從日本山崎案談營業秘密不法取得之管理

從日本山崎案[1]談營業秘密不法取得之管理

資策會科技法律研究所
法律研究員　駱玉蓉
105年05月25日

壹、前言

為強化營業秘密的保護，日本從2003年開始，於不正競爭防止法（以下稱本法）中導入刑事保護的相關條文，爾後經過多次修法，在2011年調整刑事訴訟程序的同時，於本法導入了即使行為者不使用或揭露所示的營業秘密，但只要以獲取不當利益為目的，且「以複製」等方式「取得營業秘密」，亦為刑事處罰的對象[2]。2014年名古屋地院的日本山崎Mazak案件（ヤマザキマザック事件，以下稱本案）則是在此修法背景中，於少數公開判決中最先單獨引用該法條的案件。

面對層出不窮的營業秘密侵害案件，為遏止及處罰不法取得、使用或洩漏他人營業秘密的行為，我國營業秘密法亦於2013年的修法中增訂侵害營業秘密的刑事責任，將「知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密」的行為[3]納入刑罰範疇，以期可有效遏阻營業秘密侵害案件。

有鑒於營業秘密外洩情形與不法取得手法的多變，本文將先從本案營業秘密侵害行為、存取/接觸權限控管的漏洞出發，接著探討應如何從控管員工的接觸/存取權限以強化營業秘密的保護，最後從落實營業秘密管理的面向，彙整本案受法院判決肯定之營業秘密保護措施及可進一步強化之配套，期給予我國企業營業秘密管理的省思。

貳、事件概要

中國大陸籍的被告Y，於2006年4月進入工具機大廠山崎Mazak（以下簡稱原告公司）任職，於2011年8月轉調連結業務部門與研發部門的業務技術部，於2012年3月因獲得其他公司聘書而提出離職申請，預定離職日為同年4月20日。

檢察官於一審的起訴內容提到，被告Y在無業務需求的狀況下，將三萬件以上的設計圖面等由公司內部伺服器下載至私人硬碟中，更於提出離職的當月，下載約一萬件與轉職企業相關機種的設計圖面等技術資料。雖然被告Y辯稱取得該等資料的目的在於工作上的學習需求，但根據被告Y與其中國大陸友人的往來訊息可知被告Y亟欲脫手所取得的技術資料以換取現金。

原告公司在本案當時，對技術資料的權限控管為將技術資料儲存在公司內部伺服器的資料夾內，僅業務上有需要的員工才能進行存取、下載，此外，原告公司配發給員工的業務用電腦亦設定有員工個人的帳號、密碼來進行認證，並藉由IP位址來辨識存取網路資料的員工所屬部門及該員工的存取權限。有關前述IP位址的分配，為一個部門配發255個IP位址對應255台電腦，當一部門未達255台電腦時，將會有未被電腦對應的IP位址存在，被告Y便是將自己電腦的IP位址切換成未被電腦對應的IP位址，再進行檔案的存取與複製。經由上述一連串的證據與事實證明，一審法院認定被告Y以不當得利為目的而複製（取得）原告公司的營業秘密，處以拘役兩年、併科罰金50萬日幣的判決。

參、判決評析

從本案可知，原告為保護其營業秘密，針對存取/接觸營業秘密者設有相關限制管理。亦即，藉由IP位址辨識存取網路資料的員工所屬部門及存取權限，再透過存取權限的帳號、密碼進行認證管理，該種管理方式立意良好，但在實施時，卻因為有未被電腦對應的IP位址存在，而讓被告Y取巧以切換IP位址的方式逾越權限接觸並取得原告公司的營業秘密。此外，雖然原告公司有留存電腦log紀錄，因而最後能證明被告Y曾進行六千次

以上的資料存取，但若能在事前做好防備，強化管理措施，例如禁止濫用IP位址越權存取或限定存取次數等方式，增加意圖竊取營業秘密者的取得困難，相信能更遏阻潛在或食髓知味的不法行為。

以下從本案原告公司對於員工接觸權限的控管為啟發，例示限制員工存取/接觸營業秘密，可採取的強化對策。

一、適當賦予一定範圍之存取/接觸權。

例如在企業的研發單位，可依專案或產品線而拆分成多個範圍，依據範圍設定可存取/接觸的權限，藉此可避免出現如本案中，僅限定存取/接觸權、卻未區分範圍，導致一人手持帳號密碼便可通行無阻存取/接觸全部資料，造成外洩時損害程度的提高。

