SYSCOM

# 個資安全整合解決方案

## 由管理制度到資訊安全

主講人：張義明

凌羣電腦 THE SYSCOM GROUP

CMMI 5 Maturity Level Software Group

# 由罰則來看個資法

- 第四章　損害賠償及團體訴訟
  - 第二十八條 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。但損害因天災、事變或其他不可抗力所致者，不在此限。被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。 依前二項情形，如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，以每人每一事件新臺幣五百元以上二萬元以下計算。 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

# 由罰則來看個資法

- 第四章　損害賠償及團體訴訟
  - 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。依前項規定請求賠償者，適用前條第二項至第六項規定。

# 由罰則來看個資法

- 第五章　罰　　則

| 個資法 | 說明 |
| --- | --- |
| 第四十一條 違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。 | 違反個資法在個人資料在蒐集、利用時的規定 |
| 第四十二條 意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。 | 資料正確性的規定 |

# 由罰則來看個資法

| 個資法 | 說明 |
| --- | --- |
| 第四十七條 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：<br>一、違反第六條第一項規定。<br>二、違反第十九條規定。<br>三、違反第二十條第一項規定。<br>四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。 | 一、收集特種個資。<br>二、非公務機關對蒐集個資的規定<br>三、特定目的外的利用。<br>四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。 |

# 由罰則來看個資法

| 個資法 | 說明 |
| --- | --- |
| 第四十八條　非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣(市)政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：<br>一、違反第八條或第九條規定。<br>二、違反第十條、第十一條、第十二條或第十三條規定。<br>三、違反第二十條第二項或第三項規定。<br>四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 | 一、違反告知事項<br>二、查詢、提供閱覽或製給複製本、請求更正或補充<br>三、 拒絕接受行銷時，應即停止利用其個人資料行銷。<br>四 、個人資料被竊取、竄改、毀損、滅失或洩漏 ，未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 |

# 由罰則來看個資法

| 個資法 | 說明 |
| --- | --- |
| 第四十九條 非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣二萬元以上二十萬元以下罰鍰。 | 對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。 |

- 第一項:中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時。
- 第二項: 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

# 房仲洩個資 5千求職者受害

## 房仲洩個資 5千求職者受害

2011年08月17日 讚 0 +1 0

王先生收到信義房屋致歉信，坦承作業疏失。

【投訴組／台北報導】信義房屋總公司驚傳將今年1月至今的5000筆求職者履歷資料，夾帶在電子郵件中寄出，已寄出200多封，求職者的姓名、性別、出生年月日、聯絡電話一覽無遺，有外洩求職者個資之嫌。對此，信義房屋總公司坦承，承辦人員誤將求職者資料夾帶在電子郵件中寄出，已立即停止寄發，並予懲處。律師表示，民眾可依《個人資料保護法》請求損害賠償。

### 已寄200多封電郵

王先生說，他7月初到信義房屋應徵工作，8月8日收到信義房屋寄出的未錄取通知電子郵件，開啟電子郵件夾帶的檔案，內容竟是近5000筆求職者的個人資料，其中也包含他的資料，讓他相當震驚，隨即向信義房屋反映，雖然信義房屋有道歉，他仍無法接受，抱怨「萬一資料外流遭人盜用怎麼辦？」

