刑事證據法則對於電子證據適用之研究

The Application of Criminal Evidentiary Rules to Electronic Evidence

研 究 生：朱帥俊　　Student : Chu-Shuai Chun

指導教授：劉尚志　博士　　Advisor : Dr. Shang-Jyh Liu

吳巡龍　博士　　Dr. Hsun-Lung Wu

國　立　交　通　大　學

管理學院碩士在職專班

科技法律組

碩士論文

A Thesis

Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Technology Law

July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

刑事證據法則對於電子證據適用之研究

研究生：朱帥俊　　指導教授：劉尚志　博士
吳巡龍　博士

國立交通大學

管理學院碩士在職專班科技法律組

中 文 摘 要

我國於民國九十二年施行修正之刑事訴訟法，其中證據法則變動幅度甚大，尤其引入英美法系證據法則觀念，爲我國刑事證據法制之研究，帶來更多討論的題材與思考之方向，誠值對之加以關注與研究。另一方面，各種形態之數位資料如電子文件、數位照片、數位圖片、數位影像、數位聲音等，近年來大量成爲庭呈證據。然而因爲對於資訊領域的不熟悉，刑事證據法則對於電子證據之適用及範圍一直甚感陌生。因此分析及描述電子證據之各項物理性質與特徵，期能充分瞭解如何適用種刑事證據法則，爲本論文首要目標。

此外，對於刑事證據法則引入英美法系之觀念甚多，與我國固有證據法制或實務見解能否相容，於適用於電子證據時，應否加以調整或排除，誠有必要藉此機會一併分析之。尤其電子證據具有國際性、共通性，因此藉由對國外立法例與案例之分析研究，期能瞭解我國適用與調整之方向，此乃本文第二目標。

本論文首先以電腦運作及電磁紀錄之儲錄方式爲出發點，從資訊發展與人類接觸之沿革，討論電子證據如何挑戰傳統證據法則，且爲因應上開衝擊，國際組織及外國（以美國爲主）之證據法則如何因時、因地制宜或折衷協調。於歸納整理各國立法趨勢之後，進一步針對美國案例中處理電子證據之經驗，討論電子證據與傳統證據法則應有之平衡點與

調整處。

最後，本文擬從電子證據之物理特徵與國外立法方向及案例經驗爲經緯，剖析我國現行證據規則及實務案例之良弊得失，嘗試整理出各刑事證據法則下對電子證據之適用與調整等原則，以供我國現行刑事司法實務及未來刑事立法於處理電子證據之參考。

The Application of Criminal Evidentiary Rules to Electronic Evidence

Student : Chu-Shuai Chun Advisor : Dr. Shang-Jyh Liu
Dr. Hsun-Lung Wu

Institute of Technology Law
College of Management
National Chiao Tung University

ABSTRACT

The revised Code of Criminal Procedure went into effect in Taiwan in 2003, with many changes in the evidentiary rules. The introduction of the concept of evidentiary rules under the Common Law System brought many issues for further discussion in the new Code of Criminal Evidence System. On the other hand, digital data in various forms such as electronic documents, digital photos, digital pictures, digital images, digital voice recording, etc. have been increasingly admitted as court evidence in recent years. However, the applicability and scope of electronic evidence in the Code of Criminal Evidence has been an uncharted territory for many. Therefore, the paper aims at analyzing the nature of electronic evidence in order to fully understand how the evidentiary rules apply.

In addition, the new evidentiary rules have incorporated many concepts from the Common Law System. It is worthwhile analyzing whether or not these concepts are compatible with our existing evidentiary system or practical views and if they require adjustments or exclusion when applied to electronic evidence. As electronic evidence is international and common in the nature, we need to take reference from international cases to determine the future directions of such application and adjustments. This constitutes the second objective of this paper.

This paper begins with an analysis of computer operations and electromagnetic records. From the evolution of information development and its interaction with human beings, the paper then discusses how electronic evidence has challenged the conventional evidentiary rules. It goes further to analyze how the evidentiary rules of international organizations and foreign countries (mainly the United States) responded to these challenges. After delineating the legislative trends of various countries, the balance point and necessary adjustments between electronic evidence and conventional evidentiary rules are explored based on how electronic evidence was treated in US cases.

Finally, the paper analyzes the strengths and weaknesses of the existing evidentiary rules and practical cases in Taiwan based on the physical characteristics of electronic evidence as well as the legislative trends of foreign countries and international cases. The paper attempts to formulate principles for the application and adjustments of electronic evidence to the evidentiary rules of various criminal codes for the reference of how Taiwan's criminal justice system treats electronic evidence in practice and future legislation.

