GCB推動與VANS機制說明

行政院國家資通安全會報技術服務中心

109年

【普通】

大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

資通安全管理法相關規定

資通安全責任等級分級辦法	辦理項目：政府組態基準	
	A、B級公務機關	初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運
	特定非公務機關	特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項

大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

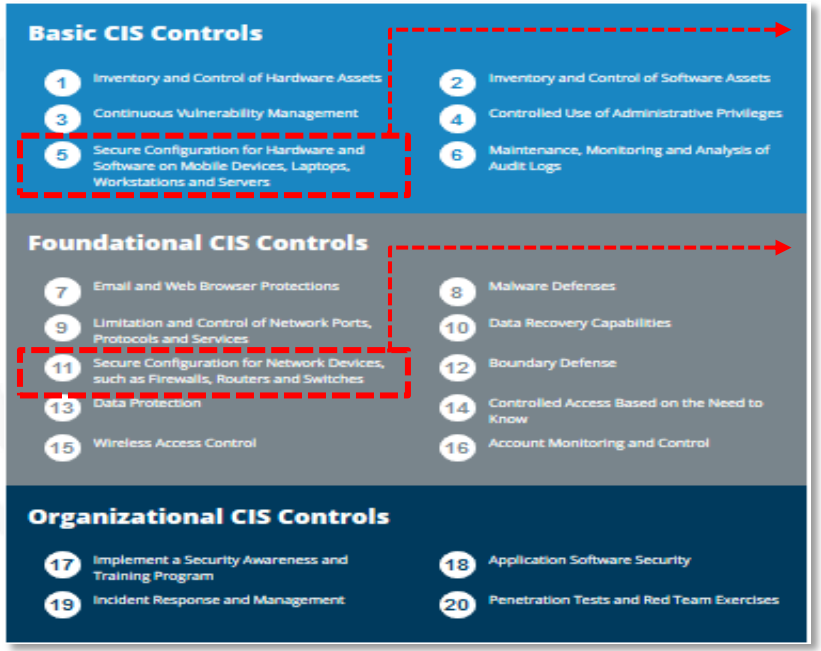
政府組態基準目的

- 政府組態基準(Government Configuration Baseline，以下簡稱GCB)目的在於規範資通訊設備(如：個人電腦、伺服器主機及網通設備等)之一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險

1. 發展一致性安全組態設定
2. 提升政府機關資通訊設備之資安防護

組態設定安全為重要的防護措施

- 美國網路安全協會於2019年公布之CIS Controls (V7.1)文件中，在Basic Controls與Foundational Controls項目皆強調安全設定(Secure Configuration)之重要性



5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

相關資安弱點：

- 不當的預設組態設定
- 預設帳號與弱密碼
- 預設啟用非必要服務

GCB項目類別

網通設備

- Wireless
- Juniper Firewall
- Fortinet Fortigate
- Cisco Firewall

作業系統

- Windows
- Linux

GCB類別

- Exchange、IIS、SQL Server
- Apache HTTP Server
- Office

應用程式

- IE
- Chrome
- Firefox
- Edge

瀏覽器

GCB發展歷程

102年度
- Windows 7
- IE 8

103年度
- Windows Server 2008 R2
- Red Hat Enterprise Linux 5(RHEL 5)

104年度
- Windows 8.1
- IE 11
- 無線網路

105年度
- Google Chrome
- Exchange Server 2013
- Juniper Firewall

106年度
- Windows 10
- Windows Server 2012 R2
- Mozilla Firefox
- Fortinet FortiGate

107年度
- Windows Server 2016
- Microsoft Edge
- Microsoft IIS 8.5
- Cisco Firewall

108年度
- Apache HTTP Server 2.4
- Microsoft Word 2016
- Microsoft Excel 2016
- Microsoft PowerPoint 2016
- Microsoft Outlook 2016

109年度

發展中：
- Red Hat Enterprise Linux 8(RHEL 8)
- Microsoft SQL Server 2016

GCB推動時程(1/2)

時間 / 單位	Y年	Y+1年				Y+2年	Y+3年	
	Q1~Q4	Q1	Q2	Q3	Q4	Q1~Q4	Q1	Q2
資安處					發文公布Y年所訂GCB		檢討	發文(檢討結果)
技服中心	發展與制定說明文件草案	文件預告	• 意見徵詢 • 巡迴研討會宣導	• 完成文件修訂 • 公告正式文件	完成實作文件		檢討	公布(網站)
機關			意見回覆		A、B級機關推動導入	A、B級機關持續推動導入	A、B級機關提供意見(管考系統填報)	推廣至C級機關導入

發文公告內容

107年發文公告106年完成制定之項目

主旨：有關推動政府機關導入政府組態基準(GCB)一案，請依說明辦理並轉知所屬，請查照。

說明：

一、本院國家資通安全會報(以下簡稱資安會報)為有效規範資通訊終端設備之一致性安全設定，以避免成為有心人士入侵管道，進而引發資安事件疑慮，自102年起制訂數項GCB項目，部署範圍從終端設備擴及伺服器與網通設備。

二、本次新增制訂之GCB項目分別為微軟個人電腦作業系統Windows 10、微軟伺服器作業系統Windows Server 2012 R2、瀏覽器Mozilla Firefox及防火牆Fortinet FortiGate，為持續加強GCB推動之深廣度，請資安責任等級列A級及B級機關(構)推動導入前揭3項GCB項目

108年發文公告107年完成制定之項目

主旨：108年度新增之政府組態基準(GCB)項目已上網公告，請貴機關依說明辦理並轉知所屬資通安全責任等級為A級與B級之公務機關。

說明：

一、本院國家資通安全會報(以下簡稱資安會報)為有效規範資通訊設備之一致性安全設定，以避免成為有心人士入侵管道，進而引發資安事件疑慮，自102年起制訂數項GCB項目，部署範圍從終端設備擴及伺服器與網通設備。

二、本次新增制訂之GCB項目，分別為瀏覽器Microsoft Edge(共計12項)、防火牆Cisco Firewall(共計44項)、伺服器作業系統Microsoft Windows Server 2016(共計690項)及應用程式Microsoft IIS 8.5(共計53項)，並已於108年11月辦理實作研習，請資通安全責任等級為A級與B級之公務機關推動導入前揭GCB項目，以持續強化資通設備之安全性設定。

GCB推動時程(2/2)

- 依上述GCB推動時程，以「109年5月」時間點為例，**A級與B級公務機關**於初次受核定或等級變更後之一年內，須完成導入**107年(含)前**所制定之**18項**GCB項目，並持續維運

項次	類別	制定年度	GCB項目
1	作業系統	102	Windows 7
2		103	Windows Server 2008 R2 SP1
3		103	Red Hat Enterprise Linux 5
4		104	Windows 8.1
5		106	Windows 10
6		106	Windows Server 2012 R2
7		107	Windows Server 2016
8	瀏覽器	102	Internet Explorer 8
9		104	Internet Explorer 11
10		105	Google Chrome
11		106	Mozilla Firefox
12		107	Microsoft Edge

