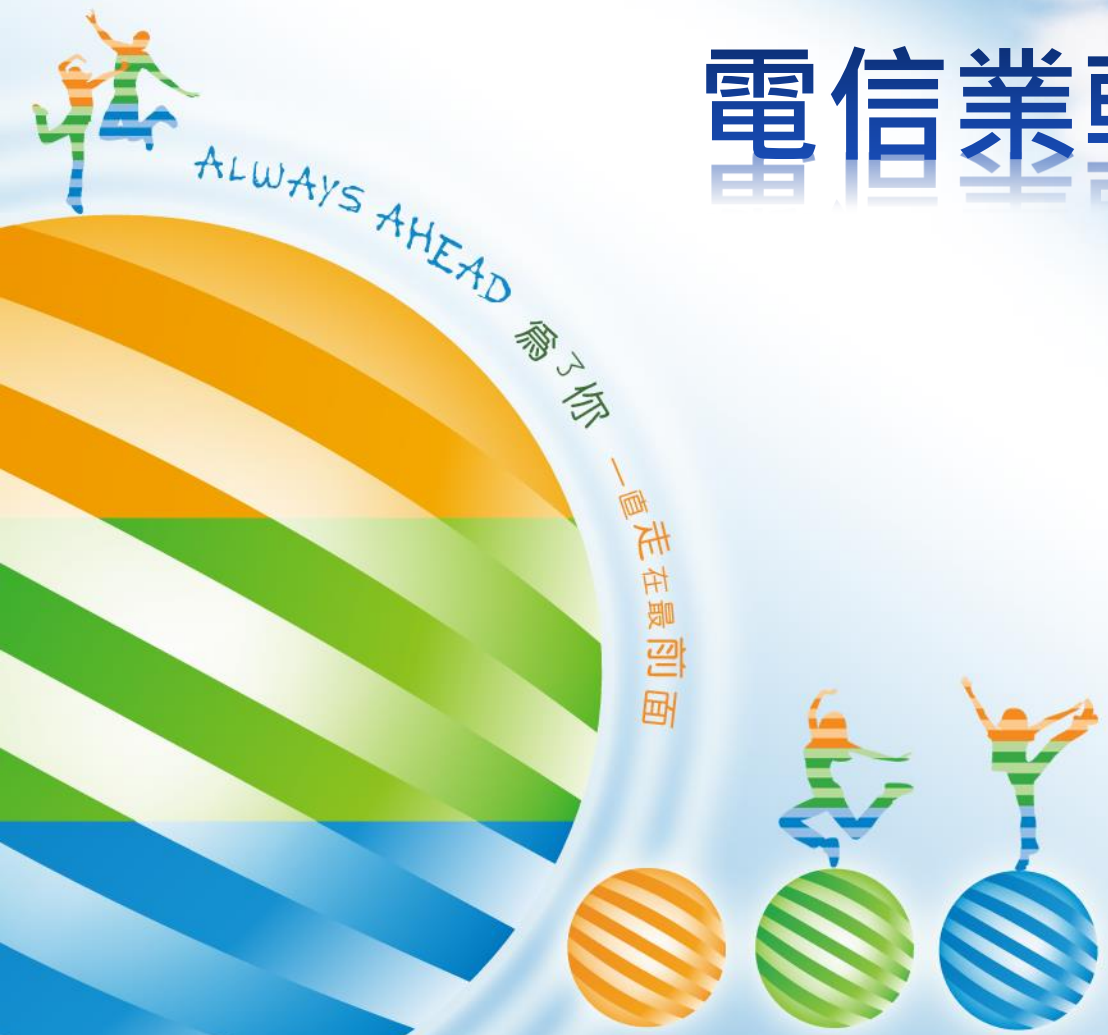
中華電信
Chunghwa Telecom




# 電信業軟體測試技術與案例分享

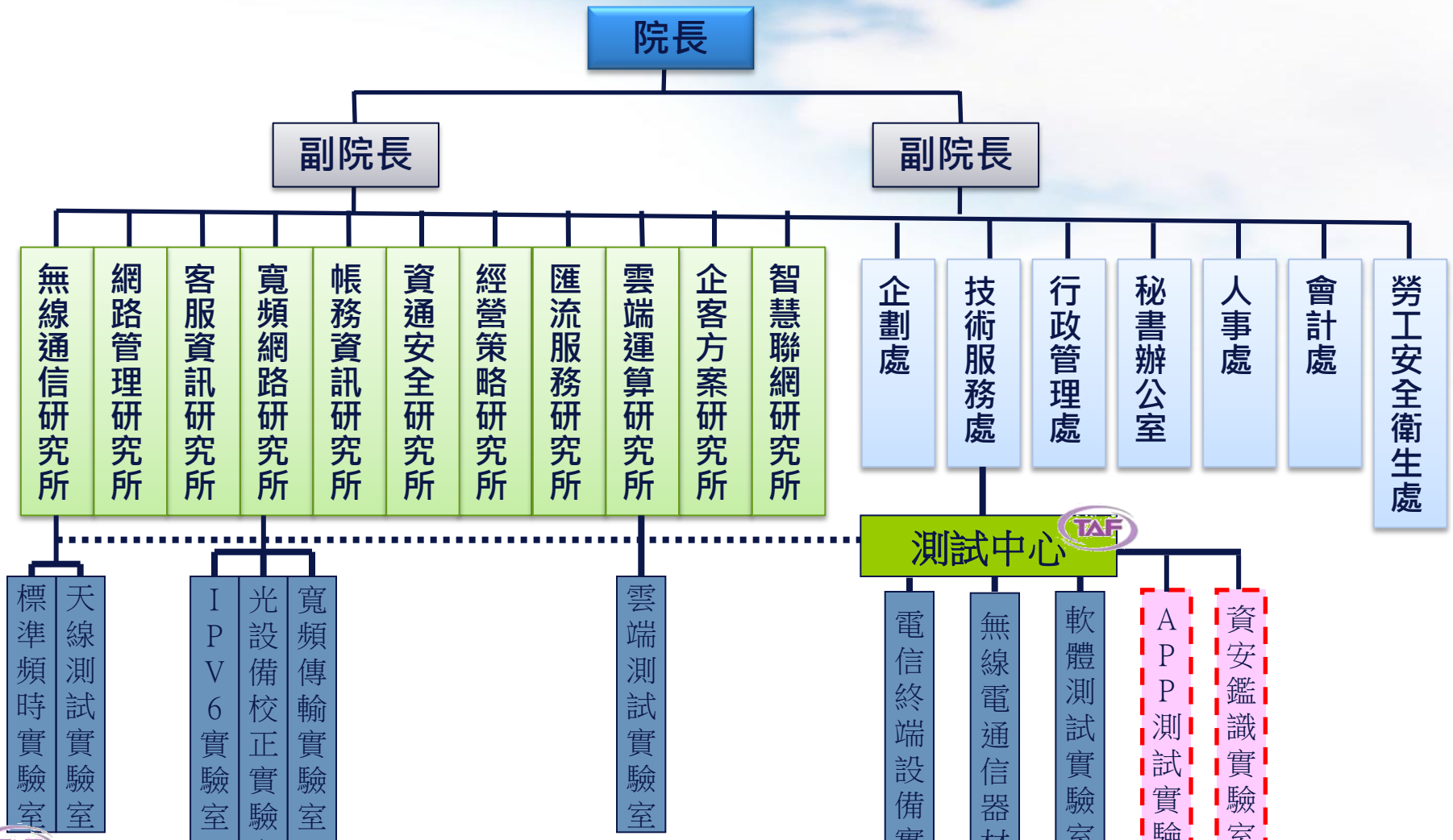
中華電信研究院
董元昕

日期：2015/09/23

# 內容

- 簡介
- 軟體測試
- 效能測試
- 安全測試
- 功能測試

# 中華電信研究院組織架構

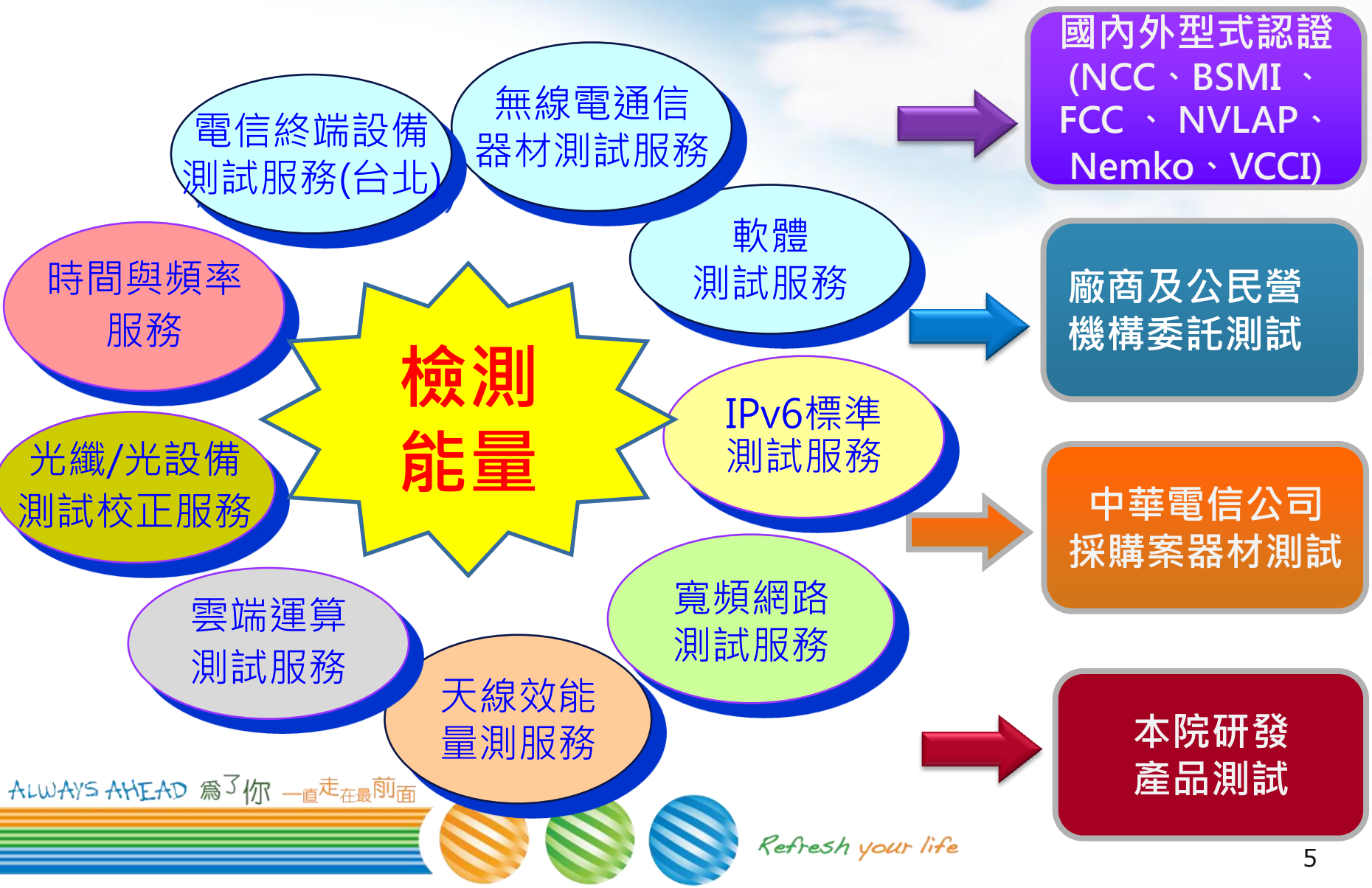


# 中華電信研究院研發領域

中華電信 Chunghwa Telecom

**3大領域**
**8項主題**
**17項關鍵計畫**

# 中華電信研究院檢測服務



# 測試實驗室認證

中華電信 Chunghwa Telecom

## 國內認證

- 全國認證基金會(TAF)認可登錄實驗室
- N.C.C指定通信介面測試實驗室
- BSMI標準檢驗局認可安規及EMC測試實驗室
- 經濟部能源局認可節能標章測試實驗室
- 環保署認可環保標章測試實驗室
- 消防署認可消防器材測試實驗室
- IPv6認可測試實驗室