誌　　謝

回顧多年來的求學生涯，很慶幸自己能夠有機會就讀交大科技法律研究所，交大科法所由劉國際長慧眼卓具的創立，結合了科技與法律、學術與實務、一般生與在職生共同的學習環境，把科法所維繫成為一個大家庭，讓大家在這裡彼此關懷、相互鼓勵，對於師生與同學之間，都有很大的成長與互動空間，在此衷心的感謝劉國際長。

此外，要感謝指導教授吳巡龍老師與劉國際長，吳老師在證據法學上的精深造詣，學理與實務兼具，讓學生獲益良多；尤其老師為人謙沖平和，虛懷若谷，身體力行回饋社會，讓學生立志日後以老師為榜樣，為社會略盡棉薄之力；劉國際長對於電子商務、科際整合的的觀念，大大的提升了學生的視野，跳脫了法律人以管窺天的促狹，並學會以更宏觀的視野檢討法律問題及制度。謝謝口試委員林志潔老師對於論文架構的提點，老師提出的許多問題是學生從未想過的，更謝謝林老師鼓勵學生要勇於提出自己的見解與看法，口試時真是感到非常震撼與受用。學生何其有幸，能得到三位老師的指導與指正，也在此向三位老師耗費心神審閱學生不成熟的論文而致歉。

東吳大學法律系劉宗榮老師、陳子平老師、盧文祥老師，分別是學生民法、刑法及電腦法的啟蒙恩師，因為三位老師馴牛般的耐心教誨，學生才得以一窺法學殿堂深邃嚴謹之美，深深謝謝三位老師。科法所倪貴榮老師、王文杰老師、王敏銓老師、鄧文炳老師、李貴敏老師、蔡明誠老師、鍾鳳玲老師、邵瓊慧老師、劉宏恩老師、洪瑞章老師對學生知識以及待人接物的啟發，讓學生衷心感謝。

學生自就業以來，歷任臺中、桃園、板橋、臺北、桃園及金門地方法院檢察署，蒙受各地檢署所有長官、學長姐及同仁提攜指教，讓學生深感幸運，在此致上由衷謝忱。科法所謙信學長、佳麟學長、三元學長、重君學姐、學倫學姐、兆國學長、于珊學姐、佳蒨學姐、慶鴻學長以及同窗紹斌學長、惠錦學姐、瑞琴學姐、惠如學姐、欣蓉學姐、世柱、育竹、俊英、宏節等一干好友的切磋砥勵，相互加油打氣，是我完

成學業以及完成論文的原動力。

感謝先父先母、岳父母以及舍妹甚珍、大姐、偉文、慧儀、韋志的關心與支持，以及寶貝女兒小彩、內人惠慈一路的陪伴與幫助，幾度在遭遇挫折與打擊，難以為繼時，幸虧有家人的關心、鼓勵與支持，才讓我得以完成學業。

學生一生之中，得到所有長輩、家人與好朋友的照顧與幫助，未一一敘明者尚有萬千，在此一併致上最誠摯的謝意。

目　　錄

圖目錄

表目錄

刑事證據法則對於電子證據適用之研究

The Application of Criminal Evidentiary Rules to Electronic Evidence

第一章　緒論

1.1　研究動機與目的

我國刑事訴訟法自民國十七年之後公布施行之後，直至民國九十二年間，變動幅度不大。惟期間國內外刑事思潮變更迅速、人權保障、訴訟平等與程序正義等趨勢尤為國際間所日益關注，學術界及實務界對於刑事訴訟法中被告人權之保障、證據及訴訟程序等規定漸有修正之意見。為符合當代刑事國際思潮、保障人權、維護訴訟平等，我國乃大幅度修正刑事訴訟法，並於民國九十二年二月六日經總統公布，同年九月一日施行。其中刑事證據法則變動幅度甚大，尤其引入許多英美證據法則觀念[1]，為我國刑事證據法制之研究，帶來前所未有之新氣象，增加了許多討論的題材與思考之方向，誠值對新制證據法則加以關注與研究。

[1] 此次就證據法則修改的重點包括：檢察官舉證責任之具體化、違法取證之證據排除、傳聞法則之建立、準備程序與審判期日明確區分、詰問法則之明定、明定共同被告之證人地位、鑑定留置及鑑定採樣程序、證據保全程序之建立、簡式審判程序之新訂及自訴強制律師代理制等。參見蔡碧玉，「2003 年刑事訴訟法新刑事訴訟法簡介（一）」，法務通訊，第 2137 期第 4 版，92 年 5 月 29 日。蔡前司長於擔任法務部檢察司長時值逢該次刑事訴訟法修正，其間協調折衝，倍極辛勞。該次刑事訴訟法修正通過後，蔡前司長撰寫「2003 年刑事訴訟法新刑事訴訟法簡介（一）至（九）」，分別刊載於法務通訊第 2137 期（92 年 5 月 29 日）、第 2138 期（92 年 6 月 5 日）、第 2139 期（92 年 6 月 12 日）、第 2141 期（92 年 6 月 26 日）、第 2143 期（92 年 7 月 10 日）、第 2145 期（92 年 7 月 24 日）、第 2147 期（92 年 8 月 7 日）、第 2149 期（92 年 8 月 21 日）及第 2150 期（92 年 8 月 28 日）。該文對於立法背景、討論過程及爭議問題論述詳明，堪屬研究該次修法極具參考價值之文獻。

另一方面，拜電腦科技發展及網際網路浪潮席捲全球，電腦與網際網路之應用對吾人傳統生活方式帶來極大的改變，隨著資訊技術之進步，每個人生活、工作、教育及娛樂等各方面之資訊均得以數位化之方式保存；數位技術也加快資訊傳遞、交換之速度，利用數位方式傳遞資訊，或在使用電腦設備之際留下數位資訊，均成為生活中不可避免之事項，因此常有趨勢專家稱現在的生活為數位化生活。

