

第十一講

資訊犯罪



本講義內容主要摘錄自：

❖ 劉江彬《資訊法論》，臺灣大學法學叢書（四三），三民書局，1988年1月，二版之第六章。



目次

❁ 一、前言

❁ 二、電腦犯罪的探討

❁ 三、電腦犯罪的形態

1. 電腦破壞

2. 竊用電腦

3. 濫用電腦

4. 安全系統之破壞

目次

❁ 四、電腦犯罪之特性

1. 破壞力大
2. 智慧型犯罪
3. 白領犯罪
4. 不易察覺
5. 偵查困難
6. 犯罪之無知
7. 量刑不重
8. 具有魅力

目次

❀ 五、電腦犯罪與適法性

1. 實體法上之困難
2. 程序法上之困難

❀ 六、個案例舉：

1. 美國法院判例

- (1973) Equity Funding Case
- (1978) U.S. v. Sampson
- (1979) Rifkin Case
- (1982) People v. Weg

2. 師濤案 (2007)

參考文獻

- 一、楊富強〈電腦犯罪〉，發表於《建構健全資訊 社會之政策與法制研究》中之第十章，行政院經濟建設委員會出版，經社法規研究叢書003，1989年10月。
- 二、Donne B. Parker, 《Fighting Computer Crime》, Scribner, New York, 1983, 此書中有許多有趣的個案。
- 三、Johnson & Nissenbaum, 《Computers, Ethics & Social Value》, Prentice Hall, 1995, Chapter 2 : Crime, Abuse, and Hacker Ethics.

參考文獻

❖ 林宜隆：《網路犯罪：理論與實務》，第三版，中央警察大學，2009

❖ 吳清吉、林宜隆等：

《資訊素養與倫理》高中二版，2009，9月

《資訊素養與倫理》國中二版，2009，9月

《資訊素養與倫理》國小二版，2009，9月

臺北市政府教育局編印

前言



前言

- ❖ 隨著文明進步，犯罪的情節也水漲船高。
- ❖ 電腦與網路的普及、方便與效用提供了新的犯罪機會。
- ❖ 資訊犯罪性質不同於一般的犯罪，如暴力、詐欺、脅迫……



電腦犯罪的探討

電腦犯罪之研究

❁ 電腦犯罪 (Computer Crime) 之研究，以立法及個案為主：

- ❖ 利用電腦作為犯罪工具。
- ❖ 電腦犯罪之定義、特徵、構成犯罪之要件與量刑之輕重等，仍為研究上的新課題。
- ❖ 現行法律對電腦犯罪之適用問題，仍待研究
- ❖ 防治電腦犯罪之立法政策，仍待研究。

電腦犯罪的觀點

❁ 對電腦犯罪有不同的觀點：

- ❖ 廣義的觀點：包含與電腦有關的犯罪行為，應以獨立法規加以規範。
- ❖ 狹義的觀點：電腦犯罪雖不應與須與一般的犯罪相混，但須與電腦直接有關。
 - 如：以密碼盜取存款，只能認為是偷竊、詐欺；與電腦犯罪無關。

什麼是腦犯罪？

❁ 電腦犯罪指以電腦為工具，使自己獲益或他人受損之犯罪行為。

❖ 如：以電腦為工具，從事欺騙、偷竊、隱瞞…以企圖獲得財物、商業、財產、或勞務之利益者。

➤ 電腦為犯罪工具範圍極廣，可視之為：刀槍、打字機、通訊設備…

❁ 對電腦本身造成威脅者。

❖ 偷竊電腦之軟、硬體

❖ 損壞電腦

❖ 以電腦為勒索目標

電腦犯罪

- ❁ 電腦犯罪不應以本身獲益為要件，因實務上有許多犯罪損人不利己。
 - ❖ 最常見之電腦犯罪為電腦安全系統之破壞。
 - ❖ 電腦犯罪通常不涉及身體上之暴力，故屬白領犯罪。
- ❁ 英、美、法對電腦犯罪並不全視為刑事犯罪。
- ❁ 有些電腦「犯罪」只是侵權行為（tort）。

電腦犯罪的形態



破壞電腦(computer sabotage)

