

資訊安全的風險管理

吳忠霖
馨鴻科技股份有限公司

議題

- ◆ 資訊安全的現況
- ◆ 資訊安全的觀念
- ◆ 資安的政策推行



議題

- ✓ 資訊安全的現況
- ◆ 資訊安全的觀念
- ◆ 資安的政策推行



現今資訊安全的問題-機密外洩(無心)

化 資：E. 行業動向

類 別：EC2 章子二(電腦硬體/電子)

新聞標題：會計師函稿台積電財報提前曝光

新聞內容：

今(23日)下午(二十七)一時多分，市櫃公司首家大會計師行某公司，代理發言人曾晉?表示，引致其誤告于師事務所未作業疏失，導致第一季財報提前(口傳口傳)一時，應將追究相關人員責任，對市場貨好有無影響不便問候，且表示「可以討論」。

台積電第一季財報昨日下午意外在證交所網站曝光，經起該公司主動連絡，下午四時證交所召開重大訊息說明會；曾晉?表示，昨日十二點二十分，因勤業會計師事務所進行測試筆試，導致原預計四月三十日下午一點公布的首季財報，先上傳至證交所網站，二、三分鐘後發現錯誤，將該資訊自網站移除。

曾晉?表示，該項疏失與台積電以關，但基於，易資往普邏件、正確件，提前公布第一季財報，不過，將追究其告于師事務所責任。

今日說明會場，有證音勤業會計師事務所執行長張良輝之後，張借故止談到收盤時以六二，五元平盤作收，會場資訊公平傳達沒有我涼，對此，苦晉?表示，「有無影響股價，可以再討論」。

至於台積電該項性質問題，是心未~~將~~真變為有心公司刻意影響股價的通案性問題，上市公司將證交所網站密佈交予非監理人員的作法是否適當等尚待商討，證交所表示，財報、重大訊息風險與責任，本將由公司負責，若公司將證交所交付的證交所網站密佈委任第三者，如果受任人有任何的疏失，甚至造成市場損失，證交所仍將以公司犯錯為前提。

現今資訊安全的問題-機密外洩(故意)

[新聞首頁](#) > [社會新聞](#) > [中時電子報](#)

2004/04/17 (星期六)

一銀行外洩客戶徵信資料

[寄給朋友](#) [列印](#)

唐玉麟／台北報導，蔡依伶／台北報導 刑事局偵破張榮祿犯罪集團，赫然發現金融聯合徵信中心客戶資料外洩問題，財政部金融局高層昨晚說，與刑事局聯繫結果，初步得知是一家銀行將聯合徵信中心客戶資料外洩，若事實證明，確實是該銀行不當使用而外洩，將加以嚴懲，並予暫停查詢資料處分。

金融聯合徵信中心總經理陳林森也說，初步了解，是銀行查詢客戶資料後而外洩，並不是徵信中心內部人士所洩漏。

目前金融聯合徵信中心與三百五十九家銀行、農漁會信用部、信合社、票券與證券公司簽訂有會員制，且該中心提供金融機構逾七、八百萬信用卡戶及五、六百萬搜信戶的資料。

陳林森指出，各會員銀行在徵信中心查詢客戶資料，僅限於內部參考與評估使用，且依規定，凡查詢客戶資料的金融機構不得公開或移轉，若有違反者，視情節輕重，將被處分停止一定時間查詢，過去實例暫停查詢處分最長為四十天或一個月。



現今資訊安全的問題-中毒癱瘓運作

台郵局遭電腦病毒：三分之一郵局改採人工作業

〔大紀元5月3日報導〕(據中廣新聞報導)中華郵政今天上午十點，首度遭名為「殺手：Sasser」的電腦病毒大規模入侵！有近三分之一郵局電腦停擺，改採人工作業！中華郵政表示：包括大台北地區合計有四百二十個郵局電腦無法開機，不過，包括郵局的主機以及ATM自動櫃員機沒有受到影響！郵局目前正在還在全力防堵以及搶修當中！（圖說：中華郵政三日因電腦終端機受到病毒入侵，導致部分支局的終端機無法與主機連線，通匯、提款業務受到影響，無法正常作業。）

週一一大早趕著到郵局辦事的民眾都得大排長龍！原因是上午十點前後，各地郵局櫃檯使用的電腦陸續發生無法開機的現象，經緊急研判是：應該是遭到了微軟才剛剛公布，來自歐洲，威力強大的W32.sasser，所謂的殺手病毒入侵！

中華郵政資訊處長陳賜得表示：初步統計，包括大台北地區有多達三百個支局的終端電腦全部中毒無法使用，其他包括台中、高雄、基隆等縣市還有120個支局也中毒，終端作業無法運作的情況下，包括儲匯郵遞等等作業，都只能改採人工處理。至於沒有受到影響的縣市包括苗栗、台東，以及屏東，受病毒災情波及的郵局達到三分之一左右！

陳賜得強調：郵局的內部的電腦以及主機都是屬於封閉系統，因此不會中毒，此外，郵局各地的ATM自動櫃員機也沒有受到影響。

至於何時修復，陳賜得表示：郵局與防毒公司的工程師還在搶修當中，希望堵住病毒入侵的入口，此外，終端機中毒的數量也相當多，修復還需要一段時間。

現今資訊安全的問題-懷恨復仇

(中央社記者陳舜協台北十四電)刑事局偵九隊今天上午宣佈偵破一起電腦惡客案，原任職台北市敦化南路某貿易公司資訊主管的男子許知野，因不滿公司懷疑他離職後蓄意破壞公司電腦網路系統，索性冒用朋友帳號侵入公司電腦，刪除客戶訂單、系統程式等電腦檔案五千多筆。許知野目前已被依毀損及詐欺罪嫌移送法辦。

警方表示，許知野(男，五十四年次)是國外某大學電腦研究所的肄業生，原本擔任受害公司的資訊主管，但因故在去(九十一)年九月間被受害公司開除，因受害公司的網路系統在許離職後常常發生問題，使得受害公司因公司電腦網路問題而必須常與許知野聯絡。

