ANCHOR

特權帳號管理平台

智弘軟體科技

State-of-the-art PAM Product

公司簡介

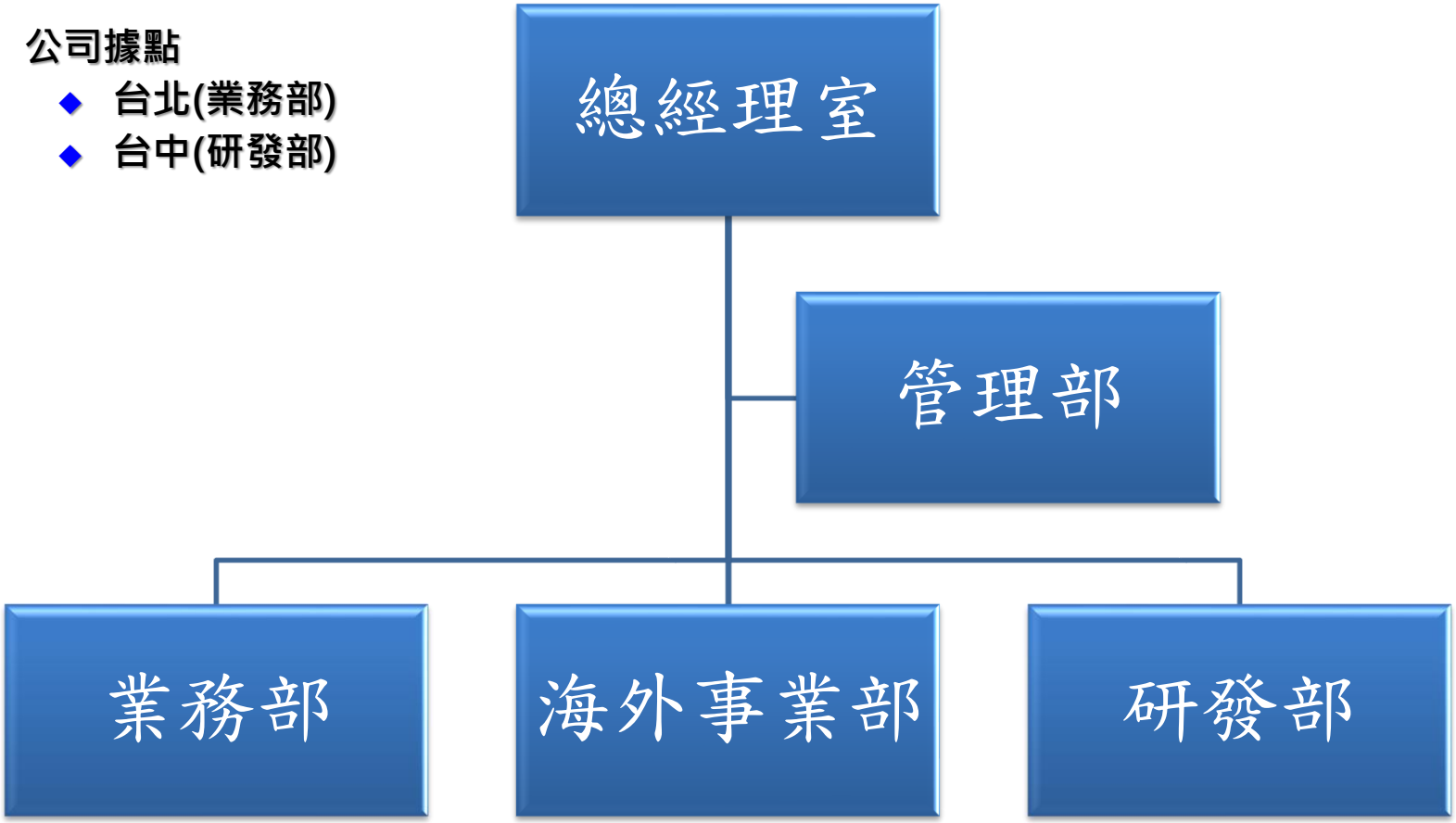
- 智弘軟體科技股份有限公司源自於新陽電腦科技股份有限公司。

- 2017/11 因應特權帳號存取管理之大勢所趨，邀請ANCHOR原研發及業務團隊創立智弘軟體並完成收購智財權。

- 2018/02 新公司智弘軟體科技(股)公司正式成立專注於ANCHOR及ANCHOR Family之產品研發並行銷國內外市場。

公司組織

- 公司據點
  - 台北(業務部)
  - 台中(研發部)



APT攻擊事件說明

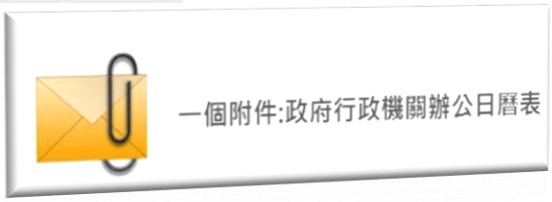
APT攻擊事件簿

https://www.ithome.com.tw/news/117386

臺灣金融業歷年遭駭事件簿

- 2010年4月：[redacted]銀行遭駭客利用木馬程式入侵，超過16,000筆客戶個資外洩，並未有帳款遭盜領，[redacted]遭金管會罰鍰400萬元
- 2016年7月：[redacted]銀行ATM盜領案，駭客以[redacted]倫敦分行的電話錄音系統作為跳板，最終遙控了全臺灣41臺[redacted]ATM，盜走8,327萬餘元，多數款項都已追回
- 2016年9月：[redacted]銀行及[redacted]證券遭駭客進行分散式阻斷服務攻擊（DDoS），個人網銀、企金網銀、證券商電子下單平臺的服務分別中斷數小時
- 2017年1月24日～2月3日，券商集體遭冒名Armada Collective的駭客組織發動DDoS勒索攻擊，有13家券商受害，攻擊時間約持續15分鐘～1小時
- 2017年2月7日：冒名Armada Collective的駭客發動第二次攻擊，有4家證券業者的網路下單系統受害，平均都在30分鐘內恢復運作
- 2017年8月：[redacted]證券、[redacted]證券遭到DDoS的駭客攻擊，但是並未接到威脅或勒索，兩家券商也未有損害。[redacted]證40分鐘內即排除狀況，[redacted]證則在事發前成功阻斷DDoS攻擊
- 2017年10月：駭客入侵[redacted]銀行的國際匯款交易系統（SWIFT），植入惡意程式，並遭駭客暗中盜匯高達6,000萬美元鉅款出國

APT攻擊的路徑示意



INTERNET

隔離內網

BINGO!

