論電磁紀錄提供命令
—以 2025 年（令和 7 年）修法為中心*

文／緑大輔　譯／顏榕

上

壹 問題之所在

本文擬就偵查中數位證據之蒐集方式，先就日本的狀況進行說明，其後進一步檢討其課題所在。

2026 年 5 月 21 日，日本刑事訴訟法中關於電磁紀錄提供命令之修正正式施行。我認為電磁紀錄提供命令可能改變日本之偵查實務。本文以下第一，首先確認，日本偵查實務迄今在蒐集數位證據方面，面臨何種問題。第二，概要說明今年施行之電磁紀錄提供命令究屬何種制度、其有何種理論上之課題問題，以及立法者如何回應此等課題。同時，確認電磁紀錄提供命令對於過往之課題得以提供何種解決。第三，刑事訴訟法亦就令狀電子化進行修正。本文就此項修正之討論提出我個人的分析，並在此基礎上確認數位證據蒐集所涉及之課題，進而提出若干觀察。

貳 蒐集數位資料之現況與問題

一、令狀主義之規律——作為前提之制度

日本憲法第 35 條規定，除非有司法官簽發之令狀，人民不受搜索、扣押或侵入之權利不得受侵害。此即所謂令狀主義。偵查機關欲實施搜索、扣押等強制處分時，原則上必須向法官聲請簽發令狀。受理令狀聲請之法官，應審查實施該處分之必要性——以扣押為例，應審查該犯罪之態樣與輕重、應扣押物之證據價值及重要性、應扣押物有無遭隱匿或毀損之虞、扣押對受扣押人所造成之不利益程度，以及其他一切情事[1]。審查之結果，如認有實施該處分之必要，法官即向偵查機關簽發令狀，偵查機關始得執行該處分。

此種令狀主義係繼受美國憲法增修條文第 4 條而加以採用。因此，日本對於令狀主義之理解，基本上與美國一般見解相同，說明如下：第一，透過法官審查實施個別處分之必要性，防止實施欠缺必要性而屬濫用權限之處分。第二，由於令狀中會特定並明示記載成為處分對象之物，因此偵查機關僅得於令狀所記載之範圍內行使權限。藉此防止對權利利益造成過度侵害[2]。

為實現上述意旨，憲法第 35 條規定，僅於存在「正當理由」時，始得簽發「明示應搜索之場所及應扣押之物之令狀」並據以限制權利、利益。然而，日本國憲法係於 1947 年施行。當時，隱私之觀念在日本尚未確立，此處所設想之權利利益，主要係財產上之管理權或占有利益。

二、數位證據蒐集所涉及之爭點

如前所述，日本國憲法原係以財產上之管理權及占有利益作為保護對象，刑事訴訟法也因此導入以財產權為核心之法體系。此一制度設計，在將數位資料作為證據加以蒐集時，遂產生若干限制。

（一）放寬與犯罪嫌疑事實之關聯性要求——取得過剩之資訊

第一，數位資料雖屬無體物，但為取得數位資料，實務上係以取得內含該數位資料之有體物占有的「扣押」方式進行。所謂扣押，係指強制移轉有體物之占有之處分。並非以數位資料之個別檔案為單位，判斷是否有取得之必要，而是以有體物為單位，判斷是否有取得之必要。隨著資訊科技革新，電腦、智慧型手機等各種有體物所儲存之資料容量，已大幅增加。然而，只要有體物之分割可能性存在其界限，在以有體物為單位實施扣押之制度下，各該有體物內所包含之資料，便會全部成為偵查機關取得之對象。換言之，僅扣押一部電腦，即可能一併取得數百 GB 之全部資料。

