

國內金融業零信任導入之 現況與展望



- 1 國內外金融業零信任導入現況
- 2 證券業導入零信任的現況與對策
- 3 未來方向與計畫

Agenda



1

國內外金融業零信任 導入現況

國外金融機構零信任現況

	北美	歐洲	亞太地區
導入現況	全球領先 多數金融機構已啟動零信任專案，成熟度最高。	啟動率偏低 少數金融機構已啟動零信任專案，但為了因應新法規壓力，已被視為關鍵實踐。	加速追趕中 多數亞太區的金融機構在疫情後將零信任列為優先事項，主管機關已陸續推出相關規範。
主要驅動因素	由上而下的「政府強制推動」 美國政府指令（OMB M-22-09）強制要求聯邦機構實施，其標準化框架（NIST, CISA）順勢成為金融業的業界標準。	營運韌性法規的「間接驅動」 英國央行（BoE）和歐盟的DORA 規定雖未明文要求，但其對威脅遏制的要求，例如微分段和最小權限原則，皆使零信任成為滿足法規的最佳技術實踐。	直接回應威脅 為應對勒索軟體、供應鏈攻擊等具體威脅，並跟進政府部門（如澳洲防護安全政策框架及新加坡金融管理局）的要求與建議，金融機構已展現出強烈的策略性導入動機。