1. 中招

2. 掃瞄登入過帳號/側錄密碼

內部人員
(不小心的好人)

3. 橫向移動
(Ex: PtH入侵、蛙跳)

4. 偷建後門帳號

5. 掃瞄登入過帳號/側錄密碼

中繼主機
(倒楣的主機)

6. 橫向移動

7. 進入內網

橫跨內外網主機
(最後的稻草)

重要資料主機

OA網段

Gartner Top 10 Security Projects

State-of-the-art PAM Product

Gartner副總裁兼傑出分析師尼爾·麥克唐納（Neil MacDonald）解釋了Gartner為CISO提供的10大安全項目，重點關注2018年Gartner安全和風險管理峰會。

第1名：特權帳戶管理

此項目旨在使攻擊者更難以訪問特權帳戶，並允許安全團隊監視異常訪問的行為。CISO至少應為所有管理員制定強制性多因素身份驗證（MFA）。還建議CISO使用MFA進行第三方訪問，例如承包商。

June 18, 2019 | Contributor: Kasey Panetta

Security and risk management leaders should implement these 10 security projects to address the changing needs of cybersecurity and reduce risk.

When George took over as the CISO of a retail company, IT security was relatively simple. But as the organization has grown — adding online ordering, more employees and a host of cloud-based platforms and technology to support digital business across the organization — so have the security vulnerabilities. Plus, increased attacks and phishing attempts make it difficult to know what security projects to focus on and where to get the most ROI.

"For new security projects, focus on those that can address a high degree of business impact"

"Security and risk management leaders are constantly bombarded with both maintaining existing security projects and bringing forward new projects," says Brian Reed, Senior Director Analyst, Gartner. "As priorities for new security projects, focus on those that can address a high degree of business impact and also have an ability to reduce a high amount of risks."

Gartner has identified 10 security projects — in no particular order — for organizations that have already adopted all basic security measures.

Project 1: Privileged access management (PAM)

Privileged accounts (or administrative or highly empowered accounts) are attractive targets for attackers. A PAM project will highlight necessary controls to apply to protect

特權帳號的管理難題

史上最嚴格的歐盟個資法GDPR上路

讚

2018-05-24

國發會盤點 金融、航空及電子商務業受影響最大

〔記者陳梅
發會主委陳
業在主管機
盟適足性認

新聞

GDPR上路後最嚴厲處分！英航遭重罰年營收1.5%高達1.8億英鎊

英國航空因2018年的個資外洩案，遭英國官方判處年營收1.5%，高達1.83億英鎊的罰金，成了GDPR上路以來，英國當局對個資管控不當企業所祭出的最嚴厲處份

文/ 林妍溱 | 2019-07-09 發表

讚 6萬 按讚加入iThome粉絲團 讚 342 分享

ico.
Information Commissioner's Office

About the ICO / News and events / News and blogs /

Intention to fine British Airways £183.39m under GDPR for data breach

去年9月發生網站和行動app遭駭導致大批旅客信用卡及個資外洩的英國航空，周一因違反歐盟個資法GDPR，遭英國主管機關重罰1.83億英鎊（約台幣64億元）。比先前Google遭重罰5千萬歐元（約台幣7億元）高了好幾倍。

iThome Weekly 電腦報
按讚追蹤 iThome 最新報導
讚 6萬

熱門新聞

21萬人要提高自主健康管理意識，24位艦隊感染確診者全臺足跡緊急公布！（內有足跡連結）
2020-04-20

Zoom的安全問題不只是漏洞，更是信任問題
2020-04-20

教育部閃禁Zoom，讓學校措手不及！
2020-04-20

Tomcat Server存在Ghostcat漏洞，有中國駭客在臺灣校園網站上傳BiFrost後門程式
2020-04-18

特權帳號濫用事件

State-of-the-art PAM Product

2018/

英

即時 要聞 選舉 娛樂 運動 全球 社會 專題 產經 股市 房市 健康 生活 文教 評論 地方 分享

竹縣生醫園區女總經理離職 刪萬筆研發資料遭起訴

分享 分享 留言 列印 存新聞 A- A+

2018-03-26 12:14 聯合報 記者張雅婷／即時報導 讚 49 分享

新竹縣竹北生醫園區一家公司廖姓研發部女總經理，2014年遭資遣，離職當天她趁公司指定辦理交接人員不注意，在15分鐘內，刪除公司1萬多筆的研發檔案，造成公司損失慘重，公司向檢調報案，新竹地檢署依刑法「無故刪除他人電磁紀錄」罪嫌起訴廖女。

檢方調查，廖女2013年開始在竹北生醫園區某公司擔任研發部總經理，並由公司配發筆記型電腦一台，廖女手中握有公司研發中產品的程式原始碼、佈局圖、印刷電路板圖、規格等資料，均屬公司營業秘密。由於廖女2014年3月起，未經公司同意，陸續以隨身碟或儲存式硬碟等裝置，將營業秘密交給競爭對手公司，公司進行資訊安全檢查時發現後，便將她資遣。

2014年6月廖女離職當天下午5點多，在公司指派的特助協助辦理交接電腦及離職手續時，向特助佯稱要刪除私人照片等為由而開啟電腦，廖女趁特助不注意，在15分鐘內刪除公司所有關於醫療研發的檔案，共計1萬4882筆，公司立即向新竹市調查站報案，廖女坦承大量刪除公司配發筆電內檔案，辯稱是接任的總經理要她把個人及不重要的資料刪除，當時刪掉的資料，都是不重要的。

