新加坡 CSA 網路安全標籤計畫 (CLS) 深度研究報告：CCC SP-151-4 IoT 評估方法論與合規實務全解

編輯原稿

1. 執行摘要 (Executive Summary)

隨著物聯網 (Internet of Things, IoT) 設備在家庭、醫療及工業領域的滲透率呈指數級增長，其相關的網路安全風險亦隨之攀升。作為全球數位化轉型的領先國家，新加坡網路安全局 (Cyber Security Agency of Singapore, CSA) 推出了亞太地區首個多層次的網路安全標籤計畫 (Cybersecurity Labelling Scheme, CLS)。該計畫旨在透過可視化的安全標籤，提升消費者對 IoT 產品安全性的認知，並激勵製造商採取「安全設計 (Security-by-Design)」的開發原則。

本研究報告將針對 CLS 架構中的核心技術文件——**CCC SP-151-4 CLS(IoT) Assessment Methodology (IoT 網路安全標籤計畫評估方法論)** 進行詳盡的解析。該文件不僅定義了製造商 (Manufacturers) 必須遵循的合規路徑，更是測試實驗室 (Testing Laboratories, TLs) 執行第三方驗證的標準依據。報告內容涵蓋 2023 年至 2025 年間的重大制度變革，包括強制性實驗室審查的引入、與德國 BSI 及韓國 KISA 的互認協議 (Mutual Recognition Arrangements, MRAs)，以及針對 Wi-Fi 家庭閘道器 (Home Gateways) 新增的專屬評估標準。

本報告旨在為網路安全專家、合規工程師及 IoT 產品開發者提供一份權威性的參考指南。透過深入剖析從 Level 1 到 Level 4 的具體評估條款、證據提交要求 (Supporting Evidence) 及驗收標準 (Acceptance Criteria)，本報告將協助利害關係人理解如何滿足 CSA 的嚴格要求，從而順利取得市場准入資格並建立品牌信任。

---

2. CLS(IoT) 制度背景與架構演進 (Institutional Background and Framework Evolution)

2.1 全球 IoT 安全監管趨勢 (Global IoT Security Landscape)

在深入探討 CCC SP-151-4 之前，必須先理解其所處的全球監管脈絡。近年來，國際社會對於 IoT 設備缺乏基礎安全防護（如預設密碼薄弱、缺乏更新機制）的問題日益重視。

- 歐洲：歐盟透過 ETSI EN 303 645 標準確立了消費級 IoT 安全的基線，並透過《網路韌性法案》(Cyber Resilience Act, CRA) 強制執行。
- 美國：白宮發布的物聯網網路安全行政命令及 FCC 的「美國網路信任標誌 (U.S. Cyber Trust Mark)」計畫，均強調了標籤化管理的重要性 [1]。
- 新加坡的戰略定位：新加坡 CSA 的 CLS 計畫並非孤立存在，而是與上述國際標準高度對齊（特別是 ETSI EN 303 645），並透過簽署互認協議 (MRA)，致力於成為亞洲 IoT 安全認證的樞紐 [3]。

2.2 CSA 出版物體系與 CCC SP-151-4 的核心地位

CLS(IoT) 的運作依賴於一系列相互關聯的技術出版物 (Publications)。理解這些文件的層級關係，對於掌握評估方法論至關重要：

1. **CCC SP-151-1**：計畫概覽 **(Overview of the Scheme)**
    - 定義了 CLS 的治理結構、標籤等級 (Level 1-4) 的意義以及申請流程。
2. **CCC SP-151-2**：計畫規範 **(Scheme Specifications)**
    - 列出了具體的安全要求（例如：「設備不得有通用預設密碼」）。這是「做什麼 (What)」的標準。
3. **CCC SP-151-4**：評估方法論 **(Assessment Methodology)**
    - 本報告焦點。它詳細說明了「如何 (How)」驗證是否符合 SP-151-2 的規範。它規定了證據的形式（截圖、文件引用、測試報告）、測試的具體步驟以及評估者 (Assessor) 的判斷標準 [1]。
4. **CCC SP-151-5**：**Level 4** 最低測試規範 **(Minimum Test Specifications for Level 4)**
    - 針對最高等級的滲透測試提供技術指引。
5. **CCC SP-151-4A**：家庭閘道器評估方法論 **(Assessment Methodology for Home Gateway)**
    - **2025** 年新增。針對路由器與閘道器這類關鍵基礎設施設備，制定了獨立且更嚴格的評估方法 [3]。

