開放銀行的關鍵挑戰
第三方服務提供者之治理模式選擇

臧正運[1]/ 國立政治大學法學院助理教授

一、 前言

開放銀行（Open Banking）係金融科技時代的重要發展，有助於下列目標之實現：首先，活化消費者資料利用，藉由營造資料在不同業者間的安全與便捷流通環境，重新賦權予消費者，讓消費者在金融消費關係中居於主導地位；其次，資料流通權利由消費者主導，新進業者可在消費者同意下以較有效率的方式，取得利用消費者資料的機會，有助於降低新進業者與既有銀行業者的競爭門檻，期能提升市場競爭，達到鼓勵金融創新效應，進而增加消費者的選擇與福祉；最後，透過開放銀行的實踐，消費者資料不僅可在銀行端（或金融機構）與第三方服務提供者（如金融科技新創業者，即國際上所俗稱之「FinTech Firms」）間雙向流動，亦可促進資料在不同金融機構間相互流動，甚或是在金融機構與其他產業機構（如大型科技平台業者，即國際上俗稱之「BigTech Firms」[2]）間流動（如圖 1 所示），具有帶動整體經濟活力的潛質，也有助於國家調整現行產業結構，進而實現經濟轉型之願景[3]。

為實現上述目標，許多國家或地區，如歐盟、英國、新加坡、澳洲、日本、香港乃至於我國，均陸續以不同方式推行開放銀行。以我國為例，係採類似於香港的模式，鼓勵業者自主推動而不修法強制的方式，分成三個階段，依序就「商品資訊」、「客戶資訊」及「交易資訊」推展開放應用程式介面（Open Applications Programming Interface, Open API），促進銀行與第三方服務業者間的資料流動[4]，責由財金資訊股份有限公司（下簡稱「財金公司」）研擬 Open API 相關技術、資料與資安標準，並由銀行公會針對銀行與第

---

1 美國杜克大學法學博士，現為國立政治大學法學院助理教授、金融科技監理創新實驗室執行長。本文作者感謝科技部「監理科技之發展運用對金融監理法制的影響與因應」(計畫編號：MOST 108-2410-H004002) 之經費支持，及研究助理蕭佩瑋及朱瑞翔協助製圖與校閱，惟文責由作者自負。

2 關於 FinTech 及 BigTech 用語的分類及所指涉之對象，參照：FIN. STABILITY BD., FINTECH AND MARKET STRUCTURE IN FINANCIAL SERVICES: MARKET DEVELOPMENTS AND POTENTIAL FINANCIAL STABILITY IMPLICATIONS 1 (2019).

3 上述關於開放銀行可實現目標之論述，參照：臧正運，「從國際發展趨勢論我國推動開放銀行應有之思考」，金融聯合徵信雜誌，第 34 期，頁 12（2019）。

4 工商時報，開放銀行第一階段 月底上路，2019 年 7 月 22 日，亦可見：https://www.chinatimes.com/newspapers/20190722000209-260202?chdtv。

