CNF

2025.10

글로벌 데이터센터 재난 사례 분석: 화재와 지진 이후의 성공적 복구 전략

본 백서는 전 세계에서 발생했던 다양한 데이터센터 재난 사례를 심층적으로 분석하여, IT 의사결정자들이 재난의 실질적인 위협을 이해하고 효과적인 대응 전략을 수립하는 데 필요한 통찰력을 제공하고자 합니다. 화재, 지진, 그리고 전쟁이라는 각기 다른 유형의 재난이 데이터센터에 어떤 영향을 미쳤는지, 복구 과정에서 어떤 교훈을 얻었는지 상세히 살펴볼 것입니다.

hello@cncf.co.kr

02-469-5426

www.cncf.co.kr

Contents

1 서론: 왜 데이터센터 재난에 주목해야 하는가?

데이터센터는 현대 디지털 경제의 대동맥이자 중추신경계입니다. 클라우드 컴퓨팅, 인공지능(AI), 빅데이터 분석, 사물인터넷(IoT) 등 우리가 누리는 모든 디지털 혁신은 이 물리적인 공간 위에서 작동합니다. 스트리밍 서비스와 소셜 미디어 같은 일상적인 활동부터 금융 거래, 공공 서비스, 국가 안보에 이르기까지, 현대 사회를 구성하는 모든 디지털 서비스는 데이터센터라는 물리적 기반 없이는 존재할 수 없습니다. 이처럼 데이터센터는 더 이상 단순한 서버 보관 시설이 아니라, 사회와 경제의 존립을 좌우하는 '핵심 기반 시설(Critical Infrastructure)'로 자리매김했습니다. 이러한 상황에서 데이터센터의 '중단'은 단순한 서비스 장애를 넘어, 기업의 생존을 위협하고 사회적 혼란을 야기하는 치명적인 '재난'으로 이어질 수 있습니다.

과거에는 데이터센터의 성능을 평가할 때 '가동 시간(Uptime)'이 가장 중요한 척도였습니다. 하지만 이제 IT 의사결정자들은 가동 시간을 넘어 '회복탄력성(Resilience)'이라는 더 넓은 개념에 주목해야 합니다. 회복탄력성은 단순히 장애를 피하는 것을 넘어, 예측 불가능한 재난이 발생했을 때 얼마나 신속하게 핵심 기능을 복구하고 비즈니스를 정상 궤도에 올려놓을 수 있는지를 의미합니다. 화재, 지진, 홍수와 같은 전통적인 재해는 물론, 전쟁, 테러, 공급망 붕괴와 같은 지정학적 리스크까지 고려해야 하는 시대가 도래한 것입니다. 세계경제포럼(WEF)은 데이터센터가 이제 에너지 공급망만큼이나 중요한 국가 안보 자산이 되었으며, 지정학적 긴장의 중심에 놓여 있다고 분석합니다.

데이터센터의 다운타임 비용은 상상을 초월합니다. 2016년 Gartner의 연구에 따르면 데이터센터 다운타임의 평균 비용은 분당 5,600달러에 달했으며, 최근 Ponemon Institute의 보고서에서는 이 수치가 분당 약 9,000달러까지 치솟았다고 분석했습니다. 이는 시간당 수십만 달러에서 수백만 달러의 직접적인 매출 손실을 의미합니다. Uptime Institute에 따르면, 주요 장애의 60% 이상이 10만 달러 이상의 손실을 초래하며, 100만 달러를 넘는 경우도 상당수입니다. 하지만 눈에 보이지 않는 비용은 더욱 심각합니다. 브랜드 신뢰도 하락, 고객 이탈, 데이터 영구 손실, 법적 분쟁 등 비즈니스의 근간을 흔드는 장기적인 피해로 이어질 수 있습니다.

본 백서는 전 세계에서 발생했던 다양한 데이터센터 재난 사례를 심층적으로 분석하여, IT 의사결정자들이 재난의 실질적인 위협을 이해하고 효과적인 대응 전략을 수립하는 데 필요한 통찰력을 제공하고자 합니다. 화재, 지진, 그리고 전쟁이라는 각기 다른 유형의 재난이 데이터센터에 어

떤 영향을 미쳤는지, 복구 과정에서 어떤 교훈을 얻었는지 상세히 살펴볼 것입니다. 이를 통해 독자 여러분은 단순한 기술적 대응을 넘어, 비즈니스 연속성을 확보하고 미래의 위협에 대비하는 견고한 회복탄력성 체계를 구축하는 데 중요한 지침을 얻게 될 것입니다.

2 재난의 유형과 원인 분석

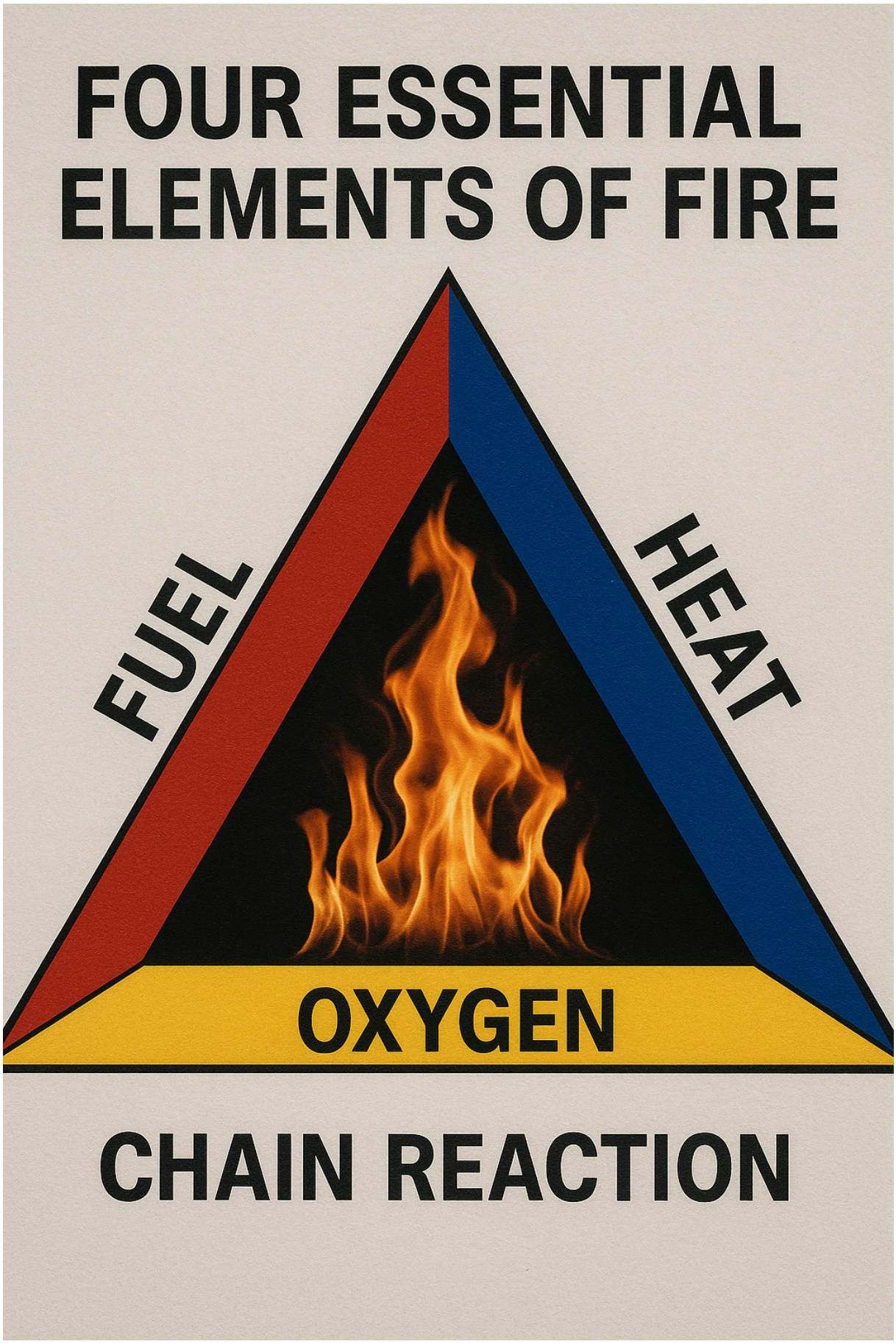
데이터센터를 위협하는 재난은 다양한 형태로 나타나며, 그 원인 또한 복합적입니다. 효과적인 대응 전략을 수립하기 위해서는 먼저 우리가 맞서야 할 적이 누구인지 명확히 알아야 합니다. 데이터센터 재난은 크게 화재, 자연재해, 그리고 인적/지정학적 재난의 세 가지 범주로 나눌 수 있습니다.

2.1 화재: 가장 흔하고 파괴적인 위협

데이터센터 재난 중 가장 빈번하게 발생하며 치명적인 결과를 초래하는 것은 단연 화재입니다. 고밀도의 전력 장비와 복잡한 케이블, 그리고 24시간 가동되는 냉각 시스템은 잠재적인 화재 위험을 항상 내포하고 있습니다. 화재의 발생 원리를 이해하는 것은 예방의 첫걸음입니다. Dgtl Infra의 분석에 따르면, 화재는 '화재의 4요소(Fire Tetrahedron)'로 알려진 연료, 열, 산소, 그리고 연쇄 반응이 충족될 때 발생합니다.

화재 발생의 4가지 필수 요소: 연료, 열, 산소, 연쇄 반응

- 연료(Fuel): 데이터센터는 가연성 물질로 가득 차 있습니다. 서버, 라우터, 스위치 등 IT 장비 자체의 플라스틱 케이스와 인쇄 회로 기판(PCB), 수많은 전력 및 데이터 케이블의 절연 피복, 심지어 장비 포장에 사용되는 종이와 판지 상자까지 모두 잠재적인 연료가 될 수 있습니다.
- 열(Heat): 데이터센터는 IT 장비 운영으로 인해 엄청난 열이 발생하는 공간입니다. 서버 랙의 전력 밀도가 증가하고, '핫 아일(Hot Aisle)'과 같은 공기 흐름 관리 기법이 도입되면서 특정 구역의 온도는 38°C(100°F)를 훌쩍 넘기도 합니다. 이러한 고온 환경은 가연성 물질의 발화점을 낮추는 위험 요소로 작용합니다.
- 산소(Oxygen): 공기 중에 존재하는 산소는 연소를 지속시키는 필수 요소입니다.
- 연쇄 반응(Chain Reaction): 연소 과정에서 발생하는 열이 주변의 다른 가연성 물질을 발화시키고, 이 과정이 연쇄적으로 일어나며 화재가 확산됩니다.



[그림 1] 화재 발생의 4가지 필수 요소: 연료, 열, 산소, 연쇄 반응

이러한 요소들을 바탕으로 데이터센터 화재의 주요 원인은 다음과 같이 구체화됩니다.

2.1.1 전기적 결함 (Electrical Failures)

데이터센터 화재의 가장 흔한 원인으로, 과부하된 회로, 오작동하는 장비, 결함 있는 배선 등이 원인이 됩니다. 특히 '전기 서지(Electrical Surges)'와 '아크 플래시(Arc Flashes)'는 치명적입니다. 전기 서지는 갑작스러운 과전압으로 회로에 과부하를 일으켜 강한 열을 발생시키며, 무정전 전원 장치(UPS)와 같은 장비에 화재를 유발할 수 있습니다. 아크 플래시는 전기 시스템 내에서 발생하는 강력한 방전 현상으로, 주변의 가연성 물질을 즉시 발화시킬 수 있는 고열과 섬광을 동반합니다.