新聞圖片來源：蘋果日報

# 當事件發生在個資法生效後

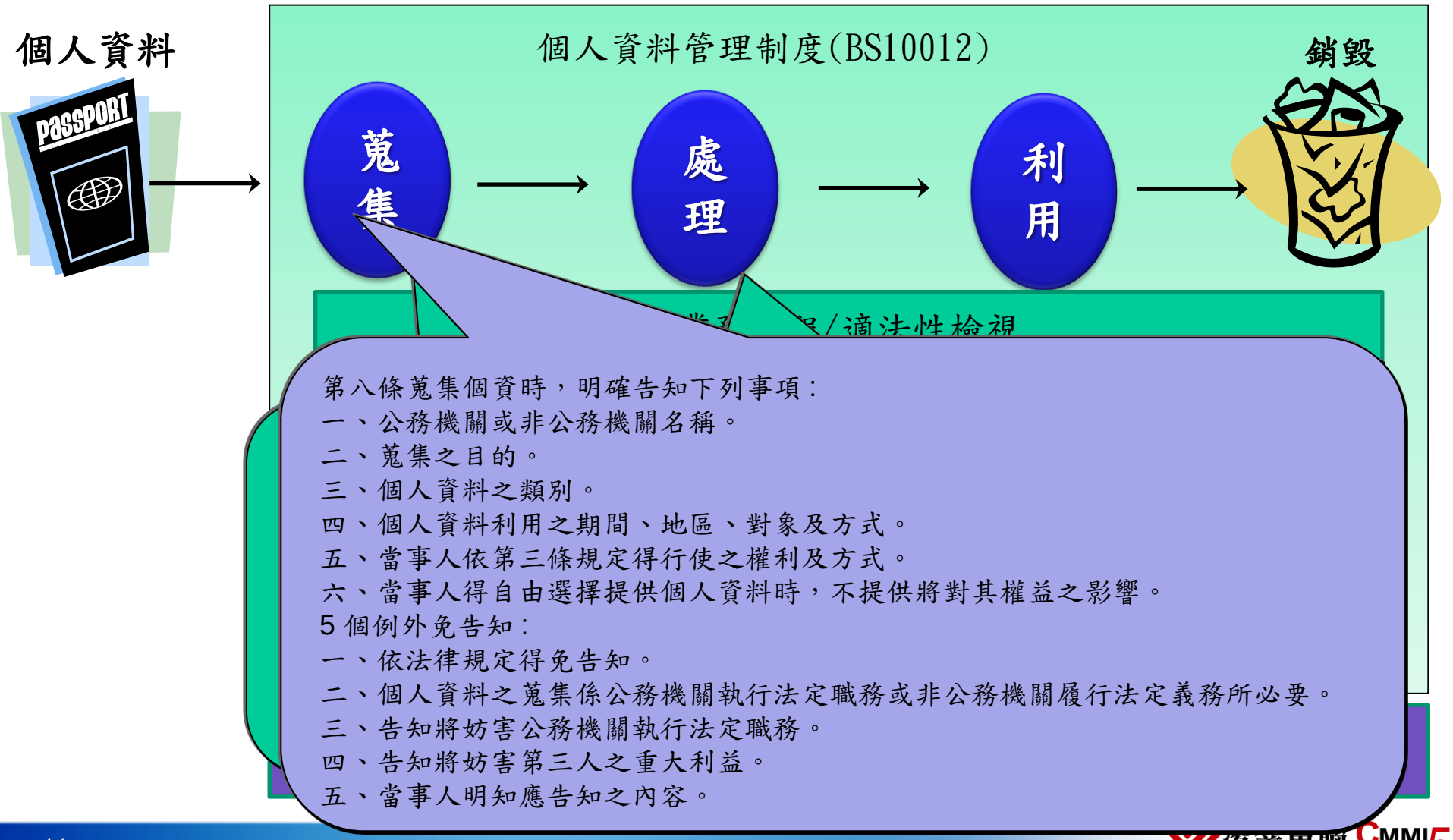
| | 罰則<br>(每件500～20,000) | 行政裁罰<br>(縣市政府/主管機關) |
|---|---|---|
| 房仲業者 | 2,500,000～<br>100,000,000 | 個資法第48條<br>二萬元以上二十萬元以下罰鍰 |

- 第五十條 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。
- 如有其他原因，可能須負刑事責任

# 如何因應個資法

- 讓公司現行跟個資有關的業務合法，並持續保持
- 讓公司新增跟個資有關的業務合法，並持續保持
- 確保資料安全

# 由資料生命週期談個資因應



# 適當安全維護措施

- 施行細則第十二條 定義適當安全維護措施、安全維護事項、適當之安全措施
  - 一、配置管理之人員及相當資源。
  - 二、界定個人資料之範圍。
  - 三、個人資料之風險評估及管理機制。
  - 四、事故之預防、通報及應變機制。
  - 五、個人資料蒐集、處理及利用之內部管理程序。

# 適當安全維護措施

- 施行細則第十二條 定義適當安全維護措施、安全維護事項、適當之安全措施
  - 六、資料安全管理及人員管理。
  - 七、認知宣導及教育訓練。
  - 八、設備安全管理。
  - 九、資料安全稽核機制。
  - 十、使用紀錄、軌跡資料及證據保存。
  - 十一、個人資料安全維護之整體持續改善。

# 由了解個資業務流程與個資位置

| 資產編號 | 流程名稱 | 個人資料檔案名稱 | 資料形式 | 法律依據 | 個人資料之範圍 | 有否特種資料？何種？ | 蒐集 | | 處理 | 利用 | | | 保存 | | 銷毀 | 揭露 | | | 衝擊值 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | 單位 | | 單位 | 期間 | 地區 | 對象 | 目的 | 單位及 | | 方式 | 個人資料之範圍 | | |
| V0-DA-004 | 客戶使用帳號維護) | 基料檔客戶資本 | DA | 無 | 姓名行動電話 | | CSD | | CSD | 合約期間 | 台灣 | CSD | 客戶服務聯絡 | | 存 | | | | 1 |

產出 log

蒐集或處理：非公務機關第 19 條，應有特定目的並並符合下列情形之一者
一、法律明文規定。
二、與當事人有契約或類似契約之關係。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人書面同意。
六、與公共利益有關。
七、個人資料取自於一般可得之來源。

# 利用UC矩陣的概念進行關聯

- U/C矩陣是用來表達過程與資料兩者之間的關係。矩陣中的行表示數據類，列表示過程，並以字母U（Use）和C（Create）來表示過程對資料的使用和產生。
- 將個資清冊中，處理個資的系統利用UC矩陣概念把系統功能與個資行為描述清楚

