金融聯合徵信中心
Joint Credit Information Center

# 金融徵信與資訊安全

鄭 祺 耀

111年 1月 18日

金融聯合徵信中心
Joint Credit Information Center

# 簡報大綱

壹、金融徵信簡介
貳、資訊網路系統
參、資訊安全防護
肆、資安人才需求

# 壹、聯徵業務簡介

金融聯合徵信中心
Joint Credit Information Center

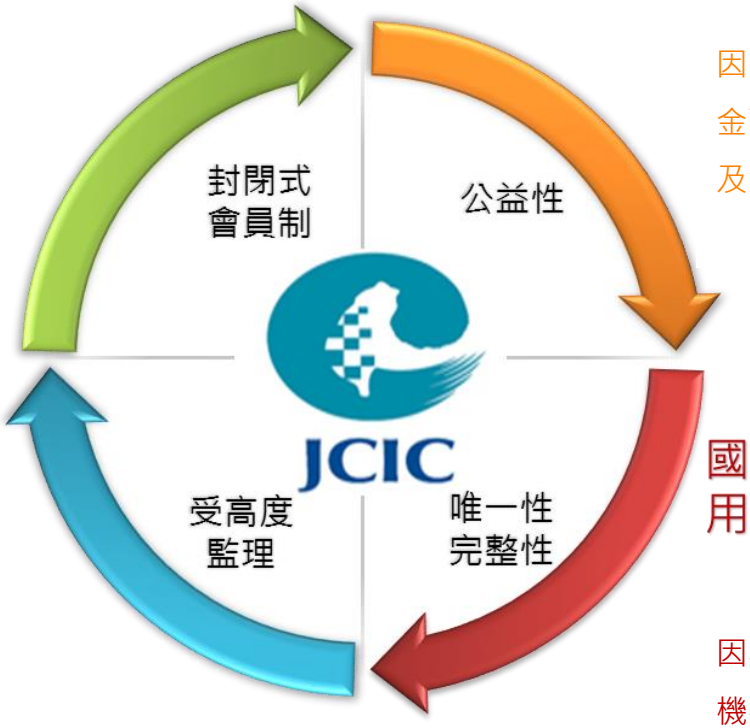
聯徵中心成立於1975年，依據銀行法第四十七條之三第二項、「銀行間徵信資料處理交換服務事業許可及管理辦法」及金融監督管理委員會主管政府捐助及經指定民間捐助財團法人監督管理辦法設立與營運。營業範圍為(一)金融機構間徵信資訊之蒐集、處理及利用;(二)其他經主管機關指定辦理與設立宗旨相關之事項。(營業執照)

## 成為會員之門檻極高

目前資料蒐集範圍主要是會員機構、政府及其他單位資料；是封閉式模式對於資料報送品質、會員查詢及資料的控管，具有積極正面效益。

## 非營利之財團法人組織

因屬非營利之財團法人，兼顧整體金融體系安全穩定的監理目的，以及滿足會員機構的業務營運需求。




## 受主管機關業務面、資安面的高度監理

完整蒐集金融機構信用資料，協助金融穩定、提供金融監理資訊，且受主管機關高度監理，因而受到會員機構的信賴。

## 國內唯一的跨金融機構間信用報告機構。完整蒐集個人與企業信用資料

因其唯一性與完整性，大幅降低會員機構信用資訊成本；惟因此特性，建立資訊安全與資料保護的高規格遵循標準。

# 壹、聯徵業務簡介


JCIC依據「銀行法」、「銀行間徵信資料處理交換服務事業許可及管理辦法」及「金融監督管理委員會主管政府捐助及經指定民間捐助財團法人監督管理辦法」設立與營運，並受金管會高度監理

