後量子密碼遷移指引

版本 1.00

後量子資安產業聯盟
財團法人資訊工業策進會
發行
中華民國 114 年 4 月 16 日

前言

量子電腦的出現將徹底改變現行的網路安全與加密體系。一旦功能完備的量子電腦實現，其將幾乎完全破解現有公鑰加密系統的安全性。相較之下，傳統的共享金鑰加密系統（如 AES）雖受影響較小，但其有效安全強度也將下降至目前水準的約一半。

此變化將對保護電子通訊與數位交易的系統造成災難性衝擊。目前大多數安全的網路流程仰賴公鑰加密技術，包括保護網站、銀行交易、安全電子郵件及數位簽章的協定。進入量子運算時代後，企業與個人在網路上的活動均將不再安全。

我國資通訊及半導體產業在全球 ICT 供應鏈中佔有重要地位，如何確保產業能因應量子電腦帶來的安全挑戰，已逐漸成為成為受關注的焦點。因此在數位發展部數位產業署的支持下，制定本指引，本指引簡要回顧傳統密碼技術的現況及其面臨的量子威脅，大致說明當前後量子密碼的技術發展路徑，並透過解析 NIST 及相關國際組織陸續發布的後量子密碼遷移研究報告，提出後量子密碼遷移路線圖，涵蓋以下步驟：建立量子準備計畫、盤點加密資產清單、與技術供應商討論量子準備計畫、確認供應鏈的量子準備程度，並提出盤點加密資產清單的自動化工具操作實例。

本指引由後量子產業聯盟及財團法人資訊工業策進會編寫團隊戮力完成。懇請產業先進及專家不吝批評指正，以助後續完善。

目錄

表目錄

圖目錄

壹、文件概述

一、指引目的

為了保護傳輸資料的安全，加密機制已運用在各類數位服務中，目前各行各業的數位服務系統中多使用 RSA 加解密演算法來保護資料安全，但未來面對駭客利用量子電腦運算力而發動的破密攻擊，需相對應提升至「後量子加密」(Post-quantum cryptography, PQC）系統來強化各行各業數位服務系統的防護能力。

本指引主要參考美國國家標準及技術研究所（National Institute of Standards and Technology, NIST）公布之後量子遷移文件，所參考文件包括：NIST-SP-1800-38A、NIST-SP-1800-38B、NIST IR 8547 、 QUANTUM-READINESS ： MIGRATION TO POST-QUANTUM、TNO CWI AIVD The PQC Migration Handbook，彙整 4 個步驟，提出產業應考量的後量子遷移的內外部構面，以協助臺灣廠商規劃後量子遷移。

二、適用範圍

本指引適用之範圍為規劃後量子遷移之組織，並作為後量子遷移之一般性參考。

個別產業可參考本指引，考量國際規範、國內法規或產業特性等需求，對指引步驟及內容進行調整，以符合產業遷移實際需要。

三、名詞定義

- 後量子密碼（Post-Quantum Cryptography, PQC）
  本指引之後量子密碼特指能夠在現有電腦上實現的、具有抵抗未來量子電腦攻擊能力之數學密碼，不包含依賴量子力學特性的量子密碼（Quantum cryptography, QC）。
- 量子準備計畫（Quantum-Readiness Roadmap）
  描述組織從現有加密技術向後量子密碼遷移的計畫和路線圖。包括遷移策略、遷移時機以及資源的分配。
- 加密敏捷性（Cryptographic Agility）
  組織快速替換或升級演算法，以應對新威脅或新標準的能力。
- 加密資產清單（Cryptographic Inventory）
  紀錄組織內所有使用加密技術的資產清單。
- 加密資產（Cryptographic Assets）

指所有使用加密技術保護的系統、憑證、金鑰、軟體及硬體等。

- 混合式加密方案（Hybrid Cryptography Solutions）
  同時使用傳統加密演算法和後量子加密演算法。以利遷移期間的相容性及安全性。

貳、後量子遷移需求背景說明

一、傳統密碼演算法介紹

每種加密系統的基礎，皆奠基於一項複雜的數學難題。目前主流的公鑰加密與解密系統，例如 RSA 加密演算法及橢圓曲線密碼系統（ECC），其背後仰賴的數學難題（如大整數分解因數問題與橢圓曲線上的離散對數問題），對於傳統電腦而言極其複雜，難以破解；然而，這些難題卻正是量子電腦最擅長解決的類型。原因在於，這些數學問題的解答可轉化為具週期性的結構。理論上，只要能夠識別出該結構的週期，就能相對輕鬆地破解問題。對於傳統電腦而言，當涉及極大數字時，尋找週期是一項極為艱鉅的任務；但對量子電腦來說，卻是輕而易舉之事。1994 年，彼得·肖爾（Peter Shor）提出的演算法恰好能夠有效尋找週期，從而具備破解當前主流公鑰加密系統的能力。

相較之下，常見的對稱式加密系統（如 AES）只需將金鑰長度增加一倍，即可確保相同的安全性。然而，基於 RSA 與 ECC 的公鑰加密系統，在足夠強大的量子電腦出現後，將不再具備安全性。因此，隨著量子電腦技術的蓬勃發展，勢必對日常生活中的隱私保護構成顯著威脅，以下大略說明目前主流之傳統密碼演算法。

(一)對稱金鑰加密

1. 特性：

   使用相同金鑰進行加密與解密，運算效率高但需安全交換金鑰。

2. 代表演算法：

   - DES：一種對稱金鑰的區塊加密演算法，實際金鑰長度僅 56 位元，因安全性不足，已被淘汰。
   - AES：現代標準區塊加密演算法，支援 128/192/256 位元金鑰，取代 DES。
   - 3DES：將 DES 重複三次以提升安全性，但效能較低且逐漸淘汰。
   - RC4：串流加密法，生成隨機金鑰流與明文結合，適用於即時通訊。

(二)非對稱金鑰加密

1. 特性

結合非對稱加密與雜湊函數，確保訊息完整性與不可否認性。

2. 代表演算法：

- RSA：基於大數因式分解問題，用於數位簽章與金鑰交換，推薦 2048 位元以上金鑰。
- ECC：基於橢圓曲線離散對數問題，提供更短金鑰長度的同等安全性，適用於嵌入式裝置與加密貨幣。
- DSA：由 NIST 標準化，基於模指數運算，用於電子簽章驗證。

(三)雜湊函數

1. 特性

單向不可逆轉換，輸出固定長度雜湊值，無需金鑰。

2. 代表演算法：

- SHA-2：提供 224/256/384/512 位元輸出，用於資料完整性檢查。
- SHA-3：設計更安全且靈活，補充 SHA-2 的不足。

(四)數位簽章

1. 特性

結合非對稱加密與雜湊函數，確保訊息完整性與不可否認性。

2. 代表演算法：

- RSASSA-PKCS1-v1.5：基於 RSA，廣泛用於電子簽章。
- ECDSA：基於 ECC，效能優於 RSA，適用於資源有限環境。
- EdDSA：改進版橢圓曲線簽章，效能更高。

(五)其他類型

- 金鑰交換協議：如 Diffie-Hellman，允許雙方在未共享金鑰的情況下建立共享金鑰。

表 1：傳統密碼演算法主要類型及技術比較表

類型	代表演算法	安全基礎	效能特性	應用場景
對稱加密	AES	大數運算複雜度	高效能	大量資料加密
非對稱加密	RSA	大數因式分解問題	運算較慢	金鑰交換、數位簽章
雜湊函數	SHA-256	雜湊碰撞難度	單向不可逆	資料完整性驗證
數位簽章	ECDSA	橢圓曲線離散對數問題	高效能、短金鑰長度	智能裝置、加密貨幣

資料來源：團隊自行整理

二、量子電腦的威脅與因應作法

(一)量子電腦出現對傳統密碼的影響及挑戰

量子電腦在可見的未來即將商用化，這對依賴因數分解或離散對數問題的公鑰加密系統構成重大威脅。即使在尚未有商用化量子電腦的現在，組織的加密資產仍面臨著先竊取，後解密（Harvest Now, Decrypt Later）的風險，即攻擊者現在蒐集以傳統密碼保護之資料，待在量子技術成熟後進行解密。

