政府機關導入零信任架構初探

資誠聯合會計師事務所

黃承漢經理

| 經歷 |

- 資誠聯合會計師事務所
  資訊安全暨鑑識科技實驗室品質負責人
- 資誠聯合會計師事務所 風險及控制服務 經理
- 資誠聯合會計師事務所 風險及控制服務 資深顧問
- 資誠企業管理顧問股份有限公司　資深顧問
- 華碩電腦 IT運營專案課 資安工程師
- 曜揚科技 技術服務部組長
- 曜揚科技 技術服務部 系統工程師

| 專長 |

- 資訊安全管理制度(ISMS)輔導諮詢服務
- 營運持續管理系統(BCMS) 輔導諮詢服務
- 個人資訊管理系統(PIMS)輔導諮詢服務
- 品質管理(QMS)輔導諮詢服務
- 資訊科技服務管理(ITSM)輔導諮詢服務
- 零信任架構
- 資安治理成熟度分析
- PCIDSS
- 資通安全管理法應辦事項因應
- 上市上櫃公司資通安全管控指引因應
- 資訊風險管理、防毒軟體、DLP解決方案導入

| 專業資格和證照 |

- PMP(Project Management Professional)
  國際專案管理師認證2012~2025年
- EC-Council CHFI v8資安鑑識調查專家認證
- ISO 27001:2005，ISO 27001:2013, ISO 27001:2022資訊安全管理制度Lead Auditor
- BS 10012:2009 個人資訊管理制度 Lead Auditor
- BS 10012:2017 個人資訊管理制度 Lead Auditor
- ISO 29100:2011 個人隱私保護管理隱私框架Lead Auditor
- ISO 27018:2014 雲端個人隱私資料管理制度Lead Auditor
- ISO 27701:2019 個人資料隱私管理系統 Lead Auditor
- ISO 22301:2019 營運持續管理制度Lead Auditor
- ISO 17025 : 2017 資安實驗室主管驗證訓練合格
- SGS「資通系統防護基準–合規技術專員」證書
- ITIL v3 Foundation 認證
- Trend Certified Security Expert 趨勢認證資訊安全專家認證
- 微軟MCTS(Hyper-V 虛擬化解決方案)
- 微軟MCTS(Exchange 2010)
- 微軟MCTS(SharePoint 2010, Configuring)
- 中華數位SPAM SQR專業證照

Agenda

1 零信任架構概論

2 政府零信任架構說明

3 導入實務與挑戰

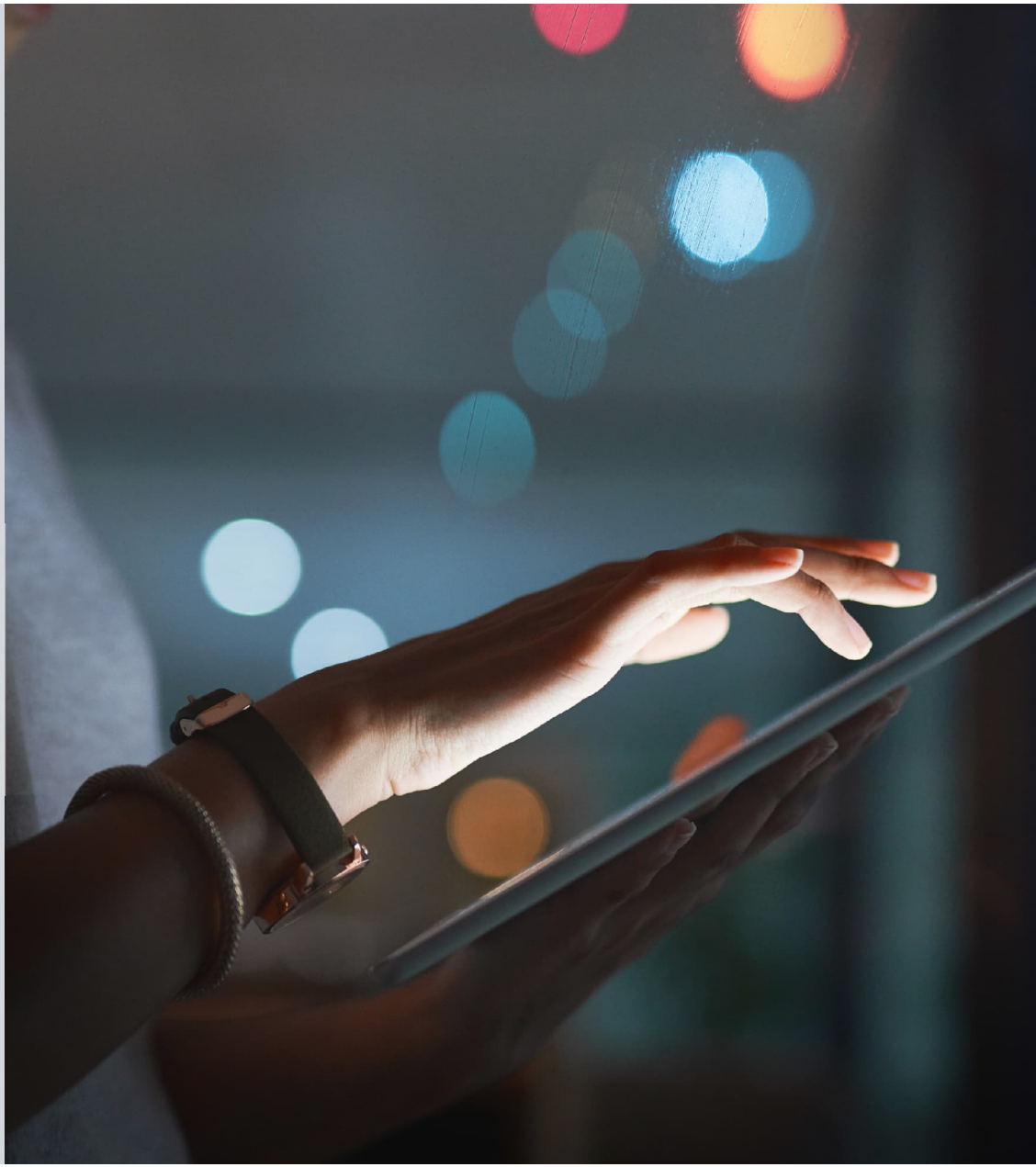
4 導入零信任架構對ISO 27001之影響

1

零信任架構概論

零信任架構的定義：

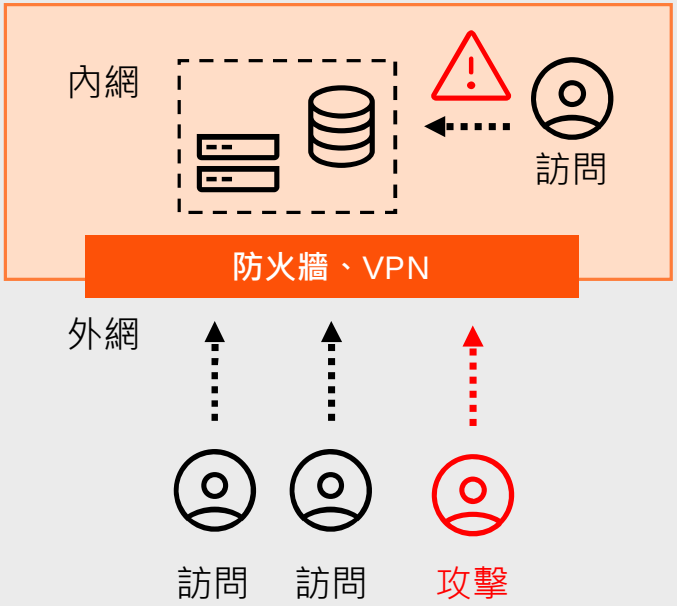
永不信任，持續驗證



零信任架構的定義：永不信任，持續驗證

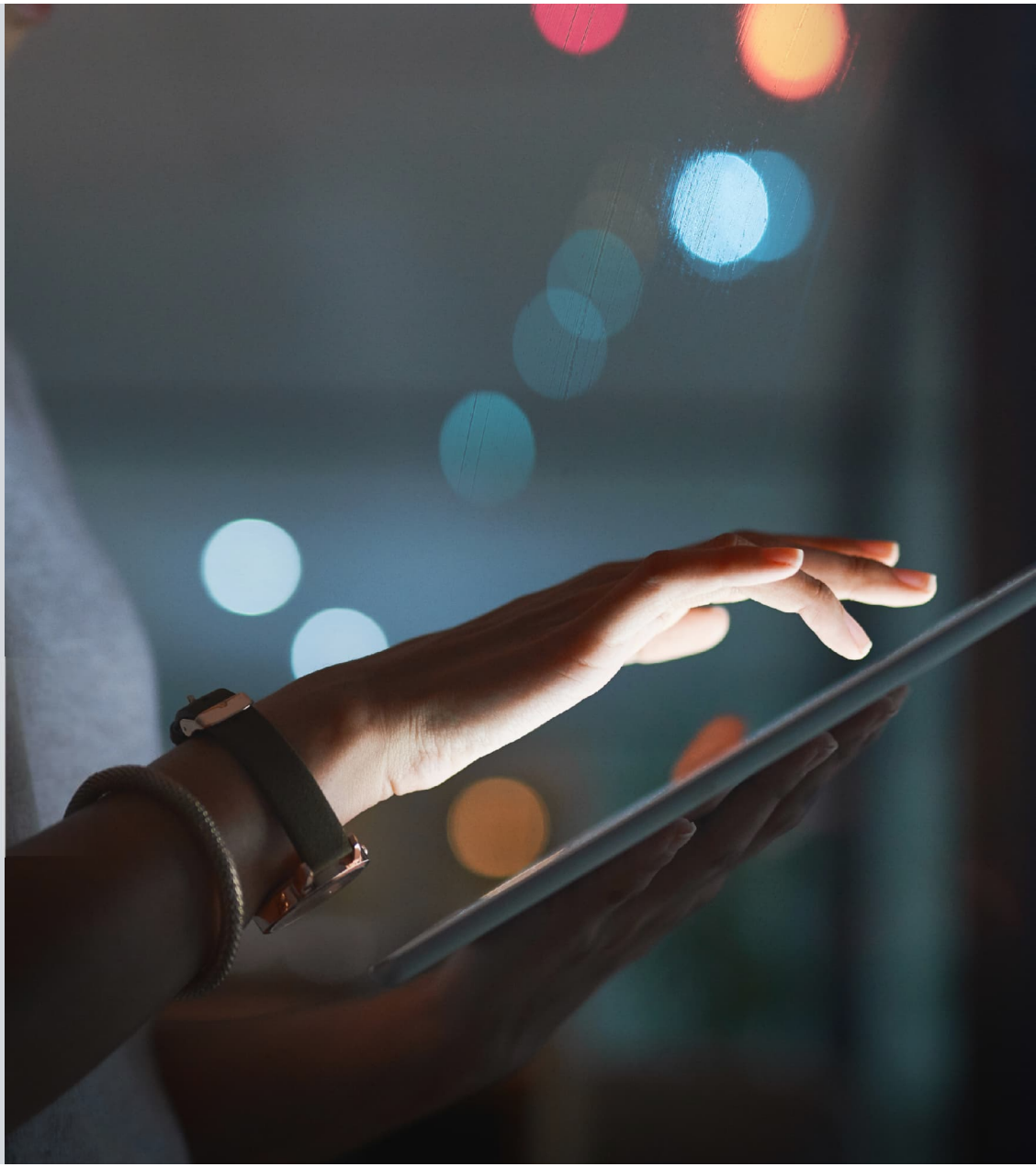
傳統邊界安全模型

- 傳統上，資訊安全的重點是設置「明確的網路邊界」，如同監管嚴密的城堡，防止外部威脅進入內部網路。
- **特點**
  依賴於防火牆和VPN等技術，主要保護企業內部網路內的資料和資源。
- **局限性**
  隨著遠程辦公、雲端服務和移動設備的增加，邊界逐漸模糊，破壞了原有的信任假設，使得內部威脅被忽視。



本頁內容參考「政府零信任架構說明_V2.1」

NIST SP 800-207標準簡介



PwC

NIST SP 800-207 標準簡介

- 背景：當傳統的安全模型不再滿足現代需求時，其內部資料橫向移動便不再安全。
- 目的：防止資料外洩並限制內部橫向移動，提供不同環境的安全適應性。

本頁內容參考NIST SP 800–207 零信任架構

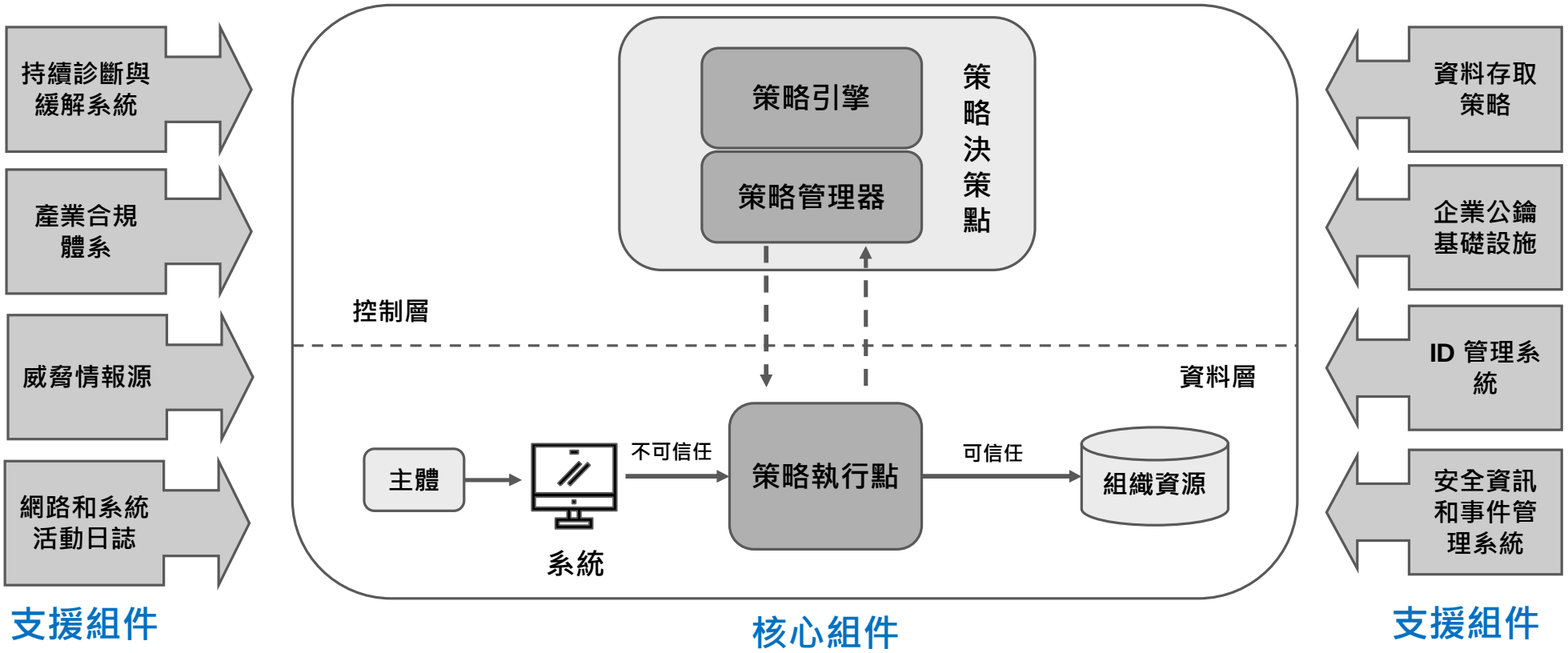
NIST SP 800-207 零信任7大原則

1. 所有資料來源和計算服務都被視為資源。
2. 無論網路位置如何，所有通訊都是安全的。
3. 各個企業資源的存取權限是按每個會話授予的。
4. 企業監控和測量所有擁有和相關資產的完整性和安全狀況。
5. 對資源的存取由動態策略決定，包括客戶端身分、應用程式、服務和請求資產的可觀察狀態，並且可能包括其他行為和環境屬性。
6. 所有資源身份驗證和授權都是動態的，並且在允許存取之前嚴格執行。
7. 企業收集盡可能多的有關資產、網路基礎設施和通訊當前狀態的信息，並利用這些資訊來改善其安全狀況。

