雲林縣政府
YUNLIN COUNTY GOVERNMENT

107年雲林縣政府GCB
政府組態基準導入說明會

rapixus.com

大綱

- 專案目標與範疇
- GCB推動進程與現狀
- GCB規範內容
- GCB導入流程

RAPIXUS
瑞思資訊股份有限公司

1

專案目標與範疇

RAPIXUS
瑞思資訊股份有限公司

專案目標與範疇

為配合行政院國家資通安全推動政府組態基準設定(以下簡稱GCB)，以提升用戶端安全性，降低成為駭客入侵管道，將於本府各單位及所屬單位導入政府組態基準(GCB)設定。

建置GCB管理系統

專案建置GCB管理專用系統，並協助建立共通GCB套用範本。

GCB用戶端程式部署及GCB規則導入

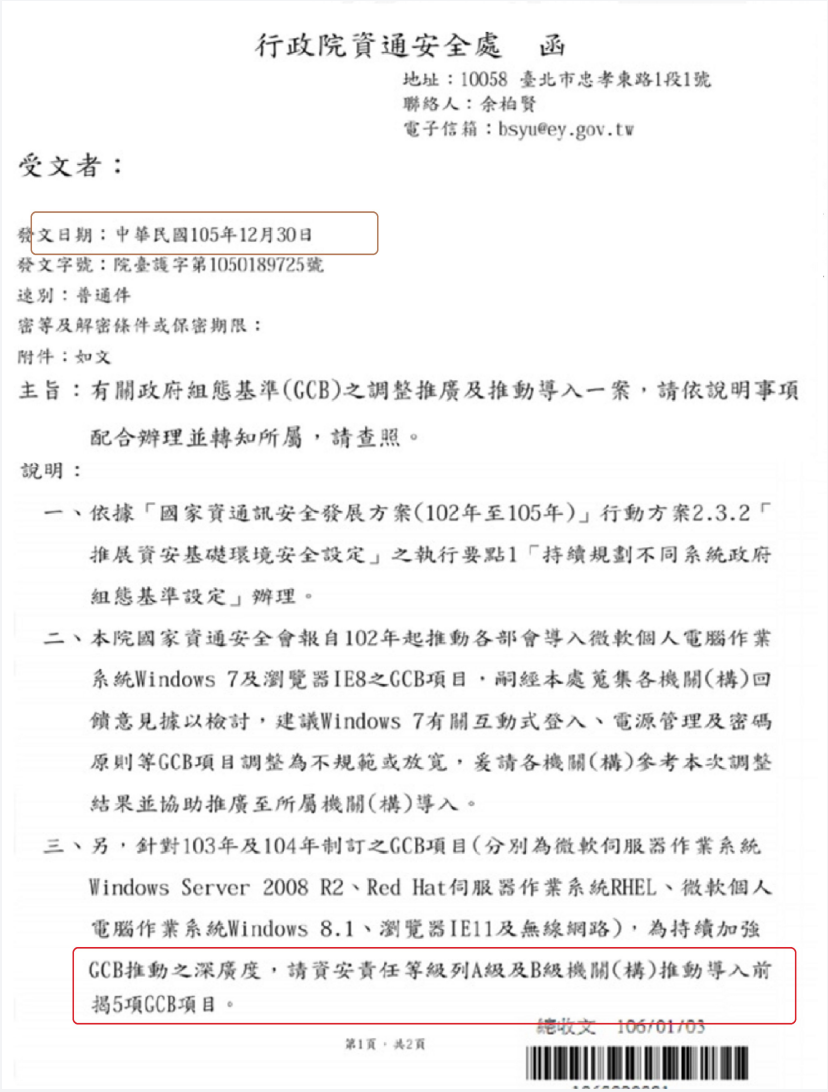
107年 11/30 目標導入2,000台Client端程式佈署，以A、B級機關優先導入，後續導入C+機關，並協助建立GCB管理規則。

2

GCB推動進程與現狀

GCB推動進程與現況

行政院資通安全處函文



行政院資通安全處　函

地址：10058 臺北市忠孝東路1段1號
聯絡人：余柏賢
電子信箱：bsyu@ey.gov.tw

受文者：

發文日期：中華民國105年12月30日
發文字號：院臺護字第1050189725號
速別：普通件
密等及解密條件或保密期限：
附件：如文

主旨：有關政府組態基準(GCB)之調整推廣及推動導入一案，請依說明事項配合辦理並轉知所屬，請查照。

說明：

一、依據「國家資通訊安全發展方案(102年至105年)」行動方案2.3.2「推展資安基礎環境安全設定」之執行要點1「持續規劃不同系統政府組態基準設定」辦理。

二、本院國家資通安全會報自102年起推動各部會導入微軟個人電腦作業系統Windows 7及瀏覽器IE8之GCB項目，嗣經本處蒐集各機關(構)回饋意見據以檢討，建議Windows 7有關互動式登入、電源管理及密碼原則等GCB項目調整為不規範或放寬，爰請各機關(構)參考本次調整結果並協助推廣至所屬機關(構)導入。

