글로벌 IT 대란이 주는 교훈 : 대응 전략과 미래 과제

조영준[1], 최고은[2], 안현철[3]
[1]한국정보산업연합회 선임 연구원
[2]한국정보산업연합회 책임 연구원
[3]국민대학교 비즈니스IT전문대학원 교수
choyj@fkii.org, cge@fkii.org, hcahn@kookmin.ac.kr

Lessons from the Global IT Crisis: Response Strategies and Future Challenges

Young-Jun Cho[1], Go Eun Choi[2], Hyunchul Ahn[3]
[1]FKII (The Federation of Korean Information Industries)
[2]FKII (The Federation of Korean Information Industries)
[3]Graduate School of Business IT, Kookmin University

요 약

이번 글로벌 IT 대란에서 국내 금융 및 공공 분야는 '망 분리' 규제 덕분에 피해가 미미했으나, 클라우드 확산이 가속화되면서 향후 이러한 보호가 약화 될 가능성이 있다. 클라우드 도입이 불가피한 상황에서 서비스 제공자와 고객 간의 분쟁 예방 및 해결 방안 마련이 필수적이다. 이번 사태는 규제 강화보다는 사이버 공급망 위협에 대한 선제적 대응과 IT 역량 강화를 위한 기회로 삼아야 한다.

1. 서론

2024년 7월 19일, 글로벌 보안업체 크라우드 스트라이크(Crowd Strike)의 보안 소프트웨어인 '팰컨 센서(Falcon Sensor)'의 업데이트 패치가 전 세계 IT 산업에 심각한 영향을 미친 사건이 발생했다. 팰컨 센서의 최신 패치는 마이크로소프트 윈도우 운영체제를 사용하는 PC 또는 서버에서 치명적인 오류, 즉 '죽음의 블루 스크린(BSOD)' 또는 재부팅 루프에 빠지는 현상을 초래했다. 이 오류는 단순한 기술적 결함에 그치지 않고 전 세계 주요 산업 및 공공기관에 걸쳐 시스템 중단을 초래했으며, 글로벌 IT 환경에 큰 충격을 주었다[1-2].

이 사건은 단순한 기술적 오류 이상의 의미가 있다. 현대 사회에서 IT 인프라의 핵심적 역할을 감안할 때, 시스템 중단이 발생할 경우 그 파장은 사회 전반에 걸쳐 매우 광범위하게 미친다. 이번 사건은 특히 글로벌 보안 및 시스템 운영의 중요성을 다시금 부각시키며, 기술적 결함이 국가 경제, 공공 안전, 사회적 신뢰에까지 미치는 영향을 재조명하는 계기가 되었다. 본 논문에서는 크라우드 스트라이크의 팰컨 센서 오류로 촉발된 글로벌 IT 대란을 분석하고, 이를 통해 드러난 시스템 안정성 및 보안의 중요성, 그리고 향후 재발 방지를 위한 대응 방안을 모색하고자 한다.

2. 글로벌 IT 대란: 원인과 배경 주요 원인

1) 보안 소프트웨어 업데이트 오류

2024년 7월 글로벌 IT 대란은 크라우드 스트라이크의 보안 소프트웨어 팰컨 센서의 업데이트 오류로 발생했다. 초기에는 마이크로소프트 클라우드 서비스 문제로 지목되었으나, 이후 크라우드 스트라이크의 '채널 파일 291' 업데이트 과정에서 입력값 불일치로 시스템 충돌이 발생한 것으로 밝혀졌다[1].

문제가 된 업데이트는 21개의 입력 필드 중 1개가 누락되어 보안 소프트웨어와 윈도우 운영체제 간의 호환성 문제를 야기했고, 그 결과 마이크로소프트 애저(Azure) 클라우드에 연결된 약 850만 대의 단말기가 '죽음의 블루 스크린' 오류와 재부팅 루프를 겪어 대규모 서비스 중단이 초래되었다[1].

2) 내부 품질관리 실패

크라우드 스트라이크의 팰컨 센서 업데이트 오류는 품질보증(QA) 절차가 제대로 이행되지 않아 발생한 문제였다. 소프트웨어 업데이트 과정에서 고객사의 운영체제와의 호환성을 철저히 검증하는 것이 필수적이나, 크라우드 스트라이크는 신속한 배포를 위해 QA 절차를 일부 생략했다. 특히, 2024년 4월 리눅스 커널에서도 유사한 문제가 보고되었음에도 해결되지 않은 채 업데이트가 배포되었다[2-3].