本頁內容參考NIST SP 800–207 零信任架構

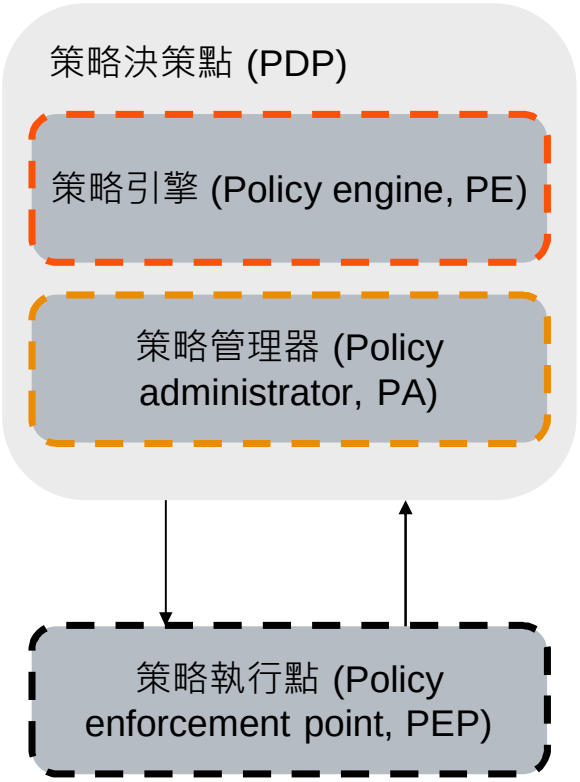
NIST SP 800-207 零信任架構

- 核心組件：即策略引擎，執行鑑別、決定授權及管理連線
- 支援組件：支援存取決策的資訊與系統



NIST SP 800-207 零信任架構的核心元件

存取權限是透過策略決策點 (PDP) 和相應的策略執行點 (PEP) 授予的。



策略引擎 (Policy engine, PE)
負責制定並記錄決策（批准或拒絕），決定最終授予給定主體對資源的**存取權限**。與策略管理器(PA)配對。

策略管理器 (Policy administrator, PA)
PA 在建立通訊路徑時與PEP 通訊，負責建立和/或關閉主體和資源之間的通訊路徑（透過向相關 PEP 發出指令）。
接收PE授予的決策：允許，PA 會設定 PEP 以允許會話啟動；不允許，PA 會向 PEP 發出信號以關閉連線。

策略執行點 (Policy enforcement point, PEP)
負責啟用、監控並最終終止主體與企業資源之間的連線。

本頁內容參考NIST SP 800–207 零信任架構

NIST SP 800-207 零信任架構的支援元件

持續診斷與緩解(Continuous diagnostics and mitigation, CDM)系統

- 該系統收集有關企業資產當前狀態的資訊並對配置和軟體元件應用更新。

產業合規體系

- 這可確保企業始終遵守其可能遵守的任何監管制度（例如 FISMA、醫療保健或金融業資訊安全要求）。

威脅情報源

- 提供來自內部或外部來源的信息，幫助策略引擎做出訪問決策。

網路和系統活動日誌

- 此企業系統聚合資產日誌、網路流量、資源存取操作和其他事件，提供有關企業資訊系統安全狀況的即時（或近實時）回饋。

NIST SP 800-207 零信任架構的支援元件(續)

資料存取策略

- 這些是有關存取企業資源的屬性、規則和策略。這組規則可以被編碼（透過管理介面）或由策略引擎動態產生。

企業公鑰基礎設施（Public key infrastructure, PKI）

- 該系統負責產生和記錄企業向資源、主體、服務和應用程式頒發的憑證。

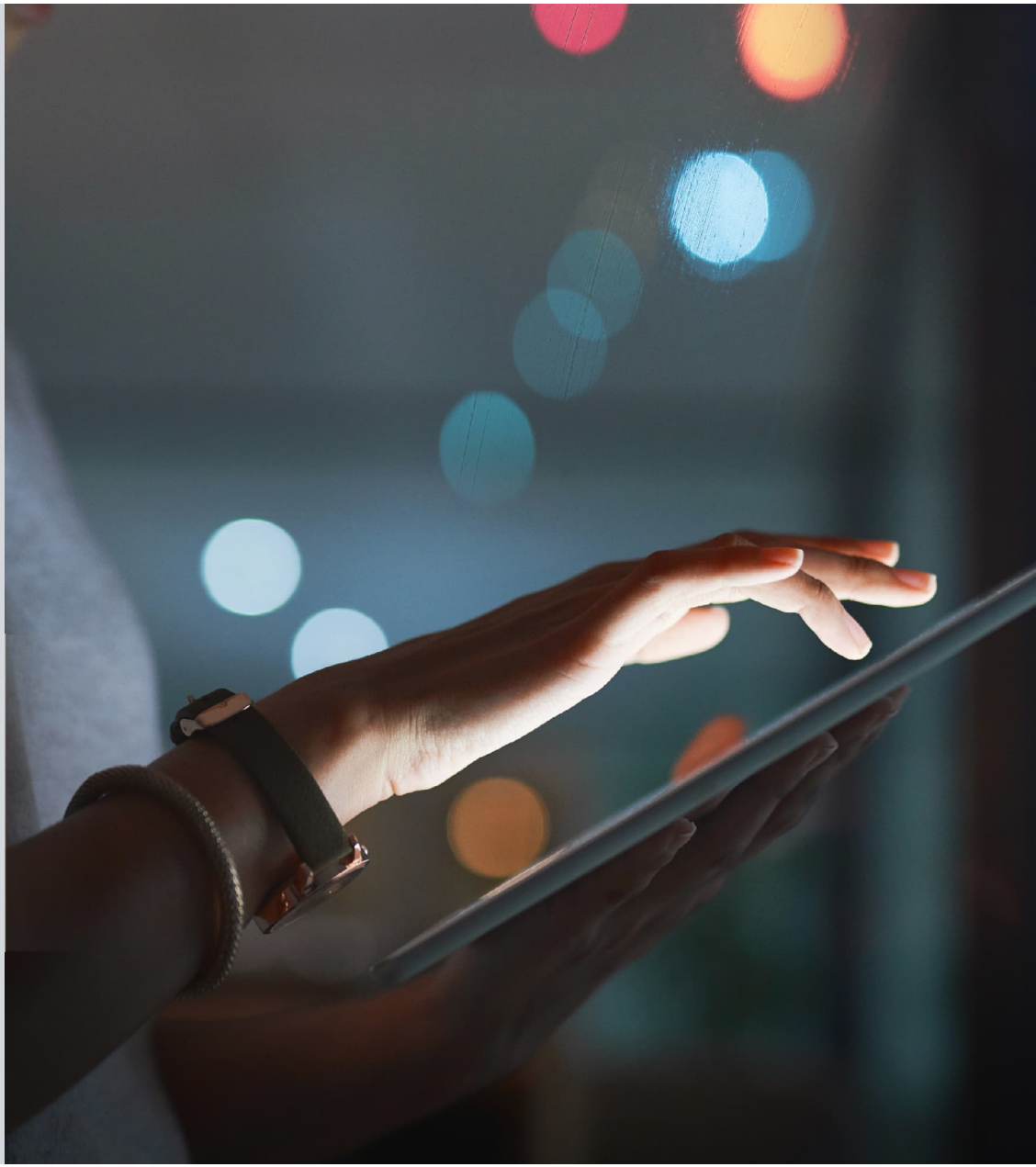
ID 管理系統

- 負責建立、儲存和管理企業使用者帳戶和身分記錄（例如，輕量級目錄存取協定（LDAP）伺服器）。

安全資訊和事件管理 (Security information and event management, SIEM) 系統

- 此系統會收集以安全為中心的資訊以供日後分析。然後，這些數據用於完善策略並警告可能針對企業資產的攻擊。

政府推動零信任架構的背景與目標



政府推動零信任架構的背景

推動零信任架構的核心目標是建立以身分為中心、動態持續的安全防護體系，不再依賴靜態網路邊界，實現對政府資料與服務的精確保護，同時支援數位政府創新服務的安全發展。日益複雜且不斷演變的網路安全威脅，主要為以下幾種：

1 網路威脅增長

APT攻擊、供應鏈攻擊日益增加，傳統邊界防護已難以有效防禦，需要更精細的存取控制機制。

2 數位轉型

政府機構正在進行數位轉型，使用更多的雲端服務、移動設備和IoT技術，而傳統網路邊界模糊，零信任架構能更有效保護分散式資源。

3 內部威脅

不僅僅是外部威脅，內部攻擊者或受感染的設備也能輕易在網路中橫向移動。

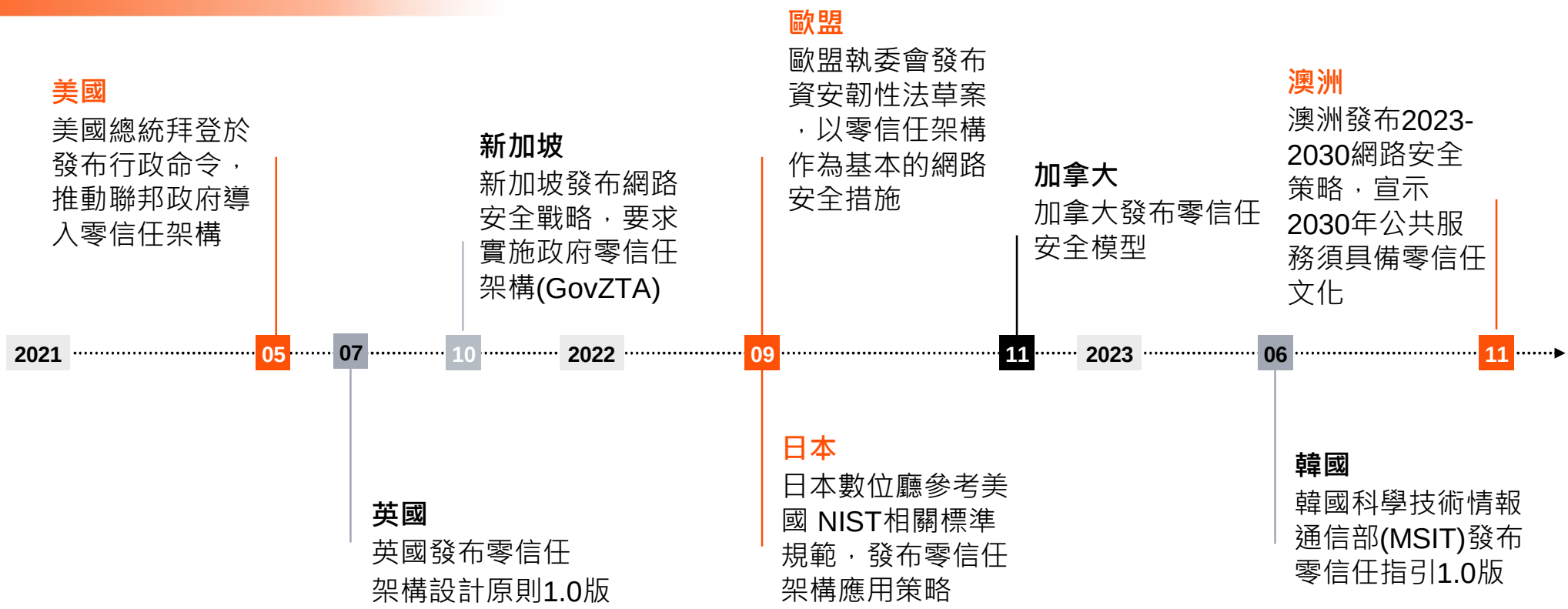
4 合規要求

資安法規日趨嚴格，零信任架構能協助政府機關實現更精細的權限控制。

本頁內容參考政府機關導入零信任架構參考指引-身分與設備鑑別(V1)

政府推動零信任架構的背景

各國政府推動零信任策略



本頁內容參考「政府零信任架構規劃與經驗分享」

政府推動零信任架構的目標

增強安全防護

最大限度地減少信任，僅授予實際需要的訪問權限，以減低資源暴露面和攻擊風險。

實現持續驗證和授權

對每一個用戶和設備進行連續性驗證和授權管理，不再僅依賴初次登入時的認證。

防止橫向移動

在網路中採用微分段，使任何潛在的威脅行為被侷限在有限的範圍內。

推動技術創新

鼓勵公共機構探索並實施新技術和方法來提高安全性，支持整體的技術進步。

提高彈性和應變能力

架構使政府系統能夠快速檢測和回應異常行為，加強機構的網路彈性。

兼容性和政策合規

確保零信任架構能與現有的網路安全政策、風險管理框架相兼容，並滿足相關法律和合規要求。

政府推動零信任架構的策略

我國政府推動零信任架構的做法

03

提供實施資源與引導

實施建議
與支援資源

- 《政府零信任架構說明 V2.1》：提供架構設計與部署原則 。
- 《政府機關身分與設備鑑別參考指引 V1 / V1.2》：提供身分與設備鑑別的實作規範 。
- 產業合作與認證：多家廠商推出通過國家資通安全研究院驗證的身份與設備解決方案 。
- 金管會亦為金融機構提供「金融業導入零信任架構參考指引」，鼓勵以高風險、低衝擊場域優先，分階段部署零信任架構 。

政府推動零信任架構的策略

我國政府推動零信任架構的做法

01
政策與法規支持

資訊安全政策制訂

- 第六期《國家資通安全發展方案（110年-113年）》 將「善用智慧前瞻科技、主動抵禦潛在威脅」列為資安策略之一，以推動政府機關導入零信任網路架構，優先A級機關逐步導入三大核心機制：身分鑑別、設備鑑別與信任推斷 。

