Draft

국가·공공기관

양자내성암호 전환 가이드북

체계적인 양자내성암호 전환을 위한 단계별 실무 프레임워크



POST-QUANTUM CRYPTOGRAPHY
MIGRATION
GUIDEBOOK

2026. 11.

국가정보원
NATIONAL INTELLIGENCE SERVICE

NSR
국가보안기술연구소

Draft

국가·공공기관

양자내성암호 전환 가이드북

체계적인 양자내성암호 전환을 위한 단계별 실무 프레임워크

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK

2026. 11.

본 「국가 · 공공기관 양자내성암호 전환 가이드북」 발간 과정에서 소중한 자문과 도움을 주신 분들께 깊이 감사드립니다.

한국전자통신연구원	강유성 실장	국가수리과학연구소	심경아 팀장
아주대학교	곽진 교수	국민대학교	염용진 교수
국민대학교	김동찬 교수	금융보안원	오중효 본부장
성신여자대학교	김성민 교수	성신여자대학교	이주희 교수
성신여자대학교	김수리 교수	한컴위드社	길광은 부장
한국지능정보사회진흥원	김영희 센터장	라온시큐어社	박수정 수석
한국인터넷진흥원	김준섭 팀장	케이사인社	송상헌 부장
한양대학교 ERICA	서승현 교수	NSHC社	윤기순 연구소장
한성대학교	서화정 교수	드림시큐리티社	장형도 실장
성신여자대학교	손용하 교수	삼성 SDS社	조지훈 마스터

[문서의 영향과 범위]

이 문서는 국가정보원의 국가 암호기술 정책서 배포 계획에 의해 기획 · 작성 · 출판되었으며, 향후 국가 암호기술 사용 정책 및 암호모듈 검증제도(KCVMP) 등 제반 여건에 따라 개정될 수 있습니다.

이 문서의 내용은 국내외 학계, 산업계, 연구계가 축적한 지식을 바탕으로 국가정보원과 국가보안기술연구소가 수립한 가이드라인입니다. 이 문서 자체는 법적 강제력을 가지지 않으나, 별도 법·시행령 등에서 구속력 있는 의무화 지침으로 활용될 수 있습니다. 또한 의무화 지침으로 활용되지 않더라도 국가·공공기관 등에서 이 문서 전체 혹은 일부를 활용, 준수해야 할 보안 통제 수단 등의 기술적 기준으로 사용할 수 있습니다.

이 문서를 활용하여 중앙행정기관 및 그 소속기관, 지방자치단체 및 그 소속기관, 공공기관 및 국가 기반시설 운영기관 등이 안전한 정보보안 정책을 수립하고 정보시스템을 운영하는 과정에서 종합적인 기술적 기준으로 활용하기를 기대합니다.

[이용 대상]

이 문서는 주요 정보자산을 처리하거나 보호해야 하는 모든 국가기관과 공공기관을 대상으로 작성되었습니다. 특히 각 기관에서 보안 정책을 수립하거나, 보안 시스템을 기획, 도입, 운영하는 담당자, 그리고 보안 점검 및 대응 업무를 수행하는 실무자, 공공조달 기업체 등을 주요 대상으로 작성되었습니다.

[저작권]

- 국가정보원과 국가보안기술연구소와의 사전 협의 없이 문서의 전부 또는 일부를 상업적 목적으로 복제 및 배포 금지
- 비상업적 목적으로 문서 내용의 전부 또는 일부를 이용하고자 할 때는 반드시 출처 명기

[문서 개정 이력]

개정일	버 전	내 역	비 고
2026.11.	Draft	초안 출판	

문서 이용 안내

[표 색상 범례]

본 가이드북은 표의 색상을 활용하여 실무 관련 사항, 산출물, 마일스톤, 개념 이해, 주의사항, 용어를 아래와 같이 구분하여 제시합니다.

강조 박스 유형	의미 및 사용 예
실무 관련 사항	실무 지침, 실무 시나리오, 자가진단, 실무 참고 등 담당자가 실무에 바로 활용할 수 있는 구체적인 정보 예 : 「기기 교체 가이드라인」, 「실무 시나리오」, 「실무 담당자용 1분 자가진단」, 「실무 참고 : 인벤토리 구축과 예산 계획의 관계」
산출물	해당 단계에서 작성하거나 확보해야 하는 문서 · 산출물 목록 예 : 「주요 산출물」
마일스톤	로드맵의 각 시행 단계마다 전체 국가 · 공공기관이 공통으로 달성해야 하는 목표 예 : 「▶ 국가 공통 마일스톤(~2027년)」
개념 이해	핵심 개념 및 용어 설명, 구체적인 적용 예시, 자주 묻는 질문에 대한 답변, 특정 절차 · 정책이 필요한 배경 논리 등 예 : 「예시」, 「인벤토리 구축 시 자주 받는 질문」, 「왜 초기 거버넌스 수립이 중요한가?」
주의사항	실무상 유의해야 할 점이나 혼동하기 쉬운 사항 예 : 「점수 산정 시 주의사항」

※ 일반 데이터 표에 사용된 회색·청색 계열의 표 머리글 색상은 본 범례의 대상이 아니며, 통상적인 표 서식으로 사용됩니다.

들어가는 말

[양자내성암호 전환, 지금부터 준비해야 하는 장기 과제]

양자컴퓨팅 기술의 발전은 현재 국가·공공기관의 정보시스템과 디지털 서비스에서 폭넓게 사용되고 있는 공개 키 암호의 장기적인 안전성에 영향을 미칠 수 있다. 특히 현재 암호화된 정보를 수집해 두었다가 향후 충분한 성능의 양자컴퓨터를 이용하여 복호화하는 HNDL(Harvest Now, Decrypt Later) 공격을 고려하면, 실제 양자컴퓨터가 기존 공개 키 암호를 해독할 수 있는 시점에 이르러서야 전환을 시작하는 것은 충분하지 않을 수 있다.

양자내성암호 전환은 특정 암호 알고리즘이나 제품을 단순히 교체하는 작업도 아니다. 기관에서 어떤 시스템과 서비스가 공개 키 암호를 사용하고 있는지 파악하고, 데이터의 중요도와 보호 기간, 다른 기관·시스템과의 연계, 범정부 공통 인프라 의존성, 공급업체의 지원 여부, 시스템 교체 계획, 조달·예산 여건 등을 함께 고려하여 전환 대상과 우선순위를 정해야 한다. 또한 실제 적용 과정에서는 기존 시스템과의 상호운용성, 서비스 연속성, 암호모듈 검증제도(KCMVP), 제품·서비스의 가용 시점 등을 함께 검토해야 한다.

특히 양자내성암호 전환은 아직 많은 국가·공공기관에 익숙하지 않은 과제이다. 기관 내에서 어떤 암호가 어디에 사용되고 있는지 파악하지 못하거나, 양자내성암호 전환을 정보보안 부서의 기술적인 업무로만 인식할 수도 있다. 그러나 실제 전환은 정보보안뿐 아니라 정보화사업, 시스템 운영, 조달·계약, 예산, 공급업체 관리 및 기관 간 협력이 함께 이루어져야 하는 중장기적인 변화이다. 현재 본문도 전환을 준비할 때 가장 먼저 부딪치는 질문을 “우리 기관의 무엇을 바꾸어야 하는가”로 제시하고, 암호가 사용되는 지점을 먼저 파악해야 계획·예산·일정을 구체화할 수 있다고 설명한다.

[가이드북의 목적]

본 가이드북은 국가·공공기관이 양자컴퓨팅 위협과 양자내성암호 전환의 필요성을 이해하고, 기관의 현재 상황과 전환 여건을 스스로 파악하여 향후 전환을 체계적이고 단계적으로 준비할 수 있도록 지원하는 것을 목적으로 한다.

이 가이드북의 목적은 모든 기관이 지금 즉시 모든 시스템을 양자내성암호로 전환하도록 요구하는 데 있지 않다. 각 기관이 먼저 전환의 필요성을 인식하고, 암호 사용 현황과 의존 관계를 파악하며, 전환 우선순위를 정하고, 조달·예산·사업 계획과 연계하여 실제 전환을 수행할 수 있는 준비 역량을 갖추도록 하는 것에 중점을 둔다.

따라서 본 가이드북은 양자내성암호 알고리즘의 수학적 원리나 세부 구현 방법을 설명하기 위한 문서가 아니다. 특정 알고리즘이나 제품의 도입을 일률적으로 정하거나 모든 기관에 동일한 전환 시점과 방식을 적용하도록 하는 의무 기준도 아니다. 기관의 규모, 업무 특성, 정보시스템 환경과 전환 여건을 고려하여 전환을 준비·계획·이행·점검하는 과정에서 참고할 수 있는 실무 안내 자료이다.

본 가이드북은 관련 법률, 시행령, 시행규칙 및 국가의 보안 정책을 대체하지 않는다. 실제 전환을 추진할 때에는 관계 기관의 최신 정책과 기준을 우선하여 확인해야 한다. 또한 국가 암호기술 사용 정책, 국내외 표준, 암호모듈 검증제도(KCMVP), 범정부 공통 인프라 및 관련 제품·서비스의 지원 환경 변화에 따라 본 가이드북의 내용도 지속적으로 보완·개정될 수 있다.

[국가·공공기관의 특성을 고려한 전환 준비]

국가·공공기관의 정보시스템은 기관 내부에서 독립적으로 운영되는 시스템만으로 구성되지 않는다. 범정부 공통 인프라와 전자서명 인증체계, 기관 간 정보연계, 대국민 서비스, 클라우드 서비스, 상용 보안제품 및 외부 공급업체 등에 폭넓게 의존하고 있다. 또한 장기간 운영되는 레거시 시스템과 장수명 장비, 장기간 보존해야 하는 행정정보와 전자기록물 등 민간의 일반적인 정보시스템 환경과는 다른 특성을 가진다.

이러한 환경에서는 하나의 기관이나 시스템만 독립적으로 암호체계를 변경하기 어려운 경우가 많다. 기술적으로 전환이 가능하더라도 관계 기관이나 공통 인프라가 새로운 암호 방식을 지원하지 않거나, 검증필 암호모듈과 상용제품이 아직 충분히 제공되지 않으면 실제 적용 시점이 달라질 수 있다. 따라서 국가·공공기관의 양자내성암호 전환은 위험도와 시급성뿐 아니라 실제 전환 가능성을 함께 고려하여 단계적으로 추진하는 것이 중요하다. 현재 가이드북도 국가·공공부문의 높은 공통 인프라 의존성, 레거시·장수명 장비, 공급업체 및 공공조달·검증제도 등을 고려하여 단계적·점진적 접근이 필요하다고 설명하고 있다.

[주요 이용 대상]

본 가이드북은 주요 정보자산을 처리하거나 보호하는 중앙행정기관, 지방자치단체, 공공기관 및 국가기반시설 운영기관 등의 모든 국가기관과 공공기관을 대상으로 한다.

특히 다음과 같이 양자내성암호 전환의 준비와 이행에 관여하는 담당자가 함께 활용하는 것을 전제로 한다.

이용 대상	주요 활용 내용
전환 총괄 책임자 · 관리자	전환 필요성 인식, 추진체계 구성, 주요 의사결정 및 기관 로드맵 관리
정보보안 담당자	암호 사용 현황 파악, 위험평가, 보안 정책 및 검증기준 검토
정보화사업 담당자	신규 · 차세대 정보화사업에 전환 요구사항 반영
시스템 운영 담당자	시스템 영향, 연계 · 호환성, 장애대응 및 서비스 연속성 검토
조달 · 계약 담당자	제품 · 서비스 지원 계획 확인, RFP 및 계약조건 반영
예산 담당자	정보화사업 · 장비교체 일정과 전환 소요예산 연계
외부 위탁 · 공급업체 관리 담당자	공급업체의 지원 로드맵, 업그레이드 · 교체 계획 및 기술지원 확인

양자내성암호 전환은 특정 담당자만의 과제가 아니므로, 기관은 관련 부서가 공동으로 전환 현황과 계획을 공유하고 기관 차원의 추진체계를 마련할 필요가 있다.

[가이드북에서 다루는 내용]

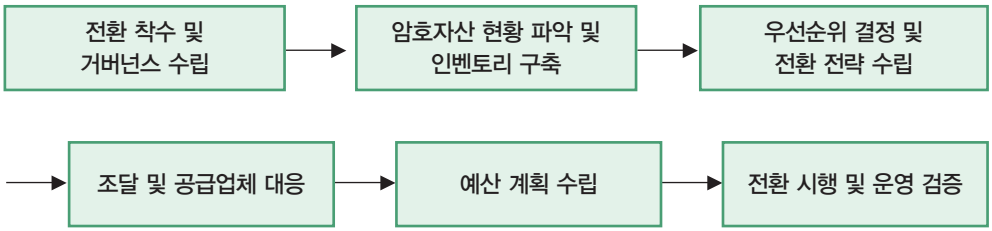
본 가이드북은 “양자내성암호가 무엇인가”를 설명하는 데 그치지 않고, 국가·공공기관이 실제 전환을 준비하면서 마주하게 되는 질문을 중심으로 구성한다.

구분	핵심 질문	주요 내용
1장 양자 위협 및 대응	왜 지금부터 준비해야 하는가?	양자컴퓨팅 위협, HNDL, 양자내성암호, 점진적 전환 필요성
2장 국가 · 공공기관 암호 사용 지점 진단과 전환 파급 범위	우리 기관의 무엇이 영향을 받는가?	기관 내 암호 사용 지점과 운영 · 조달 · 기관 연계 · 데이터 등 전환 파급 영역
3장 양자내성암호 전환 프레임워크	전체 전환은 어떤 흐름으로 추진하는가?	전환 절차, 단계별 산출물 및 국가 · 공공기관 전환 로드맵
4장 단계별 전환 실행 가이드	실제로 무엇부터 해야 하는가?	거버넌스, 암호자산 인벤토리, 우선순위, 조달 · 공급업체, 예산, 적용 · 검증
5장 전환 시 상황별 고려사항	환경별로 무엇을 추가로 고려해야 하는가?	하이브리드, 암호 민첩성, 공개 키 기반구조, 클라우드, 레거시 · HSM, OT · ICS, 장기보존 데이터, 서비스 연속성
6장 전환 이행 방향과 향후 과제	준비 수준을 어떻게 지속적으로 높이는가?	실행 출발점, 표준화 대응, 전환 완료 기준 및 성숙도 관리

[단계적으로 준비하고 지속적으로 보완한다]

모든 암호자산을 처음부터 완벽하게 파악하거나 모든 제품과 기술이 준비될 때까지 기다린 뒤 전환을 시작할 필요는 없다. 기관은 현재 확인할 수 있는 범위에서 주요 시스템과 암호 사용 현황을 먼저 파악하고, 우선순위가 높은 영역부터 준비하면서 조사 범위와 전환 계획을 지속적으로 보완할 수 있다.

본 가이드북은 이러한 준비를 위해 다음의 흐름에 따라 전환을 추진하도록 구성한다.



각 단계에서 제시하는 산출물, 체크리스트, RFP, 평가표 및 예시 문구는 모든 기관이 동일한 형식으로 작성해야 하는 의무 양식이 아니다. 기관의 규모와 업무 특성, 시스템·서비스 운영 환경에 따라 필요한 항목을 선택·조정하여 활용할 수 있다. 실제 본문의 체크리스트도 기관의 상황에 맞지 않는 문항은 삭제하고 필요한 항목을 추가하여 사용할 수 있도록 구성되어 있다.

CONTENTS

국가·공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK

Chapter 01 양자컴퓨팅 위협 및 대응 1

제1절 양자컴퓨팅 위협 2

제2절 양자내성암호 9

제3절 점진적 전환 전략의 필요성 15

Chapter 02 국가·공공기관 암호 사용 지점 진단과 전환 파급 범위 21

제1절 기관 시스템 내 암호 사용 지점 22

제2절 양자내성암호 전환의 기관 파급 영역 39

Chapter 03 양자내성암호 전환 프레임워크 53

제1절 양자내성암호 전환 절차 개요 54

제2절 단계별 주요 산출물 61

제3절 국가·공공기관 전환 로드맵 68

Chapter 04 단계별 전환 실행 가이드 81

제1절 전환 착수 및 거버넌스 수립 86

제2절 암호자산 현황 파악 및 인벤토리 구축 98

제3절 우선순위 결정 및 전환 전략 수립 122

제4절 조달 및 공급업체 대응 전략 148

제5절 예산 계획 수립 166

제6절 전환 시행 및 운영 검증 181

Chapter 05 전환 시 상황별 고려사항 199

제1절 하이브리드 운영 원칙과 네트워크 제약 해결 201
제2절 암호 민첩성 확보 및 지속 관리 방안 205
제3절 전자서명 인증체계 전환 및 상호운용성 208
제4절 공공 클라우드 환경의 양자내성암호 전환 고려사항 211
제5절 기존 시스템(레거시) 및 하드웨어(HSM/보안장비) 처리 전략 213
제6절 IoT·OT·ICS 시스템의 양자내성암호 전환 특수 전략 214
제7절 데이터 전환과 장기보존 데이터의 무결성·진본성 보존 216
제8절 체크리스트 : 전환 시 주요 고려사항 218

Chapter 06 전환 이행 방향과 향후 과제 223

제1절 실천적 출발점과 핵심 성공 요인 224
제2절 중장기 이행 로드맵과 표준화 대응 226
제3절 양자내성암호 전환 완료 기준 및 성숙도 측정 체계 226
제4절 양자내성암호 전환은 미래가 아닌 현재의 과제 228

■ 주요 용어 231

■ 참고 문헌 243



[표 차례]

[표 1] 암호 유형별 양자 위협 영향 및 대응 방향 4

[표 2] 주요 기관의 CRQC 등장 시기 예측 5

[표 3] 모스카 부등식 구성 변수의 정의 8

[표 4] 주요 양자내성 키 캡슐화 알고리즘 9

[표 5] 주요 양자내성 전자서명 알고리즘 10

[표 6] 양자내성암호 적용에 따른 주요 기술적 고려사항 11

[표 7] 주요 국가의 양자내성암호 전환 목표 비교 13

[표 8] 양자내성암호 전환 시 고려해야 하는 핵심 사항 15

[표 9] 단계별 전환 시나리오 예시 17

[표 10] 암호기술 주요 적용 5대 지점 및 요구 기능 24

[표 11] 5대 암호 사용 지점별 전환 긴급성 자가 점검표 38

[표 12] 국가·공공기관 양자내성암호 전환 로드맵 69

[표 13] 자체 로드맵 수립 시 주요 고려사항 77

[표 14] 의사결정 사항 및 결정 주체 예시 92

[표 15] 전환 전담 인력 운영 모델 93

[표 16] 암호자산 인벤토리 구축을 위한 주요 점검 대상 및 항목 예시 101

[표 17] 암호자산 인벤토리 구축 방식 107

[표 18] 단계별 암호자산 인벤토리 구축 전략 112

[표 19] 기관별 암호자산 인벤토리 구축 접근 방법 예시 119

[표 20] 전환 우선순위 기준 124

[표 21] 전환 우선순위 평가 기준 및 배점표 134
[표 22] 우선순위 총점 구간별 권장 대응 방향 136
[표 23] 전환 전략 유형 141
[표 24] 전환 전략 예시 143
[표 25] 주요 공급업체 유형별 대응 방법 150
[표 26] 시스템 유형별 대응 방법 152
[표 27] RFP 반영 핵심 포인트 156
[표 28] 전환을 위한 주요 예산 항목 168
[표 29] 전환 예산 편성 시 기존 사업 연계 방안 예시 172
[표 30] 예산 상황에 따른 단계별 접근 방법 173
[표 31] 전환 대상 선정 기준 182
[표 32] 전환 단계적 적용 절차 184
[표 33] 성능 검증 항목 185
[표 34] 주요 상호운용성 확인 사항 187
[표 35] 장애 시나리오 및 대응 방법 예시 188
[표 36] 기존 데이터 처리 방법 190
[표 37] 5가지 주요 위험 요인 및 대응 방안 200
[표 38] 주요 통신 규약별 양자내성암호 적용 가이드 205
[표 39] 인증서 폐기 기반시설(CRL/OCSP) 영향 및 완화 방안 210
[표 40] IoT·OT 환경에서의 전환 핵심 과제 및 보완 방안 214
[표 41] 저장 데이터의 재암호화 4단계 절차 예시 217
[표 42] 본 가이드북의 핵심 메시지 5가지 229



[그림 차례]

[그림 1] HNDL 공격 흐름도 7
[그림 2] 모스카의 부등식 8
[그림 3] 전형적인 국가·공공기관 IT 아키텍처 내 5대 암호 사용 지점 23
[그림 4] 전환이 기관 전반에 미치는 4개 영역 40
[그림 5] 국가·공공기관 양자내성암호 전환 로드맵 70
[그림 6] 양자내성암호 6단계 전환 절차 84

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



Chapter 01

양자컴퓨팅 위협 및 대응

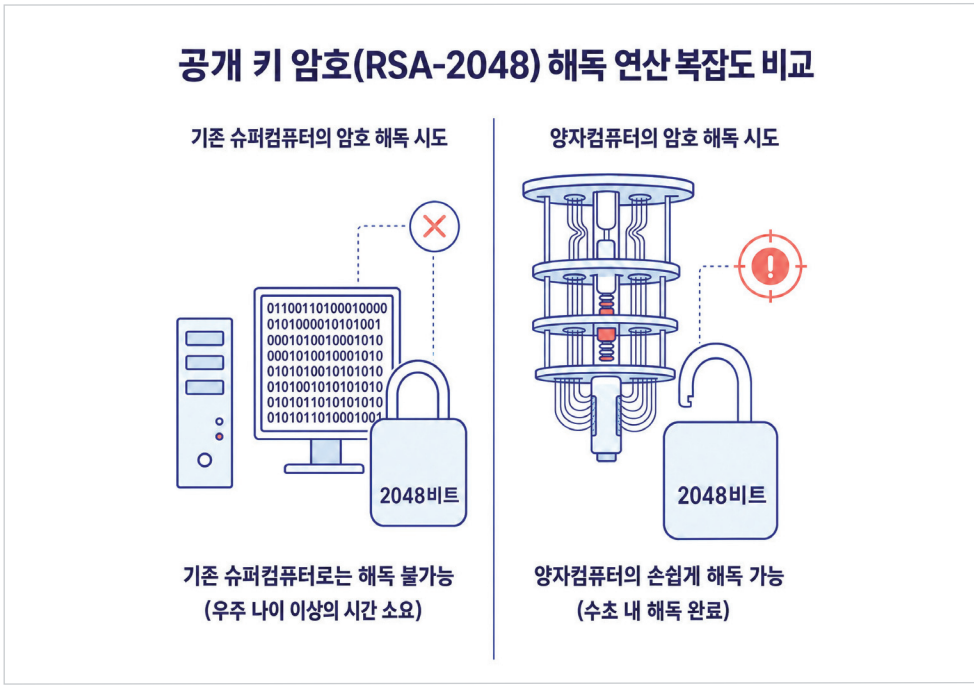
Chapter 01

양자컴퓨팅 위협 및 대응

제1절 양자컴퓨팅 위협

현대 디지털 인프라의 보안은 비대칭 키 암호 알고리즘(최근 국내외 표준·기술 문서의 용례를 고려하여 이하 '공개 키 암호'로 통칭)에 크게 의존하고 있다. 전자정부 서비스, 금융거래, 의료 정보 교환, 행정정보 공동이용 등 다양한 분야에서 RSA, ECDSA, ECDH 등의 공개 키 암호가 암호화, 키 설정, 전자서명 및 인증 등에 폭넓게 활용되고 있다.

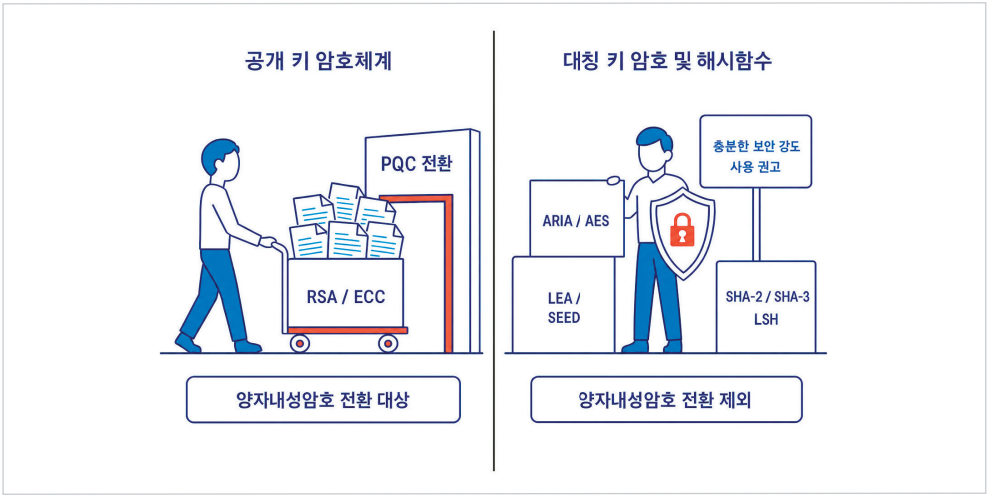
이러한 공개 키 암호의 안전성은 정수 인수분해 문제나 이산대수 문제를 현실적인 계산 자원으로 해결하기 어렵다는 가정에 기반한다. 그런데 이 가정은 1994년 피터 쇼어(Peter Shor)가 양자컴퓨터에서 정수 인수분해 문제와 이산대수 문제를 현실적인 시간 내에 해결할 수 있는 알고리즘을 제안하면서 근본적인 도전에 직면하게 되었다[34]. 충분한 규모의 오류정정이 가능한 양자컴퓨터에서 쇼어 알고리즘을 구현할 경우, RSA, ECDSA, ECDH 등 현재 널리 사용되는 주요 공개 키 암호의 안전성이 근본적으로 무력화될 수 있다. 이는 특정 암호 알고리즘에서 발견되는 개별적인 취약점이 아니라 현재의 공개 키 암호 체계 전반에 영향을 미치는 구조적인 위협이다.



반면, ARIA, LEA, AES 등의 대칭 키 암호 알고리즘(또는 비밀 키 암호 알고리즘, 이하 '대칭 키 암호'로 통칭)과 SHA-2, SHA-3, LSH 등의 해시함수에 미치는 양자컴퓨터의 영향은 상대적으로 제한적이다. 대칭 키 암호와 해시함수에는 그로버(Grover) 알고리즘이 주요 양자 위협으로 거론되지만[23], 공개 키 암호와 같이 알고리즘의 안전성 기반이 직접적으로 무력화되는 것은 아니다. 다만 양자 공격을 고려한 충분한 보안강도를 확보할 수 있도록 키 길이와 해시 출력 길이, 사용 알고리즘의 적절성을 함께 검토할 필요가 있다. 또한 실제 공격에는 대규모 양자 자원이 필요하며, 그로버 알고리즘을 이용한 공격은 고전적 전수조사와 달리 병렬화에 제약이 있다는 분석도 있으므로, 이론적인 연산 복잡도뿐만 아니라 현실적인 공격 비용과 구현 가능성을 함께 고려할 필요가 있다[24].

이러한 차이를 고려하여 본 가이드북에서는 **양자내성암호 전환 대상을 공개 키 암호로 한정**한다. 여기에는 공개 키 기반의 암호화, 키 설정 및 전자서명에

사용되는 암호가 포함되며, 이후 별도의 언급이 없는 한 **전환 대상은 공개 키 암호**를 의미한다.



암호 유형별 주요 양자 위협과 영향 수준 및 대응 방향을 요약하면 [표 1]과 같다.

[표 1] 암호 유형별 양자 위협 영향 및 대응 방향

암호 유형	KCMVP 검증대상 암호	양자 알고리즘	영향 수준	대응 방향
공개 키 암호	RSAES, RSA-PSS, (EC)DH, ECDSA, (EC-) KCDSA	쇼어	치명적 (완전 해독 가능)	양자내성암호로 전환 필요
대칭 키 암호	ARIA, SEED, HIGHT, LEA, AES	그로버	제한적 (이론적으로 보안 강도가 감소하나, 실제로는 대규모 양자 자원이 필요하여 위협이 제한적)	키 크기 확대 검토
해시 함수	SHA-2, SHA-3, LSH			출력 크기 확대 검토

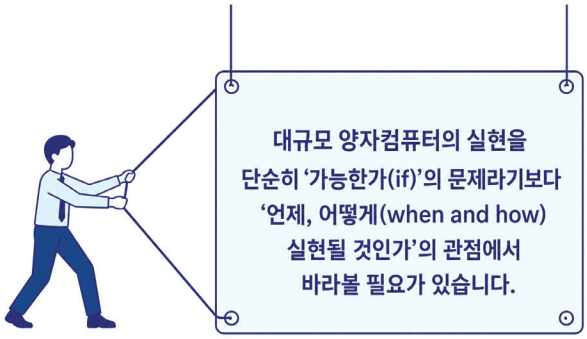
암호학적으로 유의미한 양자컴퓨터(CRQC : Cryptographically Relevant Quantum Computer)를 실현하기 위해서는 대규모 양자 연산을 안정적으로 수행할 수 있어야 하며, 이를 위한 양자 오류정정(QEC : Quantum Error Correction) 기술의 발전이 핵심 과제 중 하나이다. CRQC의 실현 시점을 정확히 예측하는 것은 어렵지만, 주요 기관과 전문가 그룹은 위험 요인 관리 목적으로 [표 2]와 같은 전망을 제시하고 있다.

[표 2] 주요 기관의 CRQC 등장 시기 예측

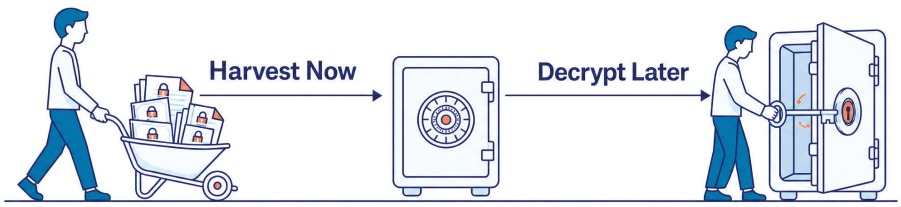
출처	연도	예측 시기	성격 및 근거
Quantum Threat Timeline Report 2025 [26]	2026	〈RSA-2048 해독 가능 CRQC 등장 확률 전망〉 • 10년 내 : 28%~49% • 15년 내 : 51%~70% • 30년 내 : 81%~93%	10년 내 실현 가능성 전망이 상승하여 2030년대 중반(~2035년) 구축 가능성에 무게 (전문가 26명 설문)
EU NIS Cooperation Group 로드맵 [27]	2025	• 보수적 전망 : 최대 16년 내(2040년까지) • 오류정정 기술 발전 가속 시 약 10년 내로 단축 가능	BSI 의뢰 독립 연구기관의 기술 분석

양자내성암호 전환을 준비하는 기관은 이러한 전망을 CRQC의 실현 시점에 대한 확정적 예측이 아니라, 양자 위협에 대비한 위험평가와 전환 계획 수립을 위한 참고 기준으로 활용할 필요가 있다. 핵심은 정확한 실현 시기를 예측하는 것이 아니라 불확실성을 고려하여 선제적으로 대비하는 것이다.

「Quantum Threat Timeline Report 2025」는 대규모 양자컴퓨터의 실현 시점에는 상당한 불확실성이 존재하지만, 현재까지 이를 원천적으로 불가능하게 하는 근본적인 장벽은 확인되지 않았다고 설명한다. 이에 따라 대규모 양자컴퓨터의 실현을 단순히 '가능한가(if)'의 문제라기보다 '언제, 어떻게 실현될 것인가(when and how)'의 관점에서 바라볼 필요가 있다고 제시하고 있다[26].

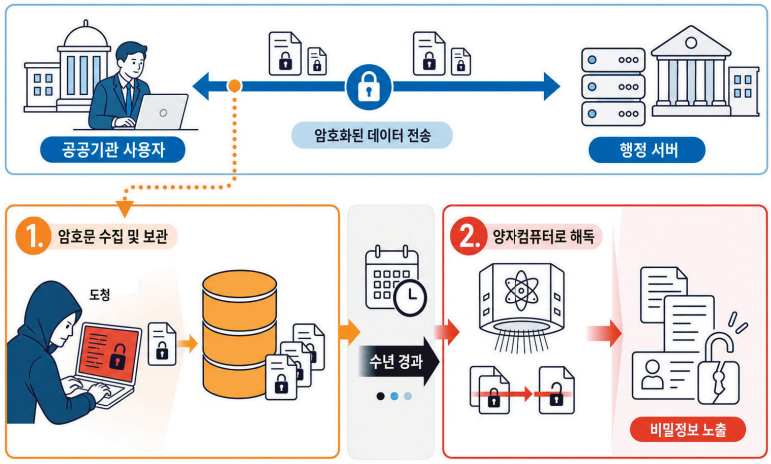


이러한 시점의 불확실성과 별개로 현재부터 고려해야 할 대표적인 위협은 HNDL(Harvest Now, Decrypt Later) 공격이다. HNDL 공격은 공격자가 현재 공개 키 암호로 보호되어 전송되는 데이터를 수집·보관한 뒤, 향후 이를 해독할 수 있는 양자컴퓨터가 등장하면 저장해 둔 데이터를 복호화하는 공격 방식이다.



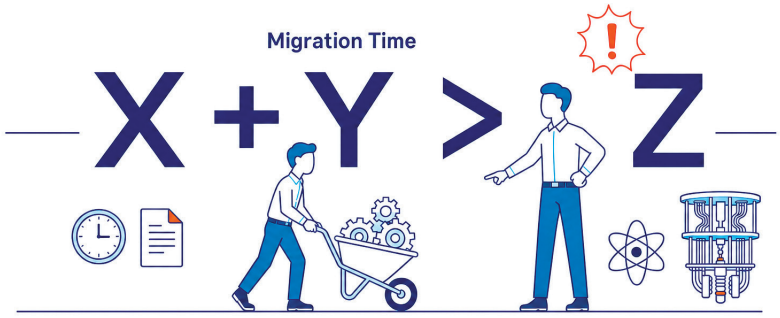
즉, 복호화가 가능해지는 미래의 어느 시점을 위해 공격자는 현재부터 암호화된 데이터를 수집·저장할 수 있으므로 장기간 기밀성을 유지해야 하는 정보에 대해서는 선제적인 보호조치가 필요하다. [그림 1]은 HNDL 공격의 전체 과정과 데이터 노출 가능 시점을 나타낸다.

[그림 1] HNDL 공격 흐름도



따라서 국가 기밀 데이터나 개인정보 등 장기간 기밀성 보호가 필요한 정보를 처리하는 시스템은 데이터의 보호 필요 기간과 공개 키 암호의 사용 여부를 확인하고, 그 결과에 따라 양자내성암호 전환 준비를 추진할 필요가 있다.

양자컴퓨팅 위협에 대비한 전환 착수 시점을 판단하는 데 활용되는 대표적인 개념이 모스카(Mosca)가 제안한 '모스카 부등식(Mosca's Inequality)'이다.



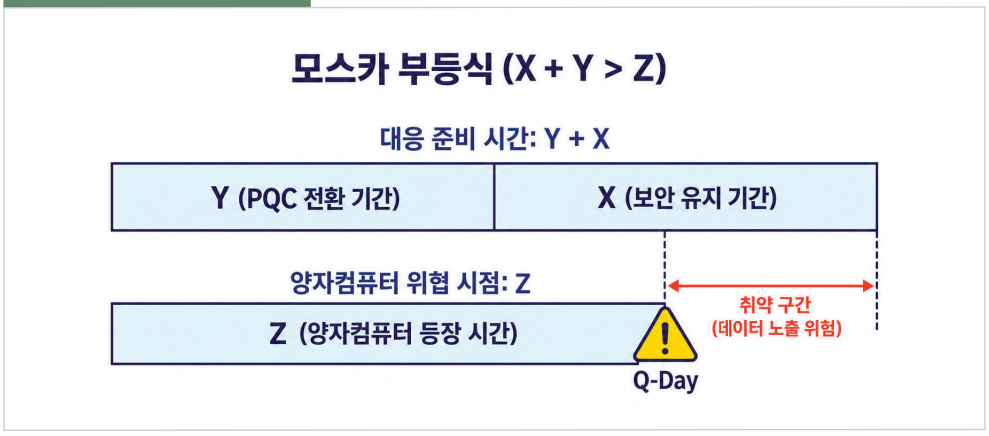
모스카 부등식은 데이터 보호 필요기간과 양자내성암호 전환 소요기간의 합을 CRQC 실현까지의 예상기간과 비교하여, 양자 위협에 대비한 전환 필요성을 평가하는 데 활용된다. 이를 위해 세 가지 핵심 변수 X, Y, Z를 [표 3]과 같이 정의한다.

[표 3] 모스카 부등식 구성 변수의 정의

변수	의미	설명 및 예시
X	데이터 보호 기간	암호화한 데이터가 안전하게 보호되어야 하는 기간 (예 : 공공 기록물 보호 기간 30년, 장기 기밀 금융 데이터 등)
Y	전환 소요 기간	양자내성암호 기반 시스템 구축 및 검증을 거쳐 최종 인프라 전환을 완료하는 데 걸리는 총 기간 (예 : 통상 5~10년 소요)
Z	CRQC 실현까지 남은 기간	기존 공개 키 암호를 해독할 수 있는 양자컴퓨터(CRQC)가 실현되기까지 남은 기간 (예 : 전문가 예측에 따른 10~15년)

이 세 가지 변수를 바탕으로 전환의 시급성을 판정하는 부등식은 다음과 같다.

[그림 2] 모스카의 부등식



X+Y>Z인 경우, 현재부터 전환을 준비하더라도 데이터의 보호 필요 기간과 전환 소요 기간이 CRQC 등장까지의 예상 기간을 초과하므로 선제적인 대응이

필요한 상태로 판단한다. 특히 장기간 기밀성을 유지해야 하는 데이터는 HNDL 위협을 고려하여 전환 우선순위를 높게 평가할 필요가 있다. CRQC의 실현 시점은 불확실하므로 Z를 짧게 가정할수록 보다 보수적인 판단이 이루어진다.

제2절 양자내성암호

양자내성암호는 양자컴퓨팅 기반 공격에도 안전성을 유지할 수 있도록 설계된 공개 키 암호 알고리즘이다. 기존 컴퓨터와 통신 환경에서도 구현할 수 있으므로, 양자역학적 특성을 이용하는 양자암호통신과 달리 기존 정보시스템의 하드웨어 및 소프트웨어 환경에 적용할 수 있다.

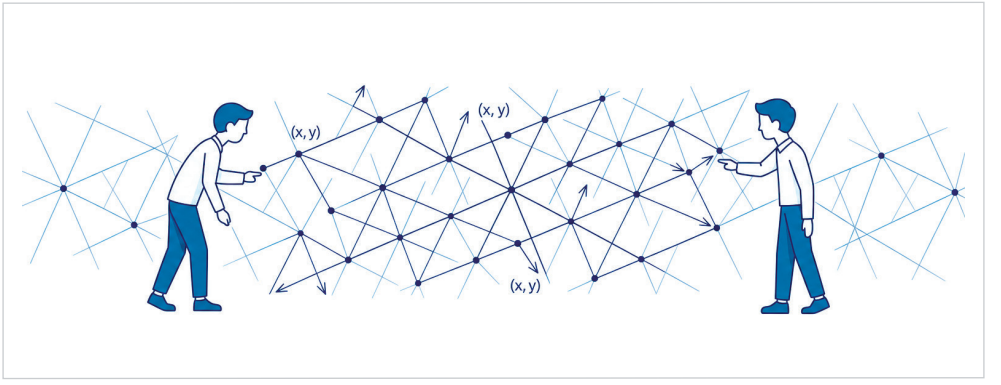
미국 국립표준기술연구소(NIST)는 2016년 양자내성암호 표준화 공모를 시작한 이후 장기간의 공개 검증과 평가를 거쳐 2024년 8월 미국 연방정보처리표준 FIPS 203 · 204 · 205를 발표하였다[28, 29, 30]. 대한민국은 2021년부터 KpqC 공모전을 통해 국내외 공개 검증을 진행하고, 2025년 1월 키 캡슐화 2종과 전자서명 2종 등 총 4종을 한국형 양자내성암호로 선정하였다[7]. [표 4]와 [표 5]는 국내외 주요 양자내성암호를 정리한 것이다.

[표 4] 주요 양자내성 키 캡슐화 알고리즘

암호	기반 문제	표준 문서
SMAUG-T	격자 (MLWE, MLWR)	• KS 제정 제안 제출(2026년)
NTRU+	격자(NTRU)	
ML-KEM	격자(MLWE)	• NIST FIPS 203 (2024년 8월) • ISO/IEC 18033-2:2006/Amd 2:2026 (2026년 6월)
HQC	부호 (QC-SDP)	• NIST 표준화 진행 중(2025년 3월 선정, 최종 표준 2027년 예정)
Classic McEliece	부호(SDP)	• ISO/IEC 18033-2:2006/Amd 2:2026 (2026년 6월)
FrodoKEM	격자(LWE)	• ISO/IEC 18033-2:2006/Amd 2:2026 (2026년 6월)

[표 5] 주요 양자내성 전자서명 알고리즘

암호	기반 문제	표준 문서
HAETAE	격자 (MLWE, MSIS)	• KS 표준 제정 제안 검토 중
AIMer	대칭 키 (일방향성)	
ML-DSA	격자 (MLWE, MSIS)	• NIST FIPS 204 (2024년 8월)
SLH-DSA	해시함수 (원상 저항성 등)	• NIST FIPS 205 (2024년 8월)
FN-DSA	격자(NTRU)	• NIST FIPS 206 (표준 문서 준비 중)
XMSS	해시함수 (원상 저항성 등)	• NIST SP 800-208 (2020년 10월) • ISO/IEC 14888-4:2024 (2024년 6월) • RFC 8391 (2018년 5월)
LMS	해시함수 (원상 저항성 등)	• NIST SP 800-208 (2020년 10월) • ISO/IEC 14888-4:2024 (2024년 6월) • IRTF RFC 8554 (2019년 4월)



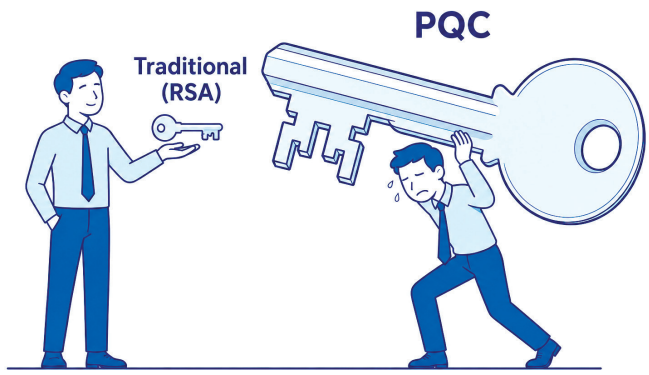
양자내성암호는 기존 공개 키 암호와 비교하여 대체로 키·암호문·전자서명 등의 크기가 크며, 이러한 특성은 네트워크 대역폭, 저장 공간 및 처리 성능에 영향을 미칠 수 있다. 따라서 실제 전환 과정에서는 사용하는 알고리즘과 시스템

환경에 따라 메시지 크기 증가, 패킷 분할, 인증서 크기 증가, 제한된 자원을 사용하는 IoT · 임베디드 환경에서의 처리 부담 등을 사전에 검증할 필요가 있다.

[표 6] 양자내성암호 적용에 따른 주요 기술적 고려사항

주요 고려사항	내용
TLS 핸드셰이크 메시지 분할 및 호환성 문제	키 교환 데이터 증가에 따른 메시지 분할, 통신 지연 증가 및 네트워크 장비와의 호환성 문제
인증서 및 인증서 체인 크기 증가 문제	양자내성 전자서명과 공개 키의 크기에 따른 인증서 및 인증서 체인의 데이터 크기 증가
IKEv2 메시지 단편화 및 호환성 문제	메시지 크기 증가에 따른 IP 단편화 및 일부 네트워크 장비와의 호환성 문제
IoT · 임베디드 환경의 자원 부담 문제	큰 공개 키 · 암호문 · 서명 처리에 따른 메모리 · 연산능력 · 통신 대역폭 부담 증가

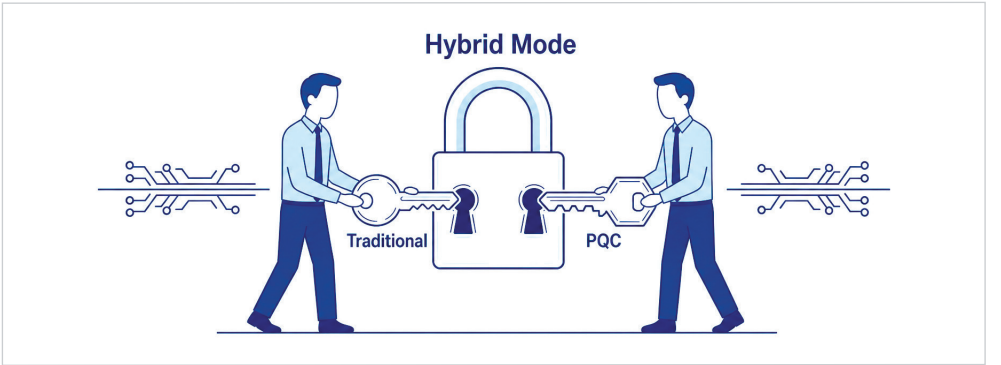
Cloudflare, Google, Meta의 적용 사례에서는 양자내성암호 키 교환 데이터 증가로 TLS ClientHello가 여러 패킷으로 분할되어 추가 지연이 발생하거나, 일부 네트워크 장비와의 호환성 문제가 나타나는 사례가 확인되었다[16, 22, 25]. 이러한 사례는 양자내성암호를 실제 운영 환경에 적용할 때 성능과 네트워크 호환성에 미치는 영향을 사전에 검토할 필요가 있음을 보여준다.



한편, 양자내성암호는 RSA, Elliptic Curve Cryptography(ECC) 등 기존 공개 키 암호에 비해 연구·검증의 역사가 짧으므로 알고리즘 자체의 안전성과 구현 안전성에 대한 지속적인 검증이 중요하다. 일례로 NIST 양자내성암호 표준화 과정의 4라운드 키 캡슐화 후보였던 SIKE는 2022년 새로운 키 복구 공격이 발표되면서 안전성이 사실상 무력화되었다[15]. NIST 추가 양자내성 전자서명 공모전 3라운드 후보로 선정되었던 HAWK는 2026년 Claude Mythos Preview를 활용한 Anthropic의 연구를 통해 기존보다 크게 향상된 공격 기법이 제시되면서, 당초 예상보다 보안 강도가 상당히 저하된 것이 확인되었다[12].

SIKE와 HAWK의 사례에서 볼 수 있듯이, 양자내성암호는 표준화와 도입 과정에서도 새로운 암호분석 결과에 따라 안전성 평가가 달라질 수 있으므로 지속적인 검증이 필요하다. 전환 과정에서는 관계 기관의 정책과 검증 기준, 알고리즘의 표준화 및 안전성 검토 현황을 지속적으로 확인하고, 전환 단계와 시스템 특성에 따라 기존 공개 키 암호와 양자내성암호를 함께 사용하는 하이브리드 방식의 적용을 고려할 필요가 있다.

양자내성암호 전환 과정에서는 시스템 특성과 상호운용성 요구에 따라 하이브리드 방식을 활용할 수 있으며, 본 가이드북에서는 이를 하이브리드-AND 방식과 하이브리드-OR 방식으로 구분한다. 구체적인 유형(PQ/T, PQ/PQ), 특성 및 적용 시 고려사항은 5장 1절 ❶에서 다룬다. 본 가이드북에서 별도의 구분 없이 '하이브리드 방식'으로 표현한 경우에는 하이브리드-AND 방식을 의미하며, 하이브리드-OR 방식은 별도로 명시한다.



이와 같은 양자내성암호 전환 방식은 국내외 관련 정책과 표준화 방향, 기관별 역할 등을 고려하여 적용할 필요가 있다. 다양한 국가와 기관들은 각기 다른 역할로 양자내성암호 전환을 주도하고 있다. 미국은 연방정부 차원의 정책에 따라 관계 기관별 역할을 분담하여 전환 정책 수립, 표준화 및 기술 지원을 추진하고 있으며, 특히 NIST는 양자내성암호 표준과 관련 기술 지침의 개발을 담당하고 있다. EU는 회원국 간 조정된 양자내성암호 전환을 추진하고 있으며, EU 차원의 정책과 공동 로드맵을 바탕으로 주요 회원국도 자국 환경에 맞는 전환 정책과 계획을 마련하고 있다.

대한민국은 국가 암호 인프라의 주권을 확보하고 미래 양자컴퓨팅 위협에 선제적으로 대응하기 위해 범정부 차원의 양자내성암호 전환을 추진하고 있다. 정부는 중장기 전환 계획을 수립하는 한편, 국내 표준화와 실증 사업, 인증제도 개선 등을 병행하며 국가 차원의 전환 기반을 마련하고 있다.

미국, 영국, 캐나다 등의 주요국이 2030~2031년 고위험 · 민감 시스템 선행 전환과 2035년 전체 전환 완료라는 이중 목표 기한 구조로 수렴하고 있다. [표 7]은 주요 국가 및 글로벌 사이버보안 표준화 기구들의 양자내성암호 전면 전환 목표와 고우선순위 시스템의 선행 전환 시한을 보여준다.

[표 7] 주요 국가의 양자내성암호 전환 목표 비교

국가		전체 전환 목표	고우선순위 전환 목표	특이사항
미국	연방정부 [35, 33]	2035	2031	• 고가치자산 · 고영향 시스템 우선 전환 • 키 설정은 2030년, 전자서명은 2031년까지 전환 • 2035년까지 나머지 연방 시스템 전환 완료
	국방부 [32, 21]	2031	–	• 2030년까지 모든 시스템이 양자내성암호 지원. 미지원 시스템은 퇴출 • 2031년까지 모든 시스템에 양자내성암호 사용 • 국가안보시스템은 CNSA 2.0 적용

국가	전체 전환 목표	고우선순위 전환 목표	특이사항
독일 [27, 13]	2035	2030	• 장기 기밀성이 요구되는 고도로 민감한 응용 우선 전환 • 하이브리드 사용 권고 • 고수준보안 응용에서는 하이브리드 방식 요구
프랑스 [10, 11]	–	–	• 3단계 점진적 전환 • 하이브리드 방식 중심의 양자내성암호 전환 권고 • 하이브리드 양자내성암호 적용 제품에 대한 보안 인증 추진
EU [27]	2035	2030	• 데이터별 전환 완료 시점 – ~2030년 : 고위험 데이터 – ~2035년 : 중위험 데이터
영국 [36]	2035	2031	• 3단계 전환 – 2028년 : 발견 · 계획, – 2031년 : 고우선순위 전환 – 2035년 : 전체 전환
대한민국 [2, 3]	2035	*	• KpqC 알고리즘 선정 및 국내 표준화 추진 • 기관 · 분야별 위험도와 전환 우선순위를 고려한 단계적 전환 추진 • 하이브리드 양자내성암호 적용 제품에 대한 보안 인증 추진
캐나다 [14]	2035	2031	• 연방정부 의무 • 2026년 4월 전환 계획 제출
일본 [17]	2035	–	• 정부 시스템 대상 • 장기적 관점에서 선제적 전환 준비
싱가포르 [18]	–	–	• 양자 준비도 지수를 통한 조직별 양자안전 준비 수준 자가진단 • CII(Critical Information Infrastructure) 운영자 · 정부기관 등을 중심으로 단계적 전환 준비 지원

* 대한민국도 본 가이드북에서 기밀·기반시설 등의 주요시스템에 대해 2031년까지 우선 적용을 권고하고 있다.

주요국은 위험도와 우선순위를 고려하여 단계적인 양자내성암호 전환을 추진하고 있으며, 본 가이드북의 전환 방향도 이러한 국제적 추세와 부합한다. 다만 구체적인 전환 대상과 시기는 기관별 위험평가 결과와 국가 암호정책 및 검증 제도를 고려하여 결정해야 하며, 이를 위해서는 시스템의 중요도와 전환 여건을 고려한 점진적인 전환 전략이 필요하다.

제3절 점진적 전환 전략의 필요성

양자내성암호 전환은 단순히 개별 암호 알고리즘을 교체하는 작업이 아니라, 양자컴퓨터의 암호해독 공격에 취약한(이하 '양자취약'이라 통칭한다) 공개 키 암호가 적용된 프로토콜 · 암호체계 · 인프라 등을 단계적으로 변경하는 장기적인 전환 과정이다. 미국 NIST는 새로운 양자내성암호 알고리즘을 도입하기 위한 프로토콜 · 암호체계 · 인프라의 변경에 수십 년이 소요될 수 있다고 설명하고 있으며, 일본 CRYPTREC도 RSA와 ECC가 제안에서 사회적 보급까지 약 20년이 소요된 점을 들어 양자내성암호 역시 이와 유사한 기간이 필요할 것으로 예상하고 있다[17, 31].

따라서 양자내성암호 전환은 단기간에 일괄적으로 추진하기보다 기존 시스템과 서비스의 연속성, 기술 · 제품의 준비 수준 및 전환에 따른 영향을 고려하여 단계적으로 추진해야 한다. 특히 국가 · 공공기관은 전환 과정에서 공공서비스와 주요 인프라의 안정성을 유지하면서 장기간에 걸친 전환을 체계적으로 관리하는 것이 중요하다. 이를 위해 전환 과정에서 고려해야 할 핵심 사항을 [표 8]과 같이 정리하였다.

[표 8] 양자내성암호 전환 시 고려해야 하는 핵심 사항

핵심 고려 사항	세부 과제 및 필요성	전환 시 주요 고려사항
운영 연속성 확보	대민 · 행정 서비스의 중단 및 장애 최소화 전환 수행	• 캐나다(CCCS) – 영향 평가 · 롤백(Rollback) 계획 · 스테이징 검증 · 전환 후 모니터링을 포함한 변경관리 권고[14]

핵심 고려 사항	세부 과제 및 필요성	전환 시 주요 고려사항
상호운용성 유지	부처 및 기관 간 연계망의 단계적 호환성 확보	• 캐나다(CCCS) – 미전환 레거시망과의 호환을 위한 일정 기간 하위 호환 프로토콜 유지[14]
기술 성숙도 반영	표준 및 최신 구현체의 기술적 안정성에 맞춘 단계적 전환	• 미국(Meta 실사례) – liboqs의 멀티스레딩 충돌 사례를 통해 양자내성암호 구현체의 사전 검증 필요성 확인[25]
하이브리드 활용	과도기 보안 강화를 위해 기존 공개 키 암호와 양자내성암호 병행	• EU 18개국 사이버보안 기관 공동성명 – 대부분의 사용 사례에서 하이브리드 방식 활용을 강하게 권고[19]
실전 적용 사례 반영	대규모 상용화 사례에서 확인된 기술 장애 요인에 대한 선제 대응	• 미국(Cloudflare · Google 적용 사례) – 양자내성암호 적용에 따른 패킷 분할 · 지연 증가 · 연결 장애 사례를 통해 네트워크 영향 사전 검증 필요[16, 22]

AIVD · CWI · TNO가 공동으로 발간한 「The PQC Migration Handbook」은 시스템별 양자 위험 수준과 조직의 위험 수용 수준을 고려하여 전환 시나리오를 긴급(Urgent), 준긴급(Semi-Urgent), 일반(Less Urgent)으로 구분한다[9]. 본 가이드북은 이를 참고하여 국내 국가 · 공공기관의 환경과 암호 검증 체계를 고려한 단계별 전환 시나리오 예시를 [표 9]와 같이 제시한다.

[표 9] 단계별 전환 시나리오 예시

대상	예시	전환 착수 일정	전환 시나리오
긴급 전환 (Urgent)	• 주민 · 세무 대규모 개인정보 보유 시스템 • 국가안보망 • 수명 10년 이상의 장기보존 인프라	즉시 착수 (M+12개월 내 시범 검증 완료)	• 선제적으로 자산 식별, 위험 요인 평가 개시 • 하이브리드-AND 프로토콜을 사전 테스트베드에 긴급 시범 적용
준긴급 전환 (Semi-Urgent)	• 행정망 내부 VPN • 타 부처 연계망 • 일반 대민 서비스 웹 서버	단계적 대기 및 진입 (M+18개월 내 전환 조달 완료)	• CBOM 등 암호자산 인벤토리와 시스템 간 의존 관계를 사전에 파악 • 양자내성암호 라이브러리, 국내외 검증필 암호모듈 및 상용 제품 등의 가용 시점을 고려하여 조달-시험-전환 추진 • 연계기관의 전환 일정과 호환성을 함께 고려
일반 전환 (Less Urgent)	• 내부 테스트 서버 • 단기 운용 웹사이트 • 외부 연계가 없는 격리된 독립 시스템	생태계 성숙 후 순차적 전환	• 상위 인증기관 및 주변 연동망의 전환이 완전히 완료된 후 점진적 전환 추진 • 레거시 암호와의 하위 호환성을 장기 유지하며 최하순위로 자연스러운 교체 유도

이러한 단계적 전환을 위해서는 우선 기관 내 암호 사용 지점을 파악하고, 양자내성암호 전환에 따른 파급 범위를 검토할 필요가 있다. 암호 사용 지점의 진단과 전환 파급 범위에 관한 구체적인 내용은 2장에서 다룬다.

1장 핵심 정리 — 실무자가 기억해야 할 8가지

1. 양자내성암호 전환의 핵심 대상은 '공개 키 암호'입니다.
2. 양자컴퓨터의 실현은 이제 '만약(If)'이 아니라, '언제(When)'와 '어떻게(How)'의 문제입니다.
3. '지금 수집하고 나중에 해독'하는 HNDL 공격은 이미 현재 진행형입니다.
4. 전환 소요 시간과 데이터 보호 기간의 합이 위협 도래 시간보다 길다면, 이미 위험 상태입니다.
5. 양자내성암호는 기존 공개 키 암호 대비 키와 서명의 크기가 대체로 증가하므로, 이에 따른 시스템 영향을 검토해야 합니다.
6. 전환 과도기에는 하이브리드-AND 방식을 우선적으로 검토합니다.
7. 주요국은 고위험·고가치·민감 시스템 등에 대하여 2030~2031년을 공통 중간 마일스톤으로 설정해 선행 전환을 추진하고 있습니다
8. 글로벌 공통 전환 완료의 목표 지향점은 2035년입니다.

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



Chapter 02

국가·공공기관 암호 사용 지점 진단과 전환 파급 범위

Chapter 02

국가·공공기관 암호 사용 지점 진단과 전환 파급 범위

기관이 양자내성암호 전환을 준비할 때 가장 먼저 부딪치는 질문은 “우리 기관의 무엇을 바꾸어야 하는가”이다. 이 질문에 답하지 못하면 전환 계획, 예산, 일정 등을 구체적으로 수립하기 어렵다.

암호는 시스템 곳곳에 눈에 보이지 않게 들어가 있다. 직원이 매일 사용하는 행정정보시스템 로그인, 부서 간 문서 송수신, 민원포털 인증, 백업 데이터의 저장, 외부 기관과의 데이터 연계 등 다양한 과정에서 암호가 작동하고 있지만, 실제로 이를 의식하면서 일하는 사람은 거의 없다. 이러한 특성 때문에, 전환을 시작하기 전에 암호가 어디에 어떤 방식으로 쓰이고 있는지부터 그림을 그리는 작업이 필요하다.

본 장은 그 그림의 기초가 되는 다섯 개의 암호 사용 지점을 2장 1절에서 제시하고, 암호 교체를 넘어 시스템·운영 전반에 미치는 양자내성암호 전환의 파급 효과를 2장 2절에서 정리한다. 본 장의 이해는 4장 단계별 전환 실행 가이드의 출발점이 된다.

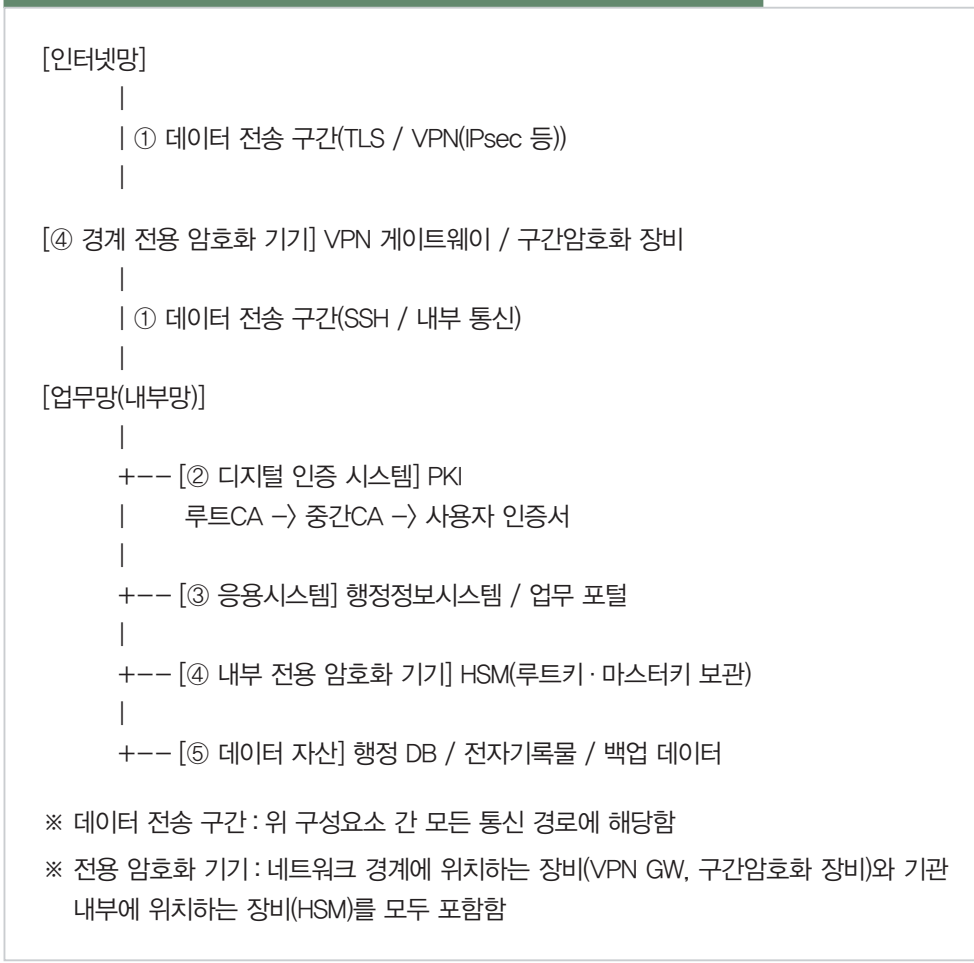
제1절 기관 시스템 내 암호 사용 지점

암호기술은 정보의 수집, 가공, 저장, 송수신 중에 정보의 위·변조, 유출, 훼손 등으로부터 보호하기 위한 기술적 수단 및 방법론의 집합이다. 기관 시스템에서 암호가 작동하는 위치는 매우 다양하지만, 이를 다섯 개의 지점으로 묶어 볼 수 있다.

