全面啓動
個資保護任務

敦陽科技資安顧問　楊伯瀚

資安人員的生存心法

個資從哪外洩？

由外而內的網路控制

由內而外的網路控制

問題與討論


資安人員的生存心法

在一個資安研討會…

新版個資法說個資就是…

個人的姓名
出生年月日
身分證統一編號
護照號碼
特徵
指紋
婚姻
家庭
教育
職業

病歷
醫療
基因
性生活
健康檢查
犯罪前科
聯絡方式
財務情況
社會活動

可直接或間接識別人的資料

個資外洩誰之錯？

個資是誰外洩的？

漫不經心的**使用者**

所以誰要負責？

老闆說：當然是**資安官**

What？What？ Why？

這就是**人生**啊，孩子！

資安人員悲歌

什麼是資安**CIA**三原則？

嘻嘻，說起來重要

哀哀，做起來次要

誒誒，忙起來不要

翻譯：

沒事你別來鬧

有事你來負責

Stark Technology Inc.
敦陽科技股份有限公司

資安人員的三角不平衡

安全
Security

效能
Performance

便利
Convenient

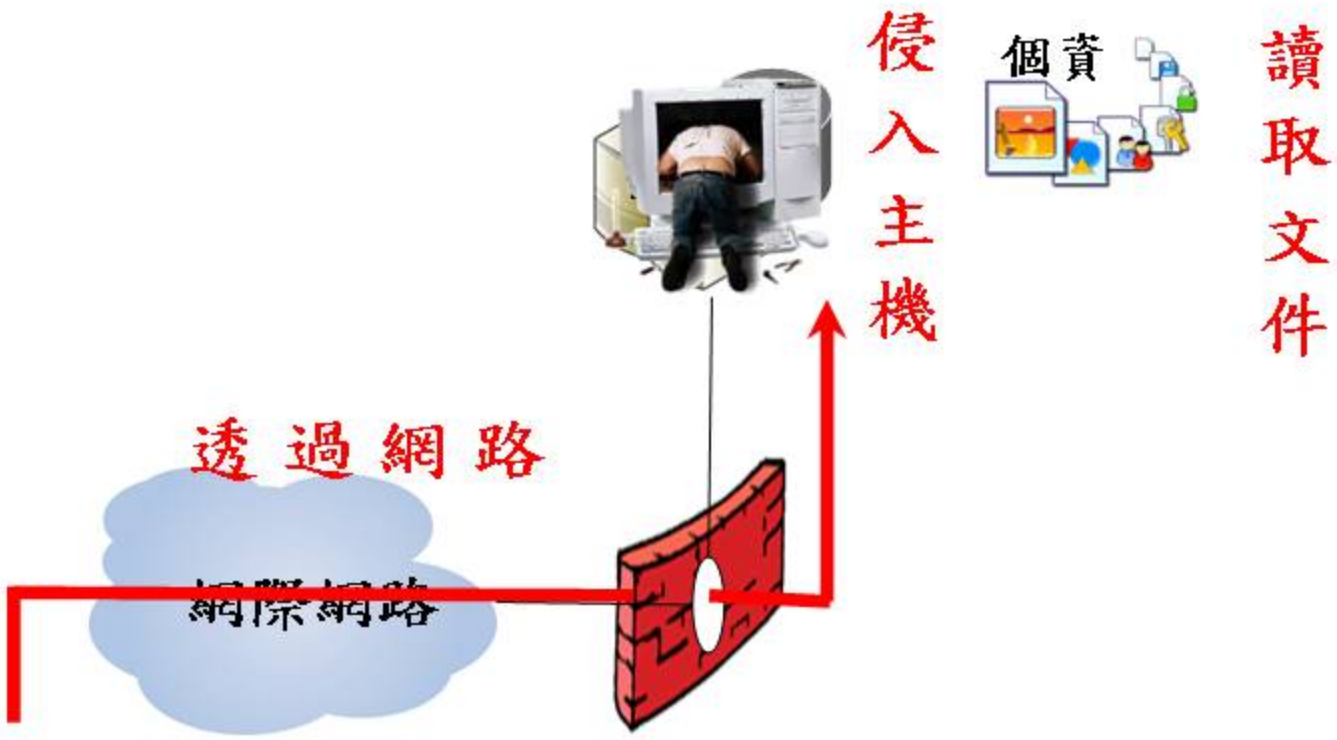
管理/實作能力
Administration

成本
Cost

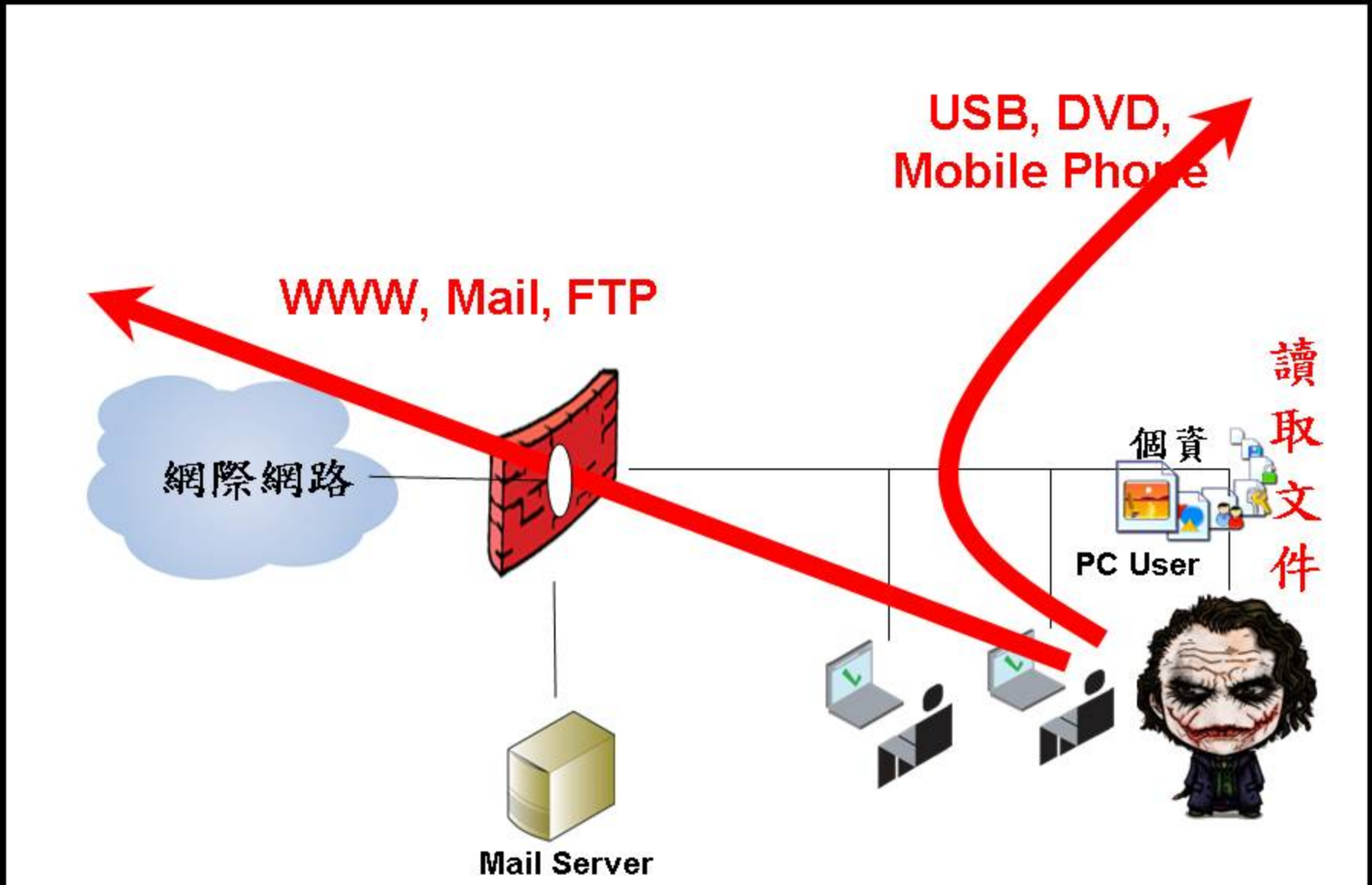
Stark Technology Inc.
敦陽科技股份有限公司


外洩？
在哪？
個資從哪外洩？

入則有敵國外患



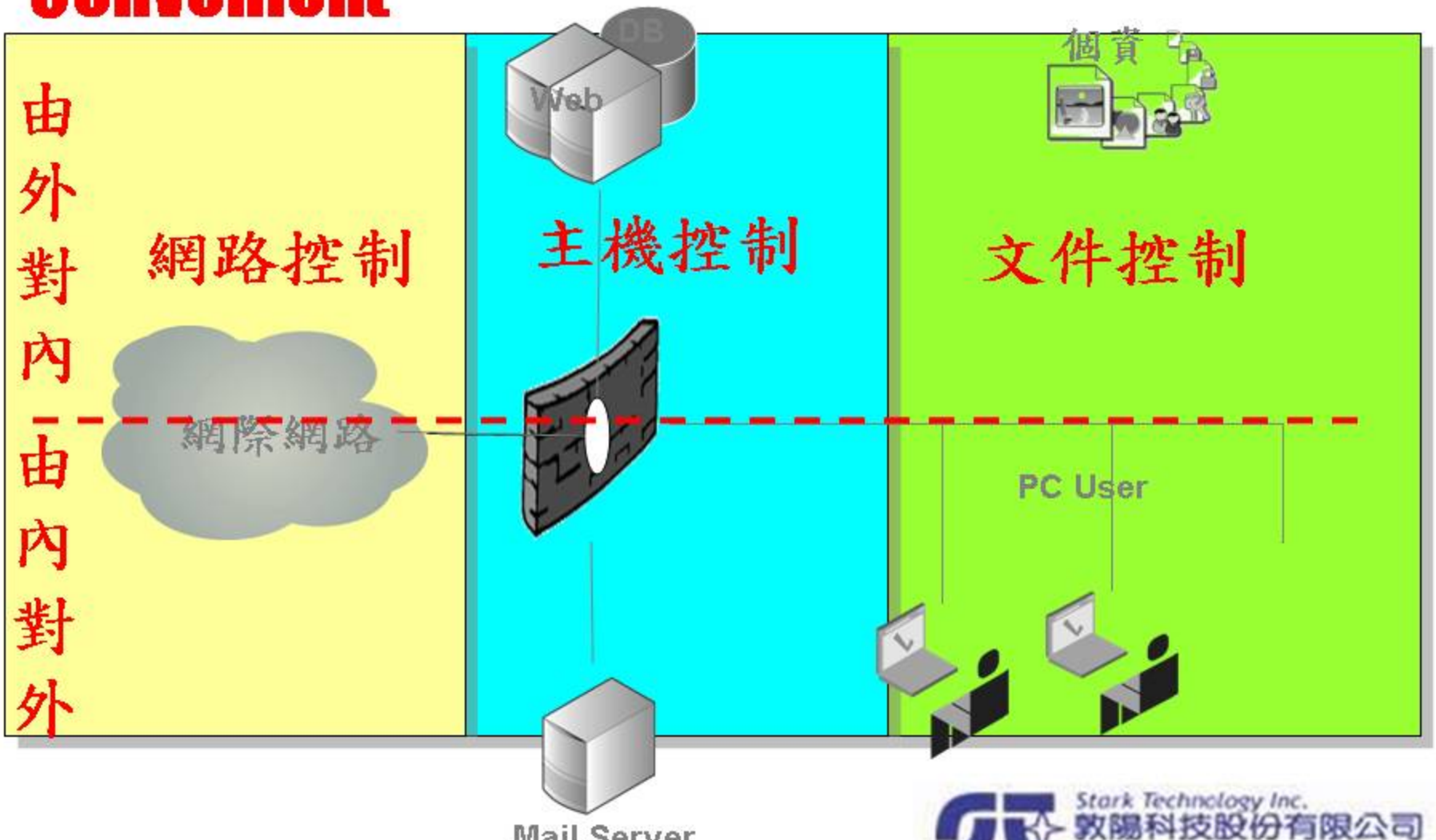
出則無法家拂士


USB, DVD,
Mobile Phone
WWW, Mail, FTP
讀取文件
網際網路
個資
PC User
Mail Server

個資防洩

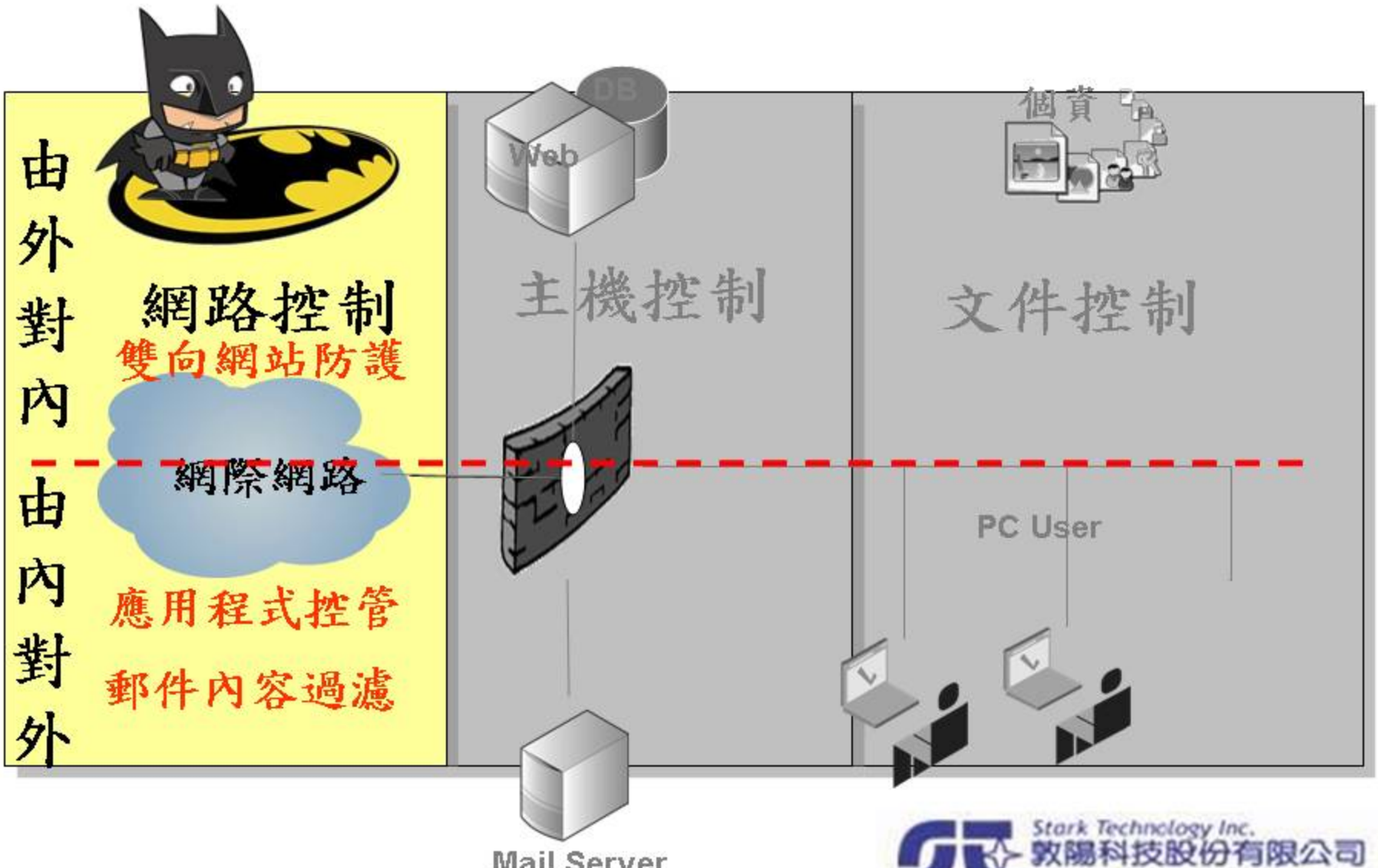
便利 ⟷ 不便

