從刷卡開門到Identity、Authority：台灣Access Control三十年產業演變與下一步

總會諮詢顧問 施正偉



從技術、產業結構與應用市場的三十年變化，看Access Control如何由刷卡開門與弱電設備，逐步走向Identity、Authority、Physical/Virtual Access與Cyber-Physical Security。

本文受眾：安控、Access Control、RFID、生物辨識、智慧鎖、SI/VAR、智慧建築、零售物流、高科技製造、醫療、交通，以及OT/IT Cybersecurity從業者。

Highlight：研究過去三十年，不是懷舊，而是看下一個10～30年

如果只是把過去三十年出現過的門禁公司重新列一次，這只是在寫歷史。真正值得研究的是：為什麼某一類技術與公司會在某個時間點出現？原有產品解決不了什麼問題？新的角色出現後，又把市場帶向哪裡？

台灣Access Control三十年的變化，或可以從三條主軸來看：

演變面向	早期問題	三十年間的變化	下一階段
技術	怎麼辨識一個人？	Card → RFID → Biometrics → Mobile → Smart Lock	Digital Identity、Context、Device Identity、AI
產業結構	誰做 Reader、Controller？	Hardware → Software Platform → VAR／SI → Ecosystem	Identity、Cybersecurity、OT、Cloud
應用市場	誰能進哪一道門？	考勤、辦公室 → 工廠、零售、物流、醫療、交通、高科技	Physical＋Virtual＋Machine＋Data Access

真正的變化不是設備愈來愈複雜，而是Access（進出）管理的對象與邊界愈來愈大。

一、為什麼打卡鐘公司會走進Access Control？

企業最早想管理的，往往不是「誰能進哪一道門」，而是：誰來上班？幾點到？幾點走？

因此，卡鐘、考勤、人事管理很早就成為企業管理的一部分。商合行、震旦等業者從卡鐘、差勤或辦公室服務往門禁延伸，並不是偶然。因為：考勤管理的是Time；Access Control管理的是Space；兩者共同管理的，其實都是Employee Identity。

當機械卡鐘走向電子化與資料庫化，企業開始能把某個人、某個時間與某個身份連結起來。下一步自然就是：這個人除了來上班，還可以進哪裡？

所以Attendance走向Access，不只是增加Reader，而是Employee Identity ，從時間管理延伸到空間與權限管理。

二、為什麼RFID、Reader、Controller會形成一整個產業？



機械鑰匙可以開門，但不容易大量發行、撤除、設定時段，也很難留下可追溯紀錄。

因此市場需要一種可由系統辨識與管理的Credential（憑證）。

磁條卡、感應卡、125K RFID、MIFARE、Smart Card等技術陸續出現，核心目的都是：

把人的身份，轉成機器可以辨識、發行、撤除與管理的Credential。

台灣也在這個過程中形成完整供應鏈。所羅門代理EM Marine感應晶片；韋僑從卡片與RFID封裝切入；聯暘、辰皓、集佳、亞元、鵬驥等則分別從 RFID、Reader、Module、Auto-ID或應用設備進入。

Reader/Controller層則逐步形成漢軍、飛麒、鵬驥、倬茂、茂旭、SYRIS、台信、日懋、七友等不同業者。

這個階段真正重要的，不是哪一家Reader最大，而是：Credential＋Reader＋Controller已經形成可大量複製的Access Architecture。

組織開始進入到可以把「誰能進哪裡」，轉成由系統執行的規則。

三、生物辨識：Access從「你拿什麼」走向「你是誰」



RFID解決了身份載體問題，但留下另一個漏洞：卡片代表某個人，不等於拿卡的人就是本人。卡可以借、Badge可以被偷、PIN可以被分享。

因此 Biometrics 的真正意義，不只是多一種Reader，而是Access的認證邏輯開始從：What do you have？走向：Who are you？

台灣很早就有星友投入指紋辨識與門禁/差勤，星創投入人臉辨識，卓仕、高斯、倚辰等也分別從掌形、指紋、人臉等Biometric Technology進入Access。

但Biometrics的發展也提醒市場：技術方向正確，不等於市場立即成熟。

早期的演算法、運算能力、成本、光線與角度、使用者接受度、Privacy，都限制了市場成長。直到高科技、金融、機場、資料中心、政府高安全場域逐漸成熟，Biometrics的價值才充分明顯。

