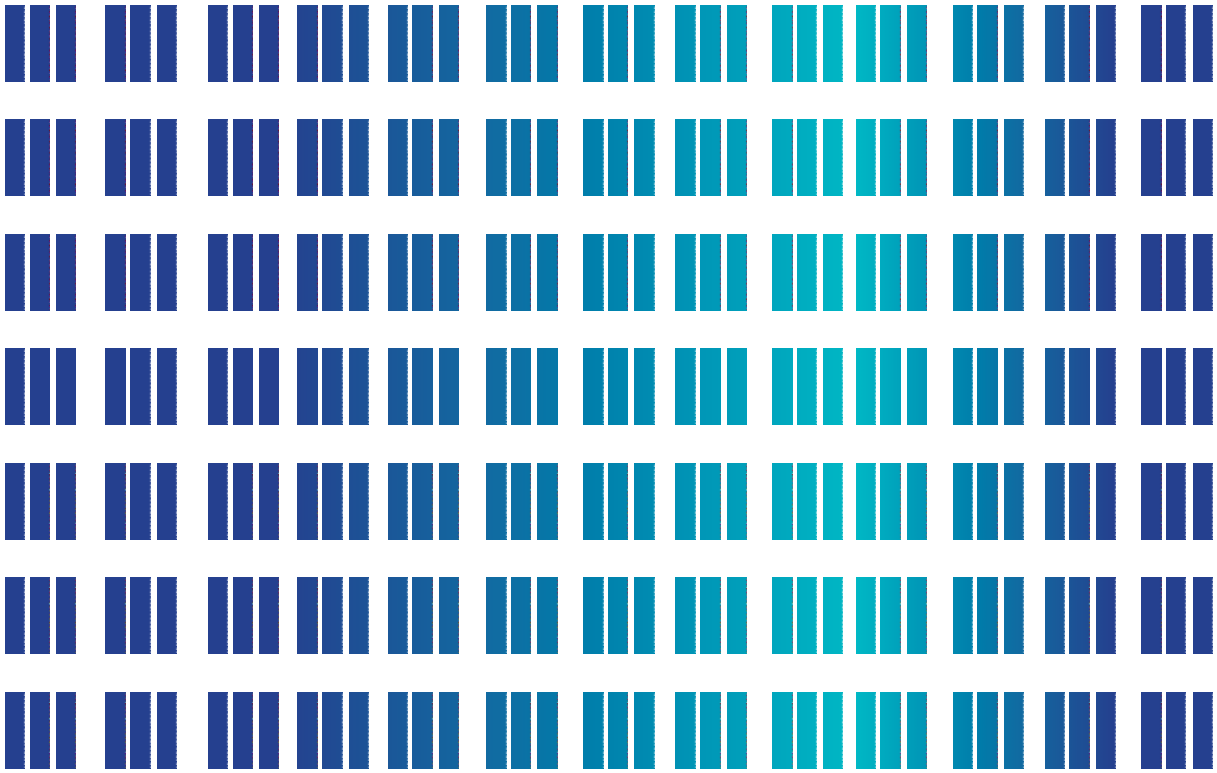
KICI DSR Vol. 25-05

한국정보통신산업연구원

Digital Safety Report

9월호



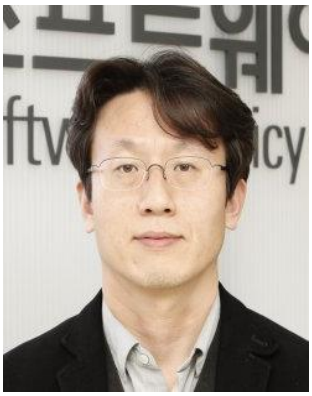
KICI 한국정보통신 산업연구원

한국정보통신산업연구원

Digital Safety Report

Digital Safety Report Contents

01 소프트웨어 안전 확보와 디지털 사회 안전



소프트웨어정책연구소(SPRi)
박태형 실장

오래된 이야기가 되었지만, 제4차 산업혁명이라 불리는 새로운 패러다임의 등장으로 전세계는 소프트웨어를 중심으로 산업 분야의 혁신과 경쟁력 강화에 국가적 총력을 기울였고, 소프트웨어 융합은 국민과 기업 그리고 정부의 전 부문에 걸쳐 새로운 가치를 창출했다. 또한 코로나 팬데믹으로 인해 디지털 사회는 그 어느 때보다 강력한 폭발력으로 그 영역을 확장해 왔다.

동시에 이러한 상황은 디지털 사회의 무한 연결성과 복잡성을 증가시킴으로써 단일 지점의 오류가 신체, 생명, 재산 등에 막대한 사회적 피해 또는 재난을 초래할 수 있음을 심각하게 인식하고, '소프트웨어 안전' 개념을 도입하게 되었다.