警方說，根據許知野供稱，因受害公司就網路系統問題向他詢問時，極道上似乎懷疑網路系統是因他蓄意破壞才無法順利運作，他自覺遭人誤解而感到非常氣憤，因此才在去年十月間多次在無人上班的深夜時間，冒用友人帳號上網，再以一般帳號密碼侵入受害公司電腦，刪除公司訂單、成本分析、報價單等各部門資料共五千餘筆，使公司大部份部門電腦系統失效並造成重大損失。

現今資訊安全的問題-社會案件

客戶資料盜賣日益嚴重



中時電子報

12. 中遠行張 社會綜合 910523

銀行員染「毒」盜賣大量客戶資料

文森玲、陳鳳唇／台中報導、游育華、洪川成／台北報導 華人巨資被盜一案震憾電子商務銀行上層不肖員，盜賣客戶資料移轉香港後，連捲竹聯大哥高大成及世華銀行業翁翁等被捕。昨天又在緝捕荷蘭銀行信川卡部員工堵大正，四海奇堂主黃志輝和其多之手下，警方依守古諺，該犯匪集區自去年十二月起利用偽卡盜刷犯案，受害又多達三十人。

中時電子報

17. 中國時報 焦點新聞 910620

漏堵一台電腦還可能會中毒

張景旨／今花報導 瘋風變種病毒利用微軟視窗漏洞攻擊，十九日首次造成上百家企業，數千台電腦中毒。趨勢科技部院長指出，企業裡只要有一台電腦沒有將漏洞堵起來，中毒電腦非會不斷發送封包，將毒傳給沒有補漏洞的其他電腦，直到網路塞滿為止。目前瘋風病毒共有A、B、C、D四種病毒，交叉感染往來，所以中毒的企业網管人員才會那麼忙亂。

疾風病毒
造成數家行庫
行內中斷連線

Internet的實際案例-網路釣魚(假)

The screenshot shows a web browser window with the following details:

- Address Bar:** Displays the URL <http://www.cheng-fan.com/MEx/2.htm>, which is highlighted with a red circle.
- Toolbar:** Standard browser toolbar with icons for back, forward, search, and file operations.
- Menu Bar:** Shows links to various government departments like 聯發公司 (Lianfa Co.), First Law Systems, Information Security, TWENTIETH, 資訊安全政策、規範與, and 經濟部中部辦公室 (Central Region Office).
- Header:** Features a banner with flowers and the text "經濟部中部辦公室" (Central Region Office, Ministry of Economic Affairs) and "Central Region Office, Ministry of Economic Affairs".
- Navigation:** Includes links for 首長信箱 (Chief Executive's Mailbox), 政風業務 (Ethics and Integrity), 意見交流 (Feedback), 網站導覽 (Website Navigation), and other administrative links.
- Content Area:** A form titled "公司登記" (Company Registration) for querying company information. It includes fields for 統一編號 (Unified Number) (filled with 70594200), 公司名稱 (Company Name), 負責人 (Responsible Person), and two buttons at the bottom: "查詢" (Query) and "清除" (Clear).
- Left Sidebar:** A green sidebar with a list of links including: 本室介紹, 组织架构, 制度公告, 申辦流程, 行政中心, 行业登记(劳工考核), 公司登记, 市場及典故辅导管理, 商業行政, 電子下單, 為民服務, 向善行政, 留言板, and 回首頁.

Internet的實際案例-網路釣魚(真)

Internet的實際案例-網路釣魚(真)