國內證券業導入零信任的背景

1 政策驅動

行政院：「**國家資通安全發展方案**（**110年至113年**）」將導入零信任列為重點。

金管會：發布「**金融資安行動方案2.0**」鼓勵金融業部署零信任，強化數位轉型下的資安韌性。

2 產業指引

金管會於113年7月發布「**金融業導入零信任架構參考指引**」，倡議「永不信任，持續驗證」的核心思維，協助業者循序漸進強化防護。

3 現況掌握

臺灣證券交易所委託 PwC 進行本次問卷調查，旨在了解**國內證券業導入零信任現況**，並提出以下結果：

- 建立現況基準 (**Baseline**)
- 識別關鍵缺口
- 提出推動建議

證券業導入零信任的 現況與對策

資誠與證交所合作完成零信任的產業現況普查



資料來源

本調查結果的分析基礎來自**全台灣 68 家證券商**所蒐集的問卷資料。



核心評估支柱

以各系統之完整存取路徑（即**身分、設備、網路、應用程式、資料五大支柱**）之現況作為填答之依據。



評估架構

遵循金管會指引，採「**風險導向**」原則，聚焦於高風險場域與關鍵系統。



成熟度模型

採用金管會指引的**漸進式模型**，評估以下三級：

- Level I：傳統
- Level II：起始
- Level III：進階

****註：**為提升分析效度，本次問卷未納入 Level IV (最佳化) 相關題項。

選擇系統分析 – 系統分類

核心業務與交易系統類：

涵蓋了從前台的線上開戶、下單到後台的帳務系統。

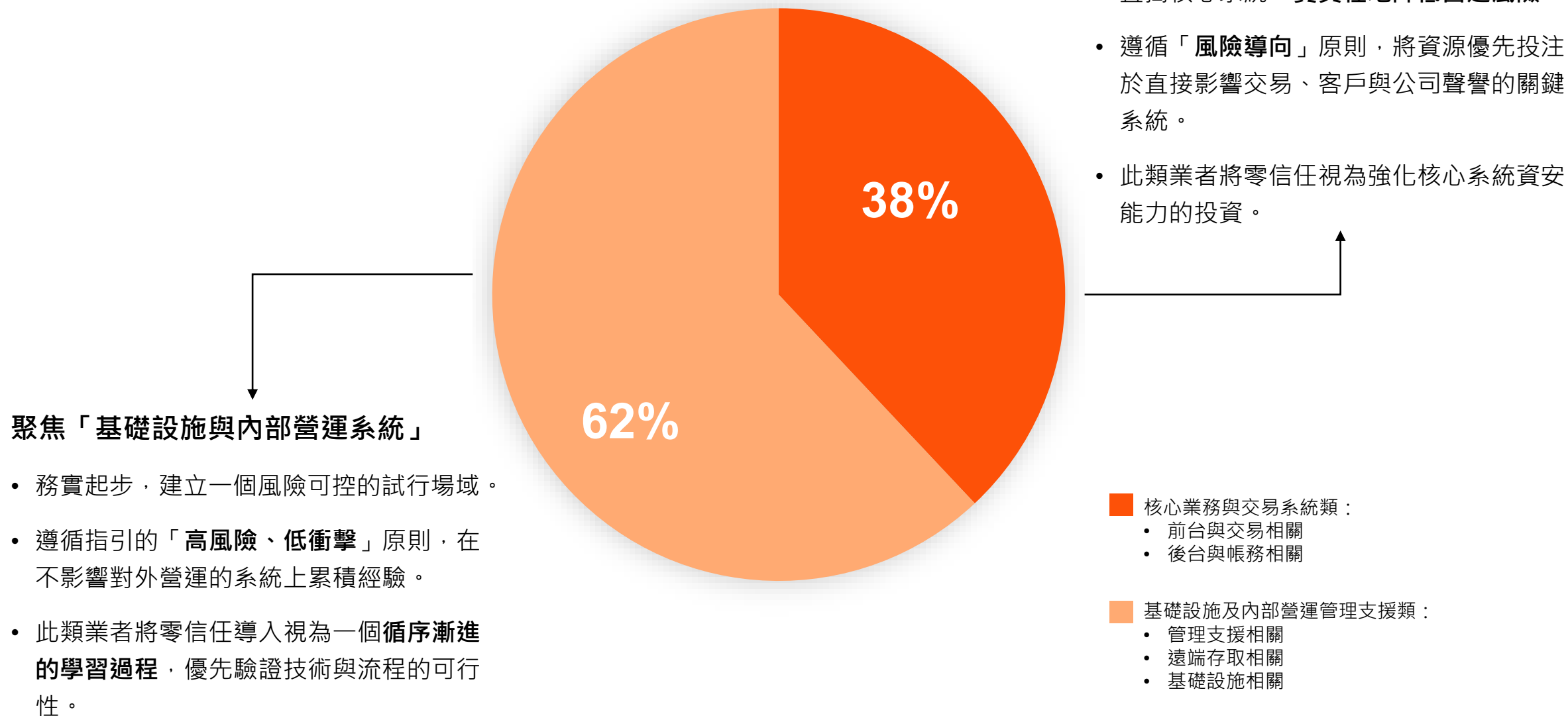
基礎設施及內部營運管理支援類：

涵蓋了啟用安全遠距辦公的VPN與VDI、管理高權限帳號的CyberArk系統，以及支援內部作業的人資、公文系統等。

**右列表格系統名稱僅為範例

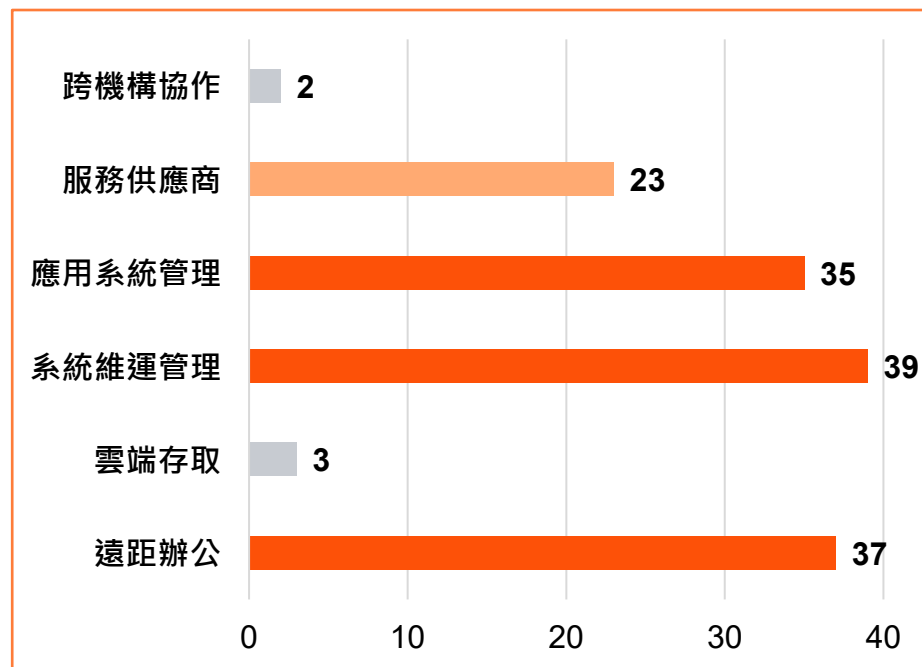
核心業務與交易系統類	前台與交易相關	- 線上開戶系統 - 數位櫃台系統 - 下單系統 - 帳務行情報價系統
	後台與帳務相關	- 證券後台作業整合系統 - AS400
基礎設施及內部營運管理支援類	遠端存取相關	- SSL VPN / Citrix VPN - Hosted Virtual Desktop (HVD)
	基礎設施相關	- 廠商維運系統 - 特權帳號管理系統
	管理支援相關	- 人資系統 - 電子公文系統 - 文件管理系統 - 稽核法遵系統 - 電話錄音系統

選擇系統分析 – 系統策略分析



- 核心業務與交易系統類：
 - 前台與交易相關
 - 後台與帳務相關
- 基礎設施及內部營運管理支援類：
 - 管理支援相關
 - 遠端存取相關
 - 基礎設施相關

選擇場域分析 – 場域數量



國內證券業者針對場域的選擇

場域被選擇數量 > 30

「系統維運管理」、「遠距辦公」與「應用系統管理」為最多業者關注的場域，國內證券業者普遍選擇這三個場域導入零信任架構。

場域被選擇數量 20-30

「服務供應商」為次之國內證券業者選擇之場域。

場域被選擇數量 < 5

「雲端存取」與「跨機構協作」為最少國內證券業者選擇之場域。

選擇場域分析 – 場域策略分析



優先聚焦內部核心 場域被選擇數量 > 30

「系統維運管理」、「遠距辦公」與「應用系統管理」為業者選擇**最多**的場域。此現象清晰反映業者普遍採行「**由內而外**」的務實策略，優先從企業內部、可完全掌控的核心領域著手，以確保在**導入初期能有效降低風險與複雜度**，同時能降低目前系統的**現有風險**。



