**🚨 털리고, 터지고, 마비되고! 연쇄 디지털 재난 속 K-보안의 민낯**

**– SKT, KT, 롯데카드 해킹과 국가정보자원관리원 화재, '예견된 재앙'이었다**

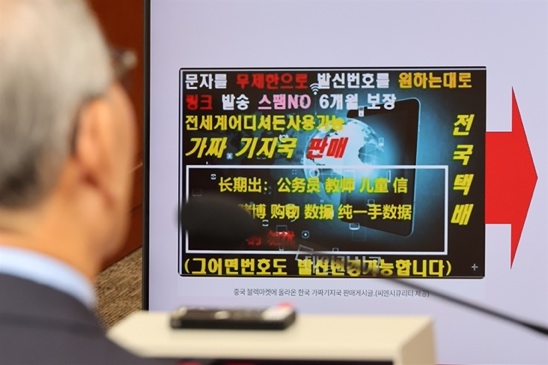
21010075 이효주

최근 몇 달 사이 국내에서 디지털 인프라 관련 재난이 연달아 터지고 있습니다. 우리가 매일 쓰는 통신망과 금융 서비스, 나아가 국가 행정을 떠받치는 데이터센터까지 하나둘씩 삐걱거리거나 멈춰 섰죠. 표면적으로 보면 ‘해킹’이라는 사이버 공격과 ‘화재’라는 물리적 재앙은 전혀 다른 문제처럼 보입니다. 그런데 정말로 이 사건들이 우연히, 특정 기업들에만 국한된 일일까요?【1】【2】

오늘 뉴스레터에서는 통신사와 금융사에서 벌어진 해킹 사건들, 그리고 국가정보자원관리원의 화재 사고를 한데 모아 들여다보려 합니다. 각 사건을 따로따로 보면 다른 이야기 같지만, 자세히 뜯어보면 공통된 문제가 보입니다. 바로 **시스템의 기술적 허점**과 **안전 관리의 부실**입니다.

이 두 가지가 어떻게 맞물려 ‘K-디지털 인프라’의 취약성을 드러냈는지, 그리고 비슷한 재난이 다시 반복되지 않도록 정부, 기업, 개인 차원에서 어떤 노력이 필요한지 차근차근 살펴보겠습니다.

**Part 1. 기술적 결함: 디지털 재앙을 부른 시스템의 허점**

****

ⓒ News1 ⓒ 연합뉴스

사진2: 김영섭 KT 대표이사가 중국 온라인 쇼핑몰에서 판매되고 있는 가짜 기지국 관련 질문에 답하고 있다

최근 이어진 디지털 재난들은 우리 사회 핵심 인프라에 내재한 **기술적 허점**이 얼마나 치명적인 결과로 이어질 수 있는지를 명확히 보여주었습니다.

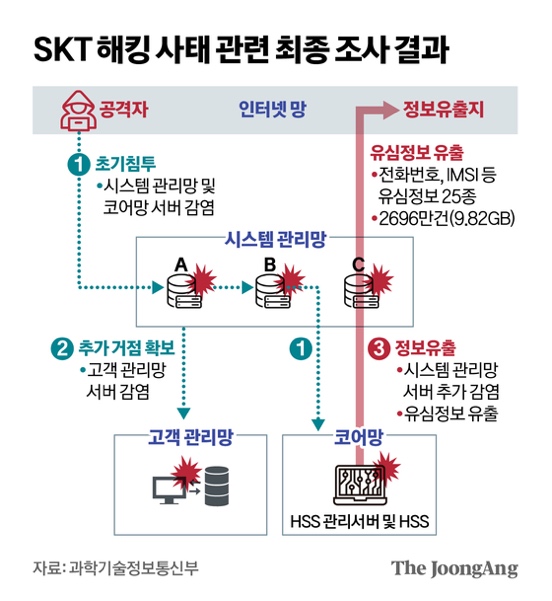
먼저 지난 달 발생한 국가정보자원관리원 화재 사건의 경우 UPS(무정전 전원장치) 전원이 화재 66분 전에 차단됐는데도 불길은 걷잡을 수 없이 번졌습니다. 전원 차단만으로는 안전을 확보할 수없는 **구조적 결함**이 있었던 겁니다. 리튬이온 배터리에는 전류가 남아 있어 위험이 계속되고, UPS전원이 꺼지면 보호 회로까지 멈춰버려 안전 장치가 사실상 무용지물이 된 것입니다.【1】

