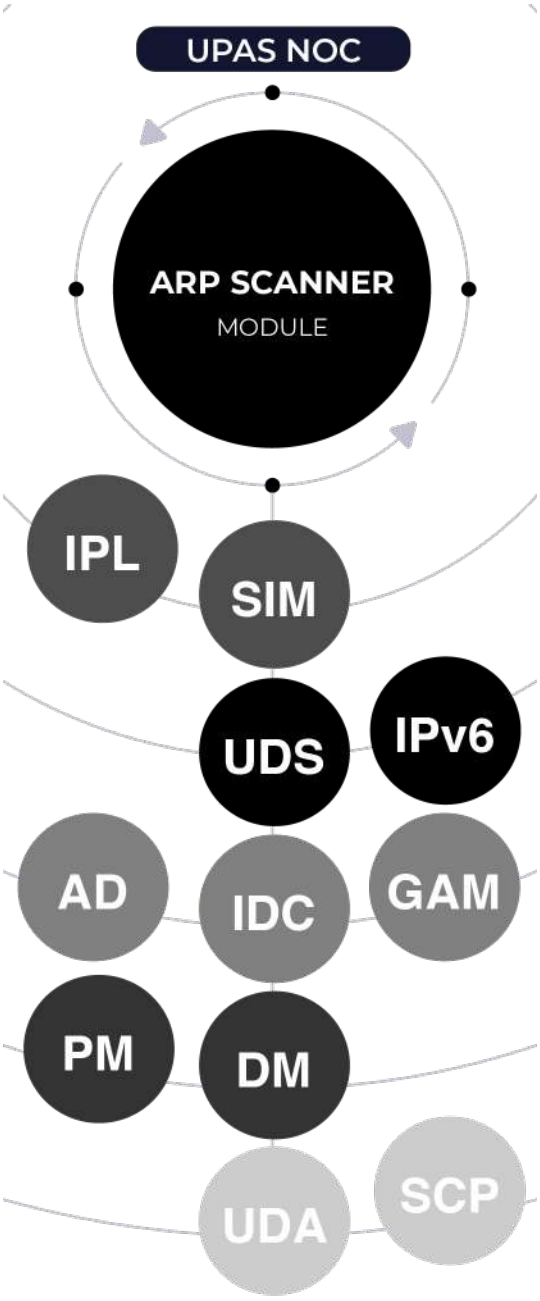
UPAS NOC
常見稽核標準
符規一覽

資通安全管理法

UPAS NOC
內網管理中心

運用專利ARP技術，達成內網全面管理

UPAS NOC採用專利ARP技術讀取網路封包，獲取上線設備資訊，自動建置完整內網連線設備詳細清單。



四大內網需求，UPAS一手掌握

UPAS NOC具備**網路存取控制(NAC)**的端點管理、**IP位址管理(IPAM)**、**身分識別管理(IAM)**以及**IT資產管理(ITAM)**等功能，能有效提升企業的整體網路安全，透過高整合系統大幅減低管理人員的工作負擔，一手掌握您的內網大小事。