본 가이드북에서는 기관의 시스템 환경을 망 구성, 시스템 배치환경, 서비스 유형 등 서로 다른 관점으로 구분하여 표현한다. 망 구성은 업무망, 인터넷

망, 폐쇄망 및 기관 간 연계 구간 등 네트워크의 연결 구조를 의미하고, 시스템 배치환경은 기관 자체 구축 환경과 클라우드 환경 등 시스템이 구축·운영되는 형태를 의미한다. 서비스 유형은 대국민 서비스, 내부 업무 서비스, 기관 간 연계 서비스 등 서비스 제공 대상을 기준으로 구분한다. 이들 요소는 서로 독립적으로 조합될 수 있으며, 본 가이드북에서 '운영 환경'은 이러한 요소와 실제 운영 특성을 종합적으로 지칭하는 일반적인 표현으로 사용한다.

[그림 3] 전형적인 국가·공공기관 IT 아키텍처 내 5대 암호 사용 지점



※ 데이터 전송 구간 : 위 구성요소 간 모든 통신 경로에 해당함

※ 전용 암호화 기기 : 네트워크 경계에 위치하는 장비(VPN GW, 구간암호화 장비)와 기관 내부에 위치하는 장비(HSM)를 모두 포함함

국가정보원이 운영하는 국가 망 보안체계(N2SF)는 각급기관의 업무정보와 정보시스템을 식별하고, 업무 중요도에 따라 C(기밀, Classified), S(민감, Sensitive), O(공개, Open) 등급으로 분류한 후 등급별로 차등적인 보안통제를 적용하는 보안 프레임워크이다. 또한 정보시스템의 물리적·논리적 위치도 C/S/O 등급과 연계하여 위협식별과 보안대책 수립에 활용한다.

따라서 본 가이드북의 5대 암호 사용 지점 자체를 N2SF 등급으로 분류하기보다는, 각 암호 사용 지점과 관련된 업무정보·정보시스템·위치의 C/S/O 등급과 보안통제 우선 검토사항을 확인할 필요가 있다. 이러한 결과는 데이터 중요도, 보호 필요기간, 외부 노출 수준, 기관 간 연계 등 양자내성암호 전환 위험요소와 함께 전환 우선순위를 판단하는 참고 자료로 활용할 수 있다.

암호모듈 적용과 보안적합성 검증에 관한 구체적인 요건은 N2SF 등급만으로 결정하지 않고, 해당 정보시스템에 적용되는 관련 법령·지침과 국가 암호정책 및 검증기준을 별도로 확인해야 한다.

암호기술이 적용되는 주요 다섯 개의 지점과 세부 설명 및 요구되는 핵심 암호기능은 다음 표와 같다.

[표 10] 암호기술 주요 적용 5대 지점 및 요구 기능

지점		설명	주요 요구 암호기능
1	데이터 전송 구간	시스템 간 데이터가 오가는 통신 경로	– 데이터 기밀성(구간 대칭 키 암호화) – 데이터 무결성(MAC 패킷 검증) – 세션키 설정(TLS/VPN 핸드셰이크의 키 교환·키 캡슐화) – 통신 상대 인증(TLS 서버 인증, VPN 피어 인증 등)
2	디지털 인증 시스템	디지털 환경에서 신원을 증명·확인하는 인프라	– 사용자 신원확인(GPKI/NPKI 인증서 인증) – 행위 부인방지(전자서명을 통한 서명자 및 서명 행위 확인) – 데이터 무결성(전자서명 검증을 통한 위·변조 확인)
3	응용시스템	기관의 업무를 처리하는 소프트웨어	– 사용자 신원확인(업무 웹 포털 로그인) – 데이터 기밀성(DB 내 민감 개인정보 암호화) – 데이터 무결성(입출력 메시지 유효성 검증)

지점		설명	주요 요구 암호기능
4	전용 암호화 기기	암호 연산과 암호 키 관리를 전용 장비 형태로 수행하는 구성요소	– 데이터 기밀성(HSM 내 루트 개인 키 암호학적 격리) – 사용자 신원확인(VPN 게이트웨이 인증) – 행위 부인방지(HSM 내 전자서명 연산의 감사 가능성 보장)
5	데이터 자산	보호해야 할 정보 그 자체	– 데이터 기밀성(장기 보존 대상 정보 암호화) – 데이터 무결성(행정 기록물 위·변조 방지) – 행위 부인방지(양자내성암호 기반 기록물 중복서명 각인)

용어 : 암호기술의 주요 기능

- **데이터 기밀성** : 허락되지 않는 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 기능
- **데이터 무결성** : 허락되지 않는 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 기능
- **사용자 신원확인** : 사용자 또는 객체의 디지털 정체성(identity)을 식별하는 기능
- **행위 부인방지** : 전자적으로 특정 행위를 한 사실을 부인하지 못하도록 하는 기능

❶ 데이터 전송 구간

데이터 전송 구간이란 시스템 간에 데이터가 오가는 통신 경로를 의미한다. 이 구간에서는 TLS, SSH, IPsec 등의 보안 프로토콜이나 VPN과 같은 보안 통신 방식을 이용하여 전송 데이터의 기밀성과 무결성을 보호한다. 이러한 보호가 적절하게 적용된 경우 공격자가 네트워크상에서 전송 중인 데이터를 가로채더라도 그 내용을 확인하거나 임의로 위·변조하기 어렵다.

예시 : 데이터 전송구간

- 직원이 행정정보시스템에 접속할 때(TLS)
- 여러 지역에 위치한 기관 간 내부망 연결, 또는 외부에서 기관 내부망에 접속할 때(VPN)
- 시스템 관리자가 서버에 원격 접속해 점검할 때(SSH)
- 공공기관 데이터센터 내 서버 간 직접 통신 보호(IPsec–양자내성암호 키 교환 적용 시 IKEv2 필요)

통신 과정에서는 먼저 통신 주체 간 신원을 확인하고, 데이터를 보호하는 데 사용할 키를 안전하게 공유한 후 실제 데이터를 암호화하여 전송한다. 이 과정에서 사용자 신원확인, 키 교환, 데이터 기밀성 및 무결성 등을 위한 암호기술이 사용된다.

데이터 전송 보안에는 키 교환과 사용자 신원확인 등에 사용되는 공개 키 암호와 데이터 암호화에 사용되는 대칭 키 암호가 함께 사용된다. 다만 공개 키 암호와 대칭 키 암호는 양자컴퓨터에 의한 위협의 영향과 이에 필요한 대응 방식이 서로 다르므로, 양자내성암호 전환 시 이를 구분하여 검토할 필요가 있다.

데이터 전송 구간에서 양자내성암호 전환의 핵심 대상은 **TLS/VPN 핸드셰이크의 키 설정 및 인증 단계**이다. 실제 데이터를 암호화하는 AES·ARIA 같은 대칭 키 암호는 양자내성암호 전환 대상이 아니다. 따라서 실무자는 TLS를 사용하고 있으므로 전체 암호체계를 교체해야 한다기보다, TLS 내에서 양자취약 공개 키 암호가 사용되는 키 설정 및 인증 구간을 식별하여 **전환 범위를 파악**할 필요가 있다. 최근 주요 브라우저와 통신 프로토콜을 중심으로 기존 공개 키 암호와 양자내성암호를 결합한 하이브리드 방식의 적용과 지원이 확대되고 있어, 실제 서비스 환경에서도 양자내성암호 전환을 고려할 필요가 있다. 참고로 일부 주요 브라우저에서는 TLS 키 설정 과정에 기존 공개 키 암호와 ML-KEM을 결합한 하이브리드 방식을 적용하고 있다.

실무 시나리오

행정정보시스템의 TLS 설정을 점검하던 보안 담당자는 운영 중인 웹서버가 TLS 1.2만 지원한다는 사실을 확인했다. 현재 표준화된 ML-KEM 기반 하이브리드 키 교환을 적용하려면 TLS 1.3을 사용해야 하므로, 웹서버의 TLS 1.3 지원 여부를 우선 확인해야 했다. 그러나 TLS 1.3으로 업그레이드하는 과정에서 일부 구형 업무 단말과 방화벽이 TLS 1.3을 지원하지 않아 호환성 문제가 발생할 수 있음을 확인했다.

⇨ 양자내성암호 전환을 준비할 때는 서버의 암호 설정뿐 아니라, 통신 경로 전반의 TLS 버전 지원 현황과 호환성부터 파악해야 한다.

실무 담당자용 1분 자가진단 : 데이터 전송 구간

- **핵심 질문** : "우리 기관 홈페이지와 중요 서버 연계망, 그리고 내부 원격 관리에 쓰이는 웹서버/보안장비의 프로토콜 버전이 TLS 1.3인가?"
- **자가진단 Action** :
  1. 외부 노출 웹 서버와 내부 VPN 통신망의 TLS 설정 값을 확인하여 TLS 1.2 이하로 제한되어 있는지 점검한다.
  2. 자체 점검과 공급업체 확인 등을 통해 하이브리드 키 설정 기능의 현재 지원 여부와 향후 지원 계획을 확인한다.

용어

- **SSL**(Secure Sockets Layer) : 인터넷상에서 데이터 통신 보안을 제공하는 암호 프로토콜
- **TLS**(Transport Layer Security) : 인터넷상에서 데이터의 도청이나 변조를 막기 위한 암호 프로토콜. SSL의 보안 취약점을 개선한 후속 표준으로, SSL의 모든 버전은 현재 폐기(deprecated)되어 사용이 권장되지 않는다. TLS 1.3(RFC 8446, 2018)에서는 핸드셰이크 구조, 암호 스위트(cipher suite) 구성 및 키 유도 방식이 이전 버전과 크게 달라졌다. 양자내성암호 전환 시에는 TLS 1.3의 키 교환 과정에서 양자내성 KEM 또는 기존 키 교환 방식과 결합한 하이브리드 방식을 활용할 수 있다.
- **VPN**(Virtual Private Network) : 공중망 상에 사설망을 구축하여 마치 사설 구내망 또는 전용망 같이 이용하는 통신망. 구현 방식에 따라 IPsec VPN, SSL VPN 등이 있다.
- **SSH**(Secure Shell) : 보안 순위가 낮은 네트워크상에서 보안 순위가 높은 원격 접속 개시나 데이터 전송을 실현하는 프로토콜. OpenSSH 9.9부터 ML-KEM-768과 X25519를 결합한 하이브리드 키 교환 방식(mlkem768x25519-sha256)이 추가되었으며, OpenSSH 10.0(2025년)부터 해당 방식이 기본 키 교환 방식으로 채택됨.
- **IPsec**(Internet Protocol Security) : 망 계층(network layer)인 인터넷 프로토콜(IP)에서 보안성을 제공해 주는 표준화된 기술. IPsec에서 RFC 9370에 따른 양자내성암호 키 교환을 적용하려면 IKEv2(RFC 7296) 환경이 필요하며, RFC 9370의 다중 키 교환(Multiple Key Exchanges) 방식을 이용하면 기존 키 교환과 양자내성암호 키 교환을 연속적으로 수행하여 양자내성 키 교환을 적용할 수 있다. 따라서 IKEv1을 사용하는 시스템은 IKEv2로의 전환을 함께 검토해야 한다.

❷ 디지털 인증 시스템

디지털 인증 시스템이란 디지털 환경에서 사용자, 기기, 또는 소프트웨어의 신원을 확인하고 권한을 부여하는 보안 체계이다.

예시 : 디지털 인증 시스템

- **행정전자서명 인증서(GPKI)** : 행정기관 · 공무원의 디지털 신원 확인과 공문서 처리(예 : 시스템 로그인, 공문서 결재, 기관 간 문서 송수신)
- **공동인증서(NPKI)** : 국민의 본인 확인과 전자거래(예 : 정부24 민원 신청, 홈택스 세금 신고)

여기서 암호가 하는 일. 이 지점의 핵심 암호 기법은 전자서명이다. 인증기관(CA)은 자신의 개인 키로 인증서에 서명하여 "이 공개 키가 해당 사용자 · 기기 · 서비스에 속한다"는 사실을 보증한다. 사용자는 인증서의 공개 키에 대응하는 자신의 개인 키로 전자서명을 생성하며, 이를 통해 해당 개인 키의 보유 여부와 서명된 데이터의 무결성을 확인할 수 있다. 즉 인증서는 공개 키와 신원 정보를 연결하여 CA가 보증한 문서이고, 전자서명은 해당 공개 키와 쌍을 이루는 개인 키로 생성되어 서명자 확인과 데이터 무결성 검증에 활용된다. 이러한 보증은 일반적으로 루트 CA → 중간 CA → 사용자 · 서버 인증서와 같은 인증서 체인을 통해 이어지며, 각 전자서명 인증체계(PKI)가 적용되는 분야 안에서 디지털 신원 확인의 기반이 된다.

양자내성 전자서명 알고리즘을 전자서명 인증서비스에 적용할 경우에는 「전자서명법」에 따른 전자서명인증업무 운영기준(2022.4.20. 시행, 과학기술정보통신부고시 제2022-5호)과 관련 기술기준의 적용 여부를 함께 검토할 필요가 있다. 특히 현행 「전자서명법」 제7조제2항은 전자서명 및 전자문서의 위 · 변조 방지대책, 가입자 확인방법, 관련 시설 및 자료의 보호방법 등을 포함한 전자서명인증업무 운영기준을 과학기술정보통신부장관이 정하여 고시하도록 하고 있다. 또한, GPKI(행정전자서명 인증체계)에 대해서는 「전자정부법」 제29조 및 동법 시행령 제34조제3항에 따른 '행정전자서명 인증업무지침'(2026.5.18.,

행정안전부고시 제2026-34호)의 평가 · 인증 기준 개정 및 적용 여부도 검토할 필요가 있다.

해당 지점에서 양자내성암호 전환 대상. 디지털 인증 시스템에서 쓰는 핵심 암호는 대부분 공개 키 암호 영역에 속한다. 따라서 전자서명 인증체계에서 사용되는 전자서명과 인증서 발급 · 검증 체계는 양자내성 전자서명을 수용할 수 있도록 전환 계획을 세워야 한다. 전환 대상에는 루트 CA와 중간 CA의 키, CA가 발급하는 사용자 인증서 · 서버 인증서 · 코드서명 인증서 등의 키 쌍, 인증서 검증을 수행하는 업무시스템과 단말 환경이 포함된다.

다만 전자서명 인증체계 전환은 CA 키만 먼저 바꾸면 끝나는 작업이 아니다. 기존 공개 키 암호 기반 인증서를 즉시 폐기하기 어렵기 때문에, 일정 기간 기존 인증서 체계와 양자내성암호 기반 인증서 체계를 병행 운영해야 할 수 있다. 또한 새 인증서를 발급하더라도 이용자 단말, 서버, 브라우저, 보안장비, 업무시스템이 해당 전자서명과 인증서 형식을 검증할 수 있어야 실제 적용이 가능하다. 따라서 기관은 상위 인증기관의 전환 일정, 하위 인증서 발급 정책, 인증서 배포 방식, 검증 소프트웨어의 지원 여부, 기관 간 호환성 시험을 함께 고려해야 한다.

특히 한국 공공 전자서명 인증체계의 핵심적 특성인 **GPKI-NPKI 간 상호연동(cross-certification) 및 행정정보 공동이용 시스템을 통한 다기관 연계 검증 체계**에 미치는 영향을 간과할 수 없다. 양자내성암호 도입 시 전자서명 알고리즘이나 키 형식 불일치로 상호 연동 검증이 실패할 수 있으므로, 상위 루트 CA 간 양자내성암호 적용 방식에 대한 합의와 크로스 인증서 갱신 계획을 우선 수립하고, 이에 맞춰 하위 응용시스템의 라이브러리 연동 테스트를 유기적으로 설계할 필요가 있다.

실전 교훈 – 인증서 체인의 연쇄 파급 : GPKI 루트 CA가 양자내성 전자서명으로 전환되면, 그 루트 CA가 서명한 모든 중간 CA 인증서와 하위 사용자 · 서버 인증서까지 재발급이 필요할 수 있다. 여기에 더해 재발급된 인증서를 검증하는 업무시스템 · 보안장비 · 브라우저 · 모바일 앱이 새로운 서명과 키 형식을 지원하지 않으면 인증 자체가 실패한다. 루트 CA 한 곳의 암호 교체가 연계된 수십만 개 인증서와 이를 검증하는 수천 개 시스템 전체로 파급되는 구조이므로, **루트 CA**

전환 전에 하위 체계의 양자내성암호 지원 여부를 반드시 사전 점검해야 한다.

실무 시나리오

행정전자서명(GPKI) 담당자는 상위 인증기관으로부터 "2028년부터 중간 CA 인증서에 양자내성암호가 적용될 예정"임을 통보받았다. GPKI 인증서를 검증하는 시스템 목록을 확인한 결과 행정정보시스템·민원포털·문서관리시스템·모바일 앱을 포함해 7개에 달했고, 그 중 4개 시스템의 인증서 검증 라이브러리가 양자내성암호를 아직 지원하지 않았다. CA 교체 전에 각 시스템의 라이브러리 업데이트가 선행되어야 했으며, 이에 따라 추가 예산과 일정 조정이 필요했다.

⇨ 전자서명 인증체계 전환 계획은 CA의 전환 일정만이 아니라 검증 라이브러리 현황 파악부터 시작해야 한다.

실무 담당자용 1분 자가진단 : 디지털 인증 시스템

- **핵심 질문** : "상위 CA(GPKI/NPKI 등)로부터 양자내성암호 인증서가 발급될 때, 우리 기관의 하위 단말과 업무 시스템이 이를 성공적으로 검증할 수 있는가?"
- **자가진단 Action** :
  1. 기관이 발급받아 사용하는 인증서(공무원용 GPKI, 공동인증서 등)의 전체 개수와 해당 인증서를 검증하는 시스템 목록을 취합한다.
  2. 각 검증 시스템의 양자내성암호 적용 가능 여부와 관련 보안 라이브러리의 지원 계획을 해당 공급업체에 공식 질의한다.

❸ 응용시스템(암호 라이브러리/모듈)

응용시스템은 기관의 업무를 처리하기 위해 사용하는 소프트웨어이다. 로그인, 데이터 저장, 문서 처리, 시스템 간 연계, 배치 작업 등은 응용시스템이 수행하는 업무 기능이며, 이 과정에서 사용자 확인, 데이터 보호, 문서 위·변조 방지 등을 위해 암호기능이 사용된다.

예시 : 응용시스템

- 행정정보시스템 로그인 과정에서 인증서, 일회용 인증값, 비밀번호 기반 키 유도 함수 등을 이용해 사용자를 확인하는 경우
- 정부24 등 민원포털에서 본인확인 서비스나 인증서를 호출해 민원 신청자의 신원을 확인하는 경우
- 주민 · 세무 · 복지 등 행정 데이터베이스에 저장되는 민감 항목을 암호화하는 경우
- 타 기관 시스템과 API로 데이터를 주고받을 때 요청 · 응답의 출처, 위 · 변조 여부, 민감정보 보호를 확인하는 보안 기능을 사용하는 경우
- 야간 배치 작업에서 대량의 자료를 암호화 · 복호화하여 데이터베이스에 저장하는 경우
- 클라우드 · SaaS 기반 업무시스템에서 사용자 인증, 저장 데이터 암호화, 연계 API 보호 기능을 사용하는 경우

여기서 암호가 하는 일. 응용시스템은 사용자 확인, 데이터 저장 시 암호화, 시스템 간 요청 · 응답 보호, 전자문서 서명 등 여러 암호기능을 업무 처리 과정에 결합해 사용한다. KISA 동향조사에 따르면 공개 키 암호 활용 제품의 판매 산업군 중 행정 분야가 34.7%를 차지하며, 세부적으로는 행정 데이터베이스(21.7%), 전자정부(17.4%), 정책 및 계획 관리 시스템(10.4%) 순으로 활용되고 있다[8].

양자내성암호 전환 시 유의할 점. 응용시스템은 암호기능을 직접 구현하기보다 암호 라이브러리, 암호모듈, 통신 프로토콜, 운영체제 기능을 호출해 사용하는 경우가 많다. 따라서 응용시스템을 점검할 때는 화면이나 업무 기능만 볼 것이 아니라, 그 기능이 어떤 암호, 인증서, 암호 키, 외부 보안 모듈에 의존하는지도 함께 확인해야 한다. 실제 점검 방법으로는 소스코드 내 암호 함수 · 라이브러리 호출 검색(정적 분석), SBOM/CBOM 도구를 활용한 의존성 자동 추출, 네트워크 패킷 캡처를 통한 통신 구간 암호 식별 등이 있다.

용어

- **암호 라이브러리** : 암호 알고리즘과 관련 기능을 구현한 소프트웨어 모듈. 응용시스템이 암호 연산을 직접 구현하는 대신 OpenSSL, BouncyCastle 등 암호기능을 제공하는 라이브러리나 모듈을 호출하여 사용한다.
- **암호자산 명세서**(CBOM, Cryptographic Bill of Materials) : 소프트웨어가 사용하는 암호·라이브러리·인증서·키의 전체 목록. SBOM(소프트웨어 명세서)의 암호 특화 버전이다.
- **정적 분석**(Static Analysis) : 소프트웨어를 실행하지 않고 소스코드·바이트코드를 분석하여 암호 함수 호출 위치와 암호를 식별하는 방법
- **키 유도 함수**(KDF, Key Derivation Function) : 비밀값이나 패스워드 등의 입력값으로부터 용도에 맞는 암호 키를 생성하는 함수. 국가·공공기관에서는 KCMVP 검증대상 키 유도 방식인 KBKDF(HMAC·CMAC 기반), PBKDF(HMAC 기반) 등 적용 환경에서 요구되는 검증 기준을 고려한다.

실무 시나리오

민원처리 시스템의 암호 사용 현황을 목록화하던 개발 담당자는 화면 상 "인증서 로그인"이라는 단일 기능이 실제 소스코드에서는 RSA 호출 코드가 3개 모듈에 분산되어 있음을 발견했다. 더 확인하자 그 중 하나는 이미 지원이 종료된 사내 암호 라이브러리를 직접 참조하고 있었다. 양자내성암호로 전환하려면 라이브러리 교체와 함께 분산된 암호 호출 코드를 중앙 모듈로 정비해야 해서, 처음 예상한 공수를 크게 웃도는 작업이 되었다. 응용시스템의 암호 사용 현황은 화면 기능이 아니라 소스코드와 라이브러리 의존성을 직접 확인해야 파악된다.

실무 담당자용 1분 자가진단 : 응용시스템

- **핵심 질문** : "유지보수 업체나 자체 개발한 소스코드 내에 특정 암호(RSA, ECC 등)가 하드코딩되어 강하게 결합되어 있지는 않은가?"
- **자가진단 Action** :
  1. 소스코드 정적 분석 도구(SAST)를 사용하거나 내부 정기 점검 시 암호 라이브러리 및 API 호출 위치를 전수 점검하여, 설정값 교체만으로 암호 교체가 가능한지 확인한다.
  2. 외부 납품 소프트웨어의 암호 정보가 기술된 CBOM을 조달 및 계약 요건으로 계약 상대자에게 요구하여 사전에 확보한다.

❹ 전용 암호화 기기

전용 암호화 기기는 암호 연산을 수행하거나 암호 키를 생성 · 보관 · 사용하기 위해 별도로 도입 · 운영하는 전용 장비를 의미한다.

예시 : 전용 암호화 기기

- HSM(하드웨어 보안 모듈)에서 인증서 개인 키나 마스터 키를 생성 · 보관 · 사용하는 경우
- VPN 장비 또는 VPN 게이트웨이가 외부 접속자나 기관 간 연결의 인증, 키 교환, 통신 암호화를 수행하는 경우
- 구간암호화 장비가 본청–지청, 데이터센터–재해복구센터 등 특정 네트워크 구간의 통신을 암호화하는 경우
- TLS 복호화 · 검사, SSL VPN, IPsec VPN 기능을 수행하는 방화벽 등 네트워크 보안장비가 인증 · 키 교환 · 암 · 복호화를 처리하는 경우
- KCMVP 검증필 암호모듈을 탑재한 보안장비를 사용하는 경우

여기서 암호가 하는 일. 전용 암호화 기기는 인증, 키 교환, 전자서명, 암호화 · 복호화, 해시값 계산, 암호 키 생성 · 보관 · 사용 같은 실제 암호기능을 수행한다.

양자내성암호 전환 시 유의할 점. 전용 암호화 기기가 기존 RSA · ECC 기반 키 교환이나 전자서명 기능을 수행하고 있다면, 해당 기기가 양자내성암호와 관련 키 · 인증서 형식을 지원하는지 확인해야 한다. 기존 기기가 이를 지원하지 않는 경우에는 펌웨어 업데이트나 암호모듈 업데이트를 통해 지원 가능한지 확인해야 하며, 이마저 불가능한 경우에는 장비 교체가 필요하다.

또한 양자내성암호는 기존 공개 키 암호보다 공개 키, 서명, 암호문 등의 크기가 커질 수 있으므로 기기의 처리 성능, 저장 공간, 인증서 처리 방식, 네트워크 메시지 크기 제한에도 영향을 줄 수 있다. 공공기관에서는 암호기능을 제공하는 제품이나 모듈을 도입할 때 KCMVP 등 국가용 보안요구사항의 충족 여부를 함께 확인해야 하므로, 양자내성암호 전환도 암호 자체뿐 아니라 암호 모듈과 장비에 국가용 보안요구사항이 어떻게 반영되는지를 함께 고려해야 한다.

실무 시나리오 : VPN 장비 수명과 공급업체 로드맵 불일치

도입한 지 4년 된 VPN 게이트웨이의 양자내성암호 지원 여부를 공급업체에 문의한 결과, "양자내성암호 알고리즘은 차기 펌웨어 v6.0에서 지원 예정이나 해당 모델은 v6.0 업그레이드를 지원하지 않아 신규 장비 구매가 필요하다"는 답변이 돌아왔다. 담당자는 해당 장비의 잔여 내용연수 2년과 기관의 양자내성암호 전환 목표 시점을 비교한 결과, 기존 조달 일정대로 장비를 운영할 경우 전환 일정에 차질이 생길 수 있다고 판단하였다. 이에 다음 조달 주기를 앞당겨 양자내성암호 지원 장비로 교체하기로 결정했다.

⇨ 이 기관처럼 전환 검토 시점에 이미 장비 교체 판단이 필요한 경우가 빈번하므로, 공급업체의 양자내성암호 펌웨어 로드맵은 조달 계획 수립 이전에 반드시 확인해야 한다.

실무 시나리오 : HSM 장비의 양자내성암호 지원과 검증필 암호모듈 적용 시차

기관 인증서 발급 CA의 개인 키를 HSM에서 관리하는 담당자는 해당 HSM의 양자내성암호 알고리즘 지원 여부를 공급업체에 문의했다. 공급업체는 "양자내성암호 지원 펌웨어는 내년 상반기 출시 예정이나, 국내외 검증필 암호모듈을 적용하기 위해서는 추가 1~2년이 소요될 것으로 예상된다"고 답변했다. 담당자는 펌웨어 출시 직후 양자내성암호로 전환할 수 있을 것으로 예상했으나, 기관의 보안 요구사항과 검증필 암호모듈 적용 여부를 검토한 결과 실제 도입 가능 시점이 달라질 수 있음을 확인하였다.

⇨ 기관의 CA 양자내성암호 전환 일정은 HSM 공급업체의 제품 출시 일정이 아니라 검증필 암호모듈 적용 여부에 따른 일정을 고려하여 수립해야 한다. 전용 암호화 기기의 양자내성암호 전환 가능 시점은 공급업체 로드맵과 검증필 암호모듈 적용 일정 및 여부를 구분하여 확인한다.

실무 담당자용 1분 자가진단 : 전용 암호화 기기

- **핵심 질문** : "내용연수가 남아 있는 기존 하드웨어(HSM, VPN 장비 등)의 양자내성암호 전환 비용과 양자내성암호를 적용한 검증필 암호모듈 적용 일정을 고려하였는가?"
- **자가진단** Action :
  1. 운영 중인 전용 보안장비(구간암호화 장비, HSM 등)의 단종 주기와 잔여 감가상각 기간을 파악한다.
  2. 공급업체에 펌웨어 수준에서 양자내성암호 하이브리드를 업그레이드로 지원할 수 있는지, 혹은 신규 칩셋 도입이 수반되는 하드웨어 교체가 필요한지 여부를 확인하여 중장기 교체 계획을 수립한다.

❺ 데이터 자산(장기보존 · 민감정보)

2장 1절 ❶부터 2장 1절 ❹까지는 암호가 어디에서 어떻게 사용되는지를 파악하는 것이라면, 데이터 자산은 해당 암호기술이 어떤 정보를 보호하고 있는지를 파악하는 데 초점을 둔다. 동일한 암호기술을 사용하더라도 보호 대상 데이터의 중요도와 보호 기간, 외부 제공 · 연계 여부 등에 따라 양자내성암호 전환의 필요성과 우선순위가 달라질 수 있으므로, 기관은 암호자산과 함께 해당 암호자산이 보호하는 데이터의 특성을 확인할 필요가 있다.

기밀성 보호 기간이 긴 전자기록물, 행정문서, 증빙 자료 등은 기록물의 특성에 따라 장기간 기밀성 · 무결성 · 진본성 등 요구되는 보안속성을 유지할 필요가 있다. 「공공기록물 관리에 관한 법률 시행령」 제26조는 기록물의 보호 기간이 1년, 3년, 5년, 10년, 30년, 준영구, 영구로 구분하고 있다. 따라서 장기간 보존되는 기록물의 기밀성이나 전자서명 검증 등을 위해 공개 키 암호가 사용되는 경우에는 해당 기록물에 요구되는 보호 기간을 고려하여 양자내성암호 전환 필요성을 검토할 필요가 있다.

암호화되거나 서명된 데이터를 장기간 보존하는 경우에는 기밀성 보호와 전자서명의 장기검증을 구분하여 검토할 필요가 있다. 이와 관련한 저장 데이터의 재암호화, 암호 키 보호방식 전환, 장기검증 및 중복서명 등의 구체적인 대응 방안은 2장 2절 ❹와 5장 7절에서에서 다룬다.

> 진본성(authenticity)이란 「공공기록물 관리에 관한 법률 시행령」 및 암호 표준 지침에 따라 "기록물이나 전자문서가 정당한 권한을 가진 주체에 의해 생성되었고, 임의로 변조되지 않았으며, 공식 절차에 따라 관리되어 온 진짜 기록임을 증명할 수 있는 신뢰성의 성질"을 의미하며, 진본 전자서명 관리 체계 전환의 핵심 원칙이자 기준이 된다.

주민등록번호, 고유식별정보, 바이오정보 등 개인정보 보호 법령에 따라 보호가 요구되는 정보와 국가 기밀정보 · 중요 업무정보 등 유출 시 피해가 큰 정보도 함께 확인해야 한다[1]. 개인정보처리시스템을 운영하는 기관은 관련

법령과 고시에서 정하는 암호화 및 안전성 확보 기준을 준수하고, 향후 양자내성암호 전환과 관련된 기준이나 정책의 변경 여부를 지속적으로 확인할 필요가 있다. 이러한 정보는 단순히 현재 적용된 암호기술만을 확인하는 것이 아니라, 정보의 중요도와 향후 보호가 필요한 기간을 함께 고려하여 현재의 보호체계가 충분한지를 검토해야 한다.

행정정보 공동이용, 타 기관 시스템 연계, 클라우드·SaaS 이용 등을 통해 외부 기관이나 민간 사업자와 주고받는 데이터도 점검 대상에 포함할 필요가 있다. 외부 제공·연계 데이터는 한 기관의 암호체계만 변경할 경우 상대방이 데이터를 정상적으로 처리하거나 검증하지 못할 수 있으므로, 데이터를 제공하는 기관과 이용하는 기관의 암호체계 및 지원 환경을 함께 확인하고 전환 방식과 일정을 조율할 필요가 있다.

데이터 자산의 양자내성암호 전환 우선순위를 판단할 때에는 1장 1절에서 설명한 HNDL 위협을 중요하게 고려해야 한다. 특히 데이터의 보호 필요 기간이 길고 유출 시 피해가 큰 경우에는 양자내성암호 전환 우선순위를 높게 검토할 필요가 있으며, 이는 4장 3절의 우선순위 결정에서 주요 판단 기준으로 활용할 수 있다.

실무 시나리오

30년 보존 의무 전자기록물을 담당하는 기록물관리자는 2010년에 RSA-2048로 서명된 문서 수십만 건의 보호 기간 만료 시점이 2040년임을 확인했다. 이 기간이 양자컴퓨터 등장 예상 구간(2031~2041년)과 겹칠 수 있어 양자내성암호 기반 중복서명(over-signing)이 필요한 상황이었다. 그러나 현행 기록관리 시스템이 양자내성암호 타임스탬프와 중복서명을 지원하지 않아, 전면 재서명 이전에 시스템 고도화를 먼저 추진해야 했다.

⇨ 장기보존 데이터의 경우 보호 기간 만료 시점과 양자 위협 구간의 교차 여부를 먼저 계산하고, 그 결과를 기록관리 시스템 고도화 요건에 즉시 반영해야 한다.

실무 시나리오

사회복지 급여 시스템을 운영하는 기관의 DB 담당자는 AES-256으로 암호화된 주민등록번호 200만 건을 관리하고 있었다. 안전해 보였지만, 점검 과정에서 AES 암호화에 사용된 데이터 암호화 키(DEK)가 RSA-2048로 암호화되어 보관되는 방식임을 확인했다.

⇨ 해당 데이터는 수십 년간 보존 의무가 있어 미래 양자컴퓨터 등장 시점까지 보호되어야 하는데, RSA가 양자컴퓨터에 취약해지면 키 래핑(key wrapping)이 풀리는 순간 AES 복호화도 가능해진다. HNDL 공격에 대한 대응은 데이터 자체의 암호화뿐 아니라 암호 키를 보호하는 키 래핑 방식까지 점검해야 완성된다.

실무 담당자용 1분 자가진단 : 데이터 자산

- **핵심 질문** : "우리 기관이 보유한 백업 아카이브 및 30년 이상 장기보존 행정 문서 중 공개키(RSA/ECC)로 암호화/서명된 데이터가 얼마나 존재하는가?"
- **자가진단 Action** :
  1. 데이터 보존 연한이 10년 이상인 암호화 저장소 및 파일의 현황을 조사하여 암호자산 인벤토리 대장에 별도 표기한다.
  2. 기존 RSA-PSS 등으로 서명된 장기보존 전자기록물에 대해, 알고리즘 만료 시점 이전에 양자내성암호 기반 중복서명 및 장기검증 정보를 갱신할 수 있도록 시스템 요구사항 정의에 반영한다.

용어

- **LTV**(Long-Term Validation) : 전자서명에 사용된 인증서가 만료되거나 관련 검증환경이 변경된 이후에도 서명의 유효성을 장기간 검증할 수 있도록 인증서, 인증서 상태정보, 타임스탬프 등 필요한 검증정보를 확보·보존하는 방식으로, 전자서명 시점의 인증서 상태 정보(OCSP·CRL)와 타임스탬프를 함께 저장하는 기법. PAdES-LTV, CAdES-LTV 등의 표준이 있다.
- **중복서명**(Over-signing) : 기존 전자서명 위에 새로운 암호로 추가 전자서명하여 원본 서명의 신뢰 유효기간을 연장하는 기법. 원본 전자서명을 삭제하지 않으므로 법적 증거력을 유지한다.
- **DEK/KEK**(Data Encryption Key / Key Encryption Key) : DEK는 실제 데이터를 암호화하는 키, KEK는 DEK를 암호화(래핑)하는 상위 키. RSA로 DEK를 래핑하면 RSA가 취약해질 때 AES 암호화된 데이터까지 노출될 수 있다.
- **키 래핑**(Key Wrapping) : 암호 키를 다른 키로 암호화하여 안전하게 저장·전송하는 방법. 주로 RSA 또는 AES-Wrap 암호를 사용한다.

❻ 5대 암호 사용 지점 전환 긴급성 자가 점검

2장 1절 ❶부터 2장 1절 ❺까지 살펴본 내용을 바탕으로, 5대 지점별 HNDL 위협 수준, 전환 긴급성, 핵심 전환 대상, 우선 확인 사항을 다음 표로 정리한다. 기관 실무자는 이 표를 자가 진단의 출발점으로 활용하고, 4장에서 구체적인 전환 일정과 우선순위를 수립한다.

[표 11] 5대 암호 사용 지점별 전환 긴급성 자가 점검표

	지점	HNDL 위협	전환 긴급성	핵심 전환 대상	우선 확인 사항	주요 영향 영역 (2장 2절)
1	데이터 전송 구간	높음	매우 높음	TLS·VPN 키 캡슐화 및 인증 암호	현재 운영 중인 TLS 버전과 키 캡슐화 종류 확인	운영·조달·연동
2	디지털 인증 시스템	중간	높음	CA 전자서명·인증서 체인 전체	상위 CA 전환 일정 및 하위 시스템·단말 양자내성암호 지원 여부	운영·연동
3	응용시스템	중간	높음	인증·전자서명·키 캡슐화에 사용하는 공개 키 암호	암호 라이브러리 의존성 및 하드코딩된 암호 여부 파악	운영·조달
4	전용 암호화 장치	중간	높음	장비 내 RSA·ECC 기반 키 캡슐화 및 전자서명 기능	펌웨어·암호모듈 업데이트 가능 여부 및 공급업체 양자내성암호 지원 로드맵	조달
5	데이터 자산	매우 높음	보호 기간 비례	암호화된 장기보존 데이터·서명한 문서	기밀성 보호 기간 10년 이상인 암호화·서명 데이터 목록화	운영·데이터 관리

"높음" = 현재 전송 중인 데이터가 즉시 HNDL 수집 대상이 될 수 있음.
상세 우선순위 산정 방법은 4장 3절 「우선순위 결정 및 전환 전략 수립」을 참조한다.

실무 시나리오 : 양자내성암호 전환 첫 점검에서 드러나는 5개 지점의 과제

A 지자체 정보보안 담당자는 국가정보원 · 행정안전부의 양자내성암호 전환 준비 권고를 받고 소속 기관의 현황을 처음 점검하기로 했다. [표 11]을 기준으로 5개 지점을 하나씩 확인한 결과, 각 지점에서 예상하지 못했던 문제를 발견하였다.

① 데이터 전송 구간 : 행정포털 웹서버는 TLS 1.3을 지원했지만, 본청–지청 간 내부 통신에 사용 중인 IPsec VPN 게이트웨이는 여전히 구형 프로토콜만 지원하고 있었다.

② 디지털 인증 시스템 : GPKI 인증서를 검증하는 시스템이 행정정보시스템 · 민원포털 · 전자결재 등 6개임을 파악했는데, 담당자는 이 목록을 그제야 처음 작성했다.

③ 응용시스템 : 전자결재 시스템 개발사에 암호 라이브러리 버전을 문의하자 "하청 개발사에 확인해야 한다"는 답변이 돌아왔다. 공급망 의존성이 기관 내부에서 파악되지 않는 상태였다.

④ 전용 암호화 기기 : 구간암호화 장비 2종이 운영 중이었는데, 한 공급업체는 양자내성암호 지원 로드맵을 공개했지만 나머지 한 공급업체는 "검토 중"이라는 답변만 반복했다.

⑤ 데이터 자산 : 기밀성 보호 기간 30년인 전자기록물 12만 건 중 2015년 이전에 서명된 것이 3만 건이었다. 전자서명 현황을 기록관리 시스템에서 일괄 조회하는 것이 불가능했다.

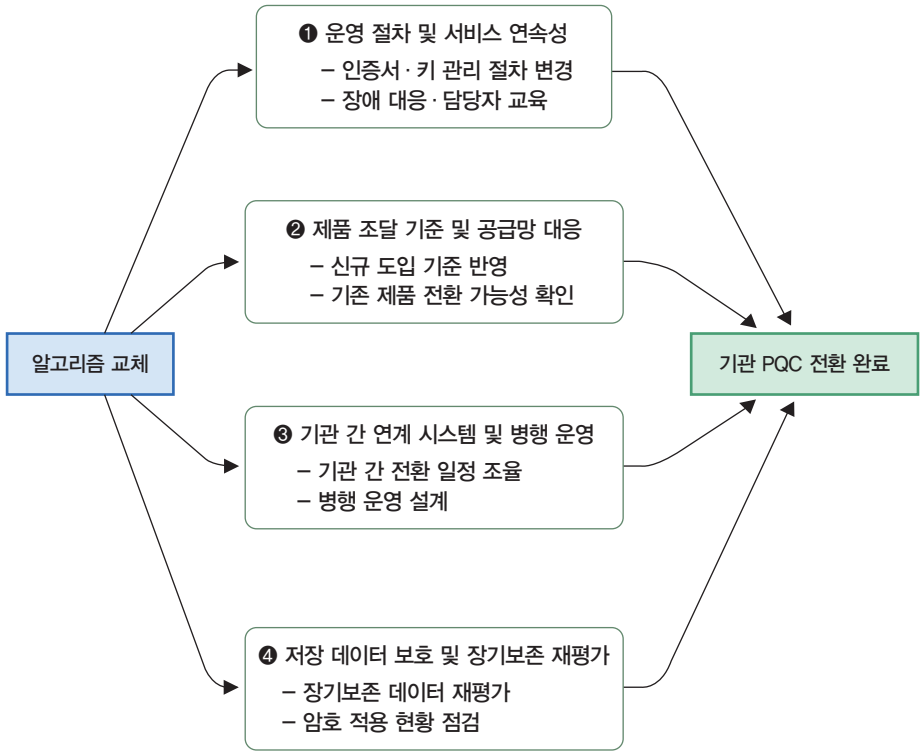
⇨ 담당자는 5개 지점 어디에서도 "준비 완료"라고 말할 수 있는 곳이 없음을 확인했다. 동시에 각 지점이 독립적이지 않다는 것도 드러났다. ③ 응용시스템의 라이브러리 업데이트가 ② CA 전환보다 먼저 완료되어야 했고, ④ 구간암호화 장비 교체는 ① 내부 통신 구간 전환 계획과 연동되어야 했다. 양자내성암호 전환 준비는 5개 지점을 독립적으로 체크하는 것이 아니라, 지점 간 의존 관계를 고려한 순서로 접근해야 한다.

제2절 양자내성암호 전환의 기관 파급 영역

양자내성암호 전환은 단순히 기존 공개 키 암호를 새로운 암호로 바꾸는 작업에 그치지 않는다. 암호가 바뀌면 그 암호를 사용하는 시스템, 인증서와 암호 키 관리 절차, 제품 조달 기준, 기관 간 연계 방식, 장기보존 데이터 관리 방식까지 함께 영향을 받는다.

특히 대부분의 정보시스템은 암호를 손쉽게 교체할 수 있도록 설계되어 있지 않기 때문에, 전환 과정에서는 기술 교체뿐 아니라 운영 절차와 정책도 함께 정비해야 한다. 따라서 양자내성암호 전환의 영향을 다음 그림처럼 네 가지 측면에서 검토할 필요가 있다.

[그림 4] 전환이 기관 전반에 미치는 4개 영역



❶ 운영 절차 및 서비스 연속성

양자내성암호 전환은 암호 알고리즘이나 제품을 교체하는 기술적 작업에 그치지 않고 운영 절차 전반에 영향을 미친다. 인증서와 암호 키의 생애주기 관리, 전환 기간의 운영 방식, 장애 대응 체계, 담당자의 역할과 관련 문서 등을 함께 정비해야 한다. 기술적 전환만 이루어지고 운영 절차가 기존 방식으로 유지될 경우, 전환 이후에도 기존 암호체계가 사용되거나 장애 발생 시 적절하게 대응하지 못하는 등의 운영상 공백이 발생할 수 있다.

양자내성암호 전환에 따라 기존 RSA·ECC 등 양자취약 공개 키 암호를 사용하는 인증서와 암호 키의 교체가 필요한 경우에는 새로운 암호체계에

맞게 생성 · 발급 · 배포 · 보관 · 갱신 · 폐기 등 생애주기 전반의 관리 절차를 검토해야 한다. 특히 인증서와 키의 형식이나 크기, 지원 알고리즘, 저장 · 관리 방식 등이 달라질 수 있으므로, 이러한 변경사항을 기관의 인증서 및 암호 키 관리 기준과 실제 운영 절차에 반영할 필요가 있다.

모든 시스템을 동일한 시점에 양자내성암호로 전환하기 어려운 경우에는 일정 기간 기존 공개 키 암호 방식과 양자내성암호 방식이 병행될 수 있다. 기관은 시스템별 전환 상태와 적용 중인 암호 방식을 파악하고, 기존 방식의 사용 종료 시점과 예외 적용 조건 등을 정하여 전환 기간의 운영 기준을 마련할 필요가 있다. 이를 통해 서로 다른 암호체계가 혼재하는 기간에도 시스템별 전환 상태와 적용 방식을 일관되게 관리할 수 있어야 한다.

전환 과정에서는 인증 실패, 시스템 접속 오류, 연계 시스템과의 통신 실패, 성능 저하 등 기존 환경에서는 발생하지 않았던 장애가 나타날 수 있다. 따라서 예상 가능한 장애 유형별 확인 · 조치 방법, 담당자 연락 체계, 원상 복구를 위한 롤백(Rollback) 절차 및 임시 조치 기준 등을 사전에 마련하고, 실제 장애 발생 시 관련 담당자가 정해진 절차에 따라 대응할 수 있도록 준비할 필요가 있다.

시스템 관리자, 보안 담당자 등 전환과 운영에 참여하는 인력의 역할과 책임도 함께 정비해야 한다. 각 담당자가 새로운 암호 방식과 변경된 운영 절차를 충분히 이해할 수 있도록 필요한 교육을 실시하고, 인증서 · 암호 키 교체, 장애 대응, 전환 상태 관리, 관계 기관 및 공급업체와의 협의 등 주요 업무별 담당 주체와 역할을 명확히 할 필요가 있다.

마지막으로 양자내성암호 전환으로 변경된 사항은 관련 보안 정책과 운영 문서에도 반영해야 한다. 인증서 발급 · 갱신 · 폐기, 암호 키 관리, 시스템 접속 및 인증, 장애 대응 등의 절차가 변경되는 경우 관련 지침, 운영 매뉴얼, 점검표 등을 함께 갱신하고 최신 상태로 관리해야 한다. 이를 통해 실제 운영 과정에서 기존 절차가 계속 적용되어 발생할 수 있는 장애나 보안 공백을 방지할 필요가 있다.

실무 시나리오

양자내성암호 시범 전환을 마친 기관의 보안팀은 새 인증서 발급 절차서 갱신을 미루고 있었다. 수개월 후 다른 부서 담당자가 기존 절차서를 그대로 참고해 RSA 기반 인증서를 신청했고, 시스템 접속 오류가 발생한 후에야 혼선이 드러났다.

⇨ 암호 전환 완료와 운영문서 갱신과 담당자 교육은 반드시 동시에 이루어져야 한다. 전환을 기술 작업으로만 관리하고 절차 문서와 교육을 후순위로 미루면, 전환 이후에도 기존 방식이 반복되는 운영 공백이 생길 수 있다.

실무 시나리오

인증서 발급 시스템·행정정보시스템·민원포털을 순차적으로 전환하기 위해 3개월 병행 운영 계획을 수립한 기관이 있었다. 그러나 어느 시스템이 현재 양자내성암호 방식을 사용하고, 어느 시스템이 아직 기존 방식인지를 추적하는 내부 전환 상태 대장이 없었다. 인증 관련 장애가 발생했을 때 중간에 투입된 지원 인력은 인증서 재발급 요청을 새 시스템에 해야 할지 기존 시스템에 해야 할지 파악하지 못해 대응이 지연됐고, 서비스 중단 시간이 필요 이상으로 길어졌다.

⇨ 병행 운영 기간에는 각 시스템의 전환 상태를 한눈에 파악할 수 있는 내부 대장을 운영하고, 담당자가 교체되더라도 즉시 현황을 파악할 수 있는 인수인계 체계를 갖춰야 한다.

❷ 제품 조달 기준 및 공급망 대응

양자내성암호 전환은 기존 시스템의 교체 시점에만 고려해서는 충분하지 않다. 현재 새로 도입하는 장비와 소프트웨어가 양자내성암호를 지원하지 않거나 암호 알고리즘을 변경하기 어려운 구조라면, 향후 해당 제품이 기관 전체의 전환을 지연시키는 요인이 될 수 있다. 따라서 전환 준비는 기존 시스템의 교체 계획과 함께 신규 구축·도입 사업의 조달 단계부터 시작하는 것이 바람직하다.

신규 도입·계약 갱신 단계에서는 양자내성암호 지원 여부와 지원 예정 시점, 소프트웨어·펌웨어 업데이트 가능 여부, 암호 알고리즘 변경 가능 여부 등을 확인하고, 기존 운영 제품은 공급업체의 지원 로드맵과 교체 필요성을 파악할 필요가 있다. 클라우드 서비스 등 서비스 제공자 의존 환경에서는 기관과 서비스

제공자의 관리 범위를 구분하여 전환 가능 시점을 판단해야 한다. 구체적인 공급업체 질의, 계약 · RFP 반영 및 조달 대응 방법은 4장 4절에서 자세히 다룬다.

실무 시나리오

정보보안팀이 신규 방화벽 도입을 위한 제안요청서(RFP)를 작성할 때 양자내성암호 지원 여부 항목을 포함하지 않았다. 도입 후 2년이 지나 양자내성암호 전환 계획을 수립하던 중, 해당 장비가 양자내성암호를 지원하지 않고 펌웨어 업데이트도 불가하다는 사실이 확인됐다. 남은 유지보수 기간 3년이 낭비될 수밖에 없었다.

⇨ 조달 단계에서 양자내성암호 지원 여부를 필수 요건으로 명시했다면 피할 수 있었던 상황이다. 지금 도입하는 모든 장비 · 소프트웨어의 RFP에는 양자내성암호 지원 계획을 확인하는 항목이 필요하다.

❸ 기관 간 연계 시스템 및 병행 운영

기관의 정보시스템은 내부 시스템이나 타 기관의 시스템과 연계되어 운영되는 경우가 많다. 이러한 연계 구간에서 한쪽 시스템의 암호체계만 양자내성암호로 전환할 경우, 상대 시스템과 지원하는 암호 방식이나 인증체계가 달라 통신 단절이나 인증 · 검증 오류가 발생할 수 있다. 따라서 기관 자체의 전환 준비뿐만 아니라 연계 대상 시스템의 현황과 준비 수준을 함께 파악하고 전환 일정을 조율할 필요가 있다.

먼저 기관 내부 및 외부 기관과 데이터를 주고받는 시스템과 연계 구간을 파악하고, 각 시스템에서 사용하는 RSA 등 기존 공개 키 암호와 양자내성암호 지원 여부 및 향후 지원 계획을 확인해야 한다. 특히 외부 기관과 연계된 시스템은 개별 기관이 전환 시기를 단독으로 결정하기 어려울 수 있으므로, 관계 기관과 전환 시기와 방식, 사전 연동 시험 일정 및 장애 발생 시 대응 절차 등을 사전에 협의할 필요가 있다.

연계 대상별로 양자내성암호 지원 여부나 전환 일정이 다른 경우에는 상호 운용성 확보를 위해 하이브리드–OR 방식을 한시적으로 적용할 수 있다. 이 경우 연계 대상별 적용 암호 방식과 전환 시점을 관리하고, 연결 실패나 인증 · 검증

오류 등이 발생할 경우 기존 방식으로 복구할 수 있도록 롤백 대응 절차를 사전에 마련할 필요가 있다.

양자내성암호는 기존 공개 키 암호와 비교하여 키, 서명, 암호문 등의 크기와 연산 특성이 달라질 수 있으므로, 연계 시스템의 통신 및 처리 환경에 미치는 영향도 사전에 확인해야 한다. 실제 적용 전에는 연계 구간별 시험을 통해 정상 접속과 데이터 송수신, 인증·전자서명 검증, API 연계, 네트워크·보안장비 정상동작 여부 및 성능 영향을 확인하고, 장애 상황에서의 대응 절차가 정상적으로 작동하는지도 검증할 필요가 있다.

양자내성암호 전환으로 시스템 간 연계 방식이나 암호체계가 변경되는 경우에는 관련 문서와 운영 절차도 함께 갱신해야 한다. 데이터 송수신 방식, API 연계 규격, 인증·암호화 및 검증 방식, 오류 처리 절차와 운영 매뉴얼 등에 변경 사항을 반영하여 전환 이후에도 기관 간 연계가 안정적으로 유지될 수 있도록 관리할 필요가 있다.

실무 시나리오

A 기관이 TLS 키 교환을 X25519+ML-KEM 하이브리드 방식으로 전환한 직후, 행정정보 공동이용으로 연계된 B 기관 시스템이 ML-KEM을 지원하지 않아 API 연동이 전면 중단됐다. 연계 기관과 사전 협의 없이 단독으로 전환을 진행한 것이 원인이었으며, 긴급 롤백 후 B 기관의 전환 일정에 맞춰 전환을 재조율해야 했다.

⇨ 연동 구간이 있는 기관은 자기 기관의 전환 일정을 먼저 확정하는 것이 아니라, 연계 기관의 양자내성암호 지원 시점을 먼저 파악한 뒤 함께 조율해야 한다.

실무 시나리오

C 기관과 D 기관은 양자내성암호 전환 일정을 사전에 협의하고 같은 날 전환하였다. 그러나 전환 직후 D 기관의 전자서명 검증 API가 전면 실패했다. 원인은 암호 호환성이 아니었다. 양자내성암호 알고리즘 서명의 크기(약 2,420바이트)가 RSA-2048 전자서명(256바이트)의 약 10배에 달했고, D 기관의 API가 설정한 요청 본문 크기 제한(1,024바이트)을 초과한 것이었다.

⇨ 양자내성암호는 키·서명·암호문 크기가 기존보다 크므로, 전환 전 연계 구간별 실제 환경 시험을 통해 메시지 크기·버퍼·타임아웃 설정을 반드시 검증해야 한다.

❹ 저장 데이터 보호 및 장기보존 재평가

양자내성암호 전환 시에는 현재 운영 중인 시스템뿐만 아니라 이미 저장·보존되고 있는 데이터에 적용된 암호체계도 함께 검토해야 한다. 저장 데이터는 시스템이나 통신 구간과 달리 전환에 따른 영향이 즉각 드러나지 않아 점검 대상에서 간과되기 쉽다. 그러나 HNDL 공격의 특성상 현재 암호화된 데이터가 수집된 후 향후 양자컴퓨터를 이용해 복호화될 수 있으므로, 장기간 저장·보존되는 데이터는 보호 기간을 고려하여 선제적으로 점검할 필요가 있다. 특히 백업과 아카이브 데이터는 운영 DB와 별도의 암호 설정이나 키 관리 체계를 사용하는 경우가 있어 점검 범위에서 누락되지 않도록 유의해야 한다.

장기간 보호가 필요한 전자기록물·민감정보·국가 중요정보 등에 대해서는 현재 적용된 암호체계가 요구되는 보호 기간 동안 충분한 안전성을 제공할 수 있는지 재평가할 필요가 있다. 특히 장기간 기밀성을 유지해야 하는 데이터는 현재 사용 중인 공개 키 암호가 향후 양자컴퓨팅 위협에 노출될 가능성을 고려하여 양자내성암호 전환의 필요성과 우선순위를 검토해야 한다.

양자내성암호 전환을 준비할 때에는 운영 데이터뿐만 아니라 백업 및 아카이브 데이터를 포함하여 보호가 필요한 데이터에 적용된 암호 현황을 함께 파악해야 한다. 이 과정에서는 데이터에 적용된 암호 알고리즘뿐만 아니라 암호 키의 생성·저장·보호 방식과 전자서명 및 무결성 검증에 사용되는 암호기술을 확인하여, 양자취약 공개 키 암호에 의존하는 부분이 있는지를 식별할 필요가 있다.

외부 기관이나 민간 사업자에게 제공하거나 공동으로 활용하는 데이터는 제공기관과 수신 기관의 암호체계 및 검증 방식이 상호 호환되어야 한다. 따라서 향후 제공되는 데이터의 전자서명·암호화·검증 방식은 관계 기관의 양자내성암호 전환 일정과 연계하여 조정할 필요가 있다. 기존에 제공된 데이터에 대해서도 장기적인 진본성·무결성 또는 기밀성 유지가 필요한 경우에는 재제공, 재서명 또는 검증정보 갱신 등의 필요 여부를 검토하고 관계 기관과 협의할 필요가 있다.

실무 시나리오

암호화 현황을 점검한 DB 담당자는 운영 DB와 백업 데이터가 AES-256으로 암호화되어 있음을 확인하였다. 그러나 야간 배치로 생성되는 백업 파일의 데이터 암호화 키(DEK)는 2015년 도입 당시 구성된 RSA-2048 공개 키로 암호화하여 보관하고 있었다. 또한 해당 RSA 복호화 키의 관리 부서와 책임자가 명확하게 확인되지 않았다. RSA-2048의 즉각적인 사용 중단 여부와 별개로, 장기간 보존되는 백업 데이터는 향후 양자 위협에 대비하여 RSA 기반 키 보호 구조와 키 관리 책임을 사전에 파악하고 전환 계획에 반영할 필요가 있는 상황이었다.

⇨ 백업·아카이브 데이터는 데이터 암호화 방식뿐 아니라 데이터 암호화 키(DEK)의 보호 방식과 키 관리 체계가 운영 시스템과 다를 수 있으므로 점검 범위에서 빠지지 않도록 주의해야 한다.

실무 시나리오

E 기관은 공공데이터 포털을 통해 RSA-2048로 서명된 토지대장 원본증명 데이터 수십만 건을 타 기관 및 민간 사업자 30여 곳에 제공하고 있었다. 양자내성암호 전환 계획을 수립하면서 기존 서명 데이터를 양자내성암호 알고리즘으로 재서명하기로 했지만, 수신 기관들에게 재서명 일정을 사전에 알리는 공지 채널이 없었다. 재서명 완료 후 일부 수신 기관이 기존 RSA 전자서명으로 검증을 시도하다 진본 확인 실패 오류가 발생했고, 해당 기관들은 원본 데이터의 위변조 여부를 의심했다.

⇨ 외부에 제공한 전자서명 데이터를 재서명할 때는 수신 기관 목록을 먼저 파악하고, 전환 일정·검증 방식 변경을 사전에 공지하는 절차를 반드시 수립해야 한다.

❺ 체크리스트 : 양자내성암호 전환 파급 영역 자가 점검

※ 본 체크리스트는 예시이며, 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인		내용	날짜
운영 절차	□	양자내성암호 전환 후 달라지는 인증서 · 암호 키 관리 절차(생성 · 발급 · 배포 · 보관 · 폐기)를 식별하고 갱신 계획을 수립하였다. ※ 예시 : 기존 RSA · ECC 기반 인증서와 암호 키를 양자내성암호 기반 체계로 전환할 때 변경되는 생성 · 발급 · 배포 · 보관 · 폐기 절차를 확인하고, 상위 인증체계의 전환 방식과 일정에 맞추어 기존 인증서 · 키의 교체 시점, 신규 인증서 · 키의 적용 순서 및 기존 키 폐기 절차를 포함한 갱신 계획을 수립	
	□	병행 운영 기간 중 시스템별 전환 상태를 추적하는 내부 대장을 설계하였다. ※ 예시 : 시스템별로 현재 적용 중인 암호 방식, 양자내성암호 적용 여부, 전환 예정일 · 완료일, 담당자를 기록하여 기존 방식과 신규 방식이 혼재하는 기간에도 전환 현황을 확인할 수 있도록 관리	
	□	양자내성암호 전환 관련 장애 유형별 대응 절차와 담당자 연락 체계를 최신화하였다. ※ 장애 유형 : 인증 실패, 시스템 접속 오류, 연계 시스템 간 통신 실패, 성능 저하 등	
조달 · 공급망	□	현재 진행 중이거나 예정된 신규 조달 RFP에 양자내성암호 지원 여부 확인 항목을 포함하였다. ※ 양자내성암호 지원 여부 · 지원 예정 시점, 펌웨어 · 소프트웨어 업데이트 제공 여부, 암호모듈 검증 또는 보안적합성 검증 관련 계획 등을 제안요청서의 확인 항목에 포함	
	□	기존 운영 장비 · 소프트웨어의 양자내성암호 전환 가능 여부를 공급업체에 공식 문의하였다. ※ 예시 : 업체에 양자내성암호 지원 여부 확인과 함께 미지원 시 펌웨어 · 소프트웨어 업그레이드 또는 장비 교체 여부와 예상 지원 시점 · 추가 비용 · 기존 시스템과의 호환성 등을 확인	
	□	클라우드 · SaaS 계약에 암호 공개 의무 및 양자내성암호 전환 계획 제출 조항이 포함되어 있다.	
기관 연계	□	외부 기관과 데이터를 주고받는 연계 시스템 목록을 작성하고, 각 상대 기관의 양자내성암호 전환 일정을 파악하였다.	

