資安事件應變與二方稽核實務

林瑞龍

國家衛生研究院

112年3月24日

簡報大綱

壹、資安事件、豁免不易

貳 、面對挑戰、冷靜分析

參、問題處置、措施適當

壹. 資安事件、豁免不易

個資外洩案例-iRent(1/2)

首頁 > 生活

iRent個資外洩！賠償方案出爐　40萬會員快收信

記者 呂欣芷 報導
發佈時間：2023/02/04 16:48
最後更新時間：2023/02/04 16:48

小 中 大

資料來源：中時新聞網 112/2/4 報導，
https://www.chinatimes.com/realtimenews/20230204002651-260410?chdtv

- 據報導：事件發生原因為「內部用來記錄應用程式Log檔之暫存資料庫，因未適當阻擋外部連線，導致該資料庫可能遭外部專業資訊人員使用特定工具及技巧進入該資料庫內查詢近三個月的會員異動資料。
- 曾紀錄之個資包含會員姓名、電話、地址、經遮蔽之信用卡資訊（排除盜刷疑慮）、身分證、生日、Email、緊急聯絡人、申請會員上傳照片檔（經編碼），有遭外部查詢之可能。

個資外洩案例-iRent(2/2)


自由時報 Liberty Times Net
即時 熱門 政治 社會 生活 健康 國際 地方 蒐奇 影音 財經 娛樂 藝文
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

iRent 40萬筆個資外洩！公總認定有疏失 開罰20萬限期改正

iRent個資外洩40萬筆，公總認定有疏失，依法開罰20萬元，要求持續改正。（資料照）

2023/02/09 12:29

- 公路總局確認該公司未依「個人資料保護法」與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」，採行適當安全措施致個人資料洩漏，又未訂定完整個人資料檔案安全維護計畫，且該公司屆期仍未改正，發生外洩風險個資筆數達40萬筆。
- 違規情節重大，已明確違反個人資料保護法第27條第1項及第2項規定。因此，公總就依據個人資料保護法第48條第4款規定，對該公司處最高罰鍰新台幣20萬元。

資料來源：自由時報112/02/09報導，https://news.ltn.com.tw/news/life/breakingnews/4205839

個資外洩案例-華航(1/2)

新聞

您現在位置：首頁 > 新聞

華航遭駭客攻擊，賴清德、張忠謀、林志玲等會員個資外洩

2023 / 01 / 17 - 編輯部

Facebook LinkedIn Twitter 新增至最愛文章

- 駭客先後於今年1月4日和1月11日陸續曝光10位和50位會員個資。
- 包括臺灣知名的政界、商界、明星和名嘴等知名人士的資料，資料除了華航的會員編號外，還有中英文姓名、出生年月日、電子郵件和手機等個人資訊。

資料來源：資安人112/01/17報導，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10297

個資外洩案例-華航(2/2)

華航會員個資外洩案 交通部擬開罰

中央社 2023.03.03

華航1月時接獲匿名勒贖，會員資料庫遭駭客公開圖／本報資料照片

資料來源：工商時報112/03/03報導，https://ctee.com.tw/news/industry/818247.html

- 華航1月時接獲匿名勒贖，會員資料庫遭駭客公開，不乏重要政經人士會員個人資料外洩。
- 交通部請數位發展部協助民航局調查，初步認定華航有疏失，擬對華航開罰。
- 根據「個人資料保護法」，罰鍰為新台幣2萬元至20萬元。

近年公務機關個資外洩事件表

時間	事件內容
2023年1月	華航會員資料庫遭駭，國外論壇公布會員資料，包含賴清德、張忠謀、林志玲等人。
2023年1月	健保署前主秘葉逢明、現任承保組科長謝玉蓮、職員李仁輝三人，疑竊取民眾及11情治單位健保資料長達13年，遭調查局偵訊。
2022年12月	部立桃園醫院遭爆採用中國醫療資訊系統(內有簡體中文附註的程式碼)，自2020年8月起遭駭，竊取個資與醫護資料，部桃新聞稿稱案發後即請資安公司鑑識，僅有一台主機資料遭竊，且內無個資。
2022年10月	戶政資料遭駭，並在外國論壇公開兜售，疑為2,357萬餘筆。
2020年5月	美國資安公司Cyble 在暗網發現外洩資料庫，內容稱是全臺戶籍資料，包含超過2千萬筆民眾個資，資料庫來源是內政部戶政司。
2019年6月	銓敘部爆發公務人員個資被置於國外論壇販賣案，外洩資料內含國安局等機敏機關，超過20萬筆公務員資料。
2016年7月	勞動部勞發署發現所屬之「台灣就業通」網站，遭民間債務催收公司駭入，竊取5萬8千多筆求職民眾個資，以賺取催收債務傭金。
2016年5月	中華郵政商城因網站漏洞遭中國駭客侵入，逾1.7萬筆的交易資料遭竊