이러한 품질관리 절차의 생략은 시스템 장애의 위험성을 높였으며, 결국 수백만 대의 시스템이 장애를 겪는 대규모 IT 사고로 이어졌다. 보안 소프트웨어의 핵심 기능을 충분히 테스트하지 않은 것이 이번 사건의 주요 원인이었다.

3) 마이크로소프트의 개방형 설계

이번 글로벌 IT 대란의 1차 원인은 크라우드 스트라이크의 보안 소프트웨어 업데이트 오류였지만, 마이크로소프트 윈도우 운영체제의 개방형 설계도 중요한 역할을 했다는 비판이 제기되었다[4]. 마이크로소프트는 2009년부터 제3자 소프트웨어 개발자들에게 윈도우 커널에 접근할 수 있도록 허용해 왔다. 이는 다양한 보안 솔루션과 응용 프로그램 개발을 촉진했지만, 커널에 깊이 관여하는 소프트웨어 오류가 발생할 경우 시스템 전체에 치명적인 영향을 미칠 수 있는 위험을 초래했다.

반면, 애플은 2020년부터 MacOS에서 커널 접근을 제한해 운영체제의 안정성을 강화했다. 마이크로소프트의 개방형 설계는 윈도우 생태계를 확장했지만, 외부 소프트웨어 오류가 운영체제 전체에 미치는 위험을 증가시켰다는 비판을 받았다[5].

4) 주요 피해 사례[1][6]

크라우드 스트라이크의 보안 소프트웨어 업데이트 오류로 촉발된 이번 글로벌 IT 대란은 다양한 산업 분야에 걸쳐 심각한 피해를 초래했다. 특히 포춘 500(Fortune 500) 기업들에 미친 경제적 손실은 약 54억 달러에 이를 것으로 추산되며, 피해 범위는 항공, 금융, 의료 등 다방면에 걸쳐 있다.

4-1) 항공사 및 공항 피해

미국의 주요 항공사인 아메리칸 항공, 델타 항공, 유나이티드 항공은 모두 이번 IT 대란의 영향을 받았다. 연방항공청(FAA)은 여러 항공편의 운항을 중단시켰으며, 유럽에서도 영국의 개트윅, 루턴, 스탠스테드 공항과 네덜란드의 스히폴 공항에서 체크인 시스템 오류가 발생했다. 인도와 아시아의 여러 공항에서도 탑승권 등록 문제로 혼란이 빚어졌다.

결과적으로 전체 항공편의 23%만이 제시간에 출발했으며, 1,300편 이상의 항공편이 취소되거나 지연되었다. 미국 내 일부 항공사들은 여행 면제권을 제공하며 사태를 수습하려 했으며, 네덜란드의 KLM은 대부분의 운영을 중단해야 했다.

4-2) 의료 기관 피해

미국과 영국의 의료 기관들은 이번 대란으로 인해 비긴급 수술과 절차를 취소해야 했으며, 매사추세츠 종합병원에서는 대규모 소프트웨어 중단으로 다수의 환자가 피해를 보았다. 영국의 국립보건 서비스(NHS) 예약 시스템과 약국 결제 시스템 또한 장애를 겪었으며, 북아일랜드 의료 서비스에서는 환자 기록에 접근할 수 없어 심각한 영향을 받았다.

4-3) 금융 기관 피해

영국 런던 증권 거래소를 비롯한 여러 금융 기관에서 서비스 중단 사태가 발생했다. 로이드 은행, 비자와 같은 주요 금융 서비스 제공 업체가 영향을 받았으며, 미국의 JP모건 체이스 직원들도 회사 시스템에 접근하는 데 어려움을 겪었다. 그 외 다른 국가의 금융 기관에서도 서비스 장애가 보고되었다.