확인		내용	날짜
기관 연계	□	양자내성암호 적용 시 메시지 크기 증가로 인한 API 버퍼·타임아웃 설정 변경 필요 여부를 확인하였다. ※ 양자내성암호 적용으로 공개 키·전자서명·인증서 등의 데이터 크기가 증가하면서 기존 API의 요청·응답 크기 제한을 초과하거나 처리 시간이 늘어날 수 있음	
저장 데이터	□	기밀성 보호 기간 10년 이상 데이터 중 공개 키 암호(RSA·ECC)로 보호된 항목(암호화·전자서명·키 래핑)을 식별하였다. ※ 키 래핑(Key Wrapping) : 데이터를 암호화하는 키를 다른 상위 키로 다시 암호화하여 보호하는 방식으로, 상위 키 보호에 RSA·ECC 등 양자취약 공개 키 암호가 사용되는지 확인 필요	
	□	백업·아카이브 데이터의 암호 적용 현황을 운영 DB와 별도로 점검 완료하였다.	
데이터 전송 구간	□	현재 운영 중인 모든 웹서버·API 게이트웨이의 TLS 버전이 1.3 이상인지 확인하였다.	
	□	내부 통신에 사용 중인 VPN/IPsec 장비가 IKEv2를 지원하는지 공급업체에 확인하였다.	
	□	내부 통신에 SSH를 사용 중인 장비의 경우 OpenSSH 9.9 이상을 지원하는지 확인하였다.	
	□	TLS 통신 경로상의 방화벽·미들박스가 양자내성암호의 큰 패킷 크기를 허용하는지 시험하였다. ※ 양자내성암호 적용 시 공개 키, 서명, 인증서 등의 크기가 증가할 수 있음	
디지털 인증 시스템	□	기관 내 GPKI/NPKI 인증서를 검증하는 시스템 목록을 작성하였다.	
	□	상위 CA의 양자내성암호 전환 예정 일정을 공식 경로로 확인하였다.	
	□	각 시스템의 인증서 검증 라이브러리가 표준 양자내성암호를 지원하는지 점검하였다.	
응용 시스템	□	암호기능을 사용하는 응용시스템 목록을 CBOM 형태로 목록화하였다. ※ CBOM : 제품·소프트웨어에서 사용하는 암호 알고리즘, 라이브러리, 인증서, 키 등의 정보를 정리한 암호자산 명세서	

확인		내용	날짜
응용 시스템	□	소스코드 · 라이브러리 정적 분석으로 공개 키 암호(RSA · ECC 등) 호출 위치를 식별하였다. ※ 정적 분석 : 프로그램을 실행하지 않고 소스코드 · 바이트코드 등을 분석하여 RSA · ECC 등 암호 함수나 라이브러리가 호출되는 위치를 찾는 방법	
	□	외주 개발사 · 클라우드 서비스의 암호 현황을 계약 또는 협의로 확인하였다. ※ 예시 : 외부 납품 소프트웨어의 암호 정보가 기술된 CBOM 명세서 제출을 조달 및 계약 조건으로 요구	
전용 암호화 장치	□	운영 중인 VPN GW · HSM · 구간암호화 장비별로 공급업체에 양자내성 암호 지원 로드맵을 문의하였다.	
	□	HSM의 경우, 양자내성암호를 지원하는 검증필 암호모듈의 적용 가능 시점을 파악하였다.	
	□	잔여 내용연수와 양자내성암호 전환 목표 시점을 비교하여 교체 일정을 계획하였다.	
데이터 자산	□	기밀성 보호 기간 10년 이상인 전자기록물의 전자서명 현황을 조회하였다.	
	□	DEK 키래핑 방식(RSA 사용 여부)을 포함한 운영 DB · 백업 · 아카이브 암호화 현황을 파악하였다. ※ DEK(Data Encryption Key) : 실제 데이터를 암호화하는 키로, DEK를 다른 상위 키로 암호화하여 보관하는 것을 키 래핑이라 함. 데이터 자체가 대칭 키 로 암호화되어 있더라도 DEK 보호에 RSA 등 양자 취약 공개 키 암호가 사용될 수 있음	
	□	HNDL 위협 기준으로 모스카 부등식(X+Y>Z)을 적용하여 우선순위를 도출하였다. ※ X는 데이터 보호 필요 기간, Y는 양자내성암호 전환에 필요한 기간, Z는 현행 공개 키 암호를 위협할 수 있는 양자컴퓨터 등장까지 예상되는 기간을 의미. X+Y>Z인 경우 보호 필요 기간과 전환 소요 기간을 고려할 때 조기 전환 준비가 필요한 대상으로 판단	
영향 영역	□	양자내성암호 전환 후 인증서 · 키 관리 절차서, 장애 대응 매뉴얼을 갱신할 계획이 있다.(운영)	

확인		내용	날짜
영향 영역	□	진행 중인 조달 사업의 RFP에 양자내성암호 지원 요건이 포함되어 있다.(조달)	
	□	연계 기관과 양자내성암호 전환 일정을 협의하고 사전 연동 시험 일정을 확정하였다.(연동)	
	□	외부 제공 데이터의 재서명 계획과 수신 기관 공지 절차를 수립하였다.(데이터 관리)	



Chapter 03

양자내성 암호 전환 프레임워크

Chapter
03

양자내성암호 전환 프레임워크

현재 국가·공공부문 정보시스템은 다양한 운영 환경과 기술 체계가 혼재되어 있으며, 범정부 연계 체계와 공통 인프라 의존성이 높다. 일부 시스템은 장기간 운영되는 레거시 구조와 장수명(long-life) 장비를 포함하고 있으며, 외부 공급업체 솔루션 및 클라우드 환경과 긴밀히 연계된 시스템도 있다. 특히 국가·공공부문은 국가정보원의 보안적합성 검증 체계, 국가 암호정책, 공공조달 구조, 정보화사업 추진체계 등 국내 특수 환경의 영향을 크게 받는다. 이러한 상황을 고려할 때 양자내성암호 전환은 단기간 내 일괄적으로 완료하기 어려우며, 위험도와 운영 환경을 고려한 단계적·점진적 접근이 필요하다.

본 장에서는 국가·공공기관이 양자내성암호 전환을 추진하기 위해 수행해야 하는 전체 절차를 개괄적으로 설명한다. 이를 위해 전환 과정을 6단계로 구분하여 각 단계의 목적과 주요 고려사항을 설명하고, 단계별 주요 산출물과 의사결정 요소를 함께 제시한다. 또한 기관별 상황에 따라 유연하게 적용 가능한 단계형 전환 로드맵을 소개한다. 이는 이후 장에서 설명할 세부 절차와 실무 방법론의 전체 흐름을 이해하는 데 도움이 될 것이다.

제1절 양자내성암호 전환 절차 개요

공개 키 암호는 TLS, VPN, 전자서명 인증체계 등 국가·공공기관 정보시스템 전반에서 다양한 방식으로 사용되고 있다. 본 가이드북에서는 국가·공공기관 환경을 고려하여 양자내성암호 전환 과정을 다음 6단계로 구분한다.

① 전환 착수 및 거버넌스 수립

② 암호자산 현황 파악 및 인벤토리 구축

③ 우선순위 결정 및 전환 전략 수립
④ 조달 및 공급업체 대응 전략
⑤ 예산 계획 수립
⑥ 전환 시행 및 운영 검증

각 단계는 독립적인 절차가 아니라 상호 연계된 구조로 수행되어야 하며, 각 기관의 규모와 운영 환경에 따라 일부 단계는 병행하여 추진할 수 있다. 또한 전환 6단계는 기관 전체에 한 번만 적용하는 일회성 절차가 아니라, 전환 대상 시스템과 사업의 특성에 따라 반복하여 적용할 수 있는 실행 절차이다. 이때 기존에 수립한 추진체계와 암호자산 인벤토리, 전환 계획 등을 활용하고, 대상별로 필요한 사항을 갱신·보완하면서 전환 전략을 정교화할 수 있다.

실제 전환 과정에서는 국내·국제 표준화 진행 상황, 국가 정책 변화, 공급업체 지원 수준 등에 따라 단계별 추진 일정과 우선순위를 조정할 수 있다. 특히 국가·공공기관은 정보화사업 및 유지관리사업 단위로 시스템 개선이 이루어지는 경우가 많으므로, 양자내성암호로의 전환 역시 기존 사업 구조와 연계하여 단계적으로 반영하는 접근이 현실적일 수 있다. 예를 들어, 신규 구축 시스템이나 차세대 사업에는 양자내성암호 대응 구조를 미리 반영하고, 기존 시스템은 유지관리 및 장비 교체 시점과 연계하여 순차적으로 전환하는 방식을 적용할 수 있다.

현재 양자내성암호 관련 기술이 지속적으로 발전 중이며, 표준화 또한 진행 중이므로 일부 알고리즘은 향후 변경 또는 보완 가능성도 존재한다. 따라서 실제 전환 시에는 관련 표준과 기술의 성숙도, 기존 시스템과의 호환성 등을 고려하여 적용할 양자내성암호 알고리즘과 전환 방식을 결정할 필요가 있다. 전환 과정에서 기존 공개 키 암호와 양자내성암호의 병행 운영이 필요한 경우에는 한시적으로 하이브리드 OR 방식을 활용할 수 있으나 가능한 하이브리드 AND 방식을 사용을 권고하며, 장기적으로는 향후 암호 알고리즘이나 적용방식의 변경에 유연하게 대응할 수 있도록 암호 민첩성(Crypto Agility)을 확보하는 방향으로 전환하는 것이 바람직하다.

이하에서 각 단계의 목적과 주요 고려사항을 설명한다.

① 전환 착수 및 거버넌스 수립

양자내성암호 전환은 단순 기술 교체 과제가 아닌 기관 차원의 중장기 정보보호 전략으로 접근해야 한다. 따라서 전환 초기 단계에서는 **기관 내 추진체계와 의사결정 구조를 우선적으로 수립**해야 한다. 특히 국가·공공기관은 정보화총괄·정보보호·운영·조달·예산 등 관련 부서가 연계되어 있으므로, 기관 내 역할과 책임을 명확히 정의할 필요가 있다.

거버넌스 수립 단계에서는 다음 사항을 시행한다.

- 기관 차원의 양자내성암호 전환 추진 방향 수립
- 전환 검토 대상 및 추진 범위 설정
- 추진 조직 및 협의체 구성
- 시범 적용 추진 여부 결정
- 기관 내 중장기 로드맵 수립
- 국가 정책 및 가이드라인 검토

또한 국가정보원의 보안적합성 검증 체계, 국가 암호정책, 범정부 공통 인프라와의 연계성도 함께 고려할 필요가 있다. 거버넌스 수립의 세부 절차, 역할 분장표 예시, 인력 운영 모델은 4장 1절을 참고한다.

② 암호자산 현황 파악 및 인벤토리 구축

양자내성암호 전환을 위해서는 **우선 기관 내 공개 키 암호 사용 영역을 탐색하고, 각 시스템의 공개 키 암호 사용 현황과 보호 대상 정보를 파악**할 필요가 있다. 이후 이를 체계적으로 정리·관리하는 과정을 암호자산 인벤토리(Cryptographic Asset Inventory) 구축이라고 한다.

특히 국가·공공기관은 업무망, 인터넷망, 폐쇄망 등 복합 네트워크 환경을 운영하는 경우가 많으며, 클라우드 서비스(IaaS·PaaS·SaaS) 및 외부 솔루션과 연계된 시스템도 증가하고 있다. 따라서 단순 장비 목록이 아니라 망 구성, 시스템 배치환경, 서비스 간 연계 및 공급업체·클라우드 의존성을 포함하여 실제

암호 사용 구조를 파악하는 것이 중요하다. 구체적인 식별 항목과 수집 방법은 4장 2절을 참고한다.

③ 우선순위 결정 및 전환 전략 수립

모든 시스템을 동시에 양자내성암호로 전환하는 것은 현실적으로 어렵다. 따라서 각 기관은 암호자산 인벤토리를 바탕으로 시스템별 위험도와 전환 필요성을 평가하고, 그 결과에 따라 **전환 우선순위를 정하여 단계적인 전환 계획을 수립**할 필요가 있다. 특히 HNDL 공격을 고려하면, 현재의 위험 수준뿐 아니라 정보가 보호되어야 하는 기간까지 고려하여 전환 시점을 판단할 필요가 있다.

이 단계에서는 다음 요소를 종합적으로 고려한다.

- 데이터 중요도
- 데이터 보호 기간
- 외부 노출 수준
- 파급력
- 기관 간 연계 여부
- 공급업체 의존성
- 핵심 신뢰 인프라 여부
- 시스템 교체 계획
- 전환 난이도

또한 각 기관은 다음과 같은 전환 전략 방향을 함께 검토한다.

- 신규 시스템에 선제적 적용
- 하이브리드 방식을 통한 단계적 전환
- 인증체계 전환
- VPN 및 외부 연계 우선 전환

우선순위 결정의 세부 기준(9개 평가 지표와 점수 산정 방법) 및 한국형 특화 고려사항은 4장 3절을 참고한다.

④ 조달 및 공급업체 대응 전략

국가·공공기관의 정보시스템은 상당수가 외부 공급업체와의 조달·유지관리 계약을 통해 구축·운영된다. 따라서 **공급업체의 양자내성암호 지원 여부와 조달 요구사항 반영**은 실질적인 전환 속도를 결정하는 핵심 요소다.

각 기관은 현재 사용 중인 상용 솔루션 및 보안장비의 양자내성암호 지원 여부를 해당 공급업체에 확인해야 한다. 미지원 시에는 공급업체의 지원 계획, 업그레이드 가능 여부 및 전환 로드맵을 사전에 확인해야 한다. 또한 향후 신규 사업 발주 시에는 다음 요소를 요구사항에 반영할 것을 권장한다.

- 암호 민첩성 적용(알고리즘 교체·추가가 가능한 구조, 복수 공개 키 암호 지원, 중앙 집중형 설정 관리 등)
- 양자내성암호(기존 공개 키 암호와의 하이브리드-AND 방식 적용(5장 1절 ❶)) 지원 여부 및 적용 계획 제출
- 향후 국가정보원 KCMVP 검증기준 등 암호정책 변경에 대응하기 위한 전환 계획 제출
- CC인증 또는 보안기능 확인서 취득 제품에 TLS 1.3 의무 적용 등 양자내성암호 적용을 요구하는 경우, 추후 인증 취득 및 적용 계획 제출

국가·공공부문에서는 공공조달과 유지관리사업 구조가 실제 전환 속도에 큰 영향을 미칠 수 있으므로, 이 단계는 특히 중요하다. 특히 국가 표준·정책이 완전히 확정되지 않은 현시점에서도, 특정 알고리즘의 강제 적용을 요구하는 것이 아니라 '암호 민첩성을 지원하는 구조 확보'와 양자내성암호 지원 계획 제출은 지금 당장 RFP에 반영할 수 있다. 표준이나 제품 지원체계가 충분히 성숙한 이후에야 조달 요구사항을 검토하기 시작하면 기존 장비의 교체 주기나 사업 발주 시점과 맞지 않아 전환이 지연될 수 있다는 점도 고려해야 한다. 다만 CC인증 또는 보안기능 확인서를 취득한 보안제품에 양자내성암호 적용을

요구할 경우 기존 인증·확인서의 효력에 영향을 줄 수 있으므로, RFP 작성 전 추후 인증 취득 및 인증된 버전의 적용 계획을 제출하도록 요청하는 것을 권고한다. 세부 RFP 요구사항 항목 및 예시 문구는 4장 4절 ❺를 참고한다.

⑤ 예산 계획 수립

양자내성암호 전환은 단기간에 완료 가능한 사업이 아니며, 장기간에 걸쳐 단계적으로 추진해야 한다. 또한 기관별 정보시스템 구조, 공급업체 지원 수준, 장비 교체 주기 등에 따라 실제 추진 방식과 소요 자원은 다양하게 달라질 수 있다. 따라서 각 기관은 단기적 예산 편성보다 기존 정보화사업·유지관리사업·노후 장비 교체사업과 연계한 **중장기 추진 관점에서 접근**할 필요가 있다. 특히 다음 사항을 함께 고려한다.

- 신규 정보화사업 및 차세대 사업과의 연계 가능성
- 유지관리사업 및 노후 장비 교체 시점 활용 가능성
- 기관 내 시험환경 및 시범 적용 필요성
- 국가 공통 인프라 및 기관 간 연계 체계와의 정합성
- 공급업체 제품의 업그레이드 지원 가능 시점
- 차기 사업 발주 및 조달 일정과의 연계 가능성
- 단계적 적용 확대를 고려한 우선순위 검토
- 장기 운영 시스템에 대한 지속 관리 방향

초기 단계에서는 대규모 일괄 교체보다 시범 적용과 단계적 확대를 고려하여 예산과 사업 계획을 유연하게 수립하는 것이 바람직하다. 한편 국가·공공기관의 정보화사업은 예산 요구와 사업 기획이 실제 사업 착수보다 앞서 이루어지므로, **기관별 예산 편성 및 사업 계획 일정을 고려하여 양자내성암호 전환 수요를 사전에 반영**해야 한다. 차세대 사업처럼 규모가 큰 경우에는 착수 2~3년 전부터 기획 단계에 정보보안 담당자가 참여하여 양자내성암호 요구사항을 반영해야 사업 기회를 놓치지 않는다. 예산 항목별 세부 내용, 기존 사업 연계 방법, 제한된 예산 상황에서의 단계적 접근 전략은 4장 5절을 참고한다.

⑥ 전환 시행 및 운영 검증

마지막 단계에서는 실제 양자내성암호 적용과 운영 검증을 수행한다. 이 단계의 핵심 원칙은 **'점진적 적용'**이다. 모든 시스템에 한꺼번에 전환을 적용하면 문제가 발생했을 때 미치는 영향을 통제하기 어렵다. 따라서 처음 적용할 대상은 우선순위가 높은 시스템 중에서 독립성이 높고 전환이 용이한 시스템부터 시범 적용하여 경험을 축적한 후, 단계적으로 확대하는 방식이 현실적이다. 또한 모든 전환 작업에 앞서 반드시 롤백(원상 복구) 계획을 수립하고 시험 환경에서 복구 절차를 사전 검증해야 한다.

현재 초기 전환 단계에서는 기존 공개 키 암호 체계와 양자내성암호를 병행하여 사용하는 하이브리드 방식이 현실적인 적용 방안 중 하나로 검토되고 있다. 국내에서도 이러한 흐름을 반영하여 암호모듈 검증제도에 양자내성암호 기반 하이브리드 방식 관련 검증 내용이 추가되었다[5]. 다만 실제 운영 환경에 적용하기 위해서는 충분한 시험과 검증이 필요하다. 각 기관은 다음 요소를 종합적으로 검토해야 한다.

- 성능 영향
- 네트워크 영향
- 상호운용성
- 인증체계 영향
- 운영 안정성
- 장애 대응 절차
- 로그 및 모니터링 체계
- 기존 데이터 처리 방안(저장 데이터 재암호화, 인증서 재발급, 서명 데이터의 장기검증 등)

국가·공공기관은 업무망·인터넷망·폐쇄망 등 다양한 망 구성을 가지고 있으며, 시스템의 구축·운영 형태도 기관 자체 구축형과 클라우드 서비스 이용형 등으로 다양하다. 또한 대국민·내부 업무·기관 간 연계 등 서비스

유형도 다양하므로, 각 시스템의 망 구성, 구축·운영 형태, 서비스 특성 및 연계 관계를 고려하여 전환 시행 및 운영 검증을 수행할 필요가 있다. 구체적인 검증 절차와 항목은 4장 6절을 참고한다.

제2절 단계별 주요 산출물

양자내성암호 전환을 체계적으로 추진하기 위해서는 각 단계에서 확보해야 할 주요 산출물을 정의하고 관리하는 것이 중요하다. 단계별 산출물은 단순한 문서 작성 결과가 아니라 기관의 현재 상태를 객관적으로 파악하고 이후 단계의 의사결정을 지원하는 핵심 자료로 활용된다.

특히 국가·공공기관은 정보화사업 관리 체계, 보안성 검토 체계, 공공조달 및 예산 구조 등의 영향을 크게 받으므로, 전환 과정에서 단계별 산출물을 체계적으로 관리한다면 향후 국가 정책 변화, 표준 변경, 예산 확보 및 사업 발주 과정 등에 보다 유연하게 대응할 수 있다.

본 절에서는 각 단계 종료 시 기관이 확보해야 하는 주요 산출물과 주요 의사결정 포인트를 간략히 소개한다. 이 중 이해를 돕거나 실제 작성 시 참고가 필요한 산출물에 대해서는 예시 또는 세부 설명을 추가하였다.

① 전환 착수 및 거버넌스 수립

전환 초기 단계에서는 기관 차원의 추진 방향과 조직 체계를 정의하는 것이 핵심이다. 이 단계에서의 산출물은 이후 전환 절차 전체의 기준 문서로 활용된다.

주요 산출물

- 양자내성암호 전환 추진계획서
- 참여 주체별 역할·책임 분장표(R&R)
- 전환 추진 협의체 운영 계획
- 초기 위험 요소 목록

이 단계에서는 다음 사항에 대한 기관 차원의 의사결정이 필요할 수 있다.

- 전담 조직 구성 여부
- 시범사업 수행 여부
- 외부 전문기관 협력 여부

② 암호자산 현황 파악 및 인벤토리 구축

암호자산 인벤토리 구축 단계에서는 기관 내 공개 키 암호 사용 현황을 파악하고, 장기 보호가 필요한 데이터와 전환 영향이 예상되는 시스템 및 장비를 식별하는 것이 중요하다. 특히 국가·공공기관은 장기 운영 시스템과 외부 솔루션 의존성이 높은 경우가 많으므로, 단순 시스템 목록 수준이 아니라 실제 공개 키 암호 사용 구조와 공급업체·장비 의존성까지 함께 분석할 필요가 있다.

이 단계에서는 다음 사항을 결정할 수 있다.

- 전수조사 완료를 기다릴 것인지, 핵심 시스템 파악만으로 다음 단계를 병행 착수할 것인지 여부
- 외부 전문기관 지원을 활용할 것인지 여부
- 암호자산 인벤토리 갱신 주기 및 담당자 지정

주요 산출물

- 암호자산 인벤토리 목록
- 장기 보호 데이터 식별 결과
- 공급업체·외주사 암호 현황 자료
- 파악 미완료 항목 목록

■ 암호자산 인벤토리 목록

기관 내 공개 키 암호 사용 현황을 정리한 문서로, 다음 정보가 포함될 수 있다.

- 시스템명
- 시스템 수명주기
- 사용 알고리즘
- 암호 적용 구간 및 프로토콜(TLS, VPN(IPsec 등), SSH 등)
- 인증서 체계
- 키 길이
- 사용 목적
- 운영 위치
- 관리 조직
- 유지관리 계약 만료 시점
- 기관 간 연계 구조
- 운영 환경(인터넷망 · 행정망 · 폐쇄망 등)

■ 장기 보호 데이터 식별 결과

장기간 보호가 필요한 정보와 시스템을 식별한 결과 문서로, 다음 정보가 포함될 수 있다.

- 개인정보
- 장기 보존 행정정보
- 국가 주요 정보
- 인증 로그
- 장기 서명 데이터

■ 외부 솔루션 · 공급업체 의존성 현황

기관 내에서 사용 중인 외부 솔루션, 보안장비 및 상용 제품 현황을 정리한다.

③ 우선순위 결정 및 전환 전략 수립

이 단계에서는 암호자산 분석 결과를 기반으로 실제 전환 우선순위와 기관 맞춤형 전략 방향을 수립한다.

이 단계에서는 다음 사항을 결정할 수 있다.

- 우선 전환 대상
- 하이브리드 적용 여부
- 단계별 적용 순서

주요 산출물

- 우선순위 평가표
- 양자내성암호 전환 대상 분류 목록
- 기관 자체 전환 전략서
- 연도별 전환 로드맵(초안)

■ 우선순위 평가표

시스템별 위험도와 전환 가능성을 종합적으로 평가하여 전환 우선순위를 산정한 문서이다. 4장 3절에서 제시하는 9개 평가 지표와 점수 산정 방법을 적용하여 작성할 수 있다.

■ 기관 자체 전환 전략서

우선순위 평가 결과를 바탕으로 기관의 전환 방향과 적용 전략을 구체화한 문서이다.

이 단계에서는 다음 사항을 결정할 수 있다.

- 우선 전환 대상
- 하이브리드 적용 여부

- 단계별 적용 순서

④ 조달 및 공급업체 대응 전략

국가·공공기관은 대부분 외부 조달과 유지관리사업 기반으로 시스템을 운영하므로, 공급업체 대응과 조달 요구사항 정의가 중요하다.

주요 산출물

- 공급업체 대응 현황표
- 양자내성암호 요구사항 정의서
- 교체 필요 장비·소프트웨어 목록
- 공급업체 질의서 회신 파일

■ 공급업체 대응 현황표

각 솔루션 및 장비 공급업체의 양자내성암호 지원 현황을 정리한 문서로, 다음 정보가 포함될 수 있다.

- 양자내성암호 지원 예상 시점
- 하이브리드 지원 여부
- 업그레이드 가능 여부
- 교체 필요 여부
- 국내·국제 표준 암호 지원 현황
- CC인증·보안기능 확인서 및 KCMVP 검증 정책에 대한 대응 계획
- 클라우드 서비스 제공자(CSP)의 양자내성암호 지원 로드맵 보유 여부

■ 양자내성암호 요구사항 정의서

향후 사업 발주 및 조달 과정에서 적용할 요구사항 문서로, 포함될 수 있는 항목의 예시는 다음과 같다.

- 암호 민첩성 지원(다중 알고리즘 지원, 향후 알고리즘 교체 가능성 등)

- 표준 기반 구현
- 하이브리드 지원

⑤ 예산 계획 수립

양자내성암호 전환은 장기간 추진되는 사업이므로 단계별 예산 계획이 중요하다.

주요 산출물

- 단계별 예산 계획서
- 기존 사업 연계 검토서
- 교체 필요 장비·소프트웨어 목록 및 비용 추정 목록

■ 단계별 예산 계획서

기관의 양자내성암호 전환을 단계적으로 추진하기 위해 필요한 예산, 인력 및 운영 자원 계획을 정리한 문서이다. 기관은 이를 바탕으로 단계별 전환 우선순위와 추진 일정을 검토할 수 있다. 또한 노후 장비 교체, 유지관리사업 및 기존 운영계약과의 연계 가능성을 함께 검토함으로써, 중장기 관점에서 단계적 전환 방향을 수립하는 데 활용할 수 있다.

기관은 이 단계에서 다음 사항을 검토할 수 있다.

- 연차별 추진 범위
- 우선 투자 대상
- 신규 예산 확보 여부
- 기존 사업 연계 여부
- 차기 예산·사업 계획에 반영할 항목 및 시점

⑥ 전환 시행 및 운영 검증

마지막 단계에서는 실제 운영 환경에 양자내성암호를 적용하고 검증을 수행

한다. 특히 국가·공공기관은 다양한 네트워크 환경과 운영 구조를 가지므로, 충분한 시험과 검증 절차가 중요하다.

이 단계에서는 다음 사항을 결정할 수 있다.

- 확대 적용 여부
- 추가 보완 필요 여부
- 운영 정책 반영 여부
- 장기 운영 가능 여부
- 관련 보안인증·검증에 미치는 영향 및 추가 절차 필요 여부

주요 산출물

- (시범)적용 및 검증 결과서
- 운영 절차 및 대응 계획서
- 기존 데이터 처리 결과서
- 갱신된 암호자산 인벤토리

■ (시범)적용 및 검증 결과서

전환 기술 (시범)적용 과정에서 확인된 성능 변화, 상호운용성, 운영 안정성 및 기술적 제약사항 등의 내용을 종합적으로 포함한 문서이다. 시범 적용의 경우, 향후 실제 운영 환경 확대 적용 여부를 검토하는 기초 자료로 활용할 수 있다.

■ 운영 절차 및 대응 계획서

양자내성암호 적용 이후 필요한 운영 절차, 장애 대응 방안, 모니터링 및 로그 관리 방향 등을 정리한 문서이다. 실제 운영 환경 적용 시 참고 자료로 활용할 수 있다.

각 단계에서 생성된 산출물은 이후 단계의 주요 참고 자료로 활용된다. 따라서 기관은 산출물을 일회성 문서로 관리하기보다 전환 진행 상황과 기술·정책 환경의 변화에 따라 지속적으로 갱신·관리해야 한다.

제3절 국가·공공기관 전환 로드맵

대한민국 정부는 2035년까지 국가·공공부문 주요 공개 키 암호 체계의 양자내성암호 전환 완료를 목표로 추진하고 있다[3]. 미국, 영국, 캐나다 등 주요국에서도 2035년을 전환 완료 목표 시점으로 제시하고 있어, 국내외적 전환 방향은 대체로 유사하다고 할 수 있다. 한편, 미국, 유럽연합을 비롯한 주요국은 고위험·고가치·핵심 인프라 등 중요 시스템에 대해서는 2030~2031년을 중간 마일스톤으로 설정하여 전체 전환에 앞서 우선 전환을 추진하고 있다. 따라서 국가·공공기관은 전환 계획 수립 시 N2SF에서 C 또는 S 등급으로 분류된 업무정보·정보시스템 여부를 우선순위 판단의 참고 요소 중 하나로 활용하고, 주요정보통신기반시설 여부, 데이터 보호 필요기간, 양자 위협 노출 가능성, 기관 간 연계 및 실제 전환 가능 시점 등을 종합하여 전환 우선순위를 결정할 필요가 있다.

각 기관은 본 로드맵을 기준으로 자체 전환 로드맵을 수립하되, 기관별 정보시스템 환경, 보유 데이터의 중요도, 보안적합성 검증(KCMVP 포함) 완료 제품 가용 시점, 조달·예산 여건 및 운영 환경 특성을 반영하여 일정과 우선순위를 조정할 수 있다.

❶ 양자내성암호 전환 로드맵

[표 12] 국가·공공기관 양자내성암호 전환 로드맵

구분	국가 공통 마일스톤	기관별 달성 내용
~2027년	전환 시행 체계 수립	• 기관 차원의 전환 추진체계 및 역할·책임 확립 • 전환 대상 범위 설정 • 국가 정책을 반영한 기관별 전환 로드맵 초안 작성
~2028년	주요 암호자산 인벤토리 구축 및 전환 우선순위 설정	• 주요 시스템·서비스의 암호자산 식별 및 인벤토리 구축 • 주요 암호자산 전환 우선순위 설정 • 암호자산 인벤토리·우선순위를 반영한 기관별 전환 로드맵 수립
~2031년	고위험 영역 우선전환	• 전환 우선순위가 높은 주요 시스템·서비스의 양자내성암호 전환
~2034년	전 영역 확대 전환	• 기관 내 주요 시스템·서비스 전반으로 전환 확대
2035년	전환 완료 및 지속 관리 체계 수립	• 전환 이행 현황 점검 및 잔여 대상의 전환 추진 • 암호자산 정보의 정기적 현행화 및 암호 민첩성 기반의 지속 관리 체계 수립

※ 국가 공통 마일스톤은 전환 추진을 위한 권고 일정으로, 기관 특성 및 예산 확보 상황 등을 종합적으로 검토하여 필요한 경우 세부 전환 일정을 조정할 수 있다.

[그림 5] 국가·공공기관 양자내성암호 전환 로드맵



❷ 단계별 이행 방향

가. 전환 시행 체계 수립(~2027년)

이 단계에서는 모든 국가·공공기관이 양자내성암호 전환을 기관 차원의 공식 과제로 인식하고, 향후 단계적 전환을 추진하기 위한 기본적인 추진체계를 마련한다. 이 시기의 목적은 실제 암호체계를 교체하거나 상세한 암호자산 인벤토리를 구축하는 것이 아니라, 기관 내 전환 추진체계와 역할·책임을 확립하고 전환 대상 범위를 설정한 후, 이를 바탕으로 양자내성암호 전환 추진계획서와 단계별 추진 일정의 초안을 마련하는 것이다.

특히 국가·공공기관의 정보시스템은 정보화사업, 유지관리사업, 공공조달 및 예산 계획 등과 연계되어 운영되므로 정보보호부서만으로 전환을 추진하기 어렵다. 따라서 초기 단계부터 정보보호·정보화·운영·조달·예산 등 관련 부서가 참여하는 추진체계를 마련하고, 각 부서의 역할과 책임을 명확히 할 필요가 있다.

또한 기관은 상세한 암호자산 인벤토리 구축에 앞서 어떤 시스템과 서비스까지 전환 검토 대상으로 포함할 것인지 전환 대상 범위를 설정해야 한다. 이를 위해 주요 정보시스템과 서비스, 공개 키 암호 사용 가능 영역, 장기 보호가 필요한 정보, 외부 솔루션·보안장비 및 유지관리 대상 등을 기초적으로 파악할 수 있다. 이 단계의 기초 현황 파악은 개별 암호자산을 상세하게 조사하는 것이 아니라, 다음 단계의 암호자산 인벤토리 구축 대상과 범위를 정하기 위한 사전 작업에 해당한다.

기관은 이러한 준비 결과와 국가의 양자내성암호 전환 정책·표준화 및 검증 제도 추진 방향 등을 고려하여 양자내성암호 전환 추진계획서(초안)를 작성하고, 그 안에 단계별 추진 일정(로드맵 초안)을 포함한다. 이후 암호자산 인벤토리 구축과 전환 우선순위 분석 결과를 반영하여 추진계획과 로드맵을 구체화한다.

이 시기 기관이 준비해야 할 주요 사항은 다음과 같다.

- 기관 내 전환 담당조직 및 부서별 역할·책임 확립
- 정보보호·정보화·운영·조달·예산 부서 등이 참여하는 내부 협의체 구성
- 주요 시스템·서비스를 대상으로 전환 검토 범위 설정
- 전환 범위 설정을 위한 공개 키 암호 사용 가능 영역 및 장기 보호 데이터 등에 대한 기초 현황 파악
- 외부 솔루션·보안장비·유지관리 대상 등 공급망 의존 영역의 기초 현황 확인
- 국가 정책 및 기관의 정보화·조달·예산 여건 등을 고려한 기관별 전환 로드맵 초안 작성
- 신규 정보화사업 및 차세대 사업에 '암호 민첩성' 적용 가능성 검토

마일스톤(~2027년)

모든 국가·공공기관은 양자내성암호 전환을 위한 기관 차원의 추진체계와 역할·책임을 확립하고, 전환 대상 범위를 설정하여 기관별 전환 로드맵 초안을 마련한다.

나. 주요 암호자산 인벤토리 구축 및 전환 우선순위 설정(~2028년)

이 단계에서는 각 기관이 실제 암호자산 현황을 파악하여 인벤토리를 구축하고, 이를 기반으로 전환 우선순위를 설정한다. 기관 내 암호 사용 영역과 전환 영향 범위를 가시화하고, 어떤 시스템과 서비스를 먼저 전환해야 하는지 판단할 수 있는 수준의 정보를 확보하는 것이 핵심이다.

암호자산 인벤토리는 단순한 시스템 목록이 아니라, 실제 공개 키 암호의 사용 위치와 기능, 보호 대상 데이터, 외부 시스템과의 연계 및 공급업체 의존성 등 향후 전환의 필요성과 난이도를 판단할 수 있는 정보를 포함하여 관리할 필요가 있다. 각 기관은 이러한 인벤토리를 바탕으로 암호자산별 위험과 전환 여건을 검토하고, 장기 보호 필요성, 시스템·서비스 중요도, 외부 노출 및 연계 정도, 전환 난이도 등을 고려하여 전환 우선순위를 설정한다.

국가·공공부문 특성상 다음 사항에 특히 주의하여 암호자산 현황과 전환

여건을 파악한다.

- 업무망 · 인터넷망 · 폐쇄망 등 망 구성별 암호 사용 현황 구분
- 기관 자체 구축 · 클라우드 서비스 이용 등 시스템 구축 · 운영 형태별 암호 사용 현황과 관리 범위 확인
- 국가융합망, 차세대 지방행정정보시스템 등의 범정부 공통 인프라 및 기관 간 연계 구간의 개편 · 전환 일정 확인
- 외부 솔루션 · 보안장비 · 유지관리 대상 시스템의 공급업체 양자내성암호 지원 계획 확인
- 장기간 보호가 필요한 데이터와 장기 운영 · 레거시 시스템 식별

마일스톤(~2028년)

모든 국가 · 공공기관은 주요 암호자산의 현황을 식별하여 인벤토리를 구축하고, 이를 기반으로 전환 우선순위를 설정하여 기관별 전환 로드맵을 수립한다.

다. 고위험 영역 우선전환(~2031년)

이 단계에서는 앞 단계에서 구축한 암호자산 인벤토리와 전환 우선순위를 기반으로 우선순위가 높은 주요 시스템 · 서비스부터 실제 양자내성암호 적용을 추진한다. 모든 시스템을 동시에 전환하기보다는 장기 보호 필요성, 시스템 · 서비스 중요도, 외부 노출 및 연계 정도, 전환 난이도와 운영 지속성 등을 고려하여 고위험 영역을 중심으로 단계적으로 전환하는 것이 핵심이다.

특히 장기간 보호가 필요한 중요정보를 처리하거나 국가 · 공공서비스의 연속성에 미치는 영향이 큰 시스템은 양자 위협에 따른 위험과 전환 소요 기간을 함께 고려하여 우선적으로 검토할 필요가 있다. 다만 실제 적용 시점과 방식은 관련 표준과 국가 암호정책, 검증된 암호모듈 및 이를 적용한 제품의 가용성, 기존 시스템과의 호환성 등을 고려하여 결정한다.

국가 · 공공부문에서 우선전환 대상으로 검토할 수 있는 영역의 예시는 다음과 같다.

- 장기 보호가 필요한 국가 중요정보·대규모 개인정보 처리 시스템
- 국가 중요 기반 및 주요 공공서비스 관련 시스템
- VPN·원격접속 체계 및 보안 통신 구간
- 소프트웨어·펌웨어 업데이트 검증 체계(전자서명 기반)
- 클라우드 전환·차세대 구축 등 신규 설계 또는 대규모 개편이 예정된 시스템

국가·공공기관의 정보시스템은 신규 정보화사업, 차세대 사업, 노후 장비 교체, 클라우드 전환 및 유지관리 등을 통해 지속적으로 변경된다. 따라서 우선전환 대상에 대한 양자내성암호 적용을 별도의 독립적인 기술사업으로만 추진하기보다, 기존 정보화사업과 시스템 교체·고도화 시점을 활용하여 단계적으로 적용하는 방안을 고려할 수 있다. 이를 통해 기존 시스템의 교체 주기와 전환 계획을 연계하고 중복 투자와 서비스 영향을 줄일 수 있다.

또한 신규 구축·교체 또는 유지관리 과정에서 양자내성암호 적용이 필요한 경우에는 향후 알고리즘 변경에 대응할 수 있도록 암호 민첩성, 인증서·키 관리 체계의 확장성, 소프트웨어·펌웨어 지속적인 업데이트 가능성, 공급업체의 양자내성암호 지원 계획 등을 함께 검토할 수 있다.

마일스톤(~2031년)

각 국가·공공기관은 암호자산 인벤토리와 전환 우선순위를 기반으로 고위험·고우선순위 주요 시스템·서비스부터 양자내성암호를 우선 적용한다.

라. 전 영역 확대 전환(~2034년)

이 단계에서는 고위험·고우선순위 영역을 중심으로 추진한 우선전환 결과를 바탕으로, 기관 내 주요 시스템·서비스 전반으로 양자내성암호 적용 범위를 확대한다. 앞 단계가 위험도가 높은 영역을 우선적으로 전환하는 단계라면, 이 단계에서는 그 과정에서 확보한 기술적·운영적 경험을 활용하여 상대적으로

우선순위가 낮았던 영역까지 전환 대상을 확대하는 것이 핵심이다.

기관은 암호자산 인벤토리와 전환 로드맵을 기준으로 우선전환 이후 남아 있는 주요 시스템 · 서비스를 확인하고, 시스템의 교체 · 고도화 일정, 양자내성암호 지원 제품의 가용성, 공급업체 지원 계획, 예산 및 운영 여건 등을 고려하여 단계적으로 전환을 확대한다. 앞선 우선 전환 단계에서 확인된 성능 · 호환성 · 상호운용성 및 운영상의 문제와 개선 사항은 이후 전환 대상에 반영할 필요가 있다.

아울러 기관 단독으로 전환하기 어려운 다음과 같은 영역은 관련 정책 및 공통 인프라의 전환 방향을 확인하면서 기관 소관 시스템의 전환을 연계하여 추진할 필요가 있다.

- 전자서명 인증체계
- 국가정보통신망 · 행정망 · 국가융합망 연계 구간
- 공공 클라우드 보안체계 및 기관 간 데이터 연계 시스템
- 중앙부처 · 지자체 · 공공기관 등 다른 기관과 연계되는 시스템

마일스톤(~2034년)

각 국가 · 공공기관은 우선전환 결과를 바탕으로 기관 내 주요 시스템 · 서비스 전반으로 양자내성암호 적용 범위를 확대하고, 미전환 대상과 향후 전환 일정을 지속적으로 관리한다.

마. 전환 완료 및 지속 관리 체계 수립(2035년)

이 단계에서는 앞선 단계에서 추진한 양자내성암호 전환 이행 현황을 점검하고, 2035년까지 국가 · 공공부문의 공개 키 암호 사용 영역에 대한 전환을 완료하는 것을 목표로 잔여 대상의 전환을 추진한다. 이와 함께 전환 이후에도 암호자산과 적용 암호기술을 지속적으로 관리하고 향후 기술 · 표준 · 정책 변화에 대응할 수 있는 관리 체계를 정착시키는 것이 중요하다.

각 기관은 암호자산 인벤토리와 전환 로드맵을 기준으로 전환 완료 여부를

점검하고, 아직 전환되지 않은 시스템·서비스의 현황과 사유를 확인하여 잔여 대상의 전환을 추진한다. 이 과정에서 시스템 교체·고도화 일정, 관련 제품과 서비스의 지원 여부, 기관 간 연계 및 공통 인프라 의존성, 예산과 운영 여건 등을 고려하여 구체적인 전환 시기와 방법을 관리할 필요가 있다.

다만 장수명 장비, 폐쇄망 내 특수시스템, 산업제어시스템, 일부 중요 기반시설의 장비, 물리적 교체 주기가 긴 현장 장비 등은 기술적·운영적 제약으로 인해 2035년까지 전환하기 어려운 경우가 있을 수 있다. 이러한 시스템은 단순히 미전환 상태로 남겨두는 것이 아니라 예외 사유와 잔여 위험을 확인하고, 필요한 보완통제와 향후 전환·교체 계획을 수립하여 지속적으로 관리할 필요가 있다.

또한 양자내성암호 전환 과정에서 구축한 암호자산 인벤토리는 전환 완료 후에도 정기적으로 현행화해야 한다. 신규 시스템의 도입, 기존 시스템의 변경·폐기, 인증서와 키의 변경, 암호 알고리즘 및 관련 제품의 변경사항 등을 지속적으로 반영함으로써 기관이 현재 어떤 암호기술을 어디에서 사용하고 있는지를 파악할 수 있는 상태를 유지하는 것이 중요하다.

이러한 관리 체계는 향후 새로운 암호 취약점이 발견되거나 국가 암호정책·표준이 변경되는 경우에도 영향을 받는 시스템과 서비스를 신속하게 식별하고 필요한 암호기술을 변경할 수 있는 암호 민첩성의 기반이 된다. 따라서 양자내성암호 전환은 2035년에 종료되는 일회성 사업으로 보기보다, 향후 암호기술의 변화에 지속적으로 대응할 수 있는 상시적인 암호자산 관리 체계로 전환하는 계기로 활용할 필요가 있다.

2035년까지 달성해야 할 상태는 다음과 같다.

- 공개 키 암호 사용 영역의 양자내성암호 전환 완료
- 전환 이행 현황 점검 및 잔여 대상의 전환·교체 계획 관리
- 양자내성암호 전환에 필요한 조달·인증·검증 기준 및 절차 정비
- 암호 민첩성 기반의 지속적인 암호자산 관리 체계 수립
- 불가피한 미전환 시스템의 예외 사유·잔여 위험·보완통제 관리

- 암호자산 인벤토리의 정기적 현행화 체계 정착

마일스톤(2035년)

국가·공공기관은 주요 공개 키 암호 사용 영역의 양자내성암호 전환을 완료하고, 암호자산 인벤토리의 정기적 현행화와 암호 민첩성에 기반한 지속 관리 체계를 수립한다.

❸ 기관별 자체 로드맵 작성 시 고려 사항

각 기관은 국가·공공기관 전환 로드맵을 기준으로 자체 세부계획을 수립하되, 기관별 업무 특성에 따라 일정과 우선순위를 조정할 수 있다. 기관 규모와 역량에 따라 접근 방식이 달라질 수 있으나, 다음 사항은 모든 기관이 공통적으로 반영해야 한다.

- 2035년 전환 완료 목표를 기준으로 역산하여 계획 수립
- 장기 보호 데이터와 고위험 시스템을 우선 검토
- 신규 시스템은 초기 설계 단계부터 양자내성암호 및 암호 민첩성 반영
- 조달·예산·유지관리사업과 연계하여 단계적으로 전환 추진
- 기관별 전환 로드맵은 주기적으로 갱신하는 관리 문서로 운영
- 국가 정책, 국내·국제 표준, 보안적합성 검증(KCMVP 포함) 체계, 공급업체 지원 상황 변화에 따라 유연하게 수정

[표 13] 자체 로드맵 수립 시 주요 고려사항

기관 유형	자체 로드맵 수립 시 주요 고려사항
중앙부처· 광역 지자체	공통 인프라(행정전자서명, 범정부 PKI) 전환 일정과 연계 필수. 산하기관·지자체 연계 시스템의 상호운용성 계획 포함
중소규모 국가·공공기관	공급업체 의존도가 높으므로 조달 요구사항 반영이 핵심. 범정부 공통 서비스 활용 비중 파악 후 기관 단독 전환 가능 영역 식별

기관 유형	자체 로드맵 수립 시 주요 고려사항
공공 클라우드 이용 기관	이용 중인 클라우드 서비스 제공자(CSP)의 양자내성암호 지원 로드맵 및 예상 시점 우선 확인. SaaS의 경우 기관이 직접 암호 설정을 변경할 수 없으므로 서비스 제공자의 암호화 구조와 전환 정책 파악이 필요. IaaS·PaaS는 기관이 직접 통제 가능한 레이어(앱 레벨 암호화, VPN 설정 등)부터 우선 전환 검토. 계약 갱신 시 양자내성암호 지원 일정을 서비스 수준 협약(Service Level Agreement, SLA)에 반영
연구기관·과학기술기관	장기 보존 연구데이터는 수집 후 복호화(HNDL) 위협에 대한 대응을 우선 검토하고, 장기간 보존해야 하는 전자서명 데이터는 장기검증 방안을 함께 검토할 필요가 있음. 연구망에 대한 성능 영향 분석과 국제 공동연구 연계 구간의 상호운용성 검증도 필요. 데이터 보호 기간이 긴 시스템은 전환 우선순위가 높아질 수 있음
국가핵심기반·OT/ICS 운영기관	운영 중단 자체가 사회적 혼란으로 이어질 수 있으므로, 즉시 전환보다 장기 예외 관리 중심으로 접근한다. 제조사 지원이 없는 장수명 장비는 장기 교체 계획 수립 및 보완통제 유지. OT/ICS 특성상 시험환경 분리 구축 비용 별도 확보 필요

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



Chapter 04

단계별 전환 실행 가이드

Chapter
04 단계별 전환 실행 가이드

본 장에서는 국가·공공기관이 양자내성암호 전환을 실제로 추진할 때 각 단계에서 무엇을 준비하고 어떻게 실행해야 하는지를 구체적으로 설명한다. 3장에서 전환 과정을 6단계 프레임워크로 개괄하였다면, 본 장에서는 각 단계의 실행 방법, 주요 고려사항, 참여 주체별 역할, 산출물 예시, 체크리스트를 실무 담당자가 직접 활용할 수 있는 수준으로 제시한다.

본 장에서 다루는 6단계는 순차적으로 완료해야 하는 고정된 절차가 아니다. 기관의 규모, 운영 환경, 예산 여건, 시스템 특성에 따라 일부 단계는 병행 추진하거나 순서를 조정할 수 있다. 다만 각 단계는 상호 의존적이므로, 앞 단계의 결과물이 다음 단계의 참고 자료로 활용된다는 점에 유의해야 한다. 각 단계의 주요 활동과 산출물을 충실히 확보하지 않으면 후속 단계의 추진에 어려움이 발생하거나 전환 계획의 신뢰도와 완성도가 저하될 수 있다. 예를 들어, 암호자산 인벤토리(②단계)가 충분히 구축되지 않으면 우선순위 결정(③단계)의 신뢰도가 낮아지고, 우선순위가 명확하지 않으면 예산 산정(⑤단계)의 근거를 확보하기 어렵다.

본 장의 구성

단계	구분	주요 내용	해당 절
①	전환 착수 및 거버넌스 수립	추진체계·역할 분장·의사결정 구조 수립	1절
②	암호자산 현황 파악 및 인벤토리 구축	공개 키 암호 사용 현황 파악·인벤토리 구축	2절

단계	구분	주요 내용	해당 절
③	우선순위 결정 및 전환 전략 수립	위험도 · 중요도 기반 우선순위 결정 및 기관별 전략 수립	3절
④	조달 및 공급업체 대응 전략	공급업체 지원 확인, RFP 요구사항 반영, 조달 체계 연계	4절
⑤	예산 계획 수립	단계별 예산 항목 정의, 기존 사업과의 연계 방안 검토	5절
⑥	전환 시행 및 운영 검증	시범 적용 · 성능 · 상호운용성 · 운영 안정성 검증	6절

각 절은 **목적과 배경, 주요 활동 및 고려사항, 산출물 예시, 실무 체크리스트**로 구성된다. 체크리스트는 각 단계 종료 시 기관이 달성해야 할 핵심 사항을 '실무용 확인표' 형태로 제공하며, 담당자가 현재 상태를 자가 점검하고 다음 단계 진입 여부를 판단하는 데 활용할 수 있다.

담당자별 활용 방법

본 장은 정보보안, 정보화사업, 조달 · 계약, 운영 등 다양한 부서의 담당자가 함께 참조하는 실무 안내 내용을 포함하고 있다. 담당자별로 중점적으로 활용해야 할 절이 다를 수 있으므로, 아래 표를 참고하여 업무 역할에 맞는 절부터 시작할 것을 권장한다.

담당자 유형	주요 활용 절
정보보안 담당자	1절(거버넌스), 2절(인벤토리), 3절(우선순위), 6절(검증) 중심으로 활용
정보화사업 담당자	2절(인벤토리), 3절(전환 전략), 4절(조달 반영), 5절(예산) 중심으로 활용
조달 · 계약 담당자	4절(공급업체 대응 · RFP 반영), 5절(예산 계획) 중심으로 활용
운영 담당자	2절(현황 파악), 6절(적용 · 검증 · 장애 대응) 중심으로 활용

양자내성암호 전환은 어느 한 부서만의 과제가 아니다. 특히 거버넌스 수립(4장 1절)은 모든 담당자가 공통으로 숙지해야 하며, 전환이 원활하게 추진되려면 정보보안 · 정보화 · 조달 · 예산 부서 간의 긴밀한 협력이 전 단계에 걸쳐 필요하다.

[그림 6] 양자내성암호 6단계 전환 절차

양자내성암호 6단계 전환 절차

1단계

전환 착수 및 거버넌스 수립

- 기관 차원의 양자내성암호 전환 추진 방향 수립
- 전환 검토 대상 및 추진 범위 설정
- 추진 조직 및 협의체 구성
- 시범적용 추진 여부 결정
- 기관 내 중장기 로드맵 수립
- 국가 정책 및 가이드라인 검토

2단계

암호자산 현황 파악 및 인벤토리 구축

- 기관 내 공개 키 암호 사용 영역 탐색
- 각 시스템의 공개 키 암호 사용 현황과 보호 대상 정보 파악
- 수집한 정보를 암호자산 인벤토리로 정리·관리

3단계

우선순위 결정 및 전환 전략 수립

- 암호자산 인벤토리와 위험평가 기반 시스템별 우선순위 산정
- 현재 위험 수준과 데이터 보호 기간을 고려한 전환 시점 판단

4단계

조달 및 공급업체 대응 전략

- 상용 솔루션 및 보안장비의 양자내성암호 지원 여부와 지원 예상 시점 확인
- 신규 사업 발주 요구사항에 암호 민첩성·표준 기반 구현·하이브리드 지원 조건 반영
- 양자내성암호 적용에 따른 인증·확인서 영향 및 후속 인증·검증 계획 확인

5단계

예산 계획 수립

- 연차별 전환 범위와 우선 투자 대상 설정
- 필요 예산·인력·운영 자원과 장비·소프트웨어 교체 비용 산정
- 기존·예정 사업 예산에 양자내성암호 전환 비용 반영
- 공급업체 지원 시점과 발주·조달·예산 편성 일정을 반영한 중장기 추진계획 수립

6단계

전환 시행 및 운영 검증

- 우선순위가 높은 그룹에서 운영 영향과 전환·검증 가능성을 고려해 시범 대상 선정
- 전환 전·후별 계획을 수립하고 시험환경에서 복구 절차 사전 검증
- 기관의 운영환경 특성을 고려한 검증 절차 충분히 수행

본 장을 활용하기 전 유의사항

본 장의 내용을 활용하기 전 다음 사항을 먼저 확인한다.

- 본 장은 기술 설계서나 구현 지침이 아니다. 특정 제품이나 솔루션의 선택, 알고리즘 파라미터 설정, 프로토콜별 구현 방법 등 기술 구현 수준의 내용은 다루지 않는다. 이에 관한 사항은 NIST, IETF, ISO/IEC 등 관련 국제표준 및 기술 문서를 참고한다.

- 사용할 양자내성암호 알고리즘 및 보안 강도는 2026년 11월 배포한 「국가·공공기관 암호 안전성 기준」 및 암호모듈 검증제도 등의 국가정보원 정책에 따른다. 본 장은 전환 절차와 방법론을 안내하는 것을 목적으로 하며, 알고리즘 선택 기준이나 허용 범위 등 구체적인 암호기술 기준은 다루지 않는다.

- 본 장 전반에서는 초기 전환 대응 방식으로 하이브리드-AND 방식(양자내성암호와 기존 공개 키 암호의 병행 운용)을 기본 전제로 한다. 이는 관련 정책, 검증 체계 및 상호운용성 환경이 정비되는 전환 과도기에 현실적으로 적용 가능한 방식이며, 특정 알고리즘에 대한 의존도를 낮추고 전환 위험을 완화하는 데 도움이 된다. 기존 공개 키 암호에 대한 단독 의존을 종료하는 시점은 국가 정책 및 공공부문 적용 기준에 따라 결정한다.

- 본 장의 각 단계에서 제시하는 산출물 예시와 체크리스트는 기관이 자체 상황에 맞게 조정하여 활용할 수 있는 참고 형식이다. 모든 기관이 동일한 산출물을 동일한 방식으로 작성해야 하는 것은 아니다. 또한, 체크리스트는 예시로써 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

- 국내·국제 표준, 국가 정책, 암호모듈 검증제도, CC인증 및 보안기능확인 제도, 제품 지원 현황은 지속적으로 변화하고 있다. 본 장의 내용은 가이드북 작성 시점을 기준으로 하며, 이후 변경된 사항은 관련 기관의 최신 정책·기준·공지 등 공식 자료를 통해 확인할 필요가 있다.

제1절 전환 착수 및 거버넌스 수립

양자내성암호 전환은 보안 담당 부서만의 과제가 아니다. 전환 과정에서는 현황 파악, 위험 평가, 사업 발주, 예산 확보, 시스템 적용, 운영 검증 등 다양한 업무가 연계되므로, **정보보안, 정보화사업, 조달·계약, 운영 등 여러 부서가 함께 참여하는 기관 차원의 추진체계**가 필요하다. 이 구조가 초기에 명확히 갖춰지지 않으면, 실제 전환이 진행되는 단계에서 역할 혼선, 의사결정 지연, 예산 부족 등의 문제가 발생할 수 있다.

본 절에서는 양자내성암호 전환을 공식 착수하기 위해 필요한 추진체계 구성 방법, 참여 주체별 역할·책임 분장, 의사결정 구조, 인력 운영 모델, 주요 산출물을 설명한다.

❶ 이 단계의 목적과 중요성

거버넌스 수립 단계의 주요 목적은 두 가지다. 첫째, 양자내성암호 전환을 기관의 공식 과제로 확립하는 것이다. 둘째, 이후 모든 전환 단계가 원활하게 진행될 수 있도록 추진 구조, 역할, 의사결정 체계를 명확히 정의하는 것이다. 이 단계에서 추진체계가 명확히 수립되지 않으면 다음과 같은 문제가 발생할 수 있다.

- 암호자산 현황 파악 단계에서 협조 부서가 불분명하여 데이터 수집이 지연됨
- 우선순위 결정 단계에서 의사결정 주체가 불명확하여 전환 대상 확정이 어려움
- 조달 단계에서 양자내성암호 요구사항이 RFP에 반영되지 않아 전환 기회를 놓침
- 예산 편성 시 담당 부서가 불분명하여 예산 확보가 지연되거나 누락됨

왜 초기 거버넌스 수립이 중요한가?

국가·공공기관은 정보화사업 계획 수립과 예산 편성이 사업 착수 1~2년 전에 이루어지는 경우가 많다. 거버넌스가 갖춰지지 않은 상태에서는 양자내성암호 요구사항을 사업 계획에 반영할 시기를 놓치기 쉽다. 특히 차세대 사업이나 클라우드 전환 사업처럼 수년에 걸쳐 진행되는 사업에 초기부터 양자내성암호 대응 구조를 반영하려면, 착수 단계에서 정보화사업 담당자가 전환 작업에 함께 참여하는 것이 필수적이다.

또한 외부 공급업체와의 계약 및 유지관리사업이 진행 중인 경우, 기존 계약 조건을 검토하고 양자내성암호 지원 여부를 사전에 확인하는 작업도 이 단계에서 시작되어야 한다.

❷ 추진 조직 구성

국가·공공기관의 양자내성암호 전환은 단일 부서가 단독으로 추진하기 어렵다. 전환 과정 전반에 걸쳐 정보보안, 정보화사업, 조달·계약, 운영 부서가 유기적으로 협력해야 하며, 외부 공급업체도 전환 준비 과정에 참여시켜야 한다. 이를 위해 기관은 전환 총괄 책임자를 지정하고, 부서 간 협의체를 구성하여 전환 전 과정을 체계적으로 관리해야 한다.

가. 전환 총괄 책임자 지정

전환 총괄 책임자는 기관 차원에서 양자내성암호 전환 전체를 총괄하는 역할을 담당한다. 일반적으로 정보화총괄부서장 또는 이에 준하는 고위 책임자가 이 역할을 수행한다. 전환 총괄 책임자는 단순한 행정적 승인자가 아니라, 전환의 필요성을 기관 내부에 인식시켜 공유하고, 각 부서 간 협력을 촉진하며, 주요 의사결정 시점에 결정권을 행사하는 실질적 추진 리더 역할을 한다. 전환 총괄 책임자가 수행해야 할 주요 역할은 다음과 같다.

- 양자내성암호 전환을 기관의 공식 중장기 과제로 확립하고 관련 부서에 공지
- 추진 조직 구성 및 역할 분장 승인

- 단계별 주요 의사결정 사항 확인 및 결정(전환 범위, 예산 방향, 시범 적용 등)
- 정기 보고 확인 및 외부 기관 협력 창구 역할
- 전환 추진 과정에서 발생하는 부서 간 이견 조정

나. 전환 추진 협의체 구성 및 운영

부서 간 협력을 지속적으로 유지하기 위해서는 정기 협의체를 운영해야 한다. 협의체는 각 부서의 진행 상황을 공유하고, 단계별 의사결정 사항을 논의하며, 발생하는 문제를 조정하는 역할을 한다. 협의체 구성 및 운영의 핵심 요소는 다음과 같다.

- 구성원 : 전환 총괄 책임자(의장), 정보보안 담당관, 정보화사업 담당자, 조달·계약 담당자, 운영 담당자. 필요 시 외부 공급업체 담당자 참여
- 회의 주기 : 초기 착수 단계에는 월 1회 이상, 이후 단계 진행 상황에 따라 조정
- 안건 범위 : 단계별 진행 현황 보고, 의사결정 사항 논의, 부서 간 협력 이슈 조정, 국가 정책·표준 동향 공유
- 의사결정 방식 : 협의체에서 검토 후 전환 총괄 책임자가 최종 결정. 예산·계약 관련 사항은 관련 부서장의 별도 결재를 거침
- 기록 관리 : 회의록 작성 및 보관. 의사결정 근거 문서화

소규모 기관의 현실적 접근

정보보안 담당 인력이 1~2인인 소규모 기관의 경우, 별도 협의체를 구성하기 어려울 수 있다. 이 경우 기존 정보화위원회나 정보보안 점검 회의 등 기존 협의체를 활용하거나, 전문 컨설팅 기관의 지원을 받는 방식을 검토한다. 중요한 것은 별도의 협의체 구성 여부가 아니라, 주요 담당자가 함께 참여하는 협의 체계를 확보하는 것이다.