這正說明：Technology Maturity ≠ Product Maturity ≠ Application Maturity ≠ Market Maturity。

而且Biometrics並沒有完全取代Card。未來更可能走向：Credential＋Biometrics＋Context。

四、台灣Access Control三十年產業地圖



三十年的發展，已經形成一條相當完整的 Access 供應鏈。

產業層級	解決的問題	技術演變	台灣代表性脈絡/業者	下一階段
Attendance/Employee Data	誰來上班、何時到？	卡鐘 → 電子考勤 → HR Data	商合行、震旦等	Employee Identity
Credential/Card	如何代表一個人？	磁卡 → Proximity → Smart Card	商合行、韋僑、辰皓等	Digital Credential
RFID/Module/Auto-ID	如何讀取與識別？	LF／HF／UHF、NFC	韋僑、聯暘／興暘、辰皓、集佳、亞元、鵬驥等	Connected Identity
Reader	如何取得 Credential？	Proximity → Smart Card → Secure Reader	漢軍、飛麒、鵬驥、倬茂、茂旭、SYRIS、台信、日懋、七友等	OSDP、Cyber-secure Reader
Controller	如何執行 Access Decision？	Standalone → Network Controller	漢軍、茂旭、倬茂等	Edge Decision
Biometrics	Credential 是否等於本人？	指紋、掌形、人臉、掌靜脈、虹膜	星友、星創、卓仕、高斯、倚辰等	Multimodal Authentication
Access Software Platform	大量 Identity／Authority 怎麼管理？	PC → Client/Server → Web → Cloud	嘉因等	Identity Governance
VAR/Application SI	如何符合企業 Workflow？	Customization、Integration、Workflow	智碁、銓宇、泰宇、鍵祥等	Policy Integration

產業層級	解決的問題	技術演變	台灣代表性脈絡/業者	下一階段
Electromechanical Lock	系統如何真正開／鎖門？	電磁鎖、陽極鎖、陰極鎖、剪力鎖	翔光、禮銳、連冠等	Smart Door
Door Hardware/Smart Lock	機械安全如何電子化？	Mechanical → Electronic → Connected Lock	福興、Klacci、田晉、日堡、敦義、WAFERLOCK、瑋豪等	Smart Access Ecosystem
AIDC/Asset Access	不只管理人，也管理物	Barcode、RFID、PDA、WMS	精聯、欣技、立象等	Asset Identity／Traceability
Enterprise Security Integration	多系統如何共同治理？	PACS＋HR＋Video＋OT＋IT	大型 SI／Security Service Ecosystem	Cyber-Physical Security
Virtual/OT Access	系統、設備、機器誰可以使用？	IAM、PAM、Zero Trust、Device Identity	IT／OT Security 生態	Unified Access Principle

這張表真正說明的是：台灣Access Control從來不是一個Reader產業，而是一條由Credential、Hardware、Software、SI、Door Hardware到Identity與Cybersecurity組成的供應鏈。

五、為什麼Reader、Controller做到後來，一定會需要Software Platform？

當公司只有幾十人、十幾扇門，Controller本身可以處理多數需求。

但企業變成幾千人、數百道門、多廠區、多身份、多時段後，真正困難的不再是：Controller能控制幾道門？

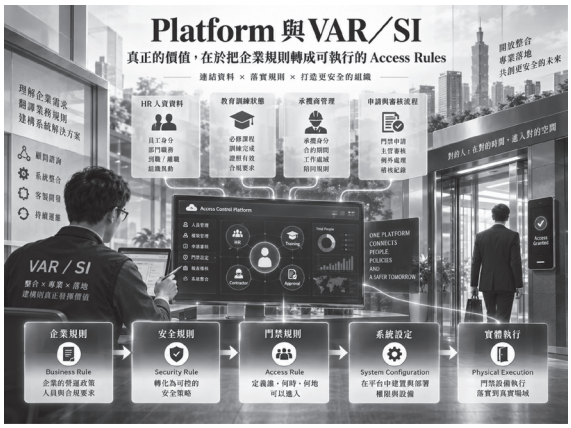
而是：幾千個Identity與幾萬種Authority，要怎麼管理？這就是Software Platform出現的原因。