在不同層面的後量子密碼學遷移過程中，各種應用場景皆面臨潛在風險與相應的技術挑戰。

1. 設備的數位簽章

由於某些設備在出廠後可能無法更新簽章驗證機制，如果這些傳統演算法的使用壽命超過量子電腦可破解現有加密演算法的時間，就必須確保數位簽章採用抗量子演算法，以維持軟體供應鏈的安全性。其次，身分驗證系統依賴非對稱加密來保護身分認證，而現行的加密機制在量子計算技術成熟後將面臨安全風險。儘管目前仍可使用這些機制，但是當量子電腦足以破解這些演算法時，組織將必須全面升級至具備量子安全的身分驗證系統。

2. 網路安全協議

傳輸層安全性協定（TLS, Transport Layer Security）和虛擬私人網路（VPN, Virtual Private Network）受「先儲存，後解密」（Harvest Now, Decrypt Later）威脅的影響較大，因為攻擊者可以先收集傳輸的加密資料，等到量子電腦成熟後再解密，因此，企業應優先遷移網路安全協議，以確保前向保密性，而身分驗證機制的遷移時機則需根據風險評估決定。

3. 電子郵件與文件簽章加密

數位簽章能夠確保電子通訊的完整性，常見的 RSA、ECC 演算法在量子時代將不再安全，因此需逐步過渡至量子安全的簽章演算法。此外，S/MIME 等電子郵件加密標準也應納入後量子遷移計畫，以防止攻擊者提前收集加密郵件，待未來量子電腦可用時解密。

整體而言，後量子遷移涉及數位簽章、身分驗證、通訊協議與資料加密等多個層面，組織需根據技術可行性與風險承受能力，制定適當的遷移計畫，以確保在量子威脅到來前完成必要的防禦措施。

(二)國際面對量子威脅的因應作法

1. 歐洲地區

(1) 德國

資訊聯邦安全辦公室（Bundesamt für Sicherheit in der Informationstechnik, BSI）於 2024 年 11 月聯合 EU members 發布了《Joint statement on Post-Quantum Cryptography》[1]，該文件強調量子計算對當前加密系統的潛在威脅，並呼籲政府、企業和關鍵基礎設施儘早準備後量子密碼遷移。

(2) 荷蘭

荷蘭應用科學研究組織（Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO）於 2024

[1] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3

年 12 月發布《PQC Migration Handbook》[2]，TNO 將遷移分成三步驟：角色分析、制定遷移規劃、遷移執行。並提供具體的、可行的指導，協助組織遷移到後量子密碼學。

(3) 英國

英國國家網路安全中心（National Cyber Security Centre, NCSC）於 2025 年 3 月 20 日發布白皮書《Timelines for migration to post-quantum cryptography》[3]，旨在幫助英國的產業、關鍵基礎設施在 2035 年前全面過渡到後量子後密碼；文件提出分階段時間表（2028 年盤點、2031 年優先級遷移、2035 年完全遷移），以應對量子電腦對當前加密的威脅。

2. 加拿大、韓國及澳洲：

(1) 加拿大

加拿大創新、科學和經濟發展局（Innovation, Science and Economic Development Canada, ISED） 於 2024 年 7 月發布了《Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES, Quantum-Readiness Working Group》[4]。該文件概述了遷移的五個階段、加密資產庫存清單、加密敏捷性用例、後量子密碼遷移路線圖以及第三方評估清單，旨在指導企業解決密碼學相關量子計算威脅。

(2) 韓國

韓國國家情報局和科學技術資訊通訊部(The Ministry of Science and ICT, MSIT）[5]於 2023 年 7 月發布了後量子密碼學總體規劃《為量子轉型時代做準備》，將在 2035 年之前將其國家密碼系統轉為後量子密碼學。

---

[2] https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

[3] https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[4] https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

[5] Press Releases - 과학기술정보통신부 >

韓國國家情報院（NIS）與國家安全研究所（NSR）於 2021 年聯合發起的一項全國性計劃，韓國後量子密碼學競賽（簡稱 KpqC）[6]， KpqC 競賽的設計參考了 NIST 的後量子密碼標準化流程，旨在徵集、評估並最終選定適合韓國需求的後量子密碼演算法。KpqC 競賽經過兩輪的比賽，從 2021 年啟動至 2025 年結束，成功選出 HAETAE、SMAUG-T、LEMON 和 AIMer 四個演算法。

(3) 澳洲

澳洲網路安全中心（Australian Cyber Security Centre, ACSC）2023 年 5 月更新了《Planning for post-quantum cryptography》[7]，該文件建議組織應開始識別使用加密的系統和數據、評估其價值，並制定遷移計劃。

(三)美國發布後量子密碼標準之流程與最新發展

美國國家標準及技術研究所（National Institute of Standards and Technology, NIST）自 2016 年起舉辦「後量子密碼學標準化競賽」，旨在因應量子電腦可能破解現有加密系統的威脅，選定能抵禦量子攻擊的新一代公鑰加密與數位簽章演算法。以下說明競賽過程以及最終結果。

1. 公開競賽選定後量子密碼標準

(1) 競賽啟動與第一輪評估

競賽於 2016 年啟動，NIST 在當年 PQCrypto 會議上宣布徵集提案，聚焦於量子安全的公鑰加密（特別是金鑰封裝機制，KEM）和數位簽章系統。2017 年 11 月 30 日徵集截止，共收到 82 份提案，經初步審查後，69 份被視為完整且適當，進入第一輪評估。

第一輪評估期間，密碼學家對這些候選演算法進行密集分析與攻擊，

(2) 第二輪評估

[6] https://www.kpqc.or.kr/competition_02.html

[7] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography

2019 年 1 月 31 日，NIST 宣布 26 個演算法進入第二輪。同年 8 月，於加州聖塔芭芭拉大學舉辦第二次會議，進一步評估性能與安全性。

(3) 第三輪評估

2020 年 7 月 23 日，15 個演算法進入第三輪，涵蓋多數基於格論（lattice-based）、編碼論（code-based）及雜湊函數（hash-based）的方案。

第三輪持續至 2022 年 7 月，NIST 宣布選定四個主要演算法：CRYSTALS-KYBER 用於 KEM，CRYSTALS-Dilithium、FALCON 和 SPHINCS+用於數位簽章。這些演算法除 FALCON 尚在討論中外，其餘三個演算法於 2024 年 8 月 13 日發布標準化文件，分別為 FIPS 203(ML-KEM，源自 KYBER)、FIPS 204（ML-DSA，源自 Dilithium）和 FIPS 205（SLH-DSA，源自 SPHINCS+）。

(4) 最新發展

目前尚未定案的剩餘候選演算法， NIST 於 2025 年 3 月 11 日正式宣布，選定 HQC（Hamming Quasi-Cyclic）[8] 作為第五個主要後量子密碼演算法，並指定其為目前主要加密演算法 ML-KEM 的備用替代方案。此舉是為因應未來若 ML-KEM 在實務應用中出現安全性缺陷或難以抵禦特定量子攻擊時，仍能有穩定且可靠的備援機制。根據 NIST 的規劃，HQC 的標準草案預計將於 2025 年底對外發布，並於 2027 年前完成標準制定，提供業界與政府單位充足的過渡期以完成系統轉型與整合。

[8] https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

表 2：各國後量子密碼遷移發布統整

國家	後量子密碼遷移相關文件	各國作法
德國	《Joint statement on Post-Quantum Cryptography》 2024 年 11 月	● 與歐洲多國聯合發布聲明：倡議早期遷移、強調混合加密部署。 ● 在 2030 年前完成保護敏感資料系統與基礎設施的遷移規劃與初步部署
荷蘭	《PQC Migration Handbook》 2024 年 12 月	三階段框架： ● 診斷（資產發現、風險分析） ● 規劃（遷移策略、預算與優先順序） ● 執行（部署與驗證）
英國	《Timelines for migration to post-quantum cryptography》 2025 年 3 月	● 2028 年前：完成資產盤點與初步規劃。 ● 2031 年前：完成優先資產的遷移。 ● 2035 年前：完成全面遷移。
加拿大	《Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES, Quantum-Readiness Working Group》 2024 年 7 月	● 步驟 0-2：準備→資產盤點→量子風險評估。 ● 步驟 3-5：實施遷移與驗證。 ● 提供檢核表與範例合約條款
韓國	《為量子轉型時代做準備》 2023 年 7 月	● 2021 年啟動「KpqC 後量子密碼競賽」，參考 NIST 流程，旨在選出符合韓國需求的 PQC 演算法。 ● 預計於 2035 年前完成國家密碼系統的全面轉換。
澳洲	《Planning for post-quantum cryptography》 2023 年 5 月	● 建立資產與應用清單。 ● 評估加密資產所保護資料的重要性。

