公務資料威脅與防護

國家資通安全會報 技術服務中心
應中龍 黃博禮

Mar. 20, 2009

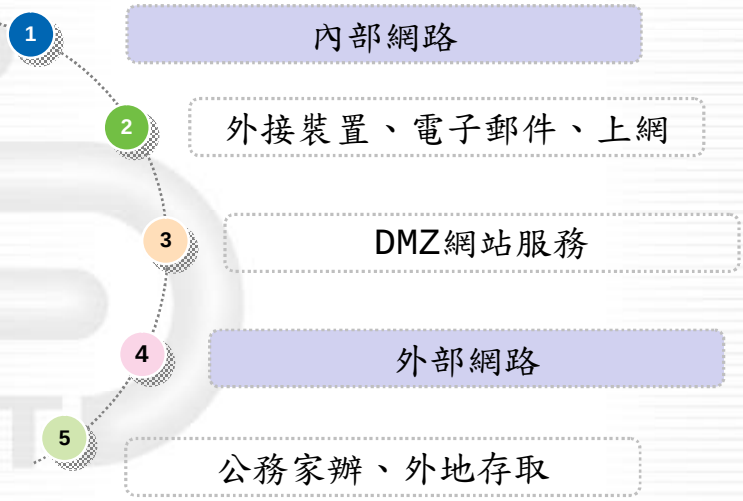
大綱

1. 3個安全邊界
2. 攻擊手法Demo與防護對策
3. 竊取資料的犯罪集團
4. 文件生命週期
5. 建議防護方案

清晨的森林

盜伐過程很難發現

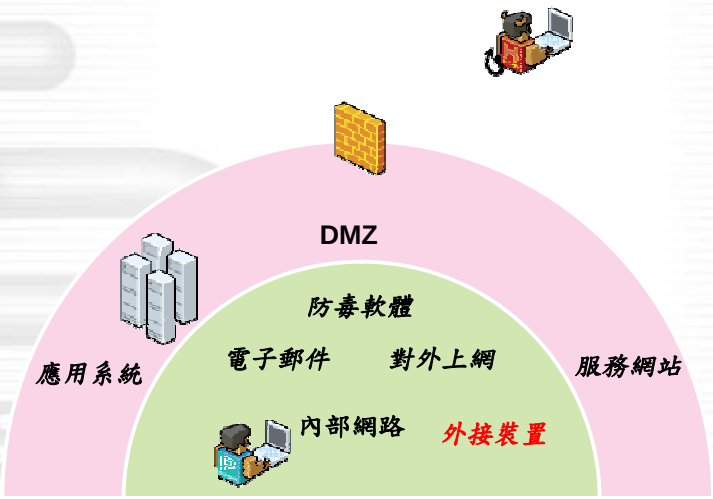
3個安全邊界



內部網路基本存取需求？

- 對外上網
- 電子郵件
- 外接裝置：USB、外接硬碟、手機
- 應用系統：公文系統、服務網站

MIS面對的簡化防護邏輯



USB Worm Demo

外接裝置的防護對策

- 安全政策：使用與否、公務家辦、資料複製
- 防護目標：禁止自動播放、防止惡意程式
- 基礎防護方案：登錄檔關閉限制自動播放功能
- 進階防護方案：
  - 端點防護軟體
  - 評估考量

