中小企資訊保安

中小企資訊保安

- 資訊及資訊的重要
- 什麼是資訊保安?
- 如何裝備你的資訊系統?
- 如何防禦及處理資訊保安事故?
- 實用網址及軟件介紹

資訊及資訊的重要

- 資訊資產包括：
  - *數據資產*
    - 有意思的數據
  - *服務資產*
    - 如用電腦直接傳送至客戶的服務

- 數據資產和服務資產之間有很密切的關係

資訊資產

- 數據經過記錄、計算、分析或調整
  - *參考(歷程記錄)*
  - *追蹤(足印)*
  - *跟隨(指引)*
  - *指示*
  - *計劃*
  - *報告*

資訊資產

- 服務資產
  - *網絡服務*
  - *自動櫃員機服務*
  - *互聯網服務*

資訊資產

- 傳送、使用或儲存在實型或非實型的媒體

資訊資產

- 公司不可或缺的資產
  - *非敏感資料*
    - 公司網址
    - 公司地址
    - 公司服務及產品
    - 聯絡資料
    - ……

資訊及資訊的重要

- *敏感資料*
  - 利害關係者(Stakeholders)
    - 員工、供應商、客戶……
  - 財務及會計
  - 項目或合約
  - 報告
    - 市場策略、公司方向

資訊及資訊的重要

- 需要對資產有適當的保護
  - ➢ *資訊保安*
    - 容易被濫用和破壞
    - 不單純粹是機構內部事務，外界有時亦有理由要求 / 期望該機構的資訊得到良好的保護
      - – 警方
      - – 信用卡公司
      - – 藥廠

什麼是資訊保安?

- 資訊保安的目的：-

  - *有以下三個主要原則：*
    - 可用性 (Availability)
      - 讓資訊可供使用者在需要時取用
        - » 機構網頁

        - » 售賣系統
        - » 醫療系統

資訊保安三個主要原則

- 完整性 (Integrity)
  - 保護資訊免受未經授權人士更改
    - » 網頁
    - » 文件 (合約、單據)
    - » 訊息

  - 原因
    - » 中間人攻擊 (Man-in-the-middle Attack)
    - » 非法修改網頁 (Defacement)
    - » 程式錯誤 (Software bug)

資訊保安三個主要原則

- 機密性 (Confidentiality)
  - *保護資訊免向未經授權人士披露*
    - » 需要知道原則 (need-to-know basis)
    - » 加密
    - » 存取控制 (IRM - 資訊版權管理)
  - 手法
    - » 中間人攻擊 (Man-in-the-middle Attack)
    - » 密碼破壞程式

資訊保安的目的

- 在廣闊的資訊網絡上：
  - *確保業務可以得以連續運作*
  - *增加投資回報及商業機會*
  - *有機會發生的危險合理地減到最少*

資訊保安措施

- 實施合適的控制達到目的，如
  - *政策*
  - *程序*
  - *指引*
  - *系統 (電腦 / 非電腦)*

資訊保安措施

- 合適的監控需要：
  - *小心設計及計劃*
  - *注意監控之細節*
  - *公司內所有員工 (最少要求)*
  - *所有其他有關人士 (最理想)*
    - 供應商
    - 外判商
    - 合作伙伴
    - 客戶

如何裝備你的資訊系統?

- 認識及了解貴公司的：
  - *公司業務及架構*
    - 業務性質
      - 為何要保護公司資訊
        - » 公司業務策略及目標
        - » 潛在的影響
        - » 契約的要求
        - » 社會及文化的環境
        - » 法律責任

如何裝備你的資訊系統?

- *公司架構*
  - 面對的困難
    - 管理層的支持
    - 系統支援 (人力及物力)
    - 用戶的配合

資訊類型

- *資訊類型*
  - 什麼類型的資訊?
    - 機密、限制、非限制
    - 個人性、敏感性、一般性

資訊用途

- *什麼用途的資訊?*
  - 內部使用
  - 外部受權者使用
  - 公用

資訊處理方式

- 如何儲存、使用及分享?
  - 儲存方式
    - » 紙張
      - 合約
      - 文件
      - 報告
      - 記錄 ……
    - » 電子媒體
      - DVD
      - CD
      - USB
      - FLOPPY ……

資訊使用方式

- 使用及分享
  - *互聯網、內聯網 (Internet、Intranet)*
  - *網絡檔案分享 (File Sharing、FTP)*
  - *電子媒體 (USB、Floppy)*
  - *紙張*

資訊的威脅

- 資訊及系統上要面對的威脅
  - *資料被透露*
  - *資料遺失*
  - *資料被修改*
  - *資料及系統損壞*
  - *服務停止*

保護的程度

- 資訊需要保護的程度
  - *威脅發生的可能性*
  - *對業務的影響*
  - *資源*

資訊系統

- 資源
  - ➢ *技術、知識及保護方法*
  - ➢ *技術、知識*
    - 現有的系統及可用的技術
      - 操作系統
        - Windows
        - Linux \ Unix
        - Mac

技術、知識

- 應用系統
  - *電子郵件*
  - *即時訊息*
  - *會計*
  - *倉存*
  - *客戶管理*
  - *文件管理*

保護方法

- 電腦系統控制
  - *網絡架構*
  - *資源分配*
  - *用戶控制*
- 非電腦系統控制
  - *政策管理*
  - *用戶及操作指引*

如何防禦及處理資訊保安事故?

- 教育
- 政策管理
- 技術性監控
- 重要成功因素

教育

- *雇用相關技術人才*
  - 保安意識不足
    - 不察覺問題
  - 影響保安管理
    - 改變現有保安設定

教育

- *在職培訓*
  - 用戶保安意識訓練
  - 技術人員訓練
  - 講座 / 會議
    - 資料保安
    - 系統應用

教育

- *資訊發放*
  - 通告
    - 發佈日期
    - 發佈人
    - 員工簽署
  - 電郵
    - 讀取通知

政策管理

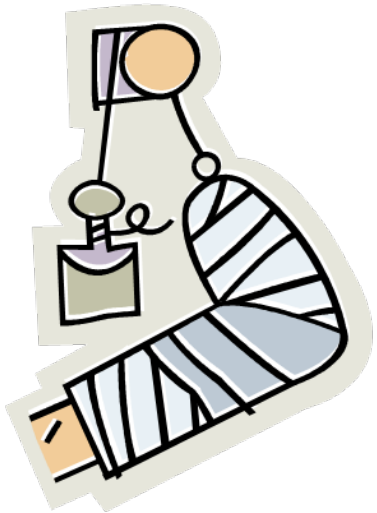
- *制定資訊保安政策*
  - 達到合理、具體而可行的保安管理
    - 減輕對業務的影響達到合理水平
    - 容易明白
    - 清晰指引
  - 配合公司業務方向
    - 有實際關係