正視供應鏈安全挑戰 場域被選擇數量 20-30

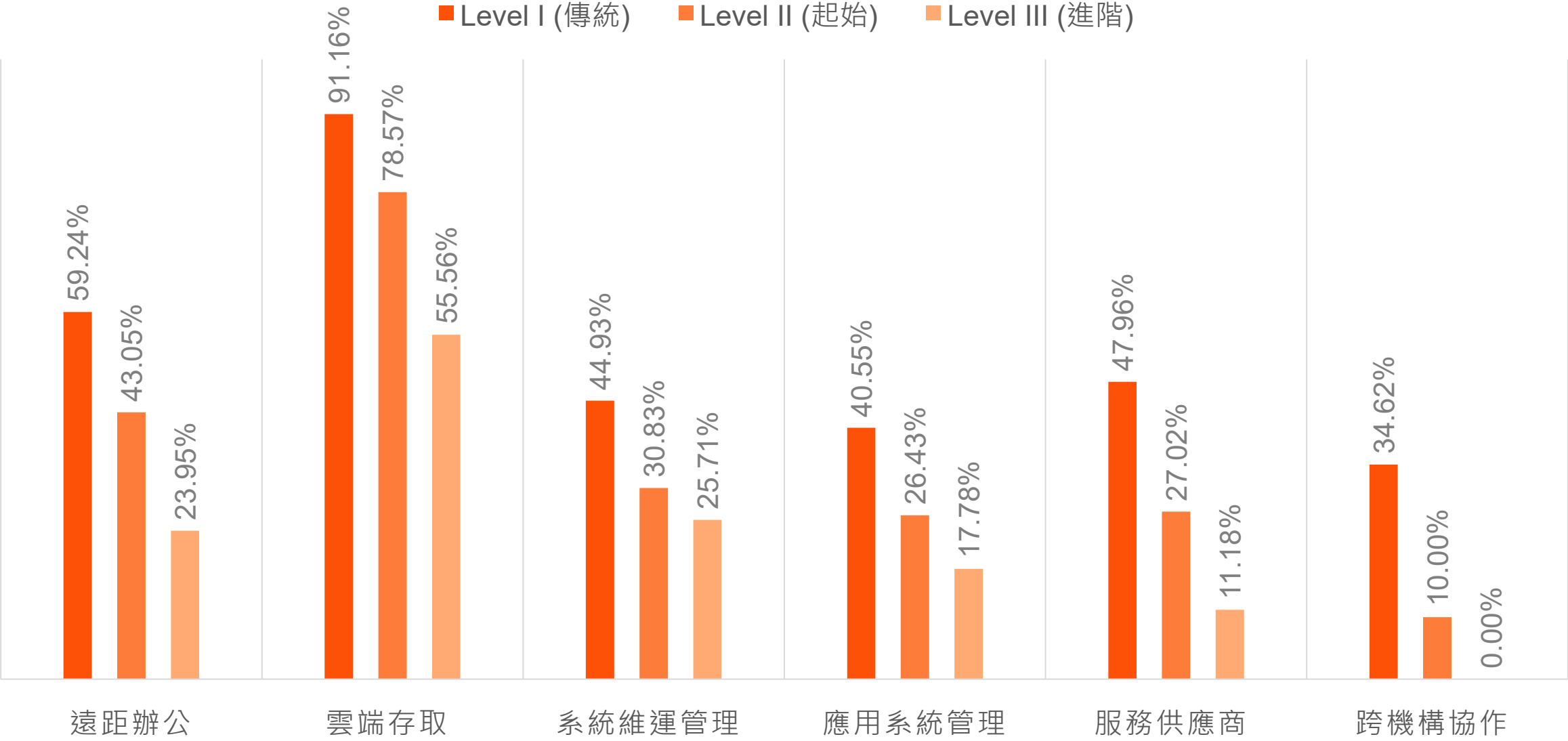
「服務供應商」的選擇數量居次。這顯示在這些公司已辨識出**供應鏈與委外廠商**是其資安防禦的顯著風險點，並開始投入資源著手處理這個涉及跨組織協調的複雜議題。



著手於未來挑戰 場域被選擇數量 < 5

「雲端存取」與「跨機構協作」的選擇數量最少。前者印證了證券業系統採用**雲端尚不普及**；後者則因**治理複雜度**，兩者皆被普遍定位為更長期的導入目標。

業界總體達成率表現概覽



結果分析 – 強項分析(遠距辦公)

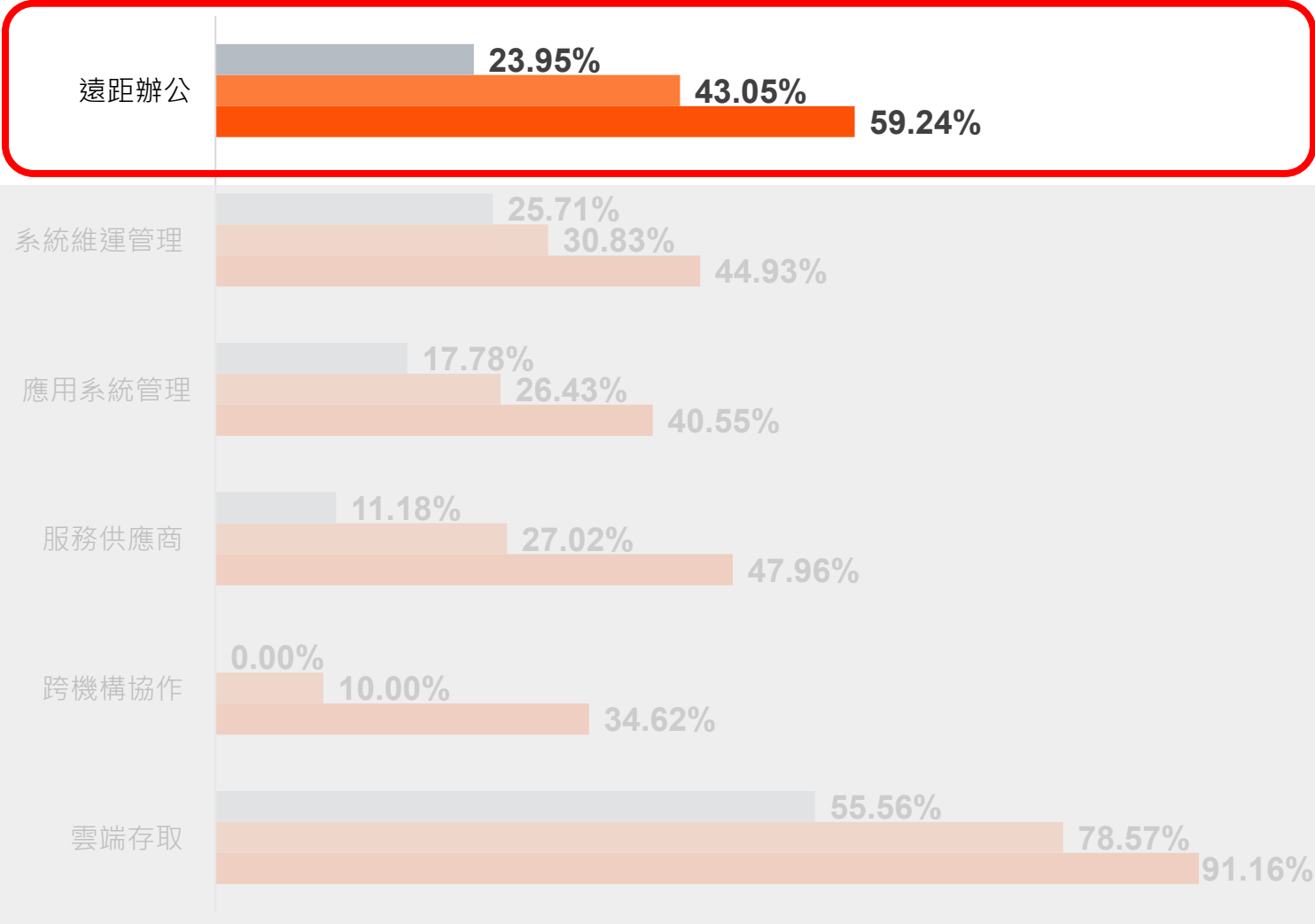
國內證券業者總體成就表現概覽

關鍵資料表現

- 選擇家數最多：共 37 家 業者選擇此場域。
- Level I 達成率：59.2% (第二名)
- Level II 達成率：43.1% (第二名)

