政府零信任架構規劃與經驗分享

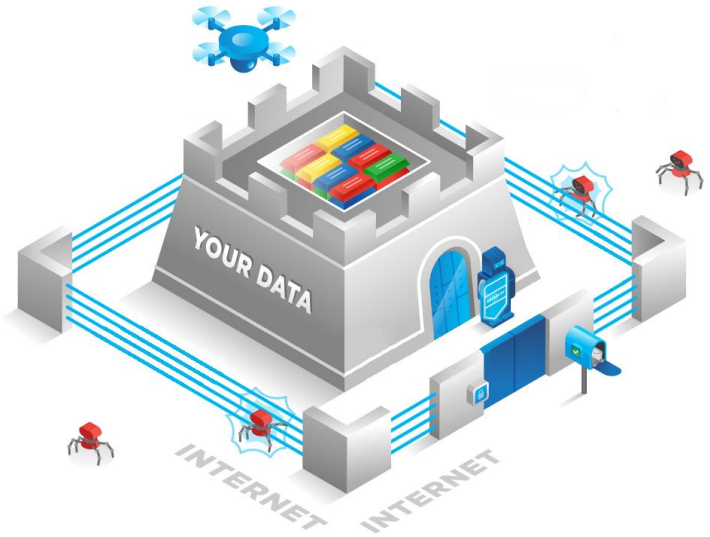
大綱

- 緣起
- 國際零信任架構推動概況
- 政府零信任架構規劃
- 零信任架構功能符合性驗證
- 政府機關導入經驗分享

緣起

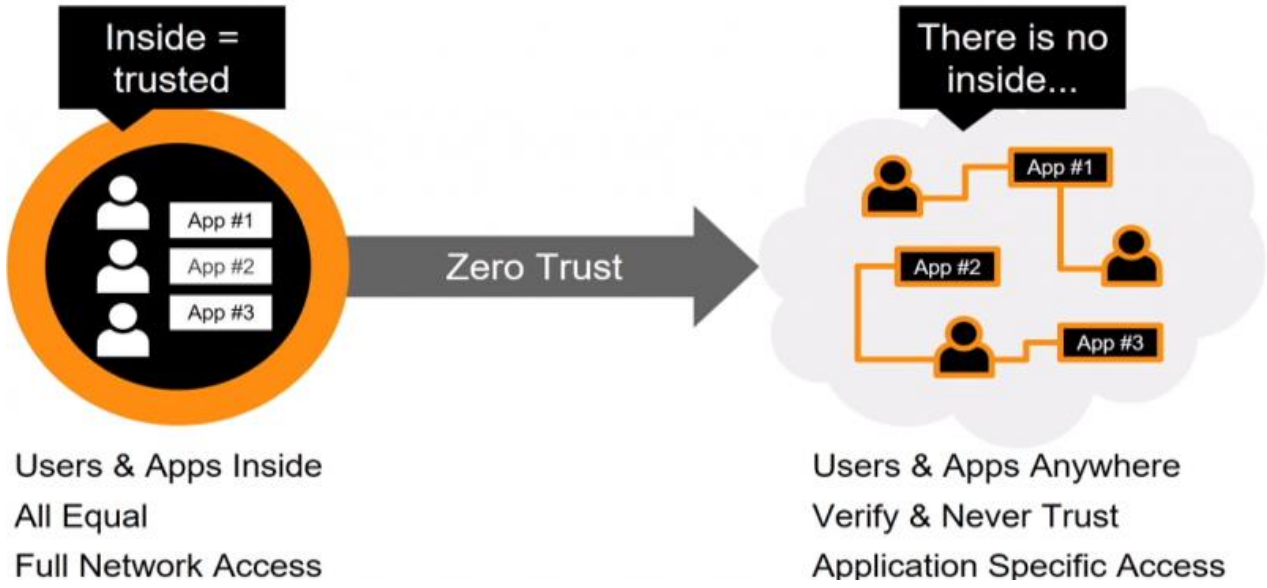
傳統網路模型的資安窘境

- 隨著資料/服務雲端化、使用者行動化及存取設備多元化，傳統網路模型已現資安窘境
  - 傳統奉行基於信任邊界的網路威脅模型，邊界內存取受信任、邊界外存取不受信任，惟許多攻擊直接或間接來自信任邊界內，且面對複雜的網路環境變化，邊界的形成越發困難



零信任概念

- 突破傳統網路模型之資安窘境，保護資料存取
  - –非保護網路存取，聚焦保護**資料/應用**存取
  - –無具體邊界，使用者/設備與資料/應用無處不在
  - –任何資料存取**永不信任**(Never Trust)且**必須驗證**(Always Verify)
- 實施零信任會是一段過程，而不是一次大規模替換基礎架構，且與傳統模式會同時混合運作



零信任定義與原則

- 零信任定義
  - 定義：不預設信任任何使用者與設備，透過持續驗證、細緻存取控制，授予最小權限
    - 不預設信任內外部的任何使用者、設備、網路流量
    - 在授予存取權限前，需要明確的身分驗證程序
- 零信任6大原則
  1. 不信任任何存取
  2. 一致集中政策管理與執行
  3. 使用者與設備強認證
  4. 細緻存取控制
  5. 建立邏輯邊界
  6. 持續監控驗證

國際零信任架構推動概況

全球零信任推動概況

- 零信任架構已從**概念探討階段**進入**實務部署規劃**，各國紛紛建立零信任架構推動策略

美國

2021年 5 月，美國總統拜登於發布行政命令，推動聯邦政府導入零信任架構

新加坡

2021年10月，新加坡發布網路安全戰略，要求實施政府零信任架構(GovZTA)