三、另，針對103年及104年制訂之GCB項目(分別為微軟伺服器作業系統Windows Server 2008 R2、Red Hat伺服器作業系統RHEL、微軟個人電腦作業系統Windows 8.1、瀏覽器IE11及無線網路)，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5項GCB項目。

總收文 106/01/03

第1頁，共2頁

RAPIXUS 瑞思資訊股份有限公司

GCB政策為何？

- **根據 107/7/6 最新公布資通安全管理法施行細則草案總說明**
  https://join.gov.tw/policies/detail/42d0853b-76f8-46c2-a879-e72f13d0dc9e

附表一　資通安全責任等級 A 級之公務機關應辦事項
附表三　資通安全責任等級 B 級之公務機關應辦事項

政府組態基準	經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。

法遵依循

GCB皆為技術面應辦事項

A、B、C級單位導入期程

	資安責任等級區分	GCB導入期程
A	1. 總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府 2. 立法院、司法院、考試院、監察院及行政院等所屬二級機關、相當二級機關之獨立機關。但其業務或組織單純者，得報經其上級機關核准，調整為B級或C級。 3. 凡涉及外交、國防、國土安全及掌理全國財政、經濟、警政等重要業務之機關，如外交部領事事務局、內政部警政署刑事警察局等。 4. 負責能源、水資源、通訊傳播、交通、金融、緊急救護、高科技園區等關鍵資訊基礎設施之營運機構，如交通部民用航空局飛航服務總臺、台北市自來水事業處等。 5. 保有全國性個人資料檔案之機關，如勞動部勞工保險局、衛生福利部中央健康保險署等。	106~107年推廣導入
B	1. 縣(市)政府。 2. 凡涉及社會秩序及人民財產業務之機關，如地方政府警察局、地方政府地政事務所等。 3. 保有區域性或地區性個人資料檔案之機關，如財政部各區國稅局、地方政府戶政事務所等。	
C	其他地政府機關及地方政府民意機關等。	107年推廣導入