成功關鍵因素

- 業界普遍使用VPN系統
主流 VPN 方案已普遍整合多因子認證 (MFA) ，強化使用者驗證強度。
VPN本身即是透過加密技術，已保障傳輸過程中的資料安全。
已具備基礎能力，能做到僅允許受納管的設備進行連線。



■ Level III (進階) ■ Level II (起始) ■ Level I (傳統)

結果分析 – 強項分析(系統維運管理)

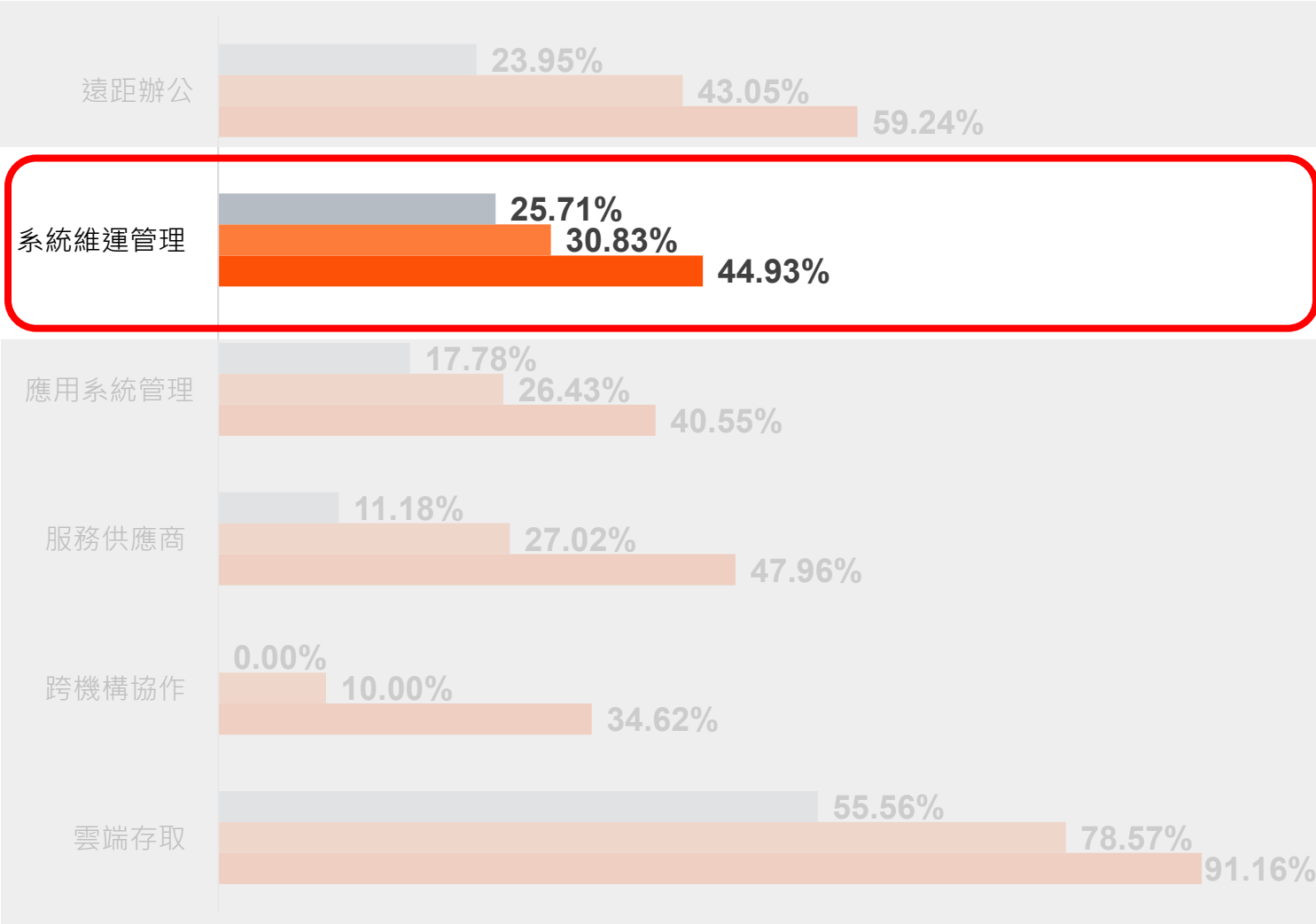
國內證券業者總體成就表現概覽

關鍵資料表現

- Level III 達成率：25.7% (第二名)
- 成熟度降幅最小：從 Level II (30.8%) 至 Level III (25.7%) 降幅僅 5.1%，顯示進階導入的動能強勁。

成功關鍵因素

- 導入特權帳號管理系統
普遍導入特權帳號管理系統並整合 MFA，落實最小權限原則。
- 可視性與分析
日誌已集中至 SIEM / SOC 平台進行分析。
部分業者已具備進階威脅偵測能力 (如 IOC, MITRE ATT&CK)，滿足 Level III 的即時偵測要求。



■ Level III (進階) ■ Level II (起始) ■ Level I (傳統)

結果分析 – 弱項分析(應用系統管理)