		● 建立測試與轉換計畫。 ● 與供應商溝通遷移需求。 ● 教育與內訓相關部門。
美國	《NIST IR 8547》 2024 年 11 月 《PQC-migration-nist-sp-1800-38B》 2023 年 12 月 《QUANTUM-READINESS：MIGRATION TO POST-QUANTUM》 2023 年 8 月	● NIST 主導後量子密碼演算法的標準制定。 ● 強調測試場域與技術細節。 ● 要求聯邦機關率先規劃遷移。

資料來源：團隊自行整理

2. 後量子密碼標準與安全等級

美國於 2024 年 8 月公布了三個標準，包含 FIPS 203、FIPS 204、 FIPS205，旨在取代傳統的非對稱式加密，以應對量子電腦對傳統密碼的威脅。

NIST 公布這些標準的參數集設計，主要考慮了安全性和性能的平衡，FIPS 203 和 FIPS 204 基於模格（Module-Lattice-Based）理論，適合廣泛應用；FIPS 205 基於雜湊函數，適合無狀態需求，個別說明如下：

(1) FIPS 203：ML-KEM

FIPS 203 指定了基於模格（Module-Lattice-Based）的金鑰封裝機制標準（ML-KEM），源自 CRYSTALS-KYBER，允許兩方在公共通道上安全建立共享金鑰。參數集包括 ML-KEM-512（等級 1）、ML-KEM-768（等級 3）、ML-KEM-1024（等級 5），每個參數集有特定大小和安全性能。

NIST 建議預設使用 ML-KEM-768，提供合理性能和安全邊際，詳細的具體參數內容可參考 FIPS 203 標準文件[9]。

(2) FIPS 204：ML-DSA

FIPS 204 指定了基於模格（Module-Lattice-Based）的數位簽章標準（ML-DSA），源自 CRYSTALS-Dilithium，用於驗證資料完整性和身分。參數集為 ML-DSA-44（等級 2）、ML-DSA-65（等級 3）、ML-DSA-87（等級 5），每個集有不同鍵和簽章大小[10]。

(3) FIPS 205：SLH-DSA

FIPS 205 指定了無狀態雜湊基數位簽章標準（SLH-DSA），源自 SPHINCS+，適合高安全需求。參數集涵蓋安全等級 1、3、5，使用 SHA2 或 SHAKE，優化為小簽章（'s'）或快簽章（'f'），如 SLH-DSA-SHA2-128s 等[11]。

[9] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
[10] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf
[11] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

表 3：FIPS-203,204,205 內容與參數集

用途	傳統演算法	標準	規範名稱	初始名稱	參數集
金鑰交換	DH, ECDH, RSA…	FIPS 203	ML-KEM	CRYSTALS-Kyber	ML-KEM-512、ML-KEM-768、ML-KEM-1024
數位簽章	RSA, DSA, ECDSA…	FIPS 204	ML-DSA	CRYSTALS-Dilithium	ML-DSA-44、ML-DSA-65、ML-DSA-87
數位簽章	RSA, DSA, ECDSA…	FIPS 205	SLH-DSA	SPHINCS+	SLH-DSA-SHA2-128/SLH-DSA-SHAKE-128、SLH-DSA-SHA2-192/SLH-DSA-SHAKE-192、SLH-DSA-SHA2-256/SLH-DSA-SHAKE-256

資料來源：FIPS-203,204,205，團隊自行整理

3. 後量子密碼安全等級

NIST 將後量子密碼演算法的安全等級分為 1 至 5 類，每一類對應於與量子安全和傳統安全相同的安全等級，分別對應於 AES-128、SHA-256、AES-192、SHA-384 和 AES-256（官方分類見 NIST SP800-57 第 1 部分[12]及 NIST IR 8547[13]）。

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[13] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

表 4：後量子安全等級

	安全等級（Security Category）				
	第 1 級	第 2 級	第 3 級	第 4 級	第 5 級
攻擊類型	對 128 位元金鑰區塊密碼的金鑰搜尋	對 256 位元雜湊函數的碰撞搜尋	對 192 位元金鑰區塊密碼的金鑰搜尋	對 384 位元雜湊函數的碰撞搜尋	對 256 位元金鑰區塊密碼的金鑰搜尋
範例	AES-128	SHA-256	AES-192	SHA3-384	AES-256

資料來源：NIST IR 8547 草案，團隊自行整理

表 4 總結了 ML-KEM、ML-DSA 和 SLH-DSA 中安全等級與參數集之間的關係。隨著安全參數的提高，計算時間自然會增加，因此使用者必須根據自身情況選擇合適的安全等級。

表 5：FIPS 203、204、205 的安全等級

	安全等級（Security Category）				
	第 1 級	第 2 級	第 3 級	第 4 級	第 5 級
ML-KEM（FIPS 203）	• ML-KEM-512	--	• ML-KEM-768	--	• ML-KEM-1024
ML-DSA（FIPS 204）	--	• ML-DSA-44	• ML-DSA-65	--	• ML-DSA-87
SLH-DSA（FIPS 205）	• SLH-DSA-SHA2-128 • SLH-DSA-SHAKE-128	--	• SLH-DSA-SHA2-192 • SLH-DSA-SHAKE-192	--	• SLH-DSA-SHA2-256 • SLH-DSA-SHAKE-256

資料來源：FIPS-203,204,205，團隊自行整理

(四)傳統加密演算法的棄用與禁用時間表草案

1. 非對稱式加密

NIST 已於 2024 年 11 月 12 日發布 NIST IR 8547 初步公開草案[14]，文件標題為”過渡至後量子密碼標準”，內容為提出未來加密演算法的棄用[15]與禁用[16]時間表建議，並對大眾諮詢意見，目前使用的傳統非對稱密碼技術，如 RSA、ECDSA、EdDSA、ECC 等，2030 年起將進入棄用階段，並於 2035 年後全面禁用(見表 5、表 6)。

表 6：數位簽章演算法因應量子脆弱性之作法

數位簽章演算法家族[標準]	參數值	狀態
ECDSA[FIPS186]	• 112 位元的安全強度	• 2030 年後棄用 • 2035 年後禁用
	• ≥128 位元的安全強度	• 2035 年後禁用
EdDSA[FIPS186]	• ≥128 位元的安全強度	• 2035 年後禁用
RSA[FIPS186]	• 112 位元的安全強度	• 2030 年後棄用 • 2035 年後禁用
	• ≥128 位元的安全強度	• 2035 年後禁用

資料來源：NIST IR 8547 草案，團隊自行整理

[14]https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

[15]Deprecated（棄用）：演算法與密鑰長度可使用，但使用者須接受某些安全風險。這表示雖然可以繼續使用，但存在安全風險，使用者需評估風險是否可接受。

[16]Disallowed（禁用）：演算法或密鑰長度不再允許用於應用加密保護。這表示該演算法或密鑰長度已被禁止用於新的加密保護。

表 7：金鑰交換方案因應量子脆弱性之作法

金鑰交換方案 [標準]	參數值	狀態
有限域 DH 和 MQV [SP80056A]	• 112 位元的安全強度	• 2030 年後棄用 • 2035 年後禁用
	• ≥128 位元的安全強度	• 2035 年後禁用
橢圓曲線 DH 和 MQV [SP80056A]	• ≥112 位元的安全強度	• 2030 年後棄用 • 2035 年後禁用
	• ≥128 位元的安全強度	• 2035 年後禁用
RSA[SP80056B]	• 112 位元的安全強度	• 2030 年後棄用 • 2035 年後禁用
	• ≥128 位元的安全強度	• 2035 年後禁用

資料來源：NIST IR 8547 草案，團隊自行整理

2. 對稱式加密

對稱式密碼現有標準（如雜湊函數 SHA、區塊密碼、金鑰衍生函數等）相較非對稱式密碼（如 RSA 或 ECC）對量子攻擊的脆弱性較低。所有提供至少 128 位元的對稱式密碼，在 NIST 後量子密碼標準化過程中均至少滿足第 1 類安全等級，故於 2030 年後仍可繼續使用，然而，112 位元安全等級的標準則被認為不足以應對未來威脅，將於 2030 年後被禁用。這反映 NIST 為應對量子計算威脅而制定的轉型策略，確保長期安全性(見表 7、表 8)。

