資安產業跨域聯防推動計畫-
資安募資輔導與資安認驗證機制推動

行動應用App基本資安檢測實驗室
檢測技術一致性會議

114年第2次會議

中華民國 114年 10月 29日

性別主流化

1.根據聯合國經濟暨社會理事會(ECOSOC)定義，「性別主流化」強調於各領域政治、經濟與社會層面政策與方案中，融入性別觀點降低不平等現象。
2.終極目標是達成性別的實質平等，即性別平權。

性別平權

1.消除社會中對婦女及性別一切形式的歧視
2.使社會大眾檢視生活週遭的性別不平等情況
3.促進女性參與決策，落實任一性別不少於三分之一，縮小性平差距。
4.建立尊重多元性別的態度及平等相處的互動

家庭暴力零容忍

1.被害人可撥打110或113保護專線
2.依需要就近向當地社政、警政、醫療衛生單位求助
3.可透過家暴庇護安置方案，接受緊急庇護或中長期安置服務。

性騷擾防治

1.防治性騷擾之政策宣示
2.舉辦性騷擾防治教育訓練
3.建立內部性騷擾申訴系統

性別平等相關政策與法規

國外
消除對婦女一切形式歧視公約(CEDAW)

國內
※消除對婦女一切形式歧視公約施行法
※性別平等政策綱領
※性別教育平等法
※性別工作平等法
※性騷擾防治法

關懷e起來

家暴案件線上通報
113線上諮詢
https://ecare.mohw.gov.tw

什麼是「性騷擾」

違反他人意願而向他實施與性或性別有關之行為，若造成對方的嫌惡，不當影響他的正常生活進行的，都算是「性騷擾」。

如有性別相關問題，可查詢行政院性別平等處網址http://www.gec.ey.gov.tw

moda 數位發展部 Ministry of Digital Affairs

數位發展部 數位產業署

蒐集個人資料告知事項暨個人資料提供同意書

- 數位發展部 數位產業署 委託計畫執行單位-台北市電腦商業同業公會辦理資安產業跨域聯防推動計畫(以下簡稱本計畫)，因應個人資料保護法及相關個人資料保護規定，在向您蒐集個人資料之前，依法向您告知下列事項，當您勾選「我同意」，表示您已閱讀、瞭解並同意接受本同意書之所有內容：
- 一、蒐集目的及類別
  為本計畫相關 報名作業管理、通知聯繫、活動訊息發布、問卷調查、相關統計分析之蒐集目的，而須獲取您下列個人資料類別：姓名、電話、E-mail、公司、職稱。
- 二、個人資料利用之期間、地區、對象及方式
  您的個人資料，除涉及國際業務或活動外，將提供本機關(構)於中華民國領域，於上述蒐集目的之必要合理範圍內加以利用至前述蒐集目的消失為止。
- 三、當事人權利行使
  依據個人資料保護法第3條，您可向計畫執行單位請求查詢或閱覽、製給複製本、補充或更正、停止蒐集/處理/利用或刪除您的個人資料。
- 四、不提供個人資料之權益影響
  如您不提供或未提供正確之個人資料，或要求停止蒐集/處理/利用/刪除個人資料、服務訊息的取消訂閱，本機關(構)將無法為您提供蒐集目的之相關服務。
- 五、各項通知服務、相關訊息之停止寄送
- 您可於上班時間聯繫計畫執行單位活動承辦人（電話(02)2577-4249，分機：889）。

個人資料同意提供：

- 一、本人確已閱讀並瞭解上述告知事項，「同意」授權本機關(構)於所列目的之必要合理範圍內，蒐集、處理及利用本人之個人資料。
- 二、本人瞭解此同意書符合個人資料保護法及相關法規之要求，並同意提供予貴機關(構)留存及日後查證使用。

議 程

時間	內容	主講者
13:30~13:40	主席致詞	行動應用聯盟 陳俊良 會長
13:40~13:50	聯盟報告事項	行動應用聯盟 秘書組
13:50~15:00	檢測議題討論 聯盟宣導事項	行動應用聯盟 秘書組
15:00~15:20	臨時動議	行動應用聯盟 秘書組
15:20~15:30	結論	陳俊良 會長