Convenient



Stark Technology Inc.
敦陽科技股份有限公司

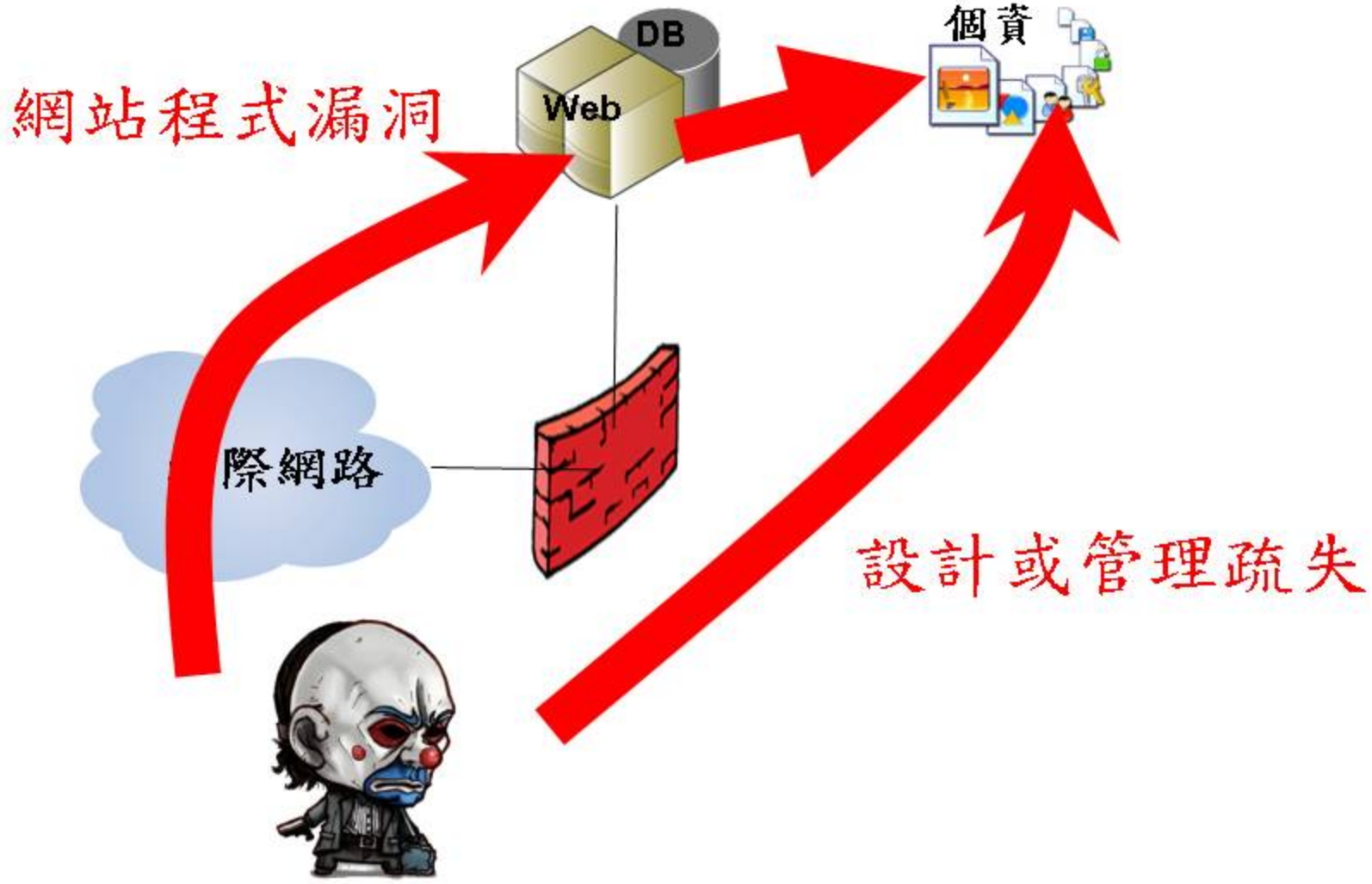
負擔最小的網路控制



Stark Technology Inc.
敦陽科技股份有限公司


天外飛来
不速之客

網站洩露個資



完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

雙向網站防護

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

高階應用層交付暨安全系統

網站防火牆

Stark Technology Inc.
敦陽科技股份有限公司

滲透測試

由專家人力進行

- 模擬駭客思維
- 應用駭客技術
- 嘗試取得機密資料
- 不具駭客破壞行為

發掘

- 網站程式漏洞
- 網站設計或管理疏失

WAF實作案例：

以Citrix Netscaler Application Firewall爲例

補強設計與管理疏失

首頁.htm

新聞頁.htm

訂閱新聞.asp

今日新聞.asp

會員登入.php

下單交易.php

個人資料.doc

會員測試.bak

研討會名單.xls

後台管理.asp

WAF正面表向白名單

首頁.htm

新聞頁.htm

訂閱新聞.asp

今日新聞.asp

會員登入.php

下單交易.php

個人資料.doc

會員測試.bak

研討會名單.xls

後台管理.asp

程式設計師
不小心放上的
檔案與個資


首頁.htm
沒有登入系統
員工資料.doc
交易記錄.log
信用卡號.xls
自拍影片.mpg
強制
登入
驗證
Citrix WAF驗證 或 AD驗證
Stark Technology Inc.
敦陽科技股份有限公司