BSMI 標準檢驗局

## 國外認證

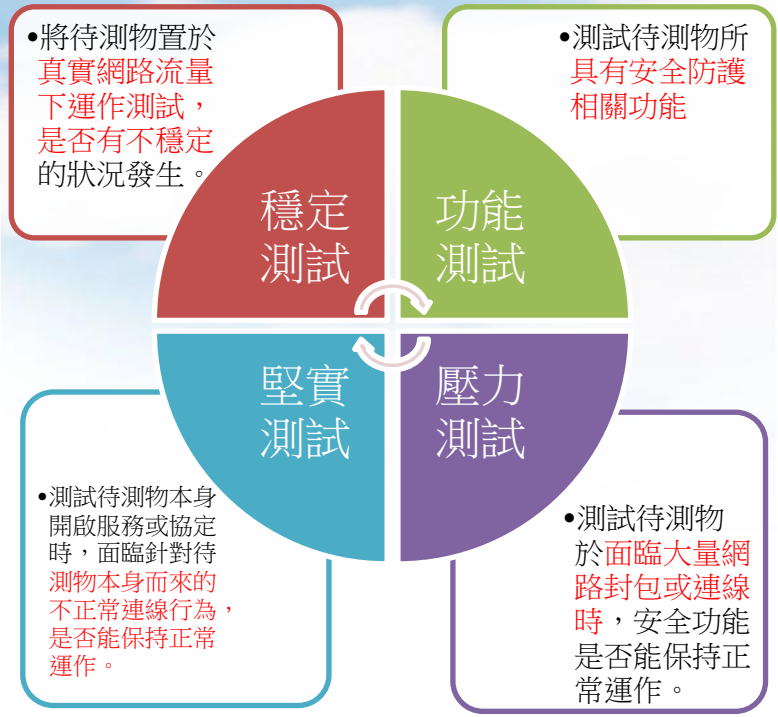
- TUV認可安規測試實驗室
- UL認可安規測試實驗室
- UL認可EMC測試實驗室
- 亞太APEC MRA登錄認可測試實驗室
- NVLAP登錄認可測試實驗室
- Nemko登錄認可測試實驗室

# 資通安全認證

中華電信 Chunghwa Telecom

## ❖ 測試項目

| | |
|---|---|
| 1.網路型防火牆 | 5.網頁應用防火牆 |
| 2.入侵偵測防禦系統 | 6.應用軟體控管 |
| 3.防毒閘道設備 | 7.乙太網路交換器 |
| 4.網路垃圾郵件過濾設備 | 8.路由交換器 |




## ❖ 應用成果

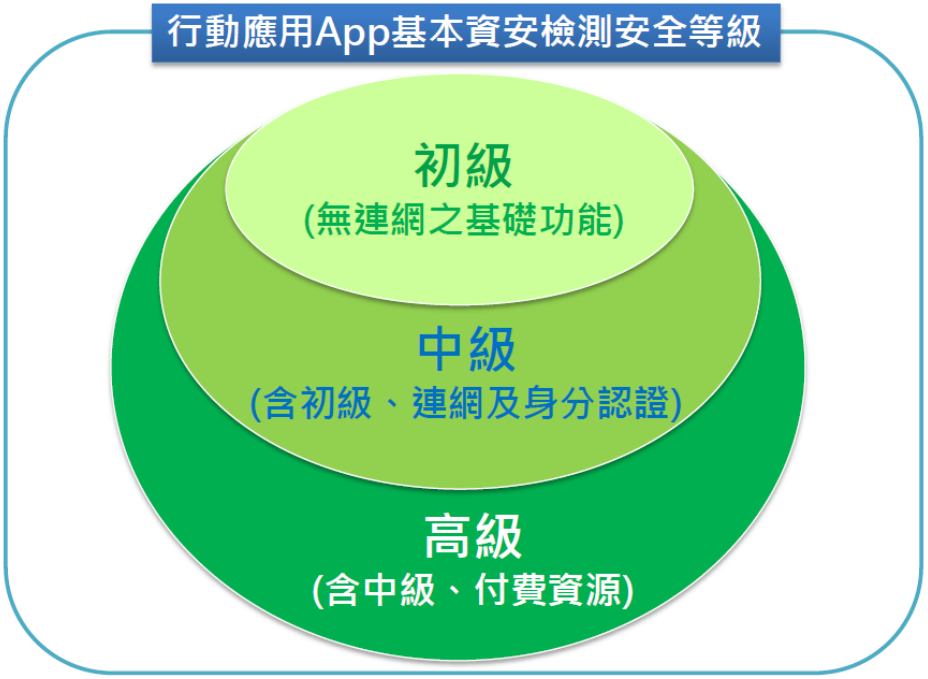
- 為確保資通訊設備選用品質，NCC訂有資通訊設備檢測技術規範(IS0008~IS0015)，而測試中心於2014年經全國認證基金會(TAF)認證符合該技術規範，取得ISO/IEC 17025認證。
- 針對資通設備提供資通安全認證，提供穩定、功能、堅實與壓力測試服務，此測試技術也可應用於ICT設備的測試。