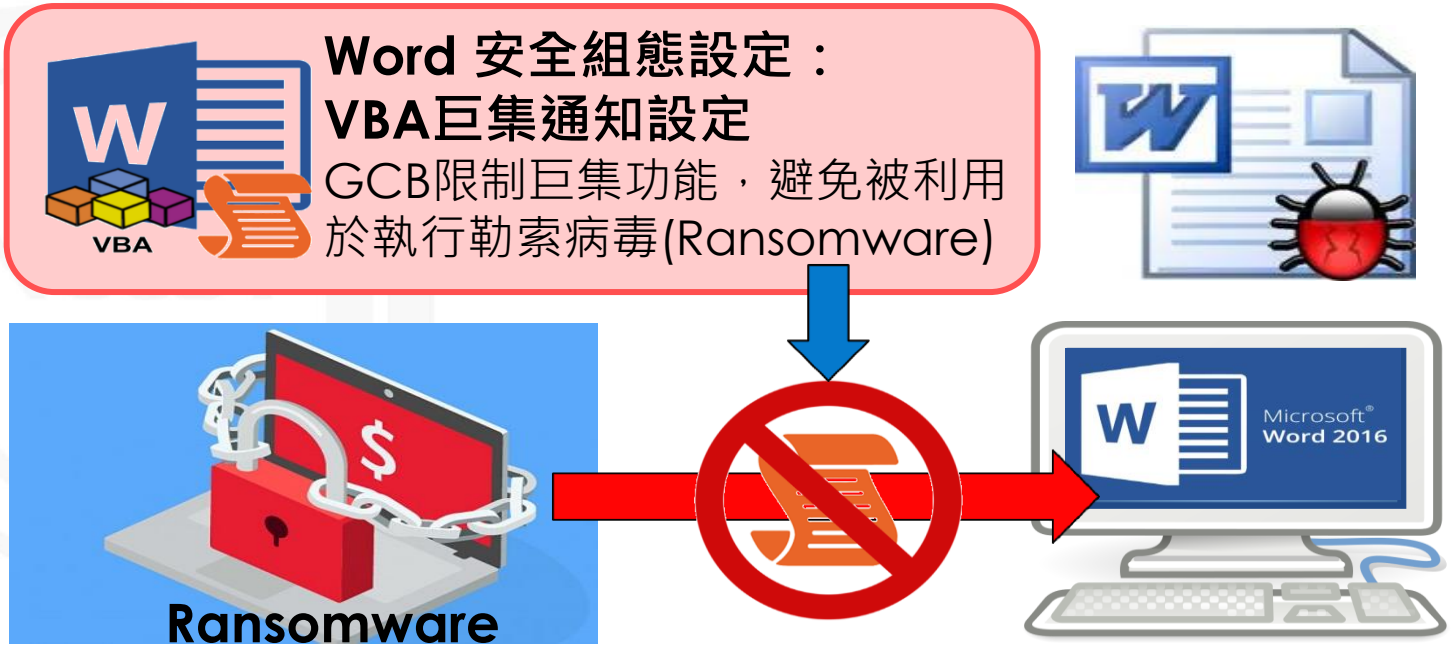
項次	類別	制定年度	GCB項目
13	網通設備	104	無線網路
14		105	Juniper Firewall
15		106	Fortinet FortiGate
16		107	Cisco Firewall
17	應用程式	105	Exchange Server 2013
18		107	Microsoft IIS 8.5

109年預定公告之GCB項目

項次	類別	GCB項目	項數
1	應用程式	Microsoft Word 2016	44
2	應用程式	Microsoft Excel 2016	56
3	應用程式	Microsoft PowerPoint 2016	39
4	應用程式	Microsoft Outlook 2016	91
5	應用程式	Apache HTTP Server 2.4	64

Microsoft Office Word 2016

- 資安案例：資安研究單位於2017年公布檔案加密勒索病毒qkG，為利用VBA巨集撰寫惡意程式碼的檔案加密惡意程式
- GCB防護



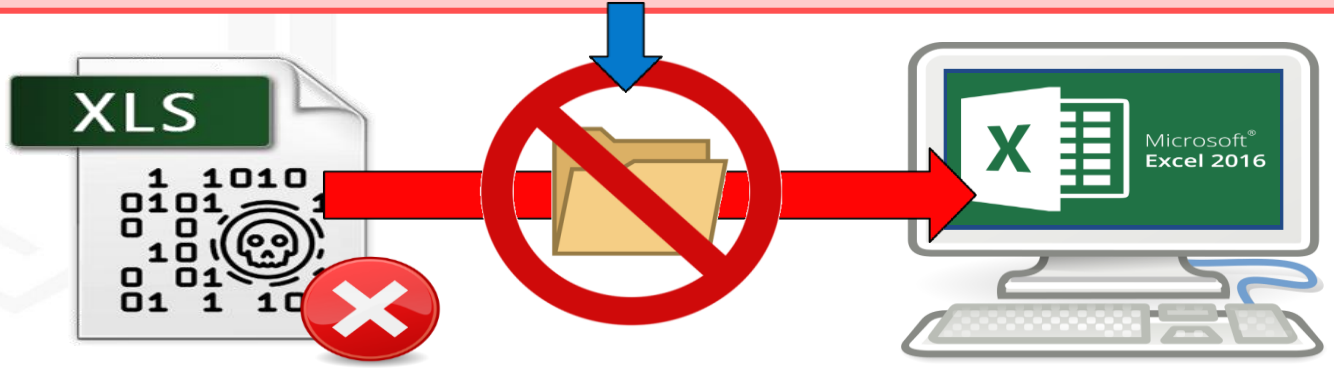
Microsoft Office Excel 2016

- 資安案例： Excel支援一些早期的檔案格式，如Sylk文件(符號連結格式)，研究人員指出Sylk文件可被利用於隱藏惡意內容進行攻擊
- GCB防護

Excel安全組態設定：

強制副檔名符合檔案類型與檔案封鎖設定

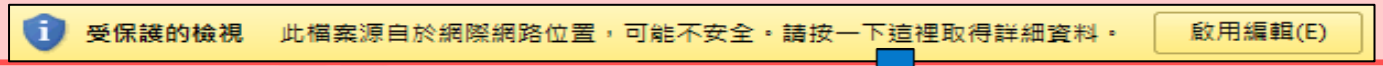
GCB設定Excel不開啟**副檔名不相符**的檔案，避免被攻擊者利用偽裝的excel檔案隱藏惡意內容，繞過安全檢查機制，執行惡意程式攻擊使用者電腦



Microsoft Office PowerPoint 2016

- 資安案例：資安研究單位於2017年公布POWHOV.A木馬，其包裝成PowerPoint的PPSX或PPS播放檔，開啟檔案若啟用編輯，將會執行內嵌的惡意PowerShell腳本並連線C&C伺服器
- GCB防護

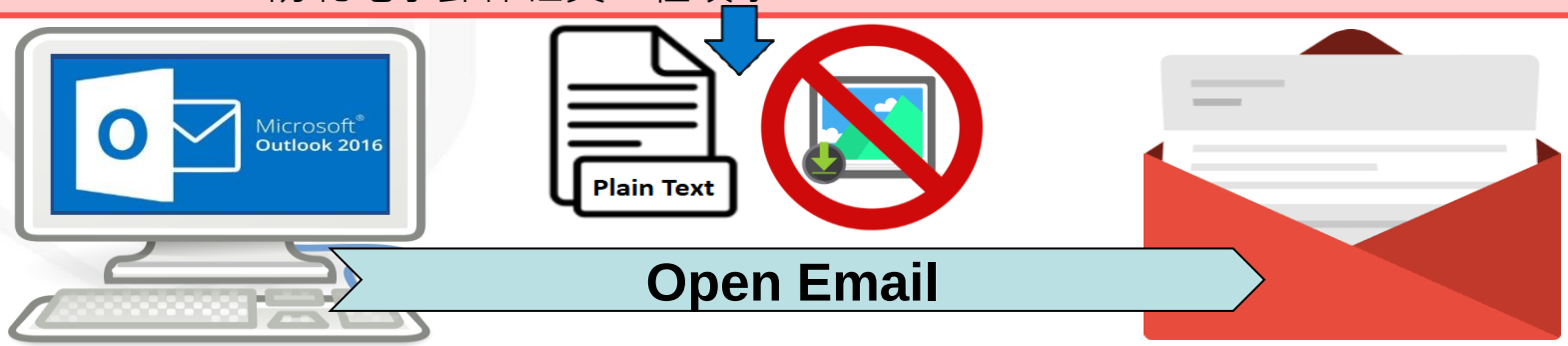
PowerPoint安全組態設定：
在受保護檢視中開啟不安全位置的檔案
來自網際網路與其他不安全位置的檔案，可能包含病毒、蠕蟲及其他惡意程式碼，GCB設定使用**受保護檢視**開啟檔案，以唯讀模式禁止編輯，降低可能發生的風險