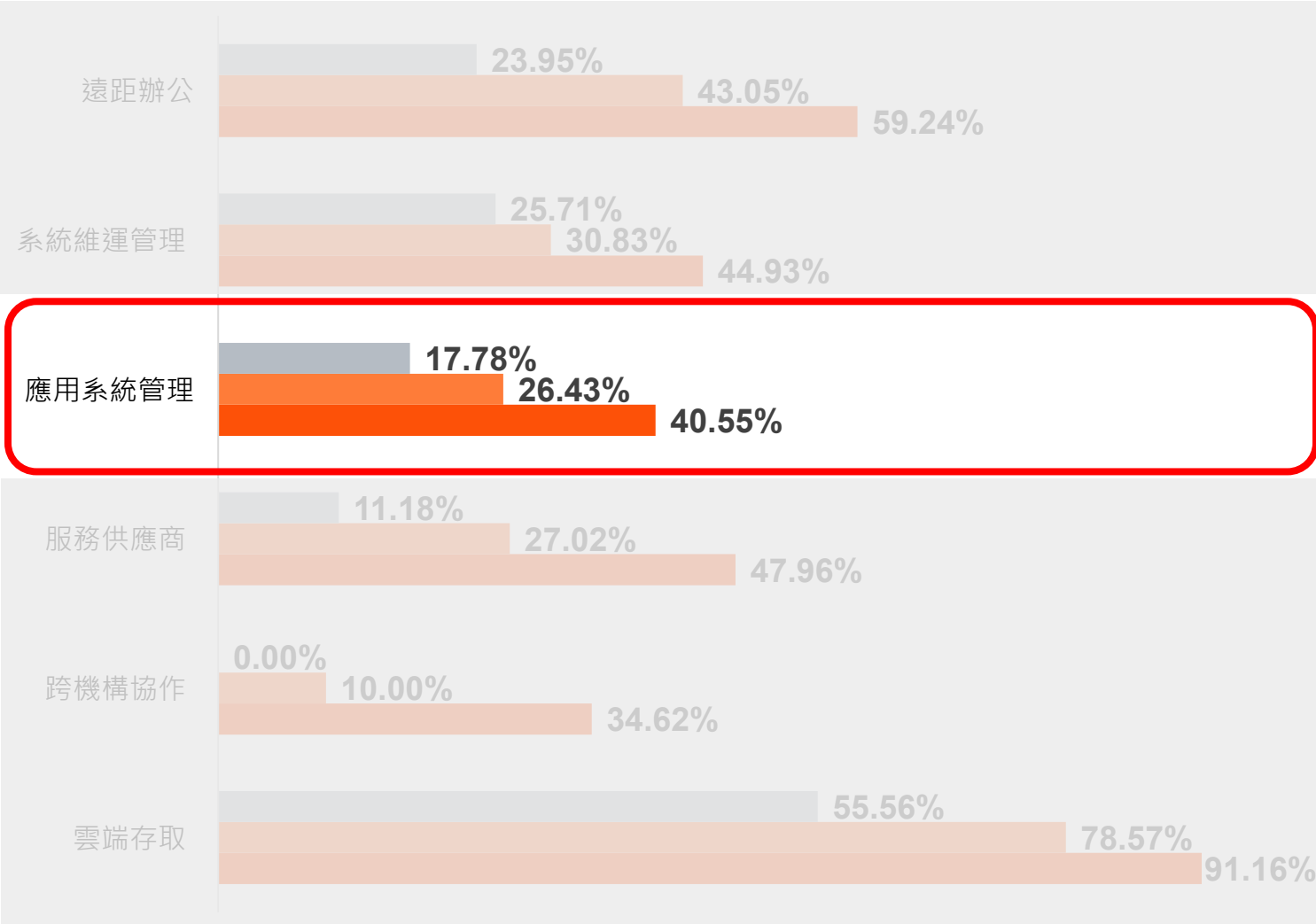
國內證券業者總體成就表現概覽

關鍵資料表現

- **Level I 達成率**：40.6% (倒數第二)
- **Level III 達成率**：僅 17.8% (進階能力明顯不足)

資料背後的原因

- **應用程式的「客製化」先天限制**
系統高度異質化，缺乏**標準化管理介面與日誌格式**。導致難以整合**統一的監控工具** (如 PAM, SIEM)，增加安全納管的複雜度。
- **跨越技術的「跨部門治理」挑戰**
系統所有權在**業務單位**，因應資安的調整需**跨部門協調**。惟業務單位常以「**穩定性**」為優先，資安變革推動不易，資訊單位難以單獨主導。



■ Level III (進階) ■ Level II (起始) ■ Level I (傳統)

結果分析 – 弱項分析(服務供應商)