4-4) 공공 서비스 및 기타 분야 피해

미국의 여러 주에서 긴급 911 서비스가 중단되었으며, 알래스카, 미네소타, 애리조나 등에서 서비스 장애가 발생했다. 또한, 영국의 대형 소매점 테스코, 모리슨스, 세인즈버리 등은 결제 시스템에 문제가 생겨 고객 응대에 차질을 빚었다. 미디어 업계에서도 MTV, VH1, 스카이, BBC 등 일부 채널이 피해를 보았으며, 파리올림픽 조직위원회도 IT 운영에 차질을 겪으며 유니폼 및 인증서 배달에 문제가 발생했다.

4-5) 선거 및 기타 공공 행사 피해

미국 마리코파 카운티의 선거 시스템도 이번 대란의 영향을 받아 특정 투표 장소에서 문제가 발생했고, 철도 운영사와 스포츠 관련 기관 등도 서비스 중단을 겪었다. 크라우드 스트라이크의 보안 소프트웨어 팰컨 센서를 사용하는 많은 기업과 기관들이 이번 사태로 인해 업무에 큰 차질을 빚었다.

<표 1> 글로벌 IT 대란 국내 외 피해 상황

피해 상황	
국내	국외
- LCC 3곳 (이스타·제주·에어프레미아) 예약·발권 시스템 마비 - 펄어비스·그라비티 게임 검은사막 ·라그나로크 등 장애 - 쿠팡 등 일부 기업 PC 장애 발생, 주요 통신 서비스 피해 無	- 미국·유럽·일본 등 전세계 항공사 운항 차질, 5,000대 이상 취소 - 시카고상품거래소 ·런던 증권거래소 일부 기능 중단 - 영국·뉴질랜드 일부방송사 방송 중단 - 파리올림픽 일부IT서비스 차질

3. IT 대란이 불러온 글로벌 문제와 대응 과제

1) 소프트웨어 품질보증 체계에 대한 반성

이번 글로벌 IT 대란은 크라우드 스트라이크의 팰콘 센서 업데이트 과정에서 품질보증 절차의 실패가 주요 원인 중 하나였다. 팰콘 센서는 시스템 핵심인 커널 모드에서 작동하며, 시스템 전체에 큰 영향을 미칠 수 있는 보안 소프트웨어이므로, 엄격한 품질 보증 절차가 필수적이다. 그러나 신속한 대응을 위해 품질보증 과정이 단순화되었고, 그 결과 치명적인 결함이 사전에 발견되지 않았다. 이에 따라 업데이트된 소프트웨어가 검증 없이 배포되었고, 시스템 충돌을 일으키며 대규모 IT 장애를 초래했다[2].

이번 사건은 보안 소프트웨어에서 신속한 대응과 철저한 검증 간의 균형이 얼마나 중요한지를 보여주며, 향후 품질보증 시스템의 개선 필요성을 시사한다.

2) IT 장애 발생 시 긴급 대응 및 복구에 대한 관심 환기

이번 글로벌 IT 대란은 대규모 피해를 초래했음에도 불구하고, 크라우드 스트라이크와 마이크로소프트의 신속하고 효과적인 대응 및 복구 작업이 긍정적으로 평가되었다. 크라우드 스트라이크는 잘못된 업데이트가 배포된 지 17분 만에 문제를 인식하고 즉시 배포를 중단했으며, 빠르게 수정판을 준비해 배포했다[3].

마이크로소프트 역시 수백 명의 엔지니어를 고객사에 파견해 서비스 복구를 지원하며 적극적으로 대처했다. 또한, 크라우드 스트라이크와 마이크로소프트는 긴밀한 협력을 통해 확장할 수 있는 솔루션을 개발하여 문제 해결에 나섰으며, 수동 수정 작업을 위한 안내문서와 스크립트를 신속히 개발하고 배포했다[1].

그 결과, 사건 발생 5일 만인 7월 24일 기준으로 전체 영향을 받은 시스템 중 97% 이상이 정상화되는 성과를 거두었다[3]. 이러한 신속한 복구 작업은 IT 장애 발생 시 긴급 대응과 복구 체계의 중요성을 재확인시켜 주었으며, 협력과 효율적인 대응 체계가 대규모 피해를 최소화하는 데 핵심적인 역할을 한다는 중요한 교훈을 남겼다.