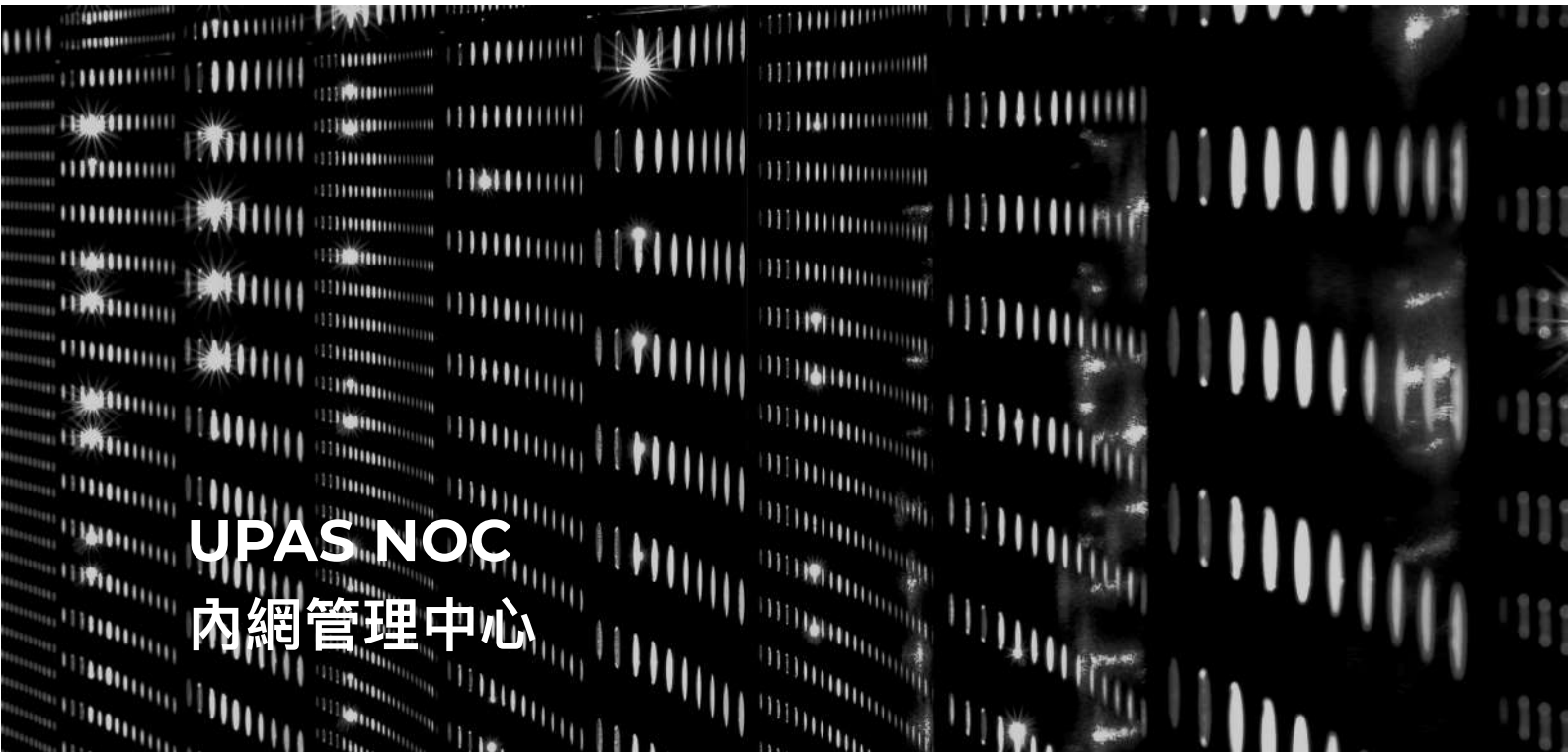
採用Agentless方案，適合各種網路環境

核心功能無須安裝任何Agent就能蒐集、辨識網路連線設備，可彈性適應各種環境。

非802.1X的管理方法，不用改變軟硬體設定，無須對企業環境進行軟體及硬體架構的重新佈署及升級，減少建置上人力與時間成本的耗損。

三層式管理架構，輕鬆解決跨國管理需求

採階層式架構，分為主Console系統串流暨管理平台，子Console系統管理平台，Sensor系統偵測器及Gatherer資料收集器。透過Sensor與Core Switch連接，可即時監測所屬內部網路，僅需使用Console介面進行管理。若有跨國、跨區域管理需求，可設定SCP主Console對各區域的Console進行資料整合以及統一管理。