❸ 참여 주체별 역할·책임(R&R)

양자내성암호 전환에는 정보보안, 정보화사업, 조달·계약, 운영 및 공급업체

등 다양한 주체가 참여한다. 각 참여 주체의 주요 역할과 책임은 다음과 같으며, 기관은 자체 조직 구조와 업무 분장에 맞게 조정하여 적용할 수 있다.

가. 정보보안 담당

정보보안 담당은 양자내성암호 전환의 실질적 주관 부서로, 전환 전 과정에서 기술적 검토와 보안 요구사항 정의를 주도한다. 거버넌스 수립 단계에서 정보보안 담당이 우선적으로 해야 할 일은 다음과 같다.

- 양자내성암호 전환 관련 최신 정부 정책 검토
- 기관 내 암호 사용 현황에 대한 초기 파악 착수(4장 2절 암호자산 인벤토리 구축의 선행 작업)
- 기관의 보안 정책 · 보안적합성 검증 요구사항과 양자내성암호 전환의 연계 방향 검토
- 전환 과정에서 발생 가능한 보안 공백(하이브리드 운영 중 구간별 보안 수준 차이 등)에 대한 초기 위험 식별
- 다른 부서(정보화사업, 조달 등)에 양자내성암호 전환의 필요성과 방향을 설명하는 내부 커뮤니케이션 수행

보안제품 인증·검증 관련 유의사항

CC인증 또는 보안기능 확인서를 취득한 제품의 암호기능을 변경할 경우 기존 인증 · 확인서 효력에 영향을 줄 수 있음을 인지하고, 관련 정책 동향을 지속적으로 모니터링해야 한다. 양자내성암호 알고리즘은 국내 · 국제 표준 알고리즘을 사용할 수 있도록 하고 KCMVP 검증필 암호모듈 혹은 검증대상 알고리즘을 사용해야 하는 경우 검증대상 선정 여부를 확인하고 전환 시점과 방법에 대해 국가정보원과 관계기관의 지침을 확인하여야 한다.

나. 정보화사업 담당

정보화사업 담당은 양자내성암호 전환이 실제 정보화사업으로 구체화될 수 있도록 사업 계획 단계부터 연계 구조를 만드는 역할을 한다.

- 현재 추진 중이거나 계획 중인 중·장기 정보화사업, 클라우드 전환 사업 등의 목록과 일정 파악
- 각 사업의 착수·발주·계약 갱신 시점을 확인하고, 양자내성암호 요구사항 반영이 가능한 시점 식별
- 신규 사업 기획 시 초기 설계 단계부터 암호 민첩성 및 양자내성암호 대응 구조 반영 가능성 검토
- 정보보안 담당과 협력하여 현행 시스템 목록과 운영 현황 공유
- 범정부 공통 인프라(행정정보시스템, 전자서명 인증체계, 국가융합망 등) 연계 현황 파악 및 개편 일정 모니터링

다. 조달·계약 담당

조달·계약 담당은 양자내성암호 전환 요구사항이 실제 계약과 조달 과정에 반영될 수 있도록 하는 역할을 한다.

- 현재 운영 중인 유지관리 계약, 보안장비 운영 계약, 클라우드 서비스 계약 조건과 갱신 시점 파악
- 기존 계약 내 암호 관련 조항(암호 알고리즘 사용 기준, 업그레이드 의무 등) 검토
- 향후 신규 사업 발주 시 RFP에 반영할 양자내성암호 관련 요구사항을 정보보안 담당과 사전 협의
- 공급업체의 양자내성암호 지원 여부 확인을 위한 질의 절차 및 계약 반영 방안 검토(조달 및 공급업체 대응(4장 4절) 연계)

라. 운영 담당

운영 담당은 현행 시스템의 실제 운영 현황을 가장 잘 파악하고 있는 주체로, 암호자산 인벤토리 구축과 전환 영향 분석의 핵심 역할을 담당한다.

- 운영 중인 시스템·장비의 현황 자료 제공(소프트웨어 버전, 설정 현황, 운영 환경 등)

- 업무망 · 인터넷망 · 폐쇄망 및 기관 간 연계 구간 등 망 구성 현황을 파악하여 정보보안 담당과 공유
- 전환 적용 시 운영 연속성에 영향을 미칠 수 있는 요소(야간 연속 작업, 실시간 서비스, 장애 허용 범위 등) 사전 파악
- 유지관리 공급업체와의 소통 창구 역할 수행

마. 공급업체

공급업체는 양자내성암호 적용을 위한 제품 · 서비스 지원, 시스템 개발 · 변경, 유지관리 등 전환 과정에서 필요한 역할을 수행한다. 따라서 원활한 전환을 위해서는 초기 단계부터 관련 공급업체의 참여와 협조를 확보하는 것이 중요하다.

- 담당 시스템의 양자내성암호 지원 여부 및 지원 가능 시점 확인
- 자사 제품 · 솔루션의 양자내성암호 전환 로드맵을 기관에 제출
- 미지원 또는 지원 계획 미확정 시, 대안 및 예상 일정 제시
- 기관의 전환 계획 수립을 위한 기술 정보 및 자료 제공 협조

※ 공급업체의 참여와 협조를 확보하기 위해 관련 요구사항을 계약 조건에 반영하는 방안을 검토한다. 유지관리 계약 갱신 또는 신규 계약 체결 시 양자내성암호 지원 및 관련 계획 제출, 기술 정보 제공 및 전환 지원 협조 등을 계약상 의무로 부여할 수 있다.

❹ 의사결정 구조 수립

양자내성암호 전환 과정에서는 전환 범위 결정, 예산 편성, 시범 적용 착수 등 여러 시점에서 명확한 의사결정이 필요하다. 의사결정 구조가 사전에 정의되어 있지 않으면 결정이 지연되거나 책임 소재가 불명확해질 수 있다.

다음 표는 전환 과정에서 발생하는 주요 의사결정 사항과 이를 담당할 주체를 예시로 제시한다. 이를 각 기관의 결재 체계에 맞게 조정하여 활용한다.

[표 14] 의사결정 사항 및 결정 주체 예시

의사결정 사항	결정 주체	검토·보고 주체	비고
기관 전환 추진 계획 확정	기관장 또는 위임된 고위 책임자	정보화 총괄 책임자+ 정보보안담당	기관 차원의 공식 착수 선언
전환 적용 범위 결정	전환 총괄 책임자	정보보안담당+ 정보화사업담당	시스템 범위·우선순위 포함
예산 편성 계획 수립	예산 담당 부서장+ 기획조정관	정보화사업담당+ 전환 총괄 책임자	중장기 계획과 연계
RFP·계약 조건 반영 여부	계약·조달 담당 부서장	정보보안담당+ 정보화사업담당	법무 검토 병행
시범 적용 착수 및 확대 결정	전환 총괄 책임자	정보보안담당+ 운영담당	검증 결과 보고 후 결정
외부 공급업체 대응 방향 결정	전환 총괄 책임자+ 계약담당 부서장	정보보안담당+ 조달담당	계약 변경 시 별도 결재

의사결정 구조를 수립할 때 다음 원칙을 고려한다.

- 결정 지연 방지 : 주요 의사결정 사항은 사전에 결정 주체를 명확히 지정하여 검토 지연이 발생하지 않도록 한다.
- 문서화 : 모든 주요 의사결정 사항은 회의록 또는 검토 보고서 형태로 문서화하여 근거를 남긴다.
- 상위 보고 체계 : 예산 규모가 크거나 기관 운영에 중대한 영향을 미치는 사항은 기관장 또는 위임된 상위 책임자에게 보고하는 체계를 마련한다.

❺ 인력 운영 모델

양자내성암호 전환을 위한 전담 인력을 별도로 확보하는 것이 이상적이지만, 모든 기관이 이를 실현하기 어려운 것이 현실이다. 기관의 규모와 여건에 맞는 현실적인 인력 운영 모델을 선택하는 것이 중요하다.

[표 15] 전환 전담 인력 운영 모델

운영 모델	적합한 기관 규모	구성 방법	유의사항
전담팀 구성	중앙부처, 광역지자체, 대형 공공기관	정보보안 · 정보화 · 운영 인력으로 별도 전환 전담팀 구성. 필요 시 외부 전문가 자문 포함	전환 기간 동안 지속 운영 필요. 기존 업무와 병행에 따른 업무 부담에 유의
겸임 TF 구성	중소 규모 공공기관, 지자체	기존 부서 인력이 겸임으로 참여하는 한시적 TF 운영. 정기 회의체 운영으로 진행 관리	겸임으로 인한 전환 지연 가능성 관리 필요. 책임자 지정 필수
담당자 지정+ 외부 지원	소규모 공공기관, 기초지자체	내부 담당자 1~2인 지정 후 전문 컨설팅 기관 지원 활용	외부 지원 의존도가 높을 경우 내부 역량 축적 병행 필요

인력 운영 모델과 무관하게 공통적으로 고려해야 할 사항은 다음과 같다.

- 담당자 지정 : 어떤 모델을 선택하든, 양자내성암호 전환 전체를 조율하는 담당자를 최소 1인 이상 명확히 지정해야 한다. 담당자가 명확하지 않으면 전환 과제의 지속적인 관리와 추진이 어려울 수 있다.
- 역량 확보 : 담당자는 양자내성암호 기술의 전문 개발자일 필요는 없지만, 전환 필요성과 진행 흐름을 이해하고 각 부서 간 협력을 조율할 수 있는 역량이 필요하다. 전환 지원 기관의 교육 프로그램, 전문기관 컨설팅, 관련 가이드라인 학습 등을 통해 역량을 확보한다.
- 인수인계 계획 : 담당자 교체 시 전환 진행 현황과 관련 문서가 체계적으로 인수인계될 수 있도록 기록 관리 체계를 초기에 마련한다.

⑥ 국가 정책 및 공통 인프라와의 연계

국가 · 공공기관의 양자내성암호 전환은 기관 단독으로 이루어지는 것이 아니라 국가 차원의 전환 계획 및 공통 인프라 정비 방향과 연계하여 추진되어야 한다. 거버넌스 수립 단계에서부터 다음 사항을 파악하고 전환 추진 방향에 반영한다.

- 범국가 양자내성 암호체계 전환 종합 추진계획[3] 및 관련 후속 지침의 주요 내용과 국가·공공기관에 대한 요구 사항 파악
- 국가정보원의 보안적합성 검증 체계 및 KCMVP 검증 일정 모니터링 : 국가·공공기관 적용을 위해 필요한 검증이 완료된 제품의 가용 시점을 사전에 확인
- 행정전자서명, 전자서명 인증체계, 범정부 공통 인프라의 양자내성암호 전환 일정 파악 : 개별 기관의 전환 계획이 공통 인프라 개편 방향과 충돌하지 않도록 사전 조율
- 전환 지원 기관의 컨설팅, 교육, 테스트베드 프로그램 활용 가능 여부 확인

공통 인프라 의존성이 높은 경우 접근 방법

전자서명 인증체계처럼 범정부 공통 인프라에 의존하는 시스템은 기관 단독으로 전환하기 어렵다. 이 경우 기관은 공통 인프라 운영기관의 전환 일정을 파악하고, 해당 일정에 맞춰 기관 자체 전환 계획을 조정하는 방식으로 접근한다. 공통 인프라가 전환되기 전까지는 하이브리드 방식을 유지하거나 전환을 잠시 보류하는 전략도 현실적인 선택지가 될 수 있다.

❼ 초기 추진 범위 설정

거버넌스 수립 단계에서 모든 시스템을 동시에 전환 대상으로 설정하면 조사 범위가 지나치게 넓어지고 시작 자체가 어려워진다. 초기에는 '우선 현황을 조사해야 할 영역'과 '조사 결과를 바탕으로 단계적으로 전환을 추진할 영역'을 구분하는 것이 현실적이다. 여기서 조사 우선순위와 실제 전환 시기는 반드시 일치하는 것은 아니다.

우선 현황 조사 대상으로 고려할 수 있는 영역은 다음과 같다.

- 공개 키 기반 인증서를 사용하는 대민 서비스·핵심 행정서비스
- VPN, TLS, SSH 등 공개 키 기반 통신 구간
- 장기 보호가 필요한 데이터(개인정보, 장기 보존 행정기록)를 처리하는 시스템

- 차세대 사업·장비 교체 등이 예정되어 있어 지금 반영하지 않으면 전환 시기를 놓칠 수 있는 시스템
- 행정정보공동이용 등 기관 간 또는 범정부 공통 인프라와 연계된 시스템

기관 간 연계 시스템과 범정부 공통 인프라 연계 구간은 기관이 단독으로 변경하기 어렵더라도, 적용 중인 암호기술과 연계 구조 및 영향 범위를 조기에 파악할 필요가 있으므로 우선 조사 대상에 포함한다. 다만 실제 전환은 관계 기관 및 공통 인프라의 전환 일정과 연계하여 추진해야 한다.

다음 영역은 장기 검토 또는 예외 관리 대상으로 분류할 수 있다.

- 단기간 내 폐기·교체 예정 시스템
- 인터넷과 완전히 분리된 폐쇄망 내부 시스템(단, 장기 보호 데이터 처리 여부는 별도 확인 필요)
- 제조사 지원 종료가 임박한 장비 : 교체 일정에 연계하는 것이 효율적
- 범정부 공통 인프라와 연계되어 기관 단독 변경이 불가능한 시스템 : 현황과 영향을 우선 파악하되, 실제 전환은 공통 인프라의 전환 일정이 확정된 이후 이에 맞추어 추진

이 구분은 영구적인 것이 아니라 초기 부담을 줄이기 위한 출발점이다. 범위 설정 과정에서는 운영 담당자와 유지관리사업자가 참여해야 공식 자산 목록에 없는 시스템이나 비공식 연계 구간을 놓치지 않을 수 있다.

⑧ 주요 산출물

거버넌스 수립 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다. 이 산출물들은 이후 모든 전환 단계의 기준 문서로 활용된다.

산출물	내용
양자내성암호 전환 추진계획서	추진 배경·목적, 적용 범위, 추진 조직 및 R&R, 단계별 추진 일정(초안), 주요 고려사항, 초기 위험 요소

산출물	내용
참여 주체별 역할·책임 분장표(R&R)	부서별·담당자별 역할, 책임 사항, 협력 관계, 보고 체계
전환 추진 협의체 운영 계획	협의체 구성원, 회의 주기, 안건 범위, 의사결정 절차, 보고 체계
초기 위험 요소 목록	예상 장애 요인, 기관 특수 제약(폐쇄망, 레거시 등), 외부 의존성 항목

■ 양자내성암호 전환 추진계획서 예시

기관 차원의 계획서로, 정보보호부서, 정보화부서, 운영부서, 조달부서, 예산부서, 외부 위탁사업 관리 조직 등의 역할과 책임(R&R)을 고려하고 다음 사항을 포함하여 작성할 수 있다.

- 추진 배경 및 필요성
- 단계별 추진 방향
- 조직 구성 방향
  - 양자내성암호 전환 전담팀 구성 및 관련 부서(정보보호부서, 정보화부서, 운영부서, 조달부서, 예산부서, 외부 위탁사업 관리 조직 등)의 역할과 승인 주체 및 책임(R&R)을 정의
- 기관 적용 범위

  (예시)
  - 내부 업무시스템
  - 대국민 서비스
  - VPN 및 원격접속 체계
  - 전자서명 인증체계
  - 클라우드 연계 시스템
  - 기관 간 연계 구간

- 예상 일정
- 주요 고려사항
- 초기 위험요소

산출물의 형식과 분량은 기관 규모에 따라 달라질 수 있다. 소규모 기관의 경우 간략한 내부 검토 보고서 형태로 작성하여도 무방하며, 형식보다는 관련 내용(역할 분장, 의사결정 경로, 추진 범위)이 명확히 담겨 있는 것이 중요하다.

⑨ 단계 완료 체크리스트

다음 체크리스트를 활용하여 거버넌스 수립 단계의 핵심 사항이 이행되었는지 확인한다. 모든 항목을 완료한 후 다음 단계(4.2 암호자산 현황 파악)로 진행할 것을 권장한다.

※ 본 체크리스트는 예시이며, 기관의 시스템 · 서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인	4.1 전환 착수 및 거버넌스 수립 – 실무 확인표
□	양자내성암호 전환을 기관의 공식 과제로 확립하였으며, 기관 내 주요 부서에 공지하였다.
□	전환 총괄 책임자(또는 담당자)를 지정하였다.
□	정보보안 · 정보화사업 · 조달 · 운영 담당자가 전환 추진에 참여하는 구조(협의체 또는 TF)를 구성하였다.
□	참여 주체별 역할 · 책임 분장(R&R)을 문서화하였다. ※ 예시 : 정보보안 부서는 위험평가 · 표준 · 정책 검토, 정보화 부서는 시스템 개선, 조달 부서는 계약서 반영
□	정기 협의체(또는 회의체) 운영 계획을 수립하였다.
□	주요 의사결정 사항과 결정 주체를 정의하였다. ※ 예시 : 예산 · 계약 관련 사항은 기관장 결재, 기술적 우선순위 조정은 협의체 심의
□	국가 정책(범국가 양자내성 암호체계 전환 종합 추진계획)을 검토하였다.

확인	4.1 전환 착수 및 거버넌스 수립 – 실무 확인표
□	범정부 공통 인프라의 전환 일정 파악을 시작하였다. ※ 국가정보원과 행정전자서명 운영기관 등의 정책 지침서 확인
□	현재 운영 중인 유지관리·공급업체 계약 현황을 파악하였다.
□	전환 추진계획서(초안)를 작성하였다. ※ [참고] 양자내성암호 전환 추진계획서 목차 예시 1. 추진 배경 및 목적 1.1 양자컴퓨팅 위협 개요 1.2 국가 정책 및 추진 근거 2. 적용 범위 2.1 전환 대상 시스템 범위(초안) 2.2 제외 또는 별도 검토 대상 3. 추진 조직 및 역할·책임 분장 3.1 전환 총괄 책임자 및 협의체 구성 3.2 부서별 역할·책임(R&R) 4. 단계별 추진 일정(초안) 5. 주요 고려사항 및 초기 위험 요소 6. 관련 정책 및 참고 문서 목록
□	초기 위험 요소(전환 제약 사항)를 식별하여 문서화하였다. ※ 초기 위험 요소 예시 : 예산 미확보, 전담 인력 부족, 레거시 장비 업체 지원 종료, 표준 알고리즘 미확정에 따른 재작업 가능성, 연계 기관의 전환 지연 등
□	다음 단계(암호자산 인벤토리 구축)를 위한 역할 분담 및 일정이 수립되었다.

제2절 암호자산 현황 파악 및 인벤토리 구축

암호자산 현황 파악은 양자내성암호 전환 준비 과정에서 가장 기초가 되는 단계이면서, 동시에 많은 기관이 어디서부터 시작해야 할지 막막함을 느끼는 단계이기도 하다. 기관 내 어떤 시스템에서 어떤 암호가 어떻게 사용되고

있는지를 체계적으로 파악하는 작업, 즉 **암호자산 인벤토리(Cryptographic Asset Inventory) 구축**은 이후 모든 전환 단계의 기반이 된다.

이 단계의 핵심은 완벽한 전수조사가 아니라, **우선순위 결정과 전환 계획 수립에 필요한 수준의 정보를 단계적으로 확보**하는 것이다. 처음부터 100% 완전한 인벤토리를 구축하는 것은 불가능할 수도 있으므로, 현실적인 접근 방법과 단계적 구축 전략을 선택하는 것이 중요하다.

❶ 암호자산 인벤토리

암호자산 인벤토리란 기관이 운영하는 시스템과 서비스에서 공개 키 암호가 어디에, 어떤 방식으로, 어떤 알고리즘이 사용되고 있는지를 체계적으로 정리한 목록이다. 단순한 시스템 목록이나 자산 대장과 다르게, 암호자산 인벤토리는 **암호 사용 구조와 전환 영향 범위를 파악하는 것**에 초점을 맞춘다. 암호자산 인벤토리가 필요한 이유는 다음과 같다.

- 전환 대상 파악 : 어떤 시스템이 양자취약 공개 키 암호를 사용하는지 파악해야 전환 계획을 세울 수 있다.
- 우선순위 결정 근거 : 데이터 보호가 필요한 기간, 외부 노출 수준, 전환 난이도 등을 판단하려면 현황 정보가 먼저 있어야 한다.
- HNDL 공격 대응 : 현재 공개 키 암호로 암호화된 데이터뿐 아니라, 대칭키로 암호화된 데이터라도 키 교환 과정에 공개 키 암호(TLS, VPN 등)가 사용된 경우 향후 양자컴퓨터로 해독될 수 있으므로, 장기 보호 데이터와 해당 데이터의 전송 · 접근 경로를 함께 식별하고 대응해야 한다.
- 전환 완료 여부 추적 : 전환이 진행됨에 따라 어떤 시스템이 완료되었고 어떤 시스템이 전환 대상으로 남아 있는지 관리하는 기준으로 활용된다.

암호자산 vs. 일반 IT 자산 목록의 차이

일반 IT 자산 목록은 '서버 A에 어떤 소프트웨어가 설치되어 있는가'를 파악한다. 암호자산 인벤토리는 '서버 A가 어떤 프로토콜로 통신하고 있으며, 그 통신에 어떤 공개 키 암호가 사용되고 있는가', '서버 A에서 발급된 인증서의 알고리즘과 만료일은 언제인가', '서버 A가 처리하는 데이터 중 장기 보호가 필요한 것은 무엇인가' 등을 파악한다.

기존 IT 자산 관리 대장이 있더라도 이를 그대로 암호자산 인벤토리로 사용할 수 없는 이유가 여기에 있다. 기존 자산 목록은 암호자산 인벤토리 구축의 출발점(시스템 목록 파악)으로는 활용할 수 있지만, 그 이후의 암호 사용 구조 파악은 별도로 수행해야 한다.

양자내성암호 전환은 특정 시스템이나 일부 암호 알고리즘을 교체하는 수준을 넘어, 국가·공공기관 전반에서 사용 중인 공개 키 암호와 그 적용 위치를 폭넓게 식별하고 장기간에 걸쳐 전환해야 하는 대규모 암호 전환이다. 그동안 암호 기술은 다양한 시스템·소프트웨어·보안장비 등에 분산되어 사용되어 왔기 때문에, 기관에 따라서는 어떤 암호 알고리즘이 어디에서 사용되고 있는지를 기관 전체 차원에서 파악할 수 있는 암호자산 인벤토리가 충분히 구축되어 있지 않을 수 있다. 이러한 기관에는 이번 전환이 **기관 내부에 흩어져 있던 암호 사용 현황을 처음부터 체계적으로 확인하고 관리 체계를 정비할 수 있는 중요한 기회**가 될 수 있다.

특히 암호자산 인벤토리 구축 과정에서는 양자컴퓨터에 취약한 RSA·ECC 등의 공개 키 암호뿐 아니라, 기존 시스템에 남아 있는 **SHA-1, DES, TDEA (3DES) 등 현재 보안 용도로 사용하기에 부적절하거나 사용이 제한·폐지된 기존 암호 알고리즘**이 함께 발견될 수 있다. 암호자산 인벤토리는 양자내성암호 전환 대상을 찾기 위한 목록에 그치지 않고, 이처럼 그동안 파악하기 어려웠던 취약·노후 암호기술을 식별하고 정비하는 수단으로도 활용할 수 있다. 실제로 암호자산을 상세히 파악하면 취약한 암호 알고리즘의 사용 현황을 식별하는 데 도움이 되며, 양자내성암호 전환을 암호자산 관리 수준을 높이는 기회로 활용할 수 있다는 점이 해외 전환 가이드에서도 명시되어 있다[9].

❷ 암호자산 인벤토리 구축 대상 설정

암호자산 인벤토리 구축을 시작할 때 가장 먼저 결정해야 하는 것은 **조사 대상 범위의 결정**이다. 범위를 너무 넓게 잡으면 정확한 파악이 어렵고, 너무 좁게 잡으면 중요한 전환 대상을 놓칠 수 있다. 인벤토리 구축에서는 분류 체계를 만드는 것보다 대상이 누락되지 않도록 하는 것이 더 중요하다.

이 가이드북에서는 국가·공공기관이 암호자산 인벤토리 구축 범위를 빠짐없이 점검할 수 있도록, 다음 다섯 가지 점검 관점을 예시로 제시한다. 기관의 환경에 따라 소스코드 수준의 암호 라이브러리, 데이터베이스 암호화, 물리적 보안 장치 등도 암호자산 인벤토리 대상이 될 수 있지만, 대부분의 국가·공공기관에서 가장 현실적이고 우선순위가 높은 점검 관점을 다음 표로 분류하였다. 이 분류는 서로 배타적으로 나뉘는 것이 아니라 일부 중첩될 수 있으며, 이는 자연스러운 현상이다. 대상을 인위적으로 완전히 분리하려 하기보다는, **여러 관점에서 교차로 점검함으로써 누락되는 영역이 없도록** 하는 것이 오히려 대상 파악에 효과적이다. 따라서 아래 표는 고정된 분류 체계가 아니라, 암호자산 인벤토리를 다양한 관점에서 점검하기 위한 예시로 활용하는 것을 권장한다.

[표 16] 암호자산 인벤토리 구축을 위한 주요 점검 대상 및 항목 예시

주요 점검 대상	확인 항목	국가·공공기관 해당 예시
보안 통신 프로토콜	TLS 버전 및 설정, VPN 프로토콜(IPsec/SSL), SSH 사용 여부, HTTPS 적용 구간	행정포털 HTTPS, 원격근무 VPN, 내부망 SSH 접속
인증서	발급기관, 유효기간, 암호 알고리즘	웹서버 인증서, 행정전자서명 인증서, 내부 CA
자체 개발 시스템	공개 키 암호 라이브러리, 오픈소스 의존성	전자결재 시스템, 인사 시스템
응용시스템	내부 업무시스템의 암호기능, 기관 간 연계 여부	민원처리시스템, 인사시스템, 세금납부 포털

주요 점검 대상	확인 항목	국가·공공기관 해당 예시
상용 제품	상용 제품의 암호기능 제조사의 양자내성암호 지원 계획 및 로드맵	방화벽, IPS, WAF, 업무 소프트웨어, 클라우드 서비스(IaaS, PaaS, SaaS)
기타	기타 주요 보안 소프트웨어 및 보안장비의 암호기능	키 관리 체계, HSM

이 외에도 기관별로 특수한 환경이 있을 수 있다. 예를 들어 산업제어시스템(ICS)이나 물리 보안 시스템을 운영하는 기관은 해당 시스템의 암호 사용 현황을 별도로 파악할 필요가 있다. 기관은 위 기본 범위를 먼저 파악한 후, 기관 특성에 따라 추가 대상을 검토한다.

⚠ 암호자산 인벤토리 구축 시 흔한 오해

'모든 것을 조사해야 한다'는 부담으로 인해 시작을 미루는 경우가 많다. 암호자산 인벤토리는 처음부터 완전할 필요가 없다. 처음에는 가장 중요하고 파악하기 쉬운 영역(예를 들면, 인터넷 연결 서비스의 인증서와 TLS 설정)부터 시작하는 것이 좋은 출발점이 된다.

또한 데이터베이스 암호화(DB 내부 암호화)나 애플리케이션 레이어의 대칭 키 암호화 자체는 일반적으로 양자취약 공개 키 암호와 직접 관련이 없다. 그러나 해당 데이터가 TLS, VPN 등 공개 키 기반 키 교환 구간을 거쳐 전송되었거나 전송될 경우, 대칭 키 암호로 보호된 데이터라도 HNDL 위협의 영향을 받을 수 있다. 따라서 대칭 키 암호화 여부만으로 암호자산 인벤토리 대상에서 제외하지 말고, 해당 데이터의 전송, 접근, 백업 경로에 공개 키 암호가 개입하는지를 함께 확인한다.

키 교환 구간이 없는 폐쇄망 내 저장 전용 시스템의 경우에도 양자취약 공개키암호 사용 여부와 백업·반출 경로 등을 확인할 필요가 있다. 다만 외부와의 연결 및 데이터 반출이 엄격히 통제되고 양자컴퓨팅 위협에 따른 위험이 낮은 것으로 평가되는 경우에는 암호자산 인벤토리의 상세 조사 우선순위를 낮출 수 있다.

❸ 주요 점검 대상별 주요 파악 항목

암호자산 인벤토리 구축 시에는 단순히 시스템 목록을 작성하는 것만으로는

충분하지 않다. 주요 점검 대상별로 어떤 정보를 수집해야 하는지와 국가·공공기관 환경에서 유의해서 확인해야 할 사항을 함께 파악해야 한다.

가. 보안 통신 프로토콜

보안 통신 프로토콜은 가장 먼저 파악해야 할 대상이다. TLS, VPN, SSH 등 네트워크 통신에 사용되는 프로토콜의 버전과 암호 스위트 설정을 확인한다. 국가·공공기관은 다양한 상용 솔루션과 외부 기관 연계 환경을 운영하므로, 현재 암호화 통신 구성을 파악하여 양자내성암호 적용 시 영향을 받는 구간과 전환 가능성을 검토해야 한다.

주요 파악 항목은 다음과 같다.

- **TLS** : 사용 버전(TLS 1.0/1.1/1.2/1.3), 허용된 암호 스위트 목록, 인증서와의 연계 관계
- **VPN** : 프로토콜 종류(IPsec IKEv1/IKEv2, SSL-VPN 등), 사용 알고리즘, 원격근무 확대로 인한 VPN 이용 현황
- **SSH** : 사용 버전, 키 교환 알고리즘, 관리자 접속 구간 현황
- **이메일** : 공문서 암호화 또는 전자서명 기능(S/MIME)이 사용되는 경우 적용 알고리즘 확인

※ 국가·공공기관 유의사항 : IPsec IKEv1은 보안 취약점이 알려져 있으나, 실제로 구 버전 VPN 장비에서 여전히 사용되는 경우가 있다. TLS 1.0/1.1은 이미 폐지 권고가 있으나 레거시 시스템과의 호환성 때문에 유지되는 사례가 있으므로, 현황 파악 시 반드시 포함한다.

나. 인증서

인증서는 공개 키 암호 사용의 가장 가시적인 지점이다. 만료 일정 파악과 함께 알고리즘 현황을 확인하는 것이 양자내성암호 전환 관점에서 중요하다.

주요 파악 항목은 다음과 같다.

- **X.509 인증서** : 발급기관(CA), 전자서명 알고리즘(RSA-PSS, KCDSA, ECDSA 등), 키 길이, 유효기간
- **인증서 종류별 현황** : 서버 인증서(TLS), 클라이언트 인증서, 코드 서명 인증서, 내부 CA 발급 인증서
- **행정전자서명 인증서** : 발급 알고리즘, 유효기간, 전환 일정에 따른 영향

※ 국가·공공기관 유의사항 : 행정전자서명은 범정부 공통 인프라에 해당하며, 개별 기관이 단독으로 전환하기 어렵다. 현황 파악 시 행정전자서명 관련 인증서를 별도로 표시하고, 공통 인프라 전환 일정에 연동하여 계획할 필요가 있다.

다. 자체 개발 시스템

자체 개발 시스템은 시스템에서 실제로 사용되는 공개 키 암호와 암호 라이브러리, 그리고 향후 양자내성암호로의 교체 가능성을 함께 확인해야 한다. 특히 알고리즘이 직접 구현되어 있거나 특정 암호 라이브러리에 강하게 의존하는 경우에는 전환 시 수정 범위와 비용이 크게 증가할 수 있으므로 이를 우선적으로 파악한다.

주요 파악 항목은 다음과 같다.

- **사용 중인 공개 키 암호** : RSA(키 길이), ECDSA(곡선 종류), DH/ECDH 등 사용 알고리즘
- **암호 라이브러리** : OpenSSL, NSS, BouncyCastle 등 사용 중인 암호 라이브러리와 버전
- **알고리즘 구현 방식** : 알고리즘이 직접 구현(하드코딩)되어 있는지, 라이브러리 또는 API를 통해 호출되는지 여부
- **암호 민첩성 수준** : 알고리즘을 정책 또는 설정 변경만으로 교체할 수 있는지, 소스코드 수정 및 재개발 필요 여부

※ 국가·공공기관 유의사항 : 외주 개발사가 구축한 시스템은 소스코드 접근이 어렵거나 유지관리가 종료된 경우가 있다. 이 경우에는 외주 개발사로부터 사용 중인 암호 라이브러리와

알고리즘 정보를 우선 확인하고, 확인이 어려운 경우에는 실행 파일, 패키지 의존성, 설치된 라이브러리, 운영체제 및 미들웨어 구성 등을 통해 사용 현황을 간접적으로 파악한다.

라. 응용시스템

응용시스템은 앞서 살펴본 보안 통신 프로토콜, 인증서, 암호 라이브러리 등을 기반으로 공개 키 암호를 사용한다. 응용시스템 단위에서는 개별 암호 기술보다는 해당 시스템이 어떤 암호자산에 의존하는지와 양자내성암호 전환 시 서비스에 미치는 영향을 중심으로 파악하는 것이 중요하다.

주요 파악 항목은 다음과 같다.

- **서비스 유형** : 대국민 서비스, 내부 업무 서비스, 기관 간 연계 서비스
- **망 구성** : 업무망, 인터넷망, 폐쇄망, 기관 간 연계 구간 등
- **시스템 배치환경** : 기관 자체 구축, 클라우드 등
- **사용 중인 보안 통신 프로토콜 및 인증서와의 연계 관계**
- **장기 보호 데이터 처리 여부** : 개인정보, 국가 중요 정보, 장기 보존 행정기록 등 장기간 보호가 필요한 데이터 포함 여부
- **시스템 교체 · 변경 주기** : 유지관리 계약, 차세대 사업 계획, 제품의 지원 종료 예정 여부
- **기관 간 연계 여부** : 행정정보공동이용, 타 기관 API 연계 등 외부 시스템과의 연계 현황

마. 상용 제품

국가 · 공공기관은 상용 솔루션 또는 클라우드 서비스가 제공하는 암호기능을 활용하는 경우, 양자내성암호 지원 현황과 전환 계획을 확인해야 한다. 따라서 상용 제품은 기관이 직접 암호기능을 변경하기보다 제품의 양자내성암호 지원 현황과 전환 계획을 확인하는 것이 중요하다.

주요 파악 항목은 다음과 같다.

- **상용 보안장비** : 방화벽, IPS, WAF, VPN 장비, 보안 게이트웨이 등의 관리 인터페이스 및 통신 구간에서 사용하는 암호 알고리즘과 프로토콜
- **클라우드 서비스**(IaaS, PaaS, SaaS 등) : 서비스 제공자의 암호 정책, 양자내성암호 지원 계획 및 전환 로드맵. 특히 SaaS는 기관이 암호 설정을 직접 변경하기 어려우므로, 서비스 제공자의 지원 계획을 확인
- **상용 소프트웨어 및 외주 개발 시스템** : 사용 중인 암호 라이브러리와 알고리즘, 유지관리 계약 여부, 양자내성암호 지원 계획 및 업그레이드 가능 여부
- **외부 연계 제품 및 서비스** : 연계 프로토콜, 인증 방식, 상대 기관 또는 서비스 제공자의 전환 일정 및 지원 계획

※ 국가·공공기관 유의사항 : 상용 제품은 기관이 직접 수정하기 어려운 경우가 많으므로, 암호자산 인벤토리 구축 단계에서 제조사 또는 유지관리 업체에 양자내성암호 지원 여부와 향후 제품 로드맵을 확인하는 것이 바람직하다. 신규 도입이나 유지관리 계약 갱신 시에는 양자내성암호 지원 계획을 함께 확인하는 것을 권장한다.

바. 기타

앞서 제시한 다섯 가지 관점 외에도 기관 공통으로 사용하는 보안 소프트웨어와 보안장비는 별도로 확인할 필요가 있다. 이러한 자산은 여러 시스템이 함께 사용하는 경우가 많아 개별 시스템 점검 과정에서 일부 확인될 수도 있지만, 영향 범위가 넓은 공통 암호 인프라이므로 누락을 방지하기 위해 별도로 점검하는 것이 바람직하다.

주요 파악 항목은 다음과 같다.

- **HSM** : 모델명, 펌웨어 버전, 지원 알고리즘, 양자내성암호 지원 여부 및 업그레이드 계획
- **키 관리 체계** : 키 생성·보관·배포·갱신·폐기 절차, 개인 키 보관 방식(소프트웨어 키, HSM 등), 사용 알고리즘 및 키 길이
- **기타 보안 소프트웨어 및 보안장비** : 통합인증(SSO/IAM), 전자문서 보안, 백업 솔루션 등 자체 암호화 기능을 사용하는 제품의 적용 알고리즘 및 양자

내성암호 지원 여부

※ 국가 · 공공기관 유의사항 : HSM과 키 관리 체계는 여러 응용시스템이 공동으로 사용하는 기관의 핵심 암호 인프라인 경우가 많다. 따라서 개별 시스템 점검과는 별도로 기관 전체의 HSM 및 키 관리 체계 현황을 파악하고, 제조사 또는 공급업체를 통해 양자내성암호 지원 여부와 업그레이드 계획을 확인하는 것이 바람직하다.

❹ 암호자산 수집 방식

암호자산 인벤토리를 구축하는 방식은 크게 네 가지로 구분된다. 실제 현장에서는 한 가지 방식만으로 충분한 경우가 드물며, 기관 환경에 따라 여러 방식을 조합하여 활용하는 것이 효과적이다.

[표 17] 암호자산 인벤토리 구축 방식

수집 방식	적합한 대상	장점	한계 및 유의사항
문서 기반	구축 · 운영 문서가 잘 갖춰진 시스템, 발주 · 검수 문서 보유 시스템	기존 자료 활용 가능. 전체 구조 파악에 유리	문서가 오래되거나 실제와 다를 수 있음. 최신 상태 반영 여부 반드시 확인
담당자 인터뷰	문서가 부족한 레거시 시스템, 운영 현황 파악이 필요한 시스템	실제 운영 현황 반영 가능. 문서에 없는 정보 수집 가능	담당자 기억 의존으로 누락 가능성. 체계적 질문지(인터뷰 가이드) 준비 필요
설정 점검	TLS/SSH 설정, 인증서 유효기간, 알고리즘 설정값 확인	실제 적용 설정 직접 확인 가능. 문서와 실제 차이 발견 가능	접근 권한 필요. 폐쇄망 환경에서는 별도 절차 필요. 시간 · 인력 소요
스캐닝 · 자동화 도구	인터넷 연결 시스템, TLS 인증서 대규모 점검, 네트워크 구간 파악	대규모 시스템의 빠른 현황 파악. 인증서 만료일 · 알고리즘 일괄 확인	행정망 · 폐쇄망에는 적용 어려움. 도구가 탐지 못 하는 내부 암호 로직 존재. 상황에 따라 수기 보완 필요

가. 문서 기반 수집

기존에 보유한 문서와 자료를 활용하여 암호 사용 현황을 파악하는 방식이다. 별도의 기술적 접근이나 도구 없이 시작할 수 있어, 암호자산 인벤토리 구축의 첫 번째 단계로 적합하다. 활용 가능한 문서의 예시는 다음과 같다.

- 시스템 구축 제안서 및 기술규격서 : 구축 당시 적용된 암호와 프로토콜 확인 가능
- 보안성 검토 결과서 : 국가정보원 또는 보안담당관의 보안성 검토 시 암호 관련 사항 확인
- 인증서 관리 대장 : 기 보유한 경우 활용, 없는 경우 이번 기회에 구축
- 시스템 운영 매뉴얼 : 통신 설정, 인증 방식 등이 기재된 경우 참조
- 정보보호 관련 감사 결과 : 취약점 점검 결과 등에서 암호 관련 항목 확인

주의할 점은 문서가 실제 운영 현황과 다를 수 있다는 것이다. 특히 운영 기간이 오래된 시스템일수록 문서와 실제 설정이 다른 경우가 많다. 문서 기반 수집 결과는 반드시 담당자 인터뷰나 설정 점검을 통해 검증해야 한다.

나. 담당자 인터뷰

시스템 운영 담당자, 개발 담당자, 유지관리 외주사 담당자를 대상으로 인터뷰를 통해 암호 사용 현황을 파악하는 방식이다. 문서화가 부족한 레거시 시스템이나 오랫동안 운영된 시스템의 현황을 파악하는 데 효과적이다. 효과적인 인터뷰를 위해 다음 사항을 준비한다.

- 사전에 질문지 작성 : 즉흥적 인터뷰보다 체계적인 질문지를 준비하면 누락을 줄일 수 있다. (예시 질문) '이 시스템은 외부와 HTTPS로 통신하는가?', '인증서는 어디서 발급받았으며 갱신 주기는?', 'VPN을 사용하는가? 어떤 방식인가?'

- 대상자 선정 : 개발 · 운영 담당자 외에 유지관리업체 담당자도 포함하여 인터뷰 시행
- 결과 기록 : 인터뷰 내용을 암호자산 인벤토리 항목에 즉시 반영하고, 불확실한 사항은 추가 확인 필요로 표시

다. 설정 점검

실제 시스템의 설정값을 직접 확인하는 방식이다. 문서나 인터뷰로 파악한 내용과 실제 설정이 일치하는지 검증하고, 정확한 암호 설정 현황을 파악할 수 있다. 주요 점검 항목과 방법의 예시는 다음과 같다.

- 웹서버 TLS 설정 : Apache/Nginx/IIS의 SSL/TLS 설정 파일 또는 관리 콘솔에서 확인. TLS 버전, 허용 암호 스위트, 인증서 정보 확인
- 인증서 상세 정보: 서버에서 제공하는 인증서의 서명 알고리즘, 공개키 알고리즘 및 키 길이, 만료일을 직접 확인
- VPN 설정 : VPN 장비 관리 콘솔에서 IKE 버전, 암호 알고리즘, 인증 방식 확인
- SSH 설정 : /etc/ssh/sshd_config 파일에서 HostKeyAlgorithms, KexAlgorithms 확인

※ 국가 · 공공기관 유의사항 : 폐쇄망 또는 행정망 시스템의 경우 설정 점검을 위해 별도의 접근 절차(보안담당관 승인 등)가 필요할 수 있다. 사전에 접근 권한과 절차를 확인한다.

라. 자동화 분석 도구의 활용

암호자산 인벤토리 구축 과정에서 자동화 분석 도구를 활용하면 대규모 시스템의 암호 사용 현황을 효율적으로 파악할 수 있다. 특히 다수의 정보시스템과 대국민 서비스를 운영하는 기관의 경우, 자동화 도구를 통해 조사에 소요되는 시간과 인력을 크게 절감할 수 있다.

자동화 분석은 크게 정적 분석과 동적 분석으로 구분할 수 있다.

① 정적 분석(Static Analysis)

소프트웨어를 실행하지 않고 소스코드, 바이너리, 설정 파일 등을 분석하는 방식으로, 소프트웨어 개발 단계 또는 CI/CD 파이프라인에 통합하여 활용할 수 있다.

- 소스코드·설정 파일 분석 :
  - 사용 중인 암호 라이브러리, 공개 키 암호, 하드코딩된 암호 설정 등을 확인하는 데 활용 가능. 정적 분석 도구(예 : CodeQL)을 활용하여 소스코드 내 암호 관련 취약 알고리즘의 사용 위치를 식별할 수 있음
- CBOM(Cryptographic Bill of Materials) :
  - 소프트웨어 구성요소의 암호 라이브러리 및 암호기능 사용 현황을 기계 가독형 형식으로 정리한 목록. 정적 분석 도구를 통해 출력한 결과를 CryptoBOM-forge 등의 도구를 통해 유효한 형식으로 변환하여 생성 가능. SBOM(Software Bill of Materials) 개념을 암호 분야에 적용한 것으로, 소프트웨어 공급망의 암호 의존성을 파악하는 데 활용할 수 있음

② 동적 분석(Dynamic Analysis)

실제 운영 중인 시스템과 통신 트래픽을 대상으로 암호 사용 현황을 분석하는 방식이다.

- TLS/인증서 스캐닝 도구 : 도메인별 인증서 암호, 만료일, TLS 버전, 암호 스위트 설정 등을 일괄 확인. 오픈소스(예 : testssl.sh, nmap) 또는 상용 도구 모두 활용 가능
- 네트워크 트래픽 분석 도구 : 실제 통신 트래픽에서 사용 중인 암호 프로토콜, 인증서, 키 교환 방식 등을 캡처·분석(예 : Wireshark, tcpdump). 네트워크 스캐닝 결과와 함께 활용하면 보다 정확한 암호 사용 현황 파악이 가능

다만 자동화 분석만으로는 모든 암호자산을 파악할 수 없으며, 다음 영역은 수기 확인이 필요하다.

- 행정망 · 폐쇄망 구간 : 인터넷 기반 스캐닝이 어려우므로 내부 접근 권한이 있는 도구를 별도 활용하거나 수기 점검 필요
- 애플리케이션 내부 암호 로직 : 소스코드에 직접 구현된 암호 처리 방식은 네트워크 분석만으로 확인하기 어려우므로 소스코드 검토 또는 담당자 인터뷰 필요
- 키 관리 체계 및 HSM 운영 현황 : HSM 등 보안장비 내부의 키 생성, 보관, 폐기 절차와 내부 설정 정보는 스캐닝 도구만으로 확인하기 어려움
- 기관 간 연계 구간 : 상대 기관의 협조 없이는 연계 구간 전체의 암호 적용 현황을 확인하기 어려움
- 운영 정책 및 절차 : 인증서 갱신 절차, 키 교체 주기, 예외 처리 방식 등은 문서 검토 및 담당자 확인 필요

자동화 분석 도구는 암호자산 인벤토리 구축의 효율성과 정확성을 높이는 유용한 수단이지만, 모든 암호자산을 완전하게 식별할 수는 없다. 실제 암호자산 인벤토리 구축 과정에서는 자동화 분석 도구를 수기 조사 및 담당자 인터뷰와 병행하여 활용하는 것이 효과적이다.

❺ 단계적 암호자산 인벤토리 구축 전략

암호자산 인벤토리는 한 번에 완성되는 것이 아니라, 전환 추진 과정 전반에 걸쳐 단계적으로 구축하고 지속적으로 갱신해야 한다. 특히 대규모 전수조사를 먼저 완료한 후 다음 단계로 넘어가겠다는 접근은 현실적이지 않다. '이 정도면 우선순위 결정이 가능한 수준'이라 판단될 때 다음 단계로 진행하는 방식이 실용적이다.

[표 18] 단계별 암호자산 인벤토리 구축 전략

구축 단계	시점	주요 활동	예상 성과
1단계 (초기 파악)	거버넌스 수립 후 즉시 착수	– 기존 문서(시스템 목록, 구축문서, 보안 정책) 검토 – 주요 시스템 담당자 인터뷰 – 인증서 목록 및 VPN·TLS–SSH 사용 구간 파악	– 전체 현황의 약 40~60% 수준 파악 – 우선순위 결정에 필요한 핵심 정보 확보
2단계 (심화 파악)	우선순위 결정 (4장 3절) 착수와 병행	– 우선 전환 대상 시스템 상세 점검 – 설정 점검 및 자동화 도구 적용 (인터넷 연결 구간) – 공급업체·외주사에 암호 사용 현황 자료 요청	– 주요 시스템의 암호 사용 구조 상세 파악 – 전환 난이도 및 영향 범위 분석 가능
3단계 (지속 관리)	전환 추진 기간 전반	– 신규 시스템 구축·변경 시 암호자산 인벤토리 갱신 전환 완료 – 시스템 반영 미전환 시스템 현황 주기적 점검	– 전환 진행 현황 추적 가능 – 예외 관리 체계 기초 자료로 활용

단계적 구축에서 주요 고려 사항은 다음과 같다.

- 시작 기준 완화 : 완벽한 암호자산 인벤토리가 아니어도 핵심 시스템(인터넷 연결 서비스, VPN, 주요 인증서) 파악만으로도 우선순위 결정을 시작할 수 있다.
- 갱신 트리거 정의 : 신규 시스템 구축, 계약 갱신, 시스템 변경 시 암호자산 인벤토리를 반드시 갱신하는 절차를 수립한다.
- 불확실 항목 표시 : 파악이 불완전한 항목은 '확인 필요'로 표시하고 이후 보완한다. 공백으로 남기는 것보다 불확실 상태를 명시하는 것이 관리에 유리하다.
- 담당자 인수인계 대비 : 암호자산 인벤토리는 특정 담당자의 기억이 아닌 문서로 관리되어야 한다. 담당자 교체 시에도 현황이 유지될 수 있도록 문서화 체계를 갖춘다.

실무 참고 : 암호자산 인벤토리 구축과 예산 계획의 관계

암호자산 인벤토리는 양자내성암호 전환 예산을 산정하기 위한 가장 중요한 기초 자료이다. 어떤 시스템을 전환해야 하는지, 어느 정도의 장비 교체와 소프트웨어 수정이 필요한지 파악해야 예산 규모를 추정할 수 있기 때문이다. 또한 암호자산 인벤토리 구축 자체에도 일정한 비용이 발생한다. 암호자산 현황 파악을 위한 컨설팅 용역, 자동화 스캐닝 도구 도입 또는 임시 이용, 담당자 인터뷰 및 설정 점검에 투입되는 내부 인력 시간 등이 이에 해당한다.

즉, 암호자산 인벤토리는 예산 계획 수립의 기초 자료인 동시에, 이를 구축하는 데에 별도의 예산이 필요하다. 이러한 이유로 암호자산 인벤토리 구축은 예산 관점에서 전형적인 '닭과 달걀' 문제로 볼 수 있다. 따라서 초기 단계에서는 모든 암호자산을 완벽하게 식별하기 위한 대규모 조사를 수행하기보다, 인터넷 연결 서비스, VPN, 인증서 기반 시스템 등 우선순위 결정에 필요한 핵심 영역부터 조사하고, 이후 전환 추진 과정에서 점진적으로 범위를 확대하는 접근이 현실적이다. 암호자산 인벤토리 구축 및 유지관리 비용에 대한 자세한 내용은 4장 5절을 참고한다.

이와 같이 단계적으로 구축한 암호자산 인벤토리를 지속적으로 갱신·관리하기 위해서는 암호자산 정보를 표준화된 형태로 관리하는 방안도 함께 고려할 수 있다. 대표적으로 CBOM은 시스템에서 사용되는 암호 알고리즘, 프로토콜, 인증서 및 관련 암호 구성요소 등의 정보를 표준화된 구조로 식별·기술하여 암호자산의 가시성과 관리 가능성을 높이기 위한 방법이다. 기존에 기관이 보유한 암호자산 인벤토리와 별개로 관리하기보다는 기존 자산관리 체계와 연계하여 활용할 수 있으며, 기관은 암호자산 인벤토리를 구축하거나 갱신하는 과정에서 CBOM과 같은 기계 판독 가능한 표준 형식을 적용함으로써 암호자산의 지속적인 탐지·갱신 및 관리 자동화를 지원할 수 있다.

CBOM을 지원하는 CycloneDX는 Ecma International의 국제 표준(ECMA-424)으로 제정되어 있으나, CBOM을 양자내성암호 전환에 활용하기 위한 구체적인 도구와 관리 방식은 현재도 지속적으로 발전하고 있다. 따라서 기관은 특정 형식이나 도구를 전환 초기부터 고정적으로 적용하기보다는 관련 표준과 도구의 발전 상황을 확인하면서 기관의 암호자산 식별·관리 및 전환에 적합한 활용 방식을 검토할 수 있다.

CBOM에 기록되는 암호자산 정보는 정적·동적·네트워크 분석 등의 도구를

활용하여 상당 부분 자동으로 탐지·수집할 수 있다. 예를 들어 사용 중인 암호 알고리즘, 암호 관련 라이브러리 및 버전, 프로토콜, 인증서와 관련 파라미터 등은 소스코드, 바이너리, 실행환경 또는 네트워크 통신을 분석하여 식별할 수 있다. 다만 실제로 자동 식별할 수 있는 정보와 정확도는 분석 방식과 도구, 대상 시스템에 따라 달라질 수 있으므로 필요한 경우 담당자의 확인과 보완이 필요하다.

한편 시스템의 업무 중요도, 양자내성암호 전환에 따른 업무 영향도, 외주·유지관리 계약 현황, 시스템 교체 계획 등은 CBOM이 표현하는 암호자산의 기술 정보와 구분하여 볼 필요가 있다. 이러한 정보는 양자내성암호 전환 대상과 우선순위, 일정 등을 결정하기 위한 조직의 자산·업무·운영관리 정보에 해당한다. 따라서 실제 양자내성암호 전환 계획을 수립할 때에는 CBOM을 통해 파악한 암호자산 현황을 기관이 보유한 시스템·업무·자산관리 정보 등과 연계하여 종합적으로 검토하는 것이 바람직하다.

본 가이드북에서는 이러한 표준화된 형식의 활용 방법을 설명하기 위해 CycloneDX 형식의 CBOM 예시를 제시한다[20].

예시 : CycloneDX 1.7 CBOM의 암호 알고리즘 항목(RSA-2048)

```
"components" : [ {
  "type" : "cryptographic-asset",
  "bom-ref" : "algo-rsa-2048",
  "name" : "RSA-2048",
  "cryptoProperties" : {
    "assetType" : "algorithm",
    "algorithmProperties" : {
        "primitive" : "pke",
        "parameterSetIdentifier" : "2048",
        "executionEnvironment" : "software-plain-ram",
        "implementationPlatform" : "generic",
      "certificationLevel" : [
```

```
            "none"
          ],
          "cryptoFunctions" : [
            "sign",
            "verify",
            "encapsulate",
            decapsulate"
          ],
          "nistQuantumSecurityLevel" : 0
        },
        "oid" : "1.2.840.113549.1.1.1"
      }
    } ]
```

(출처 : https://github.com/qtonicquantum/cbom-cyclonedx-examples/blob/main/examples/nginx/nginx.cbom.json)

CycloneDX CBOM은 알고리즘, 인증서, 프로토콜, 키와 같은 관련 암호자재(related cryptographic material) 등을 암호자산으로 구조화하여 표현하고, bom-ref 및 관련 참조정보를 이용하여 암호자산과 다른 구성요소 간의 관계를 나타낸다. 따라서 시스템과 암호자산의 규모가 커질수록 JSON 원문을 사람이 직접 검토하기보다는 CBOM 생성·분석 도구나 관리 시스템을 활용하여 필요한 정보를 조회·분석하는 방식이 효율적이다.

다음 표는 위 CBOM JSON을 단순히 표 형식으로 변환한 것이 아니라, CBOM을 통해 파악·관리할 수 있는 암호자산 기술 정보와 기관이 별도로 확인·관리해야 하는 업무·운영 정보를 연계한 실무 예시이다. 암호 알고리즘, 프로토콜, 인증서, 키와 같은 관련 암호자재 및 관련 구현·구성요소 등은 CBOM을 통해 구조화하여 관리하고 일부 정보를 도구를 통해 자동으로 탐지·수집할 수 있는 반면, 시스템의 업무 중요도, 양자내성암호 전환 영향도, 외주·유지관리 현황, 시스템 교체 계획 등은 담당자가 기관의 자산·업무·운영관리

체계 등을 통해 별도로 확인 · 관리해야 하는 정보이다. 따라서 다음 표를 활용할 때에는 각 항목의 정보 출처와 수집 방식을 구분하여 관리할 필요가 있다.

[예시] ○○공공기관 CBOM 기반 암호자산 인벤토리(초기 파악 단계)
작성일 : 20XX년 X월 / 작성자 : 정보보안담당관 / 버전 : v0.1(1단계 초기 파악)

시스템	암호기능	암호자산 유형	암호자산 · 주요속성	구현 · 관련 구성요소	식별 · 확인 방식	양자내성 암호 전환 검토	운영 · 전환 참고사항
민원포털	TLS 서버 인증	프로토콜 · 인증서 · 알고리즘	TLS 1.2 / RSA-2048	OpenSSL 1.1.1	자동 탐지	높음	인증서 및 TLS 구성 전환 검토
내부 인사시스템	TLS 서버 인증	프로토콜 · 인증서 · 알고리즘	TLS / RSA-2048	OpenSSL 1.0.2	수동 확인	높음	외주 · 유지관리 현황 확인
원격접속 VPN	VPN 키교환	프로토콜 · 알고리즘 · 키	IKEv1 / RSA-2048	VPN Appliance	업체 확인	매우 높음	장비 · 프로토콜 전환 검토
전자결재	전자서명	알고리즘 · 키 · 인증서	ECDSA P-256	Java JCA	SBOM · 구성정보 연계	높음	인증 · 서명체계 전환 검토
공문서 보관	저장 암호화	알고리즘 · 키	AES-256	DB 암호화 모듈	수동 확인	간접 영향	장기 데이터 보호 · 키 관리 검토
행정정보 공동이용	TLS 통신	프로토콜 · 알고리즘 · 인증서	TLS / RSA-2048	연계 모듈	업체 확인	높음	공동 인프라 일정과 연계
방화벽	관리 인터페이스	프로토콜 · 알고리즘 · 인증서	TLS / RSA-2048	공급업체 펌웨어	업체 확인	중간	제조사의 양자내성 암호 지원 계획 확인

※ 식별 · 확인 방식은 해당 암호자산 정보를 파악한 경로를 예시한 것이다. '자동 탐지'는 정적 · 동적 · 네트워크 분석 등의 도구를 통해 암호자산을 식별한 경우를 의미하며, 'SBOM · 구성정보 연계'는 기존 소프트웨어 구성 정보 등을 활용하여 관련 암호 구현 또는 구성요소를 확인한 경우를 의미한다. '수동 확인'과 '업체 확인'은 자동화된 탐지만으로 확인하기 어려운 정보를 문서 · 설정 검토 또는 공급업체 확인 등을 통해 보완한 경우이다. '양자내성암호 전환 검토'와 '운영 · 전환 참고사항'은 CycloneDX CBOM의 암호자산 정보를 그대로 나타낸 항목이 아니라, CBOM에서 파악한 암호자산 현황을 실제 양자내성암호 전환 우선순위와 계획 수립에 활용하기 위해 기관이 별도로 관리하는 정보를 결합한 예시이다.

위 예시에서 도출되는 초기 분석 결과

① 우선 전환 대상 식별

- 원격접속 VPN(RSA-2048, IKEv1 사용)
- 민원포털(RSA-2048, TLS 1.2 사용)

② 공급업체 의존 자산 식별

- 행정정보 공동이용 → 공통 인프라 전환 일정과 연계 필요

③ 벤더 의존 자산 식별

- VPN 장비, 방화벽 → 제조사 또는 공급업체의 양자내성암호 지원 계획 확인 필요
- 내부 인사시스템 → 외주 개발사의 암호 라이브러리 및 업그레이드 계획 확인 필요

④ 전환 우선순위 검토

- 위 초기 파악 결과를 바탕으로 4장 3절의 전환 우선순위 검토를 위한 기초 자료로 활용 가능

CBOM 생성 도구 : 무료(오픈소스) 우선 활용, 상용 제품은 필요시 검토

CBOM은 반드시 상용 제품이 있어야 작성할 수 있는 것은 아니며, 다음과 같은 무료 · 오픈소스 도구로도 충분히 시작할 수 있다.

- PQCA CBOMkit : 리눅스 재단(Linux Foundation) 산하 Post-Quantum Cryptography Alliance (PQCA)의 오픈소스 CBOM 도구 모음이다. SonarQube 기반 소스코드 암호자산 탐지, GitHub Action을 통한 CI/CD 연계, 컨테이너 이미지 · 디렉터리 분석, CBOM 저장 · 조회 · 시각화 등의 기능을 제공하며 CycloneDX 형식의 CBOM을 생성한다.
- cryptobom-forge : Santander Security Research가 공개한 오픈소스 도구로, GitHub CodeQL Multi-Repository Variant Analysis 결과를 처리하여 CBOM 작성에 활용할 수 있다. (4장 2절 ❹ 참고)

- cdxgen : 다양한 언어와 패키지 관리자를 지원하는 오픈소스 CycloneDX BOM 생성 도구이다. 일반적인 SBOM 생성뿐 아니라 암호자산 식별을 위한 CBOM 생성 기능도 제공한다. 문서 작성일 기준 공식 문서에서는 Java · Python · .NET 프로젝트의 CBOM 생성 기능과 JavaScript · TypeScript 소스코드의 암호 알고리즘 식별 기능 등이 명시되어 있으며, 언어 · 생태계에 따라 암호자산 탐지 방식과 지원 범위에는 차이가 있다.

이러한 오픈소스 도구는 별도의 상용 라이선스 비용 없이 활용할 수 있지만, 조직 환경에 따라 SonarQube · CI/CD · 컨테이너 환경 설정, 탐지 규칙 조정, 결과 검증 및 지속 운영을 위한 기술 인력이 필요할 수 있다. 대규모 시스템을 보유하거나 광범위한 암호자산 탐지, 통합 관리 및 기술 지원이 필요한 기관은 유료 상용 도구로 삼성SDS S-CAPE, SandboxAQ AQtive Guard, IBM Quantum Safe Explorer 등 기업용 암호자산 탐지 · 관리 솔루션 또는 플랫폼을 검토할 수 있다.

CBOM 기반 암호자산 인벤토리의 활용

기존 암호자산 인벤토리가 '어떤 시스템이 어떤 암호를 사용하는가'를 기록하는 데 중점을 둔다면, CBOM 기반 암호자산 인벤토리는 암호 알고리즘뿐 아니라 암호 구성요소, 관리 방식, 변경 이력 등을 함께 관리하는 것을 목표로 한다. 이를 통해 향후 자동 탐지, 변경 이력 관리, 양자내성암호 전환 영향 분석을 더욱 효율적으로 수행할 수 있다.