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

高階應用層交付暨安全系統

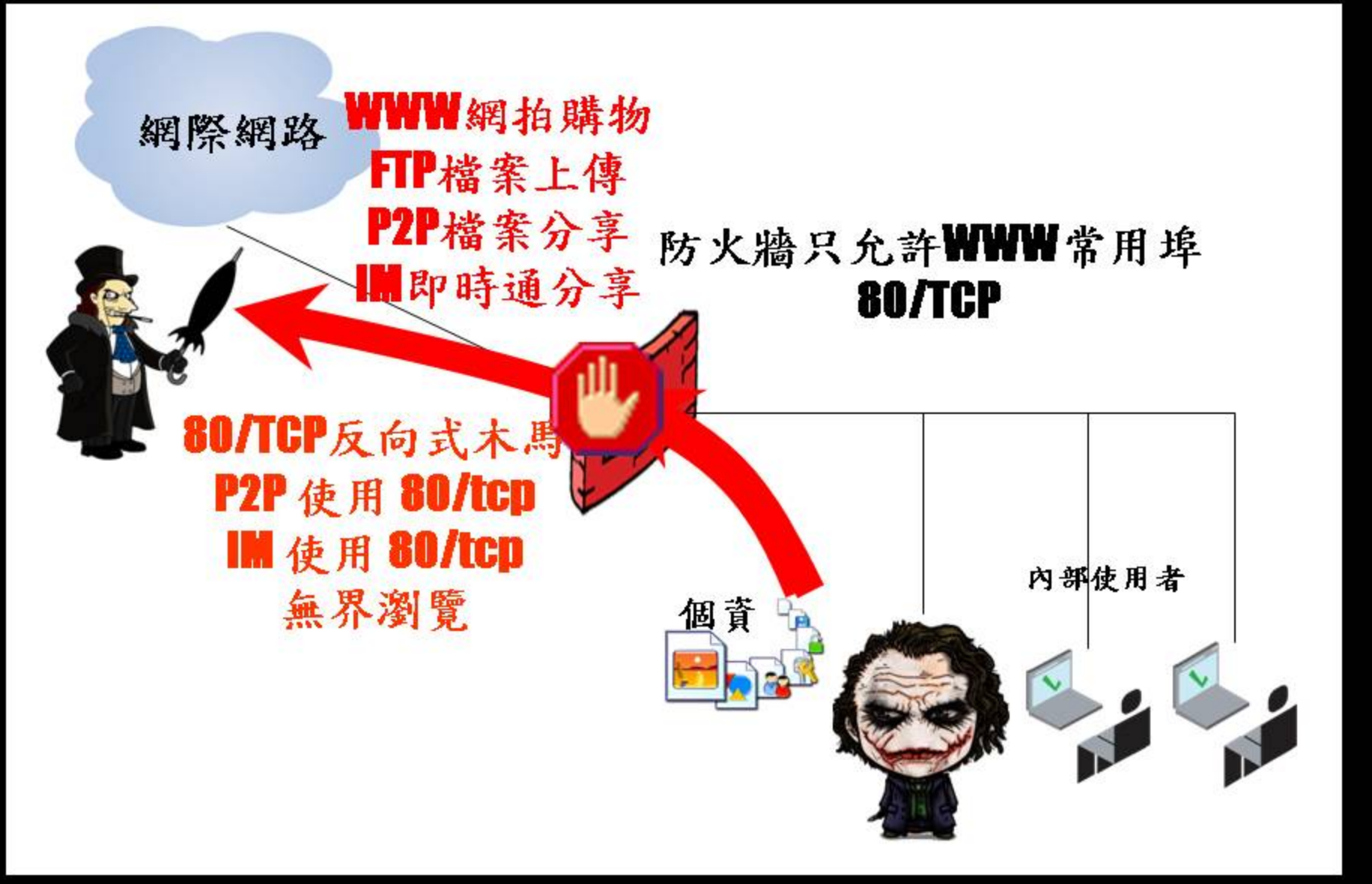
Citrix NetScaler WAF

Stark Technology Inc.
敦陽科技股份有限公司

家裏養小鬼

事事都搞鬼

內鬼洩露個資


網際網路
WWW網拍購物
FTP檔案上傳
P2P檔案分享
IM即時通分享
防火牆只允許WWW常用埠
80/TCP
80/TCP反向式木馬
P2P 使用 80/tcp
IM 使用 80/tcp
無界瀏覽
個資
內部使用者