# 利用UC矩陣的概念進行關聯

系統名稱 :Service Online

| | 建立客戶資料 | 建立服務 | 表單 | 服務表單結案 |
|---|---|---|---|---|
| 工程部門 | | U | U | U |
| 品管中心 | | | | U |
| 業務 | CO/CR/E | | | |

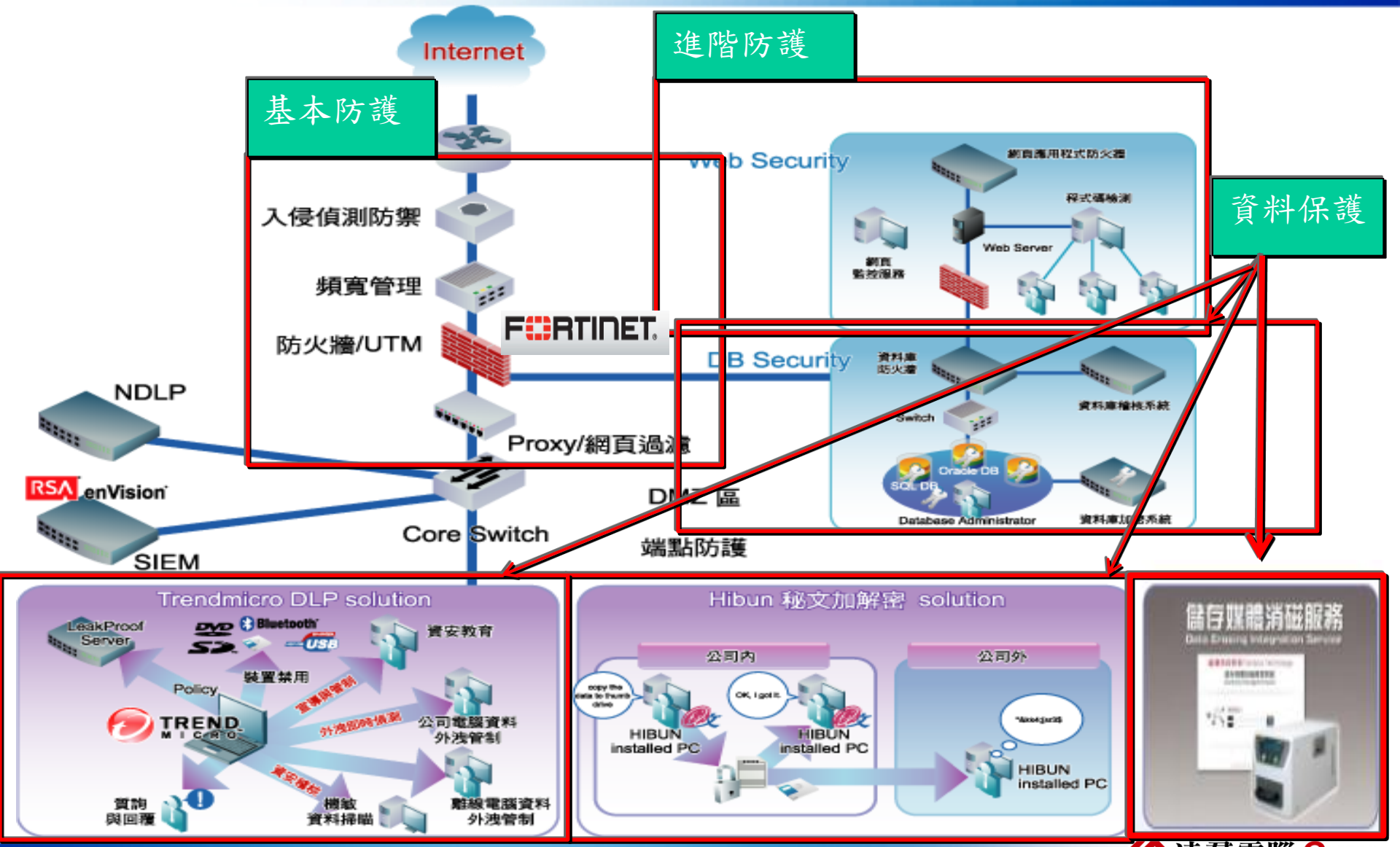
產出 log

授權，產出 log ，資料保護

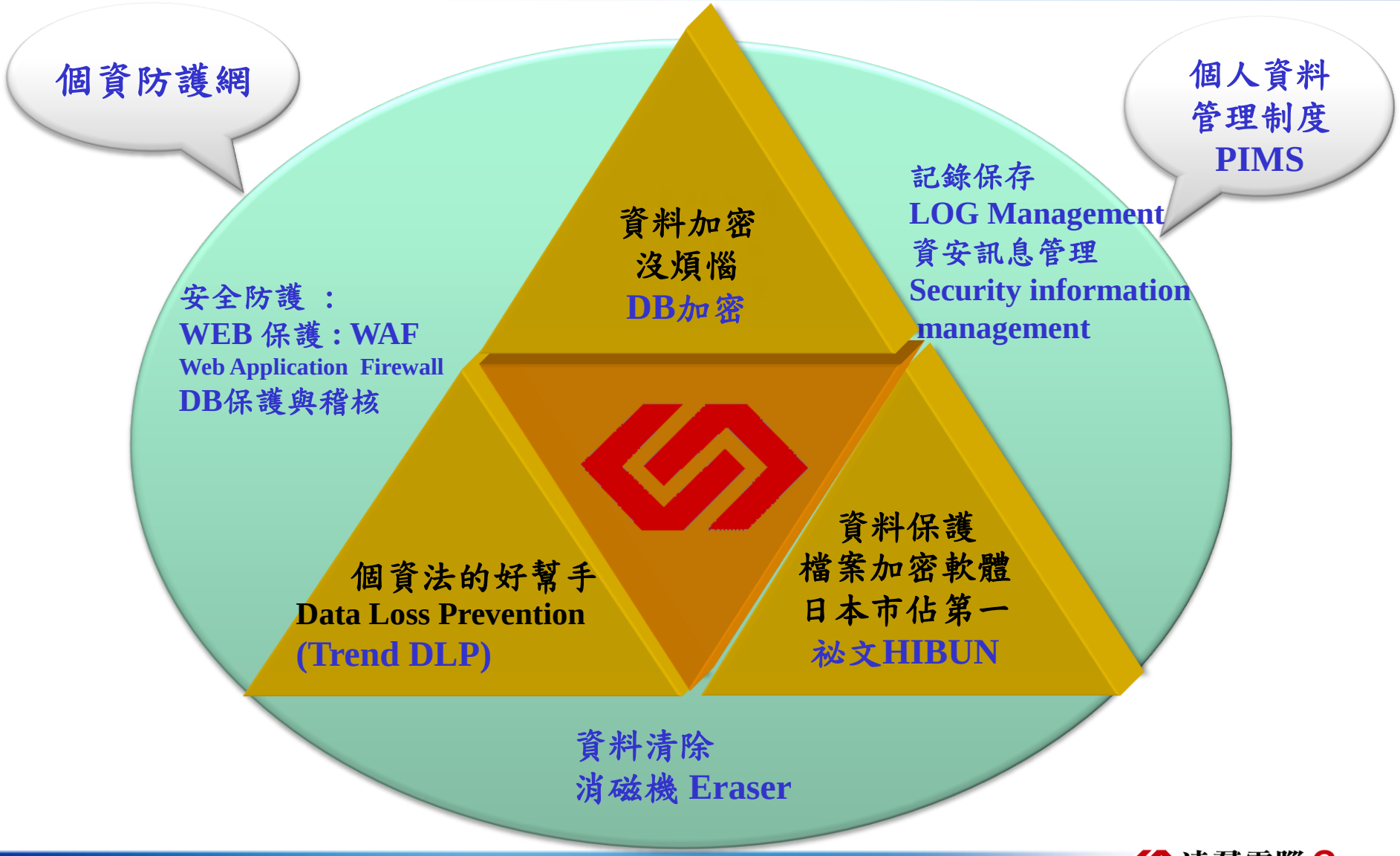
蒐集或處理 ：非公務機關第 19 條，應有特定目的並並符合下列情形之一者
一、法律明文規定。
二、與當事人有契約或類似契約之關係。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人書面同意。
六、與公共利益有關。
七、個人資料取自於一般可得之來源。

- CO :
- S : 儲

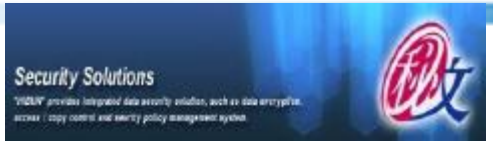
# UC矩陣表示的系統架構示意與資安防護



# 凌羣個資防護網



# 凌羣個資整合解決方案




TREND MICRO™

Hibun

DLP

PIMS

國網法人中華民國國家資訊基本建設產業發展推進會
National Information Infrastructure Enterprise Promotion Association

RSA SECURITY™

SIEM

凌羣電腦
THE SYSCOM GROUP

Log

RSA SECURITY™

DBF

消磁機

ORiENT

iMPERVA®

WAF

DB加密

SafeNet

# 房仲洩個資 5千求職者受害

## 房仲洩個資 5千求職者受害

2011年08月17日 讚 0 +1 0

王先生收到信義房屋致歉信，坦承作業疏失。

【投訴組／台北報導】信義房屋總公司驚傳將今年1月至今的5000筆求職者履歷資料，夾帶在電子郵件中寄出，已寄出200多封，求職者的姓名、性別、出生年月日、聯絡電話一覽無遺，有外洩求職者個資之嫌。對此，信義房屋總公司坦承，承辦人員誤將求職者資料夾帶在電子郵件中寄出，已立即停止寄發，並予懲處。律師表示，民眾可依《個人資料保護法》請求損害賠償。