02
實施作法

實施階段與優先範圍

- 2022年8月起：遴選A級公務機關逐步導入零信任，推行身份驗證與設備管理，並透過政府公告與廠商驗證平台支援 。
- 2024年起：重點轉向第三階段「信任推斷」階段，發展具行為分析與動態授權能力的機制 。

政府推動零信任架構的策略

政府零信任架構身分與設備鑑別功能符合性驗證通過名單

項次	廠商名稱	產品名稱	通過時間	檢核表版本	備註
1.	全景軟體股份有限公司	ZTA 零信任網路設備鑑別系統	112.09	V1.0	● 通過全景軟體股份有限公司團隊執行之滲透測試，無中高風險議題 ● 通過 Fortify 源碼掃描，無中高風險議題
2.	來毅數位科技股份有限公司	Keypasco 零信任設備鑑別系統	113.03	V1.2	● 通過 ZAP 網頁應用程式掃描，無中高風險議題 ● 通過 SonarQube 源碼掃描，無風險議題
3.	中華電信股份有限公司	中華電信零信任系統 xTrust	113.10	V1.2	● 通過中華電信股份有限公司團隊執行之滲透測試，無中高風險議題 ● 通過 Nessus Professional Scanner 系統弱點掃描與 Web Vulnerability Scanner 網頁弱點掃描，無中高風險議題 ● 通過 Fortify 源碼掃描，無中高風險議題 ● ZTDA-7.2 有註記事項，詳見檢測結果報告

本頁內容參考「政府零信任架構身分與設備鑑別功能符合性驗證通過廠商清單」

政府推動零信任架構的策略

政府零信任架構身分與設備鑑別功能符合性驗證通過名單(續)

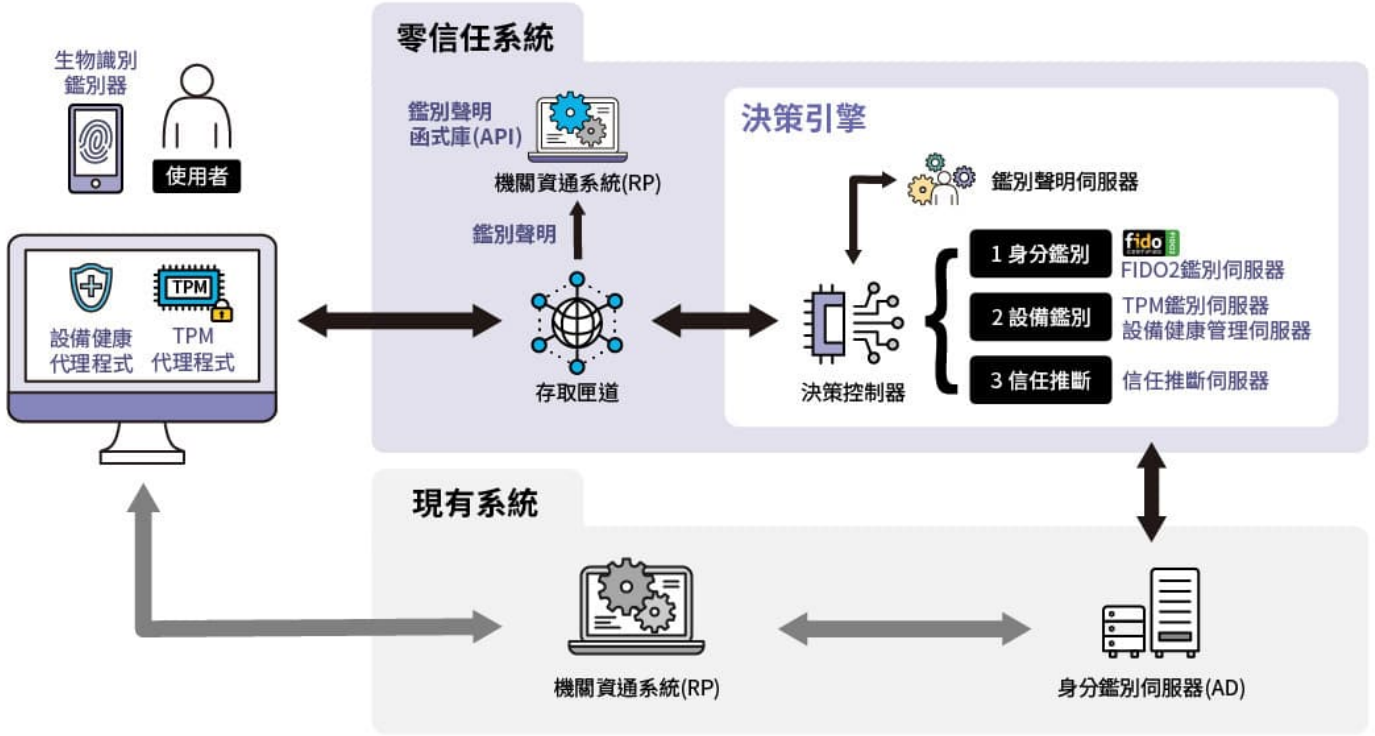
4.	台灣微軟股份有限公司	微軟零信任網路設備鑑別系統	114.02	V1.2	● 通過 IOActive 團隊執行之滲透測試，無中高風險議題 ● ZTDA-7.2 有註記事項，詳見檢測結果報告
5.	臺灣網路認證股份有限公司	TWID 零信任架構之多元身分鑑別及設備鑑別系統	114.07	V1.2	● 通過臺灣網路認證股份有限公司團隊執行之滲透測試，無中高風險議題 ● 通過 Checkmarx 源碼掃描，無風險議題
6.	偉康科技股份有限公司	OETH One 零信任解決方案	114.07	V1.2	● 通過偉康科技股份有限公司團隊執行之滲透測試，無風險議題 ● 通過 Fortify 弱點掃描，無風險議題

2

政府零信任架構說明

政府零信任架構系統

- 參考NIST SP 800-207，我國採取資源門戶之部署方式(Resource Portal-Based Deployment)，優先推動A級公務機關導入零信任架構。
- 當員工使用電腦存取機關資通系統時，連線會先經過存取閘道。員工需用實體金鑰鑑別身份，電腦則需代理程式和公私鑰鑑別。最後，決策引擎依據身份、設備、來源IP、登入時間和設備狀態等資料，決定是否允許存取。

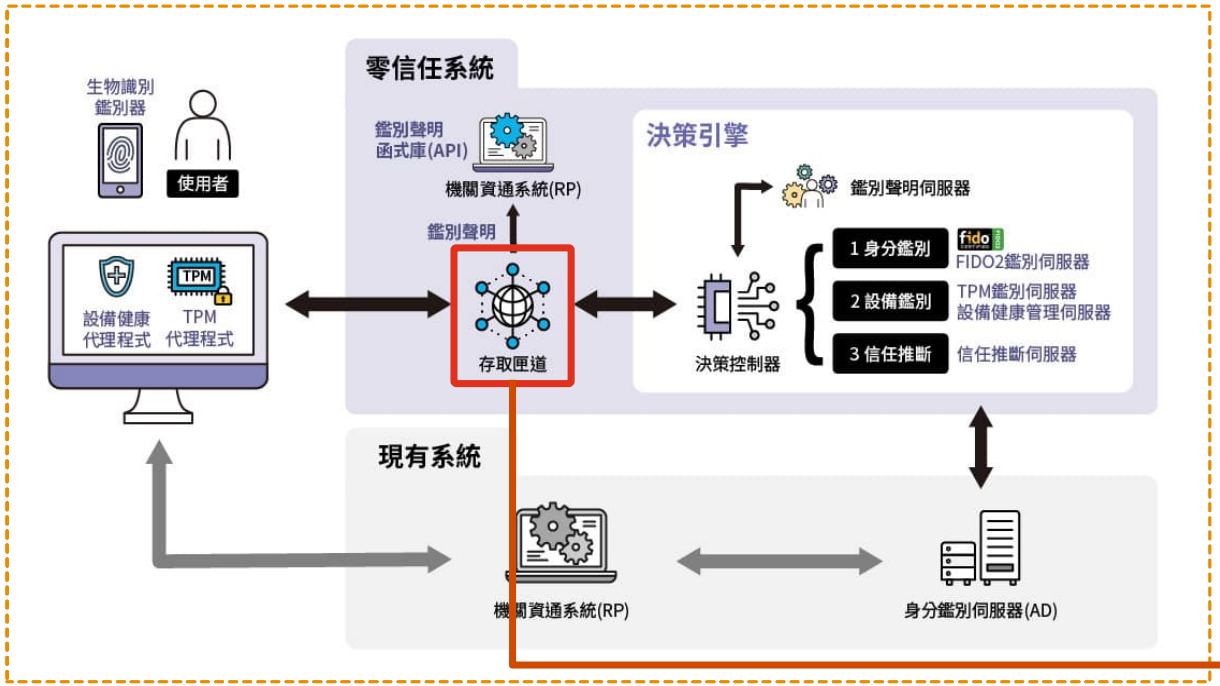


本頁內容參考國家資通安全研究院「政府零信任架構說明」及 https://moda.gov.tw/press/multimedia/blog/9773

政府零信任架構之資源門戶部署方式

存取閘道(Access Gateway)

存取閘道為機關資通系統之存取門戶，其依據決策引擎之存取決定，負責建立、監控及終止使用者與機關資通系統間之網路連線。



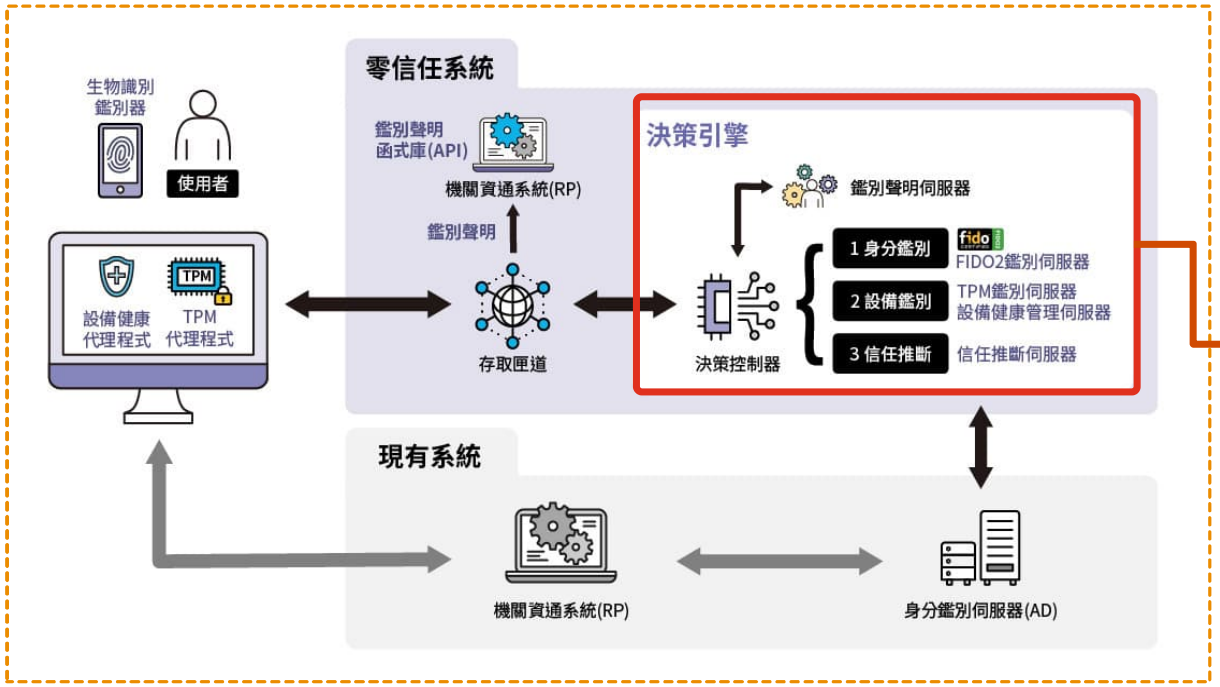
- 不論來自內部或外部網路之存取，必須且唯一經由存取閘道
- 為唯一公開存取之組件，存取全程必須隱藏內部網路路徑(如利用反向代理技術)
- 必須實施負載平衡機制以避免效率瓶頸
- 必須實施可有效防止阻斷服務攻擊之機制

本頁內容參考國家資通安全研究院「政府零信任架構說明」

政府零信任架構之決策引擎

決策引擎(Decision Engine)

負責接收存取請求、決定允許與否及授予存取憑據，其中包含決策控制器、3大核心機制，以及鑑別聲明伺服器。



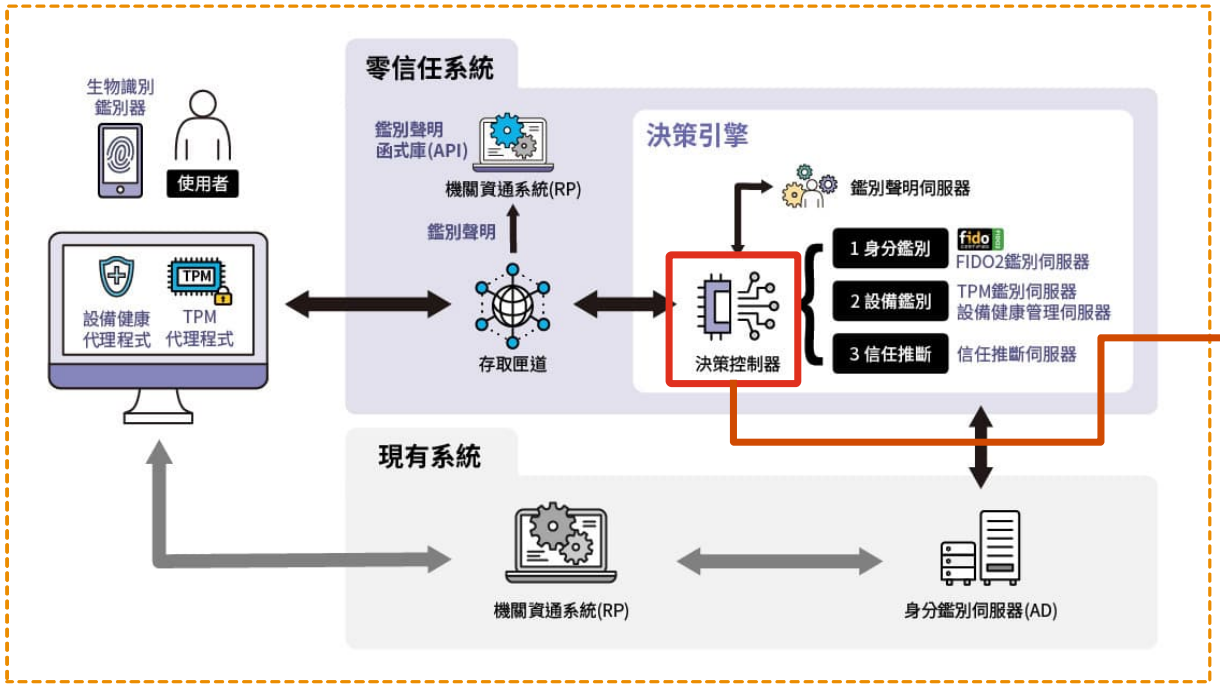
- **決策控制器**：負責控制存取決策之流程，包含設定存取允許條件、接收存取請求、驅動3大核心機制及授予鑑別聲明。
- **3大核心機制**：由身分鑑別、設備鑑別及信任推斷進行驗證與評估，並將結果回饋給決策控制器。
- **鑑別聲明伺服器**：針對獲得允許之存取，發行鑑別聲明，做為存取Resource Portal, RP之憑據。