http://www.cetnrae.gov.tw/04/03a_01.asp

經濟部中部辦公室
Central Region Office, Ministry of Economic Affairs

首長信箱 政風業務 意見交流 網路資源 網站導覽

工業行政 行業登記(匠工考驗) 公司登記 市場及攤販輔導管理 商業行政

本室介紹
組織職掌
訊息公告
申請業務
工业行政
行业登记
(匠工考驗)
公司登记
市場及攤販
輔導管理
商業行政
表單下載
為民服務
回首頁

申請業務 ■ 公司登記

公司登記案件查詢

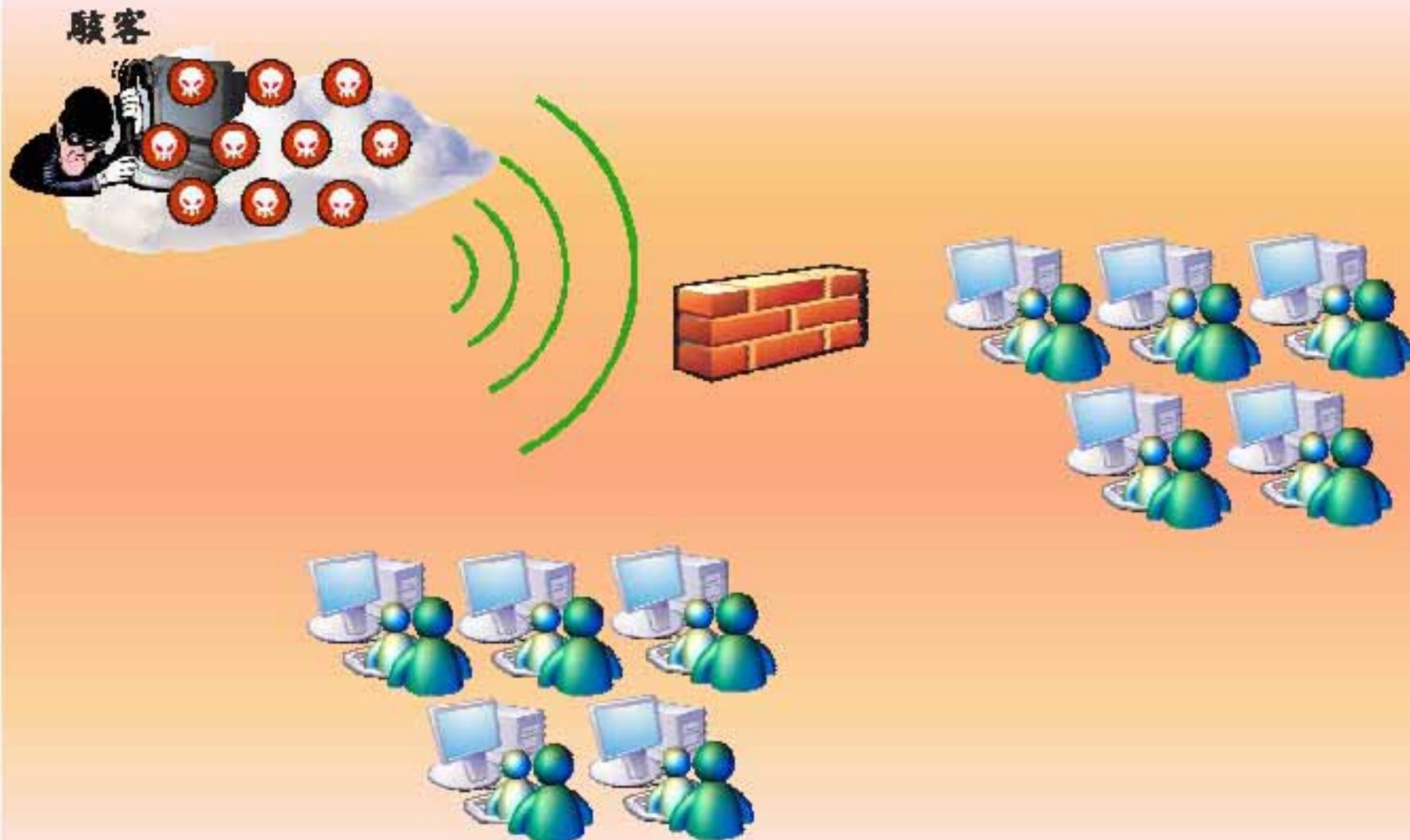
請輸入查詢條件！

統一編號：
文 號：
預查號碼：
公司名稱：

查詢

查詢規則：

系統弱點攻擊



Internet的新威脅—MSN, skype..

躍升三倍：IM病毒今年大流行

CNET

黑客盡情利用即時訊息進行攻擊入侵企業及其僱員的電腦

IE

根據

ICC

這比

持每

由於

嚴重

Me:

Web

[200
訊息和
升三倍
(NASD
Edition
的辦公
共IM
種通訊

IM的風
全球消
會帶來
過傳送
他更廣

黑客專釣Yahoo即時通訊

病毐快報／MSN病毐散播 強迫你上色情網站

2003/09/23 10:51

釣魚信
料。

本週四
向Ya
求用戶

用戶才
夠存取
表。



MSN射手病毒，透過MSN瘋狂傳播。
(圖／射手病毒透過MSN瘋狂傳播)

記者 許瑜菁／編譯

使用微軟即時傳訊軟體MSN Messenger可能要小心了，最近有一種名為「MSN射手」的病毒透過MSN傳播，並拖慢網路傳輸速度。

這支病毒名為Smess，是去年7月出現的Simmen病毒變種，南韓中央日報指出，它會在遭感染的電腦內，搜尋MSN的聯絡人名單，發送名為SMB.exe的檔案，雖然這種病毒不會直接造成電腦損毀，但是會導致網路連接速度變慢，系統資源遭到佔用，嚴重影響用戶的上

網速度。

電子郵件攻擊

<http://www.yahoo-tw.com>
yahoo@yahoo.com.tw

寄送經過設計的e-mail, 夾帶惡意程式的附件進行後門植入的攻擊, 或者蓄意假造位址, 寄送垃圾郵件

駭客



Internet的新威脅—垃圾郵件

新華社
國際網安警報
INTERNATIONAL



**東日本太子
自拍事件**
台灣素人影像藝術
露毛自拍裸文入鏡，三百張以上！！！
景點遍及台北捷運、內湖科技園區、
市府周邊、西門電動天橋、東湖別墅區、
知名美術館、K書中心、無一倖免。
裸露模擬演出 全三冊（附原聲CD）
NT.888元
為免爆動、總量 **500** 冊管制中。

網路都是誰在用???

檢討方式 開關鍵字 檢查選項: 全部群組 第 1 頁 / 共 86 頁 (共 2566 筆資料) 全選 反選 刪除 重送 轉寄

Spam SQR

郵件記錄 郵件設定 政策管理 DoS 防禦 透過名單 透過條件 檢視信件數關鍵字設定 郵件標註 郵件回收 統計報表 系統設定

統計報告

2005 11 03 郵件分類統計

類別名稱	標註(標記)郵件(封)	標註(標記)郵件(KB)	未標註(標記)郵件(封)	未標註(標記)郵件(KB)	總次數(封)	總流量(KB)	總次數(封)
肉品促銷類	00	2106	11	505	94	2642	1.05%
漢藍美容類	8	233	13	1125	21	1423	0.82%
Sex 色情類	295	3756	39	1411	334	5177	12.98%
電子報	118	1430	37	471	148	1951	5.75%
金融理財	175	2713	35	1453	210	4203	0.16%
法律類	267	4151	45	972	313	5133	12.16%
名產行銷行銷類	87	730	20	420	107	1210	4.15%
求職類	10	130	0	0	10	180	0.39%
其他廣告類	110	21152	21	870	513	24857	21.1%
民地直銷類	33	245	-	5	34	250	1.32%
是非八卦類	34	117	3	22	37	139	1.44%
旅遊類	67	1725	7	70	74	1000	2.86%
告銷類	33	2735	3	730	41	2120	1.59%
病毒情報類	20	144	2	3	22	152	0.86%
疑似病毒行銷類	62	9311	7	153	69	7081	2.66%
健康醫療類	50	170	20	120	70	505	2.84%
愛情婚姻類	21	136	2	3	26	221	1.01%

Internet的新威脅—無線網路

無線盜波惹禍？銀行推動態密碼及網路ATM最安全

2005/01/13 12:31

記者胡秀珠／台北報導

針對刑事警察局首度破獲利百「無線盜波」盜接上網、入侵網路銀行的盜領案一事，國內銀行業者指出，事實上，為防護網路銀行的安全機制，銀行積極推動動態密碼、網路ATM等，安全機制有相當大功用，此外，銀行公會也通令銀行，網路銀行不得接受非約定帳戶轉帳。銀行主管強調，要強化交易安全，最重要的是客戶勿使用生日等「懶人密碼」，並勿亂填問券等，才能確保自己的個人資料不外洩。