行動應用App基本資安檢測實驗室

檢測技術一致性會議

聯盟報告事項

行動應用App基本資安檢測實驗室一致性會議，於10/29(三) 501會議室召開，統計如下：

- 出席名單：18家檢測實驗室、委員及顧問
- 出席數：共71人包括實驗室59人(實體：22人；線上37人)；委員及顧問實體8人；秘書組4人
- 提案數：於10/16截止收件，共9案

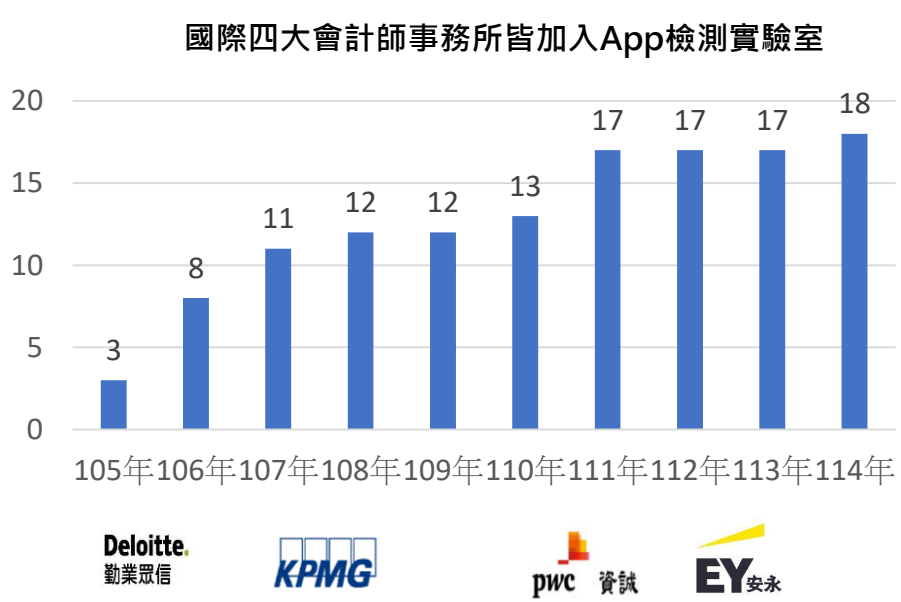
	實驗室	提案數	出席數
1	中華電信股份有限公司電信研究院	1題	實體：2人；線上：7人
2	安華聯網科技股份有限公司	1題	實體：2人
3	財團法人台灣商品檢測驗證中心	3題	實體：1人；線上：2人
4	數聯資安股份有限公司	4題	實體：2人；線上：4人
5	三甲科技股份有限公司	未提案	實體：2人；線上：1人
6	光盾資訊科技有限公司		線上：4人
7	安永諮詢服務股份有限公司		實體：3人；線上：1人
8	安侯企業管理股份有限公司		線上：3人
9	安碁資訊股份有限公司		實體：2人
10	行動檢測服務股份有限公司		線上：3人
11	財團法人電信技術中心		線上：3人
12	國家中山科學研究院資訊安全中心		線上：2人
13	勤業眾信聯合會計師事務所		實體：2人
14	新北市政府資訊中心		實體：2人
15	資誠企業管理顧問股份有限公司		線上：2人
16	關貿網路股份有限公司		實體：2人；線上：2人
17	耀睿科技股份有限公司		線上：3人
18	鑒真數位有限公司		實體：2人