本頁內容參考國家資通安全研究院「政府零信任架構說明」

政府零信任架構之決策控制器

決策控制器

負責存取條件管理、存取請求介面，以及決策流程控制。



- **存取條件管理**：可設定存取允許之條件，做為存取允許或拒絕之依據。
- **存取請求介面**：建置3大核心機制所需之前端系統，包含身分註冊網頁、登入網頁、設備鑑別代理程式驅動模組、情境資料擷取等。
- **決策流程控制**：
  - 接收存取請求
  - 與現有系統協作
  - 驅動3大核心機制
  - 確認是否滿足存取允許條件
  - 驅動鑑別聲明產生
  - 進行Resource Portal, RP存取導向

本頁內容參考國家資通安全研究院「政府零信任架構說明」

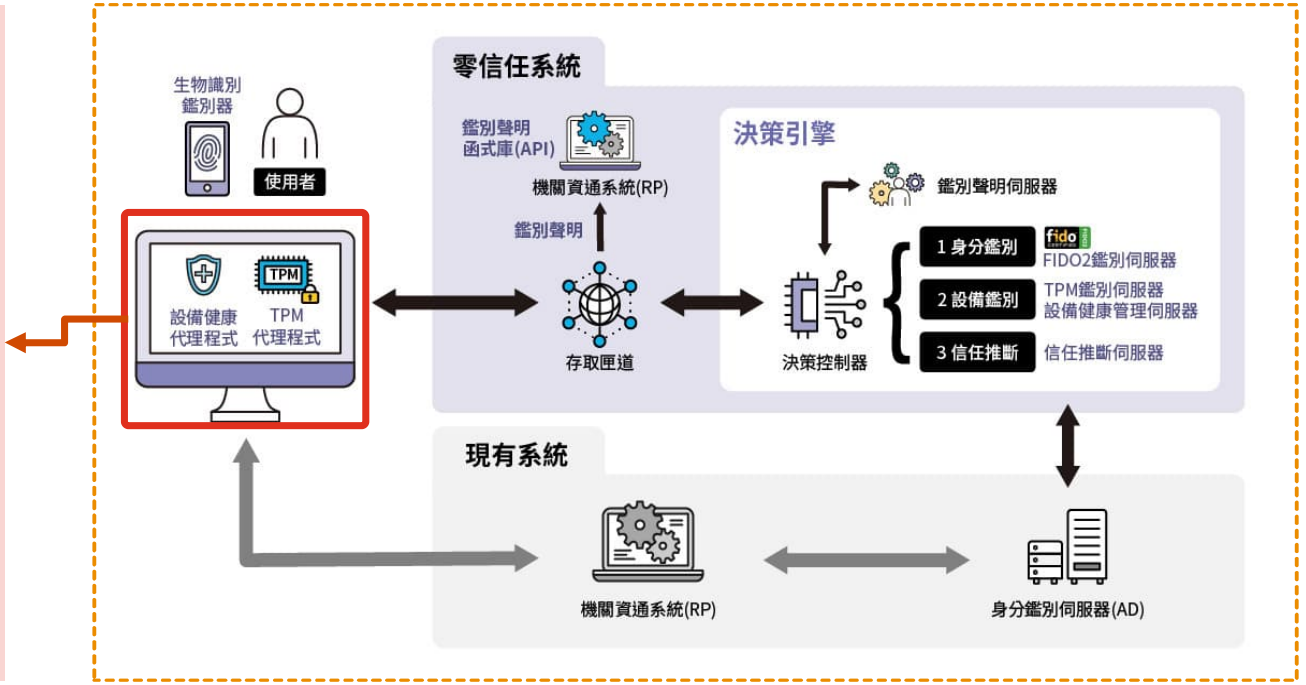
政府零信任架構之設備TPM及設備健康代理程式

- **設備TPM代理程式**

  Client端設備部署TPM代理程式，負責TPM之輸入與輸出。

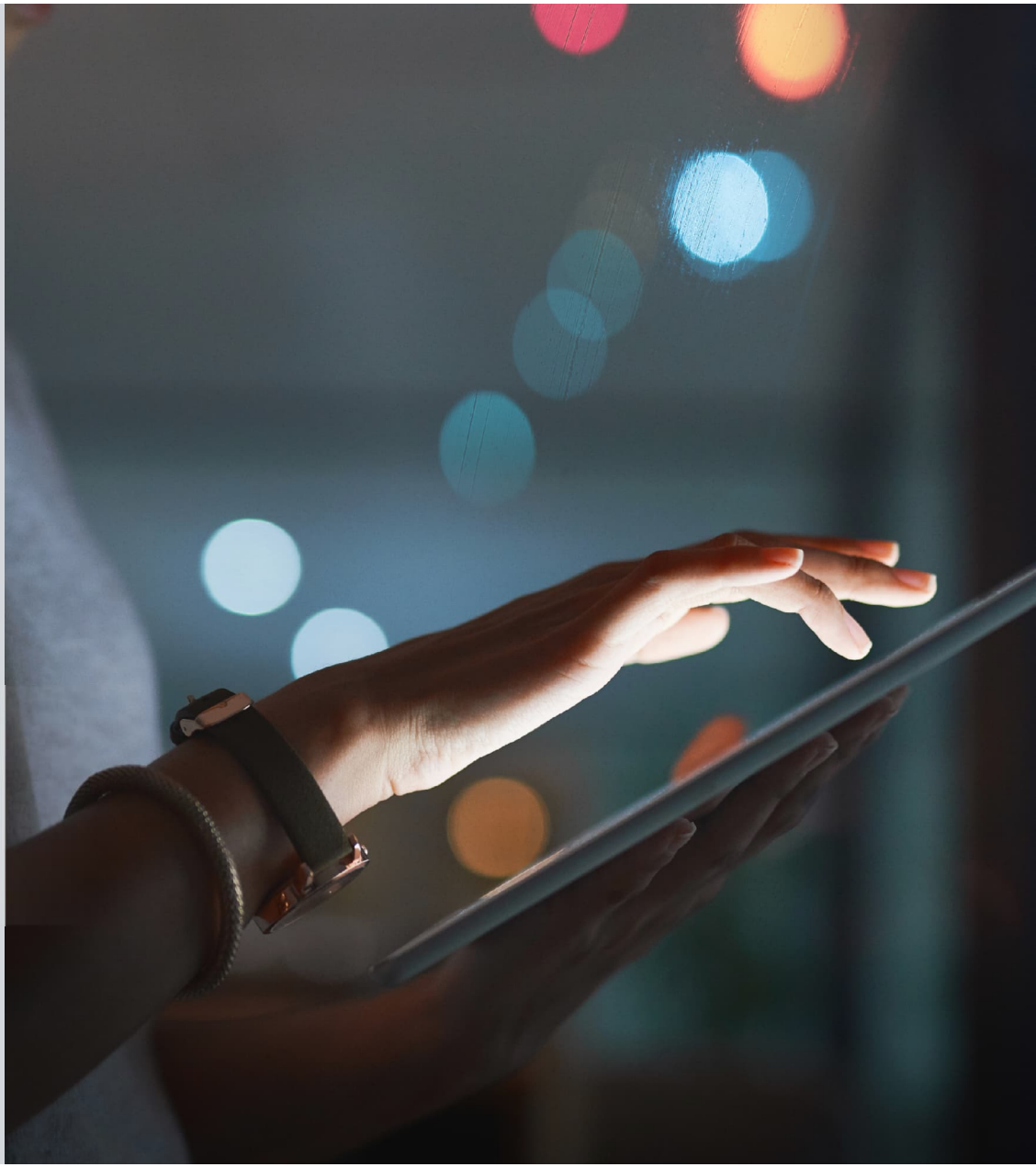
- **設備健康代理程式**

  Client端設備部署設備健康代理程式，提供作業系統與病毒保護等設備健康資訊，並進行必要之設備健康修補。



本頁內容參考國家資通安全研究院「政府零信任架構說明」

身分鑑別機制



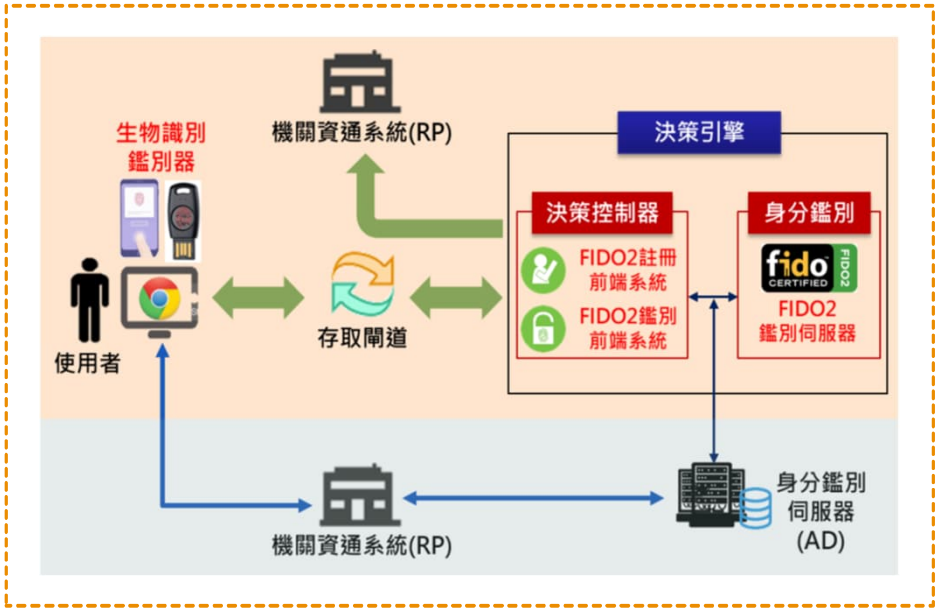
身分鑑別機制

身分鑑別

以實體安全金鑰或手機APP進行無密碼多因子身分鑑別(如FIDO2)，並可與現有身分鑑別伺服器(如AD)共存與同步。

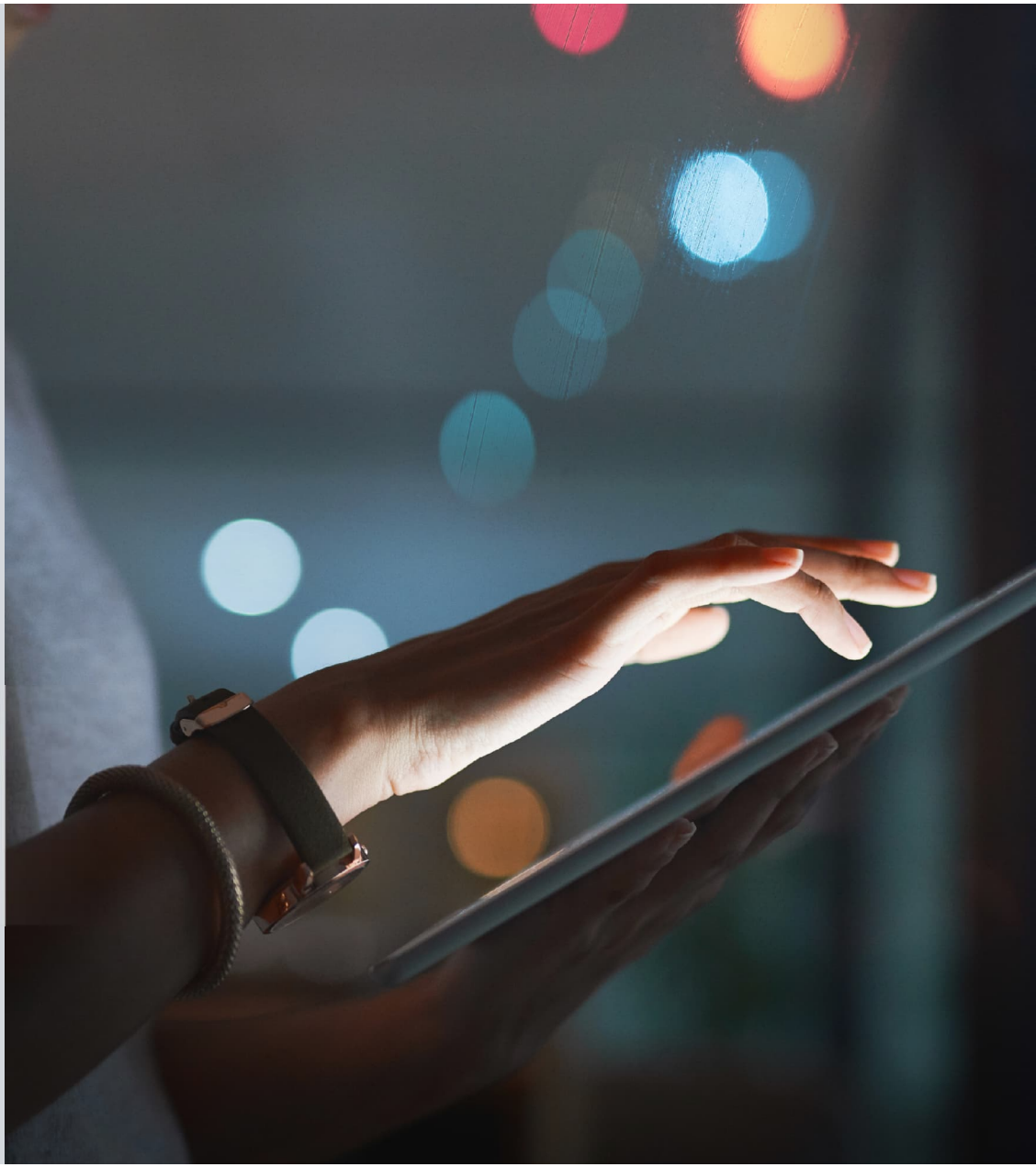
建置流程

1. 建置FIDO2鑑別伺服器，並與現有身分鑑別伺服器(如AD)維持帳號狀態一致
2. 建置FIDO2註冊前端系統與FIDO2鑑別前端系統，提供使用者身分註冊與登入網頁
3. 使用者以生物識別鑑別器(實體安全金鑰或手機APP)進行身分鑑別