電子郵件的威脅

- 垃圾郵件、附件挾帶惡意程式
- AntiSPAM
- 社交工程釣魚信件
- 圖形化垃圾郵件
- 貝式演算法失效
- 社交工程演練

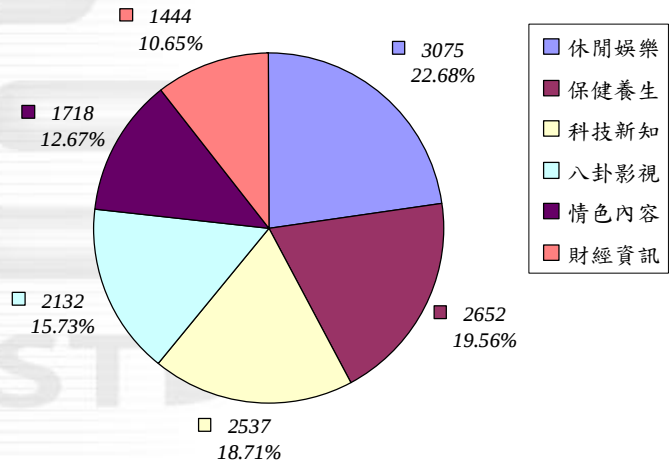
資安攻防演練電子郵件社交工程

項目	受測人數	記錄人數	人數比
開啓郵件	28,962	6,592	22.76%
點閱連結	28,962	3,712	12.82%

機密等級: C

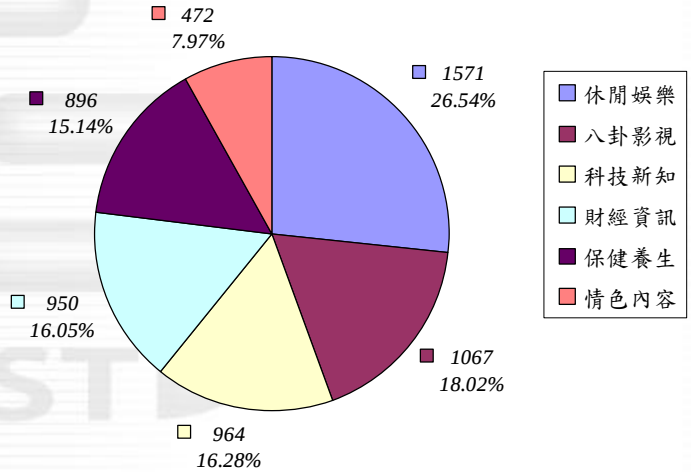
資安攻防演練電子郵件社交工程

Ÿ 社交工程郵件類型開啟比例

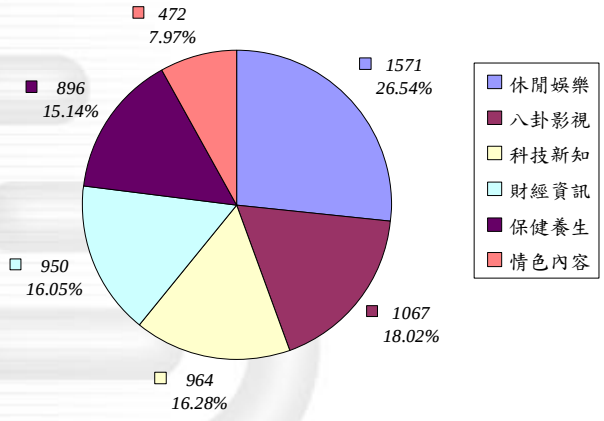


資安攻防演練電子郵件社交工程

- 社交工程郵件類型點閱比例

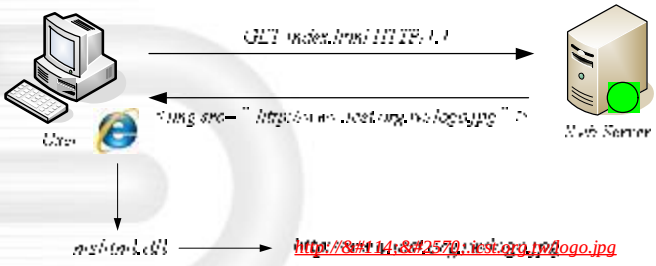


社交工程的省思



- 教育訓練才能加強辨識能力與警覺心
- 用戶端才是真正的入侵目標！

IE7 漏洞 demo

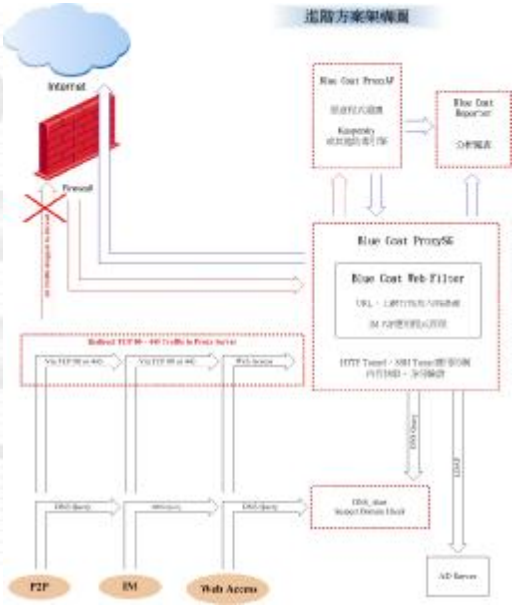

GET /index.html HTTP/1.1
<img src=" http://www.test.org/logo.jpg " >
User
Web Server
mshtml.dll
http://www.test.org/logo.jpg