우리는 이미 2020년「소프트웨어 진흥법」전면 개정을 통해 '소프트웨어 안전' 확보를 위한 법적 근거를 마련하였다. 이는 산업 도메인 별로 국제 표준을 기준으로 적용되어 오는 기능 안전 개념을 법 체계 안에서 명문화한 세계 최초의 사례이다.

「소프트웨어 진흥법」제2조제8호에 따르면, '소프트웨어 안전'이란 외부로부터의 침해행위가 없는 상태에서 소프트웨어의 내부적인 오작동 및 안전기능(사전 위험분석 등을 통하여 위험발생을 방지하는 기능을 말한다) 미비 등으로 인하여 발생할 수 있는 사고로부터 사람의 생명이나 신체에 대한 위험에 충분한 대비가 되어 있는 상태를 말한다.

또한, 동법 제4장 제1절 소프트웨어 융합 촉진 및 소프트웨어 안전 확보 제30조(소프트웨어 안전 확보) 제1항에 따라 소프트웨어 안전 확보를 위한 시책을 마련할 수 있고, 제2항에 따라 소프트웨어 안전 관련 위험 분석, 소프트웨어 안전 확보를 위한 설계 및 구현 방법, 소프트웨어 안전 검증 방법, 운영 단계의 소프트웨어 안전 확보 방안, 그 밖에 소프트웨어 안전 확보에 필요하다고 인정되는 사항 등 소프트웨어 안전 확보를 위한 지침을 정하여 고시하도록 하였다.

이에 따라,「소프트웨어 안전 확보를 위한 지침」을 고시하여, 공공기관이 안전 확보가 필요한 소프트웨어를 개발하거나 운영하는 경우에 적용할 수 있도록 하였다. 생명, 신체 또는 재산에 피해를 발생하는 사고를 유발할 수 있는 소프트웨어나 시스템의 전주기에 걸쳐 적용하는 것이다.

그러나 이러한 '소프트웨어 안전 확보'를 위한 법 체계는 우리가 디지털 사회의 안전성을 어느 국가보다도 중요하게 고려하고 있음을 보여주는 의미를 가지고 있음에도 불구하고, 적용이 공공기관에만 제한될 뿐만 아니라 권고규정으로 제정·고시되어 그 실행력 확보에 어려움을 겪고 있다.

한편, 2022년 10월 경기도 성남 판교 SK C&C 데이터센터에서 발생한 화재는 카카오의 주요 서버를 멈추게 했고, 카카오톡을 비롯해 카카오택시, 카카오맵 등 생활 전반에 밀착된 서비스들이 동시에 마비되면서 디지털 사회의 안전성 확보 이슈가 수면 위로 부상하였다.

이를 계기로 「방송통신발전 기본법」 개정을 통해 기존의 재난관리 의무를 이행해 온 SKT, KT 등 기간통신사업자 뿐만 아니라 네이버, 카카오 등 부가통신 사업자 등에 대해서도 매년 통신재난관리계획을 수립·제출하게 하고 이행토록 의무를 부과하였다. 특히, 서비스 안정성 확보를 위한 기술적·관리적 측면의 지침을 수립·이행하도록 함으로써 넓은 의미에서 '소프트웨어 안전'을 확보하도록 하고 있다.

정부는 위 주요 부가통신사업자의 통신재난관리계획에 대한 관리·이행 현황을 점검함으로써, 통신재난 관리의 전 주기(예방-대비-대응-복구)에 걸쳐 관리·이행의 실행력을 확보하고 있다.

다시 디지털 사회의 안정성 확보를 생각해 보자. 디지털 사회의 안전은 사이버보안(Security)과 소프트웨어 안전(SW Safety)이라는 두 개의 핵심 축(pillar)으로 유지된다. 이 두 축은 모두 위험과 사고를 기반으로 강화된다. 이것은 곧 위험과 사고에 대한 안전관리의 관점(예방-대비-대응-복구)에서 접근하고 관리 체계를 구축해야 한다는 말이다.

또한 한 축이 담당하는 영역에서의 사고가 빈번하다고 해서 더 비대해지고 강화된다면, 지지하고 있는 디지털 사회의 안전성은 기울어질 수 밖에 없다. 사이버보안 사고에 비해, 아직까지는 소프트웨어 안전 사고가 상대적으로 적은 빈도로 더 작은 피해를 낳아 왔다고 해서, 소프트웨어 안전의 관리체계가 빈약해지거나 소홀해져서는 안 된다는 것이다.