特權帳號管理相關合規資訊

ISO-27001

- A.9存取控制領域的使用者存取之相關控制措施
- A.12運作安全領域的側錄及稽核的相關控制措施

行政院資通安全法

- 資通系統防護基準-存取控制
  - ✓ 帳號管理
  - ✓ 最小權限
  - ✓ 遠端存取

NYDFS Part.500

- 存取及身份控制
- 第三方廠商之存取控管
- 雙因素驗證
- 安全事件的稽核追蹤

F-ISAC之11項防護措施

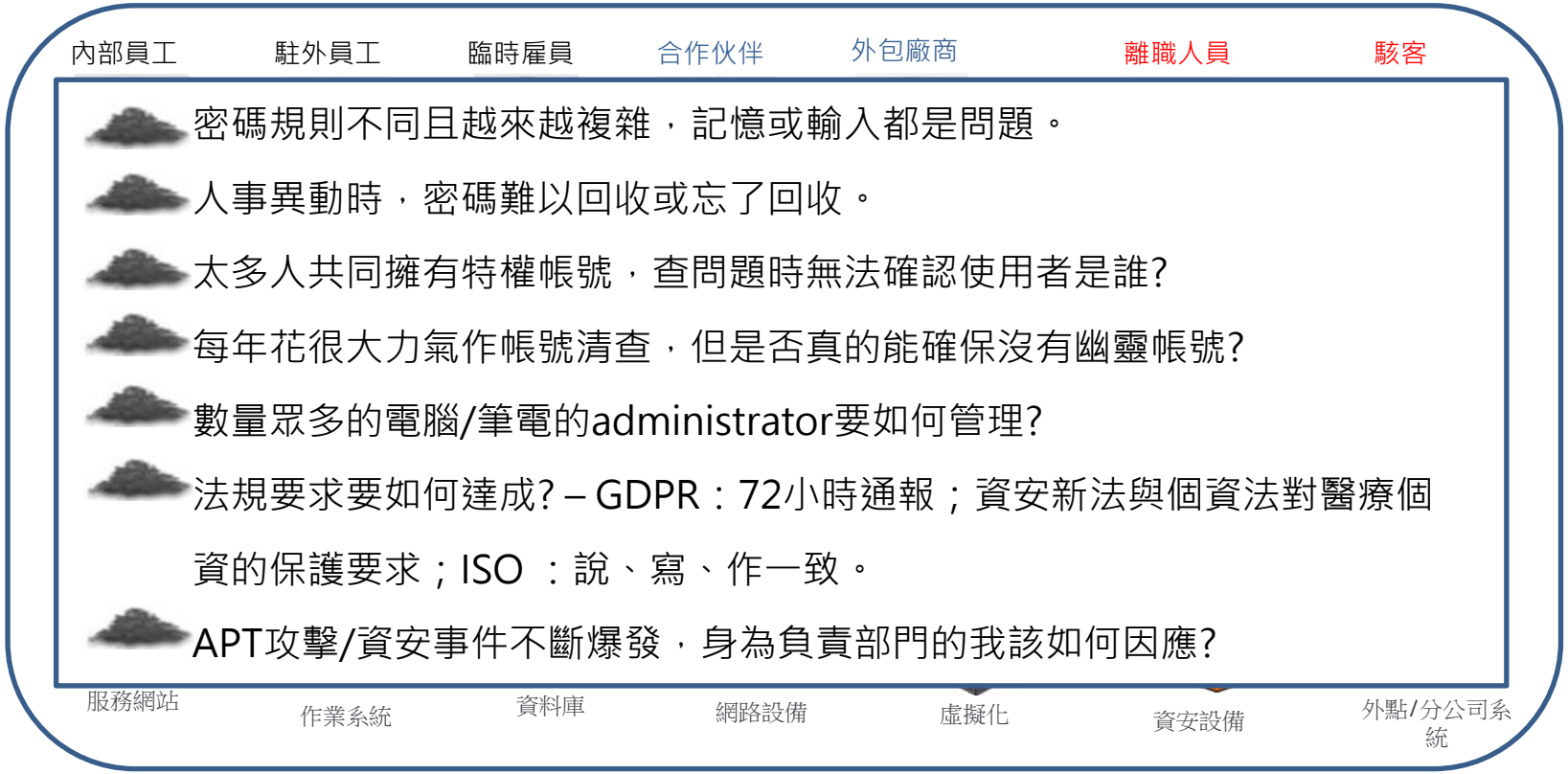
- 第1項之定期檢視並監控特權帳號的活動
- 第6項強化管理者帳戶的認證機制

特權帳號管理相關合規資訊

PCI-DSS

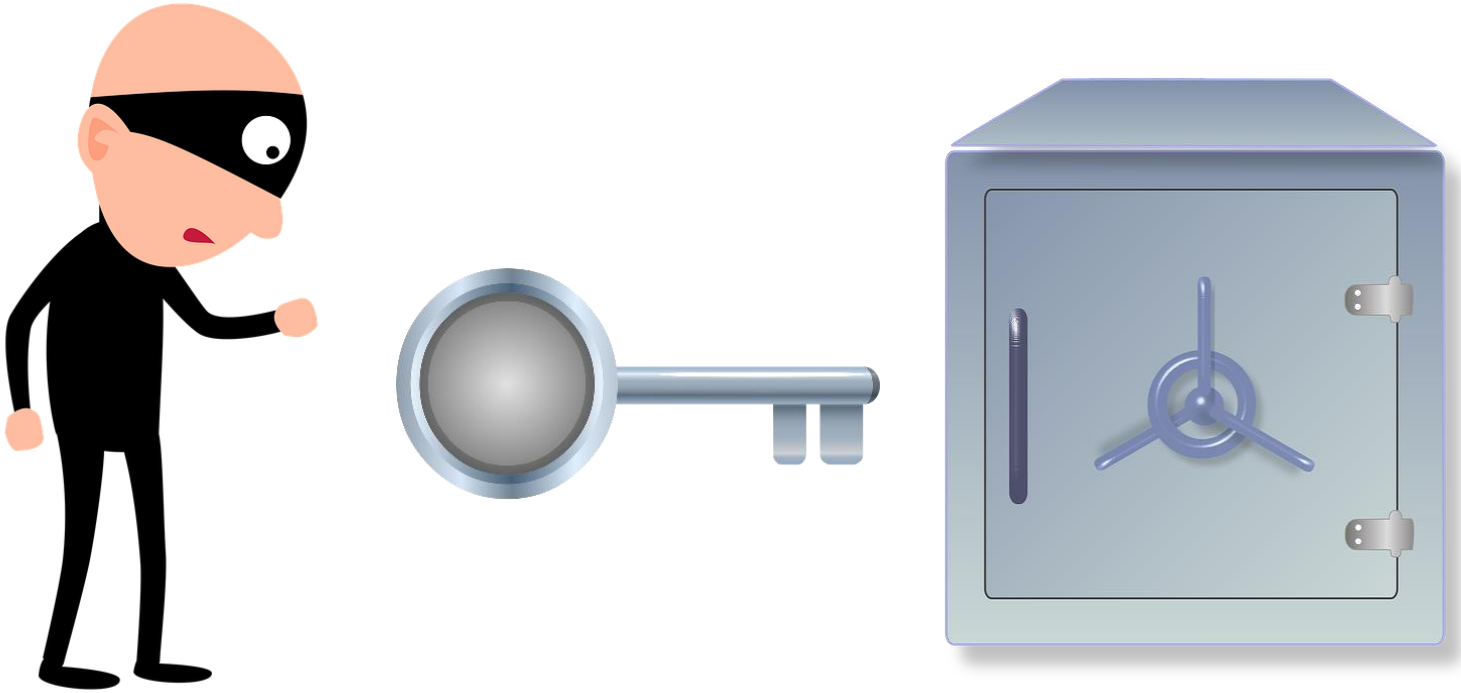
- 2、不要使用供應商提供的預設系統密碼和其他安全參數
  - 盤點並找出預設帳戶及管理其密碼
- 5、為所有系統提供惡意軟體防護並定期更新殺毒軟體或程式
  - 管理防毒軟體管理權限的帳號
- 6、開發並維護安全的系統和應用程式
  - 管理維運人員及開發人員，分別只能存取生產及開發環境，避免存取錯誤設備。
- 7、按業務知情需要限制對持卡人資料的訪問
  - 依使用者權責分配最小存取權限
  - 提供申請及審核流程
- 8、識別並驗證對系統元件的訪問
  - 確保帳戶存取為本人(唯一id)，雙因子認證
  - 確保存取申請、時段、權限，為合法授權
  - 管理密碼原則、密碼生命週期
  - 確保密碼儲存安全性
- 10、跟蹤並監控對網路資源和持卡人資料的所有訪問
  - 確保存取過程全記錄(含側錄)
  - 確保不存在不明帳號
- 12、維護針對所有工作人員的資訊安全政策
  - 控管存取來源位置
  - 控管帳戶的異動