Target

對外上網的防護對策

- 技服中心 DNS Alert 警示系統
- 內容過濾機制
- 研考會建置GSN骨幹內容過濾防護機制
- 專線與安全政策考量，可考慮自建過濾機制

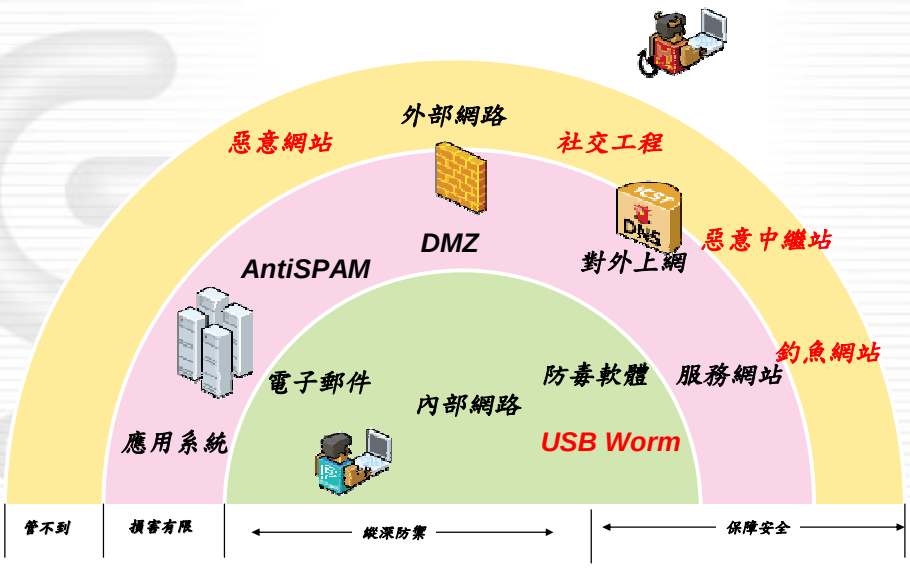
對外防護上網示意圖



3個安全邊界

1. 內部網路
2. 外接裝置、電子郵件、上網
3. DMZ網站服務
4. 外部網路
5. 公務家辦、外地存取

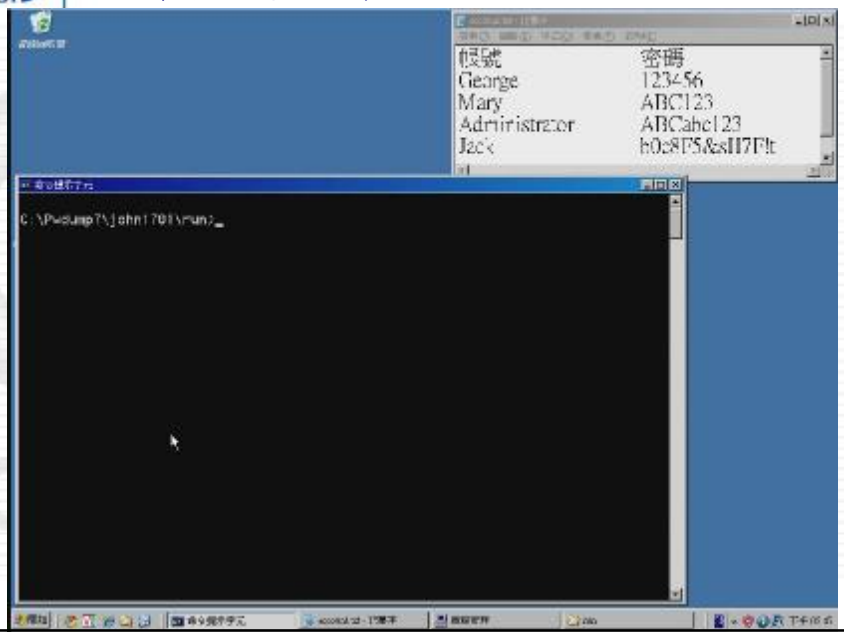
安全邊界:DMZ也是內部網路



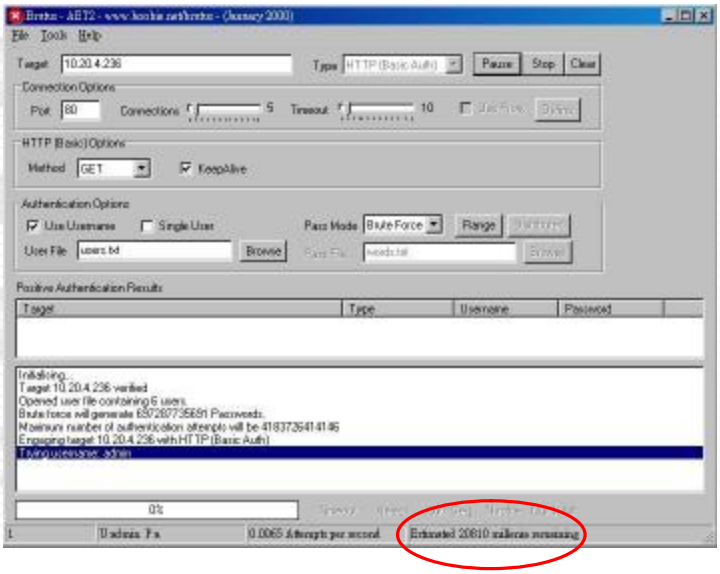
暴力破解密碼 Demo

- Local password cracker
- Remote brute force password

破解密碼檔案



遠端破解密碼



網站服務的防護考量

- 安全設定：目錄權限、錯誤訊息關閉
- 輸入驗證：
  - 輸入字元程式檢查不足，SQL injection的防護
  - 強化政府機敏資料防護及Web AP安全品質
- 系統更新：作業系統、應用系統、網路設備
- 身份驗證：
  - 最基本重要
  - One Time Password、自然人憑證、Smard Card

過度揭露安全資訊