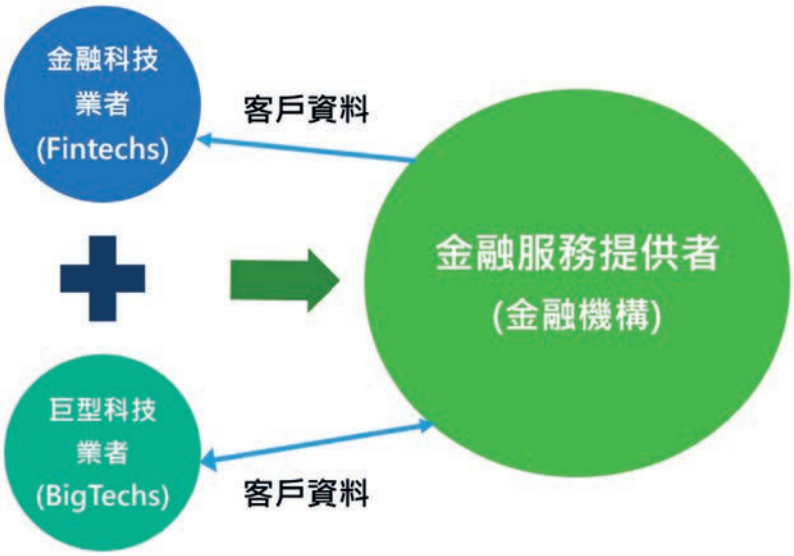

圖 1　Open Banking 環境下的消費者資料流動

三方服務提供者間合作時所涉及的權利義務關係，訂定自律規範與相關契約條款[5]。從金融監理之觀點而論，開放銀行最重要的監理目標，除確保開放過程中金融體系穩定運作、既有銀行機構健全業務經營不受負面影響外，另一重要目標則為確保資料流通過程中，消費者權益與資料隱私受到充分保障。

而實踐此兩大監理目標之關鍵，包括技術面（Technological Aspects）及治理面（Governance Aspects）的問題；在技術層面部分，主要為 Open API 相關資料與資安標準的決定、驗證與執行；而在治理層面，則為當銀行透過 Open API 將消費者資料與第三方服務提供者（Third-Party Services Providers or Third Party Providers，下簡稱「TSP 或第三方業者」）分享時，倘資料發生毀損滅失、外洩或第三方業者不當利用時，相關責任應如何歸屬、分擔與追究等議題。本文之重點即聚焦於治理面問題，從國際經驗與個人觀察，探索並嘗試第三方業者的治理模式類型化及分析其優劣，並對我國制度提出建議。由於第三方業者的治理模式將隨開放銀行所選擇之發展模式而不同，故本文第二部分將先依照國際實踐經驗，梳理開放銀行三大發展模式，第三部分再針對第三方業者治理模式加以分析，最後在第四部分提出淺見建議。

二、開放銀行的發展模式

世界各地實現開放銀行的背景與目標不盡相同，發展模式各有差異。根據本文作者研究，目前國際上開放銀行之發展模式可大致分為三類[6](如圖 2)：

5　經濟日報，推動開放銀行 業者擬結盟新創，2019 年 7 月 19 日，亦可見：https://money.udn.com/money/story/5613/3940467。

6　作者所提此一分類及相關論述曾撰於財金公司與政大金融科技研究中心的「開放銀行 (Open Banking) 研究合作專案計畫」之「台灣開放銀行政策研究報告」中。

(一) 以香港、新加坡及日本為代表之「開放API框架模式」（Open API Framework Model）。

(二) 以英國為代表之「API管理中心模式」（Open Banking API Platform Model）。

(三) 以澳洲為代表之「標準制定機構模式」（Data Standards Body Model）。

首先，「開放 API 框架模式」係由政府鼓勵開放銀行程式介面的發展，但未以法規強制，而是採取諸如「鼓勵業者自主開放」、「頒布時間表」、「篩選出候選應用程式介面」、「建置 Open API 網站或程式介面註冊庫」以及「提出 TSP 治理流程建議」，甚至是由政府或公協會共同頒布「Open API 的發展標準指引或建議」等作法[7]，營造發展開放銀行的產業環境。

至於「API 管理中心模式」則係指在政府的支持或要求下，新設或委由具公信力之機構，負責協調、制定 API 標準與資料交換格式，並設計一套治理架構，釐清及管理所有利害關係方的權利義務關係、頒布 API 上架相關流程與規範、確保資訊安全的管理機制、並處理各方間可能的爭議。如英國即是在其競爭及市場管理局（Competition and Markets Authority，CMA）的要求下由九大商業銀行等機構出資成立開放銀行實施組織 (Open Banking Implementation Entity，OBIE），其主要任務包括建置 API 標準及相關資訊的規定與格式、管理及維護規定、更改及發布規定、支援用戶使用結構及流程、處理開放銀行中應適用的條款及條件、負責開放銀行系統指導原則，以及根據相關法律與監理規範進行系統維護，並建立安全機制與管理架構。