디지털 사회에서 안전은 비용이 아니라 성장의 원천 자산이다. 공공과 민간을 구분짓지 않는다. 소프트웨어 안전은 규제 강화의 언어로만 말하면 작아지고, 경쟁력 확보의 언어로 말하면 커진다. 「소프트웨어 진흥법」과 「방송통신발전 기본법」이 연 소프트웨어 안전 관리의 문턱을 넘어, 단계적 방식으로 일원화되고 효율적인 체계가 구축되도록 해야 한다.

법 제도가 지양하는 위험의 최소 수준을 기준 삼아, 정부와 기업 그리고 시민 사회가 자발적이고 능동적인 안전의 지향점을 만들어가자. 그러한 노력이 실천될 때 디지털 사회의 안전 신뢰를 두텁게 하고, 디지털 국가 경쟁력을 높이는 가장 빠른 길이 될 것이다.

02 해외 사업자에 대한 통신재난관리 규범 체계 이행 유도 및 이행강제 확보 방안

KICI 디지털안전본부
박민지 선임연구원

들어가며

2025년 현재 「방송통신발전기본법(이하 '방송통신발전법')」상 통신재난 관리 수범대상 사업자는 국내 사업자로는 네이버, 삼성전자, 카카오, 쿠팡의 4개사, 해외사업자로는 구글 엘엘씨, 넷플릭스서비시스코리아, 메타플랫폼스, 아마존웹서비스코리아의 4개사이다.

과학기술정보통신부는 매년 사업자의 통신재난 관리계획을 제출 받아 그에 대한 이행현황을 점검하고 미흡한 사항에 대하여는 시정 조치를 단행하고 있다.

1. 현황

사업자의 주요 소재지가 국내외인 것을 불문하고 대형 부가통신사업자가 제공하는 메신저, 사회연결망서비스(SNS), OTT(Over The Top), 클라우드에 이어 CDN(Content Delivery Network)서비스 등 부가통신서비스는 국민 일상에 매우 밀접하게 영향을 끼친다. 국내 사업자의 경우 국내 법규범 준수에 적극적인 태도를 보이고 있으나, 해외 사업자의 경우 국내에서 부가통신역무 제공 시에는 부가통신사업 신고 등 「전기통신사업법」의 적용대상이 명백함에도 불구하고 글로벌사업자로서의 특이성을 이유로 협력적이지 않은 경우가 발생하고 있다.

행정의 실효성 확보를 위한 수단은 통상 ① 행정상 의무위반에 대한 제재로서 '행정벌', ② 행정상 의무불이행 등과 이행강제 수단으로서 '행정상 강제집행' 및 '행정상 즉시강제', ③ 자료획득 작용으로서 '행정조사', ④ 기타의 수단으로서 '금전상 제재' 등이 있다. 이 법에서는 시정조치, 금전상 제재로서의 과징금, 행정질서벌로서의 과태료를 규정하고 있다. 현재 「방송통신발전기본법」상 부가통신사업자에 대한 통신재난관리와 관련한 제재조치는 이하 표와 같다.

〈 부가통신사업자에 대한 통신재난관리와 관련한 제재조치 〉

구분	방송통신발전기본법
시정조치 (제36조의2 제2항)	과학기술정보통신부장관과 방송통신위원회는 주요 방송통신사업자가 제출한 방송통신재난관리계획에 따른 이행 여부를 지도·점검할 수 있으며, 점검결과 보완이 필요한 사항에 대하여 시정조치
과징금 (제40조의4)	방송통신재난관리계획의 이행 여부에 따른 시정명령 위반시 주요 방송통신사업자에게 그가 제공하는 방송통신서비스의 직전 3개 사업연도의 연평균 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과

과태료 (제48조)	통신시설의 등급지정에 따른 근거자료의 미제출 또는 거짓 제출시 3천만원 이하의 과태료 부과 (제35조의3 제1항 위반)
	통신시설의 지정된 등급에 따른 구체적인 관리 기준 위반 시 3천만원 이하의 과태료 (제35조의3 제3항 위반)
	수립지침을 따르지 않은 방송통신재난관리계획에 대한 보완명령 위반시 3천만원 이하의 과태료 (제36조 제3항 위반)
	경계 이상 방송통신재난 발생 또는 장애발생 이동통신사업자의 무선통신시설 공동이용 요청에 따른 명령 위반시 3천만원 이하의 과태료 (제37조의2 제2항 위반)
	기준에 따른 통신재난관리 전담부서 또는 전담인력을 운용하지 않은 경우 3천만원 이하의 과태료 (제39조의2 제2항 위반)
	방송통신재난관리계획의 미제출 또는 거짓 제출시 1천만원 이하의 과태료 (제36조 제2항 위반)
	방송통신재난의 미보고 또는 거짓 보고시 1천만원 이하의 과태료 (제38조 위반)
	방송통신재난의 피해복구 진행 상황 등에 대한 대책본부 보고를 하지 않거나 거짓 보고시 1천만원 이하의 과태료 (제39조 제4항 위반)
	방송통신재난책임자 미지정시 1천만원 이하의 과태료 부과 (제39조의2 제2항 위반)
	방송통신설비 설치·운용의 적정 여부를 확인, 국가비상사태·재해 및 재난 시의 원활한 방송통신 확보, 통신시설의 등급 지정 및 관리상태의 적정성 확인을 위한 보고의 미이행 또는 거짓보고, 그에 따른 검사를 거부·방해 또는 기피시 1천만원 이하의 과태료 (제43조 제1항 위반)

