金融監督管理委員會一一〇年度委託研究計畫

開放銀行所涉使用者資訊之管理及客戶權益保障機制之研究

委託單位：金融監督管理委員會銀行局

研究單位：勤業眾信聯合會計師事務所

計畫主持人：林彥良資深副總經理

協同主持人：葉奇鑫所長

研究助理：廖柏侖協理、游千瑩經理、陳怡儒副理、伍庭婷資深顧問、林柏涵資深顧問、王慕民律師、吳彥欽律師、陳品安資深顧問

中　華　民　國　一　一　〇　年　十　一　月　三　十　日

GRB計畫編號：PG11005-0062

摘要

本計畫旨在參酌主要國家推動開放銀行交易面情境下的資訊安全與消費者保護議題，提出我國開放銀行第三階段「交易面資訊」推動方式之具體可行建議。隨著金管會近年積極推動開放銀行政策，第一階段「公開資料查詢」已於 108 年正式上線運作；第二階段「開放帳戶資訊」金管會則在 109 年 12 月核准 7 家銀行申請合作案後正式上路；第三階段「交易面資訊」之推動，包括轉帳申請、帳單支付等交易以及申請類服務等，也將在第二階段執行成果的基礎上，進一步將金融服務融入消費者的日常生活中，發展出更健全的金融生態系。

針對我國開放銀行交易面應用服務所涉資訊安全和消費者保護議題，本研究透過 OWASP 發布之十大 API 安控風險作為分析架構，進而檢視國內外推動開放銀行相關規範，針對 API 安全提出強化現行規範的監控與限制性能與可用性、強化存取控制管理、API 開發掌握以及威脅防護提出四點建議。針對我國開放銀行交易面應用服務所涉消費者保護議題，本研究透過檢視我國金融消費者保護和個資保護相關法規以及歐盟一般資料保護規範（General Data Protection Regulation, GDPR）後，據以提出短、中、長期政策建議；短期內將在現行制度運作的基礎上提升開放銀行之發展，以鼓勵金融機構與 TSP 業者參與為原則，維持金融機構自律模式，並以自律規範作為金融機構篩選、控管 TSP 業者對消費者個資保護之方式；中期則在開放銀行發展較為成熟後，可依據 TSP 業者提供之不同服務內容（查詢、申請、交易等）進行評估，以「訂定 TSP 業者應具備之資訊安全與個資保護能力標準（查核項目）」為目標，作為金融機構提供一致性之參考依據；長期而言，研究團隊建議仍須針對未來各業別資料將走向資料開放的趨勢，研議 TSP 業者的跨部門治理架構，以利對消費者有全面性及一致性之保障。評估金融機構承擔 TSP 業者的個資侵害賠償責任適當性，以強化我國推動開放銀行調整相關政策之參考並檢討解決我國所面臨相關問題。

Abstract

This research aims to discuss the issues of information security and consumer data protection in the context of open banking transactions in major countries, so as to promote "Transaction Information" in the third phase of Taiwan's open banking policy. As the Financial Supervisory Commission R.O.C. has actively promoted the open banking policy in recent years, the first phase of "Open Information Enquiry" was officially implemented in 2019; the second phase of "Open Account Information" was also implemented in December 2020, 7 local banks was approved to have further cooperation with third party service providers. After the second phase was officially implemented, the third phase "Transaction Information", including transfer applications, bill payment, other transactions and application services, will also further integrate financial services into consumption based on the second phase.

Regarding the information security and consumer data protection issues involved in the open banking transactional application services of Taiwan's open banking policy, this study applies the OWASP top ten API security risks as an analysis framework to examine relevant regulations among major countries, so as to strengthen the current regulations for API security. This research discusses 4 issues for API security, including lack of resources & rate limiting, broken function level authorization, API development and security misconfiguration. This research also examines Taiwan's financial consumer protection and personal information protection regulations, and the EU's General Data Protection Regulation (GDPR), providing short-term, medium-term and long-term open banking policy suggestions. In the short term, this research suggests maintaining the self-discipline model of open banking policy, and use self-discipline standards to regulate TSP companies' information security and data protection level. In the medium term, financial services, including information inquiry, application and transaction, provided by TSP companies should be evaluated. In the long term, it's still necessary to evaluate financial institutions'responsibility to handle customer dispute. In addition, it's also importmant to set cross boundary governance model for the open data trend across several industries.

目　次

圖　目　次

表　目　次

壹、緒論

本章將說明本研究之研究背景、目的、執行進度及研究大綱。第一節為研究背景說明，著重於我國開放銀行政策推動進程；第二節之研究目的，將在開放銀行第三階段「交易面資訊」的方向上，釐清本研究欲探討開放銀行第三階段的資訊安全和消費者保護議題；第三節研究大綱將會就本研究之研究架構、資料蒐集方法和研究流程進行說明。藉由本章之說明，將確立本研究之問題意識和研究規劃。

一、研究背景

新興科技的發展改變傳統銀行的營運模式，影響大眾對金融商品的消費偏好和行為。自 1967 年第一台 ATM 於倫敦問世、展開 Bank 2.0 時代以來，金融服務變革的節奏越來越快；時至 2018 年，Bank 4.0 金融生態系的發展已開始萌芽。傳統銀行業者面對的是一個不同以往的消費生活場景，需要透過新型態的「異業結合」、與第三方服務提供者（Third-Party Services Providers, TSP）合作打造更貼近當代消費者需求的金融服務場景並重塑服務認知（King, 2018；iThome, 2019）。

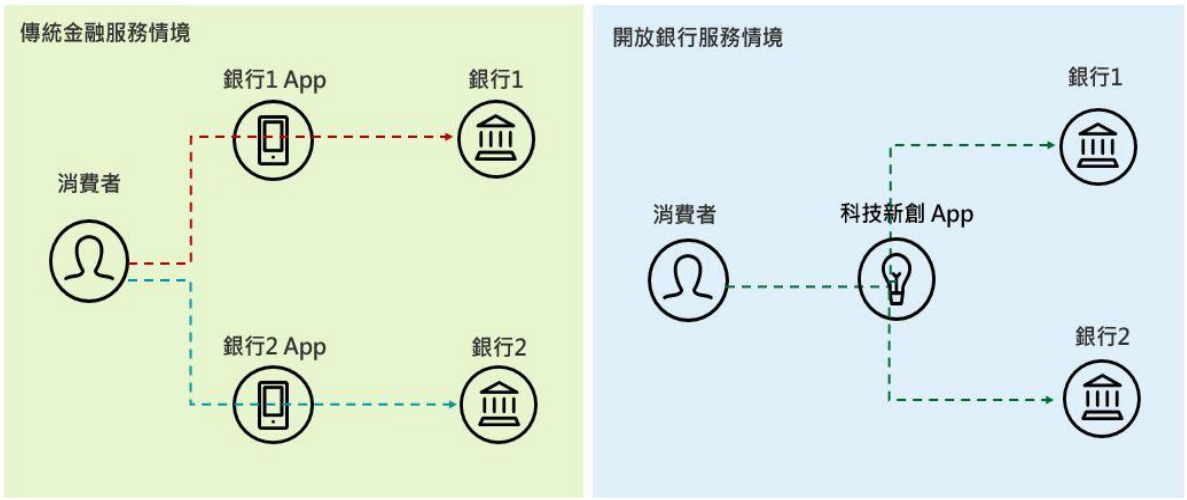

圖 1 傳統金融與開放銀行金融服務流程示意圖

資料來源：本研究整理

開放銀行作為一種因應 Bank 4.0 金融變革的手段，受到各國政府

和專業機構積極研究，認為其可加速金融創新的發展並建立新型態的金融生態圈（王儷玲，2021）。近年，全球金融發展重鎮開始大力推動開放銀行政策。英國與歐盟作為發展先驅，新加坡、香港、澳洲以及臺灣等國家也分別推出符合當地金融產業結構的推動機制與進程。

我國金融監督管理委員會於 2019 年決定推動臺灣開放銀行政策，並採香港、新加坡模式，以「自律作法」來推動開放銀行，即在不修法的前提下，讓金融業者和公會訂定自律規範，鼓勵金融機構基於自身營運策略與業務需求與 TSP 業者合作，加入開放銀行行列。目前第一階段「公開資料查詢」已於 2019 年正式上線運作；「商品公開資料」即利率、匯率、ATM 位置、分行資訊、產品資訊等，TSP 業者透過 API（Application Programming Interface TSP）介接到各銀行的商品資訊，消費者則透過 TSP 業者建置的 App，即可輕鬆比較各銀行的相關商品服務。

2020 年 12 月，金管會核准華銀、元大、中信、兆豐、一銀及國泰世華銀行等六家銀行與集保合作案，以及遠東銀行與遠傳電信等申請合作案，拉開第二階段「消費者資料查詢」之序幕。至於第三階段「交易面資訊查詢」之推動，包括轉帳申請、帳單支付等交易以及申請類服務等，則為本研究欲探討之重點，其後將分別自資訊安全和消費者保護議題進行探討。

表 1 第二階段開放銀行獲金管會核准之合作案

TSP 業者	參與合作銀行	提供客戶服務內容
臺灣集中保管結算所	華銀、元大、中信、兆豐、一銀及國泰世華銀行	查詢客戶在六家銀行的臺幣、外幣活存與定存數額和交易明細等資料
遠傳電信	遠東銀行	查詢客戶在遠東銀行的臺幣、外幣活存與定存數額、交易明

		細等資料和信用卡歷史帳單等資料

資料來源：聯合新聞網，2021

二、研究目的

本委託將以資訊全安和消費者保護為標的，檢視英國、澳洲、歐盟、香港及新加坡等主要國家推動開放銀行涉交易面應用之作法，包括國際標準和監理要求；再針對國際推動開放銀行交易面應用服務之消費者使用情境進行研析。除前述情境展開各類 API 威脅與安控議題，本研究亦將延伸探討 TSP 業者在消費者個資保護、雲端服務、代理登入等關鍵安控領域，並就我國開放銀行第三階段「交易面資訊」提供資訊安全和個資保護之政策建議，以期提高銀行參與開放銀行之誘因，達到消費者便利、金融機構及 TSP 業者互利發展之局面。綜合以上，本研究之問題意識可初步歸納為以下二大項，以及各項次下之子議題：

(一) 開放銀行國際趨勢探討

本研究將分析比較英國、澳洲、歐盟、香港及新加坡等主要國家推動開放銀行涉及交易面之推動現況，包括以下議題：

1. 探討開放銀行交易面應用服務之消費者使用情境與風險
2. 探討開放銀行的 API 安控措施
3. 探討 Partner API 之安控議題和管理建議，其樣態包括金融機構提供 API 予其他業者，及其他業者提供 API 予金融機構等樣態。
4. 探討 TSP 業者在雲端服務、代理登入等其他關鍵安控領域的現況和管理因應，包括消費者透過 TSP 業者向銀行申請業務之種類與範圍、以及 TSP 業者與銀行合作後，是否仍允許代理登入之議題。
5. 探討開放銀行交易面應用服務之消費者保護議題。

(二) 研提開放銀行第三階段之政策建議

由英國、澳洲、歐盟、香港及新加坡等國推動開放銀行作法，探討我國推動開放銀行第三階段「交易面資訊」過程所面臨之資安和消保議題，以及銀行辦理開放銀行之誘因，據以研提誘因機制設計建議。

三、研究方法與範圍

(一) 研究架構

本研究歸納出各國開放銀行推動與發展模式的各項重點，包含開放情境、應用場景以及適用之安控標準等，並規劃就各風險議題議題，包含 API 管理、身份識別、資料安全、系統與網路安全以及第三方風險管理等議題進一步規劃研究，期望探討國際和我國於開放銀行發展和推動之差異，從而對我國開放銀行第三階段交易面應用場景相關安控和消費者保護議題，提出參考和建議。

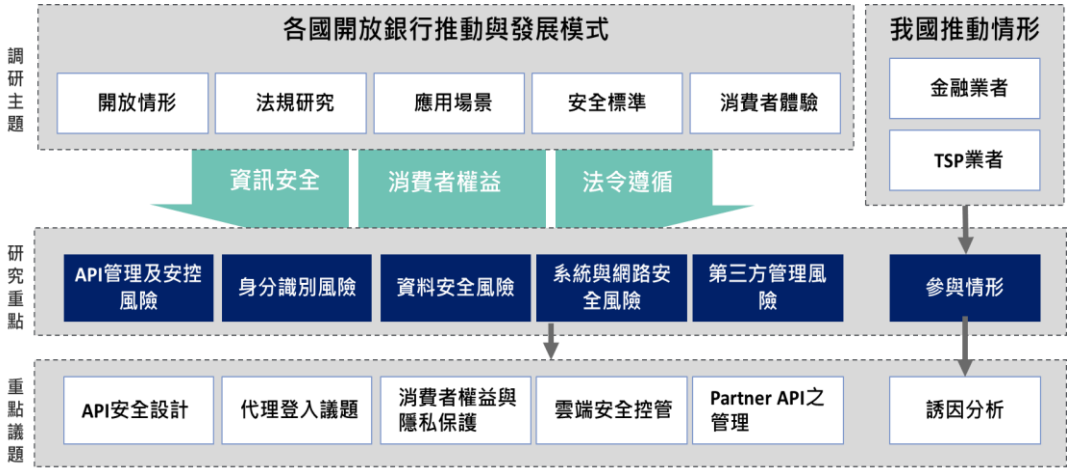

圖 2 開放銀行交易面應用場景重點研究議題

資料來源：本研究整理

根據前述研究背景與目的，本研究就我國推動開放銀行第三階段發展之重點，將分別就開放銀行之國際趨勢、我國開放銀行現況，以及推動開放銀行第三階段發展之相關政策建議等議題，以資

訊安全和消費保護的角度切入進行研析。

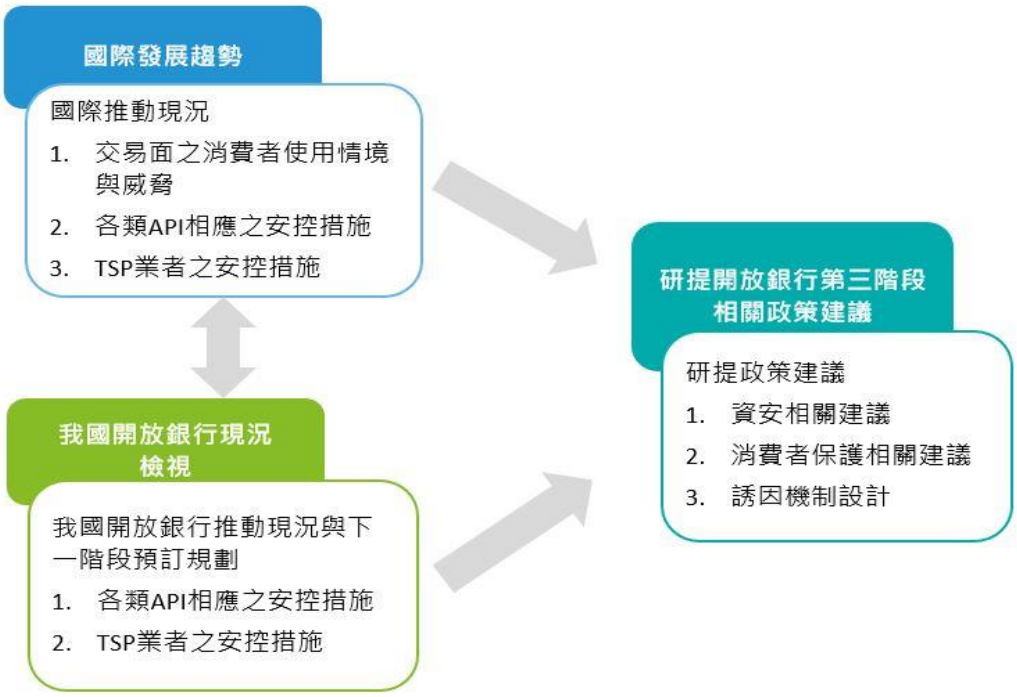

圖 3 研究架構圖

資料來源：本研究整理

(二) 資料蒐集方法與研究流程

本研究以前瞻研究中常見的研究方法蒐集相關資料以深入探討相關研究議題，透過蒐集質性資料的文獻回顧(literature review)與個別深度訪談(interview)等，在訪談過程中搭配進一步的文獻檢視、收斂相關學術與實務界之意見，據以提出開放銀行第三階段政策建議。

表 2 研究設計摘要

研究議題		**資料蒐集方法**	**資料來源/受訪者類別**
開放銀行國際趨勢探	交易面之消費者使用情境	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資

研究議題		資料蒐集 方法	資料來源/ 受訪者類別
討			訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料
	開放銀行之各類 API 相應之安控措施	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料
	TSP 業者在消費者個資保護、雲端服務、代理登入等關鍵安控領域的管理因應	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料
我國開放銀行發展現	我國現行 API 相應之安控措施	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資

研究議題		資料蒐集 方法	資料來源/ 受訪者類別
況	我國現行 TSP 業者在消費者個資保護、雲端服務、代理登入等關鍵安控領域之管理因應	• 文獻回顧法	訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料
研提開放銀行第三階段之政策建議	資安相關建議	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料
	消費者保護建議	• 文獻回顧法	• 中英文期刊資料庫，包括但不限於 Airiti Library 華藝線上圖書館、財金資訊季刊、彰銀資料、Deloitte Insight 等 • 相關產業調查 • 開放銀行相關網路論壇資料 • 開放銀行服務提供者 • 第三方服務提供者
	誘因機制設計	• 文獻回顧法 • 深度訪談法	

資料來源：本研究整理

(三) 個別深度訪談

個別深度訪談之目的主要在於取得實證分析之資料，其進行的方式是研究者透過口頭對話的方式，從受訪者言談中蒐集第一手資訊（陳向明，2002）。訪談目的在於從受訪者的經驗、想法與觀點中，發現有助於研究者發現真相並深入描述事務之本質。訪談大綱除組織背景了解，另分成 Open API 平台參與度調以及研發技術和資安能量等二大主題；如表 3 所示，本研究針對開放銀行誘因機制設計，將採取半開放式訪談進行資料蒐集，依訪談對象之類別準備訪談題綱，再根據訪談狀況進行調整。

表 3 訪綱設計

訪談大綱 / 受訪者類別		銀行業者	TSP 業者
Open API 平台參與度調	有關我國推動開放銀行之政策，以及鼓勵銀行業者參與開放 API 平台，組織抱持的態度為何？	✓	✓
	整體來說，組織參與(或未來規劃參與)開放銀行的誘因為何？	✓	
	整體來說，公司參與(或未來規劃參與)財金公司 Open API 平台的誘因為何？		✓
	對於 Open API，組織傾向加入財金公司的 Open API 平台，或自行開發 Partner API 建立創新生態圈？請說明原因。	✓	
	請問公司傾向下列何種方式與金融機構合作？並請說明原因。 1. 透過加入財金公司的 Open API 平台與金融機構對接		✓

訪談大綱 受訪者類別		銀行業者	TSP 業者
	2. 自行與各金融機構合作，並透過金融機構的的 Partner API，以及加入金融機構的創新生態圈		
	組織是否有透過財金 Open API 平台參與我國 open API 第一階段，或自行開放「公開資料查詢」的 API？請說明有意使用的 API 類型為何？	✓	✓
	呈上題，若組織有參與財金公司 Open API 第一階段，請問其參與的過程與結果，是否有影響(提升/降低)組織進入第二階段「消費者資訊查詢」，或自行開放 API(Partner API)的意願？ 如有，請進一步分享結果與考量的因素。	✓	✓
	組織是否有透過財金 Open API 平台參與我國 open API 第二階段，或自行開放「消費者資訊查詢」的 API？	✓	✓
	呈上題，若組織有參與財金公司 Open API 第二階段，請問其參與的過程與結果，是否有影響(提升/降低)組織進入第三階段「交易面資訊」，或自行開放 API(Partner API)的意願？ 如有，請進一步分享結果與考量的因素。	✓	✓
	組織是否預計透過財金 Open API 平台參與我國 open API 第三階段，或	✓	✓

訪談大綱 受訪者類別		銀行業者	TSP 業者
	預計自行開放「交易面資訊」的 API？		
	呈上題，若未預計參與第三階段，請與我們分享組織的考量因素為何？	✓	✓
	組織目前已開放的 API 數量為何？	✓	
	公司目前已串接的 API 數量為何？		✓
	公司目前希望金融機構能開放串接的 API 類型為何？(包含透過財金 open API 平台或金融機構自行開放的 Partner API)		✓
	組織是否預計於近期(3 年內)自行發展組織本身的開放銀行生態圈，並預計開放更多組織的 API 以達到更多異業合作？	✓	
研發技術與資安能量	請問與組織合作的 TSP 業者是否有使用雲端服務？(不包含銀行自己本身使用的雲端服務)？請問 TSP 是使用 IaaS、PaaS 或 SaaS 服務?	✓	
	是否有要求 TSP 業者對雲端服務提供商負擔監督管理責任，並已導入合適的安控機制？如有，請說明相關安控機制。	✓	
	有關組織提供 TSP 業者消費者的個資時，針對下列項目目前組織是否已導入合適的安控機制？ 1. 身份驗證與授權管理 2. 數位身份識別	✓	

訪談大綱 / 受訪者類別		銀行業者	TSP 業者
	3. 訊息正確性 4. 威脅防護準備		
	現行組織是否有與 TSP 業者合作以代理登入方式提供消費者金融服務？	✓	

資料來源：本研究整理

貳、開放銀行交易面應用服務之消費者使用情境與風險分析

本章將就開放銀行的全球發展趨勢進行探討，根據文獻檢閱成果梳理出當前開放銀行各類應用場景的消費者使用情境，以及國內針對各應用情境衍生威脅之監理措施因應。第一節將說明開放銀行的全球發展趨勢；第二節將釐清開放銀行的界定與範疇；第三節將探討開放銀行下的 API 運用；第四節將探討開放銀行交易面應用服務之消費者使用情境，並以 OWASP API 安控十大風險展開分析架構，作為後續精進我國開放銀行第三階段 API 安控規範之建議基礎。

一、國際發展趨勢

開放銀行的發展始於歐洲。鑑於英國九大銀行長期壟斷金融市場，金融創新的腳步停滯、競爭力不足的問題，英國政府甫於 2015 年起開始規劃、制定通用 API（Application Programming Interface，應用程式介面）共同標準，要求英國九大銀行必須透過開放 API（Open API），將顧客資料授權給非銀行之第三方服務業者（Third Service Providers，以下簡稱 TSP 業者）以活化國內金融市場並降低提供金融服務的新創業者進入市場門檻。同年，歐洲議會也通過「第 2 號支付服務指令」（Payment Service Directive 2, PSD2）要求歐盟各銀行在 2018 年 1 月前將 PSD2 納入法規中，成為歐盟推動開放銀行的法律基礎。

根據 Allied Market Research 於 2020 年出版之報告，全球開放銀行市場規模為至 2026 年會成長至 431.5 億美元的規模，總計 2019 年至 2026 年之複合年增長率為 24.4%。此外，各國政府推動開放銀行的治理模式也逐漸分成市場機制或國家監理導向等兩種類別（Economist Intelligence Unit, 2020）。而英國被作為開放銀行的領跑國家，其競爭及市場管理局（Competition and Markets Authority，以下簡稱 CMA） 於 2016 年率先決定採取強制的開放銀行政策，要求英國前 9 大銀行建立並採用統一的開放銀行 API 共同標準，強制銀行將顧客資料透過這套開放 API 提供給授權的 TSP 業者使用，打破了金融數據資料長期集中

於大型金融業者的局面。此後，歐盟各國開放銀行的發展，也在 PSD2 的法律基礎上陸續要求歐盟各國銀行開放其金融數據。對比較偏向市場機制導向模式的美國，其開放銀行規範主要依循市場機制。美國消費者金融保護局（Consumer Financial Protection Bureau）於 2017 頒布《消費者保護原則：消費者授權之金融數據共享與整合》報告，其開放銀行運作模式是交由銀行以及 TSP 業者自行決定，而亞太各國的開放銀行發展，則普遍處於初始階段。

截至目前為止，亞太地區國家開放銀行的相關規範與試行，仍以國家政策鼓勵為主要發展動能。例如，新加坡與香港政府皆已發表供銀行及 TSP 業者參考的指引文件。新加坡金融管理局（MAS, 2021）和新加坡銀行協會（ABS）共同發布「金融即服務 API 手冊」（Financial as a service API playbook），此規範並未強制銀行開放資料，而是訂定了 API 治理框架讓銀行和 TSP 業者各自依照合作需求，建立以契約規範為基礎的開放銀行推動模式，以期提升銀行業者與 TSP 業者參與開放銀行之意願。

綜合上述，目前各國開放銀行採用之推動模式大致可分為以下三類：法令強制、政策鼓勵、市場驅動。此三類推動模式各有其代表國家，而不同推動模式也已為各國開放銀行之開展帶來相異優劣勢（見下圖）。

推動模式	法令強制	政策鼓勵	市場驅動
國家	英國、歐盟、澳洲、加拿大、日本	香港、新加坡、台灣、紐西蘭等	美國、中國
優點	● 有相關法令規範可強制推動政策 ● 提供必要註冊機制立認證規範 ● 鼓勵TSP業者加入此生態系	● 大多以週邊單位推動，執行較有彈性 ● 規格可以依該地區想推動的場景來設計	● 彈性最大，依市場需求可以設計各種不同情境應用
缺點	● 無法針對市場快速推出必要的API，僅針對共通項目規範	● 因採自願性質，規模大的金融機構有資源整合，而中小型金融機構較不易，會有市場競爭不平狀況	● 因為市場推動，初期推動速度會較快；但後期可能會有多家規格競爭，整合不易

圖 4　開放銀行三大推動模式

資料來源：王儷玲（2021）

針對銀行業者開放銀行之發展，數位交易顧問公司 INNOPAY 亦於 2020 年 5 月提出開放銀行發展監測指標《INNOPAY Open Banking Monitor》針對世界 300 多家銀行，以 API 功能範疇和 API 開發人員使用體驗作為標準，其將參與開放銀行的金融業者分為四類（請見圖 4 的四個象限）。在兼顧二項評比標準的第一象限「專業開放」（Masters in Openness）領域，共 11 間銀行上榜，其中 6 間為歐洲銀行：BBVA（西班牙外換銀行）、bunq（荷蘭網銀）、Deutsche Bank（德國德意志銀行）、DNB（挪威銀行）、Erste Bank（奧地利第一儲蓄銀行）、NBG（希臘國家銀行）；3 間為亞洲銀行：DBS（新加坡星展銀行）、Kuveyt Turk（土耳其銀行）、UnionBank（菲律賓聯合銀行）；2 間為美國銀行：Citibank（美國花旗銀行）、Federal Bank（美國聯邦銀行）。在 API 功能範疇上以亞洲銀行表現較佳，在開發者使用體驗上則由歐美銀行領先。

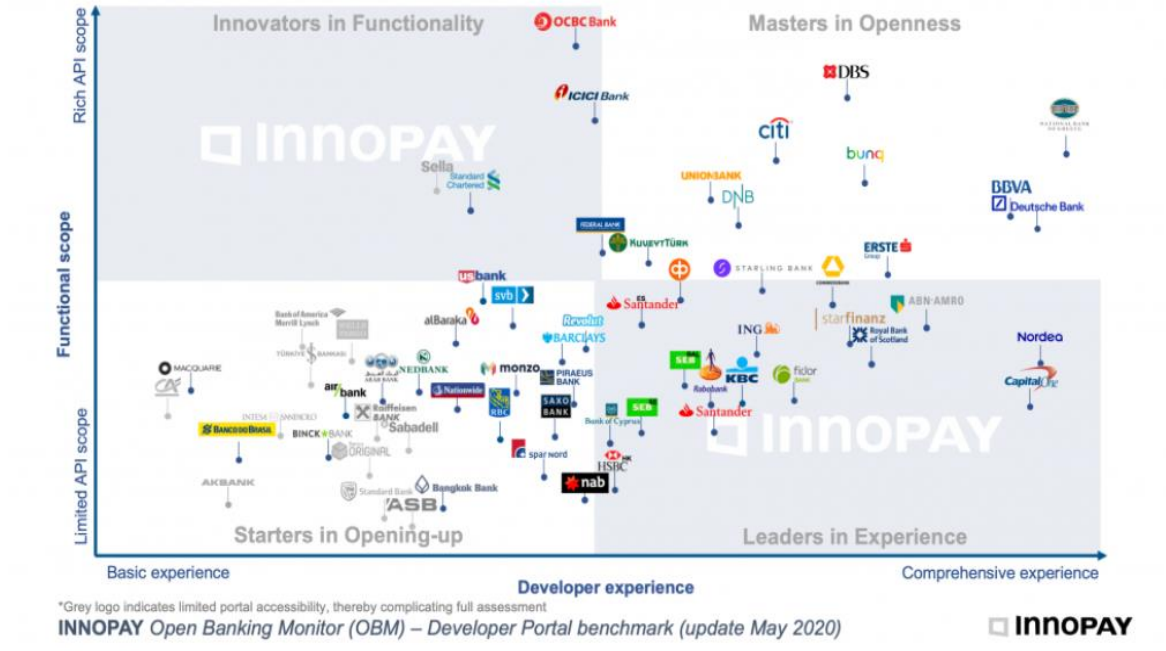

Figure 1: The INNOPAY Open Banking Monitor (updated May 2020)

圖 5 Open Banking Monitor

資料來源：Innopay, 2020

二、開放銀行的定義和範疇

根據英國開放銀行執行組織（Open Banking Implementation Entity ,OBIE）的定義，開放銀行是「一種讓一般用戶與企業，透過利用自身交易所產生之數據資料，獲取優化之金融商品與服務。」在開放銀行此一新興產業生態，金融機構與金融科技業者，唯有取得使用者同意，才能使用其數據資料。」歐洲銀行協會開放銀行工作小組綜合產業和學術界意見後則指出，開放銀行是一隸屬於金融科技領域的金融服務，涵蓋以下行動：

1. 使用開放 API，讓第三方開發者能夠圍繞金融機構構建應用程序和服務。
2. 藉由數據應用，為金融帳戶持有人提供更透明的財務透明選擇。
3. 使用開源技術實現以上目的。

過往，消費者在銀行留下的交易資訊通常會很直觀地被界定為銀行的資產。開放銀行則將銀行交易資訊的主導權交還給消費者，讓消費者能夠自行決定是否開放個人交易資訊給其他銀行或是非銀行的第三方服務機構；而銀行和其他第三方服務業者在取得消費者同意後，可藉由應用程式介面(Application Programming Interface，以下簡稱 API) 共享消費者的金融數據，並在金融數據的基礎上建置應用程式，為消費者提供更靈活多樣的金融創新服務（2018，陳英慧）；此外，開放銀行亦能促進銀行與金融科技公司的合作與競爭，最終達到客戶利益極大化的目標（2021，王儷玲）。

進一步言之，開放銀行的目的在於透過還給消費者資料自主權，促進金融市場行為主體之間的競爭與互補，催生創新的產品與服務並提升客戶體驗與消費者福祉（2019，臧正運）。與傳統金融服務的樣態相比，推動開放銀行將能為一般消費者、企業客戶與整體金融產業帶來以

下效益（2021，Deloitte India）：

1. 以消費者為中心的服務

透過即時的分析消費者的金融資料，開放銀行具有提升使用者體驗的潛力，並促進「以消費者為中心」的商業模式，在適當的時機提供量身定制的金融產品/服務。

2. 提高營運效益

金融資料的共享將提高產品定價的透明度，金融機構將可依據其制定更明智的決策，並藉此提高金融機構提供金融服務的效率。

3. 提升金融機構盈利能力

開放 API 提供金融機構「隨插即用」的創新營運模式(plug and play model)，金融機構除可以較低的營運成本提供全方位的服務，並提升獲利，金融機構亦可透過有效的資料利用提高產品和服務的市場滲透率。

4. 提高協同能力

開放銀行把所有銀行資料整合到一個應用程式(APP)中，使用者(消費者)只需登錄一次即可查看、編輯和控制他們的所有帳戶。同時該 APP 也可融合其他服務，例如用餐卡餘額、航班和飯店資訊。

三、開放銀行下的 API 應用

開放銀行的本質是銀行數據的共享，用以回應日益激烈競爭環境和客戶期望；在此背景下，應用程式介面（Application Programming Interface, API）扮演了數位發展黏著劑（Digital glue）的角色，其功能為在金融服務提供者和消費者之間介接資料與服務，為金融創新帶來更多的可能（Rogier, 2019；Lees,2019）。承上，開放銀行中的開放意涵，即在資料共享所涉之 API 技術上點對點對接規格，故討論開放銀行 API

應用時，將討論到一家銀行跟數家 TSP 業者串接資訊的情境，若 API 規格未能一致，將導致銀行業者建置成本大增，影響其參與開放銀行的意願；因此，我國開放銀行推動的進程，現階段係由金管會責成財金公司建置 Open API 平台來因應，API 開放範圍則以帳戶（Account）為主，下一階段之目標則為支付（Payment）領域。

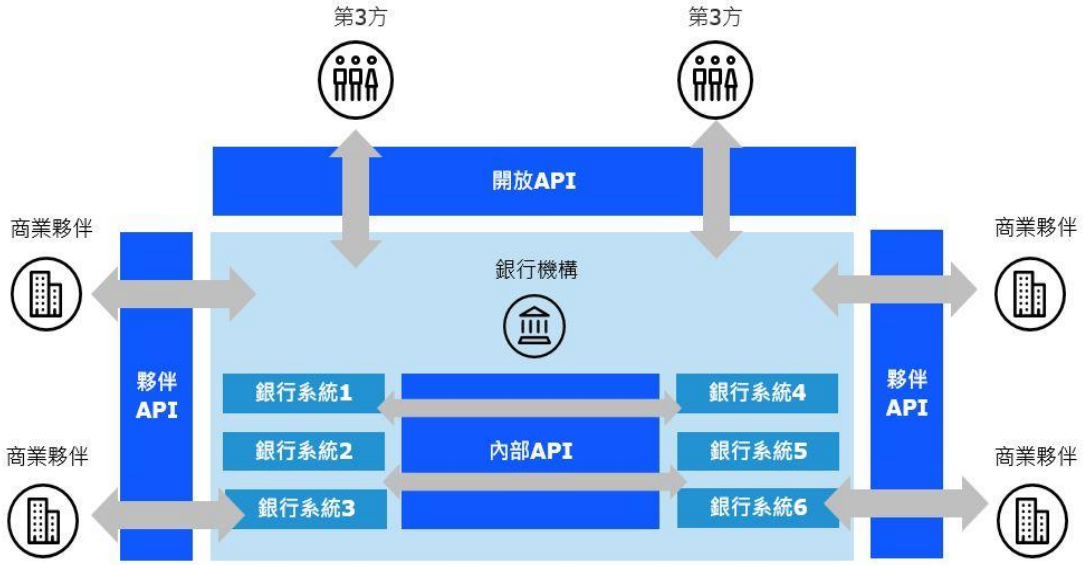

圖 6 開放銀行適用 API 類型示意圖

資料來源：Trend Micro, 2019

開放銀行下的 API 應用類型可以分為三類，即內部 API （Private API）、合作夥伴 API（Partner API）以及開放 API（Public/Open API）。內部 API 通常僅供企業內部開發者使用，透過少量對接公開數據、業務流程和應用程式功能，適合不願意公開數據和應用程式的企業。夥伴 API 主要用於機構對機構之間的商業模式（Business to Business, B2B）如金融同業間資料交換的標準，其通常是根據業務協議授權，對於規模較小的合作夥伴而言具備較大吸引力。開放 API 則用於對組織之外公開應用程式功能，主要提供外部合作夥伴、第三方開發者使用，較前兩類 API 開放程度更深、合作層面更廣，為開放銀行領域廣泛採用。金融機構普遍依據共享數據的資料敏感程度，選擇合適的類型進行分層管理。

根據 McKinsey 定義，企業開發之 API 類型可分為以下三類：

(一) 內部 API（Private API）

內部 API 是企業只開放給組織內部開發者或特定使用者使用之 API，透過該 API 得以存取企業後端資訊或應用程式。透過內部 API 可使得內部開發者共享公司內資源，加快開發速度（2020，洪國峻、蕭培均）。對金融機構而言，內部 API 是指銀行內部系統間的 API，用以促進業務系統間的資訊互通，僅供銀行內部使用。（2021，王儷玲）。根據 Mckinsey （2019）的統計，共有 91%的 API 屬於此類型。

(二) 合作夥伴 API（Partner API）

合作夥伴 API 是開放和私有介面模型的混合形式，其允許外部公司存取可以增強其既有或創新產品和服務的資料，並有效簡化程式設計和實現 API 的過程。對金融機構而言，合作夥伴 API 是由銀行與特定合作夥伴制訂，其目標為支援特定之業務流程或產品（2021，王儷玲）。不過根據 Mckinsey 的統計，只有 7%的 API 屬於此類型，且多數主要是因為 PSD2 的要求。

近幾年因應金融科技、Open Banking 及 Open Data 的產業發展趨勢，才開始透過 Open API 將金融資料釋放出來。透過這種開放式的「隨插即用 API 網路」(plug-and-play application network)，企業可更高效的運用並提供差異化的消費者體驗。

(三) 公開 API（Public/Open API）

公開 API 也是我們目前常見的 API 類型，意即將 API 開放給外部或內部的人員輕鬆的串接使用。一個開放的 API 發布組織通

常會尋求與代理應用開發社群合作，刺激創新應用的開發並為其核心業務增加價值，無需直接投資於開發工作，也可降低開發成本（API Academy, 2015）惟據 Mckinsey (2019) 的統計，只有 2%的 API 屬於此類型。

對金融機構而言，公開 API 是指銀行較前兩類 API （內部 API、合作夥伴 API）更深入且廣泛地向應用方提供標準介面與服務。外部機構可透過公開 API 獲取銀行提供之金融服務。（2021，王儷玲）

四、消費者使用情境

根據資策會（2019）研究，全球開放銀行的開放 API 比重以帳戶資訊（32.9%）以及支付轉帳（28.7%）為主，其次則為交易（18.2%）、借貸融資（7%）、投資（6.3%）、外匯交易（4.2%）及保險（2.8%）。由此觀察，除了帳戶資訊、支付和交易資訊外，徵信也成為開放銀行應用的發展重點，而證券和保險之開放銀行市場，亦有發展潛力。

目前我國開放銀行之進程，API 開放範圍主要是以「公開資料」和「消費者資訊查詢」為主，涉及議題涵蓋客戶資料所有權、消費者個資保護、顧客權益保障、爭議處理機制及第三方服務提供者管理方式等。本研究綜合各國推動開放銀行典範案例，並整合英國 FCA Open Call For Input: Open Finance 對開放銀行消費者使用情境之示例，將就以下三種消費者使用情境和個案進行分析：

(一) 帳戶類情境

帳戶類情境主要功能為協助彙整消費者理財資訊，提供客戶一站式的理財資訊使用體驗，該類型 API 應用場景可大致分為以下幾類：

1. 個人理財管理 (Personal Finance Management, PFM)

   個人理財管理是開放銀行業務運作最常見的情境，消費者透

過 TSP 業者提供個人理財管理服務，以下為該模式的常見服務情境：

1. 財務訊息彙總

   消費者透過開放銀行將多個帳戶資訊整合至單一瀏覽平台，提高客戶對其財務狀況了解的透明度，也能提升理財顧問了解客戶財務情況的效率。

2. 智能轉帳管理

   智能轉帳管理搭配前述情境，提出替代產品建議或協助到切換替代產品以及帳戶之間轉換，協助消費者作出滿意的決策，例如如何在現金間分配儲蓄，或協助消費者自動化處理其規律性轉帳活動。

3. 貸款評估、信用評等類型

   銀行或放貸機構可以在消費者同意的前提下，可調閱其金融或信評資料，改善了處理流程的效率，提升信貸機構對消費者資格審核效率。

■ 案例研析：英國租屋信用紀錄平台 CreditLadder

1. 營運模式

在個人理財管理情境，本研究將以英國租屋信用紀錄平台 CreditLadder 為例說明開放銀行應用場景。CreditLadder 於 2016 年開始運行，其與國際消費者信用資訊巨頭 Experian、EQUIFAX 合作，免費提供無信用證明的租戶記錄租金繳納狀況；在租戶的同意下，CreditLadder 在分析其租金繳納狀況後，計算出租戶的個人的信用評分。

CreditLadder 目前已被英國當地 24 家傳統銀行(如 CMA9 家銀行中的 Barclays Bank、HSBC Group、Nationwide、Natwest、Santander)、數位銀行(如 Starling Bank,

Tesco Bank)及純網銀(如 Revolute, Transferwise)等銀行業者認可。若租戶平日按時繳交租金，在有貸款需求時，可授權貸方銀行取得其於平台上的信用證明，以證明其信用可靠性。未來 CreditLadder 亦規畫推出房客的背景確認、租金擔保保險推薦、代收租金、協助追討欠款、租金收取自動通知，以及依租戶或地址管理租金匯款狀況等服務，以鼓勵更多房東加入該平台。

2. 使用技術與 API 類型

CreditLadder 是透過整合 TrueLayer1的 Data API 技術，連接銀行的資訊，其服務應用之 API 功能包含下列五項：

表 4 CreditLadder 使用之 API

序	API 功能	說明
1	帳戶	帳戶持有人姓名，帳號，IBAN 等資訊
2	信用卡	信用卡網路、信用卡後四碼、信用卡姓名等資訊
3	交易資訊	描述、金額、類別、零售商等資訊
4	餘額	現在餘額、可用餘額等資訊
5	定期付款	常規交易與直接支出等定期交易

資料來源：本研究整理

[1] TrueLayer 為歐洲領先的開放銀行平台，目標為建立一個開放的銀行網絡，並整合支付、金融資料和身份驗證。True Layer 現已佔英國、愛爾蘭和西班牙等所有開放銀行逾半數的流量，並處理數十億英鎊的支付交易。Revolut、Trading 212 和 Payoneer 皆有串接 TrueLayer 以提供客戶服務。