App資安標章整體概況

資安認驗證機制推動現況

行動應用App資安檢測實驗室18家

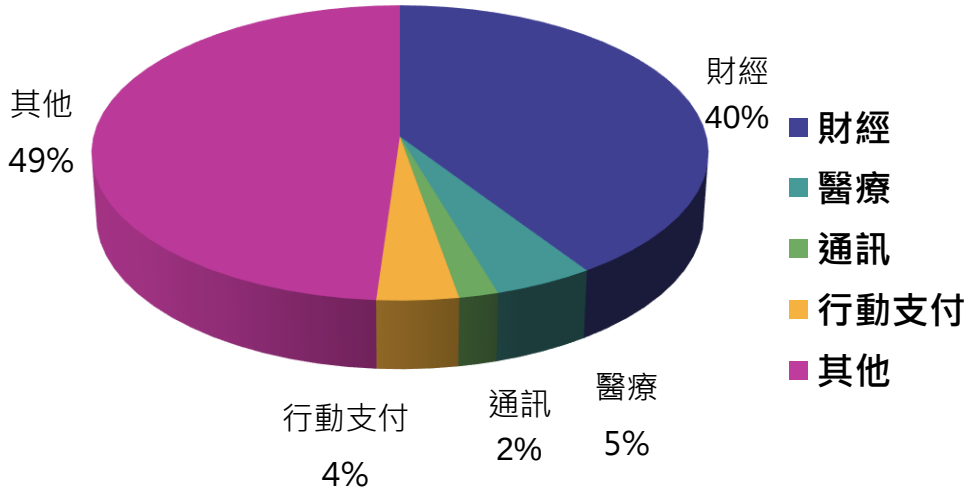
序	實驗室
1	鑒真數位有限公司
2	勤業眾信聯合會計師事務所
3	中華電信(股)公司電信研究院
4	安華聯網科技(股)公司
5	行動檢測服務(股)公司
6	財團法人台灣商品檢測驗證中心
7	安碁資訊(股)公司
8	安侯企業管理(股)公司
9	#財團法人電信技術中心
10	數聯資安(股)公司
11	關貿網路(股)公司
12	資誠企業管理顧問(股)公司
13	光盾資訊科技(股)公司
14	#國家中山科學研究院
15	安永諮詢服務(股)公司
16	三甲科技(股)公司
17	耀睿科技(股)公司
18	新北市政府資訊中心



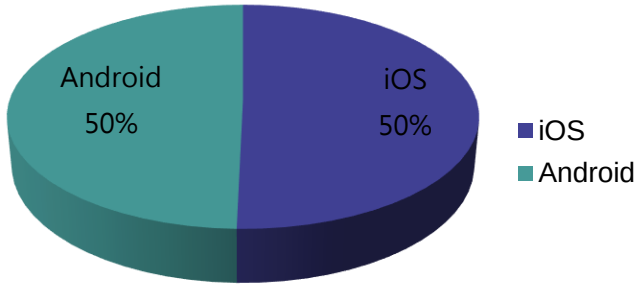
備註：#不收民間單位案件

App資安標章整體概況
113年度通過分析

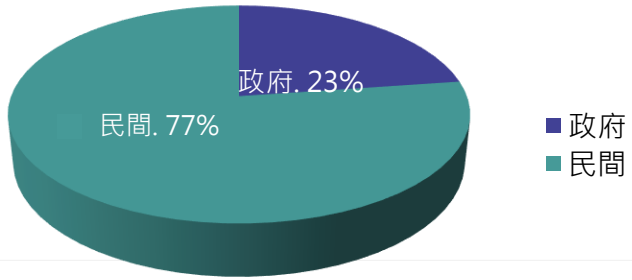
- 113年度行動應用App基本資安檢測基準App收件1,507件、通過1,507件（政府343件、民間1,164件）。較112年同期（1,270件）成長18.5%，政府成長率9.9%（112年同期政府312件）、民間成長21.3%（112年同期民間958件）
- App類別包括，通訊28件、財經613件、 行動支付58件、醫療71件、其他類別737件