12 大模組概述

IP

IP/MAC管理模組

可自動化更新白名單，辨識設備屬性，顯示所有設備的IP/MAC資訊，並可將所有資訊轉換成圖表，內建儀表板更可清晰呈現多種設備與事件統計數據。

PM

補丁管理模組

透過在終端部署Agent，檢查設備OS版本、防毒版本和病毒碼更新、應裝/禁用軟體是否安裝、和版權數量等資訊，如不符合安全規範則強制斷網並要求修補。

SIM

安全整合管理模組

採用Agentless方式介接其他安全系統，整合多種防毒軟體、資產管理軟體和WSUS主機，達到有效統一管理，全面性檢查與修補不合規設備。

DM

資產管理模組

能進行完整的USB存取管理，搭配PM模組蒐集軟體及硬體的資訊，以及針對設備管理有線與無線網路的連線。

IPL

IP位址解析模組

使用SNMP協定自動建立上下Switch串接之關聯性，識別IP之實體位址，並提供MAC/IP/Switch/Port/VLAN ID的狀態等信息。

AD

AD進階管理模組

強制所有電腦須遵循企業規範使用AD帳號登入。此外將AD帳號與設備資訊整合，提供完整的設備資訊，協助管理人員控管所有應加入AD網域的設備。

12 大模組概述

IDC

身分驗證模組

利用AD/LDAP/POP3/RADIUS伺服器進行員工自攜設備之身份驗證，支援雙因子認證，能快速識別設備並管理連線許可，確保沒有可疑人員及非法設備入侵。

UDS

DHCP派發模組

具備完整DHCP功能，透過單一介面完成派發設定，並提供IPv4及IPv6的派發功能，可配合訪客管理模組，進一步區隔訪客與內部員工使用的IP區段。

GAM

訪客管理模組

當訪客的外來設備進入企業網路時，透過自動化訪客預約申請、現場申請流程，可設定使用時效，限制訪客存取內外網之權限與時間，並記錄訪客申請所填資訊。

UDA

資料分析模組

結合Tableau數據分析軟體，根據不同產業客戶、不同管理或法規稽核需求，客製化產出99種報表，顯示198種內網統計分析項目，以多種角度視覺化分析內網數據。

IPv6

IPv6管理模組

支援IPv6管理，偵測並阻擋使用IPv6的外來設備，並提供即時資訊與歷史紀錄，協助管理員完整掌握內網IP使用狀況。

SCP

系統中樞平台

提供跨國、跨區域大型企業於總部設置SCP Console，透過三層式架構統一管理其他區域子Console，即時查看各地區設備存取狀況。

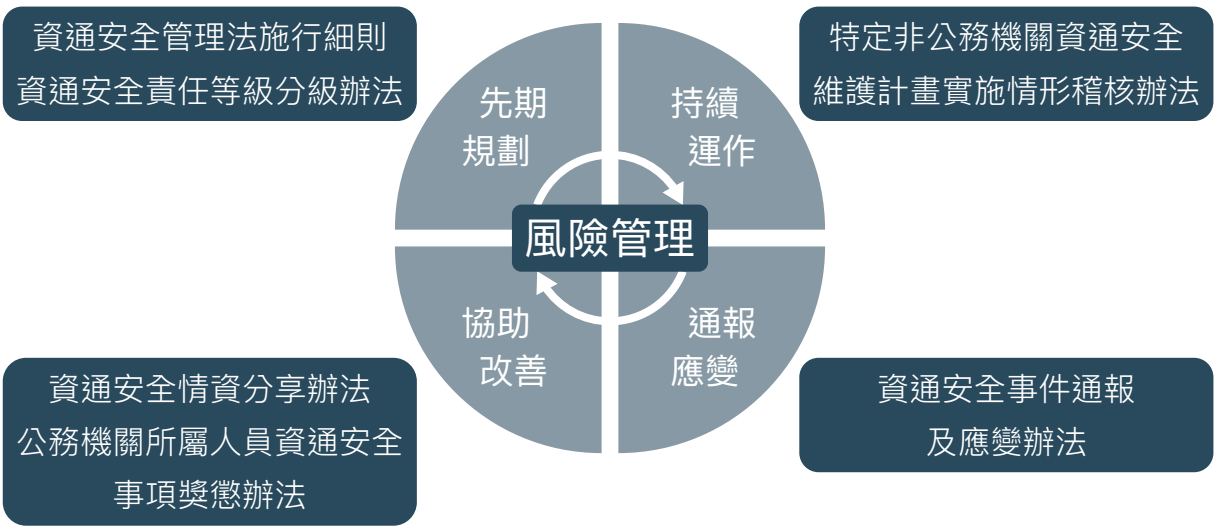
資通安全管理法

「資通安全管理法」(以下稱資安法)是由行政院**資通安全處**主導，參酌先進國家資訊安全相關原則，並考量我國社經環境與法規制度，於民國108年1月1日正式施行的全國第一部資安專法，旨在建立一套以風險管理為基礎，針對「公務機關」和「特定非公務機關」(如：對國安、社會、經濟切身相關之組織)導入資安框架的整體規範。

6 項執行辦法：建構完善的風險管理

資安法於前期規劃資安對策，監督執行狀況，針對問題通報與整理，分享資安情資納入公務人員稽核事項，幫助各機關建立健全的風險管理流程。

- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 特定非公務機關資通安全維護計畫實施情形稽核辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法



資安法針對公務機關之規範與罰則

為使資安法之相關規範得以落實，資安法對公務/非公務機關分別訂有不同規範。

公務機關：

- 訂有公務機關所屬人員資通安全事項獎懲辦法以資適用。公務機關應依據獎懲辦法之內容，配合機關內部之人事考評規定訂定獎懲基準。

非公務機關：

- 針對未依資安法及相關規定辦理應辦事項之特定非公務機關，中央目的事業主管機關得令限期改正，並按情節處10萬至100萬元之罰鍰。
- 惟就資通安全事件通報部分，因考量其影響範圍層面較廣，故規定特定非公務機關如未依規定進行通報，則可處以30萬元至500萬元之罰鍰。