歐盟

2022年9月，歐盟執委會發布資安韌性法草案，以零信任架構作為基本的網路安全措施

韓國

2023年6月，韓國科學技術情報通信部(MSIT)發布零信任指引1.0版

英國

2021年7月，英國發布零信任架構設計原則1.0版

日本

2022年9月，日本數位廳參考美國 NIST相關標準規範，發布零信任架構應用策略

加拿大

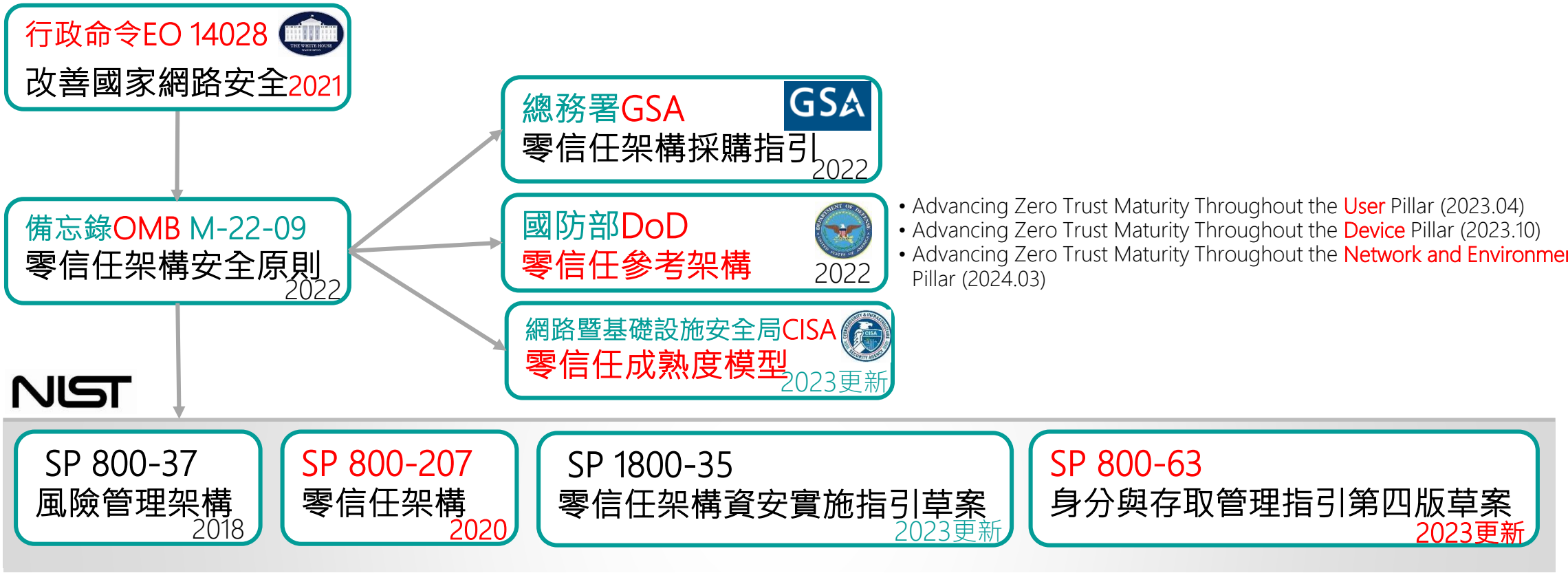
2022年11月，加拿大發布零信任安全模型

澳洲

2023年11月，澳洲發布2023-2030網路安全策略，宣示2030年公共服務須具備零信任文化

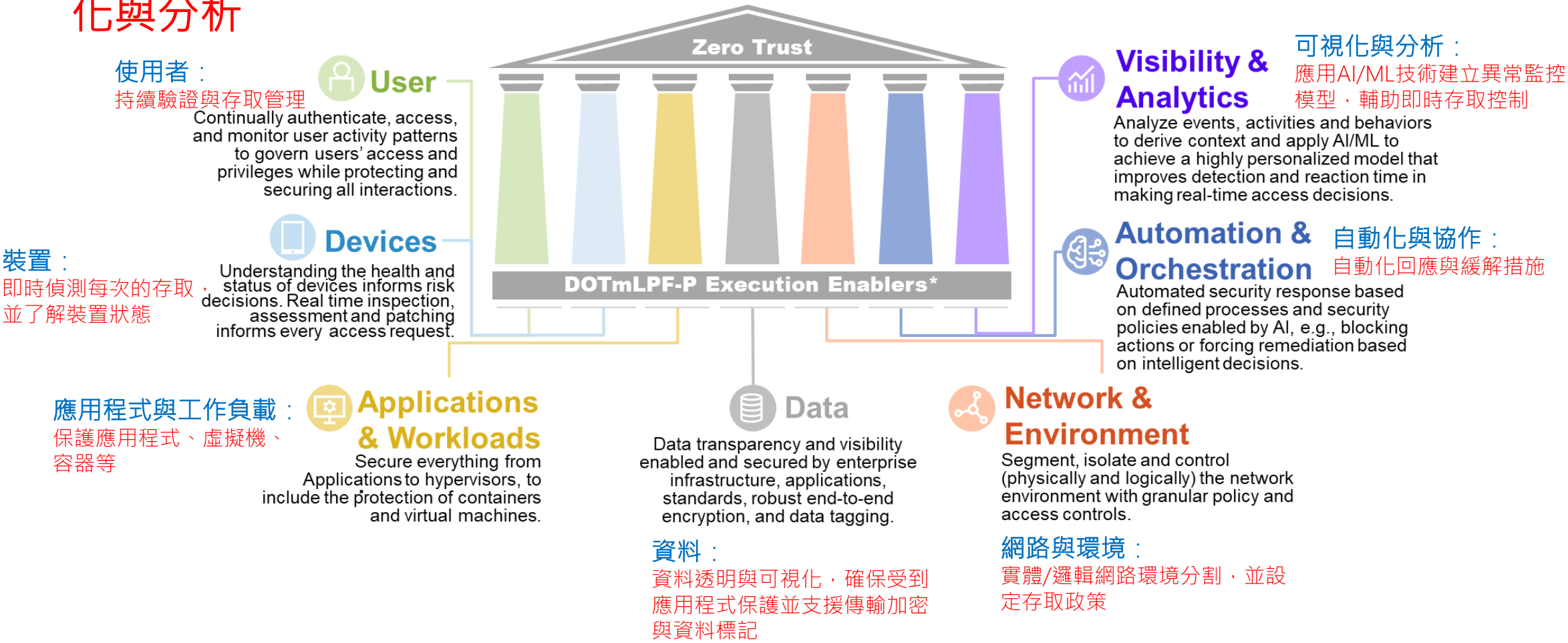
美國推動零信任架構相關文件

- 美國推動零信任架構係依總統之行政命令(EO 14028)，要求聯邦政府遵循零信任架構，並採取一系列措施強化資安，以防禦外部攻擊



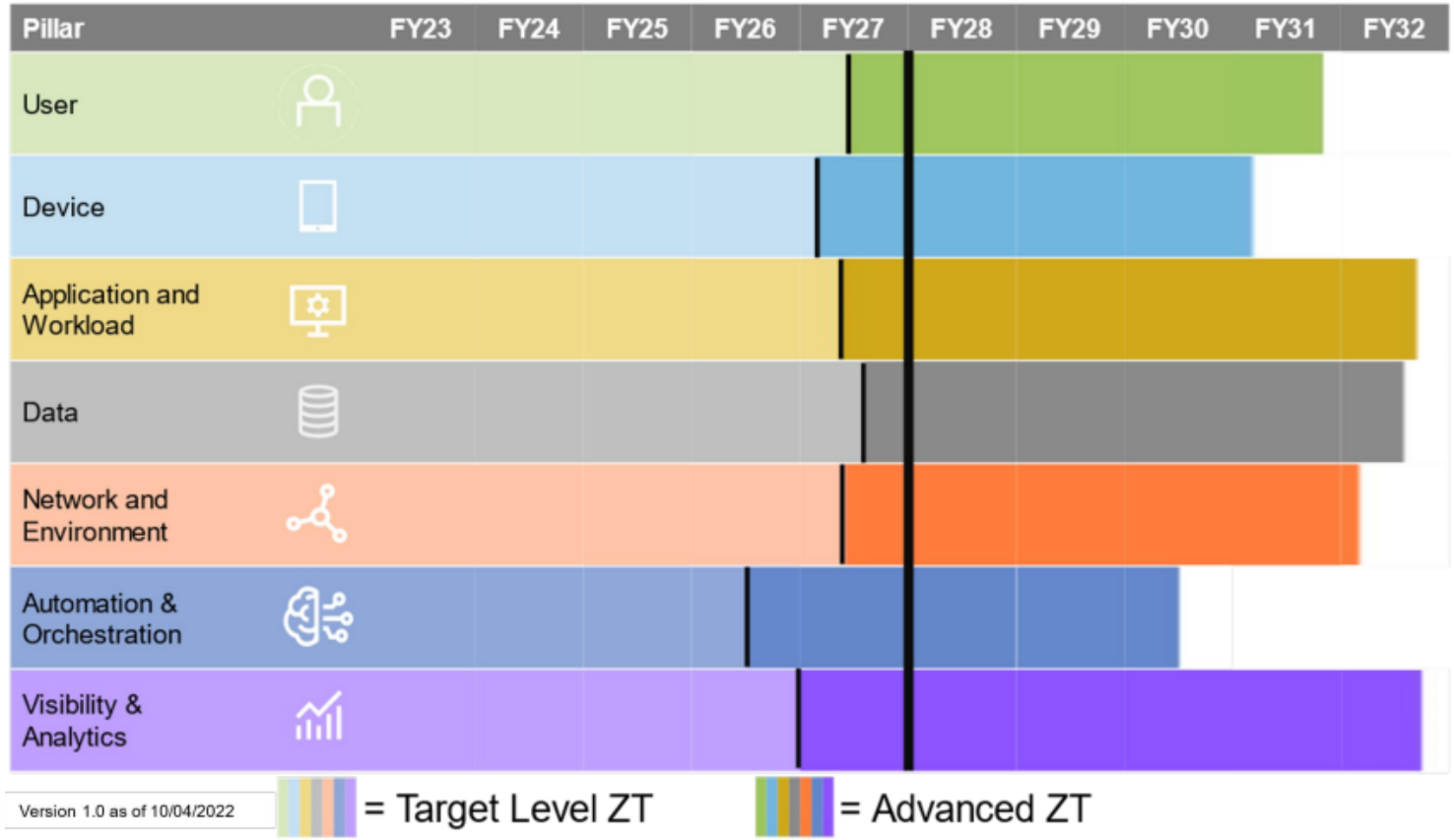
美國DoD零信任參考架構(1/3)