本頁內容參考國家資通安全研究院「政府零信任架構說明」

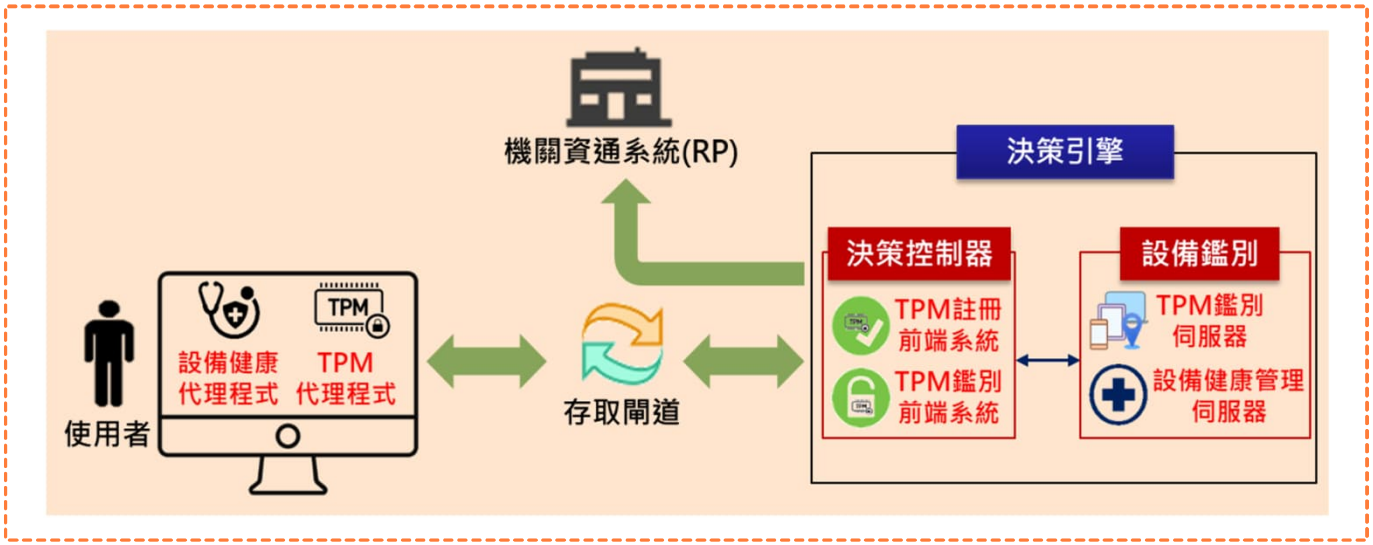
設備鑑別機制



設備鑑別機制

設備鑑別

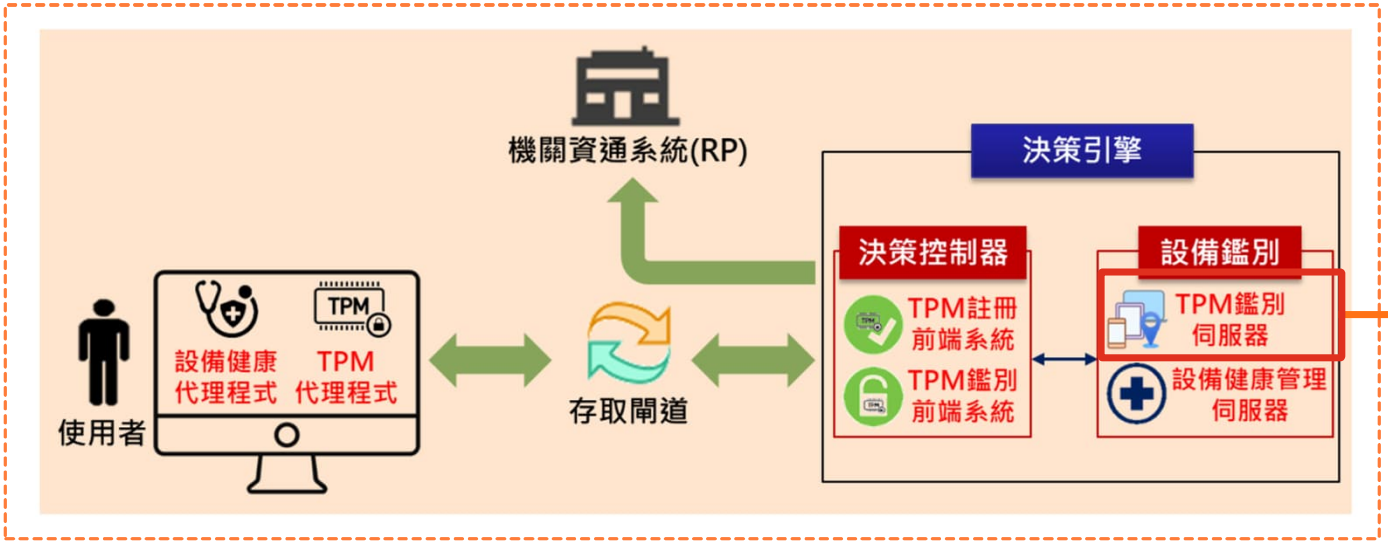
可確認使用者設備為受機關管理之設備，且在可接受之資安狀態，可因應遠距與居家辦公之資安需求。



1. 存取控管可透過設備鑑別(金鑰驗證)，或其他特徵(如設備唯一識別碼)確認設備的合法性，並應符合採用設備所屬在信任清單當中為可信任設備之依據，以非對稱金鑰執行解密驗簽完成設備鑑別
2. 由決策控制器整合設備鑑別結果資訊進行決策控制，如要求須通過身分鑑別與設備鑑別才能存取某資通系統，並確認存取資源遵循最小授權原則(如僅授權存取特定目標資通系統)

本頁內容參考國家資通安全研究院「政府零信任架構說明」及「政府零信任架構身分鑑別與設備鑑別機制導入建議(V1.0)」

設備TPM鑑別

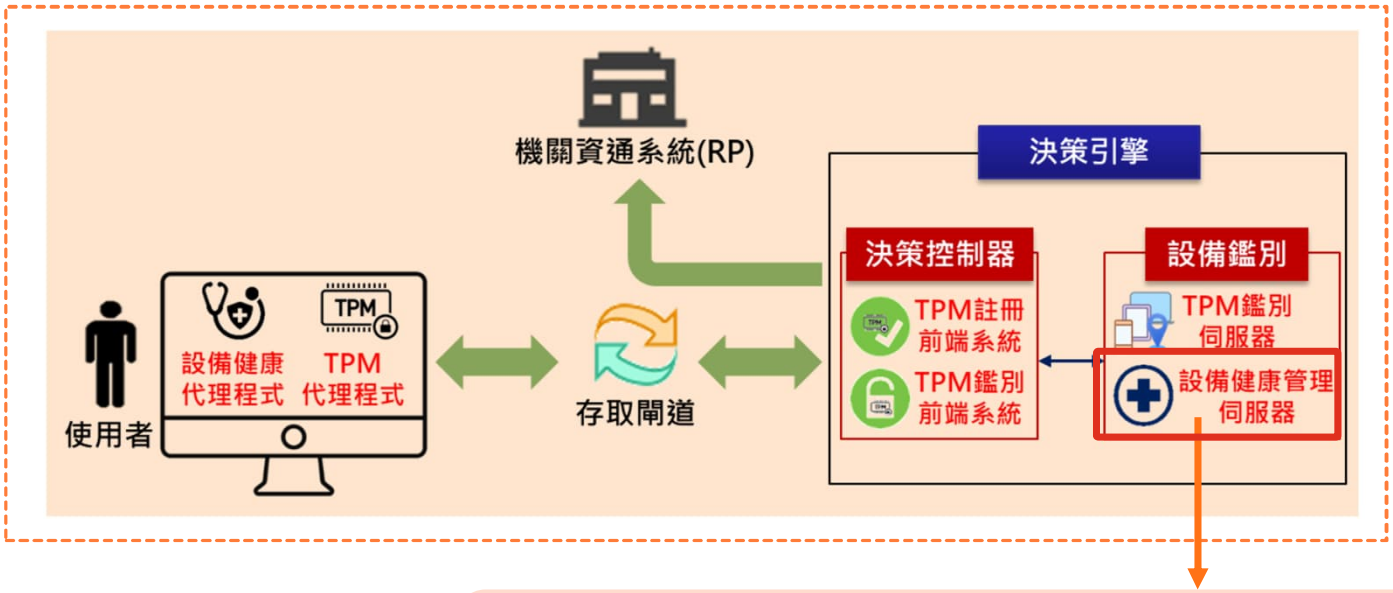


設備TPM鑑別

- 使用者設備須具備信任平臺模組(TPM)
- 執行基於TPM私鑰之鑑別協議，以驗證使用者設備是受管理設備
  - Client：部署TPM代理程式，負責TPM之輸入與輸出
  - Server：建置TPM鑑別伺服器，負責TPM鑑別協議之驗證，並建置TPM註冊前端系統與TPM鑑別前端系統，負責驅動TPM代理程式進行設備之TPM註冊與鑑別作業

本頁內容參考國家資通安全研究院「政府零信任架構說明」

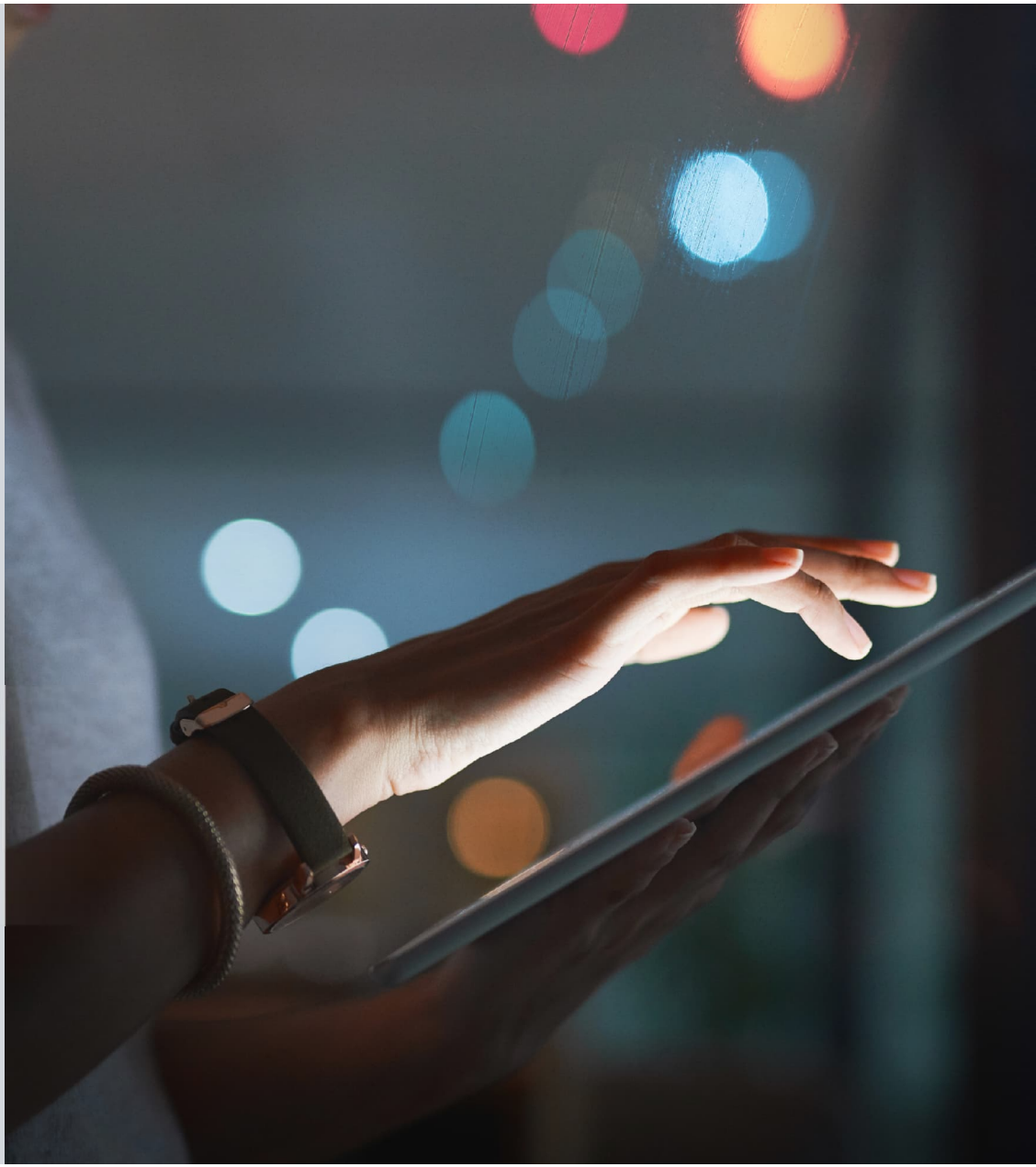
設備健康管理



設備健康管理

- 使用者設備部署設備健康代理程式，提供作業系統與病毒保護等設備健康資訊，並進行必要之設備健康修補
- 建置設備健康管理伺服器，隨時匯整使用者設備健康資訊，監控設備健康狀態，並分析設備健康信任等級，以提供存取決策依據

