科技法學評論，5 卷 1 期，頁 103（2008）

**科法新論**

# Matrix駭客任務：刑法第358條入侵電腦罪

蔡榮耕*

## 摘　要

刑法第 358 條並沒有定義什麼是電腦。不過，這應該是正確的作法，因爲實務可以因而有較大的彈性，以因應未來的科技發展。即便是要在法條中明文電腦的意義，也應該參考美國聯邦電腦詐欺及濫用防制法（CFAA）的規定，採取較爲開放的定義。本文也建議，刑法第 358 條的構成要件行爲應修正爲「無故入侵」電腦即爲已足。至於「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」應屬蛇足的規定。「無故入侵」的解釋，可以參考美國聯邦電腦詐欺及濫用防制法（CFAA）中，關於「無（越）權使用」的規定及相關判決。

關鍵字：電腦犯罪、入侵電腦、刑法第 358 條、聯邦電腦詐欺及濫用法、無權使用電腦、越權使用電腦

---

* 美國印地安納大學布魯明頓校區法學院法學博士候選人。

投稿日：2008 年 1 月 2 日；採用日：2008 年 2 月 21 日

Cite as: 5 Tech. L. Rev., Apr. 2008, at 103.

# Matrix－Criminal Law Article 358 Intrusion of Computer

Rong-Geng Tsai

Abstract

It is accurate for the legislature not to define what a computer is in article 358 because the absence of the definition makes it flexible for the law enforcement to respond the rapid technology development. The legislature ought to visit CFAA even though it wants to give a definition. This article suggests that actus reus requirements of the current article 358 are improper. It is unnecessary to narrow down the actus reus requirement to inputting other's account and password, hacking the protecting measure of a computer, and making use of the hole of computer system. The proper actus reus requirement should be "accessing a computer without authorization, or exceeding authorized access." When interpreting and applying, we could refer to CFAA and the judicial decisions thereof.

Keywords: computer crime, intrusion of computer, article 358 of criminal law, the Computer Fraud and Abuse Act of 1986, access a computer without authorization, or exceeding authorized access

# 1. 前言

隨著電腦的問世，人們的生活有了莫大的改變。電腦，帶來許多生活上的便利，卻也對於犯罪行爲產生影響。這一類利用電腦的新犯罪型態，多半被稱之爲「電腦犯罪」。電腦犯罪之所以有別於一般犯罪，是因爲行爲人利用了電腦來完成違犯刑法的行爲；再者，證明這一類犯罪所需的證據，多半都是以電磁的型態所紀錄著。電腦犯罪所造成的損害，也相當廣泛及嚴重。在 2004 年，美國聯邦調查局估計，電腦犯罪共造成該國境內約 4,000 億美元的損失[1]。另外，在 2000 年，光是 I Love You 病毒就造成了約 67 億美元到 100 億美元的損失[2]。但是，實際上的損失，應該遠比這一個數字爲大，原因在於，很多的受訪者擔心如實回答的話，將對企業形象造成不良的影響。

在刑事法的領域討論電腦犯罪時，討論的議題包含了實體法及程序法兩個層面。電腦犯罪的實體法可以分爲濫用電腦行爲及利用電腦所進行的傳統犯罪。這兩者的不同在於，濫用電腦行爲是因爲電腦的發明才產生的新型態犯罪，其中包括了駭客行爲（hacking offenses）、散布電腦病毒（virus crimes）及癱瘓電腦（denial-of-service）等。其所使用的方式，不外乎是無（越）權使用電腦（或稱之爲入侵電腦），以及使他人無法使用一定電腦設備。這一些犯罪的結果，多半都是發生在電腦的虛擬世界裡。至於利用電腦所進行的傳統犯罪，則是在電腦發明前就已經存在，只是在現在改以電腦作爲工具而已。這一類犯罪的結果則多半出現在現實世界中，例如網路詐欺、散布猥褻物品及竊取商業秘密等。電腦犯罪在程序法部分所涉及的爭議，大抵是搜索、扣押及隱私的問題。所面臨到的議題是，在電腦的世界中，什麼是搜索？什麼是扣押？其應該遵守的程序限制爲何？在使用電腦時，人民的

---

1 *See* MCAFEE VIRTUAL CRIMINOLOGY REPORT (2005), http://www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf.

2 *See* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 36 (2001).

隱私受到什麼樣的保障？

本文所討論的主題，主要是一個基本的電腦犯罪規定：刑法第 358 條。本條限定入侵電腦的行爲方式必須是「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」進而入侵電腦。本條的規範架構爲何？法院所認定的「無故輸入他人帳號密碼」是怎麼樣的案件類型？實務上又如何解釋及適用「破解使用電腦之保護措施」？這一些都是值得探究的問題。他山之石，可以攻錯。美國各州在 1978 年開始，便已經針對抗制電腦犯罪有所立法，聯邦則是在 1984 年正式將電腦犯罪的行爲刑罰化。該國在這方面的理論發展、法條規範以及實務判決，應該可以供作我國學理討論及法院處理相關案件時的參考。是故，以下我們先分析我國入侵電腦罪的規定及實務判決。緊接著，會介紹美國的相關法規及法院見解。最後，本文會從美國實務及學理上的角度，針對我國刑法第 358 條的規定提出修法及解釋上建議。

## 2. 刑法第 358 條的基本結構、要件及相關判決

我國在 2003 年 6 月增訂刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」其立法理由是：「……鑑於對無故入侵他人電腦之行爲採刑事處罰已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行爲之危害性應已達科以刑事責任之程度，爲保護電腦系統之安全性，爰增訂本條。」這一個法條限定了入侵電腦的行爲方式；立法上，也沒有未遂的處罰規定。法院對於本條的解釋，多半都是認爲，行爲人在進入到電腦系統內，並處於隨時得接觸其內部資訊的狀態後，才算是入侵電腦。再者，實務上對於應該如何適用刑法第 358 條來解決以輸入帳號密碼的方式入侵電腦，則會因爲事實的差異而有不同解釋。

## 2.1　本條的基本結構

依照刑法第 358 條的規定，必須要是以「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」的方式，入侵他人電腦才會構成本條的入侵電腦罪。以其他方式入侵電腦者，並不能以刑法第 358 條相繩。例如，如果被害人的電腦系統沒有設定電腦密碼、保護電腦措施或系統漏洞，便不在本條的保護範圍之內。又例如，爲了讓 X 可以從其電腦中查看通訊錄中 A 的電話號碼，Y 便向 X 說了其電腦的開機密碼。不料，X 除了看了 A 的電話號碼之外，還偷看了其電子郵件。按照目前的條文文字，X 的行爲並不會構成入侵電腦罪[3]。另一個例子就是社會上沸沸騰騰的藝人陳冠希事件，使用者單純地直接刪除掉硬碟上的資料，他人利用 undelete 的指令或是檔案復原軟體予以回復[4]。後者的行爲，也很難爲刑法第 358 條的文字所涵括。不過，本條在行爲方式上，是否有必要作這樣的限縮，值得商榷。

再者，本條並沒有未遂規定。換言之，即便行爲人嘗試輸入他人的帳號密碼、破解電腦的保護措施或利用系統漏洞，只要沒有成功，沒有進入到電腦系統內，就不會構成刑法第 358 條的犯罪。然而，值得留心的是，類似的輸入帳號密碼的行爲，恐已影響到立法者想要保護的「電腦系統之安全性」，甚至會造成系統運作上極大的負擔[5]。

---

3　不過，以美國電腦犯罪的條文設計，例子中 X 的行為是可罰的無（越）權使用電腦的行為。關於美國電腦犯罪的條文規定及判決，在下文「3.」會有更詳盡的說明。

4　請參照「淫照事件／陳冠希友人：他家有暗門，私藏影帶和照片」，ETtoday，2008 年 2 月 5 日，ETtoday 網站：http://www.ettoday.com/2008/02/05/11445-2228182.htm（最後點閱時間：2008 年 3 月 28 日）。