制定資訊保安政策

- *基於法律要求*
  - 資料保密條例
  - 個人私隱條例
  - 合約條例
  - 知識產權條例

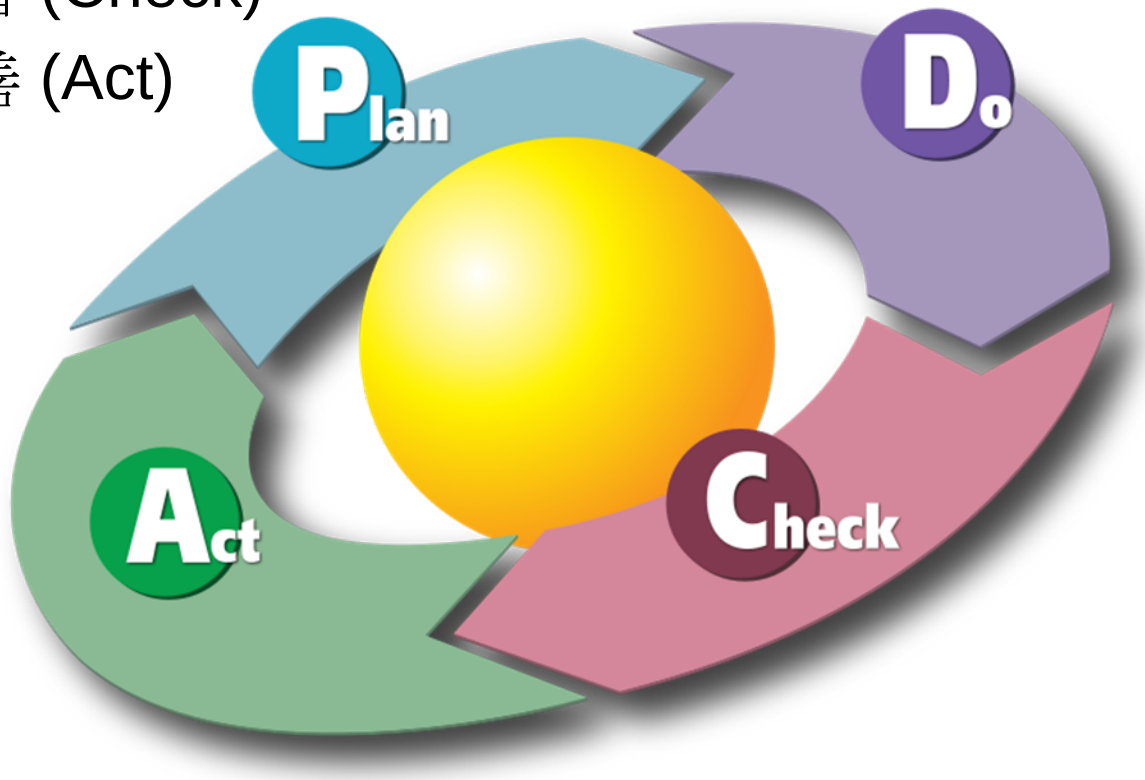
制定資訊保安政策

- *考慮跟隨保安常規*
  - 資訊保安政策文件
  - 分配資訊保安職責
  - 處理資訊保安事故及改善工作



制定資訊保安政策

- *保安政策需要：*
  - 建立 (Plan)
  - 執行 (Do)
  - 復審 (Check)
  - 改善 (Act)



技術性監控

- 技術顧問

- 保養及維修人員
  - *公司員工*
  - *外判支援 (合約性)*
  - *非合約性支援*

技術性監控

- 專業資訊渠道
  - *香港電腦保安事故協調中心 (www.hkcert.org)*
  - *政府資訊科技總監辦公室 - 資訊安全網 (www.infosec.gov.hk)*
  - *香港政府一站通：資訊保安*
  - *NEWSGROUP*
  - *代理、供應商*

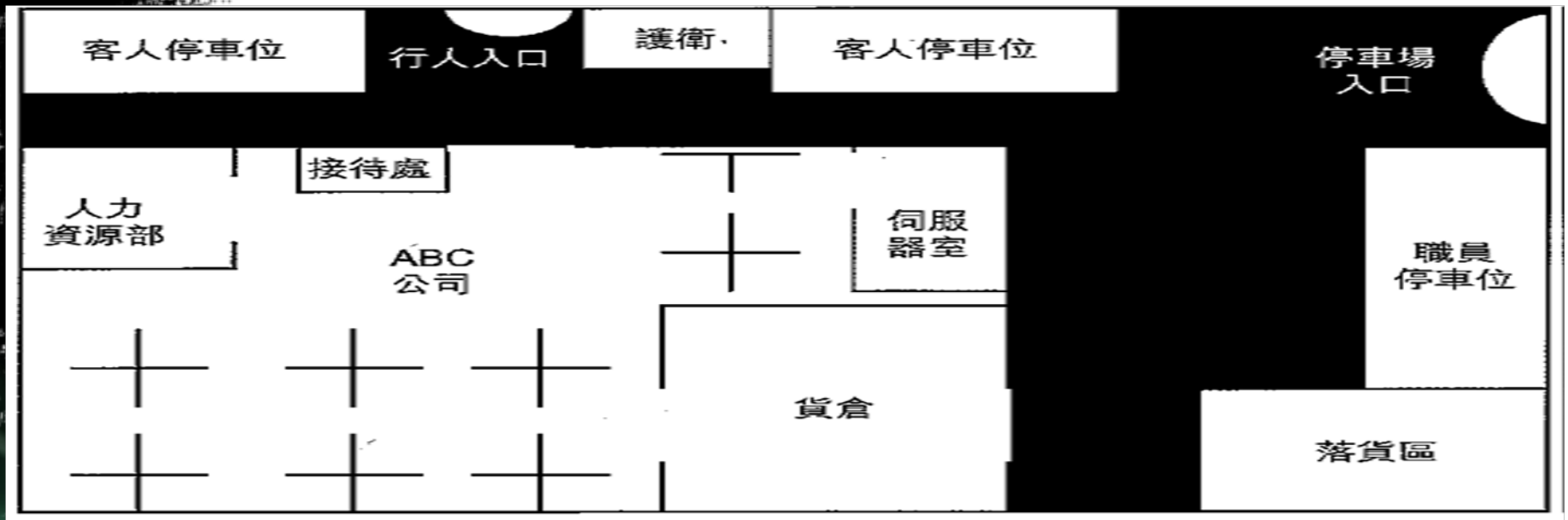
- 技術性檢測
  - *定期審核*
  - *使用可靠檢測程式*
    - *Nessus, WinAudit……*

重要成功因素

- 致使成功施行資訊保安政策
  - *由管理層表現的清晰支持*
  - *了解及明白資訊保安的要求*
  - *提供及保持合適資訊保安警覺性、教育及訓練*
  - *定期進行資訊保安審核*

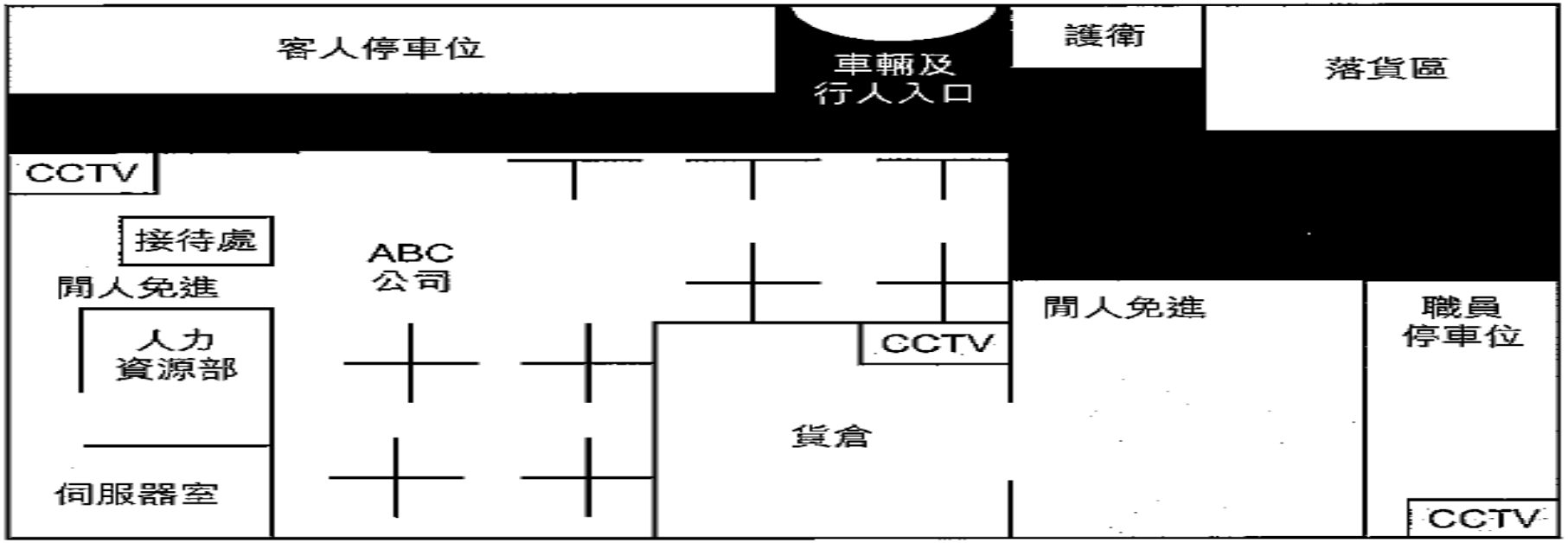
保安風險緩減具體方向

- 實體性出入及環境保安管制
  - ➢ *確保人命及資訊處理設施安全*
    - 人命是實體性保安風險的第一考慮
  - ➢ *電腦及網絡系統的位置*
    - 安全地方
      - – 避免非受權人士接觸
      - – 避免容易毀壞 (故意 / 意外)
      - – 公共地方、貨物裝卸區……