Microsoft Office Outlook 2016

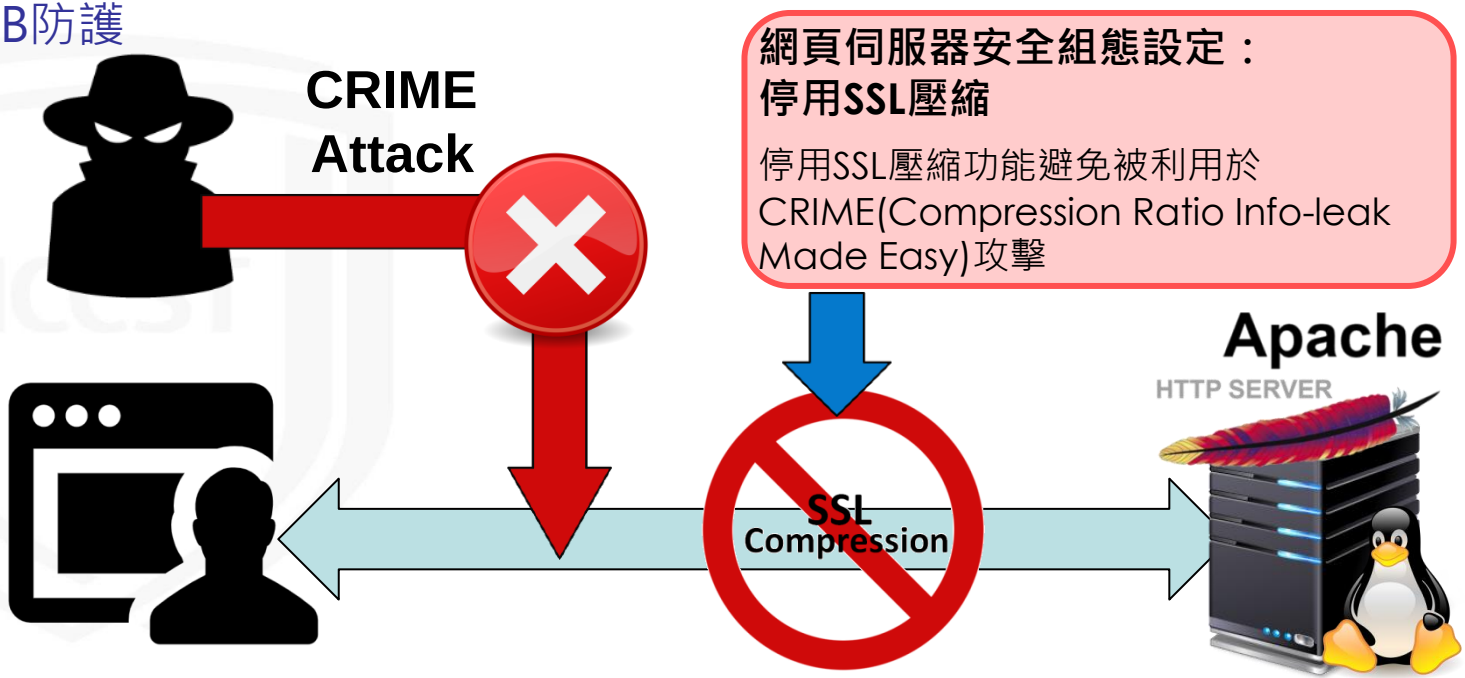
- 資安案例：資安團隊分析，自2020年2月新冠病毒(COVID-19)疫情蔓延，有大量以新冠病毒為主題之釣魚信件，誘使收件者點擊
- GCB防護

Outlook安全組態設定：
以純文字格式讀取電子郵件與限制自動圖片下載
GCB設定Outlook以**純文字格式**讀取電子郵件，避免自動執行郵件的html語法觸發惡意連結，**限制自動圖片下載**避免自動連線下載惡意程式，防範電子郵件社交工程攻擊



Apache HTTP Server 2.4

- 資安案例：NVD於2012年公布編號CVE-2012-4929之TLS/SSL協定漏洞，由於TLS/SSL支援壓縮傳輸資料，攻擊者藉由解析SSL壓縮的請求，取得身分驗證的Cookie，進而發動連線劫持與後續攻擊，導致機敏資料洩露
- GCB防護



大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

GCB導入說明(1/4)

- 導入GCB時，可從下列面向進行規劃

導入GCB

人 — 團隊有誰？
- 主要負責人員
- 可支援人員
- 委外廠商
- …

事 — 進行方式？
- 蒐集資源
- 分段測試
- 進行例外管理
- 部署及驗證
- …

物 — 相關物件？
- 導入標的、範圍
- 導入工具、GPO範本
- 測試環境軟硬體
- 文件
- …

時
- 規劃階段
- 審核階段
- 測試階段
- 部署階段
- …

各階段時程？
可否準時完成？

GCB導入說明(2/4)

建立團隊

- 指派GCB導入負責人員，負責統籌、規劃、追蹤導入進度，並彙整及保管完成導入與測試階段所產生之文件(如：測試紀錄、例外管理表單等)
- 建立團隊，納入相關支援人力

導入標的

- 確認欲進行導入之GCB項目，
  如：Windows 10、Internet Explorer 11、Google Chrome等

導入時程

- 規劃GCB導入預計起訖日
- 設定各階段作業之目標與預計起訖日

GCB導入說明(3/4)

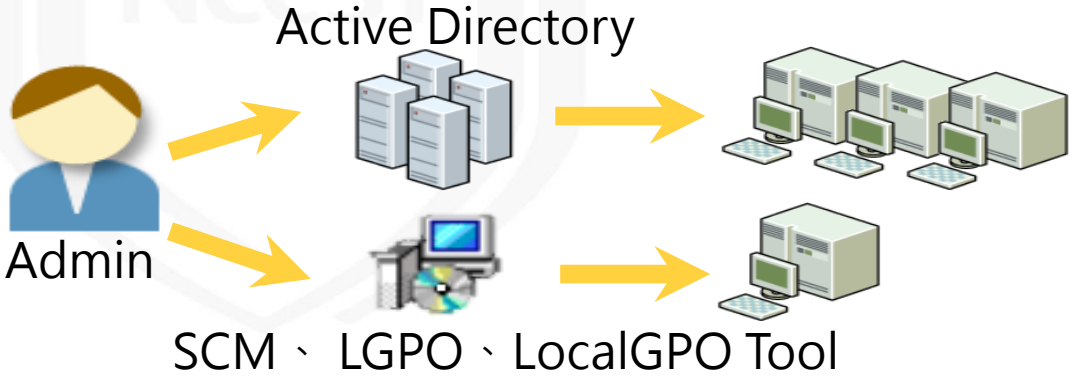
導入範圍

- 盤點機關內有多少台電腦符合導入標的，以確認須部署之範圍
- 用以盤點使用者電腦作業系統與應用程式之方式

資產清冊

導入工具

- 選定導入工具
- 確認使用之GPO範本來源
- 備妥測試環境

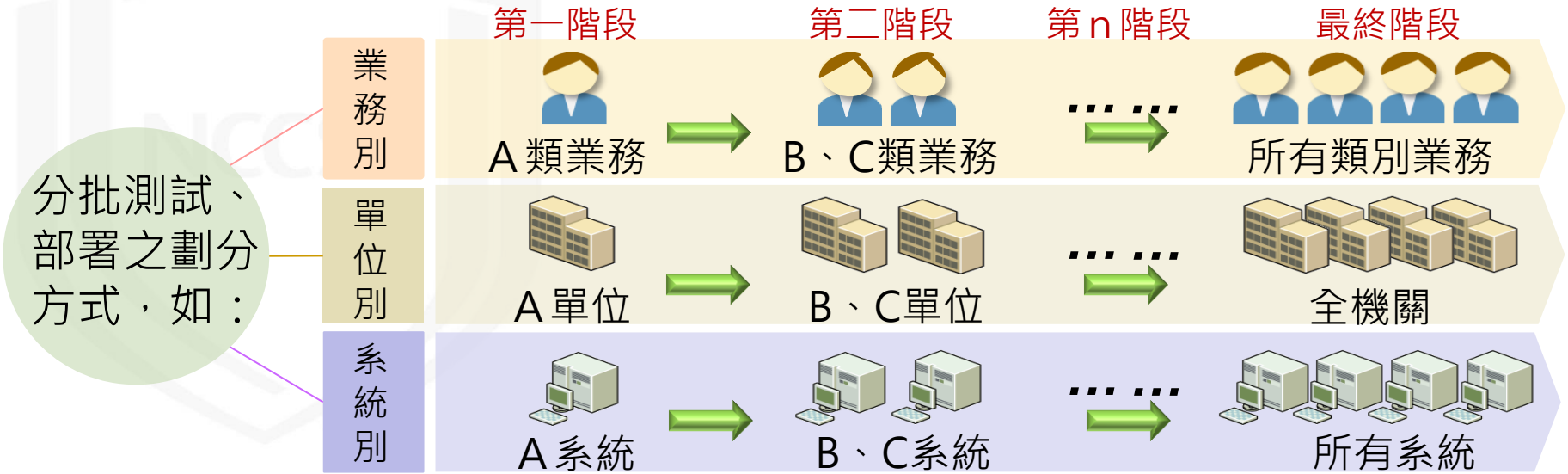


GCB部署參考資源

GCB導入說明(4/4)