2.3 2023-2025 年關鍵制度變革 (Key Regulatory Updates)

自 2020 年推出以來，CLS 經歷了數次重大迭代，這些變化直接影響了 CCC SP-151-4 的應用方式：

- **測試實驗室 (TL) 權限擴大 (2023 年 9 月)**：CSA 授權認可的測試實驗室 (Approved CLS Testing Laboratories) 審查所有級別的符合性聲明。這意味著評估工作從政府直接審查轉向了市場化的第三方專業驗證 [6]。
- **強制性實驗室審查 (2025 年 4 月起)**：這是一項顛覆性的變革。過去，Level 1 和 Level 2 的申請主要依賴製造商的自我聲明 (Self-Declaration)，CSA 僅進行抽查。然而，自 2025 年 4 月 1 日起，所有級別（包括 Level 1/2）的申請在提交給 CSA 之前，都必須先經過認可測試實驗室 (TL) 的審查 [3]。這一政策消除了「自我聲明」可能帶來的誠信風險，但也增加了合規成本與門檻。
- **互認協議 (MRA) 的擴展**：新加坡已與芬蘭、德國 (BSI) 和韓國 (KISA) 簽署 MRA。這意味著依據 CCC SP-151-4 通過評估的產品，可以更便捷地進入這些國家的市場。特別是與德國的互認，要求家庭閘道器必須符合特定的 SP-151-4A 標準 [3]。

---

3. 評估程序總論：從自我聲明到第三方驗證 (Assessment Process Overview)

CCC SP-151-4 確立了一套基於「聲明—證據—驗證」的嚴謹評估邏輯。無論申請哪個級別，評估的核心都在於證明設備滿足了特定的安全條款 (Provisions)。

3.1 證據提交框架 (Supporting Evidence Framework)

根據最新版的 CCC SP-151-4，製造商不再只是簡單地勾選「符合」清單，而是必須提交具體的支持性證據 **(Supporting Evidence)**。CSA 甚至提供了專門的 PowerPoint 範本 (CLS(IoT) – Company – Supporting Evidence v1.0) 來引導廠商填寫 [5]。

證據的類型與要求：

1. 文件引用 **(Document References)**：
    - 要求：必須引用產品手冊、技術規格書或隱私政策的具體章節。
    - 評估標準：評估者會檢查引用的文件是否真實存在，且內容是否與聲明一致。
2. 螢幕截圖與摘要 **(Screen Captures & Snippets)**：
    - 要求：這是 SP-151-4 中最常見的要求。製造商需提供顯示設備配置介面、App 設定畫面或軟體更新通知的真實截圖。
    - 評估標準：截圖必須清晰，且能證明功能已實際實作（Implemented）。例如，為了證明「強制更改密碼」，必須提供顯示該強制流程的 UI 截圖。

3. 流程圖與工作指導書 **(Process Charts & Work Instructions)**：
    - 要求：針對非功能性要求（如漏洞揭露流程、安全開發生命週期），需提供內部的標準作業程序 (SOP) 文件或流程圖。
    - 評估標準：評估者會檢查這些流程是否合理且具備可執行性。
4. 技術聲明 **(Technical Declarations)**：
    - 要求：針對無法直接觀察的內部機制（如加密演算法、隨機數生成器），製造商需簽署技術聲明。

