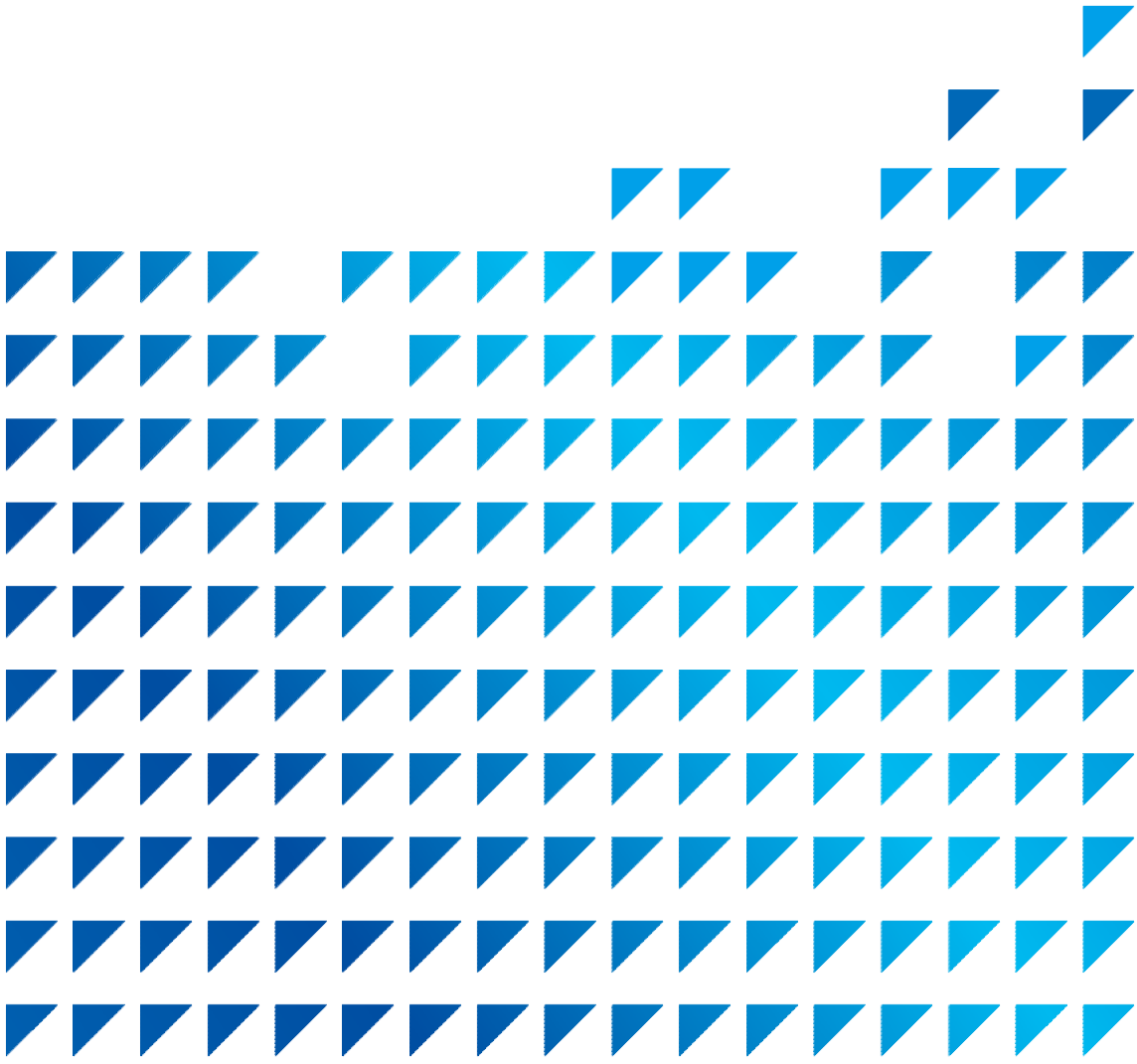
KICI DSR Vol. 26-01

한국정보통신산업연구원

Digital Safety Report

1월호



KICI 한국정보통신산업연구원

KICI 한국정보통신산업연구원

한국정보통신산업연구원

Digital Safety Report 1월호

Contents

KICI Greeting

한국정보통신산업연구원, 디지털 시대 안전 버팀목으로

한국정보통신산업연구원장 백 운 일

존경하는 정보통신산업 관계자 여러분, 그리고 KICI Digital Safety Report 독자 여러분, 안녕하십니까? 한국정보통신산업연구원장 백운일입니다. 2026년 병오년(丙午年) 새해에는 정보통신산업의 성장과 여러분들의 건승을 기원합니다.

작년 2025년 한해도 우리 연구원은 '디지털 안전 전문기관'이라는 국내 유일 기관으로서의 역할을 성실히 수행하였습니다. 정부로부터 디지털 재난관리 업무를 위탁받아 국가 차원의 디지털 안전관리 체계 구축을 지원하였고, 그 성과를 현장과 공유하기 위해 KICI Digital Safety Report를 창간하여 디지털 안전 인식 확산에 힘써 왔습니다. 특히 2025년 3월의 영남지역 대형산불, 7월·8월의 집중호우, LG헬로비전 김해국사 화재사고, 국가정보자원관리원 화재 사고 등으로 인해 발생한 디지털 장애를 신속하게 복구하기 위해서 과기정통부, 지자체, 소방청, 사업자 등 관계기관과 긴밀히 협력하며 상황을 공유하고 대응·복구를 지원했습니다. 우리 연구원의 지원은 정부의 디지털 장애 대응·복구에 대한 필요한 조치를 적시에 이뤄질 수 있도록 하였습니다. 그리고 디지털 장애·재난을 예방·대비하기 위한 안전 점검과 상시 관제 업무를 성실히 수행하였습니다.

새롭게 맞이하는 2026년에는 우리 연구원이 '디지털 안전 전문기관'으로 자리매김할 수 있도록 노력하고자 합니다. 이를 위해 우리 연구원이 2026년에 노력하고자 하는 세 가지 과제를 말씀드리고자 합니다.

첫째, 최근 5년간 축적한 실증 데이터를 기반으로 재난 유형별·시기별 위험을 정밀하게 예측하여, 사후 대응을 넘어 선제적 예방이 가능한 디지털 안전 생태계를 구축하겠습니다.

