

digicert®

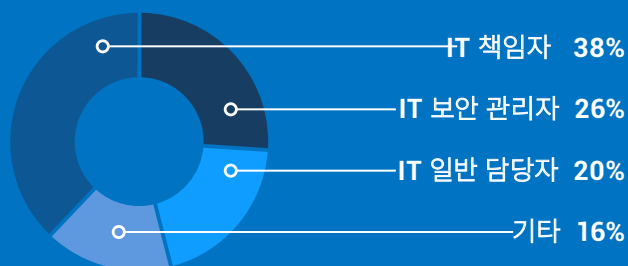
# 양자 컴퓨팅에 대한 기대와 위험성 2019 DIGICERT 양자내성암호(PQC) 조사 보고서

## 방법론

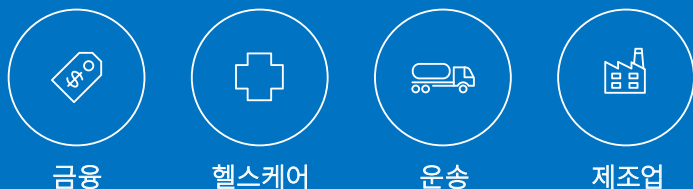
DigiCert는 텍사스주 댈러스에 위치한 ReRez 리서치에 의뢰하여 미국, 독일, 일본의 400여 개 기업의 1,000여 명 이상의 IT 전문가를 대상으로 설문 조사를 진행했습니다.



응답자는 IT 책임자, IT 보안 관리자 및 일반 담당자로 구성되었습니다.



설문 조사는 4가지 핵심 산업에 중점을 두었습니다.



## 양자 컴퓨팅에 대한 기대와 위험성

IBM에서는 2019년 1월 세계 최초로 회로 기반 상업용 양자 컴퓨터인 IBM Q 시스템을 발표했습니다. 양자 컴퓨터의 상업적 접근성은 아직 요원함에도 불구하고 많은 사람들은 양자 컴퓨팅이 기존의 디지털 컴퓨터가 해결하기에 너무 어려운 문제를 쉽게 해결할 것으로 기대하고 있습니다. 머신 러닝, 의학, 입자 물리학은 양자 컴퓨팅에 의해 획기적으로 변화할 것으로 예상되는 주요 분야입니다.

하지만 양자 컴퓨팅의 전망이 밝지만은 않습니다. 미국표준기술연구소(NIST) 및 많은 전문가들은 미래의 양자 컴퓨팅이, 아마도 다음 10년 이내에 현재의 정교한 암호화 알고리즘을 무효화하고 심각한 보안 문제를 유발할 것이라고 예측하고 있습니다.

그 전에, 업계는 양자 컴퓨팅 위협에 대응할 수 있는 새로운 암호화 알고리즘을 개발해야 합니다. 이러한 알고리즘은 양자내성암호(Post Quantum Cryptography, PQC)라고 불립니다. 하지만 PQC가 완전한 해결책은 아닙니다.

IoT를 예로 들어봅시다. PQC는 양자 컴퓨팅의 공격을 방어할 수 있는 알고리즘을 설명하기 위해 업계가 사용하는 용어입니다. 하지만 라이프 사이클이 긴 IoT 장비와 애플리케이션을 이용하는 기업들의 경우, 최초의 양자 컴퓨터로 위협이 발생한 후에도 이 제품을 계속 운영할 수 있어, 한때 안전했던 제품들이 골칫거리가 될 수도 있습니다. 센서, 내장 컴퓨터, 인터넷 연결을 사용하는 자동차의 경우를 예로 들어봅시다. 오늘날 이러한 장비/제품을 제조할 때 양자 컴퓨팅으로부터 안전한 전략을 세우지 않는다면, 미래에 문제가 생길 수 있습니다.