- 2022年7月，美國發布國防部(DoD)零信任參考架構2.0版，包含七個支柱：使用者、裝置、應用程式與工作負載、資料、網路與環境、自動化與協作及可視化與分析



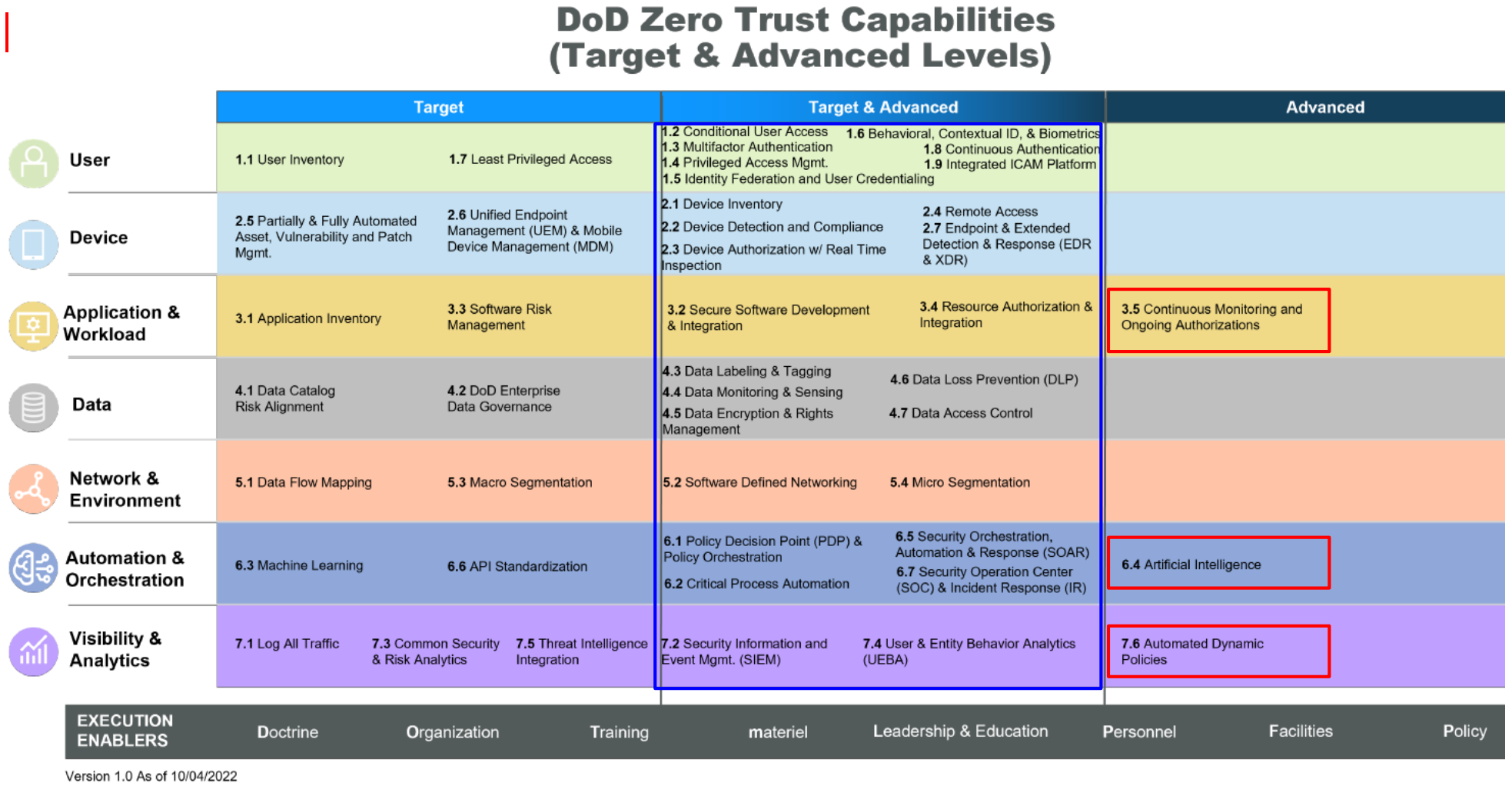
美國DoD零信任參考架構(2/3)

- 2022年11月，美國發布國防部(DoD)零信任策略，DoD零信任參考架構七個支柱之Target Level(目標等級)與Advanced Level(進階等級)推動期程，規劃2027年完成零信任架構部署達到Target Level之目標



美國DoD零信任參考架構(3/3)

- DoD零信任參考架構七個支柱細部展開，共45個能力(Capabilities)要求，其中**持續監控與自動化**、**人工智慧**及**自動動態政策**等3個能力完全屬於Advanced level



美國CISA零信任成熟度模型

- 2023年4月，美國網路暨基礎設施安全局(CISA)發布零信任成熟度模型2.0版，零信任能力包含五個支柱：**身分**、**裝置**、**網路**、**應用程式與工作負載**及**資料**，其中**可視化與分析**、**自動化與協作**及**治理**橫跨以上五個支柱

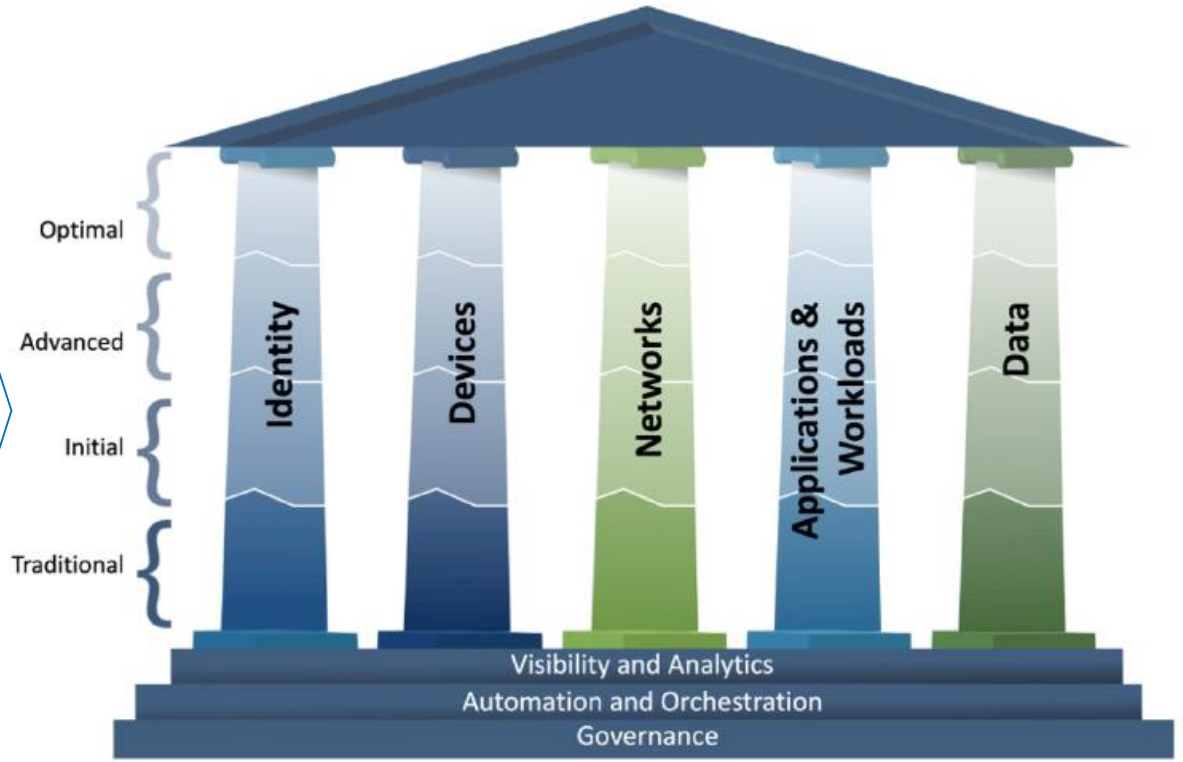
CISA零信任成熟度模型4個階段

最佳階段：完全自動化，動態政策，門檻形式動態最小授權，全域狀態感知

進階階段：自動控制，集中可視化，風險導向最小授權，支援預先定義之回應

起始階段：開始自動化設定，導入決策引擎，內部系統開始做可視化

傳統階段：手動設定，靜態安全政策，手動回應



韓國MSIT零信任準則

- 2023年6月，韓國科學技術情報通信部(MSIT)發布零信任準則1.0版，為導入零信任架構之政府機關、地方政府及企業組織提供必要資訊
- 參考NIST SP 800-207、CISA零信任成熟度模型等
- 建議規劃成熟度目標與考量組織內外部影響因素，如現有技術與政策法規等，並考量相關驗證，如ISMS驗證、雲端安全驗證、資訊通訊網路設備資安驗證等
- 零信任成熟度模型，新增「系統」支柱
  - **身分**：整合IAM、MFA、細緻存取控制
  - **設備**：資產盤點、EDR布建
  - **網路**：DNS/HTTP加密、邏輯隔離
  - **系統**：強認證、最小權限、微分割
  - **應用**：軟體安全驗證、第三方稽核
  - **資料**：資料治理、即時去識別化、存取稽核