둘째, 복합 재난 상황에서도 핵심 디지털 서비스가 중단되지 않도록 제도 정비와 기준 고도화를 적극 지원하고, 현장의 목소리를 반영한 실효성 높은 정책 대안을 지속적으로 제시하겠습니다.

셋째, 본 리포트를 통해 현장에서 즉시 활용 가능한 구체적 가이드라인과 사례 중심 정보를 제공함으로써, 정책과 현장을 유기적으로 연결하는 디지털 안전의 나침반이 되겠습니다.

우리 연구원은 사후 대응에 머무르지 않고, 축적된 데이터와 현장 경험 노하우를 토대로 위험을 미리 찾아내어, 예방 중심의 디지털 안전 체계를 구현하겠습니다. 또한 사회 기반이 되는 디지털 서비스가 안정적으로 제공될 수 있도록 정부와 기업, 통신 산업 현장과 연계하여 디지털 시대의 안전을 지키는 버팀목이 되겠습니다.

올 한 해도 여러분의 평안과 성장을 진심으로 기원합니다.

감사합니다.

01 부가통신 재난관리 대상 지정 기준 개선 필요성

KISDI
정광재 실장

디지털 재난 관리의 중요성과 국내 제도 경과

2022년 10월 일어났던 SK C&C 판교 데이터센터 화재는 부가통신서비스의 재난 관리 정책에 있어 중요한 전환의 계기가 되었다. 데이터센터 화재로 인하여 카카오 서비스 중단, 네이버 서비스 오류 등 주요 부가통신서비스가 장시간 장애에 노출되면서 다수의 이용자가 불편을 겪게 되었고, 부가통신서비스가 일상생활에 미치는 영향력에 대해서 다시 생각하는 계기가 되었다. 그 결과로 과거 기간통신서비스에 집중되었던 전기통신서비스의 재난관리 정책을 확장하여 부가통신서비스의 재난 관리 필요성에 대한 논의가 이루어졌으며, 2023년 1월 [방송통신발전 기본법(이하 방송통신발전법)]의 개정을 통해 부가통신사업자도 통신재난관리기본계획을 수립하도록 규제가 신설되었다.

부가통신사업자(또는 디지털 서비스)에게 디지털 재난에 대한 보안을 강화하도록 의무를 부과하는 취지는 부가통신서비스의 필수적 성격이 점차 강화되고 있다는 것을 의미하고 있다. 인터넷이용실태조사에 따르면 2024년 기준으로 인터넷 이용률은 90%를 넘어섰고, 인스턴트 메신저의 이용률은 97.7%를 보이는 등 일상의 다양한 활동이 디지털로 전환됨에 따라 부가통신서비스의 필수성이 점차 강화되고 있다. 더불어 코로나 확산 때 백신 접종 예약이나 QR체크인 기능과 같은 사례로 볼 때 일부 인프라 기능의 역할 또한 점차 강화되는 환경으로 변화하고 있다.

개정된 법령은 이러한 점을 고려하여 통신재난관리 의무가 부여되는 사업자를 선정하는 기준으로 이용자 규모와 서비스를 통해 발생하는 트래픽의 양을 규정하고 있다. 방송통신발전법 시행령 제23조 제2항에 따르면 직전년도 10~12월의 일평균 이용자 수가 1,000만명 이상이거나, 일평균 국내 트래픽 양 비중이 2% 이상인 부가통신사업자를 의무 대상으로 규정하고 있다. 이에 따라 2023년 7월에 네이버, 카카오, 삼성전자, Google LLC, Meta Platforms Inc., 넷플릭스서비시스코리아, Amazon Web Services Inc. (총 7개사)가 지정되었으며, 2024년에는 쿠팡이 추가로 지정되었다.

의무 대상 사업자를 선정하는 기준인 이용자 수와 트래픽 양은 디지털 서비스 또는 제공 사업자가 가지는 영향력을 나타내는 기본적인 지표라고 할 수 있다. 이 두 지표는 매출액 산정이 어려운 부가통신서비스의 특성 때문에 상대적으로 측정이 쉬운 대체 지표로 볼 수 있다. 때문에 통신재난관리 분야 뿐만 아니라 부가통신사업자의 서비스 안정성 확보 의무(전기통신사업법 제22조의7), 불법촬영물 유통방지(동법 제22조의5), 정보보호 관리체계 인증(정보통신망법 제47조) 등 디지털 서비스의 규제 대상을 선정하는 기준으로 폭넓게 활용되고 있다.

AI 환경에서 부가통신 재난관리 대상사업자 선정 기준의 한계점

이용자 수와 트래픽 양이 부가통신사업자의 전반적인 영향력을 나타내는데 가장 효과적인 지표이지만 디지털 서비스의 통신재난관리 규제의 특성을 고려할 때 대상 사업자를 지정하는 기준으로서는 한계가 있다고 볼 수 있다. 디지털 서비스에 대한 통신재난관리 의무를 부과하는 배경에는 해당 서비스의 필수성과 디지털 사회의 인프라적 기능에 대한 요소를 고려하여야 할 필요가 있는데, 이용자 수나 트래픽 양에 대한 지표만으로는 필수성이나 인프라적 기능을 온전히 설명하기 어려운 부분이 있다. 이 때문에 국민의 안전과 관련이 없는 서비스는 통신재난관리기본계획 의무 대상에서 제외하자는 국회 법안도 최근에 발의되었다.

부가통신사업자에 대한 통신재난관리기본계획 수립 의무가 부과된 이후 약 2년 동안 인공지능(Artificial Intelligence, AI) 기술의 활용이 급격하게 확산되면서 디지털 서비스의 환경이 변화한 것도 향후 대상 사업자를 선정하는 데 있어서 고려해야 할 중요한 요소이다. AI 에이전트와 API 중심의 디지털 생태계에서는 최종 이용자가 직접 발생시키는 트래픽 양보다, 기계 간 통신 또는 AI의 학습을 위해 백엔드(Backend)에서 발생되는 트래픽의 중요도가 상대적으로 더 높다고 볼 수 있다. AI 기술이 확산될수록 이러한 트래픽 양은 증가할 것이며, 이들에 대한 안정성 관리는 더욱 중요해질 것이다. 하지만 현재 사업자 선정 기준인 트래픽 양 측정 기준으로는 생성형 AI 모델이 동영상 스트리밍보다 더 낮은 트래픽 양을 나타낼 수 있다. 이용자 수 역시 유사한 문제점을 안고 있다. 생성형 AI 이용의 확산으로 기업들은 파운데이션 모델의 필수성과 다른 서비스에 미치는 영향력이 매우 높아짐에도 불구하고 이러한 중요도를 명확히 식별하지 못하는 문제가 발생할 수도 있다.