嘉因便代表這個產業節點。它不是以Reader、Controller為主，而是以軟體平台管理 Person、Card、Door、Authority、Event，並整合不同Controller、人事系統與其他設備。

這代表Access的價值開始從Device 往：Database、Authority、Integration移動。

更值得注意的是，這類Access Software Platform在台灣出現的時間，並沒有明顯落後國際企業級Access的發展邏輯。這說明台灣當時的技術認知，也已經理解：門禁不只是硬體，Platform會成為新的價值中心。

六、有了Platform，為什麼還會出現VAR/SI？



Software可以管理Person、Card、Door、Time Zone、Authority、Event，卻不會天然知道每一家企業怎麼運作。

例如：員工完成HR報到後才能拿卡；完成教育訓練後才能進特定區域；承攬商只在工程期間有效；離職後權限必須同步撤除；不同主管只能核准特定區域。

這已經不是單純Software Feature，而是企業Workflow。

因此市場自然產生：VAR/Application SI。

像智碁這類角色，真正的價值不是「幫軟體公司施工」，而是把：Business Rule → Security Rule → Access Rule → System Configuration → Physical Execution 連接起來。

所以Reader廠商解決「怎麼讀」，Controller解決「怎麼控制」，Platform解決「怎麼管理」，VAR/SI則解決：企業真正的規則，如何被系統執行。

這也是Access比一般設備更容易形成產業型SI/VAR 的原因。

七、為什麼影像監控較少形成完全相同的VAR結構？

影像監控當然也需要SI，但傳統Video與Access有一個基本差異。

Video主要處理：Observe、Record、Verify。

Access則必須在事件發生前做：Allow/Deny。

因此Access必須先回答5W1H。

5W1H	Access真正要處理的問題
Who	員工、訪客、承攬商、醫師、學生、設備維護者？
What	可以開門、操作設備、領物、讀取資料、執行交易？
Where	辦公室、實驗室、倉庫、病房、Fab、Server？
When	上班時間、專案期間、維護時段、臨時授權？
Why	工作、維修、訪客、物流、醫療或緊急任務？
How	Card、Biometrics、Mobile、MFA？誰批准、如何撤權？

因此Access天然會進入企業內部制度。

也因此，大型Access SI真正累積的是：Application Know-how＋Customer Trust＋Process Understanding＋Integration Capability。

二十幾年前，銓宇這家公司能從企業級安控SI，發展到被國際集團收購，就很能說明：真正有價值的，不只是設備，而是已掌握的大型客戶、流程與整合能力。（如果你在這市場有近三十年，你就會知道這家公司）

八、為什麼精聯這類AIDC公司，也應該進入Access產業地圖？(AIDC：自動辨識與資料擷取)