### 已寄200多封電郵

王先生說，他7月初到信義房屋應徵工作，8月8日收到信義房屋寄出的未錄取通知電子郵件，開啟電子郵件夾帶的檔案，內容竟是近5000筆求職者的個人資料，其中也包含他的資料，讓他相當震驚，隨即向信義房屋反映，雖然信義房屋有道歉，他仍無法接受，抱怨「萬一資料外流遭人盜用怎麼辦？」

新聞圖片來源：蘋果日報

# 原因分析-房仲業者

- 發生原因
  - 因承辦人誤將求職者資料夾帶在電子郵件中寄出
- 問題
  - 針對擁有個資檔案的業務流程是否有標準程序與稽核機制?
  - 是否有資訊技術可協助防止惡意或疏忽的資料外洩?
  - 當事故發生時，是否有足夠的紀錄來舉證?

# 當協助房仲業導入凌羣解決方案後

- 有管理制度協助流程管制與查核
- 有Fortinet的產品做基礎防護
- 有HIBUN祕文將檔案加密
- 有TrendMicro DLP 防止明碼資料外洩
- 有RSA enVision做紀錄保全

SYSCOM

# 個資安全整合解決方案

## 由管理制度到資訊安全

## 經驗分享

主講人：張義明

凌羣電腦 THE SYSCOM GROUP

CMMI Maturity Level 5 Software Group

# PIMS 授證


**《圖說》**凌羣電腦8月20日舉辦《過過PIMS(BS10012:2009)認證暨個資安全整合解決方案記者會》在輔導單位NII吳國維執行長(照片左)見證下，由SGS東亞區國際認證部黃世忠副總裁(照片右)正式頒證予凌群，並由凌群電腦總經理劉瑞隆(照片中)代表接受證書。

# 個資整合解決方案合作夥伴

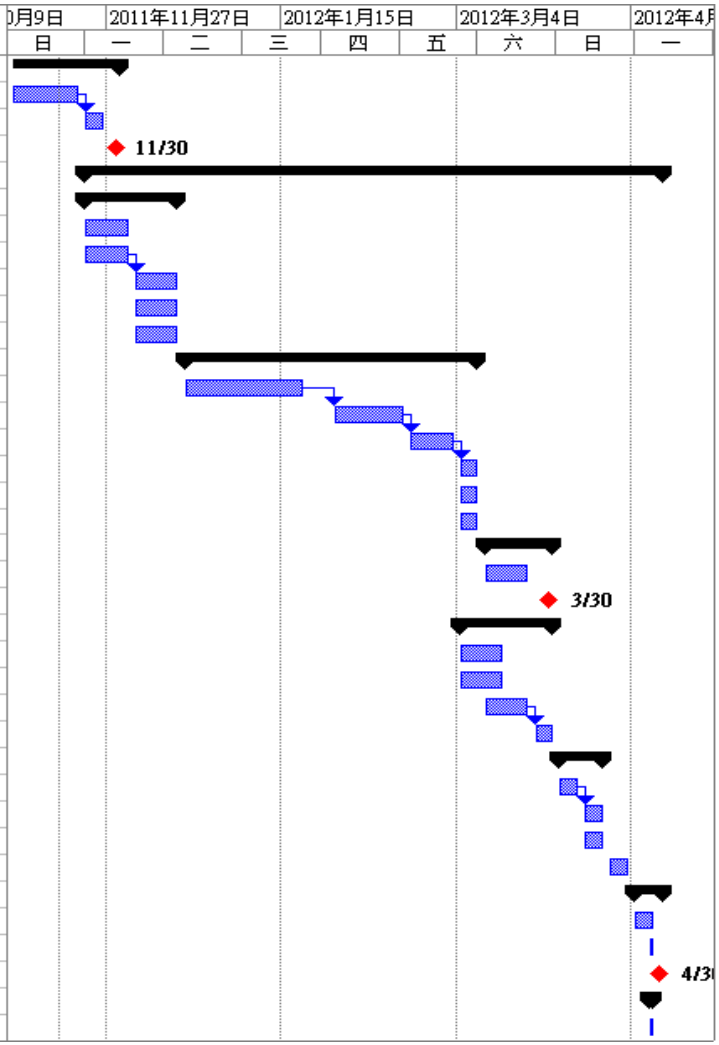

【圖說】<凌羣個資安全整合解決方案>8月20日正式發表，各家廠商代表由左至右分別為:
HAT日立亞細亞台灣總經理安田憲司/Hitachi Solutions部長田中孝典/NII執行長吳國維/凌羣電腦總經理劉瑞隆/SGS東亞區國際驗證部副總裁黃世忠/趨勢科技台灣及香港區總經理洪偉淦/Fortinet台灣區總經理陳鴻翔/凌羣電腦市場暨產品行銷事業群副總經理李振寰/RSA台灣區經理黃惠美/SafeNet台灣區業務經理吳昇穎及Orient台灣區經理福島昭寬等