이러한 디지털 생태계의 환경 변화를 고려해 볼 때 통신재난관리기본계획 의무 대상이 되는 부가통신사업자를 선정하는 기준에 대해서 재고하고 AI 환경에서 통신재난관리 관련 규제의 효용성을 높이기 위한 의무 사업자 선정 기준에 대한 패러다임을 전환할 필요가 있다.

사업자 선정 기준의 패러다임 전환

통신재난관리 의무 대상이 되는 사업자를 선정하는 데 있어 이용자 수, 트래픽 양 등 사업자의 규모를 중심으로 판단하기에 앞서 해당 부가통신서비스가 일상생활에 가지는 필수성이나 디지털 생태계에서 인프라적 속성을 먼저 고려하는 것이 필요하다. 일상생활의 필수성이란 재난 등으로 인한 장애가 발생할 경우 기본적인 의사소통, 정보 접근, 거래 등 일상생활에 즉각적이고 광범위한 문제를 발생시키는 자가 고려되어야 하며, 이를 대체할 수단이 충분한 지 등이 고려되어야 한다. 디지털 생태계 내 인프라적 속성은 해당 서비스의 기능이 다른 서비스를 운영하는 데 핵심적인 기반으로 작동하고 있어 장애 발생 시 연쇄적으로 다른 디지털 서비스에 영향을 미칠 우려가 높은 지가 고려되어야 할 것이다. 이러한 속성을 고려하여 통신재난관리의 필요성이 높은 주요 부가통신서비스를 사전적으로 분류하고 해당 분류 안에서 이용자 수, 트래픽 양과 같은 사업자 규모를 판별할 수 있는 지표를 적용하여 의무 대상 사업자를 선정하는 방식이 필요하다.

2023년 개정된 EU의 NIS(Network and Information Security)2 지침은 대상 사업자 선정에 있어 참고할 만한 사례로 볼 수 있다. NIS2 지침은 유럽연합의 사이버 보안 수준을 강화하기 위하여 중요도가 높은 인프라를 지정하여 보안 의무를 부과하는 규제이다. 지침에서는 의무 부과 대상을 필수 그룹(essential entity)과 중요 그룹(important entity)으로 구분하고 있는데, 필수 그룹에는 디지털 인프라, 중요 그룹에는 주요 디지털 서비스가 의무 대상 분야로 지정되어 있다. 디지털 인프라는 접속(connectivity)을 제공하는 통신 네트워크 제공 사업자(우리나라의 기간통신사업자에 해당)가 포함되어 있지만, 국내에서 부가통신사업자로 분류되는 클라우드 컴퓨팅 서비스 제공사업자, CDN(Content Delivery Network) 사업자, IXP(Internet Exchange Point) 사업자 등이 포함되어 있다. 해당 사업자들이 트래픽 전송을 직접 제공하는 것은 아니지만 전송에 있어 중요한 영향을 준다고 판단한 것으로 보인다. 디지털 서비스 분야에서는 온라인 마켓 플레이스, 검색엔진, SNS가 지정되어 있다. 세 가지 서비스를 선정한 배경에는 해당 서비스가 가지는 거래, 정보 접근, 의사소통의 기능이 일상생활에 미치는 영향력을 고려한 것으로 판단된다.

〈표1〉 EU NIS2 지침의 디지털 인프라 및 디지털 서비스 분류

구분	분류 기준	디지털 인프라 및 디지털 서비스
디지털 인프라	필수 그룹	인터넷 익스체인지 포인트 제공자(IXPs), 도메인네임시스템(DNS) 서비스 제공자, 최상위도메인(TLD) 네임 레지스트리, 클라우드 컴퓨팅 서비스 제공자, 데이터센터 서비스 제공자, 콘텐츠 전송 네트워크 제공자, 신뢰서비스제공자(TSP), 공중전자통신네트워크 제공자 등
디지털 서비스	중요 그룹	온라인 마켓, 검색엔진, SNS

디지털 생태계 내 다른 서비스를 구성하는 데 있어 중요한 기능을 제공하는 서비스들 또한 향후 통신재난관리에 있어서 중요하게 살펴봐야 할 대상이 될 수도 있다. 인도의 경우 전자정부 시스템을 구축하는 데 있어 디지털 신원 확인 시스템을 중요한 디지털 공공 인프라(Digital Public Infrastructure)로 보고 있으며, 판교 데이터센터 화재 사고의 경우에도 카카오톡 인증 기능을 사용하는 다수의 서비스가 영향을 받은 사례가 있다. 이와 같은 인증 시스템이나 간편 결제, 앞서 서술한 파운데이션 모델 등 다수의 서비스에 영향을 미칠 수 있는 중요 기능을 제공하는 서비스를 식별하여 향후 통신재난관리 대상 사업자를 선정하는 기준에 활용할 필요가 있다.

위의 요소들을 고려하여 통신재난관리의 필요성이 높은 중요 서비스를 선정하고 이들을 중심으로 의무를 부과하기 위해서는 통신재난관리의 대상을 사업자 중심에서 서비스 중심으로 전환하는 것도 필요하다. 현행 방송통신발전법의 구조상 의무를 부여받는 주체가 부가통신사업자로 되어 있기 때문에 이용자 수, 트래픽 양 기준에 따라 의무 대상 사업자로 지정되면, 해당 사업자가 제공하는 모든 서비스가 통신재난관리의 대상이 된다. 부가통신 분야는 기간통신 분야와 달리 대부분의 사업자가 성격이 다른 여러 개의 서비스를 함께 제공하기 때문에, 사업자들이 제공하는 서비스 중에는 관리의 필요성이 높지 않은 서비스들도 존재한다. 이러한 점들을 고려하여 통신재난관리의 필요성이 높은 서비스를 중심으로 의무를 부과하는 방향으로 정책 전환을 검토해야 한다.