根據中外調查報告顯示，在一九九八年至二○○三年間，美國 B2B 電子商務市場規模由四百八十億美元成長至一兆三千億美元，消費者利用網際網路交易之金額則由三十九億美元成長至一千零八十億美元；且在一九九五年至一九九七年間，資訊科技對美國經濟成長之貢獻度則超過其中三分之一，在一九九七年至一九九八年間，資訊科技在美國經濟成長所占比率由百分之四．二成長至百分之八．二，幾近兩倍；另在一九九四年，使用網際網路之人口數約為三百萬人，到了一九九八年，每週至少使用網際網路之人口數超出一．四七億，至二○○○年網際網路之用戶已激增至三．二億，及至二○○五年則達到七．二億之高峰。[2]另外，二○○三年全球 B2C（Business to Customer，企業經營者與個人間）電子商務市場規模達二千零三十七億美元，預計至二○○六年則可成長至五千六百十八億美元，二○○二年至二○○三年 B2C 市場規模成長百分之五十二點四，二○○三年至二○○四年則成長百分之四十六[3]。

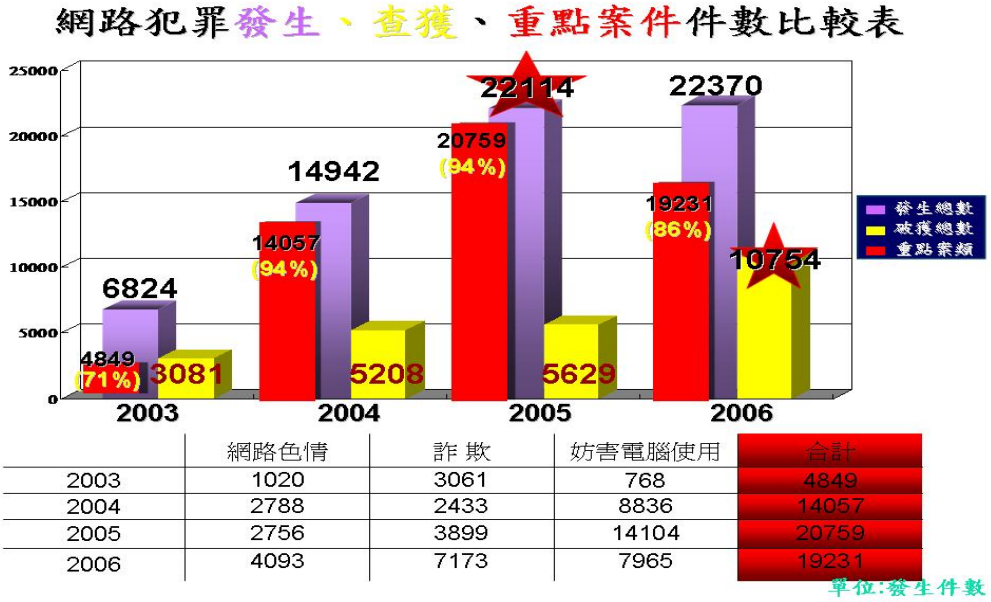
---

[2] *See*, Jeffrey J. Norton & Noah P. Barsky, "*MANAGEMENT CONTROL ISSUES AND LEGAL CONCERNS SURROUNDING BUSINESS-TO-BUSINESS E-COMMERCE: TRANSACTIONS IN THE ELECTRIC UTILITY INDUSTRY*", University of Pittsburgh-The Journal of Law and Commerce, 2002
（http://www.lexis.com/research/retrieve?_m=92af733708afc0d3b48b63d4ebc4d335&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-SkAl&_md5=84d52e74afde656f7d7ce0da4e539c21）,last visited on June 8, 2007.

[3] 林世懿，國內電子商務經營現況及發展趨勢分析，頁 4-5，92 年度電子商務環境整備及企業對個人電子商務推動計畫，經濟部商業司。

我國上網人口，根據經濟部之統計，自民國八十五年六月，連網戶數僅有三十六萬左右的人口；但是到了八十七年底，上網人數即突破三百萬；今（九十六）年第一季，我國有線寬頻戶數已達四百五十一萬戶，經常上網人口為九百九十萬。[4] 至於網路犯罪相關案件之成長，自民國九十年的四,八四九件，到了民國九十五年已經成長到一九,二三一件，其中民國九十四年更一度達到二萬件之多。[5]

圖 1-1　2003 年至 2006 年網路犯罪數量統計



	網路色情	詐欺	妨害電腦使用	合計
2003	1020	3061	768	4849
2004	2788	2433	8836	14057
2005	2756	3899	14104	20759
2006	4093	7173	7965	19231

資料來源：內政部警政署刑事警察局科技犯罪防制中心

由上開數據觀察，不論個人或商業，使用電腦與網路越普及，利用數位方式交流意見或從事相關犯罪之數量也因此而大幅增加，無論是發生爭端須要解決，或對於犯罪須要進行告訴、訴追時，各種形態之數位資料如電子文件、數位照片、數位圖片、數位影像、數位聲音等皆有可能成為庭呈證據之一種，由被害人或當事人之一方提出於法院。

[4] 關於我國上網各項數據資料，請參見資策會網站 http://www.find.org.tw/find/home.aspx?page=many&cal=上網人口&p=1,last visited on June 8, 2007.