銀行資訊室主管指出，不管是有線寬頻或無線寬頻，都只是上網的管道之一，重要的是客戶個人資料的保密最為重要。目前銀行在網路銀行的使用上有三層確認作業，一是客戶的身份證代號、二是自己命名的代號、三為客戶個人設定的密碼。

銀行業表示，有不少非法集團利用假網站進行「網路釣魚」，竊取客戶的個人資料，持卡人應提高警覺，確認網站的真實性。



新聞快
討論 | 聊天

相 閱

匯豐銀
熱氣球

立院協
100年起

中信銀
貿易融

中華銀

Internet的新威脅—無線網路

盜盜波犯案 飄忽難追蹤

刑事局偵九隊隊長李相臣於去年八月間，接獲國內某銀行報案，指稱該銀行遭受偽卡盜刷攻擊，致損失慘重，遂要求該隊偵三組組長孔令果率員偵辦，警方數度追蹤其 I P 位址，發現歹徒上網地點飄忽不定，始知歹徒是盜用無線網路盜波上網犯案。

經連月追查，好不容易才確認住台中的林啓順涉有重嫌，昨天將林啓順、女友曾莉莎（卅一歲，中國籍女子）、鄧莞真（二十八歲）、凌嘉聲（二十八歲，詐欺通緝）帶回偵辦，警方並在林嫌住處頂樓 **查扣一根六公尺長的「無線網路盜波捕捉器」**。

警方發現，林嫌經不斷測試發現中國信託商銀網路銀行的登入機制，可以任意四位數字測試帳號、密碼，一旦成功進入，便可取得網路銀行客戶的姓名、身分證字號、銀行帳號、存款金額、信用卡卡號、約定轉帳戶等資料，再透過安全認證憑證的系統漏洞，成功突破認證程序進而盜領存款。

另一方面，林嫌取得信用卡卡號後，因缺少信用卡的有效年月期限，會再連上發卡銀行網站，以測試出有效年月，等到手後就冒用大肆盜刷，有十多家銀行受害。

Internet的新威脅—移動式系統

專家警告發現可摧毀作業系統手機病毒

【大紀元4月8日訊】由芬蘭一家資訊安全公司發現一名為“FONTAL.A”手機新病毒。專家警告：這是一種能摧毀手機作業系統的木馬病毒，可完全摧毀作業系統。

據美國《連線》雜誌網站4月6日報道，“FONTAL.A”手機新病毒，它能通過手機文件共用或因特網聊天向手機作業系統植入惡意文件，使手機下次啟動時因作業系統崩潰而失敗。並能破壞手機作業系統的程式管理器。

資訊技術安全專家稱，目前這種病毒只感染安裝了“辛比安”作業系統的諾基亞手機。並表示要徹底消除這種病毒，只有將手機記憶體格式化並重新安裝作業系統，這將使許多重要的資料喪失。