5　例如，行為人以「試誤」的方式來找到正確的帳號及密碼，就有可能造成電腦系統極大的負擔。關於試誤程式，請詳見註 42 的說明。

## 2.2 本條的構成要件及相關實務判決

如同前述，刑法第 358 條對於「入侵他人之電腦」有其行爲方式上的限制。實務上在判斷行爲人是否構成這一個犯罪時，也都緊扣著法定的行爲方式在討論及說明。近年來法院已經針對何謂「無故輸入他人帳號密碼」及「破解使用電腦之保護措施」作成相當多的判決，值得參考及進一步討論。至於「利用電腦系統之漏洞」型的入侵電腦，因爲實務上似乎還沒有形成相關的意見，本文先不擬予以討論。

### 2.2.1 無故輸入他人帳號密碼

歸納我國的判決後可以知道，多數法院認爲，「無故輸入他人帳號密碼」「入侵他人之電腦」指的是，行爲人在輸入帳號密碼後，進入到他人系統內部，並處於隨時可取得內部資訊的狀態[6]。舉例來說，在 96 年度上訴字第 153 號判決中，台灣高等法院台南分院便認爲，輸入帳號及密碼，連線進入他人系統，並取得其電腦資料的行爲，構成刑法第 358 條的入侵電腦罪。本案的事實是，被告在從聯合國際公司離職後，另外成立數位聯網公司。爲了與原任職公司競爭，被告經由該公司的系統漏洞，在輸入帳號密碼後，入侵該公司電腦，並取得其客戶及業務資料[7]。台南高分院表示，被告的行爲同時構成刑法第 358 條無故輸入他人帳號密碼而入侵他人電腦罪，以及同法第 359 條無故取得他人電腦之電磁紀錄罪[8]。至於入侵內部網路的電腦系統，法

---

6 資料搜尋的對象是以司法院「法學資料檢索」裡的「裁判書查詢」。搜尋的條件是 2003 年至 2007 年 9 月，以及刑法第 358 條。以下的實務判決，都是以這樣的條件搜尋得知。

7 台灣高等法院台南分院 96 年度上訴字第 153 號判決（審判長楊明章），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

8 類似入侵系統的案件，可以參照台灣高等法院高雄分院 95 年度上易字第 872 號判決（審判長周賢銳），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。本件中的被告入侵數個學校的電腦系統後，取得帳號及密碼，並將自己的網站的部分內容放置於該等學校的伺服器內，以供他人下載。高雄高分院認為，被告的行為

院也是採取相同的態度。在高等法院 95 年度上訴字第 765 號案中，被告是在內政部消防署服務的公務員，其輸入他人的帳號及密碼後，進入消防署的差勤系統，取得被害人的個人公差統計及刷卡紀錄等資料。高等法院認爲，被告的行爲構成了無故入侵電腦罪[9]。

至於輸入他人的帳號及密碼，並進入他人的電子郵件信箱的行爲，也同樣構成無故侵入他人電腦罪[10]。在台灣高等法院 96 年度上訴字第 1127 號判決中，被告輸入告訴人的帳號及密碼，侵入告訴人的電子郵件信箱，並以告訴人的名義，寄出郵件。之後，被告刪除掉該郵件的寄件備份，以掩飾行爲。除了刑法第 358 條的入侵電腦罪外，高等法院認爲行爲人的行爲也構成了刑法第 359 條的刪除他人電腦的電磁紀錄罪[11]。高等法院也判定，利用電腦

---

構成了刑法第 358 條的無故入侵電腦罪。有問題的是，被告是以連線的方式入侵被害學校的電腦，但是，無論是檢察官或是法院都不認為被告的行為涉及刑法第 359 條的無故取得變更他人電腦資料罪。不過，以連線的方式入侵他人電腦，在技術上，不可能不取得該電腦的資料。再者，將自己的檔案複製進他人電腦，也一定會變更他人電腦資料。為何檢察官及法院都未論及刑法第 359 條？可能是實務在處理類似案件時，並不熟悉電腦的運作所致，不過，這也導致了這一類判決有適用法律違誤的可能。

9 請參閱高等法院 95 年度上訴字第 765 號判決（審判長劉景星），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。高等法院認為，本件的被告同樣構成刑法第 359 條的無故取得他人電腦電磁紀錄罪。值得玩味的是，這一個法條有「致生損害於公眾或他人」的要求，而被告的行為是入侵內政部消防署的差勤系統後，列印出被害人的人事紀錄，而沒有變更或是刪除任何紀錄。但是，高等法院仍認為，被告的行為已致生損害於被害人「對於電腦差勤系統登入管控機制之安全信賴性」，所以，被告的行為仍該當刑法第 359 條的要求。如果連對於「安全信賴性」的影響都可以該當「致生損害於公眾或他人」的要求，那麼「致生損害於公眾或他人」應該就屬於多餘的規定。

10 台灣高等法院 96 年度上訴字第 1127 號判決（第四庭，蔡秀雄審判長）。關於輸入他人帳號密碼，入侵他人電子郵件信箱的行為，還可以參考台灣高等法院 95 年度上訴字第 2674 號判決（審判長吳昭瑩），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

11 有趣的是，行為人所刪除的是自己所製作的紀錄，而不是告訴（被害）人所有，不

連線進入銀行系統，轉帳盜領他人存款的行爲，也構成第 358 條的犯罪[12]。

值得說明的是，法院認爲，刑法第 358 條中前後兩個「他人」並不需要是同一個人。也就是說，這一個行爲態樣除了包含 X 無故輸入 Y 的帳號及密碼以入侵 Y 的電腦外，也包括了 A 無故輸入 B 的帳號及密碼而入侵 C 的電腦的行爲。台灣高等法院 95 年度上訴字第 2482 號判決便爲適例。本號判決中，行爲人以強暴的方式從被害人處問得其於天堂遊戲上的帳號及密碼後，在某網咖的電腦上，輸入被害人的帳號及密碼。地方法院及高等法院都認爲，被告的行爲已經構成了無故輸入他人帳號及密碼入侵他人電腦罪[13]。實際上，被告最終所入侵的不是被害人的電腦，而是遊戲橘子公司的伺服器及設備。不過，法院仍認爲，被告的行爲構成了刑法第 358 條的犯罪。

除了前述幾個以連線的方式入侵電腦的案例外，實務上認爲，刑法第 358 條的「入侵」不限於以連線的方式。也就是說，即便是行爲人走到他人電腦前，親自無權或越權地使用該電腦，都可以該當「入侵」的要件。不過，因爲本條限制只有以一定的方式入侵電腦才構成犯罪，所以如果他人的電腦沒有任何的開機密碼、保護措施或是系統上的漏洞，那麼單純使用該電腦，並不會構成刑法第 358 條的犯罪。這樣的立場在台灣高等法院 94 年度上易字第 1418 號判決可見一斑。本件的事實約莫是，被告使用了被害人的筆記

過，法院認為，行為人的行為仍構成刪除他人電腦之電磁紀錄罪。也就是說，高等法院認為，只要行為人所刪除的是他人電腦中的紀錄，就會該當刑法第 359 條的要求。至於該紀錄由何人所製作，在非所問。

12 請參照台灣高等法院 95 年度上訴字第 4568 號判決（第八庭，鄭文肅審判長），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。本件中的被告將帳戶售予另案判決確定的證人胡可之使用。胡的手法是利用網路入侵銀行，將他人的存款轉帳到所購得的人頭帳戶，再從該人頭帳戶中將現金提領出來。法院認為，胡的行為構成刑法第 358 條的入侵他人電腦罪、第 359 條無故取得變更他人電磁紀錄罪。

13 台灣高等法院 95 年度上訴字第 2482 號判決。類似判決，可以參考高等法院台中分院 94 年度上訴字第 1844 號判決，司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