表 8：AES 因應量子脆弱性之作法

演算法	金鑰尺寸	加密狀態	棄用年份	禁用年份	建議替換參數組
AES	112 位元	2030 年後禁用	N/A	2030	AES-256
AES	128 位元	可接受，但後量子安全不足	N/A	N/A	AES-256
AES	192 位元	可接受	N/A	N/A	AES-256
AES	256 位元	可接受，後量子安全推薦	N/A	N/A	-

資料來源：NIST IR 8547 草案，團隊自行整理

表 9：雜湊/XOF 演算法安全強度及等級對照表

雜湊/XOF 演算法類型	變體	碰撞安全強度	碰撞安全等級	原像安全強度	原像安全等級
SHA-1 [FIPS180]	SHA-1	80 bits	<1	160 bits	1
SHA-2 [FIPS180]	SHA-224 SHA-512/224	112 bits	<1	224 bits	3
	SHA-256 SHA-512/256	128 bits	2	256 bits	5
	SHA-384	192 bits	4	384 bits	5
	SHA-512	256 bits	5	512 bits	5
SHA-3 [FIPS202]	SHA3-224	112 bits	<1	224 bits	3
	SHA3-256	128 bits	2	256 bits	5
	SHAKE128	128 bits	2	128 bits	2
	SHA3-384	192 bits	4	384 bits	5
	SHA3-512	256 bits	5	512 bits	5
	SHAKE256	256 bits	5	512 bits	5

資料來源：NIST IR 8547 草案，團隊自行整理

(五)訂定國家安全系統使用後量子演算法時程

美國國家安全局（National Security Agency, NSA）於2022年9月推出商業國家安全演算法套件2.0(Commercial National Security Algorithm Suite 2.0, CNSA2.0)(見表11)，作為未來國家安全級別的密碼標準，確保關鍵系統能夠抵禦量子電腦帶來的潛在威脅。

NSA於2024年12月發布CNSA常見問題更新版[17]，計劃在2035年之前所有國家安全系統（National Security System, NSS）具備量子抵抗能力，自2027年1月1日起，所有國家安全系統的新採購都必須符合CNSA2.0標準，到2030年12月31日，所有無法支援CNSA2.0的設備和服務都必須逐步淘汰，到2031年12月31日，強制要求使用CNSA2.0演算法。

NSA預計在2031年NSS完成向CNSA2.0的轉換之前，會有很長一段時間系統同時使用CNSA1.0(見表10)和2.0，隨著產業採用CNSA2.0演算法，NSA也將要求現有設備轉換到CNSA2.0，這在某些情況下可能需要硬體更新。

針對系統同時使用CNSA1.0和2.0之情形，一般稱之為混合式密碼方案（Hybrid Cryptographic Algorithms），另於下節介紹。

[17] https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

表 10：CNSA1.0 內容與參數集

演算法	功能	規格	參數集
高級加密標準（AES）	對稱區塊密碼，用於資訊保護	FIPS PUB 197	使用 256 位元金鑰
橢圓曲線 Diffie-Hellman（ECDH）	非對稱演算法，用於金鑰建立	NIST SP 800-56A	使用 P-384 曲線
橢圓曲線數位簽章演算法（ECDSA）	非對稱演算法，用於數位簽章	FIPS PUB 186-4	使用 P-384 曲線
安全雜湊演算法（SHA）	計算資訊壓縮表示的演算法	FIPS PUB 180-4	使用 SHA-384
Diffie-Hellman（DH）	非對稱演算法，用於金鑰建立	IETF RFC 3526	最小 3072 位元模型
RSA（金鑰建立）	非對稱演算法，用於金鑰建立	NIST SP 800-56B rev 1	最小 3072 位元模型
RSA（數位簽章）	非對稱演算法，用於數位簽章	FIPS PUB 186-4	最小 3072 位元模型

資料來源：CNSA1.0

表 11：CNSA2.0 內容與參數集

演算法	功能	規格	參數集
高級加密標準（AES）	對稱區塊密碼，用於資訊保護	FIPS PUB 197	對所有分類等級使用 256 位元金鑰
ML-KEM（原 CRYSTALS-Kyber）	非對稱演算法，用於金鑰建立	FIPS PUB 203	ML-KEM-1024 適用於所有分類等級
ML-DSA（原 CRYSTALS-Dilithium）	非對稱演算法，用於數位簽章，適用於任何用例，包括簽署韌體和軟體	FIPS PUB 204	ML-DSA-87 適用於所有分類等級
安全雜湊演算法（SHA）	計算資訊壓縮表示的演算法	FIPS PUB 180-4	對所有分類等級使用 SHA-384 或 SHA-512
特定應用允許的演算法			
Leighton-Micali 簽章（LMS）	用於數位簽署韌體和軟體的非對稱演算法	NIST SP 800-208	所有參數均適用於所有分類等級。建議使用 LMS SHA-256/192
擴展 Merkle 簽章方案（XMSS）	用於數位簽署韌體和軟體的非對稱演算法	NIST SP 800-208	所有參數均適用於所有分類等級
安全雜湊演算法 3（SHA3）	用於計算資訊壓縮表示的演算法，作為硬體完整性的一部分	FIPS PUB 202	SHA3-384 或 SHA3-512 僅允許用於內部硬體功能（例如，啟動完整性檢查）

資料來源：CNSA2.0

三、混合式密碼方案介紹[18]

(一)混合式密碼方案概述

混合式密碼方案（Hybrid Cryptographic Algorithms）是一種在傳統公鑰加密演算法和後量子加密演算法之間過渡的解決方案。該方案結合了現有的成熟傳統演算法和新興的量子抗性演算法，旨在確保在量子計算威脅日益增加的情況下，仍

[18]https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.ipd.pdf

能維持當前加密系統的安全性。這樣的過渡可以繼續使用傳統演算法，同時在後量子加密技術成熟之前，逐步過渡到完全的後量子密碼演算法。

混合式密碼方案的目的是結合傳統公鑰加密演算法和後量子加密演算法的優勢，以應對量子計算帶來的挑戰。常見的混合演算法形式包括傳統簽章演算法（如橢圓曲線數位簽章演算法 ECDSA）與後量子簽章演算法（如 ML-DSA）的結合，或傳統金鑰建立演算法（如 Diffie-Hellman 金鑰交換）與後量子金鑰封裝機制（如 ML-KEM）的結合。

(二)混合方案的優缺點

- 優點：
  - 安全過渡：混合簽章或金鑰建立方案能夠在過渡過程中提供穩定的安全保障，減少轉向完全後量子密碼後的風險。
  - 靈活性：混合演算法能夠支持多種加密套件，增加協議的靈活性和適應性。
- 缺點：
  - 協議複雜性增加：使用混合方案會導致加密協議的結構變得更加複雜。
  - 資源消耗：混合方案需要更多的計算資源和帶寬，對系統性能會產生額外負擔。
  - 二次遷移：當傳統演算法被棄用時，系統可能需要再次遷移，增加長期成本。
  - 安全分析：混合方案的安全性分析更複雜，需要確保兩種演算法的組合不會引入新漏洞。

(三)混合式密碼方案的場域

1. 安全通訊協議

如 TLS(傳輸層安全協議)和 IPsec(網際協議安全)，混合方案可用於關鍵交換。例如，客戶端和伺服器可以同時執行 Diffie-Hellman 關鍵交換（參考 SP 800-56A，SP

800-56A）和 ML-KEM（FIPS-203），通過雜湊函數結合共享金鑰，確保對抗經典和量子攻擊。

2. 數位簽章

在軟體更新、文件簽章或區塊鏈交易中，可以使用混合簽章，如 ECDSA（傳統）和 ML-DSA（FIPS-204）的組合，確保至少一種簽章有效。

3. 安全電子郵件

如 S/MIME 協議，可以使用混合簽章保護郵件完整性和發送者身分。

4. 身分驗證系統

在訪問控制或單點登錄（SSO）中，混合方案可確保身分驗證過程的安全性。

(四)混合式密碼方案與加密敏捷性之關連

1. 靈活的演算法支持

透過混合方案，系統可以同時支持多種演算法，例如在 TLS 協議中使用混合金鑰建立方案（如 ECC 與 CRYSTALS-KYBER 結合），允許在遷移期間逐步淘汰傳統演算法。