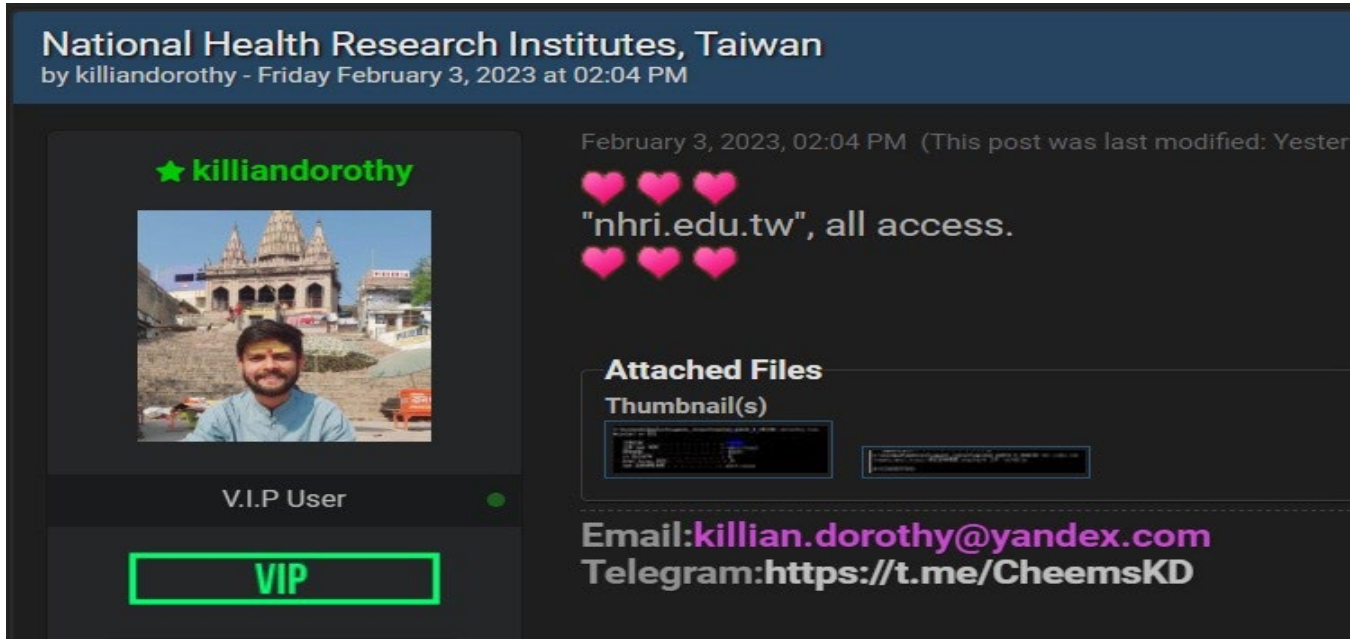
劉世芳盤點，自2016年以來，國內8起公務機關的重大個資外洩事件。（圖由洪申翰辦公室提供）

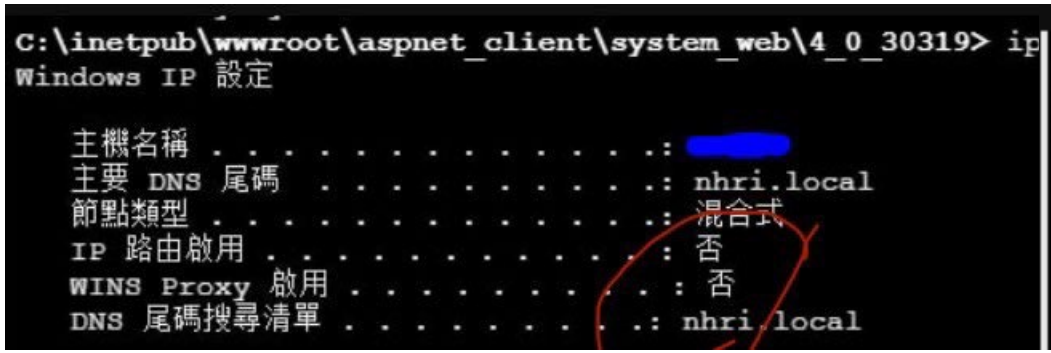
資料來源：自由時報112/1/18報導，https://news.ltn.com.tw/news/politics/breakingnews/4188767

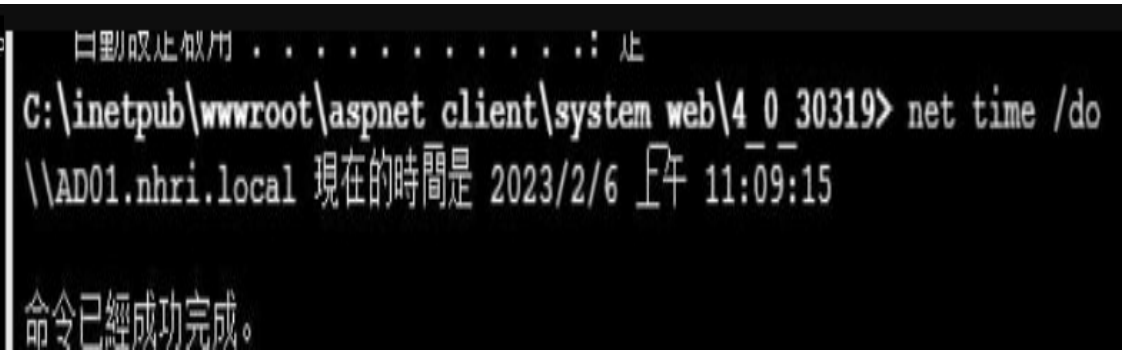
貳、面對挑戰、冷靜分析

一.發現事件(1/2)