3. 申請及支付步驟

(1)輸入詳細資訊: 透過 APP 介面回答身份驗證之簡短問題即可確認消費者的身份。提供消費者的租賃詳細信息，以便將來的租金支付可以提供給信貸機構。

(2) 串接消費者的銀行以進行只有讀功能的存取: 在 FCA 的監管下，CreditLadder 透過與銀行的合作，使用資料加密技術讀取消費者的銀行帳戶資料。

(3) 支付租金: CreditLadder 透過提供的安全存取權限讀取並識別租金支付紀錄。所有租金紀錄將在支付後的 6 週內顯示在 Experian 和 Equifax 法定信用報告中。

(二) 支付類情境

支付類情境即將支付服務內嵌於消費情境，可藉由增進數據蒐集與分析有效提升客戶體驗。開放銀行常見支付場景可大致分為以下情境：

1. 白牌支付系統

   提供無商標的支付系統，提供不同的通路業者使用，這類公司往往專注於技術底層跟串接通路。並交由專屬通路商進行行銷規劃。

2. 支付獎勵引導消費行為

   串聯銀行帳戶和信用卡帳戶進行支付，並以點數、現金回饋等方式鼓勵消費者購買特定商品或服務。常見銀行與特定店家聯盟進行合作。

3. 跨境轉帳

   跨境轉帳付務透過協助消費者跨境無縫進行支付、轉帳和匯款，強化資金流動。

4. 跨通路收款整合

   跨通路收款整合透過整合企業、店家及所有角色，利用

API 串接修改，在各種場景下均可提升其服務體驗。通常這類業者會強調可以輕易插入中小企業現行服務內，協助其金流建置。

案例研析：新加坡提款 APP --SoCash

1. 營運模式

SoCash 是一個協助使用者提款的軟體，幫助其在極難尋找 ATM 的地方以更方便的方式提取現金。SoCash 透過與 DBS、OCBC、ICBC 等銀行的開放 API 平台進行串接，使用者透過 SoCash 驗證銀行帳戶後，將可使用掃描 QRcode 的方式，向中小型商店提取現金。

Socash 於 2018 年 7 月的第一輪的募資活動獲得約 550 萬美金，並於隔年 2019 年 7 月的第二輪的募資活動籌獲約 600 萬美金。截至 2020 年 5 月，SoCash 下載量超過 34 萬次至 2019 年底，已有 1500 家以上的當地中小型商店(如連鎖超市、711 連鎖商店、咖啡店)等成為合作夥伴。目前該 App 使用人口以東南亞人居多，主要建立在該區域銀行分行或是 ATM 設施相對較不普遍之故。消費者可以隨時利用 SoCash 與 Google Map 的介面查詢合作商店，並透過 QR Code 從各個商店直接向店員提取現金。此商業模式不僅增加了消費者提款便利性，也為中小型商家帶來更多元的商機。

另因應 COVID-19 疫情，2021 年時 SoCash 與當地電子錢包業者 Singtel Dash 合作，透過 Singtel Dash 的加值服務，SoCash 協助當地移工透過電子錢包將錢以更安全便捷的方式匯回家鄉。

2. 使用技術與 API 類型：以 SoCash 與 OCBC 的合作為例，其使用之 API 包含下列 10 項項目

表 5 新加坡 SoCash 使用之 API 功能類型

序	API 功能類型
1	Get Regular eNets transaction limit
2	Update Regular eNets transaction limit
3	Authorization
4	Customer Accounts
5	PayNow
6	PayNow QR
7	PayNOW Enquiry
8	PayNow Registration
9	Corporate PayNow Collection
10	Provide Consent
11	Revoke Consent
12	Validate Consent

資料來源：本研究整理

(三) 中小企業相關情境

開放銀行下常見的中小企業情境，多半是基於財務資訊的整合與分析，並對自身及客戶進行進一步的身份認證服務。

1. 帳戶財務彙總

開放銀行可協助企業一站式查詢所有帳戶，讓企業更快速地了解其財務狀況，並協助公司作出財務決策。

2. 自動化會計作業

將財務、會計和審計模式直接連結到中小企業銀行帳戶，在極短的時間內管理會計報表、或填寫相關表單（稅務、商品申請等）。

3. 信評借貸能力

利用開放銀行存取企業的金融資訊，更快地做出精準決策，同時簡化信評、放貸流程，協助中小企業取得放貸或信評需求。

五、Open API 安控風險

開放銀行中的開放意涵，即在資料共享所涉之 API 技術上點對點對接規格，故討論開放銀行 API 應用時，將討論到一家銀行跟數家 TSP 業者串接資訊的情境，若 API 規格未能一致，將導致銀行業者建置成本大增，影響其參與開放銀行的意願；因此，我國開放銀行推動的進程，現階段係由金管會責成財金公司建置 Open API 平台來因應，API 開放範圍則以帳戶（Account）為主，下一階段之目標則為支付（Payment）領域。

開放銀行的發展促使傳統銀行業者突破其原先的封閉運營模式和 IT 基礎設施，並透過向第三方服務提供商(TSP)開放資料的串接，觸及更多消費族群並提供更多元的金融服務。在此發展趨勢之下，歐盟、英國、澳洲、香港、新加坡等發展重鎮以及我國，也透過強制或鼓勵方式推動 Open API，使當地金融業者開放其 API 至統一的 Open API 平台或自建開放銀行生態圈與 TSP 業者建立合作。以英國為例，截至今年 4 月，已有 226 家 TSP 業者通過核准受到 OBIE 的管控。根據 OBIE 於 2020 年的統計 ，發現英國前 9 大銀行(CMA 9)於當年度中的開放銀行活動增長了 2.4 倍，其中絕大多數與資料應用活動有關，另外有關支付相關的活動大幅增長。另一方面，採以鼓勵政策的新加坡則由金管局(MAS)督導銀行開放 API，並透過各銀行自主開放 API 的方式推行產業發展。截至 2020 年新加坡已開放 1,686 支銀行 API 。

為完整分析開放銀行下的 API 風險議題，本研究將以網路安全權威性的非營利基金會於 2019 年開放網路應用程式安全專案（The Open Web Application Security Project，OWASP）發布之 API 十項威脅因素為

基礎，作為後續探討各國 API 安控規範之分析架構。以下將分別釐清 OWASP 發布之 10 項 API 安全風險的內涵：

(一) 無效的對象層級授權 (API1:2019 Broken Object Level Authorization)

攻擊者可透過操作客戶端發送的 Object ID request，進而利用不安全授權的 API，意即客戶端可從 API 存取未經授權的資訊。此一安控問題在 API 的應用程式中非常普遍，攻擊者可以任意存取其他 ID 身份的資料，通常會導致未授權的資訊洩露、資料被竄改或破壞，而造成這種情況的原因，通常是後台權限控管無效而造成資安漏洞。

(二) 無效身份認證 (API2:2019 Broken User Authentication)

由於 API 經常設置為在 Web 或行動應用程式環境中且可不受限制地進行存取，其作業方式為由發出原始請求的使用者設置權限，並將這些權限傳遞給 API。然而，若驗證(Authentication)與 Session 管理之應用程式函式未正確實作，如允許簡易密碼、URL 含有機敏資訊與 Token 未驗證等。攻擊者可繞過使用者身份驗證過程時，API 本身不受限制的存取權限機制將提供駭客進入組織存取所有資料的資安破口，進而危害 API 的整體安全。

(三) 過多資訊洩漏 (API3:2019 Excessive Data Exposure)

開發人員可能因未考量資料的機敏性的情況下，僅依賴客戶端將敏感數據過濾，進而將所有敏感資料暴露。在暴露過多的機敏資料情況下，若沒做好資訊的控管，可能導致使用者能無限制地讀取其個人訊息，惡意攻擊者亦可能透過網路監聽流量進行分析來略過應用程式的過濾與限制，竊取本不應公開的機敏資料與數據。

(四) 缺乏資源與速率限制 (API4:2019 Lack of Resources & Rate

Limiting)

API 常設計用來提供客戶端對 API 發出請求與查詢回傳資料，但往往未對 API 資源大小、請求數量進行任何速率或資源的限制，可能導致消耗大量網路、CPU、記憶體和儲存空間。一般來說，使用者輸入和業務邏輯決定了請求所需的資源量。若管控不當，API 可能會發布過多封包而造成服務停擺。攻擊者利用這些問題造成阻斷服務攻擊 (DoS) 和相關端點中斷，影響 API 服務器的性能。

(五) 無效功能權限控管 (API5:2019 Broken Function Level Authorization)

組織應針對不同層次結構、角色的存取權限進行嚴格控管與驗證，明確制定哪個角色可以執行哪些功能。否則在管理功能、常規功能難以區分的模糊灰色地帶時，攻擊者可能將 API 請求發送到他們不應該存取的其他用戶資源，從而取得未經授權的功能，例如增添、更新或刪除客戶紀錄或甚至接管整個服務的控制權。例如，當程式開發者急著上線時因疏於設定網站資料夾的權限控管，駭客可透過該項弱點進行路徑暴力猜測破解以取得存取權限，進而得知程式或整體系統架構，進一步攻擊取得系統的管理權限，並持續尋找其他目標以進行攻擊與橫向擴散。

(六) 批量配置不當 (API6:2019 Mass Assignment)

為降低開發時間成本並提高生產力，大多數現代的網頁程式框架具備支援自動將使用者輸入內容與物件的內部變數綁定的功能，然而若未做適當的過濾，如建立相關 API 參數的白名單、黑名單機制，亦可能有安控疑慮。一般而言，使用者應該能夠更新他的名稱、聯絡資料或其他個人資料，但他們無法更改權限，如調整帳號餘額或操作類似於管理者權限的功能。但如果 API 端點自動將用戶端輸入的內容轉換為內部物件屬性，卻不考慮這些屬性的敏感度和可暴露度等級，該 API 端點就很容易遭到惡意的攻擊，

這將使得攻擊者可以非法更新不應該存取的內容、惡意竄改資料或導致安全機制遭受繞行的風險，若不了解 API 對應邏輯關係，也可能出現整個網站被竊取的危機。

(七) 不安全的組態設定 (API7:2019 Security Misconfiguration)

隨著越來越多的應用程式相互串接，開發人員的壓力也日益提升，其必須因應更複雜的 API 安控狀況。例如，在程式設計的源頭上出現的組態設定安全漏洞，以及在通訊協定、請求方式、請求參數、版本過舊等情形，導致如身份認證、越權漏洞等安控問題出現。不法分子可以利用這些 API 漏洞竊取使用者資訊與企業的核心資料，包含在開發過程中使用非 POST 請求方式、開發環境與正式環境重疊、Cookie 傳輸密碼、格式錯誤而產生的威脅、資料未確實去識別化等。為確保整體安全，銀行與 TSP 間應依據開放標準約定，在開發、部署 API 的整套生命週期中共同遵守 API 設計標準，並對於弱點處進行強化控管，以降低 API 不安全的組態設定可能性。

(八) 注入攻擊 (API8:2019 Injection)

注入攻擊發生於不信任之資料傳輸，內容可包含部分指令(Command)或資料庫查詢(Query)語法，攻擊者將惡意程式碼注入易受攻擊的軟體中，將異常資料寫入資料庫、擷取機敏資料或更改執行軟體的方式。一般常見的注入攻擊為 SQL、NoSQL、OS 指令、物件關係對映 (ORM)、LDAP 等，主因通常是因為沒有經過妥善的檢查、排除符號等造成的弱點風險。如此將會提高服務解釋錯誤或讓竊取者獲得未經授權的資料庫存取權限，進而發生作業系統漏洞，執行系統指令，甚至讓主機被竊取者接管等安控問題出現的機率，帶來資料遭竊、丟失、損壞或阻斷服務等負面影響。

(九) 版本控管不當 (API9:2019 Improper Assets Management)

版本控管不當往往會淪為攻擊者破壞系統的方法之一，雖然目前許多組織採用 DevOps、雲端化應用等多重部屬，若尚未修復與更新的舊版本或測試的 API，因版本控管與維護不當，可能會遭受攻擊者藉機以舊版本 API 做為侵入點，進而存取敏感數據或連接到尚未修復的舊版 API 接管整個伺服器。

(十) 紀錄與監控不足 (API10:2019 Insufficient Logging & Monitoring)

根據研究與統計指出，駭客潛伏到發動攻擊超過 200 天，若記錄日誌和監視有所欠缺或不足，如未記錄可稽核的事件，包含登入成功與失敗、未產生告警和錯誤，日誌檔資訊不足或不明確、未透過應用系統產生日誌檔來監控可疑的活動等，幾乎無法追蹤 API 的可疑活動並及時做出反應，讓駭客得以長期潛伏，使攻擊者有足夠的時間攻擊、篡改、存取、破壞系統並且竊取資料。

參、開放銀行交易面應用服務之 API 安控議題探討

根據全球領先的網路安全和應用交付解決方案提供商 Radware 在最近一次的研究報告《2020-2021 State of Web Application Security Report》[2]中指出，有鑑於人們越來越依賴透過 API 支援的 Web 應用程序，API 逐漸被濫用處理各種敏感資料(如用戶憑證、支付資訊、社會安全碼等)。而這將導致 API 成為最常見的攻擊媒介。事實上，根據 Radware 的統計，近 40% 的受訪組織表示，他們的應用程式中有一半以上透過 API 暴露於網際網路或第三方服務、大約 55% 的企業至少每月經歷一次針對其 API 的 DoS 攻擊、49% 的企業至少每月經歷某種形式的注入攻擊，42% 的企業至少每月經歷一次元素/屬性操縱。Radware 指出，API 安全是企業在 2021 年應該修補的最關鍵的漏洞。

本章節將分別針對開放銀行下的 Open API 資料安全風險、Partner API 的管理模式、開放銀行之國際監理策略、開放銀行之交易面應用服務 API 類型、重點市場對於開放 API 安控相關法令法規等議題進行探討，並以第貳章之 OWASP 十大 API 風險分析架構為基準，進行各國 API 安控規範比較分析。

一、Open API 資料安全風險

為確保消費者資訊介接金融創新服務運作過程的安全，銀行與 TSP 業者間，應依據開放標準約定共同遵守的 API 設計標準，防範如格式錯誤的 XML 威脅、JSON 威脅和惡意腳本注入威脅等攻擊行為；簡言之，Open API 不只包括了「公開的 API」，同時需考量特定合作夥伴間、特定成員間，利用這些以開放標準訂定的 API 來串接行為安全管理議題。根據政治大學金融科技研究中心於 2019 年提出的研究，Open API 必須審慎考量到消費者資料介接後的在 Open API 應用個階段身份辨識與權限控管的問題，包含數位身份授權、資訊正確性維護與威脅偵測機制等環節。

[2] https://www.radware.com/newsevents/pressreleases/2021/api-abuse-threat-bot-traffic

(一) 身份驗證與授權管理

開放 API 架構設計的共通性規範係是參考國際標準 Open API Specification（OAS）建立，在 OAS 規範的 RESTful APIs 定義下，API 互通介面不受程式語言限定，除可跟產業或政府單位進行更多元的開放資料介接，也可朝向我國開放銀行 Open API 與接軌國際的目標。惟使用 API 的系統數量繁多，意味著每天必須進行數以萬計的連接和數百萬次操作的身份驗證和存取特權管理作業。在這些應用程序平台中，大量有價值的交易資料也成為犯罪、駭客行為、間諜活動等威脅行動覬覦的目標。

(二) 數位身份識別

透過 API 進行開放銀行交易面應用服務時，網路安全基礎設施保護的重要性也日益受到重視，而使用 API 金鑰進行應用身份驗證也成為未來趨勢所在。為因應跨平台的身份識別之挑戰，數位身份驗證、授權管理與身份追蹤機制是確保消費者資料及交易之安全之重要關鍵，如 OAuth 2.0 的身份驗證機制，可限制應用存取其允許的資源，更關注使用者終端設備的安全防護，以及註冊和交易時的身份與授權驗證機制等，所採用的手段包含確實對使用者說明資料使用之機構、範圍、管控，以及資料授權及拒絕等權利行使方式，並取得客戶的同意。

OAuth 2.0 身份驗證機制為目前國際間慣用讓 TSP 業者來存取客戶資料的做法。因授權委任存取涉及的利益相關者包含第三放業者、銀行與消費者，管理流程極為複雜，使用者存取過程中，駭客可能透過預先取得授權碼(Auth code)的方式，在使用者登入 TSP 業者的網站服務時，以釣魚方式讓使用者代為登入，駭客得以藉使用者取得存取金鑰（Access Token），再以存取的金鑰冒充使用者操作，來取得使用者的資料甚至存款。在駭客與使用者存取控制行為均被判定為為合法使用者的狀況下，企業並不容易偵測出

來。因此，這類資安議題牽涉業者難以管控的用戶端，使用者在資訊素養的欠缺和使用行為疏失，包括社交工程、ATP 等攻擊手法皆對使用者乃至銀行和 TSP 業者端帶來巨大威脅。對此，企業在管理自家 API 時需要有更嚴謹的做法。

(三) 訊息正確性

設計安全的 API 架構，是做好安全防護的最重要議題。目前一般均透過認證後發放 Token，各 API 再藉由驗證 Token 來辨識呼叫 API 的使用者端身份，並確認使用者端是否有呼叫此 API 的權限以為管控。為確保資料內容未有被竄改以及 Token 沒有有被第三方冒用，相關研究皆建議採用不易被破解的加密協定與雜湊函數，例如我國現行自律規範要求須採用 TLS 1.2 以上加密通訊協定確保訊息之正確性及完整性。因此，傳輸層的加密是邁向安全 API 的第一步。 若不使用適當的傳輸安全性協定，將提升竊聽者讀取和篡改數據的機會。

(四) 第三方服務供應商安全管理

在第三方服務供應商安全管理議題，透過銀行與 TSP 業者異業結合，提供能更精準滿足消費者需求的創新的金融服務。達到消費者、金融機構、TSP 業者三贏的局面，但回到其資訊安全議題的探討，所有的金融創新都應是「負責任地創新」，應對消費者負起資訊安全與隱私保護的責任。

目前我國銀行公會所訂的自律規範中，已列出了銀行對合作的 TSP 業者的遴選原則及應遵守事項，故銀行對 TSP 業者，現有管控方式為以合約條款進行約束。參照香港開放 API 框架要求銀行應對於 TSP 業者需進行風險評估與盡職調查等。但若 TSP 業者無充足的資源可投注在資安的防護機制，可能會對本身平台保留的資料缺乏適當的保護，在此情況下與合作銀行間的 API 介接，

將增加駭客進入後台伺服器竊取機敏資料的機會；利用網路服務科技為基礎所架設的網路平台，也可能遭到駭客 DDoS 攻擊，對業務或營運產生重大的影響。在迎向金融創新的無限可能性之前，更重要的是得先了解銀行業在 TSP 業者資訊安全管理議題將面臨的各類風險，並預備風險因應措施。

(五) 威脅防護議題

網路犯罪的攻擊具有針對性及持續性，使用先進的惡意軟體並搭配專門設計用來偽裝成網路上合法使用者，以致監控上的困難。這些攻擊手法可很輕鬆躲過防火牆、入侵偵測系統及防毒軟體等預防性安全技術，而潛藏在內部網路中的惡意軟體，讓駭客得以染指企業寶貴的智慧財產、商業機密或客戶資料，增加企業風險。因此，如何防範與日漸增的網路犯罪事件，並持續強化開放銀行 OpenAPI 平台之網路安全，以保護消費者避免遭受個資及隱私之威脅，將是未來須持續關注之課題。

二、Partner API 管理模式研析

承續第二段一開始的分析，API 分為三個種類，包含內部 API、夥伴 API、公開 API，其中只有後兩者會將內部資料拋送至外部單位。透過分析各國推動開放銀行政策推動模式可知，在推動開放 API（Open API）的過程中，強制推行的國家其策略通常是針對開放 API 制定法令法規著手，而鼓勵策略者則是訂定自律規範鼓勵並引導業者參與。

(一) Partner API 國際管理趨勢以導向委外管理為主

針對合作夥伴 API（Partner API）的管控多數國家並未在推動開放銀行的過程中強調著墨，只有新加坡 Playbook 中有提到依據金融機構是否擁有合作後的使用者經驗，分成兩種模式進行管控。其他國家的治理方向傾向以開放 API(Open API)為主，針對 Partner API 則傾向導向以委外合作的方式或其他相關業務規範進行管控。

考量銀行過去已有許多不同的業務已透過 Partner API 跟第三方單位合作並行之有年，我國目前未對 Partner API 另外進行修規、而是採以委外合作的式進行控管，尚屬合理。

研究團隊也透過與各銀行之訪談，了解傳統的銀行業務中，如信用卡收單與電子支付服務皆是透過 API 與廠商進行合作，對應 Mickinsey 的定義則屬於 Partner API 的範疇。但因各業務已有各自的業務法令法規(如電子支付機構資訊系統標準及安全控管作業基準辦法)或甚至國際規範(如 PCI DSS)，其不論是對於訊息防護措施、機敏資料隱密、加解密演算法與身份認證等，可能皆不亞於或甚至勝過 Open API 的管理規範要求。另外考量 Open API 與 Partner API 使用產業及業者規模有所不同，如要制定一份統一的 Partner API 規範並適用所有銀行的 Partner API 業務，恐工程浩大且實務執行上會加重銀行業者的負擔。

(二) 透過 Partner API 的創新合作恐無法可管

然而隨著 Open API 的推動，Partner API 的關係已不再僅限於傳統金融業務，許多銀行業者也開始透過 Partner API 自行與 TSP 業者洽談創新合作業務。但這些創新合作業務，不像傳統金融業務已有完整的管理框架，也不在 Open API 的管控範圍內；銀行與第三方業者僅需遵循雙方所簽訂之契約內容，而無需遵循開放應用程式介面業務安全控管作業規範。這可能使消費者的個人資料在透過 Partner API 傳遞時，因雙方無嚴謹的規範而造成個資外洩的風險。

(三) Partner API 管控方針建議

有鑑於 Partner API 的範圍較廣，且部分業務現已有明確、完整的規範要求，研究團隊建議可目標納管的 Partner API 範圍進行縮限，並專注在高風險的 Partner API 管控上。

(四) 是否涉及消費者個人資料

銀行與第三方業者使用之 API 如無涉及消費者的個人資料，則該些資料相較之下對組織風險影響較低。建議導向以委外方式進行合作，交由銀行與第三方業者自行判斷與決議應遵循的事項或規範，避免雙方投入過多的資源於低風險且未涉及消費者個資的事項而限制彼此發展。

(五) 是否已有控管規範

1. 已有相關法規規範

   如該業務已訂定相關法規，且對 API 的安全控管強度不亞於目前 Open API 的安全控管作業規範要求，則建議依循現有規範進行管理。

2. 無外部規範或相關法規

   鑒於 API 只是一套傳輸資料的工具，不論是 Open API 或 Partner API，其面臨的風險相當近似，差異僅為參與的主體複雜性。若銀行與第三方業者所使用之 API 涉及消費者個人資料的處理和利用，且該業務目前無外部規範或法規訂定，本研究建議先評估以修訂既有規範、擴大適用範圍的方式進行調整，將 Partner API 視同 Open API 進行控管，以降低目前 Partner API 因未受外部規範或相關法規控管所帶來的風險。

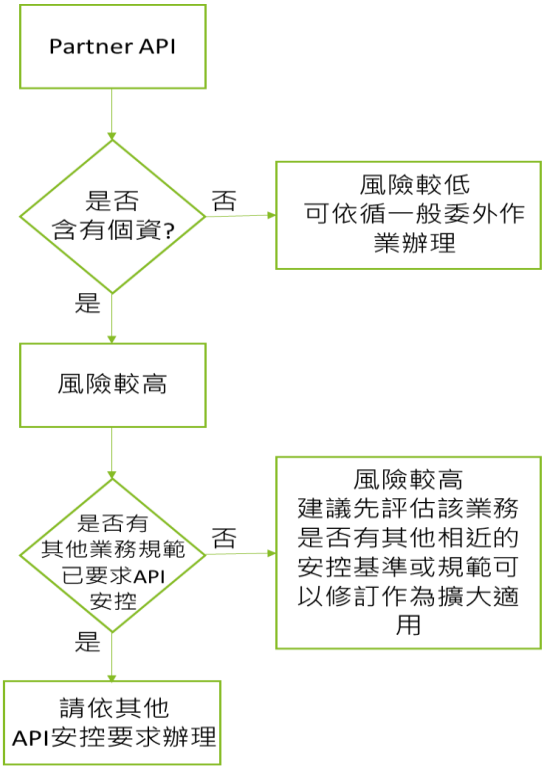

圖 7　Partner API 納管流程

資料來源：本研究整理

三、開放銀行之交易面應用服務 API 類型

本節將針對英國、歐盟、新加坡與澳洲開放之 API 類型進行整理，並根據其資料開放之性質，對應之我國開放銀行發展的規劃階段，就交易面服務 API 之應用，尋求 API 安控之治理模式之參考依據。英國 CMA 目前 Open API 類型係以唯獨資料和可讀寫資料為主；歐盟則以帳戶資訊服務和支付發起服務為主；澳洲開放銀行政策針對其類型，現行規範係以產品參考資料、信用卡、金融卡、存款帳戶以及交易資料以及抵押帳戶資料以及個人信貸資訊與其他產品；香港目前則以產品及服務資訊、產品及服務的訂閱和新申請、帳戶資訊以及交易資訊等四類為大宗；新加坡目前開放之 API 類型，則以產品、銷售與行銷、服務以及交易為主，詳如表 6 說明：

表 6 各國開放 API 類型一覽表

國家	主政單位	序	Open API 類型	備註	開放進度 與相關服務	對應之 我國開放階段
英國	CMA	1.1	唯讀資料(Read)	包括銀行的總行地點及營業時間、分行的地點及營業時間、ATM 的地點、個人及企業活存帳戶、利息、中小企業借貸條款及條	已開放	第一階段

國家	主政單位	序	Open API 類型	備註	開放進度 與相關服務	對應之 我國開放階段
				件。		
		1.2	可讀寫資料(Read/Write)	可讀寫資料則規範了交易面以及支付面的API 類別，包括國內外交易發起、國內外交易同意、個人借貸等等各種相關應用	已開放	第二階段、第三階段
歐盟	歐洲銀行業管理局(EBA) *僅依服務類型區別	2.1	帳戶資訊服務(AIS)	TSP 能夠取得消費者的帳戶資訊 並且讓TSP 透過詳細的金融資訊幫助消費者提供分析與建議	已開放	第二階段
		2.2	支付發起服務 (PIS)	TSP 能夠代替消費者發起支付指令，簡化支付流程也提高應用性和方便性	已開放	第三階段
澳洲	競爭和消費者委員會(ACCC)、資訊專員辦公室(OAIC)、聯邦科	3.0	產品參考資料	資料持有者(Data Holder)所提供的金融產品的資料，例如功能、費率和費用。	Major-ADI 已開放	第一階段
		3.1	信用卡、金融卡、存款帳戶以及交易資	[消費者資料第一階段] 信用卡、金融卡帳戶、存款帳戶、稅收帳戶、	尚未完全開放	第二階段、第三階段

國家	主政單位	序	Open API 類型	備註	開放進度 與相關服務	對應之 我國開放階段
	學與工業研究組織(CSIRO)		料	電信帳戶及個人基本帳戶等資料		
		3.2	抵押帳戶資料	[消費者資料第二階段] 房屋貸款、個人貸款帳戶及抵押抵銷（Mortgage offset）帳戶等資料	尚未完全開放	第二階段、第三階段
		3.3	個人信貸資訊與其他產品	[消費者資料第三階段] 企業金融、投資貸款、信貸額度、資產融資、退休儲蓄帳戶、信託帳戶、外幣帳戶等	尚未完全開放	第二階段、第三階段
香港	金融管理局(HKMA)	4.1	產品/服務資訊	[第一階段] 查閱產品與服務資料	已開放	第一階段
		4.2	產品/服務的訂閱和新申請	[第二階段] 接受銀行產品申請	已開放	第二階段
		4.3	帳戶資訊	[第三階段] 賦予讀取或更改帳戶資訊的權利	尚未開放	第三階段

國家	主政單位	序	Open API 類型	備註	開放進度 與相關服務	對應之 我國開放階段
		4.4	交易	[第四階段] 接受消費者授權的銀行交易及支付服務。	尚未開放	第三階段
新加坡	MAS	5.1	產品	提供金融產品資訊和匯率。	已開放 (視銀行與 TSP 業者雙方合作意願，自願自律開放)	第一階段
		5.2	銷售與行銷	處理產品申請、銷售和交叉行銷、潛在消費者生成		第二階段、第三階段
		5.3	服務	管理消費者資料/帳戶詳細資訊，以及消費者查詢/反映		第二階段、第三階段
		5.4	交易	提供消費者的付款、資金轉帳、結算、清算、交易確認和交易指令		第二階段、第三階段

四、開放銀行之國際監理策略

(一) 歐盟

支付服務指令(Payment Service Directive，以下簡稱 PSD)最初於 2007 年公告施行，目的為降低非銀行業者進入歐洲支付服務市場的困難度，活化支付市場的競爭並提供消費者更多的選擇，同時強化消費者保護作為。2015 年歐盟執委會通過並執行第 2 號支付服務指令修正案 (Payment Service Directive 2，以下簡稱 PSD2)，要求歐盟各國亦被要求須於 2018 年 1 月前，將 PSD2 納入法規中，成為歐盟各國開放銀行政策的立法基礎。

PSD2 旨在減輕跨境支付及其他歐盟境內金融服務之風險，同時提高金融業的創新付費技術競爭力。該法案對金融產業最大的影響在於銀行業者必須開放其重要資產(消費者資料及內部支付服務)給非銀行的第三方業者存取。其他 PSD2 修正目標包含：

1. 提高歐盟支付市場的整合以及效率。
2. 提升支付服務提供者(包含新參進者)的營運範圍。
3. 確保強化消費者保護以及資訊安全。
4. 鼓勵支付服務的減價。
5. 促進共通技術規範以及互用性(interoperability)的形成

另 PSD2 將 Open Banking 參進者區分為三大角色，其中包含

1. 帳戶支付服務提供者 (Account Service Payment Service Providers，以下簡稱 ASPSPs)，意即提供開放 API 的業者。
2. 第三方服務供應商(Third Party Providers，以下簡稱 TPPs[3])

[3] TPPs 之於歐盟與英國，等同於 TSPs 之於臺灣；另外在英國，TSP 指的是技術服務提供商(Technical

TPPs 指為提供資訊服務之第三方業者，其中 TPPs 又區分為兩種資格[4]：

(1) 帳戶資訊服務提供商(Account Information Service Provider，以下簡稱 AISP)：

AISP 主要提供帳戶資訊服務(AIS 服務)，使消費者透過網路或應用程式，串接所有不同銀行帳戶並顯示在同一個地方(如 APP)，甚至進一步分析消費者的消費資訊，提供消費者估算預算、產品推薦或價格比較網站。

(2) 支付發起服務提供商（Payment Initiation Service Provider，以下簡稱 PISP）：

PISP 主要提供支付啟動服務(PIS 服務)。PISP 可使消費者直接啟動從帳戶扣款之方式，而非透過信用卡等第三方機構(如 Visa 或 MasterCard)進行扣款。

3. 支付服務用戶 (The Payment Service User，以下簡稱 PSU)：PSU 是 ASPSP 持有的帳戶所有者(即消費者)，並在使用服務其間授予 TPPs 認證，以存取帳戶資訊或從這些帳戶啟動支付作業。

因應 PSD2 的通過，歐洲銀行監理總署(European Banking Authority，以下簡稱 EBA)制定了技術標準--監管技術標準(Regulatory Technical Standards，以下簡稱 EU-RTS)[5]。該標準草案自 2017 年公告後，於 2018 年正式公告施行，並要求 2019 年 9 月正式適用。EU-RTS 包含兩大技術監管重點：

1. 強客戶身份驗證 (Strong Customer Authentication，以下簡

Service Provider)，通常為提供銀行業者資訊技術服務之廠商。

[4] https://www.fca.org.uk/consumers/account-information-and-payment-initiation-services

[5] https://www.europeanpaymentscouncil.eu/news-insights/news/european-commissions-final-rts-are-official-journal

稱 SCA)

SCA 旨在降低交易欺詐，打造更安全的線上支付環境。SCA 要求 TPPs 必須在交易過程中導入以下驗證程序，並在驗證時至少使用「使用者的知識 (只有使用者知道的內容，如密碼)、所有物 (只有使用者擁有的物品，如行動電話或憑證)、固有屬性 (使用者的屬性，如人臉辨識或指紋)等三種要素其中兩種，其授權必須相互獨立。

圖 8 英國 SCA 適用與排外時機

資料來源：歐盟執委會

2. 通用安全通訊 (Secure Open Standards of Communication，以下簡稱 CSC)

CSC 中最重要的兩個議題為「取得同意(Consent)」和「安全的通訊渠道(Secure Communication Channel)」

(1) 取得同意：客戶必須給出明確的同意 AISP 或 PISP 共享他們的付款帳戶資料或發起支付交易。

(2) 安全的通訊渠道：ASPSP 必須提供 AISP 或 PISP 安全通訊渠道以存取消費者的支付帳戶資料，如 API。其中 ASPSP 必須提供 TPPs 存取消費者資料的應變機制，以避免 API 臨時無法使用。此段機制我們會在第伍章節對於代理登入機制的研究進行更詳細的說明。若 ASPSP 所提供之 API 已符合 RTS 中定所要求的品質標準，且 API 已成功通過市場測試並獲得國家主管部門批准，則可不用提供應變機制。

3. 小結

針對 TPPs 在執行業務上的風險，EBA 因應 PSD2 要求，於 2017 年制定、公告職業責任保險指南(Professional Indemnity Insurance (PII) Guidelines)，以加強管理電子支付交易中不同參與者之間互動的責任制度。EBA 要求所有 PISP 和 AISP 在申請業務時，必須需擁有 PII 或類似的擔保，以作為獲得授權的先決條件。

目前，歐盟的 Open Banking 推動進度已發展到近似於臺灣第三階段的範圍，並已有不少銀行與 TPS 合作推出交易或是擁有金流的金融服務。

表 7 歐盟開放銀行監理要點

開放銀行監理要點	
主要法令法規	■ PSD2 ■ EU-RTS ■ PII Guidelines

開放銀行監理要點	
法規生效時間	2015 年
主要主管機關	EBA 制定、歐盟執委會通過
主要主管機關	修訂法規，強制執行

資料來源：本研究整理

(二) 英國

緣起於歐盟的 PSD2 於 2015 年公告及脫歐政策背景，英國競爭及市場管理局(CMA)於 2017 年發布「零售銀行市場調查行政命令(The Retail Banking Market Investigation Order)」開啟第一波開放銀行的發展。因應 2017 年 CMA 的行政命令，英國前九大銀行(CMA9)共同出資成立開放銀行執行組織(Open Banking Implementation Entity，以下簡稱 OBIE[6])，主導推動英國 Open Banking 進程，並負責制定相關標準規範、安全以及爭端解決機制

2017 年，英國財政部亦參考 PSD2，發布 Payment Services Regulations 2017 (2017 支付服務案，以下簡稱 PSRs 2017)。英國開放的 API 範圍與內容已於 CMA 的行政命令中被定義，主要分為兩類：

表 8 英國 Open API 類型

資料類型	說明
唯讀資料(Read)	包括銀行的總行地點及營業時間、分行的地點及營業時間、ATM 的地點、個人及企業活存帳戶、利息、中小企業借貸條款及條件。
可讀寫資料	可讀寫資料則規範了交易面以及支付面的 API

[6] OBIE 於 2019 年後因正式設立為為公司，故改名為 Open Banking Limited，但產業上多以 OBIE 稱之。

資料類型	說明
(Read/Write)	類別，包括國內外交易發起、國內外交易同意、個人借貸等等各種相關應用

資料來源：OBIE, 2019

英國對於 Open Banking 參進者的分類與 PSD2 相同，將參進區分為 ASPSPs、AISPs、PISPs。然而對於 ASPSPs 的定義上，從 FCA 2019 年提出之「開放金融-徵求意見書」(Call for Input: Open Finance)中可了解，英國對於 ASPSPs 的定義，未來可能擴大至保險業者、證券業者及其他掌管消費者帳戶的產業。

在監理機構的角色議題，FCA 作為 TPPs 資格審核機關，要求 TPPs 應於審查資料中，提出其商業模式、服務細節、系統安全、資料存取以及其他政策文件；參考 PSD2 的配套措施，FCA 要求 TPPs 必須要擁有職業責任保險(Profession Indemnity Insurance)才具備申請資格，以確保 TPPs 的責任賠償能力。

表 9 英國開放銀行監理要點

開放銀行監理要點(英國)	
主要規範	■ The Retail Banking Market Investigation Order ■ PSRs 2017
主管機關	■ FCA 與 CMA 主要監管 ■ OBIE 實際執行
推動策略	修訂法規，強制前九大銀行執行

資料來源：本研究整理

(三) 澳洲

1. 監理組織

相較於歐盟與英國從開放銀行到開放資料的策略，澳洲則對開放銀行參與者課以更高的消費者保護義務，其於 2017 年修訂之《競爭與消費者法》（Competition and ConsumerAct 2010，CCA）成為後續 2018 年的《消費者資料權法案》(Consumer Data Right，CDR) 的修訂依據。CDR 建立了開放資料(Open data)的大框架，並以適用全產業作為最終目標，先行從銀行產業實施(即開放銀行 Open Banking)。能源產業、電信產業也已被列為後續開放的產業。

2020 年澳洲競爭和消費者委員會（Australian Competition and Consumer Commission，以下簡稱 ACCC）因應產業需求推出「消費者資料權利註冊和認證應用平台」(the Consumer Data Right Register and Accreditation Application Platform，以下簡稱 RAAP) 和「消費者資料權參與入口網站」(the Consumer Data Right Participant Portal)，以下簡稱入口網站)。 RAAP 和入口網站與我國財金公司的 Open API 平台類似。RAAP 主要是建立一個可信任的資料環境，提供受到加密的資料，且限制資料僅在受核可的參與者之間進行共享；而入口網站則提供一個門戶，使企業可以透過門戶網站申請認證。透過推出 RAAP 和入口網站，企業將能申請成為經認證的資料接收者。

表 10 澳洲開放銀行組織監理架構

澳洲開放銀行組織監理架構	
聯邦財政部 (The Federal Treasury)	■ 聯邦財政部為 CDR 主管機關；並自 2021 年 2 月 28 日之後，「退休金、

澳洲開放銀行組織監理架構	
	金融服務與數位經濟部部長」接管[7]未來 CDR 的規則制定。
競爭和消費者委員會(Australian Competition and Consumer Commission，以下簡稱 ACCC)	■ 負責初期 CDR 規則訂定及競爭與消費者層面；自 2021 年 2 月 28 日之後，規則制定權責移交至聯邦財政部。 ■ 認證潛在資料接收者(potential data recipients) 。 ■ 建立及維護獲認證之人員及資料持有者(Accedited Persons and Data Holders)清冊。 ■ 與 OAIC 共同監管業者合規性，並在必要時採取法律行為。 ■ 指導 CDR 生態圈中的利益相關者其相關之權利與義務。
資訊專員辦公室(Office of the Australian Information Commissioner，以下簡稱 OAIC)	■ 負責隱私層面的法規修訂並就 CDR 對隱私的影響向 ACCC 和 DSB 提供建議。另外也與 ACCC 共同監管業者合規性，並在必要時採取法律行為。
資料標準單位(Data	■ DSB 為財政部底下之單位，並由聯邦

[7] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

澳洲開放銀行組織監理架構	
Standards Body，以下簡稱 DSB)[8]	科學與工業研究組織(CSIRO)的 Data61 擔任，主司資料標準(Consumer Data Standards)之制定與維護，並與 ACCC 並列為 CDR 最高主管機關。

資料來源：本研究整理

2. 開放資料類型

CDR 旨在交還資料權予消費者，並提供消費者對於其所擁有的資料更大的控制權力。從市場上來看，CDR 也將提升各服務提供商之間的良性競爭，不僅提供更好的價格之外，澳洲政府也期待 CDR 更可以為市場帶來更多創新的產品和服務。在 CDR 的框架下，將開放資料類型分為兩種類型：

(1)產品參考資料(Product Reference Data)

產品參考資料是指有關資料持有者(Data Holder)所提供的金融產品的資料，例如功能、費率和費用。資料類型也較近似於我國第一階段開放的資料。一般來說任何人都可以透過 API 公開獲取。

(2)消費者資料(Consumer Data)

消費者資料是指與特定消費者及其金融產品相關的資料。根據使用不同的產品類型，可能包含消費者的交易資料、帳戶餘額、借貸資料、收款人資訊等。消費者可以透過同意，與經認可的第三方共享這些資料。資料類型較近似於我國第二、三階段開放的資料。CDR 在消費者資料上亦有

[8] https://consumerdatastandardsaustralia.github.io/standards/#introduction

依照資料機敏性規劃三階段的開放時程如下表所示：

表 11　CDR 在消費者資料開放時程表

第一階段	第二階段	第三階段
信用卡、金融卡帳戶、存款帳戶、稅收帳戶、電信帳戶及個人基本帳戶等資料	房屋貸款、個人貸款帳戶及抵押抵銷（Mortgage offset）帳戶等資料	企業金融、投資貸款、信貸額度、資產融資、退休儲蓄帳戶、信託帳戶、外幣帳戶等

資料來源：CDR, 2019

3. 澳洲開放銀行參與者

根據 CDR Privacy Safeguard Guidelines 的定義，澳洲開放銀行將生態圈中的參與角色分為兩種類型：資料持有者(Data Holder)以及經認證的資料接收者(Accredited Data Recipient，以下簡稱 ADRs[9])。

(1)資料持有者(Data Holder)

資料持有者是持有消費者資料的企業，在 CDR 的規範下，資料持有者必須根據消費者的要求將資料傳輸給 ADRs。在開放銀行的階段上，CDR 的資料持有者則為澳洲政府已授權認證的存款機構(Authorised deposit-taking institution，以下簡稱 ADI)，之於臺灣即指銀行業者、信用合作社及農漁會信用部等機構[10]。根據官方統計，截至 2021 年 7 月，澳洲共有 138 家 ADI，其中包含當地數位銀行 86400、Volt Bank 以及 Judo。