對整體信用市場風險有效監控，並做為監理政策制訂之重要參考。


增加資訊透明度，提升信用可得性；透過信用報告的提供，提升社會大眾對信用的正確認知，進而審慎使用並珍惜信用。

於風險管理與業務拓展中取得平衡，依借款人之信用風險程度進行准駁，並決定適當之利率，提升信用決策的效率與品質。

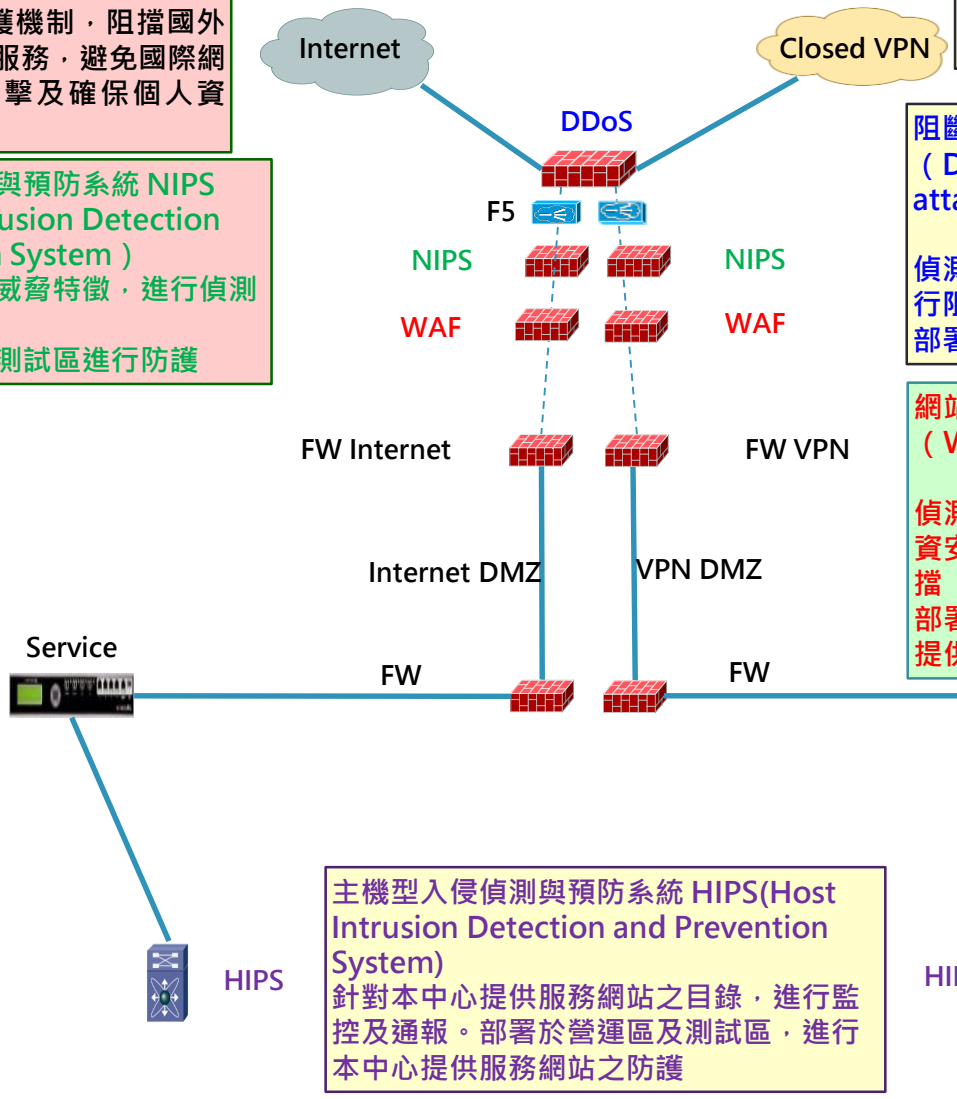
提升信用交易之安全、效率、市場紀律；促進產業、經濟發展。

# 貳、資訊網路系統-縱深防護

金融聯合徵信中心
Joint Credit Information Center

個人線上查閱服務設有DDos防護機制，阻擋國外IP連線之服務，避免國際網路駭客攻擊及確保個人資料安全。

網路型入侵偵測與預防系統 NIPS
（Network Intrusion Detection and Prevention System）
針對弱點與攻擊威脅特徵，進行偵測及阻擋
部署於營運區及測試區進行防護