⑥ 기관 특성을 고려한 현실적 접근 방향

암호자산 인벤토리 구축의 어려움은 기관마다 다르다. 규모, 인력, 시스템 구조, 외주 의존도에 따라 현실적으로 적용 가능한 방법이 달라질 수 있다. 다음 표는 기관 유형별로 고려할 수 있는 적용 예시를 제시한다.

[표 19] 기관별 암호자산 인벤토리 구축 접근방법 예시

기관 유형	예상 주요 특성 및 어려움	권장 접근 방법	우선 착수 영역
중앙부처 (대형 기관)	시스템 수가 많고 외부 연계 구간 다수. 공통 인프라 의존성 높음. 담당 인력 다소 여유	전담 TF 구성 후 시스템 유형별로 분류하여 단계적 파악. 자동화 도구(인터넷 연결 구간)와 수기 조사 병행	인터넷 연결 대국민 서비스, VPN, 전자서명 인증체계 관련 시스템
지방 자치단체	시스템 다수이나 담당 인력 부족. 행정정보 공동이용 등 타기관 연계 많음. 외주 의존도 높음	유지관리업체에 현황 자료 요청 우선. 광역지자체 지원 또는 전환 지원 기관의 컨설팅 활용. 핵심 서비스 위주 우선 파악	대민 서비스(민원, 세금), 인증서 관련 시스템
중소 공공기관	전담 정보보안 인력 1~2인. 대부분 외주·SaaS 의존. 내부 시스템 규모는 상대적으로 작음	공급업체·위탁사에 현황 파악 협조 요청이 가장 효율적. 전환 지원 프로그램 활용. 간단한 점검표 기반 자가 진단	VPN, 인증서 만료 현황, 주요 SaaS 서비스
연구기관·공공기관 (IT집약)	내부 개발 시스템 비중이 높고 암호 라이브러리 직접 사용 가능성 있음. 기술 역량은 비교적 높음	소스코드 수준의 암호 사용 현황 파악 포함. 내부 개발팀과 협력하여 라이브러리 의존성 분석	내부 개발 시스템의 암호 라이브러리, 자체 인증서 운영 구간

기관 유형과 무관하게 공통으로 적용할 수 있는 현실적 원칙은 다음과 같다.

- **'지금 당장 할 수 있는 것'**부터 시작 : 인증서 목록 파악, VPN 설정 확인처럼 쉽게 시작할 수 있는 것부터 착수하면 전체 진행이 쉬워진다.
- 외주사를 암호자산 인벤토리 구축 파트너로 활용 : 외주 개발·운영 환경에서는 유지관리 계약 범위 내에서 암호 현황 자료 제출을 요청할 수 있으며, 계약 갱신 시 관련 요구사항을 반영하는 방안을 검토할 수 있다.
- 국가 지원 활용 : 정부 및 유관기관의 양자내성암호 전환 지원사업, 정보보호 컨설팅, 기술 가이드 등을 적극 활용하여 전문적인 지원을 받을 수 있다.

- 완벽함보다 지속성 : 처음부터 완전한 암호자산 암호자산 인벤토리를 구축하기보다는 지속적으로 갱신·보완되는 관리 체계로 운영하는 것이 현실적이다.

암호자산 인벤토리 구축 시 자주 받는 질문

Q. 암호자산 인벤토리를 전부 파악하기 전에 다음 단계(우선순위 결정)로 넘어갈 수 있나요?

A. 가능하다. 인터넷 연결 서비스, VPN, 인증서 현황만 파악되어도 초기 우선순위 결정은 가능하다. 완벽한 암호자산 인벤토리를 기다리다 전환 자체가 지연되는 것이 더 큰 문제이다.

Q. 외주사가 암호 현황 자료 제출을 거부한다면?

A. 시스템 운영 정보 제공은 유지관리 계약의 범위에 포함되는 것이 일반적이다. 계약서를 확인하고, 필요시 계약을 갱신할 때 암호자산 현황 제공 의무를 명시적으로 포함한다. 기존 계약에 관련 조항이 없다면 협조 요청 공문을 발송하는 방식도 활용할 수 있다.

Q. 행정망 내부 시스템은 어떻게 파악해야 하나요?

A. 행정망 내부 시스템은 인터넷 기반 외부 스캐닝만으로는 확인하기 어려우므로, 내부망에 설치·운영되는 자산관리 도구, 에이전트 기반 탐지 도구, 취약점 진단 도구, 네트워크 분석 도구 등을 활용하여 암호 사용 현황을 조사할 수 있다. 자동화 도구로 확인하기 어려운 애플리케이션 내부 암호 로직, 키 관리 체계, 운영 정책 등은 담당자 인터뷰와 설정 점검을 통해 보완적으로 확인하는 것이 필요하다.

❼ 주요 산출물

이 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다.

산출물	내용
암호자산 인벤토리	시스템·서비스별 암호 사용 현황(프로토콜, 암호, 인증서, 환경 등)을 정리한 문서(4장 2절 ❺의 예시 형식 참고)
장기 보호 데이터 식별 결과	장기 기밀성 보호가 필요한 데이터와 이를 처리하는 시스템 목록
공급업체·외주사 암호 현황 자료	외주 시스템 및 상용 제품의 암호 사용 현황. 공급업체 질의 결과 포함
파악 미완료 항목 목록	'확인 필요'로 표시된 항목과 추가 파악 계획

산출물은 기관 규모에 맞게 간소화할 수 있다. 소규모 기관은 스프레드시트 형태의 간단한 목록으로도 충분하다. 형식보다 내용의 정확성과 지속적인 갱신이 더 중요하다.

⑧ 단계 완료 체크리스트

다음 체크리스트를 활용하여 암호자산 현황 파악 단계의 핵심 사항이 이행되었는지 확인한다. 모든 항목의 완료를 기다리기보다, 핵심 항목이 충족된 시점에 다음 단계(4장 3절 우선순위 및 전환 전략 수립)와 병행 착수하는 것을 권장한다.

※ 본 체크리스트는 예시이며, 기관의 시스템 · 서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인	4.2 암호자산 현황 파악 – 실무 확인표	확인 날짜
□	암호자산 인벤토리 구축 대상 범위를 확인하였다. ※ 참고 : 망 구성(업무망 · 인터넷망 · 폐쇄망 등), 시스템 배치환경(기관 자체 구축 · 클라우드 등), 서비스 유형(대국민 · 내부 업무 · 기관 간 연계 서비스 등)을 구분하여 조사 대상 시스템을 정리하고, 폐지 예정 시스템이나 단순 정보 게시용 시스템 등 조사 우선순위가 낮은 대상은 별도로 표시	
□	기관 내 인터넷 연결 서비스(대국민 포털, 웹서비스 등)의 TLS 버전 및 인증서 현황을 파악하였다. ※ TLS 1.2 이하로 운영 중인 서비스는 별도 표시	
□	VPN · 원격접속 구간의 프로토콜 및 암호 알고리즘 현황을 파악하였다. ※ VPN 장비 관리 콘솔에서 지원 프로토콜(IKEv2 등)과 암호 스위트 설정값 확인	
□	주요 인증서(서버 인증서, 행정전자서명 관련)의 알고리즘 만료일을 목록화하였다. ※ 인증서 발급 대장에서 전자서명 알고리즘과 만료일을 확인하여 갱신 예정 인증서 별도 표시	
□	업무망 · 폐쇄망 내 주요 시스템의 암호 사용 현황 파악을 시작하였다. ※ 예시 : 시스템 운영 담당자 인터뷰와 설정 파일 점검을 병행하여 업무시스템별 암호 사용 여부 조사	

확인	4.2 암호자산 현황 파악 – 실무 확인표	확인 날짜
□	HSM 모델명 및 지원 알고리즘을 확인하였다. ※ HSM 제조사 · 모델명을 확인하고 제조사 홈페이지 또는 문의를 통해 양자내성암호 지원 계획 파악	
□	외주 개발 · 유지관리 시스템에 대한 공급업체 현황 자료 요청을 완료하였다.	
□	상용 보안장비의 암호 설정 현황 확인 또는 공급업체 문의를 시작하였다.	
□	행정정보공동이용 등 타기관 연계 구간을 식별하고 단독 전환 불가 영역으로 표시하였다. ※ 연계 시스템 목록에서 상대 기관과 협의가 필요한 구간은 별도 표시	
□	장기 보호 데이터, 민감 데이터, 중요 데이터 등을 처리하는 시스템을 식별하였다. ※ 예시 : 전자기록물 관리대장에서 기밀성 보호 기간 10년 이상 항목과 이를 처리하는 시스템을 매칭하여 목록화	
□	암호자산 인벤토리 초안을 작성하였다.	
□	파악 미완료 항목을 '확인 필요'로 표시하였으며, 추가 파악 계획을 수립하였다.	
□	암호자산 인벤토리 갱신 주기 및 갱신 담당자를 지정하였다.	

제3절 우선순위 결정 및 전환 전략 수립

모든 시스템을 동시에 양자내성암호로 전환하기는 어렵기 때문에, 기관은 우선 대응이 필요한 영역을 식별하고 단계적인 전환 전략을 수립해야 한다. 우선순위는 보안 위험도뿐 아니라 실제 전환 가능성과 준비 여건을 함께 고려하여 결정한다.

양자내성암호 전환은 단순한 암호 알고리즘의 기술적 교체가 아니라 자산 식별, 공급업체 대응, 조달 계획, 기술 검증, 예산 확보 등이 함께 이루어져야 하는 장기적인 활동이다. 기관은 모든 시스템을 동시에 전환하기 어렵기 때문에, 우선 대응이 필요한 영역을 식별하고 단계적인 전환 전략을 수립해야 한다.

양자내성암호 전환의 우선순위는 위험도만으로 결정되지 않는다. 국가 · 공공

기관은 데이터 중요도, 수집 후 복호화(HNDL) 공격 등 보안상 위험 요소뿐 아니라 사업 추진 시점, 공급업체 지원 현황, 보안적합성 검증 가용성, 조달 일정, 범정부 공통 인프라 의존성 등 실제 전환 가능성도 함께 고려해야 한다. 따라서 기관은 위험도와 전환 여건을 종합적으로 검토하여 단계적 전환 계획을 수립할 필요가 있다. 이하에서는 이러한 복합적 요소를 반영한 우선순위 결정 기준과 전환 전략 수립 방법을 설명한다.

❶ 수집 후 복호화 위협과 우선순위의 관계

우선순위 결정 시 고려해야 할 주요 요소 중 하나는 **수집 후 복호화(HNDL) 공격**이다. 이는 공격자가 현재 암호화된 통신이나 데이터를 수집·저장해 두었다가, 미래에 암호 해독이 가능한 양자컴퓨터가 등장하면 이를 복호화하는 공격 시나리오를 의미한다.

이 위협의 핵심은 **공격이 미래에 발생하더라도 피해는 현재 수집된 데이터에서 발생**한다는 점이다. 따라서 "양자컴퓨터가 실용화된 이후에 대응하면 된다"는 접근은 HNDL 위협에 충분한 대응이 되지 못할 수 있다. 지금 이 순간 전송되거나 저장되는 데이터가 이미 공격자에 의해 수집·보관되고 있을 수 있기 때문이다.

HNDL 위협이 국가·공공기관에 가장 위험한 영역

HNDL 위협이 국가·공공기관에 가장 위험한 영역

HNDL 위협은 데이터 자체의 암호화 방식뿐 아니라, 암호화에 사용되는 키를 교환·설정하는 과정에서 사용되는 공개 키 암호에도 영향을 받는다. 실제 대부분의 정보시스템은 데이터 보호를 위해 AES와 같은 대칭 키 암호를 사용하지만, TLS, VPN, 전자서명, 인증서 기반 인증 등에서는 공개 키 암호를 이용하여 키 교환이나 신뢰성 검증을 수행한다. 따라서 장기간 보호가 필요한 데이터는 현재 대칭 키 암호로 보호되고 있더라도 HNDL 위협의 영향을 받을 수 있다. 다음과 같은 데이터를 처리하는 시스템은 HNDL 위협 노출 가능성이 높으므로 우선순위 결정 시 상위 대상으로 고려할 필요가 있다.

- **10년 이상 기밀성 유지가 필요한 정보** : 외교 · 안보 문서, 공공기록물, 장기 보존 행정기록, 장기간 보호가 필요한 개인정보
- **국가 핵심기반 관련 데이터** : 에너지, 수도, 교통, 통신 등 국가 핵심 인프라 관련 운영 데이터
- **대규모 개인정보** : 주민등록, 복지, 민원 정보 등 국민 식별 및 행정서비스 제공에 활용되는 정보로서 유출 시 대규모 피해가 발생할 수 있는 정보
- **국가 간 이전 데이터** : 외교 통신, 국제 협력 업무 정보 등 장기간 기밀성이 요구되는 정보

반면 인증 · 전자서명은 HNDL 위협과는 다른 위협 구조를 가진다. 인증 · 서명은 검증 시점에 공격자가 위조할 수 있어야 위협이 실현되므로, 양자컴퓨터가 실제로 등장한 이후에야 직접적인 위협이 된다. 그러나 인증서 발급 · 검증 인프라, 코드서명 체계는 다른 수많은 시스템이 의존하는 '신뢰 루트(Root of Trust)'이므로, 전환 영향 범위와 전환 난이도를 고려하면 지금부터 계획적으로 준비해야 한다.

❷ 우선순위 결정 기준

본 가이드북은 국가 · 공공기관 환경을 반영하여 양자내성암호 전환이 필요한 시스템을 대상으로 다음 9개 기준에 따라 전환 우선순위를 평가할 것을 권장한다. 우선순위는 특정 기준만으로 결정하지 않고, 각 시스템의 특성을 고려하여 9개 기준을 종합적으로 평가한다. 이미 적용 환경에 적합한 양자내성암호로 전환이 완료된 시스템은 우선순위 평가 대상에서 제외하고, 암호자산 인벤토리를 통해 적용 현황을 지속적으로 관리한다.

[표 20] 전환 우선순위 기준

평가 항목	평가 내용	높은 점수 예시	낮은 점수 예시
① 데이터 중요도 (1~3점)	보호 대상 정보의 성격과 침해 시 영향도	• 국가핵심기반시설 운영 정보 • 국가 안보 · 외교 정보	• 기관 홍보 자료 • 공개된 통계 자료

평가 항목	평가 내용	높은 점수 예시	낮은 점수 예시
② 데이터 보호기간 (1~3점)	정책이나 규정에 의해 명시된 데이터 보호 기간	• 영구·준영구 보존 전자기록물 • 외교 문서	• 단기 행정처리 데이터 • 단기간 사용 후 폐기되는 임시 데이터
③ 외부 노출 수준 (1~3점)	인터넷 접속 가능 여부, 공격자 접근 가능성	• 대국민 포털 • 민원 시스템	• 폐쇄망 내부 시스템 • 물리적 격리 환경
④ 파급력 (1~3점)	침해·장애 발생 시 다른 시스템·서비스로 파급되는 범위와 심각성	• 국가 핵심기반시설 • 대규모 행정서비스	• 보조 업무시스템 • 대체 업무수단이 있는 소규모 시스템
⑤ 기관 간 연계 여부 (0~2점)	다른 기관 시스템과의 상호운용성 의존도	• 행정정보공동이용 • 범정부 연계 시스템	• 물리적 격리 환경
⑥ 공급업체 의존성 (0~2점)	암호 교체·설정의 외부 업체 의존도	• 상용 암호화 기기 의존 시스템 • 외부 위탁개발 시스템	• 자체 개발·운영 시스템
⑦ 핵심 신뢰 인프라 여부 (0~2점)	다른 시스템에 인증 신뢰 기반 제공	• 인증서 발급·검증 인프라 • 코드서명 체계	• 독립 운영 시스템
⑧ 시스템 교체 계획 (1~3점)	가장 가까운 교체·갱신까지의 시간	• 단시일 내 교체 및 고도화 예정 시스템	• 조기 폐기 예정 시스템 • 최근 개편 완료 시스템
⑨ 전환 난이도 (0~2점)	기술적 복잡성, 예상 소요 기간 및 투입 인력	• 다수 이기종 시스템과의 연동 시스템 • 아키텍처의 광범위한 수정이 필요한 시스템	• 대체가능한 상용 암호화 기기 존재 • 설정 변경만으로 전환 가능한 시스템

이하에서는 9개 기준 각각의 의미와 국가·공공기관 환경에서의 특수한 고려사항을 설명한다.

① 데이터 중요도

이 기준은 해당 시스템에서 처리·저장·전송하는 데이터 자체의 민감성과 보호 중요도를 평가한다. 국가 망 보안체계(N2SF)에 따라 분류된 C/S/O 등급을 참고하되[4], 양자내성암호 전환 관점에서는 특히 암호체계가 무력화되었을 때 **기밀성·무결성 등의 훼손으로 회복하기 어려운 피해가 발생할 수 있는 정보를 중요하게 고려**한다. 국가·공공기관 환경에서 중요하게 고려할 수 있는 정보 유형의 예시는 다음과 같다.

- 국가 비밀 및 안보 관련 정보 : 가장 높은 중요도. 비밀 취급 인가 체계와 연계하여 판단
- 대규모 개인정보 : 주민등록·가족관계 정보, 세금·복지 수급 정보, 공공의료 기록, 공공기관 보유 민원·인허가 정보 등 유출 시 대규모 국민 피해와 사회적 파급 효과가 발생할 수 있는 중요 정보
- 국가 핵심기반 운영 데이터 : 에너지·수도·교통·통신 등 핵심 인프라 운영 관련 데이터
- 행정 고유 식별 데이터 : 납세, 건강보험, 부동산 등 국민 전체에 영향을 미치는 핵심 행정 데이터
- 외교·국제 협력 관련 정보 : 대외 관계 문서, 국제기구 협의 관련 정보

② 데이터 보호 기간

이 기준은 HNDL 위협의 핵심 판단 요소다. **데이터를 암호화된 상태로 얼마나 오래 보호해야 하는가**를 평가한다. 보호 필요기간이 길수록 현재 수집된 암호화 데이터가 미래에 복호화될 가능성을 고려해야 하므로 HNDL 관점의 전환 우선순위가 높아질 수 있다. 특히 보호 기간이 양자 위협 예상시점과 중첩될 가능성이 있는 경우에는 우선적으로 검토할 필요가 있다. 데이터 자체가 AES 등 대칭 키 암호로 보호되어 있더라도, 데이터 전송이나 키 설정 과정에서 양자 취약 공개 키 암호가 사용된다면 해당 구간의 HNDL 노출 가능성을 함께 확인해야 한다. 따라서 보호 기간에 대한 평가는 데이터 암호화 방식과 함께 해당

시스템의 공개 키 암호 사용 구간을 반드시 병행하도록 한다. 국가·공공기관 환경에서 특히 장기 보호가 필요한 데이터 유형의 예시는 다음과 같다.

- 공공기록물 : 「공공기록물 관리에 관한 법률」 및 기관별 기록관리기준표에 따라 영구·준영구 또는 10년 이상 보존 대상으로 분류되는 전자기록물, 행정정보 데이터, 주요 정책·의사결정 기록 등에서 암호화된 상태로 저장·전송되는 기록
- 국민 식별 및 행정서비스 정보 : 주민등록·가족관계·민원·인허가 등 국민 식별과 행정서비스 제공에 장기간 활용되는 정보
- 공공보건·사회보장 정보 : 감염병 대응, 예방접종, 건강검진, 복지급여, 사회보장 수급 이력 등 장기간 보존·활용되는 국민 생활 밀접 정보
- 연금·고용·보훈 등 장기 급여·자격 정보 : 국민연금, 공무원연금, 고용보험, 산재보험, 보훈대상 정보 등 수십 년에 걸쳐 자격 확인과 급여 산정에 활용되는 정보
- 수사·감사·조사 및 권리구제 기록 : 수사·형사, 감사, 조사, 징계, 행정심판·소송 대응 등 장기 보존 필요성이 있고 기밀성 유지가 중요한 기록
- 국가핵심기반 및 공공서비스 운영 데이터 : 에너지, 교통, 통신, 재난안전, 환경, 물관리 등 국가·공공서비스의 운영 연속성과 관련된 데이터로 장기간 보호가 필요한 운영 정보, 구성 정보, 로그 및 이력 정보

※ 데이터 보호 기간을 평가할 때에는 현재 저장되어 있는 데이터뿐만 아니라 해당 시스템이 향후 지속적으로 처리할 데이터에 요구되는 보호 기간도 함께 고려한다. 현재 데이터의 잔여 보호 기간이 짧더라도 향후 장기간 기밀성 보호가 필요한 데이터를 지속적으로 처리하는 시스템이라면 양자내성암호 전환의 필요성과 시점을 검토할 필요가 있다.

③ 외부 노출 수준

공격자가 데이터나 통신에 접근할 수 있는 가능성을 평가한다. 인터넷에 직접 연결된 시스템일수록 공격자가 데이터를 수집(harvesting)하기 쉽다. 국가·공공기관의 망 구성과 외부 연계 수준은 다양하므로, 실제 연결 구조를 다음과 같이 구분하여 평가한다.

- 인터넷망 : 대국민 서비스 포털, 민원 시스템, 공개 API, 이메일 서버 등. HNDL 위협에 가장 직접적으로 노출
- 인터넷망 연계 구간(DMZ) : 방화벽으로 분리되어 있으나 인터넷과 일부 통신이 있는 구간. 노출 수준 중간
- 업무망 : 원칙적으로 인터넷과 분리된 내부망. 그러나 VPN 또는 연계 구간을 통해 간접 노출 가능성 있음
- 폐쇄망 : 인터넷과 완전히 차단된 환경. HNDL 위협 노출 수준 낮음. 그러나 물리적 접근 위협은 별도 고려

※ 국내 특이 사항 : 공무원이 업무용 PC로 인터넷과 행정망을 함께 사용하는 경우, 악성 코드를 통한 내부 데이터 유출 위험이 있으므로 완전 폐쇄망으로 보기 어려운 경우가 있다. 실제 네트워크 분리 수준을 운영 담당자와 함께 확인한다.

④ 파급력

이 기준은 해당 시스템의 암호체계가 침해되거나 전환 과정에서 문제가 발생할 경우, 그 영향이 국민, 기관, 업무, 관련 시스템 등으로 얼마나 크고 광범위하게 확산될 수 있는지를 평가한다. 특정 시스템이나 업무에 영향이 제한되는 경우와 달리, 다수의 국민 및 기관이 이용하거나 여러 업무 시스템과 관련된 경우에는 장애 및 침해로 인한 영향이 광범위하게 확산될 수 있으므로 전환 우선순위를 높게 고려할 필요가 있다.

국가·공공기관 환경에서 파급력이 큰 영역의 예시는 다음과 같다.

- 국가 핵심기반시설 운영 시스템 : 에너지, 수도, 교통, 통신 등 장애·침해 시 국민 생활과 사회·경제 활동에 광범위한 영향을 미칠 수 있는 시스템
- 대규모 대국민 서비스 : 다수 국민이 이용하는 행정, 민원, 복지 등의 서비스로, 장애·침해 시 많은 이용자와 관련 업무에 영향을 미칠 수 있는 시스템
- 다수 기관·시스템이 공동으로 이용하는 시스템 : 여러 기관이나 업무 시스템이 공동으로 이용하여 장애·침해 시 다수 기관과 관련 업무에 동시에 영향을 미칠 수 있는 시스템

- 기관의 핵심 업무를 지원하는 시스템 : 장애 · 침해 시 기관의 주요 기능 수행, 행정서비스 제공 또는 업무 연속성에 중대한 영향을 미칠 수 있는 시스템

교체 주기가 1~3년 이내인 시스템은, 해당 데이터의 중요도가 상대적으로 낮더라도 **'지금 반영하지 않으면 기회를 놓친다'**는 이유로 우선순위를 높게 부여할 수 있다. 특히 예산 확보와 사업 계획 수립이 1~2년 전에 이루어지는 국가 · 공공기관 특성상, 더 이른 준비가 필요하다.

⑤ 기관 간 연계 여부

이 기준은 국가 · 공공기관 환경에서 특히 중요한 요소다. 행정정보공동이용, 범정부 연계 서비스, 공공 API 등을 통해 다른 기관과 긴밀히 연결된 시스템은 **개별 기관이 단독으로 전환하기 어려운 경우가 많다**. 기관 간 연계 여부를 평가할 때 다음 사항을 확인한다.

- 행정정보공동이용 연계 : 전자정부법에 따른 행정정보 공동이용 시스템. 공동이용 기관 전체의 전환 일정 조율이 필요
- 범정부 공통 서비스 연계 : 전자서명(GPKI), 전자인증, 공통 API 등. 공통 서비스 운영기관의 전환 일정에 의존
- 타기관 핵심 서비스 연동 : 다른 공공기관의 시스템이 해당 시스템에 의존하는 경우(예 : 지자체가 중앙부처 시스템 결과를 받아 민원 처리). 전환 시 상대 기관 업무 영향 고려 필수
- 민간 금융 · 통신 시스템 연계 : 전자납부, 공인인증서 등을 통한 민간 연계. 민간 생태계 전환 일정과의 정합성 고려

연계 의존성이 높은 시스템은 '우선 전환 필요'이지만 '단독 전환 불가'인 역설적 상황에 처할 수 있다. 이 경우 **단기적으로 하이브리드 방식을 유지하면서, 관계 기관과 전환 일정을 협의하는 것이 현실적 접근**이다.

⑥ 공급업체 의존성

암호 설정과 교체에 대한 실질적 통제권이 기관에 있는지, 아니면 외부 공급

업체에 있는지를 평가한다. 공급업체 의존성이 높은 시스템은 기관이 원한다고 해서 바로 전환할 수 없으므로, 공급업체 협력 체계 구축이 선행되어야 한다. 공급업체 의존성은 두 가지 방향으로 우선순위에 영향을 미친다.

- 선제 대응 필요(높은 우선순위) : 공급업체 의존도가 높고 현재 공급업체가 양자내성암호 지원 계획을 제시하지 못하는 경우, 또는 지원 종료가 임박한 제품인 경우. 지금 당장 공급업체 대응이나 대체 방안 마련을 시작해야 함
- 실행 가능성 고려(우선순위 조정) : 아무리 전환이 시급해도 공급업체가 양자내성암호를 지원하지 않으면 실질적 전환이 불가능. KCMVP 검증대상 양자내성암호 알고리즘 확정 및 해당 알고리즘을 적용한 제품의 가용성과 함께 '지금 전환할 수 있는가'를 현실적으로 평가

국가·공공기관에서 공급업체 의존성이 특히 높은 영역은 다음과 같다.

- 상용 보안장비(방화벽, IPS, VPN 장비, WAF) : 대부분 펌웨어 업그레이드를 통해서만 알고리즘 교체 가능
- HSM(하드웨어 보안 모듈) : 하드웨어 교체 없이는 지원 알고리즘 확장이 제한될 수 있음
- 외주 개발 시스템 : 유지관리업체가 관리하는 경우, 암호 설정 변경 및 관련 기능 개선 시 업체의 기술 지원이나 별도 사업 발주 필요

⑦ 핵심 신뢰 인프라 여부

이 기준은 해당 시스템이 기관 또는 여러 시스템·서비스의 운영에 필요한 공통 데이터, 인증·전자서명, 암호 키 관리, 정보 연계 등 핵심 기능을 제공하는 기반 역할을 수행하는지를 평가한다. 이러한 시스템은 자체 기능을 수행하는 데 그치지 않고 다른 시스템·서비스 또는 기관이 필요로 하는 데이터나 공통 기능을 제공하므로, 해당 시스템의 암호체계를 전환할 경우 이를 이용하거나 의존하는 다른 시스템·서비스의 전환에도 연쇄적인 영향을 미칠 수 있다.

'④ 파급력'이 침해·장애 또는 전환 실패 시 발생하는 영향의 크기와 범위를 평가하고, '⑤ 기관 간 연계 여부'가 다른 기관·시스템과의 연계 정도를 평가

한다면, 이 기준은 해당 시스템이 다른 시스템·서비스가 의존하는 핵심 기반의 위치에 있는지를 평가한다.

국가·공공기관에서 핵심 신뢰 인프라로 고려할 수 있는 주요 영역은 다음과 같다.

- 인증·신뢰 기반 : 인증서 발급·관리 체계, 전자서명 인증체계, 시점확인 체계 등 다수의 시스템·서비스에서 인증, 전자서명, 인증서 검증 및 신뢰 관계 형성에 공통으로 이용되는 기반이다. 암호 알고리즘이나 인증서 체계의 변경이 이를 이용하는 시스템에 연쇄적으로 영향을 미칠 수 있으므로 관련 시스템과의 호환성 및 전환 일정을 함께 고려할 필요가 있다.
- 암호 키 관리 기반 : HSM, KMS 등 여러 시스템에서 사용하는 암호 키의 생성·저장·보호·관리 등을 담당하는 기반이다. 양자내성암호 전환에 따라 키의 형식이나 크기, 알고리즘 및 관련 인터페이스 등이 변경될 수 있으므로 이를 이용하는 시스템과의 호환성 및 암호모듈, 장비의 지원 여부 등을 함께 검토할 필요가 있다.
- 소프트웨어·업데이트 신뢰 기반 : 코드서명·펌웨어 서명 등 소프트웨어의 출처와 무결성을 확인하고 안전한 배포·업데이트를 지원하는 기반이다. 서명 알고리즘이나 인증서 체계의 전환은 소프트웨어 개발·배포뿐 아니라 이를 검증하는 시스템 및 단말·장비에도 영향을 미칠 수 있다.
- 공통 연계·서비스 기반 : 여러 기관이나 업무시스템이 공동으로 이용하는 정보연계, 중계, 공통 플랫폼 등의 기반이다. 이러한 기반에서 사용하는 암호체계의 변경은 연결된 여러 시스템의 통신·연계방식과 상호운용성에 영향을 미칠 수 있으므로 관련 기관 및 시스템의 전환 일정과 함께 검토할 필요가 있다.

이처럼 핵심 신뢰 인프라는 다른 시스템과의 의존 관계가 크므로, 해당 시스템 자체뿐 아니라 연계 대상의 호환성, 전환 일정, 공급업체 지원 여부 등을 함께 검토해야 한다. 실제 전환 시점과 방식은 관련 시스템과 기술 생태계의 준비 수준을 고려하여 결정한다.

⑧ 시스템 교체 계획

이 기준은 시스템의 생애주기와 사업 추진 일정을 고려하여 양자내성암호 전환을 반영할 수 있는 시점을 평가하기 위한 것이다. 핵심 질문은 **"지금 이 시스템에 양자내성암호 요구사항을 반영하지 않으면 다음 반영 기회까지 얼마나 기다려야 하는가"**이다.

국가·공공기관의 정보시스템은 예산 편성, 사업 기획, 조달 및 구축 절차를 거쳐 운영되므로, 시스템 개선이나 장비 교체가 가능한 시점을 미리 파악하는 것이 중요하다. 특히 신규 구축, 재구축, 계약 갱신, 장비 교체와 같은 시점은 양자내성암호 요구사항을 반영할 수 있는 중요한 기회가 된다.

국가·공공기관의 주요 시스템 개선 또는 개편 시점

국가·공공기관의 정보시스템 개선은 대부분 다음과 같은 사업 유형을 통해 이루어진다. 각 유형의 착수 시점은 양자내성암호 요구사항을 반영할 수 있는 기회라고 할 수 있다.

- **차세대 사업(5~10년 주기)** : 전체 시스템을 재구축하거나 대규모 개편하는 사업으로, 아키텍처와 암호 체계를 근본적으로 개선할 수 있는 가장 중요한 시점. 이 사업이 지나가면 다음 기회까지 5~10년을 기다려야 함
- **유지관리·운영 계약 갱신(1~3년 주기)** : 계약 조건에 양자내성암호 지원 요구사항 포함 가능. 가장 활용성이 높은 기회
- **노후 장비 교체(3~7년 주기)** : 보안장비, 네트워크 장비, HSM 등의 교체 과정에서 양자내성암호 지원 여부를 기술 요구사항에 반영할 수 있는 기회
- **클라우드 전환·클라우드 네이티브 전환 사업** : 클라우드 서비스 또는 플랫폼 선정 과정에서 양자내성암호 지원 기능과 향후 전환 가능성을 검토할 수 있는 시점. 특히 클라우드 네이티브 전환 사업은 MSA(마이크로서비스 아키텍처), 컨테이너 기반 구조 등으로 시스템 아키텍처를 재설계하는 경우가 많으므로 이 단계에서 암호 민첩성을 지원하는 구조를 반영하면 이후에 양자내성암호로 전환해야 하는 비용과 적용 난이도를 줄일 수 있음

교체 주기가 1~3년 이내인 시스템은, 해당 데이터의 중요도가 상대적으로 낮더라도 **'지금 반영하지 않으면 기회를 놓친다'**는 이유로 우선순위를 높게

부여할 수 있다. 특히 예산 확보와 사업 계획 수립이 1~2년 전에 이루어지는 국가 · 공공기관 특성상, 더 이른 준비가 필요하다.

⑨ 전환 난이도

이 기준은 해당 시스템의 양자내성암호 전환 작업을 완료하는 데 필요한 기술적 복잡성, 예상 소요 기간 및 투입 인력을 평가한다. 양자내성암호 전환은 시스템의 구조와 암호기술 적용 방식에 따라 단순한 설정 변경으로 가능한 경우도 있지만, 소스코드나 아키텍처의 광범위한 수정, 장비 교체, 이기종 시스템 간 연동 및 시험 · 검증 등이 필요한 경우에는 상당한 기간과 인력이 소요될 수 있다.

시스템 교체 계획이 신규 구축 · 재구축 · 장비 교체 등 양자내성암호 요구사항을 반영할 수 있는 시점을 평가한다면, 전환 난이도는 실제 양자내성암호 전환을 위해 필요한 변경 · 검증 작업의 규모와 복잡성을 평가한다. 전환 난이도가 높은 시스템은 준비가 늦어질 경우 목표 시점까지 전환을 완료하기 어려울 수 있으므로, 충분한 준비기간을 확보하여 조기에 분석 · 설계 등 전환 준비에 착수할 필요가 있다.

국가 · 공공기관에서 전환 난이도가 높게 예상되는 대표적인 경우는 다음과 같다.

- 레거시 · 하드코딩 암호 : 소스코드에 암호 알고리즘이 직접 구현 · 지정되어 있거나 암호 기능이 시스템 구조와 밀접하게 결합되어 있어 코드 분석과 광범위한 수정 · 재개발이 필요한 경우
- 이기종 시스템 간 연동 : 서로 다른 제조사 · 세대의 장비와 소프트웨어가 연계되어 있어 암호체계 변경에 따른 인터페이스 수정과 상호운용성 시험 · 검증에 상당한 시간과 인력이 필요한 경우
- 대규모 수정 · 재구축 : 양자내성암호 적용을 위해 다수의 애플리케이션 · 모듈 수정, 시스템 아키텍처 변경, 장비 교체 또는 데이터 · 설정 이관 등 광범위한 작업이 필요한 경우

- 광범위한 시험·검증 : 양자내성암호 적용에 따른 성능·용량 영향과 기존 시스템과의 호환성 등을 확인하기 위해 대규모 시험·검증이 필요한 경우

반대로 설정이나 표준 라이브러리 변경 등으로 적용할 수 있고 시스템 수정 및 시험·검증 범위가 제한적인 경우에는 전환 난이도가 낮은 것으로 평가할 수 있다.

※ 이 기준은 전환에 장기간의 준비가 필요한 시스템을 식별하여 전환 준비의 착수 시점을 앞당길 필요가 있는지를 판단하기 위한 기준이다. 실제 적용 단계에서 초기 적용 대상을 선정하기 위한 4장 6절 ❶의 전환 용이성과는 목적이 다르다. 전환 난이도가 높은 시스템은 분석·설계·시험 등 준비를 조기에 시작하되, 실제 적용 시점과 순서는 기술 검증 및 시스템 여건 등을 고려하여 결정할 수 있다.

❸ 우선순위 점수 산정 방법

9개 기준을 체계적으로 종합하기 위해, 본 가이드북은 각 기준에 배점을 부여하고 총점으로 우선순위를 산정하는 방식을 권장한다. 이 방식은 주관적 판단을 완전히 배제하지는 못하지만, 부서 간 협의와 의사결정 근거를 마련하는 데 유용하다.

[표 21] 전환 우선순위 평가 기준 및 배점표

평가 기준	배점	점수 기준	비고
① 데이터 중요도	최대 3점	높음=3 / 중간=2 / 낮음=1	국가비밀·대규모 개인정보는 자동 3점 권고
② 데이터 보호 기간	최대 3점	10년 이상=3 / 3년 이상~10년 미만=2 / 3년 미만=1	'수집 후 복호화' 위협의 핵심 기준
③ 외부 노출 수준	최대 3점	인터넷 직접 연결=3 / 부분 연결=2 / 완전 폐쇄=1	DMZ 구간 포함 시 2점 이상
④ 파급력	최대 3점	높음=3 / 중간=2 / 낮음=1	다수 국민·기관 서비스로 파급되는 경우 상위 점수

평가 기준	배점	점수 기준	비고
⑤ 기관 간 연계	최대 2점	핵심 범정부 연계=2 / 일부 연계=1 / 없음=0	연계 기관 수가 많을수록 상위 점수
⑥ 공급업체 의존성	최대 2점	완전 공급업체 의존 · 제품의 지원 종료 임박=2 / 부분 의존=1 / 자체 통제=0	의존도 높을수록 선제 대응 필요
⑦ 핵심 신뢰 인프라	최대 2점	인증서 발급 · 관리 및 핵심 서명 기반=2 / 인증 · 서명 검증 및 연계=1 / 해당 없음=0	파급 효과가 클수록 별도 가중 고려
⑧ 시스템 교체 계획	최대 3점	3년 이내=3 / 3년 초과~7년 이내=2 / 7년 초과 또는 조기 폐기=1	전환 시점 관점에서 높은 점수가 우선 반영 대상
⑨ 전환 난이도	최대 2점	장기(수년 이상)=2 / 중간(수개월~1년)=1 / 단기(즉시 적용 가능)=0	난이도가 높을수록 조기 착수 필요

(총점 범위 : 최저 5점 ~ 최고 23점)

9개 평가기준은 국가 · 공공기관 정보시스템의 양자내성암호 전환 필요성과 시급성뿐 아니라, 시스템 간 의존 관계와 실제 전환 여건을 함께 고려할 수 있도록 구성하였다. 평가 흐름에 따라 **①~③은 보호 필요성 및 외부 노출**(데이터 중요도, 데이터 보호 기간, 외부 노출 수준), **④~⑦은 영향 및 의존 관계**(파급력, 기관 간 연계 여부, 공급업체 의존성, 핵심 신뢰 인프라 여부), **⑧~⑨는 전환 여건**(시스템 교체 계획, 전환 난이도)으로 구분하였다.

배점은 양자내성암호 전환의 필요성과 시급성을 직접적으로 판단하는 데이터 중요도 · 데이터 보호 기간 · 외부 노출 수준 · 파급력 · 시스템 교체 계획에 각 3점, 시스템의 연계 · 의존 특성 및 전환 과정에서 추가적으로 고려할 필요가 있는 기관 간 연계 여부 · 공급업체 의존성 · 핵심 신뢰 인프라 여부 · 전환 난이도에 각 2점을 부여하였다. 2점 만점 기준에는 모두 0점을 두어 해당 특성이 없거나 영향이 미미한 경우에는 전체 우선순위 점수에 영향을 주지 않도록 하였다.

특히 파급력은 암호체계의 침해 · 장애 또는 전환 실패가 국민, 기관, 업무 관련 시스템 등에 미칠 수 있는 영향의 크기와 범위를 별도로 평가하기 위해 포함하였다. 전환 난이도는 양자내성암호 전환 작업 자체에 필요한 기술적 복잡성,

예상 소요기간 및 투입 인력을 고려하여, 준비에 장기간이 필요한 시스템을 조기에 식별하고 충분한 전환 준비기간을 확보하기 위한 기준으로 포함하였다.

다만 현재의 3점과 2점 배점은 각 평가기준의 상대적 중요도와 평가항목 간 중복 가능성 등을 고려하여 실제 적용 및 시범평가 과정에서 적정성을 추가 검토할 필요가 있다.

우선순위 결정

[표 22] 우선순위 총점 구간별 권장 대응 방향

구분	총점 범위	의미	권장 대응 방향
1순위 (즉시 전환)	19~23점	현재 양자 위협에 가장 직접적으로 노출된 영역. 지금 당장 전환 착수 필요	전담 인력 배정, 별도 예산 확보, 2031년까지 전환 목표 수립. 양자내성암호가 적용된 프로토콜(TLS, SSH 등), 양자내성암호 하이브리드 방식으로 검증된 암호모듈, 국내·국제 표준 혹은 KCMVP 검증대상 후보군 알고리즘을 적용한 제품 등 우선 적용
2순위 (우선 전환)	14~18점	단·중기 내 전환이 필요한 영역. 다음 정보화사업 또는 계약 갱신 시 반드시 반영	차세대 사업, 유지관리 계약 갱신에 양자내성암호 요구사항 포함. 시범 적용 대상 우선 검토
3순위 (계획 포함)	8~13점	중기 전환 대상. 전환 계획에 포함하되 긴급성은 낮음	기관 자체 전환 로드맵에 포함. 공통 인프라 전환 일정에 맞춰 조율
4순위 (모니터링)	7점 이하	현 시점에서 즉각 전환 필요성이 낮은 영역	양자내성암호 적용 암호모듈 및 제품 동향과 전환 추진정책 모니터링 유지. 시스템 변경 시 재평가

⚠ 점수 산정 시 주의사항

총점이 낮더라도 특정 기준에서 극단적으로 높은 점수가 나온 경우(예 : 데이터 중요도 3점+데이터 보호 기간 3점=HNDL 직접 위협)는 별도로 상향 검토한다. 반대로 총점이 높더라도 해당 영역에 적용 가능한 양자내성암호 지원 제품이 아직 충분히 성숙하지 않았거나, 공공부문 적용에 필요한 검증 · 인증체계 현황에 따라 즉시 전환보다 전환 준비를 우선 추진한다.

점수는 현재 시점의 현황일 뿐이다. 국내 · 국제 표준화 진전, 암호모듈 및 제품에서 양자내성암호 적용 현황, 정부 정책 변화에 따라 매년 또는 주요 변화 발생 시 재평가해야 한다.

우선순위 매트릭스 예시

다음은 중규모 공공기관(직원 약 1,000명, 시스템 약 20개 운영)이 4장 2절의 암호자산 인벤토리를 바탕으로 작성한 우선순위 매트릭스 예시다.

평가 대상은 국가 · 공공기관의 기존 보안제품군에 해당하는 제품, 인증 · 연계 인프라 및 업무 · 운영시스템으로 구분하여 제시하였다. 원격접속 VPN과 방화벽은 기존 보안제품군에 해당하며, 나머지 항목은 정보시스템 또는 인프라로서 해당 시스템에서 사용하는 보안제품 및 공개키암호 기능을 고려하여 평가한다.

각 평가 대상에 9개 기준을 적용하여 점수를 산정하고 우선순위를 결정한다.

[예시] ○○공공기관 양자내성암호 전환 우선순위 매트릭스

평가 기준 : ① 데이터 중요도(1~3) / ② 데이터 보호 기간(1~3) / ③ 외부 노출(1~3) / ④ 파급력(1~3) / ⑤ 기관 간 연계(0~2) / ⑥ 공급업체 의존(0~2) / ⑦ 신뢰 인프라(0~2) / ⑧ 교체 계획(1~3) / ⑨ 전환 난이도(0~2)

평가 대상 (시스템·보안제품)	① 데이터 중요도	② 데이터 보호기간	③ 외부 노출	④ 파급력	⑤ 기관간 연계	⑥ 공급업체 의존	⑦ 신뢰 인프라	⑧ 교체 주기	⑨ 전환 난이도	총점	우선 순위
보안제품											
원격접속 VPN (구간보안 제품군)	3	3	3	3	1	2	0	3	1	19	1순위
보안장비(방화벽) (침입차단 제품군)	2	1	1	2	0	2	0	2	1	11	3순위
인증·연계 인프라											
행정전자서명 인프라	3	3	1	3	2	1	2	2	2	19	1순위
행정정보 공동이용 연계	2	2	2	3	2	1	0	2	2	16	2순위
업무·운영시스템											
민원포털(HTTPS)	2	2	3	2	1	1	0	3	0	14	2순위
내부인사시스템	2	2	1	1	0	1	0	2	1	10	3순위
내부 그룹웨어	1	1	1	1	0	1	0	3	0	8	3순위
공공기록물 보관시스템	3	3	1	2	0	1	0	1	1	12	3순위
소프트웨어 업데이트 서버	3	2	1	3	0	1	2	2	0	14	2순위
물리보안 출입관리	1	1	1	1	0	2	0	1	0	7	4순위

위 매트릭스에서 도출되는 전환 전략 방향

1순위(즉시 전환) – 원격접속 VPN(19점), 행정전자서명 인프라(19점) : 별도 예산 확보 후 양자내성암호가 적용된 검증필 암호모듈 적용 제품 활용 전환 착수. VPN은 IKEv2 기반 하이브리드로 우선 전환. 행정전자서명은 관련 정책 및 공통 인증체계 전환 일정을 확인하고 이에 맞추어 준비

2순위(우선 전환) – 행정정보공동이용(16점), 민원포털(14점), 소프트웨어 업데이트 서버(14점) : 다음 유지관리 계약 갱신 시 양자내성암호 요구사항 반영. 행정정보공동이용은 관련 기관과 사전 협의 시작. 소프트웨어 업데이트 서버는 코드서명 체계 전환 준비 착수

3순위(계획 포함) – 보안장비(방화벽)(11점), 내부 인사시스템(10점), 공공기록물 보관시스템(12점), 내부 그룹웨어(8점) : 전환 로드맵에 포함하되 긴급성은 낮음. 공통 인프라 전환 일정 파악 후 조정

4순위(모니터링) – 물리보안 출입관리(7점) : 현 시점에서 즉각 전환 필요성은 낮음. 양자내성 암호 적용 암호모듈 및 제품 동향과 전환 추진정책을 모니터링하고, 장비 교체나 시스템 변경 시 재평가

※ 특이 사항 : 행정전자서명 인프라(19점)는 1순위지만 범정부 공통 인프라에 해당하여 기관 단독 전환 불가. 공통 인프라 운영기관 협력이 선행 조건

❹ 국가·공공기관 특화 우선순위 고려사항

9개 기준을 적용한 점수 산정 외에, 국가·공공기관만의 고유한 맥락에서 추가로 고려해야 할 우선순위 요소가 있다. 이 요소들은 점수로 수량화하기 어렵지만, 전환 시행 순위 결정 시 반드시 함께 검토해야 한다.

가. 행정·민원 서비스 중단 시 파급 효과

전환 작업 자체가 서비스 중단 위험을 내포한다. 특히 대국민 서비스는 24시간 365일 운영이 요구되는 경우가 많으므로, 전환 작업 일정을 수립할 때 서비스 중단 허용 시간과 장애 복구 계획을 반드시 함께 고려해야 한다.

- 서비스 중단 영향 평가 : 전환 작업 중 발생 가능한 서비스 중단이 얼마나 많은 국민에게 영향을 미치는가
- 중단 허용 시간 : 해당 서비스는 야간·주말 등에 점검이 가능한가, 아니면 연중무휴 운영이 필요한가
- 롤백 계획 : 전환 후 문제 발생 시 기존 암호 방식으로 되돌아갈 수 있는 구조인가

일반적으로 서비스 중단 영향이 큰 시스템일수록 **점진적·단계적 전환과 하이브리드 방식을 통한 무중단 전환**을 택한다.

나. 핵심 신뢰 인프라와 조기 준비의 필요성

전자서명 인증체제는 수많은 공공 서비스의 신뢰 기반이다. 이 인프라를 전환하려면 다음과 같은 준비가 선행되어야 하므로, 실제 전환보다 훨씬 이른 시점부터 준비를 시작해야 한다.

- 루트 인증서 및 하위 인증체계 전환: 루트 CA의 암호 알고리즘 변경은 중간 CA 및 하위 인증서의 발급·검증 체계에 영향을 미칠 수 있으며, 다수의 인증서와 연계 시스템에 대한 변경이 필요할 수 있음. 따라서 기존 인증체계와의 호환성 및 단계적 전환 방안을 검토해야 함
- 인증서 생태계 호환성 : 웹 브라우저, 운영체제, 보안 소프트웨어 등이 새 알고리즘을 지원해야 함. 이는 기관 단독으로 해결할 수 없는 생태계 차원의 문제
- 법적·행정적 기반 정비 : 행정전자서명 및 공공부문 인증체계에 양자내성암호를 적용하기 위해 관련 지침, 기술규격, 인증체계 및 운영기준의 정비가 필요할 수 있음
- 검증 체계 정비 : KCMVP 검증을 포함한 보안적합성 검증 체계에 새 알고리즘이 포함되어야 함

이러한 복잡성으로 인해, 핵심 신뢰 인프라의 '전환 설계와 준비'는 가장 먼저 시작해야 하지만, '전환 완료'는 생태계 전체 준비 상황에 따라 가장 나중에 이루어질 수도 있다.

다. 조달·교체 주기상 지금 반영하지 않으면 놓치는 경우

국가·공공기관의 예산·조달 구조 특성상 다음 상황에서는 우선순위와 무관하게 지금 반영해야 하는 경우가 있다.

- 차세대 사업 기획 단계 진입 : 5~10년 후를 바라보는 차세대 사업은 기획 단계에서 설계 방향이 결정됨. 이 시점에 암호 민첩성과 양자내성암호 대응

구조를 반영하지 않으면 시스템 수명 기간 동안 전환이 불가능하거나 매우 어려워질 수 있음

- 대규모 유지관리 계약 체결 예정 : 5년 이상의 장기 유지관리 계약에 양자내성암호 지원 요구사항이 빠지면, 계약 기간 동안 전환을 요구하기 어려워짐
- HSM · 보안장비 구매 또는 교체 시점 : 하드웨어는 한번 도입하면 수년간 교체하기 어려움. 구매 시점에 양자내성암호 알고리즘 지원 여부를 필수 선택 기준으로 포함해야 함
- 클라우드 서비스 계약 전환 : 클라우드 서비스 제공자 변경 또는 신규 계약 시 양자내성암호 지원 로드맵 확인을 선택 기준에 포함

❺ 전환 전략 유형 선택

우선순위와 시스템 특성에 따라 적합한 전환 전략 유형이 달라진다. 기관은 각 시스템에 대해 다음 전략 유형 중 적합한 것을 선택하거나 조합하여 기관 자체 전환 전략을 수립한다.

[표 23] 전환 전략 유형

전략 유형	적용 조건	주요 접근 방법	유의사항
고위험 선제 전환	1순위 시스템, 장기 보호 데이터, VPN · 인증 인프라	별도 예산 확보 후 양자내성암호가 적용된 프로토콜(TLS, SSH 등), 양자내성암호 하이브리드 방식으로 검증된 암호모듈, 국내 · 국제 표준 혹은 KCMVP 검증대상 후보군 알고리즘을 적용한 제품 등이 출시되면 우선 적용. 다만 양자내성암호가 KCMVP 검증대상으로 확정되기 전이라도 RSA 등 기존 검증대상 공개 키 암호와	단독 전환 가능 여부 먼저 확인. 기관 간 연계 구간은 상대 기관과 사전 협의 필수

전략 유형	적용 조건	주요 접근 방법	유의사항
고위험 선제 전환	1순위 시스템, 장기 보호 데이터, VPN·인증 인프라	양자내성암호를 결합한 하이브리드 방식으로 검증받은 암호모듈을 적용하거나, 별도로 하이브리드 방식을 구현하여 선제적으로 전환 시작 가능	단독 전환 가능 여부 먼저 확인. 기관 간 연계 구간은 상대 기관과 사전 협의 필수
사업 연계 전환	차세대 사업, 유지관리 갱신, 노후 장비 교체 예정	기존 정보화사업 설계 단계부터 양자내성암호 요구사항 반영. RFP에 암호 민첩성 조항 포함	사업 발주 1~2년 전부터 준비 필요. 사업 기획 단계에서 정보보안 담당 참여 확보
공통 인프라 연동 전환	전자서명 인증체계, 범정부 연계 구간	공통 인프라 운영기관의 전환 일정 파악 후 연동 계획 수립. 그 전까지는 하이브리드 유지	단독 전환 시도 금지. 상호운용성 문제 발생 가능성 높음
모니터링 및 점진 전환	3~4순위, 폐쇄망 내부 시스템, 조기 폐기 예정	현황 유지하되 양자내성암호 적용 암호모듈 및 제품 동향과 전환 추진정책 모니터링. 시스템 변경 시 양자내성암호 적용 여부 재검토	방치가 아닌 계획적 모니터링. 순위 재평가 주기 설정(최소 연 1회)

또한 실제 적용 방식으로는 다음 두 가지가 주로 검토된다.

- 하이브리드–AND 방식
  - 둘 이상의 암호 알고리즘을 함께 적용하고 그 결과를 안전하게 결합하는 방식으로, 적절하게 구현된 경우 하나의 알고리즘의 안전성이 약화되더라도 다른 알고리즘의 안전성을 기반으로 보호 수준을 유지할 수 있음. 다만 구현 복잡도와 성능 부담이 증가할 수 있으므로 적용 환경에 대한 사전 검토가 필요함. 구체적인 하이브리드 방식의 구분과 세부 유형은 5장 1절 ❶을 참고하고, 실제 적용은 국가 정책 및 관련 검증 기준에 따라 결정할 필요가 있음

- 현재 암호모듈 검증제도에 양자내성암호 기반 하이브리드 방식 관련 검증 내용이 추가됨[5]

• 암호 민첩성 기반 전환

- 시스템 설계 단계부터 알고리즘을 쉽게 교체하거나 파라미터 변경을 용이하게 하는 구조로 구현하는 방식

- 신규 구축 시스템에 적용하면 미래 재전환 비용을 크게 줄일 수 있음. 특히 차세대 사업이나 클라우드 전환 시 매우 효과적으로 적용 가능

⑥ 기관 유형별 전환 전략 조합 예시

우선순위 결정과 전환 전략은 기관 유형에 따라 접근 방식이 달라진다. 다음 표는 기관 유형별로 예상되는 1순위 시스템과 권장 전략 조합을 예시로 제시한다.

[표 24] 전환 전략 예시

기관 유형	주요 1순위 예상 시스템	권장 전환 전략 조합	한국형 특이 고려사항
중앙부처 (행정기관)	행정전자서명 인프라, 대국민 서비스 VPN, 국가 핵심 정보처리 시스템	① 고위험 선제 전환(인증 인프라) ② 사업 기회 연계(차세대 사업) ③ 공통 인프라 연동(전자서명 인증체계)	범정부 공통 인프라 전환 일정 주도적 파악 및 관계기관 협력 필요. 산하기관 전환 지원 역할도 병행
광역지자체	민원처리시스템, 지방세 시스템, 시·도 VPN	① 사업 기회 연계(차세대 지방행정정보시스템 등) ② 고위험 선제 전환(VPN·인증) ③ 공통 인프라 연동	차세대 지방행정정보시스템 사업에 양자내성암호 반영 여부 조기 확인 필수. 국가융합망 등 범정부 공통 통신 인프라 개편 일정 파악 필요. 기초지자체 지원 체계 검토

기관 유형	주요 1순위 예상 시스템	권장 전환 전략 조합	한국형 특이 고려사항
공공기관 (준정부기관 등)	기관 특화 업무시스템, 대국민 서비스, 연구 데이터 처리	① 사업 기회 연계(유지관리 · 차세대) ② 고위험 선제 전환(장기 보호 데이터) ③ 공급업체 대응 강화	공급업체 의존도 높으므로 공급업체의 양자내성암호 지원 로드맵 조기 확인
소규모 기초지자체 · 소형 공공기관	대부분 공통 플랫폼 · SaaS 의존	① 모니터링 유지 ② 공통 인프라 연동 ③ 담당자 지정 및 공급업체 문의 착수	단독 전환보다 범정부 공통 서비스의 전환 현황 파악이 우선

❼ 주요 산출물

이 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다.

산출물	내용
우선순위 평가표	각 시스템에 9개 기준을 적용한 점수와 순위. 4장 3절 ❸ 예시 형식 참조. 이 문서는 이후 조달 전략(4장 4절)과 예산 계획 수립(4장 5절)의 핵심 근거 자료로 활용됨
양자내성암호 전환 대상 분류 목록	즉시 전환 · 우선 전환 · 계획 포함 · 모니터링 영역으로 분류된 시스템 목록. 이후 예산 · 조달 계획의 우선순위 기준으로 활용
기관 자체 전환 전략서	시스템별 전환 전략 유형(고위험 선제 · 사업 연계 · 공통 인프라 연동 · 모니터링)과 적용 방식(하이브리드 · 암호 민첩성 등) 정리
연도별 전환 로드맵	기관의 단계별 전환 일정 초안. 3장의 국가 · 공공기관 전환 로드맵과 정합성을 확인하며 수립

이 단계의 산출물은 최초 수립 후 **최소 연 1회 재평가**가 필요하다. 특히 국가 정책 수립, 암호모듈 및 제품에서의 양자내성암호 적용 현황, 공통 인프라 전환 일정 확정 등 주요 변화 발생 시 즉시 갱신해야 한다.

❽ 단계 완료 체크리스트

다음 체크리스트를 활용하여 우선순위 결정 및 전환 전략 수립 단계의 핵심 사항이 이행되었는지 확인한다.

※ 본 체크리스트는 예시이며, 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인	4.3 우선순위 결정 및 전환 전략 수립 – 실무 확인표
□	9개 우선순위 결정 기준을 이해하였고, 기관의 시스템에 적용할 준비가 되었다. ※ 우선순위 결정 기준 : ①데이터 중요도, ②데이터 보호 기간, ③외부 노출, ④파급력, ⑤기관 간 연계, ⑥공급업체 의존, ⑦신뢰 인프라, ⑧교체 계획, ⑨전환 난이도
□	수집 후 복호화(HNDL) 위협의 개념을 이해하였고, 장기 보호 데이터를 처리하는 시스템을 식별하였다. ※ HNDL(Harvest Now, Decrypt Later) : 현재 암호화된 데이터를 수집·저장해 두었다가 향후 충분한 성능의 양자컴퓨터가 등장하면 이를 복호화하여 정보를 탈취하는 공격 방식
□	4장 2절 암호자산 인벤토리를 바탕으로 각 시스템에 9개 기준 점수를 부여하였다.
□	우선순위 매트릭스(총점 및 순위)를 작성하였다.
□	1순위(즉시 전환) 시스템을 확정하였다. ※ 예시 : 총점 19~23점(1순위 구간)에 해당하고 보안적합성 검증(KCMVP 등) 완료 제품이 있는 시스템을 1순위(즉시 전환) 대상으로 확정
□	전환 대상을 '즉시 전환 / 우선 전환 / 계획 포함/ 모니터링'으로 분류하였다. ※ 4장 3절 ❼의 산출물인 '우선순위 평가표'에 해당
□	기관 간 연계로 인해 단독 전환이 불가능한 시스템을 식별하였다.
□	양자내성암호 하이브리드 방식으로 검증된 암호모듈, 국내·국제 표준 혹은 KCMVP 검증대상 후보군 알고리즘을 적용한 제품 등의 출시 가용성을 고려하여 '전환 가능 시점'을 검토하였다.
□	범정부 공통 인프라의 전환 일정을 파악하였다.
□	주요 시스템 개선 또는 개편 시점(차세대 사업, 유지관리 갱신, 장비 교체)을 파악하고 전환 연계 가능성을 검토하였다.

확인	4.3 우선순위 결정 및 전환 전략 수립 – 실무 확인표
□	각 시스템별 전환 전략 유형(고위험 선제·사업 연계·공통 인프라 연동·모니터링)을 결정하였다. ※ 예시 : 장기 보호 데이터를 다루는 고위험 시스템은 '고위험 선제 전환', 노후 장비 교체 시기가 예정된 시스템은 '사업 연계 전환', 행정전자서명처럼 공통 인프라에 속한 시스템은 '공통 인프라 연동', 그 외 우선순위가 낮은 시스템은 '모니터링'으로 분류
□	하이브리드–AND 방식 또는 암호 민첩성 적용 여부를 시스템별로 검토하였다. ※ 하이브리드–AND 방식은 전환 과정에서 기존 공개 키 암호와 양자내성암호를 함께 적용하고 그 결과를 결합하는 방식이며, 암호 민첩성은 특정 암호 알고리즘이나 구현에 과도하게 종속되지 않고, 향후 암호 알고리즘 변경 시 시스템 전체를 재개발하지 않고도 필요한 구성요소를 신속하고 유연하게 변경할 수 있도록 하는 능력을 의미
□	기관 자체 전환 전략서(초안)를 작성하였다.
□	연도별 전환 로드맵(초안)을 수립하였다. ※ 예시 : 3장 3절의 국가·공공기관 전환 로드맵과 정합성을 갖도록 단계별 목표와 대상 시스템을 표로 정리
□	우선순위 재평가 주기(최소 연 1회)를 정하였다.

[첨부] 양자내성암호 전환 우선순위 점검표

기관은 아래 양식에 자체 시스템 · 서비스를 입력하고 각 기준별 점수를 부여하여 우선순위를 결정한다. 열은 필요에 따라 추가할 수 있다.