3.2 評估者 (Assessor) 的職責

在 CCC SP-151-4 的語境下，評估者通常指認可測試實驗室 **(Approved CLS Testing Laboratory, TL)** 的人員。他們的職責包括：

- 完整性檢查 **(Completeness Check)**：確認所有必填欄位和證據都已提供。
- 正確性評估 **(Correctness Assessment)**：驗證提供的截圖是否真實反映了安全功能的運作，檢查密碼樣本的隨機性，以及分析軟體二進位碼的掃描報告。
- 報告生成 **(Reporting)**：撰寫評估報告 (Assessment Report)，建議 CSA 授予或拒絕標籤。

---

4. Level 1 評估方法論：安全基線 (Baseline Security Assessment)

Level 1 是 CLS 的入門級別，聚焦於最基礎的網路衛生 (Cyber Hygiene)。雖然被稱為「基線」，但 CCC SP-151-4 對其評估的細緻程度極高，絕非形式主義。Level 1 涵蓋了 IoT 安全中最關鍵的三個領域：密碼管理、漏洞管理與軟體更新。

4.1 條款 5.1：無通用預設密碼 (No Universal Default Passwords)

這是全球 IoT 安全標準（包括 ETSI EN 303 645 和英國 PSTI 法案）中的第一條誡律。通用預設密碼（如 "admin/admin"）是 Mirai 等殭屍網路病毒擴散的主要途徑。

4.1.1 條款要求 (Requirement)

- 設備的預設密碼必須是每一台設備獨有的 **(Unique per device)**；或者
- 設備必須具備一種機制，強制用戶在首次設置時定義自己的密碼。

- 新密碼必須具備足夠的複雜度。

4.1.2 評估方法 (Assessment Methodology) [9]

CCC SP-151-4 對此條款的評估方法設計得非常具體，以防止廠商造假：

1. 密碼生成方法的聲明 **(Declaration of Generation Method)**：
    - 開發者必須聲明用於生成預裝密碼 (Pre-loaded Passwords) 的具體方法。
    - 合規範例：聲明使用加密安全偽隨機數生成器 (Cryptographically Secure Pseudo-Random Number Generator, CSPRNG)。
    - 評估重點：評估者會審查該方法是否能保證足夠的熵值 (Entropy)，以抵抗暴力破解攻擊。
2. 提供 **10** 個隨機密碼實例 **(10 Instances of Randomised Passwords)**：
    - 證據要求：開發者必須提供 **10** 個 實際生成的預裝密碼樣本。這些樣本需以截圖或照片的形式呈現（例如拍攝 10 台不同設備的標籤或設定介面）。
    - 為什麼是 **10** 個？：單一樣本無法證明隨機性。通過 10 個樣本，評估者可以進行基礎的模式分析。
3. 評估者的驗收標準 **(Acceptance Criteria)**：
    - 無增量計數器 **(No Incremental Counters)**：評估者會檢查密碼是否呈現 "Pass001", "Pass002" 這樣的規律。如有，則判定為失敗。
    - 無常見模式 **(No Common Patterns)**：檢查是否包含 "QWERTY", "1234", "Password" 等常見字串。
    - 無公開資訊關聯 **(No Relation to Public Info)**：評估者會比對密碼與設備的公開標識符（如 Wi-Fi SSID, MAC Address, 序號）。如果密碼顯然是由 MAC 地址推導而來（例如直接使用 MAC 後六碼），則判定為失敗。這是一個常見的設計陷阱，SP-151-4 明確禁止此類做法。

4.2 條款 5.2：漏洞揭露政策 (Vulnerability Disclosure Policy)

建立漏洞揭露政策 (Vulnerability Disclosure Policy, VDP) 是廠商承擔安全責任的標誌。它為白帽駭客與安全研究人員提供了一個合法的回報管道。

4.2.1 條款要求 (Requirement)