最後，「標準制定機構模式」乃透過制定一套開放銀行的 API 標準供參與成員遵守與落實，各參與成員施行開放銀行業務服務時須依循該標準，但政府原則上暫不另行成立專門平台或管理中心供參與成員上架 API。如澳洲的

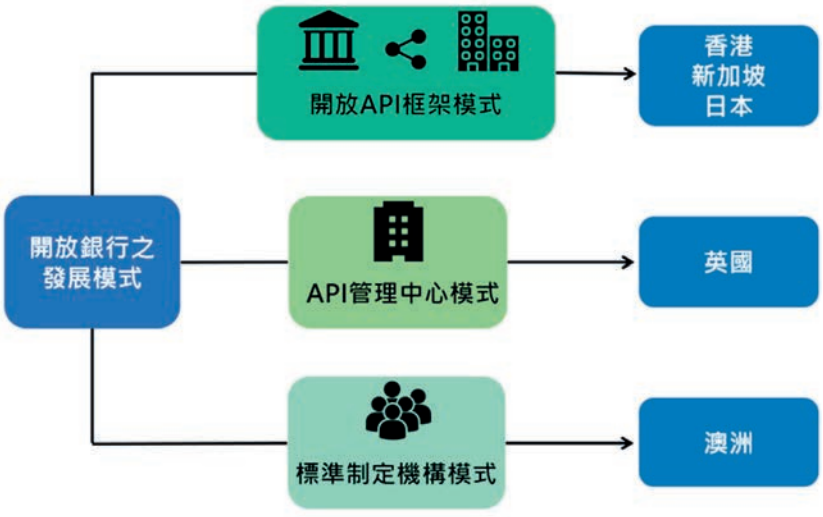

圖 2　Open Banking 發展模式類型

7　如香港即由香港金融管理局頒布「Open API Framework for the Hong Kong Banking Sector」，而日本即由其全國銀行協會（Japanese Bankers Association）發表「Report of Review Committee on Open API: Promoting Open Innovation」。

作法，即是在實現消費者資料權（Consumer Date Right）的修法框架下，成立 Data Standard Body 制定相關技術標準，並在其下設置一位獨立主席（Independent Chair），負責籌組諮詢委員會 Data Standards Advisory Committee [8]，成員包含技術專家與產業界人士，針對相關標準與法規修訂提出建議。目前 Data Standards Body 暫設於聯邦科學與工業研究組織（Commonwealth Scientific and Industrial Research Organisation，CSIRO）下之研究機構 Data61 [9]，負責 Open API 技術標準的擬定。

三、第三方服務提供者的治理模式分析

不同發展模式之選擇，對於銀行與第三方業者間治理模式的取捨有不同影響。依照本文作者研究，TSP 治理模式（或稱為「TSP Governance Model」）至少有四種類型：訴諸作業委外監理規範、委由 API 管理中心把關、制定產業自律標準以及由主管機關直接納管。採取「開放 API 框架模式」的國家，通常未設置 API 管理中心，基本上應無法委由 API 管理中心把關，且因相對欠缺法規面之要求與配套，較難由主管機關直接納管第三方業者。反觀採取「API 管理中心模式」的國家，較可由管理中心規範第三方業者應具備之技術與資安條件，抑或搭配產業所制定之自律標準，以明確界定銀行與第三方業者之關係。至於採取「標準制定機構模式」的國家，並沒有完全排除未來委由特定 API 管理中心把關的選項，因此四個治理模式的類型都有可能適用 (如表 1)。