因為Access管理的對象，已經從人擴大到物。

早期Access幾乎等於：People Access。

但零售、物流、製造、醫療會進一步問：人進來之後，可以接觸什麼？

精聯由AIDC、Barcode、RFID Reader、PDA、物流、零售與製造等應用切入，提醒我們：Access不只管理人，也管理Asset。

例如零售後場真正可能需要同時回答：

誰進入後場？拿了什麼？RFID是否出現商品移動？POS有沒有對應交易？庫存是否異常？Video是否吻合？

因此Access開始從：People Access，走向：People＋Asset＋Transaction Access。

這也是零售、物流與醫療逐漸把 Access、AIDC、RFID、POS、WMS、ERP、Video拉到同一應用架構的原因。

九、Access Control的應用市場，遠比科技廠更廣

半導體是很好的案例，因為它把Access的程序性放大到非常清楚，但它並不是唯一市場。

真正需要看的，是不同場域的 Gate 到底是什麼。

應用場域	Access 管理對象	核心 Access Issue	必須整合的系統
企業/辦公室	員工、訪客	身份、差勤、空間權限	HR、Attendance、Visitor
政府機關	公務員、民眾、承攬商	公開區／限制區	HR、Visitor、Security Procedure
半導體/高科技	員工、承攬商、維護者	機密區、無塵室、Qualification	HR、Training、Contractor、Audit
銀行/金融	員工、金庫、特殊區	高安全與多人授權	HR、Biometrics、Video、Audit
零售	員工、商品、供應商	後場、庫存、交易	POS、RFID、Inventory、Video
物流/倉儲	人、貨、車	誰能接觸哪批貨	WMS、RFID、Vehicle、ERP
醫院	醫護、病患、訪客、藥品	手術室、藥品、病歷	HIS、Pharmacy、Visitor、Identity
校園	學生、教職員、訪客	宿舍、實驗室、夜間空間	Student ID、Library、Attendance
飯店/住宅	住客、住戶、服務人員	Temporary Credential	PMS、Mobile Key、Smart Lock
交通/機場	旅客、員工、車輛	票證、禁區、安全區	AFC、Credential、Vehicle、Security
資料中心	員工、租戶、維護者	多租戶、Rack Access	IAM、Ticket、Biometrics、Audit
製造/關鍵基礎設施	人、Device、Machine	Physical＋OT 權限	OT Security、PAM、Asset Management

這張表也說明：門只是Access最早的一種Gate。

醫院的Gate可以是藥櫃，零售的Gate可以是後場庫存，資料中心的Gate可以是Rack，OT的Gate甚至可以是PLC或控制介面。

十、「門禁不只是弱電工程」，真正的內涵是什麼？

如果Access Control只是：Reader接Controller、Controller接Server、Lock接電、設定軟體、測試開門，那它確實很接近弱電工程，甚至可以逐漸Plug & Play。

但高科技廠、資料中心、銀行、醫院、機場真正重視的，並不是接線本身。

Reader 最後只回答：Yes/No。



但在Yes/No前面，其實存在完整的Decision Chain：Identity → Role → Qualification → Authority → Policy → Context → Authentication → Enforcement → Log → Audit

所以：門禁硬體可以是弱電工程，但Access Control本身，是一套把企業規則轉成真實世界行為的 Policy Execution Infrastructure。

弱電工程解決：系統怎麼接起來？

Access Control解決：誰在什麼條件下，可以做什麼？

這才是它真正的產業價值。

十一、為什麼電子門禁與傳統鎖業最後一定會相遇？

電子門禁公司熟悉RFID、Controller、Firmware、Software、Network；傳統鎖與Door Hardware則熟悉Lock Body、材料、公差、耐久、防火與Panic Hardware。

但所有Access Decision最後都必須落到：Door Open/Door Locked。

所以兩個產業一定會碰在一起。

翔光早期從磁力鎖、陽極鎖、陰極鎖走向電子機械鎖，就是很早的融合訊號。台灣福興、Klacci 一德、WAFERLOCK、東隆、日堡、敦義、瑋豪等，也都從不同路徑面對：Mechanical Security＋Electronic Access。

真正成熟的 Smart Access，必須同時處理：

Mechanical Reliability

✔ Electronics
✔ Credential
✔ Software
✔ Network
✔ Cybersecurity
✔ Installation
✔ Service

因此，Smart Lock不是一個孤立產品，而是兩個長期分離的產業開始融合。

十二、Physical Access與Virtual Access，為什麼一定會靠攏？



Physical Access問的是：你能不能進這個房間？

Virtual Access問的是：你能不能進這個系統、取得這份資料？

最後都在回答：Who are you？What are you allowed to access？Under what condition？

所以兩者雖然來自不同產業，治理 Principle 卻會愈來愈接近。

一名設備維護工程師到工廠工作，可能同時需要：進入廠區、進入特定機房、登入Maintenance Laptop、登入設備、連上OT Network、取得暫時管理權限。

表面上是六種Access，實際上管理的是：同一個Identity，在不同Resource上的不同Authority。

因此Physical Access、IAM、PAM未必會成為同一套產品，但治理邏輯會逐漸一致：Identify → Authenticate → Authorize → Enforce → Log → Revoke。

十三、OT/IT Cybersecurity正在重新定義Access Control



OT加進來後，Access管理的對象已經不只是人。

還包括：Device、PLC、Robot、Server、Application、Service Account、Maintenance Laptop、Machine、API。

這代表未來Access必須回答的不只是：Who is this person？

還要回答：What is this device？Is this machine trusted？What can this application do？

因此：Physical Access ＋ IAM ＋ PAM ＋ OT Security ＋ Device Identity會逐漸發生交集。

未來Access Control 的「Who」，不再只代表Human Identity，而會擴大到：Human＋Device＋Machine Identity。

十四、連Reader與Controller的連線，也已經是Cybersecurity問題

傳統Reader與Controller通訊，過去多被視為單純弱電問題。

今天這個假設已經改變。

從Wiegand走向OSDP，不只是Protocol更新，而是開始加入雙向通訊、裝置監督、Secure Channel與更完整的Interoperability。

