미국은 지금

트럼프의 양자컴퓨터 베팅(Feat, 행정명령)

키움증권 리서치센터 글로벌리서치팀
US Strategy Analyst 김승혁

Issue Brief

두 가지를 서명한 양자 행정명령

6 월 22 일 트럼프 대통령은 양자 행정명령 두 건에 서명했다. 하나는 실효성 있는 양자컴퓨터를 가장 먼저 확보하라는 것이고, 나머지는 양자 컴퓨터가 기존 암호를 무력화하기 전에 정부 전체의 암호 체계를 교체하라는 것이다. 2018 년부터 양자 우위를 목표로 삼은 미국에 대한 중국의 추격이 빨라졌고, 암호 데이터만을 미리 탈취 후, 양자컴퓨터 완성 뒤(암호 해제 능력 획득) 미리 탈취한 암호를 복호화하는 시도가 현실이 된 점이 행정명령 배경이다. 더 빨리 만들면서, 만들어지기 전에 막아야 하는 두 과제가 동시에 발생했다. 행정명령은 양자컴퓨터 1 대(2028 년) 도입과 기존 암호체계 전환(2030~2031 년) 일정을 기존 2035 년 목표보다 4 년 앞당겼다.

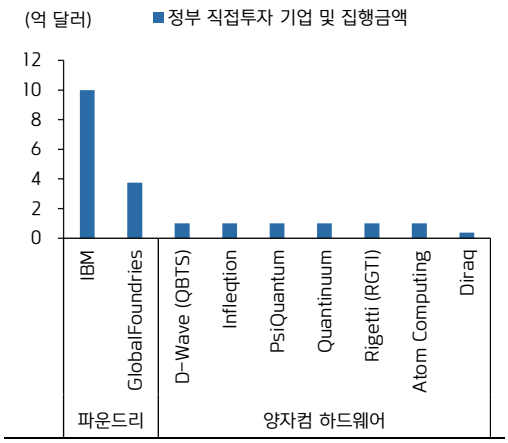
두 갈래 수혜 산업: 하드웨어와 보안

행정명령이 두 과제를 동시에 담은 만큼, 영향을 받는 산업도 두 갈래로 나뉜다. 첫째는 양자컴퓨터를 직접 만드는 하드웨어 산업이다. 아직 어떤 방식이 우위일지 정해지지 않아 중성원자·초전도·광자·트랩이온 등 서로 다른 기술 경로가 경쟁중이다. 상장사로는 D-Wave·Rigetti·Infleqtion 등이 핵심 부품을 담당하고, IBM·GlobalFoundries 등이 파운드리를 담당한다. 둘째는 양자컴퓨터로도 풀 수 없는 새 암호(양자내성암호, PQC)를 만들고 갈아끼우는 보안 산업이다. 정부와 그 납품 기업의 암호 체계를 통째로 교체하는 일로, 새 암호를 칩에 미리 심는 반도체 기업(Lattice 등)과 전환 작업을 대행하는 전문업체가 여기에 속한다. 만들 컴퓨터는 불확실해도 지킬 데이터는 분명하기에, 해당 수요는 2030~2031 년 시한까지 발생한다.

양자내성암호 산업의 상대적 우위

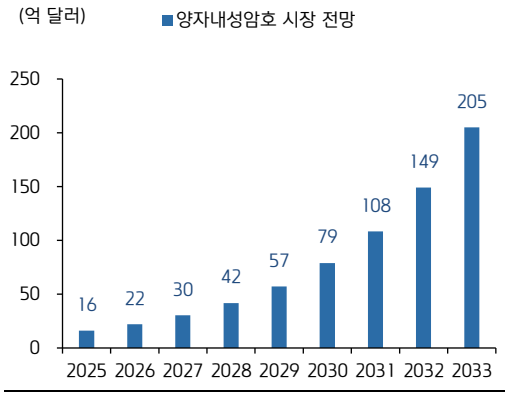
두 산업은 같은 명령에서 출발하지만 성격은 다르다. 하드웨어 산업은 '양자컴퓨터 실용성'이 중요하며 성공 보상이 크지만 그 시점이 불확실해, 투자심리에 민감하게 반응한다. 반면 양자 보안 산업 수요는 기술의 성공이 아니라 정해진 전환 시한에서 나온다. 양자컴퓨터가 언제 완성되든, 위협이 존재한다는 사실만으로 교체 작업이 일정에 따라 진행되기 때문에 수익 가시성이 높다. 기존 2035 년 전환 기한이 4 년이 앞당겨진 것은 양자 보안 산업으로의 현금 유입 시점 역시 빨라졌음을 뜻한다. 이번 양자 행정명령 수혜 산업은 '양자 하드웨어' 보다 '양자 보안'산업이라 판단하는 이유다.