完整資安服務框架

安全政策

資安稽核

安全計畫暨應變處理

人員安全 | 資料安全

應用程式安全

系統安全 | 網路安全

實體安全

應用程式控管

敦陽資安專業服務

滲透測試服務
網路弱點稽核服務
資安紀錄分析服務
資安教育訓練服務
安管中心建置服務
緊急應變服務
社交工程演練服務
資安顧問服務

多功能應用層安全閘道系統

次世代應用程式防火牆

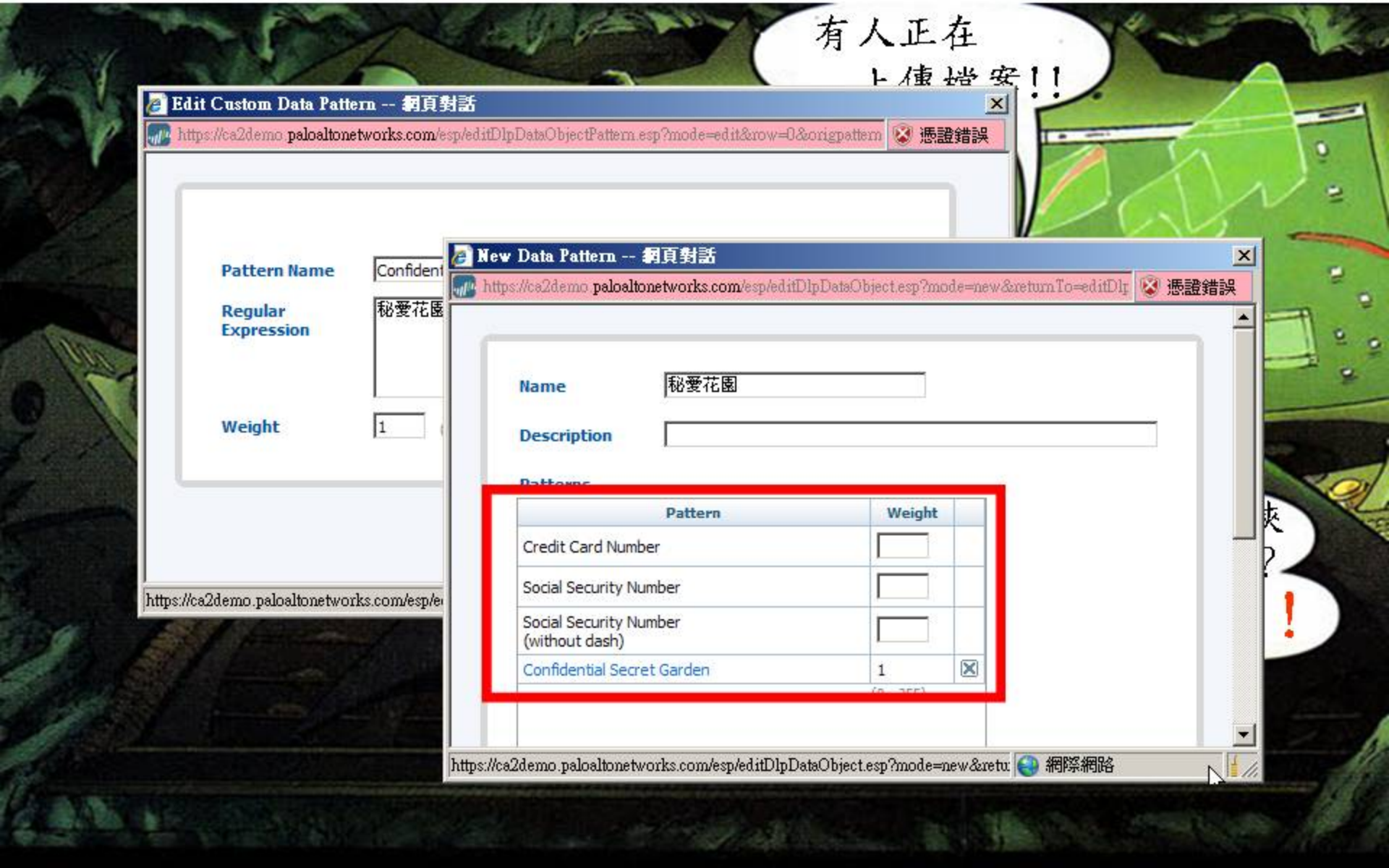
次世代防火牆實作案例：

以Palo Alto Firewall爲例

辨識使用者

掃瞄傳輸內容

掃瞄傳輸內容


有人正在
Edit Custom Data Pattern -- 網頁對話
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObjectPattern.esp?mode=edit&row=0&origpattern
憑證錯誤
Pattern Name
Confident
Regular Expression
秘愛花園
Weight
1
New Data Pattern -- 網頁對話
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&returnTo=editDlp
憑證錯誤
Name
秘愛花園
Description
Pattern
Weight
Credit Card Number
Social Security Number
Social Security Number (without dash)
Confidential Secret Garden
1
https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&retu
網際網路