型電腦以連結上網際網路，並且因而得知其電腦內部的資料內容。檢察官認爲，被告無故入侵被害人的電腦。高等法院未接受這樣的主張，並表示，被告所使用的筆記型電腦固然是被害人所有，但是，該電腦並沒有設定任何的密碼，也沒有其他的保護措施或系統上的漏洞，所以，被告的行爲不構成入侵他人電腦罪[14]。

從這一個判決可以知道，法院認爲「入侵」並不限於連線的方式。這應該是一個正確的解釋，值得予以肯定，因爲從法條的文義及立法理由上來看，入侵並不只限於以連線的方式進入到他人的電腦系統內。再者，直接操作他人的電腦也會影響到本條所想要保護的是「電腦系統之安全性」，所以，將「入侵」解釋爲包含直接操作他人的電腦，應該是適當的方向。不過，因爲刑法第 358 條對於行爲方式的限制，如果被入侵電腦的電腦沒有設有密碼或保護措施，行爲人也沒有利用系統上的漏洞，那即便行爲人使用了該電腦，並且窺知了其內之資訊，也無法以本條加以處罰。這樣的結果是否妥適，值得探究。

### 2.2.2　破解使用電腦之保護措施

除了無故輸入他人帳號及密碼外，刑法第 358 條所規範的另一個入侵型態是「破解使用電腦之保護措施」。實務上認爲，密碼帳號機制屬於這裡所稱的保護措施。那麼，這一個行爲方式，要如何與「無故輸入他人帳號密碼」區分呢？法院認爲，「無故輸入他人帳號密碼」僅限於輸入他人原有的設定數值。如果是以變更原有密碼的方式入侵系統，就已經是「破解使用電腦之保護措施」，其包括了以欺騙的方式取得新密碼，並以之入侵他人電腦。以台灣高等法院高雄高分院 95 年度上訴字第 1589 號判決爲例，本案的事實是被告爲入侵被害人的電子郵件信箱，在連線進入高雄市政府員工電子郵件系統後，輸入被害人的姓名、身分證字號、電子郵件帳號及機關代號，

---

14　台灣高等法院 94 年度上易字第 1418 號判決（審判長許國宏），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

並選擇「忘記密碼」，因而使電腦主機另外分配一組新的密碼。被告再利用帳號及該新密碼進入被害人的電子郵件信箱。

本件在一審時，高雄地方法院認爲本件屬於「無故輸入他人帳號密碼」的入侵電腦型態，不過，高雄高分院認爲，地方法院的認定有誤，其認爲被告的行爲應屬「破解使用電腦之保護措施」[15]。高雄高分院認爲，輸入他人帳號密碼指的是以任何方式得知他人的帳號密碼後，直接輸入。至於本案中被告的行爲，屬於另外取得新的密碼後再輸入，並進入系統，而不是以取得原有的密碼入侵電腦，所以也就與「無故輸入他人帳號密碼」的構成要件要素不合。也因爲被告的行爲破壞的是原有的密碼對於電腦的保護，所以法院認爲其構成的應該是「破解使用電腦之保護措施」的入侵電腦罪，而不是輸入帳號密碼型的入侵電腦罪[16]。

在這一個判決中，法院並沒有直接定義什麼是刑法第 358 條中的「使用電腦之保護措施」。但是，從判決中可以很清楚地知道，高雄高分院認爲，密碼屬於該保護措施，只要輸入的不是原設定密碼而進入系統，就應該屬於破解保護措施型的入侵電腦罪。無論法院最後認定被告所爲的是輸入帳號密碼或是破解保護措施，所構成的都是本條的犯罪，刑度也不會有何差異。是故，認定被告是利用何種方式，在實質上並不會有太大的差別。就立法政策上來看，只要是無故入侵他人電腦，就已經足以影響其系統安全性，所使用的方式爲何，應該不是重點。至於利用系統漏洞型的入侵電腦，目前實務似乎還沒有作成判決。

以上，本文介紹並討論了刑法第 358 條入侵電腦罪的架構、行爲方式及

15 台灣高等法院高雄分院 95 年度上訴字第 1589 號判決（審判長李炫德），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

16 這一個案件還有一點值得繼續研究的課題。高分院認為被告的行為並不構成刑法第 359 條的犯罪。然而，在入侵了被害人的信箱後，怎麼可能沒有「取得他人電腦之電磁紀錄」？也就是說，在邏輯上，以連線的方式入侵他人電腦，有可能只單純地入侵電腦，但是不取得他人的電磁紀錄嗎？

相關判決。以下，爲了作法制上的比較，本文擬進一步說明美國的入侵電腦罪的規定及實務判決。

# 3. 美國聯邦電腦詐欺及濫用防制法（CFAA）的入侵電腦罪

爲了抗制電腦犯罪，美國聯邦國會在 1986 年制定「聯邦電腦詐欺及濫用防制法（The Computer Fraud and Abuse Act of 1986, CFAA[17]）」。其中，主要所處罰的行爲型態是無（越）權使用電腦的行爲。下面所介紹的是 CFAA 的基本架構、該法案對於「電腦」、「無（越）權」及「使用」的規定及相關判決。

## 3.1 CFAA 的基本架構

與我國相仿，美國各州及聯邦都有電腦犯罪的專章規定。最早的是佛羅里達州（Florida），其於 1978 年就已經將利用電腦的犯罪行爲刑罰化；最晚的是佛蒙特州（Vermont），在 1999 年也已經制定了電腦犯罪刑法。美國聯邦則是在 1984 年開始通過相關的法律。在眾多聯邦電腦犯罪刑法規範中，最重要的當屬上述的 CFAA。無論是聯邦或是各州的法律，都禁止未經授權的使用電腦行爲（unauthorized access）。正因聯邦及各州都有著類似的規定，以下本文便以 CFAA 的規定作爲主要的討論對象。

與我國相同的是，CFAA 的制定是爲了要因應及抗制日益頻仍的電腦犯罪行爲。與我國刑法第 358 條一樣，CFAA 所保護的行爲客體是「電腦」；不同與我國的是，CFAA 所處罰的犯罪行爲態樣不是入侵（intrude），而是「無權或越權使用電腦（access a computer without authorization, or exceed authorized access）」，主要的刑罰條文有七個，都是在 18 U.S.C. § 1030(a)下面。第一項是 18 U.S.C. § 1030(a)(1)，所處罰的是無權或越權使用電腦，進而

17 The Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986).

取得機密資訊以造成美國之損害，或用以協助外國勢力（foreign power）。本項的適用範圍相當地窄，是故從立法至今從未有過任何判決[18]。18 U.S.C. § 1030(a)(2)是最常用以抗制非法入侵電腦行爲的條文，其禁止無權或越權使用（access）電腦，進而取得資訊。18 U.S.C. § 1030(a)(3)禁止無權使用聯邦政府電腦。18 U.S.C. § 1030(a)(4)處罰的是利用無權或越權使用電腦的詐欺行爲。18 U.S.C. § 1030(a)(5)禁止散布程式碼或無權使用電腦並造成損害。18 U.S.C. § 1030(a)(6)處罰騙取密碼的行爲。最後是 18 U.S.C. § 1030(a)(7)禁止以威脅損害電腦的方式勒索財物。18 U.S.C. § 1030(b)則規定，所有 18 U.S.C. § 1030(a)的未遂行爲都是可罰的犯罪。同前所述，上面各個條文裡最重要的，當屬 18 U.S.C. § 1030(a)(2)，以下便以這一條爲基礎來做討論及比較。

## 3.2 電腦

CFAA 對於「電腦」的定義是：「得以執行邏輯、計算及儲存功能的電子、磁性、光學、電子化學或其他高速資料運算裝置；以及其他相關，或是與上述高速資料運算裝置同工的資料儲存及通訊裝置。但是，上述的高速資料運算裝置不包含自動打字機、自動排版機、手持計算機或其他類似的裝置[19]。」這樣的立法定義相當廣泛，所能涵蓋的類型相當的多。也因著國會對於「電腦」採取較開放的定義，美國法院對於電腦也採取了很有彈性的解釋。

以 *United States v. Mitra* 案[20]爲例，可以約略知道該國實務的態度。在本案中，美國聯邦第七巡迴法院表示道，行動電話、基地台、iPod 及無線網路基地台等都是 CFAA 定義下的「電腦」。*Mitra* 案中的被告利用訊號發報器阻隔了威斯康辛州麥迪遜地區（Madison, Wisconsin）警方的無線電訊號。檢察官認爲，被告明知其無權仍有意傳送訊號並使受有保護的電腦因而受有損

18 ORIN S. KERR, COMPUTER CRIME LAW 28 (2006).

19 *See* 18 U.S.C. § 1030(e)(1)(2002).