導入方式

- 決定部署GPO之模式，如：透過AD部署、本機部署或AD與單機兩者同時施行
- 自行導入或由委外廠商協助導入
- 建議採行小範圍測試、部署，再擴及全機關

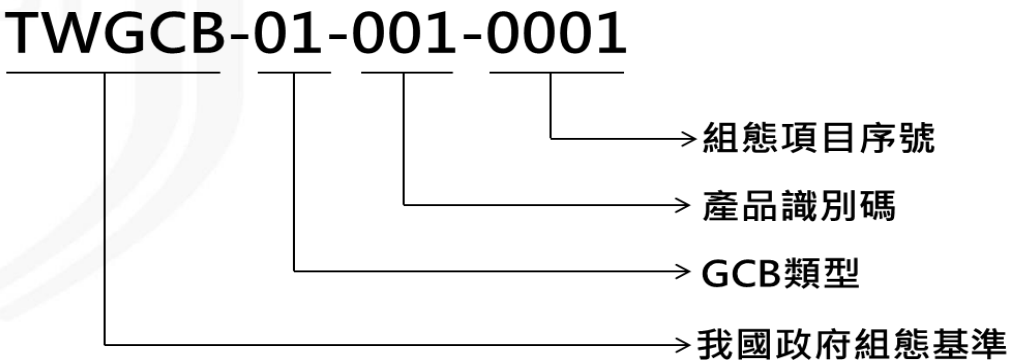


大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

TWGCB-ID介紹

- 為讓機關於GCB部署及實作過程中，可以快速識別與方便查找GCB組態設定，發展TWGCB-ID，做為我國政府組態基準編碼方式，為每項組態設定提供唯一的識別碼
- TWGCB-ID格式
  TWGCB-GCB類型-產品識別碼-組態項目序號
- 以Windows 7的「密碼最短使用期限」組態項目為例，其TWGCB-ID識別碼為「TWGCB-01-001-0001」



TWGCB-ID索引表

- 依據TWGCB-ID格式，已公告之GCB項目與TWGCB-ID對應之索引如下表，後續將依此規則遞增

項目	GCB類型	產品	TWGCB-ID區間
1	作業系統	Microsoft Windows 7	TWGCB-01-001-0001~9999
2		Microsoft Windows Server 2008 R2 SP1	TWGCB-01-002-0001~9999
3		Red Hat Enterprise Linux 5	TWGCB-01-003-0001~9999
4		Microsoft Windows 8.1	TWGCB-01-004-0001~9999
5		Microsoft Windows 10	TWGCB-01-005-0001~9999
6		Microsoft Windows Server 2012 R2	TWGCB-01-006-0001~9999
7		Microsoft Windows Server 2016	TWGCB-01-007-0001~9999
8	瀏覽器	Microsoft Internet Explorer 8	TWGCB-02-001-0001~9999
9		Microsoft Internet Explorer 11	TWGCB-02-002-0001~9999
10		Google Chrome	TWGCB-02-003-0001~9999
11		Mozilla Firefox	TWGCB-02-004-0001~9999
12		Microsoft EDGE	TWGCB-02-005-0001~9999
13	網通設備	Wireless	TWGCB-03-001-0001~9999
14		Juniper Firewall	TWGCB-03-002-0001~9999
15		Fortinet Fortigate	TWGCB-03-003-0001~9999
16		Cisco Firewall	TWGCB-03-004-0001~9999
17	應用程式	Exchange Server 2013	TWGCB-04-001-0001~9999
18		Microsoft IIS 8.5	TWGCB-04-002-0001~9999

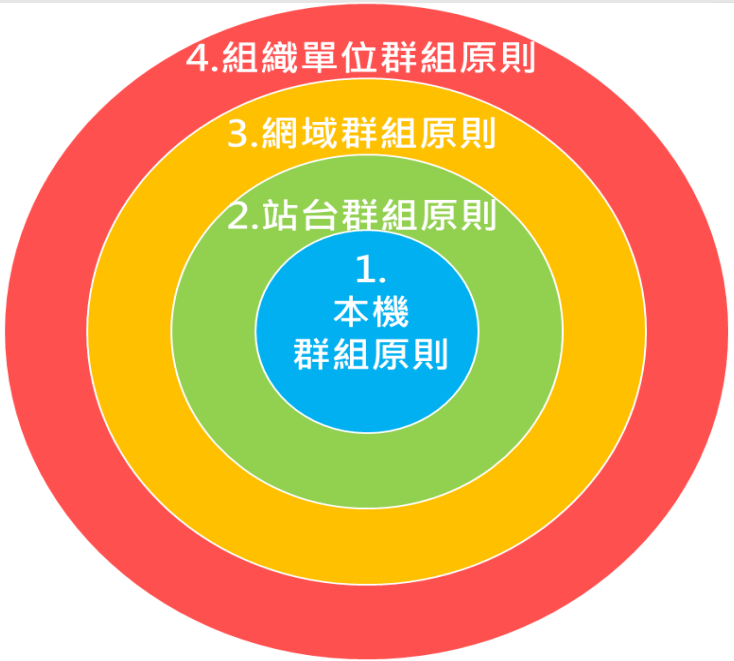
大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

常見問答(1/6)

Q1 使用網域部署政府組態基準(GCB)後，以Rsop.msc查看的設定值與使用Gpedit.msc查看的設定值不一樣，該以哪一個為標準呢？

– 在已加入網域的電腦中，若同一條群組原則在Rsop.msc與Gpedit.msc皆有設定值，依群組原則套用順序，請以Rsop.msc的設定值為標準



常見問答(2/6)