3

GCB規範內容

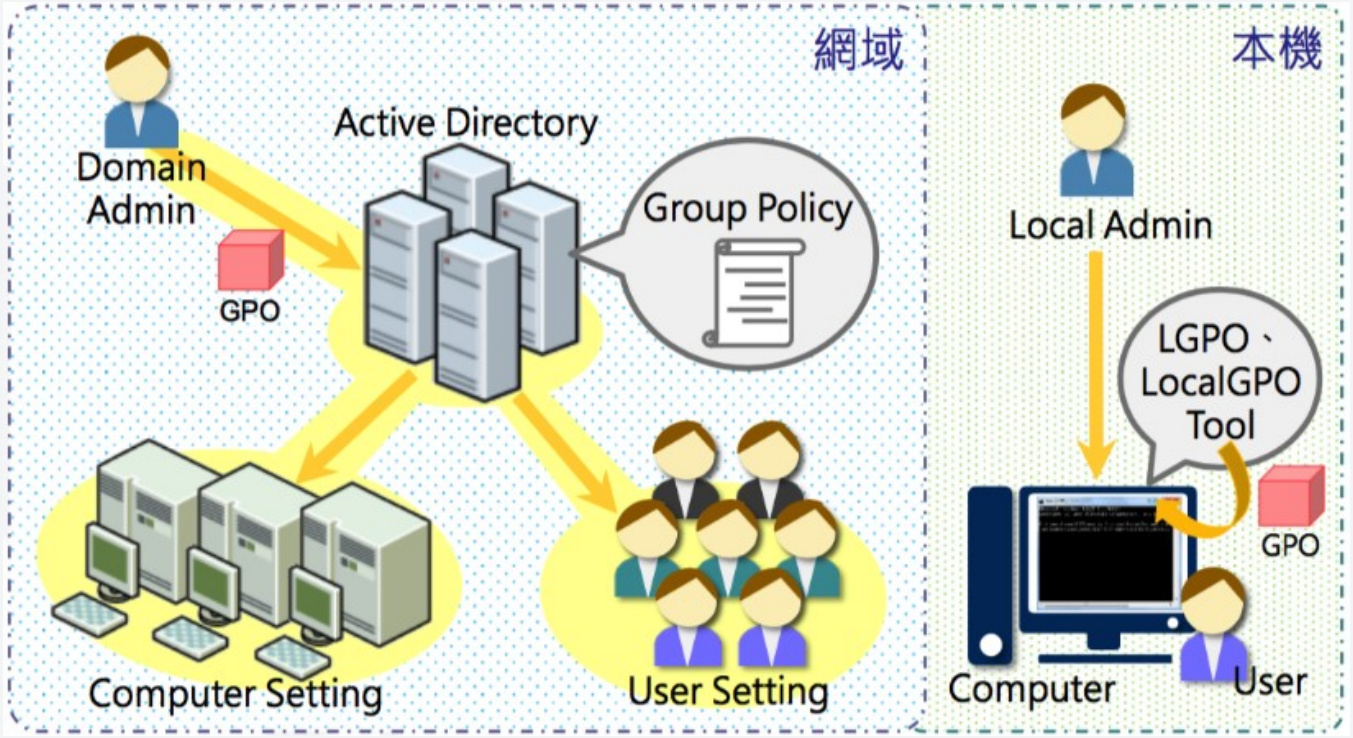
GCB起源

政府組態基準(Government Configuration Baseline)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）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 疑慮。

NIST：美國國家標準技術研究所
NCCST：行政院國家資通安全會報技術服務中心

群組原則物件 (GPO)說明

- 技服中心依據各種作業環境將各項組態設定打包為「群組原則物件」(GPO)，**GPO就是是群組原則組態設定的集合物件**
- GPO套用的方式可分為網域與本機兩種環境



RAPIXUS 瑞思資訊股份有限公司

群組原則物件 (GPO)說明

- Win7、 Win8.1、 Win10等作業系統，GPO內容依以下四大區分律定組態設定規範，不同作業系統也有不同數量的組態設定項目
  - 帳號設定（Account Policy）
  - 電腦設定（Computer Settings）
  - 使用者設定（User Settings）
  - 個人防火牆設定Firewall Settings
- 瀏覽器部分計有IE8、IE11及Google Chrome等不同組態設定規範。

GCB不同條目的規範數量

項目名稱	版本	GCB規範項目數量
Win7	V1.8	277
Win2008 R2	V1.6	332
Win8.1	V1.4	334
Win10	V1.0	345
Win2012 R2	V1.0	239
IE8	V1.8	115
IE11	V1.1	154
Chrome	V1.1	30

政組態設定安全防護案例

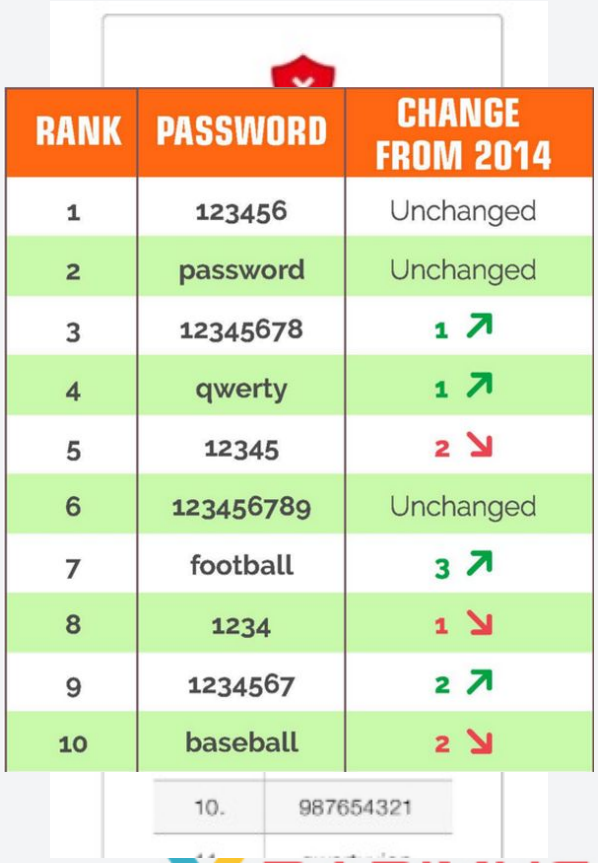
- 情境：使用者不小心將含有惡意程式的隨身碟插入公務電腦中
- 防護：
  - 組態設定禁止可攜式媒體的Autoruns與自動播放功能，因此可降低電腦自動執行惡意程式與遭受感染之機率
  - 組態設定強制作業系統進行安全性更新以保持在最新狀態，因此可大幅減少惡意程式所能利用之漏洞
  - 倘若網域內其他電腦遭受惡意程式感染，組態設定禁止電腦回應多點傳送與廣播類型的封包，可避免惡意程式的感染範圍擴大