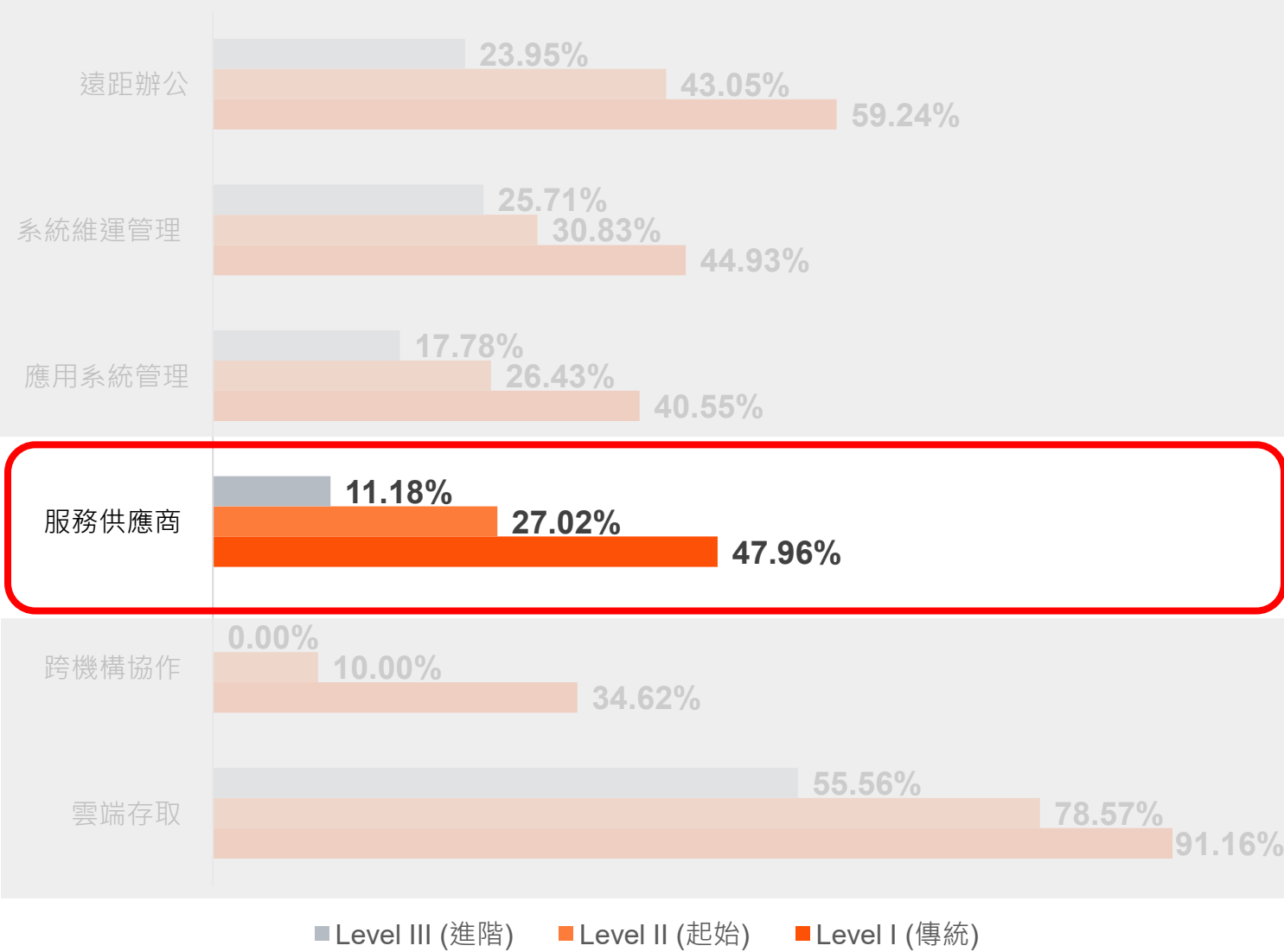
關鍵資料表現

- **Level I 達成率**：48% (第三名)
- **Level III 達成率**：僅 11.2% (倒數第二)

資料背後的原因

- **持續的動態屬性檢核**
無法即時驗證供應商人員或設備的最新狀態。
- **深度的權限與行為監控**
難以分析供應商在系統內的實際操作行為是否異常。
- **自動化的風險應對**
缺乏偵測到異常時告警、自動降權或中斷連線的機制。

國內證券業者總體成就表現概覽



結果分析 – 未來挑戰(跨機構協作)