Q2 導入政府組態基準(GCB)後，若須變更設定值該如何處理？

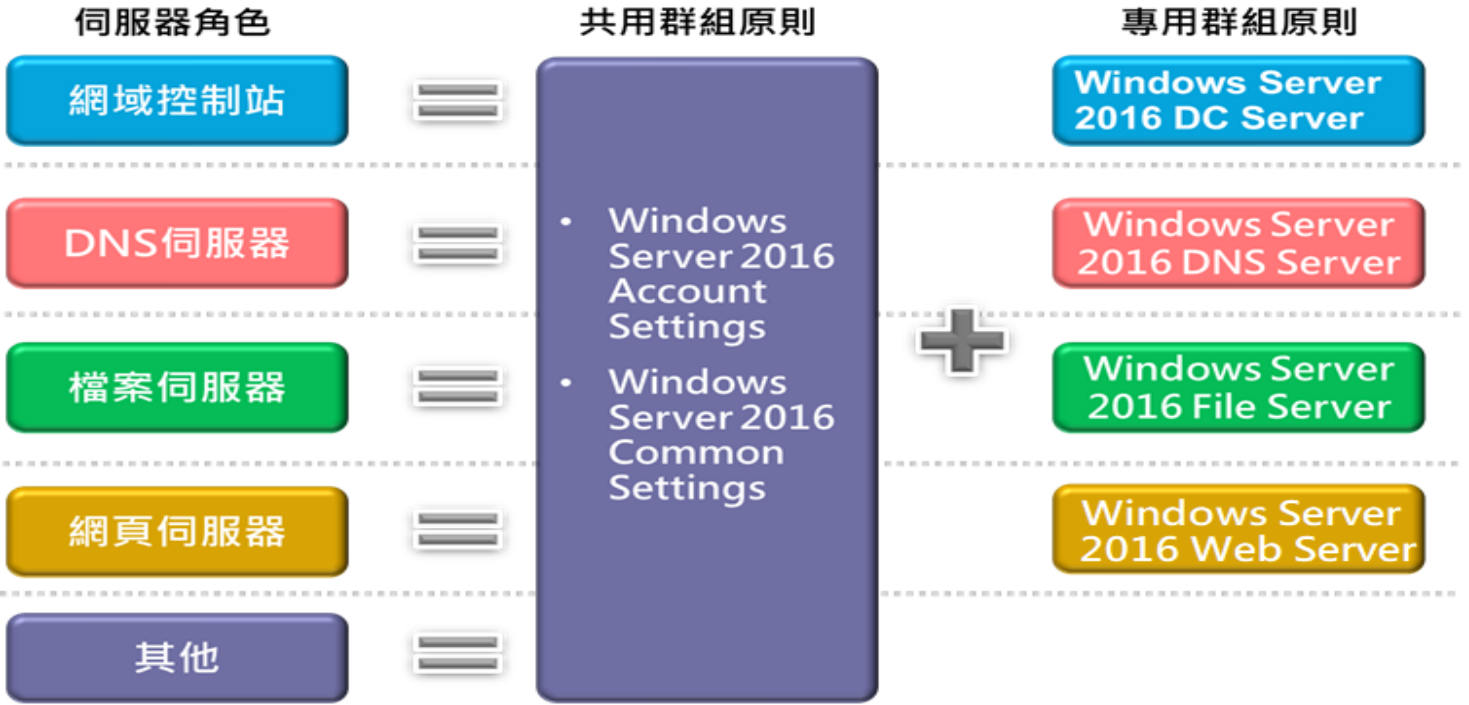
- 若機關須變更政府組態基準(GCB)條目設定值，請進行例外管理，於公告「政府組態基準文件」中表列之項目，應列入例外管理項目，惟例外項目仍應定期審核是否合宜
  - 如：使用者權限指派、安全性選項、防火牆輸入規則等

TWGCB-ID	規則名稱
TWGCB-01-001-0280	核心網路功能-動態主機設定通訊協定 (DHCP-In)
TWGCB-01-001-0281	核心網路功能-IPv6 的動態主機設定通訊協定 (DHCPV6-In)

- 不在「政府組態基準文件」表列之項目，無需列入例外管理項目
  - IE瀏覽器之信任網站(建議仍應具備審核機制)

常見問答(3/6)

Q3 Windows Server 2016伺服器劃分不同角色，該如何進行部署?



常見問答(4/6)

- GPO部署的優先順序說明
  - 當專用群組原則與共用群組原則的GPO同時套用於伺服器時，**專用群組原則應優於共用群組原則GPO**

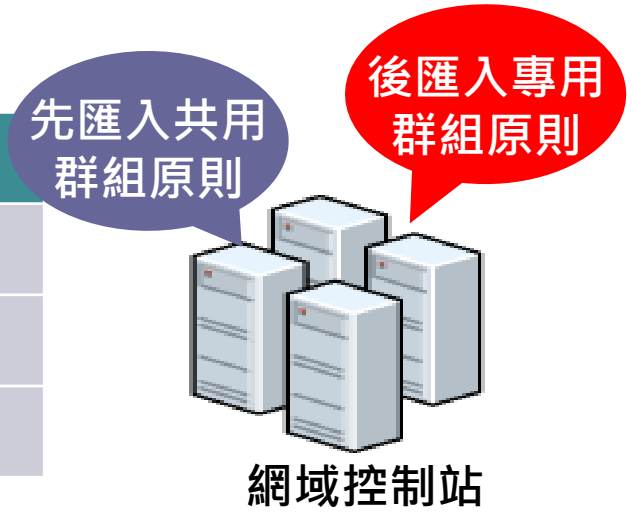
伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2016 DC Server	**專用群組原則**
	2	Windows Server 2016 Account Settings	共用群組原則
	3	Windows Server 2016 Common Settings	共用群組原則
DNS伺服器	1	Windows Server 2016 DNS Server	**專用群組原則**
	2	Windows Server 2016 Account Settings	共用群組原則
	3	Windows Server 2016 Common Settings	共用群組原則
File伺服器	1	Windows Server 2016 File Server	**專用群組原則**
	2	Windows Server 2016 Account Settings	共用群組原則
	3	Windows Server 2016 Common Settings	共用群組原則
Web伺服器	1	Windows Server 2016 Web Server	**專用群組原則**
	2	Windows Server 2016 Account Settings	共用群組原則
	3	Windows Server 2016 Common Settings	共用群組原則

常見問答(5/6)

- 以網域控制站GPO部署為範例
  - 單機部署：使用LGPO程式導入
    - 單機部署情況下，後匯入的GPO會優於之前匯入的GPO
    - 要**先匯入共用群組原則的2個GPO後，接續再匯入專用群組原則**

Windows Server 2016 DC Server GPO

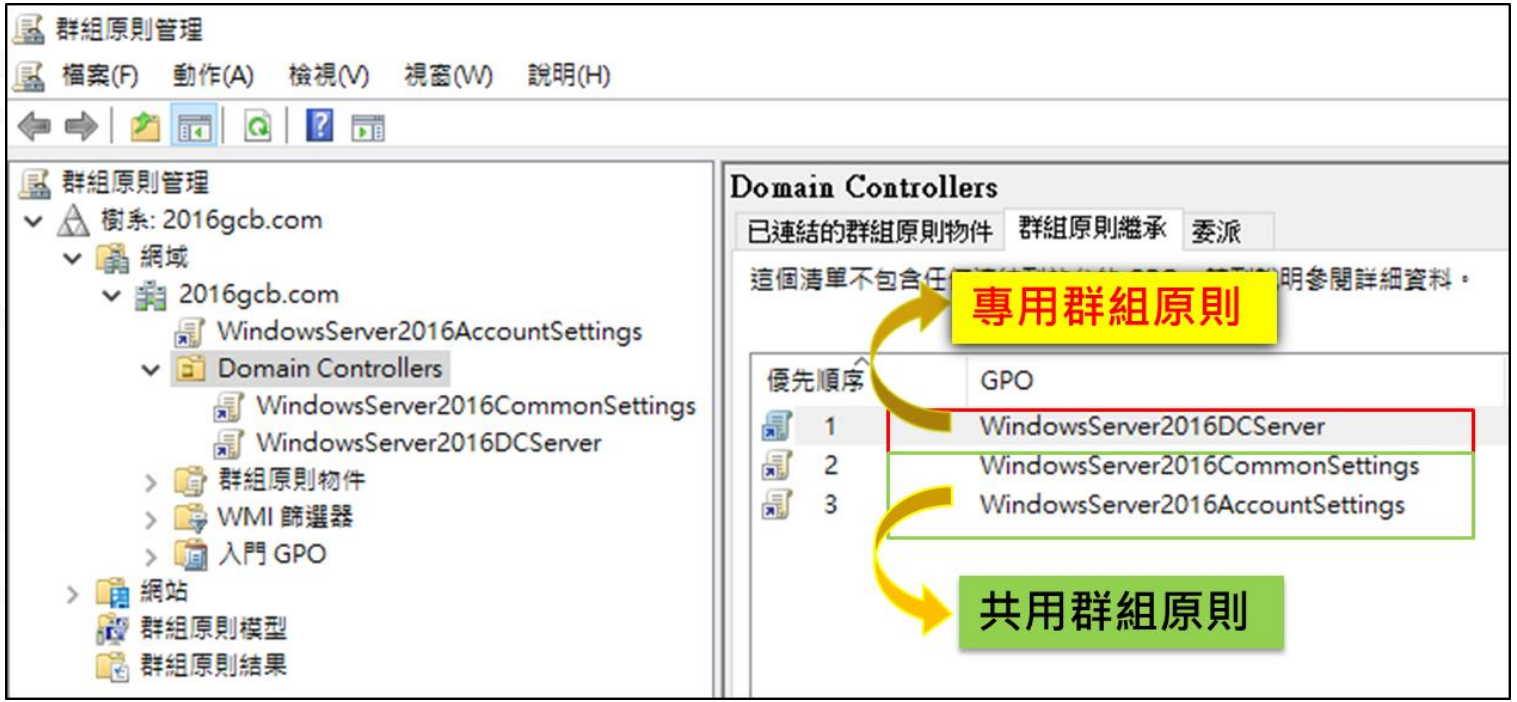
伺服器角色	GPO優勢順序	GPO	分類
網域控制站	1	Windows Server 2016 DC Server	**專用群組原則**
	2	Windows Server 2016 Account Settings	共用群組原則
	3	Windows Server 2016 Common Settings	共用群組原則