[5] 統計資料來源：內政部警政署刑事警察局科技犯罪防制中心。

表 1-1　實務上常見以電腦或網路為犯罪媒介之犯罪類型

	篇　　章	條　文　或　犯　罪　類　型
刑法	第 2 章	第 109 條、第 110 條、第 111 條 以電腦或網路竊取及洩漏國防機密
	第 4 章	第 121 條、第 122 條 貪瀆犯罪相關資料、公文、影像及帳冊均以電子化方式留存
	第 7 章	第 153 條 在網路上教導犯罪方法或言論，煽惑他人犯罪
	第 9 章	第 165 條 湮滅數位化、電子化之刑事證據
	第 10 章	第 169 條 以電子郵件或打字黑函方式犯誣告罪
	第 12 章	以掃描及彩色列印等數位化方式偽造貨幣
	第 13 章	以掃描及彩色列印等數位化方式偽造有價證券
	第 15 章	以掃描及彩色列印等數位化方式偽造文書
	第 16 之 1 章	第 235 條 以電腦及網路製造、播送或販賣猥褻文字、影像及圖畫
	第 21 章	以電腦或網路犯賭博章各罪
	第 28 章	網路恐嚇
	第 29 章	網路妨害名譽、商譽、誹謗
	第 30 章	妨害國防以外秘密、竊取數位化之個人資料
	第 32 章	網路買賣交易詐欺、不正利用電子設備詐欺、信用卡詐欺等
	第 33 章	網路恐嚇取財（網路千面人事件）
	第 35 章	毀損他人電磁記錄
	第 36 章	電腦犯罪專章各罪

各特別法	期貨交易法	地下期貨公司類型案件
	證券交易法	空中證券交易所對賭類型案件
	洗錢防制法	透過網路銀行及跨國匯兌洗錢
	兒童及少年性交易防制條例	違反第 29 條張貼性交易訊息
	著作權法	以電腦及網路違反著作權法
	商標法	以電腦及網路違反商標法
	毒品危害防制條例	以電腦及網路聯絡販賣毒品消息
	貪污治罪條例	貪瀆犯罪相關資料、公文、影像及帳冊均以電子化方式留存
	槍砲彈藥刀械管制條例	以電腦及網路聯絡販賣槍械消息、或教導如何製作爆裂物
	組織犯罪防制條例	透過網路募集不良幫派成員
	政府採購法	犯罪相關資料、公文、影像及帳冊均以電子化方式留存
	電信法	以數位化方式從事違反電信法之犯罪
	電腦處理個人資料保護法	以數位化方式違反個資法及侵害隱私之犯罪
	銀行法	透過網路銀行及跨國匯兌洗錢、不法吸金等
	藥事法	以電腦及網路聯絡販賣偽藥、禁藥等消息

資料來源：本文整理

惟由於此等電子證據與傳統證據之性質不同、調查及認定須要專業的瞭解與判斷，因此對於電子證據之採納與否？如何定性？如何合法有效的加以蒐集及保全？證據能力及證明力標準如何？傳統各種證據法則有哪些可以應用在電子證據上？又有哪些須要調整？種種課題均有待進一步加以探討，亦有必要建立檢證之標準。[6]國內相關領域的討論中，大多集中在電子證據意義之探討，或蒐證、保全及鑑識程序，對於電子證據在民、刑事證據法則之適用與調整，鮮有論及[7]，遑論聚焦於電子證據在刑事訴訟程序中產生爭議及其解決方案等問題，準此，本文將研究重點集中於新制刑事證據法則中對電子證據之適用與調整，探討電子證據所面臨之刑事證據法則相關問題。

1.2 研究範圍與研究方法

1.2.1 研究範圍

電子證據從單純不具評價性質之數位資料開始，到發生爭端時如何蒐證、保全及驗真，甚至於在訴訟活動中如何採認與排除等，都牽涉複雜之證據法則，因此本文在設計研究流程時，鑒於篇幅有限，也避免模糊研究焦點，自然不得不對研究範圍加以限制。

---

[6] *See,* Orin S. Kerr, "*DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE*", 105 Colum. L. Rev. 279, January, 2005.
（http://www.lexis.com/research/retrieve?_m=6e7ca8e2547e33442a8e42472e865062&docnum=100&_fmtstr=FULL&_startdoc=91&wchp=dGLbVtb-zSkAl&_md5=a7047eb8cf3f598de2e9450f7d7aa777）, last visited on June 8, 2007.