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup**, **Common Administrative Tasks**, and **About Custom Error Messages**.

程式碼、帳號、資料庫版本洩漏

Server Error in '/' Application.

Configuration Error

Description:

Parser Error Message:

Source Error:

```
Line 3:          <system.web>
Line 4:              <identity impersonate="true" userName="dwIS user" password="Fa|sJCt|Ur3"/>
Line 6:              Set compilation debug="true" to enable ASPX debugging.  Otherwise, setting this value to
```

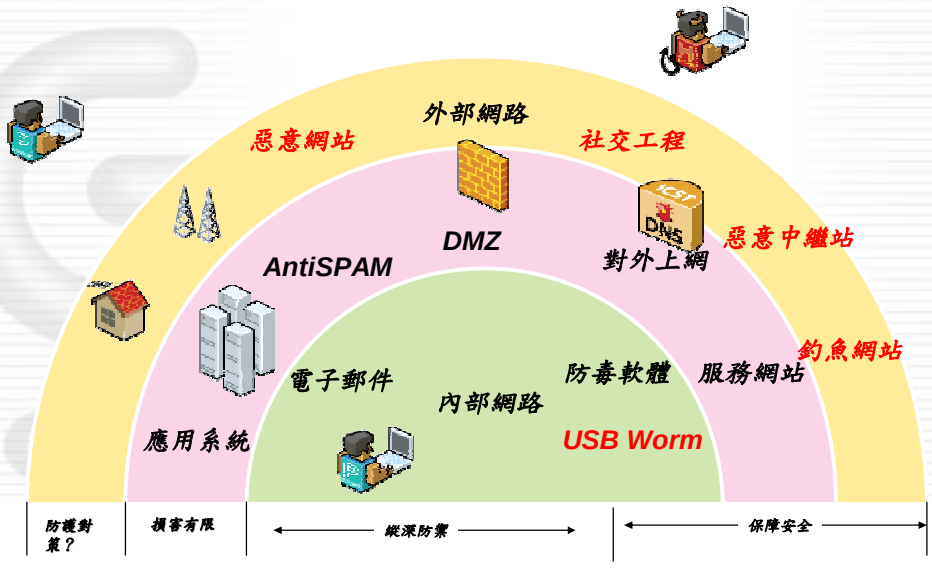
Source File: **Line:**

Version Information:

3個安全邊界

1. 內部網路
2. 電子郵件、上網
3. DMZ網站服務
4. **外部網路**
5. 公務家辦、外地存取

安全邊界:外部與內部網路

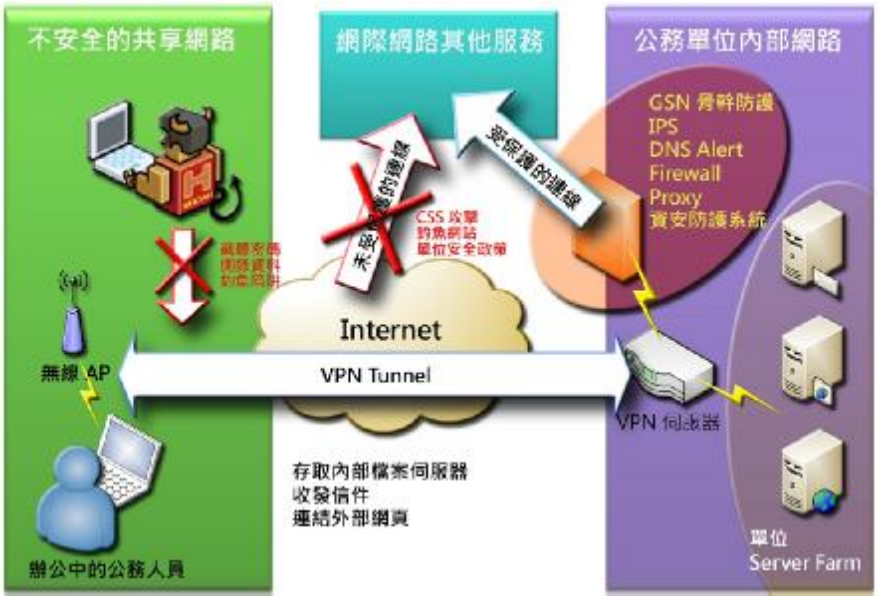


外部網路的威脅

- 公務家辦
  - 家中電腦沒有足夠的防護措施
  - 多人共用提高後門程式入侵機率
  - 存取授權的考量
- 外地存取
  - 連線竊聽
  - 公用電腦

ARP Spoofing demo

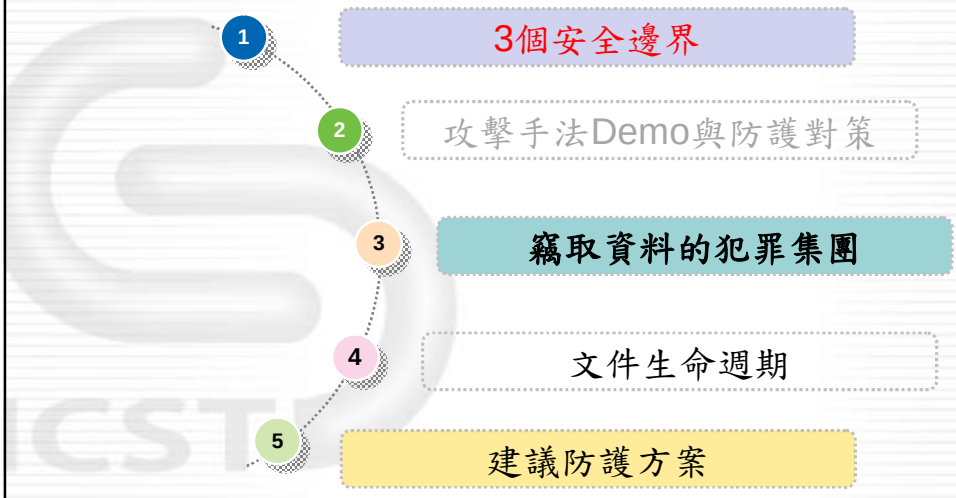
VPN Secure Zone