정부 양자 생태계 직접투자 개사



자료: 미국 상무부, 키움증권 리서치

양자내성암호(PQC) 시장 전망



자료: Grand View Research, 키움증권 리서치

공격과 수비, 한날 발표된 두 명령

2026 년 6 월 22 일 트럼프 대통령이 양자 관련 행정명령 두 건에 서명했다. 하나는 미국이 실효성 있는 양자컴퓨터를 가장 먼저 확보하란 명령이며(공격), 다른 하나는 양자컴퓨터가 기존 암호를 무력화하기 전에 정부 전체의 암호 체계를 교체하겠다는 방어 조치(수비)다. 같은 기술을 두고 추진과 방어를 동시에 명문화한 점이 이번 서명의 성격을 규정한다.

배경은 두 가지다. 첫째는 국가 간 경쟁 구도다. 미국은 2018 년부터 양자 우위를 정책 목표로 삼아왔으나 중국을 비롯한 후발국의 추격 속도가 빨라졌고, 이번 명령은 그 격차를 다시 벌리려는 의지의 표현이다. 둘째는 "지금 훔쳐 나중에 푼다(Harvest Now, Decrypt Later)"는 위협이다. 공격자가 현재 해독 불가능한 암호화 데이터를 미리 탈취해 저장해두었다가 양자컴퓨터 완성 시점에 일괄 복호화하는 방식이다. 양자컴퓨터가 아직 없다는 사실이 대응을 미룰 근거가 되지 못하는 이유다. 오늘 암호를 교체해야 오늘 유출되는 데이터를 보호할 수 있다. 두 명령이 같은 날 묶여 나온 배경이다.

행정명령의 세 가지 함의

이번 조치의 의미는 셋이다. 첫째, 양자 기술이 정부 차원의 우선 기술로 공식 지정되면서 연구개발 자원이 이 분야로 유입될 통로가 열렸다. 둘째, 추상적 목표가 아니라 시점이 명시됐다. 양자컴퓨터는 2028 년까지 에너지부 산하 국립연구소에 실사용 가능한 1 대 구축(QC-ADDS), 양자내성암호(PQC, 양자컴퓨터로도 풀기 어려운 차세대 암호)는 키 교환 방식 2030 년 말, 전자서명 방식 2031 년 말까지 정부 전반 전환을 못 박았다. 기존 2035 년 목표를 4 년 앞당긴 것으로, 시급성을 압박하는 신호다. 셋째, 단서 조항이다. 두 명령 모두 실제 자금 집행은 의회 예산 배정에 달려 있다. 서명이 곧 자금 확정은 아니며, 방향과 일정만 제시한 단계다. 관건은 약속된 예산이 실제로, 어느 기업으로 흘러가는지다.

상무부의 20 억 달러 직접투자

주목할 점은 자금의 실체가 6 월 22 일 명령이 아니라 한 달 앞선 5 월 상무부 발표에 있었다는 사실이다. 상무부는 양자 기업 9 곳에 약 20 억 달러를 지원하되, 단순 보조가 아니라 지분을 취득하는 방식을 택했다. 미국 정부의 양자 분야 역대 최대 직접투자다. 발표 당일 관련주는 D-Wave(QBTS) +33.4%, Rigetti(RGTI) +30.6%, Infleqtion(INFQ) +31.5% 급등했고, 명단에 없던 IonQ(IONQ)도 12.2% 상승했다.

자금은 두 갈래로 나뉜다. 먼저 파운드리(반도체 위탁생산) 부문 2 곳이다. 양자 핵심 부품을 미국 내에서 생산하는 인프라 역할로, IBM 이 최대 규모인 10 억 달러를 받아 신설 법인 'Anderon'을 통해 뉴욕 올버니에 초전도 웨이퍼 공장을 짓고 정부 지원금과 동일 규모를 자체 매칭하기로 했다. GlobalFoundries 는 3 억 7,500 만 달러로 다양한 양자 칩을 생산하는 보안 라인을 미국 안에 구축한다. 설비 투자 성격이라 상대적으로 안정적인 대형사들이다.

정부는 한 방식에 집중하지 않고 중성원자·초전도·광자·트랩이온·실리콘 스핀 등 서로 다른 기술 경로에 자금을 분산했다. 양자컴퓨터 하드웨어 7 곳에 분산 투자가 진행된 이유다. 우위 방식이 확정되지 않은 상황에서 위험을 나눈 셈이다.