20 United States v. Mitra, 405 F.3d 492 (7th Cir. 2005).

害，所以起訴了被告[21]。檢察官的一個重要的主張是，威斯康辛州警方的無線電系統屬於 CFAA 定義下的電腦。再者，被告利用發報器阻隔訊息的方式也構成了傳送訊號[22]，所以被告的行爲構成無權使用電腦。不過，被告反駁道，警方的無線電設備不是 CFAA 定義下的「電腦」。法院並不接受被告的主張，相反地，第七巡迴法院接受了檢察官的說法。

對於「電腦」的定義，第七巡迴法院採取了相當廣義的解釋。其認爲，因爲科技的快速發展，立法者並無意列舉禁止的行爲類型；從 CFAA 只排除自動打字機、自動排版機、手持計算機或其他類似的裝置來看，國會也無意限縮「電腦」的範圍。是故，法院認爲，威斯康辛州警方的無線電設備屬於 CFAA 的「電腦」[23]，被告的行爲也因而構成犯罪。

對於「電腦」所涵括的範圍，美國的司法及立法都採取相當有彈性的立場。如同 *Mitra* 案的判決，如果對於電腦的定義過度限縮，以現在科技發展的速度來看，恐怕無法因應社會上對於電腦犯罪立法的需要。是故，CFAA 的規定及 *Mitra* 案的判決，應該是正確的方向。

## 3.3　使用（access）

CFAA 並沒有針對「使用（access）」作有立法上的定義，探究其原因，應該是美國國會有意要讓司法有較大的彈性空間來因應各種具體情形。對於何謂「使用」電腦，學理上則提出兩種可能的解釋：一個是虛擬進入（virtual entrance）說；另一個是下達指令（instruction entrance）說。美國實務上，也針對什麼樣的行爲會構成「使用」電腦，作成許多解釋及認定。

### 3.3.1　美國學理上的解釋

依照虛擬進入（virtual entrance）說，電腦或系統就像是一個存在於電腦

---

21　*See* 18 U.S.C. § 1030(a)(5)(A)(2002).

22　*Mitra*, 405 F.3d at 494.

23　*Id*. at 495.

世界的一個處所或空間；使用電腦則可以想像成是進入該處所中。在這一個類比下，一個以使用者名稱（user's name）及密碼（password）保護的網頁，就如同一個房門上的大鎖。輸入正確的使用者名稱及密碼時，並進入電腦或系統內，就像是用鑰匙打開門鎖，進入該處所；如果輸入的資料不正確，就如使用了錯誤的鑰匙，無法進入該處所，也就沒有使用電腦。再者，如果只是看到輸入帳號密碼的網頁，而沒有輸入帳號及密碼，就像只在處所外面閒晃或張望，而沒有進到該處所，也就不算是有使用電腦[24]。

下達指令（instruction entrance）說的主張是，在討論電腦犯罪的相關議題時，不應該，也不需要將電腦類比爲現實生活中的空間，電腦就是一個可以用以交換及處理資訊的機器，所以使用電腦就是使用者向一台電腦下達指令，而該指令爲電腦所接收。是故，當使用者的指令被電腦所接受後，就是使用電腦[25]。相對地，如果使用者沒有向電腦或系統下達指令，就不構成使用電腦。

多數的案件，在判斷行爲人是否使用了電腦時，無論是採虛擬進入或是下達指令說，討論後都會得到相同的答案。例如，不管採取哪一個方法，破解他人電腦系統的防護措施，取得其管理者權限密碼的行爲，都已經構成了「使用」行爲[26]。但是，在某些兩可的案件中，採取不同立場就會有不同的答案。再者，在解釋「使用」時，下達指令說的範圍會比虛擬進入說要來得要廣。舉例來說，A 爲了使用一台受密碼保護的電腦，輸入指令要求電腦回傳可以輸入使用者名稱及密碼的網頁或是對話方塊。電腦執行該指令，如果採虛擬進入說來解釋「使用」，A 的行爲並不構成使用電腦，因爲 A 的行爲就像是走到一棟屋子的門鎖前，但是沒有試著要打開該門鎖，所以沒有進入

---

24 Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2254 (2004); *see* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1619-20 (2003).

25 Kerr, *supra* note 24, at 1620-21.

26 *See* United States v. Ivonov, 175 F. Supp. 2d 367 (2001).

房子內部，也就沒有使用電腦。但是，採下達指令說的話，A 的行爲就已經構成了使用電腦。原因在於，A 已經向電腦下達指令，而電腦也遵照指令做了回應。換言之，該指令已經「進入」A 想要使用的該電腦中。

上述兩種說法都在試圖提出得以解釋「使用」的概念基礎。虛擬進入說是將電腦比擬爲現實生活中的一個空間，所以，必須是行爲人處於得以查看到電腦內部資訊的狀態，才算是進入到該虛擬的空間，也才算是使用該電腦。下達指令說則著重於電腦的運作方式，只要行爲人所下達的指令進入了電腦，就是使用了電腦。以現今電腦技術來說，學者對於虛擬進入說提出的質疑是，該主張可能使得偵查機關幾乎無法證明入侵電腦行爲的存在。詳言之，目前每一台連結上網際網路的電腦伺服器幾乎都有工作日誌檔（log files），以記錄所有進出該伺服器的活動。但是，入侵他人電腦的駭客也都會想盡辦法取得管理者權限，以刪除該工作日誌檔，以避免留下紀錄[27]。如果採虛擬進入說來定義「使用」，在沒有了工作日誌檔的情形下，檢警將幾乎無法證明行爲人曾經入侵過電腦。這也就是學者認爲應該採較爲寬鬆的下達指令說來定義「使用」的原因。也就是說，一旦行爲人對於電腦設備或是伺服器下達指令，即便沒有試著輸入帳號或是密碼，還是會構成使用電腦。至於行爲是否構成犯罪，則可以藉由行爲人是否有權使用來加以限縮[28]。

### 3.3.2 美國法院的判決

因 CFAA 的規定並不限制「使用」的行爲方式，再加上學界不認爲這裡有限制解釋的必要，所以在該國法院判決上，也涵括了相當多的行爲態樣。以下，便以美國聯邦及各州的相關判決爲例，說明其實務上所認定的「使

---

27 Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 212 (2000).