점수 기준 요약

① 데이터 중요도 : 높음=3 / 중간=2 / 낮음=1

② 데이터 보호 기간 : 10년 이상=3 / 3~10년=2 / 3년 미만=1

③ 외부 노출 수준 : 인터넷 직접=3 / 부분=2 / 폐쇄=1

④ 파급력 : 높음=3 / 중간=2 / 낮음=1

⑤ 기관 간 연계 : 핵심 범정부 연계=2 / 일부=1 / 없음=0

⑥ 공급업체 의존성 : 완전 의존 · 제품의 지원 종료=2 / 부분=1 / 자체 통제=0

⑦ 핵심 신뢰 인프라 : 인증서 발급 · 관리 및 핵심 서명 기반=2 / 인증 · 서명 검증 및 연계=1 / 없음=0

⑧ 시스템 교체 계획 : 1~3년=3 / 4~7년=2 / 8년 이상 · 폐기=1

⑨ 전환 난이도 : 장기=2 / 중간=1 / 단기=0

No.	시스템 · 서비스명	① 데이터 중요도 (1~3)	② 데이터 보호기간 (1~3)	③ 외부 노출 (1~3)	④ 파급력 (1~3)	⑤ 기관간 연계 (0~2)	⑥ 공급업체 의존 (0~2)	⑦ 신뢰 인프라 (0~2)	⑧ 교체 주기 (1~3)	⑨ 전환 난이도 (0~2)	총점 (최대 23)	우선순위
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												

※ 우선순위 : 총점 19~23점=1순위(즉시 전환) / 14~18점=2순위(우선 전환) / 8~13점=3순위(계획 포함) / 7점 이하=4순위(모니터링)

제4절 조달 및 공급업체 대응 전략

국가 · 공공기관의 정보시스템은 상용 제품, 외주 개발 소프트웨어, 외부 서비스 등 다양한 형태로 도입 · 운영되고 있어 양자내성암호 전환 과정에서 외부 공급업체의 지원이 필요한 경우가 많다. 이 가이드북에서는 제품 · 서비스의 공급이나 개발 · 유지관리 등의 업무를 수행하는 외부 주체를 포괄하여 '공급업체'로 지칭한다. 다만, 각 주체의 역할을 구분할 필요가 있는 경우에는 제조사,

서비스 제공자, 외주 개발사, 유지관리업체 등 해당 역할을 나타내는 용어를 사용한다.

이러한 환경에서는 공급업체의 양자내성암호 지원 여부와 지원 계획이 기관의 전환 가능 시기와 방법에 영향을 미칠 수 있으므로, 기관은 전환을 추진하는 과정에서 관련 공급업체의 대응 계획을 확인하고 필요한 사항을 조달 요구사항에 반영할 필요가 있다.

본 절에서는 공급업체 유형별 대응 전략과 시스템 유형별 접근 방법, 공급업체 대응 절차, RFP 반영 요구사항 및 공급업체 질의서 양식을 제시한다.

❶ 왜 조달·공급업체 대응이 중요한가

한국의 국가·공공기관의 정보화 환경은 다음과 같이 조달·공급업체 대응을 특히 중요한 고유한 특성을 가지고 있다.

- 외주·조달 중심 구조 : 많은 국가·공공기관이 정보시스템을 직접 개발하지 않고 외주 개발사 또는 상용 솔루션을 통해 구축한다. 기관이 소스코드를 보유하지 않거나 암호 설정을 직접 변경하기 어려운 경우가 많다.
- 정보화사업 주기 의존성 : 시스템 변경은 대부분 정보화사업, 유지관리사업, 장비 교체사업을 통해 이루어진다. 사업 발주 시 RFP에 양자내성암호 요구사항이 포함되지 않으면 수년간 반영 기회를 잃게 되는 경우도 있다.
- KCMVP·CC인증 연계 : 국가·공공기관에서는 보안적합성 검증을 통과한 정보보호제품을 사용토록 하고 있다.
  이에 따라, KCMVP 필수 탑재에 해당하는 제품의 경우 이를 적용하여 CC 인증·보안기능 확인서를 발급할 수 있으므로, 이를 통해 전환 가능 시점이 결정된다는 것을 의미한다.
- 공공조달 특수성 : 나라장터(G2B)를 통한 공공조달 체계에서 계약 전 단계인 RFP 작성이 공급업체 선택에 결정적 영향을 미친다. 양자내성암호 요건이 RFP에 없으면 평가 기준에도 반영되지 않는다.

⚠ 국내 현실 : 검증대상 양자내성암호를 적용한 KCMVP 검증필 암호모듈만 RFP에 반영해야 한다는 오해

일부 기관에서는 검증대상 양자내성암호를 적용한 KCMVP 검증필 암호모듈만 적용해야 한다고 생각하여 관련 요구사항을 RFP에 반영하기 어렵다고 생각한다. 그러나 이는 양자내성암호 자체의 적용과 양자내성암호 대응 역량 확보를 혼동한 것이다.

특정 양자내성암호 알고리즘의 적용을 의무화하는 것은 신중할 필요가 있다. 그러나 암호 민첩성 확보, 양자내성암호 지원 계획 제출, 향후 업그레이드 가능 구조, 하이브리드 방식 지원 등은 검증대상 암호알고리즘 선정 등 암호모듈 검증제도 시행과 관계없이 RFP에 반영할 수 있다. 다만, 보안적합성 검증제도에서 별도 요구사항이 있을 경우 이를 RFP에 반영할 필요가 있다.

오히려 암호모듈 검증제도에서 정립·시행되는 관련된 요구사항만을 반영하겠다는 접근은 향후 수년간 구축되는 신규 시스템과 제품에 전환 준비가 전혀 반영되지 않는 결과를 초래할 수 있다. 현재 단계에서 필요한 것은 특정 알고리즘의 즉시 적용이 아니라, 향후 국가 정책과 KCMVP 기준에 따라 양자내성암호를 수용할 수 있는 구조를 확보하는 것이다.

이와 별도로, 2026년 1월부터 양자내성암호 활용 활성화를 위해 KCMVP 검증 대상인 RSA·ECC 등 기존 공개 키 암호 알고리즘과 국내·국제 표준(또는 표준화가 진행 중인) 양자내성암호를 결합한 하이브리드 방식으로 검증받은 검증필 암호모듈을 활용하여 전환을 추진할 수 있으며 특히, KCMVP 검증대상 선정 및 검증 계획에 따라 전환 준비를 추진할 수 있다.

❷ 공급업체 유형별 대응 전략

공급업체는 유형에 따라 양자내성암호 대응 방식과 계약 반영 방법이 다르다. 다음 표는 6가지 주요 공급업체 유형별 핵심 확인 사항과 대응 방법을 제시한다.

[표 25] 주요 공급업체 유형별 대응 방법

공급업체 유형	주요 확인 사항	대응 시 유의점	계약·조달 반영 방법
상용 보안장비 공급업체	방화벽·IPS·VPN·WAF 등의 양자내성암호 알고리즘 지원 여부, 펌웨어 업그레이드 계획, HSM 지원 현황	하드웨어 교체 없이 펌웨어로 지원 가능한지 여부 반드시 확인. HSM은 하드웨어 교체 필요할 수 있음	신규 장비 도입 RFP에 양자내성암호 지원 조항 포함. 기존 장비는 유지관리 계약에 업그레이드 계획 제출 의무화

공급업체 유형	주요 확인 사항	대응 시 유의점	계약 · 조달 반영 방법
클라우드 서비스 사업자 (IaaS · PaaS · SaaS)	클라우드 서비스 제공자의 양자내성암호 지원 계획	SaaS는 기관이 직접 암호 설정을 변경할 수 없으므로 서비스 제공자가 어떤 암호화 구조와 정책을 적용하는지 파악하는 것이 핵심. IaaS · PaaS는 기관이 직접 일부 설정 가능하나 인프라 계층은 클라우드 서비스 제공자에 의존함. 멀티테넌트 환경에서 기관별 전환 시점이 다를 수 있음	클라우드 서비스 계약 시 양자내성암호 지원 로드맵 제출 요구. 서비스 수준 협약(SLA)에 양자내성암호 전환 완료 시점 포함 검토
유지보수 사업자	담당 시스템의 암호 현황 자료 제출 가능 여부, 양자내성암호 전환 기술 지원 역량, 전환 지원 계획	유지보수 사업자가 암호 설정을 관리하는 경우 기관의 통제권 제한. 계약서에 자료 제출 의무 명시 필요	유지관리 계약 갱신 시 양자내성암호 지원 역량 평가 기준 포함. 암호 현황 자료 정기 제출 의무화
외주 개발사	납품 소프트웨어의 암호 라이브러리(OpenSSL 등) 버전, 하드코딩 여부, 암호 민첩성 구현 수준	소스코드 소유권 문제로 기관이 직접 수정 불가한 경우 많음. 향후 유지보수 계약 지속 여부 확인 필요	신규 개발 RFP에 암호 민첩성 구현 요건, 라이브러리 최신화 의무, 양자내성암호 전환 가능 구조 명시
인증서 · 키 관리 인프라 공급자	전자서명 인증체계 · CA 소프트웨어의 양자내성암호 기반 인증서 발급 · 검증 지원 계획, HSM 연동 여부, 기존 인증체계와의 병행 운영 및 상호운용성 지원 계획	전자서명 인증체계 전환은 생태계 전체와 연계되어 매우 복잡. 단독 교체 불가 영역 파악 선행 필수	전자서명 인증체계 솔루션 갱신 계획 수립 시 양자내성암호 지원 여부를 핵심 선택 기준으로 설정
타기관 공동 시스템 운영주체	공동 활용 시스템의 양자내성암호 전환 계획, 참여 기관 간 전환 일정 조율 여부, 연계 구간 암호 설정	단일 기관이 단독으로 결정 불가. 운영 주체 기관의 일정을 따라야 함	공동 시스템 관련 협의체에서 양자내성암호 전환 의제 공식 제기. 기관 입장 문서화

공급업체 대응의 공통 원칙은 다음과 같다.

- 조기 대화 시작 : 계약 갱신이나 신규 발주를 기다리지 말고, 현재 계약 관계 내에서 양자내성암호 지원 여부를 먼저 질의한다. 공급업체의 준비 상황은 기관의 전환 계획 수립에 직접 영향을 미친다.
- 답변 문서화 : 공급업체의 양자내성암호 지원 여부 확인은 반드시 서면(이메일, 공문, 질의서 회신) 형태로 받아 기록한다. 이는 이후 계약 협상과 의사결정의 근거자료로 활용한다.
- 단독 의존 위험 인식 : 특정 공급업체만이 해당 기능을 제공하고 양자내성암호 전환 계획이 없는 경우, 장기적으로 공급업체 변경을 검토해야 한다. 이 결정은 충분한 검토 시간이 필요하므로 조기에 파악하는 것이 중요하다.

❸ 시스템 유형별 대응 방향

조달·공급업체 대응 전략은 해당 시스템의 현재 상태에 따라 접근 방식이 달라진다. 다음 표는 6가지 시스템 유형별 대응 방향을 정리한다.

[표 26] 시스템 유형별 대응 방법

시스템 유형	주요 특성	양자내성암호 대응 방향	긴급도
신규 구축·차세대 사업	설계 단계부터 반영 가능한 가장 좋은 기회. 향후 수년~수십 년 운영 예정	초기 설계 단계부터 암호 민첩성을 지원하는 구조 반영. 양자내성암호 알고리즘 지원 가능 라이브러리 및 제품 선택. RFP에 요건 명시	★★★ 지금 반영 안 하면 사업 기간 동안 기회 소멸
계약 갱신 도래 시스템	유지관리·운영 계약이 1~2년 내 갱신 예정인 시스템	계약 갱신 전에 공급업체의 양자내성암호 지원 여부 확인. 갱신 계약 조건에 지원 계획 제출 의무 포함. 미지원 시 교체 여부 검토	★★★ 계약 갱신 시점이 전환 기회

시스템 유형	주요 특성	양자내성암호 대응 방향	긴급도
클라우드 서비스	서비스 유형(IaaS · PaaS · SaaS)에 따라 암호기능 통제 범위가 다르며, 서비스 제공자의 지원 정책 및 전환 일정에 영향을 받을 수 있음	클라우드 서비스 제공자의 양자내성암호 로드맵 조기 확인. 계약 조건에 전환 일정 반영 요구. 대안 서비스 전환 가능성 검토	★★ 클라우드 서비스 제공자 일정에 종속되므로 조기 파악 필수
지원 종료 예정 제품	제조사 지원이 곧 종료되는 장비 · 소프트웨어	양자내성암호 지원 여부 즉시 확인. 미지원 시 교체 일정을 전환 계획에 반영. 교체 전까지 보완 통제 방안 마련	★★★ 지원 종료 전 교체 혹은 보완 결정 필요
다기관 공동 활용 시스템	행정정보공동이용, 범정부 서비스 등 복수 기관이 공동 이용하는 시스템	운영 주체 기관의 전환 일정 파악 우선. 단독 전환 시도 금지. 참여 기관 협의체 통해 공동 대응	★★ 단독 대응 불가, 협력 체계 구축이 핵심
레거시 (장기 운영) 시스템	수년~수십 년 운영 중인 시스템. 문서 부족, 소스코드 미보유, 암호 하드코딩 가능성 있음	암호 사용 현황 파악 우선(4장 2절). 교체 · 개선 시점 확인 후 계획에 반영. 전환 난이도 높으면 전략적 우선순위 조정	★ 상황에 따라 다름. 암호자산 인벤토리 파악 후 결정

예시 : 계약 갱신 도래 시스템 대응 절차

상황 : A 공공기관이 운영 중인 보안장비(방화벽 · VPN) 유지관리 계약이 6개월 후 만료 예정

Step 1(즉시) : 현재 공급업체에 공문 발송 – '계약 만료 전 양자내성암호 지원 계획 및 업그레이드 가능 여부 회신 요청'

Step 2(1개월 내) : 회신 검토 후 ① 지원 가능 → 계약 갱신 조건에 지원 일정 명시 ② 지원 불가 · 미정 → 대체 제품 시장 조사 착수

Step 3(계약 갱신 시) : RFP 또는 계약서에 '향후 양자내성암호 알고리즘 지원 업그레이드 제공' 조항 포함. 미이행 시 패널티 조항 검토

결과 : 기관은 계약 갱신 기회를 활용해 추가 예산 없이 공급업체에 양자내성암호 준비 의무를 부여함

❹ 양자내성암호 지원 여부 확인 3단계 절차

각 기관은 모든 주요 공급업체에 대해 다음 3단계 절차를 통해 체계적으로 양자내성암호 대응 현황을 파악하고 조달 체계에 반영한다.

Step 1. 기존·도입 예정 솔루션 공급업체에게 양자내성암호 지원 여부 확인

먼저 현재 운영 중이거나 도입을 검토 중인 모든 주요 솔루션·장비의 공급업체에게 양자내성암호 지원 여부를 질의한다. 이 단계는 단순한 정보 수집이지만, 이후 모든 대응 전략의 기초가 된다. 확인해야 할 핵심 사항은 다음과 같다.

- 현재 양자내성암호 알고리즘 지원 여부
- CC인증·보안기능 확인서 획득 여부 또는 획득 계획 등 국가정보원의 보안적합성 검증(KCMVP 포함) 관련 기준 충족 여부
- 하드웨어 교체 없이 펌웨어·소프트웨어 업그레이드로 양자내성암호 지원이 가능한지 여부
- 제품 지원 종료 예정 여부

질의 방법은 공문 또는 이메일로 하되, 본 절 말미에 첨부된 공급업체 질의서 양식을 활용하면 체계적인 정보 수집이 가능하다.

※ 공급업체가 질의에 응하지 않거나 답변을 지연하는 경우, 해당 내용을 문서화하여 향후 계약 갱신 또는 제품 교체 결정의 근거로 활용한다.

Step 2. 미지원 시 지원 로드맵 제출 요구

Step 1에서 현재 양자내성암호를 지원하지 않는 공급업체에 대해서는, 단순히 '미지원'으로 처리하고 끝내는 것이 아니라 지원 계획과 일정을 구체적으로 제출하도록 요구해야 한다. 요구할 내용은 다음과 같다.

- 양자내성암호 지원 예정 알고리즘과 적용 예정 버전 및 일정
- 지원 방식 : 신규 하드웨어 교체 필요 여부, 펌웨어·소프트웨어 업그레이드

방식 여부

- CC인증 · 보안기능 확인서 획득 등 국가정보원 보안적합성 검증 관련 기준 충족 계획 및 예상 일정
- 하이브리드 방식 지원 계획(기존 알고리즘과 병행 운용 가능 여부)
- 지원 계획이 없는 경우, 제품 지원 종료 일정 및 후속 제품 안내

공급업체가 명확한 로드맵을 제시하지 못하는 경우, 이는 해당 제품을 계속 사용할 경우 향후 전환이 불가능해질 수 있다는 신호이다. 이 경우 대체 제품 탐색을 병행하여 시작한다.

Step 3. 사업 요구사항(RFP) 반영

Step 1과 Step 2의 조사 결과를 바탕으로, 신규 사업 발주나 계약 갱신 시 RFP와 계약 조건에 양자내성암호 관련 요구사항을 반영한다. 이 단계가 조달 · 공급업체 대응의 가장 실질적인 결과물이다.

RFP 반영 시 중요한 원칙이 있다. KCMVP 검증대상에 양자내성암호가 포함되기 전이나 정책이 완전히 확정되기 전이라도 반영 가능한 요건과 적용을 의무화 요구할 사항을 구분하여 작성해야 한다. 현재 적용 가능한 요건(암호 민첩성, 지원 계획 제출 등)은 즉시 반영하고, 특정 알고리즘의 적용은 국내 및 국제 표준, 국가 정책, KCMVP 검증기준 등을 고려하여 적용하는 것이 바람직하다.

❺ 사업 요구사항(RFP) 반영 핵심 포인트

다음 표는 신규 정보화사업 또는 계약 갱신 시 RFP에 반영할 수 있는 핵심 요구사항을 제시한다. KCMVP 검증대상 양자내성암호가 확정되기 전이라도 적용 가능한 요건 중심으로 구성하였으며, 강제 이행보다는 계획 제출과 구조 확보에 초점을 맞춘다.

[표 27] RFP 반영 핵심 포인트

요구사항 항목	구체적 요건 예시	적용 가능 시점
암호 민첩성	• 암호 알고리즘의 교체 또는 추가 적용 시 애플리케이션의 광범위한 수정 없이 대응할 수 있는 구조를 구현할 것 • 복수의 공개 키 암호를 동시에 지원하는 구조로 설계할 것 • 알고리즘 및 파라미터 설정을 중앙에서 관리할 수 있는 구조(설정 파일 · 관리 콘솔 등)를 갖출 것	신규 개발 · 구축 사업 / 클라우드 네이티브 전환 사업 구상 단계
양자내성 암호 하이브리드 방식 지원 계획	• 제안사는 자사 제품 · 솔루션의 양자내성암호 하이브리드–AND 방식 지원 계획(지원 예정 알고리즘, 예상 시점, 적용 방식)을 제안서에 포함할 것 • CC인증 · 보안기능 확인서 등 국가정보원 보안적합성 검증 기준 일정(KCMVP 포함)에 따른 적용 계획을 제시할 것 • 국내 · 국제 표준 완료 혹은 표준화 진행 중인 양자내성암호를 우선 고려하여 지원할 것 • 향후 KCMVP 검증대상 양자내성암호 알고리즘이 확정되는 경우 해당 알고리즘을 적용한 하이브리드–AND 방식으로 전환할 수 있는 구조를 지원할 것	신규 도입 · 갱신 계약 및 전환 초기 단계 적용 시스템
인증서 · 키 관리 호환성	• 기존 X.509 인증서 체계와의 하위 호환성을 유지하면서 양자내성암호 인증서를 병행 지원할 수 있을 것 • 키 생성 · 저장 · 관리 기능이 양자내성암호 적용에 유연하게 대응할 수 있는 구조일 것 • HSM 사용 제품의 경우 양자내성암호 지원 HSM 적용 또는 전환 로드맵 제공할 것	전자서명 인증체계 관련 시스템 신규 도입 시
업데이트 · 패치 정책	• 암호 관련 취약점 패치를 계약 기간 내 무상으로 제공할 것 • 양자내성암호 관련 국내 · 국제 표준의 제 · 개정, KCMVP 검증대상 양자내성암호 알고리즘의 확정 또는 관련 정책 변경 시 업데이트 · 패치 등 대응 계획을 제공할 것 • 펌웨어 · 소프트웨어 업데이트를 통해 양자내성암호를 적용할 수 있는 구조를 제공할 것	유지관리 · 운영 계약 갱신 시

요구사항 항목	구체적 요건 예시	적용 가능 시점
시험 · 검증 계획	• 납품 시 양자내성암호 지원 여부에 대한 시험 결과서를 제출할 것 • 성능 영향(키 크기 증가, 처리 속도 변화) 측정 결과를 제시할 것 • 기존 시스템과의 상호운용성 시험 계획 및 결과를 포함할 것	신규 구축 · 조달 검수 단계

다음은 위 각 항목별로 실제 RFP 또는 과업지시서에 그대로 삽입할 수 있는 문구 예시다. 기관은 사업 유형과 대상 시스템에 맞게 항목을 선택 · 조합하여 활용하고, 기관별 계약 조건 및 법무 검토를 거쳐 최종 문구를 확정한다.

① 암호 민첩성 - RFP 예시 문구

예시 문구 : 암호 민첩성(신규 개발·구축 사업 과업지시서)

제안사는 납품하는 소프트웨어 · 시스템을 암호 알고리즘을 교체하거나 추가 적용할 때 소스 코드의 광범위한 재작성 없이 설정 파일 또는 관리 인터페이스 변경만으로 대응 가능한 구조(암호 민첩성, Crypto Agility)로 설계 · 구현하여야 한다. 구체적으로 다음 요건을 충족하여야 한다.

가. 공개 키 암호(키 교환, 전자서명)의 종류 및 파라미터를 운영자가 설정 파일 또는 관리 콘솔에서 변경할 수 있는 구조로 구현할 것

나. RSA, ECDSA 등 기존 공개 키 암호와 양자내성암호를 동시에 지원하는 하이브리드 구조를 구현하거나, 향후 하이브리드 방식 적용을 위해 시스템 재설계가 필요하지 않도록 구조를 설계할 것

다. 암호 관련 모듈(라이브러리, API)은 시스템 핵심 기능으로부터 독립적으로 교체 가능하도록 계층화하여 구현할 것

라. (클라우드 네이티브 전환 사업의 경우) 암호기능을 특정 서비스에 종속되지 않도록 설계하고 향후 알고리즘 변경 시 개별 서비스의 대규모 수정 없이 적용할 수 있는 구조를 구현할 것. API 게이트웨이, 서비스 메시 등 공통 계층을 활용하는 경우에는 암호 관련 설정을 일관되게 관리할 수 있도록 설계할 것.

마. 납품 시 사용 중인 암호 라이브러리 명칭 · 버전 · 알고리즘 목록을 포함한 CBOM을 제출할 것

② 양자내성암호 하이브리드 방식 지원 계획 - RFP 예시 문구

예시 문구 : 양자내성암호 하이브리드-AND 방식 지원 요구사항(신규 도입·유지관리 계약 및 전환 초기 단계 적용 시스템 과업지시서)

제안사는 자사 제품·솔루션에 기존 공개 키 암호와 양자내성암호를 결합한 하이브리드-AND 방식을 적용하기 위한 지원 계획을 제안서 내 별도 항목으로 작성하여 제출하여야 하며, 다음의 요구사항을 충족하여야 한다.

가. 양자내성암호는 하이브리드-AND 방식으로 지원할 것

나. 하이브리드-AND 방식 적용 계획을 제시할 것. 이때 하이브리드-AND 방식에 적용할 기존 공개 키 암호 및 양자내성암호 알고리즘 목록, 현재 지원 여부 및 지원 예상 시점(연·월 단위)을 포함하여 제시할 것

※ 지원 계획을 '미정'으로만 기재하는 경우 제안 평가 시 감점 처리할 수 있음

다. 하이브리드-AND 방식 지원을 위한 업그레이드 방식(펌웨어 업데이트, 소프트웨어 패치, 하드웨어 교체 등), 지원 기간 및 미이행 시 조치 등 세부 조건은 사업 특성과 제품의 지원 정책 등을 고려하여 계약서에 명시할 것

라. TLS 통신 구간의 경우, 기존 키 교환 알고리즘(예 : ECDH)과 양자내성암호를 결합한 하이브리드-AND 키 교환을 지원하거나, 향후 이를 지원하는 버전으로의 업그레이드 제공 일정을 제시할 것

마. 국내·국제 표준이나 KCMVP 검증대상으로 양자내성암호 알고리즘이 확정되는 경우, 공식 확정 시점으로부터 최대 1년 이내에 해당 알고리즘을 적용한 하이브리드-AND 방식 지원 버전을 제공할 것

※ '최대 1년'은 예시이며 사업 특성 등을 고려하여 조정할 수 있음

바. 하이브리드-AND 방식 적용에 따른 KCMVP, CC인증·보안기능 확인서 등 보안적합성 검증 기준 충족 지원 계획 및 예상 일정을 제시할 것

사. 하이브리드-AND 방식 운용 중 기존 공개 키 암호 방식으로의 폴백(fallback) 가능 여부와 허용 조건, 동작 및 통제 절차를 기술 문서 또는 운영 매뉴얼에 명시하여 제출할 것

※ CC인증 또는 보안기능 확인서를 취득한 제품에 하이브리드-AND 방식의 양자내성암호 적용을 요구하는 경우에는 기존 인증·확인 범위에 미치는 영향을 확인하고, 필요한 인증·확인 절차 및 적용 계획을 계약 조건에 반영한다.

③ 인증서·키 관리 호환성 - RFP 예시 문구

예시 문구 : 인증서·키 관리 호환성(인증 관련 시스템 과업지시서)

제안사는 납품하는 시스템이 다음 인증서·키 관리 호환성 요건을 충족하도록 설계·구현하여야 한다.

가. 기존 RSA·ECDSA 기반 X.509 인증서와 향후 양자내성암호 기반 인증서를 동시에 처리(발급·검증·저장)할 수 있는 구조로 구현할 것. 현 시점에서 불가능한 경우 가능 시점 및 전환 계획을 제안서에 명시할 것

나. (HSM을 사용하는 경우) 해당 HSM이 양자내성암호를 지원하거나 펌웨어 업그레이드를 통해 지원 가능한 제품임을 제안서에 명시하고 제조사 공식 확인서를 제출할 것

다. 인증서 갱신·폐기·OCSP·CRL 처리 절차가 양자내성암호 기반 인증서에도 동일하게 적용 가능한 구조로 키 관리 체계를 설계할 것

라. (전자서명 인증체계와 연계되는 시스템의 경우) 해당 공통 인프라의 양자내성암호 전환 정책 및 일정에 따라 연계 방식 변경이 가능하도록 구조를 설계할 것

마. 키 생성·저장·백업·폐기 절차가 특정 공개 키 암호에 종속되지 않고, 향후 양자내성암호 적용 시에도 활용 가능한 구조로 설계할 것

④ 업데이트·패치 정책 - RFP 예시 문구

예시 문구 : 업데이트·패치 정책(유지관리·운영 계약 과업지시서)

수급인은 계약 기간 중 다음 사항을 이행하여야 한다.

가. 납품 제품·소프트웨어에서 암호 알고리즘 관련 보안 취약점이 발견된 경우, 발주기관의 별도 요청 없이도 발견일로부터 30일 이내에 무상 패치를 제공하여야 한다.

나. 국가정보원 또는 관계부처가 특정 암호 알고리즘의 사용 중단 또는 교체를 공식 권고하는 경우, 권고 후 60일 이내에 대응 방안 및 업그레이드 계획을 발주기관에 서면으로 제출하여야 한다.

다. 양자내성암호 전환 관련 국가 정책이 변경되는 경우, 변경 사항을 반영한 제품 업그레이드 계획을 3개월 이내에 발주기관에 서면으로 제출하여야 한다.

라. 계약 만료 6개월 전까지 제품의 제조사 지원 종료 예정 여부를 발주기관에 서면으로 고지하여야 한다. 지원 종료 예정 제품이 운영 중인 경우 발주기관과 협의하여 교체 계획 또는 위험 완화 방안을 마련하여야 한다.

⑤ 시험·검증 계획 - RFP 예시 문구

예시 문구 : 시험·검증 계획(신규 구축사업 검수 조건)

수급인은 납품 시 다음 시험·검증 결과를 발주기관에 제출하여야 하며, 발주기관은 이를 검수 기준으로 활용한다.

가. 암호 구성 현황서(CBOM) : 납품 시스템에 사용된 암호 라이브러리 명칭·버전·알고리즘 목록을 정리하여 제출할 것

나. 암호 민첩성 시험 결과서 : 알고리즘 설정 변경 절차 및 변경 후 정상 동작 여부를 확인한 시험 결과를 제출할 것

다. 성능 영향 측정 결과서 : 기존 공개 키 암호 대비 하이브리드 방식 적용 시 키 생성·교환 처리 시간, TLS 핸드셰이크 소요 시간, 패킷 크기 변화를 측정한 비교 결과를 제출할 것. 현 시점에서 양자내성암호 미지원 제품의 경우 지원 예정 버전에 대한 시험 계획서로 대체할 수 있음

라. 상호운용성 시험 결과서 : 발주기관의 주요 연계 시스템(방화벽, VPN 장비, 연계 API 등)과의 하이브리드 방식 운용 시 상호운용성 시험 결과를 납품 후 30일 이내에 제출할 것

⚠ RFP 작성 시 주의사항

위 예시 문구는 사업 성격(신규 구축, 유지관리, 장비 조달 등)에 따라 선택적으로 활용한다.

특정 알고리즘명(예 : NTRU+, SMAUG-T, ML-KEM 등)을 RFP에 명시하여 의무 적용을 강제하는 것은 현재 시점에서 신중할 필요가 있다. 국내 암호모듈 검증제도(KCMVP)에서 해당 알고리즘이 검증되지 않은 상태이기 때문에 특정 알고리즘 적용을 강제하면 향후 적합한 제품이 없어 사업 자체가 무산될 수 있다. 대신 국가정보원 보안 정책 및 KCMVP 검증 기준에 따라 채택 혹은 국내·국제 표준 양자내성암호를 지원한다는 유연한 구조를 요구하는 것이 적절하다.

또한 CC인증 또는 보안기능 확인서를 취득한 제품의 경우 암호 기능 변경이 기존 인증·확인서의 인정 범위 또는 유효성에 영향을 줄 수 있다. 따라서 RFP에 양자내성암호 적용을 요구하는 경우에는 인증 유지 방안, 재평가 필요 여부 및 관련 절차를 함께 검토해야 한다. 특히 현행 제도에서는 암호기능 변경이 인증 형상 변경으로 간주될 수 있으므로, 최신 CC 인증·보안기능확인 제도 및 관련 지침을 확인하고 필요 시 관계 기관과 사전 협의한 후 요구사항을 확정하는 것이 바람직하다.

❻ 주요 산출물

이 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다.

산출물	내용
공급업체 대응 현황표	각 공급업체별 양자내성암호 지원 여부, 지원 예정 시점, 하이브리드 지원 여부, KCMVP 검증 계획, 계약 갱신 시점 등을 정리한 문서. 4장 3절 우선순위 평가 및 4장 5절 예산 계획과 연계
양자내성암호 요구사항 정의서	향후 사업 발주 및 계약 갱신 시 적용할 RFP 요건 목록. 암호 민첩성, 지원 계획 제출, 업데이트 정책, 시험·검증 계획을 포함한 표준 요건 문서
교체 필요 장비·소프트웨어 목록	양자내성암호 업그레이드가 불가능하거나 EOL/EOS가 임박한 제품 목록과 교체 우선순위. 예산 계획 수립(4장 5절)의 기초 자료
공급업체 질의서 회신 파일	각 공급업체로부터 수령한 질의서 회신 원문. 이후 계약 협상과 제품 선택의 근거 문서로 보관

❼ 조달·공급업체 대응 체크리스트

다음 체크리스트를 활용하여 조달 및 공급업체 대응 단계의 핵심 사항이 이행되었는지 확인한다.

확인	4.4 조달 및 공급업체 대응 : 실무 확인표
□	주요 공급업체 유형(보안장비 · 클라우드 · 유지보수 · 외주개발 · 전자서명 인증체계 · 공동 시스템)을 파악하였다.
□	각 주요 공급업체에 양자내성암호 지원 여부 질의를 완료하였다. ※ 하단 '[첨부] 양자내성암호 지원 여부 확인 공급업체 질의서' 활용
□	공급업체별 양자내성암호 지원 여부, 지원 예정 시점, 업그레이드 가능 여부를 문서화하였다.
□	양자내성암호 미지원 공급업체에 대해 지원 로드맵 제출 요구 또는 대체 제품 탐색을 착수하였다. ※ 예시 : 펌웨어 · 소프트웨어 업그레이드 지원 여부, 하드웨어 교체 필요성, 보안적합성 검증 신청 계획 및 예상 일정 등 구체적인 로드맵 제출 요구
□	지원 종료 예정 제품을 파악하고 교체 계획에 반영하였다. ※ 하단 '[참고] 제조사 지원 종료 예정 장비 점검표' 활용
□	1~2년 내 계약 갱신 도래 시스템의 계약 조건에 양자내성암호 지원 요건 반영을 검토하였다.
□	신규 정보화사업 RFP에 암호 민첩성, 양자내성암호 지원 계획 제출 요건을 포함하였다(또는 포함 계획을 수립하였다). ※ 암호 민첩성 : 특정 암호 알고리즘이나 구현에 종속되지 않고, 향후 암호 알고리즘이나 관련 기준이 변경될 때 보안과 운영 연속성을 유지하면서 신속하고 유연하게 대응할 수 있는 역량
□	클라우드 서비스별 양자내성암호 전환 로드맵을 확인하였다(이용 중인 IaaS · PaaS · SaaS 서비스의 제공자를 대상으로). 예 : 하단의 '[참고] 클라우드 서비스 별도 점검표' 활용
□	다기관 공동 활용 시스템에 대한 운영주체 기관 협의를 시작하였다.
□	교체 필요 장비 · 소프트웨어 목록을 작성하였고, 예산 계획(4.5절)과 연계될 예정이다.
□	공급업체 대응 현황표를 작성하였다. ※ 예시 : 공급업체별 지원 여부, 지원 예정 시점, 하이브리드 지원 여부, KCMVP 검증 계획, 계약 갱신 시점 등을 정리

[참고] 클라우드 서비스 별도 점검표(서비스 이용 및 직접 구축 포함)

클라우드 서비스 환경은 이용 형태(IaaS · PaaS · SaaS)와 구축 방식(서비스 이용 또는 직접 구축)에 따라 기관이 암호 설정을 직접 제어할 수 있는 범위가 다르다. 이용 중인 클라우드 서비스 제공자의 대응 계획이 실질적 전환 가능 시점을 결정하는 경우가 많으므로, 기존 체크리스트와 별도로 아래 항목을 추가 확인한다.

확인	4.4 클라우드 서비스 점검 항목
□	이용 중인 클라우드 서비스(SaaS · IaaS · PaaS) 제공자의 양자내성암호 지원 계획 및 예상 시점을 확인하였다.
□	클라우드 서비스에서 기관과 서비스 제공자의 암호 설정 · 관리 책임 범위를 구분하였다. ※ 일반적으로, IaaS는 서비스 제공자가 기반 인프라를 관리하고 기관이 OS · 애플리케이션 · VPN 등 상위 계층의 암호 설정을 관리, PaaS는 서비스 제공자가 플랫폼 계층을 관리하고 기관이 애플리케이션 계층을 관리, SaaS는 암호 관련 설정 대부분을 서비스 제공자가 관리, 기관 직접 구축 시스템은 암호 설정 및 운영 전반을 기관이 관리
□	계약 갱신 시 양자내성암호 지원 일정을 서비스 수준 협약(SLA)에 반영하는 방안을 검토하였다.
□	공공 클라우드 보안검증 체계 일원화(2027년 7월부터 국가정보원 단일 검증체계 시행 예정)를 고려하여, 이용 중인 클라우드 서비스 제공자의 양자내성암호 지원 계획과 전환 로드맵을 확인하였다.
□	클라우드 서비스 제공자가 관리하는 인프라 계층 외에 기관이 통제하는 레이어(앱 레벨 암호화, VPN 설정 등)의 우선 전환 가능성을 검토하였다.

[참고] 제조사 지원 종료 예정 장비 점검표

제조사 지원이 종료된 장비는 양자내성암호 업그레이드가 불가능한 경우가 많다. 지금 교체 결정이 이루어지지 않으면 수년간 취약한 암호 환경을 유지해야 할 수 있으므로, 아래 항목을 별도로 확인한다.

확인	4.4 EOL · EOS 예정 장비 점검 항목
□	제조사 지원 종료 예정 장비 · 소프트웨어 목록을 파악하였다(예정 연도 포함).
□	제조사 지원 종료 예정 장비의 양자내성암호 지원 가능 여부를 확인하였다.
□	지원 종료 전 교체가 필요한 장비를 4장 5절 예산 계획에 반영할 예정이다.
□	교체 전까지의 보완 통제 방안(망 분리 강화, 접근 제한 등)을 마련하였다.

[첨부] 양자내성암호 지원 여부 확인 공급업체 질의서

다음 질의서를 공급업체에게 공문 또는 이메일로 발송하여 양자내성암호 대응 현황을 체계적으로 파악한다. 기관은 해당 제품 · 솔루션에 적합한 항목을 선택하여 활용할 수 있다.

〈 ○○기관 양자내성암호 지원 여부 확인 질의서 〉

발송 기관 : _____ / 발송일 : 20XX년 X월 X일 / 수신 공급업체 : _____

대상 제품 · 솔루션 : _____ / 계약 번호(해당 시) : _____

회신 요청 기한 : 발송일로부터 2주 이내 / 회신처 : _____

본 질의서는 당 기관의 양자내성암호 전환 계획 수립을 위한 기초 자료 수집 목적으로 발송됩니다. 성실한 회신을 부탁드립니다.

작성 안내

- '예/아니오/미정' 열에 해당 내용을 기재하고, '비고' 열에 구체적인 설명(예정 시점, 지원 방식, 제약 조건 등)을 기재해 주십시오.
- 해당 사항이 없는 항목은 '해당 없음'으로 기재해 주십시오.
- 질의 내용 중 확인이 어려운 항목은 미정으로 표시하고 추후 확인 가능 시점을 비고란에 기재해 주십시오.

No.	질의 항목	답변(예/아니오/미정)	비고(설명)
	A. 제품 · 솔루션의 양자내성암호 지원 현황		
1	현재 제품 · 솔루션에 양자내성암호(양자내성암호) 알고리즘이 지원됩니까?		
2	지원되는 경우, 어떤 알고리즘이 지원됩니까?(비고란에 구체적인 알고리즘 작성)		
3	국가정보원 보안적합성 검증(KCMVP 포함)을 획득한 양자내성암호 기반 제품이 있습니까? 또는 적용 계획이 있습니까?		
	B. 지원 계획 및 로드맵		
4	현재 양자내성암호 지원 계획(로드맵)이 있습니까?		
5	현재 미지원인 경우, 양자내성암호 지원 예정 시점이 있습니까? (비고란에 예상 연도 기재)		
6	펌웨어 · 소프트웨어 업그레이드를 통해 양자내성암호 지원이 가능합니까?(하드웨어 교체 없이 가능 여부)		
7	기존 공개 키 암호와 양자내성암호를 병행하는 하이브리드 방식을 지원하거나 지원할 계획이 있습니까?		
8	KCMVP 검증대상 양자내성암호 채택 후 제품에 반영할 계획을 가지고 있습니까?		
	C. 암호 민첩성 및 업데이트 정책		
9	암호 알고리즘의 교체 또는 추가 적용 시 애플리케이션의 광범위한 수정 없이 대응할 수 있는 구조로 구현되어 있습니까?		
10	암호 관련 취약점이 발견되는 경우 패치를 계약 기간 내 무상으로 제공합니까?		
11	양자내성암호가 국내 · 국제 표준 등재 혹은 KCMVP 검증대상으로 확정되거나 정책 변경 시 대응 절차가 마련되어 있습니까?		
12	제품 지원 종료 예정일이 있습니까?		
	D. 인증서 · 키 관리 및 호환성		
13	기존 X.509 인증서 체계와 하이브리드 양자내성암호 인증서를 병행 지원할 수 있습니까?		

No.	질의 항목	답변(예/아니오/미정)	비고(설명)
14	HSM을 사용하는 경우, 해당 HSM이 양자내성암호를 지원합니까?		
15	기관 간 연계 구간(행정정보공동이용 등)에서의 양자내성암호 전환 시 상호운용성 시험 지원이 가능합니까?		
16	TLS 1.3 이상에서의 양자내성암호 키 교환 지원 계획이 있습니까?		
	E. 시험·검증 및 기술 지원		
17	양자내성암호 적용 시 성능 영향(처리 속도, 네트워크 부하)에 대한 측정 데이터를 제공할 수 있습니까?		
18	기관의 시험 환경(테스트베드)에서 양자내성암호 적용 검증을 위한 기술 지원이 가능합니까?		
19	양자내성암호 전환 과정에서 발생하는 기술적 문의에 대한 전담 지원 창구가 있습니까?		

제5절 예산 계획 수립

양자내성암호 전환은 단년도에 완료되는 사업이 아니라 2035년을 목표로 단계적으로 추진해야 하는 중장기 과제이다. 또한 국가정보원 정책, 암호모듈 검증제도 및 제품 지원 현황이 지속적으로 변화하고 있으므로, 대규모 일괄 교체보다는 기관의 정보화 계획 및 시스템 운영 계획과 연계한 단계적 전환이 현실적이다. 이러한 전환 과정에서는 다양한 비용이 발생한다. 여기서 '비용'은 금전적 지출뿐 아니라 전환 과정에 소요되는 인력과 시간까지 포함하는 개념이다.

기관별 예산 여건에 따라 초기 단계에서는 전환 비용 확보가 제한적인 경우도 있다. 그러나 양자내성암호 **전환 준비**가 반드시 대규모 예산 투입을 전제로 하는 것은 아니므로, 공급업체 현황 조사, 전환 로드맵 수립 등은 기존 정보화사업, 유지관리사업 및 장비 교체사업과 연계하여 추진할 수 있다. 반면 장비 교체, 소프트웨어 수정, 인증서 재발급 등 **실제 전환** 단계에서는 별도의 예산이 필요할 수 있으므로 이에 대한 중장기 계획을 수립할 필요가 있다.

계획 수립 시 주의해야 할 점은, 인증체계, VPN, 기관 간 연계 구간과 같이 개별 기관 단독으로 전환하기 어려운 영역은 범정부 공통 인프라의 전환 일정과 연계하여 추진할 필요가 있다는 것이다. 이러한 영역에 대한 독자적·선제적 투자는 향후 중복 투자로 이어질 수 있으므로 신중하게 검토해야 한다.

본 절에서는 전환 비용이 발생하는 주요 요인, 예산 항목, 기존 사업과의 연계 방안, 예산 규모별 추진 전략 및 예시 예산 계획서를 제시한다.

❶ 전환 비용이 발생하는 이유

양자내성암호 전환은 단순히 알고리즘 설정값을 바꾸는 작업이 아니다. 기관 내 암호가 사용되는 모든 지점(프로토콜, 라이브러리, 인증서, 장비, 응용시스템 등)에 걸쳐 변화가 필요하므로, 다음과 같은 이유로 비용이 발생한다.

- 현황 파악 비용 : 암호자산 인벤토리는 기존 IT 자산 목록에서 자동으로 만들어지지 않는다. 담당자 인터뷰, 설정 점검, 자동화 도구 활용 등에 인력과 비용이 소요된다.
- 하드웨어 교체 비용 : 일부 보안장비와 HSM은 펌웨어 업그레이드만으로 양자내성암호 지원이 불가능하여 신규 장비 구매가 필요하다. 이는 전환 비용 중 가장 큰 비중을 차지할 수 있다.
- 소프트웨어 수정·업그레이드 비용 : 외주 개발 소프트웨어의 암호 라이브러리 교체나 소스코드 수정은 별도 용역 발주가 필요하다. 암호가 하드코딩된 경우 수정 범위가 광범위하여 비용이 증가할 수 있다.
- 인증서 재발급 비용 : 전자서명 인증체계의 알고리즘 전환 시 기존 인증서를 폐기하고 새 알고리즘 기반으로 재발급해야 한다. 인증서 수가 많은 기관일수록 관리 비용이 증가한다.
- 시험·검증 비용 : 전환 후 성능 영향, 상호운용성, 운영 안정성 검증에 시험 환경 구축과 전문 인력이 필요하다.
- 교육·운영 비용 : 담당자 역량 강화 교육, 운영 절차 수립, 내부 지침 개정 등 지속적인 관리 비용이 발생한다.

- 하이브리드 운영 비용 : 전환 과도기에 둘 이상의 암호 알고리즘을 병행 운영하면 시스템 복잡도가 증가하여 운영 비용이 일시적으로 상승할 수 있다.

⚠ 비용 과대 추정의 위험

전환 비용을 실제보다 크게 추정하여 예산 확보가 어렵다는 이유로 준비 자체를 미루는 경우가 있다. 그러나 전체 비용의 상당 부분은 기존 정보화사업과 연계하면 추가 비용 없이 흡수할 수 있다. 특히 차세대 사업에서 설계 단계부터 암호 민첩성을 고려한 설계를 반영한다면 추후 재전환의 비용을 크게 줄일 수 있다. 현재 초기 비용이 크게 보이더라도, 지금 준비하지 않아 향후 긴급하게 전환해야 할 때 발생하는 비용은 훨씬 클 수 있다.

❷ 주요 예산 항목 및 비용 관리 고려사항

양자내성암호 전환 예산은 크게 전환 준비 단계와 전환 적용 단계로 구분할 수 있다. 전환 준비 단계에서는 암호자산 인벤토리 구축 및 현행화, 우선순위 평가 및 공급업체 현황 조사를 수행하며, 이를 통해 전환 적용 단계의 예산 규모를 보다 정확하게 산정할 수 있다.

전환 준비 단계와 전환 적용 단계를 포함한 양자내성암호 전환 예산은 다음의 다섯 가지 항목으로 구분할 수 있다.

[표 28] 전환을 위한 주요 예산 항목

예산 항목	주요 세부 내용	발생 시점
① 암호자산 인벤토리 구축 및 현행화	• 암호자산 현황 파악을 위한 컨설팅 용역 • 자동화 스캐닝 도구 도입 또는 임시 이용 • 담당자 인터뷰·설정 점검에 투입되는 내부 인력 시간	초기 착수 후 정기적 갱신
② 시험 및 검증	• 시험 환경 구축 • 성능 영향 측정(처리 속도, 네트워크 부하) • 상호운용성 시험(기관 간 연계 구간 포함) • 외부 전문가 기술 검토 및 컨설팅	시범 적용 단계

예산 항목	주요 세부 내용	발생 시점
③ 시스템 적용	• 소프트웨어 · 펌웨어 업그레이드(라이선스 비용 포함) • 신규 장비 도입(HSM, 보안장비, 네트워크 장비 등) • 인증서 재발급 및 키 교체 • 외주 개발사 소스코드 수정 비용 • 클라우드 서비스 변경 또는 다른 서비스로 전환 비용 • 하이브리드 방식 운영을 위한 시스템 개선	단계별 전환 적용. 전체 비용의 가장 큰 비중
④ 운영 및 교육	• 담당자 양자내성암호 기술 교육 • 운영 절차 수립 및 내부 지침 개정 • 전환 후 모니터링 체계 구축 및 운영 • 인증서 · 키 관리 정책 갱신 • 전환 완료 후 지속 관리 비용	전환 전반 및 전환 완료 후 지속 발생
⑤ 행정 · 관리	• 전환 추진 협의체 운영 비용 • 공급업체 질의 · 계약 검토 행정 비용 • 기관 내 전환 계획서 · 보고서 작성 및 승인 절차 • 외부 자문 비용(필요시)	전환 전반 간접 비용

각 항목에 대해 다음과 같은 세부 고려사항을 반영하여 예산을 추정한다.

① 암호자산 인벤토리 구축 및 현행화 예산

암호자산 인벤토리 조사는 전환의 첫 단계이므로 비교적 이른 시점에 수행해야 한다. 기관 규모와 시스템 복잡도에 따라 비용 차이가 크므로, 우선순위 결정에 필요한 핵심 영역부터 단계적으로 조사하는 것이 바람직하다.

- 단계적 조사 수행 : 초기에는 인터넷 연결 서비스, VPN, 인증서 기반 시스템 등 핵심 영역을 중심으로 조사하고 이후 범위를 확대
- 기존 자료 활용 : 정보자산 목록, 보안성 검토 자료, 시스템 구축 문서, 운영 매뉴얼 등을 활용하여 조사 범위를 축소
- 내부 인력 우선 활용 : 초기 현황 파악은 담당자 인터뷰와 설정 점검을 중심으로 수행하고 필요 시 외부 전문기관 지원 검토

- 자동화 도구 활용 : 인증서, TLS 구성 등 일부 항목은 자동화 도구를 활용하여 조사 효율성을 향상
- 정기 현행화 예산 확보 : 최초 구축 이후에도 신규 시스템 도입, 소프트웨어 업그레이드, 외부 연계 구간 변경 등이 발생할 때마다 암호자산 인벤토리 갱신이 필요. 이를 위한 인력 투입 비용(내부 담당자 시간 또는 외부 컨설팅)을 연간 운영 예산에 반영해야 하며, 최소 연 1회 정기 검토를 계획에 포함

② 시험 및 검증 예산

시험·검증 비용은 기관 내 기존 시험 환경을 최대한 재활용하고, 시범 적용 범위를 단계적으로 확대함으로써 초기 비용 부담을 조정할 수 있다. 시험 항목은 4장 6절(적용 및 검증)의 검증 항목 목록을 참고하여 범위를 설정한다.

- 기존 시험 환경 재활용 : 기관 내 보유한 개발·스테이징 환경을 활용하여 양자내성암호 시범 적용 시험을 수행하면 전용 테스트베드 신규 구축 비용을 줄일 수 있음
- 시범 적용 범위 단계적 확대 : 처음에는 위험도가 낮은 시스템에 시범 적용하여 운영 안정성을 확인하고, 경험 축적 후 고위험 시스템으로 범위를 넓힘
- 기존 성능 시험 체계 활용 : 기존 성능 테스트 도구를 활용하여 양자내성암호 적용 후 성능 변화 측정 가능

③ 시스템 적용 예산(가장 큰 비중)

시스템 적용 예산은 전체 전환 비용에서 가장 큰 비중을 차지한다. 이 비용을 현실적으로 관리하는 핵심 전략은 **기존 사업과 연계하여 추가 비용을 최소화**하는 것이다.

- 우선순위 기반 분산 투입 : 4장 3절의 1~2 우선순위 시스템부터 순차 적용하여 연도별 예산 부담 분산
- 장비 교체 시점 연계 : 노후 장비 교체 예산에 양자내성암호 지원 제품 선택

기준을 포함하면, 장비 교체 비용 내에서 양자내성암호 전환을 함께 추진할 수 있음

- 소프트웨어 업그레이드 계약 조건 활용 : 유지관리 계약 갱신 시 양자내성암호 지원 라이브러리로의 업그레이드 제공을 조건으로 포함할 수 있으며, 이 경우 별도 용역 발주 없이 계약 범위 내에서 처리 가능. 단, 공급업체 협상 과정에서 계약 금액 조정이 발생할 수 있음
- HSM 교체 비용 별도 계획 : HSM은 하드웨어 교체가 필요할 수 있으므로 장비 예산으로 별도 책정

④ 운영 및 교육 예산

운영 · 교육 비용은 전환 기간 전반에 걸쳐 지속적으로 발생하는 비용이다. 특히 담당자 교육, 운영 절차 정비, 인증서 · 키 관리 체계 운영 및 전환 후 모니터링 활동에 필요한 인력과 시간을 고려하여 예산을 산정해야 한다.

- 교육 비용 산정 : 담당자 수, 교육 횟수, 외부 전문교육 활용 여부 등을 고려하여 교육 예산을 산정
- 인력 투입 반영 : 인증서 · 키 관리, 알고리즘 적용 상태 점검, 전환 현황 관리 등에 필요한 내부 인력 투입 시간을 운영 비용에 반영
- 정책 · 지침 정비 비용 반영 : 정보보호 정책, 인증서 관리 절차, 시스템 운영 지침 개정에 필요한 인력 투입을 고려
- 모니터링 운영 비용 반영 : 인증서 만료 관리, 키 교체 주기 관리, 적용 상태 점검 등을 위한 지속적인 운영 비용을 포함

❸ 기존 사업과의 연계 전략

국가 · 공공기관의 예산 구조상, 양자내성암호 전환을 위한 별도 대규모 예산을 단기간에 확보하기는 쉽지 않다. 가장 현실적인 접근은 **기존에 추진하거나 계획 중인 사업에 양자내성암호 요건을 자연스럽게 포함**하는 것이다.

[표 29] 전환 예산 편성 시 기존 사업 연계 방안 예시

사업 유형	양자내성암호 연계 방법	예산 절감 효과	주의사항
차세대·신규 정보화 사업	초기 설계 단계부터 암호 민첩성을 고려한 설계 반영, 양자내성암호 지원 제품 선택	별도 전환 사업 불필요. 설계 단계부터 암호 민첩성을 고려한 설계를 반영하면 이후 재전환 비용을 줄일 수 있음	사업 기획 1~2년 전부터 준비 필요
유지관리·운영 계약 갱신	계약 조건에 양자내성암호 지원 의무화, 업그레이드 제공 조항 포함	기존 계약 범위 내 처리 가능. 별도 예산 없이 의무 부여	공급업체 협상 필요. 불응 시 계약 해지·재공모 검토
노후 장비 교체사업	장비 교체 시 양자내성암호 지원 제품 선택	교체 비용에 양자내성암호 비용 포함. 중복 투자 방지	교체 일정과 양자내성암호 전환 일정 정합성 확인 필요
클라우드 전환사업	IaaS·PaaS 선택 시 양자내성암호 지원 로드맵 보유 클라우드 서비스 제공자 우선 선택. 기관이 직접 클라우드를 구축하는 경우 설계 단계부터 양자내성암호 적용 및 암호 민첩성을 고려한 설계 반영	클라우드 전환과 양자내성암호 준비를 동시 달성	서비스 제공자 선택이 장기 의존성 형성. 신중한 검토 필요
정보보호 강화사업	정보보호 예산 중 일부를 양자내성암호 전환 준비(암호자산 인벤토리·시험)에 배분	기존 정보보호 예산 활용. 신규 예산 없이 준비 가능	타 정보보호 사업과의 우선순위 조정 고려
장비·소프트웨어 조달사업	조달 규격서에 양자내성암호 지원 여부 및 국내·국제 표준 혹은 KCMVP 검증대상 알고리즘 적용 계획 보유 제품 우선 선택 기준 포함. 나라장터 RFP 작성 단계에서 보안 요구사항으로 명시	조달 시점에 국내·국제 표준 및 KCMVP 검증 요건 반영 가능. 공공조달 사업 예산 내에서 전환 준비를 자연스럽게 포함	국내·국제 표준 및 KCMVP 검증대상 알고리즘 확정 동향과 국가정보원 관련 정책 지속 모니터링 필요

⚠ 예산 편성 일정과 양자내성암호 반영 시점

국가·공공기관의 예산 편성은 일반적으로 전년도부터 준비가 시작되며, 예산 요구·심의 절차를 거쳐 연말에 확정된다. 또한 일정 규모 이상의 정보화사업은 관계 법령과 지침에 따라 사전협의, 총사업비관리 등 별도의 행정 절차가 필요할 수 있으므로 사업 착수 이전에 관련 요건을 확인해야 한다.

이 구조에서 양자내성암호 관련 예산을 해당 연도에 반영하려면 전년도 상반기까지 계획이 수립되어 있어야 한다. 특히 차세대 사업과 같은 대규모 정보화사업은 예산 확보, 사업 범위 정의, 요구사항 수립 등의 준비가 실제 구축 이전부터 진행되므로, 양자내성암호 요구사항도 사업 초기 단계에서부터 검토할 필요가 있다.

❹ 제한된 예산 상황에서의 단계적 접근

예산이 충분하지 않은 상황에서도 우선순위를 명확히 하고 단계적으로 접근하면 효과적인 전환 준비가 가능하다. 핵심은 '지금 당장 비용이 들지 않는 준비'와 '기존 사업에 포함 가능한 것'을 먼저 실행하는 것이다.

[표 30] 예산 상황에 따른 단계별 접근 방법

예산 상황	현실적 우선순위	단계별 배분 전략	활용 가능한 지원
별도 예산 확보 가능	암호자산 인벤토리 → 시험 → 고위험 시스템 순차 적용	• 1차 : 암호자산 인벤토리·계획 수립 비용 • 2차 : 시범 적용·시험 비용 • 3차 : 단계별 시스템 적용 비용	기관 내 기존 시험 환경 재활용 및 단계적 시범 적용으로 검증 비용 조정 가능
기존 정보화 예산 일부 전용(轉用)	기존 정보화사업에 양자내성암호 요건 추가 반영 우선	• 신규 사업에는 설계 비용 소폭 증가분만 반영 • 유지관리 계약 갱신에 요건 포함	사업 기획 단계부터 정보보안 담당자가 참여하여 양자내성암호 요건을 설계에 직접 반영. 요건 누락 시 사후 수정 비용이 더 크게 발생할 수 있음

예산 상황	현실적 우선순위	단계별 배분 전략	활용 가능한 지원
예산 확보 매우 어려움	지금 당장 비용이 들지 않는 준비부터 시작	• 암호자산 인벤토리 : 문서·인터뷰 기반 • 공급업체 질의 : 행정 비용만 발생 • 교육 : 공개된 국내외 표준문서·기술 자료 자체 학습	국가정보원·관계 부처 공식 가이드라인 및 지침 문서 활용, 민간 전문가·학회 네트워크를 통한 기술 자문 검토

예산이 제한된 상황에서 실천 가능한 전략을 단계별로 정리하면 다음과 같다.

가. 즉시 실행 가능 영역

- 4장 1절 거버넌스 수립 : 내부 협의체 구성, 담당자 지정
- 4장 2절 암호자산 인벤토리 초기 파악 : 기존 문서 및 정보보안 담당자 인터뷰 기반으로 수행
- 4장 4절 공급업체 질의 : 공문 발송
- 교육 : 국가정보원·과기정통부의 공식 문서, KpqC 알고리즘 관련 기술 자료, NIST PQC 표준 문서(FIPS 203·204·205 등), 국내외 학술·기술 세미나 자료 학습
- 신규 사업 기획 참여 : 내년 정보화사업 기획 단계에 정보보안 담당자 참여 요청

나. 단기 예산 확보(기존 예산 전용 또는 소규모 신규 편성)

- 암호자산 인벤토리 구축 및 현행화 심화 : 외부 컨설팅 일부 활용 또는 자동화 스캐닝 도구 도입 → 컨설팅 용역비·도구 도입비 발생
- 시범 적용 시험 : 기관 내 기존 개발·스테이징 환경을 활용하여 시험 범위를 단계적으로 확대
- 유지관리 계약 갱신 조건 반영 : 기존 계약 갱신 범위 내에서 양자내성암호 지원 의무 조항 포함 → 계약 협상 및 행정 비용 발생

다. 중기 예산 계획(기존 사업 연계)

- 차세대 · 신규 사업 반영 : 사업 예산에 암호 민첩성을 지원하는 구조의 설계 비용 반영 → 사업 규모 및 암호 사용 범위에 따라 비용 편차 큼
- 노후 장비 교체 : 교체 대상 장비 중 양자내성암호 지원 제품 선택 → 교체 비용에 포함
- 고위험 시스템 전환 : 별도 예산 편성 필요. 전환 1순위 시스템에 집중

〈예산 계획서 예시〉

다음은 중규모 공공기관이 제한된 예산 여건에서 양자내성암호 전환을 추진할 때 고려할 수 있는 주요 예산 항목과 기존 사업 연계 방안을 정리한 예시다. 별도 예산 확보 없이 착수할 수 있는 활동부터 단기 예산 확보 및 중기 예산 계획이 필요한 활동까지 구분하여 제시하였다. 구체적인 비용과 추진 시기는 기관의 전환 대상, 우선순위 및 사업 · 예산 여건에 따라 달라질 수 있다.