[7] 稍早僅有林一德，電子數位資料於證據法上之研究，臺大法研所碩士論文，2000 年 1 月，對此領域有加以討論，惟當時我國刑事訴訟法尚未修正，刑事證據規則尚屬舊制。刑事訴訟法於民國 92 年修正後，有錢世傑，「論刑事證據上關於數位資料證據資格之檢討」，月旦法學雜誌第 143 期，2007 年 4 月，對領域有加以論。錢世傑前揭文係由新制刑事訴訟證據法則之觀點討論電子證據之先驅，復以作者具完整實務經驗與資訊背景，故甚具參考價質。

本文是從界定電子證據之物理特性及其法律性質之概念為出發，再以此二者為基礎，以我國新制刑事訴訟法制下證據法則之認定流程為縱向主軸，以比較法差異論述及實務案例之導入為橫向，最後在結論中總結全文，以供國內就相關爭議問題研究參考。

新制刑事訴訟制度中電子證據之討論，涉及證據法則之概念及面對於電子證據加以調整之雙面關係，本文所著重者為證據法則對於電子證據適用與調整之層面，就爭議問題處理角度亦然。因此關於電子證據於網路交易安全、企業危機蒐證、刑事鑑識方面之問題，諸如：使用者安全機制、危機處理規劃、搜索、扣押步驟、證據保全規範、數位鑑識標準流程、數位鑑識專家證人之引進等刑事偵查層面之問題，原則上並非本文討論之範圍。又我國法制下刑事案件之當事人，除檢察官與被告外，亦有可能由自訴人充之，惟本文之研究對象主要在檢察官與被告（含辯護人）等面向，合先敘明之。

1.2.2　研究方法

本文在研究方法上，在文獻的蒐集上，除與研究主題相關之國內、外相關書籍、報紙、期刊和學術論文等書面資料外，也包括經由網際網路搜尋相關之線上新聞、官方公告、公私機構之電子文章與資料。

針對各章節，就所蒐集的資料，綜合採用歸納分析法，針對論文題目擬定相關章節之討論問題，據以作為建構本論文大綱之基礎及立論依據，對於各章節之主要議題所涉及之法律現象，則將現行法制及蒐集所得之資料，依邏輯的程序和規則，作歸納、演繹與綜合分析，以期找出問題所在，以為進一步探討解決方法與完善之道。

又由於電子證據之認定與採納為世界各國均須面對之一環，國際上之發展遠早於我國，因此在論述過程中，將運用比較法之角度，探求外國或國際上之法律體制之差異，以提高問題意識之產生，當然為加深研究之深度，有必要完整掌握各相關之法律之源起、變革與發展趨勢，本文也會運用歷史方法作為研究手段，以期對問題之掌握更為深入。

1.3 論文架構

本研究之架構如后：

第一章　緒論

除了就本文之研究動機與目的進行說明，對於研究範圍與研究方法也加以界定與釐清，以確立本文之方向。另對每章之研究重點以概述之方式敘明，使讀者對本文各章節所要討論之中心問題及所涉及之法律爭議，有初步之印象。

第二章　電子證據之意義

隨著電腦及數位設備的普及應用，數位資料當作法庭證據者日增，因此有必要對於本文希望電子證據所待涵攝之範圍，亦即其概念先加以釐清，並更進一步演繹出電子證據之意義。另外，針對電子證據物理上之性質有必要先與討論分析，待此等電磁紀錄及其運作方式經各個角度的解構與描述之後，讀者始得瞭解傳統證據法則，對於電子證據應行調整之方向為何。再就電子證據之法律性質討論，應當屬於新型態之證據類型抑或以傳統證據類型，蓋不同之刑有不同之證據調查方法，不得不注意。另外，對於文獻上各種電子證據之種類與區別實益加以檢討與分析。

第三章　電子證據立法方向與範圍

電子證據，尤其是透過網際網路傳遞之電子證據，因為具有跨國性、無國界性，故而甚受國際組織與世界各國重視，且甚早

即訂出相關規範，並經常加以修訂。是以本章嘗試分析前開組織及國家對於電子證據所作之規範與指南，介紹主要國際組織及內國立法例，將之析離出相關原理原則，作為進一步判斷電子證據應適用何種證據法則之依據。經檢討之後認為電子證據基於功能等同、平等對待等原則，在證據能力、證據力、傳聞法則、書證類型、驗真法則及最佳證據法則等範圍受到關注及討論。

第四章　電子證據之刑事證據能力與證明力

我國刑事證據觀念上雖有證據能力與證明力之觀念，惟因為過往刑事訴訟法未對此加以規定，因之證據能力與證明力亦未受到詳細的討論與關注，甚至實務上有將二者誤會混淆者。[8]因此本章由刑事證據能力及證明力之區辨為出發，討論電子證據在證據能力與證明力層面之適用。

第五章　刑事證據法則對於電子證據之適用

本章針對新制刑事證據法則對於電子證據之適用與調整，一一做出檢討。亦即以訴訟中證據檢驗組織成過濾式架構，討論證據進入法院時所面臨之證據法則。此外，對於電子證據適用於各證據法則，實務見解、攻防策略之商榷，亦一併加以討論。另外，我國新制刑事證據法則受美國影響甚深，而美國實務界對於