訊息一
發現
兜售相關



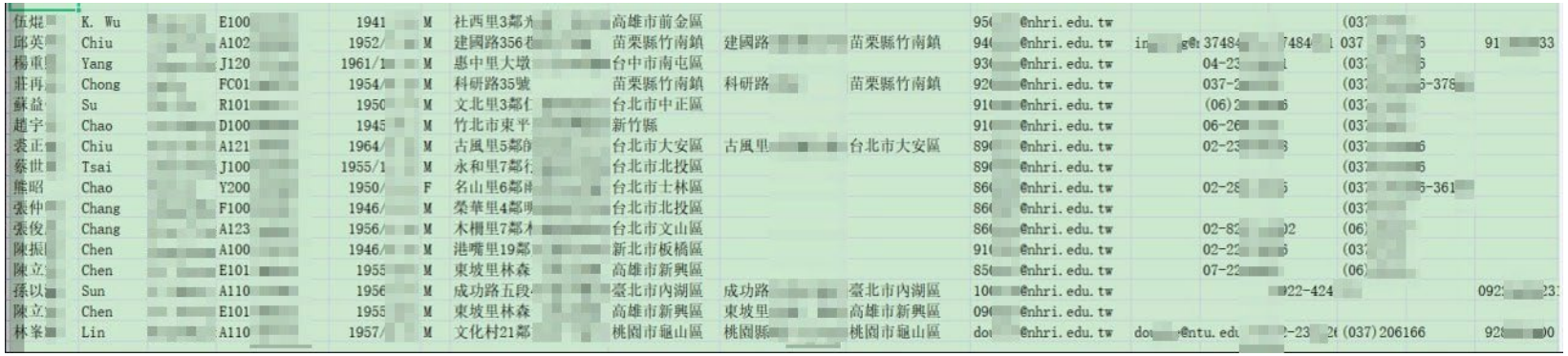




一.發現事件(2/2)　知悉資安事件

訊息二
個資外洩

資料，內容含
姓名、身分證號、出生日期、地址、電子信箱
電話



伍堃	K. Wu	E100	1941	M	社西里3鄰	高雄市前金區			95	@nhri.edu.tw		(037	
邱英	Chiu	A102	1952/	M	建國路356	苗栗縣竹南鎮	建國路	苗栗縣竹南鎮	94	@nhri.edu.tw	in g@ 37484 7484 1	037 6	91 33
楊重	Yang	J120	1961/1	M	惠中里大墩	台中市南屯區			93	@nhri.edu.tw	04-23 1	(037 6	
莊再	Chong	FC01	1954/	M	科研路35號	苗栗縣竹南鎮	科研路	苗栗縣竹南鎮	92	@nhri.edu.tw	037-2	(037 6-378	
蘇益	Su	R101	1950	M	文北里3鄰仁	台北市中正區			91	@nhri.edu.tw	(06)2 6	(037	
趙宇	Chao	D100	1945	M	竹北市東平	新竹縣			91	@nhri.edu.tw	06-26	(037	
裘正	Chiu	A121	1964/	M	古風里5鄰	台北市大安區	古風里	台北市大安區	89	@nhri.edu.tw	02-23 3	(037 6	
蔡世	Tsai	J100	1955/1	M	永和里7鄰	台北市北投區			89	@nhri.edu.tw		(037 6	
熊昭	Chao	Y200	1950/	F	名山里6鄰	台北市士林區			86	@nhri.edu.tw	02-28 5	(037 6-361	
張仲	Chang	F100	1946/	M	榮華里4鄰	台北市北投區			86	@nhri.edu.tw		(037	
張俊	Chang	A123	1956/	M	木柵里7鄰木	台北市文山區			86	@nhri.edu.tw	02-82 02	(06	
陳振	Chen	A100	1946/	M	港嘴里19鄰	新北市板橋區			91	@nhri.edu.tw	02-22 6	(037	
陳立	Chen	E101	1955	M	東坡里林森	高雄市新興區			85	@nhri.edu.tw	07-22	(06	
孫以	Sun	A110	1956	M	成功路五段	臺北市內湖區	成功路	臺北市內湖區	10	@nhri.edu.tw	22-424		092 23
陳立	Chen	E101	1955	M	東坡里林森	高雄市新興區	東坡里	高雄市新興區	09	@nhri.edu.tw			
林峯	Lin	A110	1957/	M	文化村21鄰	桃園市龜山區	桃園縣	桃園市龜山區	do	@ntu.edu	-23 2	(037)206166	92 00

二、資安事件應變處理

資安應變會議 → 問題研判 → 求證檢測

■資安專業團隊召開資安應變會議
■應變對策
■分析問題

資料仍不足

但研判可能為

■AD遭入侵
■NHRI AD 資料外洩

AD立即檢測

初步分析AD結果

■ 無惡意程式
■ 無異常活動紀錄

判斷AD仍屬安全

註：AD為帳號管理核心

三. 查檢分析

一、根據資料研判**緊急查檢**【服務可能系統】**及結果分析**

查資訊資產清冊，可能問題範圍清單

二、追查**軌跡及IP來源**

三、**受駭點及其原因**檢討

四、駭客**入侵路徑及時序檢討**

三. 查檢分析　資訊服務緊急查檢及結果分析

■查檢找出問題主機

(一)本院帳號管理系統(AD01、AD03)

- 未發現惡意程式
- 未發現異常活動紀錄

(二)本院行政資訊整合系統(NHRIPUB)

- 未發現惡意程式
- 未發現異常活動紀錄

(三)本院重要電子郵件系統系統(CAS12、CAS32)

- 發現惡意程式
- 發現異常活動紀錄

發現問題主機

2 / 3　無立即性風險 未有高風險檔案及程序

4　中風險性 檔案有被修改過，必須持續關注觀察是否有異

5　高風險性 確認留有後門程式，壞人可利程式用做壞事

No	Computer Name	Level	Result
11	SQLTEST	3	未存有高風險檔案或程序
12	SQLPROD	3	未存有高風險檔案或程序
13	WEBFTP-A	3	未存有高風險檔案或程序
14	WEBFTP-B	3	未存有高風險檔案或程序
15	CAS12	5	1.網 ege.aspx、 Expi word.aspx 2.So VPN t.jpg 二、 碼將相黏鍵功 能更 管理員 三、 -02 17:30、 202 17:57 曾遭 Psex 登入
16	CAS32	5	1.20 3 17:08 曾遭 工具登入 2.20 1 ~ 2022-01-25 期間 錄下曾有nbt 網掃 r壓縮檔程式等 執行
17	CAS52	3	未存 檔案或程序
18	CAS72	3	202 :03 曾遭 工具登入
19	MBX12	4	202 :32 遭修 相黏鍵功能更 換為 員
20	MBX32	3	未存 檔案或程序
21	AD01	4	202 :04 遭修 相黏鍵功能更 換為 員
22	AD03	3	202 5:24 曾遭 工具登入