2. 漸進式遷移

混合方案允許組織在現有基礎設施上逐步引入後量子密碼演算法，而無需立即更換所有系統。這有助於降低遷移成本和複雜性，特別是考慮到後量子密碼演算法（如 CRYSTALS-KYBER）的公鑰大小較大，可能影響性能。

3. 安全性

混合方案確保系統在遷移期間保持安全，因為即使某個演算法被量子計算機破解，另一個演算法仍可提供保護。

例如，NIST 的 FAQ[19]提到，混合金鑰建立方案的衍生金鑰在至少一個組件安全時仍安全。

4. 標準化的支持

NIST 的安全強度分類（1、2、3、4、5）有助於比較不同演算法，並為未來密碼學轉型提供靈活性。這些分類鼓勵在安全性和效率之間進行權衡，進一步支持密碼學敏捷性。

(五)運用混合式密碼方案考量因素

混合方案在 FIPS-203、204、205 標準的背景下，為遷移到後量子密碼學提供了實用的解決方案，適用於安全通訊、數位簽章和身分驗證等場景。雖然帶來複雜性和資源挑戰，但它確保了對抗傳統攻擊和量子攻擊的雙重保護，符合 NIST 密碼靈活性的目標。

混合式密碼方案提供了一個有效的過渡方案，能夠在傳統密碼和後量子密碼之間提供保障。儘管混合方案在過渡期中具有顯著的安全性優勢，但也會增加協議的複雜性和系統資源的消耗。因此，在選擇是否使用混合方案時，建議仍需要全面考慮安全需求、實施成本以及未來的技術發展。

[19]https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

參、後量子密碼遷移指引

後量子遷移的適用範圍涵蓋所有需要轉換至後量子加密技術的組織。現今數位服務系統大量使用 RSA 等易受量子攻擊的加密演算法，遷移至後量子密碼旨在提升這些系統的防禦能力。

具體而言，這包括各行各業的數位服務基礎設施，如網路協議、終端用戶系統、伺服器等，並涉及內外部層面的準備，例如技術升級、風險評估及供應鏈協調。

一、後量子密碼遷移路線圖說明

本指引主要參考美國國家標準及技術研究所（National Institute of Standards and Technology, NIST）公布之後量子遷移文件，所參考文件包括：NIST-SP-1800-38A、NIST-SP-1800-38B、NIST IR 8547 、 QUANTUM-READINESS ： MIGRATION TO POST-QUANTUM、TNO CWI AIVD The PQC Migration Handbook，綜整後量子遷移的四個步驟如下：

(一)建立量子準備計畫

組織應設立專案管理團隊，評估遷移時機（參考 Mosca 不等式：X 為資產必須保密的年限，Y 為遷移所需時間，Z 為量子電腦出現時間），並制定遷移至後量子演算法的基礎策略。這包括確認技術需求與時程規劃。

(二)盤點加密資產清單

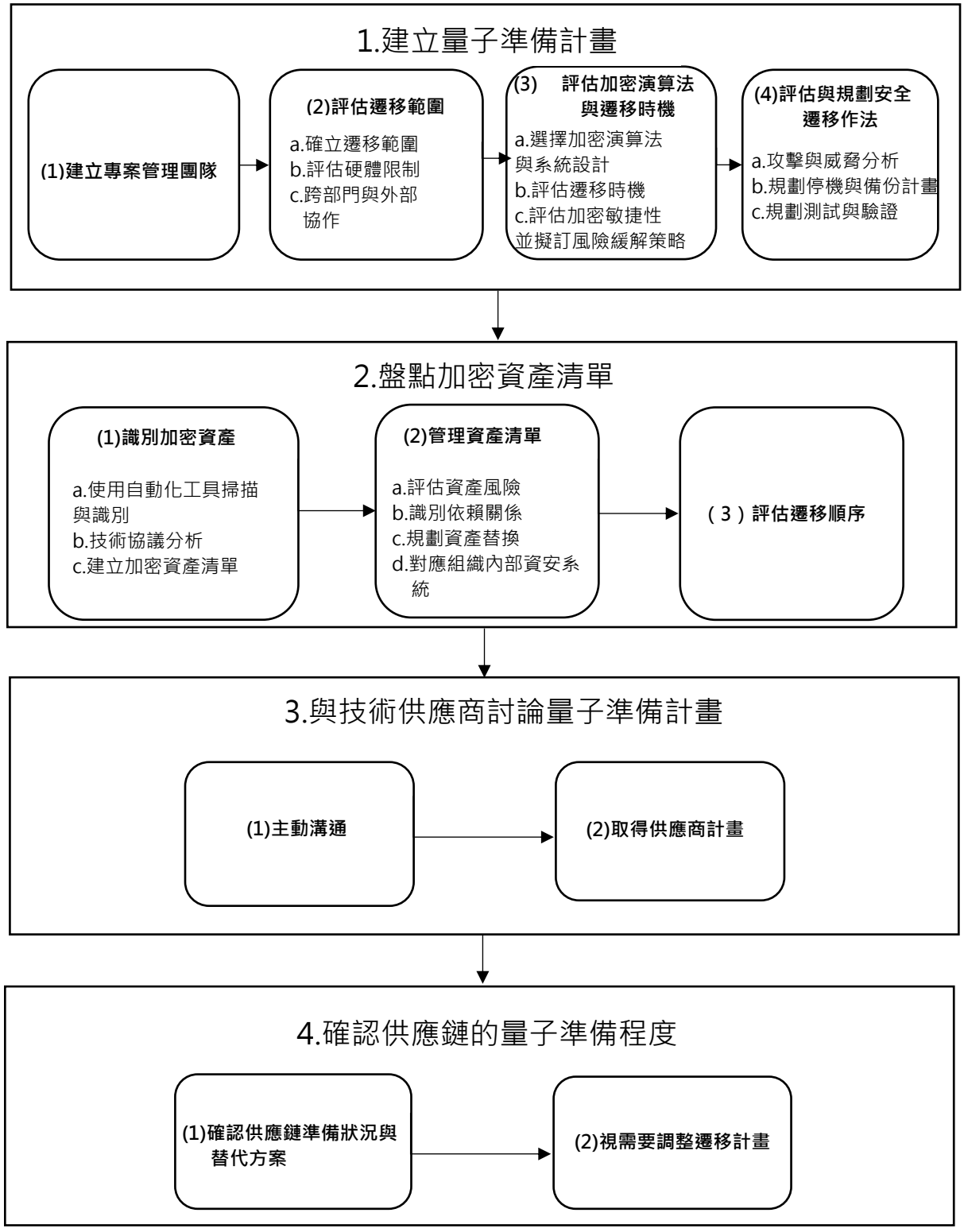
利用自動化工具識別系統中易受量子攻擊的加密演算法（如 TLS、SSH、IPsec 協議），並對資產進行優先級排序。風險評估需考量資產的重要性、故障影響、受攻擊風險及可用資源。

(三)與技術供應商討論量子準備計畫

組織應與技術供應商合作，了解其量子準備路線圖與遷移方案，確保供應商的技術支援與產品能符合後量子密碼要求。

(四)確認供應鏈的量子準備程度

組織應瞭解系統和資產中易受量子攻擊的相依性，並了解供應鏈中的供應商將如何遷移至後量子密碼。確保遷移計畫能盡可能減少量子攻擊風險，並符合組織的轉型策略。



資料來源：本計畫自行整理

圖 1：後量子密碼遷移路線圖

二、建立量子準備計畫

後量子密碼標準目前已逐步公布，組織應建立量子準備計畫以為因應。首先，應成立專案管理團隊，規劃並界定組織遷移至後量子密碼的範圍，專案團隊需主動進行密碼學發現活動，識別組織目前對量子易受攻擊密碼學的依賴，這些系統與資產包括創建和驗證數位簽章的系統，並涉及軟體與韌體更新，組織可參考下列流程建立計畫：