[8] 例如臺灣高等法院 88 年度上易字第 4209 號刑事判決：「五、按告訴人之告訴，係以使被告受刑事訴追爲目的，是其陳述是否與事實相符，仍應調查其他證據以資審認（最高法院 52 年台上字第 1300 判例參照），由上述調查所得各情，可知借用一百二十萬元之目的並非欲塗銷 167 號八十五萬元之抵押權，而所貸得之一百二十萬元經被告收受後扣抵前述費用所剩六十餘萬元應已交付告訴人吳月，至於該 167 號第二順位抵押權塗銷文件在被告手中，其非債權人保留無實益拖延四年才塗銷被告辯稱其不再經營代書因疏漏而忘記辦理。應爲實情，乃因有此疏忽致而有本案之告訴。又告訴人林○○、林○○、林○○、林○○爲吳○之子，並未參與貸款手續，所述均配合吳○之言，均乏補強證據，證據能力尚有不足。」；最高法院 89 年度台上字第 6963 號刑事判決：「我國現行刑事訴訟制度，關於證據之蒐集與調查，並不限於法院及檢察官始得爲之，司法警察官或司法警察亦有協助檢察官偵查犯罪之職權，其依法定程序所製作之詢問筆錄，即屬刑事訴訟法第 165 條第 1 項所規定，可爲證據之筆錄之一種，法院依直接審理方式，顯示於公判庭加以調查，並經言詞辯論者，仍有證據能力（本院 71 年臺上字第 6140 號、72 年臺上字第 1203 號判例參照）。原審以林○○、吳○○在苗栗調查站之詢問筆錄，經依法踐行調查證據程序後，採爲證據之一，即與證據法則無違。」

電子證據之檢討亦累積出相當之案例，因此一併加以介紹與分析，希望對於我國電子證據之採納適用有所助益。

第六章　結論

總結全文，闡明本文研究所得，以加深讀者印象，並期以本文研究結論能為我國刑事證據法制對電子證據是適用與調整等問題之解決提供些微參考價值。

第二章　電子證據之意義

2.1　電子證據概念之形成

第一部以電力驅動的電腦是在一九四五年十一月於美國製造出來的[1]，隨後電腦的發展日新月異[2]，隨著電腦大量製造，而且體積縮小、操作便利、功能強大，應用層面也隨之廣泛。電腦產生及應用日廣之後，人類面臨了更進一步的問題，就是此類電腦機具設備所產生的紀錄、文件，應否被採納為證據。

電腦是採用「0」與「1」二進位計算制為資料之紀錄方式，所謂二進位制是利用電學開關之觀念而來。電學中以「通電」代表「開（On）」，亦即是「1」;「不通電」代表「關閉（Off）」亦即是「0」。電腦是藉著在磁性或光學載體上以「通電（1）／不通電（0）」之電子運作，達到在紀錄載體上「刻畫（紀錄）」資訊之目的，例如在鍵盤上輸入人類理解的文字「A」、「B」，電腦內中央處理器（Central Process Unit，CPU）就會將之轉譯並在紀錄載體上刻畫出「1010」來代表「A」、刻畫出「1011」來代表「B」。這些磁性紀錄，遇到人類需要理解、解讀時，會再透過中央處理器轉譯為人類可以理解感知之形態，例如還原成文章、圖畫、影像，顯現在電腦螢幕上，或透過印表機印出成紙本。

---

[1] 自古以來西方科學家就一直希望製造出能夠代替人類計算的設備，有許多概念、草圖，甚至於實際設備被提出來，但是成效不彰。後來雖然有以齒輪爲基礎製造出來的計算機械能夠取代煩瑣精密的計算工作，也就是類比式計算器具，但是逐漸無法應付工業及社會的需要。美國在 1943 年 4 月間開始了電子式計算機具的製造，一直到 1945 年 11 月才完工。當時是以真空管的通電與斷電來代表「1」與「0」的訊號，以二進位制來計算，然後轉化爲人類可以順利理解 10 進位制數據。

[2] 關於電腦發展的歷史，可參考 Martin Campbell-Kelly、William Aspray 著，梁應權、胡頂立譯，我的名字是電腦（Computer：A History of the Information Machine）一書，天下遠見出版股份有限公司，臺灣，1999 年 6 月。該書對於電腦發展的歷史有詳細的介紹及圖片。

隨著數位化（Digitial）、電子化時代的來臨，任何傳統類比化（Analog）[3]形式的資料都可能、也可以被轉換成數位化[4]的形式來保存。尤其在數位儲存媒體如硬碟、USB 介面隨身碟及光碟片儲存容量越來越大、價格越來越低之際[5]，資料以數位化的形式來保

[3] 類比式是日常生活中最常見的資料保存與顯示形式，通常指的是連續性的資料，例如聲音的波形、電壓的高低圖形等。類比是一種在「量」上的連續型變數。例如就聲音而言，當我們說話時，嘴巴所產生的空氣壓力，就是一種連續型變數，被我們的耳朵截聽到，將這樣的空氣壓力轉變成耳鼓的振動，透過神經傳輸，傳到腦部，就成爲我們所聽到的聲音。參見 http://cmca.mis.ccu.edu.tw/book/IEC/Questions/IEC_QCH15.doc 、http://www.sunfar.com.tw/ecsfweb/dictionary/dirdesc.aspx?dict_no=D0081, last visited on June 8, 2007.