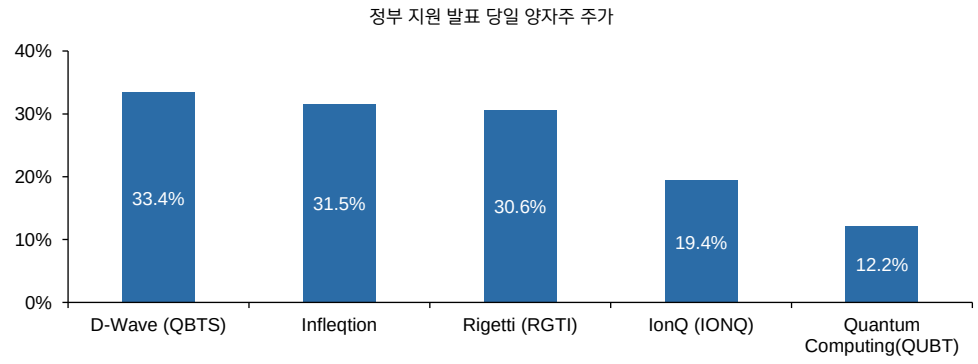
상무부 양자 지원 9 개사 (2026 년 5 월)

기업	지원액(억$)	기술·역할	상장 여부
IBM	10.0	파운드리·초전도 웨이퍼	상장 (IBM)
GlobalFoundries	3.75	파운드리·보안 국산 라인	상장 (GFS)
Atom Computing	1.0	중성원자	비상장
Diraq	~0.38	실리콘 스핀	비상장
D-Wave	1.0	초전도·어닐링	상장 (QBTS)
Infleqtion	1.0	중성원자	상장 (INFQ)
PsiQuantum	1.0	광자	비상장
Quantinuum	1.0	트랩이온	비상장 (Honeywell)
Rigetti	~1.0	초전도	상장 (RGTI)

자료: 미국 상무부(2026 년 5 월) 주)'~'는 최대 한도.

투자 관점에서 핵심은 희소성이다. 이 7 곳 중 증시에서 직접 매매 가능한 순수 양자주는 D-Wave(QBTS), Rigetti(RGTI), Infleqtion(INFQ)이다. 나머지(Atom, Diraq, PsiQuantum, Quantinuum)는 비상장이거나 대형사 산하다. 정부 수혜 익스포저를 원하는 자금이 소수 상장사로 집중되는 구조다. IonQ 와 QUBT 는 지원 명단에 없었으나 주가는 동반 상승했다. 정부가 양자 섹터 전반을 부양한다는 기대가 테마 전체를 끌어올린 결과다. 6 월 22 일 명령 당일에도 IonQ, Quantum Computing(QUBT), IBM 이 시간외에서 4~6% 상승했다.

발표 당일 순수 양자주 급등 (2026.5)



자료: Bloomberg, 키움증권 리서치

암호 전환의 구조

암호 보안 산업 측 수혜를 짚으려면 두 번째 명령이 강제한 전환 구조를 먼저 볼 필요가 있다. 앞서 키 교환은 2030 년 말, 전자서명은 2031 년 말로 시한이 갈렸는데, 이 차이가 수요의 성격을 결정한다. 암호는 성격이 다른 두 가지 기능을 수행한다. 하나는 통신 내용을 잠가 제 3 자의 도청을 막는 일이고, 다른 하나는 송신자가 누구인지, 전송 중 내용이 변조되지 않았는지 확인하는 일이다. 둘은 별개의 기능이므로 전환 시한도 따로 정해졌다.

키 교환(key establishment)은 도청이 가능한 공개 회선에서 두 당사자가 동일한 비밀 값(열쇠)을 만들어내는 방식이다. 원리는 단방향 연산에 있다. 두 값을 결합하는 계산은 빠르지만, 결합된 결과만 보고 원래 두 값을 역산하는 것은 사실상 불가능하다는 성질이다. 두 당사자는 먼저 공개된 기준값을 공유한다. 이 값은 도청자도 안다. 그다음 각자 공개하지 않는 비밀 값을 정하고, 공개 기준값에 자신의 비밀 값을 결합한 중간 결과를 회선으로 주고받는다. 도청자는 두 중간 결과를 모두 확보하지만, 단방향 연산이라 거기서 비밀 값을 끄집어내지 못한다. 마지막으로 각자 상대가 보낸 중간 결과에 자신의 비밀 값을 한 번 더 결합하면 양쪽 모두 동일한 최종 값에 도달한다. 이 값이 둘만 공유하는 열쇠다. 현재 이 단방향 성질은 이산대수 문제의 난이도에 의존하며, 일반 컴퓨터로는 역산에 수천 년이 걸려 안전이 성립했다. 문제는 양자컴퓨터가 이 역산을 단시간에 수행한다는 점이다. 역산이 가능해지는 순간 도청자는 중간 결과에서 비밀 값을 복원해 통신을 해독한다.