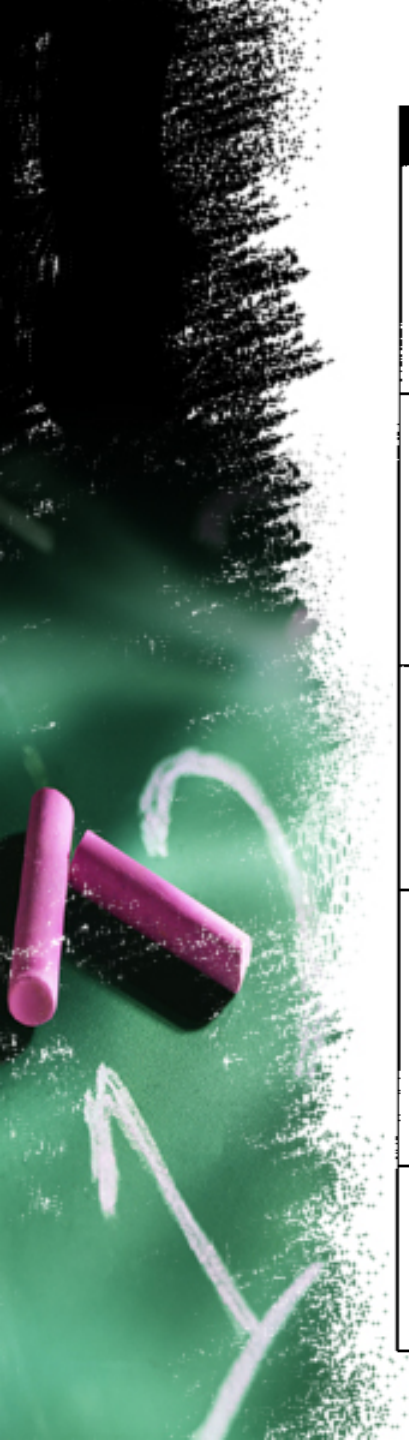


樓面佈置圖1

樓面佈置圖2是改良後的設計。透過比較兩個設計，我們可以說明幾個設計原則。



樓面佈置圖2



設計原則	樓面佈置圖2的優點
將入口的數目減至最少	• 人和車共用一個入口，並移到保安崗位旁邊。護衛員可以集中留意一個入口。 • 連接辦公室的貨倉後門被取消。 • 進入人力資源部和伺服器室的通道被改窄。
將物業跟據保安要求劃分為不同的區域	• 訪客停車區和卸貨區被移到外圍。 • 職員停車區被移到較內的位置。 • 貨倉外部被定為限制進入區域（貼上限制警告！） • 在人力資源部和伺服器室外設立限制區域，防止訪客和沒授權的職員進入。
運用多種不同科技和程序的防禦技術	• 進入敏感區域之前要經過幾層由門戶、專人監控和入侵監察系統（CCTV）組成的防禦設施。 • 為人力資源部和伺服器室加裝額外的防禦措施，例如保安進出咭閱讀器可以有效地防止未經授權的訪客和職員的進入。
監察和登記出入記錄	• 保安崗位被移到可以看到門外情況的位置。 • 接待處被移到人力資源部和伺服器外面，方便監察人流。 • 在貨倉內和外裝置CCTV，監察貨倉內外的活動。 • 在接待處裝置CCTV，監察辦公室的入口和進入人力資源部和伺服器室的通道。
專人陪同進入高度保安區域	• 要有專人陪同進入高度保安區域。 o 訪客要在公司的負責人員在場才可以在貨倉外的限制區上落貨。 o 內部職員要有負責職員陪同下才可以進入伺服器室。

環境保安管制

- 受干擾地方 (對其運作受影響)
  - *過熱*
  - *漏水*
  - *電力負荷過重*
  - *其他*
    - 鄰近機構所帶來影響
      - 業務性質

環境保安管制

- 防災設施
  - *UPS*
  - *滅火設施*
  - *空氣調節裝置*
  - *風扇*
  - *選擇合適地方*

環境保安管制

- 線路防護
  - *電腦線*
    - UTP (Unshielded Twisted Pair)
    - STP (Shielded Twisted Pair)
  - *位置*
    - 受電線干擾
    - 橫越通道

環境保安管制

- 資料儲存位置
  - *備份設備及文件*
  - *軟 / 硬件*
    - CD / DVD……
    - Hard Disk

病毒 / 惡意程式防禦

- 受襲擊而引致；
  - *資料遺失 / 刪改*
  - *資料被洩露*
  - *系統損壞*
  - *影響工作效率*
  - *不正常服務*

病毒 / 惡意程式防禦

- 如何有效監控?
  - ➢ *有效防毒軟件*
    - 合時防毒軟件版本
      - – 功能
        - » SPYWARE
        - » ADWARE
        - » 系統
        - » 應用程式
      - – 技術
        - » 殺毒技術

病毒 / 惡意程式防禦

- *合時病毒種類目錄*
  - 自動更新

- *合適防禦設定*
  - 病毒清除方法
    - 自動病毒隔離
    - 自動病毒刪除 / 消除病毒
    - 通知但不行動
    - 通知及選擇行動

病毒 / 惡意程式防禦

- 監控及保護型式
  - *檔案位置*
  - *檔案類型*
  - *系統服務*

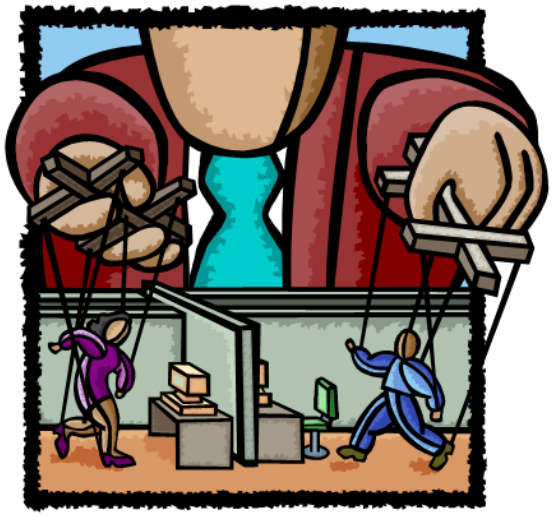
病毒 / 惡意程式防禦

- 病毒目錄更新時間表

- 實時監測及保護

進階防毒系統管理

- 防毒程式中央管理系統
  - *統一監控設定*
  - *病毒目錄更新情況*
  - *事故記錄及通知方式*



病毒 / 惡意程式防禦

- 良好習慣防備病毒入侵
  - ➢ *補釘管理 (patch management)*
    - 操作系統
    - 應用程式

病毒 / 惡意程式防禦

- 網頁瀏覽
  - *資訊下載*
  - *不明的來源*
- 軟件下載及安裝
- 不明或奇怪電郵及即時訊息

互聯網安全

- 建立網頁瀏覽監控系統
  - *濾器有問題的網站*
  - *控制網上行為*
    - 限制上 / 下載文件
    - 限制網上服務 (FTP、REMOTE…)