3) 글로벌 IT 대란이 유발한 대규모 피해와 보상 논란

이번 글로벌 IT 대란으로 인한 피해액은 전 세계적으로 약 100억 달러(한화 약 14조 원)에 달할 것으로 추산된다. 그중에서도 델타 항공은 약 5억 달러의 손해를 입은 것으로 알려졌으며, 이와 같은 여러 피해 기업이 손해 배상 소송을 제기할 것으로 예상된다. 이에 따라 대규모 피해에 대한 보상 논란이 점차 확대되고 있다[5].

그러나 크라우드 스트라이크가 고객과 체결한 계약에 면책 조항이 포함되어 있을 때, 법적으로 보호받을 가능성이 높아 실제로 감당해야 할 보상의 규모는 예상보다 적을 수 있다는 분석이 제기되고 있다. 면책 조항은 특정 상황에서 발생하는 손해에 대해 기업이 책임을 지지 않도록 규정하는 조항으로, 이 조항에 따라 크라우드 스트라이크가 피해 보상 의무에서 벗어날 가능성이 있다[7].

보험 서비스 회사 패러 매트릭스(Parametrix)는 이번 IT 대란으로 인해 포춘 500 기업들이 입은 총손실이 약 54억 달러에 이르지만, 사이버 보안 보험 정책으로 보상받을 수 있는 금액은 전체 손실의 10~20%에 불과할 것으로 전망했다. 이는 피해 기업들이 사이버 보안 보험으로 보상받을 수 있는 범위가 제한적이라는 사실을 드러내며, 대규모 IT 사고에 대비한 보험 체계의 한계를 시사한다[7].

이번 사태는 IT 대란에 따른 피해 보상의 복잡성과 보험 체계의 한계를 다시 한번 부각시켰으며, 향후 대규모 IT 사고에 대비한 보상 및 보험 체계의 개선 필요성을 강조하는 중요한 과제를 남겼다[6].

4. 글로벌 IT 대란이 한국 IT 산업에 주는 시사점

1) 사이버 공급망이 유발하는 위험성 인식

최근 몇 년간 사이버 공급망 사고는 꾸준히 증가해 왔으며, 특히 SaaS와 AI 애플리케이션의 확산으로 인해 공급업체들이 서비스 중단이나 데이터 유출의 잠재적 원인이 될 가능성이 커졌다. 그러나 한 조사에 따르면 여전히 절반 이상의 기업이 온보딩 전에 제3자 공급업체에 대한 체계적인 평가를 하지 않고 있다[6]. 이번 크라우드 스트라이크 사태를 교훈 삼아, 기업들은 외부 보안 위협뿐만 아니라 사이버 공급망에서 발생할 수 있는 내부 위험에 대한 인식을 제고할 필요가 있다.

이를 위해 신뢰할 수 있는 공급업체를 선택하는 데 더 큰 노력을 기울이고, 공급업체들이 업계 표준과 규정을 준수하도록 요구해야 한다. 또한, 다양한 기술 생태계를 구축하여 단일 실패 지점(SPOF)의 영향을 최소화하는 전략도 중요하다[8].

2) 소프트웨어 품질보증(QA) 검사 및 배표 체계 점검과 보완

크라우드 스트라이크는 이번 사태 이후, 새로운 템플릿 인스턴스에 대한 검증을 강화하고 배포 프로세스를 개선하여 단계적 배포 및 더 광범위한 수용 검사를 포함하는 방향으로 QA 절차를 업데이트했다[3]. 이를 교훈 삼아 국내 소프트웨어 기업들도 QA 및 배포 절차를 전반적으로 재검토하고 보완할 필요가 있다. 특히, 보안 관련 업데이트라도 커널처럼 시스템 핵심에 영향을 미치는 소프트웨어라면 단계적 배포 전략을 채택하고, 고객이 업데이트의 시점과 여부를 선택할 수 있도록 유연성을 부여하는 것이 바람직하다[4].

3) 복구 탄력성 강화를 위한 비즈니스 연속성 계획 수립 및 운영

아무리 완벽한 QA 체계를 갖추더라도 IT 보안 사고를 완전히 예방하는 것은 불가능하다. 따라서 예기치 못한 보안 사고가 발생했을 때 신속하게 대응하고 복구할 수 있는 복구 탄력성에 대한 기업들의 관심과 투자가 필요하다[6]. 이를 위해 백업 조치, 시스템 이중화, MacOS나 리눅스 같은 다양한 플랫폼 도입 등 여러 대책을 고려할 수 있으나, 비용 문제로 각 기업에 맞는 최적의 해결책을 찾는 것이 중요하다. 또한, 비즈니스의 핵심 기능이 사고 발생 시에도 중단되지 않도록 '비즈니스 연속성 계획(BCP)'을 수립하고 운영하여, 손실을 최소화하고 고객 신뢰를 유지하는 것이 필요하다[8].