완전하게 제품을 보호하기 위해 기업들은 지금 바로 양자 컴퓨팅 위협에 대해 논의해야 합니다. 하지만 어떻게 대비할 수 있을까요? 그리고 무엇을 해야 할까요? 기업은 PQC에 대해 얼마나 알고 있을까요?

웹사이트, 기업 애플리케이션, IoT를 위한 TLS/SSL 및 기타 디지털 인증서를 제공하는 글로벌 선도기업인 DigiCert에서는 이러한 질문과 더불어 PQC에 대한 의문점을 분석하기 위해 2019년 PQC 설문 조사를 진행했습니다. 그 결과는 업계가 즉각적인 행동에 나설 것을 촉구하고 있습니다.



# PQC에 대한 넓은 인식과 초기 혼란

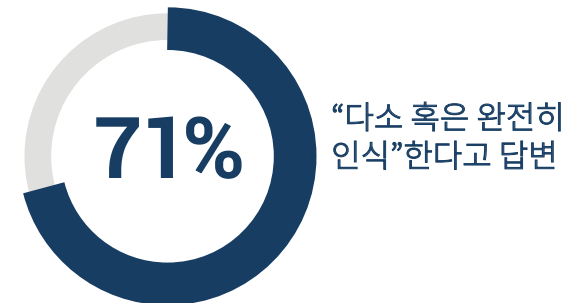
기업의 IT 관계자들은 PQC라는 용어에 친숙합니다. 이 용어를 물어보았을 때, 70%는 PQC에 대해 “다소” 혹은 “완전히” 인식하고 있지만 이는 전부가 아닙니다. 이 질문에 이어 PQC가 정확히 어떤 의미인지 확인하기 위한 질문을 제시했습니다. 3분의 2 이하가 정확한 정의를 파악하고 있었습니다.

심지어 59%의 응답자가 현재 하이브리드(PQC + RSA/ECC) 인증서를 배포하고 있다고 답변했는데, PQC 인증서는 초기 테스트 상황에 한정해 이용할 수 있기 때문에 이는 가능성이 낮다고 볼 수 있습니다.

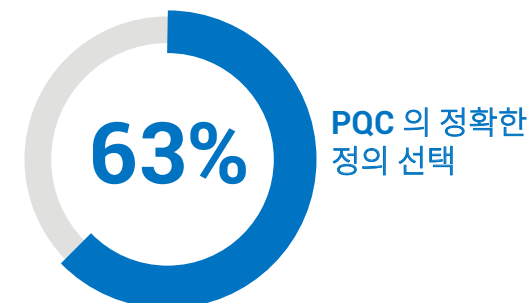
PQC는 신기술이며 사람들이 아직 그 의미와 대응법을 익히는 중이기에 이는 놀라운 일이 아닙니다. 이는 50%가 넘는 사람들이 “폭풍우가 몰아치는 날씨가” “클라우드 컴퓨팅”<sup>1</sup>에 영향을 줄 것이라고 믿었던 2012년의 한 조사결과와 유사합니다. 명백한 혼란이 있었음에도 사람들이 클라우드 컴퓨팅을 인식하고 있었고 그 혼란은 오래 지속되지 않았습니다. 오늘날 전 세계의 클라우드 컴퓨팅 시장은 2천 140억 달러 규모입니다.

많은 사람들이 양자 컴퓨팅을 염두에 두고 있으며, 양자 컴퓨팅이 기존 및 미래의 사고에 영향을 미치고 있다는 점은 분명합니다. 이 연구는 더 나아가 보안 전문가가 암호화에 있어 양자 컴퓨팅 위협에 어떻게 대응할 계획인지를 살펴봅니다