常見問答(6/6)

– AD部署：使用群組原則管理工具導入

➢ 在已連結的群組原則物件中的連結順序，**將專用群組原則的Windows Server 2016 DC Server GPO調整到優勢於共用群組原則GPO**



政府組態基準(GCB)FAQ專區

- 行政院國家資通安全會報技術服務中心網站
  - https://www.nccst.nat.gov.tw/GCB?lang=zh

政府組態基準(GCB)

政府組態基準(Government Configuration Baseline，簡稱GCB)目的在於規範資通訊設備(如個人電腦、伺服器主機及網通設備等)的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。本專區提供GCB說明文件、相關資源及常見問答，協助各機關進行導入規劃與實作。

歡迎透過意見信箱提供您的寶貴意見！

預告版說明文件 | GCB說明文件 | GCB部署資源 | 教育訓練教材 | 數位教材影片 | FAQ

作業系統

Windows 7、Windows 10、Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016、RedHat Enterprise Linux 5

瀏覽器

Internet Explorer、Google Chrome、Mozilla FireFox、Microsoft Edge

網通設備

Fortinet Fortigate、Juniper Firewall、無線網路

應用程式

Exchange Server 2013、IIS 8.5

綜合問答

GCB部署、部署工具、GCB條目測試、例外管理

大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

資安威脅與修補空窗期

- Skybox Security公布之資安弱點與威脅趨勢報告指出，2019年遭利用的弱點中，廠商釋出修補程式前即有攻擊利用程式出現，而廠商釋出修補程式幾週內為攻擊利用程式產生的高峰期
- 弱點(CVE)公布後到廠商釋出修補程式之空窗期，是駭客利用的絕佳時機

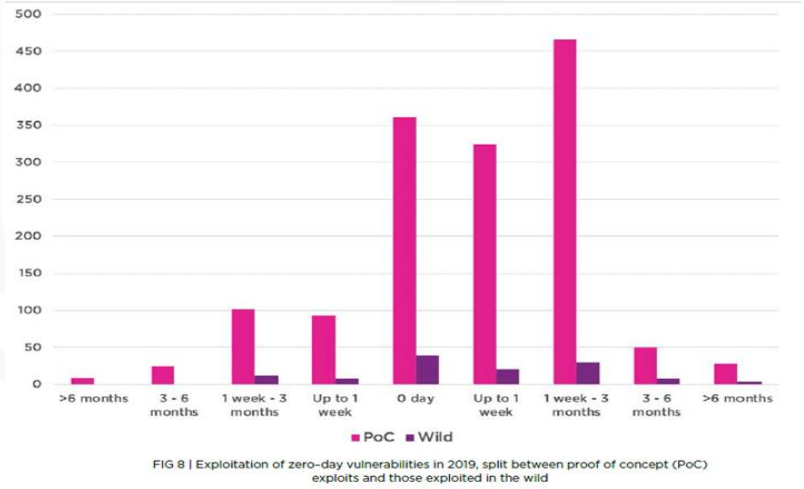
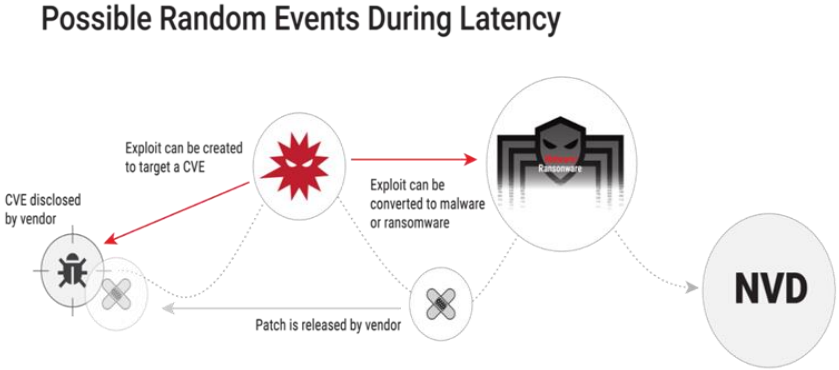


FIG 8 | Exploitation of zero-day vulnerabilities in 2019, split between proof of concept (PoC) exploits and those exploited in the wild



弱點應變關鍵

- 不定期爆發之重大弱點，若未能即時反應，將嚴重影響機關業務正常運作，亦可能造成機關形象受損。因此當弱點爆發時，如能確實掌握機關資通系統與使用者電腦情況，即可快速因應，將損害降至最低

- 如何在弱點發布後，快速反應所面臨的威脅與受影響版本
- 如何在確認受影響版本後，可確實掌握受影響範圍
- 如何在確認受影響範圍後，快速因應處理
- 如何在應變處理後，持續追蹤弱點修補情形

資通安全管理法相關規定

- 資通安全管理法第十條
  - 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫
- 資通安全管理法施行細則第六條規範資通安全維護計畫應包含之項目
  - 第六款規範機關應盤點資通系統，並標示核心資通系統與相關資產
  - 第七款規範機關應建立相關風險評估機制，以針對盤點之資產進行資通安全風險評估

資通安全管理法

政府機關

- **Windows平台資通系統與使用者電腦之軟體資產**
- Windows平台資通系統與使用者電腦之硬體資產
- 類Unix平台資通系統與使用者電腦之軟、硬體資產
- 辦公室事務設備之韌體資產

弱點告警方式

弱點比對通知

重大漏洞警訊通知

VANS機制目標

- 確認資訊資產弱點
  - 蒐集政府機關使用之軟體資訊，並與國際權威弱點資料庫資訊進行比對，當使用軟體存在重大弱點時，即時得知與應變處理
- 追蹤資訊資產弱點修補情形
  - 追蹤資訊資產弱點修補情形，並同步進行資訊資產版本資料更新，以維持資料內容之有效性
- 降低重大弱點管控與追蹤之成本
  - 利用弱點資料庫搭配自動比對方式，提供政府機關相關弱點資訊與自我檢查機制，以降低重大弱點管控與修補情形追蹤所需之人力與資源

VANS推動歷程

104~106年

- 系統開發
- 針對資安責任等級A與B級機關辦理推廣說明會
- 執行二階段機關試行專案，並依據機關意見回饋精進系統功能與服務流程
- 開放資安責任等級A與B級機關申請使用

107年

- 針對資安責任等級A與B級機關辦理推廣說明會
- 執行2次資安服務團專案，於輔導課程推廣VANS，並於實地輔導作業協助2個機關導入VANS
- 與6家國內資產管理廠商洽談合作事宜

108年

- 為提升公務機關辦公場所資安防護能力，擴增盤點範圍與資產蒐集內容
- 配合資安服務團實地輔導辦理試行導入
- 辦理2場次推廣說明會
- 開發API介接格式，供合作廠商進行軟體與VANS間之資料介接

109年

- 執行資安服務團專案，辦理輔導課程並於實地輔導作業協助機關導入VANS
- 辦理實作訓練課程，透過實機操作協助機關了解VANS運作方式
- 配合行政院辦理VANS輔導服務，協助機關進行「全機關」導入作業