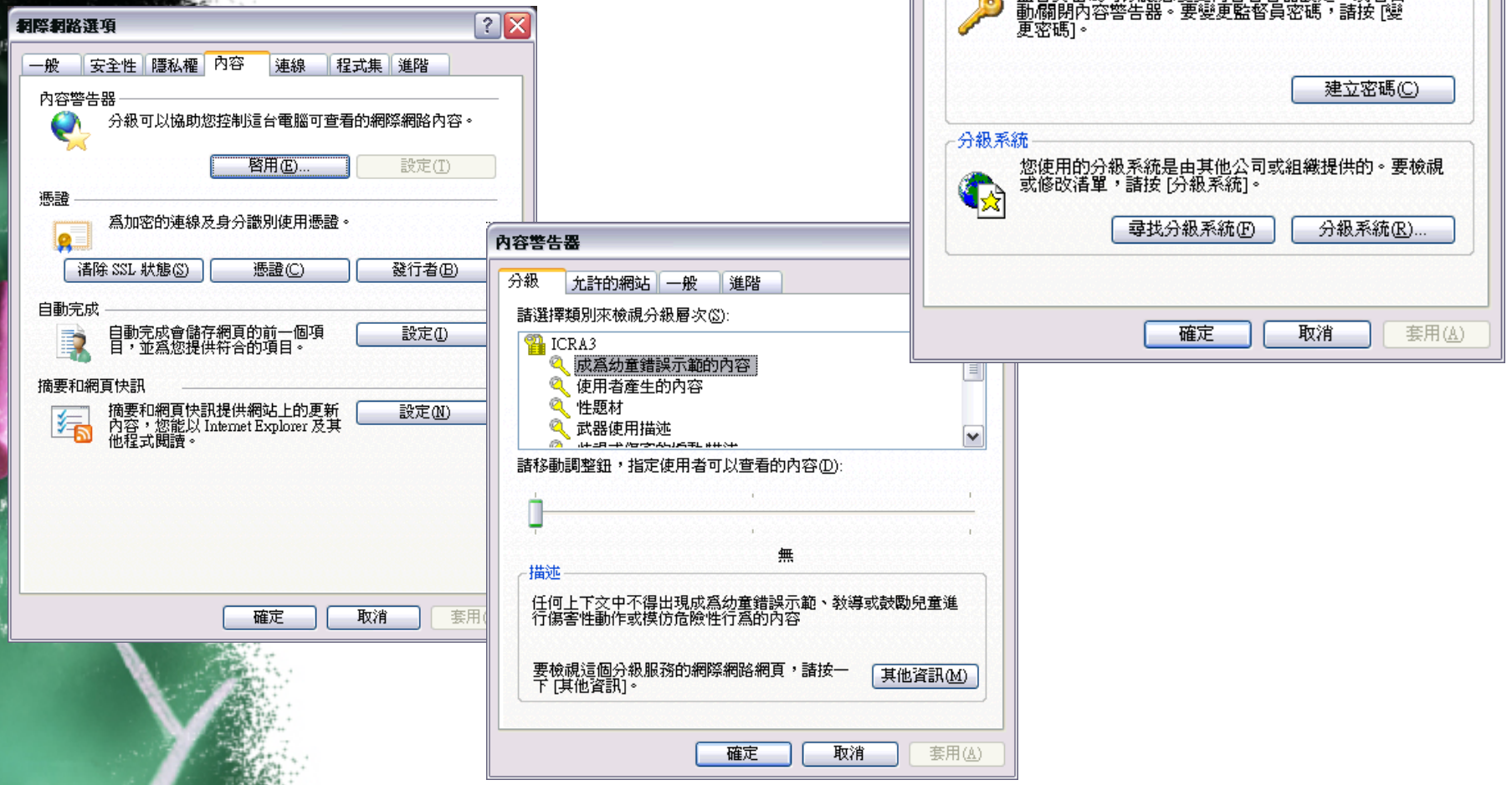
互聯網安全

- 使用安全網頁瀏覽器、應用程式或服務
  - ➢ *注意程式的提示及警告*
    - 安裝不明程式
    - 警告字眼

  - ➢ **www.tima-cn.com**

互聯網安全

- 開啟安全設定

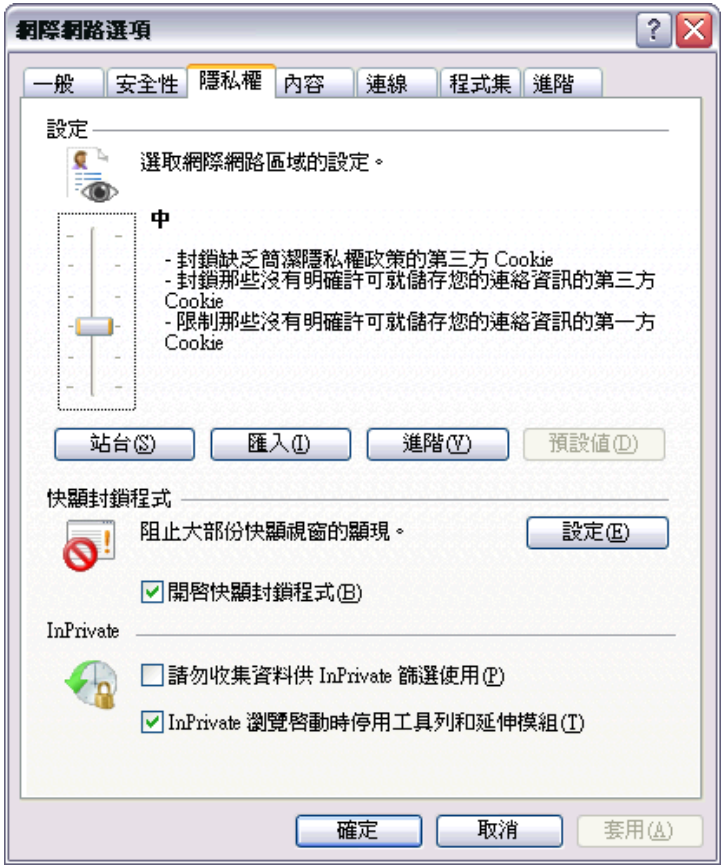


開啟安全設定


刪除瀏覽歷程記錄(D)...
Ctrl+Shift+Del
InPrivate 瀏覽(I)
Ctrl+Shift+P
網頁隱私權原則(V)...
InPrivate 篩選(F)
Ctrl+Shift+F
InPrivate 篩選設定(S)
安全性報表(R)
國際網站位址(I)
SmartScreen 篩選(T)
Windows Update(U)
檢查此網站(C)
關閉 SmartScreen 篩選(F)...
報告不安全的網站(R)
在線商城
< 2010 >
< 1