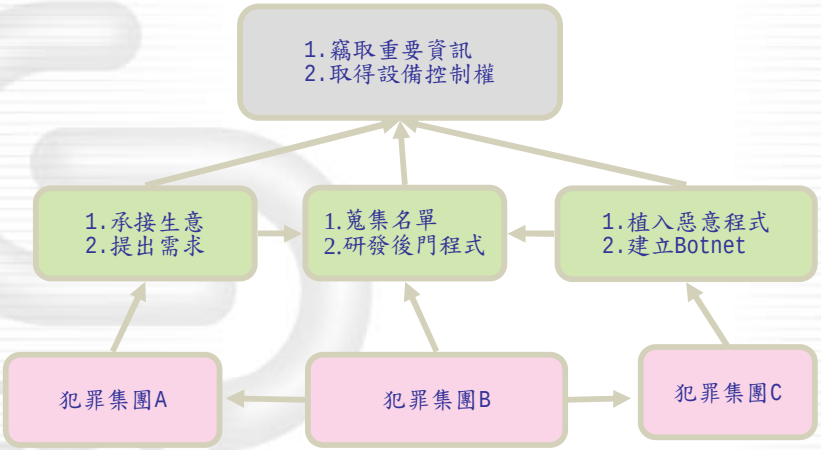
外地存取與公務家辦

威脅	防護方案		執行考量	安全政策
	基礎防護	進階防護		
資料遭未授權存取	檔案加密	*DRM*、*VPN* 虛擬桌面	密碼強度不足	密碼安全性政策
惡意程式竊取資訊	防毒軟體	虛擬桌面 *Host Check*	特徵碼無定期更新	公務用電腦安全政策
釣魚與惡意網站	瀏覽器禁用 *Script*、微軟釣魚網站防護	*VPN*、*URL*過濾設備	使用者對社交工程教育不足	強化使用者資安教育
連線傳輸竊聽	*SSL*加密、強化密碼	*VPN*、*OTP*	連線目的端無法限制	公務用傳輸加密規定