28 即使行為人的行為構成了「使用」，也不當然就構成了犯罪行為，因為 CAFF 所處罰的是「無權」或「越權」的使用電腦行為。只要行為人是有權使用，還是為法律所不禁。

用」態樣。要說明的是，因爲美國聯邦憲法採取聯邦制度，所以，各州都有著不同的電腦犯罪規定，但是，萬變不離其宗的是，各州的電腦犯罪與 CFAA 一樣，都有著無（越）權使用電腦罪的規定[29]。所以，在討論相關概念時，各州及聯邦的刑法規定及判決，都可以參考。

3.3.2.1 輸入帳號密碼

以坎薩斯州（Kansas）爲例，該州刑法同樣有無（越）權使用電腦罪[30]。*在 State v. Allen* 案中[31]，坎薩斯州最高法院認爲以數據機隨機亂數地撥打被害人電腦設備的行爲，並不構成使用他人電腦。詳言之，被害人西南貝爾通訊公司（Southwestern Bell Telephone Company）提供長途電話的服務，使用者以電腦的數據機撥打進該公司的電腦後，系統會顯示電腦已經回應了使用者的來電，並要求輸入密碼。系統同時也表明該電腦設備屬於西南貝爾公司的財產，以及使用該設備是受有管制的。在輸入正確的密碼後，使用者就可以利用該公司的長途電話服務。在這一個案件中，被告以數據機隨機撥打了被害人的電話號碼，並進到了要求帳號或是密碼的步驟，但是，法院認爲沒有證據證明被告曾經試著輸入帳號或是密碼，也沒有證據證明被告修改、毀損或複製任何被害人的資料。是故，坎薩斯州最高法院認爲，被告的行爲不構成使用被害人電腦設備[32]。

在類似的案件裡，如果行爲人試著輸入帳號及密碼，州法院就有不一樣的結論。華盛頓州（Washington）刑法所定義的「使用」是，直接或以電子數位的方式利用電腦設備[33]。在 *State v. Riley* 案中[34]，被告以數據機撥打了被

29 *See* Susan W. Brenner, *State Cybercrime Legislation in the United States: A Survey*, 7 RICH. J. L. & TECH. 28, ¶¶ 15-18 (2001).

30 K.S.A. 21-3755(b)(1).

31 State v. Allen, 260 Kan. 107, 917 P.2d 848 (1996).

32 *Id*. at 851.

33 RCW 9A.52.010(6).

34 State v. Riley, 121 Wash. 2d 22, 846 P.2d 1365 (1993).

害人的電腦設備，並試著輸入密碼以使用它的長途電話服務。雖然被告沒有成功，但是華盛頓州最高法院認爲，被告的行爲已經構成了使用他人電腦[35]。與 *Allen* 案不同的是，本案中的被告不只是撥打入他人的電腦設備，還試著要輸入帳號或密碼。這樣的事實上的差異，也造成了是否使用他人電腦的不同。

關於 *Allen* 案，實難判斷該法院所採的標準爲何。依照法院所認定的事實，無論是採虛擬進入說或是下達指令說，所得到的結論應該都是一樣的。換言之，按照虛擬進入說，因爲被告沒有處於可以得知被害人電腦內部資訊的狀態，就沒有構成使用電腦；按照下達指令說，因爲沒有證據可以證明被告曾經試圖著要輸入帳號及密碼，所以，其行爲並不構成使用電腦。不過，華盛頓州法院在 *Riley* 案中，則應該是傾向採取下達指令說[36]。也就是說，該州法院認爲，只要行爲人對於他人的電腦下達了指令，即便是沒有察看到電腦內的資訊，還是會構成使用電腦。

3.3.2.2 散布惡意程式（malware）

除了上述兩種常見的入侵電腦行爲外，美國聯邦法院也處理過一些比較不易判斷的案件類型。例如，散布電腦病毒、蠕蟲（worms）[37]或是木馬程式（Trojan Horses）。這一些程式進入到被害人的電腦內後，該散布行爲是不是會構成無權或越權使用他人電腦？對於這一個問題，美國聯邦第二巡迴法

35 *Id*. at 1373.

36 很明顯地，如果法院採取的是虛擬進入說，兩個案子的被告的行為都不會構成使用電腦。

37 蠕蟲指的是一種惡意程式（malware），藉由大量地自我複製，散布到與被感染電腦相連結的電腦上。因為蠕蟲的運作模式是「複製—散布」，所以，感染到蠕蟲的現象，大抵是單機的執行速度會變慢（因為每一台受到感染的機器都在不斷地複製蠕蟲），整個區際網路的速度也會嚴重地降低（因為連結到網路上的單機都在不斷地將蠕蟲傳送出去）。請參考 http://www.microsoft.com/taiwan/security/articles/virus101.mspx。

院持肯定意見。在 *United States v. Morris* 案中[38]，被告在政府機關、大學及軍事機構的網路上，散布電腦蠕蟲。法院認爲，對於感染到該蠕蟲的電腦，被告都構成了無權使用[39]。雖然法院並沒有明確地表示其採取虛擬進入說或是下達指令說。不過，從判決的結果來看，法院似乎認爲無論是採取哪一說，結論並不會有所不同。詳言之，如果採下達指令說，在對被害電腦下達安裝該蠕蟲程式的命令時，就已經構成了使用電腦；如果採虛擬進入說，在安裝完蠕蟲後，也就已經完成了使用電腦行爲。

3.3.2.3 掃描通訊埠（port scan）

掃描他人電腦通訊埠（port scan）的行爲，是不是會構成使用電腦？需要解釋的是，掃描通訊埠是指對於他人電腦發出一系列的訊息，藉以測試哪一些網路服務是開放的。在得知後，就可能可以藉由這一些開放的通訊埠進到該電腦系統內瀏覽檔案或使用特定程式。如果採虛擬進入說，通訊埠掃描就像是走到一棟房子前，並動手試著去開每一扇門及窗戶，以確認它們有沒有上鎖，但是並沒有進入到屋內。美國喬治亞州的聯邦地方法院認爲，掃描他人電腦通訊埠[40]，並不構成存取他人電腦的行爲。這樣的結論，似乎是因爲法院採取虛擬進入說來判斷被告是不是有使用被害人電腦。因爲被告掃描通訊埠的行爲並不會使其得以進入到系統內部，並得知其內部資訊，所以，

38 United States v. Morris, 928 F.2d 504 (1991).

39 關於這一個部分，本案主要的爭點在於，被告究竟是「無權」或是「越權」存取他人電腦。被告主張，因為其有權使用該電腦及網路，所以其散布蠕蟲的行為，應該只構成越權存取他人電腦。但是，法院審理後認為，被告固然有權使用所就讀的學校的電腦，但其並沒有權限使用其他機構的電腦，所以，其行為仍然構成無權使用。*Id*. at 509-11.

40 Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901 (N.D. Ga. Nov. 7, 2000). 每一台連結上網際網路的電腦都有 65,535 個通訊埠，而通訊埠可以想像為一個個進出該電腦的大門。有一些大門專門用以收送網頁的資訊，有一些則是用以收發電子郵件，不一而足。在資訊安全的領域，掃描通訊埠的行為多半是用以找出沒安全措置的埠，以利後續的入侵行為。

其行為並不構成使用電腦。但是，如果法院是以下達指令說為基準，那麼在被掃描電腦會回傳訊息時，被告的行為有可能就構成了 CFAA 的使用電腦。

## 3.4　無（越）權

依照 CFAA 或是其他州的規定，並不是只要有使用電腦（access a computer），就會構成犯罪。必須是「無（越）權」使用電腦，才會有入侵電腦罪的問題。所以，接下來的問題是，什麼是「無（越）權」？更進一步地問：「什麼是『有權』」？

使用一定電腦的權限，不外乎是來自於：1.取得帳號及密碼（code-based restrictions）、2.契約授權（contract-based restrictions），以及 3.社會規範（norms-based restrictions）[41]。詳言之，授權人可以利用帳號密碼的方式授權特定人使用電腦的軟硬體設備。例如，學校的教職員及學生必須要先取得電子郵件帳號及密碼，才能夠使用學校的電子郵件信箱及其他的資源。再者，在同一個團體內，不同的帳號可以使用的軟硬體資源及接觸到的資訊也可能有所不同。例如，電算中心的職員可以接觸到的軟硬體及資源就可能比一般的學生為多。以 *Morris* 案為例，本案中的被告就是利用了郵件收發軟體的漏洞、其他程式及系統的漏洞，以及試誤程式[42]得知帳號及密碼來入侵他人的電腦及植入蠕蟲[43]。被告的行為就是典型的以未取得或不當取得帳號及密碼的方式來使用他人電腦[44]。

---

41　*See* KERR, *supra* note 18, at 44-46.