透過中華電信提供之網路安全防護加值服務ACL(Access Control List)，客製化虛擬專屬網路，會員與會員間網路不能互通。

阻斷服務攻擊防禦設備 DDoS
（Distributed Denial-of-Service attack）

偵測阻斷服務之流量，並針對來源進行阻擋
部署於營運區及測試區進行防護

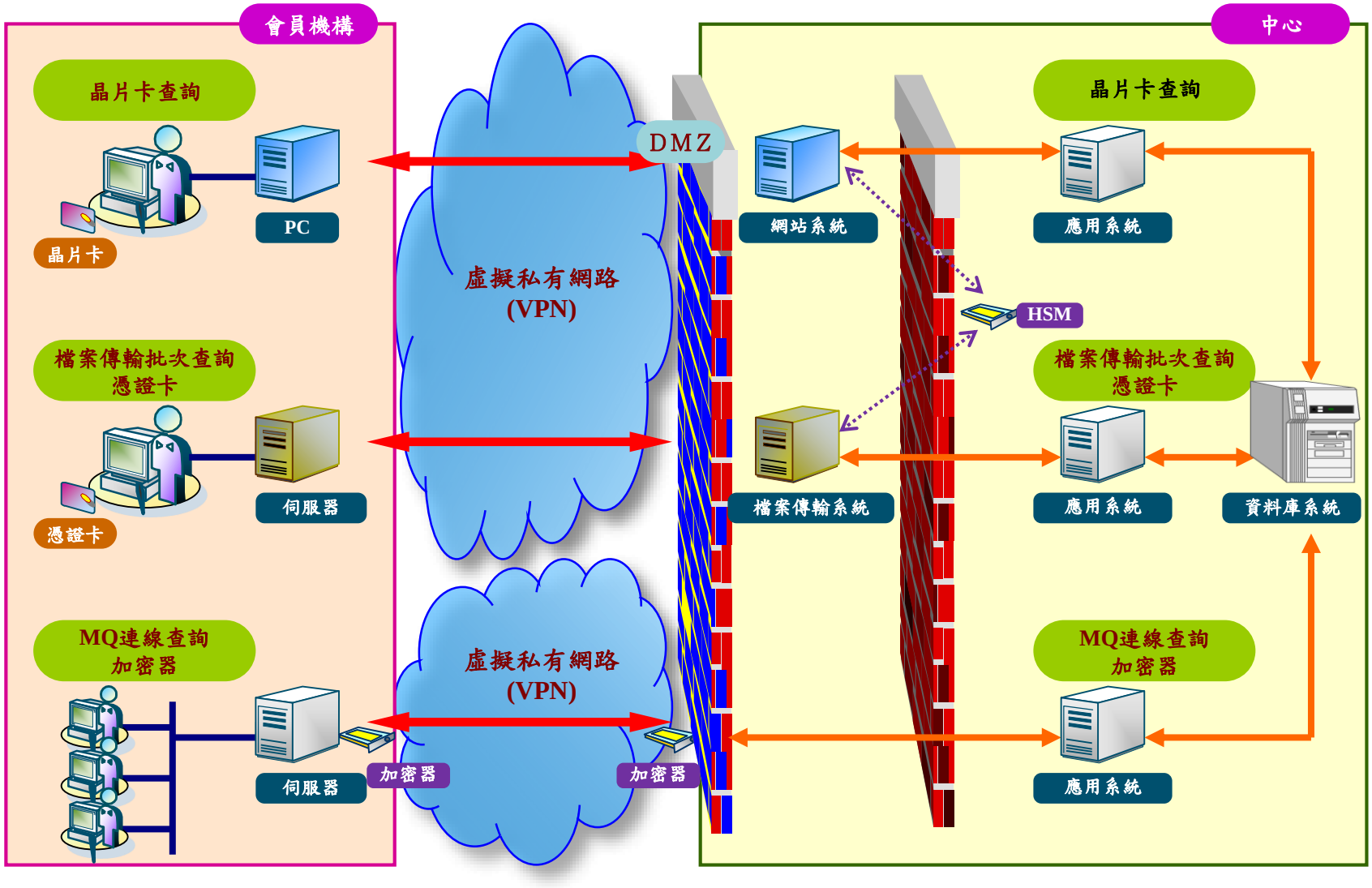
網站應用程式防火牆系統 WAF
（Web Application Firewall）