No	Computer Name	Level	Result
1	ts6	4	2021-12-29 ~ 2021-12-30 1.曾遭攻擊者執行procdump64工具以及透過Psexec登入該主機 2.利用PowerShell連往34.125.71[.]18:443下載可疑程式「xx」至主機c:\windows\temp\目錄下
2	ts7	3	未存有高風險檔案或程序
3	WIN-BJ4VDEKRAJ8	3	未存有高風險檔案或程序
4	sqlstand	2	未存有高風險檔案或程序
5	NHRIPUB-WEBTEST	3	未存有高風險檔案或程序
6	NHRIORP-WEB	3	1.未存有高風險檔案 2.事件紀錄顯示IIS所帶起CMD指令活動，但經檢視網站存取紀錄未發現異常存取軌跡，建議後續調整稽核程序紀錄，確認實際執行指令為何?
7	WEBDOC	3	2020/6/4 15:09 未存有高風險檔案或程序，但有Psexec工具執行紀錄
8	WINDOWS-R7FCDB9	3	未存有高風險檔案或程序
9	WIN104	3	未存有高風險檔案或程序
10	WIN-HEHVESR9A4C	3	未存有高風險檔案或程序

三. 查檢分析　資安事件應變處理

初部
應變處置及回報

執行
掃描工具蒐集主機資料

AD仍屬安全、採取相關防護措施
並持續蒐集、檢測其他對外服務主機，如下

初步結論如下:

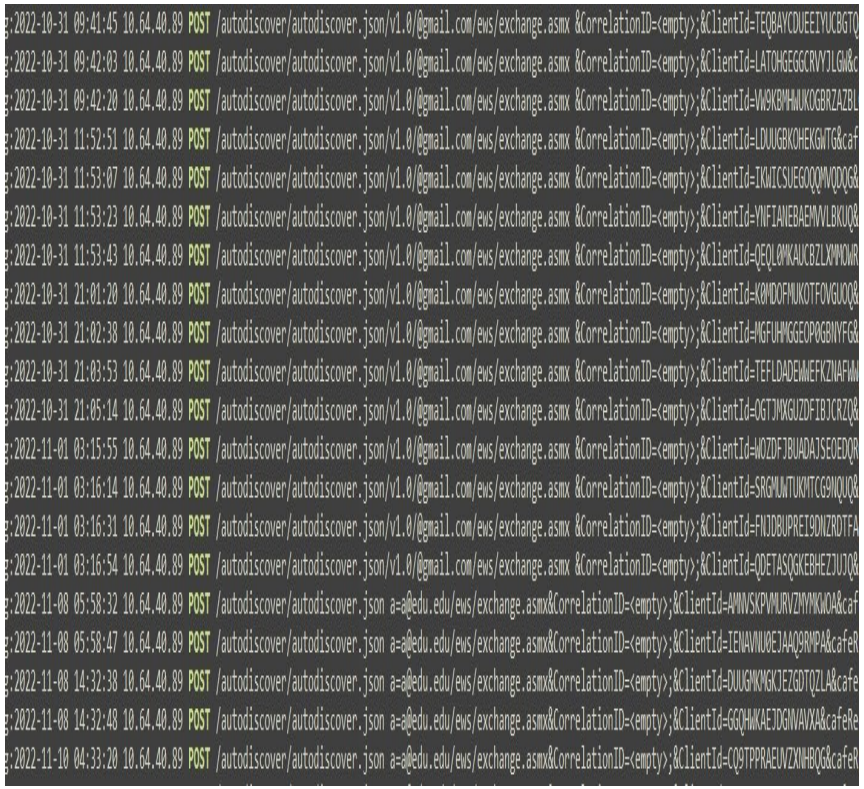
1. 目前以工具檢查目錄服務主機(AD)，未發現有入侵現象，同時全面修改特權管理帳號之密碼。
2. 原通報資安事件2級，將改為1級。
3. 接續將對本院對外服務網站用工具進行檢查(網站多需點時間)，並將結果送安碁協力資安團隊。