其結果即是憲法所要求之「正當理由」之判斷標準遂趨於寬鬆。日本學說認為，扣押得以正當化之前提，在於扣押客體須與犯罪嫌疑事實具有關聯性，而此即為日本憲法第 35 條所稱「正當理由」之具體內涵。是以，扣押與犯罪嫌疑事實無關之物，即屬欠缺必要性之扣押，自不應被允許。依循此一邏輯，與犯罪嫌疑事實無關之數位資料，原則上亦不得加以取得。惟實際上，以 GB、TB 為單位之資料皆可能儲存於單一有體物內，一旦扣押該有體物，其中即可能包含大量與犯罪嫌疑事實毫無關聯之數位資料。對此，有日本實務見解認為，在具備一定條件下，得放寬犯罪嫌疑事實之關聯性要求，而允許一併扣押與犯罪嫌疑事實無關之數位資料[3]。亦即，第一，足認該記錄媒體內存有與犯罪嫌疑事實相關資訊之蓋然性；第二，於扣押現場確認電磁紀錄內容具有困難，或於確認過程中有造成資訊毀損等風險時，即得無須逐一確認各項數位資料是否與犯罪嫌疑事實具有關聯，而直接扣押該記錄媒體，或複製其所儲存之全部資料。

上述現象之所以產生，乃係因憲法及刑事訴訟法係以有體物為單位掌握資訊取得之客體，並採取對於包含於特定有體物內之資訊，不再逐一分割，而一併取得之思維。此種思維可謂係由取得有體物占有之概念所延伸而來。此一以占有為基礎所建構之法體系，遂朝向容許取得與犯罪嫌疑事實無關之過度資訊之方向發展。日本判例在此所採取的理論基礎應是：「對於個別電磁紀錄（或記錄媒體），在某些情形下，不逐一確認其內容即逕予扣押或複製，實難謂一概不應允許；因此，被扣押人因此所受之不利益，應於審查扣押（或複製處分）是否具有相當性（必要性）時，一併納入考量。」此一理解[4]，其後亦為有關數位資料複製之判例所承襲[5]。

犯罪嫌疑事實之關聯性究應嚴格要求至何種程度，曾於利用 GPS 進行行蹤監控之案件中成為問題。日本實務就偵查機關秘密在汽車上裝設 GPS 裝置，以取得目標車輛位置資訊之偵查手法，認為原則上須有立法授權始得為之[6]。其理由在於，GPS 行蹤監控將廣泛蒐集與犯罪嫌疑事實無關之位置資訊。又就如何避免過度蒐集廣泛之位置資訊而言，縱使由法官於令狀中附加適當條件，亦難以有效達成，因此仍有透過立法加以規範之必要。就位置資訊而言，由此亦可看出，日本實務已逐漸開始意識到過度廣泛蒐集資訊所可能引發之問題。

（二）數位資料儲存地點之全球化

第二項問題，是如何取得位於國外之數位資料，此一問題亦逐漸浮現。Google Drive、Gmail 等即為典型例子；實務上，為證明犯罪事實而有取得此類雲端資料之必要，並非少見。然而，儲存於雲端之資料，並不必然存放在日本國內之伺服器，而可能儲存於美國及其他各國之伺服器。當然，日本之主權並不及於位在日本國外之伺服器。況且，雲端資料究竟儲存於哪一國之伺服器，本身即難以掌握。

在日本，偵查機關得存取儲存於雲端之檔案等資料，並將該資料複製至作為扣押標的之電腦等終端設備，或其他記錄媒體後，再扣押複製資料所在之終端設備或記錄媒體。此即所謂「遠端存取」。遠端存取之對象，係指透過網際網路與作為扣押標的之電子計算機相連之伺服器等記錄媒體，且依具體情形，足認其係用以儲存下列檔案等資料者：第一，由該電子計

（文轉三版）

註釋

* 本文為司法院與國立臺北大學於 115 年 8 月 4 日（星期二）下午 2 時 30 分，假司法院三樓大禮堂共同舉辦專題演講「論電磁紀錄提供命令—以 2025 年（令和 7 年）修法為中心」之內容。

1 最決昭和 44 年 3 月 18 日刑集 23 卷 3 号 153 頁。

2 井上正仁『強制捜査と任意捜査〔新版〕』（有斐閣、2014 年）58 頁以下等。

3 放寬扣押資料記錄媒體與被疑事實關聯性要求之判例，可參：最決平成 10 年 5 月 1 日刑集 52 卷 4 号 275 頁。容許自伺服器複製四 TB 資料之判例，可參：最決令和 3 年 2 月 1 日刑集 75 卷 2 号 123 頁。