偵測網站傳輸之流量，針對惡意攻擊、資安威脅資料庫比對，進行偵測及阻擋
部署於營運區及測試區，進行本中心提供服務網站之防護

主機型入侵偵測與預防系統 HIPS(Host Intrusion Detection and Prevention System)
針對本中心提供服務網站之目錄，進行監控及通報。部署於營運區及測試區，進行本中心提供服務網站之防護

# 貳、資訊網路系統-會員間

金融聯合徵信中心
Joint Credit Information Center



# 參、資訊安全防護作業-政策與制度

金融聯合徵信中心
Joint Credit Information Center

**政策制度**

建立內部控制制度，持續辦理內部稽核作業及自行查核作業

104年4月16日金管資字第10400560831號函，列為「資安責任等級A級機構」

108年6月26日金管資字第1080193631號函，金管會非資通安全法納管機關(構)之資通安全責任等級

資訊安全管理制度驗證( ISO 27001)

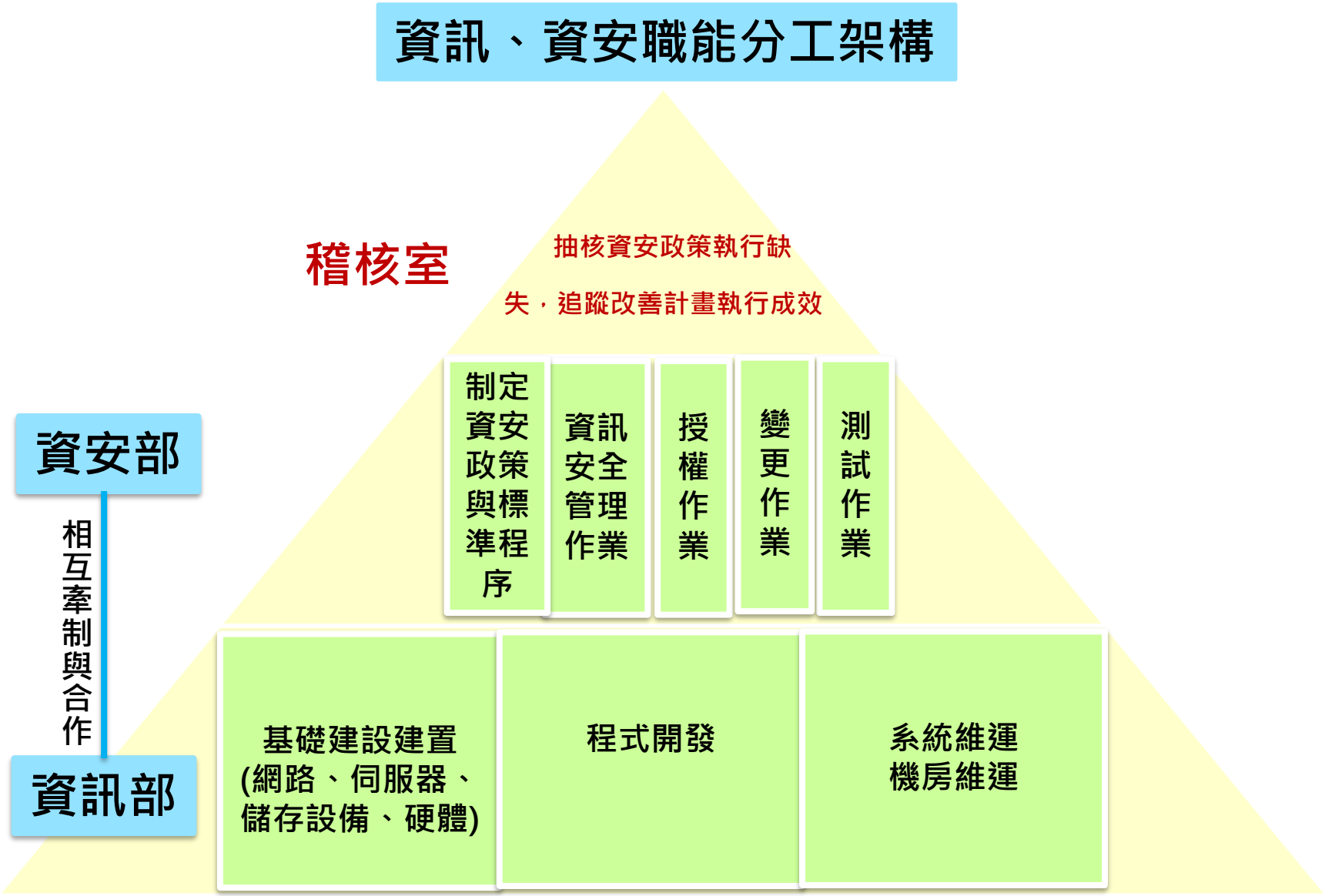
個人資料保護管理制度驗證(TPIPAS)