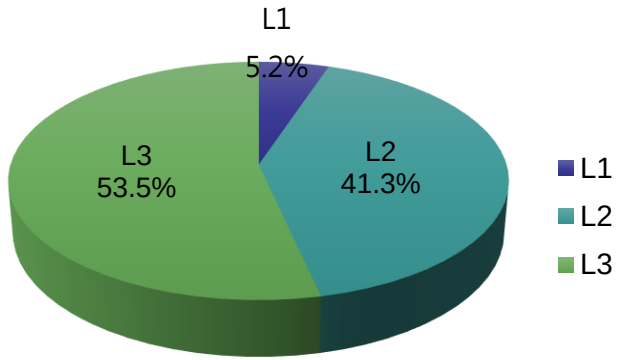
App作業系統：iOS 759件、Android：748件



政府343件、民間1,164件

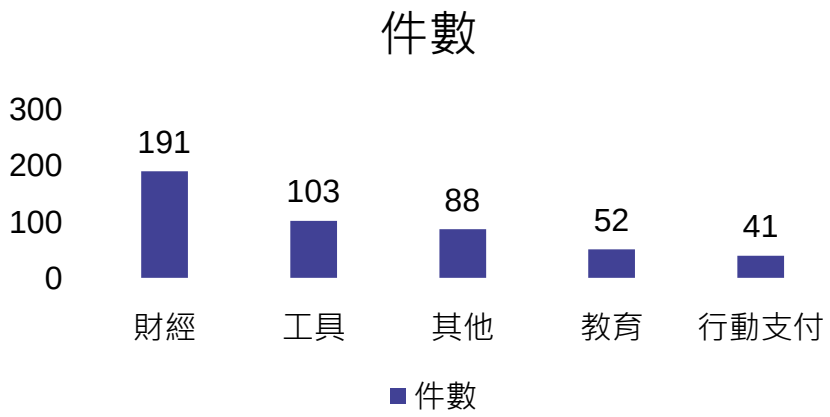


L1共78件、L2共623件、L3共806件

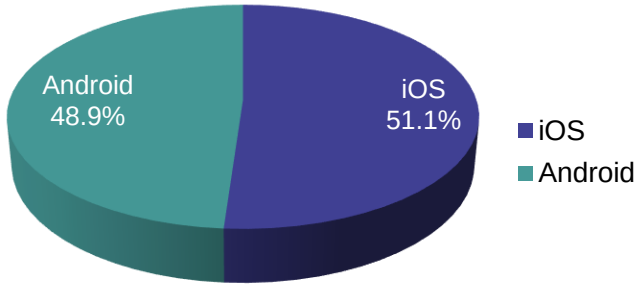


App資安標章整體概況
114年度通過分析

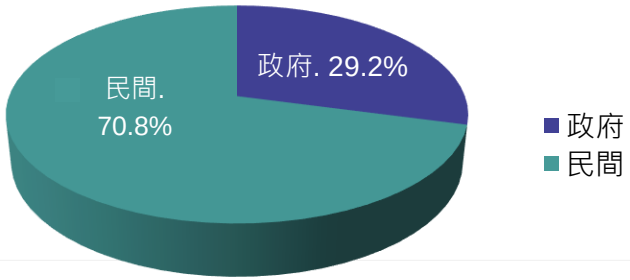
- 截至114/9/30，114年度行動應用App基本資安檢測基準App收件通過626件（政府181件、民間445件）。較113年同期（811件）負成長22.8%，政府負成長率8.1%（113年同期政府197件）、民間負成長27.5%（113年同期民間614件）。
- 前5大類分別為：財經147件、工具83件、其他80件、教育43件、行動支付35件