- 製造商必須公開一個聯絡點 (Point of Contact)，用於接收安全漏洞報告。
- 必須公開說明處理漏洞的流程與預期時間表。

4.2.2 評估方法 (Assessment Methodology)

1. **URL** 驗證 **(URL Verification)**：
    - 證據要求：提供包含 VDP 資訊的公開網頁連結 (URL)。
    - 評估重點：評估者會實際訪問該連結，確認網頁可公開存取（無須登入），且內容清晰

易懂。

2. 政策內容審查 **(Content Review)**：
    - 評估者會檢查政策是否包含以下要素：
        - 報告機制：如專用的電子郵件地址 (security@company.com) 或網頁表單。
        - 確認收到報告的時間 **(Timeline for Acknowledgement)**：例如「我們將在 48 小時內確認收到報告」。
        - 修復進度更新 **(Status Updates)**：說明如何向報告者通報修復進度。

4.3 條款 5.3：軟體更新機制 (Software Updates)

軟體更新是修復已知漏洞的唯一途徑。SP-151-4 關注的不僅是「有」更新功能，更關注更新過程的安全性。

4.3.1 條款要求 (Requirement)

- 設備必須具備軟體更新功能。
- 更新機制必須驗證軟體包的完整性 (Integrity) 與真實性 (Authenticity)。
- 必須具備防回滾 (Anti-rollback) 機制。

4.3.2 評估方法 (Assessment Methodology) [9]

1. 防回滾機制的驗證 **(Anti-rollback Verification)**：
    - 定義：防止使用者（或攻擊者）將設備固件降級到舊版本，從而利用舊版本中的已知漏洞。
    - 證據要求：開發者需提供技術聲明，說明如何實作防回滾（例如：在固件檔頭檢查版本號，若低於當前版本則拒絕刷寫）。
    - 截圖證據：理想情況下，提供嘗試刷寫舊版固件被系統拒絕的錯誤訊息截圖。
2. 完整性與真實性檢查 **(Integrity & Authenticity Check)**：
    - 證據要求：描述使用了何種加密技術來簽署固件（如 RSA-2048, ECDSA）。
    - 評估重點：評估者會確認設備在安裝更新前，是否會強制驗證數位簽章 (Digital Signature)。如果僅使用 Checksum (如 CRC32 或 MD5) 進行校驗，通常會被視為不足，因為這無法驗證來源的真實性。
3. 使用者通知 **(User Notification)**：
    - 證據要求：提供 App 或設備介面截圖，顯示當有新更新可用時，系統如何通知使用者。

---

5. Level 2 評估方法論：安全設計與資料保護 (Security-by-Design & Data Protection)

Level 2 要求設備不僅滿足基線要求，還必須在設計階段導入國際標準（主要是 ETSI EN 303 645 的全套要求），並特別強化資料保護 (Data Protection)。這一級別的評估更加全面，涉及大量的文檔審查。

5.1 條款 5.4 至 5.13：國際標準合規 (Adherence to International Standards)

雖然 Level 1 涵蓋了 ETSI 標準的前三項（密碼、VDP、更新），但 Level 2 要求符合剩餘的 10 個領域，包括：

- 安全存儲敏感參數 **(Secure Storage of Sensitive Parameters)**
- 安全通訊 **(Secure Communication)**
- 最小化攻擊面 **(Minimization of Attack Surface)**
- 確保軟體完整性 **(Ensure Software Integrity)**
- 個人資料保護 **(Data Protection)**
- 使系統具備彈性 **(Make Systems Resilient to Outages)**
- 檢查系統遙測數據 **(Examine System Telemetry Data)**
- 方便用戶刪除個人數據 **(Easy Deletion of User Data)**
- 簡化安裝與維護 **(Make Installation and Maintenance Easy)**
- 驗證輸入數據 **(Validate Input Data)**

評估方法論通則：
對於上述每一項，SP-151-4 都要求「聲明 + 證據」。例如，針對安全通訊，開發者必須聲明使用了 TLS 1.2 或更高版本，並提供 Wireshark 抓包截圖證明通訊過程是加密的。