韓國零信任成熟度

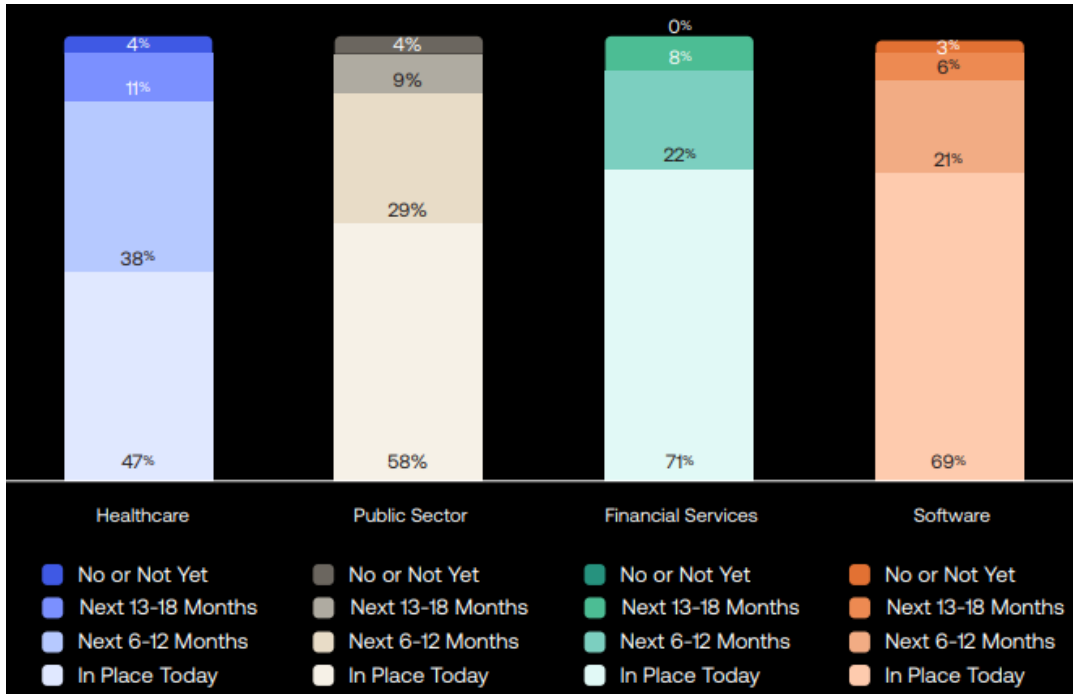
成熟度	說明	所需的安全技術特徵
傳統	尚未採用零信任架構，並且主要應用專注於網路防禦基於邊界的安全模型 (對複雜攻擊、內部攻擊等存在一些漏洞)	• 手動設定，靜態安全策略 • 本地身分(有時是 SSO 與多重身分驗證) • 對外部系統具有粗粒度依賴性的特定支柱解決方案 • 透過設定構建最低權限 • 政策應用專屬特定支柱 • 被動事件回應與緩解
進階	對零信任理念的部分採用，其中零信任原則是安全體系結構的核心功能 (部分應用最低權限訪問、網路分段、日誌記錄與監控，以實現比基本更高的安全性)	• 細粒度的用戶與設備訪問控制 • 實施集中式身分控制與政策，根據狀態進行最低權限修改 • 網路被部分分段 • 一些支柱彼此之間有一致性 • 集中可視性 • 使用預設的緩解技術回應某些事件 • 在外部系統與依賴關係方面增加了細節
最佳化	全公司範圍內應用零信任理念(透過自動化操作、網路分段及持續身分鑑別，以最小權限進行安全存取控制)	• 透過自動化/即時分析對 Federated ID與單點登錄等身分進行集中管理、持續身分與可靠性驗證及動態訪問控制 • 資產與資源的全自動盤點，授予最低權限 • 網路被劃分為具有特定訪問規則的粒度區域 • 透過開放標準實現支柱之間的互操作性 • 具有歷史功能的集中可視性，可記住特定時間點的狀態

韓國零信任應用情境

應用情境	目標與要求	實踐重點
分公司/遠端存取	● 確保分公司/遠端使用者安全連線 ● 提供一致的存取控制體驗 ● 強化身分驗證與設備安全性檢查	● 軟體定義邊界 ● 設備信任驗證 ● 應用層存取控制
第三方協作	● 即時啟用/撤銷第三方存取權限 ● 限制第三方存取範圍 ● 監控第三方行為，降低資料外洩風險	● 即時動態權限 ● 細緻存取控制 ● 持續監控
業務網路/網際網路隔離	● 維持網路隔離降低攻擊面 ● 提供彈性的使用者存取方式 ● 根據風險動態調整信任程度	● 軟體定義微分割 ● 持續信任評估
內部部署與雲端整合	● 跨內部與雲端的一致存取管理 ● 集中化身分認證與授權 ● 防止雲端資料外洩與未經授權存取	● 一致的政策管理 ● 使用者/設備統一驗證 ● 雲端DLP/CASB部署
OT/ICS工業控制	● 保護關鍵工控資產與網路 ● 最小化橫向移動風險 ● 控管可信任設備接入	● 邊界防護 ● 微分割 ● 可信任設備管理
M2M/物聯網	● 建立機器對機器的信任機制 ● 保護機器間通訊介面的安全 ● 偵測異常存取行為	● 機器身分認證 ● API安全 ● 異常行為偵測

雲端安全聯盟(CSA)調查

- 2024年1月22日，CSA發表「State of Zero Trust Across Industries」一文，針對不同產業調查零信任導入情形，總樣本量為13個國家、860名資安決策者
  - **金融產業**採用零信任服務居於領先，約71%金融機構已實施；**軟體產業69%**已實施
  - **公部門**對零信任計畫之推廣正在提升，有 58%受訪者表示該組織正在實施零信任，最主要採用的安全措施為多因子身分鑑別，34%公共部門規劃在未來12-18個月將多因子身分鑑別擴展到外部使用者
  - 80%組織受訪者調查2023年**零信任預算**比前一年提升，代表2024年導入零信任將逐漸普及
  - 採用零信任解決方案的挑戰，前三名依序為成本問題、技術差距、隱私法規/資料安全