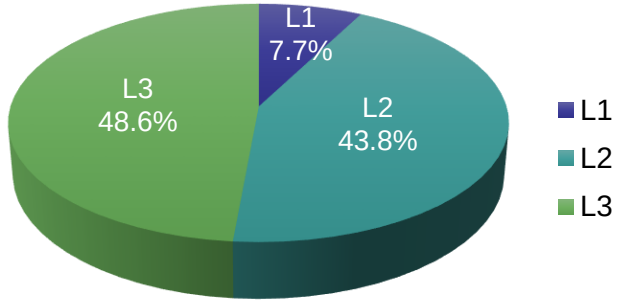
App作業系統：iOS 320件、Android：306件



政府181件、民間445件



L1共48件、L2共274件、L3共304件



行動應用App基本資安檢測實驗室

技術一致性會議

檢測實驗室提案

❑ 提案一：

- 測項：4.1.2.3.2
- 主旨：行動應用程式若無設計儲存敏感性資料於行動裝置之功能，且未檢測出敏感性資料儲存事宜時，是否仍需強制檢測「提供使用者拒絕儲存敏感性資料之功能」？
- 說明：依據檢測編號4.1.2.3.2，技術要求是「行動應用程式應提供使用者拒絕儲存敏感性資料之權利」，檢測項目 (1) 為檢查 App 是否提供此功能。
  1. 若App 在設計上就沒有將敏感性資料儲存於本地端的功能 (比如金融證券業App「記住我」、「記住帳號」)，且技術驗證也確認 App 實際上沒有儲存敏感性資料，則 App 在此項的判斷應屬於「適用條件不成立」。
  2. 依據檢測基準「符合要求」的判讀為：「符合所有檢測基準，或行動應用程式未儲存敏感性資料。」
  3. 因此，實驗室是否僅需確認 App 實際未儲存敏感性資料 ，即可直接判斷 4.1.2.3.2 為「符合要求」？
- 建議：由於近期收到審查建議要檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能，可否建議參考檢測編號4.1.2.3.1. ，行動應用程式未儲存敏感性資料，就無需強制檢查行動應用程式是否提供使用者拒絕儲存敏感性資料之功能。

決議：實驗室應自行驗證是否有儲存敏感性資料，同時實驗室宜檢附「行動應用 App 基本資安檢測資料調查表」(自主宣告表)

❑ 提案二：

- 測項：4.1.2.3.16
- 主旨：修正檢測基準說明
- 說明：基準說明為「檢查行動應用是否將敏感性資料儲存或輸出於系統日誌中。」
- 建議：將基準修正為「檢查行動應用程式是否將敏感性資料儲存或輸出於系統日誌中。」

決議：同意，將修正於文件勘誤表，並同步更新於MAS官網

❑ 提案三：

- 測項：4.1.2.4.1、4.1.4.1.2、4.1.4.2.1、4.1.4.2.2、4.1.4.2.3、4.1.4.2.4、4.2.2.1.2
- 主旨：受限於裝置、網路設定，針對封包傳輸測項處置方式
- 說明：由於受測 APP 所連接之後端伺服器屬於封閉環境，無法透過白名單設定進行開放，僅能以特定SIM卡或特定裝置進行連線。在檢測過程中，正常流程需建立 Proxy攔截封包，以進行封包傳輸相關測項的驗證與分析。然而，受限於上述網路連線限制，雖然客戶提供的受測APP 已可安裝於實驗室檢測設備並完成大部分測項測試，但因無法連線至後端伺服器，導致封包攔截與傳輸類測項無法實際執行。是否可於檢測調查表中以備註方式說明該受限原因與連線限制方式，並據此將相關封包連線測項標註為「通過（依限制情況判定）」或「不適用（N/A）」。

決議：由於無法連線，行動應用程式並無法正常使用，實際上的狀況是未測試，甚至測試情境不完整的狀況下，也會影響到其他測試項目，因此不得列為通過或不適用，應與送測機構要求提供可執行的測試環境

❑ 提案四：

- 測項：4.1.3.2.3
- 主旨：「預授權交易」定義與適用範疇
- 說明：預授權交易係指暫時保留一筆金額，但尚未完成真正的扣款行為，常見於飯店入住、租車等交易場景。此類交易通常會先向發卡銀行請求授權，待服務完成後再進行正式扣款。然而，若 App 提供「預約轉帳」功能，例如使用者設定未來某日進行轉帳，系統於當下僅記錄指令，並於指定日期執行扣款，是否亦可視為一種「預授權交易」？希望釐清預授權交易是否需具備即時保留額度的特性？或是否包含所有延後執行的交易指令

決議：預約轉帳可視為預授權，但不需要有即時保留額度，包含所有延後執行的交易

❑ 提案五：

- 測項：4.1.3.2.3
- 主旨：授權時之風險宣告是否有更明確的定義或範疇，或是範例
- 說明：風險宣告的定義是否有明確範疇？例如是否僅限於資安風險，或也包含環境、系統、流程等風險。若 App 提供如「颱風天可能導致交易延遲」或「提醒使用者交易慎防詐騙」等訊息，是否皆可視為符合此項基準？

決議：這一題最大的關鍵在於，授權未來多筆交易，風險在於未來會持續交易，直到使用者終止，舉例來講，像是水電費，如果有一天賣房了，就要自己記得停止交易

❑ 提案六：

- 測項：4.1.5.1.3
- 主旨：螢幕覆蓋攻擊防護/示警機制之適用範圍
- 說明：螢幕覆蓋攻擊防護/示警機制是否需全面套用於 App 所有畫面，或僅需針對涉及敏感資料輸入、交易操作等高風險畫面進行防護？