真正代表的是：Access Hardware本身已經成為Cyber-Physical Node。

今天的 Reader、Controller、Smart Lock 都可能具備 Firmware、Encryption Key、Network Interface、API、Remote Update。

所以高階Access未來除了問：能不能讀卡？

也必須問：Firmware從哪裡來？Credential Communication是否加密？Controller是否可能被冒充？Remote Access怎麼管理？Supply Chain是否可信？

這就是Physical Security與Cybersecurity真正開始融合的位置。

十五、三十年真正發生的，是新角色不斷被市場「叫出來」

把前面的發展收斂，可以看到一條很清楚的規律：

市場問題	原有能力為什麼不夠	新角色因此出現	代表性產業線索	價值往哪裡移
誰來上班？	紙卡無法數位管理	Attendance／Employee Data	商合行、震旦	Time
如何大量管理人員？	鑰匙難以發行撤除	Credential／RFID／Reader	韋僑、聯暘、漢軍、茂旭等	Credential
卡是不是本人？	Credential可被借用	Biometrics	星友、星創、高斯等	Identity
幾千人、幾百道門怎麼管？	Controller無法處理企業級資料	Software Platform	嘉因等	Authority
Platform 怎麼符合企業流程？	標準軟體不懂Workflow	VAR／Application SI	智碁、鍵祥等	Process／Integration
人進去後可以接觸什麼？	Door Access不足	AIDC／RFID／POS／Workflow	精聯等	Asset／Transaction
電子權限如何落到實體門？	Electronics與Mechanical分離	Electromechanical／Smart Lock	Klacci、翔光、福興 等	Physical Execution
實體與數位權限不同步	PACS、IAM各管各的	Identity Governance	IT＋Security生態	Lifecycle
Device/Machine 也需要授權	Human Identity不足	OT Security／Device Identity	OT／IT生態	Machine Trust

這張表其實就是三十年Access Control最值得研究的產業規律：

每當Access管理的Object、Scale或Risk擴大，市場就會產生一個新的Node。

十六、下一個10～30年，應該看什麼？

未來不應只預測哪一種Reader、Biometrics或Smart Lock會流行，而要看新的Access Problem出現在哪裡。

第一，Credential或許會逐漸退到後台，Identity Lifecycle會走到前台。 真正的大問題不再是刷卡、人臉還是手機，而是Identity如何建立、修改、同步與撤除。

第二，Authentication可能會走向Contextual Authorization。 證明「你是誰」還不夠，系統還會看Role、Location、Device、Qualification、Time、Task與Risk。

第三，People Access或許會擴大成People＋Asset＋Device＋Machine＋Data Access。Access Control將持續和AIDC、IAM、PAM、IoT、OT Security、Data Security交會。

第四，Hardware可能會愈來愈Plug & Play，但Governance 會愈來愈複雜。 SI/VAR的價值也會從Wiring Integration往Policy/Workflow Integration移動。

第五，Cybersecurity或許會成為Access Product Qualification的一部分。 Reader、Controller、Smart Lock已經不只是弱電設備，而是具Firmware、Network、Credential與 Supply Chain Risk的Cyber-Physical Node。

第六，Security Evidence可能會從單一Log走向Evidence Chain。Identity、Credential、Authority、Door Status、Video、Sensor與Workflow Record，需要互相驗證。

所以未來Access Control的核心，可能不再只是Permission Management，而逐步走向：

Identity Governance、Policy Execution、Security Traceability與Trust。

結語

三十年來，Access Control已從傳統Hardware主導的Top-down的商業模式，逐漸形成由場域需求、程序與Identity反推技術的Bottom-up模式，而且這兩者都並存。它不像Video那樣，很容易用Device的功能來展示價值，Access Control必須要用很多的情境、流程與模擬體驗，才能讓市場理解。Access一直像組織裡寡言的老管家，妥妥當當地安排家裡或組織中大大小小的一切，但卻話少；然而下一步真正需要的，或許不是更多的功能，而是業者如何讓access control解決方案，取得與實際價值相符的市場話語權。