[9] 經認證的資料接收者(Accredited Data Recipient) 在部份文件中也可被稱為「經認證的提供者」(Accredited Providers)

[10] https://www.rba.gov.au/fin-stability/fin-inst/main-types-of-financial-institutions.html

此外，CDR 將 ADI 依其規模與重要性，分為 Major ADI 和 non-Major ADI，Major ADI 則定義為澳洲前四大銀行，包含 Australia and New Zealand Banking Group Limited、Commonwealth Bank of Australia、National Australia Bank Limited，以及 Westpac Banking Corporation。

(2)經認證的資料接收者(Accredited Data Recipient)

ADRs 則是在取得消費者的同意前提，從資料持有者接收消費者的資料。這些 ADRs 應事先取得 ACCC 的認證，方能接收消費者資料以提供產品或服務。ADRs 在申請取得 ACCC 認證時，必須提出其合適性、資料保護能力、具備內部爭議解決流程、為相關外部爭議解決計劃的成員、擁有充足的賠償保險，以及澳洲地址等相關佐證。

4. 開放銀行之資料開放執行進程

考量不同規模的銀行業者其資源與能力也有所不同，澳洲政府針對 Major ADI、non-Major ADI 設計不同的實施時程，以利開放銀行參與者順利接軌，實施進程與各階段開放範圍如下表所示。

表 12 澳洲開放銀行之資料開放執行進程實施時間表

資料類型	參進者	第一階段	第二階段	第三階段
產品參考資料	Major ADI (已完成)	2020/02/01		2020/07/01
	Non-Major ADI	2020/10/01	2021/02/01	2021/07/01 *因應疫情延長至 2021/10/01

資料類型	參進者	第一階段	第二階段	第三階段
消費者資料	Major ADI	2020/07/01	2020/11/01	2021/02/01
	Non-Major ADI	2021/07/01	2021/11/01	2022/02/01
	其他資料擁有者	2021/03	2021/07	

資料來源：ACCC, 2020

5. 資安要求標準

澳洲的資訊安全標準(Consumer Data Standards，以下簡稱 CDS) 作為 CDR 的一部分，主要規定 API、資料與安全的相關規定。該標準的制定係參考、整合歐盟與英國的標準，並利用 OIDC 與 FAPI 作為身份認證機制。

表 13 澳洲開放銀行監理要點

開放銀行監理要點	
主要規範	CDR、CDS、Accreditation Guidelines
生效時間	2018 年
主管機關	ACCC、DSB、OAIC
推動策略	修訂法規，強制執行(階段式、分級式執行)

資料來源：本研究整理

(四) 新加坡

2016 年新加坡金融管理局(Monetary Authority of Singapore，以下簡稱 MAS) 開始大動作積極推動開放銀行發展。除了舉辦「金融世界-API 大會」之外，更聯合新加坡銀行協會(The Association of Banks in Singapore，以下簡稱 ABS)共同發布《API Playbook 指

導手冊[11]》，作為開放 API 之行政指導。

採行鼓勵策略的新加坡並沒有設定開放階段進程，取而代之的則是將 API 依功能類別，由 MAS 督導銀行開放。其分類一開始在 2016 年的 Playbook 裡區分為產品、行銷、銷售、服務、支付、監理等六大類，但根據 MAS 近期的官方網站公告[12]，已將上述 6 大類別濃縮為 4 大類別(行銷與銷售合併、移除監理類別)，而各類別又各自依其資料重要性再細分為交易(Transactional)和資訊(Informational)兩種類型。

1. 新加坡開放銀行參進者

根據 Playbook 的定義，API 的建置涉及四類利益相關者，分別為 API 提供者、API 消費者、金融科技公司與開發者群體，其中針對各類利益相關者要求整理如下：

表 14　API 相關利害關係人及需求列表

利益相關者類型	要求說明
API 提供者	1. 識別和排序所要發布之 API； 2. 評估開發 API 所需的內部基礎結構，如發布 API 之成本與收益、公司業務與 IT 策略是否保持一致、目前 IT 成熟度是否能夠支持設計與發展等； 3. 定義要求與技術準則，且須考量設計 API 時的開放性、可用性與互通性等，提供創新與靈活性。
使用 API 來存	1. 確定 API 是否滿足其業務需求的潛在能

[11] https://abs.org.sg/docs/library/abs-api-playbook.pdf
[12] https://www.mas.gov.sg/development/fintech/financial-industry-api-register

取或發送資料的組織或個人的 API 消費者	力； 2. 搜索該 API 是否可作為開放 API 使用； 3. 遵守 API 提供者指定的準則與合約，維護資訊安全標準。
金融科技公司 (FinTechs)	1. 定義需要使用的 API，確立數據交換、資訊安全和治理機制的標準化可以提供更清晰的營運方式； 2. 使用標準化原則，來構建適用於廣泛行業應用的產品或服務，從而消除為每個現有客戶與合作夥伴進行自定義的需求； 3. 遵循提供者指定的技術準則，創建具互通性與平台獨立性的產品，避免修改現有的已定義 API。
API 開發者群體	1. 收到提供者和 FinTechs 的需求與技術準則，以開發適合其業務需求的 API； 2. 基於第 1 點的要求，建立技術規格文件，並選擇使用可用於網頁服務架構的設計模型(分別為簡單物件存取協定（Simple Object Access Protocol, SOAP）、表現層狀態轉換（Representational State Transfer, REST）。

資料來源：本研究整理

2. API 設計指引與安全標準

為協助 API 提供者提供創新和彈性，Playbook 建議 API 提供者在設計 API 的時候應考量以下 8 種特性：

表 15　API 設計應考量事項

序	特性	說明
1	開放性(Openness)	應確保所有有興趣的單位皆可存取 API。
2	使用性(Usability)	應確保高品質的消費者的使用體驗。
3	互相操作性(Interoperability)	確保跨組織的資料交換時無任何技術依賴性。
4	重複使用性(Reuse)	利用現有標準和分類法以避免重工。
5	獨立性(Independence)	在提供交付模型和實施技術的選項時，應避免對於任何供應商或技術的依賴。
6	可擴展性(Extensibility)	建立擴展 API 的靈活性以擴展至新的利益相關者和業務渠道。
7	透明性(Transparency)	在溝通和治理的過程中，確保任何異動皆具有一致性和透明度。
8	鬆散耦合性(Loosely Coupled)	提供彈性並最大限度地減少對其他 API 操作的更改的影響。

資料來源：本研究整理

在資安要求層面，Playbook 的資訊安全標準(Information Security Standard, 簡稱 InfoSec) 將資安標準分為 7 個構面，包含身份認證 (Authentication) 、加密 (Encryption) 、授權 (Authorisation)、主機代管安全性 (Hosting Security)、開發安全 (Security Coding) 、脆弱性評估與滲透測試 (Vulnerability Assessment & Penetration Testing)、故障自動切換機制(Robust Failover Mechanisms)。

表 16 新加坡開放銀行監理要點

新加坡開放銀行監理要點	
主要規範	API Playbook 指導手冊
生效時間	2016 年
主管機關	MAS, ABS
推動策略	提供產業最佳實踐建議，採行鼓勵推動(MAS 督導)

資料來源：本研究整理

(五) 香港

香港金融管理局（the Hong Kong Monetary Authority，以下簡稱 HKMA） 於 2017 年 9 月宣布智慧銀行新時代(A New Era of Smart Banking)[13]，其中 Open API 行動則是七項香港迎接銀行和科技融合的主要行動之一。HKMA 相信只有在銀行業廣泛、安全且有成本效益的實施，才能真正獲得 Open API 的好處與優勢。因此，從 2017 年至 2018 年間，HKMA 辦理多場研討會、邀請多家零售銀行與外商銀行參與，並提供約 2 個月的產業諮詢期間後，HKMA 於 2018 年 7 月 18 日發布「香港銀行開放 API 框架[14]（Open API Framework For the Hong Kong Banking Sector）」作為鼓勵產業開放 API 的指導方針。

1. 香港開放 API 四大階段

香港規劃將 API 開放分為四大階段，截至 2021 年 7 月前兩階段已完成，各銀行開放 API 資料已詳列香港科技園的

[13] 香港「智慧銀行新時代」的七項措施分別為推出快速支付系統、監理沙盒升級、引入虛擬銀行、推出「銀行易」、促進開放應用程式介面(開放 API)、加強跨境金融科技合作 以及提升科研及人才培訓。

[14] https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf

Data Studio[15]。另外，為配合開放 API 第二階段的推行，香港銀行公會制定《開放應用程式介面第二階段共同基準》[16]，以響應 HKMA 的開放 API 框架。

另一方面，HKMA 針對第三及第四階段的實施計劃決定採取循序漸進方式以降低實施成本和風險。HKMA 已於 2021 年 5 月公布開放 API 框架[17]，目前已有 28 家銀行業者參與，首批 API 功能預計包含存款帳戶資訊和線上帳戶付款，相關計畫預計於 2021 年 12 月起逐步實施。

表 17 香港推動開放銀行四大階段

階段	開放 API 功能	API 範例	推出時間
1	查閱銀行產品和服務資料	存款利率、信用卡優惠、收費等公開資訊	2019 年 1 月底前 (已完成)
2	接受銀行產品申請	申請信用卡、貸款產品等	2019 年 10 月底前 (已完成)
3	讀取或更改帳戶資訊	帳戶結餘、信用卡結欠、帳戶交易紀錄、更改信用額等	首批 API 功能涵蓋存款帳戶資訊及線上帳戶付款，預計於 2021 年 12 月起逐步實施
4	進行交易	付款及轉帳	

資料來源：本研究整理

表 18 香港實施開放 API 第三及第四階段規劃

功能	最晚實施期限
「轉數快」手機應用程式至應用程式 (App-	2021 年 12 月

[15] https://datastudio-fintech.hkstp.org/
[16] http://www.hkab.org.hk/DisplayArticleAction.do?ss=22&lang=b5&sid=5
[17] https://www.hkma.gov.hk/chi/news-and-media/press-releases/2021/05/20210513-3/

功能	最晚實施期限
to-app)支付功能	
存款帳戶資訊 • 帳戶是否存在 • 帳戶狀態 • 帳戶結餘 • 交易資訊	• 對公司和中小型企業客戶: 2022 年 3 月 • 對零售客戶: 2022 年 6 月

資料來源：本研究整理

為安全並有效地實施這些 API 功能，HKMA 將協助香港銀行公會訂定資安標準，內容預期涵蓋客戶體驗和認證、技術及數據標準、資訊安全和操作標準等主要範疇。銀行公會亦會修訂目前的共同基準文件，把第三及第四階段開放 API 的實施範圍包括在內。技術標準及經修訂的共同基準文件預計於 2021 年年底前發布。

2. TSP 管理機制

根據香港銀行開放 API 框架，HKMA 建議任何 Open Banking 的合作皆須由銀行與 TSP 業者共同建立契約，而銀行業者也將須導入 TSP 的監管機制，如盡職調查、入職、控制、監控、角色和責任、消費者保護、數據保護、安全性、基礎設施彈性和事件處理。HKMA 也提出三種可行的治理方案如下表。

表 19 HKMA 對 TSP 治理的三項方案分析

方案	方案說明	本專案利弊分析
一	銀行針對與 TSP 的進行自身的風險評估和盡職調查，根據約定的性質以及銀行的既定	各自依循既有程序執行調查，對於銀行業者來說，較無其他負擔；但對合作的 TSP 業者來說，將可能需要因應不同銀行

	政策和程序，對 TSP 治理的各個方面進行調查。	的需求提供不同的資料
二	由所有相關銀行共同出資開發一套通用的 TSP 治理標準和評估服務。	流程簡化且執行效率較高；但在前期整合各銀行之需求與意見較為耗時。
三	所有相關銀行制定一套 TSP 治理共同基準，但銀行得視自身需求在基準之上增加項目。	儘管銀行可能會增加自己的獨特要求，但此方法可簡化的 API 建置流程。

資料來源：本研究整理

3. 開放銀行監理要點

表 20 香港開放銀行監理要點

香港開放銀行監理要點	
主要規範	香港銀行開放 API 框架
生效時間	2018 年
主管機關	HKMA
推動策略	與銀行業者積極討論，採行鼓勵推動

資料來源：本研究整理

(六) 臺灣

我國開放銀行產業共有五大角色，分別為主管機關、技術標準制定、金融服務產業、第三方服務提供者(Third Party Serrvice Provider, 以下簡稱 TSP)，以及第三方輔佐單位/試驗平台。

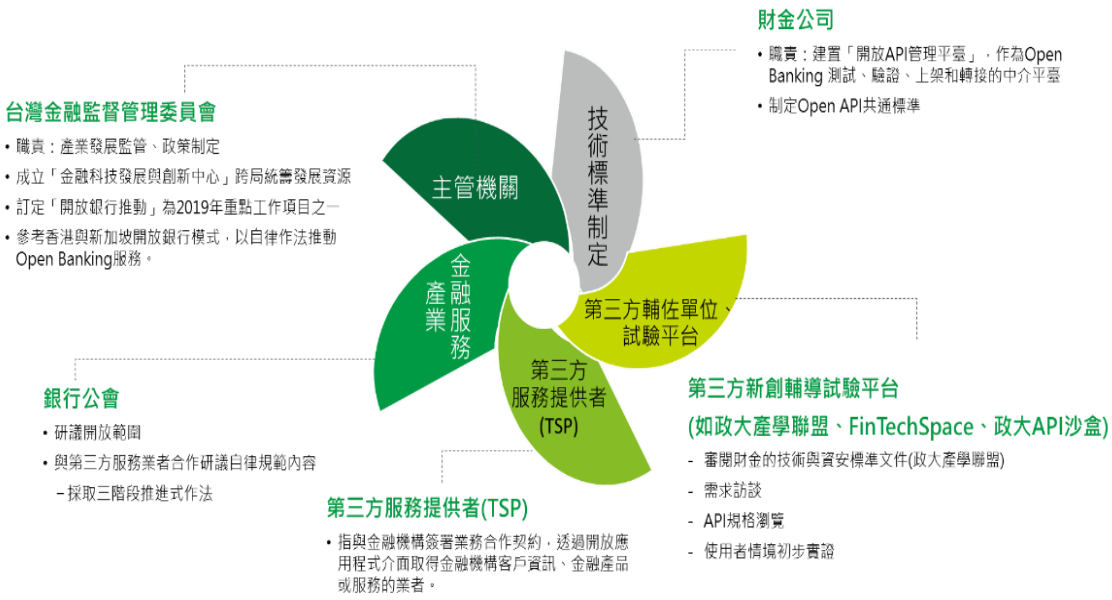

圖 9 我國開放銀行產業五大角色

資料來源：本研究整理

其中金融監督管理委員會(以下簡稱金管會)為主管機關，其在推動 Open Banking 的發展策略上，參考新加坡與香港，採自願、非強制方式推動開放銀行。因應金管會之鼓勵政策，銀行公會與財金公司分別從金融業務面與技術面建立 Open Banking/Open API 的規範文件：

1. 「中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範」(銀行公會)
2. 「開放應用程式介面(Open API)技術標準規格書」，及「開放應用程式介面(Open API)業務安全控管作業規範」(財金公司)

目前，金管會規劃臺灣開放銀行依「公開資料查詢、消費者資訊查詢和交易面資訊」三大階段循序推進，並已進入第二階段：

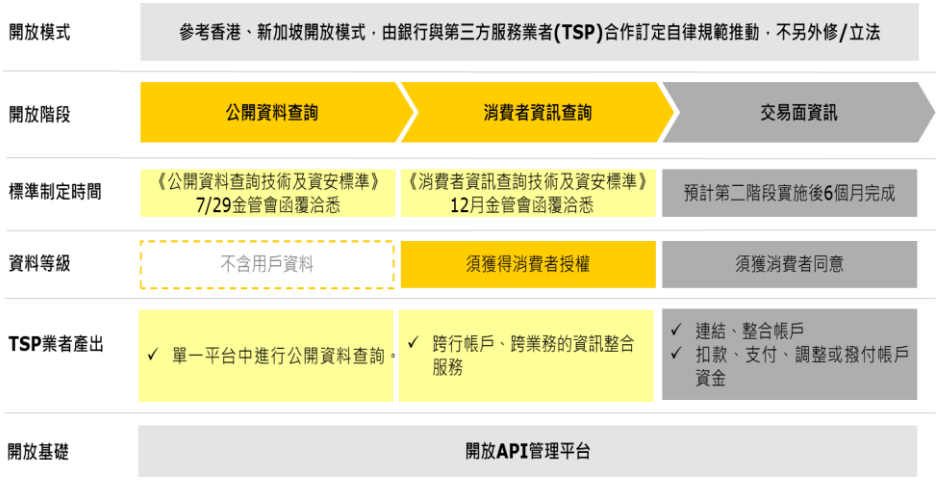

圖 10 我國開放銀行推動進程

資料來源：本研究整理

1. **公開資料查詢：**以提供非交易面金融產品為主，使消費者能於 TSP 業者處取得利率、匯率、產品等資訊。TSP 可利用 API 串接各銀行的金融商品資訊，同時消費者可以直接在 TSP 的單一平台上看到各個銀行的金融商品。

2. **消費者資訊查詢：**需獲得消費者同意或授權才能存取個人資料與消費資料。在這階段 TSP 業者可以透過 API 串接各銀行的個人資料查詢、帳務開戶作業與附屬業務申請、信用卡與附屬業務申請等。

3. **交易面資訊：**在消費者同意或授權下，於 TSP 業者的服務或 APP 上進行金融交易與支付，也是 TSP 業者最引頸期盼的階段。開放項目預計包含帳戶扣帳授權、貸款清償等。用戶可以透過第三方業者所開發的平台，直接連結帳戶扣款與消費支付等應用。

資安管控上，由財金公司制定的 Open API 技術標準規格書中主要針對訊息處理、憑證作業，以及認證機制等三大項目進行規範要求。詳細內容將於第參章、推動開放銀行後，API 之管理方式及安控要求進行分析說明。

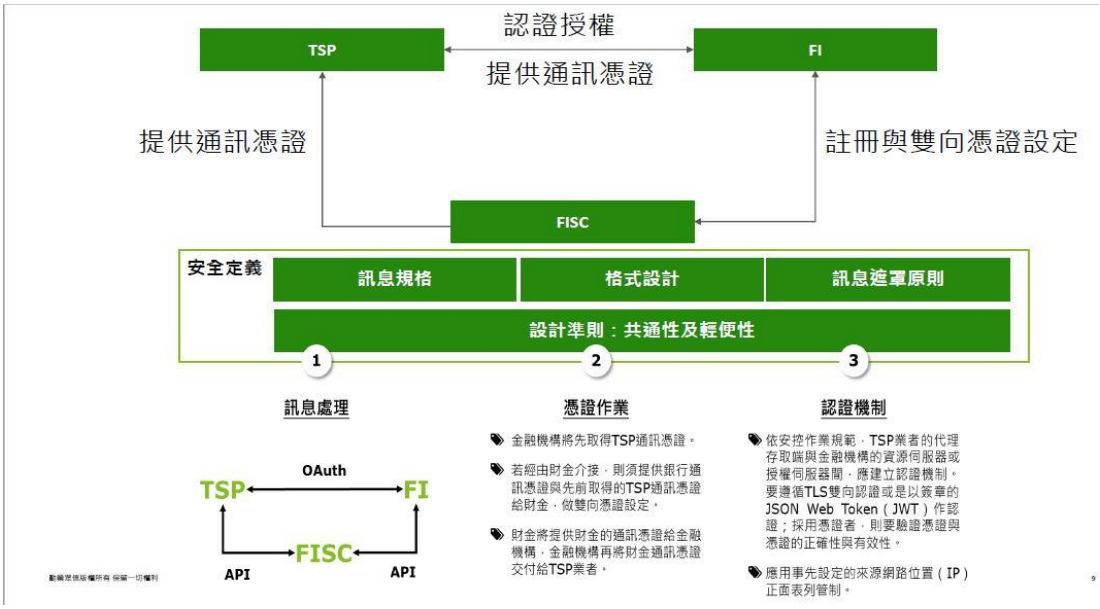

圖 11 我國開放銀行安控架構

資料來源：本研究整理

有關開放銀行監理要點，則可分成主要規範、施行時間、主觀機關以及推動策略等進行釐清。

表 21 臺灣開放銀行監理要點

臺灣開放銀行監理要點	
主要規範	1. 第三方自律規範 2. 開放應用程式介面(Open API)技術標準規格書 3. 開放應用程式介面(Open API)業務安全控管作業規範
生效時間	2020 年
主管機關	1. 中華民國銀行公會制定、金融監督管

臺灣開放銀行監理要點	
	理委員會(以下簡稱金管會)核准開放銀行之相關自律規範係由銀行公會及財金公司訂定，並報金管會備查
推動策略	1. 產業自訂自律規範，主管機關鼓勵參與

資料來源：本研究整理

勤業眾信研究團隊彙整上述各國開放銀行之進程，並與我國開放銀行三階段進行比較，以利讀者能對各國發展進程有更全面的掌握。

1. 臺灣於 2021 年 5 月進入第二階段，開放客戶的帳務資訊
2. 英國、歐盟與新加坡已有 TSP 業者達到第三階段的交易應用
3. 澳洲以金融業者的重要性進行適用的進程規劃。

香港目前已經開放至第二階段提供商品申請 API，其開放進程略等於臺灣第二階段。

圖 12 各國開放銀行進度彙整(截至 2021 年 7 月 1 日)

資料來源：本研究整理

(七) 美國

美國開放銀行發展採用由產業驅動(industry-driven initiative)的方式，相較於英國與歐盟等國家透過政府法規強制執行不一樣，美國各銀行可以從境內不同地區的狀況與發展模式吸取經驗，幫助美國銀行實現關鍵的策略目標，並加速銀行的數字化轉型工作和新業務模式的出現。

在 Deloitte USA 針對美國消費者對於開放銀行業務的意願與態度調查報告中顯示，美國消費者對開放銀行業務的態度似乎喜憂參半，在 3,000 名消費者中，僅五分之一的受訪者認為消費者認為開放銀行業務對他們具有非常高的價值，其中以 18 至 21 歲與 22 至 36 歲，兩個世代的消費者興趣最高。年輕消費者支持開放銀行業務的主要原因為能透過儲蓄、支付和預算管理等應用程式，使他們的生活更靈活與簡單。雖然這些消費者對開放銀行業務表現出興趣，但他們同時也表達了一些擔憂，尤其是對隱私以及個人數據的安全和使用的疑慮，如潛在的身份盜竊和數據濫用是他們最關心議題。

1. 監理架構

因美國的監理架構，與其他強制執行國家不同，其極為複雜並無專責主管機關進行監督管理。而最常提到且與開放銀行最為相關之主管機關為美國金融保護局(United States Consumer Financial Protection Bureau, CFPB)，該單位是根據《Dodd-Frank 法案》(Dodd-Frank Wall Street Reform and Consumer Protection Act)所授權成立，它有權頒布有關消費者金融數據共享的規則。隨著消費者金融資料共享的增加與新興金融科技應用程式和產品的產生，開放銀行

所涉及的交易類別種類越來越多，因而不容易以單一機構專責主導。

五、重點市場對於開放 API 的資安相關法令法規

近年來開放銀行發展快速，資料的開放為消費者創造更大的利益。承續第貳章對各國開放銀行之相關法令法規介紹，本章節將深入分析各重點市場對於 API 開放制定的資安管控要求與機制。以下依據不同推動策略，依序分析歐盟、英國、澳洲、新加坡、香港及我國的推動 Open API 的法制架構。

(一) 歐盟：第 2 號支付服務指令(PSD2)

2015 年歐盟通過並執行「第 2 號支付服務指令」（Payment Service Directive 2，簡稱 PSD2）。PSD2 的主要目標為提供更具有效率和整合的歐洲支付市場，在創造公平競爭環境的同時，保護消費者提供安全的支付方式。PSD2 除了要求相關銀行業者提供 Open API，令外部人員及組織可以此存取銀行內部資料外，同時也提出了嚴格的資安要求。如在 PSD2 之下的消費者身份驗證和通用安全通訊的監管技術標準(the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under PSD2，以下簡稱 EU-RTS)，就要求相關銀行業者必須採用嚴格的強消費者身份認證(Strong Customer Authentication，以下簡稱 SCA) 強制要求金融業者的通訊傳輸加密、通過稽核的資安機制，甚至必須採取雙驗證授權，包括 PIN 碼、指紋、識別碼等。PSD2 中也指出許多不安全的認證方法，如文字簡訊的一次性密碼認證方法(OTP)。

■ API 治理模式

PSD2 概述了兩種類型的受監管的第三方機構(Third-party

providers, TPPs)，分別為支付啟動服務提供者(Payment initiation service provider, PISP)，以及帳戶資訊服務提供者(Account information service provider, AISP)，兩類服務提供者將被授予直接存取消費者帳戶的權限。

1. 支付啟動服務提供者(PISP)

   PSD2 允許受監管的第三方 PISP 在獲得消費者同意的情況下直接從消費者支付帳戶發起付款。

2. 帳戶資訊服務提供者(AISP)

   受監管的第三方 AISP 不能進行轉帳或交易，僅能在消費者同意的情況下，提供讀取消費者數據的權限，使用該銀行帳戶資料來提供服務，如透過資金管理工具查看不同帳戶的支出。

■ **API 安全標準**

API 的目的是在技術上實現第三方提供商（TPP）和帳戶服務支付服務提供商之間共享支付帳戶訊息。在 PSD2 和 EU-RTS 中，歐盟從法律框架下直接規定了 API 介接的義務。此技術標準要求銀行公開有關專用介接的技術規範，以實現互通性。

1. 一般認證要求

   PISP 應具備完善的交易監控機制，使他們能夠檢測未經授權或欺詐的支付交易。交易監控機制應基於對支付交易的分析，考慮到基於風險的因素，包含每筆付款交易的金額、提供支付服務中的已知欺詐場景、個人支付服務用戶以往的消費模式、支付交易歷史、支付服務用戶與支付交易歷史相關的異常支付行為，與身份驗證過程的惡意軟體感染跡象等。

2. 強化身份驗證(SCA)

SCA 應為電子商務(e-commerce)和線上支付(online payments)引入強大的雙因子身份驗證。歐盟將強化客戶身份驗證定義為客戶必須提供兩項或以上的認證要素來證明他們是客戶本人，而每個要素來自以下不同類別：所有權(possession)、固有(inherence)和知識(knowledge)。當付款人使用驗證碼進行線上存取支付帳戶、發起電子支付交易或透過遠端執行可能造成支付欺詐或其他濫用風險的任何行動時，PISP 只接受驗證碼一次。

3. 佈署即時風險評估

消費者行為部署即時風險評估的執行，可防止並降低欺詐交易發生的機會。條文明確規定了監管機構應採取的合規措施，包括檢測來自異常或高風險的交易以及超出付款人正常行為的交易。

(二) 英國：開放銀行標準框架(The Open Banking Standard)

英國開放銀行標準框架是由財政部支持、CMA9 出資成立的的開放銀行工作小組(OBWG)所提出，旨在建立一個完善、運作良好且沒有任何障礙的開放金融生態圈。此開放銀行標準框架除制定 API 規範 (API Specifications) 與安全設定檔 (Security Profiles)外，還包括了消費者體驗指南 (Customer Experience Guidelines) 與操作指引 (Operational Guidelines)。

■ API 治理模式

為確保開放銀行標準的落實與推進，OBWG 呼籲採用的治理模式包含以下幾點措施：

1. 設立一個獨立機構

其職責包含追蹤並監督開放銀行標準的落實和部署進程，

處理消費者糾紛，確保數據安全性，維護 API 的可靠性與可拓展性，以及其他開放銀行框架下提出的要求。

2. 賦予獨立機構審查第三方的權利。

   指導第三方機構購買相應的保險，並評估保單內容與相對應的風險程度是否洽當。

3. 建立事故處理機制

   當用戶遭遇 API 相關事故時，有權利聯繫第三方或數據提供者來協商解決問題。如果逾期未處置，就可以啟動下一事故處理流程，交由獨立機構處理。

4. 分階段逐步引入治理模式

   分階段逐步引入治理模式取代過往習慣一步到位的模式，OBWG 提倡循序漸進、分階段進行。作為英國的產業推進單位，治理模式雖然會遵循歐洲 PSD2 的要求，但 OBWG 認為可以不僅限於 PSD2。另外，資金成本也是 OBWG 會考量的議題。

5. 遵循相關指南

   為實現一個運作良好與成功的開放銀行生態系統，應遵循相關指南如體驗指南 (Customer Experience Guidelines) 與操作指引 (Operational Guidelines)，內容包含規範身份授權、變更管理、可用性與性能與測試流程等，以設計有效和高性能的 API，優化消費者滿意度，同時履行其監管義務。

■ **API 安全標準**

英國開放銀行標準框架中的安全設定檔 (Security Profiles)採用國際非營利組織 Open ID Foundation (以下簡稱 OIDF)所提供的兩個標準：

1. Financial Grade API (FAPI)

以 OAuth 2.0 和 OpenID Connect (OIDC) 作為基礎，FAPI 提供金融業和其他需要更高等級安全性的產業使用 API 的技術標準。FAPI 透過以下四種關鍵方式，彌補 OAuth 2.0 和 OIDC 的安全漏洞：

- 客戶端和服務器之間的所有交換都使用 JSON Web Tokens (JWT)。
- JWT 必須使用非對稱密鑰對來確保加密密碼交換。
- JWT 交換中允許使用一組有限的安全算法。
- 提供可以自動化的一致性測試方法。

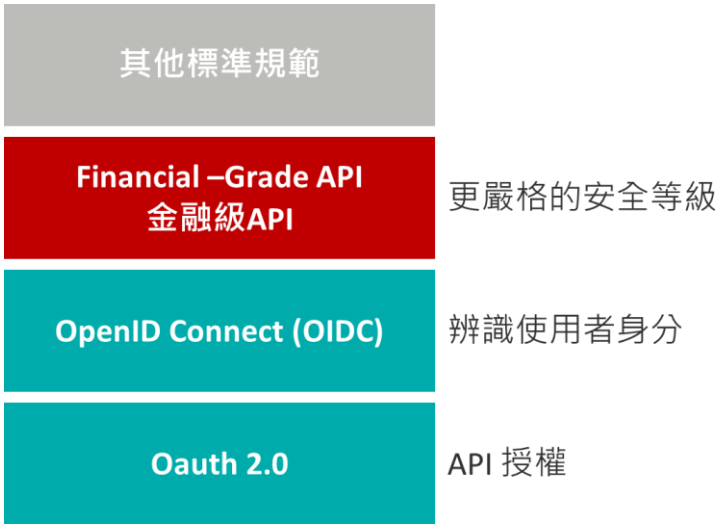

圖 13 FAPI 層級圖

2. Client-Initiated Backchannel Authentication (CIBA)

CIBA 指的是從客戶端發起的反向通道身份驗證機制。CIBA 同時具有消費設備及身份驗證設備兩種概念，其中消費者在消費設備上與依賴方互動；而在身份驗證設備上消費者可以與 Open ID 提供者進行身份驗證並授

予同意。CIBA 允許具有消費者標識符(identifier)的依賴方，可以從 OpenID 提供者獲取憑證(token)。消費者可在消費設備上與依賴方開始驗證流程，但在身份驗證設備上進行身份驗證並授予同意。

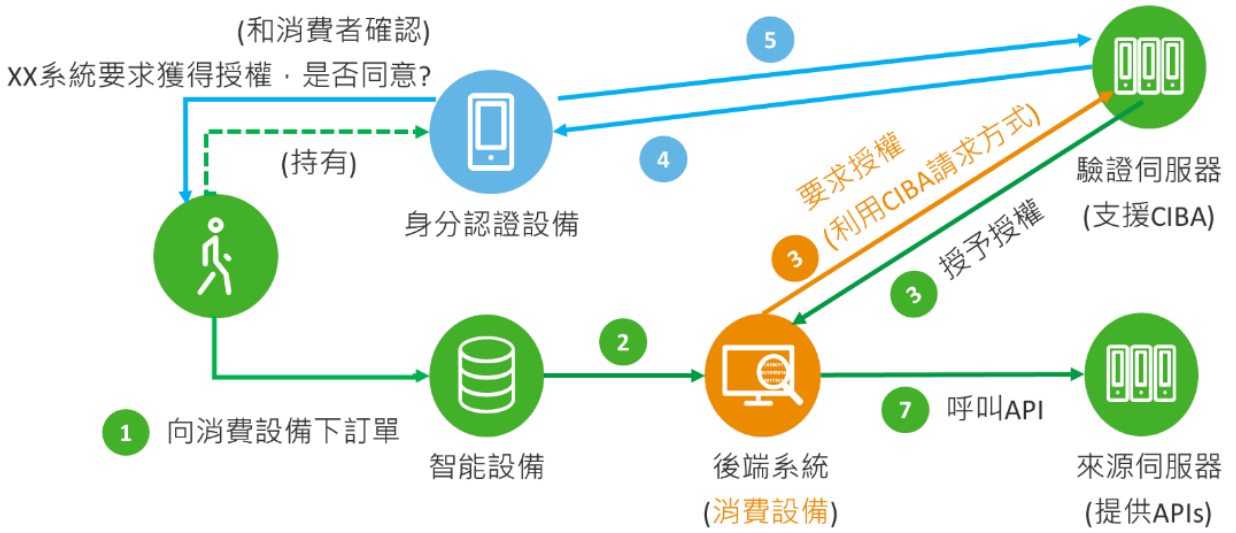

圖 14 CIBA 概念流程圖

另因應銀行 API 的存取方式(讀取與寫入)比單一讀取的存取方式具有更高的風險，故英國開放銀行標準框架中對於相應的安全控管機制增加了更多限制，主要分為三個部分：

1. 授權框架的安全性配置

FAPI 是以 REST API 為架構，可提供代表 JSON 較高風險資料做為資料格式。API 受 OAuth 2.0 授權框架的保護，適用於對金融數據的交易存取和其他類似的高風險存取，規定了對授權請求篡改、代碼注入、狀態注入和令牌請求網路釣魚等攻擊的控制。

2. 強制使用簽名 JWT (JWS) 來封裝請求參數

授權伺服器應使用「JWT 安全授權回應模式 JWT Secured Authorization Response Mode（JARM）」保護對消費者端的授權回應，從而允許消費者端請求授權伺服器在 JWT 中對授權回應進行編碼。

3. 限制可用於雙向 TLS 的密碼套件

限制可用於雙向 TLS 的密碼套件，交換機密訊息時，所有交互均應使用 TLS（HTTPS）進行加密，以降低傳輸層受損的風險。

(三) 澳洲：消費者資料權(Consumer Data Right, CDR)

在 CDR 的框架下，資料標準機構(DSB)制定了消費者資料標準(CDS)作為資安控管規範。從 API 管理面分析，CDR 要求資料持有者(如銀行等 ADI)等持有消費者資料的一方，必須在消費者的要求下，才能將資料傳輸給經認可的資料接收者(ADRs)。另外，基於 CDR 極為重視保障消費者權益的宗旨，CDR 要求 ADRs 應可讓消費者能夠決定哪些業者可以查看和使用自身的資料、亦可指定要傳輸的資料類型、希望將資料用於什麼目的、且隨時可以停止共享資料或要求刪除不再需要的資料等。另外值得注意的是，CDR 要求 ADRs 僅能保留消費者資料最多 12 個月，此項在其他國家無特別為此訂定規範。

CDS 部分則是在 Security Profile 中有進行更詳細的說明。不過因澳洲當時制定 Security Profile 時，其設計係參考英國的 Financial Grade API (FAPI) Profile 及 Open ID Connect (OIDC)，故與英國的安全管控機制相似。例如，二者皆以 REST API 為架構、OAuth 2.0 委任存取管理與採用 OIDC 與 FAPI 作為身份認證機制。此外，CDS 也嚴格要求資料的持有方(Data Holders)必須支援 Private Key JWT Client Authentication 或 Self-signed JWT Client

Authentication 的身份驗證機制。

(四) 新加坡：API 指導手冊(Finance-as-a-Service: API Playbook，簡稱 Playbook)

Playbook 提供業者在選擇、設計、使用金融 API 時的指引，其中並未細分 Public API 或 Partner API。以下將從治理模式和整理說明 Playbook 提供之資料和安全標準建議。

■ **API 治理模式**

1. 對 API 的監管考量

為提供金融機構的消費者一致的服務等級並建立信任，金融科技公司在串接金融業者的 Partner API ，其開發及部屬 API 產品和服務時也應遵循相關政策及指引。其中 Playbook 分為兩種模式說明：

(1) 金融機構<u>擁有</u>透過第三方服務業者所取得的使用者經驗：

此模式屬於金融機構的委外(outsourcing arrangement)作業，其第三方服務業者應遵循 Technology Risk Management Guidelines (TRMG) 和 Outsourcing Guidelines 兩份規範。

(2) 金融機構<u>不擁有</u>第三方服務業者取得的使用者經驗：

此模式將不屬於金融機構的委外作業。但 Playbook 鼓勵金融機構與金融科技公司仍應遵循下列基本風險管理原則：

■ **Know-your-API consuming partners**

金融機構應盡可能製定明確的審查流程來管理第三方及其他合作夥伴的 API 的存取。以協助金融機構確保只有合格的單位才能獲得對指定 API 服務的

授權，並確保其存取有受到控制。同時，審查標準應可能包括業務性質、組織的安全政策、行業聲譽和過往記錄等。

- **消費者資料保護**

  為保護消費者資料的機密性和安全性，並確保金融機構的穩定性和聲譽不受到損害，MAS 建議金融機構和金融科技公司應遵守《Personal Data Protection Act》(個人資料保護法)，並在傳輸、處理和存儲過程中對敏感的消費者資料的安全和保護採取最佳實踐保護措施，如 Playbook 中的 InfoSec 指南和 TRMG 的附錄 E 和 F 的規範。

2. 資訊安全標準(InfoSec)

Playbook 在 InfoSec 標準裡將資訊安全標準分成 7 項構面，包含身份認證、加密、授權、主機代管安全性、開發安全、脆弱性評估與滲透測試、強健的故障自動切換機制，以下針對身份認證、加密、授權、主機代管安全性與脆弱性評估與滲透測試進行簡介，並就各構面可採行之管理機制進行探討。

(1) 身份認證

- OAuth 2.0 委任存取管理

  建議採用 OAuth 2.0 委任存取管理，在基於 OAuth 的授權中，使用者在資源所有者的控制下請求對資源的訪問，提供 Web 應用程式，桌面應用程式，行動電話和家庭自動化設備等授權。

- SAML

  建議採取安全主張標記式語言 Security Assertion

Markup Language（SAML），是基於 XML 的身份驗證標準規格，目的是為了將不同安全性網域之間的身份驗證資訊進行整合。企業、政府機構、非營利組織和服務提供商都可使用它來啟用單一登錄（SSO）功能，SAML 的運作方式是由提供者將有關個人選擇的資訊傳遞給服務提供者，確保使用者的驗證資訊不被洩漏。

- 雙因子認證

  惡意攻擊者為了進行不法行動，需要找到一個入口點著手，例如利用某人的登錄憑證就。雖雙因子認證 Two Factor Authentication (2FA)並非不可破壞，但由於需要兩個不同的憑證才能獲得訪問權限，因此可降低帳號密碼遭假冒或竊用之風險，使惡意攻擊者難以輕易地觸及系統資料。2FA 則提供簡便的註冊過程，在確保安全性的同時，也能提供出色的消費者體驗。

(2) 加密

- TLS V.1.2

  TLS V.1.2 安全傳輸協議允許在傳輸或接收任何資料之前，就加密算法和密鑰進行協商和達成協議，保障隱私安全以及資料的機密性與完整性。另在 API 環境中建置 TLS 可減少 API 漏洞發生的機會，避免資料遭不法人士竊取。

- RSA Public/Private 金鑰加密 & AES 128/192/256-bit 加密

  RSA 加密演算法與 AES 進階資料加密標準為目前最為流行且安全性較高的加解密演算法，可以避免駭客從中監聽或讀取未加密的資料。

(3) 資料完整性標準

資料標準有助於定義雙方用於資料交換的參考框架，在描述當多方希望共享任何資訊與訊息時，能夠幫助接收方立即使用。

- JSON Web Token（JWT）

JWT 提供了一種輕量級的自主機制，用於在各方之間作為 JSON 對象安全地傳輸資訊。該資訊是經過數位簽章(Digital Signature)，可被驗證且信賴度較高。可以使用密碼（經過 HMAC 算法）或使用 RSA 的公鑰或私鑰來對 JWT 進行簽章，以確保發送者身份的正確性。

- Web 服務安全 (WS-Security)

WS-Security 定義了保護資訊完整性和機密性的功能，此協定包含 SAML（安全斷言標記語言）、Kerberos 和 X.509 等，主要用於通過 XML 數字簽章保護 SOAP 訊息、通過 XML 加密保護機密性以及通過安全性令牌保護憑證傳遞，確保端點到端點的傳輸安全性。

(4) 主機代管安全性

通過國際標準組織所制定的國際標準加強組織主機之安全，如 ISO27001 資訊安全管理系統、ISO22301 營運持續管理系統，有助於企業有效保護其資訊之安全與確保業務中斷之連續性等。

- ISO27001 資訊安全管理系統

為保護組織保護其資訊資產，如財務資料、智慧財產等，組織參考 ISO27000 系列，如 ISO27001 等標準，可加強組織管理資產的安全性與保護被交換的資訊資產。

- ISO22301 營運持續管理系統

  組織可參考 ISO22301，其為一項營運持續管理系統標準，替組織建立減少突發事件所帶來之衝擊，與當發生營運威脅時減少組織停工時間並加速復原等，旨在消除營運中斷的風險確保業務中斷時之連續性。
- PCI DSS 支付卡產業資料安全標準 為保障支付卡片持卡人相關的資料安全，組織應參考支付卡產業安全標準協會所制定的支付卡產業資料安全標準 PCI DSS，以確保於支付卡資料的儲存、處理與交換等相關作業之安全。

表 22　InfoSec 7 大資安標準構面及對應採行機制對照表

序	構面	可應用之機制
1	身份認證(Authentication)	■ OAuth 2.0 ■ OpenID Connect ■ Security Assertion Markup Language (SAML 2.0) ■ Two Factor Authentication (2FA)
2	加密(Encryption)	■ 加密： 　■ Transport Layer Security (TLS) v 1.2 　■ RSA Public/Private Key Encryption 　■ AES 128/192/256-bit Encryption 　■ Secure File Transfer Protocol (SFTP) ■ 資料完整性： 　■ JSON Web Token (JWT)