2.1.2 리튬이온 배터리 과열 (Overheating Lithium-ion Batteries)

리튬이온 배터리는 높은 에너지 밀도와 긴 수명 덕분에 데이터센터 UPS 시스템의 주력으로 자리 잡았지만, 동시에 심각한 화재 위험을 안고 있습니다. 배터리가 과열되거나 손상될 경우 '열 폭주(Thermal Runaway)' 현상이 발생할 수 있습니다. 이는 배터리 내부의 온도가 상승하면서 자체적으로 반응을 일으켜 온도를 더욱 급격히 상승시키는 악순환으로, 결국 발화나 폭발로 이어집니다. 한 번 열 폭주가 시작된 배터리 셀은 주변 셀로 화재를 빠르게 전이시켜 대형 화재로 번질 위험이 매우 큽니다. 2020년 15%에 불과했던 리튬이온 배터리의 데이터센터 시장 점유율은 2025년 38.5%에 달할 것으로 예상되어, 관련 위험 관리의 중요성이 더욱 커지고 있습니다.

2.1.3 부적절한 유지보수 (Inadequate Maintenance)

서버, 전원 공급 장치, 냉각 시스템 등에 먼지가 쌓이면 공기 흐름을 방해하여 과열을 유발하거나, 전도성 먼지의 경우 단락(short circuit)을 일으켜 화재의 원인이 될 수 있습니다. 정기적인 청소와 유지보수의 실패는 사소해 보이지만 치명적인 결과를 낳을 수 있습니다.

2.1.4 인적 오류 (Human Error)

Uptime Institute의 2022년 보고서에 따르면, 지난 3년간 발생한 주요 장애의 약 40%가 인적 오류로 인해 발생했으며, 이 중 85%는 정해진 절차를 따르지 않았기 때문입니다. 리튬이온 배터

[그림 2] 침수된 데이터센터

리 설치, HVAC 시스템 유지보수, 케이블 연결 등 중요한 작업 중의 실수는 화재로 이어질 수 있는 조건을 만듭니다. 안전 절차를 무시하거나, 열을 발산하는 장비 주변에 충분한 공간을 확보하지 않는 등의 부주의가 대표적인 예입니다.

2.2 자연재해: 예측 불가능한 위협

자연재해는 인간의 통제를 벗어난 광범위한 파괴를 일으킬 수 있습니다. 데이터센터는 이러한 자연재해로부터 자유로울 수 없으며, 입지 선정 단계부터 설계, 운영에 이르기까지 철저한 대비가 필요합니다.

자연재해로 인한 침수는 데이터센터에 치명적인 피해를 입힐 수 있습니다.

2.2.1 지진 (Earthquakes)

지진은 데이터센터 건물 자체의 구조적 붕괴는 물론, 내부의 서버 랙과 장비 전도, 전력 및 냉각 시스템 파손 등 복합적인 피해를 유발합니다. 지진이 잦은 지역에 위치한 데이터센터는 내진 설계가 필수적입니다. Netzero Events의 분석에 따르면, 건물 전체의 움직임을 흡수하는 '면진(Base Isolation)' 시스템, 서버 랙 자체의 진동을 줄이는 '랙 레벨 아이솔레이터', 그리고 모든 장비를 바닥에 단단히 고정하는 조치 등이 필요합니다. 지진으로 인한 1차 피해뿐만 아니라, 전력망 파괴로

인한 장기 정전, 도로 파괴로 인한 복구 인력 및 연료 보급 차질 등 2차 피해에 대한 대비도 중요합니다.

2.2.2 홍수 및 태풍 (Floods and Hurricanes)

해안가나 저지대에 위치한 데이터센터는 홍수와 태풍에 취약합니다. 침수는 전력 설비와 IT 장비에 직접적인 손상을 입히는 가장 치명적인 위협입니다. 이를 방지하기 위해 데이터센터는 해수면보다 높은 곳에 위치해야 하며, 건물의 바닥을 높게 설계(Raised Floor)하고, 방수벽과 배수 시스템을 갖추어야 합니다. 또한, 태풍으로 인한 강풍은 건물 외벽이나 냉각 장치 등을 파손시킬 수 있으므로, 내풍 설계와 견고한 외부 구조물 설치가 요구됩니다.

2.3 인적 및 지정학적 재난: 새로운 차원의 리스크

기술의 발전과 글로벌화는 데이터센터를 새로운 유형의 위협에 노출시키고 있습니다. 이제 데이터센터의 리스크 관리는 물리적 보안을 넘어 지정학적 변수까지 고려해야 합니다.

2.3.1 전쟁 및 분쟁 (War and Conflict)

최근 우크라이나 전쟁은 데이터센터가 군사 공격의 직접적인 표적이 될 수 있음을 명백히 보여주었습니다. Meritalk의 보도에 따르면, 러시아는 사이버 공격이 기대만큼의 효과를 거두지 못하자 미사일 공격 등을 통해 우크라이나의 데이터센터를 물리적으로 파괴하는 전략으로 전환했습니다. 이는 데이터센터가 단순한 민간 시설이 아니라, 국가의 기능을 마비시키기 위한 핵심 공격 목표가 될 수 있음을 시사합니다. 이러한 위협에 대응하기 위해, 국가의 중요 데이터와 시스템을 국경 밖의 안전한 지역에 위치한 글로벌 클라우드 서비스로 이전하는 '데이터 피난(Data Evacuation)' 전략이 현실적인 대안으로 떠오르고 있습니다.

2.3.2 사이버 공격 (Cyber Attacks)

랜섬웨어와 같은 사이버 공격은 물리적 파괴 없이도 데이터센터의 기능을 완전히 마비시킬 수 있는 심각한 재난입니다. 공격자들은 시스템을 암호화하여 접근을 차단하고 막대한 금전을 요구하며, 이로 인한 서비스 중단은 화재나 정전만큼이나 큰 비즈니스 손실을 유발합니다. AFCOM의

2023년 보고서에 따르면, 2022년 전 세계 조직의 3분의 2가 사이버 공격을 경험했으며, 이로 인해 평균 5일간 비즈니스가 중단되었습니다. 이는 강력한 사이버 보안 체계와 함께, 공격을 당했을 때를 대비한 데이터 백업 및 복구 계획이 필수적임을 보여줍니다.

2.3.3 공급망 문제 (Supply Chain Issues)

세계경제포럼(WEF)에서 지적하듯, 미중 기술 패권 경쟁과 같은 지정학적 갈등은 데이터센터의 핵심 부품 공급망에 직접적인 영향을 미칩니다. 특정 국가의 고성능 반도체나 네트워크 장비에 대한 수출 통제는 데이터센터의 구축 및 확장을 지연시키거나 불가능하게 만들 수 있습니다. 이는 데이터센터 운영이 더 이상 기술과 자본의 문제를 넘어, 국제 정치와 무역 환경에 깊이 연관되어 있음을 의미하며, 핵심 부품의 공급망 다변화와 같은 전략적 고려가 필요함을 시사합니다.

3 세계 데이터센터 재난– 화재 사고 사례

이론적인 위험 분석을 넘어, 실제 재난 사례를 살펴보는 것은 위협의 심각성을 체감하고 실질적인 교훈을 얻는 가장 효과적인 방법입니다. 본 섹션에서는 전 세계에서 발생한 주요 데이터센터 재난 사례를 화재, 지진, 전쟁의 유형별로 나누어 상세히 분석합니다. 각 사례는 사건의 개요, 원인, 피해 규모, 대응 과정, 그리고 IT 의사결정자를 위한 시사점 순으로 서술하여 가독성과 이해도를 높였습니다.

데이터센터 화재는 가장 빈번하게 발생하는 재난 유형으로, 전기적 결함, 배터리 문제 등 다양한 원인으로 인해 발생하며 막대한 피해를 남깁니다. 다음은 대표적인 화재 사고 사례들입니다.

3.1 카와자 타워 데이터센터 화재 (2023년 10월, 방글라데시 다카)

3.1.1 사건 개요

2023년 10월, 방글라데시 다카의 상업용 건물인 카와자 타워에서 대형 화재가 발생했습니다. 14층 건물 중 12층과 13층에서 시작된 이 화재는 해당 건물에 입주해 있던 NRB 텔레콤과 다카콜로(Dhakacolo)의 주요 데이터센터 2곳에 직접적인 영향을 미쳤습니다. 이 데이터센터들은 여러 인터넷 게이트웨이와 교환기에 연결되어 수백 개의 인터넷 서비스 제공업체(ISP)에 서비스를 제공하

는 핵심 시설이었습니다.

3.1.2 원인 분석

공식적인 화재 원인은 발표되지 않았습니다. 하지만 건물 내에 다량의 가연성 물질이 존재했고, 일부 소화기가 비치되어 있었음에도 불구하고 건물 전체에 대한 종합적인 화재 안전 계획이 부재했던 점이 초기 화재를 대형 재난으로 키운 주요 원인으로 분석됩니다.

3.1.3 영향 및 피해

이 화재로 3명이 사망하고 최소 10명이 부상하는 등 심각한 인명 피해가 발생했습니다. 또한, 방글라데시의 1,210만 광대역 사용자 중 약 40%가 인터넷 중단을 겪었으며, 1억 2,000만 모바일 인터넷 가입자 중 약 20%가 데이터 및 음성 서비스 장애를 경험하는 등 국가적인 통신 대란으로 이어졌습니다.

3.1.4 대응 및 복구 과정

화재는 15시간 이상 지속된 후에야 진압되었습니다. 일부 장비는 전소되었고, 다른 장비는 비교적 온전했지만 화재로 인한 케이블 손상과 안전을 위한 전력 차단 조치로 인해 서비스 복구에 상당한 차질이 빚어졌습니다.

3.1.5 시사점 및 교훈

이 사례는 데이터센터가 입주한 건물 자체의 안전 관리 부실이 어떻게 막대한 인명 피해와 국가적 규모의 통신 대란으로 이어질 수 있는지 보여줍니다. IT 의사결정자는 코로케이션 서비스 선택 시, 데이터센터 내부의 인프라뿐만 아니라 건물의 소방 안전 시스템, 대피 계획, 가연성 물질 관리 상태 등을 비즈니스 연속성의 핵심 요소로 평가하고 검증해야 합니다.

출처: Dgtl Infra

3.2 윈드스트림 데이터센터 화재 (2023년 9월, 미국 링컨)

3.2.1 사건 개요

2023년 9월, 미국 네브래스카주 링컨 시내에 위치한 통신사 윈드스트림(Windstream)의 데이터센터에서 화재가 발생했습니다. 이 사고로 약 20만 달러의 재산 피해가 발생했으며, 여러 카운티의 911 긴급 전화 서비스가 몇 시간 동안 중단되는 심각한 결과를 초래했습니다.

3.2.2 원인 분석

화재는 전기 제어실의 누수로 인해 시작되었습니다. 누수가 전기 장비에 영향을 미치면서 작은 폭발을 일으켰고, 이로 인해 변압기가 단락되어 건물 내 3개 스위치의 전원이 차단되었습니다. 현장의 비상 발전기가 잠시 전력을 복구했지만, 이마저도 오작동하면서 데이터센터는 배터리 백업에 의존해야 하는 상황에 처했습니다.

3.2.3 영향 및 피해

가장 심각한 피해는 공공 안전 서비스의 마비였습니다. 네브래스카주 남동부의 애덤스, 게이지, 오토, 손더스 카운티 등 여러 지역의 911 연결이 몇 시간 동안 두절되었습니다. 다행히 인명 피해는 보고되지 않았습니다.