威脅來自何方？



竊取資料的犯罪集團



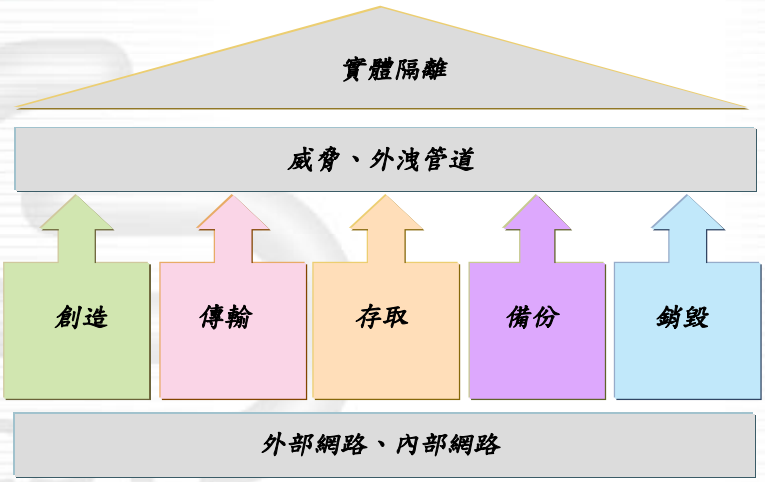
防護者的宿命

- 史記·淮陰侯列傳：智者千慮，必有一失。
- 攻擊與防守的不同，在於攻擊者僅需找到一失，而各位是需要千慮的防守者，且被期許不容一失。
- 防護比入侵要偉大！

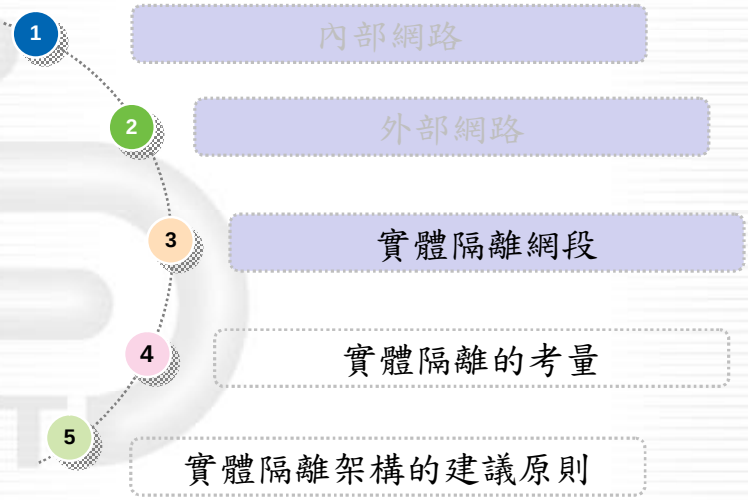
如何思考周全的威脅防護？

1. 3個安全邊界
2. 攻擊手法Demo與防護對策
3. 竊取資料的犯罪集團
4. 文件生命週期
5. 建議防護方案

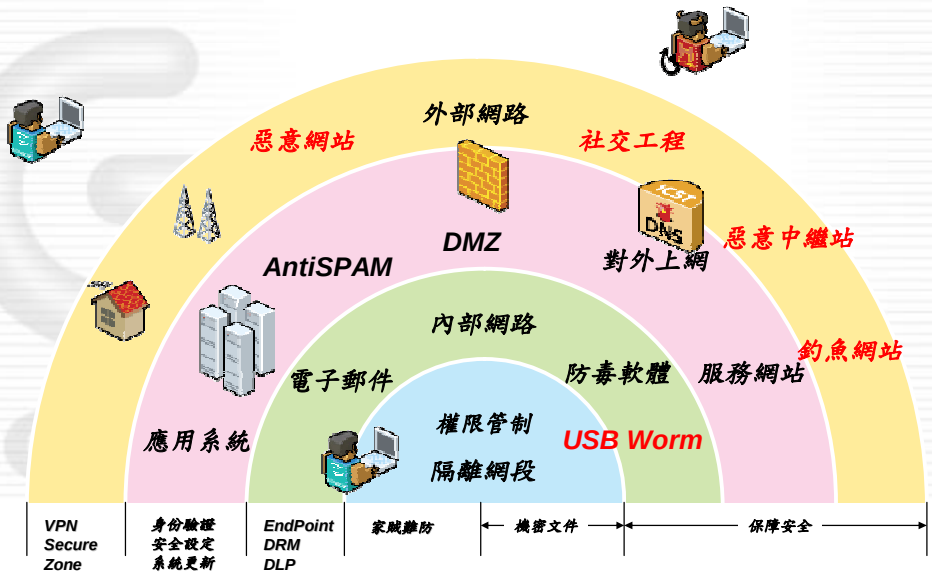
文件生命週期



3個安全邊界



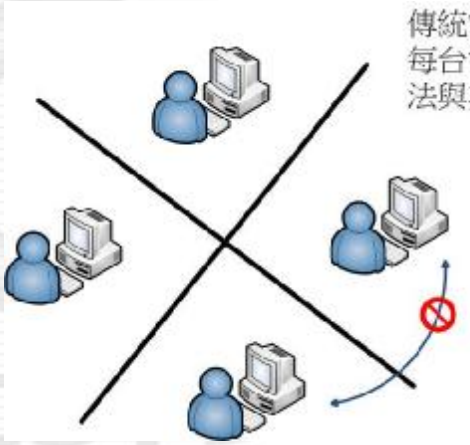
實體隔離



實體隔離的考量

- 建置經驗
  - 單機雙網
  - 雙機作業、雙機雙網
  - 資料過濾架構
  - 虛擬系統網路
- 過去的經驗
  - 便利性
  - 落實性
  - 資訊孤島