# 行動應用App基本資安檢測

中華電信 Chunghwa Telecom

TAF 經濟部工業局 INDUSTRIAL DEVELOPMENT BUREAU MINISTRY OF ECONOMIC AFFAIRS

8/17 經濟部工業局公告
「行動應用App基本資安檢測基準」V1.0

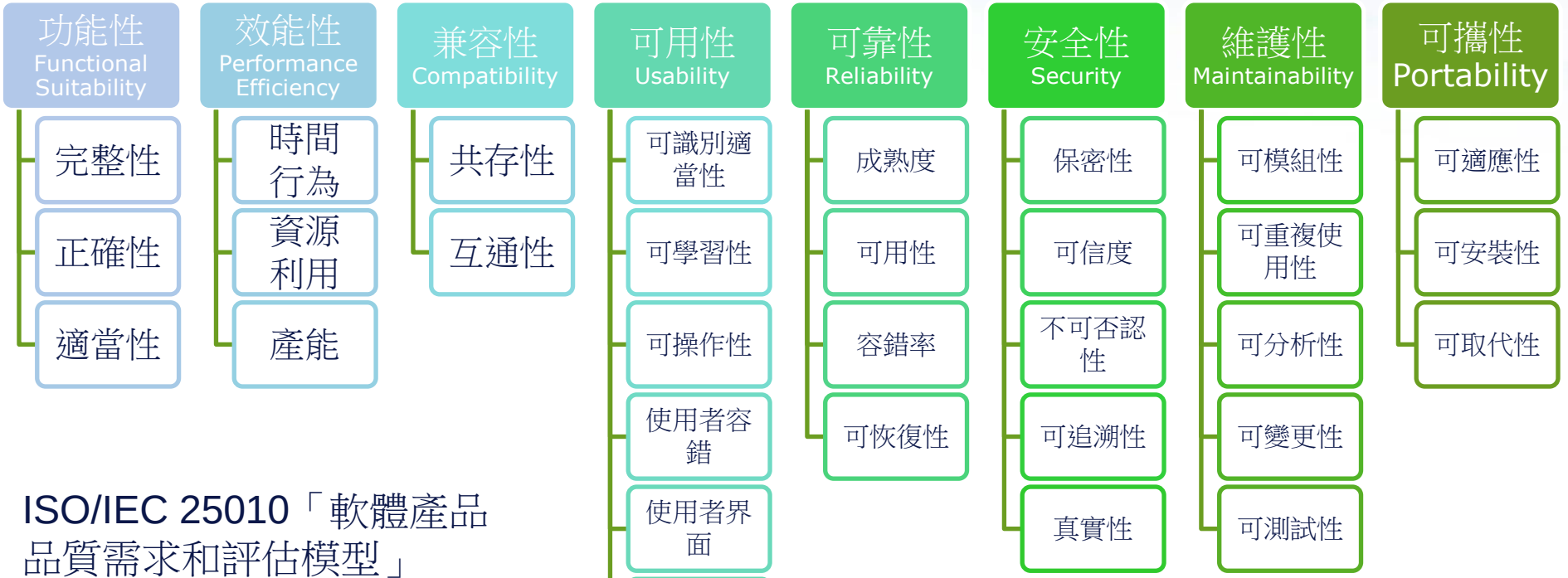



- 共計五大類、41個測試項目
- 依據安全等級分成三等級；初、中、高級
- 涵蓋Android、iOS、Windows三種平台手機

# 品質指標與軟體測試項目(1/2)

中華電信 Chunghwa Telecom

- 採用ISO/IEC 25010「軟體產品品質需求和評估模型」中的品質量化指標，建立包含功能、效能、可用、可靠及安全之軟體品質的重要衡量指標，量化為可被測量的屬性，訂定軟體品質量化指標的重要參考。

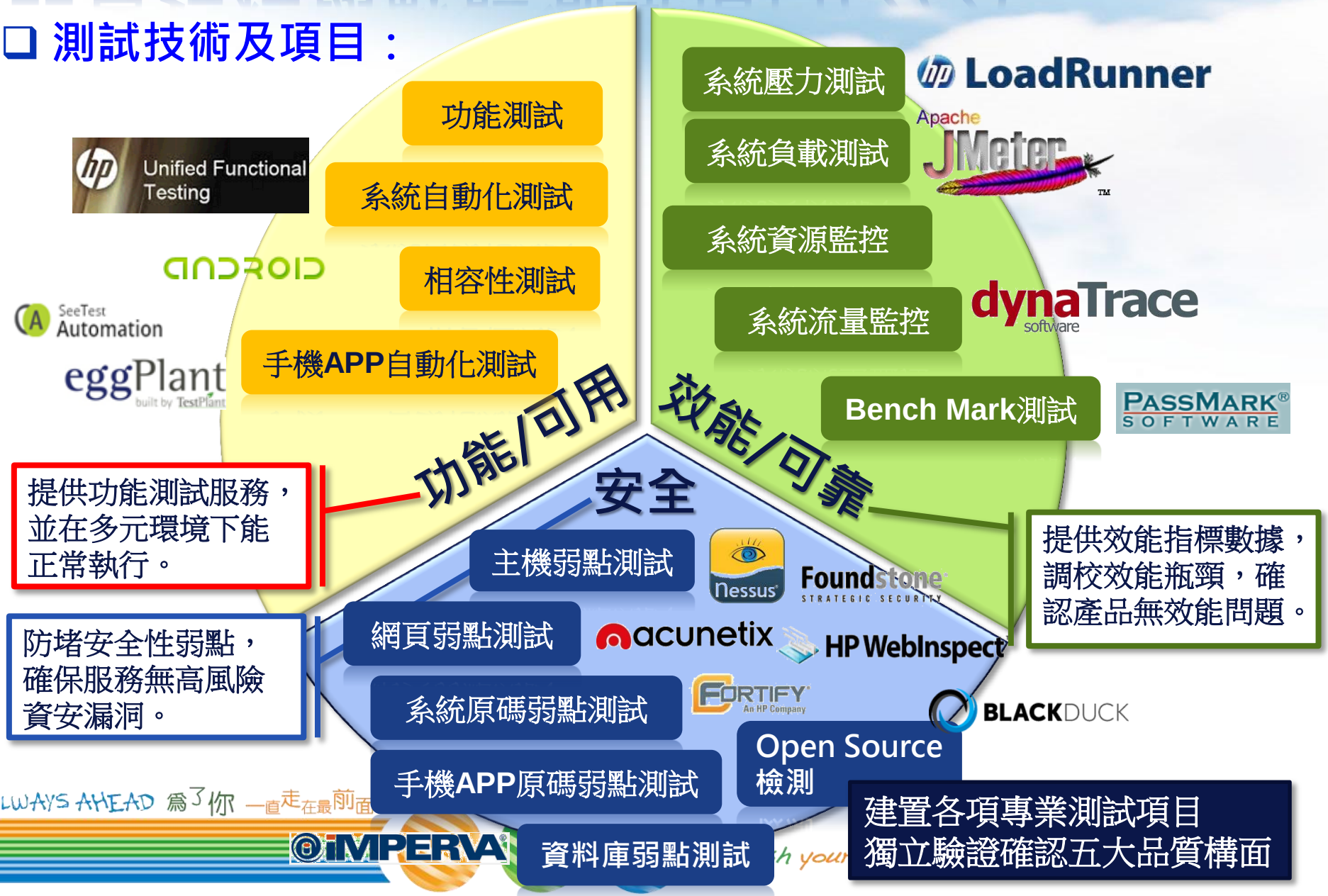



ISO/IEC 25010「軟體產品品質需求和評估模型」

# 品質指標與軟體測試項目(2/2)

中華電信 Chunghwa Telecom

## ❑ 測試技術及項目：



# 軟體測試議題

- 效能測試+雲端運算
- 安全測試+滲透測試
- 功能測試+APP自動化

# 效能測試

# 效能測試之重要性

中華電信 Chunghwa Telecom

## 高鐵又當機! 發號碼牌售票 (自由時報, 2007)

- http://www.libertytimes.com.tw/2007/new/jan/18/today-life7.htm
- 高鐵的票務系統，號稱斥資高達十五億元打造，但一面對消費者，卻脆弱得不堪一擊，問題到底出在哪？從目前發現的缺失來看，票務帳務合一、計算邏輯有誤、沒有精細地整合測試，可能都是原因。
- 歐晉德承認：票務系統沒有完整測試，導致搶票大亂