3.2.4 대응 및 복구 과정

소방관들은 건식 화학물질과 이산화탄소 소화기를 사용하여 화재를 진압했습니다. 윈드스트림 기술팀은 전력 문제 해결을 위해 3개의 스위치 중 하나를 차단해야 했고, 이로 인해 911 서비스가 영향을 받았습니다.

3.2.5 시사점 및 교훈

이 사건은 전기실과 같은 핵심 기반 시설의 사소한 누수가 어떻게 연쇄적인 시스템 장애로 이어질 수 있는지 보여줍니다. 특히 주 전원, 비상 발전기, 배터리 백업 시스템이 연달아 문제를 일으키는 '계단식 장애(Cascading Failure)'의 위험성을 경고합니다. IT 의사결정자는 핵심 설비에 대한 환경 모니터링(누수, 온도, 습도)을 강화하고, 백업 시스템이 독립적으로 작동하고 정기적으로 테스트되는지 확인해야 합니다.

출처: Dgtl Infra

3.3 프록시무스 데이터센터 화재 (2023년 8월, 벨기에 브뤼셀)

3.3.1 사건 개요

2023년 8월, 벨기에 최대 통신사인 프록시무스(Proximus)가 운영하는 브뤼셀의 넷센터 에베레(Netcenter Evere) 데이터센터에서 화재가 발생했습니다. 이로 인해 벨기에의 긴급 전화 서비스가 일시적으로 중단되었습니다.

3.3.2 원인 분석

화재의 구체적인 원인은 프록시무스에서 조사를 진행 중이며, 공식적으로 발표되지 않았습니다.

3.3.3 영향 및 피해

화재로 인해 소방 및 구급차(112), 경찰(101) 등 긴급 전화 서비스가 30분 미만 동안 중단되는 사고가 발생했습니다. 국가 핵심 인프라의 일시적 마비라는 점에서 사회적 중요성이 큰 사건이었습니다.

3.3.4 대응 및 복구 과정

소방 당국은 90분 이내에 화재를 통제했으며, 이후 데이터센터는 정상 운영을 재개했습니다. 신속한 대응 덕분에 서비스 중단 시간을 최소화할 수 있었습니다.

3.3.5 시사점 및 교훈

원인이 밝혀지지 않았음에도 불구하고, 이 사례는 911과 같은 사회 필수 서비스가 단일 데이터센터의 장애에 얼마나 취약할 수 있는지를 보여줍니다. 이러한 핵심 서비스를 호스팅하는 데이터센터는 최고 수준의 이중화 및 재해 복구 체계를 갖추어야 하며, 신속한 초기 대응이 서비스 중단 시간을 최소화하는 데 결정적이라는 교훈을 줍니다.

출처: Dgtl Infra

3.4 디지털 리얼티 데이터센터 화재 (2023년 5월, 미국 로스앤젤레스)

3.4.1 사건 개요

2023년 5월, 세계 최대 데이터센터 제공업체 중 하나인 디지털 리얼티(Digital Realty)의 로스앤젤레스 LAX12 시설에서 화재가 발생했습니다. 이 화재로 인해 시설 내 2개의 스위트가 폐쇄되고, 입주 고객사의 서버가 상당수 손상되었습니다.

3.4.2 원인 분석

화재는 특정 랙에서 시작되었으나, 정확한 원인은 조사가 진행 중으로 아직 밝혀지지 않았습니다.

3.4.3 영향 및 피해

화재로 인해 코로케이션 공간의 스프링클러 시스템이 작동하면서 많은 서버가 물에 잠기는 2차 피해가 발생했습니다. 특히, 해당 시설을 이용하던 매니지드 서비스 제공업체 이보커티브(Evocative)가 심각한 수해를 입었습니다. 2개의 스위트 중 하나는 몇 시간 만에 복구되었지만, 다른 하나는 며칠 동안 폐쇄되었습니다.

3.4.4 대응 및 복구 과정

화재 자체는 진압되었으나, 스프링클러 작동으로 인한 수해 복구에 더 많은 시간이 소요되었습니다. 디지털 리얼티는 고객사의 피해 복구를 지원하고, 영향을 받은 스위트를 단계적으로 정상화했습니다.

3.4.5 시사점 및 교훈

이 사례는 화재 진압 시스템으로 인한 2차 피해의 심각성을 명확히 보여줍니다. 전통적인 습식 스프링클러는 화재를 효과적으로 진압할 수 있지만, IT 장비에 치명적인 손상을 입힐 수 있습니다. IT 의사결정자는 데이터센터 선택 시, 물을 사용하지 않는 청정 소화 약제 시스템이나 워터 미스트 시스템과 같이 IT 장비에 미치는 피해를 최소화하는 화재 진압 설비를 갖추었는지 확인해야 합니다.

출처: Dgtl Infra

3.5 글로벌 스위치 데이터센터 화재 (2023년 4월, 프랑스 파리)

3.5.1 사건 개요

2023년 4월, 유럽 및 아시아태평양 지역의 주요 데이터센터 운영사인 글로벌 스위치(Global Switch)의 파리 캠퍼스에서 화재가 발생했습니다. 이 사고로 인해 해당 데이터센터에 입주해 있던 구글 클라우드의 'europe-west-9' 리전이 심각한 데이터 손실을 겪었습니다.

3.5.2 원인 분석

화재는 냉각 시스템의 워터 펌프 고장으로 인한 누수에서 시작되었습니다. 누수된 물이 배터리실로 흘러 들어가 배터리 부품과 접촉하면서 화재를 일으켰습니다. 이는 냉각수 시스템의 문제가 어떻게 화재로 이어질 수 있는지를 보여주는 대표적인 사례입니다.

3.5.3 영향 및 피해

화재 자체는 배터리실에 국한되었지만, 이로 인해 구글 클라우드 'europe-west-9' 리전의 인프라 장애가 발생하여 여러 구글 클라우드 서비스가 영향을 받았습니다. 특히 'europe-west9-a' 존의 일부가 침수되었고, 이후 화재로 인해 'europe-west9-a' 존 전체와 'europe-west9-c' 존의 일부가 예방 차원에서 전원이 차단되면서 상당한 데이터 손실이 발생했습니다.

3.5.4 대응 및 복구 과정

화재 진압 후, 구글 클라우드는 영향을 받은 존의 전원을 차단하고 인프라 복구 작업을 진행했습니다. 하지만 일부 고객 데이터는 영구적으로 손실되어 복구가 불가능했습니다.

3.5.5 시사점 및 교훈

이 사건은 데이터센터 내에서 물과 전기가 만나는 지점, 특히 배터리실과 같은 민감한 구역의 위험성을 강조합니다. 냉각수 배관과 전기 설비의 경로를 물리적으로 분리하고, 누수 감지 시스템을 배터리실을 포함한 모든 중요 구역에 설치해야 합니다. 또한, 클라우드 서비스 이용자라 할지라도 단일 리전(Region) 또는 단일 가용 영역(Availability Zone)의 장애에 대비하여, 여러 리전에 걸

쳐 데이터를 백업하고 서비스를 분산하는 '다중 리전(Multi-region)' 전략을 수립하는 것이 중요함을 시사합니다.

출처: Dgtl Infra

3.6 Maxnod 데이터센터 화재 (2023년 3월, 프랑스 앵)

3.6.1 사건 개요

2023년 3월, 프랑스 앵(Ain) 지역에 위치한 Maxnod 데이터센터에서 화재가 발생하여 건물이 완전히 파괴되는 사고가 있었습니다. 800제곱미터(약 242평) 규모의 이 시설은 화재로 인해 건물 전체를 재건축해야 할 정도로 심각한 피해를 입었으며, 내부의 모든 IT 장비가 전소되었습니다.

3.6.2 원인 분석

화재 원인은 시설의 태양광 패널과 연계된 배터리실에서 시작된 것으로 추정됩니다. 특히, 에너지 저장 시스템(ESS)으로 사용되던 리튬이온 배터리가 발화의 원인으로 지목되었습니다. 이는 신재생에너지와 연계된 데이터센터가 새로운 화재 위험에 노출될 수 있음을 보여주는 사례입니다.

3.6.3 영향 및 피해

데이터센터 건물이 전소되고 모든 장비가 파괴되어 복구가 불가능한 상태가 되었습니다. 또한, 화재로 인해 데이터센터의 광섬유 케이블이 심각하게 손상되면서, 지역의 FTTH(Fiber-to-the-Home) 인터넷 서비스가 중단되는 등 지역 사회에도 영향을 미쳤습니다. 진화 과정에서 소방관 1명이 경상을 입기도 했습니다.

3.6.4 대응 및 복구 과정

건물과 장비가 전소되었기 때문에 복구는 불가능했으며, 완전한 재건축이 필요하게 되었습니다.

3.6.5 시사점 및 교훈

Maxnod 사례는 신재생에너지 도입에 따른 새로운 리스크를 부각시킵니다. 태양광 등 신재생에너지와 연계된 대용량 리튬이온 배터리 ESS는 그 자체로 높은 화재 위험을 가집니다. IT 의사결정자는 ESG 경영의 일환으로 신재생에너지를 도입할 때, 관련 에너지 저장 시스템을 데이터센터의 핵심 IT 공간과 물리적으로 완벽히 분리된 별도의 공간에 설치하고, 전용 화재 감지 및 소화 시스템을 구축하는 등 최고 수준의 안전 조치를 병행해야 합니다.

출처: Dgtl Infra

3.7 사이엑스트라 데이터센터 화재 (2023년 2월, 미국 보스턴)

3.7.1 사건 개요

2023년 2월, 리테일 코로케이션 제공업체인 사이엑스트라 (Cyxtera Technologies)의 보스턴 BOS1 캠퍼스에서 전기 아크 플래시로 인한 폭발 및 화재 사고가 발생했습니다. 이 사고로 데이터센터 운영이 몇 시간 동안 중단되고, 입주 고객사가 데이터 손실을 겪었습니다.

3.7.2 원인 분석

사고는 데이터센터의 전력실에서 발생한 '아크 플래시(Arc Flash)'가 원인이었습니다. 아크 플래시는 전기 장비 내에서 발생하는 강력한 방전 현상으로, 이로 인한 폭발이 배터리 캐비닛을 파괴했습니다. 폭발의 위력은 배터리 캐비닛의 문을 날려버릴 정도였습니다.

3.7.3 영향 및 피해

건물 구조 자체는 손상되지 않았지만, 폭발과 연기로 인해 소방 당국은 안전을 위해 현장의 전력 공급을 차단하고 건물을 대피시켰습니다. 이 예기치 않은 전력 차단으로 인해 사이엑스트라의 고객사인 오라클의 넷스위트(NetSuite) 서비스에서 약 30분의 데이터가 손실되는 피해가 발생했습니다.

3.7.4 대응 및 복구 과정

소방 당국의 안전 조치에 따라 전력이 차단되었으며, 안전이 확보된 후에야 전력 복구 및 서비스 정상화가 진행되었습니다.

3.7.5 시사점 및 교훈

이 사례는 아크 플래시와 같은 전기 사고의 폭발적인 위험성을 보여줍니다. 또한, 화재 진압이나 안전 확보를 위해 소방 당국이 내리는 강제적인 전력 차단 조치가 예기치 않은 데이터 손실로 이어질 수 있음을 시사합니다. IT 시스템은 갑작스러운 전원 차단(Power-off) 상황에서도 데이터 정합성을 유지할 수 있도록 설계되어야 하며, 이를 위한 저널링, 데이터베이스 복구 기능 등을 철저히 검증해야 합니다.