互聯網安全

- 啟動防毒功能
  - *Virus*
  - *Spyware*
  - *Adware*
- Cookies設定
- 密碼儲存

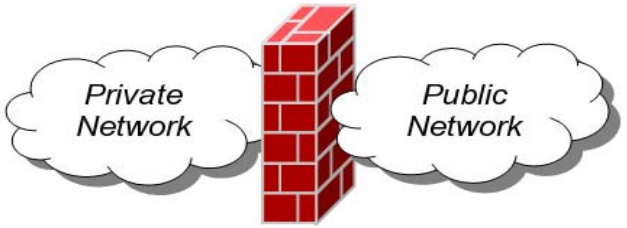


互聯網安全

- 使用安全渠道
  - *HTTPS*
  - *VPN (IPSec / SSL)*
  - *SFTP…*

網絡及系統安全

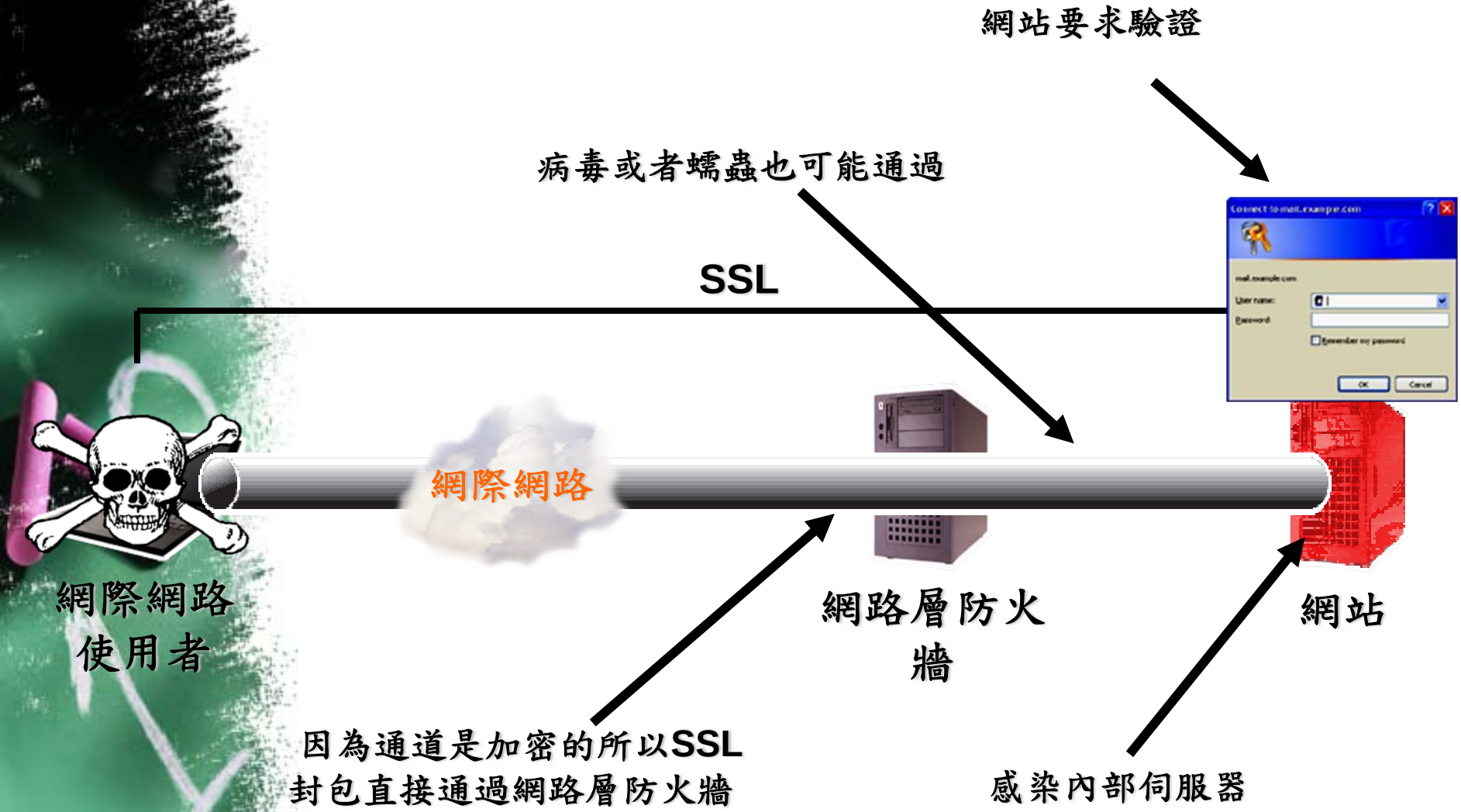
- 有效防火牆
  - *將兩個 (或以上)的網絡分隔，並依照一些預定的規則，以允許或限制的方式控制網絡行為*
    - 封包過濾、NAT……
    - 網路層 (傳統型式)
      - IP 封包過濾型式
        - » 來源 IP 位址或埠號
        - » 來源目的 IP 位址或埠號
        - » 通訊協定(TCP/IP、NWLink、AppleTalk)
      - 特性
        - » 運作快
        - » 設置簡單
        - » 有限防禦



有效防火牆

- 應用層
  - 應用程式的封包過濾型式
    - » MSN
    - » Skype
    - » 網路電視
  - 特性
    - » 資源要求較多
    - » 設置較複雜
    - » 較多方面防禦

HTTP篩選器

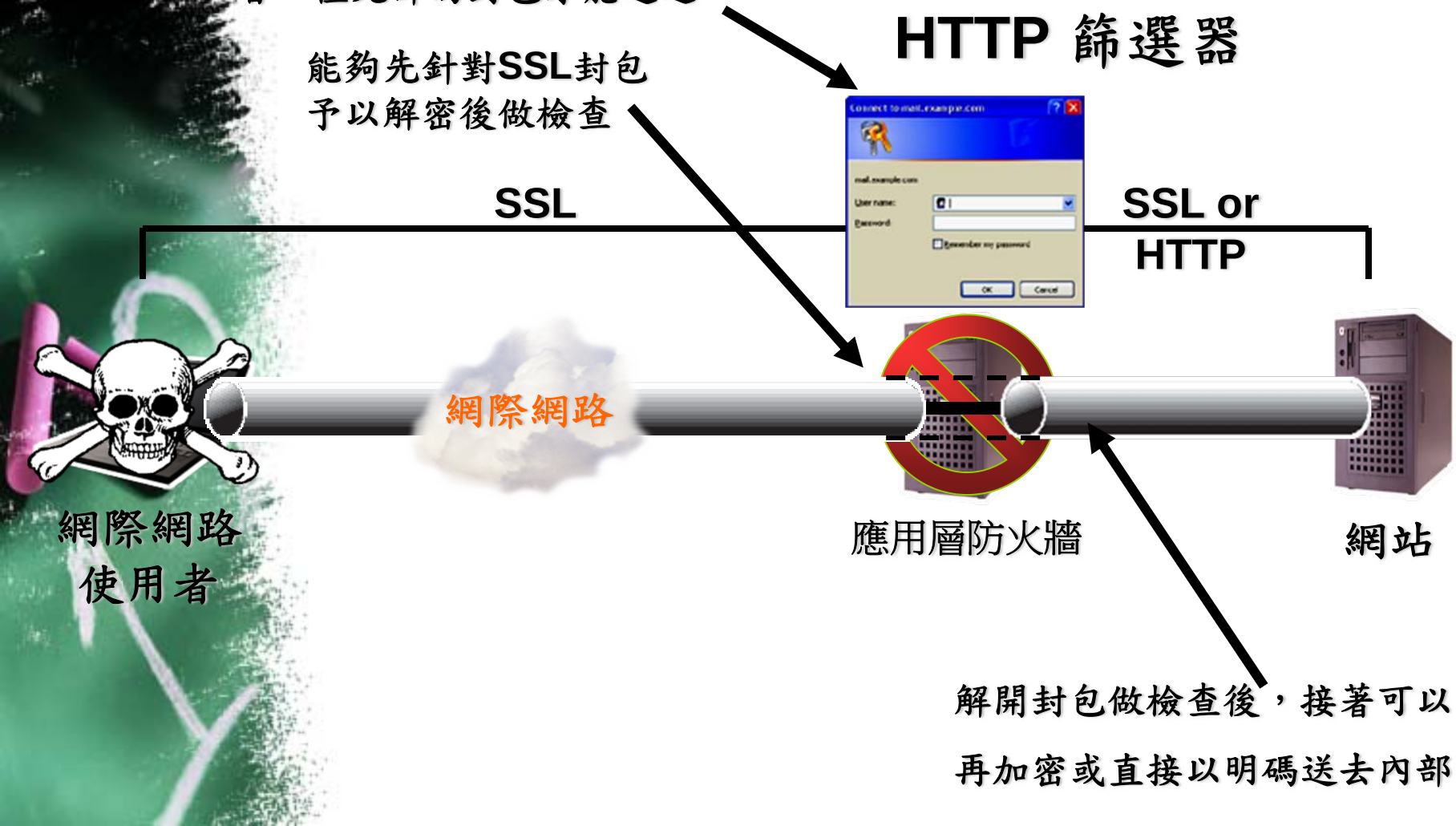

網站要求驗證
病毒或者蠕蟲也可能通過
SSL
網際網路
網際網路
使用者
網路層防火
牆
網站
因為通道是加密的所以SSL
封包直接通過網路層防火牆
感染內部伺服器