以上報告

序	系統名稱	掃描工具1安裝	掃描結果1	掃描工具2安裝	掃描結果2
1	行政系	cdir-collector	NHRIPUB-WEBTEST_20230208115712	ThreatSonar	202302081202-NHRIPUB-WEBTEST
2	行政系	cdir-collector	NHRIORP-WEB_20230208140200	ThreatSonar	202302081409-NHRIORP-WEB
3	公文系	cdir-collector	WEBDOC_20230208151709	ThreatSonar	202302081529-WEBDOC.report_bundle
4	公文系	cdir-collector	WINDOWS-R7FCDB9_20230208155232	ThreatSonar	202302081602-WINDOWS-R7FCDB9.report_bundle
5	人力資	cdir-collector	WIN104(10.64.16.231)_20230208(c)	ThreatSonar	WIN104(10.64.16.231)_20230208(T)
6	人力資	cdir-collector	WIN-HEHVESR9A4C_20230208173606	ThreatSonar	202302081742-WIN-HEHVESR9A4C.report_bundle
7	測試資	cdir-collector	SQLTEST_20230208115011	ThreatSonar	202302081151-SQLTEST.report_bundle
8	正式資	cdir-collector	SQLPROD_20230208111849	ThreatSonar	202302081120-SQLPROD.report_bundle
9	webftp	cdir-collector	WEBFTP-A_20230207172400	ThreatSonar	202302071727-WEBFTP-A.report_bundle
10	webftp	cdir-collector	WEBFTP-B_20230207173548	ThreatSonar	202302071809-WEBFTP-B.report_bundle
11	郵件系	cdir-collector	CAS12_20230208150038	ThreatSonar	202302081611-CAS12.report_bundle
12	郵件系	cdir-collector	CAS32_20230208150252	ThreatSonar	202302081611-CAS32.report_bundle
13	郵件系	cdir-collector	CAS52_20230208150351	ThreatSonar	202302081611-CAS52.report_bundle
14	郵件系	cdir-collector	CAS72_20230208150530	ThreatSonar	202302081612-CAS72.report_bundle
15	郵件系	cdir-collector	MBX12_20230208153919	ThreatSonar	202302081741-MBX12.report_bundle
16	郵件系	cdir-collector	MBX32_20230208154154	ThreatSonar	202302081649-MBX32.report_bundle
17	郵件系	cdir-collector	MBX52_20230208154412	ThreatSonar	
18	exchar				
19	exchar				
20	exchar				
21	exchar				
22	行政系				
23	行政系				
24	測試資	cdir-collector	WIN-BJ4VDEKRAJ8_20230209152536	ThreatSonar	202302091526-WIN-BJ4VDEKRAJ8.report_bundle
25	備援資	cdir-collector	SQLSTAND_20230209151640	ThreatSonar	202302091518-SQLSTAND.report_bundle
26	TS6	cdir-collector		ThreatSonar	
27	TS7	cdir-collector		ThreatSonar	
28	CAS32				

三. 查檢分析　追查問題軌跡及IP來源

- 軌跡來源: :IP: 185.248.85.10　來源：英國
- 攻擊目標: 電子郵件主機及置入後門惡意程式



IP來源

- 185.248.85.10 - 測試ProxyNotShell弱點　英國
  - United Kingdom Harrow Mullvad Vpn Ab
- 185.213.82.63 - WebShell存取　網路服務商據點超過40個國家
  - Packethub-AS030921
- 103.140.186.112 - WebShell存取　愛沙尼亞
  - Estonia
- 185.213.82.226 - WebShell存取　網路服務商據點超過40個國家
  - Packethub-AS030921
- 185.213.82.80 - WebShell存取
  - Packethub-AS030921
- 59.126.140.140 - WebShell存取
  - HINET-NET　ASUS Wireless Router RT-AC3200
- 122.116.35.139　HINET-NET - WebShell存取　中華電信
  - ASUS Wireless Router RT-AC3200
- 59.125.24.151　HINET-NET - WebShell存取
  - ASUS Wireless Router RT-AC3200
- 185.125.204.233 - WebShell存取
  - UK-HYDRACOM-20151111　英國

四、受駭點及原因檢討

- 受駭點:

電子郵件主機被植入惡意程式，放置路徑紀錄、機碼修改

- CAS12 存在多個惡意程式
  - 類型為web shell
    1. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resourcewarn.aspx
    2. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\ resources\owafont
    3. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\ resources\warn.as
    4. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium\fexppw.as
    5. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\scripts\premium\Rege.aspx
    6. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ExpiredPassword.aspx
    7. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth\Logout.aspx
    8. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\errorFF.aspx
    9. C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ ExpiredPassword.aspx
    10. C:\inetpub\wwwroot\aspnet_client\system_web\4_0_30319\iisstart.aspx
    11. C:\inetpub\wwwroot\aspnet_client\system_web\iisstart.aspx
- CAS12, MBX12 sethc.exe 機碼遭修改
  - 還有AD01也是
  - 攻擊者可以按5下shift執行taskmgr.exe (工作管理員)
    - 目的是在沒有帳號密碼的情況下可以執行cmd.exe
  - 遭修改機碼位置
    - HKLM\SOFTWARE: Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe
- CAS32 存在網路掃描工具
  - 路徑是C:\Users\Public\nbt.exe

原因檢討:

- 防護1.-駭客竊取本院同仁個人帳密；入侵本院內網。
- 防護2.-本院郵件主機未即時配合微軟更新，形成弱點漏洞。

- KB5014260 (提權)
  - 2022/5/10
- KB5019076 (提權, 資訊洩露 - 讀取目標的電子郵件)
  - 2022/10/11
- KB5019758 (ProxyNotShell)
  - 2022/11/9
- KB5022188 (Spoofing)
  - 2023/01/10