## 台灣彩券大當機! 電腦投注站吐苦水(TVBS, 2007)

- http://www.tvbs.com.tw/news/news_list.asp?no=blue20070104115144
- 中國信託強調，所有的帳務資料都正確無誤，到底哪裡出了問題，台灣彩券還在查證中。

## 實價登錄今上線、塞爆網站大當機(Yahoo!, 2012)

- http://tw.news.yahoo.com/
- 內政部實價登錄資訊凌晨正式上線，不過一上線就大爆滿，造成網頁大當機，到現在都還無法查詢。不過有學者認為，實價登錄上線有助於想買房的民眾，更了解市場行情，也可以讓亂開高價亂喊價的假象無所遁形。
- 實價登錄網頻爆問題，張善政積極協調2周內架雲端平台(鉅亨網, 2012)

# 系統效能測試與調校議題

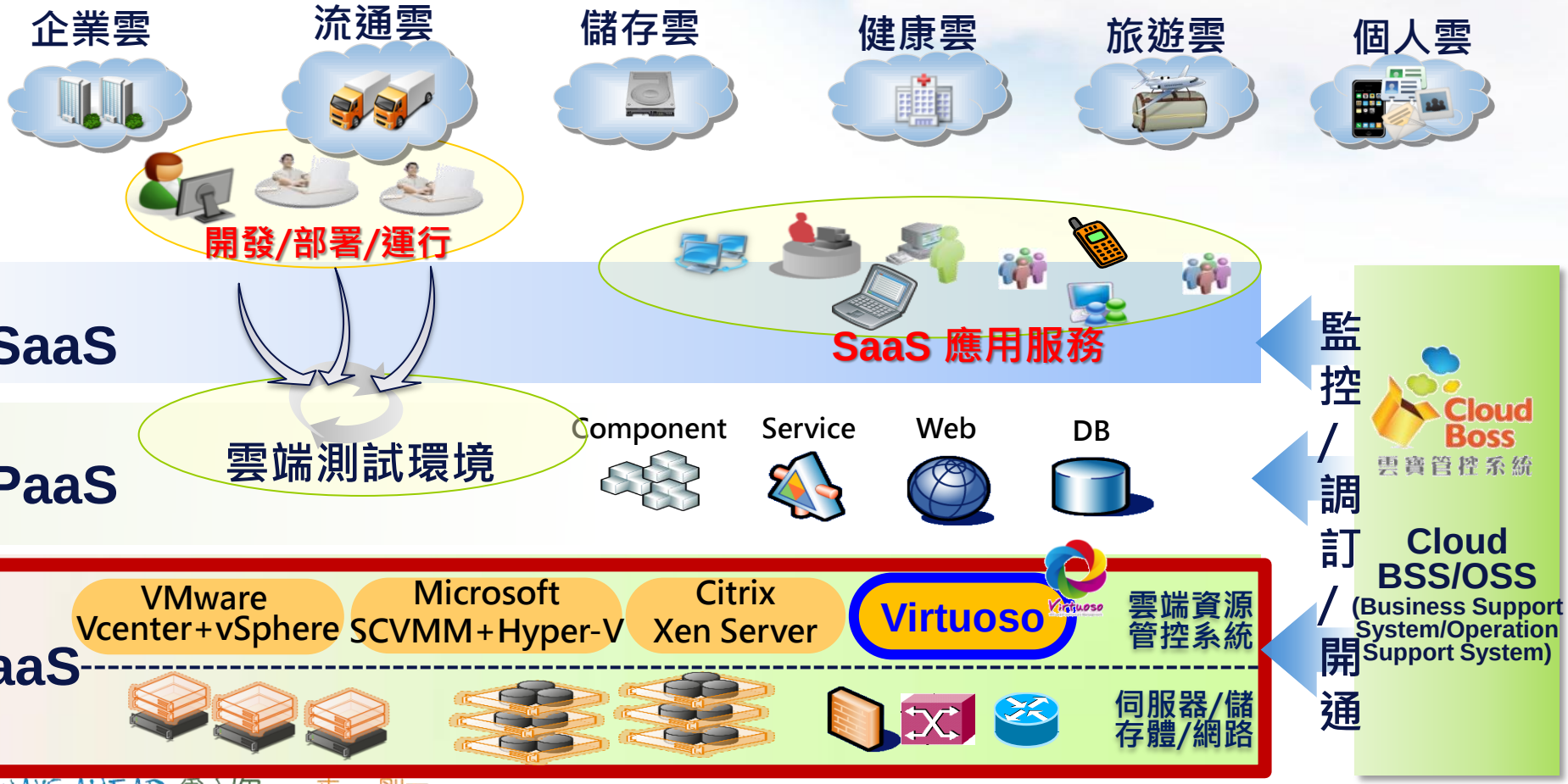


- 網站每小時湧入200萬人，每人平均處理時間30秒。如何模擬壓力測試？
- 每分鐘：2000000/60=33334人
- 同時線上：33334/2=16667人
- 壓力測試設備每台可模擬100~150人壓力量，共需要100~160台伺服器設備。
- 臨時去哪找那麼多台電腦？多大頻寬？需要多少成本？有沒有其他什麼好方法？
- 雲端運算