外部紅藍白實際攻防

# 參、資訊安全防護-人員組織

金融聯合徵信中心
Joint Credit Information Center

## 資訊、資安職能分工架構



# 參、資訊安全防護-實體安全管理及網路安全管理

金融聯合徵信中心 Joint Credit Information Center

| | 構面 | 項目內容 |
|---|---|---|
| 實體安全管理 | 終端機操作室 | 門禁管制、錄影監控、限制連線、無儲存及輸出設備之精簡型端末機(Thin Client) ，供授權、變更作業使用 |
| | 辦公區 | 精簡型端末機(Thin Client)連線營運環境作業 |
| | 環境 | 大樓24小時保全，各樓層設門禁、錄影監控、防火警報及消防系統 |
| | 人員 | 廠商人員、物品管控 |
| 網路安全管理 | 內部環境 | 實體隔離(營運區、OA測試區、管制區、終端機操作室)、電腦防毒系統(Anti Virus) 、 微軟更新服務系統(WSUS) 、設備管控系統：管制個人電腦之USB儲存及無線通訊傳輸裝置、電子郵件過濾、APT防禦系統及客製化放行系統、網站存取防禦系統(上網採取正面表列管制、阻擋可疑網站) |
| | 外部環境 | 入侵防禦系統(IPS)、網站應用程式防火牆系統(WAF)、電子郵件防護系統(SPAM)、DDoS防護系統 |
| | 資安監控系統 | 資安監控中心(SOC) |

# 參、資訊安全防護-網路安全管理_對外服務網路安全

金融聯合徵信中心
Joint Credit Information Center

網路安全管理(對外服務安全管理)

本中心對民眾之資料傳輸一律加密保護，資料傳輸於通訊層有TLS加密保護，並增加應用層以RSA機制將資料加密保護。

提供會員機構查詢及報送服務皆採封閉式專屬VPN網路架構，並於防火牆鎖定固定IP位址，查詢及報送之防護。

(1)晶片卡查詢及報送:使用者帳號之密碼輸入錯誤採自動鎖帳號，晶片卡密碼輸入錯誤3次即自動鎖卡，且以晶片卡金鑰將資料加密。強化會員端查詢結果安控機制，查詢結果無法儲存或使用PrintScreen按鍵功能印出，以降低資訊洩漏之風險。

(2)加密檔案傳輸查詢及報送:專屬資料傳輸及資料加密軟體，並以FXML電子憑證(晶片卡)對傳輸檔案加密及簽章，資料傳輸以RSA機制將資料加密保護。

(3)伺服器連線查詢:使用專屬硬體加密器，資料傳輸以RSA機制將資料加密保護。

# 參、資訊安全防護-網路安全管理_對外服務網路安全

金融聯合徵信中心
Joint Credit Information Center

網路安全管理_對外服務安全管理

提供民眾之個人線上查閱信用報告服務之防護

當事人須使用自然人憑證晶片卡，輸入身分證ID、自然人憑證晶片卡密碼及圖形驗證碼，並須經內政部自然人憑證用戶身分確認服務系統驗證，自然人憑證有效且驗證通過後才會成功登入。當事人送出申請交易資料即回覆之信用報告須用自然人憑證之RSA公鑰加密，開啟信用報告亦須用自然人憑證之RSA私鑰解密。

因採網際網路連線，已與業者(中華電信、台灣固網)簽約提供DDoS防護及阻擋國外(如:中國大陸、美國) IP連線之服務，另本中心網路設備亦設定阻擋國外IP連線，以防護網際網路DDoS之駭客攻擊。