2. 행정법상 이행강제 확보 방안

행정의 실효성 확보 수단으로, 행정상 의무불이행 등과 이행강제 수단으로서 '행정상 강제집행' 또는 '집행벌' 등이 존재한다. 그 외 사후적인 제재로서 금전상 제재(과징금, 가산세, 가산금, 부당이득세), 제재적 행정처분(허가 등의 거부·정지·철회), 공급거부, 공표, 시정명령 등의 수단이 활용되고 있다.

부가통신서비스는 매우 복잡한 소프트웨어적 통제가 이루어지므로, 해당 사업자 외의 제3자가 해당 시스템에 대하여 직접 통제하는 것이 사실상 불가능하다. 따라서 그에 대한 행정규제는 사업자가 스스로 이행하여야 하고, 다른 제3자가 임시조치를 대행하기 어려운 바, 비대체적 작위의무에 해당하는 것으로 평가된다.

따라서 해외 사업자가 자발적으로 위 법적의무를 준수하지 않을 경우, 행정규제의 실효성 확보를 위해 이행강제금을 부과하는 방식으로 간접적 강제를 할 수 있을 것으로 생각된다. 이행강제금은 의무위반에 대하여 장래의 방향으로 의무이행을 확보하는 수단으로서 과거의 의무위반에 대한 제재인 행정벌과 구별된다. 또한 행정벌과는 그 처벌 내지 제재대상이 되는 기본적 사실관계로서의 행위, 보호법익과 목적에서 차이가 있으므로 병과될 수 있으며, 그 의무의 이행이 있기까지 반복하여 부과할 수 있다.

이미지 : flaticon.com

3. 결론

해외 사업자에 대한 집행력 확보 방안을 검토할 때 부가통신서비스에 대한 행정규제는 직접적인 강제가 어려운 측면이 있다. 이는 부가통신서비스사업자에 대한 규제가 비대체적 작위의무에 해당한다는 특징에 기인한 것이다. 그에 따라 정부가 사업자의 의무를 직접 수행할 수 없는 비대체적 작위의무를 강제하여야 하는 경우, '집행벌(강제금)' 부과방안이 가장 타당하다고 보여진다.

현재 우리 법제상 강제금에 대한 일반 규정은 없기 때문에 이러한 강제수단을 확보하기 위해서는 법개정 절차를 거쳐야 한다. 다만, 이행강제금과 과태료를 함께 부과하게 되면 수범자에게는 금전적 제재의 중복 부과에 대한 부담이 발생하므로 새로 이행강제금을 도입할 때에는 과태료 부과 규정을 삭제하는 방안도 함께 검토하는 것이 바람직하다.

특히 어떠한 의무에 대하여 이행강제금의 도입을 통해 그 실효성 확보가 가장 중요한지에 대한 판단이 선행되어야 할 것이다. 방송통신재난관리에 있어서 가장 토대가 되는 기준은 사업자가 제출하는 관리계획이다. 따라서 해당 관리계획이 수립지침에 따라 작성되었는지 여부를 가장 강력하고 확실하게 담보하여야 할 것이다.

03 전문가 인터뷰

- 한국정보통신기술협회(TTA) 김진영 팀장(前 센터장)을 만나다 -

한국정보통신기술협회(TTA)
김진영 팀장

Q1. 우선 김진영 팀장님에 대해서 소개 부탁드립니다.

A1. 저는 현재 한국정보통신기술협회 소프트웨어시험인증연구소 소프트웨어품질평가팀에서 근무하고 있습니다. 2015년도부터 과기정통부의 소프트웨어 안전 정책에 따라 한국정보통신기술협회 소프트웨어안전센터에서 소프트웨어 안전 업무를 10년간 진행하였습니다.

Q2. 팀장님께서는 디지털 재난·장애의 안전관리와 관련된 업무 경험이 있으실까요?

A2. 2014년 세월호 침몰 사고 이후로 안전에 대한 경각심이 높아지면서 ICT 주무부처인 과기정통부에서는 디지털 시스템의 안전을 도모하기 위한 정책과 업무를 수행하고 있습니다. 저는 2015년부터 과기정통부 및 유관기관(NIPA, SPRi)과 함께 공공분야의 소프트웨어 안전 강화를 위한 진단 사업이나 정책 수립 등의 업무, 특히 통신 재난 관리 시스템 진단 업무를 수행하였습니다.