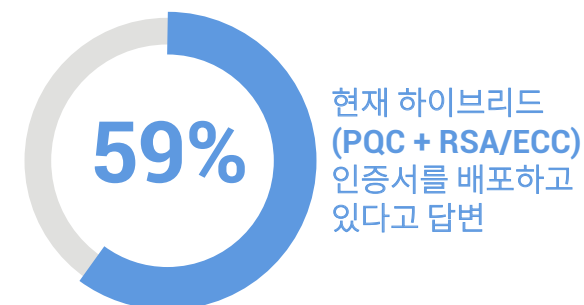
한 금융 서비스 기업의 IT 보안 관리자는, “영향을 받는 것은 우리만이 아니기에 아직은 초기 논의 단계에 있습니다. 사전 대책을 취하고 보안을 강화하는 방법에 대해 협력사 및 공급 업체와 논의하고 있습니다. 그리고 저희가 검토하는 주제 중 하나가 양자 암호화입니다” 라고 말했습니다.



그러나...



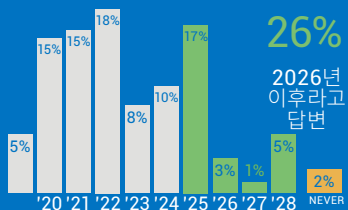
그리고...



1. 51%의 사람들이 폭풍우가 몰아치는 날씨가 ‘클라우드 컴퓨팅’에 영향을 준다고 생각 - 비즈니스 인사이더, 2012년 8월 30일

## 시기

양자 컴퓨팅은 언제쯤 기존의 암호화 알고리즘을 깰 정도로 발전할까요?



거의 모든 사람이 위험이 현실이 되었을 때 여전히 회사에서 일하고 있을 것이라고 느끼고 있음

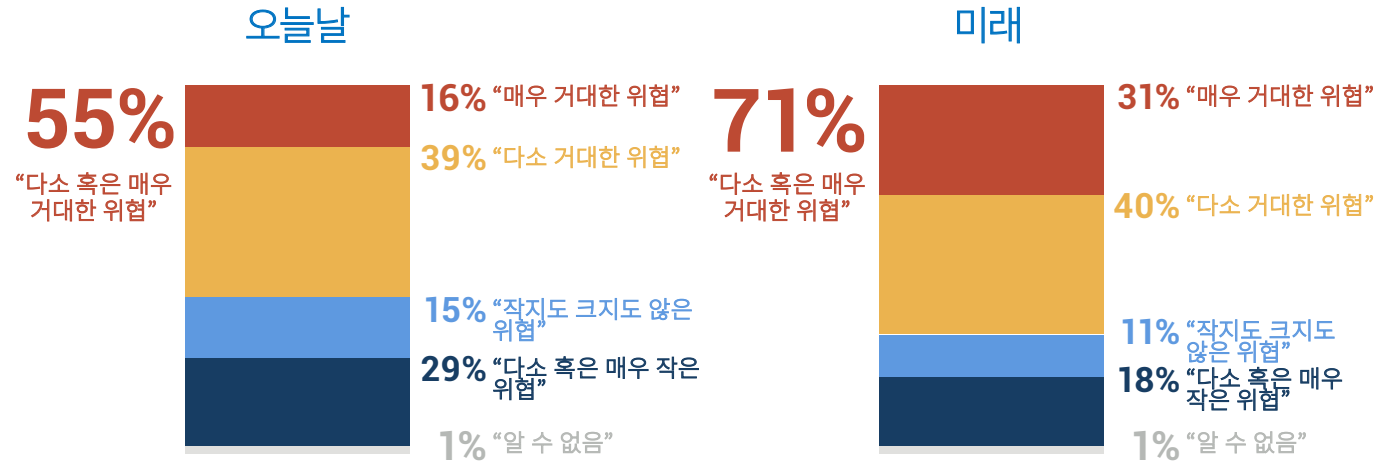
80%



IT 업계에서 양자 컴퓨팅으로부터 안전한 보안 관행을 익히는 것이 다소 혹은 매우 중요하다고 답변

# 양자 컴퓨팅 위협은 현실이며 빠르게 다가오고 있습니다

혼란에도 불구하고 IT 업계에서는 양자 컴퓨팅이 암호화에 미치는 위협을 명확하게 인식하고 있습니다. 절반이 약간 넘는 사람들(55%)이 양자 컴퓨팅이 오늘날 "다소" 혹은 "매우" 거대한 보안 위협이라고 말하고 있으며 응답자의 71%는 이것이 미래에 "다소" 혹은 "매우" 거대한 위협이 될 것이라고 말합니다.