# 歷程

- 99.06.28 : 個資檢核報告
- 99/07~100/05評估與測試各項解決方案
- 100.05.25 :個資保護資安加強計畫
- 100/06 ~ 100/10 :跟顧問討論範圍與時程
- 100/11 ~ 101/07 : 導入管理制度
- 101/09 ~ Now :導入資安產品

# 分享-時程規劃

| 識別碼 | 任務名稱 | 工期 | 開始時間 | 完成時間 |
|---|---|---|---|---|
| 1 | **(O)專案執行準備與管理** | **22 工作日** | **100/11/1** | **100/11/30** |
| 2 | 0.1專案執行計畫書 | 14 工作日 | 100/11/1 | 100/11/18 |
| 3 | 0.2專案啟始會議(含個人資料鑑別/清查方式說明) | 5 工作日 | 100/11/21 | 100/11/25 |
| 4 | **查核點1** | 1 工作日 | 100/11/30 | 100/11/30 |
| 5 | **1.個人資料管理制度建置** | **116 工作日** | **100/11/21** | **101/4/30** |
| 6 | **1.1個人資料管理現況瞭解** | **20 工作日** | **100/11/21** | **100/12/16** |
| 7 | 1.1.1現況診斷、個人資料管理制度與環境瞭解 | 10 工作日 | 100/11/21 | 100/12/2 |
| 8 | 1.1.2個人資料管理現況瞭解 | 10 工作日 | 100/11/21 | 100/12/2 |
| 9 | 1.1.3個人資料作業流程調查暨個人資料檔案盤點 | 10 工作日 | 100/12/5 | 100/12/16 |
| 10 | 1.1.4擬定個人資料資訊流之差異分析紀錄 | 10 工作日 | 100/12/5 | 100/12/16 |
| 11 | 1.1.5提供個人資料管理組織建議 | 10 工作日 | 100/12/5 | 100/12/16 |
| 12 | **1.2個人資料管理衝擊分析及風險評鑑** | **60 工作日** | **100/12/19** | **101/3/9** |
| 13 | 1.2.1 確認及鑑別個人資料並建立個人資料檔案清冊 | 25 工作日 | 100/12/19 | 101/1/20 |
| 14 | 1.2.2個人資料檔案衝擊分析 | 15 工作日 | 101/1/30 | 101/2/17 |
| 15 | 1.2.3 個人資料價值評鑑、既有控制鑑別及風險評鑑作業 | 10 工作日 | 101/2/20 | 101/3/2 |
| 16 | 1.2.4 撰寫「個人資料管理衝擊分析報告」 | 5 工作日 | 101/3/5 | 101/3/9 |
| 17 | 1.2.5 撰寫「風險評鑑報告書」 | 5 工作日 | 101/3/5 | 101/3/9 |
| 18 | 1.2.6 評定可接受風險等級 | 5 工作日 | 101/3/5 | 101/3/9 |
| 19 | **1.3風險處理作業** | **15 工作日** | **101/3/12** | **101/3/30** |
| 20 | 1.3.1 協助提供控制建議 | 10 工作日 | 101/3/12 | 101/3/23 |
| 21 | **查核點2** | 1 工作日 | 101/3/30 | 101/3/30 |
| 22 | **1.4 建立個人資料管理制度** | **20 工作日** | **101/3/5** | **101/3/30** |
| 23 | 1.4.1制定個人資?檔案安全維護計畫 | 10 工作日 | 101/3/5 | 101/3/16 |
| 24 | 1.4.2 制定業務終止後個人資?處?方法 | 10 工作日 | 101/3/5 | 101/3/16 |
| 25 | 1.4.3制定個人資料保護程序 | 10 工作日 | 101/3/12 | 101/3/23 |
| 26 | 1.4.4討論/確認個人資料管理制度文件 | 5 工作日 | 101/3/26 | 101/3/30 |
| 27 | **1.5協助辦理個人資料管理制度之監控及稽核** | **10 工作日** | **101/4/2** | **101/4/13** |
| 28 | 1.5.3 進行各單位個人資料管理制度內部稽核作業 | 5 工作日 | 101/4/2 | 101/4/6 |
| 29 | 1.5.4 撰寫內部稽核報告 | 5 工作日 | 101/4/9 | 101/4/13 |
| 30 | 1.5.5 個人資料保護管理內部稽核作業之缺失改善 | 5 工作日 | 101/4/9 | 101/4/13 |
| 31 | **1.6個人資料管理制度管理審查會議** | 5 工作日 | 101/4/16 | 101/4/20 |
| 32 | **1.7協助完成BS 10012 PIMS第三方驗證** | **6 工作日** | **101/4/23** | **101/4/30** |
| 33 | 1.7.1 協助第三方驗證作業 | 5 工作日 | 101/4/23 | 101/4/27 |
| 34 | 1.7.2 協助第三方驗證作業結果改善 | 1 工作日 | 101/4/27 | 101/4/27 |
| 35 | **查核點3** | 1 工作日 | 101/4/30 | 101/4/30 |
| 36 | **3. 其它** | **1 工作日** | **101/4/27** | **101/4/27** |
| 37 | **3.1 結案會議** | 1 工作日 | 101/4/27 | 101/4/27 |