五、駭客入侵路徑及時序總檢討

防護1.-竊取使用者帳號，透過ＶＰＮ進入本院

駭客
1月4日
185.213.82.0/24

竊取
使用者帳號
密碼

使用者帳號
通過VPN

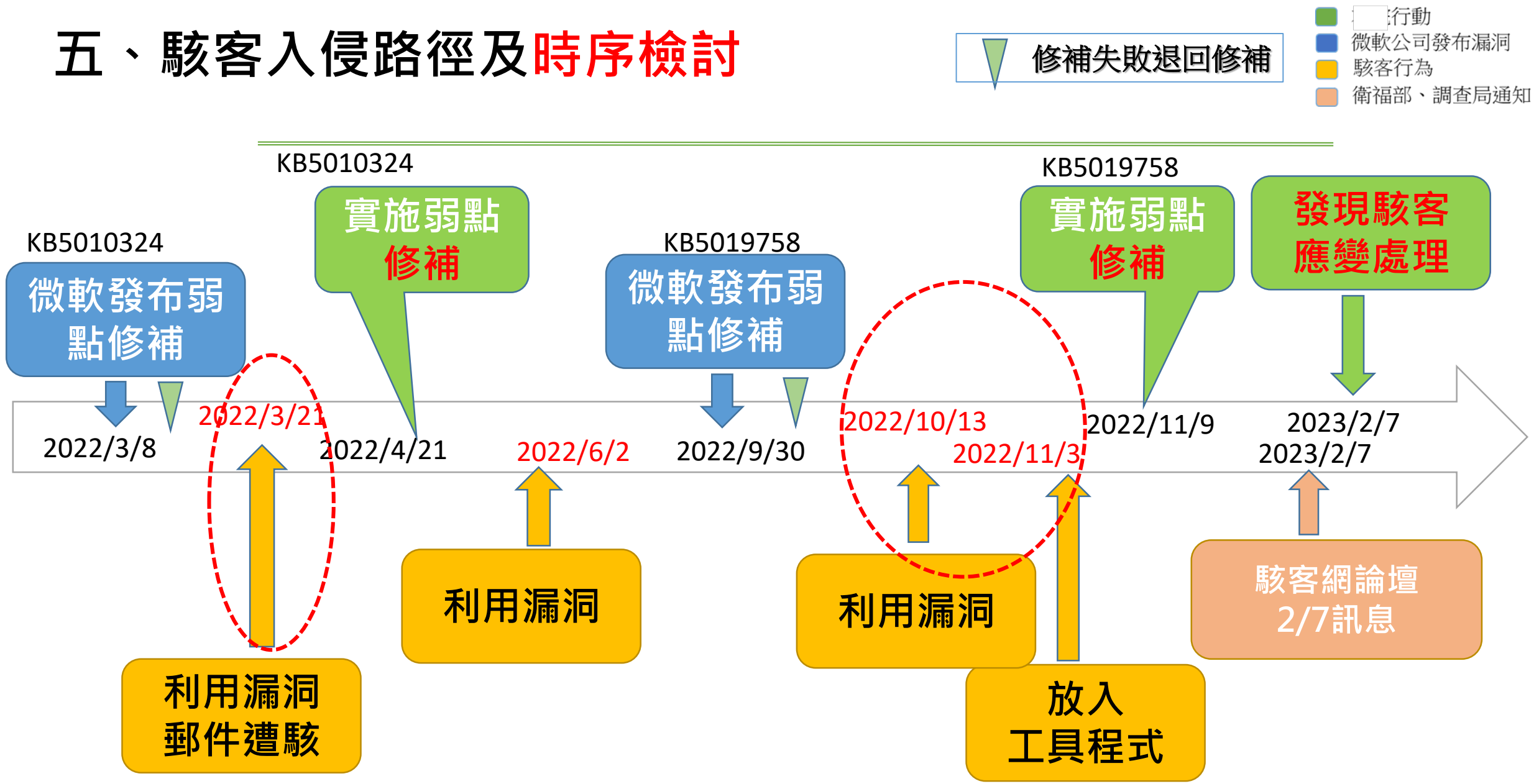
內部
網路

防護2.-利用電子郵件主機更新時間差之漏洞

利用
郵件主機更新
時間差之漏洞

竊取資訊
權限及資料

五、駭客入侵路徑及時序檢討



參.問題處置、措施適當

參.因應措施

一、駭客竊取本院同仁個人帳密；入侵本院內網，採取護措施。

二、本院郵件主機未即時配合微軟更新，形成弱點漏洞。

三、強化其他相關資通訊安全防護

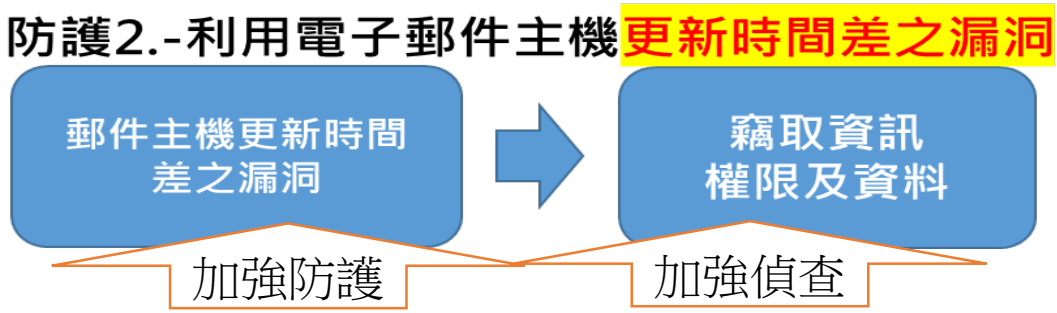
一、駭客竊取同仁個人帳密；入侵內網

防護1.-竊取使用者帳號，透過ＶＰＮ進入本院

強化:個人帳密被竊採取護措施

一、使用者密碼修改	本院使用者全面修改修改密碼。
二、第二認證因子導入	提升使用者帳號安全，防制遭暴力破密碼成功，導入第二認證因子。
三、個人電腦防毒、修補	個人電腦防毒更新派送、及漏洞修補，強化個人電腦安防毒駭。
四、個人電腦安全查檢	安排個人電腦掃描，透過自動派送機制(GPO)掃描使用者電腦，全面查檢個人電腦安全。
五、提升資安認知	強化教育訓練及社交工程演練(考核)，提升同仁資安防護認知。
六、加強智財權及個資保護	院長給全院同仁重視資安信。另公告全院加強智財權及個資保護

二、本院郵件主機未即時配合微軟更新，形成弱點漏洞



改進措施:

一、弱點及時修補 補	訂定[及時修補優先、同仁服務為次]方針，強化使用者溝通。明定資安內部稽核重點，增加年度稽核頻率，落實執行。
二、重新建置主機 建	受攻擊之郵件主機重置完成(及修補)，回復安全環境，使用者轉移至新主機。
三、防火牆防護 擋	完成防火牆設定阻擋駭客網段，原駭客無法再使用原路徑進入侵本院，起強化異常偵測查檢。
四、遭駭電腦查找及阻擋 偵	封鎖3台連結駭客網站主機，並完成使用者網段連結駭客網段封鎖，查察連結中繼網站之個人電腦。