信任推斷



信任推斷

信任推斷模型

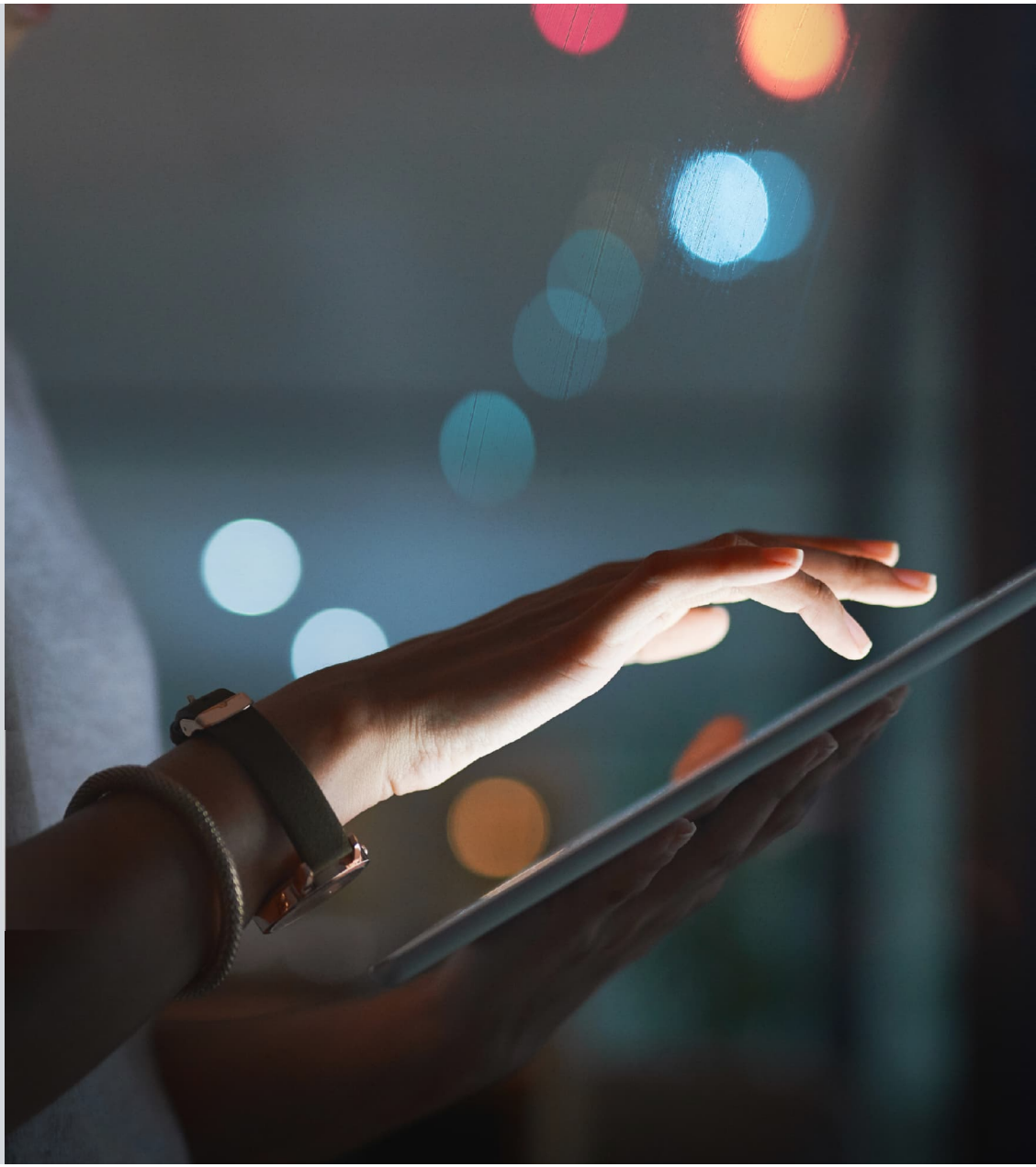
- 決定存取權限，可隨時依使用者行為與設備狀態，偵測異常存取
- 依使用情境計算每次存取之信任分數作為存取判斷依據

本頁內容參考國家資通安全研究院「政府零信任架構身分鑑別與設備鑑別機制導入建議(V1.0)」

3

導入實務與挑戰

導入零信任架構的步驟與流程

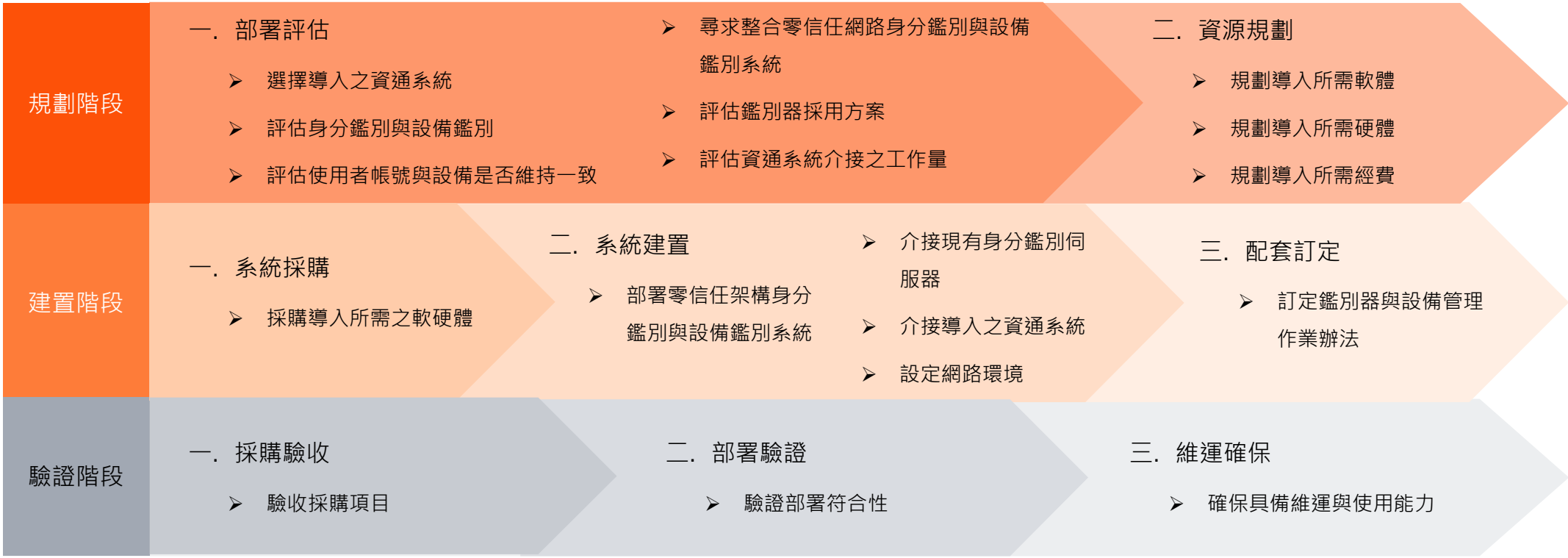


PwC

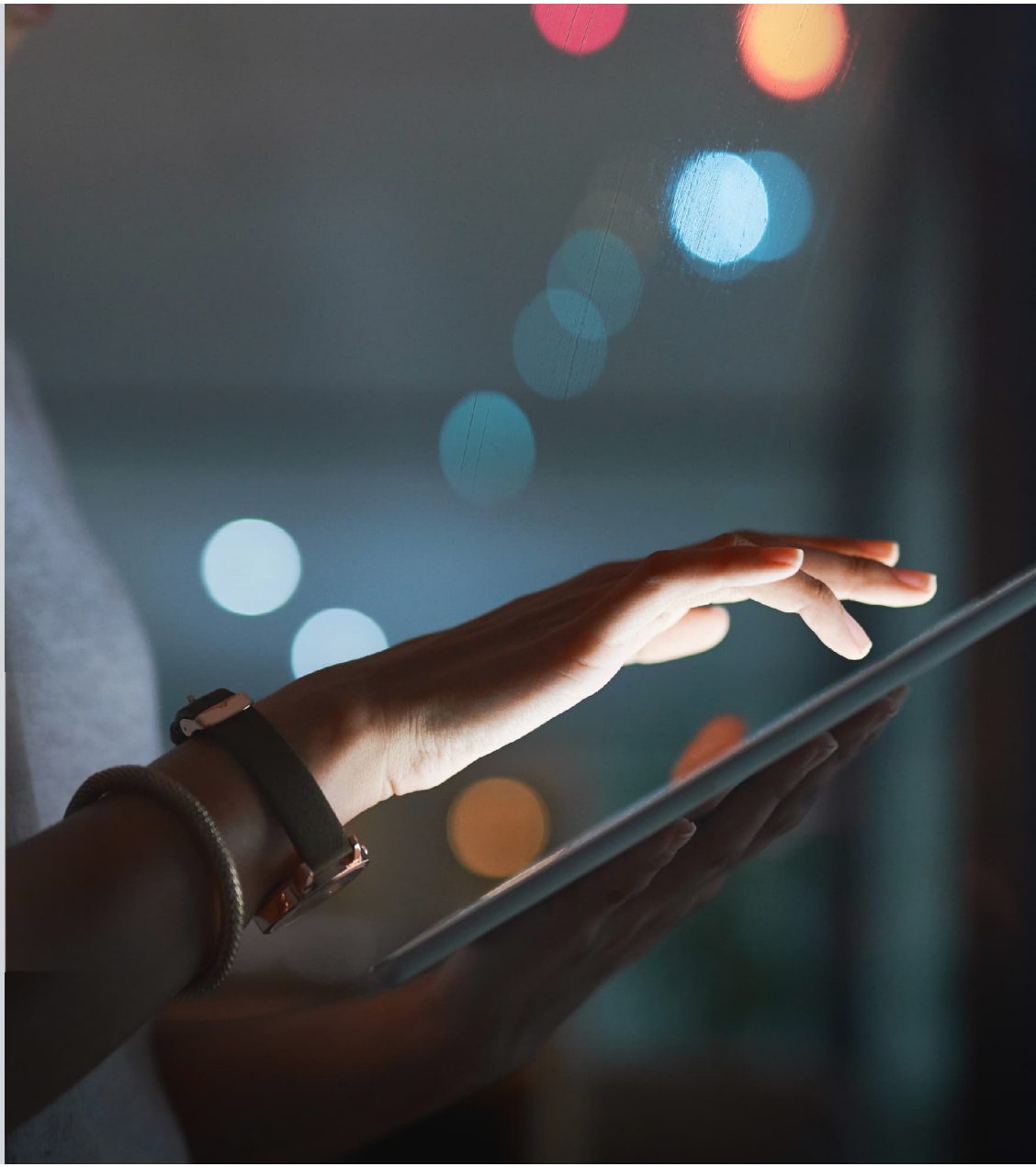
導入零信任架構的步驟與流程

參照「政府零信任架構身分鑑別與設備鑑別機制導入建議(V1.0)」整理出零信任架構導入階段之要點及細項：

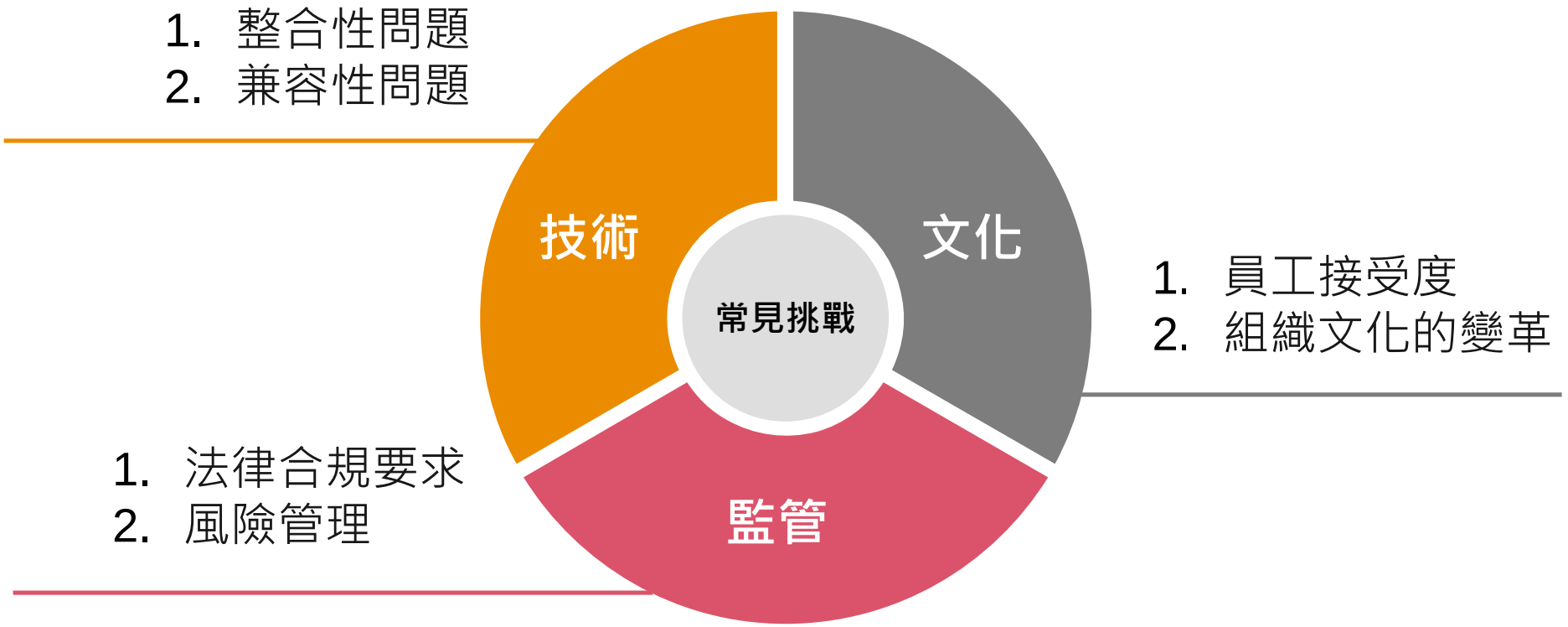
- 以介接具個資或高度敏感資料之RP系統為原則
- 與現有系統同時混合運作，逐步導入決策引擎之身分鑑別、設備鑑別及信任推斷3大核心機制