전자서명(digital signature)은 발신 주체를 증명하고 위변조 여부를 검증하는 장치다. 서명은 발신자만 생성할 수 있고 검증은 누구나 할 수 있다. 웹사이트가 진짜 해당 기관의 것인지, 업데이트 파일이 실제 제작사에서 나온 것인지 확인하는 절차가 모두 여기에 해당한다. 이 역시 풀기 어려운 수학 문제 위에서 작동하며, 양자컴퓨터가 그 문제를 풀면 서명 위조가 가능해진다.

마감이 갈린 핵심은 "지금 훔쳐 나중에 푼다" 위협이 두 기능에 다르게 작용한다는 데 있다. 키 교환으로 잠근 데이터는 공격자가 오늘 통째로 탈취해 저장해두었다가 양자컴퓨터 완성 이후 일괄 해독할 수 있다. 오늘 보낸 통신이 수년 뒤 노출될 수 있다는 의미이므로, 잠그는 쪽이 시급하다. 반면 전자서명을 위조하려면 그 문서가 오가는 시점에 이미 양자컴퓨터가 있어야 한다. 과거에 받은 정상 서명을 사후에 위조본으로 바꿀 수는 없으며, 검증은 그 순간에 끝난다. 서명에는 "지금 훔쳐 나중에 푼다"가 통하지 않고 양자컴퓨터가 실제로 구현되는 시점까지만 버티면 되므로, 시한을 1 년 늦춘 것이다.

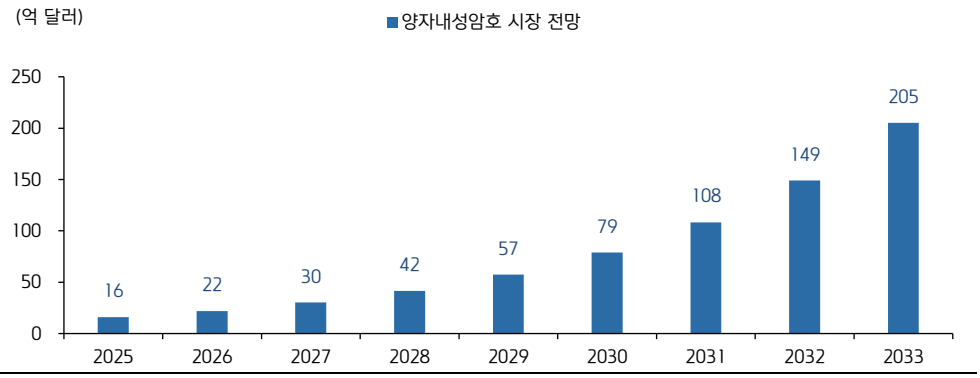
대체 표준은 미국 국립표준기술연구소(NIST)가 양자컴퓨터로도 풀기 어려운 격자(lattice) 기반 문제 위에 설계했다. 키 교환용은 ML-KEM(FIPS 203), 전자서명용은 ML-DSA 와 SLH-DSA(FIPS 204·205)다. 소인수분해 같은 기존 난제를 격자 문제로 교체한 것이 핵심이다. 여기에 더해 주목할 개념이 크립토 어질리티(crypto-agility), 즉 암호 체계를 통째로 교체하기 쉽게 설계해두는 구조다. 지금 도입하는 표준이 다시 취약해질 경우 다음 표준으로 신속히 전환해야 하므로, 최근 반도체·보안 기업은 교체 용이성을 갖춘 제품을 전면에 내세운다.

PQC 반도체에 대하여

이처럼 두 갈래 전환이 시한과 함께 의무화되면서, 수혜는 양자컴퓨터 제조사가 아니라 신규 암호를 만들고 교체를 수행하는 산업으로 돌아간다. 정부가 2030~2031 년 전환을 의무화하고 납품 기업에까지 적용을 강제했기 때문에 향후 수년간 일감이 순차적으로 발생한다. 하드웨어 진영보다 수익 가시성이 높다고 보는 시각이 우세한 이유다.