5.2 條款 6.1 至 6.5：消費者資料保護條款 (Data Protection Provisions for Consumer)

這是 Level 2 的核心增強項目，專注於隱私合規，類似於 GDPR 的技術實現。SP-151-4 對這些條款有非常具體的展示要求 [8]。

5.2.1 條款 6.1：個人資料處理資訊 (Information on Personal Data Processing)

- 要求：製造商必須向消費者提供清晰、透明的資訊，說明處理了哪些個人資料 (Personal Data)、由誰處理、以及用於什麼目的。這不僅適用於設備本身，還包括配套的 App 及任何涉及的第三方（如廣告商）。
- 評估方法：
  - 證據：隱私政策 (Privacy Policy) 的全文或連結。
  - 審查重點：評估者會逐條檢查隱私政策是否明確列出數據類型（如「錄音」、「地理位置」、「IP地址」）。模糊的描述（如「我們收集必要的數據」）將被視為不合規。
  - 公開性：評估者需確認這些資訊將會與產品列表一同在 CSA 網站上公佈，供消費者在購買前查閱。

5.2.2 條款 6.2：同意的有效性 (Valid Consent)

- 要求：若個人資料處理基於用戶同意，該同意必須以「有效的方式」取得。這意味著必須是 Opt-in（主動勾選），而非 Opt-out（預設勾選）。
- 評估方法：
  - 證據：設備初始化或 App 安裝過程中的「同意徵求」介面截圖。
  - 驗收標準：截圖必須顯示勾選框預設為未勾選狀態。如果預設已勾選，則評估失敗。

5.2.3 條款 6.3：撤回同意的權利 (Right to Withdraw Consent)

- 要求：已給予同意的消費者必須有能力隨時撤回其同意。
- 評估方法：
  - 證據：展示 App 或設備設定選單中「撤回同意」、「停止數據收集」或「刪除帳號」功能的截圖。
  - 驗收標準：該功能必須易於存取，不能隱藏在過深（如超過 3 層）的選單中。

5.2.4 條款 6.5：資料刪除 (Data Deletion)

- 要求：用戶應能簡單地刪除設備上及雲端存儲的所有個人數據。
- 評估方法：
  - 證據：「恢復出廠設定 (Factory Reset)」功能的截圖，以及該功能清除資料的說明文件。
  - 驗證：對於雲端數據，需提供說明如何請求刪除伺服器端數據的政策或介面。

---

6. Level 3 評估方法論：軟體二進位碼分析 (Software Binary Analysis)

進入 Level 3，評估的性質發生根本轉變：從「審查廠商說了什麼（文檔）」轉向「驗證設備裡裝了什麼（代碼）」。這一級別的目標是確保軟體不包含已知的漏洞。

6.1 測試對象與工具 (Target and Tools)

- 測試對象：設備的完整固件映像檔 (Firmware Image)，包括作業系統 (OS)、驅動程式、第三方函式庫及應用程式邏輯。
- 工具：測試實驗室 (TL) 使用專業的軟體成分分析 **(Software Composition Analysis, SCA)** 工具。這些工具能解包固件，識別其中包含的所有開源組件 (Open Source Components)。

6.2 評估方法與流程 (Assessment Methodology)