導入零信任架構時
常見的挑戰

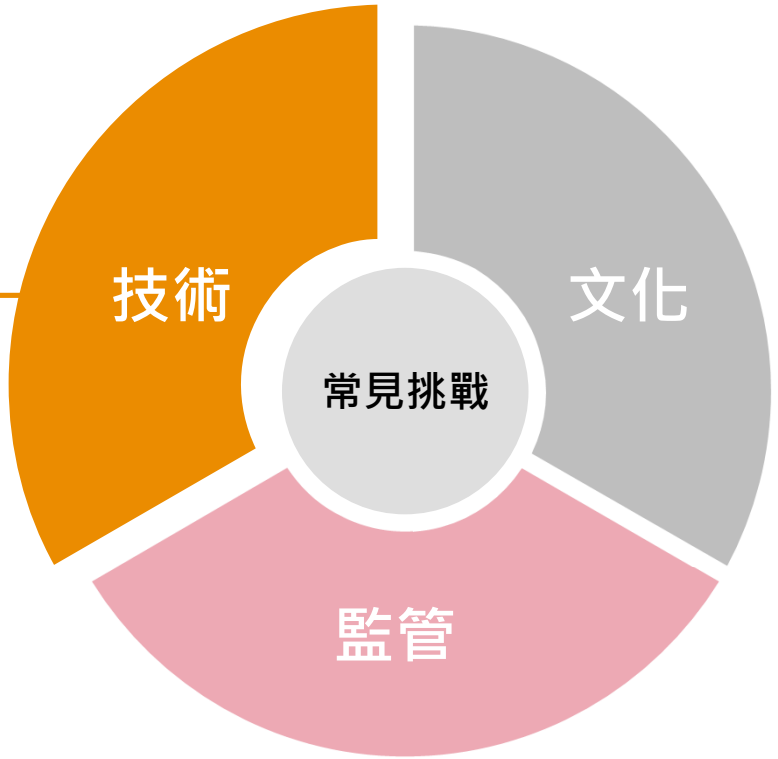


常見挑戰



技術層面

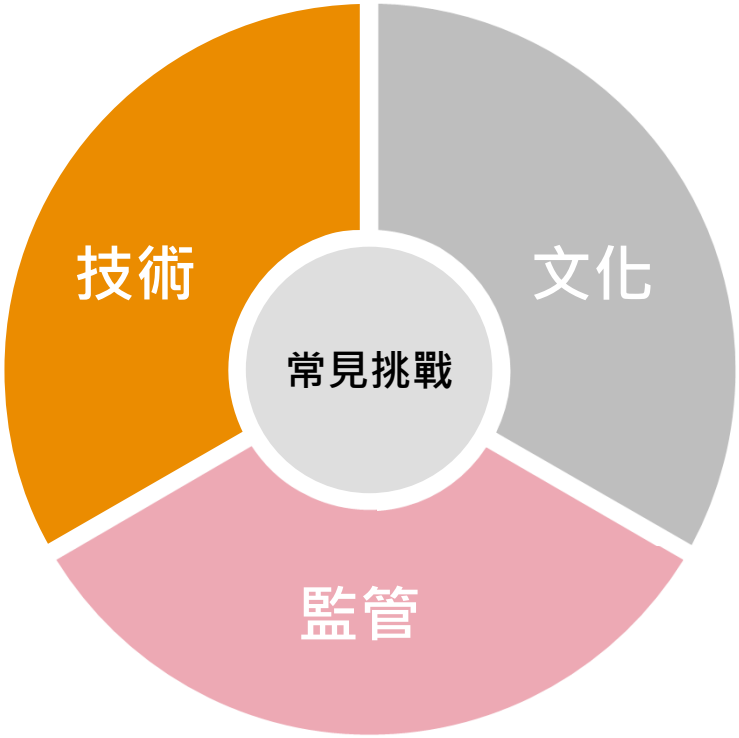
1. 整合性問題
2. 兼容性問題



政府機關導入面臨的挑戰1

整合性方面

- 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

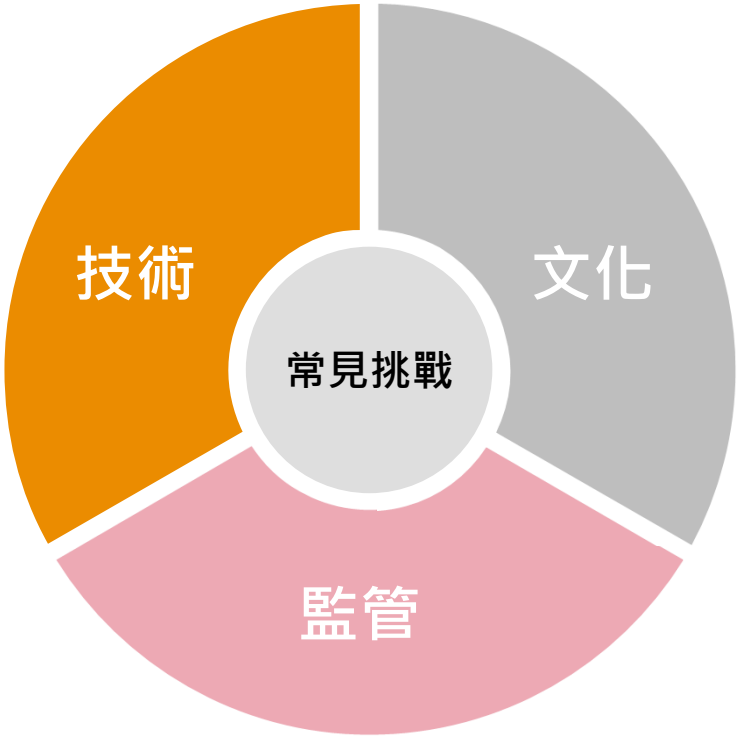


本頁內容參考國家資通安全研究院「政府零信任架構規劃與經驗分享」

政府機關導入面臨的挑戰2

兼容性方面

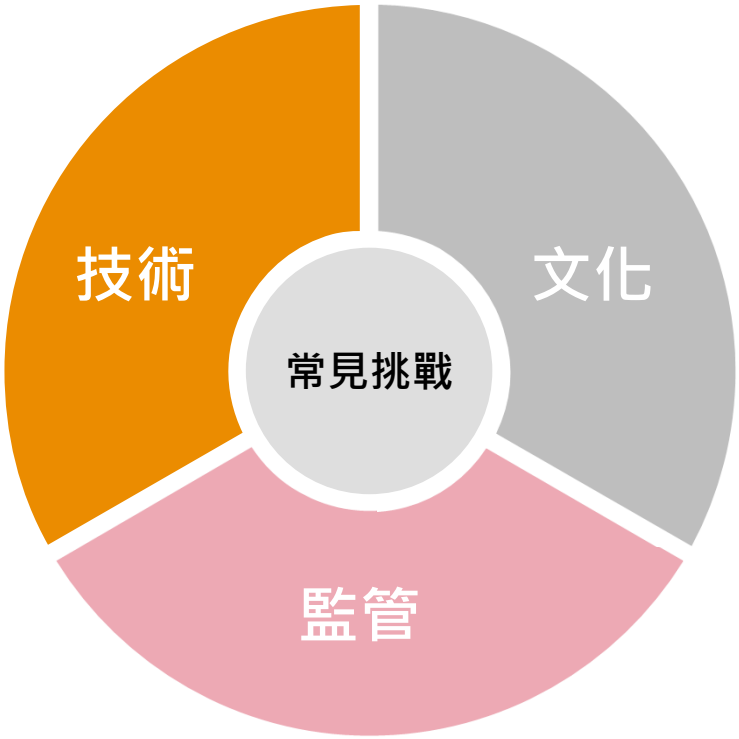
- 零信任產品後續導入相容性問題
  - 零信任架構之3大核心機制(身分鑑別、設備別、信任推斷)未必由同一家廠商提供，後續導入必須考量解決相容性與整合問題。



本頁內容參考國家資通安全研究院「政府零信任架構規劃與經驗分享」

整合性問題概述

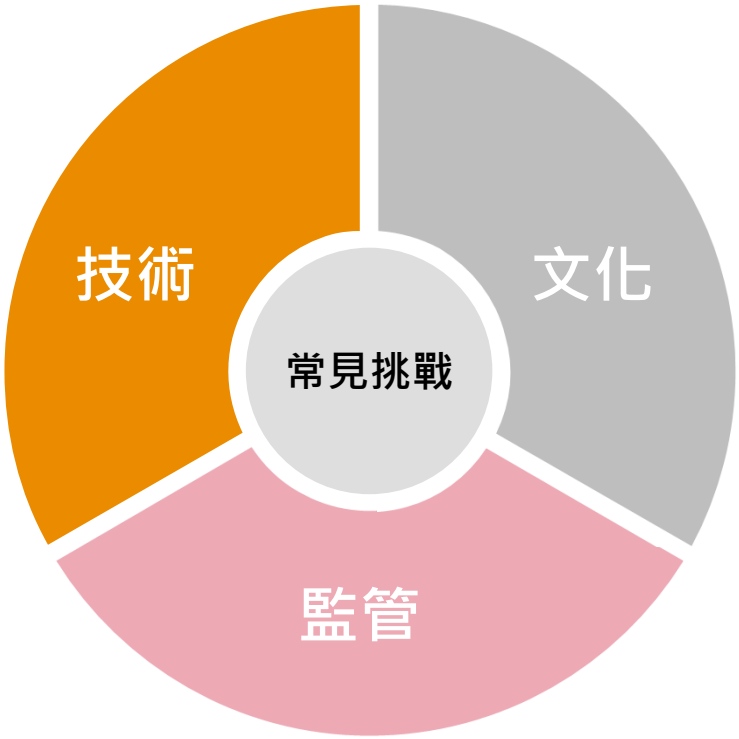
- 多系統整合困難
  - 零信任架構引入需要與現有多樣化系統和應用整合，這可能在系統兼容性和配置中出現挑戰。
  - 系統進行大規模整合時會面臨責任界線不清晰，缺乏統一標準等問題。
- 資料一致性問題
  - 保證整合過程中不丟失資料並維持一致性是最大挑戰，特別是在不同系統之間同步資料的場合。



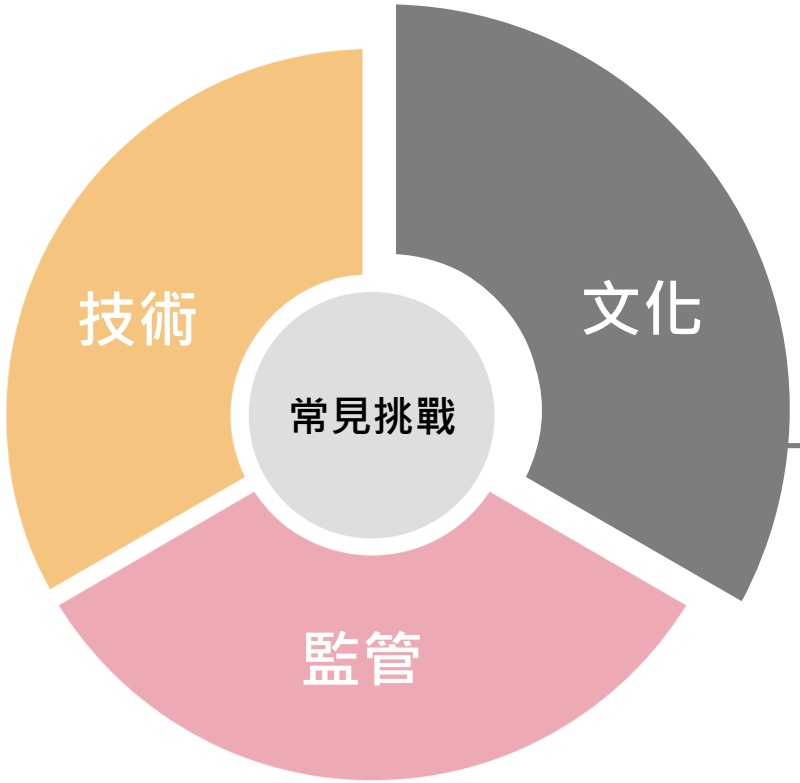
兼容性問題概述

設備與系統兼容

- 隨著新架構的嵌入，需要確保現有硬體能夠支持零信任功能，這可能引發兼容性問題。
- 不當更新或升級可能導致系統不協調，進而引發穩定性問題。



文化層面

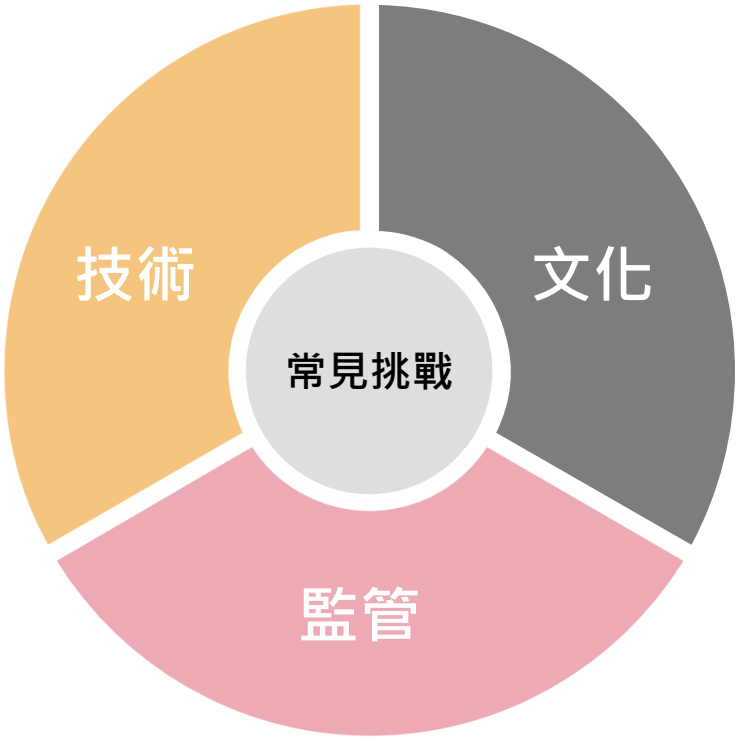


1. 員工接受度
2. 組織文化的變革

政府機關導入面臨的挑戰3

組織文化方面

- 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。

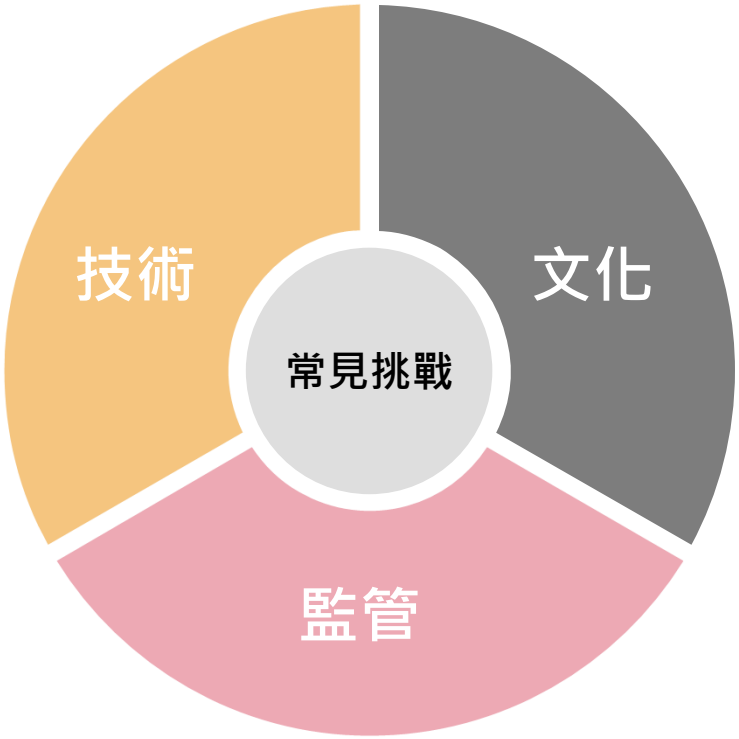


本頁內容參考國家資通安全研究院「政府零信任架構規劃與經驗分享」

員工接受度提升策劃

員工接受度概述

- 文化抗拒
  - 對於新的管理系統和程序可能存在自然的抗拒，尤其是增加了工作複雜性或改變了日常流程。
- 缺乏專業知識
  - 員工可能因缺乏對零信任的認識而影響擁抱新系統的積極性。