〈표2〉 통신재난관리기본계획 수립 의무 대상 부가통신사업자의 주요 서비스

사업자 명	네이버	카카오	삼성전자	Google LLC	Meta Platforms Inc.	넷플릭스 서비시스 코리아	아마존웹 서비시스 코리아	쿠팡
주요 서비스	검색, 쇼핑	메신저, 검색	간편결제, 앱스토어	검색, 동영상	SNS, 메신저	동영상	클라우드	쇼핑, 동영상

위의 내용들을 고려할 때 클라우드 컴퓨팅, CDN, 검색엔진, 커뮤니케이션 서비스 등 부가통신 분야에서 통신재난관리의 필요성이 높은 서비스를 통신재난관리 심의위원회를 통해 지정하고 이를 중심으로 대형 사업자에 대해 의무를 부과하고 이행 점검하는 체제로 전환하는 방향으로 정책 전환을 검토할 필요가 있다. 일상생활의 필수성이나 인프라적 기능에 대해서는 아직 통계적으로 확인할 수 있는 지표가 많지 않고, 해외 사례에서도 NIS2 지침을 제외하면 서비스를 인프라로 지정하여 규제를 부과하는 사례가 거의 없기 때문에, 정책 전환을 위해서는 시장의 이해관계자와 학계의 의견을 충분히 수렴하여 검토할 필요가 있을 것이다.

02 이슈 보고서

KICI 디지털안전본부
김성용 실장

대한민국 해저케이블: 글로벌 AI 시대의 전략적 경쟁력 강화 방향

1. AI 트래픽 폭증과 해저케이블의 중요성

최근 과학기술정보통신부는 '대한민국 AI 고속도로'를 구축한다는 비전 아래 「Hyper AI 네트워크 전략」을 발표하였다. 해당 전략은 2030년까지 AI·6G 시대를 선도할 초고성능·초지능 네트워크 인프라 구축을 목표로 하며, 이동통신망과 유선 백본망의 고도화뿐 아니라 해저케이블 확충을 핵심 과제로 명확히 제시하고 있다.

해저케이블은 국제 데이터 통신의 핵심 동맥이다. 전 세계 데이터 트래픽의 대부분은 해저케이블을 통해 이동하며, 특히 AI 기반 서비스가 확산됨에 따라 그 중요성은 더욱 커지고 있다. 초대규모 AI 모델 학습, 글로벌 클라우드 연산, 실시간 AI 서비스는 모두 초저지연·초대역폭 연결을 전제로 하며, 이로 인해 해저케이블은 AI 시대의 필수 인프라로 자리매김하고 있다. 국제 연결망이 충분히 뒷받침되지 않으면 국내 네트워크 성능이 아무리 고도화되더라도 글로벌 경쟁력 확보에는 한계가 있을 수밖에 없다.

이러한 인식 아래 정부는 해저케이블 용량을 2030년까지 약 2배 수준으로 확대하고, 현재 동남권에 집중된 케이블 상륙(landing) 지점을 서·남해 등으로 다변화하여 안정성을 제고하겠다는 목표를 제시하였다. 이는 급증하는 데이터 트래픽에 대응하는 동시에, 재해 및 지정학적 리스크를 분산하기 위한 전략적 조치로 평가된다.

2. 대한민국 해저케이블 전략의 핵심 방향

가. 용량 확대를 통한 글로벌 트래픽 대응

정부의 Hyper AI 네트워크 전략은 해저케이블 전체 전송 용량을 현재 대비 약 2배 수준으로 확대하는 것을 주요 목표로 설정하고 있다. 구체적으로는 해저케이블 용량을 약 110Tbps에서 220Tbps 이상으로 확충함으로써, 폭발적으로 증가하는 국제 AI 데이터 트래픽을 안정적으로 수용하고 글로벌 네트워크 경쟁력을 강화하겠다는 구상이다.

해저케이블은 단순한 데이터 연결 수단을 넘어 초저지연·고대역폭 국제 서비스의 기반 인프라다. 6G 시대가 본격화되고 AI 서비스가 실시간 상호작용 형태로 진화함에 따라, 케이블 용량뿐 아니라 경로의 다양성과 품질 안정성은 국가 경쟁력을 좌우하는 핵심 요소로 작용한다. 이에 따라 복수의 해저 경로 확보, 확장성이 높은 광섬유 기술 도입, 미래형 전송 규격 적용이 병행되어야 한다. 또한 프라이빗 네트워크와 AI 특화 네트워크 수요가 급증하는 상황에서, 단순한 물리적 용량 확충을 넘어 효율적인 운용 기술 확보 역시 중요하다. 예를 들어 트래픽을 실시간으로

예측·최적화하거나, 장애 발생 시 자동으로 우회 및 복구가 가능한 지능형 네트워크 운영 기술이 필수적으로 요구된다.

나. 육양국(케이블 상륙지점) 다변화를 통한 네트워크 안정성 강화

정부 발표에는 기존 동남권에 집중된 해저케이블 육양국을 서해·남해 등으로 다변화하여 네트워크 안정성을 강화하겠다는 방향도 포함되어 있다. 이는 특정 지역에 자연재해나 기술적 장애가 발생하더라도 국제 연결성이 유지될 수 있도록 하는 위험 분산 전략이다. 육양국 다변화는 국가 간 연결 경로의 다양성을 높여 네트워크 복원력(resilience)을 강화하는 효과를 가져온다. 더 나아가, 해저케이블 상륙지점과 국내 데이터센터 및 백본망을 유기적으로 연계함으로써 국제 트래픽 흐름을 최적화하고 지연시간을 최소화하는 기반을 마련할 수 있다.

〈그림1〉 국가 네트워크 고도화: 국제망

[출처] 「대한민국 'AI 고속도로',글로벌 1등 차세대 네트워크로 완성한다」, 과학기술정보통신부(25.12.17)

3. 글로벌 경쟁 구도 속 한국의 전략적 역할

해저케이블 인프라는 단순한 통신 설비를 넘어 국가 경쟁력과 디지털 주권, 나아가 지정학적 영향력을 확대하는 전략 자산으로 인식되고 있다. 글로벌 빅테크 기업들은 이미 자체 해저케이블 구축에 대규모 투자를 진행하고 있으며, 한국 기업들 역시 국제 해저케이블 시장에서 존재감을 확대하고 있다.