출처: Dgtl Infra

3.8 QTS 데이터센터 화재 (2022년 11월, 미국 피스카타웨이)

3.8.1 사건 개요

2022년 11월, QTS 데이터센터의 뉴저지주 피스카타웨이 시설에서 화재가 발생했습니다. 특이하게도 이 화재는 운영 중인 데이터센터 내부가 아닌, 당시 건설 중이던 데이터센터 증축 건물의 옥상에서 발생했습니다.

3.8.2 원인 분석

화재는 향후 설치를 위해 옥상에 보관 중이던 여러 팔레트의 지붕 자재에 불이 붙으면서 시작되었습니다. 건설 현장의 자재 관리가 화재로 이어진 경우입니다.

3.8.3 영향 및 피해

화재는 약 2시간 만에 진압되었습니다. 중요한 점은 화재가 건설 중인 건물에 국한되었고, 운영 중인 데이터센터의 장비나 고객 서비스에는 아무런 영향을 미치지 않았다는 것입니다. 부상자도 보고되지 않았습니다.

3.8.4 대응 및 복구 과정

소방 당국이 신속하게 출동하여 약 2시간 만에 화재를 완전히 진압했습니다.

3.8.5 시사점 및 교훈

이 사례는 데이터센터 증축 또는 건설 현장에서 발생하는 화재가 운영 중인 시설에 영향을 미치지 않도록 물리적으로 완벽하게 분리하는 것이 얼마나 중요한지를 보여줍니다. IT 의사결정자는 데이터센터 제공업체가 확장 공사를 진행할 경우, 기존 운영 환경의 안정성을 보장하기 위한 명확한 구획 분리, 안전 관리 계획, 비상 대응 절차를 갖추고 있는지 반드시 확인해야 합니다.

출처: Dgtl Infra

3.9 컴캐스트 데이터센터 화재 (2022년 11월, 미국 센테니얼)

3.9.1 사건 개요

2022년 11월, 컴캐스트(Comcast)의 콜로라도주 센테니얼 데이터센터에서 화재가 발생하여 몇 시간 동안 서비스가 중단되었습니다.

3.9.2 원인 분석

화재는 발전기실에서 시작되었으며, 구체적인 원인은 보고되지 않았습니다. 하지만 화재가 발전기실 내부에 국한되어 주 데이터센터 건물로 확산되는 것을 막았습니다.

3.9.3 영향 및 피해

서비스 중단은 주로 컴캐스트의 내부 애플리케이션에 영향을 미쳤습니다. 화재가 특정 구역에 한정되었기 때문에 데이터센터의 광범위한 손상은 피할 수 있었습니다. 인명 피해는 없었습니다.

3.9.4 대응 및 복구 과정

화재가 발전기실 내에서 통제되면서, 소방 당국은 주 데이터 홀의 피해 없이 화재를 진압할 수 있었습니다.

3.9.5 시사점 및 교훈

발전기실, 배터리실, 전기실 등 화재 위험이 높은 구역을 데이터 홀과 같은 핵심 IT 공간과 방화벽 등으로 완벽하게 구획화(Compartmentalization)하는 것이 매우 중요함을 보여줍니다. 구획화는 화재 발생 시 피해를 해당 구역으로 한정시켜 데이터센터 전체의 마비를 막는 핵심적인 방화 전략입니다.

출처: Dgtl Infra

3.10 SK C&C 판교 데이터센터 화재 (2022년 10월, 대한민국 성남)

3.10.1 사건 개요

2022년 10월 15일, 경기도 성남시 판교에 위치한 SK C&;C 데이터센터에서 화재가 발생했습니다. 이 화재로 인해 데이터센터의 전력 공급이 중단되면서, 이곳에 입주해 있던 카카오, 네이버 등 주요 IT 기업들의 서비스가 장시간 마비되는 '전국민적 IT 재난'이 발생했습니다.

3.10.2 원인 분석

화재는 건물 지하 3층에 위치한 배터리실에서 시작되었습니다. 국립과학수사연구원의 조사 결과, 리튬이온 배터리 랙 중 하나에서 내부 발화가 시작되어 주변으로 번진 것으로 확인되었습니다. 구체적인 발화 원인은 명확히 규명되지 않았으나, 배터리 자체의 결함이나 관리 시스템의 문제일 가능성이 제기되었습니다.

3.10.3 영향 및 피해

이 화재로 데이터센터 전체의 전력 공급이 차단되면서, 카카오의 핵심 서비스인 카카오톡을 비롯해 카카오페이, 카카오T, 다음(Daum) 포털 등 대부분의 서비스가 최장 127시간 30분 동안 중단되었습니다. '국민 메신저'의 마비는 단순한 불편을 넘어 사회·경제 활동 전반에 큰 혼란을 야기했습니다. 네이버 역시 일부 서비스에서 장애를 겪었으나, 카카오에 비해 상대적으로 신속하게 복구되었습니다. 이 사건은 특정 데이터센터의 장애가 국가 전체의 디지털 인프라를 마비시킬 수 있음을 보여주었습니다.

3.10.4 대응 및 복구 과정

화재 발생 후 안전을 위해 데이터센터 전체의 전원을 차단하는 조치가 내려졌습니다. 이는 화재 확산을 막기 위한 불가피한 선택이었지만, 결과적으로 서비스 중단을 장기화시키는 원인이 되었습니다. 카카오는 다른 데이터센터에 분산된 자원을 활용해 복구를 시도했으나, 핵심 시스템이 판교 데이터센터에 집중되어 있어 복구에 상당한 시간이 소요되었습니다. 반면, 네이버는 자체 데이터센터 간 이중화(Redundancy)가 비교적 잘 되어 있어 상대적으로 빠른 복구가 가능했습니다.

3.10.5 시사점 및 교훈

판교 데이터센터 화재는 국내 IT 업계에 재해 복구 시스템의 중요성을 다시 한번 각인시킨 중대한 사건입니다.

- 서비스 이중화의 중요성: 네이버와 카카오의 복구 속도 차이는 데이터 및 서비스 이중화 수준의 차이에서 비롯되었습니다. 핵심 서비스와 데이터는 반드시 여러 데이터센터에 걸쳐 실시간으로 복제되고, 장애 발생 시 자동으로 트래픽이 전환되는 'Active-Active' 또는 'Active-Standby' 구조를 갖추어야 합니다.
- 전원 공급 이원화: 화재로 인해 주 전원뿐만 아니라 예비 전원까지 모두 차단되는 상황에 대한 대비가 부족했습니다. 전력 공급 경로와 배터리실 등을 물리적으로 완벽하게 분리하고, 다양한 시나리오에 대비한 전력 복구 계획이 필요합니다.
- IT 의사결정자의 책임: 이 사건 이후, 재해 복구는 더 이상 기술팀만의 문제가 아닌, CEO와 이사회가 직접 챙겨야 할 핵심 경영 과제로 부상했습니다. 재해 복구에 대한 투자는 비용이 아닌, 비즈니스 생존을 위한 필수 투자라는 인식이 확산되었습니다.

출처: Dgtl Infra

3.11 구글 데이터센터 폭발 사고 (2022년 8월, 미국 카운실 블러프)

3.11.1 사건 개요

2022년 8월, 아이오와주 카운실 블러프에 위치한 구글 데이터센터 인근 변전소에서 '아크 플래시'로 인한 전기 폭발 사고가 발생했습니다. 이 사고로 현장에서 작업 중이던 전기 기술자 3명이

[그림 3] 구글 카운실 블러프 데이터센터 전경

심각한 화상을 입었습니다.

구글 카운실 블러프 데이터센터 전경

3.11.2 원인 분석

사고는 내부 오류로 인한 아크 플래시로 확인되었습니다. 아크 플래시는 기술적으로 화재는 아니지만, 수천 도에 달하는 엄청난 열을 발생시켜 주변 물질을 발화시키고 화재로 이어질 수 있는 매우 위험한 현상입니다.

3.11.3 영향 및 피해

이 사고로 인해 작업자 3명이 중상을 입고 병원으로 이송되는 등 심각한 인명 피해가 발생했습니다. 구글 서비스에 미친 영향은 구체적으로 알려지지 않았으나, 데이터센터 운영에 있어 인명 안전이 최우선 과제임을 상기시키는 사건이었습니다.

3.11.4 대응 및 복구 과정

사고 발생 즉시 부상자들은 병원으로 이송되었으며, 현장은 안전 조치 후 복구 작업이 진행되었습니다.

3.11.5 시사점 및 교훈

데이터센터 재난 대응은 서비스 연속성뿐만 아니라 인명 안전을 최우선으로 고려해야 합니다. 특히 고전압 장비를 다루는 전력실이나 변전소에서는 아크 플래시의 위험성을 항상 인지하고, 작업자들을 위한 최고 수준의 안전 장비(방호복, 헬멧 등)와 엄격한 안전 절차를 마련해야 합니다. IT 의사결정자는 협력업체 선정 시에도 이러한 안전 관리 역량을 중요한 평가 기준으로 삼아야 합니다.

출처: Dgtl Infra

3.12 에퀴닉스 데이터센터 화재 (2022년 1월, 스페인 마드리드)

3.12.1 사건 개요

2022년 1월, 세계 최대 데이터센터 제공업체인 에퀴닉스(Equinix)의 마드리드 MD2 데이터센터에서 화재가 발생하여 전력 공급이 잠시 중단되었습니다.

3.12.2 원인 분석

화재는 데이터센터의 변압기가 위치한 지하 공간에서 시작된 것으로 보고되었습니다. 이로 인해 전력실에 연기가 축적되고, 연기가 시설의 차고 공간까지 확산되었습니다.

3.12.3 영향 및 피해

화재로 인해 전력 공급이 잠시 중단되었으나, 건물 구조 자체에는 큰 피해가 없었고 정상 운영이 곧 재개되었습니다. 인명 피해는 보고되지 않았습니다.

3.12.4 대응 및 복구 과정

소방 당국이 신속하게 화재를 진압했으며, 연기 배출 후 안전 점검을 거쳐 운영이 정상화되었습니다.

3.12.5 시사점 및 교훈

변압기, 발전기 등 전력 인프라가 위치한 공간은 화재 발생 시 연기 확산으로 인한 2차 피해를 유발할 수 있습니다. 이러한 공간은 IT 장비가 있는 데이터 홀과 완벽하게 분리되어야 하며, 연기 감지 및 자동 배연 시스템을 갖추어 연기 확산을 초기에 차단하는 것이 중요합니다.

출처: Dgtl Infra

3.13 사이버 데이터센터 화재 (2021년 12월, 인도네시아 자카르타)

3.13.1 사건 개요

2021년 12월, 인도네시아 자카르타의 사이버 빌딩 1(Cyber Building 1) 2층에 위치한 사이버 데이터센터 인터내셔널(CDCI)에서 대형 화재가 발생했습니다. 이 사고로 2명이 사망하고 인도네시아의 여러 디지털 서비스가 마비되었습니다.

3.13.2 원인 분석

화재는 특정 서버의 폭발로 인해 시작된 것으로 보고되었으며, 단락(short circuit)이 원인으로 의심되었습니다. 이로 인해 건물 내외부에 상당한 물리적 손상이 발생했습니다.

3.13.3 영향 및 피해

가장 비극적인 결과는 연기 흡입으로 인해 2명이 사망한 것입니다. 또한, 이 시설을 이용하던 증권사, 디지털 결제, 호스팅 서비스, 게임 포털, ISP, 뉴스 사이트, 정부 서비스 등 인도네시아의 다양한 서비스가 광범위하게 중단되어 디지털 생태계 전반에 큰 영향을 미쳤습니다.