HTTP篩選器

代理驗證/HTTP 篩選器

即使是SSL封包，應用層防火牆 HTTP 篩選器也能夠防止網頁型態的攻擊

應用層防火牆預先驗證使用者，僅允許的封包才能通過



有效防火牆

- Windows XP / Vista / 7 (Personal Firewall)
- Linux IP table (Network Layer Firewall)
- Microsoft ISA Server
- Proxy Server
- Broadband Router
- Wireless Access Point

入侵式偵測/防禦系統

- 入侵式偵測系統 (IDS)
  - 主要功能在負責監聽網路封包
  - 網路與系統的運行狀況進行監測
  - 依據預先設定的安全策略(Security Policy)
  - 當發現異常，自動發出警訊通報給網管人員
  - 記錄各種攻擊企圖、攻擊行為或者攻擊結果

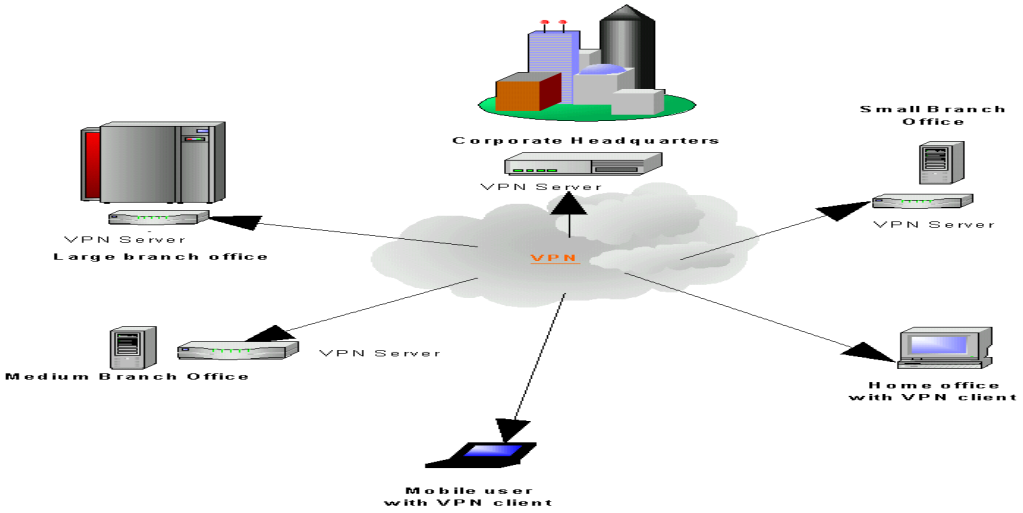
入侵式偵測/防禦系統

- 入侵式防禦系統 (IPS)
  - 將IDS的被動偵測方式變為主動防禦方式
  - 當發現網路異常封包或行為時，系統除發送警訊通報給網管人員
  - 以自動化的過程立即採取必要的處置措施

虛擬私人網絡(VPN)

- 利用 Internet 網路，建立 Internet 上的加密通道 (Tunneling) 來架構網際網路上的虛擬內聯網路(VPN)

- *避免第三者「竊聽」到通訊內容，同時還須確保網路傳送內容不被篡改破壞*



虛擬私人網絡(VPN)

- IPSec VPN
  - *將兩個區域網絡通過 IPSec VPN 連結起*
  - *兩方的電腦群互相連接*

- SSL VPN
  - *客戶端與 VPN 伺服器的連接*
  - *客戶端與客戶端之間不會互相連接*

虛擬區域網絡 (VLAN)

- 透過虛擬區網（Virtual Local Area Network，VLAN）的技術，網管人員可以對不同實體區網中的設備進行邏輯上的分群（Grouping），為區網管理提供更完整的資訊安全保障

  - 降低區網間大量資料流通時因過多無用封包充斥而導致封包雍塞的問題

  - 無需用防火牆都能有效地將網絡與網絡之間安全分隔，但沒有規定控制功能

無線網絡

- 注意的安全事項
  - *用戶確證*
    - 密碼
  - *保密協定*
    - WEP / WPA / WPA2
    - RADIUS / AD / Certificate Server
  - *系統管理控制*
    - 防火牆
    - 管理員密碼

遠端控制管理

- 工具
  - *VNC*
  - *Remote Desktop*
  - *Net Meeting*
- 存取控制
  - *防火牆*
  - *用戶、密碼*
- 網絡監測及通知

存取控制管理

- 確證 (Authentication)
  - *用戶身份*
    - 用戶名稱及密碼
      - 管理員 (administrator)
      - 訪客 或 匿名者 (Guest / Anonymous)
    - 生物認證
      - 指紋
      - 面容
      - 眼睛
    - 證書
      - 身份證

存取控制管理

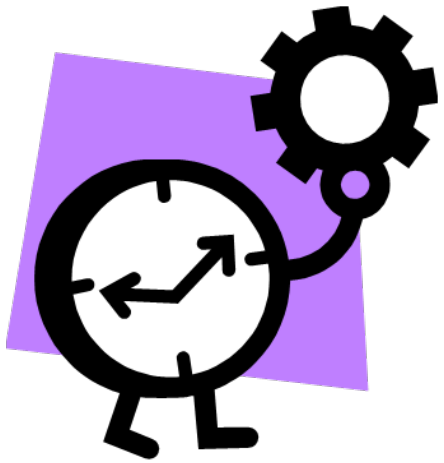
- 授權 (Authorization)
  - *存取 / 控制權限*
    - 個人 / 組別
    - 檔案
    - 應用程式
    - 服務
    - 遠端 / 本地

備份及恢復管理

- 備份軟件 / 硬件管理
  - *支援*
    - Patch
    - Formula
  - *備份媒體類型*
    - DVD、DAT/DLT Tape
  - *淘汰 (技術 / 設備)*
    - 加密技術
    - 硬體技術