特權帳號管理的難題


內部員工
駐外員工
臨時雇員
合作伙伴
外包廠商
離職人員
駭客
密碼規則不同且越來越複雜，記憶或輸入都是問題。
人事異動時，密碼難以回收或忘了回收。
太多人共同擁有特權帳號，查問題時無法確認使用者是誰?
每年花很大力氣作帳號清查，但是否真的能確保沒有幽靈帳號?
數量眾多的電腦/筆電的administrator要如何管理?
法規要求要如何達成? – GDPR：72小時通報；資安新法與個資法對醫療個資的保護要求；ISO ：說、寫、作一致。
APT攻擊/資安事件不斷爆發，身為負責部門的我該如何因應?
服務網站
作業系統
資料庫
網路設備
虛擬化
資安設備
外點/分公司系統

特權帳號的管理建議

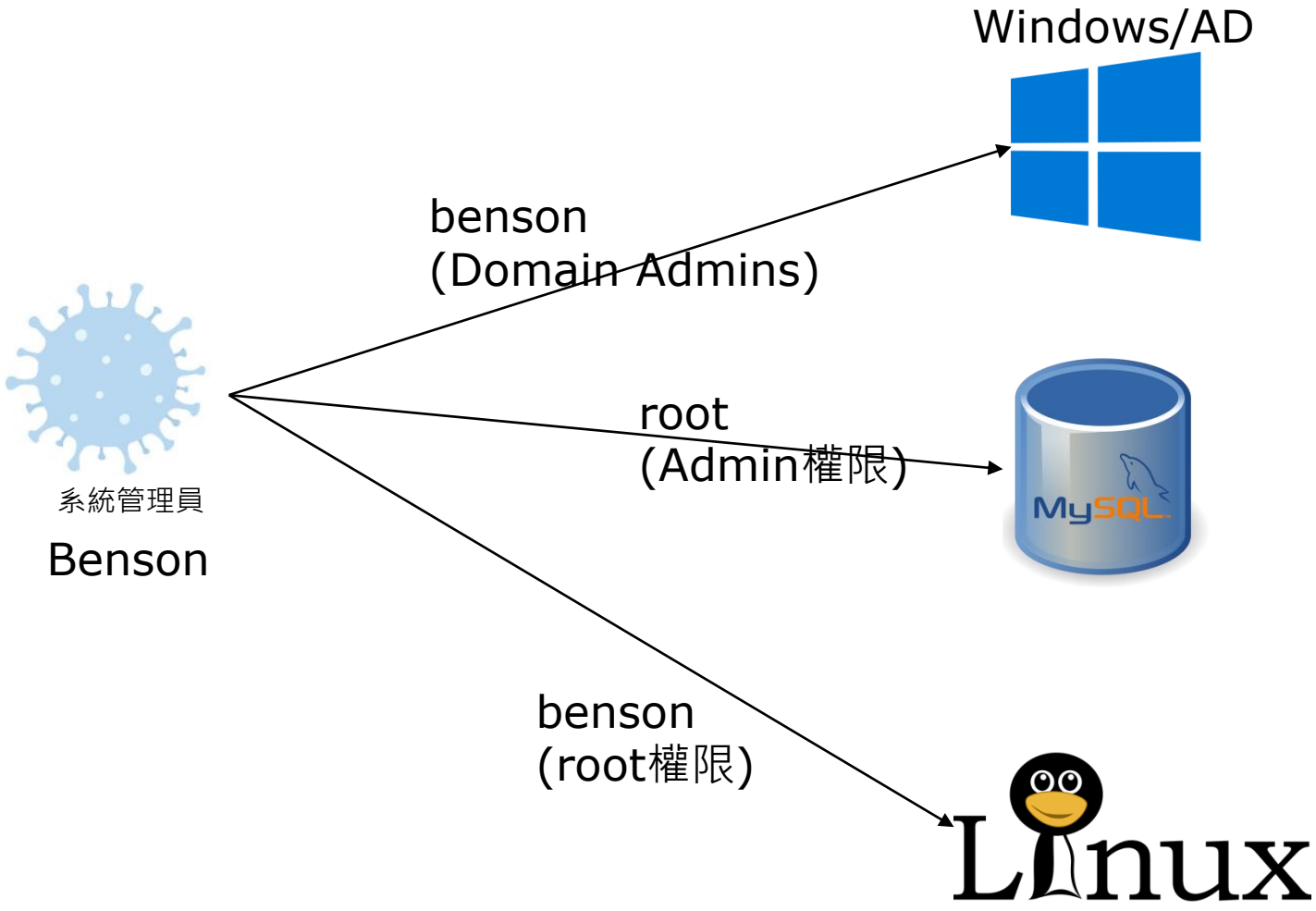
什麼是特權帳號?