3.13.4 대응 및 복구 과정

화재 진압 후, 입주 기업들은 서비스를 복구하기 위해 노력했으나, 데이터센터의 물리적 손상이 심각하여 복구에 어려움을 겪었습니다.

3.13.5 시사점 및 교훈

이 사례는 데이터센터 화재가 심각한 인명 피해로 이어질 수 있음을 경고합니다. 특히 밀폐된 공간에서 발생하는 유독 가스는 매우 치명적입니다. 데이터센터는 신속한 대피를 위한 명확한 경로와 비상 조명, 그리고 유독 가스를 차단하고 배출할 수 있는 공조 시스템을 갖추어야 합니다. 또한, 단일 서버의 단락이 건물 전체의 화재로 번질 수 있으므로, 랙 단위의 과전류 차단 및 화재 감지/진압 시스템의 중요성이 부각됩니다.

출처: Dgtl Infra

3.14 웹NX 데이터센터 화재 (2021년 4월, 미국 오그던)

3.14.1 사건 개요

2021년 4월, 유타주 오그던에 위치한 웹NX(WebNX) 데이터센터에서 비상 발전기 고장으로 인한 화재가 발생하여 장시간의 서비스 중단을 초래했습니다.

3.14.2 원인 분석

사고는 도시 전체의 정전으로 인해 데이터센터의 비상 발전기가 자동으로 가동되면서 발생했습니다. 불행히도, 가동된 발전기 중 하나가 오작동하여 화재를 일으켰고, 이로 인해 데이터센터의 화재 진압 프로토콜이 작동되었습니다.

3.14.3 영향 및 피해

화재로 인해 출동한 소방 당국은 안전을 위해 시설 전체의 전력을 차단했습니다. 이로 인해 데이터센터가 완전히 셧다운되어 오그던 시를 포함한 고객사들이 장시간 서비스 중단을 겪었습니다. 화

재가 고객 서버에 직접적인 피해를 주지는 않았지만, 소방관들이 발전기 화재를 진압하는 과정에서 일부 서버가 물에 의한 2차 피해를 입었습니다.

3.14.4 대응 및 복구 과정

소방 당국이 발전기 화재를 진압하는 동안, 시설 전체의 전력은 차단된 상태를 유지했습니다. 화재 진압 및 안전 점검이 완료된 후에야 전력 복구 및 서비스 정상화가 진행될 수 있었습니다.

3.14.5 시사점 및 교훈

비즈니스 연속성을 위한 핵심 설비인 비상 발전기가 오히려 재난의 원인이 될 수 있다는 역설적인 상황을 보여줍니다. 발전기를 포함한 모든 백업 시스템은 정기적인 테스트와 철저한 유지보수를 통해 실제 비상 상황에서 안정적으로 작동할 수 있도록 관리되어야 합니다. 또한, 발전기실 화재 진압 과정에서 발생하는 물 피해가 IT 장비에 영향을 미치지 않도록, 발전기실과 데이터 홀 사이의 배수 및 방수 처리가 중요합니다.

출처: Dgtl Infra

3.15 OVHcloud 데이터센터 전소 사고 (2021년 3월, 프랑스 스트라스부르)

3.15.1 사건 개요

2021년 3월, 유럽 최대 클라우드 서비스 제공업체 중 하나인 OVHcloud의 프랑스 스트라스부르 캠퍼스에서 대형 화재가 발생했습니다. 이 화재로 5층 규모의 SBG2 데이터센터가 완전히 전소되었고, 인접한 SBG1 데이터센터의 일부가 파손되었습니다. 전소된 SBG2에는 약 3만 대의 서버가 있었으며, 이 사고로 인해 전 세계 약 6만 5천여 고객이 심각한 서비스 중단과 영구적인 데이터 손실을 겪었습니다.

3.15.2 원인 분석

초기 조사 결과, 화재는 SBG2 데이터센터의 무정전 전원 장치(UPS)실에서 시작된 것으로 밝혀졌습니다. 구체적으로는 UPS 시스템에 사용된 리튬이온 배터리와 인버터의 결함이 화재를 일으킨 것으로 지목되었습니다. 화재는 자동 소화 설비의 부재, 전력 차단의 지연, 그리고 화재 확산을 용이하게 한 건물 구조(목재 천장, 굴뚝 역할을 한 내부 안뜰 등) 때문에 걷잡을 수 없이 번졌습니다.

3.15.3 영향 및 피해

피해는 막대했습니다. SBG2 건물이 완전히 파괴되면서 내부에 있던 모든 서버와 데이터가 소실되었고, 백업 데이터마저 동일한 건물에 보관했던 일부 고객들은 데이터를 영구적으로 잃었습니다. 이 사고로 OVHcloud는 약 1억 5백만 유로(약 1,400억 원) 이상의 직접적인 재정 손실을 입었으며, 수많은 고객사의 비즈니스가 중단되는 등 파급 효과가 엄청났습니다. 프랑스 정부 웹사이트, 온라인 게임 '러스트(Rust)' 등 다수의 유명 서비스가 장시간 마비되었습니다.

3.15.4 대응 및 복구 과정

화재 발생 직후 소방 당국은 캠퍼스 전체의 전력을 차단하고 진화 작업을 벌였으나, 이미 불길이 거세져 SBG2를 구하는 데는 실패했습니다. OVHcloud는 피해를 입지 않은 다른 데이터센터로 트래픽을 이전하고, 고객들에게 대체 서버를 제공하는 등 복구에 총력을 기울였습니다. 하지만 데이터가 영구 손실된 고객들에게는 실질적인 복구가 불가능했습니다.

3.15.5 시사점 및 교훈

OVHcloud 사고는 현대 데이터센터가 직면한 리스크를 집약적으로 보여주는 교과서적인 사례입니다.

- 리튬이온 배터리 리스크: UPS용 리튬이온 배터리가 심각한 화재 위험원임을 명백히 보여주었습니다. 배터리실은 다른 공간과 물리적으로 완벽히 분리하고, 전용 자동 소화 설비를 갖추는 것이 필수적입니다.

- 재해 복구(DR) 전략의 중요성: 백업 데이터를 원본과 동일한 물리적 위치에 보관하는 것이 얼마나 위험한지를 증명했습니다. 진정한 재해 복구를 위해서는 지리적으로 분산된 위치에 백업 데이터를 보관(Geo-redundancy)하는 전략이 반드시 필요합니다.
- 설계의 중요성: 자동 소화 설비의 부재와 가연성 건축 자재 사용 등 설계상의 결함이 작은 화재를 대재앙으로 키웠습니다. 데이터센터 설계 단계부터 화재 예방 및 확산 방지를 최우선으로 고려해야 합니다.

출처: Dgtl Infra

3.16 텔스트라 데이터센터 화재 (2020년 8월, 영국 런던)

3.16.1 사건 개요

2020년 8월, 호주 최대 통신사인 텔스트라(Telstra)의 런던 호스팅 센터(LHC)에서 화재가 발생했습니다. 화재는 3층에 위치한 공급실의 작은 일부에 영향을 미쳤습니다.

3.16.2 원인 분석

화재는 결함이 있는 무정전 전원 장치(UPS)로 인해 시작되었습니다. 결함 있는 UPS가 버스 바(bus bar)에 연결된 회로 차단기를 트립시키면서 화재가 발생했습니다.

3.16.3 영향 및 피해

화재는 공급실의 작은 부분에 국한되었으며, 서비스 중단이나 데이터 손실에 대한 구체적인 보고는 없었습니다. 인명 피해도 발생하지 않았습니다.

3.16.4 대응 및 복구 과정

화재는 신속하게 진압되었으며, 피해가 제한적이어서 빠른 복구가 가능했습니다.

3.16.5 시사점 및 교훈

이 사례는 UPS가 데이터센터 화재의 가장 흔한 원인 중 하나임을 다시 한번 확인시켜 줍니다. UPS 시스템의 상태를 실시간으로 모니터링하고, 정기적인 부하 테스트와 예방적 유지보수를 통해 잠재적인 결함을 사전에 발견하고 조치하는 것이 매우 중요합니다.

출처: Dgtl Infra

3.17 AT&T 데이터센터 화재 (2018년 10월, 미국 리처드슨)

3.17.1 사건 개요

2018년 10월, 텍사스주 리처드슨에 위치한 AT&T의 스위칭 스테이션에서 전기 화재가 발생하여 몇 시간 동안 서비스가 중단되었습니다.

3.17.2 원인 분석

화재는 전기실 내의 전원 스위치에서 시작되었으며, 구체적인 원인은 밝혀지지 않았습니다. 화재는 전기실 내부에 국한되었습니다.

3.17.3 영향 및 피해

화재로 인해 주 전력 시스템과 백업 전력 시스템 모두에 상당한 손상이 발생했습니다. 이로 인해 북부 텍사스 지역 전역의 AT&T U-verse 서비스 고객들이 영향을 받았습니다. 인명 피해는 없었습니다.

3.17.4 대응 및 복구 과정

전기실에 국한된 화재를 진압하고, 손상된 주 전력 및 백업 시스템을 복구하는 작업이 진행되었습니다.

3.17.5 시사점 및 교훈

이 사례는 전기 화재가 주 전력 시스템뿐만 아니라 백업 시스템까지 동시에 무력화시킬 수 있는 위험성을 보여줍니다. 주 전력과 백업 전력의 공급 경로, 배전반 등을 물리적으로 완전히 분리하여 한 곳의 화재가 다른 곳에 영향을 미치지 않도록 설계하는 것이 중요합니다.

출처: Dgtl Infra

3.18 마클리 데이터센터 화재 (2018년 6월, 미국 보스턴)

3.18.1 사건 개요

2018년 6월, 보스턴의 주요 인터넷 교환(IX) 허브 중 하나인 마클리 그룹(Markley Group)의 원 서머 스트리트(1 Summer Street) 데이터센터에서 소규모 화재가 발생했습니다.

3.18.2 원인 분석

화재는 건물의 8층, 무정전 전원 장치(UPS) 시스템이 위치한 곳에서 발생했습니다.

3.18.3 영향 및 피해

화재로 인해 건물의 스프링클러 시스템이 작동되었고, 이로 인해 UPS 시스템과 대형 배터리가 있는 방이 전기 아크, 연기, 물로 가득 차는 2차 피해가 발생했습니다. 이 사고는 윈드스트림, 센추리링크 등 보스턴 지역의 여러 통신사와 매사추세츠 공과대학교(MIT)가 운영하는 데이터센터 등 다수의 입주 고객에게 영향을 미쳤습니다.

3.18.4 대응 및 복구 과정

스프링클러 시스템이 화재를 진압했으나, 이후 물과 연기로 인한 2차 피해를 복구하는 작업이 필요했습니다.

3.18.5 시사점 및 교훈

디지털 리얼티 사례와 마찬가지로, UPS 및 배터리실과 같은 고위험 구역에서 발생한 화재가 스프링클러 작동으로 이어져 광범위한 수해와 전기적 2차 피해를 유발할 수 있음을 보여줍니다. 특히 여러 고객이 함께 입주해 있는 코로케이션 데이터센터의 경우, 한 구역의 사고가 다른 모든 입주사에게 영향을 미칠 수 있으므로, 입주사 간, 구역 간 방화 및 방수 구획이 철저히 분리되어 있는지 확인하는 것이 중요합니다.