- ❖ 以非法方式，故意破壞電腦硬體或軟體，而使電腦系統失效之行為。
- ❖ 若考慮資料的價值及法益的損失，均不同於傳統的毀損罪。

竊用電腦(theft of services)

❁ 竊用電腦是指使用了「無權使用的電腦」包括：

❖ 使用時間之外的使用

❖ 使用業務之外的使用

❖ 竊線 (wiretapping)

➤ 經由同一線路，竊用他人之電腦。

濫用電腦 (computer abuse)

- ❖ 濫用電腦是指以電腦為犯罪工具，利用電腦的特性以達到詐欺、侵佔等各種犯罪行為。
- ❖ 財產犯 (property crime) 或財務犯 (finance crime) 多屬此類犯罪。
- ❖ 在網路上散佈猖獗的惡意程式，俗稱電腦病毒，亦屬此類犯罪。



濫用電腦

濫用電腦的分類

✿ 從技術上，濫用電腦可分為下列方式：

❖ 輸入操縱(manipulate)

❖ 程式操縱

❖ 檔案資料操縱

❖ 輸出操縱

❖ 網路操縱

程式操縱

- ❁ 程式操縱是指用電腦程式從事不法的行為，其中寫成套裝軟體程式的形式而普遍散佈者，稱為惡意程式 (malicious code)。
- ❁ 惡意程式通常是透過媒介或網路感染或被植入電腦，從事破壞電腦的運作。
 - ❖ 惡意程式是我們厭惡的、應設法避免的

惡意程式



了解惡意程式

❁ 惡意程式可由下列的途徑了解：

❖ 感染和散播途徑

❖ 程式生態：

➤ 包括撰寫程式的語言，儲存的場所，使用的檔案、工具、巨集等，

❖ 造成傷害的程度和範圍

惡意程式的性質

❁ 依其性質，惡意程式可區分為

❖ 電腦病毒 (virus)

- 指會將本身複製並散播到其他場所 (程式或檔案) 的惡意程式。換言之，它具有感染的性質，一如病毒，有破壞能力。
- 以被動方式散播，但可跨應用程式散播，如利用各種文字編寫程式及檔案。
- 自1980年代即有電腦病毒 (在**DOS**上)，1993年後微軟的**Windows**上爆發各種病毒，防毒軟體應運而生。

惡意程式的性質

❖ 木馬程式 (Trojan)

- 指善於偽裝，躲藏在正常軟體工具內的惡意程式
- 主動散播自己，也會以被動方式散播。
- 有破壞能力

❖ 電腦蠕蟲 (worm)

- 指會將本身複製，並在區域網路(如資料分享夾) 或網際網路(如電郵)上遊走散播的惡意程式。
- 主動散播自己，區域網路愈大，散佈的數目愈多。
- 蠕蟲通常無破壞能力，但是它常與電腦病毒或木馬程式結合產生混合型的病毒。

檔案資料操縱

- ❖ 垃圾郵件 (spam mail)
- ❖ 資料拼圖
- ❖ 社交欺詐工程 (social engineering)
 - ❖ 利用訪問、電話、電郵或任何方式騙取帳號及密碼
 - ❖ 電郵夾帶惡意程式
 - ❖ 誘騙點選連線，或提供工具、檔案、圖片為幌子夾帶惡意程式

安全系統之破壞

- ❁ 電腦安全系統指：運用技術方法和人事管理程序，以保護電腦軟體、硬體及檔案資料等各方面資產的方法之系統。如：
 - ❖ 竊取程式、資料
 - ❖ 解破安全密碼
 - ❖ 可能涉及隱私權的侵害，商業秘密的侵害、智慧財產權的侵害。
- ❁ 此為廣泛之概念，少有單獨成立的情況。

結語

The background image is a landscape photograph. On the left, there is a dense cluster of tall, thin trees with light green and yellowish foliage, suggesting early spring. In the foreground, there is a body of water, possibly a pond or a slow-moving stream, with some green grass and reeds along the edge. In the background, across the water, there is a green lawn and a building with a dark roof. The sky is a clear, pale blue.

本講結束

謝謝聆聽