大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

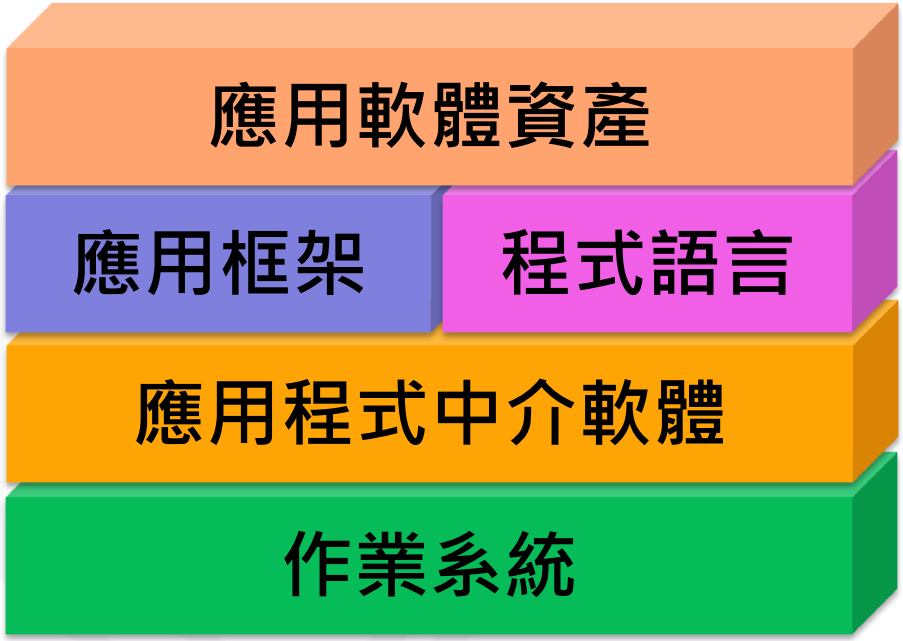
政府機關資安弱點通報機制(1/2)

- 政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並降低重大弱點爆發時可能造成之損害
  - 定期蒐集資通系統主機與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達到降低風險與管控成本等目標
  - 將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊

政府機關資安弱點通報機制(2/2)

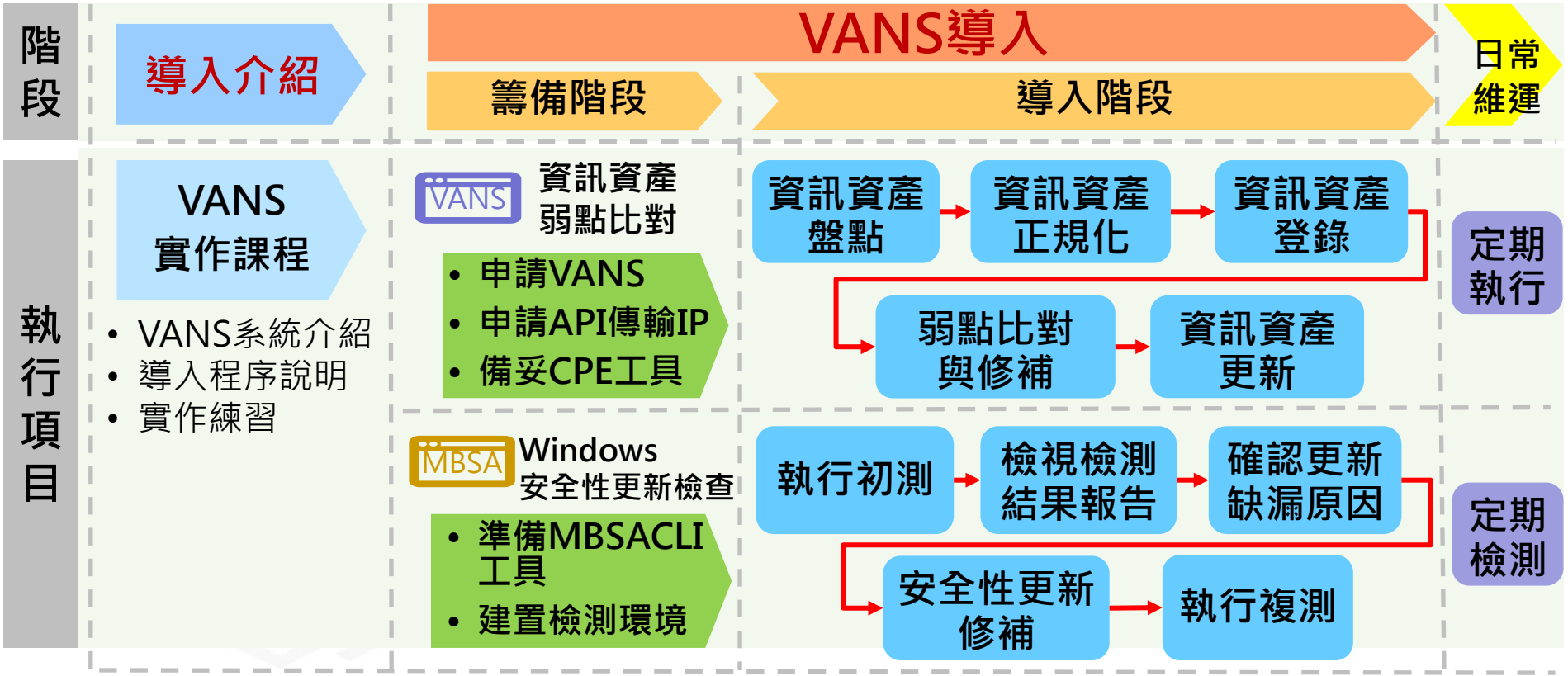
- VANS可協助機關落實資通安全管理法之資產盤點與風險評估應辦事項，並提供以下服務
  - 透過VANS持續維護資訊資產盤點資料
  - 針對機關登錄的資訊資產項目進行弱點比對，以協助進行系統化風險評估
  - 依照機關訂定之風險值門檻，即時提醒資訊資產風險情形，並進行弱點評估與修補作業
  - 提供微軟安全性更新檢測報告解析功能，協助機關以自動化方式檢視安全性更新落實程度

VANS資訊資產涵蓋範圍



Adobe MySQL Struts² php Microsoft .net Microsoft IIS Apache Tomcat Windows Server

VANS導入作業流程


階段
導入介紹
VANS導入
籌備階段
導入階段
日常維運
執行項目
VANS
實作課程
• VANS系統介紹
• 導入程序說明
• 實作練習
VANS
資訊資產
弱點比對
• 申請VANS
• 申請API傳輸IP
• 備妥CPE工具
資訊資產盤點
資訊資產正規化
資訊資產登錄
弱點比對與修補
資訊資產更新
定期執行
MBSA
Windows
安全性更新檢查
• 準備MBSACLI工具
• 建置檢測環境
執行初測
檢視檢測結果報告
確認更新缺漏原因
安全性更新修補
執行複測
定期檢測

大綱

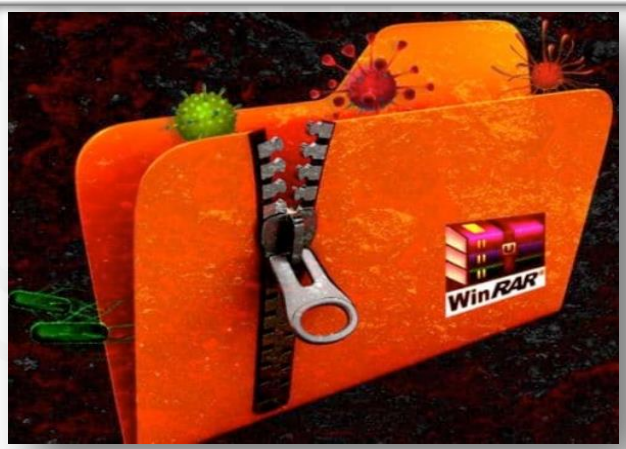
- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

WinRAR ACE弱點(1/3)

- Check Point於108年2月揭露，WinRAR存在CVE-2018-20250弱點，受影響範圍包含全球5億用戶端
- 建議儘速升級至WinRAR 5.70以後版本