출처: Dgtl Infra

3.19 콜트 DCS 데이터센터 화재 (2015년 7월, 이탈리아 밀라노)

3.19.1 사건 개요

2015년 7월, 콜트 데이터센터 서비스(Colt DCS)의 밀라노 란체티(Lancetti) 데이터센터에서 화재가 발생하여 약 9시간 동안 서비스가 중단되었습니다.

3.19.2 원인 분석

사고는 건물의 전력 인프라 과열과 외부 유틸리티 전원 공급 중단으로 인해 발생했습니다.

3.19.3 영향 및 피해

화재로 인해 약 9시간 동안 서비스가 중단되는 피해가 발생했습니다. 구체적인 물리적 손상 규모는 알려지지 않았습니다.

3.19.4 대응 및 복구 과정

화재 진압 후 전력 인프라를 복구하여 서비스를 정상화했습니다.

3.19.5 시사점 및 교훈

전력 인프라의 과열이 데이터센터 화재의 중요한 원인이 될 수 있음을 보여줍니다. 전력 사용량이 급증하는 AI 시대에는 전력 케이블, 배전반, 변압기 등 모든 전력 경로에 대한 실시간 온도 모니터

링과 적절한 냉각, 그리고 부하 관리가 더욱 중요해지고 있습니다.

출처: Dgtl Infra

3.20 BT 그룹 데이터센터 화재 (2015년 6월, 북아일랜드 벨파스트)

3.20.1 사건 개요

2015년 6월, 북아일랜드 벨파스트에 위치한 BT 그룹의 전화국 건물에서 화재가 발생하여 입주 서비스 제공업체들이 몇 시간 동안 서비스 복구에 어려움을 겪었습니다.

화재가 발생한 BT 벨파스트 전화국 건물

3.20.2 원인 분석

화재는 4층 통신실의 전원 공급 장치에 영향을 미친 사고로 인해 발생했습니다. 화재 자체는 신속하게 진압되었지만, 화재 감지 시 전력이 신속하게 차단되었다가 갑자기 복구되면서 전력 분배 장치(PDU)가 손상되는 2차 문제가 발생했습니다.

3.20.3 영향 및 피해

화재가 데이터센터 층에 직접적인 영향을 미치지는 않았지만, PDU 손상으로 인해 전력 공급에 차질이 생겨 입주 서비스 제공업체들이 몇 시간 동안 어려움을 겪었습니다.

3.20.4 대응 및 복구 과정

화재는 신속하게 진압되었으나, 손상된 PDU를 교체하거나 수리하여 전력을 정상화하는 데 추가 시간이 소요되었습니다.

3.20.5 시사점 및 교훈

이 사례는 재난 상황에서 전력을 차단했다가 복구하는 과정(Power Cycling) 자체가 또 다른 장애를 유발할 수 있음을 보여줍니다. 갑작스러운 전력 복구는 서지(Surge)를 유발하여 민감한 PDU

나 서버 전원 공급 장치를 손상시킬 수 있습니다. 따라서 비상 전력 복구 절차에는 이러한 위험을 최소화하기 위한 단계적인 전력 투입 계획이 포함되어야 합니다.

출처: Dgtl Infra

3.21 애플 데이터센터 화재 (2015년 5월, 미국 메사)

3.21.1 사건 개요

2015년 5월, 애리조나주 메사에 위치한 애플의 데이터센터 건물 옥상에서 화재가 발생했습니다. 이 시설은 애플의 파산한 공급업체였던 GT 어드밴스드 테크놀로지스의 이전 공장이었습니다.

3.21.2 원인 분석

화재는 건물 옥상에 설치된 태양광 패널에서 시작된 것으로 확인되었습니다.

3.21.3 영향 및 피해

화재는 옥상에 국한되었으며, 데이터센터 운영이나 서비스에 미친 영향은 구체적으로 알려지지 않았습니다.

3.21.4 대응 및 복구 과정

소방 당국이 출동하여 옥상 화재를 진압했습니다.

3.21.5 시사점 및 교훈

Maxnod 사례와 마찬가지로, 데이터센터 인프라에 신재생에너지원을 통합할 때 발생하는 새로운 화재 위험을 보여줍니다. 특히, 수많은 태양광 패널과 관련 전기 설비가 설치되는 옥상은 새로운 화재 위험 구역이 될 수 있으며, 이에 대한 정기적인 점검과 전용 소화 설비 설치를 고려해야 합니다.

출처: Dgtl Infra

3.22 삼성 SDS 데이터센터 화재 (2014년 4월, 대한민국 과천)

3.22.1 사건 개요

2014년 4월, 경기도 과천에 위치한 삼성SDS ICT 과천센터에서 화재가 발생하여 건물 내외부가 불타고 여러 삼성 서비스가 중단되는 피해가 발생했습니다.

3.22.2 원인 분석

화재는 4층에서 시작되었으며, 외부 비상발전기 가동을 위한 냉각탑에서 최초 발화한 것으로 추정되었습니다.

3.22.3 영향 및 피해

이 화재로 인해 삼성닷컴, 삼성 페이, 스마트 TV 등 삼성 서버에 의존하는 여러 서비스가 몇 시간 동안 중단되었습니다. 또한, 화재로 인해 4층 건물의 외벽 일부가 떨어져 나가면서 직원 1명이 떨어지는 파편에 경상을 입는 인명 피해도 발생했습니다.

3.22.4 대응 및 복구 과정

소방 당국이 출동하여 화재를 진압했으며, 삼성SDS는 다른 데이터센터로 서비스를 전환하여 복구를 진행했습니다.

3.22.5 시사점 및 교훈

이 사건은 데이터센터 화재가 어떻게 대규모 기술 생태계 전반의 통합 서비스에 영향을 미칠 수 있는지, 그리고 화재로 인한 건물 구조 손상이 인명 피해로 이어질 수 있음을 보여줍니다. 데이터센터 건물은 화재 시 구조적 안정성을 유지할 수 있도록 내화 설계가 중요하며, 외부 설비(냉각탑, 발전기 등)의 화재가 건물 내부로 확산되지 않도록 철저한 방화 대책이 필요합니다.

출처: Dgtl Infra

4 지진 재해 사례

지진은 예측이 거의 불가능하며, 광범위한 지역에 걸쳐 인프라 전체를 파괴할 수 있는 무서운 자연재해입니다. 데이터센터 역시 예외는 아니지만, 철저한 사전 대비를 통해 피해를 최소화한 모범 사례도 존재합니다.

4.1 4.1. 2011년 동일본 대지진과 일본 데이터센터 (2011년 3월, 일본)

4.1.1 사건 개요

2011년 3월 11일, 일본 역사상 가장 강력한 규모 9.0의 대지진과 쓰나미가 도호쿠 지역을 강타했습니다. 이 재앙으로 수많은 인명 피해와 함께 최대 3,050억 달러에 달하는 막대한 물리적 피해가 발생했습니다. 하지만 놀랍게도, 이 거대한 재난 속에서 일본의 데이터센터들은 대부분 심각한 손상 없이 살아남아 비즈니스 연속성을 유지하는 데 중요한 역할을 했습니다.

4.1.2 피해 최소화 원인 분석

Computerworld의 분석 기사에 따르면, 일본 데이터센터들이 지진을 견뎌낸 비결은 철저한 사전 대비에 있었습니다.

- 엄격한 내진 설계: 일본의 데이터센터들은 세계에서 가장 엄격한 건축 법규를 초과하는 수준의 내진 설계를 적용했습니다. 특히 현대적인 데이터센터들은 건물과 지반 사이에 금속과 고무로 된 거대한 '충격 흡수 장치(면진 장치)'를 설치하여, 지반이 흔들리는 동안 건물이 그 위에서 떠 있도록 하는 '면진(Seismic Isolation)' 기술을 적극적으로 도입했습니다.
- 장비 고정 및 보호: 모든 서버 랙, 냉각 장비, 발전기 등은 바닥에 단단히 고정되었습니다. 일부 데이터센터는 랙 단위의 면진 장치를 추가로 설치하기도 했습니다. 이러한 조치 덕분에 일본 전체 데이터센터에서 지진으로 인해 심각하게 손상된 서버 랙은 단 5개에 불과했습니다.

- 전략적 입지 선정: 일본 데이터센터의 약 70%가 상대적으로 지진 피해가 적었던 도쿄 지역에 집중되어 있었습니다. 또한, 쓰나미 위험이 높은 도호쿠 해안 지역에는 데이터센터를 건설하지 않는 등 입지 선정 단계부터 재해 위험을 고려했습니다.

4.1.3 영향 및 과제

데이터센터 건물과 장비의 직접적인 피해는 거의 없었지만, 2차적인 문제들이 발생했습니다.

- 전력 부족: 후쿠시마 원전 사고로 인해 일본 전역이 심각한 전력난에 시달렸습니다. 데이터센터들은 비상 발전기를 가동해야 했지만, 정부의 전력 사용량 15% 감축 명령으로 인해 운영에 큰 압박을 받았습니다. 데이터센터 업계는 정부를 설득하여 '필수 기반 시설'로 인정받아 감축 목표를 완화하는 데 성공했습니다.
- 연료 및 물자 부족: 교통망이 마비되면서 비상 발전기용 경유를 확보하는 데 어려움을 겪었습니다. 또한, 고객사 직원들이 데이터센터로 몰려들면서 식수와 담요 등 구호 물자가 부족해지는 상황도 발생했습니다.
- 통신 장애: 유선 전화망이 마비되면서 소셜 미디어가 중요한 소통 수단이 되었지만, 동시에 유언비어가 빠르게 확산되는 부작용도 나타났습니다. 태평양을 횡단하는 8개의 해저 케이블 중 3개가 손상되어 복구에 최대 27시간 이상이 소요되기도 했습니다.

4.1.4 시사점 및 교훈

동일본 대지진 사례는 재난 '예방'의 중요성을 보여주는 최고의 교훈입니다.

- 설계 단계의 투자가 핵심: 면진 설계와 같은 구조적 대비는 재난 발생 시 그 어떤 사후 대응보다 효과적입니다. 초기 건설 비용이 증가하더라도, 장기적인 비즈니스 연속성 관점에서 이는 필수적인 투자입니다. IT 의사결정자는 데이터센터 선정 시 이러한 구조적 안정성을 반드시 확인해야 합니다.
- 2차 재해에 대한 대비: 건물은 살아남았지만 전력과 연료 부족이 새로운 위협이 되었습니다. 재해 복구 계획은 건물과 IT 시스템뿐만 아니라, 전력, 연료, 인력, 물류 등 운영에 필요한 모든 자원에 대한 비상 조달 계획을 포함해야 합니다.

- 커뮤니케이션 계획의 필요성: 재난 상황에서는 고객 및 직원과의 명확하고 신속한 커뮤니케이션이 매우 중요합니다. 비상 연락망, 정보 공유 채널, 방문객 통제 계획 등을 사전에 수립하고 훈련해야 합니다.

5 전쟁 및 분쟁 사례

전쟁은 데이터센터가 직면할 수 있는 가장 극단적인 형태의 재난입니다. 물리적 파괴와 사이버 공격이 동시에 이루어지는 복합적인 위협 속에서, 데이터 주권을 지키고 서비스를 유지하기 위한 새로운 차원의 전략이 요구됩니다.

5.1 우크라이나 전쟁과 클라우드로의 데이터 피난 (2022년 ~ 현재)

5.1.1 사건 개요

2022년 2월 러시아의 침공으로 시작된 우크라이나 전쟁은 현대전에서 디지털 인프라가 얼마나 중요한지를 극명하게 보여주었습니다. 전쟁 초기, 러시아는 사이버 공격을 통해 우크라이나의 정부 및 금융 시스템을 마비시키려 시도했습니다. 하지만 이러한 시도가 기대에 미치지 못하자, 러시아군은 전략을 바꿔 미사일과 포격으로 데이터센터, 통신탑 등 물리적 인프라를 직접 파괴하기 시작했습니다.