4) 투명한 정보공개와 위기에 대응하는 현명한 리더십

이번 글로벌 IT 대란에서 크라우드 스트라이크는 투명한 정보공개와 신속한 대응으로 긍정적인 평가를 받았다. 크라우드 스트라이크의 신속한 대응 덕분에 마이크로소프트를 비롯한 여러 시장 참여자가 함께 빠르게 대처할 수 있었고, 더 큰 피해를 막을 수 있었다[1]. 특히, 크라우드 스트라이크의 CEO 조지 커츠는 사건 직후 소셜미디어를 통해 서비스 중단의 원인이 자사에 있음을 인정하고, 빠른 해결을 약속하며 사건의 원인과 대응 조치에 대해 투명하게 공개했다. 이러한 리더십 덕분에 회사 주가는 빠르게 회복세를 보였다. 크라우드 스트라이크의 위기 대처 능력과 CEO의 진정성 있는 리더십은 다른 IT 기업들에게도 중요한 교훈이 될 것이다[6].

5) 분쟁 발생을 대비한 법적, 제도적 준비

이번 글로벌 IT 대란으로 피해를 당한 기업들이 소송에 나서면서, 클라우드 기반 IT 서비스 이용 시 발생할 수 있는 문제에 대비한 법적 준비의 중요성이 주목받고 있다. 이에 대한 해법으로 서비스 수준 협약(SLA)을 체결해 서비스 제공자와 고객의 책임과 의무를 명확히 규정하는 방안이 추천된다. SLA에는 의무 위반 시 제재나 보상 방법, 재해복구 및 비상상황에 대한 대응 절차, 중요한 시스템 업데이트 전 테스트 의무화 등의 규정을 포함해야 한다. 또한, 사고 발생 시 계약에 포함된 면책 조항의 존재 여부와 그 규정 방식을 충분히 검토할 필요가 있다[8].

5. 결론 및 제언

이번 글로벌 IT 대란 속에서 국내 피해는 상대적으로 미미했다. 이는 국내 금융 및 공공 부문에 적용된 '망 분리' 등의 규제로 인해 정보 시스템이 클라우드 환경에서 분리되었기 때문이라는 분석이 있다[6]. 국내에서는 SaaS 방식으로 제공되는 크라우드 스트라이크 제품의 도입이 적었기 때문에 이번 대란의 영향을 덜 받았다[3]. 그러나 국내에서도 클라우드 확산이 계속되고 있으며, 금융과 공공 부문에서도 클라우드 도입이 가속화될 것으로 예상된다.

따라서 서비스 제공자와 고객 간 분쟁 예방 및 해결을 위한 철저한 준비가 요구된다. 이번 사태는 IT 규제를 강화하는 방향이 아니라, 사이버 공급망의 잠재적 위협을 대비하고 IT 역량을 강화하는 계기로 삼아야 할 것이다.

참고문헌

[1] Messageware. What Caused the Crowdstrike Outage: A Detailed Breakdown. Sep. 14, 2024.

[2] Polymer. Anatomy of the CrowdStrike outage: Lessons learned. Jul. 25, 2024.

[3] CrowdStrike. Preliminary Post Incident Review (PIR). Jul. 24, 2024.

[4] O'Flaherty, K. CrowdStrike reveals new details about what caused Windows outage. Forbes, Jul. 24, 2024.

[5] Evans, J. Delta CEO: Windows is the 'most fragile platform'. Computerworld, Aug. 2, 2024.

[6] 한국정보산업연합회, 안현철. FKII ISSUE BRIEF & REPORT(서울)-NO. 3. FKII, Sep. 2024.

[7] Sharma, S. Counting the cost of CrowdStrike: the bug that bit billions. CIO, Jul. 26, 2024.

[8] 구태언, 이정봉, 신호준. 2024년 크라우드스트라이크발 전산마비 사태. 법률신문, Aug. 22, 2024.