# 運用雲端資源

中華電信 Chunghwa Telecom

- 善用雲端運算特性，快速建置虛擬機，部署網路環境，要幾台有幾台
- 測試後回歸雲端資源池



# 案例分享

# 安全測試

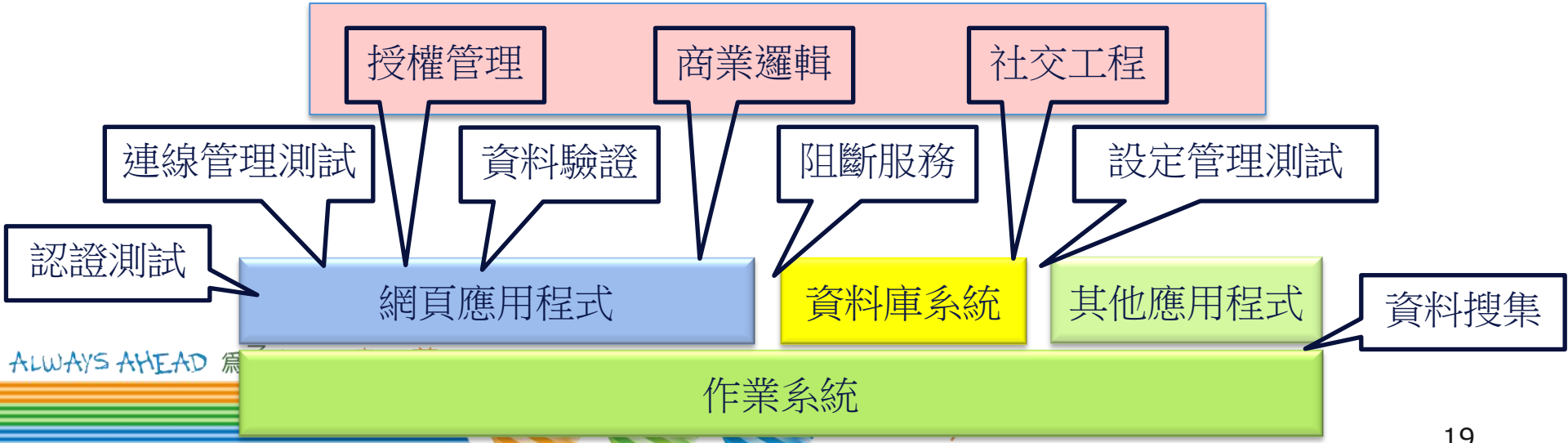
# 資安測試技術

中華電信 Chunghwa Telecom

| 檢測項目 | 檢測工具 | 說明 |
| --- | --- | --- |
| 資料庫檢測 | iMPERVA SecureSphere IMPERVA | 針對資料庫設定，進行測試，掃描出資料庫存在的弱點，評估送測資料庫的安全等級 |
| 原碼檢測 | HP Fortify SCA FORTIFY SOFTWARE | 確保程式原始碼無內部邏輯漏洞，掃描規則包含有OWASP常見弱點。 |
| 網頁檢測 | HP Webinspect或 Acunetix 9 HP WebInspect acunetix WEB APPLICATION SECURITY | 模擬駭客進行自動化攻擊，檢驗基本網站弱點，包含最新OWASP的弱點列表在內。 |
| 主機檢測 | McAfee Foundstone (Vulnerability Manager) McAfee | 掃瞄建置系統的相關主機、設備，以確認主機作業系統設定、安裝軟體版本是否有弱點。 |
| 網路測試 | IXIA BreakingPoint, Codenomicon Defensic ixia CODENOMICON defensics | 執行網路設備安全測試，包含安全性功能、堅實、效能、模糊等測試 |

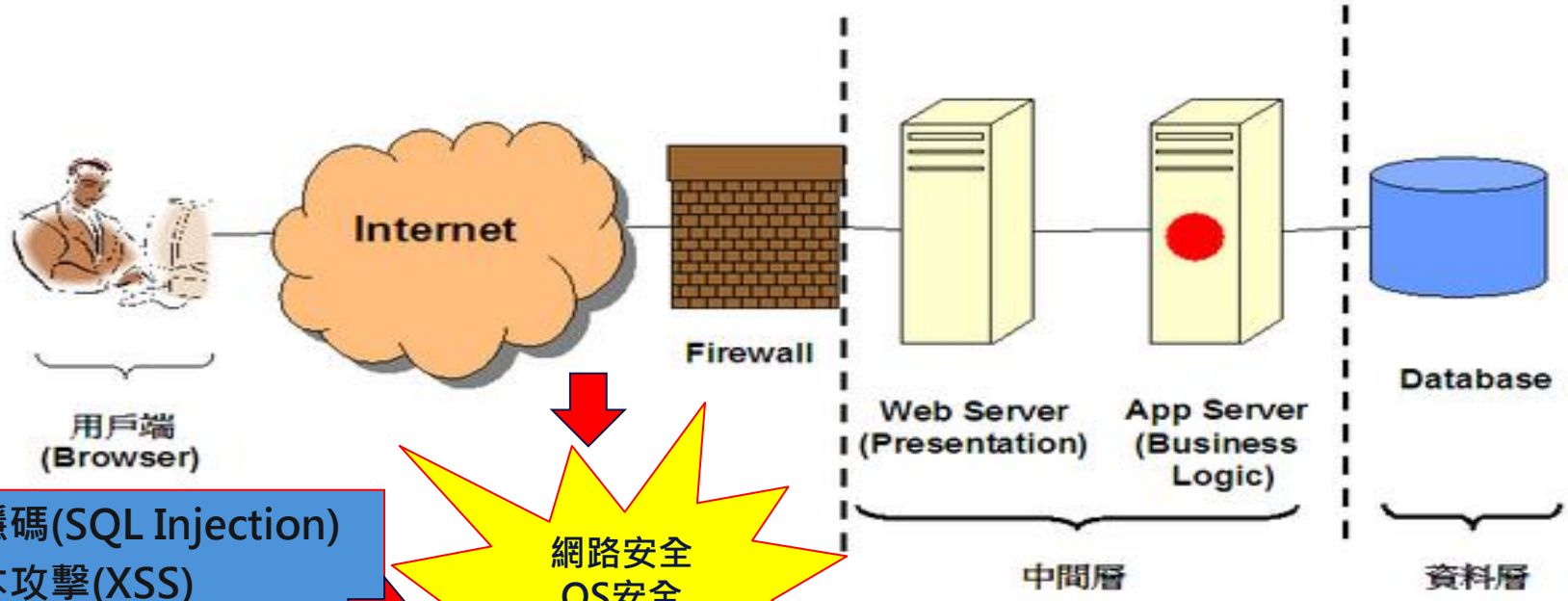
# 滲透測試

- **什麼是滲透測試？**滲透測試是以駭客的角度出發，模擬攻擊者的思考方式，利用所有可行的駭客手法試著入侵到公司內部，對目標系統進行各種入侵攻擊行為。
- **為什麼要滲透測試？**
- **與傳統資安測試有什麼不同？**