新聞案例(1) iThome,2017-01-18

2016年最常見的懶人密碼是這個，你也是嗎？

根據統計，2016年1000萬筆外洩資料中最常使用的密碼為123456，其次是123456789、qwerty、12345678等，前25大常用密碼佔1000萬筆資料的一半以上。

出自：http://www.ithome.com.tw/news/111256



RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
10.	987654321	

新聞案例(2) iThome,2017-08-04

Chrome擴充程式開發者要小心網釣郵件！駭客挾持擴充程式大發廣告財

最近傳出部份的Chrome擴充程式開發者收到網路釣魚郵件，騙取開發者帳號與密碼，駭客藉此挾持擴充程式，上傳含有廣告及垃圾訊息的版本，包括Copyfish與Web Developer等擴充程式已受害

出自： http://www.ithome.com.tw/news/116090

GPO可實現統一的資安政策

Case1-密碼長度限制，複雜度-增加入侵難度

原則	安全性設定
使用可還原的加密來存放密碼	已停用
密碼必須符合複雜性需求	已啟用
密碼最長使用期限	180 天
密碼最短使用期限	0 天
強制執行密碼歷程記錄	3 記憶的密碼
最小密碼長度	12 個字元

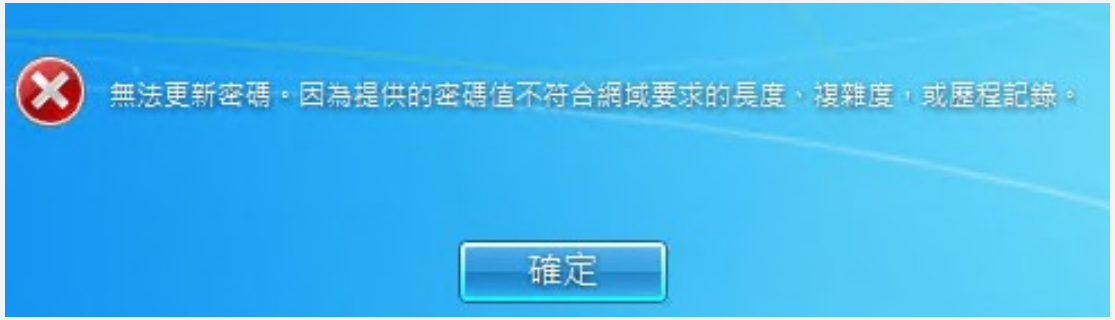
包含下列四種字元中的三種：

(1)英文大寫字元(A到Z)

(2)英文小寫字元(a到z)

(3)10進位數字(0到9)

(4)特殊符號(例如：!、$、#、%)



小提示：未加入網域用戶當變更密碼時需配合GCB政策設定複雜密碼與長度

GPO可實現統一的資安政策

Case2-禁止Google瀏覽器安裝套件-避免惡意套件安裝

CCE-ID	Title
☑ chr-030	設定擴充功能安裝黑名單

RAPIXUS 瑞思資訊股份有限公司

GPO可實現統一的資安政策

Case3-禁止 IE/Google瀏覽器自動填入-增加設備使用安全

RAPIXUS 瑞思資訊股份有限公司

GPO可實現統一的資安政策

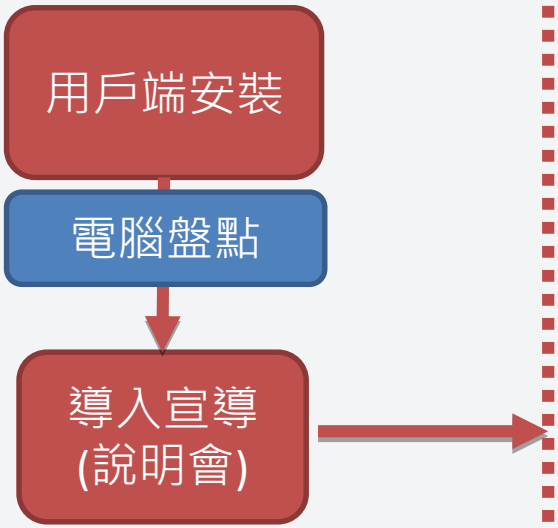
Case4-禁止 IE/Google瀏覽器取得定位-保護用戶隱私

RAPIXUS 瑞思資訊股份有限公司

4

GCB導入流程

GCB導入流程採用PDCA流程(1/2)