최근 대표적 사례로 SK브로드밴드는 아시아 7개국을 연결하는 국제 해저케이블 SJC2(Southeast Asia-Japan Cable 2)

프로젝트에 참여하여 2025년 7월 18일 상용 서비스를 개시하였다. SJC2는 한국, 일본, 싱가포르, 홍콩 등 주요 아시아 거점을 연결하는 고용량 해저케이블로, 급증하는 아시아 지역 데이터 트래픽을 안정적으로 수용하는 역할을 수행하고 있다. 아울러 태평양을 횡단해 아시아와 북미를 연결하는 차세대 해저케이블(E2A) 프로젝트에도 참여하고 있으며, 해당 사업은 향후 상용화를 목표로 구축이 진행 중이다. 이미 상용화된 해저케이블과 향후 구축될 차세대 케이블이 단계적으로 결합되면서, 한국의 국제 네트워크 위상은 점진적으로 강화되고 있다.

이에 대한 전략적 대응으로 정부는 해저케이블 확충을 국가 전략 차원으로 격상시키고 있다. 단기적으로는 용량 확대와 경로 다변화에 집중하되, 중장기적으로는 글로벌 디지털 허브로서의 역할을 강화해야 한다. 이를 위해 국내 통신사 및 장비 제조사와의 협력, 해외 파트너십 확대, 국제 표준화 활동 참여를 통해 한국이 글로벌 네트워크 지형에서 중추적 중계 노드로 기능할 수 있도록 정책적 뒷받침이 필요하다.

4. 미래 지향형 해저케이블 전략

가. 국가 주도의 R&D 및 기술 표준 확보 강화

국내 해저케이블 관련 기업들의 기술 경쟁력은 빠르게 성장하고 있으나, 글로벌 시장에서 자체 기술과 표준 주도권을 확보하는 것은 여전히 중요한 과제로 남아 있다. 이에 따라 정부는 연구개발(R&D) 지원을 확대하여 차세대 광섬유 전송 기술, 지능형 네트워크 관리 기술, 자동 장애 복구 기술개발을 적극적으로 촉진할 필요가 있다. 아울러 국제 표준화 기구에서의 활동을 강화함으로써 국내 기술이 국제 표준으로 채택될 수 있도록 전략적으로 대응해야 한다. 이는 한국이 글로벌 해저케이블 시장에서 기술 경쟁력과 시장 주도권을 동시에 확보하는 데 중요한 기반이 될 것이다.

나. 공공·민간 협력 체계 구축

해저케이블 구축과 운영에는 막대한 초기 투자와 장기적 관점의 사업 추진이 요구된다. 이를 위해 정부 주도의 인프라 투자와 함께 민간 자본 유치, 공공기관과 통신 기업 간 협력 체계 구축이 필수적이다. 정부는 주요 노선과 제도적 기반을 마련하고, 민간은 기술과 운영 역량을 바탕으로 참여하는 공유 인프라 모델을 구축함으로써 투자 리스크를 분담하고 효율성을 높일 수 있다.

다. 국제 협력 강화를 통한 글로벌 네트워크 허브 구축

한국이 해저케이블 전략을 국내 중심에서 글로벌 허브 전략으로 확장하기 위해서는 국제 협력 강화가 필수적이다. 양자 통신, 해저케이블 보안, 글로벌 연동 서비스 등 다양한 국제적 이슈에 대응할 수 있는 협력 플랫폼 구축이 요구된다.

국제기구 및 다자간 협력 네트워크 참여, AI 기반 트래픽 관리 기술 공유, 글로벌 데이터센터와의 직접 연동 강화 등을 통해 해저케이블은 단순한 데이터 전달 수단을 넘어 '디지털 실크로드'로 기능할 수 있다. 이를 통해 한국은 아시아를 넘어 유럽과 북미를 연결하는 글로벌 네트워크 허브로서의 역량을 점진적으로 강화할 수 있을 것이다.

5. 네트워크 주권과 미래 성장의 결합

해저케이블은 대한민국이 AI 시대 글로벌 경쟁에서 뒤처지지 않기 위한 핵심 전략 인프라다. 2030년까지 해저케이블 용량 확대와 경로 다변화를 추진하는 정부의 Hyper AI 네트워크 전략은 급증하는 국제 트래픽과 국가 경쟁력 확보 필요성에 대한 적절한 대응으로 평가된다.

앞으로 정부는 기술개발, 국제협력, 공공·민간 파트너십을 유기적으로 강화하여 해저케이블을 단순한 연결망이 아닌 글로벌 디지털 허브의 핵심 축으로 발전시켜야 한다. 이를 통해 대한민국은 AI 시대 초연결 네트워크 환경에서 신뢰받는 글로벌 파트너로 자리매김하며, 미래 성장의 주춧돌을 공고히 할 수 있을 것이다.

03 전문가인터뷰

SK브로드밴드
전상수 매니저

SKB 전상수매니저님을 만나다.

Q 우선 전상수 매니저님에 대해서 소개 부탁드립니다.

A 1999년에 정보통신 산업분야에 처음 발 딛고 해당 분야의 여러 현장에서 경험과 실무를 쌓고 있는 27년차 진행형 정보통신기술인 전상수입니다. 저는 ISP 회사에 재직하며 광가입자, 기간망, 백본망뿐만 아니라 방송망, 국제망에서의 실무 경험이 있습니다. 또한 실무 경험만으로는 한계가 있다는 저 나름의 각성으로 자격증에 도전하여 정보통신기술사, 통신설비기능장 자격을 취득하였습니다. 이 외에도 표준업무절차의 중요성을 실감하여 ISO 국제표준 9001, 14001, 45001 자격을 취득하였고, 2025년에는 정보통신 설계 분야의 역량 함양을 위해 설계 엔지니어 리더(VMP, CVS) 자격도 취득하였습니다. 최근에는 실무 경험과 여러 자격증을 맡은 업무에 잘 활용하려고 노력하고 있습니다.

Q 디지털 재난·장애의 안전관리와 관련된 업무 경험이 있으시다면 말씀해주시기바랍니다.