WinRAR 爆出 10 年未被發現的大漏洞：解壓縮同時會把病毒安裝到電腦裡

2019/02/23 讚 1,003 分享 unwire.hk



iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會

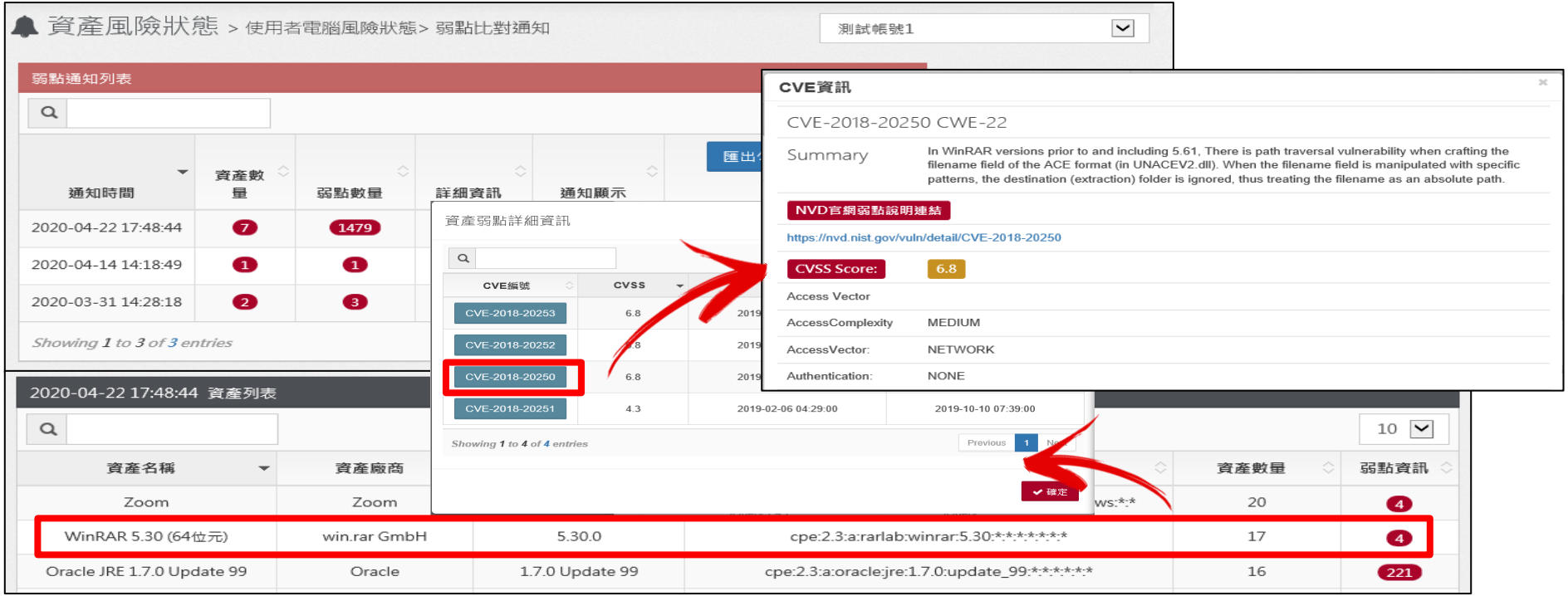
新聞

WinRAR漏洞被揭露的第一周就有超過100種攻擊

WinRAR在2月底釋出的WinRAR 5.70修補了漏洞，用戶應儘快升級或部署有效的防毒軟體

WinRAR ACE弱點(2/3)

- 透過VANS系統弱點比對功能，機關得知目前擁有之資產中有安裝17套WinRAR 5.30.0版本，該版本存在4個弱點



WinRAR ACE弱點(3/3)

- 機關更新WinRAR至5.90.0版本，並進入VANS系統更新資訊資產

- 更新後，弱點比對結果顯示已無WinRAR相關弱點

預期效益

- 縮短弱點修補空窗期
  - VANS每日與NVD更新以提供最新弱點比對結果，當使用軟體存在重大弱點時，機關得以及早得知與應變處理
- 降低重大弱點管控與追蹤之成本
  - 利用弱點資料庫搭配自動比對方式，提供相關弱點資訊與自我檢查機制，以降低重大弱點管控與修補情形追蹤的人力與資源成本
- 追蹤軟體資產弱點修補情形
  - 定時至VANS更新資訊資產項目，完整掌握各主機弱點修補情形

服務申請流程

機關提出申請
- 電話申請
- Email申請

提供申請資訊
- 單位資訊
- 聯絡資訊

參閱操作手冊
- 操作諮詢
- 服務說明

開始使用服務
- 資料建立
- 弱點比對

聯絡窗口：陳耕硯先生
聯絡電話：(02)6631–6458
聯絡信箱：
julianchen@nccst.nat.gov.tw

後續推動重點

- 目前共同供應契約中已有廠商可提供具備CPE轉換功能之軟體，可降低VANS導入所耗費之人力與時間
- VANS歷經試辦導入作業、推廣說明會、資安服務團等施行後，已依機關反應與建議精進強化，考量VANS已日趨成熟，後續**規劃納入法遵要求，並於110年底前完成A級與B級公務機關導入**，以期透過VANS進一步強化政府機關資訊資產之資安管理

大綱

- GCB推動說明
  - 資安法規要求
  - GCB發展現況
  - GCB導入說明
  - TWGCB-ID簡介
  - 常見問答
- VANS機制說明
  - 作業流程
  - 應用情境
  - 常見問答

常見問答

常見問答(1/2)

Q1 VANS與弱點掃描之差異？

項目	VANS	弱點掃描
資訊蒐集方式	透過作業系統內建工具或第三方軟體，產出已安裝資訊資產清單	透過網路遠端執行掃描
弱點查詢方式	將登錄至VANS之資訊資產項目與版本進行弱點比對	透過弱掃軟體plugin進行弱點偵測
比對範圍	登錄至VANS之所有資訊資產	目標主機對外服務使用套件
時間性	每10分鐘比對1次	定期執行掃描

常見問答(2/2)

Q2 如何得知哪些資產較危險，應立即處理？

- 弱點比對結果會顯示各資產風險指數，計算方式為將各資訊資產比對到的每個弱點CVSS分數加總平均，風險指數較高者建議優先處理

Q3 上傳資產清單時，VANS系統支援哪些格式？

- VANS系統可接受上傳之檔案格式包含Excel活頁簿(*.xlsx)、Excel 97-2003活頁簿(*.xls)及OpenDocument試算表(*.ods)等3種，機關可透過上述格式上傳資產清單

Q4 相同弱點只會通知一次呢？還是會持續寄通知信？

- VANS機制主要提供機關即時掌握弱點、有效修補弱點及做好弱點管理，進而降低資安風險，相同弱點僅會通知一次

報告完畢
敬請指教

參考資料(1/2)

- 政府組態基準(GCB)專區
  - https://www.nccst.nat.gov.tw/GCB
- CIS Controls V7.1
  - https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/
- 勒索病毒qkG
  - https://blog.trendmicro.com.tw/?paged=2&cat=1943
- Forgotten MS Office Features Used to Deliver Malware (Symbolic Link)
  - https://www.vmray.com/cyber-security-blog/forgotten-ms-office-features-used-deliver-malware/
- Abusing the SYLK file format
  - https://outflank.nl/blog/2019/10/30/abusing-the-sylk-file-format/
- 新型病毒！滑鼠滑過PowerPoint，就中毒
  - https://blog.trendmicro.com.tw/?p=50374
- 網路罪犯以新冠病毒為主題，對企業發動社交工程攻擊
  - https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24602

參考資料(2/2)

- 淺談IFrame式Clickjacking攻擊與防護
  - https://blog.darkthread.net/blog/iframe-clickjacking/
- CRIME(維基百科)
  - https://zh.wikipedia.org/wiki/CRIME
- Skybox Security Research Report
  - https://www.skyboxsecurity.com/trends-report/
- Official Common Platform Enumeration (CPE) Dictionary
  - https://nvd.nist.gov/products/cpe
- WinRAR爆出10年未被發現的大漏洞：解壓縮同時會把病毒安裝到電腦裡
  - https://buzzorange.com/techorange/2019/02/23/winrar-hacked/
- WinRAR漏洞被揭露的第一週就有超過100種攻擊
  - https://www.ithome.com.tw/news/129402
- Google Chrome漏洞
  - https://www.twcert.org.tw/tw/cp-104-3487-99440-1.html