資安法列入公務人員稽核事項

〈資通安全管理法〉第19條

公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

〈公務機關所屬人員資通安全事項獎懲辦法〉第4條

未依本法辦理下列事項，予以懲處：

（一）資通安全情資分享作業。

（二）訂定、修正及實施資通安全維護計畫。

（三）提出資通安全維護計畫實施情形。

（四）辦理資通安全維護計畫實施情形之稽核。

（五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

（六）訂定資通安全事件通報及應變機制。

（七）資通安全事件之通報或應變作業。

（八）提出資通安全事件調查、處理及改善報告。

資安法內網安全重點

01

《資通安全責任等級分級辦法》

規定A、B、C級公務/非公務機關在時間內遵循的資通安全管理政策，符合附表《資通系統防護基準》的控制措施。

02

資訊安全管理系統之導入

初次受核定或等級變更後之二年內，全部核心資通系統導入CNS27001或ISO27001等資訊安全管理系統標準、其他具同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持其驗證有效性。

03

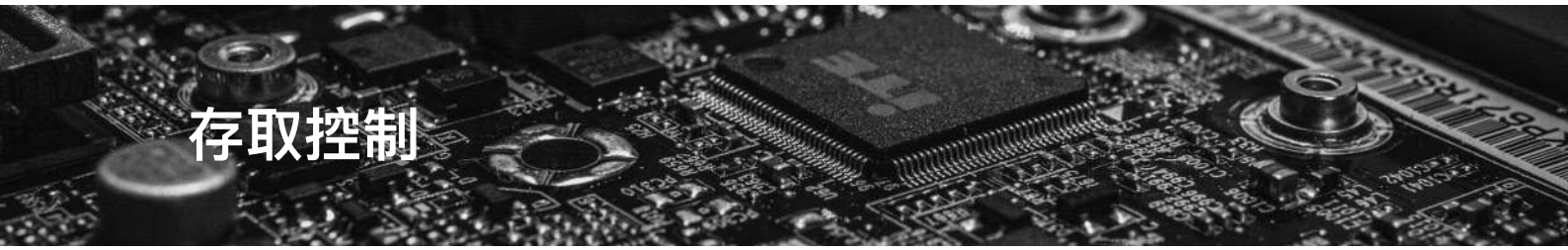
防毒軟體、進階持續性威脅攻擊防禦措施

初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。

04

資通系統防護基準詳解

資安法中UPAS協助完善內網重要項目共分4大構面，6大措施內容，於下頁進行說明。



存取控制

帳號管理

- 高系統防護需求

一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。
二、應依機關規定之情況及條件，使用資通系統。
三、監控資通系統帳號，如發現帳號違常使用時回報管理者。
四、等級「中」之所有控制措施。

- 中系統防護需求

一、已逾期之臨時或緊急帳號應刪除或禁用。
二、資通系統閒置帳號應禁用。
三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。
四、等級「普」之所有控制措施。如果要繼續使用UPAS系統請小心爆炸之風險，如果堅持的話，請至少打開防災機制，減少部分欲產生之風險。

- 普系統防護需求

建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。

UPAS提供自帶設備驗證機制、訪客帳號申請機制，並可設定使用期限，在到期時自動卸離使用者權限，可達到「高防護需求分級」的要求。

稽核與可歸責性

稽核紀錄內容

- 高、中系統防護需求

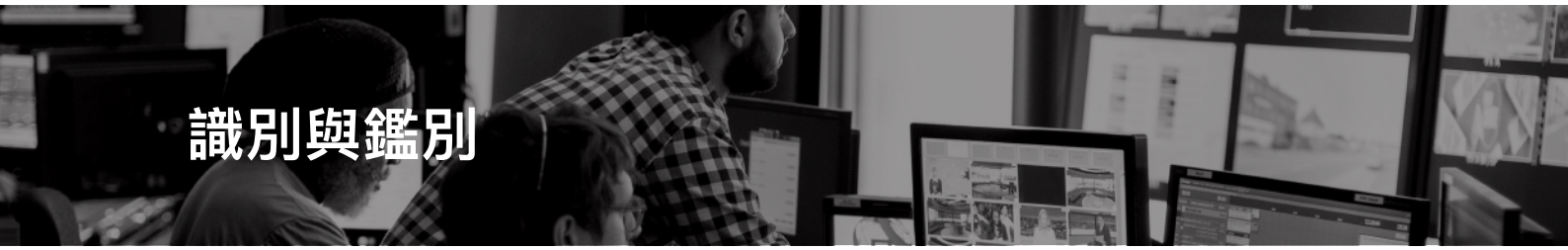
一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。