4 吉戒純一「判解」最高裁判所判例解説刑事篇令和 3 年度 29 頁以下、68 頁。

5 嚴格而言，與扣押不同，於複製之情形，並非以有體物為單位取得資料，而得選取必要之資料加以複製，因此，原本亦可能採取不允許全面性複製之作法。應可認為，判例係考量龐大資料難以於令狀執行現場，在短時間內完成確認及篩選，而容許全面性複製。

6 最大判平成 29 年 3 月 15 日刑集 71 卷 3 号 279 頁。

7 最決令和 3 年 2 月 1 日刑集 75 卷 2 号 123 頁。

8 成瀬剛「判批」ジュリスト 1577 号（2022 年）163 頁。此外，關於跨境遠端存取，亦有見解認為「雖然可能出現各種不同的案例，惟迄今相關實務經驗尚未充分累積，國際法之規範內容亦未臻明確；加以尚有極為廣泛且複雜之問題有待考量，國內外學說與實務見解亦意見分歧。鑑於上述情形，可推知最高法院認為，於現階段宜避免建立具有全面性、一般性之判斷基準」吉戒・前揭注 (4)62 頁。

9 川出敏裕「コンピュータ・ネットワークと越境捜査」酒巻匡ほか編『井上正仁先生古稀祝賀論文集』（有斐閣、2019 年）409 頁以下、428 頁。此一見解並主張「縱使於處分執行後，始發現相關資料係儲存於位於外國之伺服器，亦不致使該處分溯及地成為違法。」

10 笹倉宏紀「クラウド捜査」芝原邦爾ほか編著『経済刑

法源法
www.lawba
檢索全部法規、司法判解、行政函釋、裁判書、起訴書、論著
服務
TEL:02-2
JUDICIAL
司法
訂閱辦法
本刊每
全年
費用新臺
如蒙
請郵政
帳
5005
帳
司法院
電
02-236

法律網
ank.com.tw
一欄式檢索、各類資料進
階檢索
源資訊
專線
509-3536
L WEEKLY
周刊
周出刊
訂閱
幣400元
訂 閱
劃撥
號
4377
戶
司法周刊
話
618798

（文接二版）

算機所製作或變更之檔案等資料；第二，依其設定，得由該電子計算機變更或刪除之檔案等資料（刑事訴訟法第 218 條第 2 項、第 99 條第 2 項）。

此一制度於伺服器位於日本國內時，並無疑義。然而，若伺服器設置於國外，由於日本之主權並不及於該伺服器所在地，作為強制處分所實施之遠端存取，其效力是否及於境外，即成為問題。日本最高法院對此指出：「當儲存電磁紀錄之記錄媒體位於《網路犯罪公約》締約國境內，且對該電磁紀錄具有合法開示權限之人已合法且自願同意開示時，縱未透過國際刑事司法互助程序，仍得對該記錄媒體進行遠端存取，並複製其中之電磁紀錄。」[7]依此判決見解，對於《網路犯罪公約》締約國境內之伺服器，原則上得採取遠端存取；然而，若伺服器位於未加入該公約之國家，應如何處理，判決並未加以說明。此外，就遠端存取本身是否構成對伺服器所在國主權之侵害，判例亦迴避對此問題作出判斷[8]。

就偵查實務家而言，在許多情況下無法得知伺服器所在地國，則依上述判例見解，究竟何種情形得採取遠端存取，仍欠缺明確標準，致使偵查機關於個案判斷上可能面臨困難。

學說上亦有見解指出，若管理伺服器之電信事業未揭露資料儲存地點，以致無法確認伺服器所在地國，仍要求偵查機關取得該國之同意，無異於「要求其履行不可能之事，並非妥當」，並指出「在此種情況下，即使資料有可能儲存於國外伺服器，偵查機關亦無須事先取得該國同意或請求國際刑事司法互助，而應得逕行採取遠端存取」[9]。

