經 濟 部

IDB

「行動應用App基本資安檢測基準」說明

執行單位：財團法人資訊工業策進會

民國104年8月17日

大綱

- 背景與概述
- 主要參考依據
- 適用範圍
- 檢測基準安全等級
- 檢測基準重點摘述

背景與概述

- 「行政院國家資通安全會報」於去年第26次委員會決議手機應用軟體由經濟部工業局主責：
  - 資安檢測**標準制訂**
  - 鼓勵廠商**自主驗證**
- 於103年10月經濟部工業局委託財團法人資訊工業策進會執行
- 於103年12月完成「行動應用App基本資安規範」**草案**
- 於104年4月20日「行動應用App基本資安規範」**正式公告**於經濟部通訊產業發展推動小組網站

主要參考依據

- **行動應用App基本資安規範**
  - 經濟部工業局，民國104年4月20日
- **NIST SP800-163**
  - National Institute of Standards and Technology (美國國家標準技術研究所)
  - Special Publication 800-163 Vetting the Security of Mobile Applications, January 2015
- **OWASP Top Ten Mobile Risks**
  - Open Web Application Security Project（開放Web軟體安全計畫）
  - Mobile Security Project - Top Ten Mobile Risks

修訂歷程

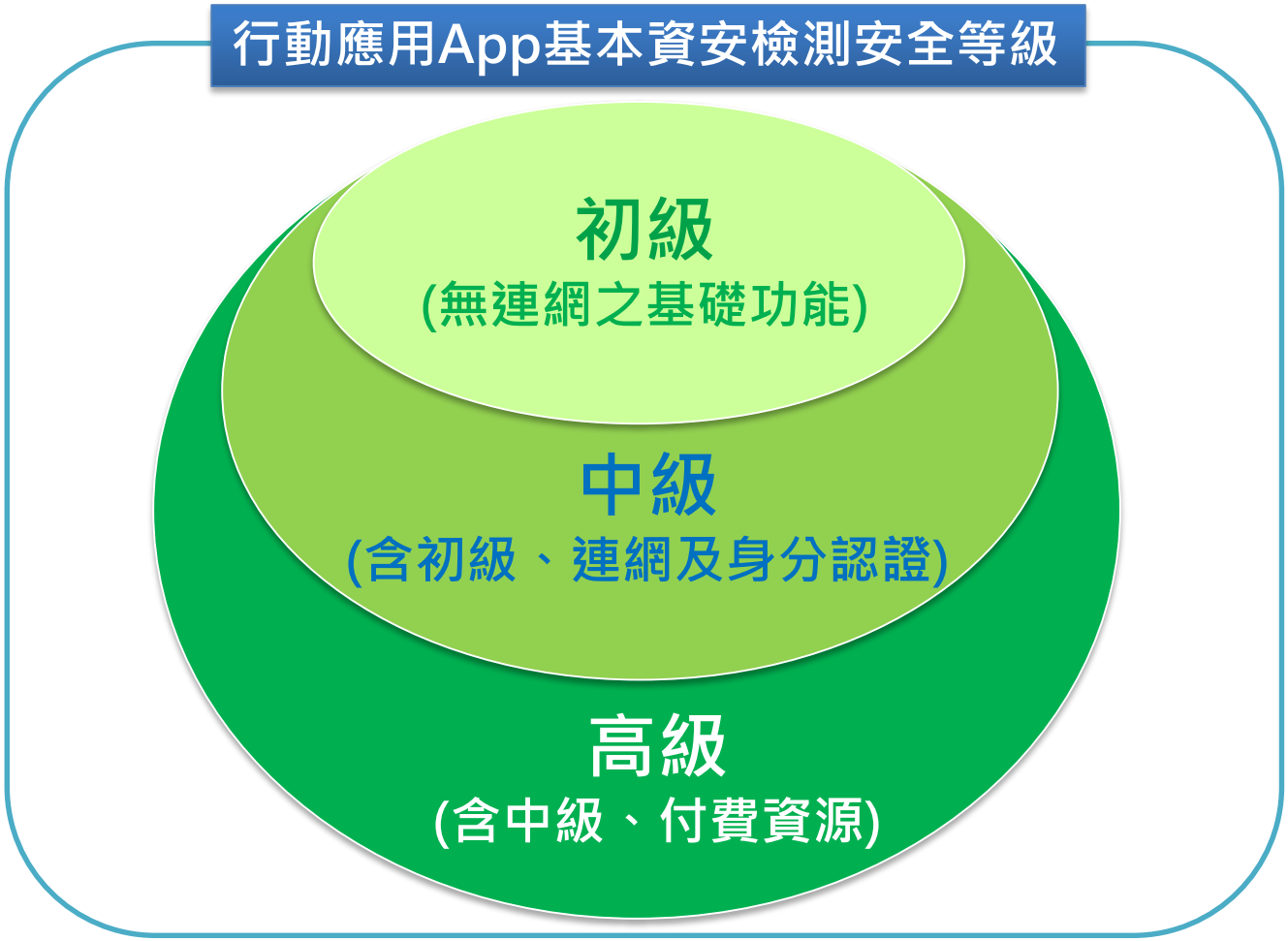
- 於104年6月1日工作小組完成「行動應用App基本資安檢測基準」**初稿**
- 於104年6月4日召開「行動應用App基本資安檢測基準」編審小組會議，並於6月9日依編審小組建議完成修訂**草案**
- 於104年6月11日召開「行動應用App基本資安檢測基準」專家座談會議，並於6月17日依專家建議完成修訂
- 於104年6月23日舉辦「行動應用App基本資安檢測基準」業界交流會，聽取各方意見
- 於104年8月14日**正式公告**於經濟部通訊產業發展推動小組網站