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

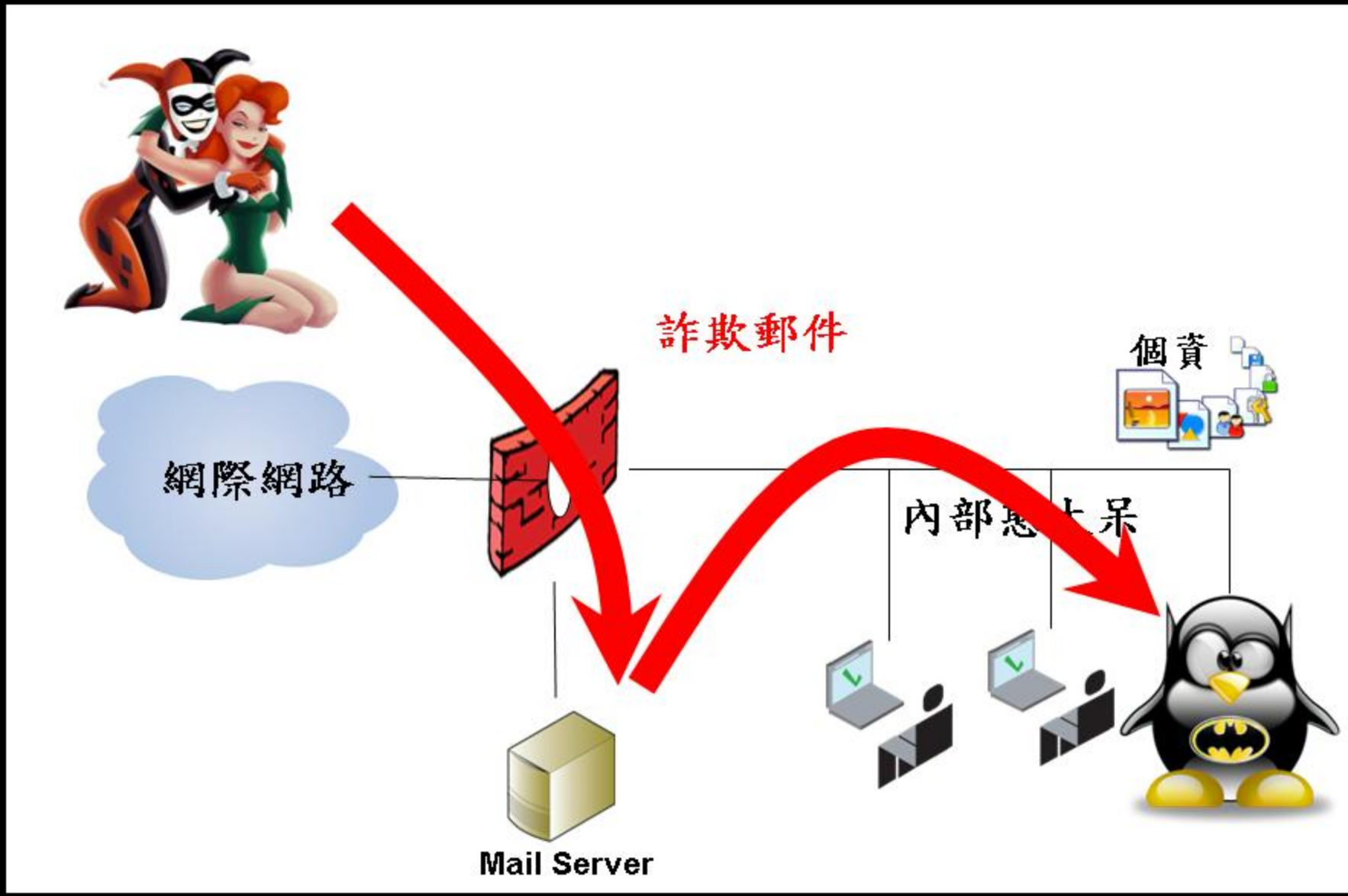
多功能應用層安全閘道系統

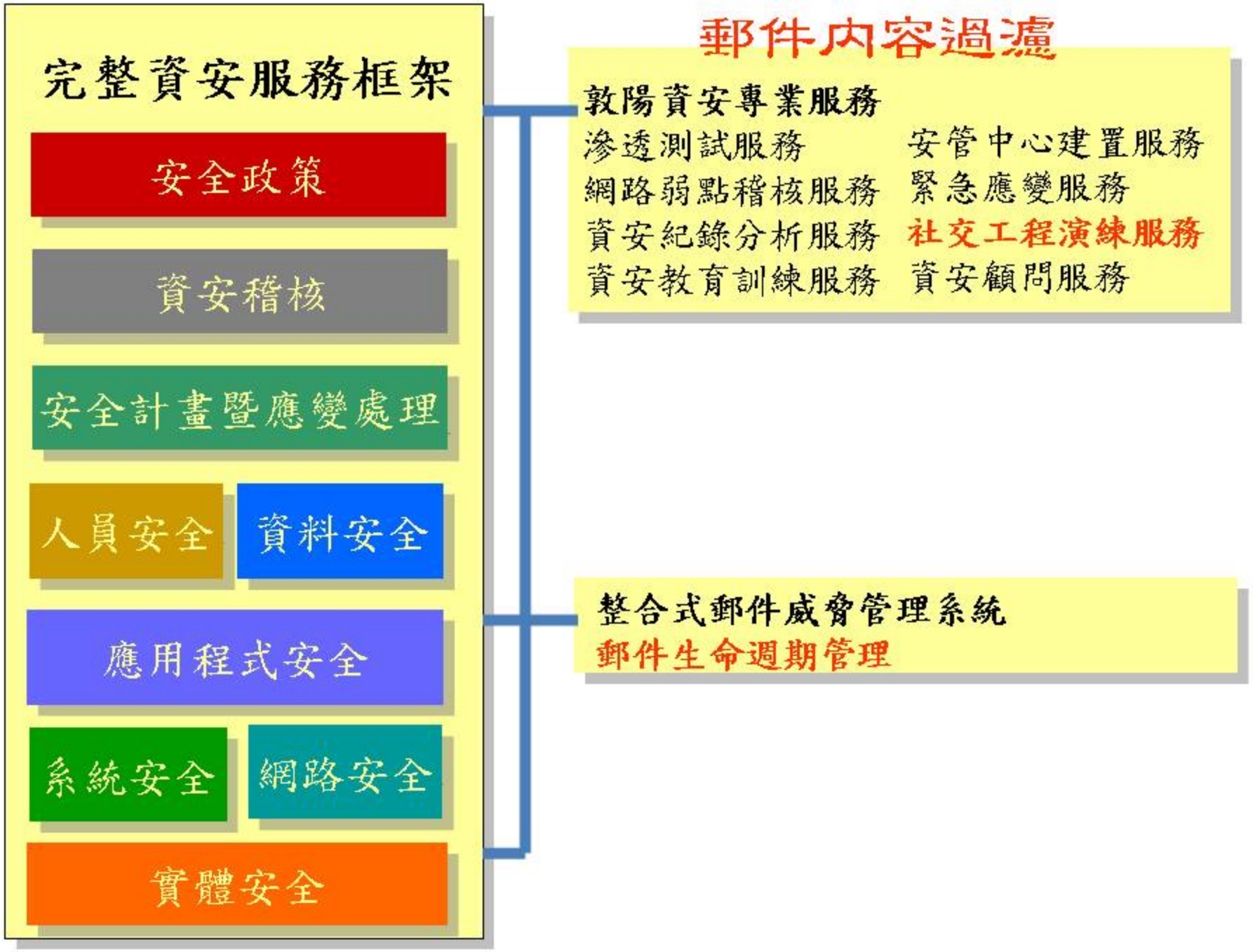
Palo Alto Firewall

Stark Technology Inc.
敦陽科技股份有限公司

人性的弱點

蠢人洩露個資




完整資安服務框架
安全政策
資安稽核
安全計畫暨應變處理
人員安全
資料安全
應用程式安全
系統安全
網路安全
實體安全
郵件內容過濾
敦陽資安專業服務
滲透測試服務
網路弱點稽核服務
資安紀錄分析服務
資安教育訓練服務
安管中心建置服務
緊急應變服務
社交工程演練服務
資安顧問服務
整合式郵件威脅管理系統
郵件生命週期管理

社交工程演練

由專家人力模擬駭客
寄發詐欺信件
統計竊得的個資
…及蠢人

次世代防火牆實作案例：

以CelloPoint UETM爲例

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

滲透測試服務	安管中心建置服務
網路弱點稽核服務	緊急應變服務
資安紀錄分析服務	社交工程演練服務
資安教育訓練服務	資安顧問服務

整合式郵件威脅管理系統
CelloPoint UETM

Stark Technology Inc.
敦陽科技股份有限公司

工商服務

完整資安服務框架

- 安全政策
- 資安稽核
- 安全計畫暨應變處理
- 人員安全
- 資料安全
- 應用程式安全
- 系統安全
- 網路安全
- 實體安全

Stark Technology Inc.
敦陽科技股份有限公司

敦陽資安專業服務

- 滲透測試服務