42　「試誤程式」指的是，利用電腦程式大量並快速地對於需要輸入密碼的電腦或網頁送出驗證密碼的指令。該電腦程式通常會帶有一個字典檔，內含有大量的字彙，程式所送出的密碼便是來自於此。如果所設定的密碼包含於字典檔中，又有足夠的時間，試誤程式就可以找到進入該系統所需要的密碼。這也就是為什麼在設定密碼時，會建議使用者選取無意義的字彙或是混用阿拉伯數字及羅馬數字。

43　*Morris*, 928 F.2d at 506.

44　類似的案例，還可以參考 Sherman & Co. v. Salton Maxim Houseware, Inc., 94 F. Supp. 2d 817 (E.D. Mich. 2000). 在本案中，法院也認為利用試誤程式得知他人密碼的行為

除了因爲取得帳號及密碼而有權使用電腦外，使用電腦的權限，也可能來自於契約。換言之，使用者可能必須要同意遵守某些規範或協議後，才可以使用一定的電腦服務，如電子郵件或是參訪特定的網站。這樣的觀念可以從美國聯邦第一巡迴法院的 *EF Cultural Travel BV v. Explorica, Inc.*[45]中，更深入地瞭解這一個觀念。

本案並不涉及實體法上的爭議，其所爭議的問題是法院應否核發禁制令[46]。在本案中，EF 以 Explorica 違反 CFAA 爲由，要求法院向 Explorica 發出禁制令。Explorica 提出異議，但是聯邦第一巡迴法院駁回。本案主要的事實是，Explorica 的副總裁 Gormley 在從 EF 離職前，曾經簽有保密協定。不過，Gormley 仍利用其在 EF 服務期間所知的網頁代碼，以電腦程式大量地抓取 EF 在網頁上所標示的旅遊行程價格，以與 EF 競爭。EF 發現了 Gormley 的行爲後，隨即以其行爲違反 CFAA 爲由，聲請聯邦地方法院向 Explorica 核發禁制令[47]。EF 主張，Gormley 的行爲已經構成了越權使用他人電腦。地方法院核准了禁制令，Gormley 不服，向聯邦第一巡迴法院提出異議，法院駁回[48]。根據 CAFF 18 U.S.C § 1030(e)(6)的定義[49]，越權指的是：「有權使用他人電腦，但是利用該權限取得（或是變更）無權取得（或是變更）的電腦資訊。」[50]根據這一個規定，巡迴法院認爲，原告（EF）有證明被告

是典型的入侵電腦行為。

45 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

46 這一個案件的性質屬於民事程序，而不是刑事。之所以在電腦犯罪章節中涉及民事爭執是因為 18 U.S.C. § 1030 同時包含了刑事犯罪與民事上的損害賠償（18 U.S.C. § 1030(g)）。感謝審稿人的提醒，讓作者有機會在這一個地方補足說明。

47 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d at 579-80.

48 *Id*. at 580.

49 18 U.S.C. § 1030(e)(6): “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]”

50 *Explorica, Inc.*, 274 F.3d at 582.

（Gormley）越權使用他人電腦的可能，所以，法院判定被告的抗告無理由[51]。

另一個類似的聯邦案件是 *America Online v. LCGM* 案[52]。在本案中，維吉尼亞州東區聯邦地方法院認爲，違反電子郵件信箱使用協議的行爲，可以構成越權使用電腦罪[53]。本案中的被告 LCGM 利用電腦程式，大量地蒐集 America Online（AOL）用戶的電子郵件信箱，並利用其在 AOL 註冊的帳號，大量散布電子郵件。該聯邦地方法院認爲，被告的行爲已經違反了 AOL 的電子郵件服務使用協議，所以構成了越權使用他人受有保護的電腦，並進而取得 AOL 的資料（其用戶的電子郵件信箱）[54]。

# 4. 討論及建議

以上討論了我國及美國關於入侵電腦罪的規定及相關判決。從上述可以知道，兩國間對於入侵電腦有不同的規定，法院的態度也有所不同。以下，就兩者進行比較及分析，並提出 CFAA 中值得我國參考的地方。

## 4.1 電腦的定義

何謂「電腦」？立法者在我國刑法第 358 條中並沒有予以定義。遍尋其他可能供作參考的法規後，也似乎沒有立法或是行政上的定義[55]。在我國實

---

51 *Id.* at 585. 這一個判決所採的立場是，違反契約授權使用他人電腦將構成越權行為，但是，也有不少判決採取相左的看法。例如，在 Commonwealth v. McFadden, 850 A.2d 1290 案中，賓西法尼亞州法院就認定，雖然警察有權使用警用電腦系統，但是如果警察在該系統上散布不實的消息，將構成無權使用電腦罪，而不僅是越權。

52 America Online v. LCGM, 46 F. Supp. 2d 444 (E.D. Va. 1998).

53 *Id.* at 450.

54 *Id.*

55 這裡是在法務部全國法規資料庫裡，以「電腦」作為關鍵字，在「法規內容」欄中搜尋的結果。

務上則認爲，公司處理業務及客戶資料的電腦系統[56]、公務機關裡處理差勤紀錄的系統[57]、電子郵件服務系統[58]、銀行處理帳戶間轉帳的系統[59]，以及個人筆記型電腦[60]都是刑法第 358 條所包含的行爲客體。從上述判決可以推知，我國實務上對於電腦應是採相當寬鬆的標準。不過，要注意的是，因爲法條上對於行爲方式的限制，所以，本條所保護的電腦，僅及於設有帳號密碼、有保護措施或有系統漏洞的電腦。

與我國刑法第 358 條的規定及相關判決相比較，CFAA 雖然對於電腦加以定義，但是其定義也是相當寬鬆。這也就是爲何美國法院在判決時，會將警方無線電系統認定爲是 CFAA 的「電腦」。美國立法及司法機關會採取這樣的態度的原因無他，其目的應該是使 CFAA 足以因應快速變化的科技。詳言之，在現今生活中，電腦扮演了越來越重要的角色，無處不可見其存在。小至人手一隻的行動電話或是 PDA（personal digital assistant，個人數位助理），大至提供網際網路或通訊服務的設備，都可以見到電腦的蹤影。這一些電腦設備都有進行快速運算的能力，也都擔任大量處理重要資訊的任務。如果在立法上或解釋上加以限縮，可能會造成將有保護必要的電腦設備排除在刑法保障外的情形。是故，本文認爲，將電腦的定義留予實務解釋，讓其

56 如台灣高等法院台南分院 96 年度上訴字第 153 號判決（審判長楊明章），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

57 如台灣高等法院 95 年度上訴字第 765 號判決（審判長劉景星），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

58 如台灣高等法院 96 年度上訴字第 1127 號判決（第四庭，蔡秀雄審判長）及台灣高等法院 95 年度上訴字第 2674 號判決（審判長吳昭瑩），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

59 如台灣高等法院 95 年度上訴字第 4568 號判決（審判長鄭文肅），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

60 如台灣高等法院 94 年度上易字第 1418 號判決（審判長許國宏），司法院法學資料檢索系統：http://jirs.judicial.gov.tw/Index.htm。

有較大的適用及因應的空間，不失妥適的立法方式[61]。至於面臨到沒有保護必要的情形，儘可交由其他的構成要件要素、違法性或有責性來處理。即便立法者在日後想明文「電腦」的定義，基於上述原因，也可以參考 CFAA，予以較爲寬鬆的定義。

## 4.2 刑法第 358 條無須限定入侵電腦的行為方式

與 CFAA 的規定相比較後可以知道，我國刑法第 358 條限定了入侵電腦的行爲方式，但是，CFAA 只規定「無（越）權使用電腦」。本文認爲，關於行爲方式的設計，CFAA 是比較穩妥的規定。就修法建議來說，本文建議可以刪除掉「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」等不必要的規定，而保留「無故入侵」即可。對於「無故入侵」的解釋，CFAA 的「無（越）權使用」或可供作參考。