A 디지털 재난·장애는 디지털이란 단어가 붙어 어떤 범주로 생각해야 할지 모호한데, 정보통신은 거의 모든 분야에서 디지털화되어 가고 있어서 정보통신 재난·장애로 해석하여 답변드리겠습니다. 우선, 현재 운용 업무를 수행하고 있는 입장에서 디지털 재난·장애는 용어만으로도 마주하고 싶지 않다는 생각이 듭니다만, 피할 수 있는 것이 아니기 때문에 최대한 디지털 재난·장애가 발생하지 않도록 노력하고 있습니다. 저는 정보통신망의 운용 업무 상황에서 E2E 서비스의 개별적인 고장, 장애 경험 외에도 장비, 선로 등 다양한 고장 상황을 겪었습니다. E2E 서비스의 고장, 장애는 일반적으로 사전 인지되는 경우와 고객 신고로 알게 되는 경우로 구분하는데, 전자의 경우에는 B/S 활동으로, 후자의 경우 A/S로 조치하게 됩니다. 단순히 장비 고장인 경우에는 상대적으로 대응 여건이 양호한 편이나, 선로 단선, 전원 오프 등 현장에서 발생하는 원인자 사고는 피해 규모가 크기 때문에 원인자 사고의 경우 상황 종료 시까지 긴장감을 계속 유지하게 됩니다.

Q 최근 몇 년간 발생한 국내외 대형 통신 장애들을 바탕으로 기술적·절차적 허점을 어떻게 해결하는 것이 좋을까요?

A 주요 국내외 대형 통신 장애 발생 사례를 살펴보니, 국내에서는 K사 전국 인터넷 장애(2021.10), S사 판교 데이터센터 화재(2022.10), 정부 행정전산망 마비 사태(2023.11)가 있었고, 해외에서는 AWS 대규모 장애(2025.10), 플레이스테이션 네트워크 장애(2025.2), 클라우드플레어 인프라 장애(2025.11) 등이 있었습니다. 그리고, 작년 경북 의성·안동·영덕 및 경남 산청 등 영남 지역에서 동시다발적으로 발생한 산불로 인하여 최대 규모의 통신 시설 피해가 발생하기도 하였습니다.

앞서 말씀드린 통신 장애가 발생한 회사 뿐 아니라 그렇지 않은 회사들도 고장·장애 상황에서 필요한 긴급 처리절차는 모두 가지고 있을 것이라 생각됩니다. 다만, 리더와 구성원이 모두 해당 절차를 정확하게 이해하고 숙지하고 있는지, 절차가 제대로 작동되는지, 기존 절차가 현재 상황에서 보면 미흡하거나 달라진 것이 있다면 상황에 맞추어 업데이트 되어 있는지는 장담할 수 없을 것입니다. 결론적으로 통신재난 관리 업무에는 일회성이 아닌 지속성이 필요하다는 것입니다. 기술적·절차적 허점은 주기적인 점검을 통해 확인, 도출하고 메꿔 가면서 더욱 안전, 안정해지고 피해도 줄일 수 있을 것이라 생각됩니다.

Q AI 기술 등이 네트워크 관제나 장애 예측에도 도입되고 있는 것으로 알고 있습니다. AI가 미래의 디지털 재난을 예방하는 데에 어느 정도 기여할 수 있다고 보십니까? 혹은 AI 의존도가 높아짐에 따른 새로운 위험 요소는 없을까요?

A AI는 분명 미래 디지털 재난을 예방하는 데 도움이 될 것입니다. 그 도움의 정도가 어느 정도일지는 저도 예측할 수 없습니다. 우리가 누리고 있는 정보통신 인프라 환경은 한 개인이 예상하는 것보다 훨씬 더 거대하고 방대하며 다양한 방식으로 연결되어 있습니다. 하지만 그것들은 모두 인터넷을 통해 하나로 연결되고 있습니다. 이러한 인프라 환경에 AI 기술을 반영한다고 하면, 기술이 상용화되기 위해 얼마만큼의 시간이 필요할까요? 우리의 기대와 실현 가능한 기술 사이의 간격은 어느 정도일까요? 그리고 그 간격은 어떻게 채워가야 할까요? 보고서의 제목과 결론을 정하기 전에 보고서의 목차를 정하는 것이 우선되어야 하지 않을까 생각합니다.
또 개인적으로는 AI의 도입으로 인해 새로운 위험 요소가 발생한다기 보다는, 이 모든 것이 인터넷 하나로 연결되어 있다는 점 자체가 단 하나의 위험 요소라고 생각합니다. 모든 정보통신 인프라가 인터넷으로 연결되어 있다는 현실이 존재하는 한 위험 요소는 다양하고 지속적으로 발생할 것입니다.

Q 디지털 재난·장애 시 골든타임 내 서비스를 복구하는 것이 핵심인데요. 실제 현장에서 신속한 복구를 저해하는 요소가 있다면 무엇이라고 생각하십니까?

A 골든타임은 과연 어느 정도가 적정한 것일까요? 아마도 서비스를 사용하는 고객은 모두 **"가장 짧은 시간"**이라고 할 것입니다. 한편, 브랜드 가치가 이윤과 밀접하게 연결되어 있는 서비스 기업의 입장에서도 골든타임을 놓쳐 피해 범위가 확대된다면 브랜드 가치의 손상으로 지속 성장할 수 없는 상황에 처하게 됩니다. 작년부터 현재까지 발생하고 있는 여러 기업들의 개인정보 유출사고는 모든 국민이 골든타임의 중요성과 그에 대한 사업자 대응내용을 인지하는 계기가 되었습니다.
이러한 환경에서 현장 실무자는 일반적으로 디지털 재난·장애가 발생하면 최대한 빠른 시간내에 조치하려고 노력합니다. 일반적으로 골든타임은 한 시간이지만, 그 한 시간은 금방 지나가 버립니다. 예를 들어 현장 직원 한 명이 근무를 하는 중에 디지털 재난·장애가 발생할 경우, 경보나 고객 신고 전화 등으로 해당 상황을 파악하고 서비스 영향 여부를 판단하게 됩니다. 그리고, 고장 포인트를 판별하기 위해 현황 자료를 포함하여 장비 EMS의 경보, 이벤트 로그 등을 살펴봅니다. 그 와중 해당 내용을 유관부서에 전파하여, 자체