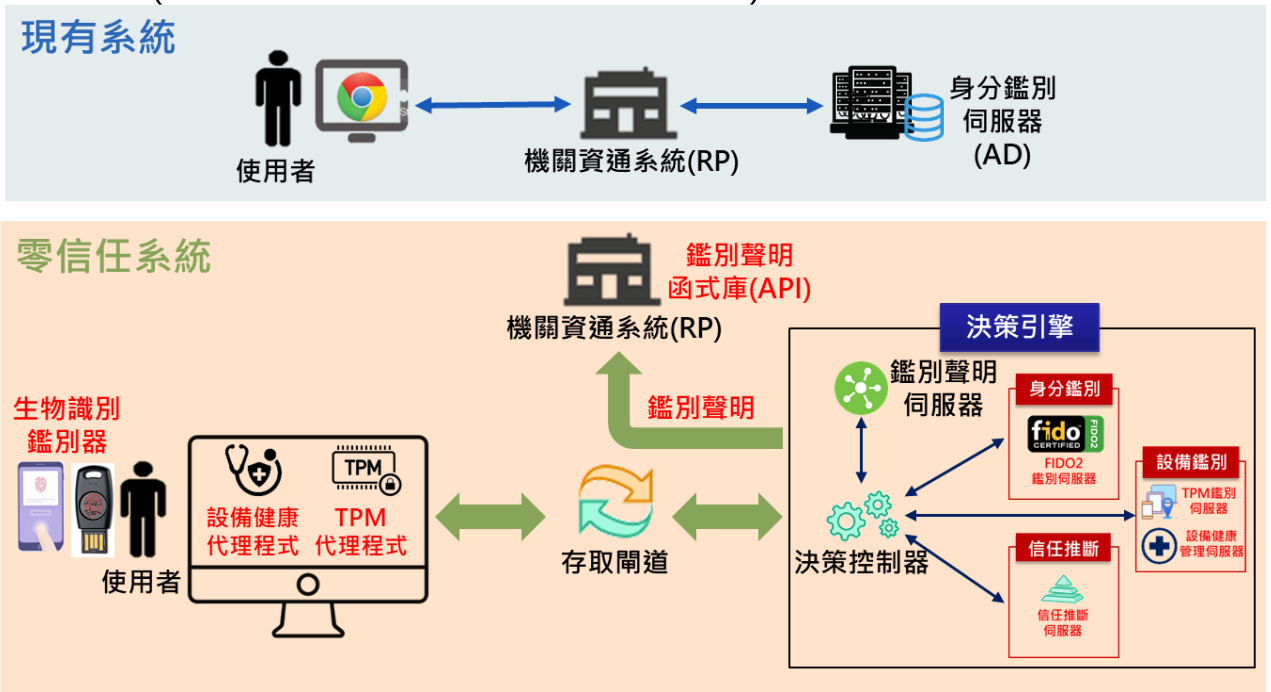
零信任實施情形調查

https://cloudsecurityalliance.org/blog/2024/01/22/state-of-zero-trust-across-industries

政府零信任架構規劃

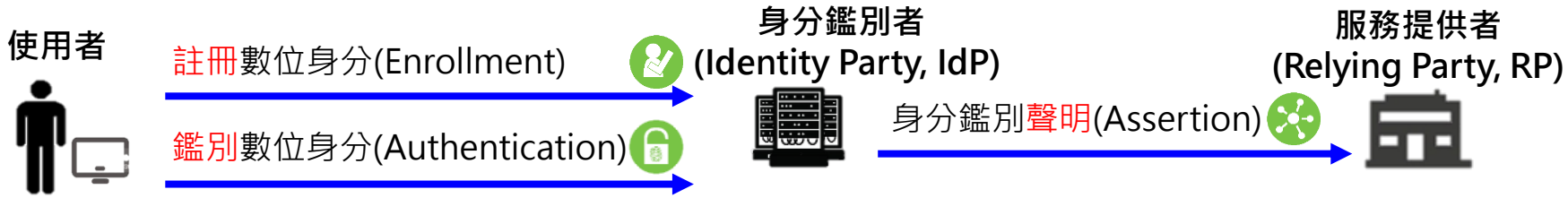
我國政府零信任架構規劃

- 參考美國國家標準與技術研究院(NIST)SP 800-207零信任架構，採取資源門戶之部署方式(Resource Portal-Based Deployment)
- 我國政府零信任架構包含3大核心機制
  - **身分鑑別**：多因子身分鑑別(如FIDO聯盟無密碼機制)與鑑別聲明
  - **設備鑑別**：設備鑑別與設備健康管理
  - **信任推斷**：使用者情境(身分、設備、行為等面向)信任推斷機制



身分鑑別機制規劃

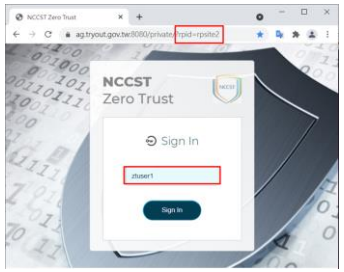
- 參考NIST SP 800-63-3對於身分保證等級(IAL)、鑑別保證等級(AAL)及聯邦保證等級(FAL)之定義，在零信任架構功能性，至少滿足IAL2/AAL3/FAL2之身分保證等級、鑑別保證等級及聯邦保證等級，以支援政府領域之資安防護需求

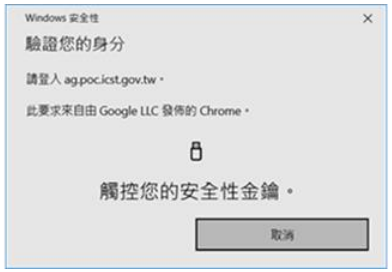


	身分保證等級(IAL) Identity Assurance Level	鑑別保證等級(AAL) Authenticator Assurance Level	聯邦保證等級(FAL) Federation Assurance Level
說明	使用者用來證明自己身分之強度	鑑別過程之防護強度	身分鑑別者(IdP)傳遞給服務提供者(RP)之身分鑑別聲明(Assertion)之防護強度
等級1	自己宣稱之身分便具有效力	至少需要單因子身分鑑別	身分鑑別聲明須經過IdP簽章
等級2	需親自提供證據進行身分證明	• 需要2種不同之鑑別因子 • 鑑別過程之通訊，需使用加密技術	身分鑑別聲明須簽章與加密
等級3	需在監督下親自提供證據與生物特徵進行身分證明	• 透過密鑰(key)進行鑑別 • 需要硬體加密鑑別器	身分鑑別聲明須簽章與加密，且使用者應向RP證明，擁有與身分鑑別聲明對應之密鑰

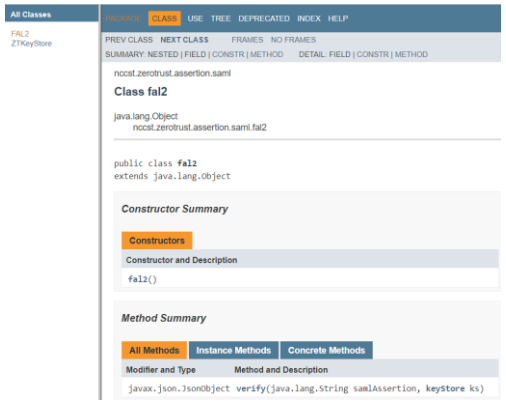
身分鑑別

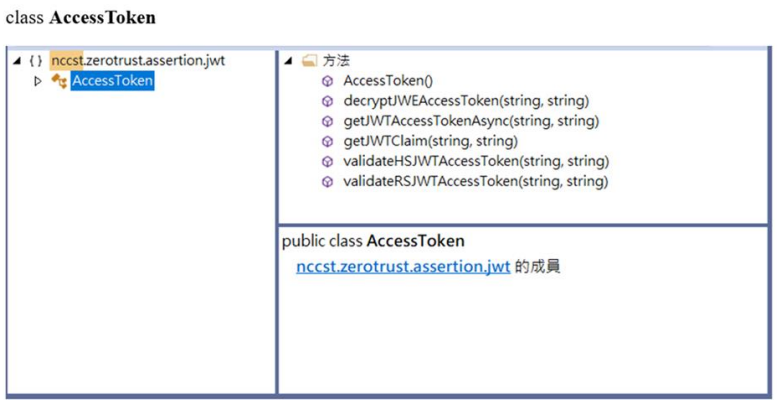
- 以無密碼雙因子方式達成身分鑑別
  - 運用如FIDO2相關技術鑑別使用者之身分





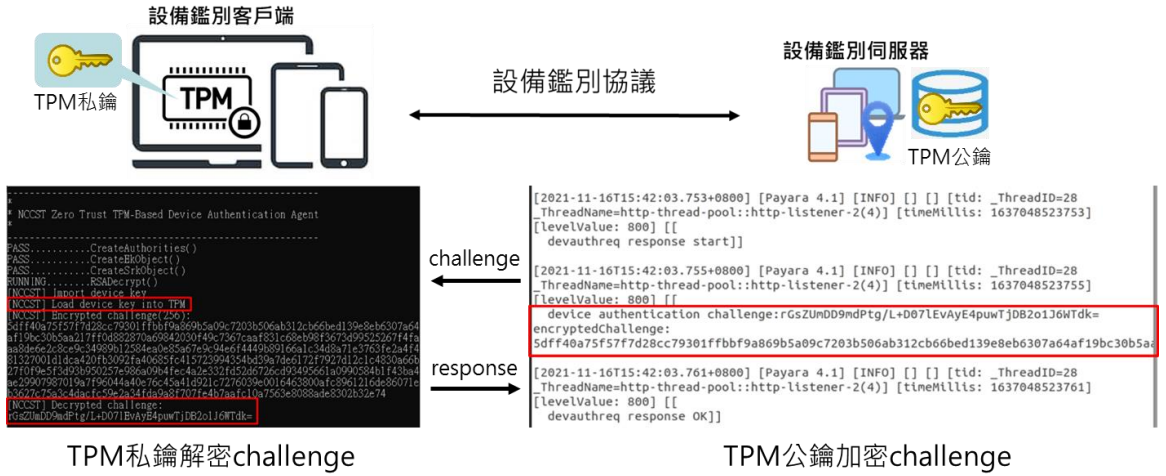
- 提供具備簽章與加密之鑑別聲明
  - 提供API函式庫，使機關之資通系統(RP)可解密並驗證鑑別聲明，以確保其機密性與完整性