此外，就遠端存取是否構成主權侵害之問題，亦有學說認為，唯有伺服器所在國明確表示反對遠端存取時，始會構成對其主權之侵害；在未有此等意思表示之前，尚不得認定已發生主權侵害[10]。亦有外交官以個人見解指出「如對資料具有合法存取權限之人位於本國境內，且偵查機關基於犯罪偵查之需要，持令狀存取、閱覽及複製該人有權限存取之資料，並未對位於外國領域之人、物，或儲存於伺服器之電磁紀錄造成任何變動，因此，原則上不致構成違法之主權侵害」，並認為「此一理解作為兼顧國內犯罪偵查需求與尊重他國領域主權之平衡方式，具有一定之合理性」[11]。然而，亦有學者提出批評，認為縱使伺服器所在國未意識到其主權受到侵害，仍不妨礙認定主權侵害已經發生[12]。此外，從國際法學之觀點而言，雖可看出國際實務有逐漸承認跨境遠端存取之趨勢，但由於「其成立要件尚未形成一致標準」，因此「仍難認已有相關國際習慣法之確立」[13]。至少就日本目前之討論而言，此一問題尚難謂已有定論。

（三）終端設備之解鎖、登入與資料取得

第三項則是近年逐漸受到關注的問題，關於如何解除智慧型手機等個人持有之終端設備的鎖定功能，以及解鎖方法是否存在界限。近年來，智慧型手機多採用臉部辨識、指紋辨識等生物特徵辨識方式作為身分驗證機制。因此，實務上亦開始出現偵查機關於扣押犯罪嫌疑人之智慧型手機等終端設備後，對犯罪嫌疑人施以有形力，使其手指接觸手機感應器，或固定其臉部進行辨識，以解除裝置鎖定之情形[14]。諷刺的是，隨著數位設備認證技術日益進步，生物特徵辨識原本係為加強個人隱私保護而設計，卻反而使解除鎖定功能之手段，再次回歸到對人施以有形力的原始方式，進而衍生新的法律問題。

此外，在解除裝置鎖定方面，如終端設備及其使用者帳號係由多人共同使用，實務上亦有取得其中一人協助，向其借用終端設備，解除裝置鎖定後，再確認犯罪嫌疑人瀏覽器搜尋紀錄之案例。

上述問題顯示，即使偵查機關已透過扣押或借用等方式，取得作為有體物之智慧型手機或平板電腦等終端設備，如欲進一步存取其中之資料，仍須完成解除裝置鎖定、登入帳號等各項操作。因此，此類行為之容許界限，亦逐漸成為偵查實務上的重要問題。

參 電磁紀錄提供命令之理論與預期帶來之變革

一、電磁紀錄提供命令之導入

（一）檢討對象

前述問題固然無法藉由單一制度立即獲得全面解決，惟從完善資料蒐集之手段之觀點，日本於令和 7 年（2025 年）修正刑事訴訟法時，導入了電磁紀錄提供命令制度。該制度已於令和 8 年（2026 年）5 月 21 日施行，目前尚未累積裁判實務可供觀察。以下首先說明電磁紀錄提供命令制度之概要，及其立法過程中的相關討論，進而探討該制度之創設可能為實務帶來何種變化，以及其對於前述各項問題究竟能發揮多大程度之因應功能。以下之討論，主要以偵查機關聲請之電磁紀錄提供命令為中心[15]。

（二）電磁紀錄提供命令之目的

電磁紀錄提供命令之導入，主要具有以下兩項目的。第一，建立得由法院命令通信事業者透過線上方式提供電磁紀錄之制度，以減輕偵查機關與通信業者之負擔。第二，也是更為重要之目的，即有別於傳統著眼於移轉有體物占有、藉由扣押電磁紀錄媒體取得資料之方式，而是創設得直接強制取得必要資料本身之處分，使作為證據之資料得以更有效率地蒐集[16]。就第二點而言，此一制度可謂將偵查機關過去透過取得有體物占有以獲取資訊之方式，轉變為直接取得作為無體物之資料本身。據此，在無法確定目標資料究竟實際儲存於哪一個終端設備，但可認有相當蓋然性儲存於雲端時，偵查機關即可透過管理該雲端服務之通信業者，取得所需之資料。