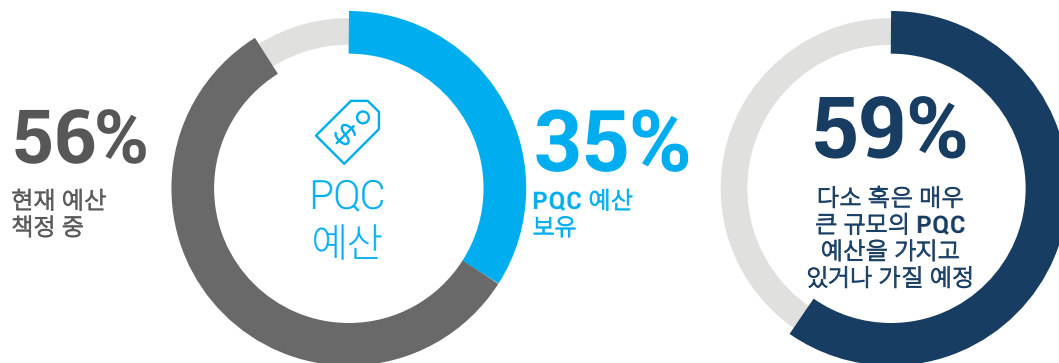


PQC에 대해서 IT 관계자들은 정확히, 언제 그 미래가 올 것으로 생각하고 있을까요? 그리 멀지 않은 것으로 보입니다. 양자 컴퓨팅에 의한 보안 위협에 맞서 싸우기 위해 PQC가 필요한 시기는 대략 2022년으로 전망됩니다. 4분의 1의 사람들(26%)이 PQC를 이용하게 되려면 2025년 만이후가 될 것이라고 말합니다.

위협이 매우 분명하게 느껴지고 그 시기가 빠르게 다가옴에 따라, 대부분(83%)의 응답자는 양자 컴퓨팅에서 안전한 보안 대응 수칙을 익히는 것은 IT 업계에 매우 중요하다고 말합니다. PQC를 익히는 것 외에도 IT 업계는 무엇을 준비하고 있을까요?

# PQC를 위한 준비






기업의 33%가 PQC 예산을 책정했고 나머지 56%는 해당 예산 책정을 위한 관련 업무에 착수하면서, 기업들은 PQC에 대비하기 시작했습니다. 상당수의 기업(59%)은 PQC 예산이 “다소 혹은 매우” 크다고 말하고 있습니다. 이 자금은 컨설턴트, 제품, 직원으로 나뉩니다.



구체적인 활동 측면에서 현 IT 종사자들의 1순위 전략은 “모니터링”이었습니다. 기업의 암호화 민첩성 수준을 이해하는 것은 그 다음 문제입니다. 이는 PQC 인증으로 전환해야 할 때가 다가오면 기업이 빠르고 효율적으로 전환할 수 있도록 준비가 되어 있어야 함을 보여줍니다.

기존 IT 전략의 상위 다섯 가지 중에는 기업의 기존 리스크 수준 이해하기, PQC 지식 강화하기, TLS 모범 사례 개발하기 등의 목표가 포함되어 있습니다.