二、等級「普」之所有控制措施。

- 普系統防護需求

資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。

UPAS系統自動產生自動產生ARP、SNMP、AD軌跡資料與資安事件、系統操作紀錄並加密保護5年以上，達到「高防護需求分級」的要求。



識別與鑑別

內部使用者之識別與鑑別

- 高系統防護需求

一、對帳號之網路或本機存取採取多重認證技術。

二、等級「中」及「普」之所有控制措施。

- 中、普系統防護需求

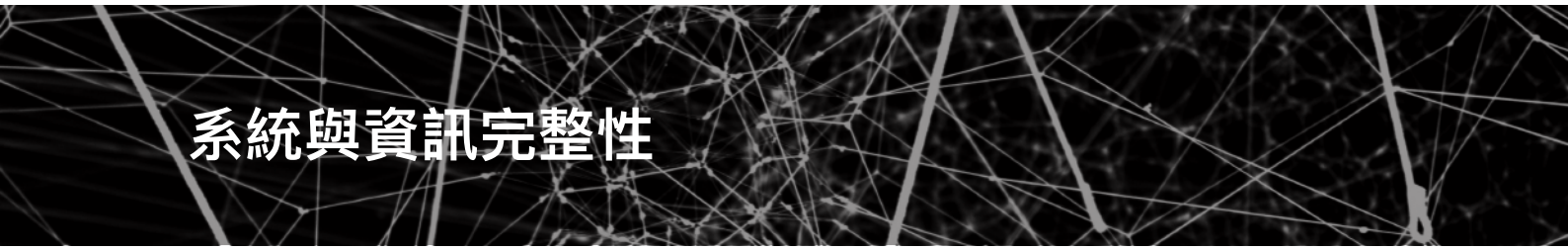
資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

非內部使用者之識別與鑑別

- 高、中、普系統防護需求

資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。

透過專利技術辨識設備屬性/電腦名稱/MAC位址對設備進行網路存取控制，禁止使用本機登入，強迫使用特定AD帳號登入電腦設備，以此確定使用者資訊，並限制所能使用人員，也可搭配AD/IDC/GAM模組進一步認證使用者身分，達到「高防護需求分級」的要求。



系統與資訊完整性

資通系統監控

- 高系統防護需求

一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。

二、等級「中」之所有控制措施。

- 中系統防護需求

一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。

二、等級「普」之所有控制措施。

- 普系統防護需求

發現資通系統有被入侵跡象時，應通報機關特定人員。

UPAS掌握全部內網的連線活動，可以自動識別連線設備是否為合法設備，並在發現非法連線時進行阻斷、主動告知管理人員，阻止災害擴大；符合「中防護需求分級」的要求。

非內部使用者之識別與鑑別

- 高系統防護需求

一、應定期執行軟體與資訊完整性檢查。

二、等級「中」之所有控制措施。

- 中系統防護需求

一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。

二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。

三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。

- 普系統防護需求

無要求。

使用PM模組可檢查應裝軟體是否正確安裝，或是否安裝盜版、禁用軟體，在發現違規時阻斷其網路使用並透過重導頁面要求修正；符合「高防護需求分級」的要求。

協助企業及政府
盡快完善內網管理

UPAS提供最全方位的解決方案，讓您快速建置內網安全，打造零信任安全架構，符合資安法內網相關規範。欲了解更完整的內網管理資訊，請查看下方資訊：

UPAS官方網站
了解更多關於UPAS的內網管理方法，包含NAC、IPAM、IAM、ITAM等內網重點管理事項。

UPAS Medium
訂閱UPAS Medium獲取更多內網安全最新即時資訊、相關資安新聞，以及UPAS產品資訊。

下載更多UPAS相關手冊
閱讀UPAS相關產品手冊，提供稽核、企業建議書等多樣內容。

申請POC測試
體驗UPAS NOC解決方案，專人與您進行需求評估，提供您最佳的內網管理方案。

UPAS NOC 內網管理中心

內網安全，一手掌握

立即聯絡我們，守護您的內網

WEBSITE MEDIUM FACEBOOK

UPAS
NETWORK OPERATIONS CENTER

UPAS 優倍司股份有限公司
https://www.upas-corp.com/

總部：台北市信義區基隆路二段51號9樓之8
TEL：02-27393226 / 02-77180425
FAX：02-27392836

研發中心：高雄市前鎮區民權二路6號18樓之3
TEL： 07-9700229
FAX： 07-9700225