# 駭客滲透無網不入

中華電信 Chunghwa Telecom




資料隱碼(SQL Injection)
跨腳本攻擊(XSS)
跨冒名請求(CSRF)
緩衝區溢位
網頁伺服器漏洞

網路安全
OS安全
Patch安全
資料存取安全

Web/App 應用程式安全

資料伺服器安全

敏感資料的安全議題

網路安全

主機安全

應用程式安全

資料(庫)安全

ALWAYS AV 一直走在最前面

Refresh your life

# 資安測試技術

中華電信 Chunghwa Telecom

* 網路/網路設備安全
* 機房安全
* 遠端存取安全(SSH,SSL,VPN)

* 作業系統(OS)安全
* VM/interVM安全
* 軟體Patch

* API安全
* 應用伺服器安全
* 應用程式安全

* 用戶資料安全
* DB伺服器安全

**安全測試與偵測**

* 網路設備測試
* 機房安全測試(防火牆/IDS/...)
* 安全的登入機制(SSL)

*主機弱點掃瞄(OS Patch)
*VM/InterVM弱點掃瞄

*應用程式弱點掃瞄
*滲透測試
*程式碼白箱測試

* DB資料庫弱點偵測
* 機敏資料掃瞄

# 滲透測試案例分享(1/3)

- 某系統提供有線上購物之功能，然而其設計流程不當，使用者於下單過程中，可竄改商品價格，將造成帳務錯誤。
- 商業邏輯的漏洞，自動化掃描工具難以找出，但影響往往極大，應是滲透測試執行的重點項目。

# 滲透測試案例分享(2/3)

中華電信 Chunghwa Telecom

## OWASP Top 10 2013

1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting
4. Insecure Direct Object References
5. S
6. S
7. M
8. C
9. U
10. Unvalidated Redirects and Forwards

**不安全的物件參考：**

重要檔案、資料存取未再經過權限驗證

藉由路徑修改取得其他伺服器上機敏資料

弱點掃描工具難以找到

**解決方式：**

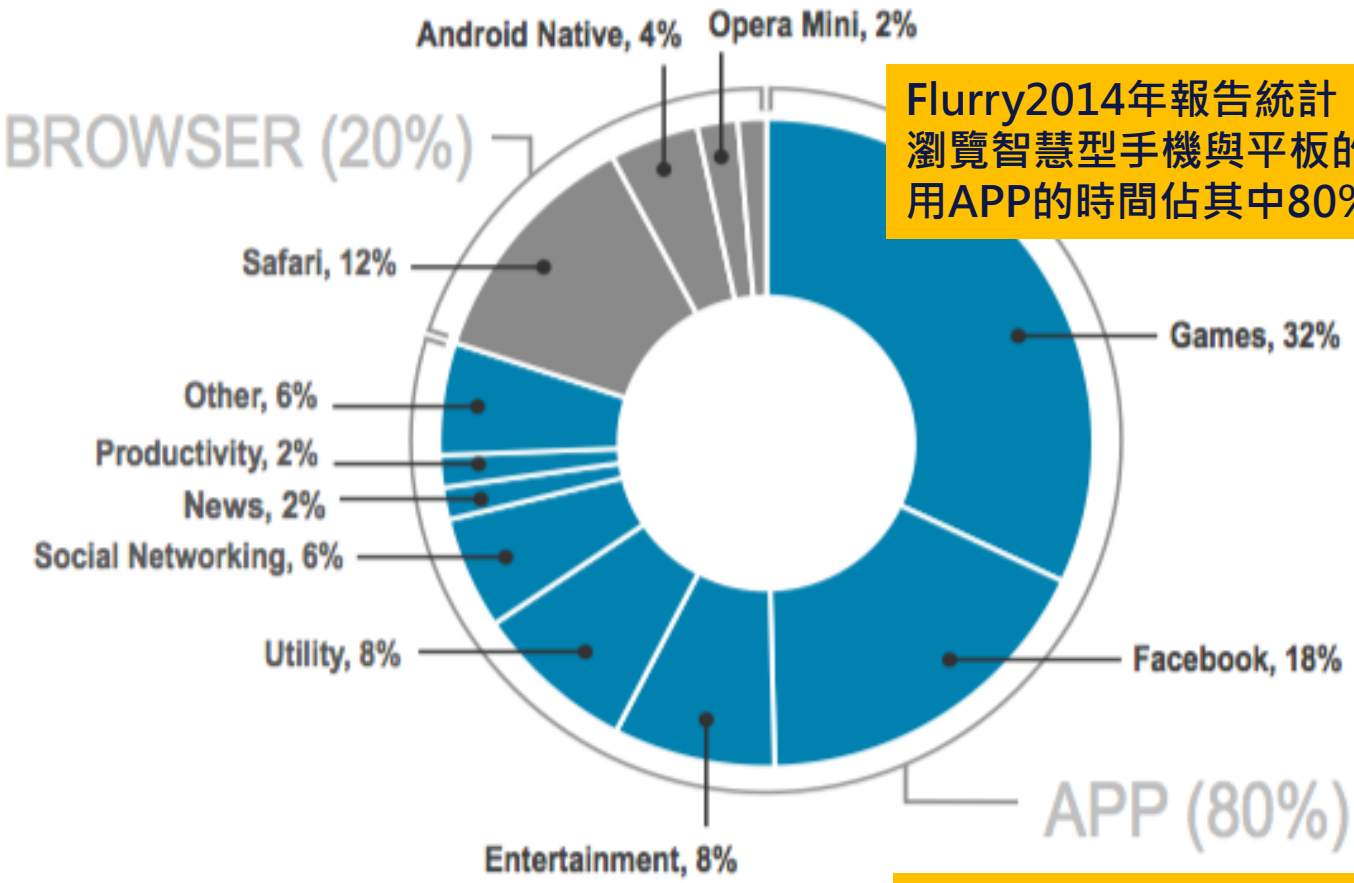
重要檔案存取前加入ACL、輸入驗證、輸出檢查

# 功能測試

# 功能測試

- 功能測試：測試人員以使用者角度，針對APP進行一般性功能操作，包含功能測試、使用者界面與使用者體驗等方面。
- 自動化測試：根據擬定之測試案例(Test Case)，撰寫測試腳本(Test Scripts)，以自動化方式執行測試腳本，進行功能測試和回歸測試，可快速完成APP測試。
- 測試工具：有許多商業化的測試工具，撰寫之測試腳本，可在各種行動裝置實施。