適用範圍

- 本檢測基準適用範圍為行動應用程式**共通性**之安全檢測
- **特定領域**之行動應用程式其資安規範應由**各目的事業主管機關**訂定
- 資訊安全本質為**風險控管**概念，故
  - 通過檢測之行動應用程式，僅**對程式本身**具有安全水準保證
  - **使用者**亦需善盡使用與管理個人相關資料之責任，以降低因蓄意或個人行為疏失所造成之風險及危害

檢測基準安全等級

- 所有檢測項目依**功能安全性**分類**為初級、中級(含初級)及高級(含中級)三個安全等級**
- 原則上行動應用程式開發商可**自行決定**送檢之安全等級



檢測基準安全等級 – 架構

檢測基準之安全等級依據資安規範技術要求事項，初級檢測項目共計29項，其中9項訂為必要檢測項目，其餘20項為非必要檢測項目

資安基本規範面向	檢測基準安全等級	資訊安全技術要求事項	檢測項目	必要項	非必要項
4.1.1.行動應用程式發布安全	高級（含中級）涵蓋規範17項要求	4.1.1.1.行動應用程式發布	2	2	0
		4.1.1.2.行動應用程式更新	3	0	3
		4.1.1.3.行動應用程式安全性問題回報	2	1	1
4.1.2.敏感性資料保護		4.1.2.1.敏感性資料蒐集	2	2	0
		4.1.2.2.敏感性資料利用	4	0	4
		4.1.2.3.敏感性資料儲存	7	4	3
		4.1.2.5.敏感性資料分享	3	0	3
		4.1.2.6.敏感性資料刪除	1	0	1
4.1.3.付費資源控管安全		4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	2	0	2
		4.1.5.3.函式庫引用安全	1	0	1
		4.1.5.4.使用者輸入驗證	2	0	2
4.1.4.身分認證、授權與連線管理安全	中級（含初級）涵蓋規範14項要求	4.1.2.4.敏感性資料傳輸	--	待訂	待訂
		4.1.4.1.使用者身分認證與授權	--	待訂	待訂
		4.1.4.2.連線管理機制	--	待訂	待訂
4.1.5.行動應用程式碼安全	初級涵蓋規範11項要求	4.1.3.1.付費資源使用	--	待訂	待訂
		4.1.3.2.付費資源控管	--	待訂	待訂
		4.1.5.2.行動應用程式完整性	--	待訂	待訂
			17	29	9	20

檢測基準安全等級 – 初級檢測必要項目

資訊安全技術要求事項	行動應用程式檢測項目
4.1.1.1.行動應用程式發布	4.1.1.1.1.應於可信任來源之行動應用程式商店發布
	4.1.1.1.2.應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途
4.1.1.3.行動應用程式安全性問題回報	4.1.1.3.1.開發者應提供回報安全性問題之管道
4.1.2.1.敏感性資料蒐集	4.1.2.1.1.應於蒐集敏感性資料前，取得使用者同意
	4.1.2.1.2.應提供使用者拒絕蒐集敏感性資料之權利
4.1.2.3.敏感性資料儲存	4.1.2.3.1.應於儲存敏感性資料前，取得使用者同意
	4.1.2.3.2.應提供使用者拒絕儲存敏感性資料之權利
	4.1.2.3.4.應避免將敏感性資料儲存於暫存檔或紀錄檔中
	4.1.2.3.6.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取