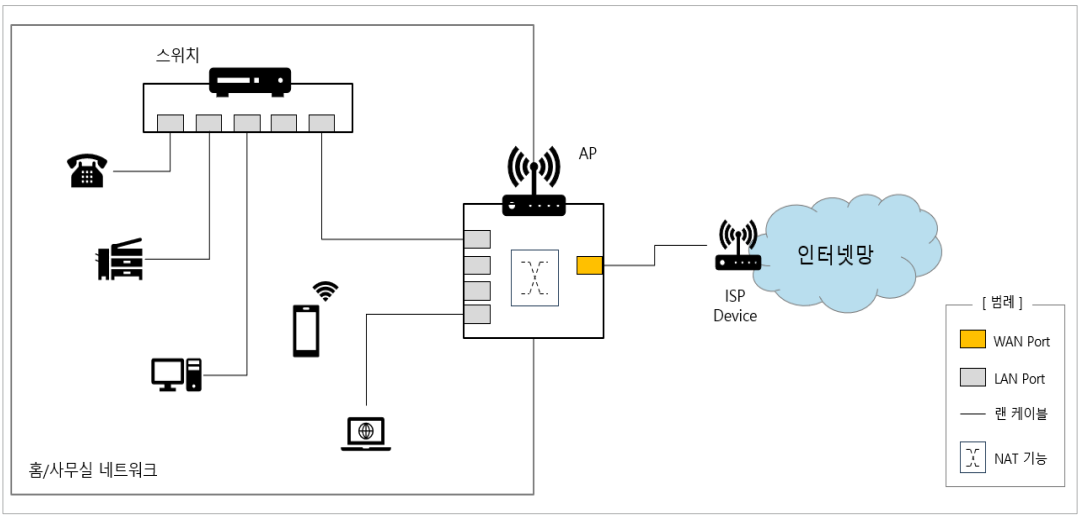
처리가 어려운 경우기술지원을 요청하기도 합니다. 그러다보면 복구 조치가 되지 않은 상태에서 상황 파악과 전파만 하다가 한 시간은 순식간에 지나가는 상황이 발생하게 됩니다. 서비스 기준으로 단순한 고장, 장애의 경우에는 수년간의 실무 경험과 절차에 따라 빠르게 조치가 가능하나, 디지털 재난·장애는 장애 진단과 함께 문제 구간 파악이 쉽지 않습니다. 정보통신 인프라는 하나가 아니라 다양한 정보통신설비의 집합체이며, 각 설비마다 수행주체가 다르기 때문에 골든타임을 최적화하기 위해 부단히 노력하고 있습니다.

이런 부분들을 AI가 대신한다면 복구시간을 단축할 수 있겠지만 앞서 이야기드린 바와 같이 준비 과정은 필요할 것으로 생각됩니다.

Q IoT 기기의 증가로 인하여 보안이 취약한 IoT 기기들이 좀비 PC가 되어 통신망에 대규모 DDoS 공격을 가할 위험이 커졌습니다. 초연결 환경에서 단말단의 취약점이 코어망 전체를 위협하지 않도록 방어할 수 있는 기술적 전략은 무엇이 있을까요?

A 인터넷서비스는 고객 댁내에 설치되어 있는 모뎀 또는 공유기(AP모뎀)를 통해 각종 단말이을 연결되어 있는 구조입니다. 일반적으로 공유기라고 불리는 AP모뎀을 사용하게 되며, 해당 AP모뎀은 NAT 기능을 가지고 있어 공인IP와 사설IP를 상호 변환해 주는 기능을 수행합니다. 댁내에서 IoT 기기는 AP모뎀을 거점으로 연결되며 사설IP가 할당됩니다. 그렇게 때문에 ISP 사업자 입장에게서 AP모뎀을 거쳐 연결되는 IoT 기기는 관리범위 밖이나, 그로 인해 발생되는 트래픽은 관제할 수 있습니다. 따라서 단말단에서 쉽게 접근이 가능한 방법은 IoT 기기를 연결하는 Gateway 역할의 기기에 대해 보안관리를 하는 것입니다. 이 때 프로토콜에 따라 사용하는 논리적 포트를 관리하는 것도 하나의 방법입니다.

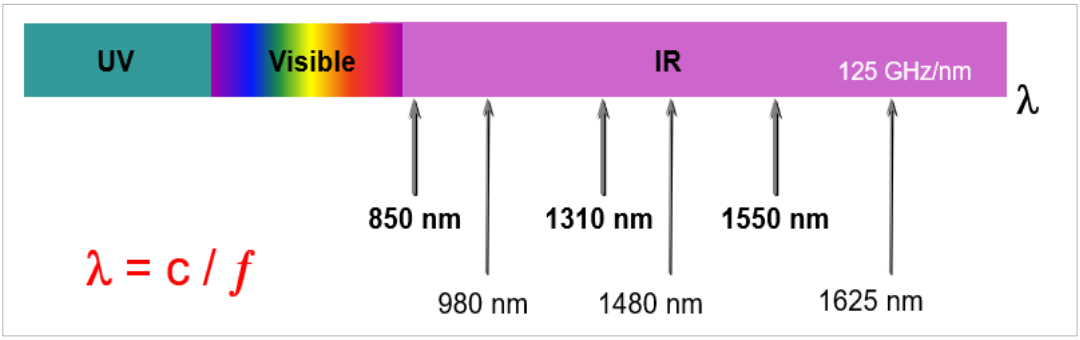
〈그림1〉 홈/사무실 내부 인터넷 네트워크 구성 예제



Q 고화질 영상 수요의 증가로 인하여 해저케이블 등의 전송 용량 및 효율을 높이는 기술이 중요해지고 있는데요. 현재의 광전송 기술로 기존 케이블의 수명이나 용량을 어느 정도까지 늘릴 수 있다고 생각하시나요?

A 제가 알기로는 기존 케이블의 수명을 늘리는 광전송 기술은 없지만 용량을 늘리는 기술은 있습니다. 광통신에서 가장 어렵고 중요한 기술은 전기 신호를 광신호로, 광신호를 전기신호로 상호 변환해주는 광파장을 이용하여 신호를 송수신하는 광모듈 기술입니다.

〈그림2〉 광통신에 사용되는 광스펙트럼



광신호는 전송신호 계위로 설명하면 더 쉬운데, PDH(Plesiochronous Digital Hierarchy, 준동기 디지털 계층의 약자로 과거 통신망에서 디지털 신호를 전송하기 위해 사용되던 전송 방식/기술 표준), SDH/SONET(Synchronous Digital Hierarchy/Synchronous Optical Network, 광통신 기반의 고속 디지털 전송 표준으로 PDH의 한계를 극복하기 위해 등장한 기술), Ethernet(가장 널리 사용되는 유선 근거리 통신 기술 표준)을 거쳐 OTN(Optical Transport Network, 대규모 광통신망에서 데이터를 더 안전하고 효율적으로 장거리 전송하기 위해 만들어진 국제 표준 기술) 계위가 현장에서 사용되고 있습니다. OTN은 OTU4라고 불리는 단일프레임으로 100Gbps/λ 속도를 제공하고 있으며, B100G(Beyond 100G, 100Gbps를 초과하는 전송 기술)로 OTNCn 계위가 상용화 진행 중으로 알고 있습니다. 이러한 논리적 구조에 따라 800Gbps의 서비스 속도가 가능해질 것입니다.