통신사들의 해킹 사고 역시 통신 서비스 전반의 기술적 취약성을 보여줍니다. SKT 해킹은 네트워크 관리 서버에침투한 악성코드를 탐지하고 차단하는 데 실패하면서, 2,600만 건이 넘는 유심 정보 유출로 이어졌습니다. 이는 **네트워크 보안 시스템 자체의 탐지 및 방어 체계 미비**라는 기술적 허점을 명확히 보여주는 사례입니다. KT 해킹에서는 **초소형기지국인 펨토셀 장비의 보안 시스템에 문제**가 있거나 필수적인 보안 검증 절차가 누락되는 심각한 기술적 문제가 발견되었고, 이는 2억 4천만원 상당의 소액결제 피해와 휴대폰의 고유 식별 정보(IMEI) 노출까지 불러왔습니다. 【4】【5】【6】

금융권도 예외는 아니었습니다. 지난 달 18일 롯데카드에서 전체 고객의 30%에 달하는 297만 명의 개인정보가대규모로 유출됐습니다. 카드 번호뿐 아니라 보안 코드까지 포함돼 있었는데요, 이는 **금융 보안 체계의 구조적 허점**을 그대로 보여주는 사건이었습니다.

겉보기에 다른 사건처럼 보이지만, 세 사건 모두 똑같은 결론을 남겼습니다. 바로 기술적 허점이 직접적인 재난의 발화점이 됐다는 사실입니다. 이는 특정 기업의 문제가 아니라, 대한민국 IT 생태계 전반이 떠안고 있는 취약성의 민낯이기도 합니다.

**Part 2. 관리 소홀: 예견된 재앙을 키운 안일함**



ⓒ 중앙일보

디지털 재난은 단순히 기술적 결함에서만 비롯되지 않았습니다. 문제 발생 가능성을 인지하고도 이를 방치하거나, 기본적인 절차조차 지키지 않는 '**관리 소홀**'은 재앙의 규모를 키우는 주요 원인이었습니다.

국정자원 화재의 경우, 배터리 교체 과정에서 **제조사 협조 요청 절차를 누락**하고 **안전 지침을 미준수**하여 대형 화재로 이어진 점은 명백한 관리 부실의 사례입니다. 경찰 수사에서도 업무상 실화 혐의와 함께 관리 부실 및 직원의 실수가 핵심 원인으로 지목되었습니다. 이는 'IT 강국'의 명성에도 불구하고 단 한 번의 관리 실수가 전국적인 행정망 마비를 초래할 수 있음을 보여주었습니다. 【1】【2】【3】

통신사 해킹 역시 마찬가지입니다. SKT는 해커의 침투 과정에서 관리망 서버 보안과 로그 관리가 허술했던 사실이 드러났습니다. KT 해킹 사건에서도 초소형 기지국 관리 소홀과 보안 인증 절차 미준수가 피해를 키운 원인으로 지적됐습니다. 【4】【5】

무엇보다 충격적인 건, 연쇄 해킹을 당한 기업들 대부분이 이미 ISMS-P(정보보호 및 개인정보보호 관리체계) 인증을 보유하고 있었다는 점입니다. 인증은 있었지만, 내부 통제 시스템은 제 기능을 하지 못했고, 실제 보안 수준과 인증은 따로 놀고 있었습니다. 결국 ‘보여주기식 보안’과 ‘안일한 관리 문화’가 만연했음을 보여주는 사례였죠. 과거부터 반복 지적돼 온 기술 업데이트 지연, 허술한 접근 통제, 직원 보안 의식 부재가 이번에도 똑같이 드러났다는 사실은 우리 사회의 관리 시스템이 얼마나 피상적이었는지를 방증합니다. 【8】

**Part 3. 데자뷔처럼 반복되는 문제: 디지털 재난의 구조적 원인**

우리가 이번 사건들을 보며 ‘또?’라는 감정을 느끼는 건 우연이 아닙니다. 해킹과 화재, 겉으로는 전혀 다른 사건 같지만, 사실은 과거부터 똑같은 문제가 반복되고 있기 때문입니다. 한마디로 우리 사회 전반에 자리 잡은 ‘IT 인프라 안전 불감증’이 여실히 드러난 셈이죠. 실제로 2023년 한 해 동안 국내 공공기관이 받은 사이버 공격은 일 평균 162만 건에 달했고, 전년 대비 무려 36% 증가했습니다. 공격은 늘어나는데, 대응은 여전히 제자리라는 얘기입니다. 【8】

🔧 고질적인 기술적 허점과 낡은 시스템

이번 사건이 특별한 이유는 아닙니다. 과거에도 대규모 개인정보 유출 사건 때마다 시스템 노후화, 보안 패치 지연, 허술한 관리자 계정 관리가 문제로 꼽혔습니다. 그런데도 똑같은 약점이 다시 그대로 노출됐습니다. 임시방편으로 구멍을 메우는 수준에 머물다 보니, “이 정도면 괜찮겠지”라는 안일한 태도가 쌓이고, 새로운 위협 앞에서 결국 더 큰 사고로 이어진 겁니다.