### 4.2.1 應刪除「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」的規定

刑法第 358 條及 CFAA 的入侵電腦罪中，最大的差異之一，應該是前者限制了入侵的行爲方式，但是，後者採取了較爲開放的條文規範。就結論來說，本文認爲，CFAA 是比較妥適的立法，值得我國在修法時參考。詳言之，以刑法第 358 條的文字來看，並不是所有的入侵電腦行爲都會構成本條的犯罪，只有以「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」等列舉的方式「入侵」電腦才會構成刑法第 358 條的犯罪[62]。這三個行爲以外的入侵電腦，在罪刑法定原則的限制下，都不

---

61 觀察我國相關的立法可以知道，並沒有法律直接針對「電腦」予以定義。可能的原因是，如同本文所主張地，立法者有意將這一個部分留由司法機關在實際的案例中解釋。

62 學說上有認為，「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」表彰了刑法第 358 條所保護的行為客體是「電腦中的登入控制程式」。李茂生，「刑法新修妨害電腦使用罪章芻議（上）」，台灣本土法學雜

能以該條相繩。也正因爲立法者使用了這樣的文字，只要不「入侵」電腦，單純的「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」也不會構成刑法第 358 條的犯罪[63]。

從立法論來檢視本條的結構，輸入密碼帳號、破解保護措施或是利用系統漏洞應該是蛇足的規定。我們認爲，「無故入侵」的字眼，已經足以表彰該行爲的可非難性；僅規定「無故入侵」也可以涵蓋更多的行爲類型，使實務運作更有彈性。雖說適用上可以透過對於上述三種行爲的解釋來因應科技的快速進步及各種不同的入侵方式，但是，文字的解釋不免有其極限。再者，訂定這三個法定的行爲方式，可能只是徒增適用上的困擾。舉例來說，以詐騙的方式使電腦系統換發一組新的帳號密碼給入侵者，其再利用該帳號及密碼進入該系統，屬於「無故輸入他人帳號及密碼」，或是「破解使用電腦之保護措施」，抑或是「利用系統之漏洞」？實務上便曾經在「無故輸入他人帳號及密碼」，或是「破解使用電腦之保護措施」兩者間擺盪。爲了避免不必要的解釋問題，本文建議，應該刪除刑法第 358 條中對於入侵方式的限制，保留「無故入侵」作爲構成要件行爲即可。

再者，從立法理由來看，立法者以被入侵「電腦系統之安全性」作爲刑法第 358 條所保護的法益。以之爲前提的話，就不應該過度限縮構成要件行爲類型。亦即，只要是危害了「電腦系統之安全性」的入侵行爲，都應該是得以本條處罰的對象，就可以發動刑罰權加以處罰。至於所使用的方式爲何，應該不是重點。刑法第 358 條侷限在三個法定的行爲方式，可能反而使

---

誌，第 55 期，頁 235-247（2004 年 2 月）。本文認為，無論是輸入帳號密碼、破解保護措施或是利用系統漏洞，除了是用以描述所入侵的電腦的特性外，同時也限制了刑法第 358 條的所得處罰的行為態樣。

63 不同的見解，請參照柯耀程，「刑法新增『電腦網路犯罪規範』立法評論」，月旦法學教室，第 11 期，頁 117-129（2003 年 9 月）。學者的看法主要是希望藉由將本罪定性為舉動犯來強化對於使用電腦的安全性，而有其見地。然而，本文認為，這樣的解釋實與條文的文字有間。

得國家無法回應部分的入侵電腦的行爲。

立法論上的另一個問題是，本條並不罰未遂行爲。也就是說，即使行爲人嘗試輸入他人帳號密碼、破解使用電腦的保護措施或利用電腦系統的漏洞以入侵他人電腦，但是最後因爲自己的「學藝不精」而未能得逞，也不會構成任何犯罪。就文義的解釋來說，這樣的結論應屬當然，但是，恐怕與一般人民的感受有所落差。這裡的問題，除了出在本罪沒有未遂規定之外，也可以歸因於本罪不當地限縮了入侵的行爲方式。是故，如果可以在修法時刪除掉行爲方式的限制，那就可能可以藉由「無故入侵」的解釋，涵蓋各種嘗試或已經影響「電腦系統之安全性」的行爲[64]。

以入侵電腦的技術來說，過於繁複且不必要的構成要件設計，會讓行爲人得以逍遙法外。詳言之，心思縝密且技術高超的電腦犯罪行爲人在以連線的方式入侵電腦後，多半都會在刪除系統中的工作日誌檔後才從系統離開。在這一種情形下，如果沒有其他的證據，檢警很難證明行爲人曾經「入侵」過該電腦系統[65]，更遑論證明行爲人是以「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或是「利用電腦系統之漏洞」的方式入侵電腦。如果行爲人是直接使用了被害人的電腦，就更不容易遺留下犯罪的痕跡，檢警也將更難證明行爲人的入侵方式爲何。

最後，從比較法來看，刑法第 358 條的構成要件行爲，應該是「無故」「入侵」電腦便爲已足。CFAA 所規範的行爲態樣主要是「無（越）越權使用（access a computer without authorization, or exceeding authorized access）電腦」，條文中並沒有限制要以什麼樣的方式「使用」。這樣的規範方式使得條文可以容納更大的解釋空間，並使得實務得以解決各種不同的案件類型。與我國相比較，CFAA 的規定顯然更有彈性。如果能將「無故輸入他人帳號

64　關於刑法第 358 條，另一個值得考慮的修法方向就是參考美國 18 U.S.C. § 1030(b)，處罰未遂的入侵電腦行為，以更周全地保護電腦系統的安全及抗制各樣的電腦犯罪行為。

65　Sinrod & Reilly, *supra* note 27, at 212.

密碼」、「破解使用電腦之保護措施」或是「利用電腦系統之漏洞」刪除，而以「無故」「入侵」他人電腦作爲構成要件行爲的話，「無故」「入侵」的一個可以參考的解釋方向就是 CFAA 所規定的「無（越）權」「使用」。

### 4.2.2 入侵

在判斷「入侵」電腦的標準時，從立法者所使用的文字及相關的判決可以知道，刑法第 358 條偏向採取虛擬進入說，而不是下達指令說。從該條所使用的文字是「入侵」電腦，語義上有行爲人進入一定（虛擬）空間，並處於得窺知該空間內狀態的意思。再者，現行條文裡的「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」或是「電腦系統」也都可以比擬爲保護該空間的措置。是故，立法者所欲處罰的行爲，應該是進入到電腦系統內部的行爲。換言之，單純向受保護電腦下達指令，但是沒有窺知其內部資料的行爲，應該不構成入侵電腦罪。是故，在我國現有判決裡，構成犯罪的行爲人都是已經進入到電腦系統內，並處於對該系統內部資訊隨時可接觸的狀態。這樣的解釋，當然合於法條的文義，也比較不會遭致處罰層面過廣的批評。不過，值得留意的是，如果採取虛擬進入說來解釋入侵，可能會面臨證明困難的問題。詳言之，如果當入侵電腦的行爲人，在入侵後一併刪除系統內的工作日誌檔，檢察機關可能將沒有其他足夠有利的證據證明行爲人曾經進入該系統內部。再者，在本條目前欠缺未遂規定的情形下，可能無法處罰確實曾經試圖進入，但是最終失敗的行爲。

相較之下，下達指令說可以避免上述的這一些問題。首先，依照下達指令說，只要檢察機關可以證明行爲人確實對於電腦系統下達指令即可。這樣一來，即便是行爲人湮滅了曾經進入到系統內部的證據，檢察機關還是可以經由證明其確實曾經無故向該電腦系統下達指令，來將之繩之以法。再者，以下達指令說來解釋入侵，也可以涵蓋那一些試圖進入電腦系統，但是最終失敗的行爲。是故，本文認爲，以下達指令說來解釋「入侵」應該是較爲穩妥的作法。不過，下達指令說最大的問題在於其可能與一般社會大眾對於