表 1　各類 Open Banking 發展模式下 TSP Governance Model 的可能選擇

	開放 API 框架模式	API 管理中心模式	標準制定機構模式
訴諸作業委外監理規範	✓		✓
委由 API 管理中心把關		✓	✓
制定並適用產業自律標準	✓	✓	✓
由主管機關直接納管			✓

以下將四種 TSP 治理模式的內涵與優劣進行扼要分析：

(一) 訴諸作業委外監理規範：從金融監理角度觀之，銀行與第三方業者間透過 Open API 介接並實現資料分享，本質上係銀行委託或使用第三人辦理銀行自身之作業（例如該銀行的商品資料或客戶帳戶及交易資料之處理）[10]。此關係在國際金融監理實務上稱之為「作業委外」，須適用相關作業委外監理規範

8　標準制定委員會（Advisory committee）：https://consumerdatastandards.org.au/about/advisory-committee/（最後瀏覽日：2019 年 8 月 26 日）。

9　Data61：https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards（最後瀏覽日：2019 年 8 月 26 日）。

10　參照：蕭長瑞，銀行法令實務第一冊，華泰文化，頁 107（2012）。關於國際上金融機構作業委外規範的重點分析，參照：Cheng-Yun Tsang, From Industry Sandbox to Supervisory Control Box: Rethinking the Role of Regulators in the Era of FinTech, J. OF L., TECH. AND POL. (Forthcoming 2019), available at SSRN: https://ssrn.com/abstract=3420539。

（Outsourcing Regulation）[11]，其核心精神在於要求身為委託者之銀行業者在整個作業委外流程中，從委外前的盡職查核、委外合約議定至委外後持續監控等，均須承擔主要且最終的法律與遵循責任。

換言之，採此一治理模式時，主管機關基本上視銀行為作業委外關係的控制點，以確保第三方業者之運作不會對消費者及金融體系產生負面影響，其優點為主管機關便於監理，然由於銀行端需承擔主要的法令遵循風險，往往會嚴格篩選、甚而將相關成本轉嫁予第三方業者，進而提高第三方業者與銀行業合作的門檻。須強調者，不論採取何種模式，基本上銀行透過Open API將相關資料與第三方業者分享，均可能適用作業委外監理規範，因此本類型所指涉者，係主管機關不採取其他模式做法，單純訴諸委外規範，以處理銀行與第三方業者間的互動及風險監理之情形。

(二) 委由API管理中心把關：即在政府要求或鼓勵下，設立API管理中心，並由該中心辦理第三方服務提供者之註冊、測試或驗證作業。申言之，API管理中心除了建置及維運Open API相關服務平台外，亦提供銀行與第三方業者系統介接、資訊傳送、規格驗證、API上架管理及線上測試等功能。在此基礎下，要求第三方業者於使用銀行提供之Open API前，須先通過API管理中心之測試與驗證後，才能正式上線相關服務。此外，第三方業者與銀行需要配合API管理中心提出Open API之規格、技術及資安標準，隨時配合上述標準修正，並調整自身內部相關資安與隱私保護政策。

此一治理模式之有效運作端仰賴幾個重要前提：首先，須設立API管理中心；其次，該管理中心須針對自身、銀行及第三方業者間的三方關係，設計明確治理政策與權利義務關係，方能透過契約、作業規範與業者聲明等具體方式，確保三方遵循。此模式之主要優點為可大幅降低個別業者相互間磋商、測試及驗證成本，有利於推廣與落實整體生態圈之共通資安及隱私保護標準，進而對消費者形成較完整的保障。然此模式之缺點為管理中心同時取得制定標準、驗證標準及執行標準之地位，若過程中未能有效將所有利害關係人之意見、需求及資源限制納入考量，可能在推展開放銀行制度時，產生對特定群體不利之狀況。舉例而言，管理中心為了嚴格控管資安以及自身潛在的法律責任，可能要求第三方業者須達到相當於銀行業的資安控管標準，反而可能使資源不足的新創業者，被排拒於開放銀行生態圈之外，而與原本開放的精神相左。