無導入特權帳號管理平台的情境

個人帳號

特權帳號



個人帳號 vs 特權帳號

個人帳號

Allen

高階主管

Benson

系統管理員

Carl

財務人員

Danny

程式發開人員

Eason

網管人員

特權帳號管理
與稽核平台

特權帳號

Administrator

root

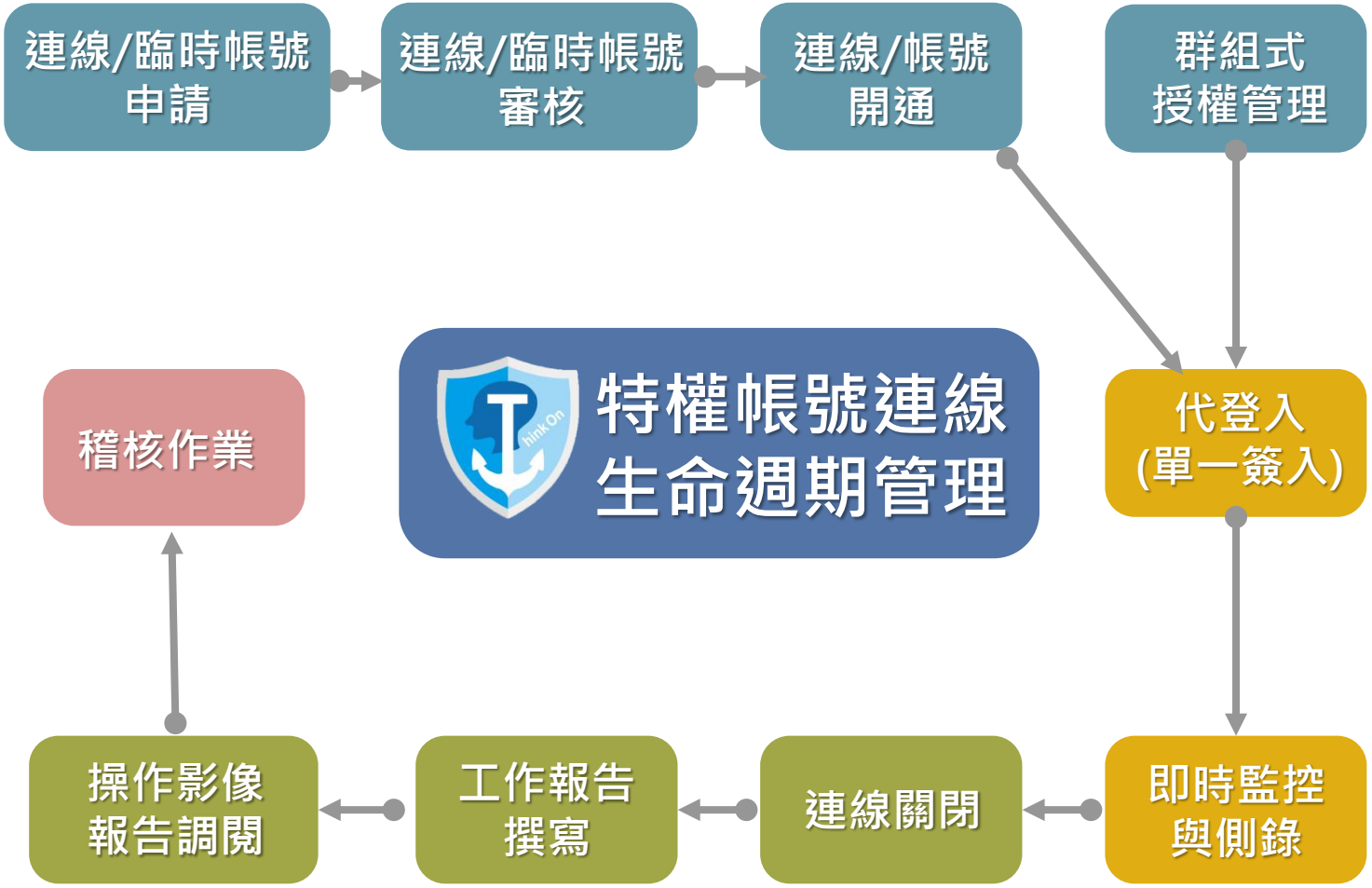
admin

ANCHOR平台模組結構

ANCHOR平台結構圖

特權帳號連線生命周期管理流程

State-of-the-art PAM Product



駭客入侵防禦