凌羣電腦 THE SYSCOM GROUP CMMI5 Maturity Level Software Group

# 分享- 時間估算過於樂觀

- 實踐執行時間：101/06
- 超出時間的工作項目
  - 業務訪談時間：超出2周
  - 個人資料盤點時間：超出約 1 個月
  - 個人盤點資料與業務流程整合：超出2周

# 分享- 教育訓練

- 約 1千多人次
  - 標準與法律
  - 個資盤點
  - 風險評估
  - 內部稽核課程
  - 制度宣導

# 分享- 找出重大問題

- 問題：在個資盤點結果中，發現大量未經當事人授權的個人資料(包含姓名、銀行帳號，護照號碼或身分ID)。
- 原因:該大量個人資料為承接國外專案時，客戶提供的測試資料
- 處理方式:與開發團隊討論是否需要真的資料才能測試？將資料進行去識別化(含姓名、銀行帳號，護照號碼或身分ID)

# 分享－認知差異


- 凌羣電腦致力於保護您的隱私權。本活動報名頁面蒐集您的個人資訊僅供活動通知之用，不作其他用途，並於活動結束後 1 個月內刪除
- 本次蒐集您的個人資料類別包含C001 ,C038 ,C061
- 我們運用各種安全技術與程序來協助保護您的個人資訊安全，避免未經授權的存取、使用或揭露。
- 您可隨時依個人資料保護法第三條之規定來行使您的權利，惟您行使您的權利時，本公司將依據法律規定與實際情形來准駁你的請求。
- 上述個資當事人權利請聯絡：pims-services@syscom.com.tw信箱
- 如您的提供的資料無法與你聯絡，將無法參加本次活動

# 分享 –認知差異

1. 凌羣電腦股份有限公司（以下簡稱「本公司」）取得您的個人資料，目的在於個人資料保護法及相關法令之規定下，依本公司「隱私權政策聲明」蒐集、處理及利用您的個人資料。
2. 您可依您的需要提供以下個人資料：(填入個人資料欄位，如電子郵件地址、單位、職稱、姓名、居住縣市別(含區))。
3. 您同意本公司以您所提供的個人資料確認您的身分、與您進行聯絡、提供您本公司及合作夥伴之相關服務及資訊，以及其他隱私權政策聲明規範之使用方式。
4. 您同意本公司蒐集、處理與利用您的個人資料之期間為：自即日起至本公司營運期間，利用地區為台灣地區，為本公司同仁進行業務聯繫、寄送電子報及合作廠商結案報告之用。
5. 您可隨時依個人資料保護法之相關規定，向本公司查詢我們所蒐集您的個人資料、要求補充或更正、請求停止蒐集處理或利用、請求查閱、複製、刪除，但因您行使上述權利而導致權益受損時，本公司將不負相關賠償責任。
   個資補充或更正、請求停止蒐集處理或利用、請求查閱、複製、刪除之聯絡信箱：info@syscom.com.tw
6. 您可自由選擇是否提供您的個人資料，但若您所提供之個人資料，經檢舉或由本公司發現不足以確認您的身分，或有其他個人資料冒用、盜用、資料不實等情形，可能造成您無法獲得本公司提供之服務與相關權益。
7. 本公司如違反個人資料保護法規定或因天災、事變或其他不可抗力所致者，致您的個人資料被竊取、洩漏、竄改、遭其他侵害者，應查明後於電話或信函或電子郵件或網站公告等方法中，擇適當方式通知您。
8. 您瞭解此一同意符合個人資料保護法及相關法規之要求，具有書面同意本公司蒐集、處理及利用您的個人資料之效果，亦同意本公司留存此同意書，供日後備查。
9. 當您勾選「本人同意」並親自簽章後，即視為您已詳閱並了解本同意書內容，且同意遵守所有事項。

☐ 本人同意
☐ 本人不同意。

簽名：

中　　華　　民　　國　　年　　月　　日

# 分享 –認知差異

---

## 來賓資料

填表人：_____ 公司名稱：_____

部　門：_____ 職　　稱：_____

地　址：_____ e-Mail　：_____

電　話：_____ ext. 傳　真：_____

**個人資料保護聲明：**

凌羣電腦致力於保護您的隱私權。我們會使用您的個人資訊，提供活動期間問卷統計，未經您的許可，凌羣不會將您的個人資訊交與第三人，除非係為完成您所請求的服務或交易所必要或法律要求者。我們運用各種安全技術與程序來協助保護您的個人資訊安全，避免未經授權的存取、使用或揭露。除了本聲明所載之上述狀況外，您所提供的個人資訊在未取得您的許可前，不會流通到凌羣或其他等單位。