[4] 電腦利用數位化的方式儲存資訊，要將一般的資料儲存在電腦中之前，必須先將資料數位化，而日常生活當中常見的資訊大多是類比式，所以我們將許多資訊存放在電腦之前，要先做類比到數位的轉換 (analog-to-digital conversion)。將不論文字、音樂、影像等形式的資料轉化爲 2 進位制數位形式，再放於電腦記憶單位內。參見 http://mypaper.pchome.com.tw/news/joehank/3/1265941409/20060311184056/ 、http://www.sunfar.com.tw/ecsfweb/dictionary/dirdesc.aspx?dict_no=D0081, last visited on June 8, 2007.

[5] 電腦儲存媒體容量增加的速度與價格滑落的速度同樣令人驚訝。講述電腦歷史的書籍多半提到 IBM 公司剛推出電腦硬碟時，容量僅有 5MB，體積比一個 007 手提箱還大，價格更是高昂，非專業實驗室無資力購買。筆者剛接觸電腦時，硬碟主流規格僅爲 340MB，未幾，市面上出現 1GB 容量的硬碟，電腦玩家激動萬分，彷彿救贖降臨。民國 87 年間，IBM 推出 10GB 硬碟，數量稀少，價格高昂，當時筆者任職桃園地檢署，與現已爲主任檢察官之同事張檢察官紹斌利用午休或下班時間自桃園市驅車前往中壢市中原大學外電腦材料行購買，多次向隅後始購得，當時二人喜悅之情，至今猶印象深刻。現在 IDE 介面硬碟已演進至 SATA Ⅱ介面，轉速由 5400 轉進步至 10000 轉，又因爲垂直寫入技術成熟，容量已突破 1TB（以資訊規格而言，1TB 相當於 1024GB；以商業規格而言，1TB 相當於 1000GB），價格亦非常合理。可錄式光碟片推出之際，爲 CD-R 規格（640MB，74 分 24 秒），最初 1 倍速燒錄機價格達 10 萬元，空白光碟片每片百元，每燒壞一片光碟片，等於多一片百元杯墊。現在 CD-R 燒錄機幾近淘汰，空白片價格在 5 元至 8 元之間，隨後 DVD 光碟（最小容量 4.7GB）、藍光（Blue Ray）光碟（最小容量 23.3GB）、HD 光碟（最小容量 15GB）容量倍速成長，燒錄機及空白片價格亦非常合理，日前報載臺大已研發出容量達 150GB 的奈米光碟。筆者接觸電腦時，大磁碟片已經被淘汰，小磁碟片容量爲 1.44MB，後來有廠商嘗試推出 2MB 容量磁碟片，接著 IOMEGA 公司推出 100MBZIP 磁碟片及 250MBZIP 磁碟片。其後又有 ORB 公司推出介於硬碟與磁碟片間，容量爲 750MB 之磁碟片。此外，尚有容量分別爲 230MB 與 640MB 之磁光碟片 MO。然而隨著 USB 介面，以 Flash Ram 所製造之隨身碟興起後，迅速取代各種規格及容量之磁碟片，成爲攜帶式儲存媒體主流。750MB 之 ORB 磁碟片雖然力圖振作，試圖整合桌上型電腦推廣至醫療院所，惟成效不彰。軟式磁碟片與 Flash 隨身碟發展的歷史，恰好與企管理論中「龍捲風暴」之理論相合。

存的趨勢就益加增多[6]。過往被當成證據被提出於法院的各種類比形式的資料，如紙本文件、聲音、影像等，在現代社會中被以數位化形式製造、保存或轉換者日益增加，也因此數位化的資料如電子文件、數位照片、數位錄音、數位影像等在訴訟活動中被提出的機會也就日益增多。職是此故，各國刑事訴訟中據以檢驗證據資料、認定犯罪事實之各項證據法則均有必要針對電子證據加以討論適用之可能性及範圍；反之，當數位資料充為訴訟上之證據時，亦必須討論應遵守證據法則之何種規範及受檢證之步驟。

電腦的紀錄及以數位化形式所保存的資料，究竟該如何定義，才能更進一步的討論這類型資料在刑事證據規則上適用的可能性。因為此類數位形式的資料產生的年代甚晚，並且在保存方式、載體、方式及適用範圍上均日新月異、一日千里、變化萬端，不論專家學者及中外司法實務工作者長久以來均聚訟盈庭，惟對之迄無定論。因此如何對電子證據妥適定義，亦應是最先應被界定的問題。

2.2　電子證據之意義

電磁紀錄或數位資料，在未經提出於訴訟中為證據之前，並不能以電子證據視之；必須是要該電磁紀錄或數位資料充為法院之證據時，才屬於電子證據。

電子證據正式的名稱及定義，中外專家學者及司法實務上迄無定論，已如上述。即便如最早討論此類證據之美國，亦無一定的用語及意義。文章及判決中常見者如 Computer Evidence[7]、