(一)成立專案管理團隊

組織應建立專案管理團隊，包含資安與隱私風險管理人員，並指派一位遷移經理，負責遷移的執行。

(二)評估遷移範圍

1. 確立遷移範圍

為評估密碼遷移範圍，組織應盤點各類系統與元件，例如作業系統、通訊產品、物聯網設備等，並考量特定應用需求，如無人機、汽車、企業資料中心、智慧家電和醫療設備等。

2. 評估硬體限制

由於後量子加密演算法計算資源較大，現有加密硬體可能無法滿足需求。若硬體性能不足，則應規劃升級或更換以確保系統安全與可行性。

3. 跨部門與外部協作

考量到不同組織間加密系統和資產的關聯性，可共同合作進行遷移計畫，使參與組織能夠更有效地完成遷移。

(三)評估加密演算法與遷移時機

1. 選擇加密演算法與系統設計

不同的後量子演算法會影響加密的效能，因此選擇加密演算法時需要考慮金鑰大小、簽章大小以及所需資源等，可參考本指引第二章中美國所公布之相關規範文件（詳見本指引表 2~表 9）。

2. 評估遷移時機

組織要判斷遷移至後量子演算法的時機可參考莫斯卡量子風險評估架構（如表 10）[20]。架構中的莫斯卡不等式由加拿大滑鐵盧大學 Michele Mosca 教授提出。莫斯卡不等式將 x、y、z 定義為以下年數：x:資產必須保密的年限，y:完成量子安全狀態所需的時間，z:估算出量子電腦出現時間，如果 x+y>z，則有問題，應考慮遷移到後量子密碼。

3. 評估加密敏捷性並擬訂風險緩解策略

由於後量子加密演算法正在持續開發與標準化，後量子遷移並非能一次完成，而是需要漸進式的更新，故組織的系統應設計成可快速適應新的加密演算法。

由於從一種加密解決方案過渡到另一種解決方案可能需要很長時間，並使組織面臨不必要的安全風險。組織可透過密碼敏捷性風險評估框架（Crypto Agility Risk Assessment Framework, CARAF）[21]評估因缺乏加密敏捷性而導致的風險並擬訂合適的風險緩解策略（評估框架參見表 11）。

(四)評估與規劃安全遷移作法

1. 攻擊模擬與威脅分析

組織為了要識別潛在的量子攻擊安全風險，可使用攻擊模擬與威脅分析流程（Process for Attack Simulation and Threat Analysis, PASTA）[22]系統性的進行風險評估，針對評估量子攻擊風險，PASTA 共分為七個步驟（分析流程參考表 12）。

2. 規劃停機與備份計畫

在遷移過程中，某些服務和系統可能需要暫時關閉，需對停機時間進行妥善規劃，制定健全的備份計畫。

[20] https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/

[21] https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForAPostQuantumWorldByManagingCryptographicRisk.pdf

[22] https://pureadmin.qub.ac.uk/ws/files/240369002/Quantum_Computing_Threat_Modelling_on_a_Generic_CPS_Setup_ACNS_Workshop_20210503.pdf

3. 規劃測試與驗證

為了提供預期的安全性水準，軟硬體的新演算法都需要經過測試階段。測試必須確保新演算法與現有基礎架構相容，並能夠提供預期的安全性水準。

表 12：莫斯卡量子風險評估架構

- **第一階段**：識別並記錄具有價值的資產，確認其加密強度及所使用的加密技術類型。
- **第二階段**：研究新興的量子計算技術及後量子加密技術的發展狀況。
- **第三階段**：識別潛在的威脅行為者，並評估其獲取量子計算技術的時間。估算出量子電腦出現時間「z」。
- **第四階段**：確認資產必須保密的年限「x」，並評估當這些資產在量子電腦出現且面臨安全風險時，可能對組織造成的影響。同時，計算組織將這些資產轉換為量子安全狀態所需的時間「y」。
- **第五階段**：透過計算「x + y > z」來評估系統的量子風險，即判斷資產是否會在組織採取防護措施之前受到影響，從而決定是否需要立即行動以應對量子安全威脅。
- **第六階段**：確定保持對量子攻擊的危機意識，準備將組織的技術遷移到量子安全狀態所需的活動，並確定其優先順序。

資料來源：Global Risk Institute

表 13：加密敏捷性風險評估框架（CARAF）

- **第一階段：識別威脅。**找出可能影響加密資產的潛在威脅。
- **第二階段：資產清單。**建立受影響資產的詳細清單，包括資產的性質以及可能面臨的安全風險與暴露情況。
- **第三階段：風險評估。**根據已識別的風險暴露情境，對資產進行優先排序，以決定風險緩解的優先順序。與一般常見的「 風險 =影響x機率 」評估方法不同，CARAF 的公式為「 風險=時間x成本 」。時間由莫斯卡定理的一、二階段得出。成本為在所需時間內將資產更新為安全狀態的成本。
- **第四階段：透過風險緩解措施保護資產。**
  1. 當資產價值較高時，應投入資源確保其安全性。
  2. 當風險的預期影響較低時，可接受風險並維持現狀。
  3. 當安全成本過高時，可分階段決策以減少對資產的影響。
- **第五階段：組織策略規劃。**組織應制定長遠的加密策略，並提供支持與指導，確保不同團隊能夠根據風險評估結果來做出最佳加密技術選擇與決策。

資料來源：FS-ISAC

表 14：攻擊模擬與威脅分析流程（PASTA）

- **階段一**：建立威脅建模流程的基礎。
  1. 識別關鍵業務目標及其安全性影響
  2. 定義特定的安全需求與法規遵循需求
  3. 為威脅建模流程建立指標
  4. 決定關鍵利害關係人及其角色
- **階段二**：定義技術範圍
  1. 記錄所有系統元件及技術文件
  2. 識別資料流
  3. 建立分析範圍
- **階段三**：應用程式分解與分析
  1. 將應用程式分解為核心元件
  2. 分析元件之間的資料流
  3. 識別安全控制及其位置
  4. 記錄相依性和整合點
- **階段四**：威脅分析
  1. 找出潛在的威脅發動者及其動機
  2. 分析攻擊模式與技巧
  3. 根據歷史資料和產業情報建立威脅檔案
  4. 將威脅對應至特定系統元件
- **階段五**：弱點分析
  1. 進行全面的弱點評估
  2. 分析系統弱點和設計缺陷
  3. 將漏洞對應至已識別的威脅
  4. 根據潛在影響優先處理漏洞
- **階段六**：攻擊模擬
  1. 建立詳細的攻擊情境
  2. 模擬潛在的攻擊路徑
  3. 在各種條件下測試安全控制
  4. 驗證現有防禦措施的有效性
- **階段七**：風險與影響分析
  1. 計算已識別威脅的潛在業務影響
  2. 評估成功攻擊的可能性
  3. 根據業務影響來排定風險的優先順序

4. 制定風險緩解策略

資料來源：Queen’s University Belfast

三、盤點加密資產清單

為了應對量子電腦的威脅，組織必須建立加密清單。此清單應列出 IT 和 OT 系統中易受量子攻擊的弱點，特別是保護敏感和關鍵資料。通過了解這些易受攻擊弱點的區域及其保護資料的重要性，組織可優先考慮遷移至後量子密碼。這需要使用工具在網路協議、終端用戶系統及伺服器等中識別加密清單。此外，組織應將此清單與現有安全計畫整合，以獲得全面視角並確定高風險區域。此清單將指導風險評估過程，確保在關鍵領域及時實施後量子密碼。

(一)識別加密資產

1. 使用自動化工具掃描與識別

   自動化工具可用來識別各個領域中的易受攻擊演算法，包括網路協議、終端用戶系統和伺服器上的資產，掃描與識別實例可參考本指引附件。

2. 分析技術協議

   組織應對多種技術協議進行掃描，以識別其中使用的易受攻擊加密技術。常見的協議包含：

   (1) 傳輸層安全協定（Transport Layer Security, TLS）

   (2) 應用層安全協定（Secure Shell Protocol, SSH）

   (3) 網際網路安全協定（Internet Protocol Security, IPsec）

3. 建立加密資產清單：組織應掌握內部加密技術使用情形，建立完整的加密資產清單，以助於確定遷移優先順序。完整的加密資產清單包含：

   (1) 盤點範圍：包含外部供應商（例如：硬體、軟體等）、內部系統（例如：通訊系統、作業系統以及未經授權的軟硬體等）、及其相關資訊（例如：產品、合約、聯絡方式等）。

   (2) 應用場景：包含內部通訊、伺服器、公共網際網路等。

   (3) 清單內容：包含記錄資料類型（例如：靜態、傳輸中、使用中等）、資料位置、機密性、價值、分級及風險評估。

(二)管理資產清單[23]