接觸主機

- 代理連線/桌面連線(VDI)
- 透過申請才能進行連線
- 指定使用者來源IP

竊取帳號

- 代登入/帳號密碼不落地
- 連線結束立即變更密碼
- 排程確認密碼同步狀態

幽靈帳號

- 自動排程帳號盤點

風險威脅警示

異常帳號警示

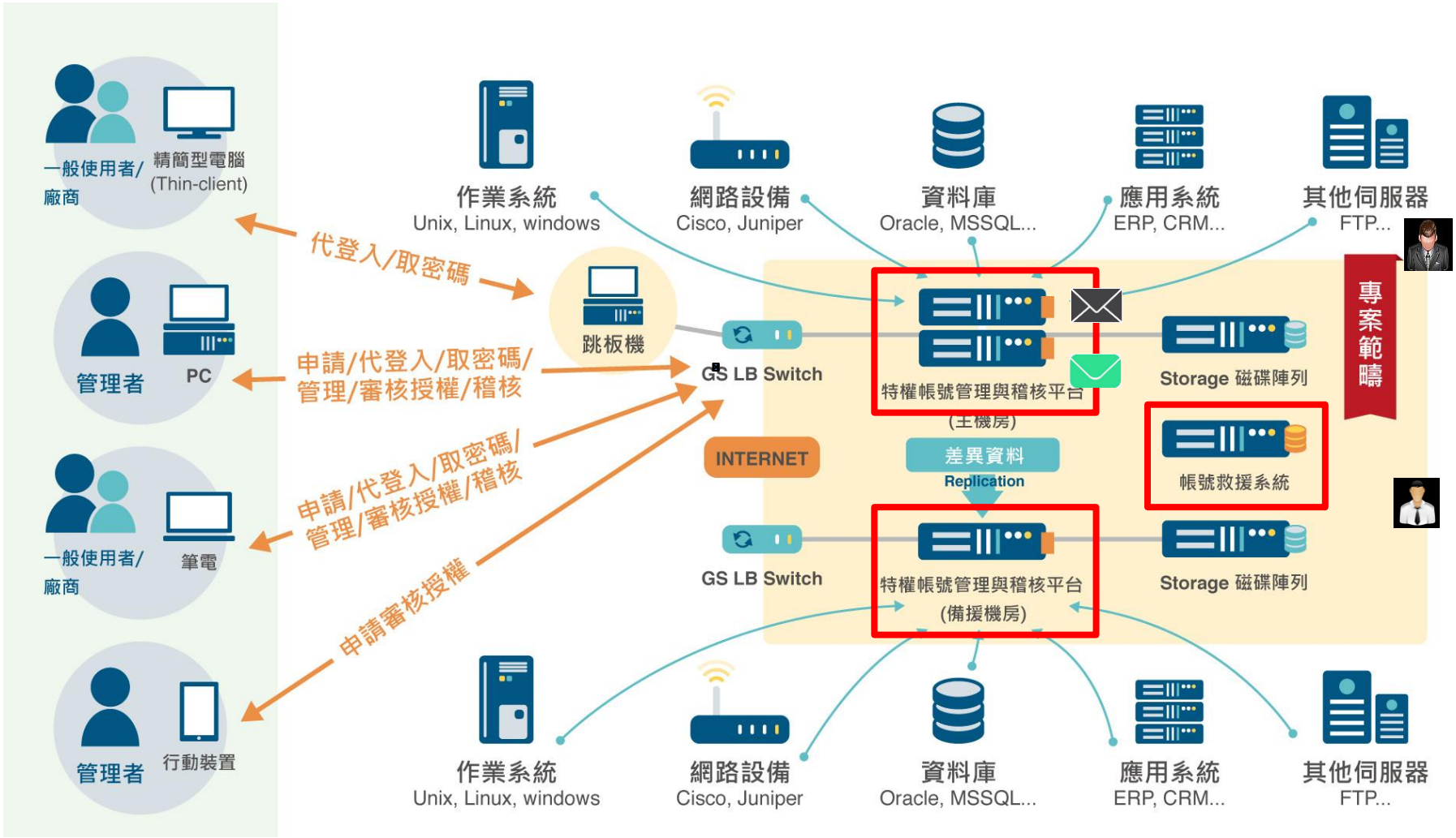
密碼異常警示

登入失敗警示

違規指令警示

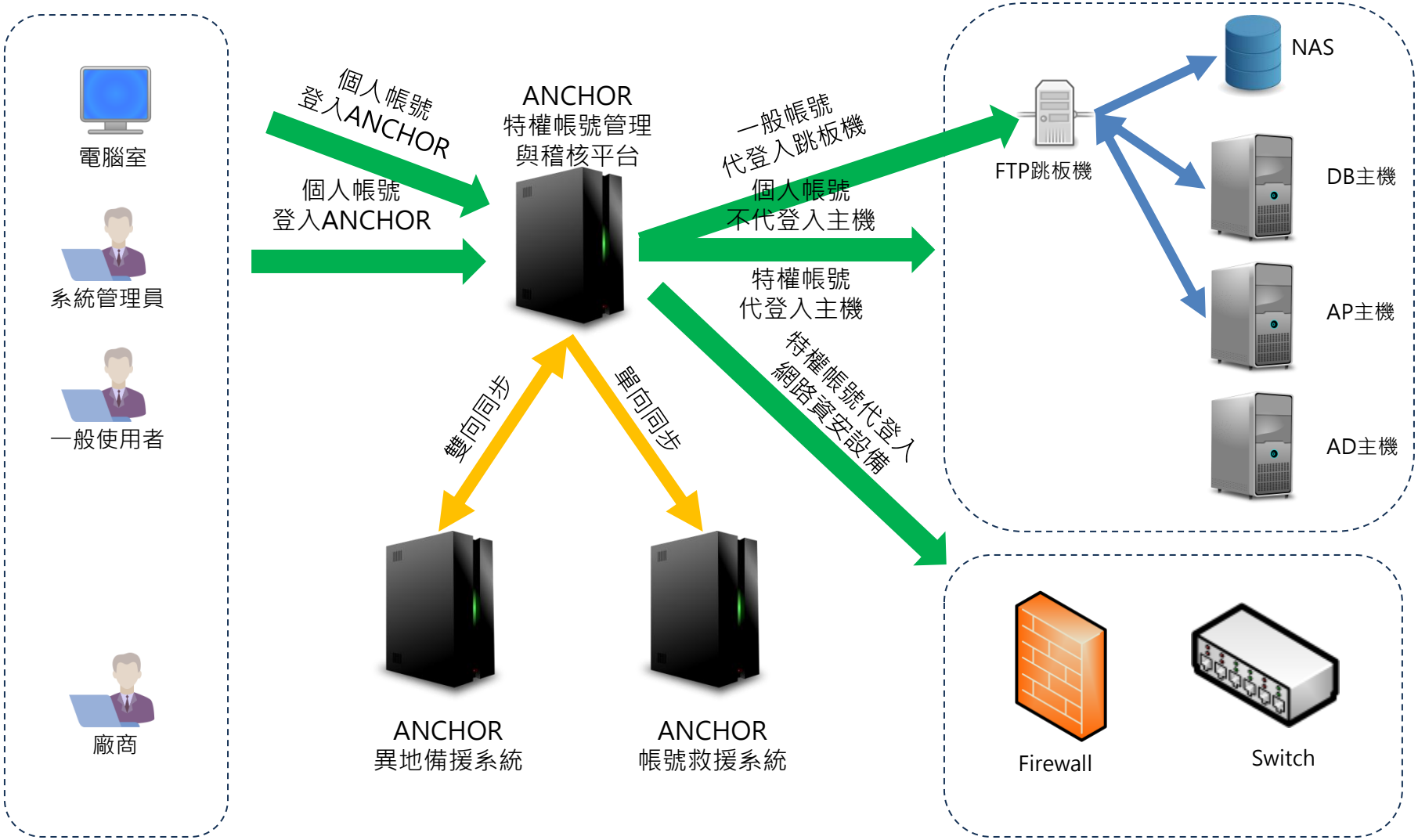
ANCHOR安全性與可用性

State-of-the-art PAM Product