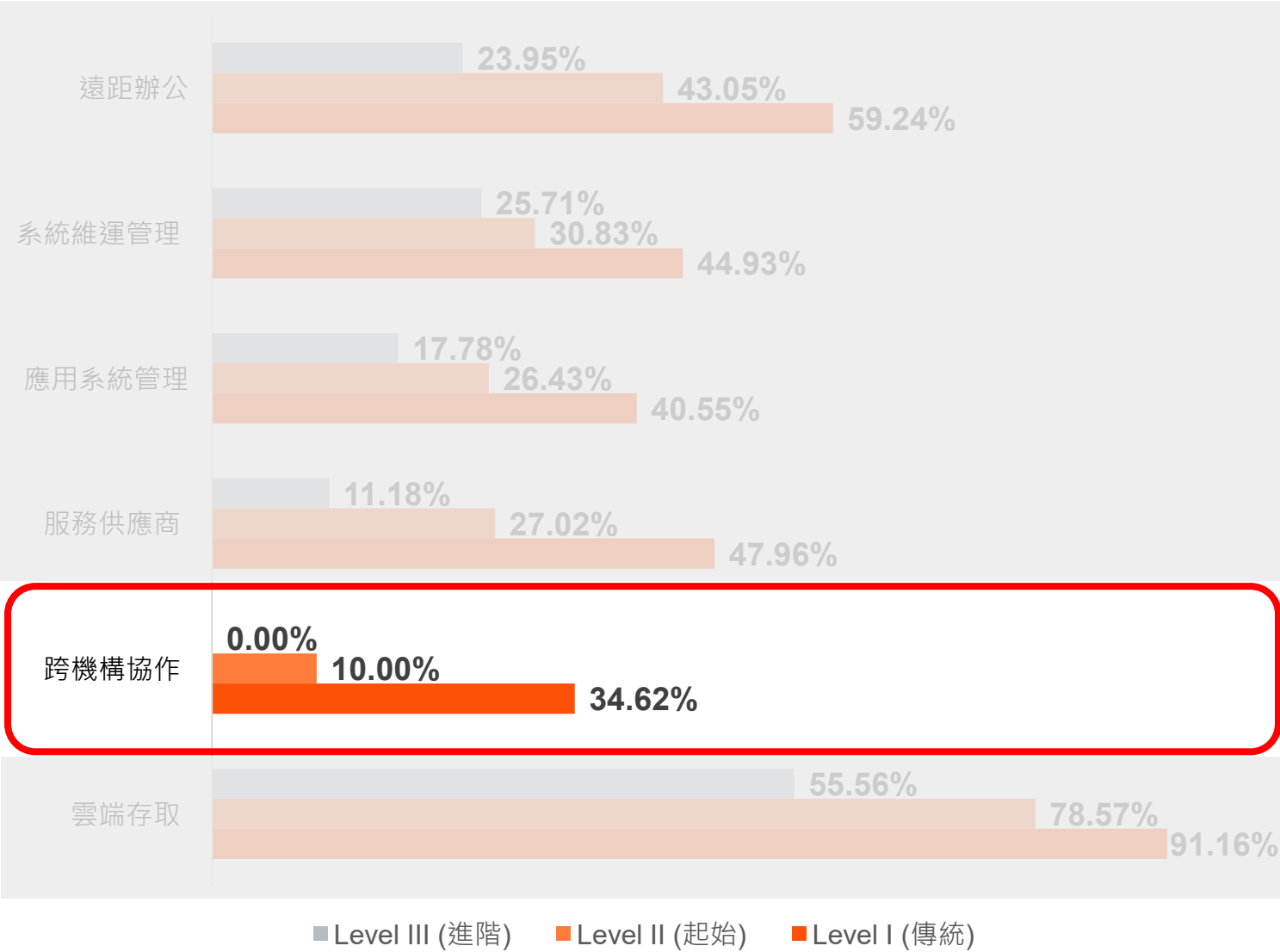
關鍵資料表現

- Level I、Level II、Level III 達成率：皆為六大場域中最低

資料背後的挑戰

- 跨機構治理：
不同法人間，各自擁有不同業務目標與風險偏好，可能導致溝通與決策成本極高。
- 信任邊界模糊：
如何建立、維持並撤銷跨組織的角色權限，涉及複雜的合約與治理議題。
- 技術整合困難：
需要考量不同的身分識別方式、設備綁定問題等高難度的技術整合。

國內證券業者總體成就表現概覽



結果分析 – 未來挑戰(雲端存取)

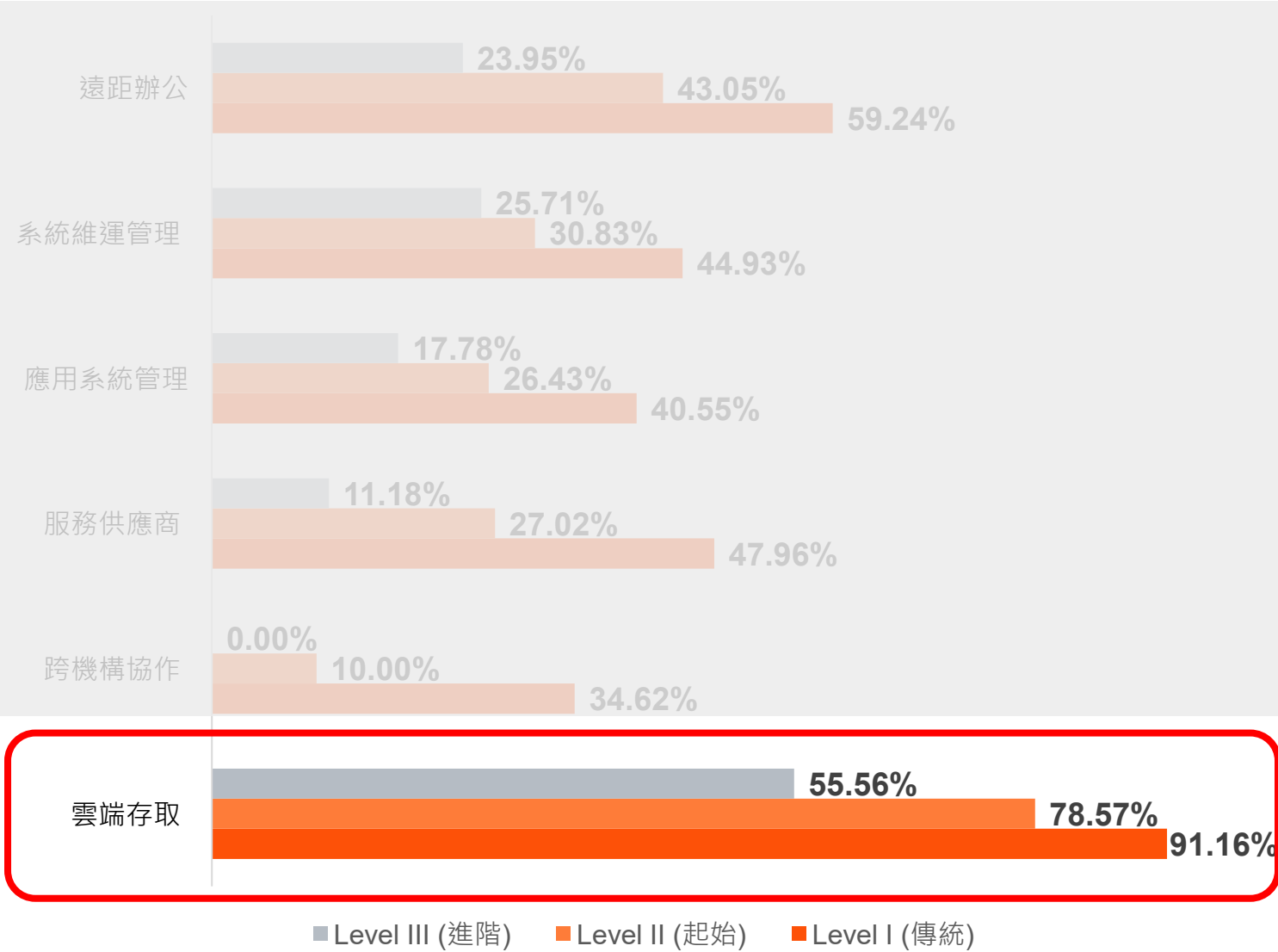
關鍵資料表現

- Level I、Level II、Level III 達成率：皆為六大場域中最高

資料背後的挑戰

- 選擇此場域業者樣態
為遵循集團全球資安標準的外資券商。這些公司在雲端採用與安全治理上起步早、標準高，其零信任策略早已是集團層級的全球性要求，而非國內證券業的普遍現況。
- 樹立典範
證明了在證券業的雲端環境中，實現高度成熟的零信任架構是完全可行的。