🧑‍💼 반복되는 관리 부실, 결국 ‘사람의 문제’

문제는 기술만이 아닙니다. 해킹 사건 때마다 내부 직원들의 보안 의식 부족, 협력업체 관리 허술, 형식적인 보안 교육이 늘 도마 위에 올랐습니다. 국정자원 화재 역시 마찬가지입니다. 수십 년 전부터 중앙 집중식 데이터센터의 위험성이 지적돼 왔지만, 이중화나 재해 복구 시스템에 대한 투자는 미뤄졌습니다. “소 잃고 외양간 고친다”는 말은 이제 진부할 정도인데, 현실은 오히려 소를 여러 번 잃고도 외양간을 고치지 않는 상황에 가깝습니다.

실제로 정보보호 최고책임자(CISO)의 81%가 ‘인적 오류’를 가장 큰 보안 취약 요인으로 꼽았고 데이터 사고의 94%는 퇴사 직원으로부터 비롯됐다는 조사 결과도 있습니다. 기술이든 관리든 결국 ‘사람의 태도’가 핵심이라는 점을 보여주는 대목입니다. 【10】

**Part 4. 'Next Step': 정부-사회-개인의 협력으로 만드는 '안전한 디지털 미래'**

반복되는 디지털 재난을 극복하고 더 나은 미래를 구축하기 위해 우리는 다각적인 변화를 모색해야 합니다. 이는 특정 기업을 넘어 대한민국 디지털 생태계 전반에 적용되어야 할 과제이며, 궁극적으로 정부의 책임감 있는 정책이 사회(기업)의 변화를 이끌고, 다시 개인의 행동 변화를 유도하는 유기적인 흐름 속에서 해답을 찾아야 합니다.

1. 정부: 강력한 제도적 감시와 실질적인 규제로 사회 변화를 선도해야 합니다.

- 'IT 강국'이라는 명성을 유지하기 위해서는 단순히 '기술적 선진국'을 넘어 '관리 및 보안 선진국'이 되어야합니다. 정부는 국정자원 화재와 해킹 사건에서 드러난 관리 부실에 대한 책임을 명확히 하고, 재발 방지를 위한 제도적 감시를 강화해야 합니다.

- 기업의 개인정보 유출 시 천문학적인 벌금 부과 또는 경영진에게 직접적인 책임을 지게 하는 강력한 법적 제재를 시행해야 합니다. 유럽의 GDPR(일반 데이터 보호 규정)이 최대 2천만 유로(약 322억원) 또는 전 세계 연간 총매출의 4%에 달하는 과징금을 부과하는 것처럼, 미온적인 처벌로는 기업의 자발적인 보안 투자를 유도하기 어렵습니다.

- 국가 핵심 디지털 인프라에 대한 투자를 확대하고, 물리적·사이버 재해 대비 시스템을 실질적으로 작동 가능하도록 끊임없이 점검하고 개선해야 합니다. 과거 경고가 묵살되는 일이 없도록, 전문가들의 의견을 적극 반영해야 합니다. KISA의 정보보호 공시제도 등을 통해 기업의 정보보호 투자를 활성화하고 인식 제고를 위한 노력을 해야 합니다. 또한 전문 보안 인력 양성 및 배치는 미래 디지털 재난을 예방하는 핵심적인 투자입니다.

2. 사회(기업 포함): '보안'을 '생존'의 필수 조건으로 인식하고 투자를 확대해야 합니다.

- 정부의 강력한 규제와 감시 속에서 기업은 보안을 더 이상 '비용'이 아닌 '생존을 위한 필수 투자'로 인식해야 합니다. 데이터센터와 통신사들이 보여준 관리 부실 사례를 반면교사 삼아, 관리 체계를 대폭 강화해야 합니다.

- 단순한 방어막 구축을 넘어, AI 기반의 예측 보안 시스템 도입이나 블록체인 기술 활용을 통해 데이터 위변조를 막는 등 첨단 기술에 대한 투자를 확대해야 합니다. 해킹과 화재 모두에서 드러난 '단일 장애점'의 위험성을 인지하고, 시스템 이중화와 재해 복구 시스템(DRS) 고도화를 규제 준수를 넘어선 '생존 필수 조건'으로 인식해야 합니다. 실제로 2023년 국내 정보보호 투자액은 약 1조 8,526억원으로 전년 대비 20.9% 증가했으며, 금융업과 정보통신업이 가장 높은 투자액을 보였습니다. 하지만 카카오, 네이버 등 일부 IT 기업의 정보보호 투자 비중은 평균치에 미치지 못하는 등 선제적 투자가 여전히 부족한 기업들이 많다는 점도 지적됩니다.