序	構面	可應用之機制
		■ WS-Security ■ Keyed-Hash Message Authentication Code (HMAC)
3	授權(Authorisation)	■ OAuth 2.0 ■ ISO 10181-3 Access Control Framework
4	主機代管安全性 (Hosting Security)	■ ISO27001 ■ ISO22301 ■ The Payment Card Industry Data Security Standard (PCI DSS)
5	開發安全(Security Coding)	■ 該手冊無進一步說明
6	脆弱性評估與滲透測試 (Vulnerability Assessment & Penetration Testing)	■ 該手冊無進一步說明
7	完整的故障自動切換機制 (Robust Failover Mechanisms)	■ 該手冊無進一步說明

(五) 香港：香港銀行開放 API 框架

在考慮架構，安全性和數據標準時，HKMA 認為相容性是縮短銀行與 TSP 服務整合磨合期很重要的要素。因此，香港的 API 框架建議使用以下標準：

1. 架構

有關 TSP 網站或行動應用程式如何連接到銀行的 Open API，HKMA 提出兩種常見的通訊協議 -- Representational State Transfer (REST) 與 Simple Object Access Protocol (SOAP)。而資料格式則為通常使用

JavaScript 物件表示法(JSON)和可延伸標記語言(XML)。考量上述方式的實用性和業界廣泛的接受度，HKMA 建議將 REST 作為通訊協議，將 JSON 作為資料格式。

2. 安全性

為了對銀行與 TSP 業者進行身份驗證，並對所傳輸的資料進行完整性與機密性的檢查，HKMA 建議使用 X.509 格式標準，以確保從銀行提取產品與服務資訊的安全性。HKMA 也建議使用傳輸層安全性協定（TLS）進行數據傳輸，以提供完整性檢查與加密保護，並採用 OAuth 2.0 做為身份授權方法，只有在在消費者提出請求時，才會授予 TSP 業者權限。

3. 資料標準

為了幫助銀行可以快速且即時與 TSP 業者進行服務整合，允許各銀行自由使用自己的資料定義與設定標準。銀行應參考行業慣例公布其資料定義(通常稱為資料字典 Data dictionary)。如使用 Swagger 知名且廣泛使用於實踐 Open API Specification 的工具。

(六) 臺灣：大框架要求，範圍內自由發展

目前我國針對金融業的 Open API 管理方針，係採取如香港、新加坡自願自律的作法，由主管機關、銀行公會及財金公司共同訂定 API 規格與標準，透過既有法規作為遵循要求基準，並搭配銀行公會訂定自律規範以及規格，以「大框架要求，範圍內自由發展」的概念，給予金融機構自行挑選合作的 TSP 廠商及資料共享與制定標準的空間，增加其規格之彈性，使金融服務創新能在各個金融科技應用組合間發酵。

就監管密度來說， 現行 TSP 業者需遵循二大規範：其一是銀行公會所制定的業務合作自律規範；其二則是由財金公司所擬定

之業務安全控管作業規範及 Open API 技術標準規格書。

1. 臺灣 Open API 技術標準規格[18]

(1)連線安全：依據規範，TSP 業者、財金公司與銀行間連線都須採用加密傳輸，並參考 PSD2 的設計(建議採用 QWAC 標準所發之憑證)，在臺灣建議使用授權的 CA 憑證公司發放憑證為主，如臺灣網路認證公司、中華電信 Digicert。

(2)憑證作業：採 TLS 雙向認證，並區分為「TSP 通訊憑證」、「Bank 通訊憑證」，以及「FISC 通訊憑證」。

(3)認證機制：若 TSP 直接介接金融機構，則根據標準要求，金融機構應依現行管控機制辦理；若 TSP 是由財金公司轉接金融機構，將採 TLS 雙向認證方式。財金公司將於 API 訊息結構 HttpHeader 中，提供 TSP 資訊包括憑證序號（X-CSN）、發證單位（X-ISR）、來源 IP（X-CIP）予金融機構辦理認證作業。綜上，財金公司要求 TSP 的代理存取端與金融機構的資源伺服器或授權伺服器間，應建立認證機制，相關必要措施如下：

A. 採用 TLS 雙向認證或以簽章之 JSONWebToken（JWT）進行認證；

B. 採用憑證者，應驗證憑證及憑證鏈的正確性和有效性

C. 應以事先設定的來源網路位置(IP)正面表列管制。

(4)開發過程：鑒於 Open Banking 使用 REST API 技術架構，因此 TSP 業者與金融機構在設計時建議以 Swagger 或

[18] https://www.cio.com.tw/open-bank-towards-phase-2-open-api-technical-compliance-and-test-description/

OAS (OpenAPISpecification) 為設計、開發及佈署的共通文件，並使用 YAML 檔案格式。

經研究分析上述各重要市場的 API 控管規範及治理模式，可歸納出以下現況：

1. 強制推行的國家對於技術規格已訂有嚴格且明確的標準

採取強制政策的歐盟、英國及澳洲，在 API 資安規範中針對各個風險點已採取相應的控管措施，對於各個技術規格也已制定嚴格且明確的標準並公開發布，使銀行與 TSP 業者能夠清楚了解各資訊標準要求以利遵循。

2. 鼓勵推行的國家在資安規範要求的顆粒度較寬鬆

採取鼓勵政策的新加玻與香港，在 API 控管規範與治理模式針對各個風險所採取的身份認證，加密技術與授權機制等，與採取強制政策國家大致相符。不過雖然其管控框架與方向明確，但 API 資安規範與細節的描述顆粒度較其他採行強制政策的國家寬鬆。

3. 我國 API 安控現況

我國目前在 API 的安全標準規範上的廣度與強度理論上將可有效減緩 OWASP 所列 10 項 API 風險。相較於新加玻與香港同樣採取鼓勵政策的國家，我國的規範考量到更多可能發生的風險，控管的範圍牽涉更廣。

(七) 美國

目前《Dodd-Frank 法案》之 1033 條為美國針對消費者獲取其財務資訊的唯一明文法，消費者有權獲取其相關金融資訊如帳戶以及交易資料以促進金融服務市場，提供消費者優質的使用體驗與創新的服務。但該法要求 CFPB 應與聯邦銀行機構進行協商制定相關

規範，無法單獨制定與行動。消費者資料保護相關議題需要聯邦銀行機構和 CFPB 之間的協調與合作。此外，除了該法案之外，美國尚未建立明確的開放銀行法源依據且未有跡象表明該國正在研議與制定新的開放銀行相關法規。

六、建議措施

本節將將延續第貳章第四節之 OWASP 發布之十大 API 安控風險作為分析架構，包括無效的對象層級授權、無效身份認證、過多資訊洩漏、缺乏資源與速率限制、無效功能權限控管、批量配置不當、不安全的組態設定、注入攻擊、版本控管不當以及紀錄與監控不足等，逐一對比臺灣開放應用程式介面(Open API)業務安全控管作業規範後，以對我國現行規範缺乏或較為薄弱之處，提出四項參考建議：

(一) 監控與限制性能與可用性

針對《OWASP API Security Top 10》第四項：缺乏資源與速率限制(Lack of Resources & Rate Limiting)，我國現行規範尚未針對此風險進行控管，為了避免攻擊者大量使用者的特定 API 進行阻斷服務攻擊，造成服務停擺，TSP 業者應參考歐盟 EU-RTS 針對 API 可用性和性能，包含 API 回應時間、呼叫速率、失敗率等進行即時監控，並透過蒐集與定期審查關鍵性能指標 KPI 來建立視覺化報表，進行主動且即時的監控，避免因 API 低可靠性與低穩定性而產生負面影響，以改善客戶體驗，提高用戶對於使用 Open API 的信任。

針對我國開放銀行下一階段將開放交易面業務，本研究建議應參考歐盟作法，TSP 業者應參考主管機關所訂定之參考詐欺率(Reference Fraud Rate)建立相關交易詐欺監控機制，定期審查詐欺交易的統計報告，含詐欺的行為、事件的數量、總價值與支付類型等，如超過適用的參考欺詐率，應向主管機關提供其採取措施的說明，用以恢復欺詐。透過對於所蒐集數據的評估，識別出系統的風險，並制定解決方案以減少詐欺的發生率。

(二) 強化存取控制管理

根據《OWASP API Security Top 10》第五項：無效功能權限控

管(Broken Function Level Authorization) 之界定，API 的存取控制為組織最常見且最疏於控管的弱點之一，攻擊者可透過後台權限控管不完善的弱點去存取帳戶敏感資料或冒充用戶，導致未授權的資訊洩露、資料竄改、惡意竊取資金或接管帳戶等災害。本研究進而提出以下建議：

1. 建議規範參與開放銀行之 TSP 業者，應實行嚴格的存取控制管理，不同角色的存取權限必須嚴格控管，避免疏於設定權限控管機制，增加資料外洩的機會與駭客透過暴力破解取得存取權限的風險。組織或其管理者應確保每個 API 功能皆設有權限控管，並且明確的定義與指定各角色可以存取與訪問的功能，以最小化權限為原則，限制角色可執行的範疇，減低越權存取其他用戶資源的機會。
2. 建議規範參與開放銀行之 TSP 業者，應定期審查帳號權限與徹底盤查特權帳戶為不可或缺的必要措施，組織必須清楚了解誰可以存取哪些資料，並確保對有價值的資產和系統實施適當的限制。除此之外，組織內離職或調職員工與委外廠商等人員也必須透過定期審查權限，並進行相關權限控管或移除。
3. 以上兩點建議雖主要為 TSP 業者應自行加強管理，但因 API 的存取控制管理不當而導致資料外洩與竊取個資事件層出不窮，銀行應加強監督，共同承擔保護客戶資料的義務。

(三) API 開發掌握

TSP 業者應對 API 的設計與開發進行嚴格的管理。若該企業無法完全掌握開發流程與細節，以及 API 攻擊可能發生的來源，將會使 API 設計疏失成為攻擊者嘗試突破的入口，進行資料的竊取或更進一步的攻擊。

因此，TSP 業者應建立研發團隊與資安團隊間的良好溝通管道，建議參考歐盟作法，要求業者須完整編制 API 文件與安全措施的實施辦法，並且定期由內部或外部獨立且合格的稽核員進行審視及評估。此外，TSP 業者應清楚了解已部屬了多少 API，以及目前有多少人正在使用這些 API，並對 API 相關資訊進行盤點，如 API 型態、使用方式、URL 命名、規則、參數等，如此可增加組織針對 API 的設計及開發的掌握度並確保 API 設計完善，透過定期盤點協助組織確保 API 開發掌握度，避免發生未知或未被保護的 API 疏於管理的狀況。

(四) 威脅防護

公開數據、服務和交易活動的整合是實現更有效率金融創新的新興商業模式，是朝向 Open API 邁進的更廣泛計劃的一部分。但因渠道的擴張會增加組織網路的滲透性，使駭客得以利用新的或已知卻尚未修補的漏洞，如《OWASP API Security Top 10》第七項：不安全的組態設定(Security Misconfiguration)、第八項：注入攻擊(Injection)、跨站腳本(XSS)、系統版本過於老舊等問題，增加企業遭受網路攻擊的風險與竊取機敏資料造成個人資料外洩的機會。因此，相關的漏洞檢測、安全測試或採用外部專業服務是強化開放銀行 Open API 平台之安全的必要手段。

1. 漏洞檢測

系統弱點掃描、網站弱點掃描、滲透測試、源碼掃描等檢測應依照規範要求之頻率執行。為求有效抵禦 API 安控威脅，除定期執行前述漏洞檢測外，應針對所識別出的漏洞進行修補。作法上，不應只是將漏洞補起來，而是要用正確的方式把問題根除。因此，TSP 業者在針對掃描與測試的結果進行風險評估後，應針對高風險事項訂定改善措施並確認後續追蹤機制；避免因未能及時改善應訂定處理時程計劃，導致高風險漏

洞發生無人追蹤管控之情況。

2. 參數竄改測試

基於對客戶端和伺服器之間通過 API 請求發送的參數，仍有被惡意攻擊者篡改的風險。例如，更改用戶憑證、權限或產品的價值與數量等。而 TSP 業者應執行參數篡改測試，以減低威脅發生的可能，確保攻擊者無法輕易竄改 API 中的參數。

3. 導入威脅防護產品

TSP 業者內部自行建立的解決辦法可能無法有效的防禦外部攻擊，應考慮採用適當的威脅防護產品來針對重要的 API 實施有效的防護，補強內部防禦能量的不足，避免 TSP 業者因環境、作業習慣、安全控管及偵測機制不足造成系統及資料安全風險。

建議針對開放銀行參與之 TSP 業者導入相關防護產品，並依產品類別進行宣導並建置相關規範，包含威脅偵測、網路入侵防護以及防護管理等。例如鼓勵使用自動化機制監控終端用戶活動，實時監控和分析等，皆可即時幫助組織發現偏離正常使用模式的違規行為，降低威脅風險。

表 23 各國 Open API 規範檢視

國家規範與策略 / API 風險	鼓勵策略			強制策略		其他
	臺灣	新加坡	香港	歐盟	英國	澳洲
	Open API 技術標準規格書、業務安全控管作業規範	API 指導手冊	開放 API 框架	PSD2	開放銀行框架	CDR
API1:無效的對象層級授權	• OAuth 2.0 • 確保授權機制安全性	• OAuth 2.0	• OAuth 2.0	×	• OAuth 2.0 • OpenID Connect(OIDC) • CIBA	• OAuth 2.0 • OpenID Connect(OIDC)
API2: 無效身份認證	• 嚴格的密碼原則 • 身份驗證(OTP/2FA)	• WS-Security/ SAML • 身份驗證(2FA/OTP)	• 身份驗證(2FA) • X.509	• 嚴格交易監控機制 • 強身份驗證(SCA)	• 身份認證保證等級(LoA) • FAPI profile • CIBA	• 身份驗證(OTP) • 身份認證保證等級(LoA) • FAPI profile

國家規範與策略 / API 風險	鼓勵策略			強制策略		其他
	臺灣	新加坡	香港	歐盟	英國	澳洲
	Open API 技術標準規格書、業務安全控管作業規範	API 指導手冊	開放 API 框架	PSD2	開放銀行框架	CDR
API3: 過多資訊洩漏	• 加密技術 (RSA/AES)	• 加密技術 (RSA/AES)	• 加密技術	• 加密技術 • 個資進行遮罩	• 加密技術 (RSA/AES)	• 加密技術 (RSA/AES)
API4: 缺乏資源與速率限制	×	×	×	• 監控效能與可用性 • 限制用戶請求次數	• 錯誤回應機制 • 監控效能與可用性	• 錯誤回應機制
API5: 無效功能權限控管	• 存取控管機制 • 定期審查權限	×	×	• 存取控管機制 • 定期審查權限	• 存取控管機制 • 定期審查權限	• 存取控管機制 • 不留存消費者密碼

國家規範與策略 / API 風險	鼓勵策略			強制策略		其他
	臺灣	新加坡	香港	歐盟	英國	澳洲
	Open API 技術標準規格書、業務安全控管作業規範	API 指導手冊	開放 API 框架	PSD2	開放銀行框架	CDR
				• 條件式禁止代理登入		
API6: 批量配置不當	• HTTP Headers(OPEN API 之設計原則)	×	×	×	×	• HTTP Headers
API7: 不安全的組態設定	TLS	TLS	TLS	TLS	TLS	TLS

國家規範與策略 / API 風險	鼓勵策略			強制策略		其他
	臺灣	新加坡	香港	歐盟	英國	澳洲
	Open API 技術標準規格書、業務安全控管作業規範	API 指導手冊	開放 API 框架	PSD2	開放銀行框架	CDR
API8: 注入攻擊	• 應進行欄位格式檢查	×	×	×	• 採用 OpenID Connect Hybrid Flow	• 採用 OpenID Connect Hybrid Flow
API9: 版本控管不當	• 遵循變更控制程序 • 由兩人以上進行營運環境變更	• 遵循版本控制規範 (Versioning)	×	• 遵循變更控制程序 • 遵循測試框架	• 遵循變更控制程序	• 遵循版本控制規範 (Versioning)
API10: 紀錄與監控不足	• 妥善保留日誌及稽核軌跡	• API 監控機制(Measure phase)	• 持續監測網路行為	• 遵循交易日誌紀錄安全機制	×	• 妥善保留日誌及稽核軌跡 • 定期檢視日誌識別異常狀況

國家規範與策略 / API 風險	鼓勵策略			強制策略		其他
	臺灣	新加坡	香港	歐盟	英國	澳洲
	Open API 技術標準規格書、業務安全控管作業規範	API 指導手冊	開放 API 框架	PSD2	開放銀行框架	CDR
	• 進行異常紀錄分析，設定告警指標			• 監控安全事件		

資料來源：本研究整理

肆、TSP 業者與銀行合作後的代理登入之議題分析研究

隨著開放銀行的發展以及消費者對隱私意識的提升，「消費者賦權」議題也浮出檯面。在各國對金融科技、金融創新表示正面的支持後，業者紛紛推出各式金融創新服務，積極的希望在市場上取得消費者的青睞、搶先佔有市場。然而，若欲提供消費者更加客製化的服務，「取得消費者的金融資料」將是各 TSP 業者的第一步門檻；在所有推動金融創新的市場中，也並非所有金融機構都有資源並願意與 TSP 業者合作。現在，許多國內外 TSP 業者嘗試透過代理登入、爬蟲技術(Screen Scraping)等其他方式嘗試取得發展服務下所需取得的資料，而其安控議題也逐漸成為討論焦點。

一、代理登入和爬蟲技術

爬蟲技術自 1990 年代後期在美國開始興起，爾後開展至歐洲甚至澳洲。該技術普遍應用在帳戶整合平台的商業模式當中。如今則更應用在廣告投放、價格彙總、預算應用、網站保存、學術研究、新聞...等多方使用情境。在開放銀行上，屬於分析型的新創公司初期也會透過爬蟲技術抓取公開資料以進行分析。

代理登入指的是 TSP 業者在取得消費者的授權及其帳號、密碼、代號、金鑰等與系統登入相關資訊的前題下，以爬蟲技術在不與企業建有合作關係的情況下獲得資訊。在金融領域上，該技術通常被貸方、財務管理應用程式、個人財務儀表板和會計產品等服務所運用，以利在取得消費者同意的前提下檢索客戶的財務資料，如消費者銀行帳戶餘額或信用卡刷卡紀錄，並傳輸回 TSP 業者的伺服器中進行儲存或處理，藉以提供消費者服務。

二、國內外應用代理登入個案分析

(一) 臺灣麻布記帳

臺灣麻布記帳 APP -- Moneybook，其服務提供了消費者連接個人網路銀行及證券資料的便捷管道。Moneybook 提供國內 30 家銀行與 13 家證券業者進行 API 或代理登入。會員在提供第三方金融機構網路銀行的用戶登入資訊之後（包含帳號、密碼、代號、金鑰以及相關所需資訊），即授權 Moneybook 麻布記帳在為會員提供約定之服務範圍，以合法代理人身份登入第三方金融機構存取網路銀行業務。Moneybook 提供金融產品資訊與提供銀行或其他公司之帳戶資訊，可選用 API 或是代理登入方式進行。客戶在 Moneybook 進行金融交易或繳費服務時，該 APP 會使用代理登入的方式彙整呈現消費者金融資料異動狀況。惟經研究團隊實際下載使用，目前該 APP 並未具備直接扣款等交易功能。

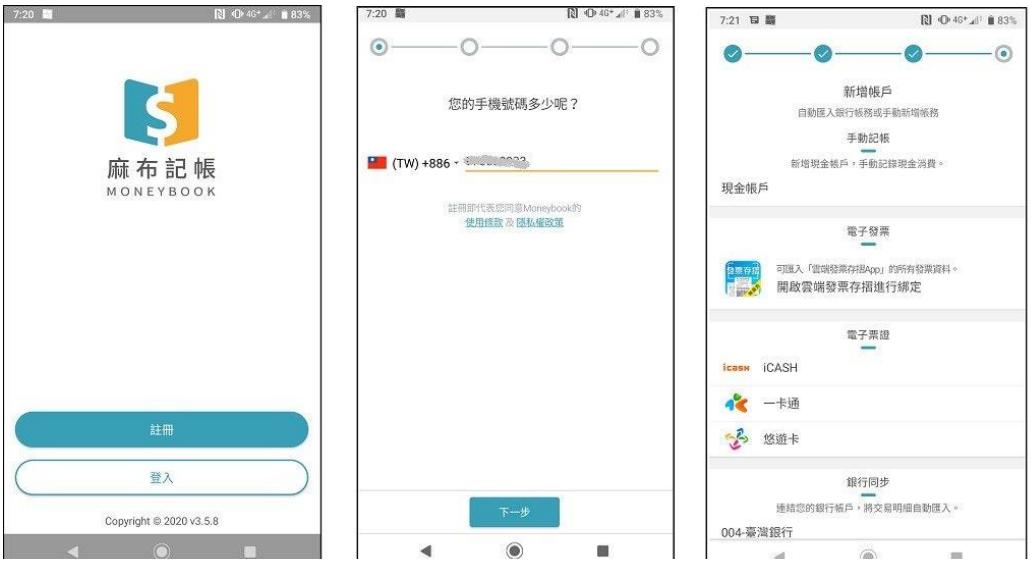

圖 15　Moneybook 麻布記帳應用程式畫面

資料來源：研究團隊以 Android 行動裝置截取 (版本：A920FXXS5CUD1)

(二) 香港個人理財 APP – GINI[19]

香港第一個個人理財 APP--GINI，提供的服務包括為消費者連接個人網路銀行及信用卡等金融資訊。目前，GINI 提供與海外 60 多個國家的銀行進行資料同步，並獲得英國 FCA 的授權。

然而，研究團隊實際下載操作試用後，從其 APP 的畫面判斷，GINI 亦是透過代理登入的方式進行資料抓取(附上申請同步 DBS 資料截圖)。且可能因受到歐盟對於代理登入的禁止政策，歐洲區域的銀行如英國的 Lloyds Bank、德國的 Deutsche Web Banking 等皆相繼出現「伺服器錯誤」的結果。後來 GINI 在官方網站中陸續發佈部分銀行暫時停用的公告。

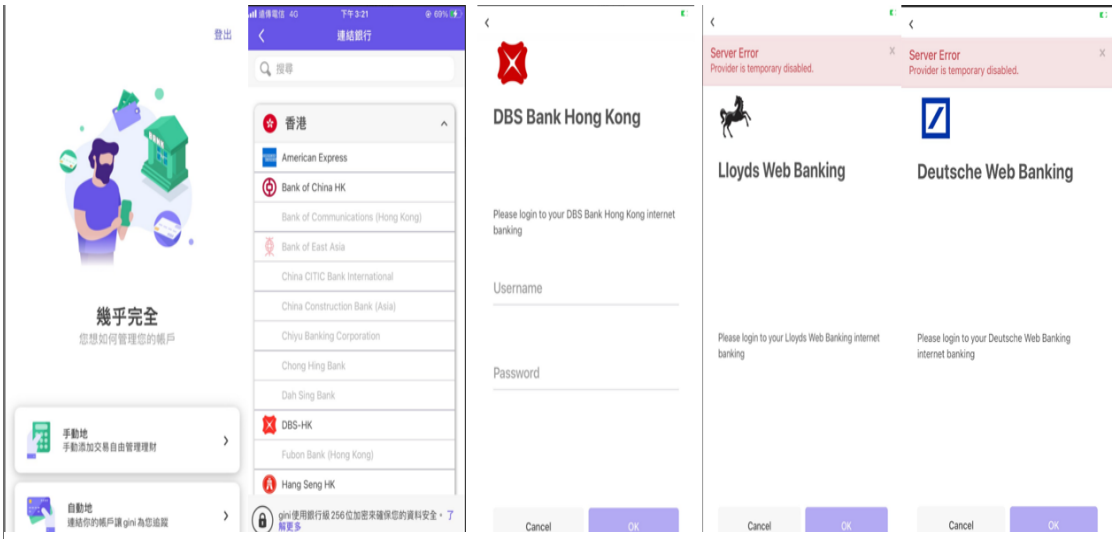

圖 16 香港第一個個人理財應用程式 GINI 應用程式畫面

資料來源：研究團隊以 Android 行動裝置截取 (版本：A920FXXS5CUD1)

[19] https://app.gini.co/zh/

(三) 美國軟體 – Mint

JPMorgan Chase 因客戶隱私保護疑慮，於 2017 年與 Intuit Mint 簽署同意書，同意透過 API 分享其客戶金融資訊給 Intuit 旗下公司 (例如: Mint、TurboTax Online 、QuickBooks Online)的應用程式使用。JPMorgan Chase 的客戶能夠自主決定是否將個人金融資訊給 Intuit，在其分享給 Intuit 資料前，客戶會明確表明同意意向，一但客戶的同意獲得驗證，JPMorgan Chase 會提供 token 給 Intuit，讓 Intuit 取得客戶的銀行資訊，客戶因此無須提供其銀行帳號密碼給 Intuit。

透過 API 串接，JPMorgan Chase 客戶將能夠快速地在 Intuit 的應用程式中檢視自己的銀行資訊，客戶亦可隨時終止或啟用 Intuit 與 JPMorgan Chase 之間的連線。此外，根據 Intuit 的「資料監管原則 (原文:Data Stewardship Principles)」，Intuit 不會將客戶數據賣給第三方。

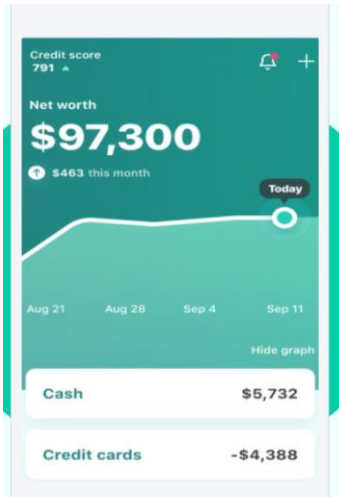

圖 17 美國軟體 Mint 畫面

資料來源：研究團隊以 Android 行動裝置截取 (版本：A920FXXS5CUD1)

(四) 新加坡軟體 – Wally[20]

Wally 是新加坡最受歡迎的記帳 APP 之一，受到超過 150 位理財專家、經濟日報、BBC 等推薦使用。Wally 提供消費者連接個人網路銀行及信用卡資料。目前，Wally 已可連結至海外 70 個國家、15,000 個銀行，並提供 200 多種貨幣選擇。研究團隊實際下載操作試用後，從 APP 的畫面判斷，Wally 使用的資料存取方式包含了代理登入及 API 登入。

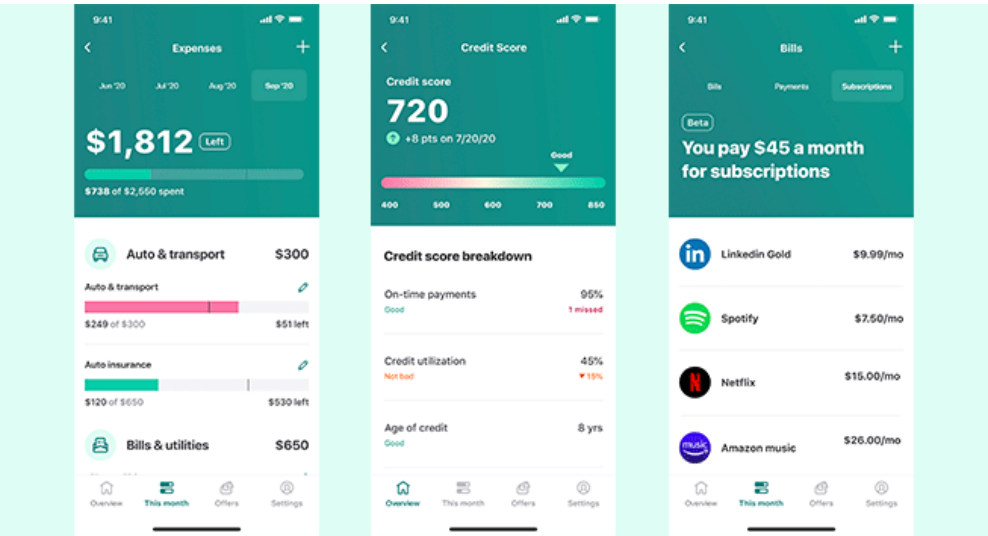

圖 18 新加坡軟體 Wally 畫面

研究團隊以 Android 行動裝置截取 (版本：A920FXXS5CUD1)

三、代理登入風險與個案研析

(一) 風險分析

整體流程上 TSP 業者是以消費者的代理人身份代為存取資料，

[20] https://www.wally.me/

然而普遍來說 TSP 業者其管理程度與金融機構既有管控機制強度有所落差。若消費者使用 TSP 業者代理登入之服務，而在過程中發生任何資安事件或個資事件時，TSP 的規模或資源可能無法承擔相對應的責任，進而導致消費者權益受到損害。以下將提供國際代理登入侵權案例與彙整代理登入風險，並從資訊安全、消費者(體驗與權益)、成本三大面向進行分類：

1. 帳密外洩

TSP 業者使用代理登入時，必須獲得消費者重要的帳號密碼資訊並儲存於組織伺服器端。然而其帳號密碼的儲存安控不夠完善，或甚至在代為登入的時候，TSP 業者必須以未加密的形式登入，都將可能導致使用者資料外洩的風險。

2. TSP 永久持有帳密

技術上來說，代理登入將提供 TSP 業者可以像消費者自己登入網路銀行，存取消費者的銀行帳戶。這意味著除了 TSP 業者自行自律執行安控要求、並刪除消費者的帳號密碼資料，否則消費者將無法對已提供給 TSP 的存取範圍、持續時間進行任何管控。而消費者唯一可以有效撤銷 TSP 對其的存取權限方法就只有更改登入密碼。

3. 消費者權益受損

當消費者提供其身份驗證資料予他人時，對於大多數銀行而言，將可能被視為自主違反帳戶的條款和條件，消費者有可能為 TSP 業者執行代理登入過程中所犯下的任何錯誤負責，進而損害消費者免受欺詐的保護。

4. 系統穩定性(存取的連續性)

代理登入(或爬蟲技術)作業方式是以掃描金融業者現有面向消費者的入口網站(如網路銀行介面)。因此若金融業者對於網路銀行有做任何微小的更改都可能為代理登入帶來系統穩定性問題。此風險除了將可能帶來差勁的消費者體驗之外，對 TSP 業者也意味著高昂的研發、人力與時間成本，因 TSP 業者必須反復修復因銀行微小的、意外的更改而損壞的功能，進而可能阻礙 TSP 業者投注資源至更好的功能。

表 24 代理登入的四大風險

類型	風險點	風險說明
資訊安全	帳密外洩	▪ 帳號密碼的儲存安控不夠完善 ▪ 以未加密的形式登入
資訊安全	TSP 永久持有帳密	▪ 帳號密碼資料可能被永久保存 ▪ 消費者難以控管 TSP 業者的執行作業
消費者權益受損	消費者權益受損	▪ 消費者有可能為 TSP 業者執行代理登入過程中所犯下的任何錯誤負責
消費者體驗差成本高昂	系統穩定性(存取的連續性)	▪ 消費者體驗差 ▪ 高昂的研發、人力與時間成本

資料來源：本研究整理

(二) 代理登入訴訟案例

1. 美國 Fintech 業者 Plaid，因被指控在尚未取得消費者同意

前，拿取消費者的銀行帳戶資訊，被罰款 5,800 萬美元。

這項訴訟起因於 Plaid 提供自家開發之 API 給 TSP 業者(包含 Venmo 等行動支付業者)，讓 TSP 業者能夠快速將自家應用程式與銀行連接，取得消費者的銀行帳戶資訊以提供金融服務。而 Plaid 被指控透過代理登入方式，撈取與其服務無關的客戶資料，在未取得消費者同意前，將資料提供給 TSP 業者。這項判決判罰 Plaid 5,800 萬美元，其中包含原告 11 人每人獲得 $5,000 美元，扣除律師費用後，剩餘金額平分給 9,800 萬位美國 Plaid 用戶，同時 Plaid 被要求減少取得之客戶資訊：Plaid 被法院要求未來只能取得為維持其營運的客戶銀行資訊量，以及提供新的使用介面：Plaid 將推出 Plaid Portal(新的 Dashboard 介面)，讓消費者能夠控管 APP 與銀行帳戶連線的狀態，能夠決定是否要保持或終止連線。

表 25 代理登入訴訟案例 Plaid 相關法律資訊

訴訟承辦單位	District Court for the Northern District of California
判罰法律基礎	1. California Consumer Privacy Act ("CCPA") 2. Comprehensive Computer Data Access and Fraud Act ("CDAFA") 3. California's Financial Information Privacy Act ("CalFIPA") 4. California Online Privacy Protection Act ("CalOPPA") 5. Computer Fraud and Abuse Act ("CFAA") 6. Stored Communications Act ("SCA") 7. Unfair Competition Law ("UCL") 8. California's Anti-Phishing Act
原告	11 位消費者(集體訴訟)。認為使用建置在

	Plaid API 上的 APP 時，Plaid 並沒有告知會拿取他們的銀行資訊或提供金融資訊給其他 TSP 業者。
爭議處理	罰款：判罰 Plaid 5,800 萬美元。原告 11 人每人獲得 $5,000 美元。扣除律師費用後，剩餘金額平分給 9,800 萬位美國 Plaid 用戶。 減少取得之客戶資訊：Plaid 被法院要求未來只能取得為維持其營運的客戶銀行資訊量。 提供新的使用介面：Plaid 將推出 Plaid Portal(新的 Dashboard 介面)，讓消費者能夠控管 APP 與銀行帳戶連線的狀態，能夠決定是否要保持連線或終止連線。

資料來源：本研究整理

2. 美國金融數據整合公司 Yodlee ，被指控未取得消費者同意，拿取消費者銀行帳戶登入資訊，並在消費者不知情的情況下，利用銀行帳戶登入資訊持續挖取客戶的銀行帳戶資料。

Yodlee 主要產品為金融數據彙整軟體，Fintech 業者安裝後便可取得用戶銀行帳戶資訊以提供金融服務，Yodlee 也會販售匿名金融數據資料給第三方如：PayPal。

表 26 代理登入訴訟案例 Yodlee 相關法律資訊

訴訟承辦單位	California district court
判罰法律基礎	1. California Consumer Privacy Act (CCPA) 2. California's Financial Information Privacy Act (CalFIPA) 3. The California Online Privacy Protection Act (CalOPPA) 4. The Gramm-Leach Bliley Act (GLBA) Privacy Rule
原告	1 位消費者，指控 Yodlee 蒐集個人帳戶資訊

	販售給第三方業者。
爭議處理	至此報告提交日尚未判決

資料來源：本研究整理

四、各國代理登入之議題管控

代理登入及爬蟲技術就法律層面分析並非簡單的法律領域，其牽涉到的個資保護議題及消費者資料權在各個區域市場上也有不同的看法。

(一) 歐盟

歐洲銀行管理局 (EBA)最初於 2018 年通過的 PSD2 法案中，因應強客戶身份驗證(SCA)，PSD2 中的 Regulatory Technical Standards(以下簡稱 EU-RTS)裡原是禁止 TPPs 再透過傳統的爬蟲技術抓取消費者個資，並強制 TPPs 改用 API 技術進行資料串接。[21]

然而 EU-RTS 的公告宛如扼殺多數市場上的 TPP 業者。EU-RTS 的要求除了大幅影響消費者的使用體驗之外(如半夜收到意外的消息警報，要求消費者進行身份驗證，以及至少每 90 天需重新授權 TPP)，更可能使多數 TPP 業者無法持續提供其創新服務；另外對於現階段無法撥出資源進行 API 串接的銀行業者來說，也因無 TPP 業者的服務，而降低消費者使用意願。

條件式禁止代理登入機制 [22]

[21] https://thepaypers.com/expert-opinion/open-banking-how-can-third-party-providers-succeed--1245820

[22] https://www.engage.hoganlovells.com/knowledgeservices/news/psd2-ban-on-traditional-screen-scraping-confirmed-in-final-strong-customer-authentication-rts

在經過數月的討論與評估下，歐洲執委會確認會禁止傳統的爬蟲技術，但禁止的前題為 TPP 業者「冒充為消費者」。若 TPP 業者「事先向銀行表明自己是 TPP」的話則可允許。而銀行也可以提供由銀行選擇其專用界面讓 TPP 業者來進行資料抓取。

1. 「應急計畫」

歐洲執委會原則上以 API 登入方式為原則。但金融機構所開放的 API 若未有完全符合特定安全條件，則該些金融機構應制定一份「應急計畫」。歐盟執委會表示，在部分條件下(連續 5 次 TPP 的 API 存取請求在 30 秒內皆沒有得到回覆)，TPP 可被允許使用爬蟲技術作為應急機制進行資料存取。

不過此時 TPP 業者必須表明其身份(而非傳統的「代理」消費者登入)。歐洲執委會也有針對此應急計畫對 TPP 業者訂定配套的限制措施，如存取、儲存及資料處理。

2. 「開放專用界面」

考量部分銀行可能尚未有資源開發 API 合作的情形，歐盟執委會開放由銀行選擇其專用界面讓 TPP 業者透過爬蟲進行資料抓取。然而銀行端必須確保該界面的功能皆正常運行、不會不公平地限制 TPP 存取，或者阻礙 TPP 業者提供支付作業、帳戶資訊服務。EU-RTS 也進一步規定此類「阻礙」可能包括：

(1) 禁止 TPP 使用消費者的安全憑證；

(2) 強制重新定向到 ASPSP 的身份驗證或其他功能；

(3) 需要超出 PSD2 要求的額外授權和註冊；和

(4) 需要額外檢查支付服務消費者的同意。

(二) 英國

延續 EU-RTS 的做法，FCA 於 2019 年更新其 PSRs 2017，強制禁止使用代理登入或爬蟲技術。但在法案公告的一年後，FCA 於 2020 年 12 月撤回 PSRs 的修訂[23]，並同步先以強客戶身份驗證和通用安全通訊方法的技術標準進行管理。

(三) 澳洲

澳洲雖對於消費者權利已訂有全面性的消費者資料權利 (Consumer Data Right) 制度，理論上應可以減少爬蟲技術的抓取需求。然而與歐盟/英國模式不同，在澳洲爬蟲技術沒有被明文禁止。故即使 CDR 制度已經到位，爬蟲技術依舊被部分單位作為資料抓取使用。

五、代理登入無法全面性禁止根因分析

綜合以上，目前世界各國皆未有「全面性」的強制關閉代理登入的方式。然而造就此結果之原因，經本研究透過訪談及公開資料研究發現，不單只是 TSP 業者端，銀行端也有其顧慮。以下摘整分析出四種「代理登入無法全面性禁止的原因」，說明如下：

(一) TSP 業者難以達到銀行合作門檻

TSP 業者若是新創公司，其人力、資源、組織架構可能都尚未到位；此時若欲與銀行合作，則銀行所要求的相關安控規範，例如導入 ISO27001，可能造成新創公司因預算、技術、人力的不足，導致無法跨過合作的門檻。

[23] https://www.pinsentmasons.com/out-law/news/psd2-fca-gives-temporary-lifeline-to-screen-scrapers

(二) 資安疑慮導致銀行不願意提供過多資訊

儘管政策發佈可透過 API 形式與銀行串接資料，由於法規對於銀行的控管通常較為嚴謹，且資料外流各責也會落到銀行端，造成銀行不願意提供過多機敏資訊予合作夥伴，因此儘管開放了相關 API 規範銀行可能最終也會選擇不開發此 API。

(三) 銀行無足夠預算可以建置 API

對大型銀行來說，因應合作夥伴需求客製 API 或因應新的政策開發 API，達成機會相比小型銀行會高出許多。如預算或開發人力較不足之小型銀行，可能無法因應需求開發 API 供其他合作夥伴使用。

從代理登入的風險、各國主管機關的管控嘗試以及目前市場上的使用原因分析，各國對於代理登入尚未能有一致的觀點與管控。然而有一件事情是一致的，那就是在管理代理登入或爬蟲技術時，必須配有配套措施，並在存取、儲存上設置限制，以避免影響消費者的使用權益。

六、代理登入與個資保護議題分析

我國法規對於個人資料之保護，主要關注「隱私與自主權保障」與「個人資料之安全（機密性、完整性、可得性）」兩面向。是以對金融消費者個人資料之保護，即落實於個人資料保護法（普通法）、特別法，以及與資訊安全相關之各項規範。至於金融消費者保護法，則著重保護金融消費者之固有財產，並非保護其個人資料，併此敘明[24]。

[24] 雖然金融消費者保護法第 10 條第 2 項規定「前項涉及個人資料之蒐集、處理及利用者，應向金融消費者充分說明個人資料保護之相關權利，以及拒絕同意可能之不利益；金融服務業辦理授信業務，應同時審酌

以下即按前述個人資料保護方向，依我國現行法規比較金融機構與 TSP 業者在開放銀行情境中，對消費者個資保護之法律責任。

(一) 隱私與自主權保障

1、 個人資料保護法與授權訂定之法規命令

A. 金融機構與 TSP 業者均為個人資料之蒐集機關

我國個人資料保護法（以下稱個資法）作為個資保護的普通法，目前僅區分「公務機關」與「非公務機關」兩類適用主體，並未就非公務機關再細分產業類別規範（應由特別法律訂之）。

非公務機關如基於自行決定之目的，蒐集、處理及利用個人資料者，即屬個資法上的蒐集機關（比較法有稱為控管者 controller，例如歐盟 GDPR），須遵守個資法關於非公務機關之義務（例如第 19 條蒐集、處理個人資料之要件、第 20 條利用個人資料之要件）；倘係受蒐集機關委託，為委託機關之目的，蒐集、處理或利用個人資料，則為個資法（及其施行細則）中的受託者（比較法有稱為處理者 processor，例如歐盟 GDPR），依個資法第 4 條規定[25]，視同委託機關，並應依個資法施行細則第 8 條規定[26]，受委託機關之監督。