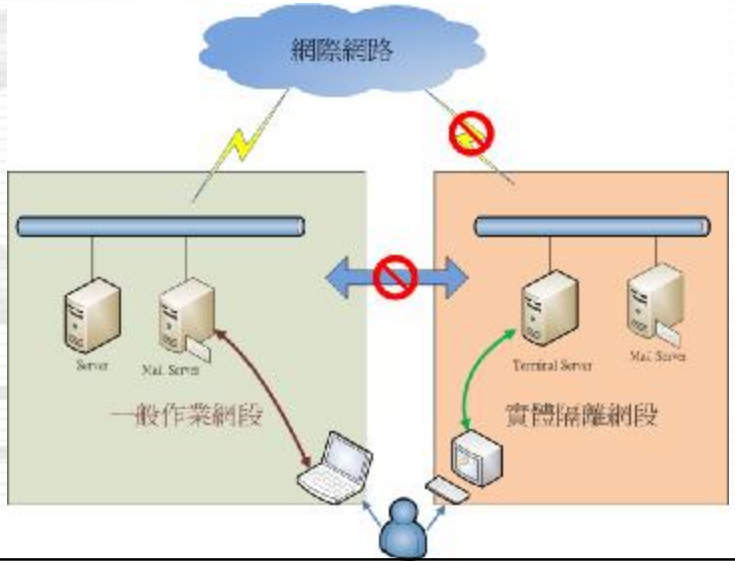
資訊孤島



傳統實體隔離方式：
每台電腦單獨隔離，無法與其他人員交換資訊

雙機雙網

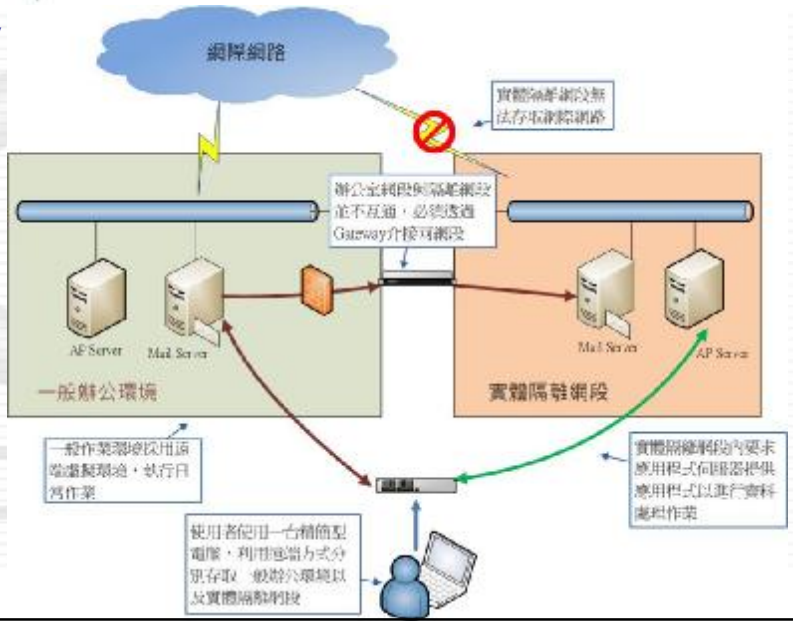
- 無法資料交換的隔離應用網路架構



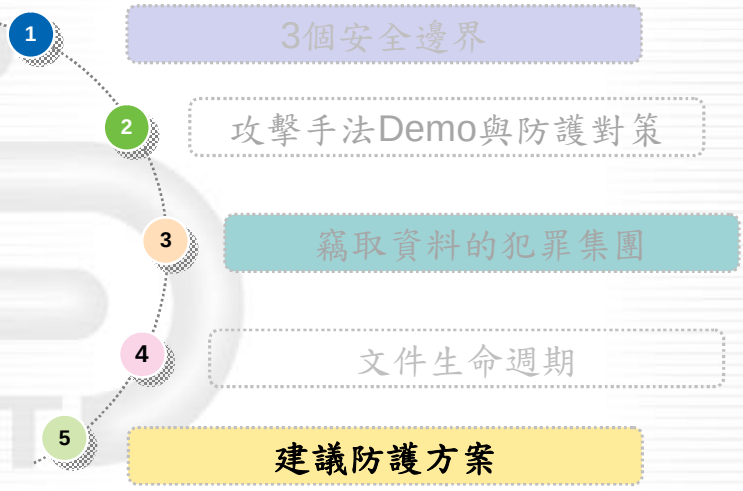
實體隔離架構的建議原則

- 具備資料交換
- 隔離網路連線架構
- 內部網路禁止文件編輯
- 用戶端精簡化
- 存取記錄稽核

實體隔離導入的示意圖



3個安全邊界的防護建議



歸納防護方案

安全邊界	威脅或問題	防護方案
外部網路	缺乏防護的用戶端 不安全的連線傳輸	端點防護 VPN Secure Zone
內部網路	外接裝置、對外上網 身分驗證、電子郵件	端點防護、內容過濾 OTP、教育訓練 數位版權管理
隔離網段	便利性 落實性 資訊孤島	5項原則

結論

防護目標

1.無意的資料外洩
2.人員訓練不足
3.外在惡意的入侵

建議防護方向

1.人員教育訓練
2.數位版權管理
3.身分驗證強化
4.端點防護強化

敬請指教