決議：整個應用程式，都應該避免螢幕覆蓋攻擊，否則非敏感功能之頁面，仍有可能存在風險，例如非敏感頁面，被偽裝成登入頁

❑ 提案七：

- 測項：4.1.5.3.1
- 主旨：修正查詢 CVSS 分數依據改為最新版本
- 說明：目前 NIST 官方針對多個 CVE 漏洞採用 CVSS 4.0 版本，並未採用 CVSS 3.0 版本
- 建議：將 CVSS 版本改為最新版，不限制於 CVSS 3.0 版本

決議：同意，若有CVSS 4.0分數，可直接參考4.0分數，後面請修改基準用字為「最新版」

❑ 提案八：

- 測項：4.1.5.4.2行動應用程式應提供相關注入攻擊防護機制
- 主旨：行動應用程式已4.1.5.4.1於前端有進行初步防護設計進行檢測(阻擋特殊字元無法輸入)，已無法有效從前端介面進行注入攻擊，故在4.1.5.4.2是否仍需進行每一項 Injection攻擊檢測
- 說明：行動應用程式於前端有進行初步防護設計進行檢測，已無法有效從前端介面進行注入攻擊

備註	未來如有新型 Injection 攻擊手法，亦納入檢測基準。 有效的注入攻擊防護機制應於伺服器端對使用者輸入之字串進行處理，基於防禦縱深概念，且本檢測基準檢測範圍為行動應用程式本身，實驗室至少須於行動應用程式對於輸入注入攻擊字串是否有初步防護設計進行檢測。

- 建議：
  1. 4.1.5.4.1 檢測App於前端已有進行初步防護設計(阻擋特殊字元無法輸入)，因已無法輸入注入攻擊字串，故 4.1.5.4.2 已無法再針對每項注入攻擊輸入攻擊字串進行有效攻擊，行動應用程式對輸入住入攻擊字串已有初步防護設計，應予以符合 (報告4.1.5.4.2如此陳述說明，審查被退件)
  2. 如認為上述不盡正確且仍須測試，請提供此條件下之正確的測試方法，以達檢測標準的一致性

決議：仍請實驗室提供截圖搭配說明，讓審查委員瞭解應用程式的輸入防護機制

❑ 提案九：

- 測項：4.2.2.1.2
- 主旨：新增白名單網域
- 說明：依據實務經驗多個 APP 登入方式會採用 Line 登入或是 Apple ID 登入，登入功能會採用 Webview 呈現功能， Line 或是 Apple 皆為大眾熟知的登入方式及網域，因此建議將 Line 登入或是 Apple ID 登入的網域參考Google登入判定方式列入白名單中。
- 建議：將Line 登入網域 (access.line.me) 以及 Apple ID 登入網域 (appleid.apple.com) 列為白名單。

決議：同意

行動應用App基本資安檢測實驗室

檢測技術一致性會議

聯盟宣導事項

❑ 宣導事項一：

- 為提升檢測報告品質，未來評量績優實驗室時，將把實驗室對「建議修正」項目的回應列為重要評分依據，藉此強化審閱意見的影響力。

為協助提升檢測報告品質，擬修訂「行動應用App基本資安檢測實驗室績效評核辦法」新辦法將以「正面表列」的形式，鼓勵檢測實驗室降低「建議修正」項目，提供實驗室在檢測作業上可參考修正與改善的項目與內容，期許各實驗室藉由調整與優化，達成品質的全面提升

❑ 宣導事項二：

■ 依據TAF「智慧連網服務系統資安檢測實驗室認證服務計畫 」
文件編號：TAF-CNLA-A24(5) 第9條規定，截圖如下，敬請檢測實驗室配合辦理。

9. 使用本會認證標誌

9.1 認證實驗室應使用最新版本試驗方法提供測試服務，並於測試報告上明確識別試驗方法及使用本會認證標誌。

9.2 認證實驗室應依據本會「使用認證標誌與宣稱認可要求」(TAF-CNLA-R03)的規定使用本會認證標誌。

❑ 宣導事項三：

■ 更新知識庫-於行動應用資安聯盟網站，公告檢測技術一致性會議決議，敬請實驗室夥伴參閱。