借款戶、資金用途、還款來源、債權保障及授信展望等授信原則，不得僅因金融消費者拒絕授權向經營金融機構間信用資料之服務事業查詢信用資料，作為不同意授信之唯一理由」，惟此規範乃重申個人資料保護法中的「透明性原則（告知義務）」，以及「同意之任意性」，本質上未增加金融服務業的法律責任。

[25] 個人資料保護法，第 4 條：「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關」。

[26] 個人資料保護法施行細則，第 8 條：「I委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適

據此，在開放銀行情境中，金融機構作為消費者個人資料的原始蒐集者，基於其特定目的與法律依據（例如履行存款契約、信用卡服務契約等），蒐集、處理消費者之個人資料。如金融機構將消費者個人資料提供予 TSP 業者，可能構成目的外利用個人資料之行為，須符合個資法第 20 條第 1 項但書各款例外事由之一[27]（例如經當事人同意），始為合法。

而 TSP 業者並非受金融機構之委託，而亦係基於自己之目的（提供特定服務），自金融機構取得消費者個人資料，同屬個資法上的蒐集機關，即應滿足個資法第 19 條第 1 項各款依據之一[28]（應為「與消費者有契約關係」），方得為之。

此外，金融機構與 TSP 業者既均為個人資料的蒐集機關，即應各自遵守個資法上的其他義務（例如第 8 條與第 9 條的告

當之監督。II前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。III第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。IV受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關」。

[27] 個人資料保護法，第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益」。

[28] 個人資料保護法，第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害」。

知義務、第 10 條與第 11 條的當事人權利行使等）。

B. 安全維護義務內容為主要差異

然而，金融機構與 TSP 業者雖均非公務機關，同樣適用個資法第 27 條第 1 項關於安全維護義務之要求[29]，惟因兩者之中央目的事業主管機關不同，則金融機構尚須遵守中央目的事業主管機關即金管會，依據個資法第 27 條第 2 項與第 3 項[30]授權訂定之《金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法》，而 TSP 業者則另行遵循其中央目的事業主管機關（例如經濟部），依前揭個資法授權訂定之法規命令。

從而，如金融機構適用之《金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法》與 TSP 業者適用之法規命令內容不一致時，雙方對於消費者個人資料的安全維護義務細節即有落差。

C. 個資侵害事故的通報主管機關不同

行政院於 110 年 8 月 11 日頒訂《行政院及所屬各機關落實個人資料保護聯繫作業要點》，要求各中央目的事業主管機關，於其依個資法第 27 條第 3 項授權訂定之安全維護辦法中，規定所監理之非公務機關就個資侵害事故，對該中央目的事業主管機關之通報義務。

---

[29] 個人資料保護法，第 27 條第 1 項：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏」。

[30] 個人資料保護法，第 27 條第 2 項：「中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法」；第 3 項：「前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之」。

據此，金融機構如發生消費者個資侵害事故，通報對象為金管會；而 TSP 業者則依其所屬事業，通報其中央目的事業主管機關（例如經濟部），此亦為金融機構與 TSP 業者對於消費者個資之法律責任上的顯著差異。

2、 金融機構作業委託他人處理內部作業制度及程序辦法

本辦法係依銀行法第 45-1 條第 3 項授權訂定，就金融機構之委外作業訂有制度與程序規範。其中，第 7 條第 1 項第 1 款即要求金融機構之委外如涉及客戶資訊（個人資料）者，應與契約或另以書面方式，使客戶知悉委外事項，並依個人資料保護法規定辦理[31]。

相較之下，TSP 業者雖於個資法上亦承擔告知義務，但個資法未限制蒐集機關的告知方式，程序上不如金融機構所受之規範嚴謹。惟依現行《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 5 條第 1 項第 1 款規定[32]，銀行似可要求 TSP 業者須遵循本辦法，實質上使 TSP 業者亦適用相同規範，提高對消費者資訊自主（知情）權的保障。

3、 金融控股公司法與授權訂定之法規命令

金融控股公司法第 43 條第 2 項，對金融控股公司之子公司間

---

[31] 金融機構作業委託他人處理內部作業制度及程序辦法，第 7 條第 1 項第 1 款：「第四條第二項第三款規定金融機構作業委外，應就客戶權益保障訂定內部作業及程序，其內容應包括：一、如涉及客戶資訊者，應於契約簽訂時訂定告知客戶之條款；其未訂有告知條款者，金融機構應書面通知客戶委外事項，並應依個人資料保護法之規定辦理。……」。

[32] 中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範，第 5 條第 1 項第 1 款：「會員銀行應要求第三方服務提供者遵循下列事項：……一、第三方服務提供者應遵循洗錢防制法、資恐防制法、個人資料保護法、消費者保護法及主管機關所訂定之相關法令規定等及本會相關自律規範之要求。」。

以客戶個人資料為共同行銷訂有規定[33]，並於同條第 3 項授權主管機關就共同行銷之條件、程序、業務範圍、資訊交互運用等應遵循事項訂定規範（即金融控股公司子公司間共同行銷管理辦法）。

據此，如參與開放銀行應用之銀行屬金融控股公司之子公司，對於消費者個人資料運用，尚須遵循前揭法規。相較之下，TSP 業者則不受此規範拘束。

4、 金融科技發展與創新實驗條例

本條例為普惠金融及金融科技發展而生，旨在建立安全之金融科技創新實驗環境，落實對參與創新實驗者及金融消費者之保護。

依本條例第 23 條第 3 項規定[34]，申請人對於參與者資料之蒐集、處理及利用，仍回歸個人資料保護法之規定。據此，如 TSP 業者金融科技創新實驗之申請人，其對參與者之個人資料保護責任，亦依前述個人資料保護法規範認定。

(二) 個人資料之安全（機密性、完整性、可得性）

1、資通安全管理法

資通安全管理法之保護標的，當包含個人資料在內，如作為開放銀行參與者之金融機構，經指定為關鍵基礎設施提供者時（成為資通安全管理法上的特定非公務機關），即應遵守該法對於特定非

[33] 金融控股公司法，第 43 條第 2 項：「金融控股公司之子公司間進行共同行銷，其營業、業務人員及服務項目應使客戶易於識別。除姓名及地址外，共同蒐集、處理及利用客戶其他個人基本資料、往來交易資料等相關資料，應依個人資料保護法相關規定辦理」。

[34] 金融科技發展與創新實驗條例，第 23 條第 3 項：「申請人對於參與者資料之蒐集、處理及利用，應符合個人資料保護法相關規定」。

公務機關之特別規範（例如第 16 條至第 18 條）。相較之下，TSP 業者若非資通安全管理法定義之特定非公務機關[35]，則不受該法拘束，其對資訊（包含個人資料）安全之義務即與經指定為關鍵基礎設施提供者之金融機構相異。

2、其他特別規範

銀行等金融機構之資訊安全重要性不言可喻，是我國對於金融機構之資訊安全訂有層層規範，且依技術發展時有增訂，例如《金融機構作業委託他人處理內部作業制度及程序辦法》、《金融機構辦理電腦系統資訊安全評估辦法》、《金融機構提供 QR Code 掃描支付應用安全控管規範》、《金融機構辦理資訊安全滲透測試計畫》、《信用卡業務機構辦理行動信用卡業務安全控管作業基準》等。

因 TSP 業者並非金融機構，本無前述規範之適用，但依前述《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 5 條第 1 項第 1 款規定，銀行可要求 TSP 業者遵循金管會訂定之相關法令，實質上課予 TSP 業者遵循義務。

然而，不同 TSP 業者之規模、性質、提供之服務、資訊重要性等均有不同，若以金融機構之監理方式課予 TSP 業者資訊安全義務，似有增加 TSP 業者進入開放銀行市場障礙之風險。惟此規範尚屬自律性質，銀行與個別 TSP 業者合作時，是否容有不同程度的規範彈性，此實務發展尚有待觀察。

---

[35] 資通安全管理法，第 3 條第 6 款：「……六；特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人」。

七、開放銀行對應之 GDPR 議題分析

關於開放銀行應用情境對應之個資保護議題及我國個資法之對應，涉及消費者個人資料的蒐集、處理與利用，在有特別法具體規範之前，即應適用我國個人資料保護法（以下稱個資法）。據此，依照我國個資法規定，並參考歐盟個資保護委員會（EDPB）發布之《PSD2 與 GDPR 關係指引》（以下稱 EDPB 指引）[36]，開放銀行的參進者─銀行與第三方服務提供者（TSP）─須留意下列個資法遵議題，確保合法性：

(一) 蒐集、處理與利用個資之法律依據與資料最小化原則

1. TSP 業者

TSP 業者為消費者提供服務，依其功能將自消費者或銀行蒐集、處理消費者的個人資料，必須滿足個資法第 19 條第 1 項列舉的 7 款依據之一[37]，始得為之；且依個資法第 20 條第 1 項本文規定[38]，原則上僅能在「蒐集目的之必要範圍內」，利用消費者的個人資料。通常情況下，TSP 業者與消費者成立使用服務契約，為履行契約（提供功能）而蒐集、處理並利用消費者的個人資料（符合個資法第 19 條第 1 項第 2 款）。惟 TSP 業者須確保所蒐集、處理及利用之個人資料，均符合契約目的之必要範圍

---

[36] European Data Protection Board (EDPB), *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR,* version 2.0, Adopted on 15 December 2020.

[37] 個人資料保護法，第 19 條第 1 項：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、經當事人同意。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害」。

[38] 個人資料保護法，第 20 條第 1 項本文：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。……」。

方屬適法。判斷標準應是「如不蒐集、處理或利用某筆個人資料，業者提供的特定功能即無法達成」，始得認為係有必要。

倘蒐集之資料逾越履行契約的必要範圍，則 TSP 業者應滿足其他法律依據（例如依個資法第 19 條第 1 項第 5 款規定，取得消費者的合法同意），否則即有違法風險。

2. 銀行

銀行向 TSP 業者提供（利用）消費者的個人資料，可能構成「目的外利用個人資料」之行為（因該行為與銀行原始蒐集其客戶資料之目的一例如提供活期存款服務、信用卡服務等一不符），必須符合個資法第 20 條第 1 項但書的各款例外之一[39]，始為合法。

在我國訂定特別法律課予銀行提供資料之義務前，銀行似應以「經當事人同意」，作為提供消費者資料予 TSP 業者之法律依據（歐盟銀行因有 PSD2，向 TPPs 提供資料屬於「履行法定義務」之行為，符合 GDPR 規定）。依照個資法主管機關之見解[40]，此處消費者對銀行目的外利用個人資料之同意，不限於消費者直接向銀行作出表示，如 TSP 業者在與消費者成立契約時，一併代銀行向消費者徵求「目的外利用個人資料」之同意，亦屬

[39] 個人資料保護法，第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。六、經當事人同意。七、有利於當事人權益」。

[40] 參法務部 106 年 6 月 12 日法律字第 10603504480 號函，其要旨為「公務機關蒐集民眾手機號碼時，技術上應得一併徵詢是否同意於中獎時由電信事業提供必要個人資料，由民眾自行評估選擇是否使用該項服務功能，使電信事業得經當事人同意而為目的外利用」。

合法。

(二) 必要性原則（資料最小性原則）

無論 TSP 業者或銀行，蒐集、處理與利用個人資料之行為，均應符合個資法第 5 條的必要性原則[41]，亦稱資料最小性原則。EDPB 指引建議，為符合資料最小性原則，TSP 業者可於流程、介面設計上，供消費者選取其願意由銀行提供的個人資料項目，TSP 業者即僅向銀行請求該個人資料，此可同時滿足 TSP 業者蒐集資料之必要性，以及銀行提供資料之必要性。

(三) 特種個人資料的要件限制

開放銀行之應用情境，原則上多不涉及特種個人資料（醫療、性生活、健康檢查等）。然而，EDPB 指引特別指出，銀行傳輸之資料本身或許不屬於特種個資，但如 TSP 以資料為分析、推估、預測時，即有可能（或有能力）產生消費者的特種個資，例如以帳戶支付對象與頻率，推測消費者的就醫情形、以消費者對特定企業的會員費用給付，推測消費者的性生活等。

我國個資法第 6 條第 1 項對於特種個資有嚴格限制[42]，原則上禁止蒐集、處理與利用，TSP 業者除非取得消費者的書面同

---

[41] 個人資料保護法，第 5 條：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯」。

[42] 個人資料保護法，第 6 條第 1 項：「有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：一、法律明文規定。二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。三、當事人自行公開或其他已合法公開之個人資料。四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限」。

意（其他各款法律依據較難適用），否則不得為之。

(四) 取得第三人資料之必要性

TSP 業者提供的服務功能，可能涉及第三人之個人資料（例如向銀行取得帳戶交易紀錄，包含他方交易人的姓名、帳戶資訊、交易項目與金額等）。對此，TSP 業者可否以前述「履行契約所必要」（個資法第 19 條第 1 項第 2 款）作為蒐集第三人個資之法律依據，應視所取得之第三人資料是否為該服務功能所必要而不可或缺。

此時第三人之資料係遭間接蒐集，當事人並不知情，且亦難期待 TSP 業者向該第三人告知此事（實際上無法執行），因此 TSP 業者對該功能所取得之第三人個資應格外謹慎，宜以不取得具有識別性之個資（欄位）為原則。EDPB 指引更建議，TSP 業者應對第三人之個資額外採取加密或其他技術措施，避免、降低第三人受到資料侵害或遭濫用的風險。

(五) 資料儲存期限

依我國個資法第 11 條第 3 項規定，蒐集資料之目的消失或期限屆滿後，TSP 業者原則上應主動，或依當事人之請求，刪除、停止處理或利用個人資料。

據此，在我國以特別法律規範 TSP 業者的資料保存期限之前，TSP 業者應視其提供之服務功能（蒐集資料之目的或期限），事前規劃消費者特定資料的保存期限，至少在消費者終止契約（退出服務、刪除帳號）後，除非符合個資法第 11 條第 3 項但

書的例外事由43，否則應主動或依當事人之請求，刪除個人資料。

(六) 透明性

我國個資法中的透明性原則，體現於第 8 條與第 9 條的告知義務之踐行。TSP 業者蒐集消費者的個人資料，即應依法向消費者明確揭露包含蒐集個資之目的、利用個資之期間與地區、對象與方式，以及消費者可行使之當事人權利等法定資訊。

實務上，TSP 業者應多藉由消費者註冊使用服務時，揭露「隱私權政策」等使用（會員）條款之方式，落實前述告知義務。EDPB 指引建議，在線上服務情境「階層式（layered）告知」應是優良實務作法，即業者應區分須告知之內容，設計第一層的簡介與標題，供消費者於螢幕上點擊有意深入瞭解之項目，再展開或連結至詳細內容，以此取代「將所有隱私權政策文字一次展示於有限空間的螢幕上（特別是手機等小螢幕行動裝置）」，否則容易造成消費者的資訊疲乏，減損資訊傳遞的有效性。

EDPB 指引亦建議，業者可考慮採用技術工具以確保透明性，同時提升消費者的控制權。以隱私儀表板（privacy dashboards）為例，如 TSP 業者於網站或應用程式的會員中心設計隱私儀表板，供消費者一望即知不同區塊揭露之資訊，同時透過控制滑塊、勾選框格等方式，即可輕易表達消費者對 TSP 業者蒐集、處理或利用其個人資料之意願；銀行亦可透過此方式，供其客戶即時表達是否同意銀行提供（目的外利用）其個人資料、提供哪

---

43 個人資料保護法，第 11 條第 3 項：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」；個人資料保護法施行細則，第 21 條：「有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：一、有法令規定或契約約定之保存期限。二、有理由足認刪除將侵害當事人值得保護之利益。三、其他不能刪除之正當事由」。

些個人資料給 TSP 業者，更可隨時以此方式撤回同意，將可大幅滿足當事人的資訊自主權。

(七) 剖析與自動化決策

在開放銀行應用情境中，TSP 業者或將提供服務而取得消費者的個人資料用於分析、推估、預測等剖析（profiling）行為，獲得數據洞察進而作為商業行為之依據，甚至利用演算法等技術，對消費者作出具有法律效果或類似重大影響之自動化決策。

我國個資法雖未如歐盟 GDPR，獨立訂定剖析與自動化決策之特別規範，然而，以消費者個人資料為分析、推估、預測，進而為業者自己，或對消費者個人作成決策，可視為「利用」個人資料之行為。據此，TSP 業者仍須依照其提供之服務功能，評估該行為是否屬於履行契約所必要，或須另行取得消費者的同意（且消費者可事後撤回同意）。另 TSP 業者亦須滿足前述透明性原則，依個資法第 8 條規定，向消費者踐行告知義務，明確讓消費者知悉此利用個資行為之目的與方式。

八、建議措施

針對本章第三節所提四大風險，可分成技術面與管理面之因應措施進行探討。針對技術面部分，可分成帳號密碼存取控制以及系統穩定性等二大面向進行討論。首先，針對帳號密碼的存取控制議題，本研究提出以下規範架構建議：

(一) 技術面

1. 組織應建立帳號管理機制。
2. 組織應定期審核資通系統帳號之建立、修改、啟用、禁用及刪

除。

3. 組織應採最小權限原則，僅允許使用者依機關任務及業務功能，完成指派任務所需之授權存取。

4. 組織應訂定密碼原則。

5. 電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。

6. 組織應針對使用之憑證進行週期性地更換。

7. 機構應識別資通系統並鑑別非機關使用者。

另針對系統穩定性議題，本研究建議組織應針對作業系統與軟體保證機制訂定相關規範，以為控管。例如，應定期辦理安全性檢測，若有採用雲端服務的狀況，應針對其服務模式訂定特別規範，如資源獨立、服務水準協議等，以即時發現問題，確保營運安全的有效性。

(二) 管理面

最後，針對管理面部分，由於我國開放銀行第三階段政策重點在於交易面應用服務之推動，勢將無法避免代理登入之狀況。本研究建議除前述技術策略作法外，應規範銀行端對消費者端之代理登入資訊揭露，以及在 TSP 業者端，運用合約規範要求 TSP 業者應對其代理登入應用善盡資訊揭露義務。具體建議作法如下：

1.TSP 業者與銀行業者說明其提供之服務中，那些服務將應用代理登入之功能。

2.依據銀行業者與 TSP 業者訂定之合約，銀行業者監督 TSP 業者是

否按合約規範執行代理登入相關安控措施，避免消費者權益受損。

3.銀行業者告知消費者，其交出銀行帳號密碼資訊之潛在風險

4.若消費者同意將其銀行帳號密碼資訊交出，銀行業者需告知消費者其需承擔之責任

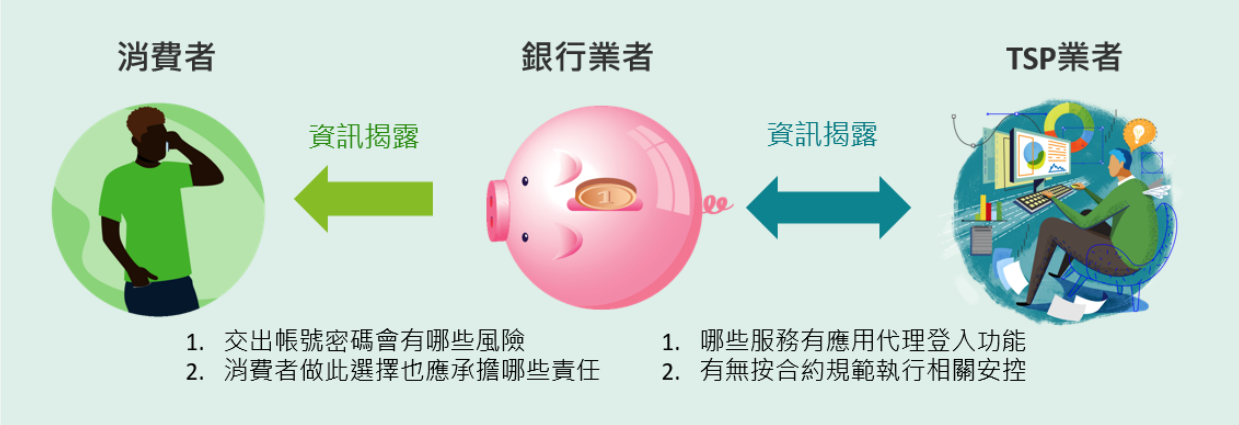

圖 19 建議銀行業者與 TSP 業者資訊揭露示意圖

資料來源：本研究整理

伍、TSP 業者使用雲端服務之控管議題探討

雲端服務基礎架構的成熟，近年來有愈來愈多金融單位選擇採用雲端資源，以帶動金融數位轉型的發展，因此，TSP 等金融科技新創業者在創新的過程中，也會面臨選擇自建資訊系統或是借力於公有雲端服務打造雲端之系統架構。雲端具備對龐大的數據乘載與運算能力，具備彈性與敏捷性，可讓 TSP 業者更快速的發展創新，有助於開放銀行之推動。然而，在開放銀行的發展過程中，Deloitte Australia（2019）調查亦指出了消費者較願意將涉及其隱私的資訊授權可信任、會妥善保管資料的機構，顯見打造一個穩定安全的共用環境，將是 TSP 業者須更加留意相關規範，以獲得客戶的信任感及忠誠度。

因此，本章節將從 TSP 運用雲端服務之情境與議題進行分析，探討 TSP 業者使用雲端服務常見之議題，解析金融機構與 TSP 業者應如何共同承擔維護資料的隱私與機密性的重要責任。

一、雲端服務之定義

根據美國國家標準和技術研究院（National Institute of Standards and Technology，以下簡稱 NIST）的定義，將雲端運算分為三種雲端服務模式、以及四大雲部署模型。

從服務模式來看雲端服務可分為下列三種類型，雲端服務模式與其之間的依賴性對於理解雲端服務安全風險控管具有非常關鍵之影響，因此討論雲端服務控管前，必須先理解所採用雲端服務模式為何。

(一) 基礎設施即服務（Infrastructure as a Service, IaaS）：IaaS 為提供運算、儲存及網路等硬體設施之服務，在此服務模式下實體設備的提供與維護皆由雲端服務提供商負責，使用者則需自行管理、架設及維運於運作平臺與軟體。

(二) 平臺即服務（Platform as a Service, PaaS）：PaaS 的營運模式係透過服務型式提供應用軟體的執行環境或者開發平臺，提供包

含程式語言、工具等，讓使用者在可在其上自行開發應用系統或架設所購買的應用服務。

(三) 軟體即服務（Software as a Service, SaaS）：SaaS 意即軟體服務商將軟體建置於雲端基礎設施之上，以服務之型式將應用系統與應用服務租賃給使用者使用為主要營運模式。

在雲端服務模式中，IaaS 是所有雲端服務的基礎，PaaS 建立於 IaaS 之上，而 SaaS 則建立在 PaaS 之上，除服務具備相依性，資訊安全風險和議題也具備了繼承關係。對於金融服務業者來說，對於雲端安全的防護責任並不因其所採用雲端運算服務與部署模式有所不同，惟相關責任分工卻有所不同。在 SaaS 架構下，雲端服務提供商將承擔最多的安全的責任，其次為 PaaS，而 IaaS 服務架構下，雲端服務使用者所需要承擔的安全能力和管理職責最多，包含負責管理與保護作業系統、應用和資料內容的安全性。

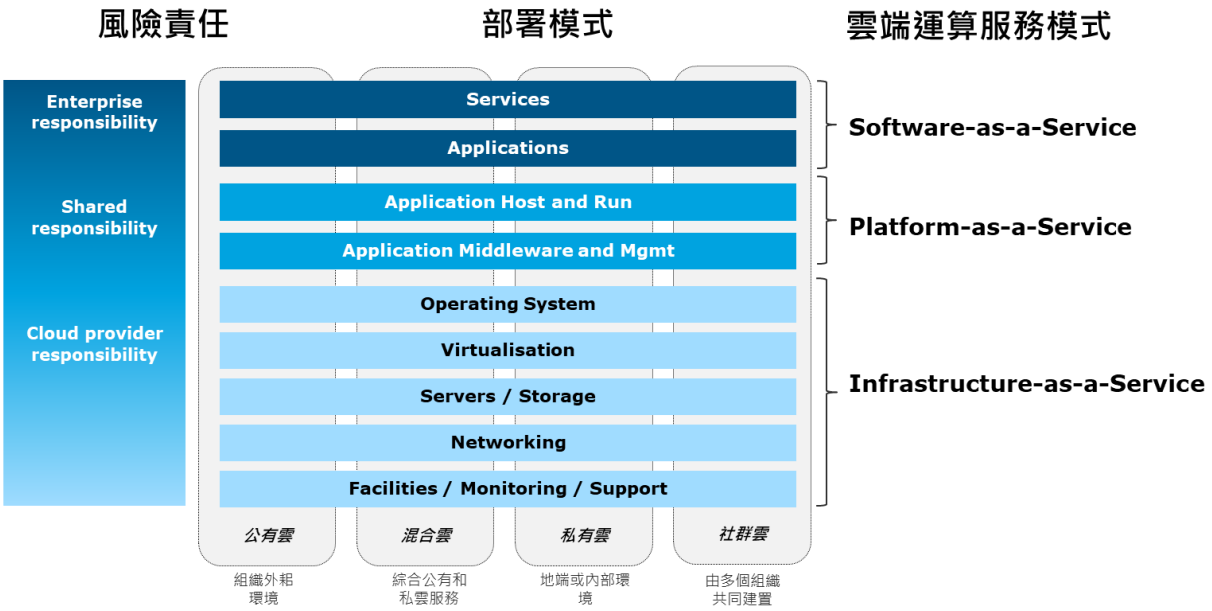

圖 20 雲端運算服務模式

資料來源：本研究整理

NIST 的雲端運算定義中，將雲端服務依部署模式區分為公有雲（Public cloud）、私有雲（Private cloud）、混合雲（Hybrid cloud），以及社群雲（Community cloud）服務對象與目的皆不同。其中，公有雲是由協力廠商雲端服務（如 AWS、Azure、GCP 等）公司架設，並提供網路的開放資源空間，如：儲存空間、程式應用等服務。目前市面上大型國際雲端服務提供商(Cloud Service Provider，以下簡稱 CSP)品牌有 Amazon 的 AWS、Microsoft 的 Azure、以及 Google 的 Google Cloud Platform(GCP)三家主要廠商。

部署模式對於雲端服務安全控管之意義，在於應由誰負責治理、安全與法規遵循的等議題，當 TSP 業者採用公有雲服務時，並不會直接造成法令遵循之影響，但必須進一步討論，如何確保在雲端，仍可保有資料的安全性及合規性，滿足各金融單位對其安全及法規遵循的要求。

二、TSP 業者使用雲端服務現況與情境

由於協力廠商雲端服務廠商所提供之公有雲服務，具備了高效能、快速擴充、高度彈性之服務，讓企業可以快速部署服務，並減少設備維護的人力與成本，同時維持一定的系統穩定性之優勢，因此對於的初創時期的 TSP 業者是為一大誘因。目前，麻布記帳即為此服務架構。以下針對各國金融科技新創業者使用雲端服務的情境，分析公有雲服務在開放銀行之應用模式：

(一) IaaS：基礎設施服務

雲端服務提供的高速且效能穩定的網路與系統服務，對於新創業者來說，在開發新服務的初期，即可快速取得資訊基礎設施服務，並將資金與人力專注於開發應用服務與市場，並在服務受到市場肯定與關注時，亦可快速調整資源以回應市場需求。雲端服務的高彈性和高擴展性，能助攻企業更快速地推出數位化的產品與服

務，強化企業對市場需求變化的敏捷性；因此，對於資源較為有限的金融科技公司來說，靈活且兼顧安全性的雲端服務是較符合其成本效益的選擇。以全球最大的協力廠商支付服務商 PayPal 集團為例，其即在 2018 年將 15%的基礎設施移轉至 GCP，以支援其須同時在 200 多的國家與地區提供其支付服務之需求，並易於其未來擴展。

(二) PaaS：API 後台管理服務

調整資源的靈活性是公有雲最大的優點，也是在開放銀行發展過程中，優化銀行 API 管理之利器。由於當 API 開放後，可能會衍生 API 不易估算流量之風險，因此，以歐洲的聯合愛爾蘭銀行(Allied Irish Banks)為例，其採用了雲端服務建立了 API 管理平臺，藉此整合平臺代管其與 TSP 間應用程式串接，除可針對 API 進行生命週期管理外，面對可能隨時接受到大量呼叫請求服務之系統，透過隨選即用的服務模式，可依據需求快速且靈活的調整資源，進行資源調度，提升維運效率。

(三) SaaS：資料分析服務

雲端服務提供了可彈性擴充的資料儲存空間與快速的運算能力，並透過強大的機器學習與分析功能，讓金融科技業者可利用機器學習等更快速且精準地分析資料，幫助其快速提昇使用者體驗。目前，國際有多家金融科技獨角獸皆有使用雲端服務進行大量的資料分析，英國一挑戰者銀行(Starling Bank)即使用雲端服務建其基礎架構，包含運用了 BigQuery 資料倉儲的分析處理能力，將數 TB 的資料轉化為即時且可使用的洞察結果，從而大規模改善 Starling Bank 與消費者的互動。美國虛擬貨幣交易所 Coninbase 也使用 AWS 的 AI 學習工具 Amazon SageMaker，開發機器學習驅動

系統，協助 Coninbase 可識別消費者身份來源中的不匹配和異常情況，進而快速辨識異常行為並採取行動，以降低消費者受詐騙威脅之情境。

三、TSP 業者使用雲端服務之風險分析

以下將從雲端服務的安全威脅及個資保護等面向分析 TSP 業者使用雲端服務之議題：

(一) 雲端服務的安全威脅

雲端安全聯盟（Cloud Security Alliance，CSA）發表的《Top Threats to Cloud Computing The Egregious 11》指出，雲端運算服務中最常見的 11 項安全威脅，包括：

1. 資料外洩

資料往往是惡意攻擊者的首要目標，若雲端發生弱點，最立即的風險就是資料可能遭竊取或外洩。而開放銀行中所涉之個人資料若是外洩，更將可能直接對客戶帶來衝擊。

2. 配置錯誤和變更控制不足

當雲端資源配置錯誤時，如：過大的權限、預設的組態設定及未開啟的安全控管等，將可能導致系統在面對惡意威脅活動時倍顯脆弱。因此，TSP 業者應訂定組態管理與變更程序，以避免雲端資源的配置錯誤而導致資料外洩，或因資料遭刪除或修改導致服務中斷。

3. 缺乏安全的架構和策略

不論公司與服務規模，對於上雲遷移、部署與使用，採用合適的安全架構和策略都是必要的，但這也是 TSP 業者採用公有雲的

過程中最大的挑戰之一，尤其若採行 IaaS 或 PaaS 之架構更應充分瞭解雲端服務提供商的環境及風險，並在雲端實現與業務目標一致的安全架構與策略。

4. 存取管理機制不足

雲端資源存取之管理不當都可能導致資訊安全事件或資料外洩，不論是雲端服務使用者或雲端服務提供商。雲端的身份管理系統(IAM)除了須能依據人員職務異動或角色之改變，自動化且及時地變更或調整其對資源訪問之權利，亦需要具備可擴展性，才能夠對大量的帳號進行全生命週期管理，才不會導致未經授權的訪問，甚至帶來災難性的破壞。

在 TSP 業者的後台權限管理中，使用者涉及多種角色於多樣化環境下的存取情境，若在應用系統與系統後台沒有訂定適當之權限控管、個人資料存取稽核軌跡留存或相關人員使用的終端設備安全性防護等，都可能提升潛藏之資訊安全風險發生之機率。

5. 帳戶劫持

在雲端服務中，風險最高的帳戶是雲端服務提供商提供服務所使用之帳號，若遭到劫持則惡意攻擊者可能獲得並濫用特權或敏感帳戶。因此，採行縱深防禦機制和 IAM 控制是 TSP 業者減輕帳戶劫持攻擊的關鍵。

6. 內部威脅

雲端服務提供商的員工或是合作夥伴，因具備了可以存取伺服器、網路與資源之權限，因此若是不論是惡意或無意地，都可能造成重大負面影響。常見的場景包含因個人有意或疏忽導致配置錯誤的雲伺服器、員工將敏感資料儲存在不安全的個人設備和系統上、內部人員誤點擊網路釣魚郵件使組織成為攻擊對象。對 TSP

業者或雲端服務提供商來說，強化高風險人員的認知訓練與行為監控皆是必要的措施，以提升其對客戶資料保護的意識，也降低因過失或蓄意造成的破壞。

7. 不安全的軟體介面

雲端運算係透過許多軟體介面提供服務，如：API 和 UI 通常是用以對外開放的，但也因此可能會不斷遭到攻擊，對於大量採用 API 進行資訊交換之開放銀行業者，不安全的 API 將直接導致服務中斷或資安事件，因此，在設計時必須考慮安全問題，以及適當的控制措施來保護它們免受攻擊。

8. 資料控管不足

當企業將資料遷移到雲端上後，其對於資料儲存、備份與刪除等控管將變得更為複雜，必須能充分確保資料的穩定性和法令執行之要求，避免招致對於資料控管不當之裁罰。因此，應掌握資料生命週期之控管，才能確保合法和履行法定義務之要求。

9. 雲端服務和應用失效

雲端服務使用者必須瞭解如何在雲端正確實施和部署應用程式，例如：為雲端環境所設計的應用程式，才能充分利用雲端平台之能力，並確保服務正常運作。

10.缺乏雲端可視性

當企業內部人員對於雲端安全可視性不足，則內部可能會充斥著許多缺乏保護的服務，即所謂「影子 IT」，常見的因素包含缺乏治理、缺代意識與缺乏安全控管等。為了確保服務的安全性，TSP 業者必須對於雲端服務之安全具可視性，才能掌握所有需要被保護的一切，不致為企業帶來法規遵循和安全的風險。

11.濫用及違法使用雲端服務

惡意攻擊者若是利用雲端運算能力來發動攻擊，可能使搭建在雲端服務中的惡意軟體看起來是可信的，或透過雲端共用工具來進行傳播，增加 TSP 業者在防禦的困難度。

雲端服務帶來便利性的同時，也帶來了諸多的安全挑戰，上述 11 項雲端服務常見威脅，是 TSP 業者自我評估是否得採用雲端服務平台的關鍵。TSP 業者應審慎評估其技術團隊對雲端技術是否足夠熟悉，能夠瞭解並掌握雲端服務之風險時，以確保其服務在雲端運作過程之機密性、完整性及可用性，若 TSP 業者本身在雲端技術之不足或缺乏妥適的雲端架構及資源配置情形下，貿然採用雲端服務進行商業應用，可能將導致營運效率不佳或資安事件發生。

表 27 雲端常見威脅與安全責任對照表

風險	雲端服務模型	TSP 業者	CSP 業者
資料洩露	IaaS、PaaS、SaaS	O	O
配置錯誤和變更控制不足	IaaS、PaaS、SaaS	O	
缺乏安全的架構和策略	IaaS、PaaS	O	
存取管理機制不足	IaaS、PaaS	O	
帳戶劫持	IaaS、PaaS、SaaS	O	O
內部威脅	IaaS、PaaS、SaaS	O	
不安全的軟體介面	IaaS、PaaS、SaaS	O	O
資料控管不足	IaaS、PaaS、SaaS	O	
雲端架構和應用失效	IaaS、PaaS、SaaS	O	O

缺乏雲端可視性	IaaS、PaaS、SaaS	O	O
濫用及違法使用雲端服務	IaaS、PaaS、SaaS	O	O

資料來源：本研究整理

(二) 雲端服務的個人資料保護議題

由於開放銀行第二及第三階段，開放之資料將涉及個人資料、消費資料與交易資料等，TSP 業者可以透過 API 串接各銀行，查詢客戶之個人資料與交易面等資料，因此對於「個人資料保護法」、「個人資料保護法施行細則」、「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」之遵循將是對於客戶權益維護的重點之一。以下將就 TSP 業者若採用雲端服務時，應考量之個人資料保護議題進行分析。

1. 蒐集：應充分告知並取得當事人同意

依據法規要求，當企業向當事人蒐集個人資料時，應明確告知當事人資料蒐集之目的、類別、期間、地區、對象與方式，以及客戶得行使權利之方式等資訊。因此，在開放銀行作業過程，TSP 業者向金融單位所取得之資料，若涉及客戶個人資訊者，應於契約簽訂時確認及訂定告知客戶之條款與責任，不論是金融機構或 TSP 業者直接透過雲端平台直接向客戶進行資料蒐集、處理或利用作業，皆應確認於個人資料告知聲明中，對於個資使用對象與地區是否已涵蓋完整，並且取得當事人同意。

2. 處理：過程皆透明、合法並符合法令規範

TSP 業者在採用雲端服務前，應釐清資料存放至雲端平台之儲存方式與地區以及處理個人資料的方式是否透明且合法。並且應事先考量資料保護措施，包含資料儲存及備份等位置、方式及管

道等，以保障消費者權益。由於開放銀行涉及之資料多為客戶極具機密性的重要資料，為確保傳輸過程中，消費者相關敏感資訊不會被攔截、竊取或竄改，TSP 業者更應考量於資料生命週期中之加密或去識別化機制，從資料上傳至雲端，直至資料刪除為止，皆維持必要之管控，並且應比照一般作業委外程序，在委託前事先規畫服務終止後之計畫，以完整相關退場機制，包含未來若解除合約關係，應能確保雲端服務提供商可確實將資料刪除。另由於雲端環境為多租戶之資訊環境，因此應確認資料區隔與事件紀錄留存機制，確保若是發生資安事件，可在不侵犯到其他租戶隱私之前提下，調閱事件相關日誌紀錄。

3. 利用：資料使用皆符合原始目的，若目的消失應可刪除資料

面對客戶資料之使用，TSP 業者必須謹慎為之，除了自身以外，若用雲端平台之服務進行資料分析，應確保雲端服務廠商應無對該些原始資料及分析後資料擁有存取權限，且未來若解除合約關係，應確保雲端服務提供商可以且確實將資料刪除。

4. 國際傳輸：資料儲存地點是否安全，以及是否已取得許可

TSP 業者若採用雲端服務處理自銀行介接的消費者個人資料，應先釐清資料拋至雲端後的儲存或備份地區，包含雲端伺服器的實體位置，是否存在國際傳輸之情形。在世界各國有許多國家法律明文禁止或限制將個人資料傳出該國，在大多數情況下，只有當資料儲存地之國家對於個人資料以及隱私權具備充分的保護時才允許傳輸。而根據我國現行法規要求，客戶重要資料應以留存在境內為原則，但不論是 TSP 業者或是金融業者，無可避免會使用境外的 CSP 服務，因此有此情形之業者，應確保資料傳輸至其他國家前（如：提供服務前），應確實告知當事人傳輸至境外的議題並取得其同意，並且應針對跨境傳輸衍生的風險管理議題，包含個人資

料跨境儲存和不同地區法律規範合規性議題進行辨識。以事先處理各國資料保護法律可能施加給其的特定限制，例如在某些情況下，可能需要事先取得許可。

(三) 雲端委外監督及管理

依據「金融機構作業委託他人處理內部作業制度及程序辦法」要求，針對金融機構若將作業委託他人處理涉及雲端服務時，已明定包含金融機構作業委外契約應載明事項、向主管機關申請核准程序等。因此，對於與金融機構合作之 TSP 業者而言，若 TSP 業者將採用雲端服務處理其自金融機構所取得之資料時，亦應遵循相關辦法之規定，以下就應考量之相關委外管理議題進行分析：

1. 委外管理與程序

TSP 業者應訂定之委外作業規範，包含消費者權益保障、風險管理與內控及內稽制度等之內部作業及管理程序等，以持續監督受委託機構，確保委外相關風險可受到控制。並應訂定妥適的緊急應變計畫，降低因作業委託而可能有服務中斷之風險，並確保資安事件發生時，能具備足夠之應變能力。

2. 委外契約應載明事項

TSP 業者與 CSP 業者間之契約應載明事項包含但不限於以下要求：

(1) 委外事項範圍及受委託機構之權責
(2) 確保其遵守相關法令及銀行公會訂定之相關業務規章或自律公約
(3) 消費者權益保障及消費者爭端解決機制
(4) 受委託機構聘僱人員之管理

(5) 與受委託機構終止委外契約之重大事由

(6) 受委託機構就受託事項範圍，同意主管機關及中央銀行得取得相關資料或報告，及進行金融檢查，或得命令其於限期內提供相關資料或報告

(7) 受委託機構對外不得以金融機構之名義辦理受託處理事項

(8) 委外事項若有重大異常或缺失應立即通知委託方

(9) 非經書面同意，不得將作業複委託；委外契約中應針對複委託情形，訂明複委託之範圍、限制或條件

3. 申請核准程序

TSP 業者若有委託 CSP 業者之情形，不論境內或境外，除應比照金融機構依規範提出申請，也應確認是否事前取得金融機構及客戶之同意。

4. 監督管理責任

TSP 業者應定期及不定期就 CSP 業者對於客戶資訊之使用、處理及控管情形進行查核及監督。TSP 業者應善盡其監督管理之責任，以確保雲端平台對於個資之處理具備相當資訊安全保護措施，能遵守合約及相關法令規範之要求。

四、國內外雲端法規要求

(一) 國際雲端運算服務安全標準簡介

1. ISO 27000 系列

國際標準組織(ISO)是獨立的非政府組織，以及全球最大

的自願性國際標準開發者。其所制定之 ISO/IEC 27000 標準系列旨在協助各類型及各種規模的組織保持其資訊資產安全。其中與雲端服務相關的標準有

(1) ISO/IEC 27017：雲端系統的資訊安全管理

ISO/IEC 27017 係基於 ISO/IEC 27002 實作雲端運算資訊安全管理系統時，用來做為選取雲端服務資訊安全性控制的參考(同時 CSP 也可以使用 ISO/IEC 27017 做為防護控制實施的指導方針)，以處理雲端特定的資訊安全性威脅和風險。ISO/IEC 27017 提供 7 項新的控制措施，藉以解決雲端運算環境內的共同角色和責任、在合約終止時移除並退回雲端服務客戶資產、保護客戶的虛擬環境並與其他客戶的虛擬環境隔離、滿足商務需求的虛擬機器強化需求、雲端運算環境系統管理操作的程序、讓客戶能夠監視雲端運算環境內的相關活動，以及結合虛擬和實體網路的安全性管理。