6

1. 組件識別與 **CVE** 比對 **(Component Identification & CVE Mapping)**：
    - TL 使用工具掃描固件，列出所有軟體組件及其版本號（例如：OpenSSL 1.0.1）。
    - 將識別出的組件與全球漏洞資料庫 (如 NVD) 進行比對，找出已知的常見漏洞與披露 **(CVEs)**。
2. 增強型二進位掃描 **(Enhanced Binary Scan)**：
    - 自 2023 年 9 月起，CSA 要求執行「增強型」掃描。這意味著掃描不能僅停留在表面，必須深入到檔案系統的每一層。
    - 評估標準：如果發現任何評分為「高 (High)」或「嚴重 (Critical)」的 CVE，且廠商未提供有效的修補證明或緩解措施 (Mitigation Plan)，則評估失敗。
3. 硬編碼憑證掃描 **(Hard-coded Secrets Scan)**：
    - 風險：開發人員有時會將 API Keys、私鑰 (Private Keys) 或測試帳號密碼遺留在代碼中。
    - 評估方法：SCA 工具會搜尋常見的憑證模式（如 "BEGIN RSA PRIVATE KEY"）。
    - 驗收標準：固件中不得包含任何有效的硬編碼敏感憑證。
4. 二進位強化檢查 **(Binary Hardening Check)**：
    - 檢查二進位檔是否使用了安全編譯選項，如 ASLR (位址空間配置隨機化)、DEP (資料執行保護) 和 Stack Canaries。雖然這不是 CVE，但缺乏這些保護會使設備更容易被

開採。

---

7. Level 4 評估方法論：滲透測試 (Penetration Testing)

Level 4 是 CLS 的最高榮譽，代表設備經過了模擬真實駭客攻擊的考驗。此級別的評估依據 **CCC SP-151-5 Minimum Test Specifications (MTS)** 進行。

7.1 結構化滲透測試 (Structured Penetration Testing)

與 Level 3 的自動化掃描不同，Level 4 高度依賴資深安全測試人員的專業技能。測試採用黑箱 **(Black-box)** 或灰箱 **(Grey-box)** 模式 [11]。

主要測試領域：

1. 物理攻擊介面 **(Physical Attack Surfaces)**：
    - 測試方法：測試人員會拆解設備，尋找並嘗試連接 UART、JTAG 或 SPI 介面。
    - 目標：試圖通過這些介面取得 Root Shell 權限或提取固件。
    - 防護要求：這些介面應被物理封死，或在軟體層面禁用，或受密碼保護。
2. 網路通訊攻擊 **(Network Communication Attacks)**：
    - 測試方法：中間人攻擊 (MITM)、重放攻擊 (Replay Attacks)、模糊測試 (Fuzzing) 網路協議。
    - 目標：攔截敏感數據或造成服務阻斷 (DoS)。
3. 應用層與雲端攻擊 **(Application & Cloud Attacks)**：
    - 測試方法：針對配套 App 和 API 進行 SQL 注入、跨站腳本 (XSS)、越權存取 (IDOR) 測試。
    - 目標：竊取用戶數據或控制他人設備。
4. 生態系統測試 **(Ecosystem Testing)**：
    - SP-151-4 強調 IoT 是一個生態系統。測試範圍可能延伸到與設備互動的雲端服務，確保後端 API 的安全性。

7.2 報告與修復 (Reporting and Remediation)

- 測試報告：TL 需提交一份詳盡的報告，記錄發現的每一個漏洞、重現步驟及風險等級。
- 修復驗證：廠商修復漏洞後，TL 必須進行複測 (Re-test)，確認漏洞已被封堵且未引入新問

題。只有所有高風險漏洞都解決後，才能獲得 Level 4 標籤。

---

8. 2025 年新規範與市場影響 (2025 Regulations & Market Impact)

CSA 於 2025 年實施的新規定徹底改變了 CLS 的合規生態。

8.1 強制性測試實驗室 (TL) 審查

自 2025 年 4 月 1 日起，Level 1 和 Level 2 的申請必須經由認可 TL 審查 [3]。

- 對廠商的影響：
  - 成本上升：除了繳交給 CSA 的申請費（Level 1: $57, Level 2: $142），廠商現在必須支付 TL 的服務費。這是一筆額外的市場成本。
  - 準備週期延長：需要預留時間給 TL 進行評估。以往 Level 1 可能幾天內完成，現在可能需要數週（視 TL 排程而定）。
  - 合規嚴謹度：廠商不能再抱有僥倖心態隨意填寫聲明。那「10 張隨機密碼截圖」將由專業人員逐一檢視，任何疏漏都會導致退件。