備份及恢復管理

- 良好習慣及手法
  - *定時備份*
  - *定時備份測試*
  - *在媒體上標示*
  - *資料加密*



備份及恢復管理

- 備份媒體處理
  - *合適保存位置*
  - *媒體品質*
  - *異地儲存*
  - *丟棄處理*

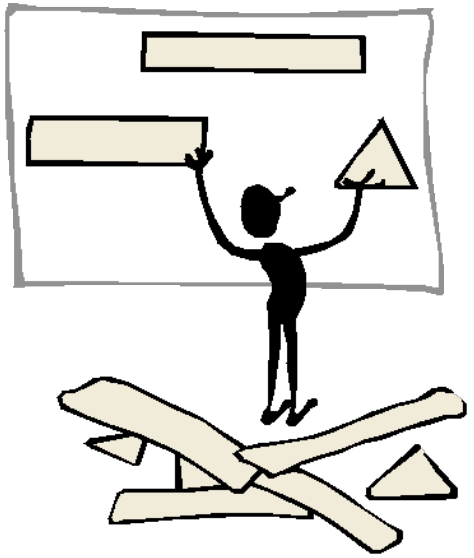
系統及程式記錄管理

- 偵測及調查非受權行為

- 調查事故發生及原因
- 疑難排解

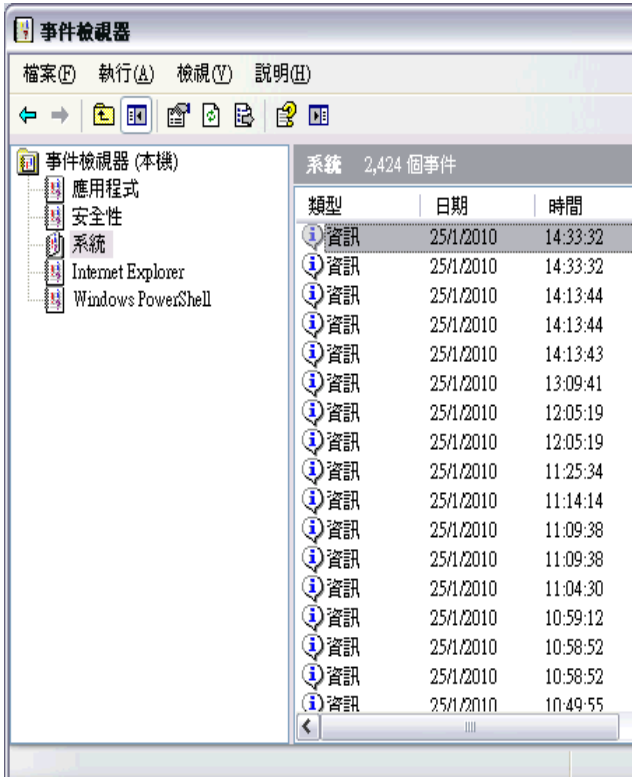
系統及程式記錄管理

- 存有敏感的資料，需要合適保護
- 任何人都不能刪改記錄內容
- 不可隨意修改記錄對象



系統及程式記錄管理

- 監測系統
  - *Windows event log*
  - *FTP Transaction Log*
  - *Firewall*
  - *Instant messenger*



系統及程式記錄管理

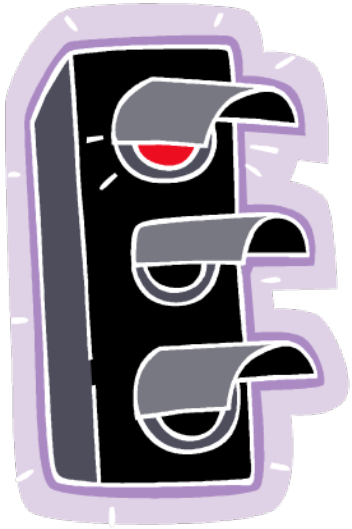
- 事故檢測控制
  - *記錄內容*
    - 用戶資料
    - 日期及時間
    - 事故類型
      - 系統
      - 安全性
      - 應用程式

系統及程式記錄管理

- *活動資料*
  - 成功 / 失敗 / 警告 …
  - “企圖進行”

系統及程式記錄管理

- 警告通知
  - *電郵*
  - *即時訊息*
    - 電話
    - 電腦
    - 指示燈

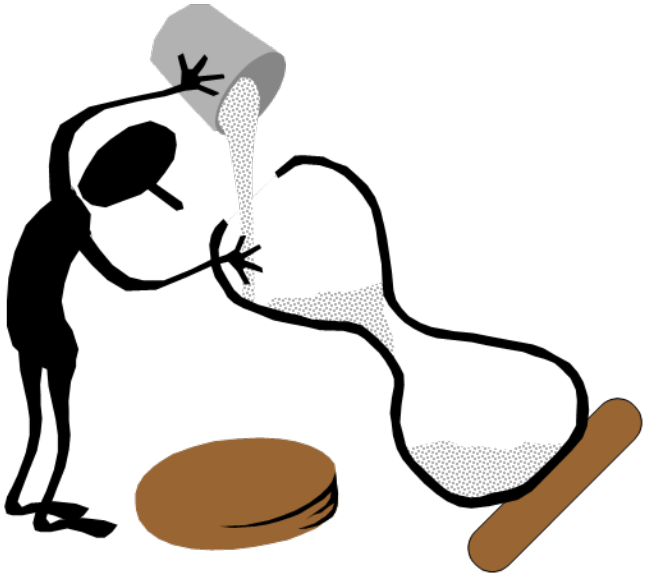


系統及程式記錄管理

- 時間同步
  - *天文台*
  - *時間伺服器*

系統及程式記錄管理

- 定期檢查
  - *合適的設定*
  - *非受權刪改*
  - *防止事故發生*



媒體處理

- 實體
  - *USB 儲存器*
  - *硬碟*
  - *磁帶*
  - *光碟*
  - *軟磁碟*
  - *紙*

- 非實體
  - *大氣電波 (聲音、無線電...)*
  - *網絡 (電郵、訊息、電話...)*
  - *顯示器 (電腦、電話...)*

媒體處理

- 處理方式
  - *加密*
  - *上鎖*
  - *特別工具開啟*
  - *顯示器的過濾器*
  - *良好的安放位置*
  - *處理棄置方法*

社會工程 (Social Engineering)

- 廣泛被駭客用來當作取得資訊的一種手段
- 欺騙手法獲得有價值的資訊或進入的權力
- 運用顯露的資料竊取想要的東西或入侵系統
- 目的:
  - *敏感 / 機密資料*
  - *非法進出 / 存取權*
  - *不適當的信任 (與機構內部人員)*

社會工程 (Social Engineering)

- 明白社會工程的原理
  - *交際的互相作用*
  - *不同途徑的遊說*
  - *感覺*
  - *基於人際 / 電腦 (human-based / computer-based)*
    - 個人特性
      - 傳播行為
      - 偶然逢迎
      - 信任關係
      - 道德責任
      - 內疚
      - 認同
      - 熱愛幫人

社會工程 (Social Engineering)

- 如何避免
  - *員工教育*
    - 高危人和物
      - 清潔人員
      - 服務台
      - 技術人員
      - 公司網頁
      - 密碼
  - *政策或指引給員工跟隨*

社會工程 (Social Engineering)

- 處理方法
  - *回電確實*
  - *使用信任媒體*
  - *共識資料及渠道*

外判支援

- 性質包括:
  - *外聘顧問 / 人員*
  - *供應商*
  - *維修人員*
  - *臨時工作人員*

外判支援

- 接觸對象
  - *硬體*
    - 伺服器
    - 個人 / 手提電腦
    - 防火牆
  - *應用系統*
    - 會計系統
    - 客戶管理系統

外判支援

- 可能接觸或獲得關於機構的資料和系統
  - *敏感或機密的資訊*
    - 人事資料
    - 批核渠道
    - 運作程序
    - 用戶賬戶和密碼
    - 基礎設備
    - 系統內（包括資訊科技及非資訊科技系統）既存的弱點和缺陷

外判支援

- 制定工作協議
  - *服務水準協議 (SLA)*
    - 服務提供者與使用客戶之間應就服務品質、水準以及性能等方面達成協議或契約
      - 反應時間 (Response Time)
      - 停止運作時間 (Service Down Time)
    - 成本及效益

外判支援

- 保密協議 (Non-disclosure Agreement)
  - *工作性質*
    - 清潔
    - 維修
  - *敏感資料及系統*
    - 人事
    - 財務及會計