Q3. 기존의 재난과 비교하여 디지털 재난·장애는 어떤 특성을 가지고 있다고 생각하시나요?

A3. (자연 재난을 제외하고) 기존의 사회 재난은 시설이나 하드웨어 중심으로 발생하여 파급 범위가 국소적이고 제한되며, 시설을 진단하는 과정에서 육안으로 상태를 확인하고 대비할 수 있었습니다. 반면, 디지털 재난은 소프트웨어와 네트워크에 기반하다 보니 시스템 규모에 따라 전국의 불특정 다수에 영향을 끼칠 수 있으며 눈에 보이지 않는 디지털, 소프트웨어의 특성상 현 상황에 대한 진단이 까다롭습니다. 우리나라에서도 최근 몇 년 동안 행정 업무 시스템의 장애로 국민 전체가 생활 전반에 불편을 겪은 사례가 이를 잘 보여줍니다.

Q4. 최근 발생한 국내외 디지털 재난 사례 중 특히 주목할 만한 사례는 어떤 것이 있을까요? 또 이러한 디지털 재난이 반복되지 않기 위해서는 어떠한 노력이 필요할까요?

A4. 디지털 시대로 들어서며, 디지털 재난·장애는 국내외를 막론하고 지속적으로 발생해 왔습니다. 최근에는 전 세계적인 대규모 시스템 마비를 불러왔던 CrowdStrike 사고가 있었는데요. 사이버보안 기업인 CrowdStrike가 배포한 소프트웨어 업데이트 파일의 결함으로 인해 윈도우 시스템 850만 대가 오류를 일으킨 사고입니다. 전 세계적으로 시스템의 연결성이 극도로 높아진 상황에서 디지털 시스템에 대한 점검이나 운영 절차가 얼마나 중요한지를 보여준 사태였습니다. 우리나라에서도 최근 몇 년동안 정부 24,

사회보장정보시스템 등의 구축 및 운영 과정에서 시스템이 정상 운영되지 못하는 장애들이 발생한 바 있고, 2023년 KT 인터넷망 장애 사고도 사회 전반에 큰 파급효과가 있었던 사례입니다. 이 모두, 디지털 인프라의 운영 안정성과 신뢰성이 얼마나 중요한지, 지속적인 관리와 제도적인 뒷받침의 필요성을 여실히 보여주는 사례라고 생각합니다.

이러한 디지털 재난·장애 사고가 반복되지 않기 위해서는 시스템 개발 시 문서 작업 문화가 개선되어야 한다고 생각합니다. 영세한 중소 사업자는 납품 기일에 맞추기 위하여 선납품 후 시범 운영 기간에 시스템을 보수하는 경우가 많은데요. 하지만 이러한 보수 중 변경사항은 문서화되지 않는다는 것이 문제점입니다. 물론 외국계 기업이나 국내 대기업의 경우 시스템 개발 초기부터 그 과정을 상세히 기록하고 있지만, 결국 중소 사업자가 대기업에 납품을 하는 구조로 이루어져 있기 때문에 중소 사업자의 시스템 개발 환경이 개선되지 않으면 사고는 반복될 수밖에 없다고 생각합니다. 따라서 개발 단계에서부터 문서화·체계화가 필요하고, 이러한 발판이 마련되어야 사고를 미연에 방지할 수 있다고 생각합니다.

Q5. 부가통신 사업자가 제공하는 서비스(클라우드, 메신저 등)에서 가장 빈번하게 발생하는 장애 유형은 무엇인가요? 또 이를 예방하기 위한 기술적 접근에는 어떤 것이 있을까요?

A5. 가장 빈번한 서비스 장애는 특정 기간에 집중된 시스템 부하를 처리하지 못 하거나 소프트웨어를 배포하는 과정에서 발생하는 장애인 것 같습니다. 반면, 빈번한 장애는 아니지만 화재나 DB/스토리지 장애 등은 한 번 발생하면 규모가 크고 복구에 시간이 소요될 수 있는 점에서 주목하여 관리해야 할 장애 유형이라고 생각합니다. 따라서, 단순히 발생 빈도 뿐 아니라 그 파급력까지 고려하여 위험을 관리할 필요가 있습니다. 또한 이런 장애들을 예방하기 위해서는 기술적인 대책도 필요하겠지만, 운영·관리적 접근이 함께 수반되어야 합니다. 기술적으로는 시스템에 결함 유입을 최소화할 수 있도록 구조적으로 설계 및 구현해야 하고, 운영적으로는 특히 업데이트가 발생하는 단계를 중심으로 운영 단계 전반에서 체계적인 점검 기준과 절차를 가지고 예외 없이 적용하는 것이 중요하다고 생각합니다.