---

11 然而實務上亦有 Open API 未必適用傳統作業委外監理規範的見解。如有論者認為銀行透過 Open API 將資訊提供予第三方係基於客戶的要求或同意，實質上係銀行系統功能的一部分，而有別於傳統的外包關係。參照：REVIEW COMMITTEE ON OPEN API OF JAPANESE BANKERS ASSOCIATION (JBA), REPORT OF REVIEW COMMITTEE ON OPEN API: PROMOTING OPEN INNOVATION29 (2017) (Observing that “[P]rovision of information from banks to third parties is based on requests/consent from users, and part of a bank’s system, which requires a high level of robustness, is not outsourced to a contractor; it may therefore not be possible to rigidly apply the framework for managing external contractors to Open API.”)

(三) 制定並適用產業自律標準：姑且不論發展模式之選擇，基本上各國均可採取此一治理模式規範銀行與第三方業者之關係，即由銀行與非銀行的第三方業者共商治理標準，將各方對於治理標準的共識形諸於書面文件，如自律規範或是指引，甚至進一步以定型化契約條款責由業者遵循，或訂定示範條款，供業者選擇並於微調後遵循。舉例而言，我國目前由銀行公會制定「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」即為此模式之適例。又如日本全國銀行協會召集利害關係人組成審議委員會（Review committee），針對銀行與第三方業者共同推動開放銀行的方式，分別就發展原則（Development Principles）、發展標準（Development Standards）及電子資訊的詳細標準（Electronic Message Specification Standards）三大方面提出指引（Guidelines）[12]，亦為此模式的呈現。採取此模式的國家通常未特別透過法規要求銀行業須將其資料以Open API開放予第三方業者使用，因此通常需要產業界自發自律，方能實現開放銀行之願景。此一模式的主要優點在於將產業自律標準訂為銀行與第三方業者間權利義務規範之最低標準，並給予業者相互間調整，以差異化市場實踐的彈性空間。然通常這類自律標準均以現行監理規範為設想基準，故實際上產業自主空間未必如想像具有彈性。而此模式的主要缺點為倘若沒有具代表性的公協會參與及支持，自律規範恐流於形式，亦難以帶動整體產業推行開放銀行的共識與動能。此外，由於第三方業者通常不若銀行業有公協會組織代表發聲，其意見很容易在自律標準形成的過程中被忽略，使得最終產業標準成為事實上（De Facto）的銀行業標準。

(四) 由主管機關直接納管：此一模式係指主管機關鑑於在開放銀行環境下，第三方業者將大量且頻繁地與銀行業者分享消費者資料，消費者將處於潛在之個資隱私風險、資訊安全風險、服務中斷風險乃至於未授權交易風險，因此為妥善保護消費者，並確保金融體系穩定運作，主管機關有必要將第三方業者視為準金融機構，並依照金融監理法規監管。須注意者，在實務運作上，銀行與第三方業者間的作業委外契約，通常會載明銀行主管機關有權定期或不定期請求第三方業者提供契約範圍內之相關資料，並在必要時，得自行或委託專業人士對第三方業者直接進行實地查核。然而此「查核權的契約化」與本文所稱之「由主管機關直接納管」不同。前者主管機關的權力，係建立於銀行業者與第三方業者的契約約定；而後者主管機關的權力，則通常源自於法規之授權。

此一治理模式之優點有助於落實消費者與金融安全防護，而將銀行業與第三方業者置於對等的受監理地位，亦提供銀行業者安心與第三方業者合作之誘因。惟主要缺點有二：首先，金融主管機關未必具備足夠的監理資源與能力以控管

12 Id.at 9-18.

非屬金融業之第三方業者，若欲採取此模式，尚須適切法律與資源配套，否則恐造成監理效能不彰。再者，第三方業者倘若直接受金融監理機關監管，勢必增加其法律遵循成本，不利新創業者或是小型企業之營運，反而導致第三方業者卻步，阻礙形成多元參與的開放銀行生態體系。