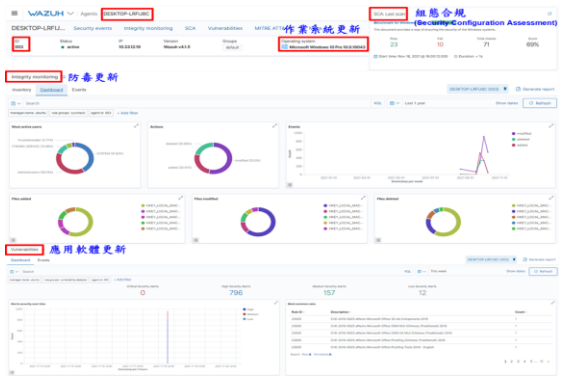


設備鑑別

- 基於公開金鑰技術之設備鑑別方法
  - 透過TPM或Agent產生金鑰與憑證，完成設備註冊與鑑別



- 設備健康管理
  - 持續性設備健康狀態監控
  - 依設備健康狀態計算設備健康信任等級

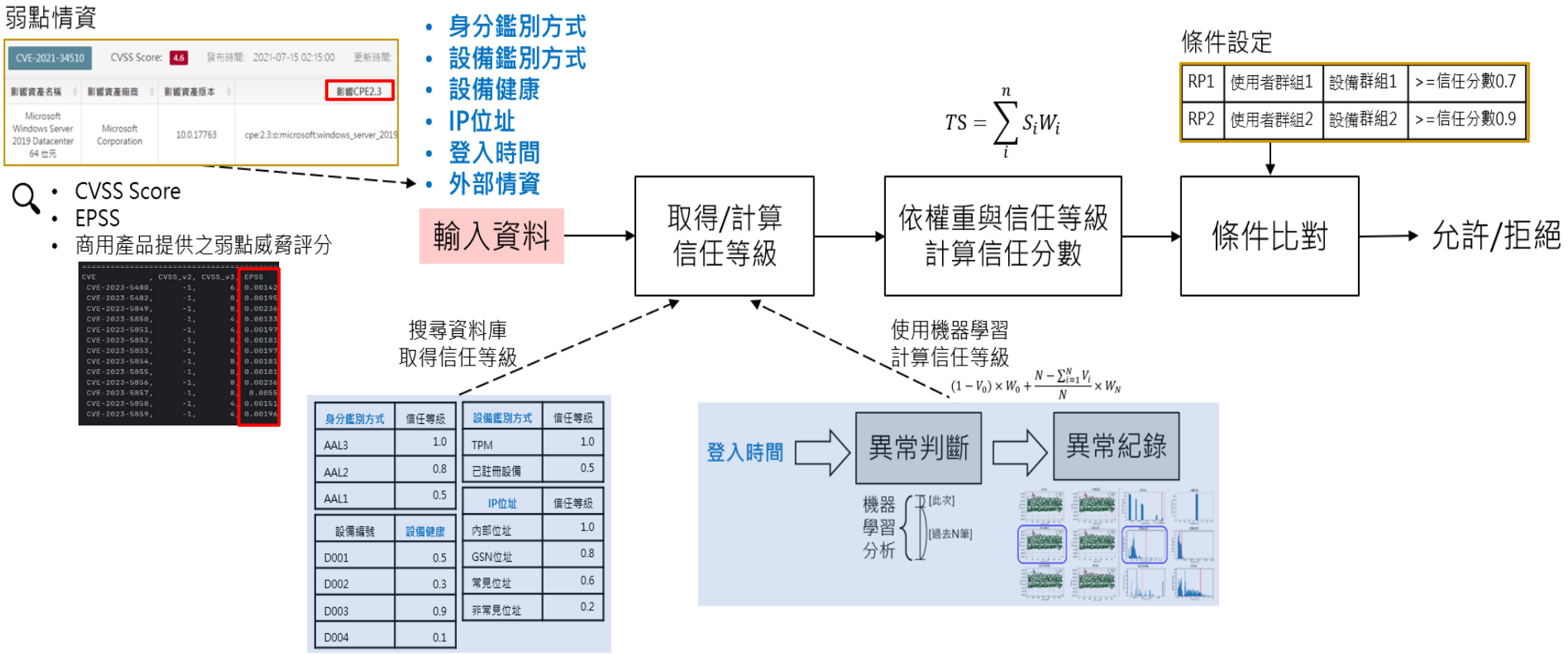


設備編號	設備健康狀態	信任等級
D001	AD	0.5
D002	CD	0.3
D003	ABC	0.9
D004	D	0.1

健康狀態/等級分配
(A)作業系統更新：0.4
(B)防毒更新　　：0.3
(C)應用軟體更新：0.2
(D)組態合規　　：0.1

信任推斷

- 基於信任推斷機制(規則、分數、規則與分數混合)決定存取權限
  - –如依使用情境計算每次存取之信任分數作為判斷依據

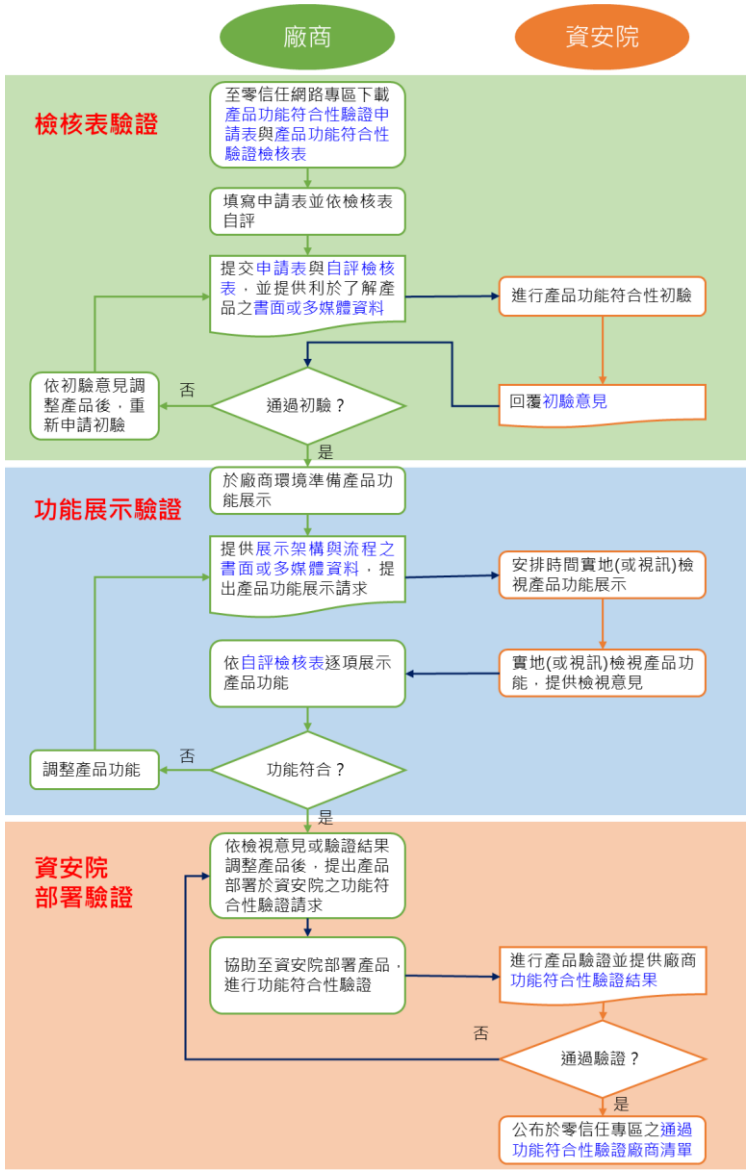


信任推斷機制概念流程-以分數為基礎

零信任架構功能符合性驗證

功能符合性驗證流程(1/2)