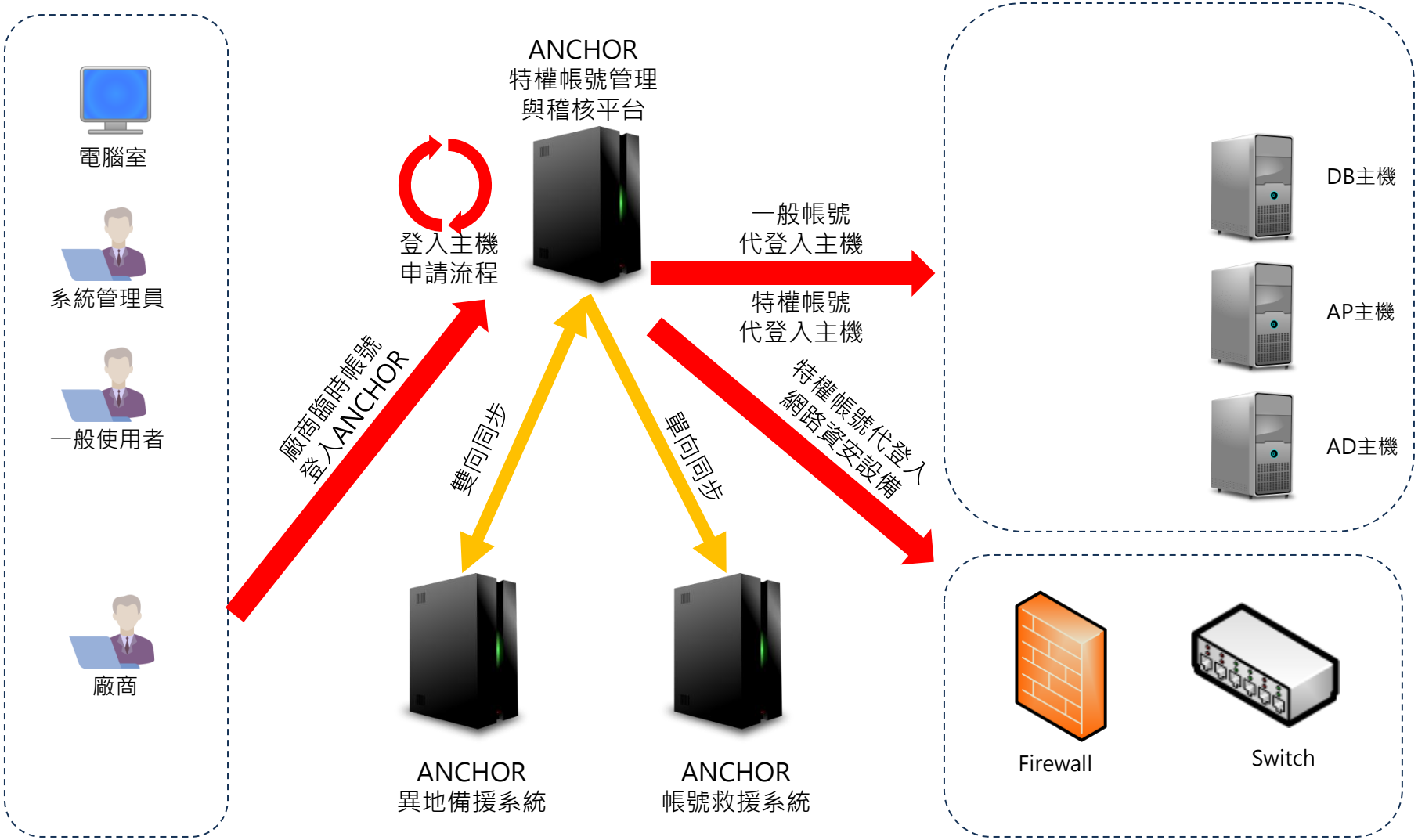


導入案例

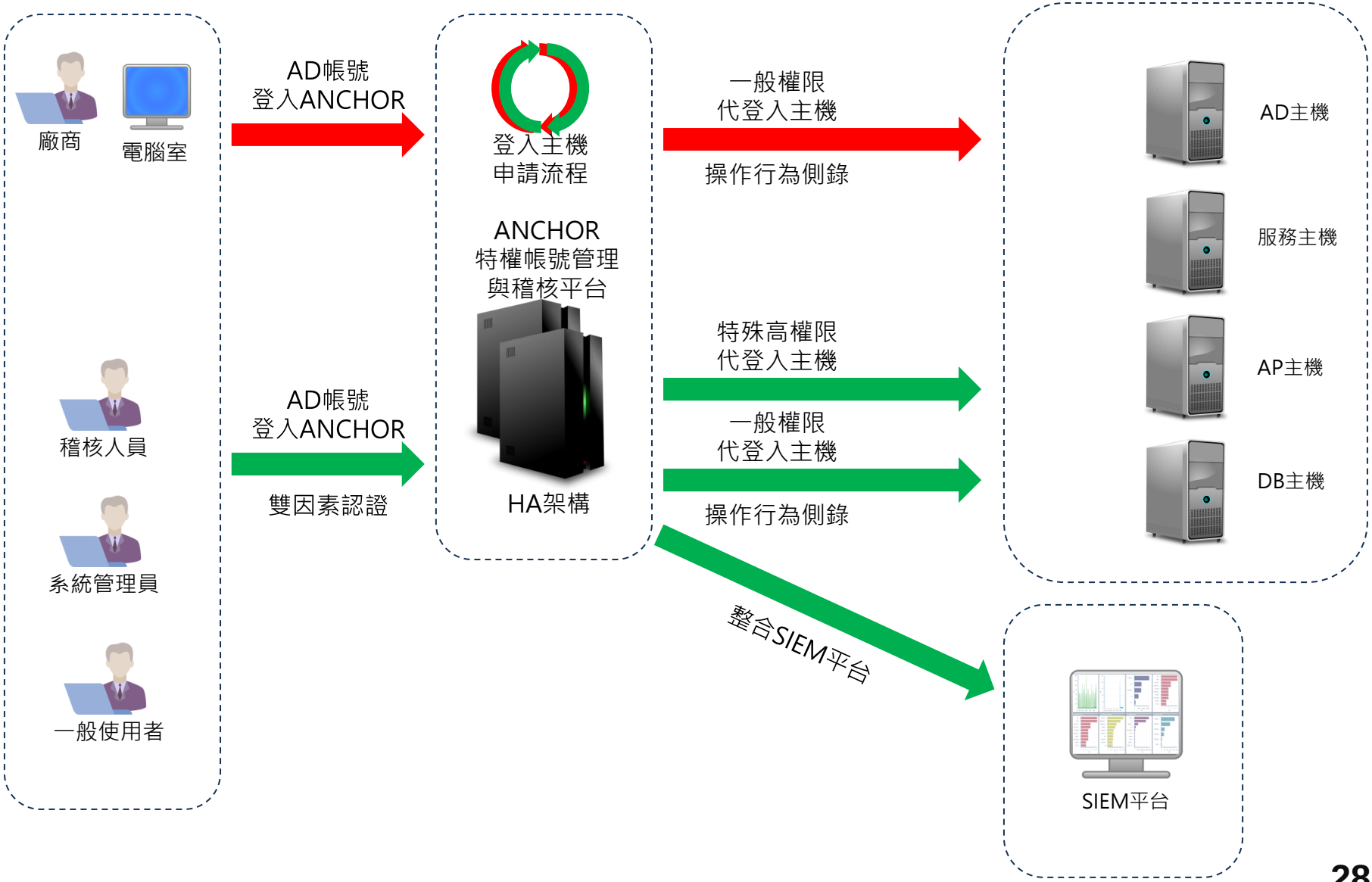
政府機關範例-內部人員


電腦室
系統管理員
一般使用者
廠商
個人帳號
登入ANCHOR
個人帳號
登入ANCHOR
ANCHOR
特權帳號管理
與稽核平台
一般帳號
代登入跳板機
個人帳號
不代登入主機
特權帳號
代登入主機
特權帳號代登入
網路資安設備
雙向同步
單向同步
FTP跳板機
NAS
DB主機
AP主機
AD主機
ANCHOR
異地備援系統
ANCHOR
帳號救援系統
Firewall
Switch