8.2 家庭閘道器專屬規範 (CCC SP-151-4A)

針對 Wi-Fi 路由器與閘道器，CSA 推出了 **CCC SP-151-4A** [3]。

- 背景：家庭閘道器是所有家用 IoT 設備的流量樞紐，其安全性至關重要。
- 特殊要求：
  - 更嚴格的網路隔離：要求訪客網路 (Guest Network) 與主網路必須在邏輯上完全隔離。
  - 防火牆規則：預設防火牆設定必須更加嚴格。
  - 管理介面保護：禁止通過 WAN 埠訪問管理介面。
- 互認意義：符合 SP-151-4A 是獲得德國 BSI 互認的前提條件（對應德國 BSI TR-03148 標準）。

---

9. 互認協議 (Mutual Recognition Arrangements, MRAs)

CCC SP-151-4 的價值不僅限於新加坡。透過 MRA，它成為了全球市場准入的通行證。

合作國家	對應標籤/標準	互認機制 **(Mutual Recognition)**	戰略意義
德國	IT Security Label (BSI)	新加坡 CLS Level 2+ $\Leftrightarrow$ 德國 IT Security Label	進入歐盟最大市場的捷徑。特別注意家庭閘道器需符合 SP-151-4A。[3]
韓國	KISA CIC Label (Basic Level)	新加坡 CLS Level 3+ $\Leftrightarrow$ 韓國 CIC Basic Level	自 2025 年 1 月 1 日生效。連接亞洲兩大科技先進國家的標準。[3]
芬蘭	Cybersecurity Label	新加坡 CLS Level 3 $\Leftrightarrow$ 芬蘭 Cybersecurity Label	歐洲首個與新加坡互認的國家，奠定了 CLS 國際化的基礎。[7]

洞察：對於出口型製造商，直接申請新加坡 CLS Level 3 或 4 是最具成本效益的策略 (Cost-Effective Strategy)，因為它可以一次性滿足多個國家的合規要求，避免重複測試的費用與時間成本。

---

10. 結論與建議 (Conclusion and Recommendations)

CCC SP-151-4 CLS(IoT) Assessment Methodology 是一份動態演進的技術文件，它見證了新加坡從推廣 IoT 安全意識走向建立嚴格市場準入機制的過程。

對於開發者的關鍵建議：

1. 證據準備要「過度」充分：在提交給 TL 之前，請自我審查那 10 張密碼截圖、防回滾機制的證

明以及隱私政策的每一個條款。TL 的審查將是二元對立的（通過/失敗），任何模糊都會導致延遲。

2. 擁抱「安全設計」：Level 1 的要求（如無預設密碼）如果沒有在硬體與固件設計初期考慮，後期修改將極其痛苦。應將 SP-151-2 和 SP-151-4 作為產品需求文檔 (PRD) 的一部分。
3. 利用 **MRA** 擴大市場：如果產品計畫銷往歐洲或韓國，務必仔細研究 Level 2 和 Level 3 的要求。雖然初期投入較高，但獲得的市場通行證價值巨大。
4. 關注 **2025** 年新規：如果您的產品屬於 Wi-Fi 路由器類別，請立即下載 **CCC SP-151-4A** 並進行差距分析 (Gap Analysis)，因為通用版 SP-151-4 已不足以涵蓋新規範。

總結來說，CCC SP-151-4 不僅僅是一份合規清單，它是構建可信賴物聯網生態系統的藍圖。遵守這些評估方法，不僅是為了獲得標籤，更是為了保護終端用戶，並在日益險惡的網路威脅環境中生存。