三、強化其他相關資通訊安全防護(1/2)

其他網路服務伺服主機，強化資安防護及弱點掃描

相關網路服務伺服主機

一、弱點及時修補

訂定[及時修補優先、同仁服務為次]方針，強化使用者溝通。
明定資安內部稽核重點，增加年度稽核頻率，落實執行。

二、主機掃描

三、網站掃描

提高弱點掃描頻率，每年至少4次(含複掃)。

四、重要資料加密

五、加強主機備份

執行與宣導重要資料加密及備份。

對策、措施、時程及相關單位

可能問題	可能情況	處理對策	措施	相關同仁	建議完成日期		追蹤否
郵件主機遭入侵	針對性盜取資料	主機重建、定期修補漏洞、變更密碼	準備機器安裝、設定	資訊中心	已完成		是
		個人更改密碼郵件密碼	設定強制更改、公告通知同仁更改	資訊中心、全院同仁	112年2月已完成		是
	資料被加密勒索	主機備份	查檢空間、定期備份	資訊中心	已完成		是
		個人重要資料下載保管	宣導	資訊中心、全院同仁	112年2月已完成		否
	新聞	新聞稿備妥預防	準備新聞稿	資訊中心	112年3月		否
多部個人電腦已被入侵控制	研究資料被盜	遭入侵個人電腦重新安裝、防毒/駭，資料備份、重要資料加密	1.遭入侵個人電腦重新安裝 2.宣導重要資料需加密自備份	資訊中心、全院同仁	112年2月已完成	持續注意及查檢	是
	機器被當犯罪跳板機	遭入侵個人電腦重新安裝、防毒/駭，資料備份、重要資料加密	1.遭入侵個人電腦重新安裝 2.宣導主機怪怪通知資訊中心監控	資訊中心、全院同仁	112年2月已完成		是

對策、措施、時程及相關單位

可能問題	可能情況	處理對策	措施	相關同仁	建議完成日期	追蹤否
個資可能部分洩漏	資料被盜賣	具個資之資訊系統、防毒/駭，資料備份、重要資料加密	落實具個資之保護管理	本院個資負責人員(蒐集、處理者)	112年4月	是
	資料被不當利用		含個資之應用系統防毒/駭，資料備份、資料加密	應用系統負責人(收集、處理、利用、保管)	112年4月	是
	新聞	新聞稿備妥預防	準備新聞稿	資訊中心	112年3月	否
多部伺服機器已被入侵控制	研究資料被盜	發現被駭主機應重新安裝、防毒/駭，資料備份、重要資料加密	1.遭入侵主機應重新安裝 2.宣導重要資料需加密自備份	資訊中心、主機管理者、應用系統負責人	持續注意及查檢	否
	機器被當犯罪跳板機	發現被駭主機重新安裝、防毒/駭，資料備份、重要資料加密	1.遭入侵主機應重新安裝 2.宣導主機怪怪通知資訊中心監控	資訊中心、主機管理者、應用系統負責人	持續注意及查檢	否

對策、措施、時程及相關單位

	處理對策	措施	相關同仁	建議完成日期
使用者加強防護防止帳號被利用	提高同仁資訊安全意識	社交工程演練、教育訓練	資訊中心、全院同仁	112年3月
	防毒軟體安裝	防毒軟體安裝、更新	資訊中心、宣導全院同仁	112年3月
	個人電腦漏洞更新	個人電腦加入網域漏洞更新	資訊中心、宣導全院同仁	112年3月
管理、技術防護強化問題	增加第二認證因子	增加第二認證因子	資訊中心、影響全院同仁	112年3月
	VPN、AD帳號管理強化	VPN、AD帳號管理強化	資訊中心、影響全院同仁	112年3月
	強化偵測告警	防火牆、流量偵測及告警通知	資訊中心、影響全院同仁	持續注意及查檢

三、強化其他相關資通訊安全防護(2/2)

- 所有檢測項目皆已安排執行，預計將於00底完成報告

作業項目 \ 112年/月/周	3月					備註
	W1 3/1~3/3	W2 3/6~3/10	W3 3/13~3/17	W4 3/20~3/24	W5 3/27~3/31	
主機弱掃						標的(27網段, 約911 IP)
網站弱掃						標的31個URL
WebShell 掃瞄檢測						31個URL
滲透測試						遠端7個IP 到府11個IP
資安健診 - 網路架構檢視						1式
資安健診 - 惡意程式檢測						1300台
資安健診 - 伺服器主機更新檢視						27 URL