政府機關範例-維運廠商

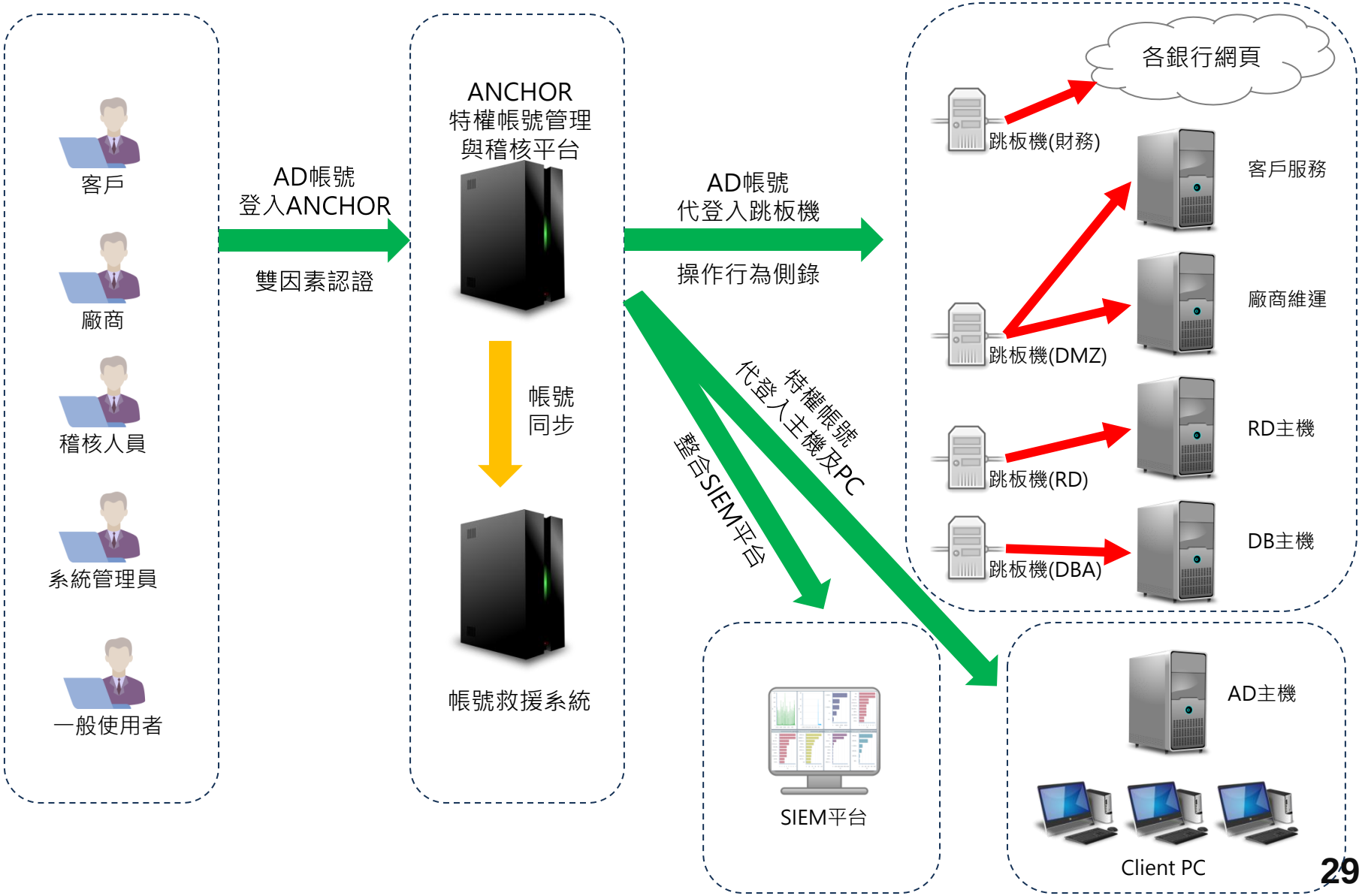

電腦室
系統管理員
一般使用者
廠商
ANCHOR
特權帳號管理
與稽核平台
登入主機
申請流程
廠商臨時帳號
登入ANCHOR
一般帳號
代登入主機
特權帳號
代登入主機
特權帳號代登入
網路資安設備
雙向同步
單向同步
DB主機
AP主機
AD主機
Firewall
Switch
ANCHOR
異地備援系統
ANCHOR
帳號救援系統

金融業範例


廠商
電腦室
稽核人員
系統管理員
一般使用者
AD帳號
登入ANCHOR
AD帳號
登入ANCHOR
雙因素認證
登入主機
申請流程
ANCHOR
特權帳號管理
與稽核平台
HA架構
一般權限
代登入主機
操作行為側錄
特殊高權限
代登入主機
一般權限
代登入主機
操作行為側錄
整合SIEM平台
AD主機
服務主機
AP主機
DB主機
SIEM平台

製造業範例

State-of-the-art PAM Product



導入效益

Why 特權帳號管理

State-of-the-art PAM Product

	導入前	導入後
連線申請	紙本作業，**曠日費時**，權責長官**公出、休假時需指派代理人**	**電子化**，自行定義簽核流程，以EMAIL通知相關人員，有手機即可操作
登入作業	密碼條方式提供，**取出、輸入及保管都是問題，不慎遺失將造成資安隱憂**	**系統代登入，密碼不落地**
操作過程	**操作過程無法控管** 若是外包廠商操作視情況需要**職員陪同及監看，浪費大量人力**	全程進行操作側錄，並**提供線上監看、違規指令告警及阻擋機制**，不受地點限制，減少內部人力消耗
密碼回收	需人工進行密碼回收、重製密碼條，亦**容易被遺漏忘了回收**	**連線到期自動變更密碼**，不需耗用人力
帳號盤點	每季稽核耗費大量人力進行盤點，且資料時效性極短	**系統排程自動盤點帳號**，若有幽靈帳號立即發出通知，不需耗用人力
後續稽核作業	紙本作業，資料散落各地，**收集及調閱都很困難**	申請、連線錄影、工作報告、稽核歷程，全**電子化調閱容易，於單一平台完成稽核作業。**

Why ANCHOR?

- **貼近國內管理慣例**
  - 臨時帳號申請機制 – 管理外包廠商連線需求
  - 緊急授權審核
  - 永久存取授權及申請/審核授權，維運更便利
  - 電子化工作報告，減少紙本使用、查詢更便利
- **功能齊全，合理的授權模式**
  - 預設提供OTP、A/B Part密碼救援機制
- **自定義稽核流程，於資安與維運便利取得最佳平衡**
- **台灣自主研發，具客製化彈性**

不只安全 還更方便

State-of-the-art PAM Product

個人帳號維護

減少個人帳號逐一維護成本

輕鬆訪問設備

HTML5 Ready
一鍵部署/零部署

工具特性保留

保留功能鍵/熱鍵Copy/Paste…等

批次設備指令

多部同類型設備執行相同指令

多層備份/移轉

系統資料與錄影自動備份移轉

緊急申請審核

審核人員不打開電腦也能授權

定義式稽核流程

設備訪問結束主動提醒關卡執行

線上工作報告

線上寫工作報告保留修改歷程

可訂閱式報表

訂閱日/週/月周期自動寄送報表

支援個人語系

支持繁中、簡中、英文、日文

補充資訊

ANCHOR 版本

State-of-the-art PAM Product

	FDT 基礎版	STD 標準版	ETP 企業版	ETP+ 企業進階版
被管理端支援： 作業系統 (Windows, Unix, Linux) 檔案存取 (FTP, SFTP, SCP)	YES	YES	YES	YES
被管理端支援： 資料庫 (Oracle, SQL Server, MySQL)、 網路/資安設備 (SSH)	No	YES	YES	YES
被管理端支援： 中、大型主機 (IBM AS/400, z/OS)、 網路/資安設備 (Web)、 Vmware；支援高可用性 (HA)	No	No	YES	YES
支援異地備援 (DR) 帳號救援系統 (破窗)	No	No	No	YES

FDT/STD/ETP皆可加購帳號救援系統模組
各版本皆能加購VDI功能授權

ANCHOR各版本內建授權數量

ANCHOR模組		授權項目	FDT 基礎版	STD 標準版	ETP 企業版	ETP+ 企業進階版
AIO (全功能)	帳管模組	同時上線人數	5	5	10	10
	側錄模組	側錄設備	25	50	100	100

同時上線人數最小加購單位為「5個同時上線人數」
側錄設備最小加購單位為「25台側錄設備」

ANCHOR 代表客戶

政府機關

- 衛生福利部 健保署
- 勞動部 勞保局、勞發署
- 經濟部 水利署
- 交通部 台鐵局、高公局、航港局
- 內政部 營建署、移民署、墾管處
- 行政院 人事行政總處、主計處
- 農委會
- 退輔會
- 新北市政府 及 新北市稅捐稽徵處

金融機構

- 合作金庫銀行
- 國泰世華銀行
- 陽信商業銀行
- 三信商業銀行
- 兆豐銀行紐約分行
- 台灣中小企銀紐約分行
- 華南產物保險公司
- 和泰產物保險公司
- 台灣產物保險公司
- 玉山證券
- 玉山銀行深圳分行
- 合作金庫銀行蘇州分行

健康醫療

- 衛生福利部台北醫院

製造業

- 啟碁科技公司
- 臺灣菸酒公司

電信公司

- 亞太電信公司

企業

- 富台工程
- 中鹿營造

財團法人

- 綠色基金會

簡報結束
謝謝您的參與！

Thank You !