二、在上述對策一的基礎上，於資訊系統中註冊存取/接觸權者的帳號。

除了落實一帳號一密碼的原則，針對單一帳號的存取/接觸權限來限制其可閱覽、存取的資料範圍或內容外，若是員工有離職、轉調等情況時，亦要配合以刪除ID、更改存取/接觸權限的方式來應對，避免如本案因作業方便而導致有空的IP位址等開後門的情況，而造成營業秘密管理功虧一簣。

三、以區分保管來限制對營業秘密的存取/接觸權限。

區分保管可大分為「空間分離保管」以及「資料區分保管」。以空間分離保管為例，可依進出人員區分為訪客可進入的區域、持有門禁卡員工均可進入的區域、僅限定該部門員工才可進入的區域、針對保管高機密性資訊區域，實施指紋等生物認證的門禁管制。而以資料區分保管為例，常見的做法有高機密性文件與一般文件區分保管。

例如在本案中，隸屬於業務技術部的人員，便不應該擁有自由存取/接觸其他部門—研發部門之研發資料的權限，建議企業可透過前述的空間分離保管、資料區分保管，兩種方式雙管齊下，實施跨部門資料存取權限的控管。

四、禁用私人紀錄媒體、落實紀錄媒體的使用及保管。

嚴禁使用外接式的私人紀錄媒體，企業除了須備足員工所需的紀錄媒體之外，更需制訂與落實紀錄媒體的使用及保管措施。在本案中，即因原告公司當時的業務技術部部長（下稱部長Q）發現到部門內的紀錄媒體使用不受控管，導致私人紀錄媒體濫用的現象，便於其轄下部門制定如：建立可攜式紀錄媒體管理清單及使用規定，落實借出/返還管理、以及明訂禁止攜入或使用私人的外接式紀錄媒體的規範等，法院因而認定原告公司已採取合理保密措施。

然而，除了明定紀錄媒體的禁止使用或限制使用等規定外，還應透過週會、組會、課程宣導等方式周知可攜式紀錄媒體的使用規則，同時透過定期稽核確保該使用規則的確實執行，避免徒有管理規範卻未落實控管。

肆、結論

本案原告公司雖明定營業秘密相關的管理規定，例如權限設定、禁用私人紀錄媒體、公司紀錄媒體使用及保管等各種管理措施，而在本案獲得勝訴判決。但除了管理措施有可強化之處外，主要的原因仍發生於管理機制於實際運作上未嚴格落實，而有部門員工長期持有企業配置的硬碟與USB隨身碟而未歸還，甚或違反禁止使用私人可攜式紀錄媒體的規定，使用私人硬碟等的狀況，造成被告Y有機可乘使用私人硬碟儲存原告公司上萬筆設計圖面等資料。

從此可知，即便企業已建立各種營業秘密相關的管理措施，仍須定期追蹤掌握管理機制的落實，例如定期內部檢視和外部稽核、不定期抽查員工電腦使用紀錄等，確保營業秘密的有效管理。同時間，企業亦應隨時預警任何不符規定的異常警報，透過log異常行為的警示設定，提早發現問題並採取證據保全措施，將營業秘密外洩風險或損害降至最低。

企業歷經營業秘密的盤點、分級、達成管理措施共識，到形成各部門遵循的管理制度等繁複流程，始確認營業秘密保護標的及合法合理的管理措施，若是未落實執行管理，除了增加營業秘密外洩的風險，於後續訴訟階段也難以處於有利舉證的立場。所謂魔鬼藏在細節裡，無論是何種對策，確實落實而不流於形式，更是保護營業秘密的不二法則。

本文同步刊登於TIPS網站（http://www.tips.org.tw）

---

[1] 名古屋地裁平成26年8月20日判決。

[2] 2011年日本《不正競爭防止法》第21條第1項第3款。

[3] 2013年我國《營業秘密法》第13條之1第1項第3款。

駱玉蓉
法律研究員 編譯整理

上稿時間：2016年06月

推薦文章