- 111年起，提供政府零信任架構身分鑑別與設備鑑別產品功能符合性與整合驗證服務；113年3月中旬起，開始接受信任推斷產品功能符合性驗證申請，以利政府零信任架構之導入
- 零信任架構功能符合性檢測流程分為3個階段
  - **檢核表驗證**：廠商依檢核表自評
  - **功能展示驗證**：廠商依檢核表Demo各項功能
  - **資安院部署驗證**：廠商至資安院之測試環境部署產品



功能符合性驗證流程(2/2)

- 檢測基準原則
  - 依照所公開之檢核表之檢核項目進行功能符合性驗測，無獨厚特定廠商規格
  - 依據檢核表採一致性功能檢核標準，確保產商產品在通過驗證前具備基準功能要求
  - 受理廠商產品案件，採先進先出，按照送件順序回應，以保持公平性
- 零信任架構功能符合性驗證說明資料公布於資安院官網「零信任架構專區」(https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/)

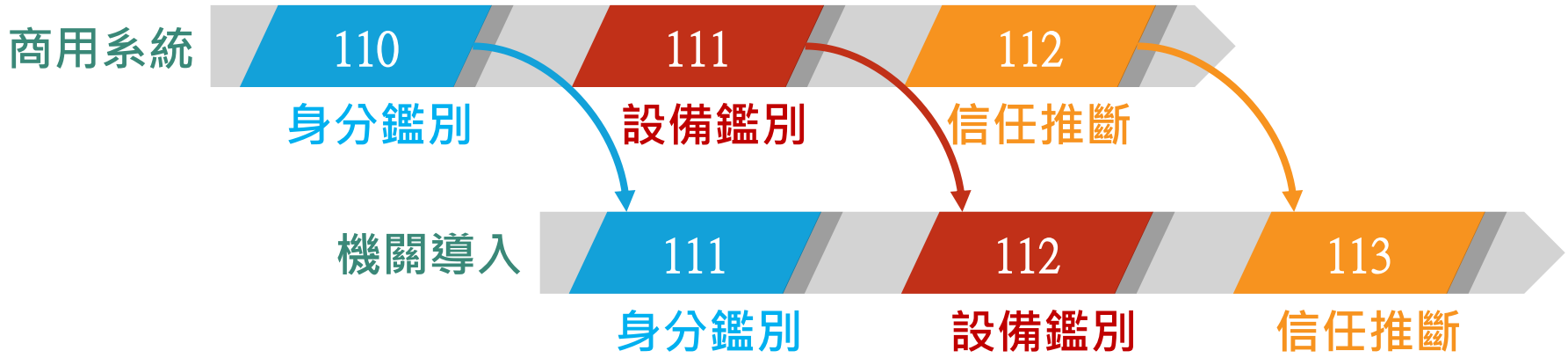
持續精進功能符合性驗證作業

- 功能符合性驗證機制可促進廠商合作整合
  - 藉由身分鑑別、身分鑑別+設備鑑別，到身分鑑別+設備鑑別+信任推斷的驗證模式，可促進廠商彼此整合與結盟，完善零信任架構的核心組件，以供後續政府及各領域參考
  - 官網公布之通過清單有聲明產品驗證範圍以「在驗證期間提交給資安院之版本」，以及根據「資安院所核定之檢核表之範圍」為限；並向政府機關宣導要向通過驗證廠商索取檢測報告
- 廠商在驗證過程中若有功能不足處，且非廠商產品既有功能時，或實於地部署驗證階段，廠商要配合開發或排除技術問題，因而延長驗證時程，需要與廠商做密切的溝通，並**優化檢驗流程**
  - 因應方式為在資料審核階段，資安院團隊會盡可能提出相關建議，以便廠商及早準備，避免廠商在驗證後期才收到相關建議
  - 了解各廠商皆有通過驗證的時程壓力，資安院團隊基於公平性會按順序受理，並**持續精進以提升受理之量能**
- 持續對廠商宣導提交送驗產品之資安檢測報告之必要性

政府機關導入經驗分享

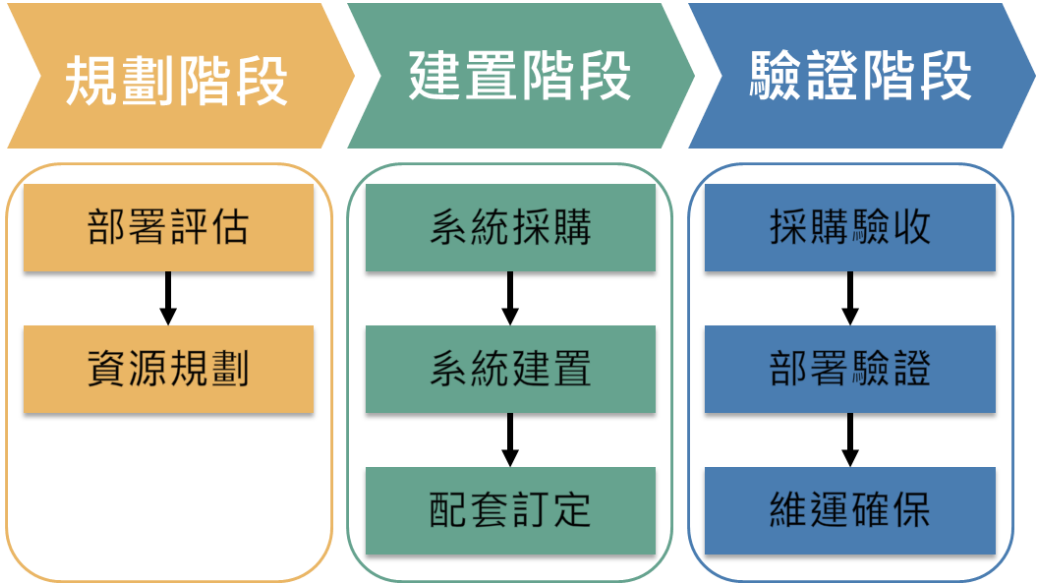
我國政府零信任架構推動規劃

- 依據「第六期國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略
  - –110年完成零信任架構與概念性驗證機制研究與部署機制
  - –111~113年遴選2個機關逐年導入身分鑑別等3大核心機制
- 辦理廠商說明會
  - –擴大廠商參與投入產業意願，建立政府機關導入所需量能



依發展方案進行機關試行與導入

- 機關遴選、試行與導入：110年 ~
  - 遴選標準
    - 機關資通系統之帳號集中度高
    - 所屬機關資通系統向上集中度高
    - 機關資通系統由外網存取之需求高
    - 機關之配合意願高