[예시] ○○공공기관 양자내성암호 전환 예산 계획(개요)

기관 규모 : 직원 약 800명, 정보시스템 약 15개 / 작성 기준 : 20XX년 X월

구분	주요 추진 항목	예산 반영 내용	기존 사업 연계 및 활용 방안
가. 즉시 실행 가능 영역	VPN · 대민 웹서비스 암호자산 초기 조사	정보보안 담당자 2명이 기존 시스템 구성도, TLS 인증서 및 VPN 설정 자료 확인	기존 정보보호 업무와 연계하여 별도 용역없이 착수
	전환 추진체계 및 공급업체 협의	정보보안 · 정보화 · 운영담당자 협의체 구성, VPN 및 웹서비스 공급업체에 양자내성암호 지원 일정 질의	기존 유지관리업체 정기 협의 활용

구분	주요 추진 항목	예산 반영 내용	기존 사업 연계 및 활용 방안
가. 즉시 실행 가능 영역	담당자 교육 및 신규 사업 검토	담당자 3명이 공개 기술자료 학습, 차년도 웹서비스 고도화 사업의 양자내성암호 대응 요구사항 검토	기존 정보보호 교육 및 정보화사업 기획에 반영
나. 단기 예산 확보	암호자산 상세 조사	15개 시스템의 암호 사용 현황 조사, 필요시 외부 컨설팅 및 자동화 도구 활용 비용 반영	기존 정보보호 사업과 연계하거나 소규모 신규 예산 확보
	VPN 시범 적용 및 시험·검증	기존 시험환경에 양자내성암호 지원 VPN 기능 적용, 성능·상호운용성·롤백 시험 비용 반영	VPN 유지관리사업 및 기존 시험환경 활용
	공급업체 지원 계획 및 계약 검토	VPN 장비 공급업체와 업그레이드 가능 버전, 지원 시기 및 계약조건 협의	유지관리 계약 갱신과 연계
다. 중기 예산 계획	원격접속 VPN 전환	VPN 장비 2대의 펌웨어 업그레이드 또는 교체, 설정 변경 및 검증 비용 반영	예정된 VPN 장비 교체사업과 연계
	대민 웹서비스 양자내성암호 대응	웹서버 및 TLS 종단 장비의 양자내성암호 지원 여부 확인, 필요한 소프트웨어 업그레이드 및 호환성 시험 비용 반영	대민 웹서비스 고도화 사업에 포함
	나머지 시스템 전환	암호자산 조사 및 우선순위 평가 결과에 따른 시스템별 개선·교체 비용 반영	차세대 정보화사업과 정기 유지관리사업에 순차 반영
전환 전반 및 지속 관리	운영·유지관리 및 암호자산 인벤토리 현행화	담당자 교육, 운영 모니터링, 암호자산 인벤토리 갱신 및 추가 검증 비용 반영	정기 정보보호·운영관리 예산에 반영

위 예산 계획의 주요 특징

① **기존 자원을 활용한 초기 준비** : 별도 예산 확보에 앞서 기존 인력과 자료를 활용하여 전환 추진체계 마련, 암호자산 현황 파악, 공급업체 지원 여부 확인 및 담당자 교육 등 준비 활동에 착수

② **기존 사업과 연계한 예산 확보** : 보안장비 업그레이드 · 교체는 노후 장비 교체사업 및 유지관리사업과 연계하고, 신규 · 차세대 시스템의 양자내성암호 대응은 정보화사업 기획 단계부터 반영하여 별도 예산 부담을 줄이는 방향으로 계획

③ **전환 우선순위에 따른 단계적 투자** : 단기적으로 암호자산 상세 조사와 시범 적용 · 시험에 필요한 예산을 확보하고, 중기적으로 전환 우선순위가 높은 시스템의 적용 · 검증에 필요한 예산을 반영

④ **기존 자원 활용 및 지속 관리** : 시험 · 검증에는 기존 개발 · 시험환경을 우선 활용하고, 교육에는 공개 기술자료와 기존 교육체계를 활용하여 비용 부담을 줄임. 전환 과정과 완료 이후에도 필요한 운영 · 유지관리 및 암호자산 인벤토리 현행화 비용을 지속적으로 반영

❺ 주요 산출물

이 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다.

산출물	내용
단계별 예산 계획서	항목별 · 연도별 소요 예산 추정, 기존 사업과의 연계 방안, 우선순위 기반 투자 순서를 포함한 중장기 예산 계획 문서
기존 사업 연계 검토서	기관 내 진행 중 · 예정 중인 정보화사업 목록과 각 사업에 양자내성암호 요건 반영 가능 여부 및 방법 정리
교체 필요 장비 · 소프트웨어 목록 및 비용 추정 목록	4장 4절 공급업체 대응 결과를 바탕으로 신규 구매가 필요한 장비 · 소프트웨어와 예상 비용 목록

예산 계획서는 최초 수립 이후에도 국가정보원의 양자내성암호 검증 추진 정책, KCMVP 검증대상 알고리즘 목록 갱신, 공급업체의 지원 현황 변화, KCMVP 검증필 암호모듈 출시 등 주요 여건 변화를 반영하여 지속적으로 갱신해야 한다. 별도의 변화가 없더라도 최소 연 1회 재검토할 것을 권장한다.

❻ 기관 특성별 예산 계획 고려사항

기관의 규모, 수행 업무, 정보시스템 운영 방식 및 대외 연계 수준 등에 따라 양자내성암호 전환에 필요한 비용과 사업 연계 전략은 달라질 수 있다. 따라서 동일한 예산 계획을 일률적으로 적용하기보다는 각 기관의 특성을 고려하여 예산 계획을 수립할 필요가 있다.

다음은 기관의 행정적 구분과 주요 업무·시스템 운영 특성을 고려한 예산 계획의 예시로, 새로운 기관 분류체계를 제시하는 것은 아니다. 각 기관은 해당하는 특성을 복합적으로 고려하여 필요한 사항을 선택적으로 참고할 수 있다.

■ 중앙행정기관

- 범정부 공통 플랫폼·공통 인증체계와 연계되는 시스템이 많으므로, 개별 기관 단독 전환보다 공통 인프라 개편 일정과 연계한 예산 계획이 현실적이다.
- 단독 변경이 가능한 VPN·인터넷 노출 서비스 등은 별도 예산으로 선행 추진하고, 공통 인증체계 연계 영역은 범정부 일정에 맞춰 중기 예산으로 반영한다. 또한 산하기관 전환 지원 예산도 함께 검토할 필요가 있다.

■ 지방자치단체

- 공통 행정시스템과 범정부 공통 인프라 활용 비중이 높고 자체 전문인력이 제한적인 경우가 많으므로, 대규모 독립 전환사업보다 기존 유지관리사업 및 정보화사업과 연계한 단계적 접근이 현실적이다.
- 광역지자체는 '차세대 지방행정정보시스템' 사업 일정에 양자내성암호 요구사항을 조기에 반영하는 등 대규모 정보화사업 또는 공통 행정시스템 개편 사업 추진 시 양자내성암호 요구사항 반영 여부를 조기에 검토할 필요가 있다.
- 기초지자체는 공통 인프라 의존도가 높은 만큼 상위 기관 및 전문기관의

지원 체계를 적극 활용하는 방안을 함께 고려할 수 있다.

■ 공공기관 · 준정부기관

- 장기 운영 레거시 시스템과 특정 공급업체 종속 구조가 많으므로, 장비 교체 시점을 활용한 예산 연계가 핵심이다. 특히 HSM · 보안장비의 노후 교체 예산에 양자내성암호 지원 제품 선택 기준을 포함하고, 외부 전문 컨설팅이나 민간 보안기업의 기술 지원을 활용하여 전환 준비를 단계적으로 진행하는 것이 효과적이다.
- 공급업체 의존도가 높은 시스템은 유지관리 계약 갱신 시점을 기회로 활용한다.

■ 연구개발 중심 기관

- 장기간 보호가 필요한 연구데이터의 기밀성 유지와 전자서명 데이터의 장기검증을 고려하여, HNDL 공격 및 데이터 중요도와 보호 필요기간 등에 따른 전환 우선순위를 평가하고 그 결과를 예산 계획에 반영할 필요가 있다.
- 연구망과 국제 공동연구 연계 구간에서는 양자내성암호 적용에 따른 성능 및 상호운용성 영향을 사전에 검토하고, 필요한 시험 · 검증 및 시스템 개선 비용을 예산에 반영할 필요가 있다.

■ 국가핵심기반시설 및 OT/ICS 운영기관

- 운영 중단에 따른 영향이 크므로 충분한 사전 시험과 단계적 전환에 필요한 예산을 확보할 필요가 있다. 단기간 내 전환이 어려운 장수명 장비는 교체 예산과 함께 전환 전까지 필요한 보완통제 및 예외관리 비용을 반영한다. 제조사 지원이 없는 장수명 장비는 교체 예산을 장기 투자 계획에 별도 반영하고, 그 전까지 망 분리 강화 등 보완 통제 유지 비용을 계상해야 한다.
- 시험환경 분리 구축 비용도 별도로 확보하는 것이 바람직하다.

❼ 단계 완료 체크리스트

다음 체크리스트를 활용하여 예산 계획 수립 단계의 핵심 사항이 이행되었는지 확인한다.

※ 본 체크리스트 및 질의서는 예시이며, 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인	4.5 예산 계획 수립 – 실무 확인표
□	양자내성암호 전환 비용이 발생하는 주요 영역을 파악하였다. 예 : 장비 교체, 소프트웨어 업그레이드, 컨설팅, 인증서 재발급 등 비용 발생 영역을 항목별로 정리하였다. ※ 전환 비용 발생 예시 : 장비·소프트웨어 교체 또는 업그레이드, 시스템 개발·수정, 시험·검증 환경 구축, 인증서·암호 키 전환, 컨설팅, 외부 전문지원 및 교육 등
□	4장 3절 우선순위 평가 결과와 4장 4절 공급업체 대응 현황을 바탕으로 예산 항목을 도출하였다.
□	기관 내 진행 중·예정 중인 정보화사업(차세대, 유지관리, 장비 교체, 클라우드 전환 등)에 양자내성암호 요건 반영 가능 여부를 검토하였다.
□	기존 사업과 연계하여 추가 비용 없이 처리 가능한 항목을 식별하였다. ※ 예정된 장비 교체, 소프트웨어 업그레이드, 차세대 사업 등 확인
□	별도 예산이 필요한 항목과 규모를 추정하였다.
□	교체가 필요한 장비·소프트웨어 목록과 예상 비용을 산출하였다.
□	외부 전문 지원(컨설팅, 민간 전문교육기관, 국내외 공개 자료 등) 활용 가능 항목을 파악하였다.
□	연도별 예산 투입 시기를 계획하였다. ※ 3장 3절의 국가 전환 로드맵 단계에 맞춰 단계별로 투입할 예산 항목과 규모 배분
□	예산요구서 작성 일정(통상 전년도 전반기)에 맞춰 필요 예산을 반영할 준비가 되었다.
□	단계별 예산 계획서(초안)를 작성하였다. ※ 예시 : 시스템별 전환 우선순위와 추진 시기를 바탕으로 연도별 대상 사업, 주요 예산 항목, 예상 소요비용 및 기존 사업과의 연계 여부 등을 정리
□	예산 계획 갱신 주기(최소 연 1회)를 정하였다.

제6절 전환 시행 및 운영 검증

양자내성암호 전환의 마지막 단계인 전환 시행 및 운영 검증은 앞선 단계에서 수립한 계획을 실제 운영 환경에 적용하고 그 결과를 확인하는 과정이다. 아무리 철저한 계획을 수립하더라도 실제 적용 과정에서는 예상하지 못한 성능 저하, 상호운용성 문제, 운영상 오류가 발생할 수 있다.

이 단계에서 가장 중요한 원칙은 '점진적 · 단계적 적용'이다. 모든 시스템에 전환을 일괄 적용할 경우 문제 발생 시 영향 범위가 크게 확대될 수 있다. 따라서 영향 범위가 작은 시스템부터 적용하여 운영 경험을 축적하고, 검증된 절차를 바탕으로 전환 범위를 점차 확대해 나가는 것이 바람직하다.

특히 국가 · 공공기관 환경에서는 '기능이 동작하는가'보다 '운영 환경에서 안정적으로 작동하는가'가 더 중요한 경우가 많다. 기관 간 연계 인증 실패, 특정 모바일 환경에서의 인증 오류, 성능 저하로 인한 서비스 지연 등은 기술 검증만으로는 발견하기 어려우며 실제 운영 환경에서만 드러나는 경우가 많다. 따라서 '적용'보다 '검증'에 더 많은 시간과 인력을 투입하는 것이 결과적으로 전환 실패를 방지하는 현실적인 접근이다. 또한 현재 시점에서는 상당 기간 기존 공개 키 암호 체계와 양자내성암호 기반 구조가 병행 운영될 가능성이 높으므로, 하이브리드 환경에서의 상호운용성 · 성능 · 운영 절차를 함께 검증하는 것이 중요하다.

본 절에서는 적용 대상 선정 기준, 주요 검증 항목(성능 · 상호운용성 · 장애 대응 · 운영 절차 · 기존 데이터 처리), 단계적 적용 절차, 그리고 실제 적용 예시와 체크리스트를 제시한다.

❶ 적용 대상 선정 기준

전환 대상의 기본적인 추진 순서는 4장 3절에서 산정한 우선순위(1~4순위)를 따른다. 다만 실제 적용 단계에서는 동일한 우선순위 그룹에 여러 시스템이 포함될 수 있으므로, 이 절에서는 그중 어떤 시스템을 먼저 적용할 것인지 판단하기 위한 시범 적용 대상 선정 기준을 제시한다.

4장 3절 ❸의 배점 체계에서는 파급력(④)과 전환 난이도(⑨)가 모두 우선순위 점수에 정(+)의 방향으로 반영된다. 전환 난이도에 높은 점수를 부여하는 것은 준비에 장기간이 필요한 시스템을 조기에 식별하여 충분한 준비기간을 확보하기 위한 것이다. 그러나 우선순위 점수만을 실제 적용 순서로 사용할 경우, 전환 난이도가 높거나 실패 시 영향이 큰 시스템이 초기 적용 대상이 될 수 있다.

따라서 첫 번째 시범 적용 대상은 원칙적으로 우선순위가 높은 그룹에서 선정하되, 해당 그룹 내 시스템의 독립성, 중단 허용 가능성, 전환 난이도, 검증 가능성 및 영향 범위를 함께 고려하여 상대적으로 안전하게 적용·검증할 수 있는 시스템을 선정한다.

[표 31] 전환 대상 선정 기준

선정 기준	내용	적합한 시범 대상 예시	부적합 시범 대상 예시
독립성	다른 시스템과 연계가 적어 단독으로 전환·롤백이 가능한 시스템	• 내부 전용 VPN • 독립 운영 내부 시스템	• 전자서명 인증체계 연동 시스템
중단 허용 가능성	전환 작업 중 서비스 중단이 허용되거나 중단 영향이 제한적인 시스템	• 야간 점검이 가능한 시스템 • 소수 사용자 내부 서비스	• 24시간 365일 운영 대국 민 서비스
전환 난이도	암호 알고리즘 설정 변경이 비교적 용이하고 소스코드 수정이 최소화되는 시스템	• 설정 파일로 TLS 설정 변경 가능한 웹서버 • 암호 민첩성을 지원하는 구조를 갖춘 시스템	• 대규모 소스코드 수정이 필요한 레거시 시스템
검증 가능성	전환 전후 암호 알고리즘 동작을 검증할 수 있는 충분한 테스트 환경과 기술 역량이 확보된 시스템	• 시험·검증 환경 활용이 가능한 시스템	• 운영계와 개발계가 분리되지 않은 시스템
영향 범위	전환 실패 시 영향 범위가 제한적이어서 복구가 용이한 시스템	• 단일 부서 내부 시스템 • 소수 사용자 서비스	• 루트 CA • 코드서명 인프라 • 핵심 인증 기반

다섯 가지 선정 기준은 시스템이 속한 우선순위 그룹과 무관하게 동일하게 적용된다. 따라서 시범 대상은 원칙적으로 우선순위가 가장 높은 그룹부터 검토하며, 해당 그룹 안에 위 조건을 충족하는 시스템이 없는 경우에 한해 예외적으로 차순위 그룹에서 대상을 선정한다.

위 기준을 종합하면, 시범 적용에 가장 적합한 첫 번째 대상은 다음 조건을 모두 충족하는 시스템이다.

- 기관 내부에서만 사용되어 외부 연계가 없거나 적음
- 서비스 중단 창(Maintenance Window)이 확보되어 있음
- 암호 설정이 설정 파일 또는 관리 콘솔에서 변경 가능한 구조
- 시험 환경(개발계 · 스테이징 환경)이 별도로 존재
- 전환 실패 시 롤백이 용이한 구조

예시 : 첫 번째 시범 적용 대상 선정 과정

○○공공기관의 전환 1순위 시스템은 앞서 4장 3절 ❸의 매트릭스 예시에서 확인한 '원격접속 VPN(19점)'과 '행정전자서명 인프라(19점)' 두 곳이다. 그러나 행정전자서명 인프라는 범정부 공통 인프라와 연계되어 있어(독립성 기준 미충족) 기관 단독 전환이 불가능하다. 원격접속 VPN은 독립 운영이 가능하지만, 전 직원이 상시 사용해 서비스 중단 창을 확보하기 어렵고 전환 실패 시 전 직원의 원격근무가 함께 중단되는 등 영향 범위가 크다. 즉 1순위 그룹 안에는 지금 당장 안전하게 시범 전환을 시작할 수 있는 시스템이 없다.

이러한 경우 기관은 1순위 시스템(원격접속 VPN, 행정전자서명 인프라)에 대해서는 4장 3절 ❺의 '고위험 선제 전환' 전략에 따라 예산 확보, 하이브리드 설계, 관계 기관 협의 등 착수 준비를 계속 진행하는 한편, 실제 **첫 번째 시범 전환 대상**은 예외적으로 2순위 그룹에서 선정한다. 5가지 선정 기준을 모두 충족하는 '소프트웨어 업데이트 서버(14점)'가 이에 해당한다. 이 시스템은 ① 내부 전용 시스템으로 외부 연계 없음 ② 업무 시간 외 중단 가능, ③ 설정 파일 변경만으로 TLS 알고리즘 교체 가능, ④ 별도 시험 서버 보유, ⑤ 롤백이 설정 파일 복구로 가능 – 의 조건을 모두 충족한다.

○○공공기관은 소프트웨어 업데이트 서버에서 축적한 경험을 바탕으로, 사전 준비를 마친 1순위 시스템인 원격접속 VPN의 전환에 착수했다.

❷ 단계적 적용 절차

모든 전환 작업은 다음 5단계 절차에 따라 진행한다. 각 단계는 완료 기준을 충족한 후 다음 단계로 진행하며, 문제 발생 시 즉시 롤백하는 원칙을 적용한다.

[표 32] 전환 단계적 적용 절차

적용 단계	시점	주요 활동	완료 기준
사전 준비	전환 작업 착수 전	• 완전한 시스템 백업 및 복구 시험 • 롤백 절차 수립 및 문서화 연계 • 기관·부서 사전 통보 시험 • 환경 구축 및 사전 검증	• 백업 복구 성공 확인 • 롤백 절차 문서화 완료 • 관련 기관 협의 완료
시험 환경 적용·검증	운영 전환 1~2개월 전	• 시험 환경에서 양자내성암호 적용 • 성능·상호운용성·장애 대응 시험 • 기존 데이터 처리 방안 검증 • 시험 결과 분석 및 보완	• 모든 검증 항목 기준 충족 • 발견된 문제점 해결 완료
운영 환경 파일럿 적용	전환 우선순위 높은 시스템 중 독립성과 전환 용이성을 고려	• 전환 우선순위가 높은 시스템 중 독립성이 높고 전환이 용이한 대상에 우선 적용 • 실제 운영 중 모니터링 강화 • 문제 발생 시 즉시 롤백	• 파일럿 기간 동안 장애 없음 • 성능·상호운용성 기준 충족
단계적 확대 적용	파일럿 성공 후	• 우선순위 순서대로 점진적 확대 • 단계별 모니터링 및 이상 징후 감지 • 연계 시스템 순차 전환	• 각 단계 완료 후 안정화 기간경과
전환 완료 및 안정화	전체 적용 후	• 기존 알고리즘 지원 종료 시점 결정 • 폴백 필요성 재검토 및 불필요한 폴백 기능 제거·비활성화 • 암호자산 인벤토리 갱신 • 운영 절차·지침 최종 업데이트	• 기존 알고리즘 의존 없이 정상 운영 확인

롤백 계획 없는 전환 작업은 금지

모든 전환 작업 착수 전에 롤백(원상 복구) 절차가 준비되어 있어야 한다. 구체적으로는 ① 전환 전 전체 시스템 백업 완료, ② 백업으로부터 복구하는 절차 사전 시험 및 확인, ③ 롤백 결정 기준(어떤 상황이 발생하면 롤백하는가), ④ 롤백 담당자와 권한이 명확히 정해져 있어야 한다.

롤백 절차를 문서화하고, 실제로 시험 환경에서 롤백 시험을 수행한 후 운영 환경 전환을 착수한다.

❸ 검증 항목

가. 성능

양자내성암호는 기존 공개 키 암호에 비해 키 크기가 크고 일부 연산이 복잡하여 성능에 영향을 줄 수 있다. 전환 전후 성능 변화를 체계적으로 측정하고, 서비스 수준 협약(SLA)을 충족하는지 확인해야 한다.

[표 33] 성능 검증 항목

성능 검증 항목	측정 내용	허용 기준 설정 방법
키 생성 · 교환 처리 시간	양자내성암호 적용 후 키 생성 및 키 교환에 소요되는 시간. 기존 RSA/ECDH 대비 변화율 측정	기존 대비 처리 시간 증가율을 기관 서비스 SLA 기준과 비교. 실제 사용자 체감 지연이 발생하지 않는 수준인지 확인
TLS 핸드셰이크 소요 시간	양자내성암호 포함 TLS 연결 수립 시간	기존 TLS 핸드셰이크 대비 증가율. 대용량 트래픽 환경(동시 접속자 수 기반 부하 시험)에서 허용 범위 확인
데이터 처리량	암호화 · 복호화 · 서명 · 검증 처리량(초당 처리 건수) 및 서버 CPU 부하 변화 측정	전환 후 처리량이 피크 시간대의 서비스 요구 처리량 이상이며, 기존 대비 처리량 감소율은 기관이 정한 허용 범위 이내인지 확인

성능 검증 항목	측정 내용	허용 기준 설정 방법
패킷·메시지 크기 증가	양자내성암호 적용 후 공개키·서명·인증서 크기 증가량. 네트워크 대역폭 영향	네트워크 대역폭 여유 범위 내에서 증가 허용 여부 확인. IP 단편화 발생 여부 점검
메모리·CPU 사용률	양자내성암호 연산 적용 후 서버 메모리 및 CPU 사용률 변화	기존 대비 자원 사용률 증가가 서버 용량 내에서 허용 가능한 수준인지 확인

성능 검증 시 다음 사항을 유의한다.

- 시험 조건의 현실성 : 실제 운영 환경과 유사한 부하 조건(피크 시간대 동시 접속자 수 등)에서 시험해야 한다. 단순 단건 처리 시간만 측정하면 실제 운영에 미치는 영향을 과소 평가할 수 있다.
- 알고리즘별 차이 : 양자내성암호는 알고리즘별로 성능 특성이 다르다. 각 사용 목적에 맞는 알고리즘의 성능을 별도로 측정한다.
- 하드웨어 가속 : 일부 서버 CPU나 전용 암호 가속 카드는 양자내성암호 연산을 하드웨어 수준에서 가속할 수 있다. HSM 교체 시 이 기능 지원 여부를 확인한다.
- 네트워크 영향 : 양자내성암호의 큰 키 크기로 인해 패킷 크기가 증가한다. 특히 MTU(최대 전송 단위) 제한이 있는 환경에서 IP 단편화가 발생하지 않는지 확인한다.

나. 상호운용성

상호운용성은 국가·공공기관 환경에서 가장 복잡한 검증 항목이다. 행정망, 범정부 연계, 기관 간 공동 시스템 등 다양한 연계 구간에서 전환된 시스템이 미전환 시스템과 정상적으로 통신해야 하기 때문이다.

[표 34] 주요 상호운용성 확인 사항

검증대상 구간	주요 확인 사항	국가·공공기관 특이 고려사항
기관 내부 시스템 간	전환된 시스템과 미전환 시스템 간 통신 가능 여부. 하이브리드 방식 적용 시 양측 모두 정상 동작 여부	행정망 내 시스템은 운영 중단 없이 단계적으로 전환해야 하므로, 전환 중 기간에도 기존 시스템과 통신이 유지되어야 함
기관 간 연계 구간	행정정보공동이용, 타기관 API 연계 구간의 암호 설정 변경 후 정상 동작 여부	연계 상대 기관에 사전 통보 및 협의 후 시험 필수. 단독으로 변경하면 상대 기관 시스템 오류 발생 가능
클라이언트 호환성	웹 브라우저, 모바일 앱, 데스크톱 클라이언트에서 양자내성암호 지원 여부 확인	국가·공공기관 표준 브라우저(Chrome, Edge 등)의 양자내성암호 지원 현황 확인. 구형 IE 기반 내부 시스템 별도 주의
인증서 검증 체계	양자내성암호 인증서가 기존 인증서 검증 인프라(OCSP, CRL 등)와 호환되는지 확인	행정전자서명(GPKI) 관련 인증서 검증 체계는 범정부 공통 인프라와 연계되므로 공통 인프라 전환 일정과의 정합성 및 상호운용성 확인 필요
보안장비 통과 여부	방화벽·IPS·보안 게이트웨이 등이 양자내성암호 패킷을 정상 통과(또는 검사)시키는지 확인	일부 보안장비가 알 수 없는 암호 패킷을 차단하거나 오탐할 수 있음. 전환 전 보안장비 설정 사전 검토 필요

상호운용성 시험은 다음 절차로 수행한다.

- 연계 목록 작성 : 전환 대상 시스템과 통신하는 모든 시스템·서비스 목록 작성(4장 2절 암호자산 인벤토리 활용)
- 시험 환경 구성 : 연계 시스템과 동일한 환경을 시험 환경에 재현하거나, 시험·검증 환경 활용이 가능한 시스템
- 단계별 시험 : 기관 내부 연계 → 기관 간 연계 → 대외 연계 순서로 범위를 넓히며 시험
- 폴백 확인 : 하이브리드 방식 적용 시 양자내성암호 미지원 상대방과의 통신에서 사전에 정의된 정책에 따라 허용된 기존 암호 방식으로 폴백되는지 확인하고, 허용되지 않은 암호 방식으로의 다운그레이드가 발생하지 않는지 검증

- 결과 기록 : 연계 구간별 시험 결과를 문서화하고, 문제 발생 시 조치 내용과 재시험 결과를 기록

다. 장애 대응

전환 과정과 전환 이후 운영 중에 발생 가능한 장애 시나리오를 사전에 정의하고, 각 시나리오에 대한 대응 절차가 작동하는지 검증한다.

[표 35] 장애 시나리오 및 대응 방법 예시

장애 시나리오	영향	즉시 대응 방법	재발 방지 조치
양자내성암호 적용 후 TLS 연결 실패	특정 클라이언트나 구간에서 연결 불가	사전 준비된 롤백 절차에 따라 이전 설정으로 복구	전환 전 클라이언트 호환성 사전 점검. 단계적 적용으로 영향 최소화
성능 저하로 인한 서비스 지연	처리 속도 저하로 사용자 체감 지연 또는 타임아웃 발생	일시적으로 기존 알고리즘으로 롤백. 서버 자원(CPU·메모리) 증설 검토	전환 전 충분한 부하 시험 수행. 서버 용량 사전 확보
인증서 검증 실패	전환된 인증서가 기존 클라이언트에서 인식 안 됨	기존 인증서 병행 제공	인증서 전환 전 클라이언트 지원 범위 사전 확인
보안장비 오탐·차단	방화벽·IPS가 양자내성암호 패킷을 비정상 트래픽으로 오탐	보안장비 정책 예외 설정 또는 담당자 즉시 조치	전환 전 보안장비 담당자와 설정 사전 협의
롤백 실패(되돌리기 불가)	전환 실패 시 기존 상태로 복구 불가	사전 준비된 백업 복구 절차 실행. 운영 중단 최소화 비상 대응	모든 전환 작업 전 완전한 백업 및 롤백 시험 필수

장애 대응 검증에서 특히 중요한 것은 **'롤백 가능 여부'**를 실제로 시험하는 것이다. 롤백 절차가 문서에만 존재하고 실제로 시험해보지 않으면, 실제 장애 상황에서 롤백이 실패할 수 있다. 모든 운영 환경 전환 전에 시험 환경에서 롤백 시험을 필수로 수행한다.

- 장애 대응 시나리오 시험 : 주요 장애 시나리오(TLS 연결 실패, 성능 저하,

인증서 검증 실패 등)를 시험 환경에서 재현하고 대응 절차 작동 여부 확인
- 롤백 시험 : 전환 후 기존 상태로 완전히 복구되는지 시험. 복구 소요 시간 측정
- 장애 감지 체계 : 전환 후 모니터링 체계에서 양자내성암호 관련 장애가 감지되는지 확인. 기존 보안관제 시스템에 양자내성암호 관련 이상 징후 탐지 규칙 추가
- 비상 연락 체계 : 전환 작업 중 장애 발생 시 즉시 연락할 수 있는 담당자(정보보안 · 운영 · 공급업체 기술지원) 체계 사전 구축

라. 운영 절차

전환 후 새로운 암호 환경에서 시스템을 안정적으로 운영하기 위해, 기존 운영 절차와 지침이 양자내성암호 적용 환경에 맞게 업데이트되어 있는지 검증한다. 운영 절차 검증에서 확인해야 할 주요 항목은 다음과 같다.

- 인증서 갱신 절차 : 양자내성암호 기반 인증서의 유효기간, 갱신 절차, 폐기 절차가 기존 절차와 동일하게 작동하는지 확인. 만료 알림 체계가 정상 작동하는지 확인
- 키 관리 절차 : 양자내성암호의 키 생성 · 저장 · 폐기 · 복구 절차가 수립되어 있는지 확인. HSM을 사용하는 경우 양자내성암호 키 관리 절차 추가
- 모니터링 체계 : 전환된 시스템에서 암호 관련 이상 징후(알고리즘 다운그레이드 시도, 인증서 오류 빈발 등)를 감지하는 모니터링 항목이 추가되어 있는지 확인
- 로그 관리 : 양자내성암호 사용 기록이 로그에 정상적으로 기록되는지 확인. 감사 추적이 가능한 수준의 로그 수준 확인
- 운영 지침 업데이트 : 시스템 운영 매뉴얼, 보안 지침, 장애 대응 매뉴얼에 양자내성암호 관련 내용이 반영되어 있는지 확인
- 담당자 숙지 여부 : 운영 담당자가 새로운 암호 환경에서의 운영 절차를 이해하고 실행할 수 있는지 확인. 필요 시 추가 교육 제공

국가·공공기관 특이 사항 : 보안성 검토 및 내부 통제 갱신

국가·공공기관에서는 정보화사업 또는 보안제품 운영 과정에서 보안성 검토, 보안적합성 검증, 인증제도 등의 적용을 받을 수 있다. 양자내성암호 적용으로 기존 암호기능이나 보안 설정이 변경되는 경우에는 관련 검토·검증 절차에 영향을 미치는지 사전에 확인할 필요가 있다.

특히 보안적합성 검증대상 시스템 또는 CC인증·보안기능 확인서를 취득한 제품의 암호 기능이 변경되는 경우에는 기존 인증·검증의 유효성에 영향을 줄 수 있으므로 관련 절차를 사전에 검토해야 한다.

마. 기존 데이터 처리

암호 알고리즘 전환 시 가장 많은 혼란이 생기는 부분 중 하나가 '기존에 암호화되거나 서명된 데이터는 어떻게 해야 하는가'이다. 데이터 유형에 따라 처리 방법이 다르며, 잘못된 처리는 데이터 손실이나 법적 문제로 이어질 수 있다.

[표 36] 기존 데이터 처리 방법

데이터 유형	처리 필요 여부	처리 방법	국가·공공기관 특이 사항
전송 중 암호화 데이터 (TLS 등)	불필요 (전향적 보안)	TLS 세션 단위로 암호화·복호화되므로, 전환 후 새 세션부터 자동으로 양자내성암호 적용. 기존 세션 데이터 재처리 불필요	전환 시점 이후 맺어지는 새 연결만 양자내성암호 적용. 기존 수집된 암호화 트래픽(HNDL 위협 대상)은 이미 노출된 것으로 간주
저장 데이터 (At-rest 암호화)	조건부 필요 (위험도 기반)	공개 키 암호로 암호화된 저장 데이터는 복호화 후 새 알고리즘으로 재암호화 필요 여부 평가. 장기 보호 필요 데이터 우선 처리	공공기록물·장기 보존 개인정보 등은 우선 처리 대상임. 재암호화 작업 전 데이터 백업 또는 복구 절차를 확보할 것. 대칭 키 암호화 데이터도 공개 키 기반 키 관리 체계를 사용하는 경우 전환 영향 검토 필요

데이터 유형	처리 필요 여부	처리 방법	국가 · 공공기관 특이 사항
서명 데이터	일반적 불필요 (검증 시점 기준)	기존 서명은 서명 시점의 알고리즘으로 유효성을 검증하므로 재서명 불필요. 단, 장기 유효성 검증이 필요한 경우 타임스탬프 추가 고려	행정전자서명 기반 공문서는 법적 효력 문제와 연계되므로 별도 법적 검토 필요. 전자계약서, 전자세금계산서 등 금융 · 행정 문서 포함
인증서 · 키 (기발급 인증서)	필요(재발급)	기존 알고리즘 기반 인증서를 양자내성암호 기반으로 재발급. 기존 인증서는 유효기간 내 사용 후 폐기 또는 즉시 폐기	행정전자서명(GPKI) 인증서는 공통 인프라 전환 일정에 맞춰 재발급. 내부 CA 발급 인증서는 자체 일정으로 순차 재발급
코드서명 소프트웨어	조건부 필요	기존 서명된 소프트웨어 · 펌웨어는 재배포 시점에 새 알고리즘으로 재서명. 배포 이후 설치된 버전은 기존 서명 유지	운영 중인 시스템에 배포된 소프트웨어의 서명 업데이트는 패치 · 업데이트 배포 프로세스와 연계

① 저장 데이터 재암호화 절차

공개 키 암호로 암호화된 저장 데이터를 새 알고리즘으로 재암호화할 필요가 있는 경우, 다음 절차를 따른다.

- 재암호화 필요 데이터 식별 : 4장 3절 우선순위 기준에 따라 정책 · 규정 등에 의해 장기간 기밀성 보호가 요구되며, 양자취약 공개 키 암호로 직접 암호화된 저장 데이터를 우선 대상으로 선정
- 데이터 복구 : 재암호화 실패 시 복구 가능한 상태 확보를 위해 재암호화 작업 전에 데이터 백업 또는 복구 절차를 확보할 것
- 소량 파일럿 테스트 : 전체 데이터 재암호화 전 소량의 데이터로 재암호화 절차 시험. 결과 검증 후 전체 적용
- 데이터 무결성 확인 : 재암호화 후 데이터 무결성 검증(해시값 비교 등)
- 기존 암호화 데이터 보관 정책 : 재암호화 완료 후 기존 암호화 데이터의 보관 또는 삭제 정책 수립

② 서명 데이터의 장기 유효성 보장

전자서명은 서명 시점의 알고리즘으로 유효성이 판단되므로, 기존 서명된 문서를 재서명할 필요는 일반적으로 없다. 그러나 서명의 장기 유효성 검증이 필요한 경우(예 : 10년 이상 법적 효력을 유지해야 하는 전자계약서, 공공기록물)는 추가 조치가 필요하다.

- 장기 서명 프로파일(LTV : Long Term Validation) 적용 : 서명 당시의 인증서 상태 정보(OCSP 응답, CRL 등)를 문서에 포함하여 향후 검증 가능성 확보
- 타임스탬프 추가 : 공증된 타임스탬프를 서명에 추가하여 서명 시점 증명. 타임스탬프 인증서도 양자내성암호 기반으로 전환 필요
- 법적 검토 : 행정전자서명, 전자계약서 등 법적 효력이 있는 전자서명의 알고리즘 전환 시 관련 법령(전자서명법, 전자정부법 등) 해석과 법적 유효성에 대한 사전 법적 검토 수행

※ 주의 : 「공공기록물 관리에 관한 법률」에 따른 전자기록물의 전자서명 처리는 국가기록원의 지침을 참고하고, 필요 시 사전 협의한다.

③ 인증서 재발급 절차

기존 알고리즘 기반 인증서를 양자내성암호 기반으로 교체할 때의 실무적 절차는 다음과 같다.

- 인증서 목록 준비 : 재발급 대상 인증서 전체 목록 확보(4장 2절 암호자산 인벤토리 활용). 만료일, 발급기관, 사용 시스템 정보 포함
- 내부 CA 사용 기관 : 자체 CA에서 양자내성암호 기반 인증서 발급 가능 여부 확인. 가능한 경우 기존 인증서 유효기간 내 순차 재발급
- 외부 공인 CA 사용 기관 : CA의 양자내성암호 인증서 발급 지원 여부 확인. 발급 가능 시점에 맞춰 교체 계획 수립
- 인증서 전환 방식 확인 : 상위 인증기관 및 관계 기관이 적용할 인증서 전환 방식과 일정을 확인하고, 기존 공개 키 암호 기반 인증서와 양자내성암호 기반 인증서의 병행 제공 또는 복수 알고리즘을 지원하는 인증서 구조의

발급 · 검증 가능 여부를 확인

- 기존 인증서 폐기 : 재발급 완료 후 기존 인증서 폐기 절차 수행. 폐기 전 모든 시스템에서 새 인증서로 교체되었는지 확인

❹ 전환 완료 기준

각 시스템의 양자내성암호 전환이 완료되었다고 판단하는 기준은 다음과 같다. 이 기준을 충족한 후 암호자산 인벤토리를 갱신하고 다음 시스템 전환으로 진행한다.

- 모든 검증 항목(성능 · 상호운용성 · 장애 대응 · 운영 절차 · 기존 데이터 처리) 기준 충족
- 기존 취약 알고리즘(RSA, ECC 등 양자취약 공개 키 암호)에 대한 단독 의존이 제거되고, 양자내성암호 하이브리드 방식이 적용됨
- 운영 담당자가 새로운 운영 절차를 숙지하고 정상 운영 가능
- 모니터링 체계에서 기관이 정한 안정화 기간 동안 정상 운영됨
- KMCVP 검증대상 양자내성암호, 국내 및 국제 표준 확정 등에 따라 CC 인증 또는 보안기능 확인서를 취득한 제품의 암호기능이 변경될 경우 기존 인증 · 확인서 효력이 유지되는지 여부를 반드시 확인한 후 업데이트 여부를 결정할 것
- 관련 보안적합성 검증 · 인증 제도에 미치는 영향을 확인하고, 필요한 절차를 완료함

⚠ '전환 완료' ≠ '기존 알고리즘 즉시 제거'

전환 과도기에는 기존 공개 키 암호와 양자내성암호를 병행 사용하는 하이브리드 방식을 유지하면서, 주요 연계 시스템 및 지원 대상 클라이언트가 정상적으로 통신할 수 있는지 확인하는 것이 중요하다. 기존 알고리즘 지원 종료 시점은 국가 정책 및 공공부문 적용 기준에 따라 결정한다.

❺ 주요 산출물

이 단계에서 기관이 확보해야 하는 주요 산출물은 다음과 같다.

산출물	내용
(시범)적용 및 검증 결과서	4장 6절 ③의 5개 검증 항목별 시험 결과, 발견된 문제점과 조치 내용, 최종 합격 여부를 포함한 문서
운영 절차 및 장애 대응 계획서	양자내성암호 적용 환경에 맞게 업데이트된 운영 절차, 인증서 갱신 절차, 장애 시나리오별 대응 방법을 포함한 문서
기존 데이터 처리 결과서	저장 데이터 재암호화, 인증서 재발급, 서명 데이터 처리 결과 및 검증 내용을 포함한 문서
갱신된 암호자산 인벤토리	전환 완료된 시스템의 상태를 반영하여 갱신된 암호자산 인벤토리 문서

❻ 단계 완료 체크리스트

다음 체크리스트를 활용하여 적용 및 검증 단계의 핵심 사항이 이행되었는지 확인한다. 시스템별로 별도 작성하며, 모든 항목을 충족한 경우 해당 시스템의 전환이 완료된 것으로 간주한다.

※ 본 체크리스트 및 질의서는 예시이며, 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인	4.6 적용 및 검증 – 실무 확인표(시스템별 작성)
□	전환 대상 시스템을 4장 6절 ❶의 적용 기준(독립성, 중단 허용 가능성, 전환 난이도, 검증 가능성, 영향 범위)에 따라 선정하였다.
□	전환 전 전체 시스템 복구 가능한 상태를 확보하였고, 복구 시험을 성공적으로 수행하였다. ※ 예시 : 전환 전 시스템 백업(스냅샷)을 생성하고, 실제 복구 시험을 수행하여 정상 복원 여부를 확인

확인	4.6 적용 및 검증 – 실무 확인표(시스템별 작성)
□	롤백(원상 복구) 절차를 문서화하였고, 담당자가 숙지하고 있다.
□	연계 기관 · 부서에 전환 작업 일정을 사전 통보하였다.
□	시험 환경에서 모든 검증 항목에 대한 사전 시험을 완료하였다. ※ 검증 항목 : 성능, 상호운용성, 장애 대응, 운영 절차, 기존 데이터 처리 등 실제 운영 환경 적용 전에 확인해야 하는 항목
□	[성능] 처리 속도, TLS 핸드셰이크 시간, 패킷 크기, 자원 사용률 측정 결과가 허용 기준을 충족한다.
□	[상호운용성] 기관 내부 · 기관 간 · 클라이언트 호환성 · 보안장비 통과 여부 시험을 완료하였다. ※ 양자내성암호 적용 후 내부 시스템 및 연계기관과의 통신, 기존 클라이언트와의 접속, 방화벽 · IPS · 프록시 등 통신 경로상의 보안장비에서의 차단 · 오류 발생 여부 등 확인
□	[장애 대응] 주요 장애 시나리오에 대한 대응 절차를 시험 환경에서 검증하였다. ※ 장애 시나리오 예시 : 인증서 검증 실패, TLS 연결 실패, 연계 시스템 간 통신 오류, 성능 저하, 양자내성암호 적용 후 특정 장비 · 클라이언트의 접속 실패 등
□	[운영 절차] 인증서 갱신 · 키 관리 · 모니터링 · 로그 관리 절차를 양자내성암호 환경에 맞게 업데이트하였다. ※ 예시 : 양자내성암호 적용으로 변경되는 인증서 발급 · 갱신 · 폐기, 암호 키 생성 · 배포 · 보관 · 폐기, 장애 · 이상 징후 모니터링 및 관련 로그 확인 절차를 기존 운영 절차에 반영
□	[기존 데이터] 저장 데이터 재암호화 필요 여부를 평가하였고, 필요한 경우 재암호화를 완료하였다. ※ 재암호화 검토 대상 : 장기 보존 저장 데이터 중 RSA · ECC 등 양자취약 공개 키 암호로 직접 보호되거나, 데이터 암호화키(DEK)가 이러한 공개 키 암호로 보호된 데이터
□	[기존 데이터] 서명 데이터의 장기 유효성 보장 방안을 검토하였다. ※ 장기간 보존해야 하는 서명 데이터는 기존 전자서명 알고리즘의 안전성이 약화된 이후에도 진본성을 검증할 수 있도록 재서명, 중복서명 등 장기검증 방안의 적용 필요성을 검토
□	[기존 데이터] 인증서 재발급을 완료하였고, 기존 인증서 폐기 절차를 수행하였다.

확인	4.6 적용 및 검증 – 실무 확인표(시스템별 작성)
□	운영 환경 파일럿 적용 후 기관이 정한 안정화 기간 동안 이상 징후 없이 안정적으로 운영하였다. ※ 이상 징후 예시 : 인증·통신 오류, 성능 저하, 연계 장애, 자원 사용량 증가 등
□	기존 취약 알고리즘에 대한 단독 의존을 제거하였고, 양자내성암호 하이브리드–AND 방식을 적용하였다. ※ 하이브리드–AND 방식 : 기존 공개 키 암호와 양자내성암호를 함께 적용하고 그 결과를 결합하여 사용하는 전환 방식
□	양자내성암호로의 전환이 보안적합성 검증, CC인증, 보안기능 확인서 등 관련 검증·인증에 미치는 영향을 검토하였으며, 필요한 대응 절차를 완료하였다. ※ 암호 알고리즘, 암호모듈, 보안기능 등의 변경으로 기존 검증·인증의 유효성이나 범위가 달라지는지 확인
□	관련 운영 문서(매뉴얼·지침)를 갱신하였다.
□	암호자산 인벤토리에 전환 완료 상태를 반영하였다. ※ 전환 완료 시스템의 변경된 암호 알고리즘·라이브러리·인증서·키 등의 정보를 갱신하고, 전환 완료일과 현재 적용 상태를 암호자산 인벤토리에 반영

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



Chapter 05

전환 시 상황별 고려사항

Chapter
05 전환 시 상황별 고려사항

양자내성암호로의 전환은 개별 시스템의 암호만을 교체하는 단순 보안 업데이트 작업에 그치지 않는다. 이는 시스템 전반의 신뢰 기반(최상위 인증서 체계 등)을 재구축하고, 호환성을 유지하며, 서비스의 연속성을 보장해야 하는 종합적인 기반 시스템 개선 프로젝트이다.

본 장에서는 국내외 관계 기관 및 표준화 기구의 가이드라인과 실제 전환 사례 분석을 토대로, 실무자가 전환 실행 단계에서 검토해야 할 핵심 고려사항을 설명한다.

양자내성암호 전환 과정에서 직면할 수 있는 5가지 주요 위험 요인과 실무적인 대응 방안을 아래와 같이 요약한다.

[표 37] 5가지 주요 위험 요인 및 대응 방안

위험 요인 유형		상세 내용	업무 영향도	실무적 대응 방안
1	네트워크 성능 지연	키와 서명의 데이터 크기 증가로 인한 패킷 분할 및 전송 지연 가능성	보안장비의 일시적 차단 및 대민 서비스 반응 속도 저하 우려	– 방화벽 등 보안장비의 패킷 분할 임계치 재설정 – 성능 테스트를 거쳐 최적의 양자내성 규격 선택
2	구현 단계의 보안 취약성	암호 연산 장비의 연산 전력 변화나 작동 시간 차이를 분석해 암호 키를 알아내는 부채널 공격(SCA) 위협	보안장비 내부의 마스터 키 및 마스터 전자서명 개인 키 탈취 우려	– KCMVP 등 관련 검증 제도에 따른 검증필 암호모듈 중 부채널 공격 대응기법이 적용된 모듈의 탑재 권장

위험 요인 유형		상세 내용	업무 영향도	실무적 대응 방안
3	공급망 제품의 전환 지연	외부 도입 패키지 소프트웨어나 클라우드 서비스 제공사의 양자내성암호 업데이트 지연	타 부서 및 외부 연계 기관 시스템과의 호환성 확보 장애 우려	– 신규 도입 및 계약 갱신 시 업데이트 및 기술 지원 협의 조항 반영 – 공급업체의 양자내성 전환 로드맵 사전 확인
4	표준 사양 조정	국제 표준과 국내 표준 간 규격 차이 또는 과도기 단계의 사양 개정 가능성	이중 개발 부담 및 추후 확정되는 표준 규격과의 정합성 불일치	– 특정 암호에 종속되지 않는 모듈화 방식의 소프트웨어 설계 적용 – 하이브리드 설정을 통한 유연한 암호 스위칭 구조 확보
5	기술 전문성 부족	새로운 결합 방식 설정 오류나 이중 인증서 관리 미숙에 의한 휴먼 에러	통신 규약 결합 방식 오설정 또는 인증서 갱신 주기 관리 누락으로 인한 통신 장애	– 보안 실무자 대상 지속적인 기술 교육 제공 – 암호자산 생애주기 관리 도구 및 인증서 자동 관리 시스템 도입 검토

제1절 하이브리드 운영 원칙과 네트워크 제약 해결

양자내성암호 전환 과정에서는 시스템 특성, 상호운용성 요구, 국가 정책 및 관련 검증 기준 등을 고려하여 적절한 하이브리드 운영 방식을 선택할 필요가 있다. 본 절에서는 하이브리드 운영 방식을 하이브리드-AND 방식과 하이브리드-OR 방식으로 구분하고, 적용 시 고려해야 할 사항을 설명한다.

❶ 하이브리드-AND 방식과 하이브리드-OR 방식의 구분

양자내성암호로의 전환 과정에서는 기존 공개 키 암호와 양자내성암호를

함께 운용하거나 전환 과정의 상호운용성을 확보하기 위해 다양한 하이브리드 방식을 적용할 수 있다. 본 가이드북에서는 이를 하이브리드-AND 방식과 하이브리드-OR 방식으로 구분하며, 기관은 시스템 특성과 국가 정책 및 관련 검증 기준을 고려하여 적용 방식을 결정할 필요가 있다.

하이브리드-AND 방식은 둘 이상의 암호 알고리즘을 함께 적용하고 그 결과를 안전하게 결합하여 사용하는 방식이다. 키 설정의 경우에는 각 알고리즘에서 생성된 공유 비밀 등을 안전하게 결합하여 최종 키를 생성하는 방식으로 구현할 수 있다. 적절한 결합 방식이 적용된 경우 하나의 알고리즘에 예기치 않은 취약점이 발견되더라도 다른 알고리즘의 안전성을 기반으로 보호 수준을 유지할 수 있도록 설계할 수 있어, 전환 과정에서 폭넓게 검토되고 있다.

하이브리드-AND 방식은 결합하는 암호의 조합에 따라 PQ/T(Post-Quantum/Traditional) 방식과 PQ/PQ(Post-Quantum/Post-Quantum) 방식으로 구분할 수 있다. PQ/T 방식은 양자내성암호와 기존 공개 키 암호를 결합하는 방식으로, IETF의 RFC 10024에서는 TLS 1.3에서 ML-KEM과 ECDHE를 결합한 PQ/T 하이브리드 키 합의 방식을 규정하고 있다. PQ/PQ 방식은 둘 이상의 양자내성암호를 결합하는 방식이며, 알고리즘 간 공통 취약 가능성을 줄이기 위해 서로 다른 수학적 난제에 기반한 알고리즘의 조합을 고려할 수 있다. IETF의 RFC 9370에서는 IKEv2에서 복수의 키 교환 결과를 결합할 수 있는 메커니즘을 규정하고 있으며, 복수의 양자내성 키 교환을 사용하는 구성도 고려하고 있다.

이러한 국제 표준 사례는 하이브리드 방식의 기술적 구성과 적용 사례를 이해하기 위한 참고사항이며, 국가·공공기관의 구체적인 적용 방식은 국가 정책 및 관련 검증 기준에 따른다.

하이브리드-OR 방식은 시스템이나 통신 상대의 지원 여부 등에 따라 기존 공개 키 암호와 양자내성암호 중 하나를 선택하여 사용하는 방식이다. 기관 간 양자내성암호 전환 일정이 서로 다르거나 일부 시스템이 아직 양자내성암호를 지원하지 않는 경우에는 상호운용성을 확보하기 위한 과도기적 방식으로 활용할 수 있다. 다만 암호 협상 과정에 대한 보호가 충분하지 않으면 공격자가

양자내성암호를 지원하는 환경에서도 기존 공개 키 암호가 선택되도록 유도하는 다운그레이드(Downgrade) 공격이 발생할 수 있으므로, 암호 협상 과정의 무결성과 인증을 보장하는 등 적절한 안전조치를 마련해야 한다.

하이브리드-OR 방식의 적용 여부와 적용 기간은 시스템의 상호운용성 요구사항과 국가 정책 및 관련 검증 기준 등을 고려하여 결정한다.

하이브리드-AND 방식과 하이브리드-OR 방식은 둘 이상의 암호 알고리즘을 실제 암호기능에 어떻게 적용하거나 선택하는지에 관한 구분이다. 반면 병렬 PKI, 복합 인증서, 이중 인증서 등은 전자서명·인증을 구현하기 위한 인증서 및 전자서명 인증체계의 구성 방식으로, 하이브리드-AND 또는 하이브리드-OR과 동일한 분류 축은 아니다. 다만 실제 전자서명 생성·검증 과정에서 복수 알고리즘의 결과를 함께 요구하도록 구성하는 경우에는 하이브리드-AND 방식과 연계될 수 있으며, 시스템 또는 통신 상대의 지원 여부 등에 따라 하나의 방식을 선택하도록 구성하는 경우에는 하이브리드-OR 방식과 연계될 수 있다. 전자서명 인증체계의 구체적인 전환 고려사항은 5장 3절에서 다룬다.

하이브리드 운영의 전환 가이드라인

하이브리드 운영은 ① 국내외 암호 표준이 확정되고 안전성이 충분히 검증된 후, ② 국가 검증 단독 암호의 조달이 원활하며, ③ 상호 연동되는 관련 기관들의 전환이 완료되고, ④ 관계 감독 기관의 공식적인 지침 또는 가이드라인이 마련될 때까지 지속해서 유지하는 것이 바람직하다.

❷ 키/서명 크기 증가에 따른 IP 단편화 및 통신 지연 영향

양자내성암호는 기존 공개 키 암호에 비해 데이터 크기가 크게 설계되는 경향이 있다. 예를 들어, 기존 타원곡선 서명 대비 표준 격자 기반의 서명 데이터 용량은 수십 배 이상 커질 수 있으며, 이는 네트워크 통신 시 다음과 같은 지연이나 끊김을 유발할 수 있다.

■ IP 패킷 단편화 영향

IP 단편화(IP Fragmentation)란 전송하려는 IP 패킷의 크기가 통신 경로의 MTU(Maximum Transmission Unit)를 초과할 때 패킷이 여러 조각으로 분할되는 현상을 말한다.

■ 통신 불안정 현상 완화 방안

일부 구형 통신 장치나 보안 솔루션의 경우, 여러 TCP 세그먼트로 나뉘어 전달되는 데이터를 재조립하거나 처리하는 과정에서 후속 데이터를 정상적으로 처리하지 못하고 통신 연결을 비정상적으로 종료하는 등 오작동이 발생할 수 있다. 이를 완화하기 위해 다음 조치들을 고려할 수 있다.

- 네트워크 장비의 단편화된 IP 패킷 처리 설정을 확인하고 필요시 최적화한다.
- 네트워크 장비의 MSS(Maximum Segment Size: TCP 및 IP 헤더를 제외한 TCP 세그먼트의 최대 데이터 크기) 클램핑 설정을 점검하여 패킷 단편화 및 통신 장애 발생 가능성을 줄인다.
- VPN 통신(IPsec) 환경에서는 IKEv2 메시지 단편화(RFC 7383) 지원 여부를 확인하고, 양자내성암호 적용에 필요한 경우 중간 교환(RFC 9242) 및 다중 키 교환(RFC 9370)을 지원하는 장비의 도입을 검토한다.

실무 팁 : 대민 웹 서비스의 단말기 호환성 및 하향 안전 협상(Fallback) 구성

일반 시민들이 접속하는 대민 웹 서비스나 공공 웹 포털에 하이브리드 방식으로 양자내성암호를 도입할 경우, 오래된 브라우저나 이전 버전의 스마트폰 운영체제(OS)에서 호환성 문제로 접속이 제한되는 현상이 발생할 수 있다. 이를 완화하기 위해 양자내성암호를 지원하지 않는 구형 접속 기기와는 '하향 안전 협상(Safe Fallback Negotiation)'을 적용하여 기존의 안전한 암호 방식으로 연결할 수 있도록 서버 설정을 검토할 필요가 있다. 다만 기존 암호 방식으로 연결되는 구간에는 양자컴퓨터를 이용한 공격에 대한 위험이 남을 수 있으므로, 해당 연결의 적용 범위와 운영 현황을 관리하고 양자내성암호 지원 환경으로 점진적으로 전환할 필요가 있다.

❸ 주요 통신 규약 계층별 양자내성암호 적용 가이드

업무 성격에 따라 다양한 통신 규약의 적용 가능 규격을 파악해 두는 것이 유용하다.

[표 38] 주요 통신 규약별 양자내성암호 적용 가이드

통신 규약	양자내성암호 연계 표준 규격	실무적 주요 고려사항
TLS 1.3	하이브리드 규격 등	하이브리드 키 교환 그룹 활용 협상 검토
SSH	최신 버전 하이브리드 자체 적용 규격 등	업무 원격 관리 채널 대상 ; 공식 규격 동향을 파악하여 지원 단말 설정 추진
IPsec/IKEv2	하이브리드 키 교환 표준(RFC 9370 등)	VPN 게이트웨이 성능 검증 및 다중 키 교환 기능 지원 여부 검토
S/MIME	암호 구문 표준 등	전자우편 서명 및 암호화 ; 양자내성암호 기반 전자서명 · 암호화 지원 방식과 기존 인증체계와의 상호운용성 검토
DNSSEC	관련 표준 규격 드래프트 등	도메인 해석 서명 ; 향후 표준 확정 추이에 따라 점진적 대응 검토

제2절 암호 민첩성 확보 및 지속 관리 방안

양자내성암호 전환은 특정 알고리즘을 한 번 교체하는 것으로 끝나는 작업이 아니다. 향후 새로운 취약점이 발견되거나 암호 정책 · 표준 및 검증 기준이 변경될 수 있으므로, 기관은 필요한 암호 알고리즘과 관련 구성요소를 신속하고 일관되게 변경할 수 있는 암호 민첩성(Crypto Agility)을 확보할 필요가 있다. 이를 위해서는 기술적으로 암호기능을 유연하게 변경할 수 있는 구조뿐 아니라, 변경 필요성을 식별하고 영향 범위를 파악하여 적용 · 검증한 후 암호자산 현황을 다시 갱신하는 지속적인 관리 체계를 함께 마련해야 한다.

❶ 정책·프로세스·기술 기반의 암호 민첩성 확보

암호 민첩성은 소스코드에 특정 암호 알고리즘을 임의 고정 코딩(하드코딩)하지 않고, 필요에 따라 암호 알고리즘과 관련 구성요소를 유연하게 변경할 수 있도록 설계하는 것만을 의미하지는 않는다. 새로운 취약점이 발견되거나 암호 정책·검증 기준이 변경되었을 때 이를 신속히 인지하여 조직 내 의사결정 절차를 거쳐 일관되게 반영하고, 적용 시점(즉시 적용, 처리 중인 업무 완료 후 적용, 예정된 유지보수 시간에 적용 등)을 정하여 보안과 서비스 연속성을 유지하면서 변경을 실행할 수 있는 정책·프로세스·기술이 결합된 종합적인 역량을 의미한다.

영역	주요 고려 활동	세부 추진 예시
정책	유연한 지침 구성	– 내부 보안 규정에 특정 암호명 고정 표기 지양 – “검증된 기준 및 안전한 표준 암호 모듈 적용” 등의 문구 검토 – 새 표준 도입 시 검토 절차 및 승인 경로 명문화
절차	조달 및 관리 절차 연계 (4장 4절 참고)	– 제품 도입 시 소프트웨어 내 암호 부품 목록인 CBOM 제출 협의 – 취약점 패치 등 정기 보안 업데이트 제공 계약 조항 마련 고려 – 제품에 탑재된 암호가 표준에 부합하고 안정성이 검증되었는지 확인하는 절차 반영 – 도입 솔루션 공급업체의 양자내성암호 로드맵 점검 – 암호 정책·표준 변경이나 신규 취약점 발견 시 대응 기준과 절차 마련 – 변경 사항을 관련 부서와 연계 기관에 동시에 전파하고 이행 여부를 확인하는 변경관리 체계 구축
기술	소프트웨어 모듈화	– 소스코드 상에 특정 암호의 직접 호출 지양 – 암호 전용 라이브러리 연동 시 공통 인터페이스(API) 레이어를 이용한 결합도 완화 – 설정 파일 수정만으로 암호 파라미터가 변경되도록 구현 지향

실무 팁 : 암호모듈 검증제도(KCMVP) 대기 기간 중의 선제적 테스트 방안

신규 양자내성암호 기술에 대한 국내 공식 검증 체계(KCMVP 등) 시험 및 적격 절차 소요 기간 중에는, 실 가동용 운영 서버 대신 격리된 통합 테스트 환경을 구성하여 소프트웨어 정의(Software-defined) 기반의 암호 추상화 API를 시범 탑재하여 호환성 조율 여부를 우선 검증해 두는 것이 권장된다. 이를 통해 추후 정식 검증필 모듈 공급 시 기존 소프트웨어 전반의 교정 없이 모듈 교체(Plug-and-play)만으로 조기 배포를 마칠 수 있다.

❷ CBOM 기반 암호자산 변경 영향 식별 및 지속 관리

암호자산 인벤토리와 CBOM의 구축·관리 방법은 4장 2절에서 설명하였다. 5장 2절에서는 이를 암호 민첩성 확보를 위한 변경관리 수단으로 활용하는 데 초점을 둔다.

암호 정책·표준이나 검증 기준이 변경되거나 새로운 암호 취약점이 발견된 경우, 기관은 암호자산 인벤토리와 CBOM을 활용하여 해당 암호 알고리즘·라이브러리·인증서·키·프로토콜 등을 사용하는 시스템과 관련 구성요소를 식별하고 변경에 따른 영향 범위를 파악할 수 있다. 특히 CBOM과 같이 기계 판독 가능한 형식으로 암호자산과 구성요소 간의 관계를 관리하면 다수 시스템에서 변경 대상과 의존 관계를 보다 효율적으로 검색·추적하는 데 활용할 수 있다.

영향 범위를 확인한 후에는 변경 대상과 적용 시점을 결정하고, 시험·검증을 거쳐 운영 환경에 반영한 뒤 암호자산 인벤토리와 CBOM을 다시 갱신해야 한다. 이와 같이 암호자산의 식별부터 영향 분석, 변경, 검증 및 현행화까지의 절차를 반복적으로 수행함으로써 향후 새로운 암호체계로의 전환이나 긴급한 취약점 대응에도 신속하게 대응할 수 있는 기반을 확보할 수 있다.

다만 CBOM은 암호자산의 기술 정보를 구조화하여 관리하기 위한 수단이므로, 시스템의 업무 중요도, 공급업체 지원 계획, 교체 일정, 연계기관과의 전환 일정 등 운영·관리 정보는 별도로 관리하고 암호자산 정보와 연계하여 검토할 필요가 있다.

단계	주요 활동
변경요인 식별	암호 취약점, 정책·표준·검증 기준 변경 등 확인
영향범위 분석	암호자산 인벤토리·CBOM을 활용하여 영향받는 알고리즘, 라이브러리, 인증서, 프로토콜 및 시스템 식별
변경계획 수립	변경 대상, 적용 방식, 적용 시점 및 관계 시스템과의 의존 관계 검토
적용·검증	시험환경 검증 후 운영 환경에 변경 적용 및 정상 동작 확인
현행화	변경 결과를 암호자산 인벤토리·CBOM 및 관련 운영문서에 반영

제3절 전자서명 인증체계 전환 및 상호운용성

국가·공공기관의 전자서명 인증체계는 다수의 업무시스템, 대국민 서비스 및 기관 간 연계 시스템의 인증과 전자서명 검증에 활용되므로, 개별 기관의 단독 전환만으로는 전체 전환을 완료하기 어렵다. 따라서 상위 인증기관과 연계기관의 전환 일정, 인증서 체인 구성, 검증 시스템의 지원 여부 및 상호운용성을 함께 고려하여 전환을 추진할 필요가 있다.