附錄：**CLS(IoT)** 等級與關鍵評估活動對照表

CLS 等級	關鍵評估活動 **(Key Assessment Activities)**	強制性條款範例 **(Mandatory Provisions Examples)**	**2025** 年後審查主體
Level 1	開發者符合性聲明 + 證據提交 (截圖、文檔)	無通用預設密碼 (5.1)、漏洞揭露 (5.2)、軟體更新 (5.3)	測試實驗室 **(TL)** (原為 CSA 審查)
Level 2	Level 1 要求 + 安全設計合規 + 資料保護	資料保護 (6.1-6.5)、最小化攻擊面、通訊安全、隱私政策審查	測試實驗室 **(TL)**
Level 3	Level 2 要求 + 軟體二進位碼分析	無已知 CVE、無硬編碼憑證、增強型二進位掃描	測試實驗室 **(TL)**
Level 4	Level 3 要求 + 結構化滲透測試	抵禦常見網路攻擊、抗物理入侵、生態系統測試	測試實驗室 **(TL)**

[報告結束]

引用的著作

1. FCC FACT SHEET* Cybersecurity Labeling for Internet of Things Report and Order

PS Docket No. 23-239 Background, 検索日期：11月 24, 2025, https://docs.fcc.gov/public/attachments/DOC-400674A1.pdf
2. FCC-24-26A1.pdf, 検索日期：11月 24, 2025, https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf
3. Eurofins KCTL GMA Newsletter 02 2025 (ENG) | PDF | Radio Spectrum - Scribd, 検索日期：11月 24, 2025, https://www.scribd.com/document/924708169/Eurofins-KCTL-GMA-Newsletter-02-2025-ENG
4. CLS(IoT) Updates | Cyber Security Agency of Singapore, 検索日期：11月 24, 2025, https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/updates/
5. Singapore Updates Cybersecurity Labelling Scheme for IoT Devices - GMA Consult Group, 検索日期：11月 24, 2025, https://www.gma.trade/news/singapore-updates-cybersecurity-labelling-scheme-for-iot-devices
6. Singapore Regulatory Update on CLS(IoT) - 5m global, 検索日期：11月 24, 2025, https://5mglobal.com/csr-singapore-updates-the-cybersecurity-labelling-scheme-cls-iot-singapore/
7. Cybersecurity Certification/Labelling Schemes - ITU, 検索日期：11月 24, 2025, https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090016PDFE.pdf
8. Title Lorem Ipsum, 検索日期：11月 24, 2025, https://isomer-user-content.by.gov.sg/36/c5acd46b-158b-45df-bddd-9ee05f20d3d8/CLS(IoT)---Company---Supporting-Evidence-v1.0.pptx
9. CCC SP-151-4 Cybersecurity Labelling Scheme for IoT Publication No. 4 Assessment Methodology October 2024 Version 1.1, 検索日期：11月 24, 2025, https://isomer-user-content.by.gov.sg/36/36dea71e-248c-4af4-8a93-963ea49e7a8f/pub-ccc-sp-151-4-cls(iot)-assessment-methodology-v1-1.pdf
10. Global Digital Health Partnership (GDHP) Guidance for Medical Device Cybersecurity (GMDC), 検索日期：11月 24, 2025, https://gdhp.health/wp-content/uploads/2024/10/GDHP-Guidance-for-Medical-Device-Cybersecurity_final.pdf
11. CCC SP-151-2 CLS (IoT) Scheme Specifications v1.4 | PDF | Security - Scribd, 検索日期：11月 24, 2025, https://www.scribd.com/document/925687513/CCC-SP-151-2-CLS-IoT-Scheme-Specifications-v1-4
12. CCC SP-151-4A Cybersecurity Labelling Scheme for IoT Publication No. 4A Assessment Methodology for Home Gateway April 2025 Versi, 検索日期：11月 24, 2025, https://isomer-user-content.by.gov.sg/36/8cb4873e-7486-4a97-8c3c-2b1e7343976a/CCC%20SP-151-4A%20CLS(IoT)%20Assessment%20Methodology%20For%20Home%20Gateway%20v1.1.pdf