Q6. 디지털 재난·장애가 발생했을 경우 사회적 파급력이나 이용자에게 미치는 영향이 크다고 생각하시나요? 만약 그렇다면 어떤 유형의 서비스가 특히 그렇다고 보실까요?

A6. 디지털 재난·장애는 국지적일 수 있는 자연재난 또는 사회재난에 비해, 짧은 발생 시간만으로도 사회적 파급력이 매우 크다고 생각합니다. 특히 메신저, 포털, 클라우드 등의 서비스처럼 국민 생활과 업무 전반에 직접 연결된 서비스에서 장애가 발생하면 그 영향이 더 심각합니다. 예를 들어 메신저나 포털 서비스가 멈추면 일상적인 의사소통과 정보 접근이 마비되고, 클라우드 서비스가 중단되면 이를 기반으로 하는 수많은 기업 서비스까지 연쇄적으로 영향을 받습니다. 결국 디지털 재난·장애는 단순한 불편을 넘어 사회적 혼란과 경제적 손실로 확산될 수 있기 때문에, 특히 이러한 핵심 서비스의 안정성과 복원력을 확보하고 관리하는 것이 무엇보다 중요하다고 생각합니다.

Q7. 부가통신 사업자가 디지털 재난·장애를 대비하기 위해 반드시 필요한 인프라 설계나 기술적 고려사항에는 무엇이 있을까요?

A7. 디지털 재난·장애에 대비하기 위해 인프라 설계 단계에서는 무엇보다 단일 실패 지점(Single Point of Failure)을 제거하는 것이 중요합니다. 예를 들면, 이중화를 도입하거나 멀티 클라우드를 활용하는 등 인프라를 준비하고, 자동으로 시스템의 장애를 감지하여 신속히 전환(Failover)할 수 있는 체계가 필요합니다. 안전이 필수적인 시스템에서는 하드웨어나 설비의 이중화 뿐만 아니라 소프트웨어의 이중화·삼중화까지도 고려하는데, 부가통신 사업자가 운영하는 시스템도 이를 참고하여 장애에 대비할 수 있어야 합니다. 또한 트래픽이 급증하는 상황 등에 대응할 수 있도록 오토스케일링 등의 기술적인 대비도 필요합니다. 운영 단계에서는 무중단 배포, 실시간 모니터링 및 자동 로그 분석, 주기적인 모의 훈련을 통해 장애 대응력을 높여야 합니다. 결국 핵심은 설계 단계에서 검증 활동에 기반한 시스템의 신뢰성을 기반으로 복원력과 이중화를 구조적으로 내재화하고, 운영 단계에서 이를 지속적으로 검증·보완하는 것이라고 생각합니다.

Q8. 앞으로의 디지털 재난 대응의 관점에서 부가통신 서비스 환경에 가장 큰 영향을 미칠 기술이나 환경의 변화가 있다면 무엇이라고 생각하시나요?

A8. 부가통신 서비스가 운영되는 환경이 다양하다 보니 이에 영향을 미칠 기술이나 환경 또한 매우 다양합니다. 그 중에서 대표적으로는 클라우드의 도입에 따른 서비스 구조나 배포 방식의 변화가 가장 큰 영향을 줄 것으로 생각합니다. 이외에도 초연결 환경의 확산, 특정 기업 주도의 기술 집중, 인공지능 활용 확대도 중요한 변수가 될 것입니다. AWS, Naver Cloud와 같은 대형 클라우드 서비스의 활용도가 높아지면서 특정 사업자의 장애가 다른 부가 통신 서비스의 장애로 이어질 수 있으므로 멀티 클라우드 전략이 필요할 것이며, 초연결 환경에서는 서비스 간의 상호작용이 많아지는 만큼 영향 분석과 관리 체계는 더욱 중요해질 것입니다. 또한, 시장 적기성을 위해 이미 개발된 서비스를 활용하는 경향이 가속화되어 의존성 및 종속성의 관리나 대체 수단 확보가 중요한 과제가 될 것입니다. 끝으로, 많은 기업들이 인공지능을 이용한 업무 자동화를 이미 도입하고 있지만 앞으로 인공지능의 산업 활용도는 더욱 높아질 것입니다. 따라서, 이를 관리하고 검증하는 체계를 마련하는 것이 미래의 디지털 재난 대응에 중요하다고 생각합니다.

Q9. 인공지능을 활용하는 과정에서 디지털 재난·장애가 발생하게 될 경우에 어떤 식으로 대비·대응할 수 있을까요?