# APP應用全面進攻!



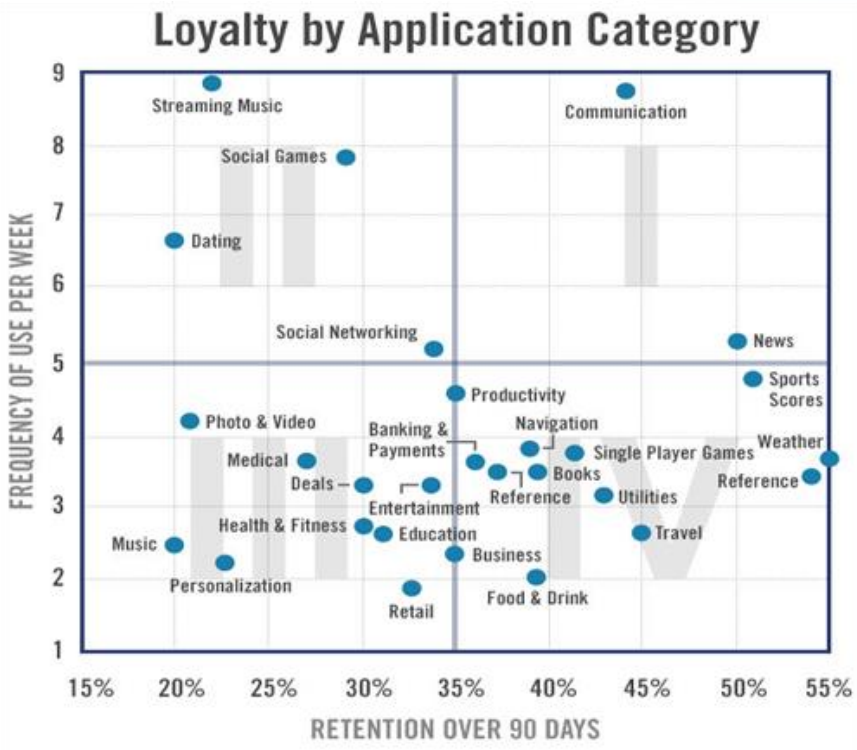

Flurry2014年報告統計，美國平均每人每日花費在瀏覽智慧型手機與平板的時間為2小時 38分鐘，使用APP的時間佔其中80%，使用瀏覽器佔其中20%

2015-08-28 獵豹移動雲平台統計發現，台灣人每天使用手機上網達197分鐘，位居全球第一，台灣人每日平均使用13.06個App。

# 行動APP測試的挑戰

中華電信 Chunghwa Telecom

- **複雜與多樣化的行動裝置與平台**
  - 不同的作業系統 (iOS、Android、Windows Phone)
  - 不同的OS版本 (iOS 5/6/7/8、Android 3.0/4.0/4.1…5.0)
  - 不同的裝置平台 (Pad/Phone)
  - 不同的螢幕像素大小 (VGA、SVGA、XGA、WUXGA…)
  - 不同的手機開發商和其各自不同的驅動程式
  - 不同的手機電信商
- **複雜與多樣化的APP種類**
  - 工具類
  - 遊戲類
- **多種異質性的無線網路環境**
  - WiFi
  - 3G
  - 4G/LTE

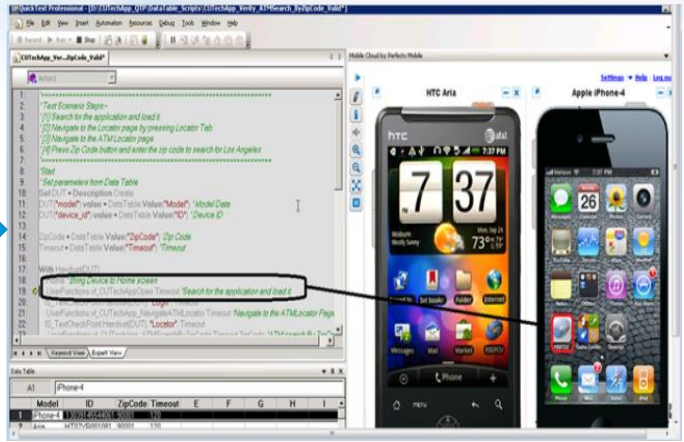


# 自動化測試的優點

- 功能測試可於開發階段同時並行處理，可早期獲得使用者回饋，增進APP軟體成熟度和加快軟體版本更新速度。
- 根據測試項目和結果報告中及早發現難以預期的程式Bug，可強化APP的Error和例外處理。
- 導入自動化功能測試，可有效縮短測試時程，同時減少人為操作的疏失。
- 透過腳本編輯、自動重播、結果檢查、報告輸出等操作，縮短回歸測試的時間，提升專案整體進度和品質。
- Robustness Test：單機執行多次後，測試是否有Resource Leak。

# APP自動化功能測試

Unified Functional Testing Mobile



Automated testing:

- Effective and efficient
- Repeatable
- Reusable
- Emulators and real devices

# 自動化APP測試情境

中華電信 Chunghwa Telecom

上傳 APP

測試報告

## 支援APP類型

Native APP | Hybrid APP | HTML5 APP | Browser APP

## APP測試案例

相容測試 | 功能測試 | 安全測試 | 效能測試

## 自動化測試工具

HP UFT | SeeTest | HP Fortify | LoadRunner

Mobile App Testing Platform

## 實機測試設備管理

Android

iOS

ALWAYS AHEAD 爲了

# 結語

- 導入國際標準與認證，發展軟體測試技術與平台，制定推動軟體品質標準與認證標章(Logo)，並成立具公信力之第三方公正機構，提供系統獨立驗證測試服務。
- 持續建立系統化、自動化及智慧化的測試技術，並提供資訊系統驗證測試服務，確保上線產品品質。
- 雲端運算、MobileAPP、資安測試是IT產業的重要發展趨勢，軟體測試與驗證技術須與時俱進，確保產品品質、縮短開發時程、降低開發門檻。

中華電信
Chunghwa Telecom

# 溝通人間情　連接世界心


*Thanks for your attention!*