(2) ISO/IEC 27018：雲端系統的資料保護

ISO/IEC 27018:2014 做為雲端隱私權的第一個國際工作條例規定並依循 GDPR，它對作為個人識別資訊 (PII) 處理者的雲端服務提供商 (CSP) 提供特定指引，以保護 PII 評估風險和實作最先進的控制措施。

2. 國際電腦稽核協會《雲端運算稽核計畫》

國際電腦稽核協會(ISACA)是一個為資訊管理、控制、安全和稽核專業設定規範的全球性組織。ISACA 於 2010 年公告四項新的稽核程序包含雲端運算、危機管理、安全管理和活動目錄管理。

其中有關雲端運算稽核所制定之《雲端運算稽核計畫》

(全名為 The Cloud Computing Audit Program) 囊括雲端運算環境的治理、服務提供商與客戶之間的關係，以及特定的控制問題。《雲端運算稽核計畫》提供企業在雲環境上放置的流程和資料，以及雲端運算的使用模式和策略指導，並提供稽核員稽核雲端環境與架構的指導原則。

3. 歐盟網路與資訊安全局《資訊安全保證架構》

歐盟網路與資訊安全局(ENISA)直屬於歐盟，並專責歐洲資安事務運作，並支援與國家資訊安全性相關的歐盟政策和法律的開發和實施。其於 2009 年頒佈之《資訊安全保證架構》(以下簡稱 IAF) 旨在提供組織一套採用雲端服務的風險評估方式，一方面比較不同的雲端服務提供商之服務，另一方面也減少雲端服務提供商的保證負擔。IAF 根據 ISO/IEC 27001、BS 25999、NIST SP 800-53 等標準中對於雲端服務提供商及受委託第三方有關之控制項及產業間最佳實踐要求，針對人員安全、供應鏈保證、營運安全、身份與存取管理、資產管理、資料與服務可攜性、業務持續管理、實體安全、環境管控及法令遵循提出十大資料保護的管控要求。

其中中小型企業尤其適用 IAF，因該架構可有效協助組織高階主管或決策層級人員評估和減緩採用雲端服務技術的風險。針對雲端服務提供商來說，亦可透過該要求，標準化其雲端服務之合規性流程。

ENISA 的《資訊安全保證架構》現行尚以歐盟各國採自願性方式導入，且層級將高於歐盟各國現行的認證計畫。

4. PCI DSS 雲端運算指南

支付卡產業安全標準協會(Payment Card Industry Security Standards Council，簡稱 PCI SSC)，為一跨國性組織。為保護持卡人資料及交易的安全，於 2004 年訂定的全球統

一規範《支付卡產業資料安全標準》（Payment Card Industry Data Security Standard，簡稱 PCI DSS），且所有與支付卡處理相關聯的機構，包括商家、服務供應商、收單機構及發卡機構皆須符合 PCI DSS 的要求。PCI DSS 透過資料流標準化、規範化的方式，達到資訊把關的目的。其中《雲端運算指南》(Cloud Computing Guidelines) 即是 PCI SSC 為了解決支付產業在導入雲端服務的趨勢下，自 PCI DSS 衍生出的安全指南，並從公司治理與法遵、設備與實體安全、資料安全、事件因應及數位鑑識調查、弱點管理等五大安全項目進行規範，供欲將支付卡業務轉移至雲端環境的支付卡組織進行參考，以協助相關單位因應新興雲端風險和其他相關的合規性挑戰。

5. 雲端安全聯盟(CSA)相關標準

雲端安全聯盟（CSA）於 2021 年 1 月公布了最新版雲端安全控制框架第 4 版(Cloud Controls Matrix v4, CCM v4)，本次修訂新增了日誌記錄和監控（LOG）控制項，並對現有的安全框架內容，包括治理、風險和合規（GRC）；審計與確信（A&A）；統一端點管理（UEM）；以及密碼學、加密和密鑰管理（CEK）等章節進行修訂。

CCM v4 共由 197 個控制目標組成，這些目標分為 17 個構面，涵蓋雲端技術安全關鍵面向，該安全框架可作為雲端服務系統的評估工具，並為雲端服務供應鏈中的的參與者提供安控指引。此外，CCM v4 的框架也符合雲安全保證和合規性實務標準 CSA 雲端運算安全指南的規範。新版的 CCM v4 涵蓋來自新的雲端技術、控制和安全責任的要求，讓雲端安全的安控議題呈現更為量化，並強化了與其他資訊安全標準的互通與相容性。

(二) 我國現行針對雲端服務相關法令規範研析

1. 金融機構作業委託他人處理內部作業制度及程序辦法

依據 108 年 9 月最新修訂之「金融機構作業委託他人處理內部作業制度及程序辦法」，金融業上雲準則包含以下八大重點：

(1) 金融機構應確保作業風險控管，評估受託機構處理的風險，採取適當風險控管措施。

(2) 金融機構對雲端服務業者負有最終監督義務，並視情況需要委託專業第三人輔助監督作業。

(3) 金融機構應確保能取得雲端服務業者執行受託作業的相關資訊，包括查核報告，以及實地查核權利。

(4) 金融機構得自行委託，或是與其他委外同一家雲端服務業者的金融機構，聯合委託具備資訊專業的獨立第三人查核。

(5) 金融機構傳輸及儲存客戶資料到雲端服務業者，應將客戶資料加密等有效保護措施，並訂定加密金鑰管理機制。

(6) 委外處理的資料應保有完整所有權，並確保雲端服務業者除了執行受託作業之外，不可在委託範圍以外利用。

(7) 金融機構也應訂定緊急應變計畫，降低因作業委託而可能有服務中斷的風險。

(8) 委託雲端服務業者處理的客戶資料以及資料儲存地，要以我國境內為原則。若是資料儲存地位於境外，應依下列規定辦理：

a. 金融機構須保有其指定資料處理及儲存地之權力。

b. 境外當地資料保護法規不得低於我國要求。

c. 除經主管機關核准者外，客戶重要資料應在我國留存備份。

2. 金融機構運用新興科技作業規範

經 109 年 4 月 17 日金管銀外字第 1090134542 號函修正金融機構運用新興科技作業規範，金融機構應積極控管的服務領域包含生物辨識、自攜設備、雲端服務、社群媒體四項的要求；其中，雲端服務安全控管共涵蓋 14 個面項：

(1) 雲端服務係指雲端服務業者以租借方式提供個人或企業得承租其網路設備、伺服器、儲存空間、資安設備、系統軟體、應用程式、分析與計算等資源，以達資源共享之服務。

(2) 安全控管範圍不包含僅提供銀行內部使用之服務。

(3) 應制定雲端服務管理政策，至少每年檢視一次。

(4) 應確保作業風險控管，充分評估雲端服務業者處理之風險，採取適當風險管控措施。

(5) 對雲端服務業者負有最終監督義務，並得視需要委託專業第三人以輔助其監督作業。

(6) 應確保其本身、主管機關及中央銀行，或其指定之人能取得雲端服務業者執行作業之相關資訊，包括客戶資訊及相關系統之查核報告，及實地查核權力。

(7) 得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核。

(8) 傳輸及儲存客戶資料或敏感資料至雲端服務業者，應採行資料加密或代碼化等有效保護措施及訂定妥適的加密金鑰管理機制（如租用硬體安全模組）。

(9) 對雲端服務業者處理之資料應保有完整所有權，除執行指定作業外，金融機構應確保雲端服務業者不得有存取客戶資料之權限，並不得為指定範圍以外之利用。

(10) 委託雲端服務業者處理之客戶資料及其儲存地以位於我國境內為原則，如位於境外，應依下列規定辦理：

a. 金融機構須保有其指定資料處理及儲存地之權力。

b. 境外當地資料保護法規不得低於我國要求。

c. 除經主管機關核准者外，客戶重要資料應在我國留存備份。

(11) 應訂定妥適之緊急應變計畫，降低因雲端作業而可能有服務中斷之風險。

(12) 採用 IaaS 或 PaaS 雲端服務模式者應符合下列規定：

a. 應評估雲端服務業者之合格條件、服務水準、復原時間、備援機制、供應鏈關係、權責歸屬及資訊安全防護等項目。

b. 應評估雲端服務業者提供之平台、協定、介面、檔案格式等，以確保互通性與可移植性。

c. 應確保雲端服務業者提供之資源與其他承租人所使用之資源各自獨立，互不影響（如防火牆區隔）。

d. 應與雲端服務業者簽訂服務協議，維持所需之服務水準並定期提出報告與操作紀錄（如服務水準報告、系統變更紀錄、作業系統映像檔存取紀錄等）。

e. 如有設備定期維護更換時(如硬碟更換)，資料也須進行全數刪除或銷毀、並留存刪除或銷毀之紀錄。

(13) 應監控並建立資通安全事件通報程序。遇事件發生時，相關單位及人員應依循前述通報程序辦理。

(14) 提供電子銀行服務者，應符合本會制定之「金融機構辦理電子銀行業務安全控管作業基準」規定。

3. 開放應用程式介面(Open API)業務安全控管作業規範

在 Open API 的法令架構上，銀行與 TSP 業者各自負擔不同的權利義務，銀行與 TSP 合作之基礎是銀行公會訂定的自律規範；目前 TSP 必須與銀行簽訂合約、符合銀行要求的資安技術和標準、取得 ISO 27001 或相當認證。銀行則要遵守 Open API 技術規格文件，以及業務安全控管作業規範。

該規範目前對銀行與 TSP 的合作規範涵蓋安全控管要求、資訊系統標準以及配套監理措施。其中，安全控管要求包括消費者註冊以及資訊查詢時的身份確認安全設計、網路型態與其安全設計、設計原則的共通要求與各類安全要求。其二是資訊系統標準，包括訂定組織、人員與設備安全的相關管理措施；應就機房、營運、網路、金鑰、系統生命週期、資安事故、營運持續管理等採取資訊安全維護措施。第三則是配套監理措施，TSP 業者需在業務申請時及其後每年由公正第三方進行檢視，提出資訊系統及安全控管作業評估報告。

綜合以上，TSP 業者在合規議題，與銀行合作前有三大重點工作，包括資格、技術、營運。

(1) 在資格部分，TSP 業者必須是合法登記公司，具備穩健經營的證明，並提供聲明書與相關文件；

(2) 在技術面，TSP 業者必須確保連線安全、API 檢驗等項目合規性；此外，TSP 業者或其委託開發廠商所開發的應用程式介面，上線前也應經安全性測試合格。

(3) 在營運面，目前規範內容要求 TSP 業者提供 ISO

27001 標準認證或相同等級的認證，以及資安防護能力經第三方驗證的證明。

此外，就雲端安全議題，開放應用程式介面(Open API)業務安全控管作業規範第十四條也已進行規範：「TSP 業者若將機敏資料儲存於雲端服務業者，應遵循銀行公會所訂之雲端服務相關自律規範」。綜合以上，研究團隊認為，後續在 TSP 業者參與開放銀行業務時，尚有部分配套措施待釐清，包括商業面、法令面、技術面和測試檢驗訓練課程、ISO 標準介接輔導，以及後續協助 TSP 進行 ISO 認證與介接自檢等，都是未來開放應用程式介面(Open API)業務安全控管作業規範應視開放銀行業業務推動滾動式修正的重要議題。

(三) TSP 業者使用雲端服務資訊安全框架建議

研究團隊檢視雲端服務應用相關國際標準，以及我國金融業現行對雲端安全運作主要規範後，綜整 TSP 業者使用雲端服務之安控，首要應著重在人員安全、供應鏈管理、營運安全、身份存取與管理、資產管理、資料與服務可攜性、業務持續管理以及法令遵循等八大面向。

後續研究執行，研究團隊將以前述架構項目檢視我國金融業在雲端服務相關監理規範的完整度，在初步篩選出現行法規不足之處後，進一步檢視對應的國際標準規範，最後提出本研究對我國雲端安全控管現況提出調整建議。

五、建議措施

雲端服務可協助資源不足的新創業者發展及管理資料，並彌補其資源之落差，然面對雲端服務的安全威脅及個資保護議題，TSP 業者及金融業者之控管要求尚有不同，以下將說明，並建議應考量將下列金融機構所應遵循之作業委外管理規範納入 TSP 業者控管要求，使金融業

者與 TSP 業者所需遵循之規範一致。

(一) 適用既有法規之控管精神

現行開放應用程式介面(Open API)業務安全控管作業規範第十四條也已進行規範:「TSP 業者若將機敏資料儲存於雲端服務業者,應遵循銀行公會所訂之雲端服務相關自律規範」,惟因金融機構採用雲端服務除自律規範外,尚有金融機構作業委託他人處理內部作業制度及程序辦法、金融消費者保護法、個資法及個資法施行細則等法令需遵循。

如前段所述,TSP 業者對於個人資料保護相關法令之適用性與金融業者並無不同,其他金融相關法規,由於中央目的事業主管機關不同,及 TSP 業者及金融機構適用之法規將出現落差。針對我國金融業現行對雲端作業委外主要兩項規範,《金融機構作業委託他人處理內部作業制度及程序辦法》與《金融機構運用新興科技作業規範》。其中,因現行 TSP 業者若採用雲端服務,依據開放應用程式介面(Open API)業務安全控管作業規範第十四條之規範,應遵循銀行公會所訂之雲端服務相關自律規範,即金融機構運用新興科技作業規範已為 TSP 業者資料上雲時所適用。故銀行與 TSP 業者合作時,間接將資料委託予雲端服務業者處理之情境,理應適用金融機構控管強度。故銀行與 TSP 業者合作時,間接將資料委託予雲端服務業者處理之情境,應適用相關規範之要求。

(二) 確立開放銀行應用雲端服務之申請核准程序

依據「金融機構作業委託他人處理內部作業制度及程序辦法」,金融業採用雲端服務若涉及業務資料或客戶資料委外處理作業者,應檢具書件向主管機關申請核准始得辦理,若金融機構在開放銀行之合作中,涉及使用雲端服務處理金融機構所蒐集之資料之情境,TSP 業者應備妥作業委外計畫書等文件,交由金融機構透過契約把

關，如限制 TSP 業者應採用自行開發之系統、限制採用境內公有雲儲存、以及雲端服務業者應通過資安認證等要求，以確保 TSP 業者挑選之雲端服務業者具備可靠、安全及穩定性。

因此，本研究建議應斟酌修訂《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》，增修上述要求外，並可增訂依開放資料之風險定義允許上雲之作業範圍，包含限制 TSP 業者應採用自行開發之系統、限制採用境內公有雲儲存，以及雲端服務業者應通過資安認證要求等要求，以確保 TSP 業者所挑選之雲端服務業者之服務可靠性、安全性及穩定性。

(三) 強化 TSP 業者採用雲端服務應負之資訊安全及管理責任

開放應用程式介面(Open API)業務安全控管作業規範第二十條「TSP 作業環境之委外管理」已對 TSP 業者之委外管理進行規範，惟對應金融機構作業委託他人處理內部作業制度及程序辦法之要求，建議針對 TSP 業者委託雲端服務應增修契約條款、風險控管、委外監督管理等規定：

1、 契約要求

TSP 業者應與雲端服務業者簽訂書面契約，參照「金融機構作業委託他人處理內部作業制度及程序辦法」第 10 條要求，契約建議應載明下列事項

A. 委外事項範圍及受委託機構之權責。
B. 受委託機構應建立消費者權益保障、風險管理、人員管理、內部控制及內部稽核制度。
C. 服務終止或解約之條款，如涉及將資料若儲存於雲端者應約定終止或結束作業委託後之資料刪除期限。
D. 受委託機構就受託事項範圍應定期辦理資訊安全稽核或

由委外廠商提出資訊安全稽核報告，並同意主管機關及金融機構及得取得相關資料或報告。

E. 受委託機構對委外事項若有重大異常或缺失應立即通知 TSP 業者。

除上述建議 TSP 業者與雲端服務業者簽訂契約應載明之事項，若金融業者合作之 TSP 業者有資料上雲需求，建議金融業者可參考本章第四節所列之國際雲端運算服務安全標準，於契約內要求 TSP 業者，針對常見雲端安全風險，向其合作之雲端服務提供商執行風險評估。本研究建議評估構面與問項如下：

表 28 建議 TSP 業者評估雲端服務提供商風險之構面與問項

評估構面	評估問項	參考標準
資產管理	1. 雲端服務提供商的資產清單是否能明確指出 TSP 業者放置在其雲端中的（衍生）資料 2. 與雲端服務提供商間之契約終止時，TSP 業者是否能及時將資料從其雲環境中移除或請其歸還 3. 雲服務提供商是否記錄其允許 TSP 業者對其資訊和相關資產進行分類與標記的服務功能	• ISO 27017 A.8 • CSA CCM v4 DCS
存取控制	1. 雲端服務提供商是否有針對使用者之註冊與註銷、存取權限配置、驗證資訊等進行管理 2. 雲端服務提供商是否能保護 TSP 業者在雲端服務運行的虛擬環境中能免受其他雲端服務客戶及未經授權的人	• ISO 27017 A.9 • ISO 27017 CLD 9.5.1 • CSA CCM v4 IAM

評估構面	評估問項	參考標準
	員影響	
加密	1. 雲端服務提供商是否提供 TSP 業者其加密控制的描述，並確保符合適用的協議與法規 2. 雲端服務提供商是否有建立並維護其密碼學、加密和金鑰管理的政策和程序 3. 雲端服務提供商是否有針對金鑰從產生到撤銷或更換等不同生命週期階段之管理政策	• ISO 27017 A10 • CSA CCM v4 CEK • ENISA Cloud Computing Risk Assessment R.12, R17
作業安全	1. 雲端服務提供商是否依據所議定之備份政策，定期進行資訊、軟體及系統映像檔之備份與測試 2. 雲端服務提供商是否提供日誌記錄及其相應安控措施 3. 雲端服務提供商是否提供有關可能影響所提供雲服務的技術漏洞管理資訊	• ISO 27017 A.12 • CSA CCM v4 LOG
通訊安全	1. 雲端服務提供商是否執行網路區隔（例如：多租戶環境中區隔個租戶、雲端服務商內部管理網路與 TSP 業者之雲端環境） 1. 雲端服務提供商是否能確保虛擬網路與實體網路之間的一致性配置	• ISO 27017 A.13 • ISO 27017 CLD.13.1.4 • CSA CCM v4 IVS • ENISA Cloud Computing Risk

評估構面	評估問項	參考標準
		Assessment R.9
系統取得、開發及維護	1. 雲端服務提供商是否提供 TSP 業者其資訊安全規格 2. 雲端服務提供商是否提供其安全開發流程，以及此開發流程與其現行政策之相容性 3. 雲端服務提供商是否建置針對應用程式之設計、開發、佈署之系統發展生命周期流程	• ISO 27017 A.14 • CSA CCM v4 AIS

資料來源：本研究整理

2、 雲端風險控管

TSP 業者採用雲端服務進行個人資料蒐集、處理及利用時，應建立適當風險控管措施，包含緊急變更計畫、契約終止後之資料移轉能力等，以避免業務中斷、確保服務金融機構應確保作業風險控管，評估受託機構處理的風險，採取適當風險控管措施。

3、 資訊安全管理責任

對於 TSP 業者採用雲端服務之資訊安全及管理責任應明確定義，包含 TSP 業者對於雲端所儲存及傳輸之消費者資料應以加密或代碼化方式保護，並訂定加密金鑰管理機制，再輔以個資法要求，以及定期雲端資料儲存及保護之規範，並約束 TSP 業者，讓 TSP 業者得以用雲端服務管理及保護使用者資料。

4、 監督管理責任

TSP 業者對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。此外，TSP 業者除應定期針對雲端業者辦理查核外，以確保雲端服務業者具備相當資訊安全保護措施，應能遵守合約及相關法令規範之要求，如涉及將資料若儲存於雲端者，亦應要求確保其本身及主管機關，或其指定之人能取得雲端服務業者執行受託作業之相關資訊，包括查核報告，及實地查核權力。

對比國際三大雲端服務業者，TSP 業者是否有能力與其互動甚至管理雲端服務業者、是否有足夠的成本擔負未來相關的法遵支出，將可能使資源較為有限或小型 TSP 業者受到限制，甚至降低其採用雲端服務之意願，但也惟此才能有效落實消費者與金融安全之保護要求。惟長期而言，則可透過法規逐步鬆綁及白名單等方式，根據服務之可靠性、安全性、服務品質等列出合格之雲端服務業者，以供 TSP 業者或金融機構選用。

陸、開放銀行與消費者權益保護

本研究針對開放銀行第三階段交易面應用場景爭議處理機制，以國際相關案例分析其爭議處理機制設計，進而比對我國現況，最後對我國開放銀行交易爭議處理提出政策建議。本節將分析體制外的國際非營利組織於金融消費爭議解決機制的效益，針對現有民間消保組織的定位和協力進一步考量，期望可以和我國現有金融消費評議機制產生互補綜效，並就未來各產業將走向資料開放的趨勢，同一 TSP 業者可能介接不同業別資料的狀況進行研析，以確保消費者有全面性及一致性之保障。

一、臺灣開放銀行政策與現況

自金管會於 2019 年推動開放銀行政策以來，我國效法新加坡與香港以「自願自律」的模式推動相關政策，在不修法的前提下，由金融業者透過公會訂定自律規範，分階段開放商品公開資訊、客戶資訊與交易資訊。我國在 2019 年 6 月完成「商品公開資訊」設計後，同年 10 月正式上線。目前我國已邁入開放銀行政策的第二階段客戶資訊的介接，許多銀行基於自身營運策略、業務需求與第三方服務業者(TSP）合作，透過消費者授權，讓 TSP 業者向銀行介接消費者自己所需要的資料，消費者進而可享受更多元的金融服務。

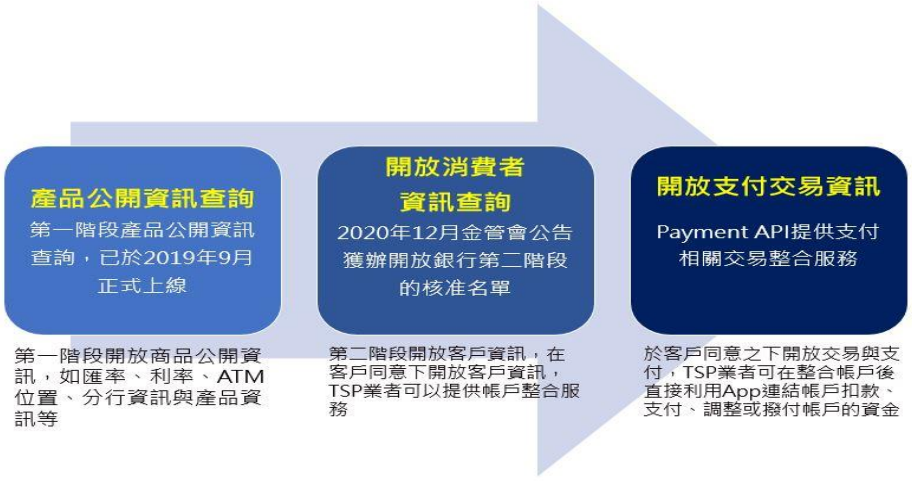

圖 21 我國開放銀行三階段開放資料類別

資料來源: 本研究整理

開放銀行帶來的整合性服務平台創新，也衍生銀行與 TSP 業者間共享資料所衍伸的資料存取、相關使用權限與隱私保護等責任分配的議題。依照目前由銀行公會、財金公司與第三方服務業者討論出的自律規範，銀行必須與 TSP 業者簽約，約定 TPS 業者要做到的資安技術標準。除了對 TSP 業者的管理方式、資訊安全和相關標準驗證導入的要求，後續因資料外洩衍生的爭議處理和損害賠償機制等，因為涉及消費者個人資料與消費者帳戶資訊，對於消費者的隱私保護與權益保障，亟需建立對資料共享潛在風險的有效控管機制。

二、國內外開放銀行業務種類分析

英國在開放銀行的發展方面處於國際領先地位。過去被金融機構視為重要資產的客戶資料，將透過 API 以適當安全管理機制授予第三方服務業者(TSP)使用，使消費者可以在未直接接觸銀行的前提之下，使用與享受更加廣泛的金融服務。本研究整合英國 Financial Conduct Authority (FCA)於 2019 年十二月所提出的「Call for Input：Open finance」和政治大學金融科技研究中心對開放銀行應用場景的界定，消費者透過 TSP 業者向銀行申請開放金融業務，主要有四大類別：

(一) 個人財務管理總覽

個人財務管理儀表板透過連結各家銀行的存款資料，讓消費者得以一次總覽所有不同銀行的帳戶，建立一站式帳戶服務，讓理財更貼近客戶需求也更為便利。例如，藉由整合銀行業者、電子票證公司與電子發票平台，解決過往消費者需要分次登入不同銀行或網銀，使用者才能掌握個人財務狀態不便利的問題。

透過銀行與 TSP 業者的合作或資料交換，TSP 業者將能在獲得使用者同意的前提下，代為向銀行提出存取使用者相關之帳戶資訊，並於其 APP 平台上進行各種消費、帳戶資訊的彙整，使消

費者能在單一介面中一次掌握自己各銀行帳戶活期存款、定期存款、貸款、信用卡、所有收支，以及消費狀態，進而隨時掌握個人財務狀況。此外，App 服務設計也能自動幫用戶將消費品分類，將 APP 的記帳功能融入網路銀行服務，目前臺灣提供整合性服務平台，TSP 業者如麻布記帳(Moneybook)、臺灣集中保管結算所(集保 e 手掌握)以及 CWMoney 等，已為消費者提供更為優化的金融服務體驗。

(二) 公開資訊統整平台

在開放銀行政策的推動下，業者將共創出資訊更透明的金融服務資訊整合平台，廣泛蒐集並呈現不同金融機構之各種金融商品與服務資訊，並可在整合後依服務類型、價格、地區等多元面向呈現給消費者，便可更快速方便獲得金融商品的報價，更精準地選擇適合自己需求且價格合理的金融服務與商品。

(三) 金融財務建議服務

透過資料的共享，財務顧問能串接銀行資料並根據消費者的財務習慣相關資料，更精準地了解消費者的金融投資需求，進而提供更精準的財務建議且更個人化的服務，藉以降低過去要消費者自行提供財務資訊、因經驗不足誤判投資決策、或因佣金被導致選錯投資商品等情況發生的機率。

(四) 信用評分與證明精準化

透過創新 TSP 業者服務，使消費者更容易的提供其財務狀況，在申請新的產品時，能夠向經紀人或貸方提供所有銀行業務資料的存取權限，從而進行全面的檢視與審核，提供更客製化的貸款建議以及方案。此外，如在英國按時繳交租金之租戶，如有貸款需求時，可授權貸方銀行取得其於平台上的信用證明，以證明其信用可

靠性，可以使在金融市場上缺乏金融數據，無法貸款的社會新鮮人，評估其信用風險，進而增加取得貸款服務的機會。

三、開放銀行與消費者賦權

根據臺灣人工智慧行動網於 2020 年 10 月辦理之「開放銀行與消費者賦權的想像及挑戰」會議針對資料賦權與消費者賦權的探討，資料賦權係指隨著大數據時代下資料的各種運作，資料被授權予業者和消費者。業者拿到資料，可催生創新服務，故資料賦權(empower)給更多產業的參與者；但從另一角度觀察，資料亦可能賦權給消費者本身。當資料在不同行業間進行跨業流通時，可能對消費者帶來便利的服務體驗，當消費者取得對自身攸關資料的主控權，可以資料可攜方式讓自己的資料在不同服務提供者間流動，最後將讓消費者面對的金融服務的選擇變多，這是開放銀行對消費者賦權議題的願景。

國際知名學術出版品供應商 IGI Global 對於消費者賦權有進一步的界定[44]，消費者賦權(Consumer Empowerment)係指消費者在市場上與其他對象互動時，能夠依照自己的需求進行決策，從而實現自己的選擇；此一觀點亦可與前述臺灣人工智慧行動網的界定互為呼應。

根據前述開放銀行應用場景分析，消費者在享受更精準的金融創新服務體驗同時，金融資料也因消費者授權給 TSP 業者進行加值利用，承受更多資訊隱私風險。以下將聚焦說明開放銀行的消費者風險議題，並對風險因應措施進行初步建議。

(一) 議題一：消費者個資蒐集同意與權利義務是否有明確告知

在隱私保護議題上，首先應思考新型態的資料利用方式是否可能導致銀行或第三方服務供應商違反個人資料保護法之法遵風險。

[44] https://www.igi-global.com/dictionary/personally-engaged-with-retail-clients/40673

例如個資蒐集與權利義務告知、個資的使用、傳輸、儲存與銷毀以及個資的糾紛與處理。銀行業者在將資料權還給消費者時，也應確保消費者明白開放資料可能帶來的資訊隱私風險，並善盡告知事宜。

在國際上，歐盟與澳洲皆從法規加強業者(並非僅金融業)對消費者的權利義務告知作業。其中又以 2016 年公告的歐盟「資料保護一般規則」(General Data Protection Regulation，以下簡稱 GDPR）在產業上為消費者授權要求建立了高標準。GDPR 要求公司的授權同意描述必須以易於理解的形式且使用清晰明瞭的文字表達，並強制規範應告知客戶有關其個人資料的蒐集、使用和揭露，以及包括個人資料將如何用於行銷或銷售的機會。

澳洲的消費者權利法規 CDR 也規範在開放銀行業務下的同意必須是明確、充分知情的積極同意，且設有時間對該同意進行限制或撤回。開放銀行的參與者所面臨的挑戰是要提供正確、詳細且確保消費者容易理解的權利行使指示，以獲得消費者的允許使用其數據，也避免存取資料時，造成消費者對服務內容不了解的恐懼和不信任感。

■ 保護強化建議

1. 制定個人資料管控程序書，成立文件控管小組，落實控管與處理流程並且定期更新程序書規範。
2. 妥善留存告知事項相關紀錄，組織應妥善保存所有告知事項記錄，包含紙本文件、電子文件或電話錄音等。並且確保保存的時限與個人資料保留的時間相同，保障當事人與組織雙方權益。

(二) 議題二：消費者個資的使用與傳輸

個人資料的使用只能用於其蒐集的主要目的，僅有在有例外的情況下方可用於次要目的。因此，透過開放銀行接收個人資料的 TSP 業者，應遵循委託銀行之合約規範，只能將資料用於合約約定的主要目的，或證明次要目的與主要目的直接相關以作為輔助使用。參考澳洲與歐盟等國際相關規範，澳洲的開放銀行創新政策始於 2017 年底開始推動 CDR，公告消費者的交易或商品相關數據可交由第三方業者使用，並以銀行業服務為優先使用第一順位，其次為能源、電信或其他產業。整體而言，澳洲的消費者資料法(Consumer Data Right)的規範框架係以消費者的資料自主權為主，消費者可要求業者提供資料調閱服務，亦可要求業者刪除或停止使用其資料，甚至也限制也者將其資料提供給他人使用。

GDPR 則規範組織應採取基於風險的方法來實施適當的技術和組織措施，確保資料的機密性、完整性，以及可用性。資料發送者必須明確告知客戶，其已經收到他們的指示。銀行的資料必須通過安全的 API 進行傳輸，使資料可以安全的從組織的系統傳輸到應用程式或其他平台。而關鍵數據安全性應考慮因素包括在轉移個人信息之前確保有識別和驗證過程。此外，個人資料在海外與第三方之間的轉移也必須考慮適用要求，包括與第三方業者簽訂的協議的必要性。

■ 保護強化建議

1. 組織應依據員工的職位與業務需要嚴格管理個資存取權限，開設不同的存取權限，確保僅有需求之員工才可以存取企業所擁有的個人資料。
2. 資料去識別化強化隱私保護。
3. 在紀錄與共享敏感資料時，應使用資料遮蔽、去識別化之

策略與技術，如差別性隱私、聯合式分析或同態加密等，以解決隱私資料保護之疑慮。

4. 建立隱私保護管理制度。
5. 企業對於隱私保護的控制實現可透過建立隱私資料管理制度(PIMS)實現，從而保護用戶個人資料。

(三) 議題三：個資儲存與銷毀

檢視 GDPR 與澳洲 CDR 之規範，二者皆在資料儲存安全有相當的要求，其採取措施包括安全控制措施必須與資料的敏感性相稱；此外，一旦任何法律、合約或法規保留期到期，應立即銷毀或使數據無法再進行辨識。再者，GDPR 賦予個人在某些情況下能行使被遺忘的權利，以刪除其資料。

■ 保護強化建議

1. 加強確認 TSP 業者的個資保護機制強化與落實性，以及其銷毀機制是否能確實抹除/去識別化消費者個人資料。並於資料保護期限屆期時確實執行、落實。
2. 針對使用雲端服務之 CSP 業者，TSP 業者應與 CSP 業者確實了解機敏資料之儲存與銷毀機制，以降低消費者個資外洩之風險。

(四) 議題四：個資糾紛與處理

近年來，世界各國發生多起掌握大量客戶個人資料的企業遭駭或個人資料外洩的重大資訊安全事件，以至於大大降低使用者對大型業者所蒐集的個人資料安全信任度。隨著開放銀行的發展，消費者將面臨更多元的開放銀行服務應用場景，企業也將面臨更多的消費爭議處理，消費者權益保障以及消費者個人資料的處理和利用爭議出現的頻率也將隨之增加。

就制度面與技術面而言，我國銀行公會與財金公司已訂定相關自律規範，包含資訊安全控管、身份認證、授權、雲端儲存等面向，與開放業務種類制定技術與資安標準等，以落實規章準則、作業程序、內部控制的因應，以健全新型態金融服務的發展生態和消費者權益的保障。不過對於事件的權責因應目前主要由銀行第一時間進行承擔。

■ **保護強化建議**

1. 從資訊系統控管和風險因應角度出發，強化組織風險管理。
2. 在證據保存議題，應確保個資軌跡與相關證據之留存符合個資法至少保存五年的規範。
3. 依照目前自律規範的規定，當開放銀行業務出現類似資料外洩爭議時，是由銀行負起對 TSP 業者監督的責任，大幅降低銀行業者參與第二階段開放銀行測試的意願。解決方向可參考英國設立中介單位--OBIE，當銀行與 TSP 業者發生資料傳輸爭議時居中調解爭議。

四、案例研析

(一) 我國之金融消費爭議處理流程

我國現設有金融消費評議中心單一專責機構，係已參考「英國金融服務暨市場法」、「英國金融公評服務機構」（Financial Ombudsman Service Ltd.）與「新加坡金融業調解中心」（Financial Industry Disputes Resolution Centre Ltd.）運作機制及《金融消費爭議處理機構設立及管理辦法》成立與運作，並依循《金融消費者保護法》公平合理、專業地處理金融消費爭議問題，建立金融消費爭議處理機制，落實強化金融消費者保護各項措施。

1. 金融消費者就金融消費爭議事件應先向金融服務業提出申訴，金融服務業應於收受申訴之日起三十日內為適當之處理，並將處理結果回覆提出申訴之金融消費者；金融消費者不接受處理結果者或金融服務業逾上述期限不為處理者，金融消費者得於收受處理結果或期限屆滿之日起六十日內，向爭議處理機構申請評議；金融消費者向爭議處理機構提出申訴者，爭議處理機構之金融消費者服務部門應將該申訴移交金融服務業處理。

2. 金融消費者申請評議後，爭議處理機構得試行調處；當事人任一方不同意調處或經調處不成立者，爭議處理機構應續行評議。

3. 爭議處理機構於受理申請評議後，應由評議委員會主任委員指派評議委員三人以上為預審委員先行審查，並研提審查意見報告。

4. 預審委員應將審查意見報告提送評議委員會評議。評議委員會應公平合理審酌評議事件之一切情狀，以全體評議委員二

分之一以上之出席，出席評議委員二分之一以上之同意，作成評議決定。

5. 當事人應於評議書所載期限內，以書面通知爭議處理機構，表明接受或拒絕評議決定之意思。評議經當事人雙方接受而成立。

6. 金融服務業於事前以書面同意或於其商品、服務契約或其他文件中表明願意適用本法之爭議處理程序者，對於評議委員會所作其應向金融消費者給付每一筆金額或財產價值在一定額度以下之評議決定，應予接受；評議決定超過一定額度，而金融消費者表明願意縮減該金額或財產價值至一定額度者，亦同。

7. 金融消費者得於評議成立之日起九十日之不變期間內，申請爭議處理機構將評議書送請法院核可。爭議處理機構應於受理前述申請之日起五日內，將評議書及卷證送請爭議處理機構事務所所在地之管轄地方法院核可。但爭議處理機構送請法院核可前，金融服務業已依評議成立之內容完全履行者，免

送請核可。

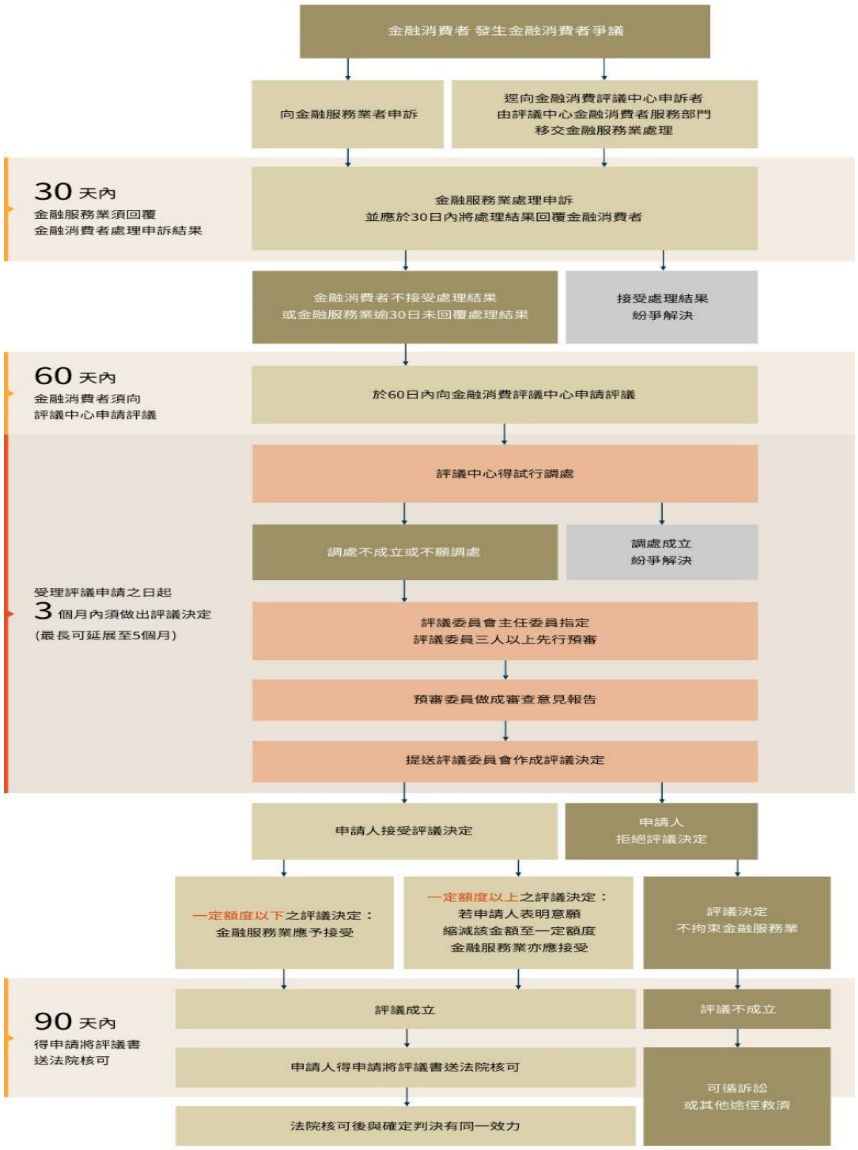

圖 22 我國金融消費評議流程

資料來源：財團法人金融消費評議中心, 2021

惟因我國開放銀行於第三階段交易面應用服務之推動，銀行透過 TSP 業者簽訂契約，並由 TSP 業者提供予消費者的金融服務內容，並不在「金融監督管理委員會組織法」第二條規定的金融服務業範疇，故在 TSP 業者提供之服務類別，並非金融業特許的核心業

務狀態下，較難直接適用現行金融消費者保護法的程序。

(二) 英國金融申訴服務 (The Financial Ombudsman Service)

英國金融申訴服務係根據《2000 年金融服務和市場法》所設定設立的法定爭議解決方案，並定為為非營利組織。根據該組織網站介紹，其所提供的金融申訴服務範圍，主要包含民眾與保險、汽車融資貸款、養老金給付、一般貸款產業之間的爭議。該組織依據為金融行為監管局 (FCA) 為其制定的規則提供服務，接受之金融服務申訴領域，涵蓋付款保險、銀行與支付、信用貸款、抵押等項目。

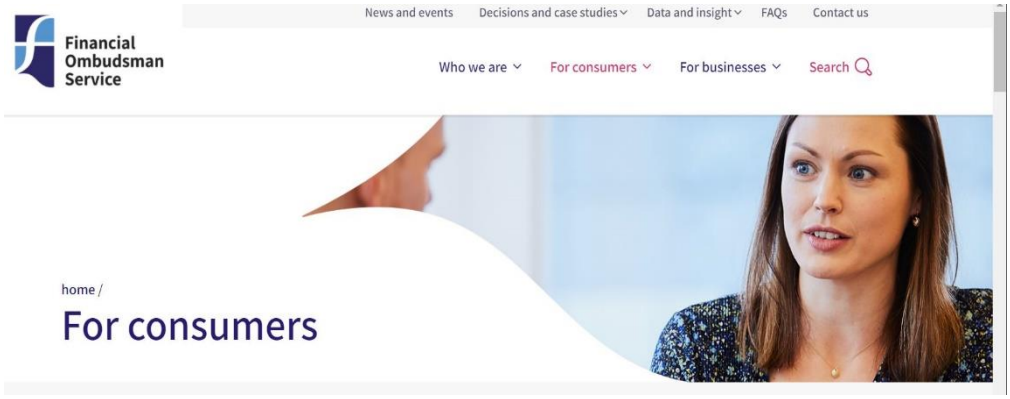

圖 23 英國金融申訴服務組織官網

資料來源：The Financial Ombudsman Service, 2021

圖 24 英國金融消費服務組織之服務項目

資料來源：The Financial Ombudsman Service, 2021

以下表整理常見的銀行消費服務爭議事件，包含被錯誤或延誤收費、其他連鎖經濟損失、非財產上損害以及詐欺損失等。在銀行與支付領域，該組織常見處理爭議類型，包括帳戶或信用貸款等支付服務爭議，與因資訊服務異常導致消費者無法正常使用其帳戶之爭議申訴案件；而近年由於銀行資安問題直接導致消費者的帳戶出現詐欺狀況亦日益增長。

