PQC 전환 준비도 진단 보고서 (샘플 발췌)

외부 TLS 암호자산 진단 및 90일 전환 실행계획

문서 종류	PQC 전환 준비도 진단 및 90일 실행계획 (Standard) — 샘플 발췌
발췌 범위	표지, 경영진 요약, 위험 우선순위, 갱신 창구 분석 (전체 16페이지 중 4페이지)
마스킹	고객사명과 호스트명은 asset-01 형식으로 치환되었습니다
실제 산출물	한국어 · 영어 각 PDF 및 DOCX, 전체 16페이지, 부록 포함
수행	컴네트워크 주식회사 · ADSAP (AI Depot Security Agent Platform)
표준 기준	NIST FIPS 203 / 204 / 205 (2024년 최종 확정), NIST IR 8547 (초안)
문의	pqc@comnetwork.net · https://adsap.comnetwork.net/

컴네트워크 주식회사 · ADSAP PQC 전환진단 · 샘플 발췌본

1. 경영진 요약

본 진단은 고객사가 지정한 외부 TLS 엔드포인트 18개를 읽기 전용으로 점검하고, 각 자산의 양자 위험도와 전환 우선순위를 산정한 결과입니다. 결론은 네 가지입니다.

결론 1. 본 진단 범위 내 외부 TLS 자산 18개는 모두 전환 계획 대상입니다

18개 자산 전부가 ECDSA(P-256) 공개키를 사용합니다. ECDSA는 Shor 알고리즘으로 다항시간 내에 해독 가능한 알고리즘군에 속하며, NIST IR 8547 초안 기준으로 2030년 이후 사용 중단(deprecated), 2035년 이후 사용 금지(disallowed) 기준점으로 **제안**되어 있습니다.[2] 이는 초기 공개초안이며 확정 규제가 아니지만, 조달 요구사항과 고객 실사 항목으로 옮겨오는 흐름은 이미 시작되었습니다. 따라서 이 18개에 대해서는 '전환할지 여부'보다 '언제 어떤 순서로 전환할지'를 정하는 것이 실질적인 과제입니다.

결론 2. 위험은 균일하지 않습니다. 3개가 치명, 15개가 높음입니다

자산별 데이터 민감도와 데이터 수명을 반영해 재산정한 결과, 치명(Critical) 3개, 높음(High) 15개로 분화되었으며 점수는 0.800에서 0.556까지 6단계로 나뉩니다. 최상위는 asset-01(0.800), asset-14(0.800), asset-04(0.750)입니다. 이 세 자산은 다른 서비스의 데이터가 통과하는 경로이거나 10년급 보존 데이터를 취급하기 때문에, 동일한 ECDSA를 쓰더라도 침해 시 파급이 다릅니다.

결론 3. 향후 89일 안에 18개 전부가 갱신 주기에 들어갑니다. 이것이 전환 창구입니다

진단 시점 기준 인증서 잔여일수는 최소 44일(asset-13), 최대 89일(asset-15)입니다. 18개 전부가 90일 이내에 갱신됩니다. 별도의 전환 프로젝트를 발주하지 않아도, 이미 예정된 갱신 작업에 새 암호 프로파일을 얹으면 전환이 시작됩니다. 추가 비용이 발생하는 지점은 인증서 발급이 아니라 프로파일 결정과 검증입니다.

특히 2026-09-29 만료 묶음에 7개 자산이 동시에 걸려 있습니다. 이 한 번의 갱신 작업이 전체 자산의 39%를 처리합니다.

결론 4. 지금 당장 실행 가능한 조치와 2027년까지 기다려야 하는 조치가 다릅니다

이 구분이 본 보고서의 핵심입니다. 'PQC 전환'은 하나의 작업이 아니라 성격이 전혀 다른 두 트랙입니다.

- 트랙 A (키 교환 / 기밀성): 오늘 실행 가능합니다. 하이브리드 키 교환 X25519MLKEM768은 이미 표준화 막바지 단계이고[5] 주요 CDN·브라우저에서 기본 동작합니다.[6] HNDL(지금 수집, 나중에 해독) 위험을 해소하는 것은 인증서 교체가 아니라 이 설정입니다.
- 트랙 B (서명 / 인증): 공인 인증서 적용에는 대기가 필요합니다. ML-DSA의 X.509 인코딩 자체는 RFC 9881로 이미 표준화되어 사설 PKI에서는 사용할 수 있으나, 공개 웹 PKI 적용은 CA/Browser Forum 기준과 브라우저 루트 프로그램 지원에 의존하며 상용 시점이 확정되지 않았습니다.[8]

핵심 판단: 본 진단이 산출한 HNDL 점수는 인증서를 바꿔서 낮아지는 값이 아닙니다. 키 교환 설정으로 낮아집니다. 그리고 그 조치는 예산 승인이나 인증서 갱신을 기다릴 필요가 없습니다. 반면 인증서의 ECDSA 서명은 소급 위조가 불가능하므로 HNDL 대상이 아니며, 2030~2035 규제 일정에 맞춘 계획 사안입니다.

1.1 30초 요약

구분	판정
전환 범위	본 진단 범위 내 외부 TLS 자산 18개 (전부 ECDSA P-256)
최우선 자산	asset-01, asset-04 (위험 최상위 + 최단 갱신 창구 동시 충족)
가장 이른 창구	D+44일 (2026-09-25) asset-13.example.com
즉시 조치	하이브리드 키 교환(X25519MLKEM768) 활성화 여부 검증 및 강제
대기 조치	공인 CA의 ML-DSA 인증서 발급 (X.509 인코딩은 RFC 9881로 표준화 완료, 상용 시점 미정)
현 성숙도	5단계 중 3단계 (인벤토리 확보 및 우선순위 산정 완료, 외부 TLS 표면 한정)
전환 기준점	2030년 사용 중단, 2035년 사용 금지 (NIST IR 8547 초기 공개초안이 제안. 확정 규제 아님)

2. 진단 결과 (발췌)

2.1 위험 우선순위

5.3의 자산 프로파일을 반영해 재산정한 결과입니다. 총점 내림차순, 동점 시 갱신 창구 순입니다.