1. 評估資產風險

為識別系統中的潛在風險，組織應進行風險評估，考量因素如下：

(1) 該系統是否為高價值資產

(2) 該系統是否有儲存高機密資訊

(3) 該系統是否與其他系統有介接

(4) 該系統是否與政府機關有資訊來往

(5) 該系統是否與其他企業有資訊來往

(6) 該系統是否涉及關鍵基礎設施

(7) 該系統需要保護的時間多長

2. 識別依賴關係

為了識別不同加密資產之間的依賴關係並確定遷移的順序，這些依賴關係應該於加密資產清單中明確標示。

3. 規劃資產替換

建立加密資產清單並釐清依賴關係後，即可規劃資產替換，對每個資產，需評估重要性、故障影響、受攻擊風險及可用資源，決定是否替換、重新設計或淘汰。

4. 對應組織內部資安系統[24]

組織應將加密資產清單與現有資安系統進行比對，例如：

(1) 身分憑證與存取管理（Identity Credential and Access Management, ICAM）

(2) 身分與存取管理（Identity and Access Management, IdAM）

[23]https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

[24]同前註

(3) 端點檢測與回應（Endpoint Detection and Response, EDR）

(4) 持續診斷與緩解系統（Continuous diagnostics and mitigation, CDM）

(三)評估優先順序

為了確保在過渡到後量子密碼的過程中，優先處理最具風險的元件，組織應依據資訊的敏感性和重要性進行優先排序。

待遷移計畫已完成初步規劃,並成功建立加密資產盤點表後,組織即可進一步參考表 15 所列之評估問題清單，以全面性檢視遷移計畫的整體準備狀態。

參考資料：FS-ISAC Post-Quantum Cryptography (PQC) Working Group 附錄 C，本團隊自行整理

表 15：組織遷移評估問題清單
● 公司資訊長是否已參與後量子密碼學相關標準的制定？
● 公司內部是否清楚量子計算到來後，必須保護的資料集是哪些？
● 公司內部是否意識到資料未來可能被量子電腦解密？
● 公司內部是否清楚所有使用加密技術的系統，以促進未來平穩過渡？
● 公司內部是否確定需要更新以反映後量子時代要求的資料安全標準？
● 公司內部是否正在確定公鑰密碼學被用於何處、為何目的，以及標記這些系統為量子脆弱的？
● 公司內部是否有辦法考慮資產價值、金鑰存儲、通訊、與其他實體的聯繫、關鍵基礎設施或資料受保護的時間長短等因素，確定加密過渡系統的優先級？
● 公司內部是否制定了用於發布新的後量子密碼學標準後進行系統過渡的路線圖？

四、與技術供應商討論量子準備計畫

建議各組織開始與其技術供應商接觸，了解供應商的量子準備路線圖，包括供應商的後量子遷移計畫。完整的路線圖應描述供應商如何計劃遷移至後量子密碼，並列出測試後量子密碼及整合至產品的時間表。

(一)主動溝通

組織應積極與技術供應商溝通，以瞭解供應商的後量子準備程度，包括遷移方案。

(二)取得供應商計畫

供應商應主動公布其量子準備計畫，計畫應概述如何過渡到後量子密碼與整合到產品中的時間表。可參考表 16 的問題清單來評估供應商的準備情況。

五、確認供應鏈的量子準備程度

組織應評估其對量子易受攻擊加密對供應鏈的依賴程度，並了解供應鏈供應商如何遷移至後量子密碼，並優先考慮高影響系統、工業控制系統和需要長期機密性的系統供應鏈。

(一)確認供應鏈準備狀況與替代方案

若組織的加密資產是由外部供應商提供。則須確保供應商是否有將資產過度到後量子密碼，否則需要尋找新的供應商。

(二)視需要調整遷移計畫

依實際情形對遷移計畫進行調整。於進行遷移計畫評估時，可參考使用檢核表對遷移計畫進行初步評估，以確認遷移計畫之完整性，檢核表可參照表 17。

表 16：供應商遷移評估問題清單

Q1：請問貴公司有什麼規劃來讓您的產品/服務支援後量子密碼學？預計何時能全面支援後量子加密？
Q2：未來貴公司的產品/服務會透過現有的合約或更新來提供後量子加密支援嗎？還是需要額外購買新版本或服務？
Q3：請問貴公司的產品/服務若要支援後量子加密，是否需要更換硬體或調整系統架構？
Q4：請問貴公司的產品/服務是否具備加密敏捷性？能否在既定的加密遷移計畫內靈活調整？如果演算法被發現有漏洞，是否能立即切換到更安全的選項？
Q5：請問貴公司會提供哪些操作指南，來協助客戶將產品/服務遷移至後量子加密？
Q6：當貴公司的產品/服務更新後支援後量子加密，是否會確保加密技術通過獨立驗證？
Q7：貴公司是否有評估第三方供應商對量子威脅的因應措施？他們的後量子加密準備狀況是否可能影響您的業務運作或客戶安全？
Q8：如果對這些問題的回答有進一步疑問，是否能提供聯絡人資訊，以便後續討論？

資料來源：Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES 附錄 G，本團隊自行整理

表 17：後量子遷移檢核表

項目	描述
確認演算法實施	驗證所有系統都使用 NIST 推薦的標準化後量子密碼，如 CRYSTALS-KYBER 和 CRYSTALS-Dilithium。
互操作性測試	確保系統之間使用新演算法能安全通訊，特別是跨不同供應商的系統。
性能評估	檢查新演算法是否顯著影響系統性能，例如處理速度或資源使用。
安全審計	進行徹底的安全審計，檢測遷移過程中是否引入漏洞，特別是與新演算法相關的潛在弱點。
文件更新	更新所有相關文件，包括安全政策、程序和技術文檔，以反映新的密碼學標準。
員工培訓	對 IT 和安全團隊進行培訓，確保他們了解新系統的操作和維護。
持續監控	設置監控系統以檢測與新後量子密碼實施相關的安全事件，例如異常流量或攻擊嘗試。
供應商合規性	確認所有第三方供應商和合作夥伴在必要時也已遷移至後量子密碼，並符合標準。
備份與恢復	確保備份和恢復過程與最新的後量子密碼標準兼容，特別是涉及加密資料的恢復。
監管合規性	驗證遷移是否符合任何適用的監管要求，例如金融部門的資料保護法規。

資料來源：Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES 附錄 E，本團隊自行整理

肆、參考文獻

[1] pqc-migration-nist-sp-1800-38a-preliminary-draft, Migration to Post-Quantum Cryptography：Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography, April 2023.

[2] pqc-migration-nist-sp-1800-38b-preliminary-draft, Migration to Post-Quantum Cryptography Quantum Readiness：Cryptographic Discovery, December, 2023.

[3] NIST Internal Report NIST IR 8547 ipd, Transition to Post-Quantum Cryptography Standards, November, 2024.

[4] QUANTUM-READINESS：MIGRATION TO POST-QUANTUM CRYPTOGRAPHY, August, 2023.

[5] TNO CWI AIVD The PQC Migration Handbook, GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY, December, 2023.

[6] TNO CWI AIVD The PQC Migration Handbook, GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY, December, 2024.

[7] Canadian National Quantum-Readiness BEST PRACTICES AND GUIDELINES, Quantum-Readiness Working Group（QRWG）of the Canadian Forum for Digital Infrastructure Resilience （CFDIR）, Version 04 -July 10, 2024

[8] NIST SP 800-208：Recommendation for Stateful Hash-Based Signature Schemes

[9] NIST FIPS 203：Module-Lattice-Based Key-Encapsulation Mechanism Schemes

[10]NIST FIPS 204：Module-Lattice-Based Digital Signature Standard

[11]NIST FIPS 205：Stateless Hash-Based Digital Signature Standard

[12]P.-Q.C.W. Group. Risk model technical paper[R].FS-ISAC Post-Quantum Cryptography Working Group, 2023.