- 網路弱點稽核服務
- 資安紀錄分析服務
- 資安教育訓練服務
- 安管中心建置服務
- 緊急應變服務
- 社交工程演練服務
- 資安顧問服務

高階應用層交付暨安全系統

Citrix NetScaler WAF

多功能應用層安全閘道系統

PaloAlto Firewall

整合式郵件威脅管理系統

CelloPoint UETM

更多專業資訊安全防禦系統工具

防火牆、入侵偵測、防毒、終端保護
內容安全、流量控管、認證、加密、
存取控制、資料庫安全、無線安全…


我們的老闆
我們的資安顧問
我們的業務
我們的工程師

我們的服務 － 什麼都幹

- 資安環境建置
  - 網頁防火牆(WAF)
  - 資料庫稽核防護(DB Real-Time Auditing/Protection)
  - 程式碼檢測工具(Code Review)
  - 網路側錄分析儀(Sniffer/Forensic)
  - 資料防洩解決方案(DLP)
- 資安服務
  - 滲透測試
  - 弱點掃瞄
  - 緊急應變
  - 程式碼檢測
  - 資安政策規劃
  - 資安SOP撰寫
- 協力服務
  - ISO 27001
  - SOC委外監控
- 教育訓練
  - 資安管理政策
  - 網路攻擊與系統防護
  - 安全程式撰寫
  - 基礎資安概念
  - 駭客攻防技術教育訓練
  - Web Application安全
  - Windows 作業系統安全管理
  - Unix系統安全管理
  - Wireless Security
  - Host Security
  - 安全漏洞剖析
  - 資訊安全內部稽核
  - 密碼設定技巧
  - 郵件社交工程
  - 其他客製課程


問題與討論
lucifer 點 yang 小老鼠 sti 點 com 點 tw