특히 GPKI와 NPKI 등 상호연동 또는 교차인증 관계가 있는 인증체계에서는 루트·중간 CA와 크로스 인증서의 전환이 상대 인증체계와 이를 이용하는 응용시스템의 검증 환경에 영향을 줄 수 있으므로, 관련 기관 간 전환 방식과 일정, 크로스 인증서 갱신 및 사전 연동시험 등을 함께 조율할 필요가 있다.

❶ 루트 CA 전환과 병렬 PKI 구성·운영

루트 CA(최상위 인증기관)는 전자서명 인증체계의 최상위 신뢰점이므로, 루트 CA의 전자서명 알고리즘·키 및 인증서 변경은 중간 CA와 하위 인증서뿐 아니라 이를 검증하는 업무시스템과 단말에도 연쇄적인 영향을 미칠 수 있다. 따라서 상위 인증체계의 정책과 전환 일정에 따라 새로운 루트 CA 키 쌍과 인증서를 충분한 시차를 두고 준비하고, 하위 CA와 검증 시스템이 새로운 알고

리즘 및 인증서 형식을 지원하는지 확인한 후 새로운 신뢰앵커를 단계적으로 배포할 필요가 있다.

전환 과도기에는 기존 공개 키 암호 기반 인증서 체인과 양자내성암호 기반 인증서 체인을 병행하여 구성·운영하는 병렬 PKI(Parallel PKI)를 고려할 수 있다. 병렬 PKI는 서로 다른 암호체계를 사용하는 인증서 체인을 각각 유지하면서 전자서명·인증 프로토콜에서 이를 활용할 수 있도록 구성하는 방식이다. 이는 하이브리드-AND 또는 하이브리드-OR과 동일한 분류 개념은 아니며, 본 가이드북의 분류에 따르면 실제 전자서명 생성·검증 과정에서 두 인증체계의 인증서와 서명을 모두 요구하는지 또는 시스템·통신 상대의 지원 여부 등에 따라 하나를 선택하는지에 따라 하이브리드 방식과 연계될 수 있다. 구체적인 적용 방식은 관계 기관의 정책, 관련 표준 및 상위 인증체계의 전환 방식에 따라 결정할 필요가 있다.

❷ 양자내성암호 전환 시 인증서 구성 방식

전자서명 인증체계에서 기존 공개 키 암호와 양자내성암호를 함께 활용하기 위해서는 전자서명 알고리즘뿐 아니라 인증서와 인증서 체인의 구성 방식도 함께 고려해야 한다. 이를 위한 방식으로 하나의 인증서 또는 암호요소에서 복수의 공개 키와 서명 요소를 함께 처리하는 방식과, 기존 공개 키 암호 기반 인증서와 양자내성암호 기반 인증서를 각각 사용하는 복수 인증서 방식 등이 논의되고 있다.

복합(Composite) 방식은 복수의 암호 알고리즘에 해당하는 키 또는 서명 요소를 하나의 복합 암호요소로 구성하여 단일 인터페이스로 처리하는 방식이다. 이를 인증서와 전자서명에 적용하면 기존 공개 키 암호와 양자내성암호의 암호요소를 하나의 구조에서 함께 처리할 수 있다.

이중 인증서(Dual Certificate) 방식은 동일한 주체에 대해 기존 공개 키 암호용 인증서와 양자내성암호용 인증서를 각각 사용하여 인증을 수행하는 방식으로 제안되고 있다. 두 인증서 체인과 이에 대응하는 전자서명을 모두 검증

하도록 프로토콜을 구성하는 경우 하이브리드-AND 방식의 인증을 구현할 수 있다. 다만 이중 인증서를 사용하는 구체적인 프로토콜과 규격은 현재 표준화가 진행 중인 사항도 있으므로 관련 표준화 동향과 적용 대상 시스템의 지원 여부를 확인해야 한다.

복합 방식, 이중 인증서 및 병렬 PKI는 하이브리드-AND 또는 하이브리드-OR과 동일한 분류 개념은 아니다. 이들은 기존 공개 키 암호와 양자내성암호를 함께 사용하는 전자서명·인증을 구현하거나 운용하기 위한 구성 방식으로 활용될 수 있으며, 실제 적용되는 하이브리드 방식은 전자서명 생성·검증 정책과 적용 프로토콜에 따라 달라질 수 있다. 따라서 실제 적용 시에는 관계 기관의 정책, 관련 표준, 인증서 발급체계 및 검증 시스템의 지원 여부를 확인해야 한다.

⚠ 주의

복합 인증서, 이중 인증서 또는 새로운 전자서명 알고리즘을 적용한다고 해서 기존 인증서 검증 시스템과의 호환성이 자동으로 보장되는 것은 아니다. 기존 시스템이 새로운 인증서 형식, 알고리즘 식별정보, 확장 필드 또는 복수 인증서의 전달·검증 절차를 지원하지 못할 수 있으므로, 실제 적용 전에 관련 표준과 제품의 지원 여부를 확인하고 시험환경에서 인증서 발급·전달·체인 검증 및 상태 확인(CRL/OCSP) 절차가 정상적으로 동작하는지 검증할 필요가 있다.

❸ 양자내성암호 전환에 따른 인증서 폐기 기반 시설(CRL/OCSP) 고도화

새로운 전자서명 도입으로 패킷 크기가 증가함에 따라 인증서 상태 폐기 정보(CRL/OCSP) 배포 서버의 대역폭 및 연산 처리 능력에 대한 관리 방안이 요구된다.

[표 39] 인증서 폐기 기반시설(CRL/OCSP) 영향 및 완화 방안

구분	주요 영향 및 예상 특징	완화 방안 예시
CRL 데이터 크기	서명 크기 증가로 인한 CRL(인증서 폐기 목록) 배포 부하 증가 및 다운로드 지연 발생 가능성	세분화된 CRL(Delta CRL : 전체 폐기 명단이 아닌 최근 변경 내역만 수집한 부분 목록) 발행 주기 최적화 검토 ; 인증서 유효기간 단축을 통한 CRL 엔트리 누적 경감 검토

구분	주요 영향 및 예상 특징	완화 방안 예시
OCSP 검증 대기	서명 데이터 양 증가에 따른 연결 협상 지연 현상 우려	OCSP 스테이플링(Stapling : 클라이언트가 폐기 상태를 서버에 매번 실시간으로 확인하는 대신, 서버가 보증 영수증을 캐시로 보관했다가 클라이언트에 즉각 건네주어 속도를 높이는 기술)기법 활용 유도
OCSP 분산 처리	대민 트래픽 집중 시 연산 부하 완화 필요성	OCSP 응답 인프라의 다중화 구성 및 상태 데이터의 캐시 유지 시간(TTL) 조정 검토
구형 시스템과의 연계	구형 장치가 신규 서명 정보를 확인하지 못하는 현상	과도기 환경을 고려하여 기존 서명 체계와 병행 배포하는 이중 응답 지원 검토

제4절 공공 클라우드 환경의 양자내성암호 전환 고려사항

클라우드 컴퓨팅 서비스 도입 흐름에 발맞추어, 공유형 시스템 구조에 맞는 특화된 양자내성암호 전환 방안의 수립이 권장된다.

❶ 클라우드 서비스 유형별 양자내성암호 전환 전략

클라우드 환경에서의 양자내성암호 전환 전략은 서비스 모델에 따라 달라질 수 있다.

IaaS(Infrastructure as a Service) 환경에서는 가상 인스턴스 내부의 운영체제와 애플리케이션에 적용되는 암호 설정을 도입 기관이 직접 관리한다. 반면 네트워크, 가상화 계층 등 클라우드 기반 인프라의 양자내성암호 지원은 클라우드 서비스 제공자(CSP)에 의존하므로, 관련 표준 준수 여부와 지원 계획을 확인하고 계약이나 서비스 수준 협약(SLA) 등을 통해 지원 사항을 명확히 하는 것이 바람직하다.

PaaS(Platform as a Service) 환경에서는 플랫폼의 암호기능을 서비스 제공자가 관리하므로, 제공사의 양자내성암호 지원 로드맵과 적용 일정을 사전에 확인해야

한다. 필요한 경우에는 플랫폼이 양자내성암호를 지원할 때까지 자체 보안 프록시 등을 활용하여 암호기능을 보완하는 방안을 검토할 수 있다.

SaaS(Software as a Service) 환경에서는 사용자가 암호기능을 직접 변경하기 어렵기 때문에, 서비스 도입 또는 조달 단계에서 양자내성암호 지원 계획을 확인하는 것이 중요하다. 또한 암호자산 명세(CBOM 등)의 정기적인 제공 및 갱신을 요구하고, 양자내성암호 전환과 관련된 보안 요구사항을 계약 및 조달 문서에 반영하는 것이 권장된다.

❷ 클라우드 HSM 및 키 관리 요구사항

클라우드 기반 키 관리 환경에서는 HSM-as-a-Service(Hardware Security Module as a Service)의 보안성을 우선적으로 확인해야 한다. 서비스가 요구되는 보안 인증 및 관련 규격을 충족하는지 검증하고, 암호 키의 생성, 저장 및 활용이 HSM의 안전한 보안 경계 내부에서 수행되도록 구성하는 것이 바람직하다. 이를 통해 암호 키가 외부 환경에 노출될 위험을 최소화할 수 있다.

또한 여러 기관이나 사용자가 동일한 클라우드 인프라를 공유하는 다중 임차(Multi-tenant) 환경에서는 테넌트 간 격리가 충분히 보장되어야 한다. 이를 위해 동일한 HSM이나 하드웨어를 공유하더라도 암호학적 파티션(Cryptographic Partition)과 같은 논리적 격리 기술을 활용하여 각 기관의 암호 키와 암호 연산이 서로 독립된 보안 영역에서 수행되도록 구성하는 것이 권장된다.

❸ 클라우드 네이티브 환경 양자내성암호 적용

컨테이너 및 클라우드 네이티브 환경에서는 서비스 간 통신과 소프트웨어 공급망 전반에 걸쳐 양자내성암호 적용 여부를 점검해야 한다.

먼저 서비스 메시(Service Mesh) 환경에서는 클러스터 내부 서비스 간 통신에 사용되는 상호 인증 기반의 TLS(mTLS, Mutual TLS)가 양자내성암호를 지원하는지 확인하고, 이를 처리하는 사이드카 프록시 및 관련 구성요소가 최신 버전으로 유지되고 있는지 점검하는 것이 필요하다. 이를 통해 내부 서비스 간

통신에서도 양자내성암호 기반의 보안성을 확보할 수 있다.

또한 컨테이너 이미지의 배포 과정에서는 이미지 서명 및 검증 체계가 양자내성암호를 지원하는지 확인하는 것이 중요하다. 이미지에 대한 서명 생성과 검증에 사용되는 도구가 안전한 양자내성암호를 적용하도록 구성함으로써, 이미지의 위·변조를 방지하고 소프트웨어 공급망의 무결성과 신뢰성을 강화하는 방안을 검토하는 것이 바람직하다.

제5절 기존 시스템(레거시) 및 하드웨어(HSM/보안장비) 처리 전략

성능이나 연산 자원이 부족한 일부 레거시 서버나 노후 기기(스마트카드, 소형 제어반 등)의 경우, 대규모 양자내성암호 키 정보를 내부적으로 신속하게 처리하기 어렵다.

❶ 암호학적 격리 및 터널링(tunneling & proxy) 전략 및 상세 설계 구조 구성

운영체제(OS) 지원이 만료되었거나 내장 암호 칩셋의 변경이 불가능한 시스템의 경우, 장비를 전면 개편하는 대신 프록시 게이트웨이를 전면에 두어 보호하는 하드랩(Hard-wrapping) 방식을 검토할 수 있다.

쉽게 이해하기 : 암호 보호막 씌우기

내부 암호기능 갱신이 불가능한 구형 컴퓨터 장치(레거시)의 앞단에 양자내성 보안 능력을 지닌 대행 서버(프록시 게이트웨이)를 방어막으로 배치하는 설계이다. 외부 통신은 이 대행 서버가 양자내성암호로 엄격하게 방어하고, 대행 서버부터 뒤쪽 내부 레거시 컴퓨터까지의 로컬 영역은 물리적으로 안전하게 분리된 전용 통로(터널)로 연결하여 중계하는 방식으로 동작한다.

❷ 하드웨어 수명주기를 고려한 단계적 교체 및 폐기(retirement)

제조사 지원 종료 시점이 다가오는 노후 핵심 기반 시설은 무리하게 업그

레이드를 고집하기보다, 정기 교체 주기에 맞추어 양자내성암호가 기본 지원되는 신형 제품을 조달하는 계획이 경제적일 수 있다. 수명이 매우 긴 핵심 제어 장비 등은 별도의 중장기 전환 예산 항목으로 분리하여 순차적으로 전환하는 것을 고려할 수 있다.

기기 교체 가이드라인

장비 교체가 즉시 불가능할 때는 잔여 수명 기간에 프록시 격리를 적용하고, 교체 시점에 맞춰 조달 스펙에 양자내성암호 요건을 반영하는 것이 비용 효율적이다.

제6절 IoT·OT·ICS 시스템의 양자내성암호 전환 특수 전략

산업용 제어망(상하수도, 전력, 원격 제어 장치 등)은 통신 대역폭 제한과 물리적 접근성 한계 등 일반 정보통신 인프라와 다른 환경을 갖추고 있으므로, 환경 특성을 반영한 우회 전략 수립이 권장된다.

❶ IoT/OT 환경의 양자내성암호 전환 핵심 과제

IoT/OT 환경은 제한된 하드웨어 자원, 장기간 운영, 폐쇄망 구조, 산업용 프로토콜 등 일반 정보시스템과는 다른 특성을 갖는다. 따라서 양자내성암호 전환 시에는 이러한 환경적 특성을 충분히 고려하여 단계적인 전환 계획을 수립해야 한다. 다음은 IoT/OT 환경에서 우선적으로 검토해야 할 핵심 과제와 주요 영향, 그리고 대표적인 보완 사항을 정리한 것이다.

[표 40] IoT·OT 환경에서의 전환 핵심 과제 및 보완 방안

해결 과제	주요 영향과 특징	해당 환경·장비 예시
하드웨어 제약	소형 칩셋의 메모리 제한으로 고연산 암호 처리에 걸림돌이 생길 가능성	스마트 기기 및 저전력 센서 등

해결 과제	주요 영향과 특징	해당 환경 · 장비 예시
업데이트 접근 제약	설치 위치에 따른 물리적 원격 펌웨어 갱신의 어려움	지하 설치 센서 등
긴 작동 기간	장비 노후화와 무관하게 10년 이상 연속 운용 설계된 경우	기반 시설 내 제어 유닛
프로토콜 상이성	산업 전용 프로토콜의 표준 업데이트 진행 속도 조율 필요성	주요 공장 및 SCADA망
물리적 차단 환경	폐쇄망 구조로 외부 노출 가능성은 낮으나 보안 채널은 유지 필요	망 간 연동 게이트웨이

❷ IoT/OT 환경별 맞춤 대응 전략

IoT/OT 환경에서는 장치의 성능과 운영 특성을 고려한 맞춤형 전환 전략을 수립하는 것이 중요하다. 먼저 메모리와 연산 자원이 제한된 장치의 경우에는 저용량 양자내성암호의 적용을 검토할 수 있다. 예를 들어, 메모리 사용량이 적은 서명이나 전송 데이터 크기를 최소화하도록 설계된 암호를 활용하면 장치의 성능 저하와 통신 지연을 줄일 수 있다. 다만 이러한 암호는 국내외 표준화 및 안전성 검증이 완료된 이후 적용하는 것이 바람직하다.

또한 자체적으로 양자내성암호를 지원하기 어려운 레거시 장비는 양자내성암호 프록시 게이트웨이를 활용하는 방안을 고려할 수 있다. 장비 외부에 게이트웨이를 배치하여 암호 연산을 전담하도록 하면 기존 장비를 교체하지 않고도 양자내성암호 기반의 통신 환경을 단계적으로 구축할 수 있다.

아울러 IoT/OT 장비는 일반적으로 5~10년 이상의 긴 수명주기를 갖는 경우가 많으므로, 양자내성암호 전환 계획을 장비의 교체 및 조달 계획과 연계하여 수립하는 것이 중요하다. 신규 장비를 도입하거나 규격서를 작성할 때에는 양자내성암호 지원 여부를 평가 항목 또는 가점 요소에 반영함으로써 장치 교체 주기와 양자내성암호 전환 일정을 함께 고려하는 것이 권장된다.

❸ OT/ICS 망 양자내성암호 전환 설계 구조

OT/ICS 환경에서의 양자내성암호 전환은 모든 시스템을 동시에 교체하기보다, 외부 네트워크와 연결되는 구간부터 현장 장비까지 계층적으로 적용하는 것이 바람직하다. 특히 연산 성능과 메모리가 제한된 현장 장비는 즉시 교체하기 어려운 경우가 많으므로, 네트워크 경계 구간부터 우선적으로 양자내성암호를 적용하고 장비 교체 주기에 맞추어 단계적으로 확대하는 전략이 권장된다.

먼저 기업망과 외부 인터넷이 연결되는 구간에서는 양자내성암호를 적용한 TLS 1.3 기반의 보안 통신을 구축하여 외부와의 통신을 보호한다. 다음으로 망 연동 게이트웨이에서는 양자내성암호를 지원하지 않는 기존 OT 장비를 위해 프록시 기능을 제공하여 암호 연산을 대신 수행하도록 구성할 수 있다.

제어국 관리 네트워크에서는 기존 공개 키 암호와 양자내성암호를 함께 사용하는 하이브리드 기반의 VPN을 적용하여 관리 구간의 통신을 보호하고, 이후 산업용 방화벽을 통해 IT 영역과 OT 영역 간의 접근을 통제한다.

마지막으로 프로세스 제어 영역에서는 장비 특성에 맞는 경량 또는 안전 채널을 구성하고, 현장 계측 장비는 서명 검증 기반의 안전한 펌웨어 업데이트를 지원하도록 설계하는 것이 바람직하다. 양자내성암호를 직접 지원하기 어려운 장비는 프록시 게이트웨이를 활용하여 보호하고, 장비 교체 시점에 맞추어 양자내성암호를 지원하는 장비로 순차적으로 전환하는 전략을 적용하는 것이 효과적이다.

제7절 데이터 전환과 장기보존 데이터의 무결성·진본성 보존

공공기관이 보유한 일부 중요 정보나 공문서 아카이브 등은 보존이 요구되는 기간이 매우 길다. 안전성 유지 기간을 분석하여 필요시 조기에 보호 조치를 수립하는 계획을 검토할 필요가 있다.

❶ 저장 데이터(data-at-rest)의 재암호화 계획

기존 공개 키 암호 기반으로 기밀성이 유지되던 장기 보관 아카이브 파일은 암호 키 경로가 향후 취약해질 우려를 대비해, 순차적으로 양자내성암호 규격을 적용하여 재암호화하는 방안의 수립이 권장된다.

대용량 파일의 재암호화 계획 수립 시, 보안장비의 처리 한도와 유휴 시간 등을 사전에 계산하여 전체 소요 기간을 추정하는 것이 권장된다.

[표 41] 저장 데이터의 재암호화 4단계 절차 예시

단계		주요 활동 내용	유의 사항 및 관리 지침
1	복호화	기존 공개 키 암호 키를 사용하여 데이터를 일시 복원	복호화 작업은 안전이 통제된 내부 영역에서 수행하는 것이 권장되며, 노출을 최소화할 필요가 있다.
2	재암호화	새로운 양자내성암호 규격을 준수하여 암호 키 재생성 및 재암호화	사용할 암호 키는 국내외 검증필 암호모듈을 통해 생성하는 것이 바람직하며, 대용량 처리는 야간 또는 유휴 시간 일괄 처리(batch)를 활용할 수 있다.
3	일치성 검증	복원 테스트 및 원본 해시값 비교 확인	데이터 규모에 따라 전수 검증 또는 표본 샘플링 및 메타데이터 대조 방식을 선택적으로 활용할 수 있다.
4	원본 소거	기존 암호화 파일의 잔재 소거	국내외 폐기 기준에 맞춰 미디어 소거를 수행하고, 삭제 전 데이터 정상 복원 여부를 미리 확인해 보는 것이 바람직하다.

❷ 전자문서 진본성 유지 및 양자내성암호 기반 중복서명(over-signing)

기존 서명의 안전 수명이 끝나기 전에 기존 서명에 양자내성암호 기반의 새로운 전자서명을 추가하는 중복서명(Over-signing)을 통해 문서의 진본성과 무결성을 장기간 입증하는 방안을 고려할 수 있다.

또한 장기 유효성 검증(Long-Term Validation, LTV)을 지원하기 위해 인증서, 인증서 폐기 상태정보, 타임스탬프 등 필요한 검증정보를 확보·보존하고, 관련 기술 표준의 검토와 주기적인 타임스탬프 갱신 등을 통해 전자서명의 장기적인 검증 가능성을 유지할 필요가 있다.

쉽게 이해하기 : 공문서 공증 도장 겹쳐 찍기

시간이 지나 기존 도장의 인장이 위조될 위험이 생기기 전에, 그 위에 새로운 국가 공인 인장(양자내성 서명)을 추가로 겹쳐 찍어 문서가 진짜임을 계속 입증하는 기법이다.

제8절 체크리스트 : 전환 시 주요 고려사항

※ 본 체크리스트는 예시이며, 기관의 시스템·서비스 운영 현황에 맞지 않는 문항(표)은 삭제하고 필요한 문항은 추가하여 사용한다.

확인		내용	날짜
기존 장비 및 레거시	□	자산 현황을 파악하고 시스템별 잔여 보안 수명과 전환 순위를 기재한 대장을 관리하는 절차를 수립하였다.	
	□	단독 업그레이드가 어려운 장치(HSM, 토큰 등)를 식별하고 우회 격리(프록시 등) 처리 방안을 검토하였다. ※ 해당 장비를 외부 통신에 직접 노출하지 않고 양자내성암호를 지원하는 프록시·게이트웨이를 앞단에 배치하거나 별도 구간으로 격리하는 방안을 검토	
	□	현장 OT 장치들의 외부 네트워크 노출 빈도를 최소화하고 경계 게이트웨이 단계부터 전환해 나가는 설계 구조를 점검하였다. ※ 예시 : 신규 장비 교체가 어려운 현장 OT 장치는 자체 지원이 어려운 경우 프록시 게이트웨이를 활용해 암호 연산을 대신 수행하도록 하고, 외부와 연결되는 경계 게이트웨이부터 우선 전환하여 노출 빈도가 높은 지점을 먼저 보호	
데이터 이전 및 무결성	□	장기 기밀 유지가 필요한 자산을 분류하고 안전 수명이 충분한지 검토하였다.	
	□	영구 또는 준영구 문서의 법적 진본성을 보호하기 위해 양자내성 중복 서명 절차 적용 가능 여부를 파악하였다.	
	□	※ 중복서명 : 기존 전자서명의 안전성이 약화되기 전에 새로운 전자서명을 추가하여, 장기간 보존되는 전자문서의 진본성과 서명 검증 가능성을 계속 유지하는 방식	

확인		내용	날짜
신뢰 체계 및 연동	□	인증서 체계 전환 로드맵을 공유받고, 병렬 전자서명 인증체계 또는 복합 인증서 규격 적용을 대비하였다. ※ 병렬 전자서명 인증체계는 기존 인증체계와 양자내성암호 기반 인증체계를 일정 기간 함께 운영하는 방식이며, 복합 인증서는 기존 공개키 암호와 양자내성암호 관련 키·서명 정보를 하나의 인증서 구조에서 함께 활용하기 위한 방식	
	□	다수 기관 연결 구간의 병목이나 통신 두절을 예방하기 위한 사전 호환 테스트 일정을 조율 중이다.	
	□	키 데이터 용량 증가로 인한 인증서 상태 확인 기반 시설(CRL/OCSP) 부하 경감 조치(스테이플링 등)를 마련하였다. ※ CRL/OCSP는 인증서의 폐기 여부를 확인하기 위한 방식이며, 인증서·서명 데이터 증가로 조회 및 응답 부하가 커질 수 있으므로 캐싱, OCSP Stapling 등 부하 완화 방안을 함께 검토	
운영 및 서비스 연속성	□	실제 운영망 적용 전에 검증용 시험망을 가동하여 연산 부하 및 지연 요소를 실측하였다.	
	□	점진적 시범(Canary) 배포 및 이상 현상 감지 시 신속하게 복원할 수 있는 원상 복구 대응 절차서를 확보하고 있다. ※ Canary 배포 : 전체 시스템에 일괄 적용하기 전에 일부 사용자·서버·트래픽에 먼저 적용하여 성능과 장애 여부를 확인한 뒤, 문제가 없으면 적용 범위를 단계적으로 확대하는 방식	
하이브리드 결합 및 망 환경	□	안정성 확보 수준을 고려하여 하이브리드 방식이 지원되는지 확인하였다.	
	□	양자내성암호 적용에 따른 패킷 크기 증가로 인한 통신 오류를 방지하기 위해 MTU·MSS 설정과 방화벽·게이트웨이의 단편화 패킷 처리 설정을 확인하였다. ※ 양자내성암호 적용으로 키·서명·인증서 데이터가 커지면 MTU 초과에 따른 IP 단편화 등이 발생할 수 있으므로, MTU·MSS 등 패킷 크기 관련 설정과 방화벽·게이트웨이의 단편화 패킷 처리 가능 여부를 확인	
	□	사용 중인 주요 통신·메시징 서비스(SSH, VPN, S/MIME 등)의 하이브리드 방식 지원 여부를 확인하고, 관련 장비·소프트웨어의 적용 일정을 수립하였다.	

확인		내용	날짜
하이브리드 결합 및 망 환경	□	※ SSH · VPN 등은 하이브리드 키 교환 지원 여부를, S/MIME 등은 하이브리드 암호화 · 전자서명 및 관련 인증서 지원 여부를 서비스 특성에 따라 구분하여 확인	
암호 민첩성 확보	□	도입 예정 솔루션의 RFP 작성 시 CBOM 제출 요구 및 양자안전 업데이트 조항 추가 가능성을 확인하였는가?(5장 2절 ❶, 5장 2절 ❷) ※ CBOM(Cryptographic Bill of Materials) : 제품 · 소프트웨어에서 사용하는 암호 알고리즘, 라이브러리, 인증서, 키 등의 정보를 정리한 암호 자산 명세서	
	□	소스코드 변경을 최소화하고 암호 모듈을 유연하게 스위칭할 수 있는 인터페이스(API) 설계 구조를 설계하였다.	
위험 관리	□	전환에 따르는 5가지 주요 위험 요인 완화 계획이 위험 관리 프로세스에 조화롭게 포함되어 있다. ※ 5가지 주요 위험 요인 : ①네트워크 성능 지연, ②구현 단계의 보안 취약성, ③공급망 제품의 전환 지연, ④표준 사양 조정, ⑤기술 전문성 부족(5장 도입부 참조)	
IoT 및 OT 환경	□	보유 단말 기기들을 연산 자원 및 펌웨어 갱신 가능성 유무별로 분류하고 특성에 맞는 전환 계획을 마련하였다. ※ 예시 : 메모리 · CPU가 충분하고 펌웨어 업데이트가 가능한 장치는 소프트웨어 방식의 전환을 검토하고, 자원이 부족하거나 업데이트가 불가능한 장치는 교체 · 격리 · 게이트웨이 보완 등의 방안을 마련	
	□	신규 IoT/OT 장치 조달 명세에 양자내성암호 요구사항을 포함하였다.	
키 캡슐화 구현 적합성	□	양자내성 키 캡슐화 구현체가 표준 규격을 준수하고 국내외 검증 체계(KCMVP 등)를 획득한 제품인지 검토하였다.	
	□	사용된 임시 키쌍이 단일 세션으로 제한되고 세션 종료 후 안전하게 소멸시켰다.	
	□	암호 연산 수행 시 발생하는 중간 값들이 메모리에서 지체 없이 소거되었다.	

확인		내용	날짜
키 캡슐화 구현 적합성	□	하이브리드 구성 시 키 결합에 안전한 키 유도 함수(KDF)가 적용되었다. ※ KDF(Key Derivation Function) : 하나 이상의 비밀값을 입력받아 실제 통신에 사용할 키를 안전하게 생성하는 함수로, 하이브리드 구성에서는 각 알고리즘에서 얻은 값을 안전하게 결합하는 데 활용	
공공 클라우드	□	CSP와의 계약에 양자내성암호 지원 의무화 및 CBOM 제출 조항을 포함하였다.	
	□	클라우드 HSM 서비스가 적용 환경에서 요구되는 암호모듈 검증 요건을 충족하고, 적용하려는 양자내성암호의 키 생성 · 저장 · 연산 기능을 지원하는지 확인하였다.	
	□	컨테이너 이미지 서명(Sigstore/Cosign) 및 서비스 메시(mTLS)에 양자내성암호 전환 계획을 수립하였다. ※ 컨테이너 환경에서는 이미지의 출처 · 무결성 확인을 위한 전자서명과 서비스 간 상호인증(mTLS)에 공개 키 암호가 사용될 수 있으므로, 관련 알고리즘 · 인증서 · 키와 사용 중인 도구 · 플랫폼의 양자내성암호 지원 여부 및 적용 가능 시점을 확인	
성숙도 평가	□	기관 자체 양자내성암호 대응 역량을 점검하고 로드맵상 향후 목표 단계를 검토하였다. ※ 대응 역량 : 암호자산 식별 · 관리, 전환 계획 수립, 기술 적용 · 검증, 전문인력 확보, 공급업체 · 관계 기관 협력 등 양자내성암호 전환을 자체적으로 계획 · 추진 · 관리할 수 있는 기관의 준비 수준	
	□	관계 부처 및 감독 기관의 안내에 따라 관련 상황을 주기적으로 점검하고 보고할 수 있는 프로세스를 구축 중이다.	

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



Chapter 06

전환 이행 방향과 향후 과제

Chapter
06

전환 이행 방향과 향후 과제

본 장에서는 국가·공공기관의 성공적인 양자내성암호 전환을 지원하기 위해 실무적 관점에서의 실천적 출발점과 핵심 성공 요인을 먼저 제시한다. 아울러 중장기 이행 방향과 국내외 표준화 동향을 살펴보고, 각 기관이 전환 진행 상황을 자체적으로 점검할 수 있도록 성숙도 단계와 정량적 평가지표를 제시한다. 이를 통해 향후 가이드북 개정이나 국가 정책 변화에도 기관이 전환 수준을 지속적으로 점검하고 보완할 수 있도록 한다.

제1절 실천적 출발점과 핵심 성공 요인

양자내성암호 전환은 CRQC가 실제 등장한 이후에 시작할 수 있는 단기적인 작업이 아니다. 기관이 운용하는 정보시스템의 암호자산을 식별하고, 전환 우선순위를 설정한 뒤 제품·서비스의 지원 여부를 확인하고 실제 시스템에 적용하기까지는 상당한 준비와 이행 기간이 필요하다. 또한 장기간 기밀성을 유지해야 하는 정보는 현재 수집된 암호문을 저장해 두었다가 향후 해독하는 HNDL(Harvest Now, Decrypt Later) 공격 가능성도 고려해야 한다. 따라서 기관은 현재부터 전환에 필요한 준비를 단계적으로 추진할 필요가 있다. 이러한 관점에서 기관이 양자내성암호 전환을 준비하고 추진하는 과정에서 우선적으로 고려해야 할 3대 주요 사항을 다음과 같이 정리하였다.

1. 암호 민첩성(Crypto Agility) 우선

양자내성암호 전환은 특정 알고리즘을 일회성으로 적용하는 데 그치지 않고,

향후 새로운 취약점의 발견이나 암호 정책·검증 기준의 변경 등에 지속적으로 대응할 수 있도록 추진해야 한다. 이를 위해서는 암호 알고리즘과 키·인증서 등의 변경이 용이하도록 시스템을 설계하는 것뿐만 아니라, 변경된 암호 정책을 시스템에 신속하게 반영하고 전환 과정에서도 서비스의 연속성과 상호운용성을 유지할 수 있는 기술적·운영적 체계를 함께 갖출 필요가 있다. 이러한 암호 민첩성을 확보하면 향후 암호체계의 변경이 필요한 경우에도 시스템에 미치는 영향을 줄이면서 보다 유연하게 대응할 수 있다.

2. 하이브리드 방식으로 전환 위험 요인 관리

양자내성암호 전환 과정에서는 제품·서비스의 지원 수준과 기존 시스템과의 상호운용성 등을 고려하여 전환 위험을 관리해야 한다. 하이브리드 방식은 이러한 전환 과정의 불확실성에 대응하기 위한 방안으로 활용할 수 있다.

3. 공급망과 연계 기관 협조

공공기관 단독의 양자내성암호 전환만으로는 충분하지 않다. 행정전자서명 인증체계(GPKI)의 양자내성암호 전환을 위해서는 상위 인증기관(CA)의 정책과 전환 일정에 맞춰 기관 인증서 발급·검증 체계 및 인증서 체인 전체의 신뢰성을 함께 고려해야 한다. 또한 연계 기관의 전환이 동반되어야 다기관 시스템이 정상적으로 작동할 수 있으므로, 범정부 조정 체계 안에서 협력적으로 전환을 추진해야 한다.

오늘 할 수 있는 일	기관의 외부 노출 TLS 서버 목록을 작성하고, OpenSSL 버전, 지원 암호 스위트(Cipher Suite), 지원 키 교환 그룹(supported_groups) 및 실제 연결에서 협상된 키 교환 그룹을 확인한다.
이번 달 할 일	주요 시스템의 암호자산 인벤토리(CBOM) 초안을 작성하고, 기밀성 보호 기간 10년 이상 데이터를 식별한다.
올해 할 일	양자내성암호 전환 전담반(TF)을 구성하고, 위험 평가 기준표를 기반으로 우선순위를 산정하여 기관 로드맵을 확정한다.

제2절 중장기 이행 로드맵과 표준화 대응

국가정보원은 양자내성암호연구단(KpqC연구단)의 공모전 최종 4종 암호 – 키 캡슐화 분야의 SMAUG-T, NTRU+, 전자서명 분야의 HAETAE, AIMer – 를 확정 발표하였다. 향후 KpqC 알고리즘이 KS 표준으로 최종 고시되면 다음 갱신판에서 본 가이드북에 구체적인 적용 지침을 추가할 예정이다.

관련 검증제도의 일정도 구체화되고 있다. 국가정보원은 2026년 9월 1일 양자내성암호 검증대상 후보군 및 향후 추진 일정을 공개하였다[6]. KpqC 키 캡슐화 알고리즘의 KS 표준화는 2026년 12월 완료될 것으로 예상되며, 국가정보원은 키 캡슐화 분야의 검증대상 알고리즘을 2027년 1월 선정한 후 2028년 1월부터 KCMVP 암호모듈 검증제도를 시행할 예정이다. 검증 시행 시에는 하이브리드 방식을 필수로 구현하도록 하고 있으며, 키 캡슐화 분야는 2029년 1월부터 해당 기능이 포함된 암호모듈에 양자내성 키 캡슐화 알고리즘 탑재를 의무화할 예정이다. 각 기관은 이러한 일정을 고려하여 검증필 암호모듈 및 이를 적용한 제품의 확보 가능 시점을 전환 계획에 반영해야 한다.

제3절 양자내성암호 전환 완료 기준 및 성숙도 측정 체계

양자내성암호 전환의 진행 상황을 객관적으로 측정하고 감독기관에 증빙하기 위한 방안으로 정량적 완료 기준과 성숙도 모델을 활용할 수 있다. 아래의 지표들은 각 기관이 양자내성암호 전환 사업의 실무적인 달성 성과를 정량적으로 증빙하고 상시 관측하기 위해 활용할 수 있는 참고용 예시이다. 각 기관은 본 예시를 기반으로 기관의 보안 규정, 예산 규모, 전산망 환경에 맞추어 지표와 목표치를 유연하게 조정하여 관리하는 방안을 고려할 수 있다.

핵심 지표(KPI)	최종 목표치(예시)	측정 방법
양자내성암호 지원 TLS 연결 비율	≥ 95%	네트워크 장비 세션 통계
신규 양자내성 서명 인증서 발급 비율	≥ 90%	CA 발급 로그

핵심 지표(KPI)	최종 목표치(예시)	측정 방법
CBOM 제출 완료 시스템 비율	100% (계약 체결 시스템)	암호자산 인벤토리 DB
암호 민첩성 적용 시스템 비율	≥ 80%	코드 감사 결과
양자내성암호 전환 불가 레거시 잔존 시스템 수	0(목표 연도 기준)	암호자산 인벤토리

아래 5단계 성숙도 모델을 기준으로 기관의 현재 위치를 자가 진단하고, 관계 부처 및 감독 기관의 안내에 따른 성숙도 단계 측정 체계와 연동하는 방안을 고려할 수 있다.

단계	명칭	달성 기준
1	인식 (Aware)	양자내성암호 전환 필요성 인지, 암호자산 인벤토리 초안구축 완료(주요 시스템 대상, 범위 약 70% 이상), 위협 평가 수행 등
2	계획 (Planned)	암호자산 인벤토리 보완(전수 조사 완료 권장) 및 CBOM 연동, 양자내성암호 전환 로드맵 수립, 예산 및 조달 계획 반영, 주요 의사결정 단계 도달 등
3	전환 중 (Transitioning)	하이브리드 양자내성암호 시험 적용, 시험 환경 검증, 점진적 시범 배포 실시 등
4	전환 완료 (Transitioned)	전체 시스템 하이브리드 양자내성암호 전환 수행, 기존 시스템 격리 또는 대체 완료 등
5	민첩 (Agile)	유연한 암호 민첩성 설계 구조 구현, CBOM 자동화 연동, 암호 교체 역량 확보, 자동화된 모니터링 운영 등

기관은 양자내성암호 전환 현황을 체계적으로 관리하고 관계 감독 기관과의 협력을 강화하기 위해 성숙도 단계와 전환 완료 지표의 달성 현황을 주기적으로 공유하는 체계를 마련하는 것이 바람직하다. 이를 통해 기관별 전환 진행 상황을 객관적으로 점검하고, 전환 과정에서 필요한 지원과 협조를 효과적으로 받을 수 있다.

우선 관계 감독 기관의 지침에 따라 기관별 성숙도 수준과 주요 전환 지표의 달성 현황을 정기적으로 보고하고 공유하는 방안을 검토할 수 있다. 또한 특정

양자내성암호의 결함이나 취약점이 발견되는 경우에는 암호자산 명세(CBOM)를 활용하여 해당 암호의 사용 현황을 신속하게 파악하고, 영향 범위를 분석하여 필요한 보안 조치를 즉시 수행할 수 있는 대응 체계를 갖추는 것이 중요하다.

아울러 전환 과정에서 생성되는 다양한 산출물은 성숙도 평가와 전환 이행의 객관적인 증빙 자료로 활용할 수 있다. 대표적인 예로는 암호자산 점검 보고서, CBOM 목록, 시험 환경에서의 성능 측정 결과, 점진적 배포 이력, 인증서 발급 및 운영 현황 등이 있으며, 이러한 자료를 지속적으로 관리함으로써 전환 현황을 체계적으로 추적하고 향후 감사나 점검에도 효과적으로 대응할 수 있다.

제4절 양자내성암호 전환은 미래가 아닌 현재의 과제

양자컴퓨터의 발전은 공개 키 암호 기반의 디지털 신뢰 체계에 근본적인 변화를 요구하고 있다. 양자내성암호로의 전환은 단순히 새로운 암호를 도입하는 기술적 변경이 아니라, 암호자산의 식별, 시스템 구조의 개선, 상호운용성 확보, 공급망 관리, 운영 체계 정비를 포함하는 장기적인 전환 과정이다.

특히 기관별 전환 일정과 기술 성숙도는 서로 다를 수 있으므로, 모든 시스템을 한 번에 교체하기보다 위험도를 고려한 우선순위를 설정하고 단계적으로 전환을 추진하는 것이 중요하다. 또한 관계 기관, 서비스 제공자, 공급업체와 긴밀히 협력하여 전환 계획을 수립하고, 표준화와 기술 동향을 지속적으로 반영함으로써 안정적인 전환을 달성해야 한다.

본 가이드북은 기관이 양자내성암호 전환을 준비하고 추진하는 과정에서 고려해야 할 주요 사항과 실무적인 대응 방안을 제시하였다. 마지막으로 다음 표에 제시한 '가이드북 핵심 메시지 5가지'는 전환 과정에서 반드시 기억해야 할 핵심 원칙을 요약한 것으로, 기관의 전환 계획을 수립하고 이행하는 과정에서 지속적으로 참고하기를 권장한다.

[표 42] 본 가이드북의 핵심 메시지 5가지

본 가이드북 핵심 메시지 – 5가지 기억할 것	
1	**지금부터 준비하라.** – HNDL 공격은 양자컴퓨터 없이도 현재 진행 중이다. – 장기간 보호가 필요한 정보는 보호 기간과 전환 소요 기간을 고려하여 우선적으로 전환을 준비한다.
2	**하이브리드 방식을 활용하라.** – 전환 과정의 불확실성과 상호운용성 문제에 대응하기 위해 국가 정책 및 관련 검증 기준에 따라 적절한 하이브리드 방식을 적용한다
3	**암호 민첩성이 핵심이다.** – 향후 취약점 발견이나 암호 정책·검증 기준의 변경에 유연하게 대응할 수 있는 기술적·운영적 역량을 갖춘다. – 임의 고정 코딩(하드코딩)은 미래의 부채다.
4	**혼자서는 할 수 없다.** – 공통 인프라, 연계기관, 공급업체 등 관련 주체가 함께 움직여야 전환이 완성된다.
5	**로드맵에 맞춰 단계적으로 전환하라.** – 고위험·고우선순위 시스템부터 전환하고 점진적으로 적용 범위를 확대한다. – 공통 마일스톤을 바탕으로 기관별 전환 계획을 수립하고 지속적으로 관리한다.

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



주요 용어

주요 용어

• 양자컴퓨팅 및 양자내성암호

| 공개 키 암호 (Public-Key Cryptography)

서로 다른 두 개의 키로 이루어진 키 쌍을 사용하여 암호화, 키 설정, 전자서명, 인증 등의 기능을 제공하는 암호기술이다. RSA, ECDSA, ECDH 등이 대표적인 기존 공개 키 암호이며, 본 가이드북에서는 양자컴퓨팅에 취약한 이러한 기존 공개 키 암호를 양자내성암호 전환의 주요 대상으로 한다.

| 대칭 키 암호 (Symmetric-Key Cryptography)

암호화와 복호화에 동일한 비밀 키를 사용하는 암호기술이다. AES, ARIA, LEA 등이 대표적이며, 공개 키 암호와 달리 양자컴퓨터로 인해 알고리즘의 안전성 기반이 직접 무력화되는 것으로 보지는 않는다.

| 암호학적으로 유의미한 양자컴퓨터 (Cryptographically Relevant Quantum Computer, CRQC)

RSA, ECC 등 현재 사용되는 공개 키 암호의 안전성을 위협할 수 있을 정도의 규모와 성능을 갖춘 양자컴퓨터를 의미한다.

| 양자 오류정정 (Quantum Error Correction, QEC)

양자 연산 과정에서 발생하는 오류를 탐지하고 보정하여 양자정보를 안정적으로 유지하기 위한 기술로, 대규모 양자컴퓨터 구현을 위한 핵심 기술 중 하나이다.

| 쇼어 (Shor) 알고리즘

정수의 소인수분해와 이산로그 문제를 효율적으로 해결할 수 있는 양자 알고리즘으로, 충분한 성능의 양자컴퓨터가 실현될 경우 RSA, ECC 등 해당 수학적 문제에 기반한 공개 키 암호의 안전성을 위협할 수 있다.

| 그로버 (Grover) 알고리즘

정렬되지 않은 탐색 공간에서 원하는 값을 고전적 탐색보다 빠르게 찾을 수 있는 양자 알고리즘으로, 대칭 키 암호의 키 탐색이나 해시함수의 일부 보안 특성에 영향을 줄 수 있다. 이에 따라 양자 공격을 고려할 경우 충분한 보안강도를 확보할 수 있는 키 길이와 알고리즘을 사용하는 것이 중요하다.

| 모스카 부등식 (Mosca's Inequality)

데이터 보호 필요기간(X)과 양자내성암호 전환 소요 기간(Y)의 합이 현행 공개 키 암호를 위협할 수 있는 양자컴퓨터 등장까지의 예상기간(Z)보다 큰지를 비교하여 전환 준비의 시급성을 판단하는 개념이다.

| 오차 학습 문제 ((Module) Learning With Errors, (M)LWE)

수학 문제에 미세한 의도적 오차를 섞어 넣어, 양자컴퓨터조차 역산하여 해를 구하기 어렵게 만든 암호 원리. (가군구조) 격자 암호의 안전성을 지탱하는 핵심 개념이다.

| (M)SIS ((Module) Short Integer Solution, 짧은 정수 해 문제)

주어진 수학적 관계를 만족하는 짧은 정수 벡터를 찾는 것이 어렵다는 성질에 기반한 수학적 난제로, SIS 및 Module-SIS는 여러 격자 기반 양자내성암호 알고리즘, 특히 전자서명 알고리즘의 안전성을 구성하는 수학적 기반으로 활용된다.

• 양자내성암호 및 표준화

| 양자내성암호 (Post-Quantum Cryptography, PQC)

양자컴퓨팅 기반 공격에도 안전하도록 격자, 해시함수 등 다양한 수학적 문제에 기반하여 설계된 암호기술이다.

| 키 캡슐화 메커니즘 (Key Encapsulation Mechanism, KEM)

공개키를 이용한 캡슐화(Encapsulation)와 개인키를 이용한 역캡슐화(Decapsulation)를 통해 통신 당사자가 동일한 공유비밀(Shared Secret)을 안전하게 설정할 수 있도록 하는 암호 메커니즘이다. 생성된 공유비밀을 대칭키암호에 사용할 키를 유도하는 데 활용할 수 있다.

| 한국형 양자내성암호 (Korean Post-Quantum Cryptography, KpqC)

양자내성암호연구단(KpqC연구단) 주관으로 2021년부터 진행한 '양자내성암호 국가공모전'을 통해 선정된 양자내성암호 알고리즘을 말한다.

| 미국 국립표준기술연구소 (National Institute of Standards and Technology, NIST)

미국의 측정과 표준 및 기술 개발을 담당하는 기관으로, 양자내성암호 표준화 프로세스를 추진하고 ML-KEM, ML-DSA, SLH-DSA 등을 FIPS 표준으로 제정하였다.

• 하이브리드 전환 방식

| 하이브리드 방식

양자내성암호 전환 과정에서 둘 이상의 암호 알고리즘을 함께 지원하거나 조합하여 암호 기능을 구성하는 방식이다. 적용 방식에 따라 둘 이상의 암호 알고리즘을 함께 적용하고 그 결과를 결합하는 하이브리드-AND 방식과, 시스템이나 통신 상대의 지원 여부 등에 따라 암호 알고리즘을 선택하여 사용하는 하이브리드-OR 방식으로 구분할 수 있다.

| 하이브리드-AND (동시 결합 방식)

둘 이상의 암호 알고리즘을 함께 적용하고, 각 알고리즘의 결과를 안전하게 결합하여 암호 기능을 구성하는 방식이다. 결합하는 암호 알고리즘의 조합에 따라 기존 공개 키 암호와 양자내성암호를 결합하는 PQ/T(Post-Quantum/Traditional) 방식과 둘 이상의 양자내성암호를 결합하는 PQ/PQ(Post-Quantum/Post-Quantum) 방식으로 구분할 수 있다. 적절한 결합 방식이 적용된 경우 하나의 암호 알고리즘에 예기치 않은 취약점이 발견되더라도 다른 알고리즘의 안전성을 기반으로 보호 수준을 유지할 수 있도록 설계할 수 있다.

| 하이브리드-OR (선택 결합 방식)

기존 공개 키 암호와 양자내성암호 중 시스템 또는 통신 상대가 지원하는 암호 방식을 선택하여 사용하는 전환 방식이다. 전환 단계에서 시스템별 지원 수준이 다른 경우 상호운용성을 확보하는 데 활용할 수 있으나, 양자내성암호가 아닌 기존 공개 키 암호만 선택되는 경우에는 양자컴퓨팅 기반 공격에 대한 안전성을 확보할 수 없다는 점을 고려해야 한다.

| 키 유도 함수 (Key Derivation Function, KDF)

하나 이상의 비밀값 등 입력값으로부터 암호 연산에 사용할 키를 안전하게 생성하는 함수이다. 하이브리드 방식에서는 복수 암호에서 얻은 비밀값을 안전하게 결합하는 데 활용할 수 있다.

| 폴백(Fallback)

우선적으로 사용하려는 암호 방식이 지원되지 않거나 사용할 수 없는 경우, 사전에 허용된 다른 암호 방식으로 전환하여 통신을 계속하는 방식이다.

| 롤백(Rollback)

시스템 또는 암호체계의 변경·전환 이후 장애나 성능 저하 등의 문제가 발생한 경우, 변경 이전의 정상 동작 상태나 설정으로 되돌리는 절차이다.

| 다운그레이드 공격 (Downgrade Attack)

공격자가 암호 협상 과정에 개입하여 시스템이 지원하는 암호 방식 중 상대적으로 보안성이 낮은 방식이 선택되도록 유도하는 공격이다. 하이브리드-OR 방식이나 폴백을 적용할 때 특히 고려해야 한다.

• 암호자산 식별·전환 및 위협 관리

| 암호자산 (Cryptographic Asset)

정보시스템에서 암호기능을 구현·제공·사용하거나 이를 보호·관리하기 위해 식별·관리해야 하는 암호 관련 자산을 의미한다. 암호 알고리즘, 암호 라이브러리·모듈, 프로토콜, 인증서, 암호 키, 암호 장비 등이 포함될 수 있다.

| 암호자산 인벤토리 (Cryptographic Asset Inventory)

기관의 시스템·서비스에서 어떤 암호자산이 어디에서 어떻게 사용되고 있는지를 식별하여 체계적으로 기록·관리하는 목록이다. 전환 대상 식별, 우선순위 결정, 공급업체 협의 및 변경 영향 분석의 기초 자료로 활용한다.

| 선수집 후 해독 (Harvest Now, Decrypt Later, HNDL) 공격

현재 암호화된 통신이나 데이터를 수집·저장해 두었다가, 향후 충분한 성능의 양자컴퓨터가 등장했을 때 복호화를 시도하는 공격이다.

| 암호자산 명세서 (Cryptographic Bill of Materials, CBOM)

소프트웨어나 시스템에서 사용되는 암호 알고리즘, 키, 인증서, 암호 프로토콜 등 암호 관련 구성요소와 정보를 식별·관리하기 위한 명세서이다.

| 소프트웨어 자재명세서 (Software Bill of Materials, SBOM)

소프트웨어를 구성하는 라이브러리, 패키지 등 구성요소와 의존 관계를 목록화한 명세서이다. CBOM은 이 개념을 암호 관련 구성요소의 식별·관리에 특화하여 활용한 형태이다.

| 정적 분석 (Static Analysis)

소프트웨어를 실행하지 않은 상태에서 소스코드, 바이너리 등의 정적 정보를 분석하여 사용 중인 암호 알고리즘, 하드코딩된 키 등 암호 관련 요소와 취약 암호 사용 여부를 식별하는 분석 기법이다.

| 동적 분석 (Dynamic Analysis)

소프트웨어나 시스템을 실행한 상태에서 실제 통신 및 동작을 관찰·분석하여 사용 중인 암호 알고리즘, 프로토콜, 인증서 등 암호 관련 요소와 취약 암호 사용 여부를 식별하는 분석 기법이다.

| 부채널 공격 (Side-Channel Attack, SCA)

암호 알고리즘의 구현·동작 과정에서 발생하는 연산 시간, 전력 소비, 전자기파 등의 물리적 정보를 분석하여 비밀정보를 추정하거나 암호체계의 안전성을 침해하는 공격이다.

| 암호 민첩성 (Crypto Agility)

특정 암호 알고리즘이나 구현에 종속되지 않고, 보안 요구사항이나 기술·표준의 변화에 따라 보안과 운영 연속성을 유지하면서 암호 알고리즘과 관련 구성요소를 신속하고 유연하게 변경할 수 있는 역량으로, 기술적 설계뿐만 아니라 변경 사항을 조직 전체에 일관되게 반영하기 위한 정책·절차적 대응 체계까지 포괄한다.

● 국가·공공 보안체계 및 공개 키 인증·전자서명

| 국가 망 보안체계 (National Network Security Framework, N2SF)

각급기관의 업무정보와 정보시스템을 식별하고, 업무 중요도에 따라 C(Classified : 기밀), S(Sensitive : 민감), O(Open : 공개) 등급으로 분류하여 등급별로 차등적인 보안통제를 적용하는 보안 프레임워크이다.

| 전자서명 인증체계 (Public Key Infrastructure, PKI)

공개 키와 전자서명을 이용한 인증서비스를 제공하기 위해 인증기관, 인증서, 인증서 발급·검증·폐기 절차 및 관련 시스템 등을 구성한 기반체계이다.

| 행정전자서명 인증체계 (Government Public Key Infrastructure, GPKI)

행정기관 등의 전자적 업무처리에서 신원 확인, 전자서명 등에 필요한 인증서비스를 제공하기 위한 공개키 기반의 행정전자서명 인증체계이다.

| 국가전자서명 인증체계 (National Public Key Infrastructure, NPKI)

민간 부문의 전자서명 및 인증서비스를 지원하기 위해 인증기관과 인증서 등을 기반으로 구성된 공개키 기반구조이다.

| 인증기관 (Certification Authority, CA)

공개 키가 특정 사용자·기관·시스템에 속한다는 사실을 인증하고 인증서를 발급·관리하는 기관 또는 시스템이다. 신뢰체계의 최상위에 있는 인증기관을 루트 CA(Root CA), 그 하위 인증기관을 중간 CA(Intermediate CA)라고 한다.

| 인증서 폐기 목록 (Certificate Revocation List, CRL)

유효기간이 끝나기 전에 폐기된 인증서의 정보를 인증기관이 목록 형태로 제공하는 인증서 상태 확인 방식이다.

| 온라인 인증서 상태 프로토콜 (Online Certificate Status Protocol, OCSP)

특정 인증서의 폐기 여부를 온라인으로 조회·확인하기 위한 프로토콜이다.

| 코드서명 (Code Signing)

소프트웨어, 실행파일, 펌웨어 등의 배포물에 전자서명을 적용하여 배포 주체를 확인하고, 서명 이후 해당 코드가 변경되거나 위변조되었는지를 검증할 수 있도록 하는 기술이다.

| 장기 서명 프로파일 (Long-Term Validation, LTV)

전자서명에 사용된 인증서가 만료되거나 검증환경이 변경된 이후에도 서명의 유효성을 검증할 수 있도록, 인증서, 인증서 폐기 상태정보, 타임스탬프 등 필요한 검증정보를 확보·보존하고 이를 활용하여 장기간 서명의 유효성을 검증한다.

| 암호모듈 검증제도 (Korea Cryptographic Module Validation Program, KCMVP)

국가·공공기관에서 도입하는 암호모듈이 시험요구사항에 따라 보안요구사항을 만족하는지를 확인하여 안전성과 구현 적합성을 검증하는 제도이다.

• 하드웨어 보안 장치

| 하드웨어 보안 모듈 (Hardware Security Module, HSM)

암호키를 안전하게 생성·저장·관리하고, 보호된 환경에서 전자서명, 암·복호화 등 암호연산을 수행하도록 설계된 하드웨어 보안 장치이다.

• 통신 및 네트워크 보안

| 인터넷 프로토콜 보안 (Internet Protocol Security, IPsec)

IP 계층에서 통신 데이터의 기밀성, 무결성 및 인증 등을 제공하여 IP 통신을 보호하는 표준 보안 프로토콜 체계이다.

| 가상사설망 (Virtual Private Network, VPN)

인터넷 등 공중망을 이용하여 사용자나 시스템 간에 안전한 논리적 사설 통신망을 구성하는 기술 또는 가상 네트워크이다.

| 전송 계층 보안 (Transport Layer Security, TLS)

네트워크 통신에서 통신 상대를 인증하고 전송되는 데이터의 기밀성과 무결성을 보호하기 위한 표준 보안 프로토콜이다.

| 보안 소켓 계층 (Secure Sockets Layer, SSL)

인터넷 통신에서 전송되는 데이터를 암호화하여 보호하기 위해 사용된 보안 프로토콜로, 현재는 보안 취약성으로 인해 TLS로 대체되었다.

| 보안 쉘 (Secure Shell, SSH)

원격 서버에 안전하게 접속하여 시스템을 관리할 수 있도록 암호화된 통신 채널을 제공하는 원격 접속 프로토콜이다.

• 클라우드 서비스 모델

| IaaS·PaaS·SaaS

클라우드 서비스 제공 범위에 따른 서비스 모델이다. IaaS는 컴퓨팅·스토리지·네트워크 등 인프라를, PaaS는 애플리케이션 실행을 위한 플랫폼을, SaaS는 완성된 소프트웨어 기능을 서비스 형태로 제공한다. 서비스 모델에 따라 기관과 클라우드 서비스 제공자의 암호 설정·관리 책임 범위가 달라질 수 있다.

• 특수 시스템 환경

| IoT·OT·ICS

IoT(Internet of Things)는 네트워크에 연결된 각종 장치와 센서 환경을, OT(Operational Technology)는 물리적 설비·공정을 제어·운영하는 기술 환경을, ICS(Industrial Control System)는 산업 설비와 공정을 감시·제어하는 제어시스템을 의미한다. 이러한 환경은 제한된 연산자원, 장기간 운용되는 장비, 높은 가용성 및 운영 연속성 요구 등으로 인해 일반 정보시스템과 다른 전환 전략이 필요할 수 있다.

국가 · 공공기관 **양자내성암호 전환 가이드북**

POST-QUANTUM CRYPTOGRAPHY MIGRATION GUIDEBOOK



참고 문헌

참고 문헌

1. 개인정보보호위원회 고시, “개인정보의 안전성 확보조치 기준”, 제7조(개인정보의 암호화).

2. 관계부처합동, “범국가 양자내성암호 전환 마스터플랜”, 2023.

3. 관계부처합동, “범국가 양자내성 암호체계 전환 종합 추진계획”, 2025.

4. 국가정보원, 국가보안기술연구소, “국가 망 보안체계(N2SF) 보안가이드라인 1.0”, 2025.

5. 국가정보원, 국가보안기술연구소, 한국인터넷진흥원, “암호모듈 구현안내서(GVIPart1)(24.11)”, 2024.

6. 국가정보원 국가사이버안보센터, “양자내성암호 검증대상 후보군 및 추진 일정 공지”, 2026. 9. 1.

7. 양자내성암호연구단, https://kpqc.or.kr

8. 한국인터넷진흥원, “2024 암호이용 동향조사 분석 보고서”, 2025.

9. AIVD, TNO, CWI, “The PQC Migration Handbook”, 2024.

10. ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, 2022.

11. ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, 2023.

12. Anthropic, “Discovering cryptographic weaknesses with Claude”, 2026.

13. BSI, “TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2026-01,” 2026.

14. CCCS, “Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001)”, 2025.

15. Castryck, W., Decru, T., “An Efficient Key Recovery Attack on SIDH,” IACR ePrint 2022/975, 2022.

16. Cloudflare, “Cloudflare now uses post-quantum cryptography to talk to your origin server,” Cloudflare Blog, 2023. 9.29.

17. CRYPTREC, “CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024年度版,” 2025.

18. CSA, “Quantum Readiness Index 2025 (Draft for Public Consultation),” 2025.

19. Cybersecurity Authorities of EU Member States, “Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography”, Joint Statement, 2025.

20. CycloneDX, “Authoritative Guide to CBOM”, 2024.

21. Department of War, Post Quantum Cryptography Strategy, 2026.

22. Google, “Advancing Our Amazing Bet on Asymmetric Cryptography,” Chromium Blog, May 23, 2024.

23. Grover, L. K., “A Fast Quantum Mechanical Algorithm for Database Search”, Proceedings of STOC, pp. 212–219, 1996.

24. Jaques, S., Naehrig, M., Roetteler, M. and Virdia, F., “Implementing Grover oracles for quantum key search on AES and LowMC”, In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 280–310, 2020.

25. Lin, S., Tan, J., Asogamoorthy, A., Nekritz, K., Misoczki, R., Delimanolis, S., “Post-quantum readiness for TLS at Meta”, 2024.

26. Mosca, M., Piani, M., “Quantum Threat Timeline Report 2025,” evolutionQ Inc. / Global Risk Institute (GRI), 2026.

27. NIS Cooperation Group, “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography”, Part 1, Version 1.1, 2025.

28. NIST,“FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard”, 2024.

29. NIST,“FIPS 204: Module-Lattice-Based Digital Signature Standard”, 2024.

30. NIST, “FIPS 205: Stateless Hash-Based Digital Signature Standard”, 2024.

31. NIST, “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms”, NIST CSWP 15, 2021.

32. NSA, Announcing the Commercial National Security Algorithm Suite 2.0, Cybersecurity Advisory, PP-22-1338, Version 1.0, 2022.

33. OMB, “Execution of the Migration to Post-Quantum Cryptography,” Memorandum M-26-15, Executive Office of the President, 2026. 6.24.

34. Shor, P. W., “Algorithms for quantum computation: discrete logarithms and factoring”, Proceedings of FOCS, pp. 124-134, 1994.

35. The White House, “Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks”, 2026. 6.22.

36. NCSC(UK National Cyber Security Centre), “Timelines for Migration to Post-Quantum Cryptography”, 2025.