事件階段完成報告

高風險部份
一、3台同仁個人帳密遭盜/電腦遭植入木馬
二、本院郵件主機遭入侵
三、院同仁個資外洩

已完成控制及處理

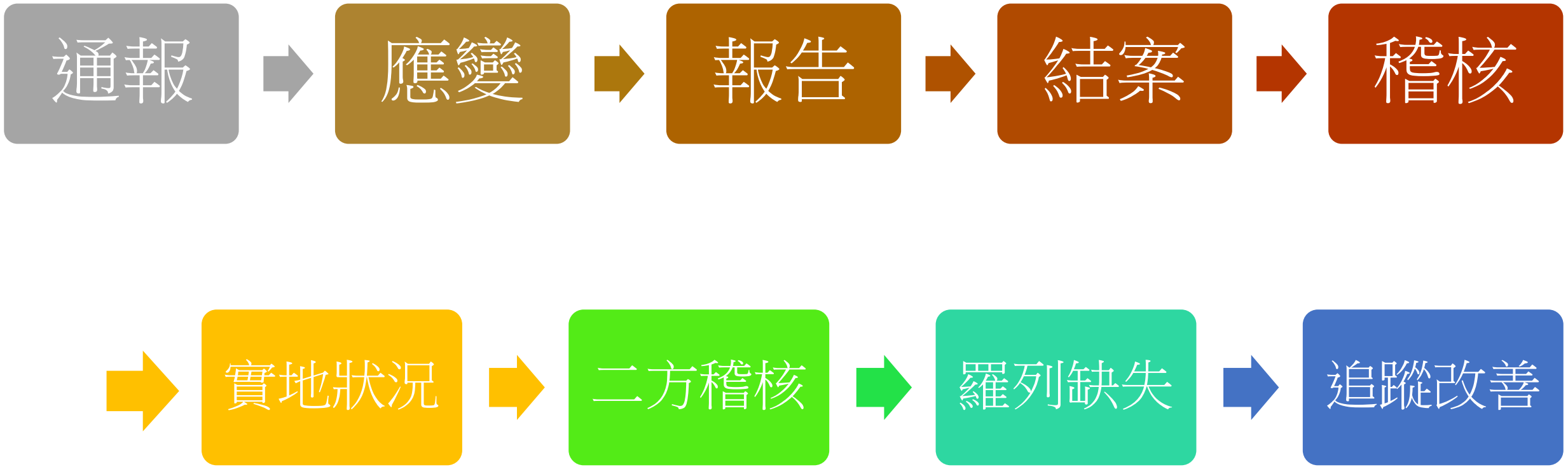
中風險部份

- 問題主機(管理用跳板機)被改機碼
- AD被改機碼

次要問題接續處理作業

完成全面掃描，初查無惡意程式、惡意活動紀錄。
進行持續加強問題主機、AD主機活動監控，操控錄影、並完成特權帳號確認查檢。

重大資安事件發生後



資通安全維護計畫作業指引(1/2)

■**適用範圍應涵蓋全校**(各系、院、所教學單位及各行政單位)

資安長之配置

宜指派**主任秘書以上人員**兼任

資安推動組織

宜由**資通安全長**召集全校各單位主管或副主管組成，**每年至少召開會議1次**

資通系統盤點

盤點範圍應包含**全校各單位**

內部資安稽核

稽核範圍應包含**全校各單位**

教育部110年12月30日臺教資(四)字第1100179797號函(國立大專校院)

發生資安事件通報資安長，有效整合其他院系所配合

問題發生後快速組成應變組織(由推動組織中產出)

問題分析時可快速釐清可能之系統

可證明內部平常資安工作有效運作

資通安全維護計畫作業指引(2/2)

資通系統盤點

⑩各校每年提交之「**資通系統資產清冊**」**至少應包含**落於**各校IP網段內**、或使用**各校網域名稱**之資通系統。

內部資安稽核

- 各校得就資通系統(保有個人資料)風險高低、教學單位特性**評估訂定推動先後順序**，**分年分階段**規劃辦理，並**明訂於**各校資通安全**維護計畫**。

教育部110年12月30日臺教資(四)字第1100179797號函(國立大專校院)

其他資安管理作業指引(加強宣導及查檢)

各級學校使用資通系統或服務蒐集及使用個人資料注意事項

教育部110年9月8日臺教資(四)字第1100122001號函

蒐集最小化

蒐集個資**不得逾越**特定目的**必要範圍**

最小授權

檔案存取權限應採**最小權限原則**

設定檢查

使用雲端服務，應**避免允許顯示其他使用者內容**，發布前應確實檢查相關設定。

加密傳輸

網路傳輸應採用加密協定(如**HTTPS**)

加密儲存

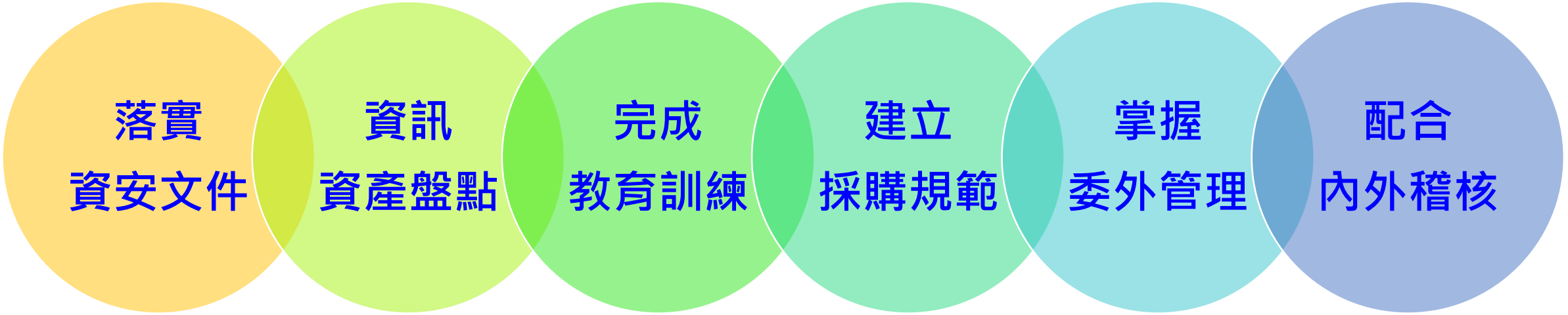
特種個資或**敏感資料**，應以**加密方式儲存**。

資料銷毀

應訂個資保存期限，並於**期限或業務終止後刪除或銷毀**。

安全資訊環境人人有責靠全體共同努力

加強管理，資安工作落實平常業務中



降低事件發生率、加速應變處理、防護衝擊及減低責任

簡報完畢．敬請指教

THANK YOU