表 29 常見銀行業消費爭議列表

常見銀行業消費爭議	範例
被錯誤或延誤收費	如果消費者銀行帳戶的付款被延遲，其可能會遭受經濟損失，包含但不限於因延誤付款而產生的費用。 例如，延遲向儲蓄帳戶付款可能意味著消費者將失去儲蓄利息。若受害者是一家小型企業，其可能會因企業帳戶中斷而遭受交易損失。
其他連鎖經濟損失	在嘗試解決銀行問題時，消費者可能需額外付出各類處理成本，例如電話費、停車費。甚至可能因此帶來更大經濟損失，例如如果消費者不得不推遲購買房屋，則可能會產生額外的法律費用。
非財產上損害	消費者可能因為經歷過的事情而遭受了麻煩、壓力或不便。 例如，其可能因為無法償還欠下的債務深感壓力，或不得不請假來解決緊急問

	題連帶造成薪資損失。
詐欺	由於銀行的資安問題直接導致消費者的帳戶出現詐欺案件。

資料來源：The Financial Ombudsman Service, 2021

該組織處理流程大略為，定期針對各投訴之事實和情境，先判斷在該消費情境的公平合理界線，並公正地聽取消費者和企業雙方之意見後，就金融法規和行為準則等做為評議金融消費裁定的基礎以進行仲裁。

此外，該組織之評議程序，會考慮其他事項，包含企業是否、以及透過何種方式，試圖與消費者達成解決方案。若消費者因該金融消費爭議導致經濟上的困難，該企業是否為消費者提供補償性支持方案，綜合前述調查重點，該組織會出具其調查結果，並和消費者解釋該組織是否認為企業有公平對待消費者。若該組織認為該企業對消費者不公平，其會列出需要採取哪些措施來糾正問題。

我國《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 10 條第 1 項中已參考香港立法例（銀行業開放 API 框架（Open API Framework for the Hong Kong Banking Sector）之要求，明訂「消費者與第三方服務提供者或會員銀行發生消費爭議時，會員銀行應提供消費者申訴管道，並應提供消費者協助，以妥適處理消費爭議。」，並要求銀行應消費者與 TSP 業者或銀行發生消費爭議時，銀行應提供消費者申訴管道，並應提供消費者協助，以妥適處理消費爭議。

惟當消費者與銀行及 TSP 業者產生消費爭議時，宜有適當管道或官方/非官方機制處理相關爭議，針對消費爭議處理機制設計。以國際相關案例分析其爭議處理機制設計比對我國現況，考量開放銀行係由 TSP 業者與銀行合作所提供之開放銀行交易面應用服務，對消費者的

銀行資訊進行共享與使用，係 TSP 業者作為消費者與銀行之中介角色，將金融消費者同意之銀行相關資訊進行約定之使用，可將 TSP 業者與銀行等同而視之。此外，從個資法觀點觀之，係銀行於金融消費者同意下授權 TSP 業者使用，TSP 業者應與銀行共同負責任。因此，相關服務或衍生之消費爭議，本質上屬金融商品或服務，避免讓金融消費者承受對 TSP 業者求償之不利益，應由銀行承擔第一線對消費者的賠償責任為妥，據此，參考英國制度尚未建立專責處理平台之前（例如數位部），建議開放銀行之消費爭議專責機構可由非官方但具有半官方與司法功能之「金融消費評議中心」擔任，當有爭議發生時，消費者得向金融機構申訴後，或直接向金融評議中心申請進行爭議解決。

由現行金融消費爭議的權責機構即金融評議中心擔任專責機制，將開放銀行消費爭議納入評議服務之範圍，考量 TSP 業者非屬金融機構，目前尚無法適用金融消費評議中心之爭議處理途徑，故建議配套措施為，應針對開放銀行之「金融消費爭議」事件明確定義，包含如因 TSP 業者之資訊服務異常導致消費者無法正常使用其帳戶之爭議情形，或 TSP 業者發生資安事件導致消費者帳戶遭入侵等情況，並考量修訂《金融服務業提供金融商品或服務前說明契約重要內容及揭露風險辦法》或另立金融消費者保護法子法，要求銀行及 TSP 業者於提供交易面服務前應對消費者說明之開放銀行之契約重要內容及風險，以提高消費者風險意識，並打造消費者、TSP 業者、金融機構三方共贏的開放銀行法律環境。

五、建議措施

綜上所述，在開放銀行情境中，如 TSP 業者非受金融機構之委託（此應為多數情形），則對於消費者個資之保護，金融機構與 TSP 業者分別均為個人資料之蒐集機關，各自承擔個資法中的法律責任（金融機構並應另行遵守特別法規範）。對金融服務消費者而言，現行金融消費爭

議處理，若無涉金融服務業範疇，無法透過金融消費評議申訴機制解決，尋求司法救濟是選項之一，現行訴訟體系已有小額 (涉訟金額 10 萬以下)以及簡易訴訟程序(10 萬以上~50 萬以下)機制，在不修法的前提下，建議強化小額/簡易訴訟的消費者認知宣導和法律諮詢協助管道，惟其缺點為消費者訴訟曠日廢時，求償意願將會大幅將低。

而金融機構與 TSP 業者的法律責任差異，主要為「資訊安全維護」的法律義務程度，以及「個資侵害事故」之通報對象（中央目的事業主管機關）。是本研究提出下列措施，供金管會作為於開放銀行情境下，強化消費者保障之參考：

(一) 短期措施(一年)

在現行以提升開放銀行之發展，鼓勵金融機構與 TSP 業者參與為原則之前提下，維持金融機構自律模式，以自律規範作為金融機構篩選、控管 TSP 業者對消費者個資保護之方式。

其中，除適時更新、增訂相關技術標準規格或業務安全控管作業規範外，尚可考量於自律規範增訂「金融機構（受 TSP 業者通知資安事件後[45]）通報主管機關之義務」，俾利金管會即時掌握開放銀行資安事件之現況、全貌，以作為政策、規範調適之參考；如事故重大而有必要，亦可作為跨部會協調聯繫之依據。

(二) 中期措施(三年)

依《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 4 條第 3 款之要求，銀行擇定 TSP 業者時，須注意業者

[45] 中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範，第 5 條第 1 項第 4 款：「會員銀行應要求第三方服務提供者遵循下列事項：……四、當第三方服務提供者發生資安事件有損消費者權益之虞時，應主動、即時通知會員銀行及消費者，並採取適當之因應措施以確保資訊安全」。

之資訊安全及個人資料保護等風險管理能力。

是於開放銀行發展較為成熟後，金管會可請銀行公會和財金公司評估依據 TSP 業者提供之不同服務內容（查詢、申請、交易等），「訂定 TSP 業者應具備之資訊安全與個資保護能力標準（查核項目）」，為金融機構提供一致性之參考依據。

(三) 長期措施(五年)

1. 評估金融機構承擔 TSP 業者的個資侵害賠償責任適當性

金管會之長期措施尚可探究金融機構對消費者與 TSP 業者間，因個資侵害事故產生爭議時的賠償責任。

現行《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 10 條第 2 項規定「會員銀行應與第三方服務提供者約定，如消費者向會員銀行提出因其與第三方服務提供者所生之消費爭議而受有損害者，除會員銀行得證明消費者有故意或過失者外，於一定金額內由會員銀行先行給付消費者，再依業務合作契約之約定向第三方服務提供者求償」，此規定所稱「消費爭議」之範圍雖未明確定義，但似不限於消費者財產損害之爭議，尚含個資外洩等侵害事故之情形，已明確定義開放銀行之消費爭議應由會員銀行擔負爭議處理之責。

據此，該規定將使銀行承擔合作之 TSP 業者對消費者的賠償責任（再透過內部關係求償）。然而就個資保護而言，銀行與 TSP 業者均為開放銀行的獨立參與者，分別基於特定目的蒐集、處理及利用消費者之個人資料，各自承擔個資法上的蒐集機關責任。是該規定責令銀行承擔 TSP 業者的過失賠償之責，是否公允似可深究。

比較法上，歐盟個人資料保護條例（GDPR）第 20 條賦予

當事人資料可攜之權利，得要求個資控管者在技術可行的情形下，直接將其個人資料傳輸予另一個資控管者[46]。歐盟個資保護第 29 條工作小組（WP29）的「資料可攜權指引」即指出，「控管者代表當事人行事，包括將個人資料直接傳輸至另一控管者。在此情況下，考量到接收方並非傳輸資料之控管者所選擇，因此該控管者無法負責接收資料控管者對資料保護法之遵循」[47]，明確表示原始的個資控管者不需為當事人選擇的個資接收者之個資保護負責。

誠然，在歐盟 GDPR 的規範下，「資料可攜」實現了法律對個資當事人的資料賦權，主動權在於當事人，控管者係基於法律義務，在當事人行使權利時，將其個人資料（在技術可行的前提下）傳輸予當事人選擇之接收者，因此不應由個資原始控管者為該接收者之個資保護負責。此與我國現行採自願、自律機制，由銀行主動發起與 TSP 業者合作之框架不同。

然而，也正因我國目前採取金融機構自願參與之政策，該規定恐將減損銀行參與開放銀行之意願，或僅願意提供不涉及申請、交易等具高消費爭議風險之服務。該規定固然為消費者的事後受償提供較足夠之保障，惟若因此使銀行自始不願進入開放銀行市場，恐非該規定之本意。

據此，無論我國開放銀行於未來是否維持現行「業者自律」政策，或發展為「法律義務」框架，金管會均可考量依開放銀行

---

[46] EU, GDPR, §20(2), "In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."

[47] Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, WP242 rev.01, 5 April 2017, p6, "They act on behalf of the data subject, including when the personal data are directly transmitted to another data controller. In this respect, the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient."

之發展情況，據以評估由金融機構承擔 TSP 業者「對消費者的個資侵害賠償責任」之適當性，以打造消費者、TSP 業者、金融機構三方共贏的開放銀行法律環境。

2. 鑒於資料開放在各產業別的趨勢，應將 TSP 業者之管理提升至跨部門治理層級，研商通則管理規範以保障消費者權益。

根據 Govlab 於 2017 年發布之研究報告「開放資料與發展中國家經濟」，各國政府皆對系統性地運用資料對達成社會經濟福祉有相當的信念；該報告指出，資料應用將衝擊的領域涵蓋醫療、人道救援、農業與食物營養供給、減緩貧窮、能源與教育領域，公民將可透過更多的資料賦權，成為產業議題的合作夥伴，增進創新和效率。

鑒於其他業別資料開放之趨勢，本研究認為開放銀行未來走向交易面應用將涉及更廣泛的民生消費層次，同時，其他產業的資料應用也日益普及，宜應將 TSP 業者資料應用管理議題提升至跨部門議題層次，由相關部會共同研議 TSP 業者之管理規範，以利對消費者有全面性及一致性之保障。

柒、銀行辦理開放銀行之誘因分析研究

針對本項研究議題，勤業眾信團隊先行檢視我國開放銀行的機會與挑戰，並透過訪談我國參與開放銀行(Open Banking)及開放 API 的單位(包含銀行與 TSP 業者)，分析影響利害關係人參與開放銀行生態系統之因素。最終，參照國內外推動開放銀在誘因政策設計的經驗，據以提出利於開放銀行發展的誘因機制與對策。

一、我國辦理開放銀行的機會與挑戰

(一) 提高金融產業服務創新發展

傳統銀行產業的範圍較限縮於存款、放款與財富管理等，若要進一步取得競爭優勢，關鍵即在於創造差異化的創新服務體驗。開放銀行生態系統之發展，有助銀行拓展其現有服務內容，藉由與自身業務互補的 TSP 業者合作，銀行業者將在傳統的存款、放款以及財富管理業務等銀行既有業務基礎上，深入了解、參考消費者在各使用場景上的習性，讓金融服務能有效介接消費者食、衣、住、行、生活、育樂等面向。

(二) 使用者友善金融環境

隨著消費者權利意識抬頭，個人在金融資料的自主決定權議題也日益受到重視，資料可攜權發展也為金融創新服務的樣態帶來更多可能，也對傳統銀行業務封閉式運作型態帶來挑戰。在開放銀行第二階段「開放客戶資訊」階段。銀行在取得消費者同意後，可自動帶入消費者的跨行金融資訊，進行跨行整合的自動化資料交換；客戶資料的取得和應用也將有條件鬆綁，可以在資訊更透明化的情況下取得更完整的金融資料。

(三) 拓展銀行業務通路

傳統銀行的業務多仰賴分行實體櫃台服務，根據華南銀行的統計，消費者在 2016 年底在 ATM 的交易規模大於網路銀行和行動裝置，但到了 2017 年第三季，個人行動銀行的交易規模開始超越 ATM，2018 年第一季行動銀行的交易量更超越了網路銀行。未來，在消費者金融消費使用行為改變的驅動力下，銀行參與 Opening Banking 生態圈，以發展不同通路的金融業務發展可能，已是必然的現在進行式。

在 Open Banking 持續發展下，銀行得以串接 API 於多個數位平台上銷售其產品和服務，消費者則可於不同樣態的平台選擇所需的金融創新服務。以現正處於 Open Banking 發展第二階段的我國而言，銀行可以和第三方服務業者合作，從公開資料查詢進階到消費者資料查詢的服務模式；應用的場景已涵蓋：帳戶餘額查詢、帳戶整合、信用卡比價、貸款比價、投資理財推薦、信用卡設定等功能。簡單來說，只要用戶同意開放個人資料，就能享有方便的整合服務。簡言之，用戶在不同銀行或是同一金控集團下的存款、基金投資、貸款等資訊都能互通，在 TSP 業者的 App 上一次查詢，提供一站式消費者金融資料整合服務。

二、銀行與 TSP 業者合作現況

研究團於 2021 年 6 月 28 日至 7 月 1 日期間，針對部分參與開放銀行之銀行和 TSP 業者的執行訪談，並彙整結果如下：

(一) 銀行業者現況

目前 4 家受訪單位中，皆有與 TSP 業者有 Open API 的合作，另外也有一些合作案正在籌備中，預計今年可以上線。但其中一家銀行因組織發展策略考量，在與一家第一階段合作之 TSP 業者約

滿後無持續續約合作。

整體來說，銀行對開放銀行的發展保持正向的態度；但部分受訪單位表示，鑑於他國在開放資料(Open Data)的發展情形，希望未來發展趨勢不僅限於從金融業將資料攜出，消費者也可以從其他平台帶來資料，使金融業者也能成為 TSP，最終達到多市場的多邊雙向的互惠創新。

(二) TSP 業者現況

目前 4 家受訪單位中，2 家業者為進入第一階段的 TSP 業者前鋒、另外 2 家業者則是與金融業者直接進入第二階段的合作。其中尚在第一階段的 2 家 TSP 業者皆表示目前正與其他金融業者洽談第二階段的合作案，並已準備相關資安要求。

(三) 一二階段參與家數落差原因分析

根據財金公司（2019）的統計，參與第一階段開放銀行的銀行家數共計 24 家，包括凱基銀、台新銀、中信銀、國泰世華銀、合庫銀、華南銀與元大銀等都將是首波完成平台上架的金融機構。另根據聯合新聞網（2021）的報導，第二階段開放銀行目前共有 7 家銀行，即華銀、元大、中信、兆豐、一銀、國泰世華銀行以及遠東商銀參與。根據初步訪談結果，未接續申請第二階段開放銀行之銀行業者大多表示，因第一階段開放銀行營運模式較單純，技術安規準備期亦較第二階段充裕。

故其目前未參與第二階段開放銀行主因，並不是沒有意願，而是仍處於準備階段，待第二階段開放銀行所要求之技術等安規建置完成後，也有極高的意願提出第二階段開放銀行合作案申請。

三、銀行與 TSP 業者參與開放銀行之誘因與阻力

(一) 誘因

1. 銀行業者

(1)**業務發展考量**：希望與時俱進，並測試創新想法之可行性。另外透過與不同類型的 TSP 業者合作，尋找與自身業務互補的合作夥伴，藉以深入了解、參考消費者在各使用場景上的習性，未來能提供更貼切消費者需求的服務。

(2)**組織學習考量**：透過合作，希望藉機了解 TSP 業者跟消費者的溝通機制、做法與邏輯，並累積對 TSP 業者的系統開發、業務發展等創新服務與運作之機制，做為未來進階運用的基礎。

2. TSP 業者

(1)**業務發展考量**：提供消費者更多創新、安全、穩定的金融服務。

(2)**技術開發考量**：透過 API 格式統一，有效將客製化程度從 100%降至 20%，可加速開發流程。

(二) 銀行與 TSP 業者參與開放銀行之阻力

1. 銀行業者

(1)**合規能量考量**：從銀行角度而言。若合作的 TSP 家數增加，銀行也需花很多時間跟人力去查核 TSP 業者，以及合約的續約與檢視。另外內控稽核及金檢查核也會針對開放銀行業務進行資料徵提和查核，對於銀行業者來說也需另外提撥資源進行因應。

(2)**賠償責任配置疑慮**：目前銀行在參與開放銀行上尚未收費，但現行規範中將創新合作案的賠償責任放在銀行上，此項可能降

低金融機構參與開放銀行的意願，也可能成為未來擴大合作的阻力。建議可以參考歐盟或英國，以要求 TSP 業者購買相關資安保險，以確保 TSP 業者有能力一起共同承擔創新合作的風險。

2. TSP 業者

(1)合規能量考量：以 TSP 業者來說，為達到資安合規，須持續進行 **ISO27001** 的驗證，同時也須取得專案查核的通過報告。另外合作的各銀行也皆須對其進行稽核。若未來合作業者家數上升，則 TSP 業者將可能需投注更多的資源與人力在接受稽核、改善發現等作業上。

四、成本效益導向之國際誘因機制案例研析

除透過訪談初步了解影響我國開放銀行各方利害關係人之參與意願因素，本研究亦自成本效益角度，探求國際在開放銀行誘因機制設計方式。

1. 案例研究一：英國開放銀行執行組織發展「Premium APIs」以提升商業合作誘因

對於採取強制國家監理模式以治理開放銀行的英國來說，其競爭及市場管理局（Competition and Markets Authority, CMA）在 2016 年開始強制要求英國前 9 大銀行開放資料時，並沒有提供特別誘因。而英國銀行業者為符合監理法規以免受罰，也就自然地皆加入了開放銀行的行列。

但為加速金融業的服務創新，英國開放銀行執行組織（Open Banking Implementation Entity, OBIE）在 2019 年發表之委託研究報告《Open Banking: Preparing for Lift Off》中提到，希望透過發展「Premium APIs」以提升商業誘因。在現存強制的「Regulatory APIs」規範之下，英國銀行必須免費、

且在不需要簽署合約的情況下，將銀行資料分享給 TSP 業者。

而「Premium APIs」則是能夠讓銀行業者與 TSP 業者，在雙方自願的情況下，簽訂合作合約、自行決定合作模式。最重要的是，銀行業者能夠向 TSP 業者收取「Premium APIs」使用費。在此委託研究報告的訪談調查中，銀行業者認為此舉能夠帶來可觀的潛在收益，這是在先前開放銀行政策下無法享受的好處。而受訪的 TSP 業者也表示，若「Premium APIs」可為業務合作創造更大的價值，他們支持「Premium APIs」這個想法，也樂於為此付費。

OBIE 更提到，「Premium APIs」應被設計為額外的 API 標準，其標準層級可高於現今的「Regulatory APIs」，且須能與現行的 API 安全框架相容(如下圖)。因「Premium APIs」目前仍在發展階段，本研究尚無法列入「Premium APIs」確切法規標準與執行方式。

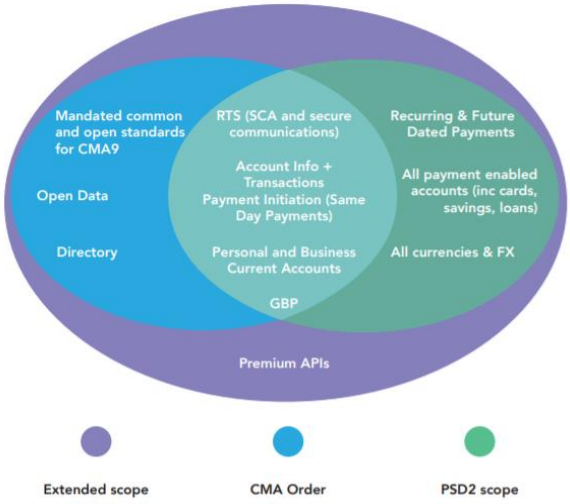

圖 25 Premium APIs 監理規範範疇示意圖

資料來源：OBIE, 2019

2. 案例研究二：澳洲規定資料交流必須為「雙向互惠」

為使銀行業者有足夠的誘因將資料分享給 TSP 業者，澳洲在

開放銀行的制度設計上，強制規範資料的交流必須為「雙向互惠」。舉例來說，TSP 業者向銀行業者提出資料申請，且取得客戶同意後，銀行就必須提供客戶資料給 TSP 業者；但之後此客戶在 TSP 業者留下的資料數據，銀行也可以要求 TSP 業者分享，而 TSP 業者並不能拒絕銀行的要求 (Scott Farrell，2019)。

3. 成本效益導向誘因機制設計成果探討

(1) 英國稅務海關總署，短短兩天內收取到 100 萬歐元稅金

2021 年 6 月，在英國開放銀行執行組織（Open Banking Implementation Entity，以下簡稱 OBIE）發表之《JUNE HIGHLIGHTS 2021》中提到英國稅務海關總署（HM Revenue & Customs，以下簡稱 HMRC）如何受惠於開放銀行政策，在兩天內收取到 100 萬歐元的稅金。

過往，英國納稅人為了繳稅，首先必須開啟他們個人的銀行系統，並且手動設定轉帳資訊，而往往錯誤就會在這個步驟中產生。為解決此問題，在 OBIE 的支持協助下，HMRC 與金融科技業者 ecospend 簽署合作合約，請 ecospend 開發了「帳戶對帳戶」支付系統（原文：account-to-account payment system）。在此系統之下，納稅人的繳稅細節資訊會自動在其銀行帳戶中生成，減少人為錯誤、也提升了 HMRC 處理稅金的速率。

(2)英國匯豐銀行透過建置 API Portal，有效促進金融服務創新發展

英國匯豐銀行與美國軟體公司 MuleSoft 合作開發 API、打造 API Portal。透過 API Portal 提供的平台，匯豐銀行能夠讓開發者更容易測試使用匯豐銀行的 API、發展合作夥

伴關係、有效管理 API、減少應用程式的開發時間。根據其統計資料顯示，雙方的合作因此減少 75% 的開發時間、創新速度提升 4 倍、有效服務 30 多個市場。

(3)API 業務驅動新加坡星展銀行 2018 年營收成長 28%

新加坡星展銀行主要依賴 API 以擴增企業客戶的數位金融服務。有別於其他銀行，星展銀行在其他家銀行尚未開展 API 業務時，就已開始布局 API 市場。API 不僅幫助 DBS 增加獲利，也能夠讓星展銀行直接打造客戶產品，而一般銀行只能單純幫忙開戶還有執行其他交易而已。(Abdul Raof Latiff，2019)。

五、建議措施

藉由訪談分析，研究團隊對參與開放銀行的利害關係人，銀行業者或 TSP 業者皆有不同的參與動機，以下針對我國銀行之誘因機制設計，研提政策建議如下：

(一) 參考英國「Premium APIs」機制，建立開放銀行合作模式收費規範

以成本效益角度觀察英國推動「Premium APIs」機制，讓銀行業者與 TSP 業者，在雙方自願的情況下，透過簽定合約、自行決定合作模式，而銀行業者能夠向 TSP 業者收取「Premium APIs」使用費。在此委託研究報告的訪談調查中也印證，銀行業者認為此舉能夠帶來可觀的潛在收益的見解；受訪的 TSP 業者也認為，若「Premium APIs」可為業務合作創造更大的價值，他們也會支持「Premium APIs」這個想法，也樂於為此付費。

(二) 簡化重複性質較高的合作案之業務申請流程

研究團隊透過訪談發現，以一個合作案從主管機關作面談報告、交付銀行公會審核，最後通過財金平台審核，整體流程需耗時至少 6 個月。而若未來銀行業者與 TSP 業者欲在現有合作基礎上再新增業務合作項目，又需再次重新耗時 6 個月的時間來申請。

本研究建議，可考量精簡現有行政流程，初步可朝至少在二次申請時簡化重複性質較高的審核程序，將可提升業者加入的意願。

(三) 根據 TSP 業者的背景和規模做分類分級管理，降低銀行業者對 TSP 業者安控監督管理的成本

考量 TSP 業者的規模與資源皆有所差異(如資本額、資訊能力)，若要求使用不同階段 API 的業者皆須達到相同等級的資安能力，將使銀行業者面臨監督管理的困難，恐須投入大量成本研議自身份級管理策略，降低銀行業者投入開放銀行意願。例如，當合作的 TSP 家數增加，銀行需花很多時間跟人力去查核 TSP 業者，以及合約的續約與檢視。另外內控稽核及金檢查核也會針對開放銀行業務進行資料徵提和查核，對於銀行業者來說，也需另外提撥資源進行因應。

本研究建議，除可外參考歐盟或英國規範，根據 TSP 業者的背景和規模做分類分級管理，並由主管機關做第一層 TSP 業者資格把關者，降低銀行業者對 TSP 業者安控監督管理的成本，亦可參考英國 OBIE 推動 Premium APIs 的概念，就開放資料的性質和類型，區分為少部分收費與大部分不須收費等二種類型，對銀行業者而言可帶來部分收益，降低其管理成本；對 TSP 業者而言，若可透過付費取得其業務開發必須的資料，則可創造雙贏局面。惟此一誘因機制設計之前題必須建立在取得消費者同意，故仍待考量其他法制或宣導配套措施。

(四) 透過政策工具，提升 TSP 業者在辦理業務前投保資安險之意願。

最後，目前銀行在參與開放銀行上尚未收費，但現行規範中將創新合作案的賠償責任放在銀行上，此項可能降低金融機構參與開放銀行的意願，也可能成為未來擴大合作的阻力。建議可以參考歐盟或英國，以要求 TSP 業者購買相關資安保險，以確保 TSP 業者有能力一起共同承擔創新合作的風險。

整體而言，目前國內資安險保單係針對大型企業需求設計，保費單件高、核保門檻高，因此推展資安險保單成效不甚理想，分析目前國內企業投保瓶頸主要有以下四個因素：

1. 企業風險意識不足

企業對資安風險意識不足或認為風險不大，或缺乏法規強制投保的誘因。對此，本研究建議可參考歐盟 PSD2 與英國的要求，以法規強制或鼓勵 TSP 業者在辦理業務前應具有投保資安險之能力。例如，現階段英國雖未強制規範 TSP 業者應投保資安險，但已明文要求 TSP 業者皆應投保專業責任險 (Professional Indemnity Insurance, PI insurance)，確保其提供專業服務過程中因意外疏忽和過錯導致服務存在瑕疵，造成服務接受方的損失，進而提供服務方應該承擔的法律賠償責任；至於資安險是否為專業責任險的一環，因近年資安議題日益受到重視，部分保險公司推出的專業責任險開始納入資安險。

2. 投保門檻高

投保企業需具備相當資訊能力、並填寫繁複的詢價資料表。對此，本研究建議，可參考富邦產險提供企業資安諮詢服務之做法，透過協助企業了解投保資安險在法遵風險的價值，

提高其投保意願。

3. 投保單件費用高

明台產險以去 2017 年為例，資安險保單平均單件保費 70 萬，並非一般中小企業可以負擔。對此，本研究建議，可參考明台產險日本母公司三井住友海上集團開發針對中小企業設計的簡易資安險保單，透過商品模組化，逐步建立中小型企業普惠投保的資安險環境和意識，是未來我國 Open Banking 和保險產業政策推動相關單位可再進一步考量之處。

4. 保險公司缺乏核保經驗

僅有部份公司具備資安險保單核保能力，且需仰賴國外再保公司報價。對此，本研究建議，宜藉由保險產業政策發展保險業者投入資安險研發的誘因機制，扶持保險業在資安險領域的商品自主開發能力。

捌、結論與建議

一、我國推動開放銀行之資安監理建議

針對我國推動開放銀行之資安監理議題，包括 API 安全、雲端安全以及 Partner API 之管理建議等，本研究研提政策建議如下：

(一) API 安全

1. 建議參考歐盟 EU-RTS 針對 API 可用性和性能，包含 API 回應時間、呼叫速率、失敗率等進行即時監控，並透過蒐集與定期審查關鍵性能指標 KPI，建立視覺化報表，進行主動且即時的性能監控，並且針對 API 資源大小、請求數量進行速率與資源的限制，以避免因 API 低可靠性與低穩定性而產生負面影響，以改善客戶體驗，提高用戶對於使用 Open API 的信任。
2. 建議參考歐盟作法建立相關交易詐欺監控機制，如定期審查詐欺交易的統計報告，含詐欺的行為、事件的數量、總價值與支付類型等。透過對於所蒐集數據的評估，識別出系統的風險，並制定解決方案以減少詐欺的發生率。
3. 建議規範參與開放銀行之組織，應實行嚴格的存取控制管理，不同角色的存取權限必須嚴格控管，避免疏於設定權限控管機制，增加資料外洩的機會與駭客透過暴力破解取得存取權限的風險。
4. 建議規範參與開放銀行之組織，應定期審查帳號權限與徹底盤查特權帳戶為不可或缺的必要措施，組織必須清楚了解誰可以存取哪些資料，並確保對有價值的資產和系統實施適當的限制。
5. 建議規範參與開放銀行之組織，應對於 API 的設計與開發進行嚴格的管理。

6. 建議針對開放銀行參與組織，應導入相關防護產品類別進行宣導並建置相關規範，包含威脅偵測、網路入侵防護以及防護管理等。

(二) 雲端安全

雲端服務可協助資源不足的新創業者發展及管理資料，並彌補其資源之落差，然面對雲端服務的安全威脅及個資保護議題，TSP 業者及金融業者之控管要求尚有不同，本研究研建議，考量將金融機構所應遵循之雲端安全管理規範納入 TSP 業者控管要求，使金融業者與 TSP 業者所需遵循之規範精神一致。

針對金融機構與 TSP 業者合作後，將開放資料放置於公有雲端平台，建議應修訂《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》，增修金融機構在開放銀行之合作中，若 TSP 業者涉及使用雲端服務處理金融機構所蒐集之資料之情境，TSP 業者應備妥作業委外計畫書等文件，交由金融機構審核，並限制 TSP 業者應採用自行開發之系統、限制採用境內公有雲儲存，以及雲端服務業者應通過資安認證要求等要求，以確保 TSP 業者所挑選之雲端服務業者之服務可靠性、安全性及穩定性。

(三) Partner API 管理

針對合作夥伴 API（Partner API）的管控，新加坡 Playbook 係依據金融機構是否擁有合作後的使用者經驗，分成兩種模式進行管控。考量我國銀行過去已有許多不同的業務已透過 Partner API 跟第三方單位合作並行之有年，本研究評估現行以委外合作的方式進行控管尚屬合理。

然而隨著 Open API 的推動，Partner API 的關係已不再僅限於傳統金融業務，許多銀行業者也開始透過 Partner API 自行與 TSP

業者洽談創新合作業務。但這些創新合作業務，不像傳統金融業務已有完整的管理框架，也不在 Open API 的管控範圍內；銀行與第三方業者僅需遵循雙方所簽訂之契約內容，而無需遵循開放應用程式介面業務安全控管作業規範。這可能使消費者的個人資料在透過 Partner API 傳遞時，因雙方無嚴謹的規範而造成個資外洩的風險。綜上，因 Partner API 與 Open API 本質皆為資料交換，本研究建議宜考量將 Partner API 納入現行 Open API 的監理架構，確保二者監理強度的一致性。

二、我國推動開放銀行之消費者個資保護監理建議

(一) TSP 業者與金融消費爭議評議

查金融消費者保護法之目的在於「保護金融消費者權益，公平、合理、有效處理金融消費爭議事件」（見金融消費者保護法第 1 條），該法適用之「金融消費爭議」，依第 5 條規定係指「金融消費者與金融服務業間因商品或服務所生之民事爭議」，其中，「金融消費者」指「接受金融服務業提供金融商品或服務者」（見金融消費者保護法第 4 條第 1 項本文）；「金融服務業」指「銀行業、證券業、期貨業、保險業、電子票證業及其他經主管機關公告之金融服務業」（見金融消費者保護法第 3 條第 1 項）。

據此，一來 TSP 業者（或稱金融科技業者）尚未由主管機關公告為適用金融消費者保護法之金融服務業；二來 TSP 業者提供服務之本質在於「資料（數據）的流通」，即便該服務最終與「金融」相關，但仍發生於銀行業等金融服務業端，TSP 業者本身提供之服務並未直接涉及「金融商品或服務」，因此目前恐較難依現行金融消費者保護法規定，將 TSP 業者納入該法適用之對象。

未來各業別資料將走向資料開放，同一 TSP 業者可能介接不同業別資料，建議由相關部會研議相關管理規範，以利對消費者有全

面性及一致性之保障。

(二) 個資侵害通報義務

在現行個人資料保護法第 12 條規範下，資料蒐集機關如有個資侵害事故發生，符合該法要件時，應自行即時通知「當事人」；此外，金管會依照個人資料保護法第 27 條第 2 項、第 3 項訂定的安全維護辦法中，第 6 條第 2 項前段另明定「非公務機關遇有重大個人資料事故者，應即通報本會」。

又依行政院於 110 年 8 月 11 日函頒之「行政院及所屬各機關落實個人資料保護聯繫作業要點」規定，各事業之中央目的事業主管機關均刻正於依照個人資料保護法第 27 條第 2 項、第 3 項訂定的安全維護辦法中，增訂要求受監理事業於個資侵害發生時，對中央目的事業主管機關之通報義務。

金管會即於 110 年 10 月 7 日預告「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第 2 條、第 6 條修正草案，其中第 6 條第 2 項修正本文明定「非公務機關遇有重大個人資料事故者，應依附件格式於七十二小時內通報本會」，增訂監理事業的事故通報時限要求。

據此，倘開放銀行服務遇有消費者個資侵害事故時，依照我國現行個人資料保護法規，應由事故發生機關依據法規，通報其中央目的事業主管機關。

針對我國推動開放銀行之消費者個資保護監理議題，本研究研提短、中、長期建議如下：

1. 短期措施(一年)

建議在現行以提升開放銀行之發展，鼓勵金融機構與 TSP 業者參與為原則之前提下，維持金融機構自律模式，以自律規範作為

金融機構篩選、控管 TSP 業者對消費者個資保護之方式。

其中，除適時更新、增訂相關技術標準規格或業務安全控管作業規範外，建議考量於自律規範增訂「金融機構（受 TSP 業者通知資安事件後 ）通報主管機關之義務」，俾利金管會即時掌握開放銀行資安事件現況、全貌，以作為政策、規範調適之參考；如事故重大而有必要，亦可作為跨部會協調聯繫之依據。

2. 中期措施(三年)

依《中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範》第 4 條第 3 款之要求，銀行於擇定 TSP 業者時，須注意業者之資訊安全及個人資料保護等風險管理能力。是於開放銀行發展較為成熟後，金管會亦可請銀行公會或財金公司評估依據 TSP 業者提供之不同服務內容（查詢、申請、交易等），訂定「TSP 業者應具備之資訊安全與個資保護能力標準（查核項目）」，為金融機構提供一致性之參考依據。

3. 長期措施(五年)

長期而言，建議評估是否納管符合一定條件之 TSP 業者，以及金融機構承擔 TSP 業者的個資侵害賠償責任適當性。就是否納管符合一定條件之 TSP 業者，建議持續追蹤國際法規實務發展趨勢，掌握開放銀行國家對於 TSP 業者在消費者個資保護方面之監理措施，並依據我國未來開放銀行的發展情形，以及其他業別資料開放之進程，由相關部會共同研議 TSP 業者之管理規範，以利對消費者有全面性及一致性之保障。

就金融機構承擔 TSP 業者的個資侵害賠償責任適當性，金管會之長期措施尚可探究金融機構對消費者與 TSP 業者間，因個資侵害事故而生爭議時的賠償責任。就個資保護而言，銀行與 TSP

業者均為開放銀行的獨立參與者，分別基於特定目的蒐集、處理及利用消費者之個人資料，各自承擔個資法上的蒐集機關責任。是該規定責令銀行承擔 TSP 業者的過失賠償之責，是否公允似可深究。

玖、參考文獻

中文參考文獻

王儷玲（2021）。我國開放銀行發展剖析與政策建言。財團法人台北外匯市場發展基金會專題研究計畫。

香港金融管理局（2021 年 5 月 13 日）。第三及第四階段開放應用程式介面（開放 API）的實施計劃，取自：https://www.hkma.gov.hk/chi/news-and-media/press-releases/2021/05/20210513-3/

Microsoft Ignite（2021 年 9 月 23 日）。**ENISA 資訊保證架構**，取自：https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-enisa

Microsoft Ignite (2021 年 9 月 15 日), 《ISO/IEC 27001:2013 資訊安全性管理標準，取自：https://docs.microsoft.com/zh-tw/compliance/regulatory/offering-iso-27001

CIO Taiwan（2020 年 7 月 1 日）。**開放銀行邁向第二階段－OPEN API 技術合規與測試說明會**。取自：https://www.cio.com.tw/open-bank-towards-phase-2-open-api-technical-compliance-and-test-description/

中國信通院（2020）。应用程序接口（API）数据安全研究报告。

香港銀行公會（2019 年 11 月 15 日）。開放應用程式介面第二階段共同基準。取自：http://www.hkab.org.hk/DisplayArticleAction.do?ss=22&lang=b5&sid=5

英國標準協會（2018）。淺談 NIST 網路安全框架及驗證方案。**BSI 臺灣電子報**。

英文參考文獻

Verhulst & Young (2017). Open Data In Developing Economies: Toward Building an Evidence Base on What Works and How. ***The GovLab.*** P.61-80.

SME Finance Forum (2018, July 26). ***Finance-as-a-Service: API Playbook***. Retrived July 15, 2021, from https://www.smefinanceforum.org/post/financial-world-finance-as-a-service-api-playbook#:~:text=The%20Association%20of%20Banks%20in%20Singapore%20has%20published,information%20standards%20supporting%20these%20APIs%20are%20also%20defined.

Singapore Government(2021). ***Financial Industry API Registe***r. Retrived July 15, 2021, from https://www.mas.gov.sg/development/fintech/financial-industry-api-register

Hong Kong Monetary Authority (2018, July 18）.***Open API Framework for the Hong Kong Banking Sector***. Retrived July 15, 2021, from Hong Kong Monetary Authority - Open Application Programming Interface (API) for the Banking Sector (hkma.gov.hk)

APIsecurity.io (2019),***API2:2019 — Broken authentication.*** Retrived July 15, 2021, from https://salt.security/blog/api2-2019-broken-user-authentication

Australian Competition and Consumer Commission (2018). ***Consumer data right.*** Retrived July 15, 2021, from https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0

Data Standards Body . ***Consumer Data Standard***, Retrived July 15, 2021, from:

https://consumerdatastandardsaustralia.github.io/standards/#introduction

Deloitte India (2021). ***Unleashing the power of data and seizing new opportunities.*** Retrived July 15, 2021, from: https://www.bing.com/search?q=Deloitte+India+(2021.01)%2C+《Unleashing+the+power+of+data+and+seizing+new+opportunities》&cvid=03b898d59ea74cedb46f56d12eb2ba21&aqs=edge..69i57.392j0j4&FORM=ANAB01&PC=U531

Dhwani Pandya (2010). ***New ISACA audit programs include cloud computing focus***. Retrived July 15, 2021, from: https://www.computerweekly.com/news/2240022355/New-ISACA-audit-programs-include-cloud-computing-focus

Dr. Ruth Wandhöfer (2020). ***Open Banking: how can third party providers succeed.*** Retrived July 15, 2021, from: https://thepaypers.com/expert-opinion/open-banking-how-can-third-party-providers-succeed--1245820

European Payments Council (2018) . ***The European Commission's final RTS are in the Official Journal.*** Retrived July 15, 2021, from: https://www.europeanpaymentscouncil.eu/news-insights/news/european-commissions-final-rts-are-official-journal

Financial Conduct Authority (2017). ***Account information and payment initiation services.*** Retrived July 15, 2021, from: https://www.fca.org.uk/consumers/account-information-and-payment-initiation-services

Hogan Lovells Solutions Limited (2017). ***PSD2: ban on traditional screen scraping confirmed in final strong customer authentication RTS.*** Retrived July 15, 2021, from: https://www.engage.hoganlovells.com/knowledgeservices/news/psd2-ban-on-traditional-screen-scraping-confirmed-in-final-strong-customer-authentication-rts

IGI Global. What ***is Consumer Empowerment***. Retrived July 15, 2021, from: https://www.igi-global.com/dictionary/personally-engaged-with-retail-clients/40673

Lucian Constantin (2020). ***APIs are becoming a major target for credential stuffing attacks***. Retrived July 15, 2021, from: APIs are becoming a major target for credential stuffing attacks | CSO Online

Lucy Kerner (2021). Critical ***API security risks: 10 best practices.*** Retrived July 15, 2021, from: Critical API security risks: 10 best practices | TechBeacon

McKinsey & Company. ***Cutting through the noise: How banks can unlock the potential of APIs***. Retrived July 15, 2021, from: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/cutting-through-the-noise-how-banks-can-unlock-the-potential-of-apis#

Open Banking Implementation Trustee (2020). ***2020 Annual Repor***t. Retrived July 15, 2021, from: Home - Annual Report 2020 (openbanking.org.uk)

Pinsent Masons LLP (2019). ***PSD2: FCA gives temporary lifeline to screen scrapers***, Retrived July 15, 2021, from: https://www.pinsentmasons.com/out-

law/news/psd2-fca-gives-temporary-lifeline-to-screen-scrapers

Radware (2021). ***Radware Research: API Abuse is a Leading Threat; Enterprises are Unprepared for Bot Traffic.*** Retrived July 15, 2021, from: https://www.radware.com/newsevents/pressreleases/2021/api-abuse-threat-bot-traffic

Reserve Bank of Australia (2020). ***Main Types of Financial Institutions.*** Retrived July 15, 2021, from: ***https***://www.rba.gov.au/fin-stability/fin-inst/main-types-of-financial-institutions.html

Sandra Gyles (***2019***). ***APIs Next Major Target for Hackers.*** Retrived July 15, 2021, from: https://vpnoverview.com/news/apis-next-major-target-for-hackers/#:~:text=Security%20experts%20believe%20that%20hackers%E2%80%99%20next%20major%20target,if%20they%20have%20something%20of%20interest%20to%20cybercriminals.