此外，電磁紀錄提供命令尚具有另一層意義。過去，日本偵查機關係根據刑事訴訟法第 197 條第 2 項之偵查相關事項查詢制度，向銀行或其他機構特定偵查所需資訊後，請求其提供相關資料。然而，偵查相關事項查詢制度欠缺直接強制或間接強制之確保履行之手段。電磁紀錄提供命令則改善了此一制度缺失，不僅透過法院之司法審查作為介入機制，並以間接強制作為確保資料提供之手段，使其得以有效發揮制度功能[17]。

（三）電磁紀錄提供命令之程序

具體而言，偵查機關得依據法官核發之令狀，為電磁紀錄提供命令（刑事訴訟法第 218 條第 1 項）。電磁紀錄提供命令係：①命電磁紀錄保管人將電磁紀錄記錄或移轉至記錄媒體，並提出該記錄媒體（媒體提出命令；第 222 條第 1 項、第 102 條之 2 第 1 項第 1 款前段）；②命相對人將電磁紀錄記錄或移轉至命令機關（即偵查機關）所管理之記錄媒體（狹義之提供命令；第 222 條第 1 項、第 102 條之 2 第 1 項第 1 款後段），使相對人提出記錄媒體或是電磁紀錄之制度[18]。換言之，偵查機關得命相對人：①將記載資料之記錄媒體作為有體物提出；或②將資料本身傳送至偵查機關所管理之記錄媒體（包括伺服器）。

偵查機關聲請電磁紀錄提供命令時，令狀應記載「應提供之電磁紀錄、應提供之人及提供方式」等事項（第 219 條第 1 項）。如對電磁紀錄提供命令令狀之核發本身有所不服，或認為執行機關要求提供之電磁紀錄已逾越令狀所載範圍等，而對處分之合法性有所爭執時，被處分人得提起準抗告（第 429 條第 1 項第 2 款、第 430 條第 1 項）。

於提供命令執行完畢後，如已無繼續禁止被處分人保有已移轉資料之必要，法院應依被處分人之聲請或依職權，於被告案件終結前，以裁定准許被處分人複製該等資料（第 222 條第 1 項、第 123 條之 2 第 1 項）。此項程序可認係相當於有體物扣押制度中返還扣押物之程序。

（下期待續）

（作者為一橋大學法學研究科教授
譯者為臺北大學法律學系副教授）

註釋

法』（商事法務、2017 年）570 頁以下。此一見解另指出，就證明問題而言，是否侵害他國主權，須於特定資料所儲存之國家後始能判明，因此，僅因有伺服器位於國外之疑慮，尚不足以推翻該遠端存取行為合法性之推定。

11 御坐智洋「インターネットの利用に関する国際的なルールにおいて領域主権が果たす機能」国際法外交雑誌 121 巻 1 号（2022 年）1 頁以下、12 頁。

12 竹内真理「サイバー捜査と国家管轄権」ジュリスト 1647 号（2020 年）75 頁、川出敏裕「判批」論究ジュリスト 37 号（2021 年）121 頁以下、127 頁。

13 石井由梨佳「国際法学の観点から— 越境リモートアクセス捜査の評価」指宿信ほか編『越境するデータと法』（法律文化社、2023 年）171 頁以下、180 頁。

14 雖然目前尚未見諸裁判例，惟於稅務調查及犯罪偵查等場合，曾多次自偵查實務工作者、新聞記者等處聽聞此類情形。

15 此外，被告、被疑人或辯護人，亦得作為證據保全之一環，向法官聲請核發電磁紀錄提供命令（第 179 條）。辯護人將於何種程度上積極運用此一制度，以及法官將於何種程度上准許辯護人之聲請，亦為值得關注之問題之一。

16 川出敏裕ほか「刑事手続の IT 化とその課題」有斐閣 Online ロージャーナル YOLJ-L2508008（2025 年 10 月 30 日公開）¶082〔中山仁〕、¶083〔保坂和人〕。

17 成瀬剛ほか「鼎談・電磁的記録命令の創設」ジュリスト 1614 号（2025 年）66-67 頁。

18 其中，①係承襲既有之附命令扣押電磁紀錄制度。隨著電磁紀錄提供命令制度之導入，關於附命令扣押之相關規定，已整合納入電磁紀錄提供命令之規範中。