## 상위 다섯 가지 완화 전략

-  **1** **모니터링**
-  **2** **암호화 민첩성**  
암호화 민첩성 수준 파악하기
-  **3** **리스크**  
조직의 현재 리스크 수준과 감당할 수 있는 리스크 수준 파악하기
-  **4** **지식 강화**  
PQC 및 그 영향에 대한 지식 강화하기
-  **5** **모범 사례**  
조직 내부에서 TLS 모범사례 개발하기

# 양자 컴퓨팅과의 전투

IT 업계는 양자 컴퓨팅으로 인한 암호화 리스크를 명확히 파악하고 있습니다. 우선, IT 업계에서는 미래의 양자 컴퓨팅 위협/공격에 맞서 싸우는 비용이 통제 가능한 범위를 넘어서게 될 것을 우려합니다. 두 번째로, 현재 기준으로 안전하게 암호화된 데이터가 미래의 양자 시대에는 쉽게 해독될 것을 우려합니다. 이는 오늘날 도난당한 데이터가 지금은 안전할지 몰라도 양자 컴퓨팅이 도래하면 취약해질 수 있음을 의미합니다.

이 문제는 IoT 장비에서도 유사하게 발생합니다. 최고의 암호화 기술이 적용되었다는 것은 현재의 공격에서 안전하다는 뜻이지, 미래의 양자 공격에는 취약할 수 있습니다. 자동차나 ATM 기기와 같이 오래 사용되는 제품에는 이것이 큰 문제가 될 수 있습니다.

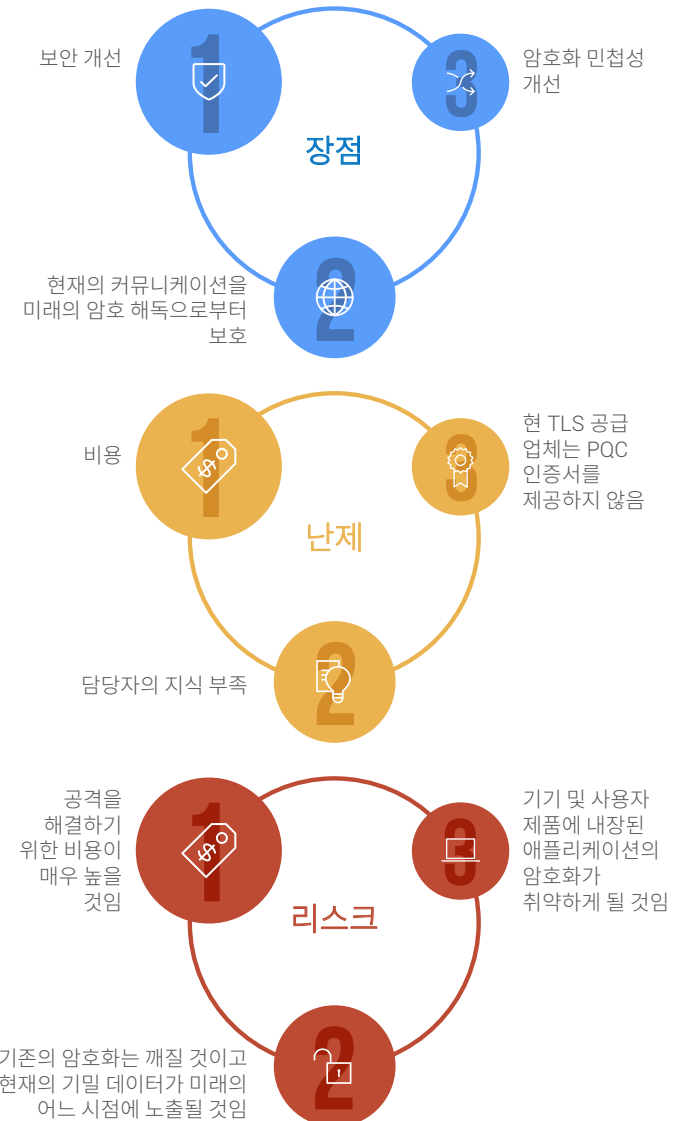
따라서, IT 업계에서는 양자 컴퓨팅 전투에 집중하고 있습니다. 그 이유는 무엇일까요? 이 전투에서 이김으로써 얻게될 혜택으로는 기업의 보안 개선, 현재의 커뮤니케이션을 미래에 발생할 암호 해독으로부터 보호, 그리고 마지막으로 암호화 민첩성 개선이 있습니다.