附錄一 專案執行進度摘要表

項次	研究議題	研究內容	交付項目	執行情形
1	開放銀行交易面應用服務之消費者使用情境分析	• 各國推動開放銀行發展模式與成果研究分析 • 各國開放銀行交易面服務 API 種類及應用場景研究分析	期中報告	• 已完成
		• 開放銀行交易面應用之創新發展策略藍圖	期末報告	• 已完成
2	推動開放銀行後,API之管理方式及安控要求	• 各國開放銀行 API 管理模式及安控要求法規研究分析 • API 設計安全研究分析	期中報告	• 已完成
		• 開放銀行 Open API 風險管理框架與策略	期末報告	• 已完成

3	消費者透過 TSP 業者向銀行申請業務之種類與範圍，及消費者個資之保護議題分析	• 業務種類分析
		• 辦理業務時的風險,包含:
		  • 身份驗證與授權管理研究分析
		  • 數位身份識別研究分析
		  • 訊息正確性研究分析
		  • 第三方服務供應商安全管理研究分析
		  • 威脅防護研究分析
		• 消費者權益及隱私保護研究分析
			期中報告	• 已完成

		• 開放銀行交易面應用場景與消費者權益保護管理建	期末報告	• 已完成

項次	研究議題	研究內容	交付項目	執行情形
		議		

4	TSP 業者使用雲端服務之控管建議	• 現行 TSP 業者使用雲端之情形研究，包含
		  • IaaS, PaaS, SaaS 個別之使用需求及比例
		  • 使用情境
		  • 風險點分析
		• 控管建議
			期中報告	• 已完成

		• 議題分析與建議	期末報告	• 已完成
5	TSP 業者與銀行合作後之代理登入之議題分析	• 國內外代理登入情境個案整理 • 代理登入風險點分析	期中報告	• 已完成
		• 議題分析與建議	期末報告	• 已完成
6	銀行辦理開放銀行之誘因分析	• 研究國外如何推動開放銀行發展 • 整理分析國內開放銀行推到第二階段人數驟減的原因	期中報告	• 已完成
		• 銀行辦理開放銀行之誘因分析與對策	期末報告	• 已完成

附錄二 訪談紀錄

(一) 訪談期間：110 年 6 月 23 日(三)~7 月 1 日(四)

(二) 訪談單位/人員：

業者類型	受訪單位名稱
銀行	中國信託銀行
銀行	永豐商業銀行
銀行	兆豐國際商業銀行
銀行	國泰世華商業銀行
TSP	金尉股份有限公司(CW Money)
TSP	臺灣集中保管結算所
TSP	睿元國際股份有限公司(Moneybook)
TSP	遠傳電信股份有限公司

(三) 訪談方式：線上訪談(Microoft Teams)

(四) 訪談結果

訪談大綱分為三大主題，包含組織背景了解、Open API 平台參與度調查、以及研發技術與資安能量調查。以下摘錄 2021/06/28~2021/07/01 的產業訪談回饋如下：

(一) 合作現況

1. 銀行業者

目前 4 家受訪單位中，皆有與 TSP 業者有 open API 的合作，另外也有一些合作案正在籌備中，預計今年可以上線。但其中一家銀行因組織發展策略考量，在與一家第一階段合作之 TSP 業者約滿後無持續續約合作。

2. TSP 業者

目前 4 家受訪單位中，2 家業者為進入第一階段的 TSP 業者前鋒、另外 2 家業者則是與金融業者直接進入第二階段的合作。其中尚在第一階段的 2 家 TSP 業者皆表示目前以正在與其他金融業者洽談第二階段的合作案，並已準備相關資安要求。

(二) 對主管機關推行開放銀行政策之想法

整體來說，受訪單位皆對開放銀行的發展保持正向的態度；但部分受訪單位表示，鑑於他國在開放資料(Open Data)的發展情形，希望未來發展趨勢不僅限於從金融業將資料攜出，消費者也可以從其他平台帶來資料，使金融業者也能成為 TSP，最終達到多市場的多邊雙向的互惠創新。

(三) 參與開放銀行之誘因分析

(1) 銀行業者

A. 業務發展考量

希望與時俱進，並測試創新想法之可行性。另外透過與不同類型的 TSP 業者合作，尋找與自身業務互補的合作夥伴，藉以深入了解、參考消費者在各使用場景上的習性，未來能提供更貼切消費者需求的服務。

B. 組織發展/相互學習

透過合作，希望藉機了解 TSP 業者跟消費者的溝通機制、做法與邏輯，並累積對 TSP 業者的系統開發、業務發展等創新服務與運作之機制，做為未來進階運用的基礎。

(2) TSP 業者

A. 業務發展考量

提供消費者更多創新、安全、穩定的金融服務

B. 技術開發考量

透過 API 格式統一，有效將客製化程度從 100% 降至 20%，可加速開發流程。

C. 主管機關期許

剛好欲發展的業務與主管機關第二階段的推動要求相符，故同意參加作為示範案。

(四) 參與開放銀行之優化建議

經彙整訪談結果發現在參與開放銀行的過程中，對銀行業者或 TSP 業者其實都有遇到相類似的困境。以下將綜合整理產業對於參與開放銀行之建議：

(1)業務申請過程過長

以一個合作案為例，從主管機關作面報、銀行公會審核，最後至財金平台審核，整體流程需耗時至少 6 個月。而若未來再新增業務合作項目，又需再次重新耗時 6 個月的時間來申請。業者提議若整體行政流程、或至少二次申請時，若相關流程可以簡化的話，將可能提升業者加入的意願。

(2)不同規模的 TSP 業者難以符合一致性的資安合規要求

考量 TSP 業者的規模與資源皆有所差異(如資本額、資訊能力)，若要求使用不同階段 API 的業者皆須達到相同等級的資安能力，則可能降低業者加入的意願。建議可以參考歐盟或英國規範，根據 TSP 業者的背景和規模做分類分級管理，並由主管機關做第一層 TSP 業者資格把關者。如此一來除了能使 TSP 的審核標準一致，銀行業者可以直接從合規的 TSP 中選擇合適的合作夥伴也能解決第 1 項的問題。

(3)其他人力及合規成本

以 TSP 業者來說，為達到資安合規，須持續進行 ISO27001 的驗證，同時也須取得專案查核的通過報告。另外合作的各銀行也皆須對其進行稽核。若未來合作業者家數上升，則 TSP 業者將可能需投注更多的資源與人力在接受稽核、改善發現等作業上。

承上，從銀行角度來說也是一樣。若合作的 TSP 家數增加，銀行也需花很多時間跟人力去查核 TSP 業者，以及合約的續約與檢視。另外內控稽核及金檢查核也會針對開放銀行業務進行資料徵提和查核，對於銀行業者來說也需另外提撥資源進行因應。

最後，目前銀行在參與開放銀行上尚未收費，但現行規範中將創新合作案的賠償責任放在銀行上，此項可能降低金融機構參與開放銀行的意願，也可能成為未來擴大合作的阻力。建議可以參考歐盟或英國，以要求 TSP 業者購買相關資安保險，以確保 TSP 業者有能力一起共同承擔創新合作的風險。

(五) 研發技術與資安能量調查

相關重點結論已彙整至前述研究案中，不再次贅述。

附錄三 研究計畫期中報告審查意見之意見回覆暨修正對照表

章節	審查委員	審查意見	修正說明
壹	查委員士朝	建議研究團隊先確認框架，再從框架下去論述各國不同種類的 API 應用場景/模式及面臨的威脅，針對不同的威脅進一步探討相對應的安全要求，並對應至法規層面的規範。	1. 謹遵委員意見辦理。針對各研究議題，已於各章節加上引言，另新增第壹章緒論，說明本研究之研究背景、目的、研究方法與範疇，以釐清本研究之研究框架和執行作法，並建立問題意識（頁 1-11）。 2. 謹遵委員意見辦理，已調整報告架構，就開放銀行之應用場景與消費者使用情境與威脅（頁 19-29）、API 安控參考建議(頁 82-90)、開放銀行之消費者保護規範（頁 148-164）等議題依序進行探討。
	張委員文熙	章節內容須再重新梳理，讓整體組織架構較為明確，問題亦應對應相關對策，並建議第陸章前增加資訊安全與消費者保護的章節介紹，較能呼應本研究案的主	謹遵委員意見辦理，已調整報告架構，就開放銀行之應用場景與消費者使用情境與威脅（頁 19-29）、API 安控參考建議(頁 82-90)、開放銀行之消費者保護規範（頁

章節	審查委員	審查意見	修正說明
		題。	148-164）等議題依序進行探討。
	童委員政彰	報告內容框架部分：建議應先有討論框架，需提出問題所在，俾利後續論述。另所引述資料宜說明資料來源。	1. 謹遵委員意見辦理，已調整報告架構，就開放銀行之應用場景與消費者使用情境與威脅（頁 19-29）、API 安控參考建議(頁 82-90)、開放銀行之消費者保護規範（頁 148-164）等議題依序進行探討。 2. 謹遵委員意見辦理，強化本研究之參考資料標示。
	張委員嘉魁	建議每章節前面可簡要摘述該章節之重點。對於國外開放銀行使用情境，可增加流程圖表，俾利了解實務運作。另建議訪談作業規劃可再納入財金公司。	1. 謹遵委員意見辦理。針對各研究議題，已於第壹至捌章開始前加上引言。 2. 因研究架構調整幅度較大，故期末報告初稿先針對第貳章消費者於交易應用場景使用情境說明補充內容，建立後續章節之分析基礎（頁 19-25） 3. 訪談財金公司規劃一案，受限於期末報告

章節	審查委員	審查意見	修正說明
			作業期程，期末報告初稿規劃先以文獻檢閱方式補強現行訪談樣本代表性之限制（頁 33-81）。
	吳委員雪瑩	建議在前面的章節增加各國開放銀行之量化資料及生態架構圖示，讓閱讀者快速掌握開放銀行的發展趨勢。	謹遵委員意見辦理，已於第貳章第一節就開放銀行之量化資料及市場生態圖示進行數據和文獻補充（頁 12-14）。
貳	張委員文熙	名詞定義、類型等論述，建議優先引用學術單位的文獻，倘需引用網頁資料，應加註瀏覽日期，以確保參考資料的可信度。	謹遵委員意見辦理，已於期末報告第貳章第二節補充開放銀行相關學術界定。(頁 15-16)。
	童委員政彰	情境描述部分：宜更接近市場現況，並說明受到何種威脅，俾利提出後續控管措施。	謹遵委員意見辦理，因考量情境風險分析架構的完整性，已於期末報告第貳章第五節運用 OWASP 十大 API 安控風險進行論述頁 25-29)。
	邱委員建宏	報告書前段論述許多國家已發展至近似於臺灣第三階段的範圍，惟較少論及實際應用的案例，建議參考國外具體案例進行情境分析(如 P.32 英	謹遵委員意見辦理，已於第柒章第五節綜合文獻回顧、案例分析以及訪談國內銀行與 TSP 業者之結果，呈現各方利害關係人參與開放銀行

章節	審查委員	審查意見	修正說明
		國租屋信用紀錄平台)，較能掌握消費者使用誘因。	生態系統之誘因機制建議（頁 172-175）。
	邱委員建宏	有關香港 Open API 在第三、四階段雖尚未開放(P.30)，惟具體推行內容為何應再加強說明；新加坡部分涉及以客戶資料進行銷售與行銷(P.31)，攸關消費者資料保護，建議再深入瞭解。	謹遵委員意見辦理，已於第陸章綜合文獻回顧和案例分析，提出促進開放銀行生態系統發展之消費者保護法規建議（頁 159-164）。
	吳委員雪瑩	報告書 P.4-5 所提開放銀行於金融產業之 4 項效益，建議宜加強論述，同時亦應一併論述潛在的威脅。	有關開放銀行相關風險威脅議題探討，本研究已於第貳章第五節針對 OWASP 十大 API 安控風險之內容進行說明（頁 25-29）。
	吳委員雪瑩	簡報 P.8 有提及美國、加拿大、日本等國家，但在報告書中未見相關論述，建議可以簡介該等國家現況，以臻周全。 報告書內相關表格倘引用國外網頁，建議標註清楚，另外，下列部分應再加強論述： P.29 僅以表格呈現各國	本研究已針對研究架構進行調整，跨國規範比較標的規劃以歐盟、英國、澳洲、新加坡、香港、臺灣，後續於期末報告簡報製作時會再注意資料內容一致性（頁 41-80）。 謹遵委員意見辦理，強化本研究之參考資料標示。

章節	審查委員	審查意見	修正說明
		開放 API 類型，建議應增加文字論述。 P.32 起所提各消費者使用情境案例之市場痛點，應再具體深入論述。 P.55 所述英國開放銀行標準框架下之消費者體驗及操作指引，建議進一步介紹該等措施之作法，以作為我國推動配套政策之參考。 P.81 有關 TSP 使用雲端運算的三種模式，建議補充說明其運作模式及差異性。	原期中報告 P.29 為各國 Open API 類型簡介，已於期末報告第參章補充文字說明（頁 37-40）。 本研究之目的和範圍聚焦於開放銀行之資安和消保爭議，背後之消費者保護議題探討，考量研究期程限制，暫未規劃於本次研究架構。 針對期中報告 P.81 有關 TSP 使用雲端運算的三種模式，建議補充說明其運作模式及差異性。已於期末報告第伍章針對 TSP 業者使用雲端運算的情境、風險與安控規範之比較和分析建議進行說明（頁 120-144）。
參	張委員嘉魁	有關 Partner API 之議題: 1. 應較具體說明 Partner API 與 Open API 之差異，並舉例說明國內 Partner API 之實際	針對 Partner API 議題，已於第貳章第三節（頁 16-18），以及第參章第二節進行分析說明（頁 33-36）。

章節	審查委員	審查意見	修正說明
		應用案例。 2. 依報告內容所述 Partner API 可能以委外方式控管，惟 P.48 及 P.67 對於委外適用情境似有不同，建議予以釐清。	
肆	查委員士朝	1. 有關報告書 P.98-106 代理登入議題，建議建立威脅模型，再探討相關議題，並建議應該採取相關具體加強措施。 2. 有關報告書 P.68-80 個資保護部分，應該要對應不同 API 種類，進而論述資安保護議題。另應參考歐盟「一般資料保護規範(GDPR)」，納入自動決策、意外事件處理、參與者的法律責任探討。	1. 針對本研究威脅模型議題探討，應研究架構之調整，將以第貳章第五節探討之安控風險為主延伸探討（頁 25-29）。 2. 謹遵委員意見辦理，已於期第肆章新增歐盟 GDPR 自動化決策等法律責任論述（頁 115）。

章節	審查委員	審查意見	修正說明
	張委員嘉魁	有關代理登入之議題控管部分(P.103-106)： 1. 報告內容多論述強制立法之國家亦無法全面性禁止，建議應再搜集更多經驗，包括客戶將帳號、密碼交付他人，是否完全由客戶自負責任等，俾提出解決機制。 2. 建議應訪談銀行對於代理登入之看法。 另其他相關修正建議如附件，請併同修正或補充說明。	針對代理登入議題，已於第肆章第八節補充建議措施（頁 115-117）。
			針對本研究提及第一、第二階段開放銀行參與銀行家數落差之原因，已於第柒章第二節補充說明（頁 167）。
	李委員志祥	有關代理登入風險部分(P.99)，因 TSP 業者是以消費者的代理人身份代為存取資料，涉及該業者是否取得存取權之問題，建議補充說明 TSP 業者是否取得消費者同意，以及消費者是否知悉代理登入之風險。	針對代理登入議題，已於第肆章第八節補充建議措施（頁 115-117）。

章節	審查委員	審查意見	修正說明
	張委員文熙	有關報告書 P.89 係探討雲端法規，惟內容亦提及網路安全框架，建議兩者應有所區別，分開論述。	謹遵委員意見辦理，已於第伍章將雲端安全獨立論述（頁 122-129）。
伍	查委員士朝	雲端安全部分，建議也要先建立架構，再討論各種不同雲端服務，並著重在如何監管，且議題應先著眼於 API 介接的後台控管，不全然聚焦在雲端。	已於第伍章第五節針對雲端安全監控建議措施進行說明（頁 138-144）。
	張委員嘉魁	有關 TSP 業者使用雲端服務控管建議研究之資安與個資議題(P.81-86)：依據財金資安標準規定，TSP 業者如使用雲端服務，應符合銀行公會「金融機構運用新興科技作業規範」有關雲端服務安全控管，建議可檢視前開規範後再建議應加強部分。	已於第伍章針對「金融機構運用新興科技作業規範」進行補充（頁 134-136）。
	童委員政彰	法規建議部分：目前國內相關規範已有銀行公會「中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範」(簡	謹遵委員意見辦理，已於期末報告第陸章新增法規短、中、長期政策建議（頁 160-164）。

章節	審查委員	審查意見	修正說明
		稱公會自律規範)、財金公司「金融機構與第三方服務提供者辦理開放應用程式介面（OPEN API）業務安全控管作業規範」(簡稱財金資安標準)，報告內容除檢視國外有那些要求外，宜在安全與便利中取得平衡，提出國內相關規範可再強化之相關建議。	
	張委員嘉魁	有關 Open API 消費者權益及隱私保護研究分析之保護強化建議(P.75-80)： 1. 因公會自律規範、財金資安標準相關內容已對消費者權益及隱私保護訂有相關要求，爰應先檢視前開相關規定後，再進一步提出精進建議。 2. 有關建議參考英國設立中介單位，居中調解銀行與 TSP 業者之爭議一節(P.80)，因我國開放銀行之政策推動方向，係採自律自願方式辦理，爰本研究	謹遵委員意見辦理，已於期末報告第陸章新增法規短、中、長期政策建議（頁 160-164）。

章節	審查委員	審查意見	修正說明
		案可再增列推動方式相近國家之案例及參考國情提出相關建議。	
	李委員志祥	有關建議參考英國設立中介單位(OBIE)，居中調解銀行與 TSP 業者之爭議一節(P.80)，建議補充介紹該中介單位；另因設立中介機構在我國有其困難性，且時效上可能緩不濟急，宜提出與我國國情較相近之案例或建議。	謹遵委員意見辦理，已於第陸章新增我國金融消費評議中心以及英國金融申訴服務等不同類型金融消費申訴機構運作機制之說明，作為提出建議措施之基礎（頁 153-159）。
柒	張委員文熙	有關報告書 P.83 提及 TSP 業者使用雲端服務誘因分為 5 項，惟下方內容僅有 3 項，情境描述亦不夠深入，成本效益也建議加強論述(如降低企業建置成本等)。	謹遵委員意見辦理，已於第柒章第四節新增開放銀行參與誘因之成本效益案例分析，作為結論與建議之參考（頁 169-172）。
	邱委員建宏	訪談對象建議增加實際有在辦理開放銀行業務之國外銀行。	經詢問外資銀行受訪意願，目前其暫無受訪意願，故此部分資料蒐集受到限制。
	吳委員雪瑩	訪談部分，考量我國開放銀行參與之銀行業者眾多，僅訪談 4 家樣本數偏低，樣本代表性不足，建議增加其他訪談對象。	考量期末報告資料蒐集期程和受訪者意願限制，故本研究以文獻和案例補充分析各方利害關係人參與開放銀行之誘因機制（頁 168-169）。

附錄四 研究計畫期末報告審查意見之意見回覆暨修正對照表

章節	審查委員	審查意見	修正說明
貳	查委員士朝	1. 建議不要將 OWASP Top 10 當作結論，其中第 3 項「過多資訊洩漏」、第 5 項「無效功能權限控管」、第 6 項「批量配置不當」、第 8 項「注入攻擊」似有誤解，宜再釐清： (1) 第 3 項「過多資訊洩漏」(API3:2019 Excessive Data Exposure)：非指傳輸安全，本控制項要探討的是有一些單位因 Open data 資料量太多的情況。 (2) 第 5 項「無效功能權限控管」(API5:2019 Broken Function Level Authorization)：意指不同 API 之間呼叫功能的衝突，導致使用者原本不該有這個 API，但其湊一湊功能就呼叫出來。 (3) 第 6 項「批量配置不當」(API6:2019 Mass Assignment)：查委員士朝: 意指今天若有大量資料上傳的情況，若沒有做檢查可能會遇到的問題，此一控制項情境會比較像今天我有一個 API 要去分析他安不安全。 (4) 第 8 項「注入攻擊」(API8:2019 Injection) ：係指針對 Command 輸入作一些攻擊。 2. 建議著重於 TSP 業者之安全要求、連線安全與客戶端程式要	謹遵委員意見辦理，已重新檢視將 OWASP Open API 十大風險內容，並針對委員所提第 3, 5, 6, 8 之內容正確性進行修正，查 OWASP 發布之風險項目原文較偏原則性論述，故在修正方式上較為限縮（頁 25-29）。

章節	審查委員	審查意見	修正說明
		求，按照報告書表格之欄位進行各國之比較(如第 87 頁)	
	張主任文熙	頁 16 的 API 列舉 McKinsey 定義過於簡單，建議補充其他資訊科學界定義。可於頁 2 初次提及 API 時加以定義。	謹遵委員意見辦理，已補充英國開放銀行執行組織以及我國學者王儷玲教授之界定，以為補充(頁 15)。
	吳委員雪瑩	1. 第 12 頁所提數位交易顧問公司對於開放銀行發展之分類，第一象限「專業開放」領域，共 11 間銀行，但由於第 13 之圖示清晰度不夠，建議敘明該等銀行之名稱。 2. 第 14 頁對於開放銀行的定義和範疇之論述，有引述他人文章，宜以插入注腳方式備註。 3. 第 15 頁所述開放銀行下的 API「開放銀行的本質是銀行數據的共享……，下一個階段之目標則為支付（Payment）領域」，與第 23 頁五、Open API 安控風險之內容重複，建議調整。 4. 第 23 頁（三）消費者使用情境，其中有關中小企業相關情境，是否可列舉實際案例？	謹遵委員意見辦理，已於頁 14 進行補充，並調整圖之清晰度(頁 14)，另也已調整本章文字敘述，於文中註明係綜合引用英國開放銀行執行組織以及我國學者王儷玲教授之見解，另有關中小企業相關情境，因我國尚無實際案例和需求，故仍以服務樣態方式呈現(頁 15、頁 24-25)。
參	張主任文熙	1. 頁 53 之表 15 透明性英文為 stability 應為誤植，請再檢視。 2. 頁 53 hosting security 應為主機	1. 謹遵委員意見辦理，已將透明性英文修正為

章節	審查委員	審查意見	修正說明
		代管安全性，非為主機安全，請再確認文義。 3. 頁 53 身分認證拼字錯誤應為 authentication。 4. 頁 53 Failover 譯為「故障轉移」，資訊業者多以「故障自動切換」翻譯，建議修正。 5. 頁 60 之圖 10 過於簡略，建議應融入訊息處理、憑證作業及認證機制之間的資訊流及互動關係分層表示(information flow 和 interaction among layers)。 6. 頁 64 - 65 API 治理制度描述至少要有盤點、申請、建置、上下架等實務作為，目前均未論述相關作法，建請補充。 7. 頁 74 有關資料標準一段，提及 open API specification (也稱 swagger) 不完全正確，open API specification 為規範；swagger 為實踐規範的工具，建議補強解釋。 8. 頁 76 我國安控現況，結語是我國規範考量更多風險，似不明確，建議增加對照表條例強弱之處。	Transparency（頁 55）。 2. 謹遵委員意見辦理，已將 hosting security 翻譯修正為主機代管安全性（頁 55）。 3. 謹遵委員意見辦理，已將身分認證英文修正為 Authentication（頁 55）。 4. 謹遵委員意見辦理，已將 Failover 翻譯修正為故障自動切換機制（頁 55）。 5. 已調整圖 10 內容， 融入訊息處理、憑證作業及認證機制之間的資訊流及互動關係分層狀態(頁 61)。 6. 已補充 OBWG 呼籲

章節	審查委員	審查意見	修正說明
			採用的治理模式應包含措施（頁 67-68）。
	吳稽核雪螢	1. 建議將新加坡 API 指導手冊提及之 7 大安全構面做個別說明。目前研究報告只有針對 2 構面做說明。 2. 有關 API 安全控管建議，查財金公司所訂「金融機構與第三方服務提供者辦理開放應用程式介面（OPEN API）業務安全控管作業規範」及 Open API 技術標準規格文件，已就存取控制、帳號權限控管及 API 開發及控管等有相關規範，倘經本次研究分析，仍需再精進，建議宜提出具體之作法，俾利本會未來督促財金公司調整之參考。 3. 有關簡報第 21 頁比較各國對開放銀行的政策類型之表格（查該表格應引自其他研究報告之資料），有提及美國、加拿大、日本等國家，但在報告書中未見相關論述，宜再釐清，另建議參採該表格方式將本次所研究之國家比較分析後納入報告書。 4. 有關銀行與 TSP 業者參與開放銀行之誘因，參考澳洲之規定資料交流必須為「雙向互惠」(第	1. 謹遵委員意見辦法，已補充新加坡 API 手冊其他構面議題，然仍有部分構面在該手冊原文並無進一步論述，亦於表 22 更新呈現（頁 76-77）。 2. 已將簡報 P.21 之表格補充進報告（頁 13） 3. 已針對本研究後欲引述之訴訟案例，補充美國監理架構(頁 64-65/ 頁 80-81)。 4. 已針對澳洲開放銀行採取雙項互惠之方式，補充說明(頁 169-170) 5. 已針對本研究第參章第六節

章節	審查委員	審查意見	修正說明
		160-161 頁)，建議補充該互惠資料之具體內容。 5. 第 78 頁有關對「開放銀行交易面應用服務之 API 安控議題探討」之建議措施，前言有重複，建議精簡。	建議措施部分進行調整，移除重複論述(頁 82-85)。
	張委員嘉魁	報告書提及 API 之開發與掌握、威脅防護之建議(第 80-87 頁)，經比較其他國家與財金公司所訂之相關規範，我國在 API 第 4 項風險「缺乏資源與速率限制」方面尚無相關規範(第 84 頁)，建議可針對此部分深入探討並提出相關建議。	謹遵委員意見辦理，已於本研究第參章第六節建議措施部分進行調整，並強化缺乏資源與速率限制之探討 (頁 82-85)。
	李委員志祥	有關報告書第 167 頁提及 Partner API 的創新合作業務，銀行與第三方業者僅需遵循雙方所簽定之契約內容，而無須遵循開放應用程式介面業務安全控管規範，其規範強度是否足夠，宜再補充相關因應措施。	謹遵委員意見辦理，已於本章進行相關補充，強化期末審查會議簡報的建議論述 (頁 176-177)。
肆	查委員士朝	1. 有關 TSP 業者代理登入部分，因代理登入涉個人資料安全及相關法令等疑義，本章切入角度建議調整。因代理登入的狀況起因於有些銀行不開放 Open API，才會有人想用代理登入的方式去繞；近期芬蘭國中小即有案例是有人用自己方式去爬蟲，做出更好的學習 App 讓他人使用，但也衍生不少爭議。 2. 委員認為代理登入整體而言就違反了安全的原則，建議可參	1. 實務上運用代理登入已行之有年，短期內要全面禁止有相當難度，是以本章著重於風險減輕角度探討，期望藉由風險控管降低相關爭議發生之機率，另本研究亦補充

章節	審查委員	審查意見	修正說明
		照國外做法，從個人資料保護層面切入，進一步探討相關議題。例如，從個人資料的擁有權的角度去促進銀行機構要求他們提供資料給 TSP 業者，或從個資法角度去探討解，我們期望業者怎麼樣去做。	近年美國新創公司代理登入訴訟爭議，其權益侵害類型即聚焦於個資保護範疇(頁 97-100)。 2. 已於本章第四節提出對 TSP 業者於技術面與管理面之安控建議(頁 115-117)。
	張組長嘉魁	1. 麻布記帳是否已經到第三階段交融交易和繳費? 若已達到，則可提供運作模式供銀行局參考。 2. 根因分析中提及代理登入無法全面禁止，其一原因為銀行合作門檻過高，建議補充說明如何讓 TSP 合法加入開放銀行之納管機制。 3. 頁 36 提到代理登入因應風險提到的「在有條件開放的前提下」，此處的有條件，意指哪些條件? 4. 有關 TSP 業者使用雲端服務之控管建議提及「建立 TSP 業者使用雲端服務之申請核准程序」(第 122 頁)，因該服務係基 TSP 業者與銀行之合作關係，	1. 麻布記帳現行提供服務以帳戶資訊整合為主，目前尚未達到交易模式(P.92)。 2. 有關 TSP 業者與金融服務業範疇適法性分析，整併於第捌章進行說明(頁 179)。

章節	審查委員	審查意見	修正說明
		宜再調整報告書內容及用語。 5. 想了解國外的代理登入運作，TSP 業者會不會跟金融業執行正常金融服務一般，第一時間通知消費者?	
	童委員政彰	1. API 跟銀行、監理機關或評議中心之間的法律關係要再釐清，對金融業來說，它有拿到特許執照，以銀行來講，它特許的範圍圍繞在存放款，在這範圍之外也不是銀行的專屬業務。所以在銀行局在核可其範圍內，若業者沒有碰到特許的範圍內，就不用受到高度監管。 2. TSP 業者本身僅代客戶執行這些交易，它本身沒有碰觸到這些業務。若這些法律關係都是很清楚確定的，它就沒有張組長剛剛提到的申請問題。 3. 既然 TSP 業者不是特許的金融服務業，它與消費者產生糾紛時，後續的爭議處理機制要循什麼樣的管道，因為目前研究結果傾向透過評議中心，這就會涉及法制的問題。最近評議中心才剛把一個業者納入小額匯兌，這個業者他也拿到小額匯兌的特許執照，評議中心就必須把他納進來管理。故在此法律框架下是否可以透過評議	有關 TSP 業者與金融服務業範疇適法性分析，整併於第捌章進行說明，按現行法規 TSP 業者難以適用金融服務業規範(頁 179)。

章節	審查委員	審查意見	修正說明
		中心的機制，就必須再釐清一下。 4. 例如研究團隊提到的英國 FOS 機制，他也是定義在 (Businesses that provide financial services)，例如 TSP 業者的定性就是提供金融服務的業者，而被英國的評議機構納入它的爭議處理機制，再請研究團隊就英國的法規稍微釐清一下。	
伍	查委員士朝	建議將重心重新填整，將重點置於「金融機構作業委託他人處理內部作業制度及程序辦法」與其他規範之差異，強化報告可讀性。	有關 TSP 業者與金融服務業範疇適法性分析，已整併於第捌章進行說明按現行法規 TSP 業者難以適用金融服務業規範(頁 179)。
	張主任文熙	1. 頁 109-110 有用雲服務、雲端、雲端服務、雲端架構，表示相同意義，建議統一用語。頁 111 後，也有用雲端運算服務或雲端計算等，請一併檢視所述範圍為服務本質或運算架構，來決定適當用語，以精準為原則。	謹遵委員意見辦理，已將第伍章相關用字進行調整，統一用字。
	邱科長建宏	1. 若提及委外申請程序，需明確說明規範主體為銀行業者或 TSP 業者 2. 建議具體說明合作銀行委外 TSP 業者之項目為何，以及確認是否符合國內現行委外規定	謹遵委員意見辦理，已修正報告用字，惟針對銀行委外予 TSP 業者之服務項目，可參考研究報告第貳章

章節	審查委員	審查意見	修正說明
			第四節消費者使用情境 (頁 19-24)。
	張組長嘉魁	1. 須注意「建立 TSP 業者使用雲端服務之申請核准程序」相關用字容易招致誤解，應明確表達金融機構才為申請核准程序之主體。 2. 頁 58 的個資糾紛處理提到英國對 TSP 業者的資安能力有一定要求，建議再行確認要求 TSP 業者投保資安險，是否為強制規定。 3. 有關金融消費評議中心做為爭議處理的相關探討，建議釐清國外做法，是由類似金融消費評議中心的角色來做，還是機制類似但由不同類型的機構執行？另外是否也是將其納入金融服務業範疇？這些議題都應該要先釐清。	1. 謹遵委員意見辦理，已修正報告用字。 2. 謹遵委員意見辦理，已進行補充，現行英國對 TSP 業者之保險規範，係要求其必須依法投保必要之商業險，惟近年在商業險的商品樣態，亦有加入資安險的狀況(頁 172)。 3. 謹遵委員意見辦理，於報告第陸章第六節，已說明關金融消費評議中心做為爭議處理機構之法規限制，並已針對 TSP 業者管理所涉跨部門議題進行釐清 (頁 163-

章節	審查委員	審查意見	修正說明
			164)。
	李委員志祥	報告書第 104 頁第 10 行「法規遵循的等議題」、報告書第 167 頁第 7 行「本研究研建議」，贅字部分請再修正。	謹遵委員意見辦理，已統一用詞。
陸	查委員士朝	消費糾紛及爭議處理部份，建議著重在消費者權益保護，例如發生交易爭議時，個人資料保護是消費者權益之一，應著重在個人擁有資料的存取權，要求銀行提供格式化資料，俾利爭議之釐清與後續處理。	因消費爭議處理之探討涉及各方參與者，程序則可分為非訟與訴訟處理機制，本研究於非訟處理機制已將英國 TSP 業者應擇定消費爭議機構之作法納入考量，惟消費爭議處理機構至消費者端之權利義務歸責和請求權，建議宜在契約和個資法規範架構下，對請求權基礎進行釐清。
	李委	有關報告書第 154 頁提及金管會可	刑法懲處對象為

章節	審查委員	審查意見	修正說明
	員志祥	考量開放銀行之發展情況，據以評估金融機構承擔 TSP 業者「對消費者的個資侵害賠償責任」，所稱承擔之責任係指為何，因違反個資法所需負擔之責任除民事責任外亦包含刑事責任。	行為人，無涉連帶責任議題，本研究所指連帶責任，係指民事責任，合先敘明。
	吳委員雪瑩	有關簡報第 63 頁以新加坡消費者協會(CASE)作為個人資料保護之案例，以及簡報第 81 頁強化現行司法小額/簡易訴訟之建議措施，於報告書內均無提及，請釐清是否要納入報告書。	因小額/簡易訴訟為我國現行訴訟制度一環，故於後續進行補充，已將我國訴訟制度補充於本章內容(頁 159-160)。
捌	張主任文熙	1. 頁 165 (二) 雲端安全一節過於簡略，提及「考量將下列金融機構···納入規範···要求··」，所稱下列金融機構不知道在哪裡，似有漏文，請再檢視。且結論為研究重點，應再加強論述。 2. 研究報告 頁 166~167 提及之短、中、長期建議，建議補充期程，更可具體說明如何處置。	謹遵委員意見辦理，已進行適當修正。並補充期程說明短、中、長期分別訂為一年、三年及五年(頁 159-164)。
	邱科長建宏	1. 開放銀行的資安監理建議所涉有二，為 TSP 業者應該由誰管理? 管理架構則為主管機關直接納管，或是將作業委外由銀行和合作業者做責任的分攤管理，由銀行來管理。其二能否由 TSP 業者訂定自律的標準來管理，由 TSP 業者遵循。	1. TSP 業者應由何單位管理，此一議題牽涉至資料開放涉及產業，按現行法規，TSP 業者不屬於金融服務業範

章節	審查委員	審查意見	修正說明
		(1) API 安全 對於 API 可用性與性能即時監視之建議，目前監理建議方向還是不清楚，要先確定要採取監理還是治理的方向，到底誰來監控 TSP 業者 (合作的銀行還是有另一個主管機關)? 在什麼樣的架構下進行監控。 (2) 交易詐欺的監控機制 是由 TSP 業者來通報，還是由合作的銀行來通報? 還是由消費者跟警察機關直接進行通報? 宜再釐清。 (3) 存取控管機制 取得客戶同意後，存取控管權是屬於 TSP 業者，是否由 TSP 業者做存取控管機制，宜再釐清。 (4) 雲端安全 研究內容多次強調將金融機構作業委外管理規範納入 TSP 業者，但該辦法目前管理標的是銀行。以目前金融服務業的委外辦法規定是，銀行可以委託他人處理的事項是涉及到營業執照的部分。所以在現行委外項目中可以委外的構想究竟為何? 銀行可以委託 TSP 業者的具體項目是什麼? 若要由銀行負較高的治理角色，好處是主管機關易於管理，壞處則為銀行會將負擔轉嫁給 TSP 業者。故若採將	疇，故建議採取跨部門治理之模式(頁 179)。 2. 我國現行開放銀行架構係採由銀行業者過契約把關 TSP 業者之安控，在既定政策架構下，宜由銀行承擔相關監督責任。 3. 按現行法規，TSP 業者不屬於金融服務業範疇，故建議採取跨部門治理之模式，已調整相關論述(頁 179)。 4. 美國 Fintech 業者 Plaid 一案，原告為消費者以集體訴訟方式進行，如表 28 所載(頁 97-98)。

章節	審查委員	審查意見	修正說明
		TSP 業者納入現行作業委外規範，是否符合現行規定，宜再釐清。若要採取另外針對 TSP 業者訂定委外辦法，可能牽涉到這個另訂的委外架構它的法令依據為何？另外也可能牽涉到複委託的問題。 (5) 個資爭議 個資洩漏的請求跟通報，究竟是哪一個主體要負責通報？合作銀行，TSP 業者還是由消費者來通報。 (6) 消費爭議 以目前評議中心的角色，它其實是處理消費爭議案件，個資洩漏是否屬於評議中心管轄範圍，尚有疑慮。 (7) 判決案例的請求 簡報第 30 頁提到的美國 Fintech 業者 Plaid 被控告未取得消費者同意取得其帳戶資料，該案例原告究竟為何人？尚需確認，因這會牽涉到治理模式的選擇，因目前開放銀行架構採取的是鼓勵的方式，由銀行跟 TSP 業者合作，故是否由主管機關納管，或由自律規範去管理，這牽涉到監理架構的選擇。所以要去確認外國的運作模式，到底採取的是哪一種監理架構，相關主管機關用什麼方式進行管理，可能要提供	

章節	審查委員	審查意見	修正說明
		給銀行局更多的資訊，作為政策參考。	
	吳稽核雪螢	1. 建議針對 P.164 API 安全，提出更具體之建議措施。	謹遵委員意見辦理，已於結論與建議章節，將 API 安控建議區分為 6 點進行分析 (頁 176-177)。

附錄五 研究團隊組成

本計畫研究團隊組成，涵蓋科技法律與風險諮詢領域，並按研究架構擬定開放銀行之資安和消費者保護等二分析架構進行各章撰寫分工，詳細成員名單如下圖所示：

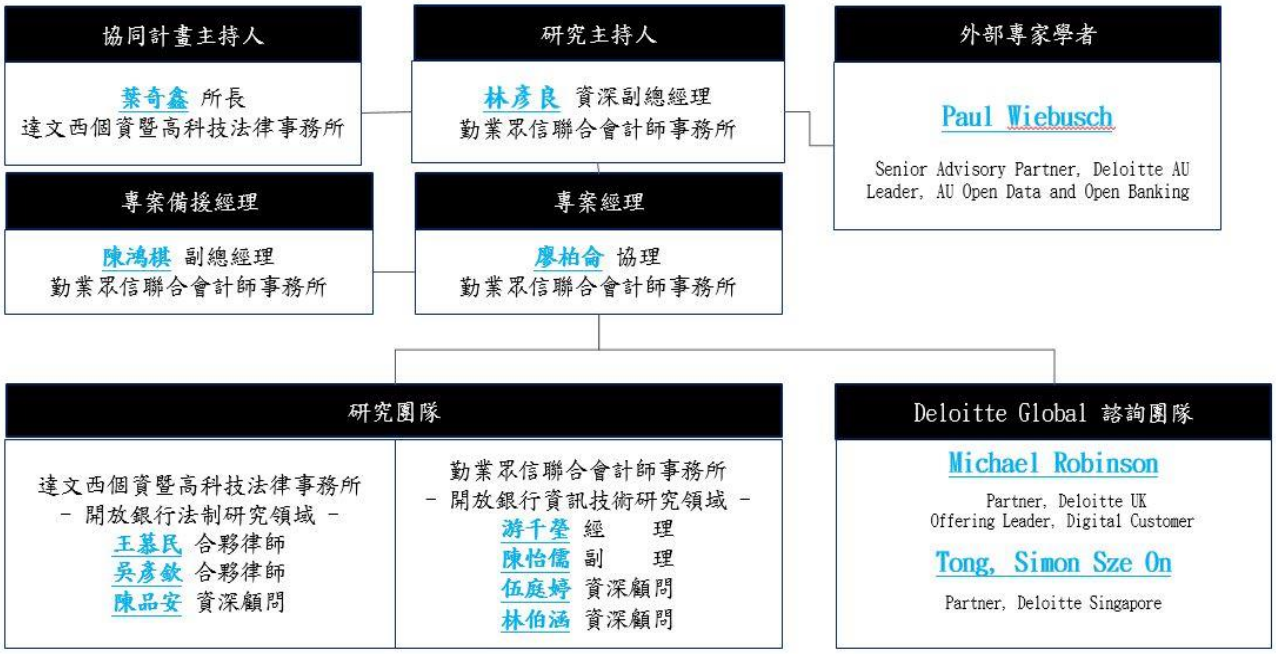

圖 26 研究團隊成員名單

資料來源：本研究