檢測基準安全等級 – 必要檢測項目

	試辦	研訂中（暫定）	
技術要求(規範4.1) 各安全等級必要檢測項目 / 安全等級	初級	中級	高級
4.1.1. 行動應用程式發布安全	3	3	6
4.1.2. 敏感性資料保護	6	8	15
4.1.3. 付費資源控管安全	0	0	4
4.1.4. 身分認證、授權與連線管理安全	0	6	6
4.1.5. 行動應用程式碼安全	0	0	5
必要檢測項目總數	9	17	36

註：「規範」為「行動應用App基本資安規範」之簡稱

檢測基準安全等級 – 標章之取得

- 第一類行動應用程式須通過初級安全檢測、第二類行動應用程式須通過中級安全檢測，第三類行動應用程式須通過高級安全檢測
- 於通過所有該等級**必要檢測項目**後，始取得該等級標章之資格

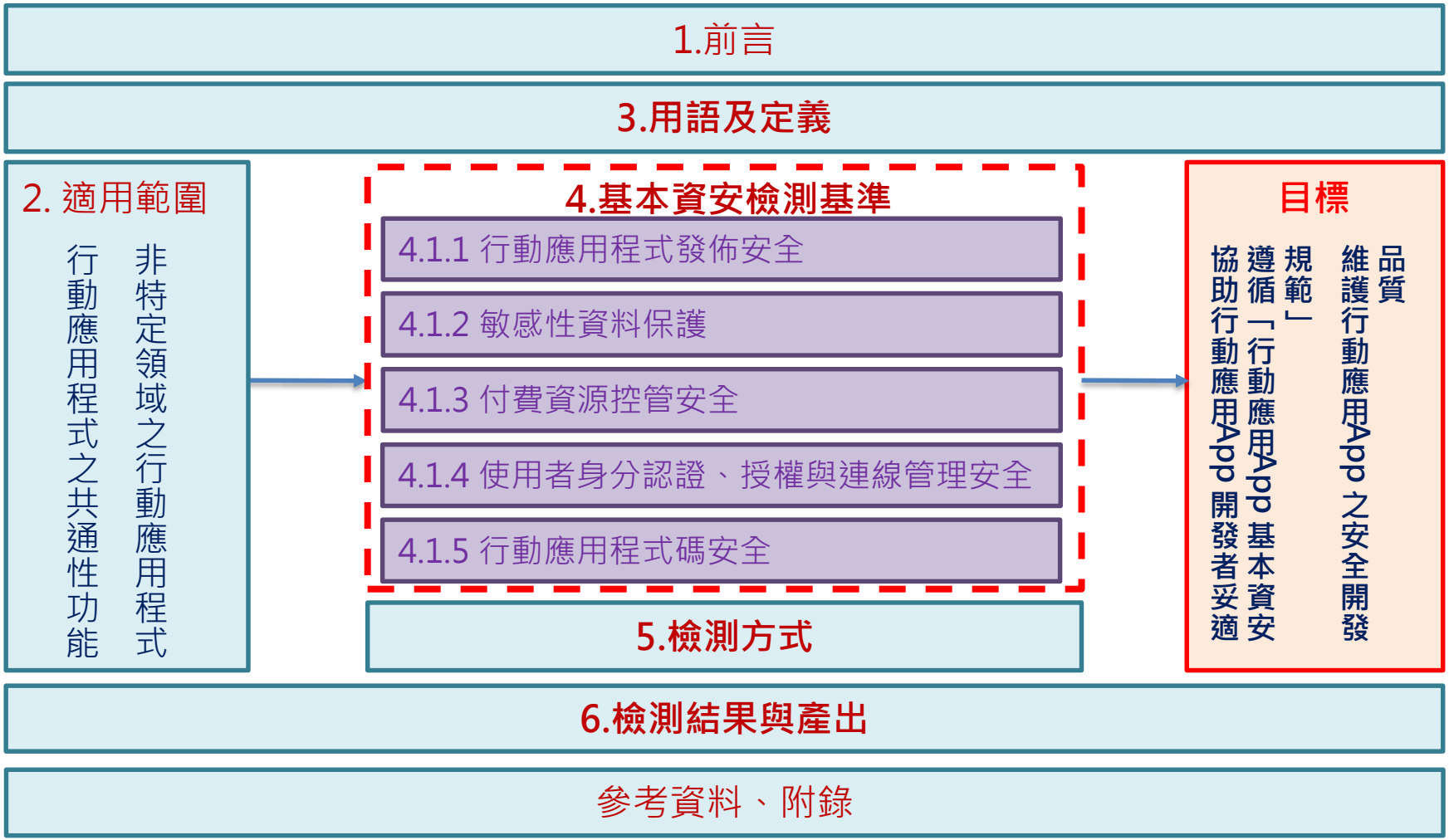
開發商參考之安全要求事項

檢測實驗室提供之檢測項目

檢測基準 安全等級 / 行動應用程式分類	初級 檢測無連網之基礎功能安全性	中級(含初級) 檢測連網及身分認證安全性	高級(含中級) 檢測付費資源之安全性
第一類 純功能性	★	V	V
第二類 具認證功能與連網行為	—	★	V
第三類 具交易功能（包括認證功能及連網行為）	—	—	★