「使用」或是「入侵」電腦的觀念有一定的落差，所以多數人可能也無法接受以下達指令說作爲基準所作成的判決結果。在這一個情形下，本文認爲，比較折衷的方式應該在修法時，增訂本條的未遂處罰規定，並且以虛擬進入說來解釋入侵，以因應上述的各種已經影響電腦系統安全性的事實類型。如此一來，也可避免指令進入說在觀念上不容易被接受的問題。

### 4.2.3　無故

並不是所有的「入侵」電腦行爲都需要以刑罰來處罰，本文建議，在刪除「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」後，可以以「無故」的要件要求來限縮刑法第 358 條的處罰範圍，以避免本條落入過於嚴厲的情形。至於如何解釋「無故」，似可參考 CFAA 的入侵電腦罪裡的「無（越）權」的規定及相關判決。

典型的「無故」，當屬未取得帳號密碼或超過帳號密碼授權範圍。這一個部分，應該沒有太大的疑義。這也是刑法第 358 條所處罰的行爲方式之一。至於「無故」，應該是指沒有正當理由的存在。有無正當理由，則可以從法律明文的規定或習慣是否許可來解釋[66]。可以進一步思考的是，當行爲人違反契約授權而使用電腦時，是不是會構成無故入侵電腦罪？換言之，違反民事上使用電腦的約定時，會不會構成刑法上的「無故」？

從上述 *Explorica* 案或 *LCGM* 案的判決可以知道，美國的法院大抵認爲，行爲人違反契約條款使用電腦時，就已經是超過原有契約的授權範圍，因而可能構成越權使用他人電腦罪。Gormley 所違反的是與 EF 間的保密協定，LCGM 所違背的則是與 AOL 間的電子郵件服務使用協議。兩案中的約定都屬於民事上的契約。從 CFAA 的條文文義來說，被告使用電腦的行爲的確都是超越了契約所授權的範圍，而屬於「無（越）權」使用被害人電腦。

但是，值得深究的是，這樣適用法條的結果，等於是國家以刑法來保護

---

66　甘添貴，體系刑法各論（第一卷），頁 305（1999）。

當事人在契約上的權利。的確，部分超越契約約定的使用電腦行爲可能確已達到得以刑法處罰的程度。但是，是不是所有契約雙方當事人對於使用電腦的規定都重要到必須以刑法強制？如果這一個答案是肯定的，那麼是不是就意味著契約當事人的一方，可以藉由契約條款的約定，來決定刑罰權的發動與否？是不是也代表著，契約的一方可以利用刑罰作爲契約內容的擔保？這樣的結果是否妥適？再者，如果契約的內容不公平，是不是還可以認定爲是越權使用電腦？[67]本文認爲，是否超越契約授權範圍使用電腦固然可以作爲無（越）權使用電腦的參考因素，但其不應該是僵化的絕對標準。實務上在判斷類似案件時，應該綜合考量到契約的條款內容、契約雙方的締約能力、行爲人使用電腦的目的、行爲態樣以及所接觸到的資訊內容等條件，用以判斷行爲人是否確實「無故」入侵被害人的電腦。如果一律將所有超越契約授權的使用電腦行爲認定爲是無故入侵電腦，那可能將產生處罰範圍過廣的問題。

## 5. 結論

刑法第 358 條是入侵電腦罪的規定。該條文限定了只有以「無故輸入他人密碼」、「破解使用電腦之保護措施」或「利用電腦系統之漏洞」的方式才能構成本罪。再者，本條除了沒有未遂規定外，也沒有針對「電腦」作成立法上的定義。

分析我國近來的判決可以知道，實務上認爲，「無故輸入他人帳號密碼」「入侵他人之電腦」指的是，行爲人在輸入帳號密碼後，進入到他人系統內部，並處於隨時可取得內部資訊的狀態。輸入帳號密碼，進入他人系統取得業務及客戶資料、刪除系統內部資料、進入他人的電子郵件信箱或進入銀行系統盜領他人存款，都構成這一個型態的入侵電腦罪。除此之外，法院也認爲，親自使用他人電腦，同樣有可能構成這裡的入侵電腦罪。按照目前

67 *See* KERR, *supra* note 18, at 60-64.

的法院態度，如果行爲人輸入的不是原有的設定數值，而是利用變更原帳號密碼的方式入侵電腦，就應該構成「破解使用電腦之保護措施」的入侵電腦罪。

CFAA 對於「電腦」有所定義，但是相當寬鬆。法院在認定上，也是採取相當有彈性的態度。其對於入侵電腦罪的行爲規定則是「無（越）權使用」。關於「使用」，美國學者提出了「虛擬進入說」及「下達指令說」兩個不同的判斷基準。虛擬進入說是將電腦比擬爲現實生活中的一個空間，行爲人要構成使用電腦，必須是其處於得以查看到電腦內部資訊的狀態。下達指令說則著重於電腦的運作方式。依該說，只要行爲人對電腦下達指令，就算是使用了電腦。美國法院則認爲，試圖輸入帳號密碼或散布惡意程式等行爲，都已經構成了 CFAA 的使用電腦。至於使用電腦的權限，美國學界指出，可能來自於 1.取得帳號及密碼、2.契約授權，以及 3.社會規範。美國法院則認爲，違反離職保密協定或電子郵件服務使用協議的行爲，都可能構成這裡的「無（越）權」。

與 CFAA 比較後，我們對於我國刑法第 358 條提出數個立法及解釋上的建議。首先，對於電腦的定義保留立法上的空白，應屬正確，因爲，如此一來，本條應該更能夠處理快速發展的資訊科技。就算是想要在法條上明定電腦的意義，也應該如 CFAA 一般，採取較爲開放的態度。再者，就本條的行爲方式來說，本文建議，應該刪除「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」及「利用電腦系統之漏洞」等蛇足的規定，僅以「無故入侵」作爲本條的構成要件行爲即可。「無故入侵」已經足以表彰該行爲的可非難性，也能更避免解釋適用上的困擾。以「無故入侵」作爲刑法第 358 條的行爲，也可以涵括更多「影響電腦系統之安全性」的行爲態樣。這樣的法條設計，也可以避免實務上操作的困難。如果修法時能以「無故入侵」作爲刑法第 358 條的構成要件行爲，CFAA 的「無（越）權使用」的相關判決及學理可以作爲解釋上的參考。

在解釋「入侵」時，本文建議，可以沿用與現在法條用語比較接近的

「虛擬進入說」，但是，應該增訂本罪的未遂規定。至於「無故」，指的應該是沒有正當理由的存在。有無正當理由，則可以從法律明文的規定或習慣是否許可來解釋。特別要注意的是，當使用電腦的權限是來自於契約時，要特別注意契約本身是否合理，以避免契約之一方不當地以刑罰來強制他方履行不公平的契約條款。

# 參考文獻

## 中文書籍

甘添貴，《體系刑法各論（第一卷）》，瑞興出版，台北（1999）。

## 中文期刊

李茂生，〈刑法新修妨害電腦使用罪章芻議（上）〉，《台灣本土法學雜誌》，第 55 期，頁 235-247，2004 年 2 月。

柯耀程，〈刑法新增「電腦網路犯罪規範」立法評論〉，《月旦法學教室》，第 11 期，頁 117-129，2003 年 9 月。

## 其他中文參考文獻

「淫照事件／陳冠希友人：他家有暗門，私藏影帶和照片」，ETtoday，2008 年 2 月 5 日，ETtoday 網站：http://www.ettoday.com/2008/02/05/11445-2228182.htm（最後點閱時間：2008 年 3 月 28 日）。

## 英文書籍

KERR, ORIN S., COMPUTER CRIME LAW (2006).

## 英文期刊

Bellia, Patricia L., *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35 (2001).

Bellia, Patricia L., *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004).

Brenner, Susan W., *State Cybercrime Legislation in the United States: A Survey*, 7 RICH. J.L. & TECH. 28 (2001).

Kerr, Orin S., *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

Sinrod, Eric J. & Reilly, William P., *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000).

## 其他英文參考文獻

MCAFEE VIRTUAL CRIMINOLOGY REPORT (2005), http://www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf.