Clouflare, 양자 위협 시점에 양자 보안 대응 가속

(2026.05.11., 양자정보연구지원센터)

□ Cloudflare, 양자컴퓨터 위협 대응 위해 양자내성보안(Post-Quantum Security) 전환 가속

○ Cloudflare는 양자컴퓨터 발전 속도가 예상보다 빨라지고 있다는 연구 결과와 산업 동향을 반영해 인터넷 전반의 양자내성보안 전환 일정을 앞당기겠다고 발표함

- 회사는 2029년까지 자사 전체 서비스에 대해 완전한 양자내성보안을 구현하는 것을 목표로 제시함
- 적용 범위에는 데이터 암호화뿐 아니라 인증(authentication) 체계까지 포함됨
- 이는 기존 암호체계가 미래 양자컴퓨터에 의해 무력화될 가능성에 대비하기 위한 조치로 설명됨

○ 최근 업계에서는 **'Q-Day(양자컴퓨터가 현재 암호체계를 실제로 해독 가능한 시점)'**가 예상보다 빨리 도래할 수 있다는 우려가 확산되고 있음

- 기존에는 저장된 데이터를 미래에 복호화하는 "Harvest Now, Decrypt Later" 공격이 주요 우려였음
- 최근에는 실시간 인증 위조 및 시스템 침투 가능성이 더 심각한 위협으로 인식되기 시작함
- 이에 따라 보안 업계의 관심도 단순 암호화 보호에서 인증 체계 보호로 확대되는 추세임

□ 양자 위협 시점(Q-Day) 단축 가능성 제기

○ Google는 최근 타원곡선암호(ECC)를 공격할 수 있는 양자 알고리즘 성능이 크게 향상되었다고 발표함

- ECC는 현재 인터넷 통신 보안 전반에 광범위하게 사용되는 핵심

암호 방식임

- 구글은 구체적 알고리즘은 공개하지 않았으나 실제 구현 가능성을 입증했다고 설명함

○ 양자 스타트업 Oratomic은 RSA-2048 및 P-256과 같은 대표 암호체계를 해독하는 데 필요한 양자 자원 규모가 기존 예상보다 훨씬 적을 수 있다는 분석 결과를 공개함

- 특히 중성원자(neutral atom) 기반 양자컴퓨터 약 1만 큐비트 수준으로 P-256 암호를 공격할 가능성을 제시함

- 이는 업계 예상보다 낮은 수치로 평가되며 큰 관심을 끌고 있음

○ 클라우드플레어는 이러한 연구 결과들이 실제 양자 공격 가능 시점을 예상보다 앞당길 수 있다고 분석함

- 양자 하드웨어・오류보정・양자 알고리즘이 동시에 발전하면서 기술 격차가 빠르게 줄어들고 있다는 평가임

- 특정 분야의 진전이 다른 분야 성능 향상까지 가속시키는 구조가 형성되고 있다고 설명함

□ **양자컴퓨터 핵심 기술 발전 동향**

○ 하드웨어 분야에서는 초전도 큐비트, 중성원자, 이온트랩, 광자 기반 기술 등 다양한 방식이 동시에 발전 중임

- 아직 실질적 암호 해독 수준에는 도달하지 못했으나 수년 전 대비 성능이 크게 향상된 상태임

○ 오류보정(error correction) 기술도 빠르게 발전하고 있음

- 기존에는 안정적인 논리 큐비트 1개 구현에 수백~수천 개 물리 큐비트가 필요했음

- 최근 중성원자 기반 재구성형 구조 등 새로운 방식이 필요한 자원 규모를 줄일 가능성이 제기됨

○ 양자 알고리즘 분야에서도 암호 해독 효율 향상이 진행 중임

- 동일한 계산 능력으로 더 적은 자원만으로 암호를 공격할 수 있는

방향으로 발전하고 있음

- 이에 따라 예상보다 작은 규모 양자컴퓨터로도 실질적 위협이 가능할 수 있다는 우려가 커지고 있음

□ 암호화보다 인증(Authentication) 위협이 더 심각

○ 클라우드플레어는 현재 가장 심각한 위험 요소로 인증 체계 붕괴 가능성을 지목함

- 양자컴퓨터가 디지털 서명을 위조하거나 신뢰 시스템을 사칭할 경우 보안 체계를 직접 우회할 수 있음

- 이는 단순 데이터 유출을 넘어 실시간 시스템 장악으로 이어질 가능성 있음

○ 공격 대상에는 다음과 같은 장기 인증 자산이 포함될 가능성이 큼

- 루트 인증서(root certificates)

- API 인증키(credentials)

- 코드 서명 키(code-signing keys)

- 네트워크 접근 인증 체계 등

○ 인증 체계가 손상될 경우

- 소프트웨어 업데이트 위조

- 네트워크 무단 접근

- 중요 인프라 통제권 탈취

- 장기간 은닉 침투 등 심각한 보안 사고 가능성이 제기됨

□ 초기 양자 공격은 고가치 목표 중심 예상

○ 클라우드플레어는 초기 양자 공격이 광범위한 인터넷 공격보다는 고가치 목표(high-value targets)에 집중될 가능성이 높다고 전망함

- 초기 양자컴퓨터는 비용이 매우 높고 제한적으로 운영될 가능성이 크기 때문임

- 국가기관, 대형 클라우드, 금융기관, 핵심 인프라 등이 우선 표적이 될 가능성이 제기됨

○ 시간이 지나 양자 하드웨어가 상용화·대형화될 경우

- 공격 범위가 일반 기업과 대중 서비스 영역까지 확대될 가능성이 있음

□ 클라우드플레어 양자내성보안 전환 일정

○ 클라우드플레어는 단계별 양자내성보안 전환 계획을 제시함

- 2026년 중반: 자사 네트워크와 원본 서버(origin server) 간 양자내성 인증 도입
- 2027년: 사용자와 클라우드플레어 네트워크 간 인증 체계 확대
- 2028년: 기업용 네트워크 제품군까지 적용 확대
- 2029년: 전체 서비스에 대한 완전한 양자내성보안 구현 목표

○ 회사는 고객 별도 설정 없이 기본값(default) 형태로 양자내성보안을 적용하겠다는 방침도 제시함

- 인터넷 전반의 기본 보안 수준을 높이는 전략의 일환으로 설명됨

□ 산업 및 정책적 시사점

○ 클라우드플레어는 기업과 정부 모두 양자보안 전환 준비를 서둘러야 한다고 강조함

- 기업에는 공급망 및 벤더의 양자내성 지원 여부 점검 필요성을 제기함
- 중요 시스템과 장기 인증키부터 우선 교체할 것을 권고함

○ 정부 차원에서는 **표준화 일정 조율, 국제 협력 강화, 인증 체계 전환 가이드라인 마련** 필요성이 강조됨

○ 클라우드플레어는 “양자컴퓨터가 기존 암호체계를 위협할 것인가”가 아니라 “언제 실제 공격이 가능해질 것인가”가 핵심 문제라고 평가함

- 특히 인증 체계 공격은 데이터 복호화보다 훨씬 직접적이고 치명적인 위험이 될 수 있다고 경고함

(원문)

1. https://thequantuminsider.com/2026/04/08/cloudflare-accelerates-quantum-security-push-as-new-research-shrinks-timeline/