[13]Considerations for Achieving Cryptographic Agility：Strategies and Practices, July, 2025

[14]Kryptografie quantensicher gestalten, Bundesamt für Sicherheit in der Informationstechnik, December, 2021

[15]Next steps in preparing for post-quantum cryptography, National Cyber Security Centre, August 2024

[16]Building safe digital Korea through consolidated cybersecurity capabilities, The Ministry of Science and ICT, July 2023

[17]Planning for post-quantum cryptography, Australian Cyber Security Centre, May 2023

[18]NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part1 – General, May 2020

[19]The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, National Security Agency, December 2024

[20]A Methodology for Quantum Risk Assessment, Dr.Michele Mosca John Mulholland, January 2017

[21]Preparing for a Post-Quantum World byManaging Cryptographic Risk, FS-ISAC's Post-Quantum Cryptography Working Group, March 2023

[22]Quantum Computing Threat Modelling on a Generic CPS Setup, Lee, C. C., Tan, T. G., Sharma, V., & Zhou, J, 2021

[23] Timelines for migration to post-quantum cryptography, NCSC ,March 2025

[24] joint statement on Post-Quantum Cryptography, BSI, November 2024

附件：運用密碼系統安全性評測工具進行加密資產清單盤點參考案例

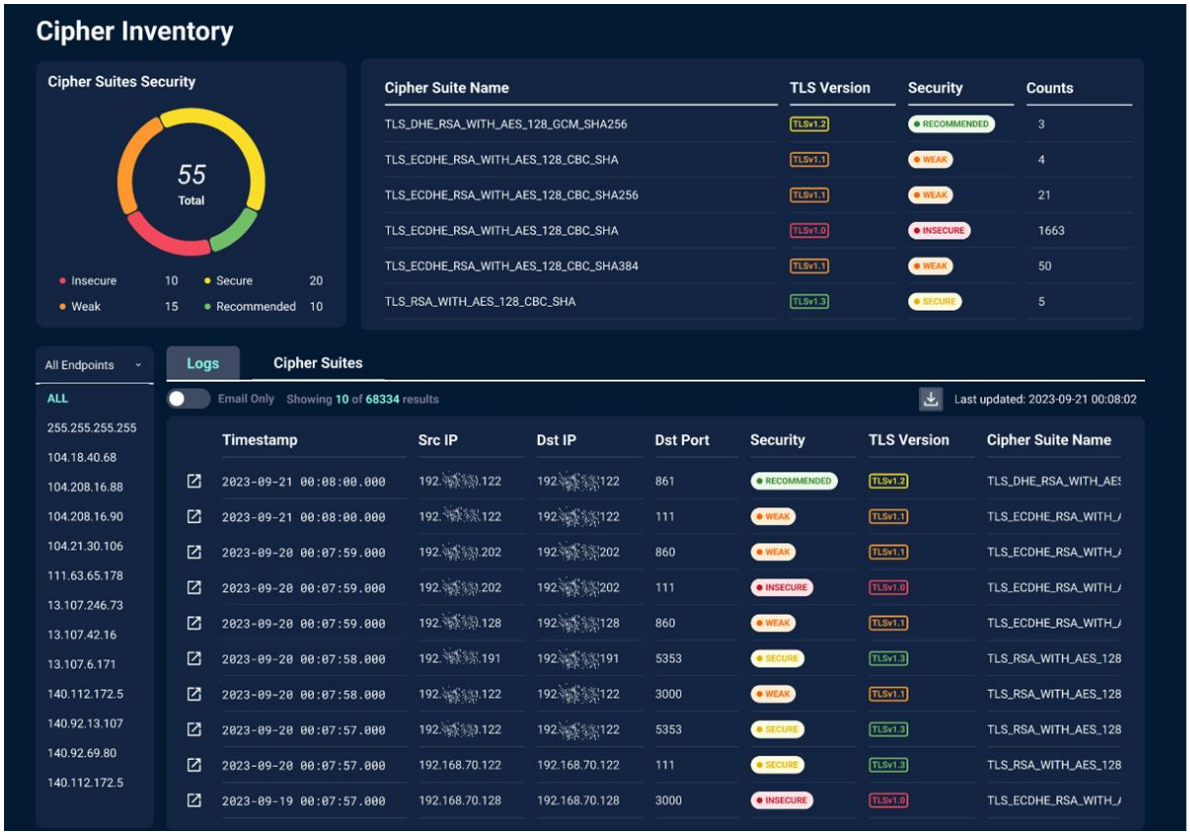
廠商可透過自動化工具檢測應用系統傳輸安全性，以流量分析加密演算法、金鑰長度、憑證加密等資訊，評估應用系統所使用的加密安全等級。，以更好地保護企業的資產和資料，以下以後量子安全評測工具之實例，說明使用自動化工具之可能作法。

一、後量子安全評測工具說明

為預防先竊取後解密（Harvest Now, Decrypt Later, HNDL）新興攻擊手法，組織可使用後量子安全評測工具針對密碼系統特徵進行盤點，並提供盤點報告，可追蹤弱加密（Weak）或不安全加密（Insecure）之端點或服務進行密碼系統升級，以提升安全性。

網路密碼系統評等可能為下列四級：

- 建議（Recommended）
- 安全（Secure）
- 脆弱／已不符合最新的加密標準（Weak）
- 不安全／已證明存在漏洞（Insecure）



(a)

時間	來源IP	來源Port	目的IP	目的Port	加密演算法	版本	服務說明	安全等級
2024-08-0(	1oo.oo.oo.oo4	64435	1xx.xx.xx.xx1	443	TLS_AES_256_GCM_SHA384	TLSv13	itxxxx.xxxx.com	RECOMMENDED
2024-08-0(	1oo.ooo.ooo.o8	55119	1xx.xx.xx.5	443	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv12	xxxmail.xxx.xxx.tw	SECURE
2024-08-0(	1oo.oo.oo.o0	60127	1xx.xx.xx.3	444	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv12	xxxmail.xxx.xxx.tw	SECURE
2024-08-0(	1oo.ooo.oo.oo3	58296	1xx.xx.xx.xx6	4461	TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv12	erpxxx.xxxx.com	WEAK
2024-08-0(	1oo.oo.oo.o9	56236	1xx.xx.xx.xx9	443	TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv12	xxxxx.xxxxx.com	WEAK
2024-08-0(	1oo.oo.oo.oo9	60276	1xx.xx.xxx.x7	4509	TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv12	aaaa.aaaaa.com	WEAK
2024-08-0(	1oo.oo.oo.o2	49281	1xx.xx.xx.xx1	10003	TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv12		WEAK
2024-08-0(	1oo.oo.ooo.o6	56391	1xx.xx.xx.x6	8443	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv12		WEAK

(b)

資料來源：本團隊自行整理

圖 1：自動化工具平台，支援下載盤點清單

二、網路密碼系統評測分析

本團隊透過先期驗證，已使用國產後量子安全評估工具，透過側錄場域資訊系統流量，進行實際場域的加密傳輸安全分析並對場域主提供建議，發現場域普遍有脆弱及已不符合最新加密標準的高風險、需關注之通訊連線。

高風險、需關注通訊連線：

- 脆弱 / 已不符合最新的加密標準（Weak）：12345 筆

具風險之密碼套件	TLS 版本	主要風險內容
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	**TLSv10**	**2013年已被證明 TLS 1.0、SSL 3.0 及更早版本的 CBC 模式易受明文攻擊。**
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv12	易受到 *DHEat 攻擊，攻擊者可以在不需要身份驗證的情況下，發起拒絕服務（*DoS）攻擊。
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv12	使用 RSA 進行金鑰交換，無法保證前向安全（*PFS）。

❖ 盤點應對建議：

1. 優先查檢盤點清單（平台或.csv）標記為 Weak 或 Insecure 之通訊行為的所屬端點設備（IP）。
2. 針對具風險之設備，不一定要全盤升級，可先評估設備服務重要性、通訊資料機敏性、升級成本等，以判斷升級急迫性，進而規劃升級計畫。

DHEat: Diffie-Hellman Exploit Against Authenticated Key Exchange

DoS: Denial-of-Service attack

PFS: Perfect Forward Secrecy

資料來源：本團隊自行整理

圖 2：場域加密傳輸風險報告

綜整場域加密傳輸重要風險，其中最為嚴重是使用已棄用之 TLS v1.0 的加密版本，此項目必須優先處理。其他使用 TLS v1.2 之弱加密演算法需進一步評估應用服務的資產重要性、資料留存的時間及應用服務的遷移時間長度，進而排入遷移規畫作業。

本團隊實證透過自動化工具掃瞄，可快速掌握場域加密傳輸之風險，加速盤點組織資產，有助於組織規劃後量子遷移計畫。

三、後量子密碼遷移技術支援

為協助企業和組織順利過渡至後量子密碼，針對後量子密碼技術發展以及國內提供後量子技術相關資源可參見資安整合服務平台-PQC 資安專區，網址如下：

https://secpaas.org.tw/W_Menu_Page?ID=33