早前，美國賽門鐵克公司和國際商用機器公司等資訊技術巨頭都會預言，伴隨智慧手機不斷推廣，手機病毒將成為資訊世界的一大禍患。

議題

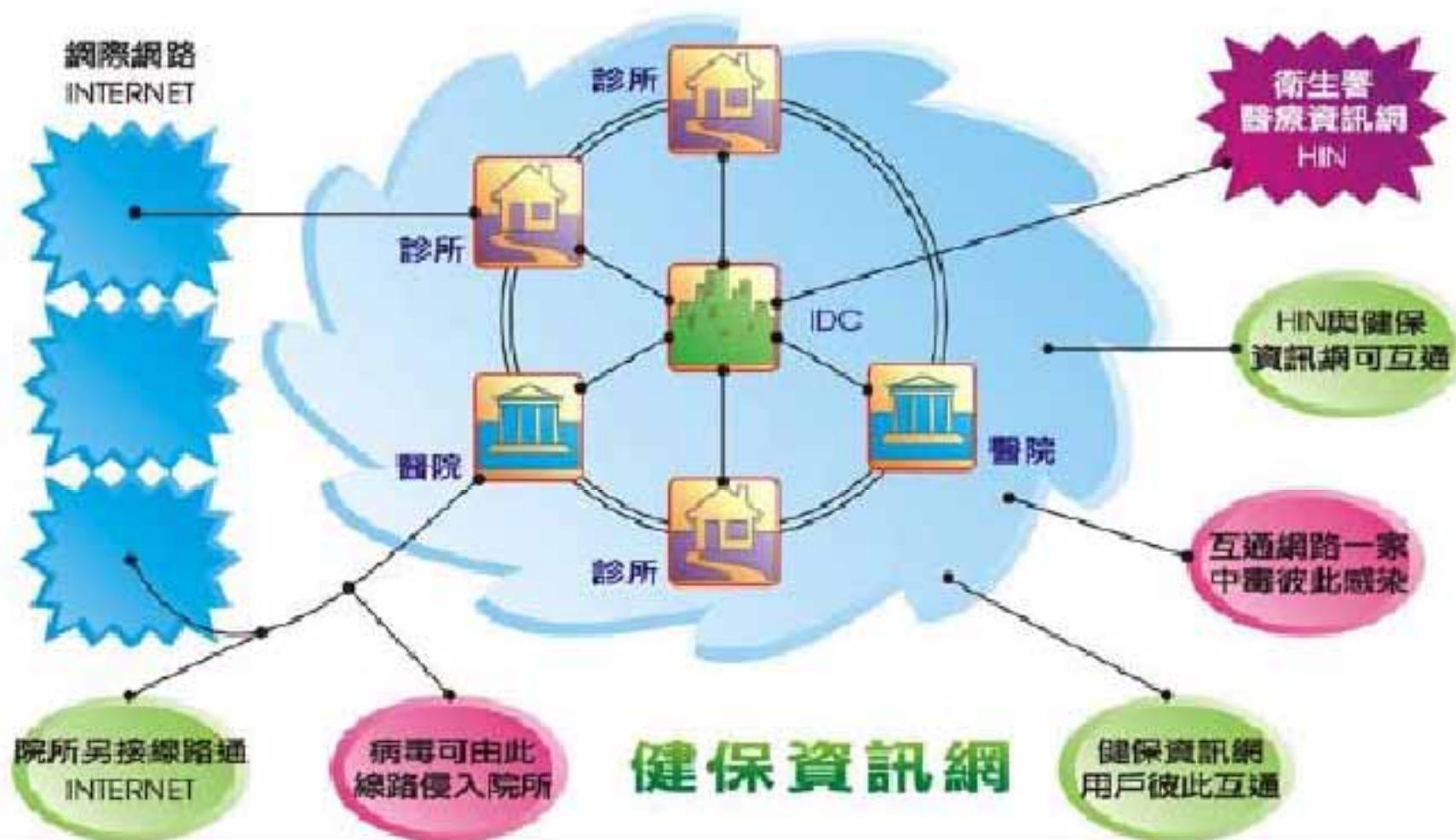
- ◆ 資訊安全的現況
- ✓ 資訊安全的觀念
- ◆ 資安的政策推行



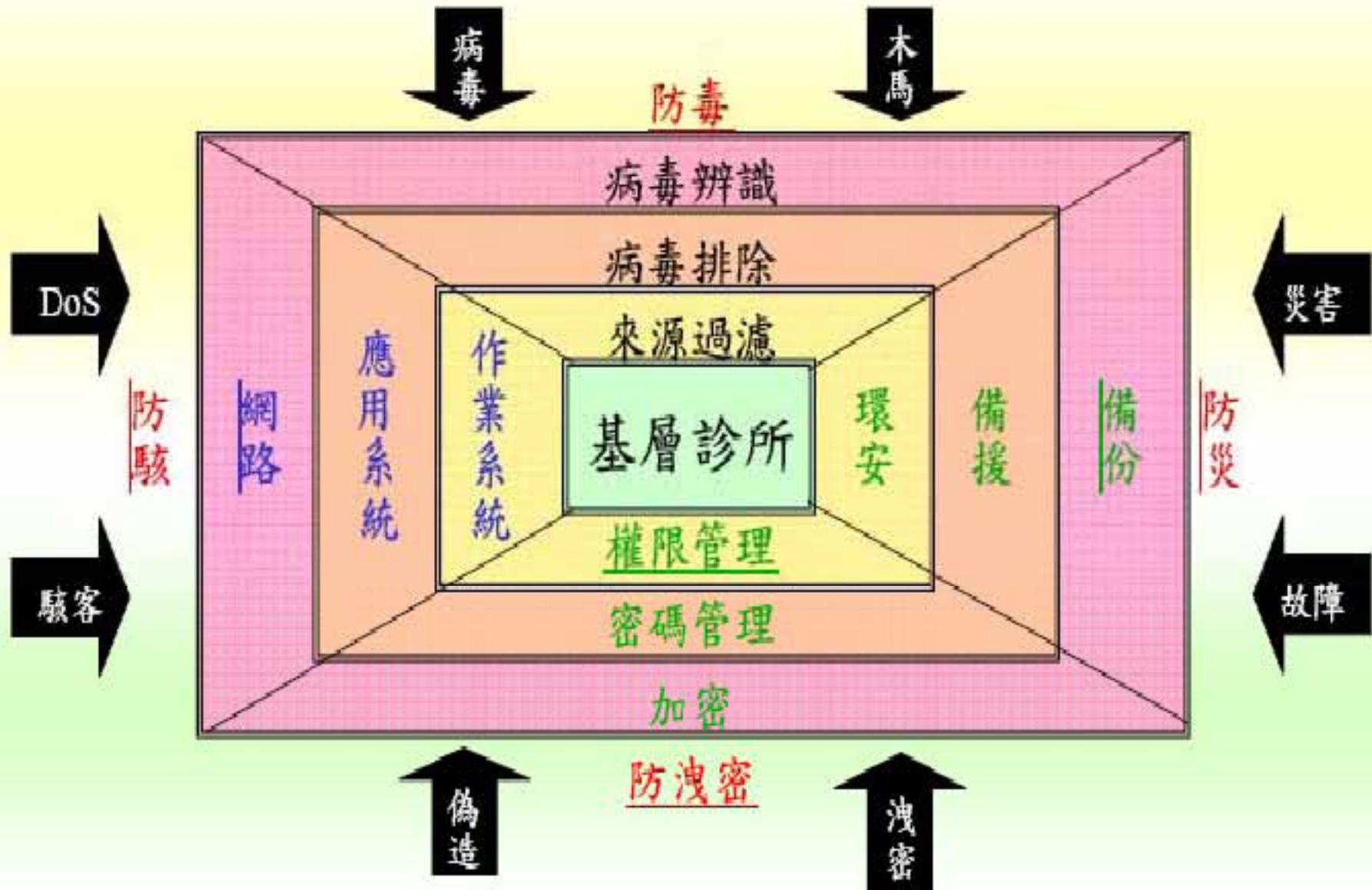
該有的觀念…

- ◆ 資訊的「重建」比「建立」更要曠日費時：一有安全漏洞而讓駭客或病毒等威脅有機可乘，皆可能造成整個企業的癱瘓。
- ◆ 機密文件操作人員若要離開座位，要先進行登出（Log Out），待回到座位再登入（Log In）
- ◆ 所設定的密碼，一定要以字母、數字與特殊符號加以組合；每一個使用者定期要更換Password，否則就會無法登入系統。
- ◆ 員工報到所給的帳號，允許員工傳送與接收Mail，以及使用ERP等應用系統，當其離職後，則應收回所有許可....等相關規定。
- ◆ 除了各項耳提面命外，對員工進行教育訓練不可少。
- ◆ 最重要的就是企業由上到下的全力貫徹。

健保資訊網資安事件的來源



基層診所資訊安全範圍



醫療院所應有的資安態度

- 架設如IP分享器或**防火牆**等，管制內外連線，藉以隔離院所內部網路與健保資訊網、Internet
- 不讓他人在遠端以**數據機**連入(或需被控制及記錄)
- 儘量不要使用**資料夾共享**(或需設定密碼)
- 採用安全掃描工具，定期進行**弱點掃瞄**
- 限制使用者的在合理的**作業時間**內連線
- 設**入侵偵測**系統，特別留意來自內部的攻擊行爲