- 아무리 기술이 발전해도 '사람이 가장 큰 보안 구멍'이라는 점을 인지하여 내부 직원들의 보안 의식을 강화하는 교육과 캠페인을 상시적으로 진행해야 합니다. 그리고 정기적인 모의 해킹으로 실제 공격 시나리오를 대비하고, 허술한 협력업체 관리에도 만전을 기해야 합니다.

3. 개인: '내 정보는 내가 지킨다'는 책임 의식으로 방어의 최전선을 지켜야 합니다.

- 정부와 기업의 노력과 더불어 개인의 보안 의식 함양은 디지털 안전망의 마지막 퍼즐입니다. 귀찮더라도 2단계 인증을 설정하고, 비밀번호를 주기적으로 변경하며, 출처 불명의 링크나 이메일은 절대 클릭하지 않는 등 기본적인 보안 수칙을 철저히 준수해야 합니다. 실제로 손상된 계정 정보(아이디, 비밀번호 등 자격 증명)는 데이터 위반의 주요 원인 중 하나로, 전체 데이터 위반의 19%를 차지하기도 합니다. 사이버 보안 필수 가이드와 같은 정보를 활용하여 정부나 기업에만 책임을 전가하는 것이 아니라, 우리 스스로도 '디지털 시민 의식'을 높여 자산인 정보를 보호해야 합니다.

**마무리하며: '지속적인 관심'이 만드는 안전한 디지털 미래**

SKT·KT·롯데카드 해킹과 국가정보자원관리원 화재. 사건의 성격은 달랐지만, 기술적 허점과 관리 부실 이라는 공통적인 문제점으로 연결되어 있었고, 이는 '대한민국 디지털 인프라 전반의 고질적인 안전 불감증'이라는 현실을 우리 앞에 명확히 드러냈습니다. 문제의 근원에는 디지털 안전에 대한 ‘관심 부족’에 있습니다. 시스템의 기술적 허점을 방치하고, 기본 안전 수칙을 외면하고, 투자를 뒤로 미루고, 직원 교육을 소홀히 한 결과가 쌓여 연쇄 재난으로 이어진 겁니다.

이제 답은 분명합니다. ‘지속적인 관심’이야말로 생존을 담보하는 가장 강력한 무기라는 사실입니다. 정부는 규제와 투자에, 기업은 시스템과 인력 관리에, 개인은 자신의 정보와 보안 습관에 끊임없는 관심을 기울여야 합니다.

‘눈 가리고 아웅’식 대응은 더 이상 통하지 않습니다. 디지털 세상에서 더 안전하고 지속 가능한 환경을 만들려면 정부, 기업, 그리고 우리 모두가 함께 책임감을 갖고 변화를 이어가야 합니다.

📑 더 읽을거리

한겨레 – 국가정보자원관리원 화재, 안전 지침 미준수 (2025.09.27)

🔗 <https://www.hani.co.kr/arti/area/area_general/1221732.html>

BBC Korea – 국정자원 화재, 전국 행정망 마비 분석 (2025.09.28)

🔗 <https://www.bbc.com/korean/articles/cvgr0epyj9do>

조선일보 – 경찰, 직원 과실·관리 소홀 원인 지목 (2025.10.02)

🔗 <https://www.chosun.com/national/regional/2025/10/02/FCIR7SOMIRFYVGSJKQ7KNPIM4A/>

동아IT – SKT 해킹, 관리 서버 로그 관리 부실 (2025.09.24)

🔗 <https://it.donga.com/107247/>

오마이뉴스 – KT 펨토셀 장비 관리 소홀 (2025.09.25)

🔗 <https://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0003168709>

더렉 – KT 해킹, IMEI 유출 및 소액결제 피해 (2025.09.25)

🔗 <https://www.thelec.kr/news/articleView.html?idxno=40960>

딜사이트 – 보안 투자 확대 필요성과 기업의 책임 (2025.09.27)

🔗 <https://dealsite.co.kr/articles/148215/068020>

프레시안 – 보여주기식 보안·안전 불감증 비판 (2025.09.25)

🔗 <https://www.pressian.com/pages/articles/20250925200001>

데일리시큐 – 2023년 공공기관, 하루 평균 162만 건 사이버 공격

🔗 <https://www.dailysecu.com/news/articleView.html?idxno=200684>

데일리시큐 – CISO 81% ‘인적 오류’, 데이터 사고 94% 퇴사 직원 원인

🔗 <https://www.dailysecu.com/news/articleView.html?idxno=156159>