★為必要通過之檢測等級　　V為可自由選擇通過之檢測等級

「行動應用App基本資安檢測基準」文件架構



基本資安檢測基準 – 檢測欄位說明

檢測編號	依據「資安規範」之「4.技術要求」編號項次 檢測編號：5碼 (4.1.x.y.z) 「4.1.x.y」為資訊安全技術要求事項之編號 「z」為向下展開之檢測編號
安全分類	「資安規範」之分類：第一類、第二類、第三類
檢測項目	本檢測項目名稱
檢測依據	「資安規範」之「4.技術要求」相對應事項
技術要求	「資安規範」之「4.技術要求」相對應事項「內容」
檢測基準	1)　檢測基準1
	2)　檢測基準2
	…
檢測結果	「符合要求」或「不符合要求」形成條件
備註	其他說明事項(如檢測時機)

註：「資安規範」為「行動應用App基本資安規範」之簡稱

基本資安檢測基準 – 檢測欄位範例1

檢測編號	4.1.2.3.4
安全分類	「行動應用App基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存限制
檢測依據	「行動應用App基本資安規範」4.1.2.3.敏感性資料儲存
技術要求	行動應用程式應避免將敏感性資料儲存於暫存檔或紀錄檔中
檢測基準	1) 檢查是否未將敏感性資料儲存於網頁暫存檔或自定義暫存檔。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
	2) 檢查是否未將敏感性資料儲存於系統日誌或自定義日誌。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合所有檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：任一檢測基準不符合
備註	無

基本資安檢測基準 – 檢測欄位範例2

檢測編號	4.1.2.3.5
安全分類	「行動應用App基本資安規範」第一類、第二類、第三類
檢測項目	行動應用程式敏感性資料儲存保護
檢測依據	「行動應用App基本資安規範」4.1.2.3.敏感性資料儲存
技術要求	敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存
檢測基準	1) 檢查行動應用程式是否採用金鑰有效長度為128位元（含以上）之先進加密標準（AES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準 2) 檢查行動應用程式是否採用金鑰有效長度為112位元（含以上）之三重資料加密演算法（Triple DES）。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準
檢測結果	符合要求：符合任一檢測基準，或行動應用程式未儲存敏感性資料 不符合要求：所有檢測基準皆不符合
備註	無

檢測方式

- 行動應用程式檢測性質屬**黑箱測試**，其檢測為滲透測試(攻與防)概念，故於本檢測基準僅提供檢測方式供參考
  - 考量行動應用程式開發商之行動應用程式原始碼屬**商業機密**
  - 「行動應用App基本資安規範」為**非強制性**，送測單位通常不會提供程式原始碼進行檢查
  - 各資安檢測業者所發展之檢測方法(Know-How)屬**商業機密**，難有標準一致性之檢測方法(SOP)
  - 檢測以**黑箱測試**方法論為主，主要以**未取得原始碼**之情況下進行測試
- 檢測方式
  - 採**靜態**分析與**動態**分析混合使用
  - 依實際檢測需要，進行行動應用App逆向工程(reverse engineering)或中間人(man-in-the-middle)測試等方法進行檢測

檢測結果與產出 – 參考項目

- 檢測結果與產出應包含但不限於以下內容
  - 檢測標的(含程式名稱、版本等)
  - 檢測範圍之宣告(檢測等級)
  - 檢測時程(含收件時程，檢測期間等)
  - 檢測方式、環境與使用工具
  - 檢測執行人員與負責項目
  - 檢測項目為「符合或不符合」之判定
  - 檢測過程紀錄及佐證資料

THANK YOU


YES!
INSTITUTE FOR INFORMATION INDUSTRY
big data
SEED NET
Y2K
NII
RFID
CMMI
Living Lab
FIND
IDEAS SHOW
ME.168.COM
e-TAIWAN
DOC
IA聯盟
雲端運算產業聯盟
台北港
聖多美號
SMART TOURISM
ADOC
SMART 101
人才培育
ISO 10646
樂活群聚
Best Link
Big-5