資訊安全的目標



所謂安全的標準(HIPAA & BS7799)

BS7799資安管理十大領域



A.3資訊安全政策 (Security Policy)

A.4資訊安全組織 (Security Organization)

A.5資產分類與控管 (Asset Classification & control)

A.6人員安全管理
(Personnel
security)

A.7實體環境安全管
理 (Physical
Environmental
Security)

A.8通訊與操作維護
(Communications
& Operations
Management)

A.10系統開發與維
護 (System
Development &
Maintenance)

A.9存取安全控管 (Access Control)

A.11營運持續管理 (Business Continuity Management)

A.12符合性 (Compliance)

複雜的資訊安全技術

網路安全產品

- Firew
- Pers
- Intru
- - Ho
- - Ne
- - Hc
- Wire
- All-in-
- (AP)
- othe

內容安全產品

評估與稽核產品

- Vulnera
- Forensic
- Log ana
- others
- others

加密產品

存取控制授權產品

- IF
- S
- P
- C
- C
- Aut.
- Ident
- Aut.
- Str



資安管理產品

委外服務類別

- Managed security services
- IS auditing consultants / services
- Business continuity planning / services

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

•

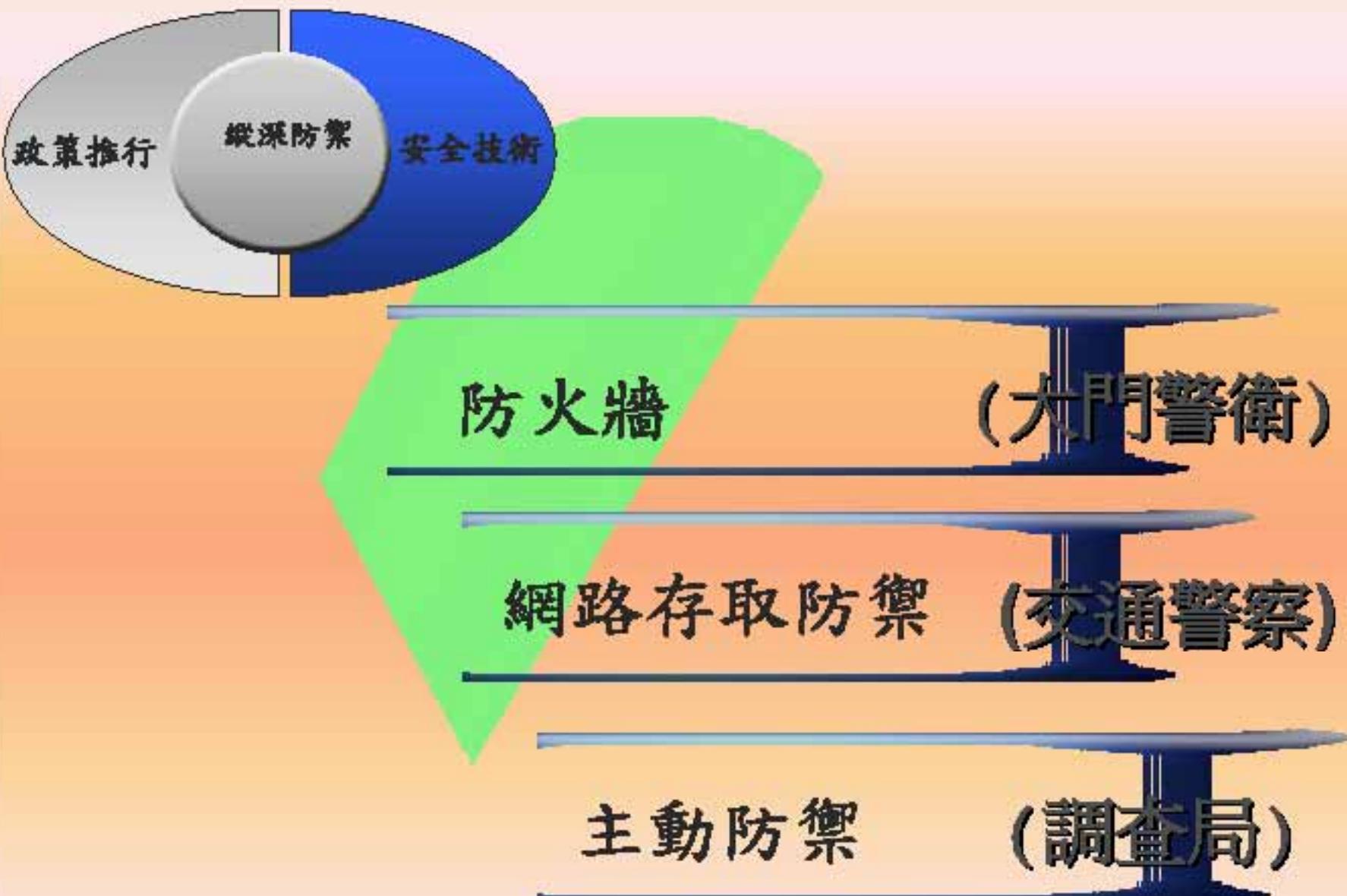
•

•

•

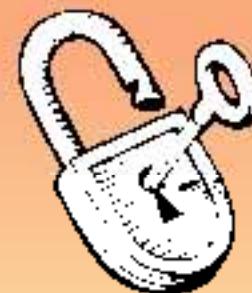
•

我們該知道的基本知識

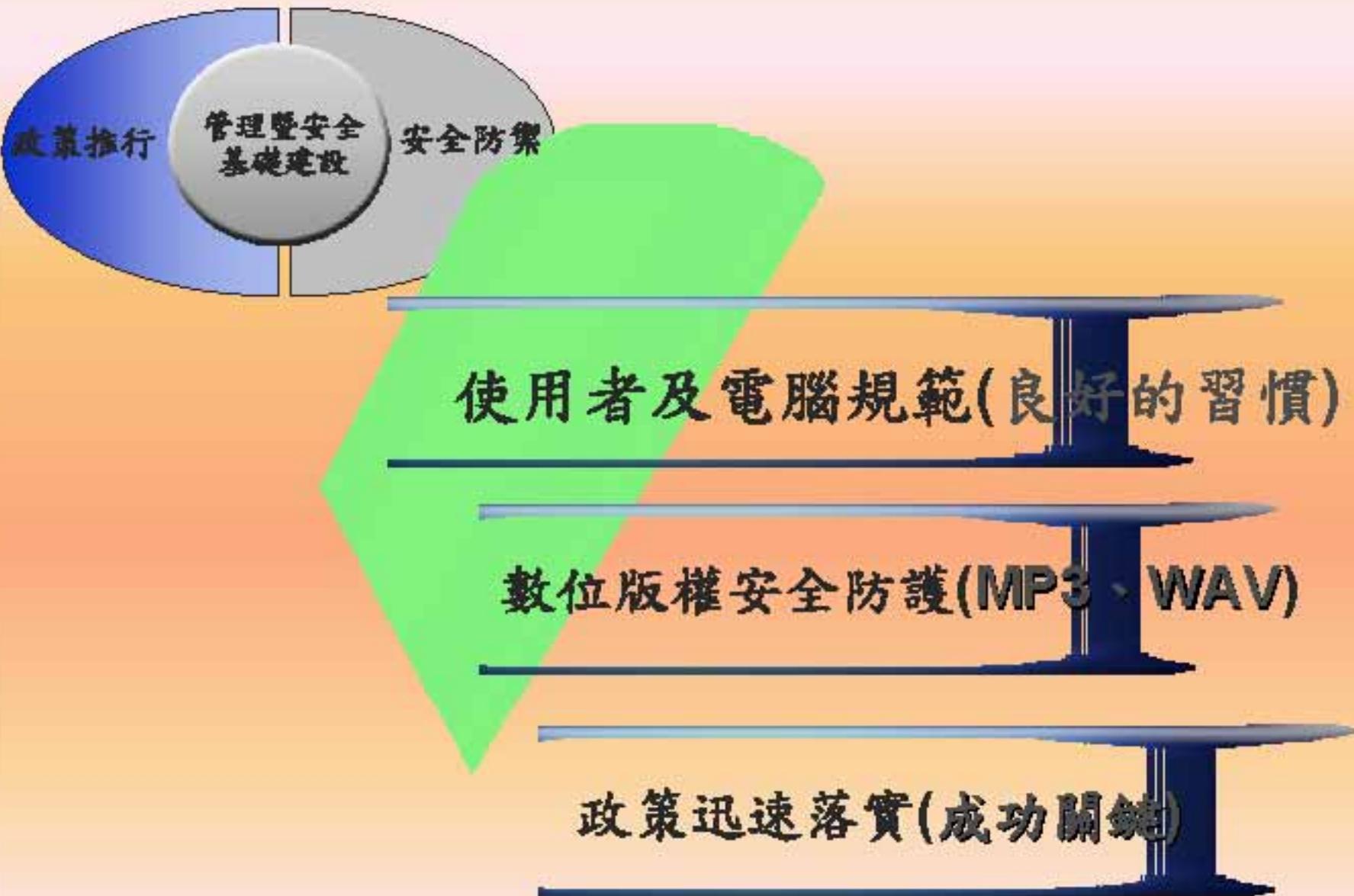


議題

- ◆ 資訊安全的現況
- ◆ 資訊安全的觀念
- ✓ 資安的政策推行



政策推行



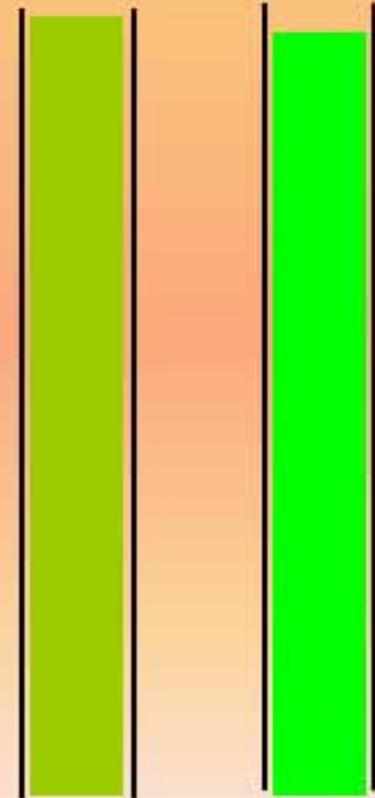
使用者及電腦規範

有效貫徹 IT 政策



使用者
滿意度

執行效率
及成效



實例應用(I) - 使用者及電腦規範

範例: Strong Password 原則



密碼複雜性：

1. 不得少於8個字元
2. 必須包含大小寫字母
3. 每3個月更新一次
4. 前24次不得重複

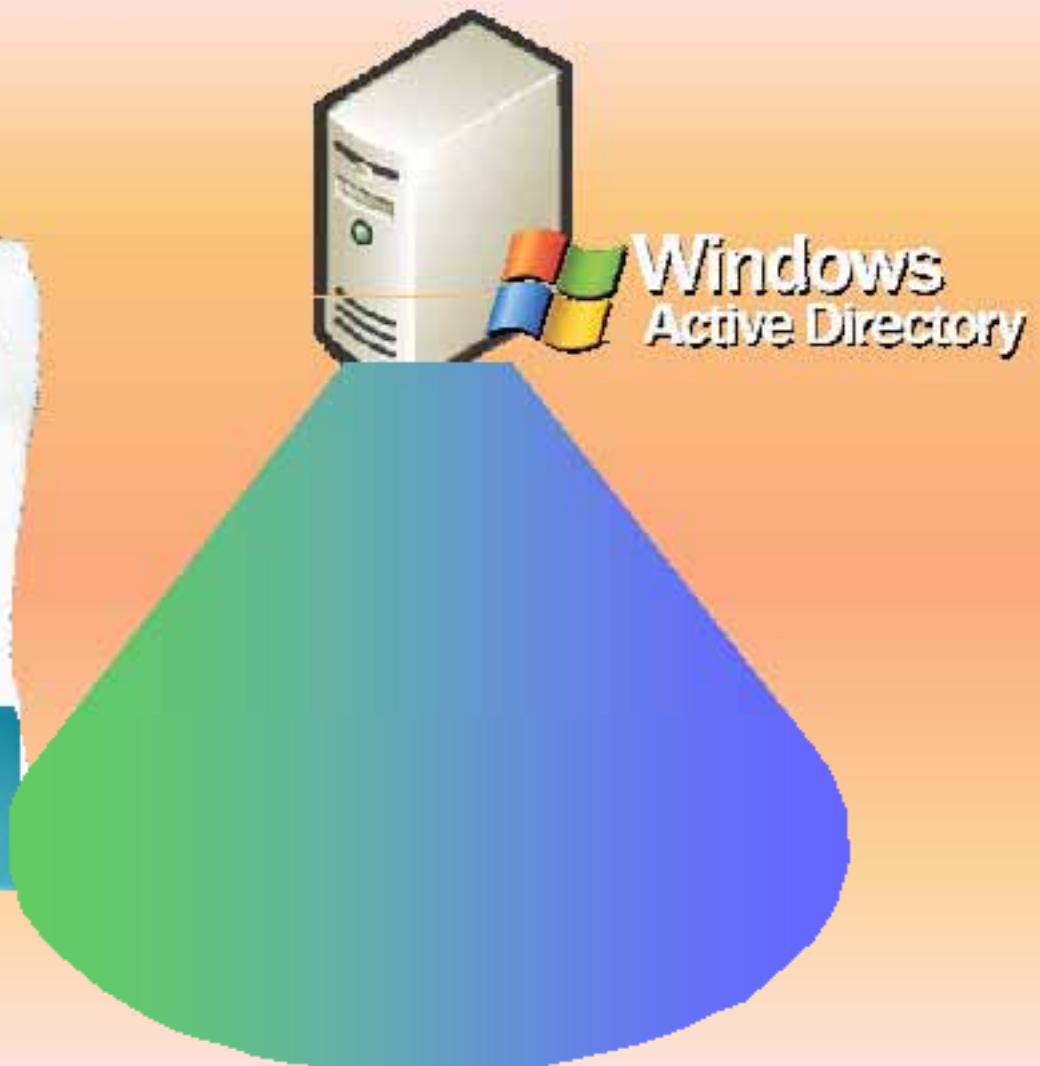
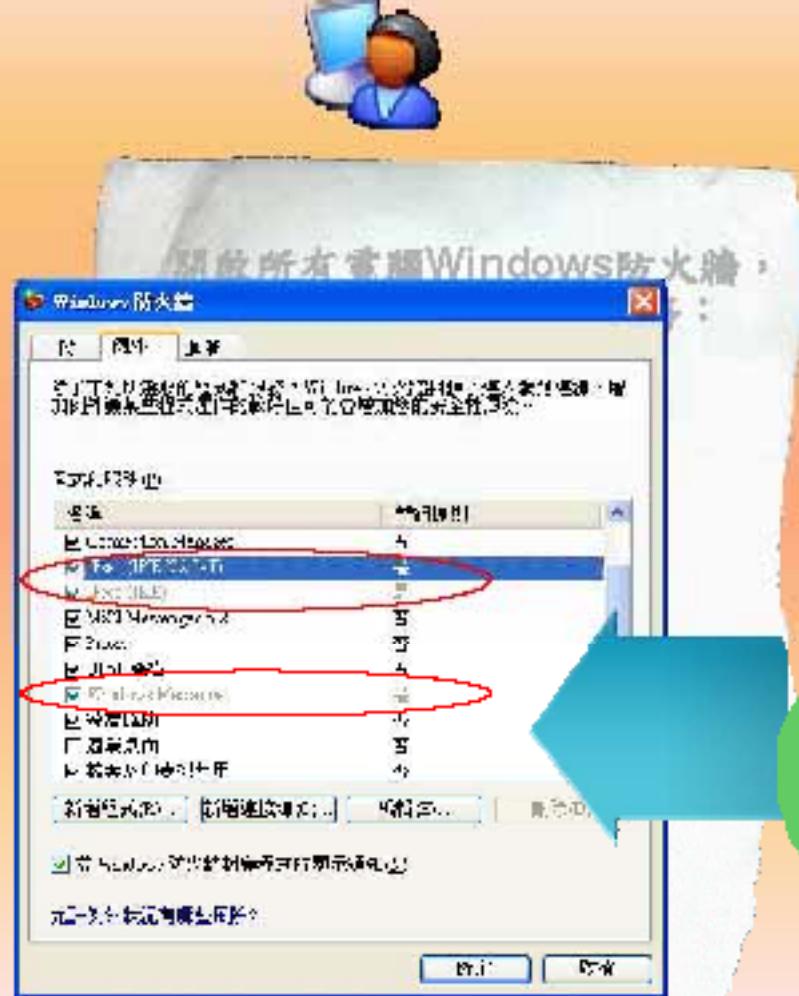


Windows
Active Directory