A9. 인공지능을 활용하는 과정에서 사람이 판단할 수 있는 부분은 굳이 인공지능에게 맡길 필요가 없다고 생각합니다. 국방 분야를 예로 들면, 미국의 MIL-STD(Military Standard) 802에서는 미사일을 발사하는 버튼은 자동화하지 않고 사람이 판단하여 조작하도록 하고 있습니다. 이와 마찬가지로 디지털 재난·장애도 오롯이 인공지능에 판단을 전가하는 것이 아니라 사람이 개입할 수 있도록 해야 한다고 생각합니다. 또한 인공지능이 잘못 판단하였을 경우 즉각 시스템을 중지할 수 있는 '레드 버튼' 등의 방안을 마련하는 등 여러 부문에서의 접근이 필요합니다.

Q10. 향후 자연재난, 사회재난 등이 증가할 것으로 예상되는데, 이러한 재난 상황에 대비하여 부가통신 사업자가 디지털 재난·장애의 대응·복구를 어떻게 운영해야 한다고 생각하시나요?

A10. 향후 자연재난, 사회재난이 증가할수록 부가통신 사업자가 제공하는 서비스 역시 재난의 영향을 받을 가능성이 높습니다. 따라서 단기적인 임시방편에 그치지 않고, 장기적 관점에서 대응할 수 있는 체계의 마련과 이해관계자들이 이를 내재화할 수 있는 환경 조성이 필요합니다.

디지털 재난도 기존의 일반 재난 산업에서 이야기하는 예방-대비-대응-복구의 틀에서 관리할 수 있다고 생각합니다. 장애가 발생하지 않도록 단일 실패를 방지하는 등 구조적 취약점을 줄이고, 만일의 사태에 대비하여 비상 대응 매뉴얼이나 장애 시 전환이 가능한 대체 서비스의 준비, 주기적인 모의훈련 등이 필요합니다. 실제 장애가 발생한 경우 피해를 최소화하고 서비스 가용성을 유지할 수 있도록 자동 장애 감지 및 신속한 장애 전환, 긴급 패치나 네트워크 우회 등의 즉각적인 임시 조치가 가능해야 하며, 장기적으로 동일 문제가 재발하지 않도록 책임을 전가하거나 비판하지 않는 문화에서 사고 원인을 찾고 보강하는 활동이 이루어져야 합니다.

또한 현재 디지털 재난·장애 관리 의무 대상 사업자(대규모 사업자)들 뿐 아니라 중소 사업자의 디지털 재난·장애 안전관리 수준을 상향 평준화하는 것이 중요한 과제라 할 수 있을 것 같습니다. 아울러 국내의 주요 부가통신 사업자는 자사의 서비스를 단순한 비즈니스로 바라보지 않고 국민 생활과 직결되는 핵심 사회 인프라로 인식하여 이에 걸맞은 책임 의식과 함께 지속적인 관리와 투자를 이어가야 한다고 생각합니다.

04 디지털 안전 관제 이슈

SmartThings

2025.08.01

삼성 SmartThings 앱 전력량 기능 관련 장애

yes24

2025.08.11

yes24(예스24) 랜섬웨어 관련 서비스 장애

X

2025.08.15

X(트위터) 웹 및 앱 게시글 장애 현상 발생

Instagram

2025.08.15

인스타그램 웹/앱 서비스 장애 현상

coupang

2025.08.20 / 2025.08.22

쿠팡 마이페이지 주문목록 관련 장애
쿠팡 장바구니 가격 오류 관련 장애

Samsung Wallet

2025.08.22 / 2025.08.24

삼성월렛-현대카드 관련 결제 오류 장애
삼성월렛-신한카드 관련 결제 오류 장애

N pay

2025.08.25

삼성페이-네이버페이 관련 결제 오류 장애

SK broadband

2025.08.30

SK브로드밴드 경기 포천시 가입자망 서비스 장애

05 Digital Safety Inside

2025 대한민국 안전산업 박람회를 관람하다.

9월 17일(수)부터 19일(금)까지 KINTEX에서 2025 대한민국 안전산업박람회가 개최되었다.
해당 박람회는 대한민국의 선진 안전산업을 선보이는 곳으로, 디지털 안전과 관련된 기술 동향도 살펴볼 수 있었다.

재난안전통신망

재난안전통신망이란 8대 분야 33개 이용 기관이 재난 상황 등 전파에 이용하고 의사소통할 수 있는 전국 단일 무선통신망이다. 기간통신사업자들은 무선통신장치, 위성통신을 이용한 배낭형 소형기지국 등을 활용하여 재난 등 비상상황 발생시에 일원화된 의사소통 체계 안에서 상호 공조 대응할 수 있도록 하고 있다.
특히 저궤도 위성통신(스타링크)가 도입된다면 선박, 산지 등 통신 음영지역을 해소할 수 있을 것으로 기대된다.