암호화 민첩성은 암호화의 세계가 미래에 빠르게 변화하며 기업은 네트워크를 그대로 유지하면서 빠르게 낡은 알고리즘을 새로운 알고리즘으로 바꿀 수 있어야 한다는 전략적인 입장입니다.

이러한 혜택을 위해서라면 노력할 가치가 충분하지만, 양자 컴퓨팅 전투에서 IT 업계가 우려하는 난제가 존재합니다. 응답자들에 따르면, 가장 큰 문제는 비용입니다. 이는 담당자의 양자 컴퓨팅 공격 및 대응법에 대한 일반적인 지식 부족으로 악화됩니다. 결국, 기존의 TLS 공급 업체가 적시에 충분한 PQC 인증서를 적시에 제공하지 못할 것이라는 일반적인 우려가 생겨납니다.

모든 것을 감안할 때, IT 업계는 그들이 맞닥뜨린 문제에 있어 현실적인 입장을 취합니다. 사실 거의 5분의 2의 응답자가 양자 컴퓨팅 공격에 맞서 보호하기 위해 암호화를 업그레이드하는 것이 다소 혹은 매우 어려울 것이라고 응답했습니다.

의료 서비스 기업의 IT 관리자는, “양자 컴퓨팅 위협은 미래에 일어날 것이고 그 시점에 완벽하게 준비되어 있어야 합니다” 라고 말했습니다.



# DigiCert가 제안하는 양자 컴퓨팅 대비 전략

양자 컴퓨팅은 기업의 미래를 여는 세 가지 핵심 기술 중 하나입니다.

그러나, 암호화에 미치는 리스크로 인해 양자 컴퓨팅의 미래 가치가 과소평가되고 있습니다. 세계적인 웹 암호화 선도 기업인 DigiCert는 기업이 미래 양자 시대에 조직을 보호하기 위한 전략으로, 다음과 같은 사항을 권장하고 있습니다.



## 리스크

리스크를 인식하고  
양자 암호화 성숙  
모델을 구축할 것



## 역량

조직 전반에 걸쳐  
암호화 민첩성  
수준의 중요성을  
이해하고 핵심 대응  
방안을 수립할 것



## 모범 사례

선도 기업과 협력해 디지털 인증서  
모범 사례를 마련하고, 해당  
기업들이 PQC 산업 변화를 파악해  
제품 및 솔루션에 반영함으로써  
변화에 앞서갈 것. 변화는 천천히  
진행되므로, 기다리지 말고 암호화  
민첩성 개선을 지금 당장 시작할 것



## 연락처

DigiCert, inc.  
2801 North Thanksgiving Way  
Suite 500  
Lehi, Utah 84043

1.800.896.7973  
[www.digicert.com](http://www.digicert.com)



DigiCert는 높은 신뢰도의 디지털 인증서를 제공하는 글로벌 선도 기업으로, 최근 급성장하는 IoT 시장을 위한 신뢰도 높은 SSL과 프라이빗 및 매니지드 PKI 구축, 그리고 디바이스 인증서를 제공하고 있습니다. 15년 전 설립 이래, DigiCert는 보다 나은 방식의 인터넷 인증을 지원하고, 고객의 니즈에 맞는 솔루션을 제공하고자 노력해왔고 이를 바탕으로 성장해왔습니다. 이제는 DigiCert의 혁신에 Symantec의 경험과 역량을 더해 업계를 선도하고 신원 확인(ID) 및 디지털 거래 분야의 신뢰도를 높일 수 있는 보다 나은 방법을 모색하고 있습니다.