1. 預先進行用戶端安裝。
2. 單位GCB管理者可於系統查看與盤點所屬電腦。
3. 宣導GCB導入提昇資安防護的必要性。

規劃
Plan

組態範本

業務系統盤點

1. 資訊中心已整理本府組態範本供各機關套用。
2. 機關GCB管理人員盤點各單位業務系統，加入IE信任網站。
3. 指派業務相關人員**測試各業務系統**。
4. 若尚有遺漏的業務系統，請提供給機關管理者。

執行
Do

種子電腦套用

全單位套用

1. 由機關GCB管理人員擇6~10台電腦作為種子電腦套用，觀察一週。
2. 若種子佈署觀察期有問題發生需協助記錄，回報駐點**提出例外申請**。
3. 若無問題則可全單位套用GCB

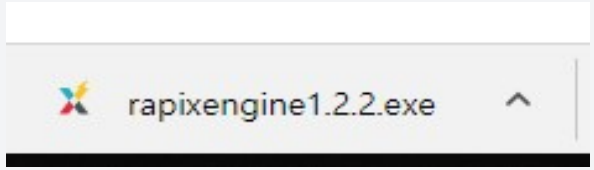
RAPIXUS 瑞思資訊股份有限公司

一、GCB用戶端程式佈署

- Microsoft AD GPO套用，電腦開機時自動安裝
- 資產管理工具進行遠端佈署
- 未納入AD管控電腦則提供一組下載路徑，公告請人員至指定處下載並點選安裝。
- 若未安裝用戶端者，由單位GCB管理者協助進行安裝

下載安裝程序:

1.開瀏覽器並點選路徑，例
https://gcb.taichung.gov.tw/api/bin/rapixengine1.2.3.exe
左下方會出現下載圖示，下載成功並點2下執行。



2.顯示提示圖，請點”是”

3.開始安裝，執行完成後會直接以無訊息模式常駐在系統中。

RAPIXUS 瑞思資訊股份有限公司

二、單位導入流程

1. 單位GCB管理人員選定種子電腦6~10台試導入
2. 套用由資訊中心所提供的GCB通用範本
3. 導入中問題發生之後續處理辦法:
   1)透過套用問題回報單進行問題記錄。
   2)由單位管理者協助一鍵還原，確認是否為GCB
      設定造成的問題。
   3)確定為GCB所造成問題，以RapixEngine Tool
      找出問題條目，紀錄並開設例外
   4)填寫例外申請表單
   5)更新單位GCB派送範本
4. 將GCB範本套用至單位全數電腦
5. 完成GCB政策導入，提高資安防護

例外管理表單範例

雲林縣政府 107 年政府組態基準(GCB)導入服務案
例外原則申請表單

#	例外管理項目
CCE-ID	CCE-9357-5 (建議由工程人員協助填寫)
規則名稱	密碼原則
基準值	8 個字元以上
變更值	12 個字元以上
變更理由	GCB 規定值 8 碼，本府設定值 12 碼。(優規)
配套措施	無

GCB導入流程採用PDCA流程(2/2)

持續監控與例外條目逐步限縮

1. GCB例外條目若是因應現況，將逐步宣導限縮
2. GCB條目將會持續更新

Check 查核

套用定期稽核

確認工具版本

1. 定期檢查單位設備GCB套用狀況
2. 定期確認GCB測試工具是否更新至最新版本

Action 改善

新系統測試

例外條目限縮

1. 單位業務系統在更板時可先透過GCB測試工具測試是否通過GCB驗證
2. 透過宣導與設備汰換時，GCB例外可逐步限縮(如事務機掃描傳檔改用電子郵件發送)

本案聯繫窗口及聯繫方式說明

負責事項	姓名	連絡電話	Email
GCB駐點窗口	大同駐點人員	府內分機2989	wakep@tatung.com
專案執行與時程管理	羅停明	0933-181707	tinminlo@tatung.com
GCB系統專案工程師	魏志學	0932-982259	wakep@tatung.com
GCB系統執行與技術問題顧問	莊旻儒	0989-684229	michael@fstop.com.tw

雲林縣政府
YUNLIN COUNTY GOVERNMENT

Thanks!

rapixus.com