- 數位發展部(含所屬機關)：111年8月 ~
  - 於建置資通系統時導入零信任網路機制，強化資安防護

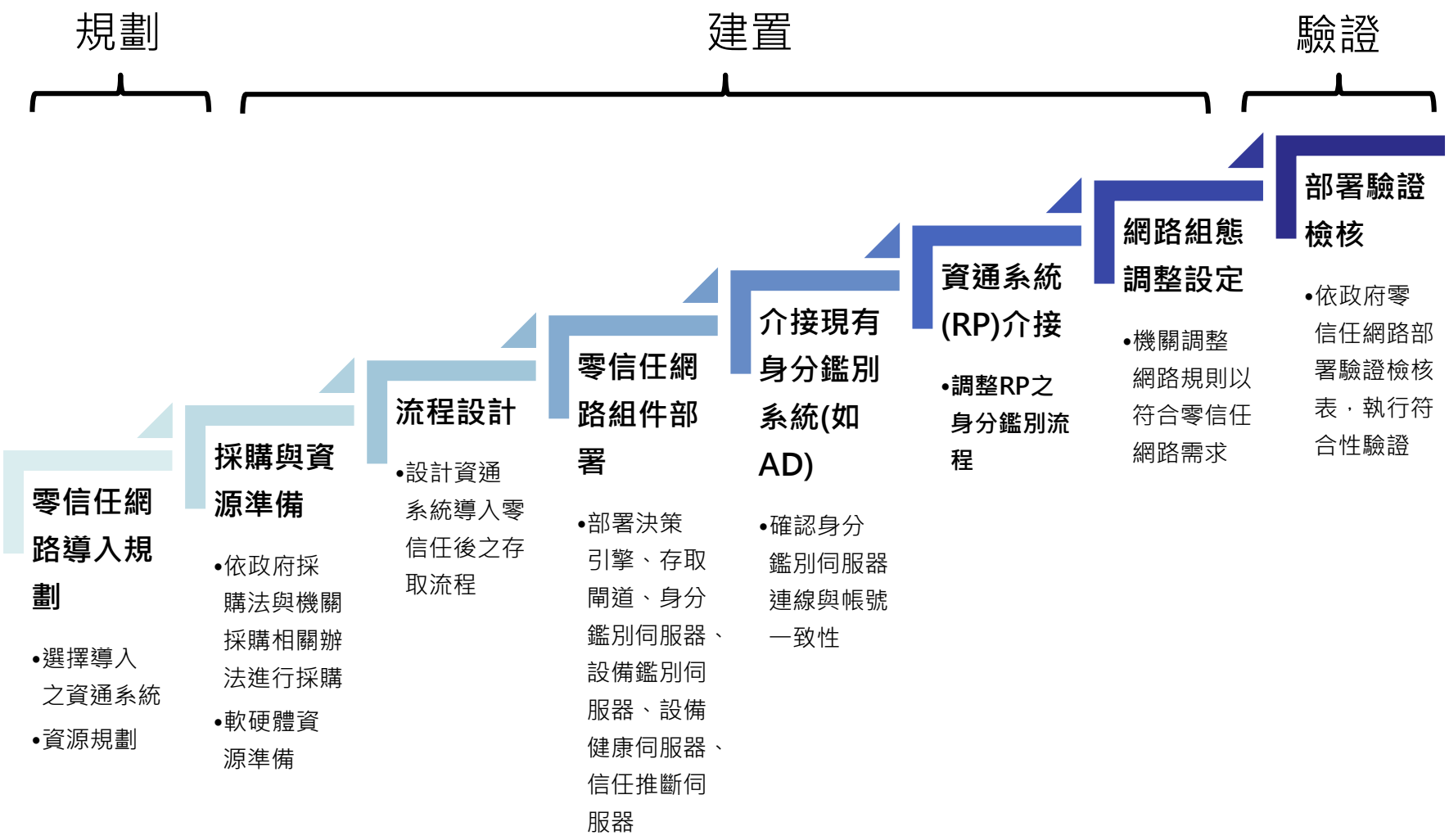
擴大推動A級政府機關導入

- 優先推動A級政府機關導入零信任架構
- 112年身分鑑別導入機關，以完成導入T-Road之機關為優先
- 112年擇定2個機關試行「設備鑑別」之導入

	前置作業	介接與設定	維運階段
數發部	1.ZTA推動說明會 2.身分鑑別採購作業	得標廠商提供ZTA API文件與範例程式碼給RP廠商進行介接	1.辦理驗收作業 2.財產移交作業
導入機關	1. 選擇導入之資通系統 2.準備導入所需環境，如虛擬機及網路環境(ZTA伺服器憑證及網域名稱)	1. RP開發廠商進行程式調整，導入身分鑑別流程 2.準備ZTA所需硬體資源(或實體安全金鑰)	1. 依資安法相關管理及機關內部規範，實施相關資安措施管理及維管 2.保固後編列預算辦理維運作業
資安院	政府零信任技術與架構諮詢		

機關導入流程

- 機關導入零信任架構主要分為規劃、建置及驗證三個階段

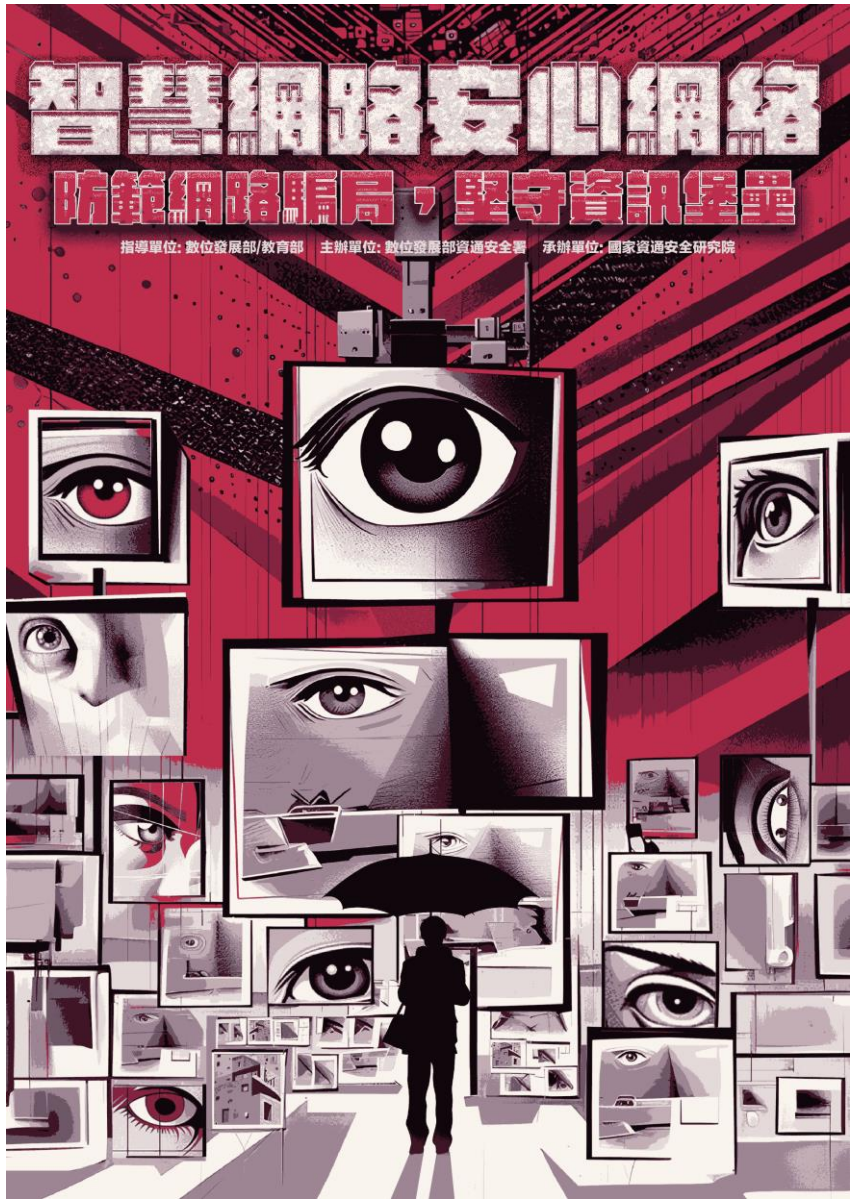


政府機關導入面臨挑戰

- 綜整政府機關試行情形，分析導入之主要挑戰與建議措施

主要挑戰	說明	建議措施
導入意願與採購成本	機關可能受限於經費與人力等配合因素影響導入意願	數位發展部已辦理公開說明會，說明零信任架構之導入目的與效益，並編列預算協助資安責任等級A級機關優先導入零信任架構身分鑑別機制
資通系統介接	機關資通系統多元，大部分委外由不同廠商開發，機關必須考量調整所需成本與廠商配合度等議題	資安院已協調通過驗證之零信任架構商用產品須提供資通系統介接多元函式庫，以降低所需成本與提高配合度
實體安全金鑰管理	實體安全金鑰相對於手機APP，可能會有遺失風險，須加強資產管理	• 資安院已協調通過驗證之零信任架構商用產品須同時支援實體安全金鑰與手機APP • 實體安全金鑰可比照門禁卡進行管理
零信任產品後續導入相容性問題	零信任架構之3大核心機制(身分鑑別、設備別、信任推斷)未必由同一家廠商提供，後續導入必須考量解決相容性與整合問題	資安院已協調通過驗證之零信任商用產品須提供API與相關說明文件供其他產品進行整合

112年資安海報第一名作品



報告完畢
敬請指教