外判支援

- 其他
  - *監督*
  - *覆檢*

知識產權

- 了解其合法使用性和安全性
  - *使用條款*
  - *版權聲明*
  - *隱私權聲明*
  - *責任聲明*

特別興趣小組

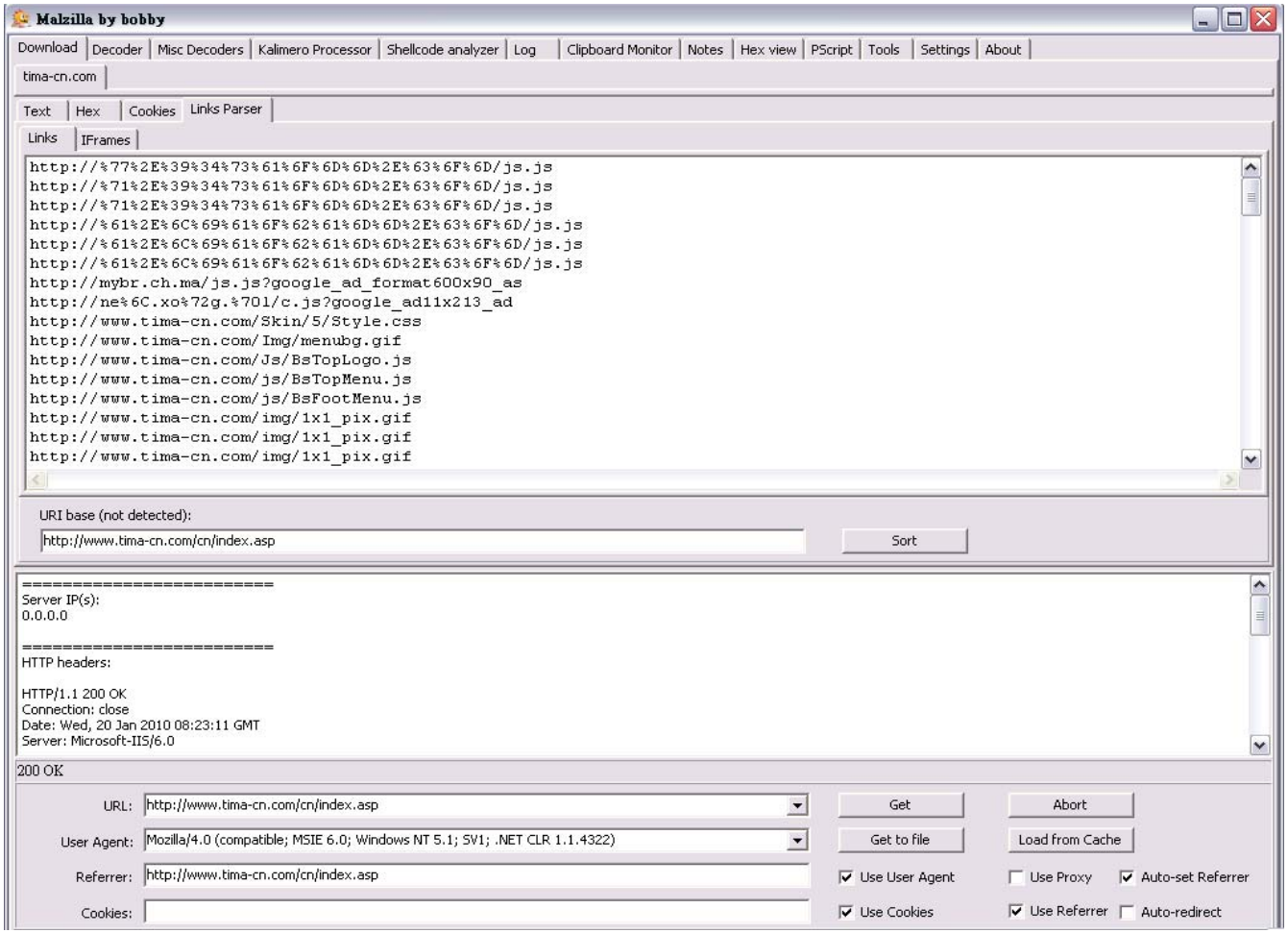
- 專業資訊渠道
  - *香港電腦保安事故協調中心 (www.hkcert.org)*
  - *政府資訊科技總監辦公室 - 資訊安全網 (www.infosec.gov.hk)*
  - *香港政府一站通：資訊保安*
  - *NEWSGROUP*
  - *代理、供應商*

有用工具及網頁

- www.zone-h.org (website defacement)
- www.cacert.org (Free Certificate)
- MRTG (Monitoring System)
- 安全檢查工具
  - *Nessus*
  - *Supper Rabbit (超級兔子)*
  - *Spyware Doctor*
  - *Lavasoft Ad-Aware*

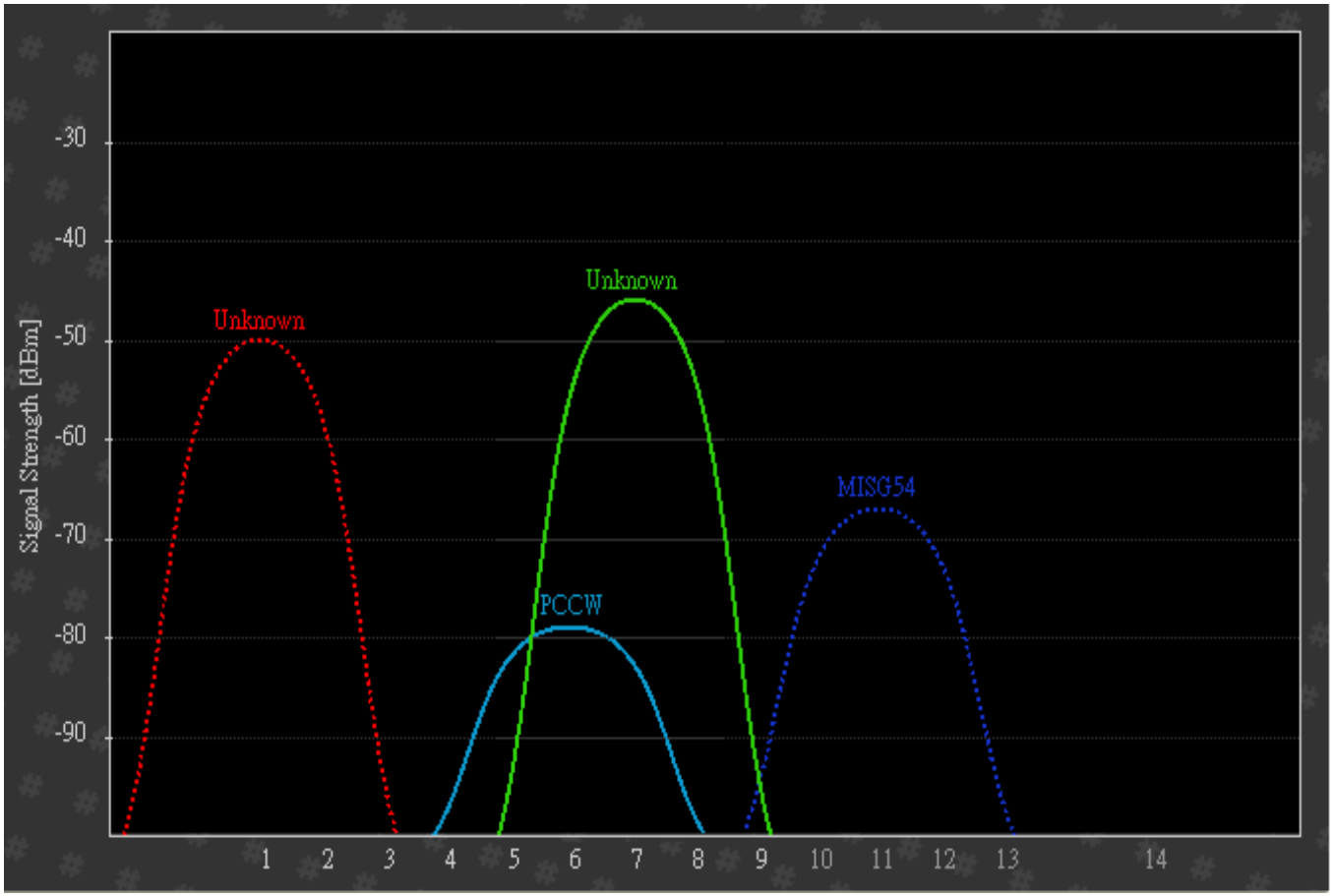
有用工具

- *Malzilla*



有用工具

- *Inssider*



有用工具及網頁

- 文件管理
  - *SVN server*
  - *MS-WSS*
- 其他
  - *PGP (Encryption software)*

Question?

Thank you!