다만, 현재 고용량 광모듈에서는 노키아, 씨에나, 화웨이 같은 외산 장비가 주로 사용되고 있다는 점이 아쉽긴 합니다. 향후에는 All Optical Network을 기대해 봅니다.

Q 해저케이블은 통신·해양·안전·안보 등 여러 분야가 복잡하게 얽혀있는 분야입니다. 현장에서 느끼시기에 해저케이블과 관련하여 아쉬운 점이나 개선이 필요하다고 느끼시는 부분이 있다면 무엇일까요?

A 현재, 한국과 연결되어 있는 해저케이블 중 최근에 개통한 SJC2를 제외하고 APCN2, C2C, EAC, FNAL 등의

해저케이블은 가용 용량이 줄어들고 있으며, 노후화되어 가고 있는 상황입니다. 지구 온난화로 인한 태풍, 해일 등 천재지변에 따른 피해 최소화와 신속한 복구를 위해 다양한 해저케이블 사업자를 활용하여 안전하고 안정적인 물리적 다원화 구조를 확보하는 것이 점점 중요해지고 있습니다. 서비스 측면에서 국가와 국가를 연결하는 해저케이블 사업을 조금 축소해서 도시와 도시를 연결하는 정보통신망 사업이라고 생각한다면, 가장 중요한 것은 물리적 이원화 구조를 확보하는 것입니다.

Q 완벽하게 디지털 재난·장애를 방지할 수 없다는 가정하에, 향후 정부와 기업은 '무결점 달성'과 '빠른 회복 탄력성 확보' 중 어디에 우선순위를 두고 기술 투자를 해야 한다고 생각하십니까?

A 최근 통신 보안과 관련하여 여러 이슈가 발생하며 서비스 대상 고객 뿐 아니라 국민 전체가 보안 부분에 대한 조치가 제대로 이루어지지 않는다고 생각하시는 것 같아 기술자로서 답답한 마음이 듭니다.

무결점 달성과 빠른 회복탄력성 확보 중 어디에 우선순위를 두어야 할까는 정말 어려운 질문인데, 저라면 빠른 회복탄력성 확보에 무게를 조금 더 두고 싶습니다. 왜냐하면 보안분야는 제로 트러스트를 거쳐 '사이버 복원력(Cyber Resilience)'로 방향으로 가고 있기 때문입니다. 모든 분야에 사람이 주가 되어 업무를 수행하기 때문에 무결점 달성은 불가능한 일이며, 사고는 언제 어디서든 발생할 수 있다고 생각합니다. 하지만 이러한 사고를 예측하여 빠르게 복구하고 피해를 최소화할 수 있다면 그것이 더 타당한 접근이 아닌가 싶습니다.

앞서 말씀드린 바와 같이, 이를 위해 준비해야 할 것들이 너무나도 많다고 다들 생각하실 겁니다. 저도 물론 그렇습니다. 요즘 붐인 AI 활용한 방법도 좋겠지만 저는 우문현답을 제시하고 싶습니다. 현장을 제대로 알고 거기서 답을 찾는 현명한 접근이 필요한 시점이라고 생각합니다.

04 디지털 안전 관제 이슈

12월 발생 이슈

01 2025.12.05.

- 클라우드플레어 DNS 오류로 인한 서비스 장애

02 2025.12.10.

- 티맵 내부 시스템 장애로 인한 서비스 접속 장애

03 2025.12.11.

- ChatGPT 안드로이드 이용 중 서비스 오류

04 2025.12.15.

- 카카오티 접속 오류, 서비스 장애

05 2025.12.15.

- 삼성페이-하나카드 결제서비스 장애

06 2025.12.16.

- 디시인사이드 서비스 접속 장애

07 2025.12.19.

- 유튜브 스트리밍 서비스 재생 오류

08 2025.12.25.

- SK브로드밴드 시스템 오류에 따른 유선 장애

05 Digital Safety Inside

2026년도 통화량 급증 예상일 조사 달력

1월(January)

일	월	화	수	목	금	토
특이사항 o 해운대 빛축제 (해운대, '25.11.29.~'26.01.18.) o 서울빛초롱축제 (청계천, '25.12.12.~'26.01.04.) o 서울 라이트 DDP 카운트다운 (중구, '25.12.31~'26.01.01)				1 신 정 o 새해 맞이 행사	2 o 백현 콘서트 (서울, 1/2~1/4) o 임영웅 콘서트 (대전, 1/2~1/4)	3 o 조용필 콘서트(광주) o 대성 콘서트 (서울, 1/3~1/4) o 잔나비 콘서트 (부산, 1/3~1/4)
4	5	6	7	8	9 o 평창 송어축제 (평창, 1/9~2/9)	10 o 화천 산천어축제 (화천, 1/10~2/1) o 이문세 콘서트(부산)
11	12	13	14	15	16	17 o 임재범 콘서트 (서울, 1/17~1/18)
18	19	20	21	22	23 o 다이나믹 듀오 콘서트 (서울, 1/23~1/25)	24 o 멘 아이 트러스트 내한 공연(서울) o 이문세 콘서트(대구) o 다비치 콘서트 (서울, 1/24~1/25)
25	26	27	28	29 o K-일러스트레이션페어 (서울, 1/29~2/1)	30	31

2월(February)

일	월	화	수	목	금	토
특이사항 o K-리그 개막 예상 ('26.02.14) ('25.02.15, 토요일 개막)						
1	2	3	4	5	6 o 2026 밀라노 동계올림픽 (2/6~2/22)	7
8	9	10	11	12	13	14 o 밸런타인데이
15	16 설날 연휴	17 설날	18 설날 연휴	19	20 o 드림씨어터 내한공연 (서울, 2/16~2/18)	21
22	23 o 원리퍼블릭 내한공연(서울)	24	25	26	27 o 원오크록 내한공연 (서울, 2/27~2/28)	28

KICI 한국정보통신 산업연구원

경기도수원시장안구하률로12번길80(천천동)
TEL.031-231-3400FAX.031-269-5210
www.kici.re.kr