須特別強調者，上述四種治理模式相互之間並非互斥的類型化概念，本文之分類旨在提供設計 TSP Governance Model 時的參考基準 (如圖 3)，實務運作上可能會有同時採行兩種以上模式之情形，而在制度設計時，亦可選擇混合模式，關鍵仍取決於一國發展模式的擇定以及對於開放銀行之生態願景。

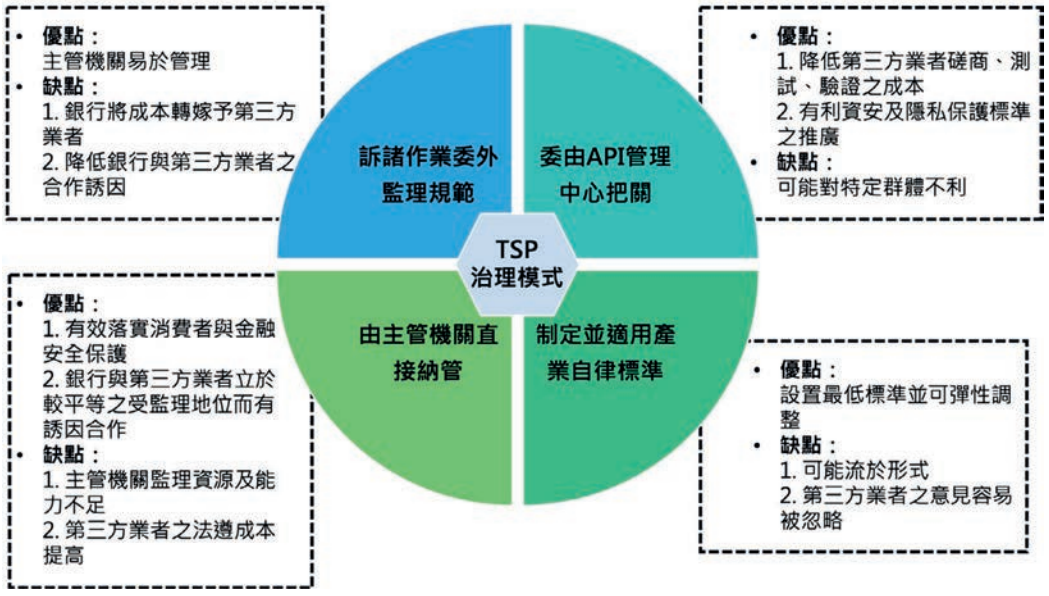

圖 3　TSP Governance Model 之類型

四、結語：我國的模式選擇與落實

根據媒體報導以及作者瞭解，我國將開放銀行政策視為重要的金融科技監理變革與發展目標，在發展模式上，係以「開放 API 框架模式」為主軸，採階段式，由銀行公會協調各方利害關係人，促進業者之自發自律，並在此軸線下兼採「API 管理中心模式」，由財金公司擔負「開放 API 管理平台」之重責大任，協助制定相關標準，以及第三方業者與銀行業介接。在上述發展模式下，可以預見我國在 TSP Governance 治理模式之選擇，可能偏向採「制定並適用產業自律標準」以及「委由 API 管理中心把關」的混合模式，屆時將由銀行公會主導自律規範的形成與落實，而由財金公司主導銀行、第三方業者及其自身間之三方權利義務關係的設計 (如圖 4)。此模式選擇基調尚稱合理，然而根據本文前開分析，在實踐上應盡可能追求下列兩大目標：(1) 須確保第三方業者在產業自律標準之形成過程中，有充分參與場域，並有具代表性的機構或組織助其發聲與表達意見，以確保最後制定出之自律規範、定型化契約書及相關作業標準為第三方業者所能負擔與遵循；(2) 針對第三方業者之技