實例應用(II) - 使用者及電腦規範

範例：啟動個人電腦防火牆原則



實例應用(III) - 使用者及電腦規範

範例：更新程式或防毒軟體原則



所有Windows XP電腦登入後，
到下列位置執行SP2安裝：
\\Share\\Upgrade\\SP2\\Setup.exe



Windows
Active Directory



XP
SP2

實例應用(IV) - 使用者及電腦規範

範例：限制使用者複製檔案至隨身碟原則



VMware

將以下的值加入選定電腦的Registry內，來阻止使用者將檔案複製到隨身碟上。

\Windows\Distribution\Editor Version 5.00

- 桌面
- 我的文件
- 我的電腦
- Windows XP (C:)
 - Local Disk (C:)
 - DVD-RAM 隨碟機 (D:)
 - DVD 半碟機 (E:)
 - 刪除式媒體 (F:)
- 控制台
- 網路上的老師
- 資源回收筒
- Arvixe
- Fox
- Info Web Download
- Pipeline JSSS & CMS
- Pipeline Status for YingPo
- Project Desktop Inf Area
- Shortcuts

- test
- CCP_01
- DISK_X801
- DFIT_5.113
- keyH
- 數位資產安全防護研究(Risk) app

\Set\Control\StorageDevicePolicies]



謝謝大家!!!