05 Digital Safety Inside

2025 대한민국 안전산업 박람회를 관람하다.

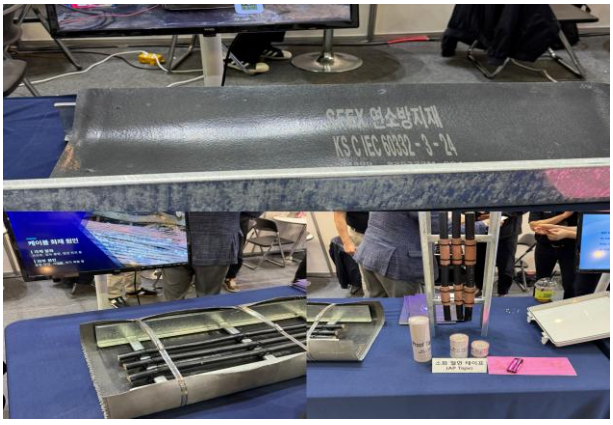
통합 관제 시스템

통합 관제 시스템이란 통신망을 이용하여 특정 정보를 종합적으로 파악할 수 있는 시스템을 일컫는다.
발전된 관제 시스템을 적용하여 재난시 실시간으로 상황을 모니터링하고 교류하여, 빠르게 재난 상황을 대응할 수 있을 것이다.

화재로 인한 통신 재난의 대비

① 케이블

케이블 화재 원인은 자체 발화(과전류, 접속 불량, 절연 파괴 등)나 외부 원인(용접 작업, 가연물, 먼지 폭발 등) 등 그 종류가 다양하다.
케이블 화재는 디지털 장애는 복구 지연·광범위한 서비스 중단 등 심각한 문제를 발생시킨다.
기업들은 화재로 인한 케이블 손상을 최소화 하기 위하여 소화 절연 테이프, 케이블 연소 방지재 등 케이블 보호 관련 제품들을 개발하고 있다.



05 Digital Safety Inside

2025 대한민국 안전산업 박람회를 관람하다.

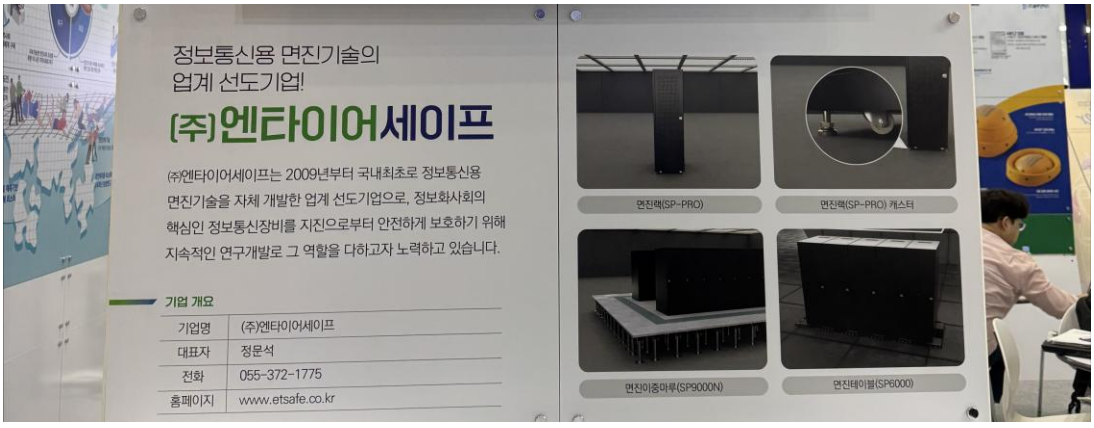
② 배터리

2022년 발생한 SK 판교 데이터센터 화재로 인한 인터넷 서비스 장애 사건과 같이 배터리 보관시설에서의 화재는 디지털 장애 발생 주요 원인 중 하나이다.

화재 확산 방지 시스템을 도입했을 경우 다른 배터리로 화재가 번져 큰 피해로 번지는 것을 막아줄 수 있었다. '배터리 보관시설 화재 확산 방지 솔루션'에서는 화재 발생시 배터리 시설의 천장 부분이 닫혀 화재 확산을 방지해주었다.

'ESS 화재 확산 방지 솔루션'에서는 화재 발생시 랙 사이로 가림막이 올라와 화재가 확산되는 것을 방지해주는 것을 확인할 수 있었다.

지진로 인한 통신 재난의 대비



면진 구조는 수평방향으로 매우 유연한 장치(면진장치)를 사용하여 건물과 지반을 분리함으로써, 지진 에너지가 구조물에 약하게 전달되도록 한다. 지진 발생시에도 방송통신설비를 안전하게 운용할 수 있도록 하여 디지털 재난 및 장애를 예방할 수 있도록 하고 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