5.1.2 대응 및 복구 과정

물리적 파괴라는 실존적 위협에 직면한 우크라이나 정부는 전례 없는 결정을 내렸습니다. 바로 국가의 핵심 데이터와 시스템을 국경 밖의 글로벌 클라우드 데이터센터로 이전하는 것이었습니다. ScienceDirect에 게재된 연구에 따르면, 우크라이나는 Amazon Web Services(AWS), Microsoft Azure, Google Cloud 등 글로벌 클라우드 기업들의 적극적인 도움을 받아 정부 등록부, 세금 시스템, 금융 데이터 등 수십 페타바이트(PB)에 달하는 데이터를 폴란드, 프랑스 등 유럽 각지에 위치한 클라우드 리전으로 성공적으로 이전했습니다.

이 과정은 '스노우볼(Snowball)'과 같은 물리적 데이터 전송 장치를 통해 이루어졌습니다. 이는 트럭처럼 생긴 견고한 스토리지 장치로, 대용량 데이터를 인터넷을 통하지 않고 물리적으로 안

전하게 운송할 수 있게 해줍니다. 데이터 이전이 완료된 후, 우크라이나의 한 정부 데이터센터가 러시아 미사일에 피격되었지만, 데이터는 이미 클라우드에 백업되어 있어 손실되지 않았습니다.

5.1.3 영향 및 시사점

우크라이나의 사례는 데이터센터 재난 대응의 패러다임을 바꾸는 중요한 전환점입니다.

- 클라우드가 궁극적인 DR 솔루션: 전쟁과 같은 극단적인 상황에서 자국의 물리적 데이터센터는 더 이상 안전지대가 될 수 없습니다. 지리적으로 분산되어 있고, 최고 수준의 물리적/사이버 보안을 갖춘 글로벌 퍼블릭 클라우드는 가장 강력하고 현실적인 재해 복구 솔루션이 될 수 있습니다.
- 데이터 주권의 재정의: 전통적으로 데이터 주권은 자국의 영토 내에 데이터를 보관하는 것을 의미했습니다. 하지만 우크라이나 사례는 데이터를 물리적으로 파괴당하는 것보다, 신뢰할 수 있는 동맹국의 클라우드에 보관하여 접근성과 통제권을 유지하는 것이 진정한 데이터 주권일 수 있다는 새로운 관점을 제시했습니다.
- 민관 협력의 중요성: 우크라이나의 '데이터 피난'은 정부의 신속한 결단과 글로벌 기술 기업들의 헌신적인 지원이 있었기에 가능했습니다. 국가적 재난 상황에서 민관 협력이 얼마나 중요한지를 보여주는 사례입니다.
- IT 의사결정자를 위한 교훈: 기업 역시 지정학적 리스크를 심각하게 고려해야 합니다. 특정 국가나 지역에 비즈니스가 집중되어 있다면, 전쟁, 정치적 불안, 무역 분쟁 등의 시나리오를 포함한 재해 복구 계획을 수립하고, 글로벌 클라우드를 활용한 데이터 및 애플리케이션 분산 전략을 적극적으로 검토해야 합니다.

참고: Harvard Kennedy School – Ukraine's Digital Transformation

6 데이터센터 재해 복구 및 비즈니스 연속성 전략

앞서 살펴본 다양한 재난 사례들은 철저한 사전 대비 없이는 비즈니스의 생존을 보장할 수 없음을 명확히 보여줍니다. 이제 IT 의사결정자는 재난 발생 시 피해를 최소화하고 신속하게 서비스를 복구하기 위한 구체적인 전략을 수립하고 실행해야 합니다. 이는 단순히 기술적인 문제를 넘어, 조직 전체의 문화와 프로세스를 아우르는 비즈니스 연속성 계획(BCP)의 관점에서 접근해야 합니다.

6.1 재해 복구(DR)의 기본

효과적인 전략을 수립하기에 앞서, 재해 복구의 핵심 개념을 이해하는 것이 중요합니다.

6.1.1 재해 복구(DR)와 비즈니스 연속성 계획(BCP)

Cutover의 설명에 따르면, 재해 복구(Disaster Recovery, DR)는 재난 발생 시 IT 시스템과 데이터를 복구하는 데 초점을 맞춘 기술적인 계획입니다. 반면, 비즈니스 연속성 계획(Business Continuity Planning, BCP)은 재난 상황에서도 비즈니스의 핵심 기능(인력, 프로세스, 공급망 등)을 유지하기 위한 포괄적인 전략을 의미합니다. DR은 BCP의 핵심적인 하위 집합이라고 할 수 있습니다.

6.1.2 RTO와 RPO: 목표 설정의 핵심 지표

모든 DR 계획은 두 가지 핵심 목표를 설정하는 것에서 시작합니다.

- 복구 목표 시간 (Recovery Time Objective, RTO): 재난 발생 후 서비스를 복구하는 데까지 허용되는 최대 시간입니다. 예를 들어, RTO가 1시간이라면, 장애 발생 후 1시간 이내에 시스템이 다시 가동되어야 합니다.
- 복구 목표 시점 (Recovery Point Objective, RPO): 재난 발생 시 유실을 감내할 수 있는 데이터의 최대 양(시간)입니다. RPO가 15분이라면, 시스템 복구 시 최대 15분 전의 데이터까지는 손실될 수 있음을 의미합니다. 이는 데이터 백업 또는 복제 주기에 의해 결정됩니다.

RTO와 RPO는 낮을수록(0에 가까울수록) 비즈니스 손실이 줄어들지만, 이를 구현하기 위한 비용은 기하급수적으로 증가합니다. 따라서 IT 의사결정자는 비즈니스 영향 분석(BIA)을 통해 각 서비스의 중요도를 평가하고, 합리적인 RTO와 RPO를 설정해야 합니다.

6.2 예방 및 완화 전략

가장 좋은 재해 복구는 재해가 발생하지 않도록 예방하는 것입니다. 다음은 재난의 위험을 근본적으로 줄이기 위한 핵심 전략입니다.

6.2.1 설계 및 입지 선정

데이터센터의 물리적 안전은 입지 선정과 설계 단계에서 결정됩니다. DataBank의 전문가들은 지진, 홍수, 태풍 등 자연재해 위험이 낮은 지역을 선택하는 것이 가장 중요하다고 강조합니다. 또한, 건물 자체의 내진/내풍 설계, 전력 및 냉각 시스템의 다중화, 그리고 화재 확산을 막기 위한 구획화(Compartmentalization) 등 회복탄력성을 고려한 설계가 필수적입니다. 예를 들어, Equinix의 마이애미 데이터센터는 카테고리 5등급 허리케인을 견딜 수 있도록 17인치 두께의 벽으로 지어졌으며, 해발 14피트 높이에 위치하여 홍수 위험을 최소화했습니다.

6.2.2 화재 예방, 탐지, 진압 시스템

화재는 가장 흔한 위협인 만큼, 다층적인 방어 체계가 필요합니다.

- 예방(Prevention): 가연성 물질 제거, 정기적인 먼지 청소, 케이블 관리, 열 관리 등 기본적인 유지보수가 화재 예방의 시작입니다.
- 탐지(Detection): 화재를 조기에 발견하는 것이 피해를 최소화하는 열쇠입니다. 일반적인 연기 감지기를 넘어, 공기 중의 미세한 연소 입자를 분석하여 화재 발생 전 단계에서 경고하는 '공기 흡입형 연기 감지기(Aspirating Smoke Detector, ASD 또는 VESDA)'가 매우 효과적입니다.
- 진압(Suppression): 데이터센터에서는 물로 인한 2차 피해를 막기 위해 '청정 소화 약제(Clean Agent)' 시스템이나 '불활성 가스(Inert Gas)' 시스템이 주로 사용됩니다. 이 시스템들은 산소 농도를 낮추거나 화학 반응을 억제하여 불을 끄며, 장비에 손상을 남기지 않습니다. 다만, 리튬이온 배터리 화재와 같이 고열을 동반하는 경우에는 냉각 효과가 있는 '워터 미스트(Water Mist)' 시스템이 더 효과적일 수 있습니다.

6.3 재난 예방을 위한 최신 기술 동향

기술의 발전은 재난을 예방하고 완화하는 새로운 가능성을 열어주고 있습니다.

- AI 기반 예측 유지보수: IoT 센서와 머신러닝 알고리즘을 결합하여 장비의 미세한 이상 징후를 실시간으로 감지하고, 장애가 발생하기 전에 미리 유지보수를 수행하는 기술이 도입되

고 있습니다. 예를 들어, UPS 배터리의 전압, 온도, 내부 저항 등의 데이터를 분석하여 열 폭주 가능성을 사전에 예측하고 경고할 수 있습니다.

- 디지털 트윈(Digital Twin): 물리적 데이터센터를 가상 공간에 그대로 복제하여 시뮬레이션하는 기술입니다. 디지털 트윈을 통해 화재 확산 경로, 냉각 시스템 장애 시의 온도 변화, 지진 발생 시의 구조적 스트레스 등을 미리 시뮬레이션해보고, 설계상의 취약점을 발견하고 개선할 수 있습니다.
- 차세대 배터리 기술: 리튬이온 배터리의 화재 위험을 줄이기 위해 나트륨-이온(Sodium-ion) 배터리나 전고체(All-Solid-State) 배터리와 같은 더 안전한 대안 기술에 대한 연구가 활발히 진행되고 있습니다. Everest Group의 분석가는 이러한 대체 기술이 향후 데이터센터의 안전 표준을 바꿀 수 있다고 전망합니다.

6.4 복구 전략

예방 노력에도 불구하고 재난이 발생했을 때를 대비한 신속한 복구 전략이 필요합니다.

6.4.1 백업 및 복제

데이터를 복구하는 가장 기본적인 방법은 백업입니다. 하지만 RPO를 줄이기 위해서는 주기적인 백업만으로는 부족하며, 데이터를 실시간 또는 거의 실시간으로 다른 저장소에 복제(Replication)해야 합니다. 특히, 재해 발생 시 주 데이터센터와 함께 백업 데이터까지 손실되는 것을 막기 위해, 지리적으로 멀리 떨어진 원격지에 데이터를 복제하는 것이 필수적입니다.

6.4.2 다양한 DR 사이트 모델

원격지에 DR 사이트를 구축하는 방식은 RTO/RPO와 비용에 따라 다양하게 나뉩니다.

- Cold Site: 전력과 네트워크 등 기본적인 인프라만 갖춘 공간. 재난 발생 시 서버와 데이터를 직접 가져와 설치해야 하므로 RTO가 매우 깁니다.
- Warm Site: 서버 등 일부 장비가 설치되어 있고, 주기적으로 데이터가 백업되는 사이트. Cold Site보다 RTO가 짧습니다.

- Hot Site: 주 데이터센터와 거의 동일한 시스템을 갖추고 데이터를 실시간으로 복제하는 사이트. 재난 발생 시 즉시 서비스를 인계받을 수 있어 RTO와 RPO가 매우 짧지만, 구축 및 유지 비용이 가장 높습니다.