순위	호스트	민감도	수명	HNDL	총점	우선순위	창구
1	asset-01.example.com	치명	10년	1.000	0.800	치명(Critical)	D+48
2	asset-14.example.com	치명	10년	1.000	0.800	치명(Critical)	D+65
3	asset-04.example.com	높음	10년	0.800	0.750	치명(Critical)	D+48
4	asset-11.example.com	높음	7년	0.560	0.690	높음(High)	D+70
5	asset-02.example.com	높음	7년	0.560	0.690	높음(High)	D+74
6	asset-17.example.com	높음	7년	0.560	0.690	높음(High)	D+75
7	asset-13.example.com	높음	5년	0.400	0.650	높음(High)	D+44
8	asset-10.example.com	높음	5년	0.400	0.650	높음(High)	D+60
9	asset-07.example.com	높음	5년	0.400	0.650	높음(High)	D+65
10	asset-05.example.com	높음	5년	0.400	0.650	높음(High)	D+69
11	asset-16.example.com	높음	5년	0.400	0.650	높음(High)	D+74
12	asset-03.example.com	높음	5년	0.400	0.650	높음(High)	D+77
13	asset-09.example.com	중간	3년	0.150	0.588	높음(High)	D+48
14	asset-15.example.com	중간	3년	0.150	0.588	높음(High)	D+89
15	asset-18.example.com	낮음	1년	0.025	0.556	높음(High)	D+48
16	asset-06.example.com	낮음	1년	0.025	0.556	높음(High)	D+48

순위	호스트	민감도	수명	HNDL	총점	우선순위	창구
17	asset-12.example.com	낮음	1년	0.025	0.556	높음(High)	D+48
18	asset-08.example.com	낮음	1년	0.025	0.556	높음(High)	D+48

2.2 갱신 창구 분석

본 진단에서 가장 실행 가치가 높은 발견입니다. 인증서 만료일은 단순한 관리 항목이 아니라, 암호 프로파일을 교체할 수 있는 유일한 무비용 기회입니다.

창구	만료일	자산 수	해당 자산	최고 위험도
D+44	2026-09-25	1개	asset-13	0.650
D+48	2026-09-29	7개	asset-01, asset-04, asset-09, asset-18, asset-06, asset-12, asset-08	0.800
D+60	2026-10-11	1개	asset-10	0.650
D+65	2026-10-16	2개	asset-14, asset-07	0.800
D+69	2026-10-20	1개	asset-05	0.650
D+70	2026-10-21	1개	asset-11	0.690
D+74	2026-10-25	2개	asset-02, asset-16	0.690
D+75	2026-10-26	1개	asset-17	0.690
D+77	2026-10-28	1개	asset-03	0.650
D+89	2026-11-09	1개	asset-15	0.588

관찰 1. 가장 이른 창구는 D+44일의 asset-13.example.com입니다. 위험도는 중위권(0.650)이고 서비스 영향도 제한적이므로, 하이브리드 프로파일을 실전 검증하는 리허설 대상으로 가장 적합합니다.

관찰 2. 2026-09-29 만료 묶음에 7개가 집중되어 있으며, 여기에 최상위 위험 자산 asset-01(0.800)와 asset-04(0.750)가 함께 포함됩니다. 즉 최고 위험 자산이 가장 큰 갱신 묶음 안에 있습니다. 이 창구를 놓치면 다음 기회는 90일 뒤입니다.

관찰 3. asset-14.example.com는 위험도 최상위(0.800)이지만 창구가 D+65일로 늦습니다. 위험 순서와 창구 순서가 어긋나는 유일한 자산이며, 만료를 기다리지 않는 조기 갱신 검토 대상입니다.

이 발췌본에 포함되지 않은 내용

실제 보고서는 아래를 모두 포함해 한국어 · 영어 각 16페이지 안팎으로 제공됩니다. 본 발췌본은 형식과 분석 깊이를 확인하실 수 있도록 일부만 공개한 것입니다.

장	내용
2. 왜 지금인가	HNDL 소급 해독 위험, Mosca 부등식, 2030 · 2035 규제 시한, 인증서 수명 단축이 만드는 부수 효과

장	내용
3. 용어	ML-KEM, ML-DSA, SLH-DSA, 하이브리드, 암호 민첩성을 검색 없이 읽을 수 있도록 정리
4. 왜 ECDSA가 위험한가	Shor 알고리즘 해설, Grover 와의 차이, 그리고 인증서 서명이 HNDL 대상이 아닌 이유
5. 진단 방법론	수집 항목과 통제 수단, 위험 점수 공식 공개, 자산 맥락 입력값과 그 한계
7. 전환 실행 계획	트랙 A · B 분리, 단계별 조치와 검증 명령, 웨이브 단위 실행 순서, 90일 로드맵, 담당자 확인 항목
8. 현 위치	5단계 전환 성숙도 판정, 국가 로드맵 및 NIST 일정 대비 위치
9. 범위 제한	진단하지 않은 영역, 기술적 한계, 면책
부록 A · B	원시 관측 데이터 전량, 각주 및 참고 출처 (URL 포함)

본 발췌본의 수치는 실제 진단 결과이며, 고객사명과 호스트명만 마스킹했습니다. 진단 문의는 pqc@comnetwork.net 으로 주십시오.