# 參、資訊安全防護-主機系統管理及應用系統管理

金融聯合徵信中心
Joint Credit Information Center

**主機系統管理**

- OA測試區病毒碼更新、系統漏洞修補。
- 營運區伺服器病毒碼(手動更新)
- 營運區伺服器漏洞修補(配合弱掃作業，手動)
- 系統安全參數設定
- 新系統設備上線前(系統、網站弱掃)
- 全面性系統、網站弱掃(半年)

**應用系統管理**

- 版本管理
- 測試管理
- 源碼檢測
- 變更管理
- 軌跡保留

# 參、資訊安全防護-作業程序

金融聯合徵信中心
Joint Credit Information Center

作業程序

- 工作手冊
- 授權管制
- 變更管制
- 輸出入管制
- 事件管理
- 營運持續

# 參、資訊安全防護-作業程序_帳號權限管理

金融聯合徵信中心
Joint Credit Information Center

**作業程序-帳號權限管理**

帳號權限管理以最小必需為原則，依職務區分不同群組並訂定營運系統使用者權限一覽表，定期執行帳號及權限盤點。

建置帳號權限申請管理系統，留存帳號權限申請、審核及執行等紀錄。

最高權限、緊急、變更等帳號須經奉核才予授權，使用完後立即回收，並每日監控是否有不當使用情事。

建置RBAC權限管理系統，管控UNIX營運主機帳號權限(指令權限、登錄來源IP、檔案權限)。

建置網域控制站(AD)，以群組管理原則統合控管網域中之WINDOWS伺服器及使用者。

# 參、資訊安全防護-作業程序_變更管理作業

金融聯合徵信中心
Joint Credit Information Center

**作業程序 變更管理作業**

- 建置變更申請管理系統，變更作業必須依表單流程執行。
- 系統、程式需要變更，申請人應檢附變更程序、復原程序、檢核程序申請變更
- 經審核後由變更人員執行變更作業，變更權限臨時由授權人員賦予，完成後回收權限。
- 變更協調員。上線檢核表。
- 留存變更過程（含授權與執行）之軌跡紀錄。製管理性分析報表，定期監控統計及檢討。

# 參、資訊安全防護-作業程序_資料輸出入作業

金融聯合徵信中心
Joint Credit Information Center

作業程序 資料輸出入作業

營運區資料若有輸出需求，必須依資料等級經權責主管核准後，由變更人員依資料等級加密後輸出。

含有個人資料之檔案禁止輸出至本中心OA測試區，如需輸出至外部單位，經申請奉核後，由變更人員依資料等級加密後輸出至管制區，再由專屬電子郵件系統，直接傳送至外部收件單位 (以正面表列管控外部收件單位)

資料輸入：多重防毒暨檔案清洗系統。

資料輸出：個資掃瞄。

每日監控輸出入管理系統運作及資料是否有未經奉核輸出之情形。留存輸出過程之軌跡紀錄。

# 參、資訊安全防護-作業程序_事件管理及營運持續

金融聯合徵信中心
Joint Credit Information Center

**事件通報**

法源依據:

-資通安全法之「資通安全事件通報及應變辦法」

-金融監督管理委員會之「銀行業通報重大偶發事件之範圍與適用對象」

訂定事件通報暨處理作業，依影響標的範圍及服務中斷時間，定義事件等級及通報對象。

**營運持續**

同地備援機制、異地備援機制

# 參、資訊安全防護-作業程序_委外管理

金融聯合徵信中心
Joint Credit Information Center

**委外管理**

- 委外廠商資格推選、評估及評鑑委外作業之執行績效。
- 保密合約、保密承諾書、軟體安全承諾書。
- 資訊安全與個資相關查核作業。
- 測試、源碼檢測、弱掃、滲透測試。

# 肆、資安人才需求

金融聯合徵信中心
Joint Credit Information Center

- 資訊安全管理系統(如主稽核員)
- 網路安全防護
- 資料保護與安全管理系統
- 權限管理(識別與存取管理)
- 應用程式安全工程師
- 資安威脅分析管理師(資安監控)
- 弱點風險分析
- 事件應變管理

# 謝謝聆聽