PQC 를 칩에 내장해 판매하는 반도체 기업으로는 Lattice Semiconductor(LSCC)가 대표적이다. 관련 기능 칩을 업계에서 선제 출시했고 시장은 2026 년 이익이 전년 대비 40%가량 증가할 것으로 기대하고 있다. 앞서 언급한 크립토 어질리티를 구현한 칩을 공급하는 기업이기도 하다. Microchip(MCHP), STMicroelectronics(STM)도 자사 칩에 PQC 를 선탑재하는 작업을 진행 중이다. 상위 시장은 NXP, Thales, AWS, Palo Alto Networks(PANW), IDEMIA 등 대형사가 절반 이상을 점유한다. 전환 작업에 특화된 전문업체로는 PQShield, CryptoNext, DigiCert, Fortanix, QuSecure 등이 있으나 상당수가 비상장이다. TAM 은 2025 년 약 16 억 달러에서 2033 년 약 205 억 달러로 연평균 38% 성장을 시장은 예상하고 있다.

양자내성암호(PQC) 시장 전망 (2025-2033)

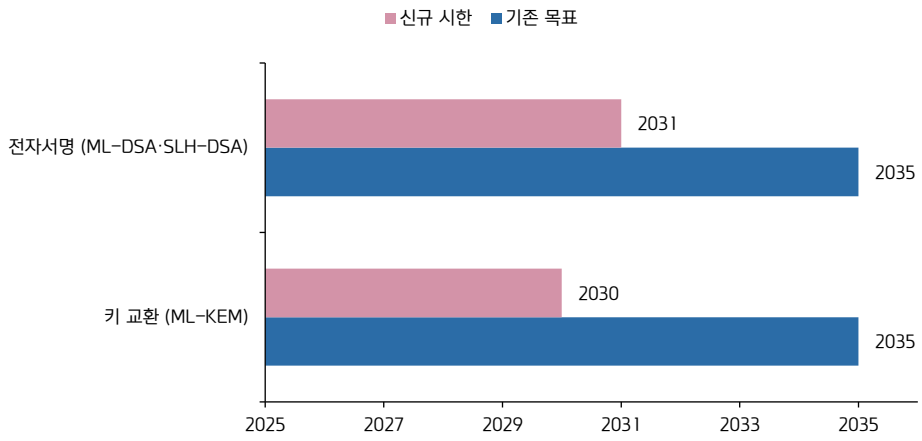


자료: Grand View Research, 키움증권 리서치

결론: 기대감 vs 안정감

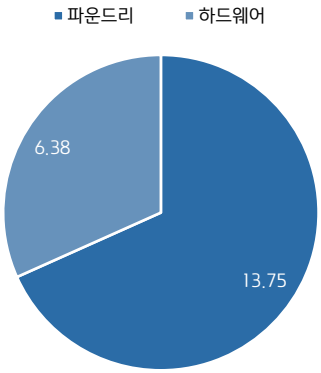
같은 양자 테마라도 두 진영의 성격은 다르다. 양자컴퓨터 제조 부문은(IonQ, Rigetti, D-Wave 등) 잠재력은 크나 상용화 성공 여부가 미확정인 산업으로, 호재에 급등하고 악재에 급락한다. 반면 암호 전환 기업은 정부의 정해진 마감 일정이 수요를 고정시켜 상대적으로 안정적이다. 양자 관련 뉴스에 따른 대응 전략이 양자컴퓨터 자체인지 암호 전환 산업인지 구분해서 접근해야 하는 이유다. 이번 2028 년까지 양자컴퓨터 패치를 명령한 것과 자금 지원이 진행되고 있다는 점은 물론 양자컴퓨터 하드웨어 산업에 긍정적이지만, 성공 여부가 불투명하다. 반대로 양자내성암호 전환은 강제적이며 상대적으로 불투명성이 적다. 2030 년 일정 확정이 수익 가시성을 높였고, 정부와 계약한 관련 기업들에게 이를 강제하고 있다는 점 역시 고정 수요를 창출한다. 이번 행정명령이 양자 산업 전반적으로 긍정적 영향을 주겠으나, 양자내성암호 산업의 상대적 장기 수혜가 예상되는 이유다.

정부 암호 전환 시한



자료: White House, 키움증권 리서치

파운드리(부품), 하드웨어(완성품 제작) 산업별 정부 지원금



자료: 상무부, 키움증권 리서치, 주) 단위는 억 달러

Compliance Notice

- 당사는 동 자료를 기관투자자 또는 제 3 자에게 사전 제공한 사실이 없습니다.
- 동 자료에 게시된 내용들은 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭없이 작성되었음을 확인합니다.

고지사항