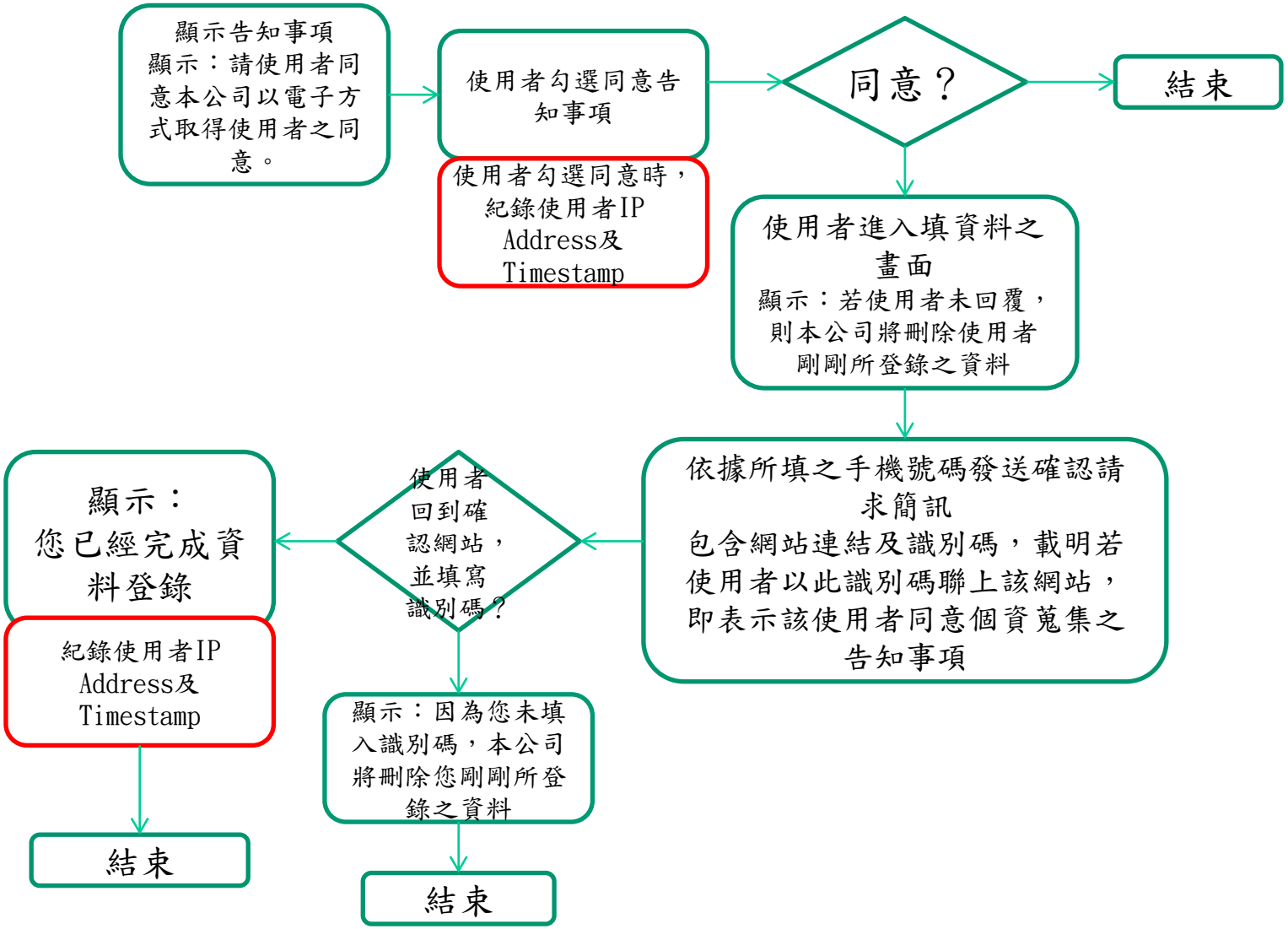
※若您同意本公司依上述聲明使用您的個人資料，請勾選右側方格 - □我同意

# 分享-流程修正需要時間

# 分享-流程修正需要時間

- 需取得書面同意
  - 個人資料保護法施行細則修正草案第十四條：本法第七條所定書面意思表示之方式，依電子簽章法之規定，得以電子文件為之。
  - 電子簽章法第 4 條:經相對人同意者，得以電子文件為表示方法。依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。
- 告知事項處理

# 分享-取得以電子方式取得同意之流程



# 分享-流程修正需要時間


- 維護團隊因人力問題無法在10/01前完成
- 建議暫時作法：

1，關閉網站訂閱功能

2，在訂閱功能頁提供電話訂閱方式

3，電話訂閱時需取得書面同意

SYSCOM

# 專注資訊服務本業
# 誠信經營、以客為尊

謝謝指教

凌羣電腦 THE SYSCOM GROUP

CMMI 5 Maturity Level Software Group