術規格與資訊能力要求，應兼顧維護資訊安全與促進生態發展，讓第三方業者有便捷及易用（accessible）的測試環境，以及可滿足各類遵循標準之多元方案。

針對上述兩大目標，本文建議我國可思考下列方案：(1) 成立「開放 API 研究暨應用發展委員會」或其他相關組織，邀集銀行業者、現有及未來有意加入開放銀行生態圈的第三方業者，共商產業自律規範、銀行及第三方業者間的合作契約條款、第三方業者的資安作業流程規範等，確保生態圈多元參與並形塑強而有力的發展共識。(2) 財金公司得仿效英國 OBIE，針對第三方業者與銀行間的 Open API 介接及使用，提供沙盒測試環境，並思考導入公正第三方辦理第三方業者是否滿足相關資安條件或隱私保護政策的驗證（Certifying）作業，如英國 IASME Consortium 即針對中小企業是否滿足英國政府的 Cyber Essentials Scheme 進行評估與驗證 [13]。此作法除能降低規模較小之第三方業者的資安遵循成本外，也有助於鼓勵我國資安驗證與稽核產業之發展。此外，針對不同規模大小的第三方業者，亦可採取分級管理制度。就大型第三方業者，可責令其遵循與銀行相近之規格要求，如 ISO 27001，而小型第三方業者，則可考慮其他多元標準與方案。[14] 從資安風險控管角度而論，分級管理也可依照第三方業者實際使用 Open API 的類型及權限執行，如涉及客戶交易資訊分享的 API 使用或具有 write-access 的權限時，須符合最高規格之資安標準，若僅是商品資訊分享，則可給予適度之調整彈性。

第三方服務提供者的治理模式選擇及設計，乃推動開放銀行能否成功之關鍵挑戰，也是多元永續生態圈可否形成的重中之重。我國開放銀行發展正值金融科技監理變革之轉捩點，能否讓現行規劃開花結果，取決於我們是否以營造生態圈的觀點，而非既定產業本位思維，在關鍵決定上作出正確的選擇，期待上述淺見，能對我國開放銀行的發展路徑設計有所啓發。（本論述不代表本刊或財金資訊公司立場）

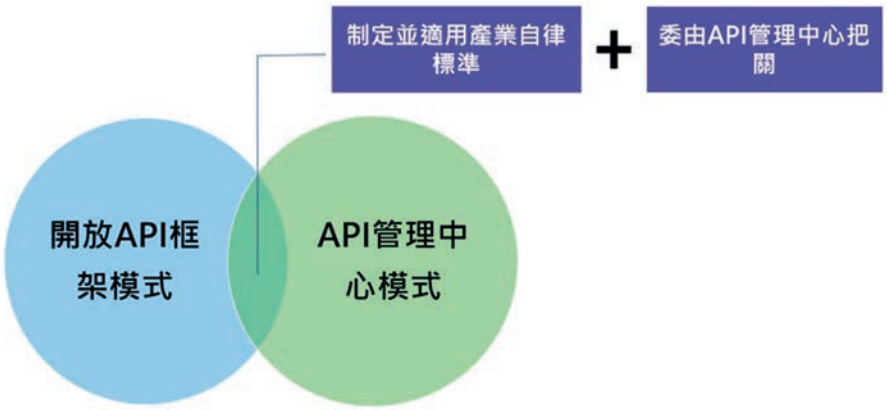

圖 4　我國所採之開放銀行發展模式及 TSP 治理模式

13　IASME, https://www.iasme.co.uk/cyberessentials/（最後瀏覽日：2019 年 8 月 26 日）。

14　如英國即採此方式。參見 OPEN BANKING LTD., OPEN BANKING - GUIDELINES FOR OPEN DATA PARTICIPANTS 9 (July 2018), available at https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Open-Data-Participants.pdf .