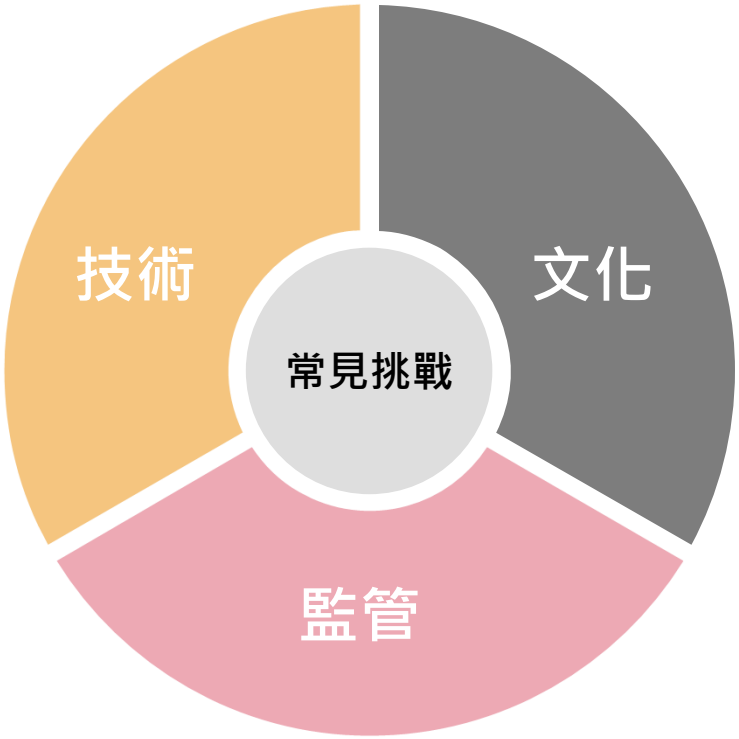


組織文化的變革挑戰

變革導向的挑戰

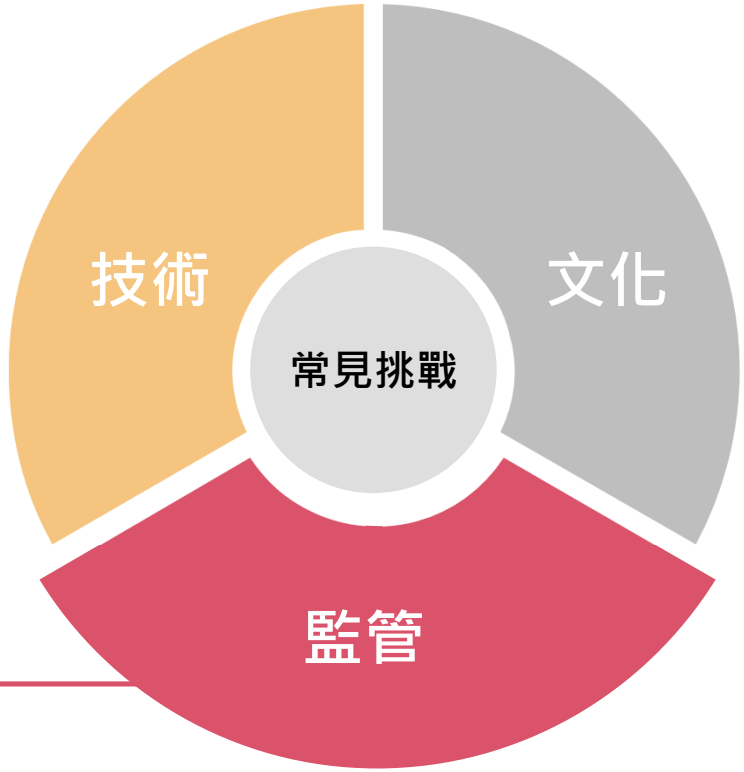
- 總體文化阻力
  - 長期累積的企業文化特質可能拒斥快速的技術轉型，尤其是對責任和權限的變更。

- 變革焦慮
  - 大範圍技術改變可能引起員工焦慮，擔心其未來職業發展和所需技能需求改變。



監管層面

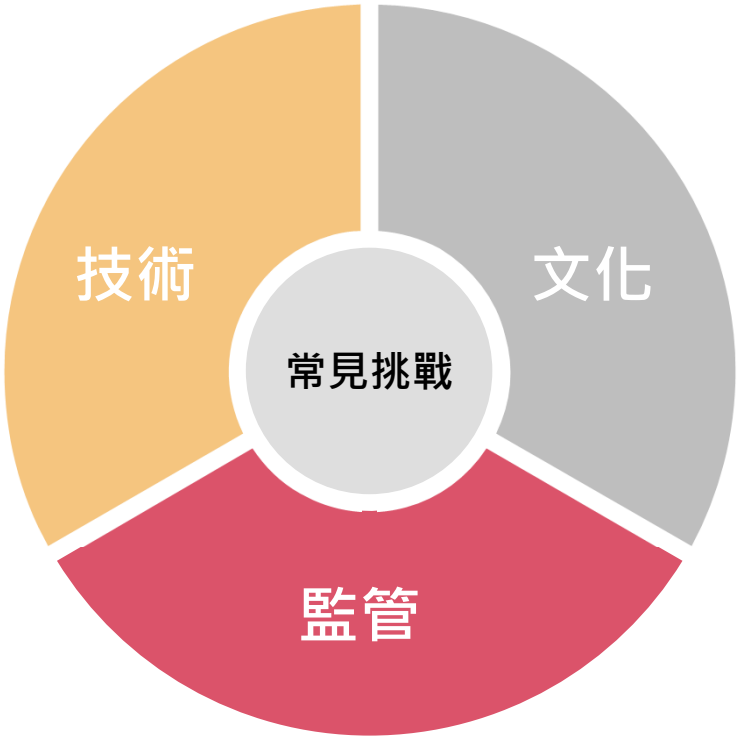
1. 法律合規要求
2. 風險管理



政府機關導入面臨的挑戰4

風險管理方面

- 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。

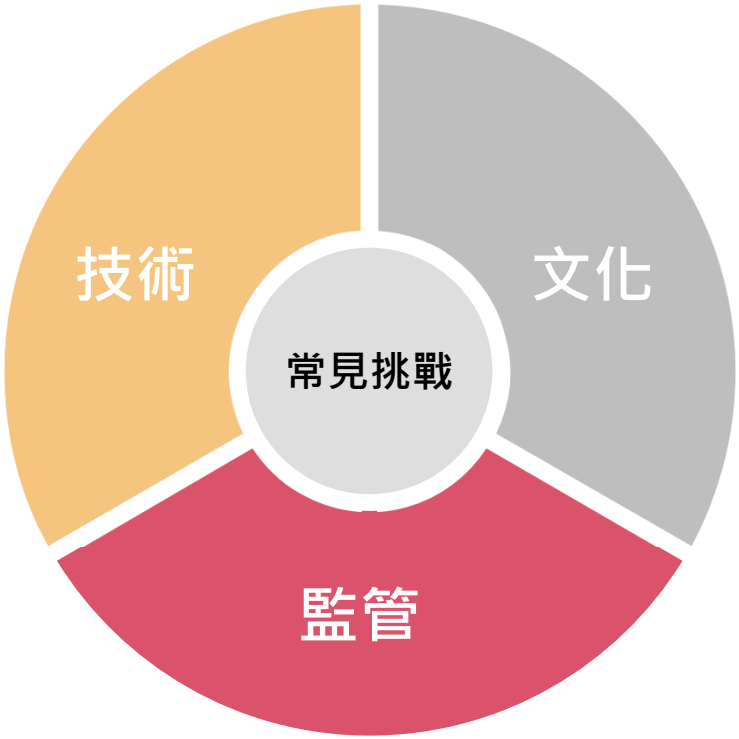


本頁內容參考國家資通安全研究院「政府零信任架構規劃與經驗分享」

監管挑戰與合規建議

法律合規挑戰概述

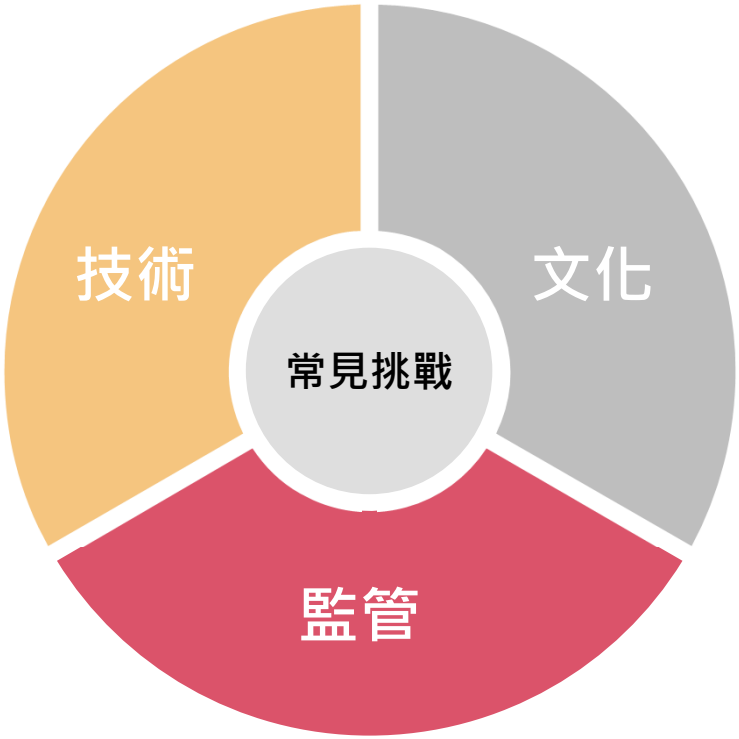
- 法規複雜性
  - 法律和行業監管要求經常變動且不一致，導致合規管理的挑戰。
- 合規風險
  - 輕視或未能及時遵從監管要求可能導致罰款、法律責任以及聲譽受損。



風險管理挑戰

風險管理概述

- 風險來源
  - 可能源於內部控制缺失、法令法規未即時更新以至於管理不當。
- 潛在影響
  - 違規行為可能導致財政損失、法律後果以及公眾信任度的下降。



4

導入零信任架構對ISO 27001之影響

零信任架構如何滿足ISO 27001標準

ISO 27001 標準要求	零信任架構對應措施
A.8.22 網路區隔	**微分段技術**
A.8.24 密碼技術使用 **A.5.15 存取控制** **A.8.3 資訊存取限制** **A.8.5 安全鑑別**	**基於身份的最小特權訪問管理** 使用多因素驗證（MFA）來管理員工訪問，降低內部威脅。
A.8.16 監視活動 **A.8.20 網路安全**	**網路流量監控與檢測** 網路流量監控工具能持續分析和監測網路流量，保障通信的安全及預防潛在威脅。

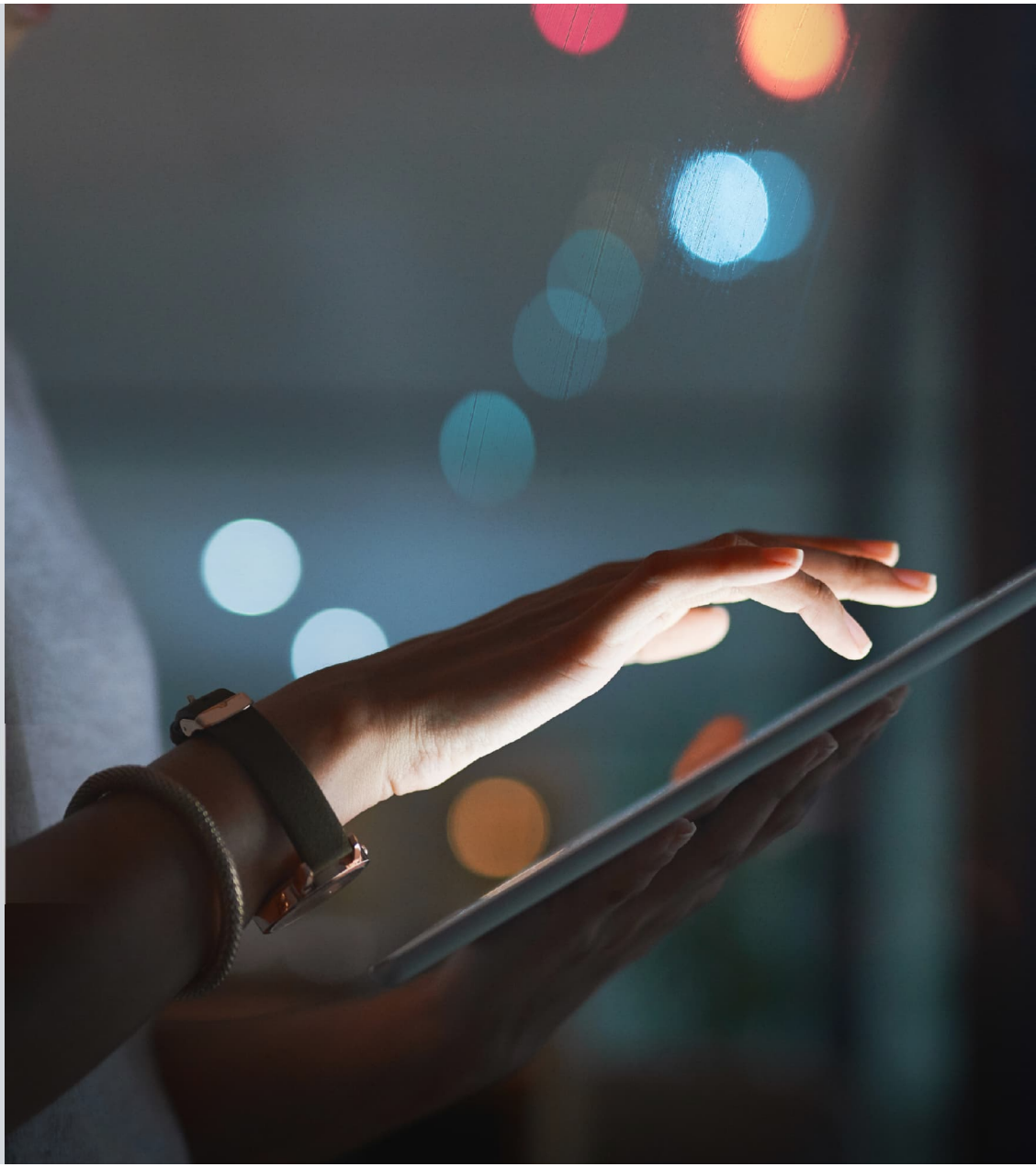
零信任架構如何滿足ISO 27001標準

ISO 27001 標準要求	零信任架構對應措施
A.5.15 存取控制 **A.5.18 存取權限**	**零信任強調「最小權限原則」與「基於身份的動態存取控制」**
A.8.16 監視活動	**零信任強調「持續監控」以發現異常**
A.8.15 存錄	**所有資源存取活動皆需產生日誌以供稽核**

零信任架構如何滿足ISO 27001標準

ISO 27001 標準要求	零信任架構對應措施
A.5.14 資訊傳送	**零信任要求對資料傳輸進行加密與路徑管控**
A.5.26 資訊安全事故之回應	**零信任與SIEM整合以快速應對與緩解威脅**

導入零信任架構的優勢

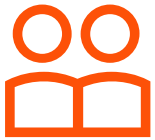


零信任導入之合規優勢

安全性提升

減少內外部威脅

零信任架構中，「永不信任，持續驗證」的理念可以有效減少未經授權的內部威脅和外部攻擊。



提高公民信任

通過零信任架構的實施和合規性管理，政府機關能夠展示其對資訊安全的承諾，提升公民對公共機構的信任。

零信任導入之合規優勢

靈活性和適應性

支持遠端辦公和混合工作模式

零信任架構允許安全的遠端和混合工作模式，在確保安全的前提下，提升工作靈活性。

快速適應技術變更

架構的靈活性意味著新技術和解決方案可以更容易地集成，確保機關在快速變化的技術環境中保持競爭力。

Thank you

Email:
michael.a.huang@pwc.com

pwc.com