國內證券業者總體成就表現概覽



場域平均成熟度

42.1%

遠距辦公

業界投入最多、成熟度最高，但動態監控能力 (L2/L3) 仍待加強。

75.1%

雲端存取

高分源於極少數外資券商，可視為未來標竿，非行業普遍水準。

33.5%

系統維運管理

進階 (L3) 能力最強，但傳統 (L1) 普及率卻偏低，領先者與落後者差距大。

28.3%

應用系統管理

受限於客製化與跨部門治理困境。

28.7%

服務供應商

缺乏進階的動態屬性檢查與行為分析能力，防禦鏈存在缺口。

14.9%

跨機構協作

因技術與治理複雜度最高，目前非多數業者優先項目。

3

未來方向與計畫

現況診斷 - Level I 普及度警示



最優先場域仍有四成未達標

- 在投入最多的「**遠距辦公**」場域，Level I 達成率僅 **59.2%**。
- 仍有約 **40%** 的業者連最基礎的控制措施（如 MFA、設備納管）都尚未完成部署。
- 業界在零信任的**基礎普及**上，存在**顯著**的提升空間。

現況診斷 - Level II 缺乏動態屬性審核能力



缺乏動態指標審核能力

- 沒有任何一個主要場域的 **Level II** 達成率達到五成，顯示業界卡在從靜態走向動態的關卡。
- 根本原因為業界仍停留在蒐集靜態屬性。缺乏動態屬性，例如：即時使用者行為、設備健康狀態...
- 由於缺乏必要的動態數據輸入，建立 **ABAC (基於屬性存取控制)** 機制無從談起，無法執行 **Level II** 核心功能：「動態撤銷、限縮授權或即時告警」。

現況診斷 – 應用系統層安全普遍落後

應用系統管理

- 系統高度異質化，缺乏標準化介面與日誌格式。難以整合統一的監控工具（如 SIEM, PAM），增加安全納管的複雜度。
- 系統所有權常歸屬於業務單位。而業務單位的考量重點與資訊安全相斥。

跨機構協作

- 身為應用系統管理，一樣有系統高度異質化問題。
- 協調對象從「內部部門」擴大為涉及「多個法人實體」。

形成「應用層」的巨大安全缺口

- 無論是內部或外部，上述挑戰共同導致零信任架構在「應用程式」這一最關鍵的支柱上難以深化。

現況診斷 – 雲端採用率挑戰

「雲端採用率」偏低所帶來的未來風險

- 絕大多數證券業者的核心系統與營運重心仍以**地端機房**為主。對多數業者而言，雲端目前尚未被視為最迫切處理的「高風險場域」。
- 隨著主管機關近年來對金融上雲、生成式**AI**等新興技術的態度**日益開放**，以及**市場競爭**的加劇，導入雲端服務以獲取彈性、成本效益與創新能力，已從「選項」逐漸成為「趨勢」。

地端累積的安全經驗，未必能直接轉移至雲端環境

- 地端安全著重於清晰的邊界防護與實體隔離；而雲端安全則是以「身分為新邊界」，更強調對**API**、**設定檔 (Configuration)** 與**自動化流程**的精細化治理。
- 業者熟悉的地端防火牆、入侵偵測系統等工具，在雲端環境需被**雲原生的安全群組 (Security Groups)**、**網路ACLs**、**雲端工作負負載保護平台 (CWPP)** 與**雲端安全配置管理 (CSPM)** 等新技術取代。

未來計畫 – 雙軌推進零信任成熟度

	深度計畫	廣度計畫
目標	打通單一系統，建立成功範例	橫向擴展，複製成功經驗
行動方案	確保各業者選擇一套代表性系統，目標是完整導入並打通 Level I 至 Level III 。	將單一系統的成功經驗，優先橫向擴展至同質性高的其他場域。
策略價值	建立一個從基礎到進階的垂直樣板。	建立一套可複製的技術與流程範本，加速全面導入。

未來計畫 – Level I 為最低要求，邁向動態化



Level I 為最低門檻

- Level I 應被視為**最低強制性合規門檻**，確保行業安全水平無過大斷層。
- 針對資源有限的**四級券商**，可將「**一套系統完成 Level I**」設定為首要目標，集中資源鞏固基礎。



從 Level I 邁向 Level II

- 從「靜態防護」跨越至「動態驗證」。唯有達到 **Level II (動態授權)**，才能算是零信任架構的開始，以有效應對不斷變化的威脅環境。
- 對於已達 Level I 的業者，應盡速引入對五大支柱的「**動態屬性**」蒐集與驗證機制。

核心策略與具體行動 – 第一階段

啟動單一場域之 Level II 動態驗證試點

設定導入目標的「標竿系統」：

建議要求所有證券商，均需擇定一具代表性的系統，作為零信任導入的「標竿系統」，以單一一套系統作為深度試點，並進一步導入 Level II 的動態屬性蒐集與即時告警機制。



每家業者根據其標竿專案的經驗，為後續擴展奠定基礎，並逐漸建立 Level I/II 的技術與流程樣板。

核心策略與具體行動 – 第二階段

▶ 標竿系統邁向 Level III

標竿系統 Level III 實現 (深度 Level III) :
標竿系統應整合 IAM、SIEM/SOC，實現 Level III 的即時偵測與自動化應變能力。



克服「成熟度懸崖」，證明 Level III 的自動化應變可行性。

▶ 其他系統推進至Level II

其他場域的Level II 補強 (廣度 Level II) :
將標竿系統成功的 Level II 動態授權策略，橫向複製到其他高風險場域，確保其他系統的 Level II 成熟度一致。



利用已有成功的一套標竿系統，快速提升整體資安水位。

▶ 應用系統逐套深度改造

應用系統逐套 Level 深化 :
鑒於「應用系統管理」的高度異質性與客製化特性，建議採行「逐套深化」的策略，以鼓勵而非強制的方式，引導業者進行長期且持續的改造。



尊重應用系統的異質性，採用分散式、高客製化的深度推進策略。

核心策略與具體行動 – 第三階段

Level III 全場景覆蓋。

其他場域的Level III 補強 (廣度 Level III) :
將標竿系統 Level III 的實踐推廣至所有適用場域，實現廣度上的成熟度統一。



實現零信任架構的全面性，將深度經驗轉化為廣度標準。

Thank you