6.4.3 클라우드 기반 재해 복구 (DRaaS)

최근에는 클라우드를 활용한 재해 복구, 즉 DRaaS(Disaster Recovery as a Service)가 각광받고 있습니다. DRaaS는 물리적인 DR 사이트를 직접 구축하고 운영하는 대신, 클라우드 서비스 제공업체의 인프라를 활용하는 방식입니다. 이는 초기 투자 비용을 크게 줄일 수 있고, 필요에 따라 유연하게 자원을 확장할 수 있으며, 글로벌 클라우드 사업자의 견고한 인프라를 활용할 수 있다는 장점이 있습니다. 우크라이나 사례에서 보듯, 클라우드는 가장 강력한 DR 솔루션이 될 수 있습니다.

6.4.4 정기적인 테스트와 훈련

전문가들은 한목소리로 강조합니다: 테스트하지 않은 DR 계획은 계획이 아니다. DR 계획이 실제로 작동하는지 확인하기 위해서는 정기적으로 모의 재난 훈련을 실시해야 합니다. 훈련을 통해 계획의 허점을 발견하고, 담당자들의 대응 능력을 숙달시키며, 복구 절차를 개선해 나갈 수 있습니다.

6.5 클라우드 네이티브와 분산 아키텍처의 역할

현대적인 애플리케이션 아키텍처는 재해 복구의 패러다임을 바꾸고 있습니다. 과거의 단일체(Monolithic) 애플리케이션은 특정 서버나 데이터센터에 종속되어 있어, 해당 인프라에 장애가 발생하면 서비스 전체가 중단되었습니다. 하지만 클라우드 네이티브 기술은 애플리케이션을 작고 독립적인 서비스 단위로 분해하여 회복탄력성을 극대화합니다.

- 마이크로서비스 아키텍처(MSA): 애플리케이션을 기능별로 잘게 쪼갠 여러 개의 마이크로서비스로 구성하는 방식입니다. 특정 서비스에 장애가 발생하더라도 다른 서비스들은 정상적으로 작동할 수 있어, 장애의 영향 범위를 최소화할 수 있습니다.

- 컨테이너와 쿠버네티스(Containers & Kubernetes): 컨테이너 기술(예: Docker)은 애플리케이션과 그 실행 환경을 패키징하여 어떤 인프라에서든 동일하게 실행될 수 있도록 합니다. 쿠버네티스는 이러한 컨테이너들을 자동으로 관리하고 오케스트레이션하는 플랫폼입니다. 재난 발생 시, 쿠버네티스는 장애가 발생한 노드(서버)의 컨테이너들을 건강한 다른 노드나 다른 데이터센터로 자동으로 이전시켜 서비스를 중단 없이 유지할 수 있습니다.
- 서비스 메시(Service Mesh): 마이크로서비스 간의 복잡한 통신을 관리하고 제어하는 인프라 계층입니다. 서비스 메시는 특정 서비스에 장애가 발생했을 때 트래픽을 자동으로 다른 정상 서비스로 라우팅(Failover)하거나, 반복적인 재시도를 통해 일시적인 장애를 극복하는 등 회복탄력성을 높이는 다양한 기능을 제공합니다.

이러한 클라우드 네이티브 아키텍처를 채택하면, 특정 데이터센터나 리전(Region) 전체에 장애가 발생하더라도 애플리케이션이 다른 리전에서 자동으로 복구되고 서비스를 지속할 수 있습니다. 이는 인프라 수준의 DR을 넘어 애플리케이션 수준에서 회복탄력성을 내재화하는 진일보한 접근 방식입니다.

6.6 비즈니스 관점의 고려사항

IT 의사결정자는 기술적인 전략을 넘어, 비즈니스 전반의 관점에서 재난 대비를 이끌어야 합니다.

6.6.1 보험 (Insurance)

재난으로 인한 재정적 손실을 보전하기 위해 적절한 보험에 가입하는 것은 중요합니다. 재산 피해, 비즈니스 중단으로 인한 손실, 데이터 복구 비용 등을 포괄하는 보험 상품을 검토해야 합니다. 보험사는 잘 갖춰진 DR 계획이 있는 기업에 대해 보험료를 낮춰주기도 합니다.

6.6.2 공급망 다변화 (Supply Chain Diversification)

특정 벤더나 국가의 하드웨어, 소프트웨어에 대한 의존도를 줄이고 공급망을 다변화해야 합니다. 이는 지정학적 리스크로 인한 부품 수급 문제를 완화하고, 특정 기술에 종속되는 '벤더 락인(Vendor Lock-in)'을 피하는 데 도움이 됩니다.

6.6.3 커뮤니케이션 계획 (Communication Plan)

재난 발생 시 혼란을 최소화하기 위해서는 명확한 커뮤니케이션 계획이 필수적입니다. 고객, 직원, 주주, 언론 등 이해관계자별로 어떤 정보를, 언제, 어떻게 전달할지 사전에 정의해야 합니다. 2011년 동일본 대지진 당시 일본 데이터센터들이 겪었던 혼란은 체계적인 커뮤니케이션 계획의 중요성을 잘 보여줍니다.

6.7 결론: 회복탄력성을 향한 제언

지금까지 우리는 화재, 지진, 전쟁 등 다양한 유형의 데이터센터 재난 사례를 통해 그 파괴적인 영향과 값비싼 교훈들을 살펴보았습니다. OVHcloud의 전소된 서버실, 판교 데이터센터 화재로 멈춰버린 국민 메신저, 그리고 미사일 공격을 피해 클라우드로 피난한 우크라이나의 국가 데이터는 더 이상 영화 속 이야기가 아닌, 우리가 직면한 현실입니다.

이 모든 사례가 가리키는 방향은 명확합니다. 이제 데이터센터 운영의 목표는 99.999%의 '가동 시간(Uptime)'을 넘어, 예측 불가능한 최악의 상황에서도 비즈니스를 지켜낼 수 있는 '회복탄력성(Resilience)'으로 전환되어야 합니다. 회복탄력성은 단순히 장애를 막는 방어적인 개념이 아니라, 위기를 기회로 전환하고 더 강한 조직으로 거듭나기 위한 능동적이고 전략적인 접근입니다. 이는 기술적 견고함(Robustness)을 넘어, 변화에 적응하고(Adaptability), 신속하게 복구하며(Rapidity), 자원을 효율적으로 활용하고(Resourcefulness), 중복성을 확보(Redundancy)하는 다차원적인 역량을 포함합니다.

IT 의사결정자 여러분께 다음의 세 가지를 제언하며 본 백서를 마무리하고자 합니다.

1. 투자의 패러다임을 바꾸십시오. 재해 복구(DR)와 비즈니스 연속성 계획(BCP)에 대한 투자는 더 이상 비용이 아니라, 기업의 생존과 성장을 위한 핵심 투자입니다. 단기적인 비용 절감에 매몰되어 DR 투자를 미루는 것은, 시한폭탄을 안고 비즈니스를 운영하는 것과 같습니다. CEO와 이사회에 재난의 실질적인 비즈니스 영향을 정량적으로 제시하고, 회복탄력성 확보를 최우선 경영 과제로 설정하도록 설득해야 합니다.
2. '만약(What if)'이 아닌 '언제(When)'의 관점에서 준비하십시오. "우리에게도 저런 일이 일어날까?"라고 질문해서는 안 됩니다. "저런 일이 언제, 어떤 형태로 일어날 것인가?"를 가정하고 모든 시나리오에 대비해야 합니다. 지리적으로 분산된 이중화 구조, 클라우드를 활용

한 유연한 DR 전략, 그리고 실전과 같은 정기적인 훈련은 이제 선택이 아닌 필수입니다. 가장 흔한 장애 원인이 자연재해가 아닌 인적, 기술적 오류라는 점을 감안할 때, 일상적인 운영 속에서도 항상 최악의 상황을 염두에 두어야 합니다.

3. 기술을 넘어 생태계를 구축하십시오. 진정한 회복탄력성은 기술만으로 완성되지 않습니다. 신뢰할 수 있는 파트너(클라우드 제공업체, 솔루션 벤더), 명확한 비상 커뮤니케이션 채널, 그리고 재난 상황에서 일사불란하게 움직일 수 있도록 훈련된 인력 등 견고한 '회복탄력성 생태계'를 구축해야 합니다. 특히, 쿠버네티스와 같은 클라우드 네이티브 기술을 적극적으로 도입하여 인프라 장애가 애플리케이션 중단으로 이어지지 않도록 아키텍처 수준에서부터 회복탄력성을 내재화해야 합니다.

디지털 전환이 가속화되고 AI 시대가 본격화되면서 데이터센터의 중요성은 날이 갈수록 커지고 있습니다. 동시에 데이터센터를 둘러싼 위협 또한 더욱 복잡하고 예측 불가능한 형태로 진화할 것입니다. 지금 바로 회복탄력성 확보를 위한 첫걸음을 내딛는 것이야말로, 불확실한 미래에 대비하는 가장 확실한 방법일 것입니다.

7 참고 자료

[1]Calculating the cost of downtime | Atlassian- https://www.atlassian.com/incident-management/kpis/cost-of-downtime

[2]Data Center Disaster Recovery: Essential Measures for Business …- https://www.datacenterknowledge.com/uptime/data-center-disaster-recovery-essential-measures-for-business-continuity

[3]https://dgtlinfra.com/data-center-fires/- https://dgtlinfra.com/data-center-fires/

[4]South Korea's data center fire triggers global scrutiny of lithium-ion …- https://www.networkworld.com/article/4065542/south-koreas-data-center-fire-triggers-global-scrutiny-of-lithium-ion-batteries-and-dr-architecture.html

[5]Natural Disaster Preparation For Data Centers | Foster Fuels - https://fosterfuels.com/blog/natural-disaster-preparation-for-data-centers/

[6]Understanding the Cost of Data Center Downtime | Sunbird DCIM– https://www.sunbirddcim.com/blog/understanding-cost-data-center-downtime

[7]Ukraine Data Centers Became Physical Targets When Cyberattacks … – https://www.meritalk.com/articles/ukraine-data-centers-became-physical-targets-when-cyber-attacks-failed/

[8]Seismic Resilience & Disaster Preparedness in Data Center Design – https://netzero-events.com/seismic-resilience-disaster-preparedness-in-data-center-design/

[9]How Japan's data centers survived the earthquake | Computerworld– https://www.computerworld.com/article/1442763/how-japan-s-data-centers-survived-the-earthquake.html

[10]How Data Centers Guard Against Natural Disasters | DataBank – https://www.databank.com/resources/blogs/how-data-centers-guard-against-natural-disasters/

[11] Data Center Disaster Recovery Strategies & Processes | Cutover–https://www.cutover.com/blog/data-center-disaster-recovery-strategies-processes

[12]The High Cost of Downtime in 2023 Data Centers | ProSource– https://www.team-prosource.com/the-high-cost-of-downtime-in-2023-data-centers/

[13]Ukraine's Digital Transformation: Innovation for Resilience – https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

[14]Russian–Ukraine armed conflict: Lessons learned on the digital …– https://www.sciencedirect.com/science/article/abs/pii/S1874548223000501

[15]AI geopolitics and data centres in the age of technological rivalry– https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/

Contact Us

hello@cncf.co.kr

02-469-5426

www.cncf.co.kr

CNF Blog

다양한 콘텐츠와 전문 지식을 통해
더 나은 경험을 제공합니다.

CNF eBook

이제 나도 클라우드 네이티브 전문가
쿠버네티스 구축부터 운영 완전 정복

CNF Resource

Community Solution의 최신 정보와
유용한 자료를 만나보세요.

씨엔에프 | CNF

전화 : (02)469-5426
팩스 : (02)469-7247
메일 : hello@cncf.co.kr