[6] 例如許多公司行號、便利商店保存監視錄影畫面，以往都是以 VHS 錄影帶來保存類比化的影像資料，現在則多半直接以可錄式光碟片或硬碟來保存數位化形式的影像資料。可錄式光碟片之規格亦從 CD-R 演變成容量更大的 DVD-R。過往法院及檢察署開庭，均以錄音帶形式進行錄音及保存，現在各地方法院檢察署已改成以 CD-R 可錄式光碟片即時錄音及錄影；各地方法院則以數位錄音並儲存伺服器中，隨時可供調取。

[7] *See,* e.g. Adam Wolfson,„ *Electronic Fingerprints": Doing Away with the Conception of Computer-*

Electronic Evidence[8]、Digital Evidence[9]、Log-file Evidence[10]、Computer-based Evidence[11]、Computer-produced Evidence[12]、Computer-generated Evidence[13]、Computer-stored Evidence[14]、Computer-related Evidence[15]、Computer Out/Printout Evidence[16]等等名稱。[17]在中文資料中，對此類證據

Generated Records as Hearsay ", Michigan Law Review,,104 Mich. L. Rev. 151，October, 2005. (http://www.lexis.com/research/retrieve?_m=9f19dd1806e9a1092816c5ad374dfdff&docnum=2&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=0b5b9a81266a707b24d5b3c65975de5c）, last visited on June 9, 2007.

[8] *See,* e.g. Alan M. Gahtan, Electronic Evidence, Thomson Canada Limited, 1999；Computer Crime and Intellectual Property Section Criminal Division（CCIPs）, Department of Justice, U.S.A., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 2002。Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 一書亦有網路版，可在 CCIPs 網站上取得，見 http://www.cybercrime.gov/s&smanual2002.htm, last visited on June 8, 2007.

[9] *See,* e.g. Mark N. Cooper, "*SYMPOSIUM BRIDGING THE DIGITAL DIVIDE: EQUALITY IN THE INFORMATION AGE: INEQUALITY IN THE DIGITAL SOCIETY: WHY THE DIGITAL DIVIDE DESERVES ALL THE ATTENTION IT GETS* ", Yeshiva University Cardozo Arts & Entertainment Law Journal, 20 Cardozo Arts & Ent LJ 73，2002。（http://www.lexis.com/research/retrieve?_m=4f3cd7388765bec5777ba57b8c108b2f&csvc=bl&cform=2758.-2&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=46ba71a77de00048855980bf6abb526a）, last visited on June 9, 2007.

[10] *See*, e.g. Norman A. Harris v. United States Department of Agriculture and Linda Jones（124 F.3d 197,（6th Cir. 1997））。

[11] *See,* e.g. The People v. Timothy Ray Ward,（037718,Court of Appeal of California,5thAppllate District 2002）。

[12] *See,* e.g. United States v. Vincent Franklin Bennett（363 F.3d 947; 2004 U.S. App. 64 Fed. R. Evid. Serv.（Callaghan）467,9th Cir. 2004）。

[13] *See,* e.g. People v. Holowko（486 N.E.2d 877,878-89（Ill. 1985））、United States v. John L. Fueero（106 F. Supp. 2d 921;U.S. Dist.（2000））。

[14] *See*, e.g. *Id* People v. Holowko；Mark A. Johnson，" *Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?* ", 75 Marq. L. Rev. 439, rquette Law Review, 1992. (http://www.lexis.com/research/retrieve?_m=a5c3fbd567f542231242d3453315e87a&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=12afbda7a64c850f82910de2d5178d60) , last visited on June 9, 2007.

[15] *See,* e.g. United States v. Criminal Triumph Capital Group, Inc. ET AL., 211 F.R.D. 31; 2002 U.S. Dist., United States District Court for The District of Connecticut,2002。

[16] *Supra* note 13。

[17] 由各項文獻來觀察，在各種英文定義中，不同領域之專家會有不同切入角度而對電子證據作不同的名詞詮釋，例如在電腦犯罪偵防領域極具盛名的電腦專家 Eoghan Casey，因爲其爲理工背景出身，因此其在大著 Digital Evidence And Computer Crime 以及 Investigating Child

亦有數位證據[18]、數據電文證據[19]、電子證據[20]、電腦（犯罪）證據[21]、電腦數據證據、電子數位資料[22]、電子數據證據[23]、電子文件證據[24]、網路（犯罪）證據[25]等等。不同的詞彙對於電子證據所涵攝範

Exploitation and Pornography （Elevsier Academic Press, 2005）等書中，以 Digital Evidence 一詞來表示此類證據「Digital Evidence: Encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.」Eoghan Casey, Digital Evidence And Computer Crime, 2nd Ed., P.668, Academic Press, 2004。而法律專家如 Alan M. Gahtan 在此領域之大作 Electronic Evidence 及美國司法部（Department of Justice，DOJ）電腦犯罪及智慧財產犯罪部門（Computer Crime and Intellectual Property Section Criminal Division，CCIPs）所出版的 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 一書中，則均以 Electronic Evidence 一詞來表示此類證據。

[18] 書籍方面如如高大宇、王旭正、資訊密碼暨建構實驗室，資訊安全，博碩文化，2003 年 6 月；王旭正、柯宏叡、ICCL-資訊密碼暨建構實驗室，資訊與網路安全安全，博碩文化，臺北，2007 年 3 月；潘建民，網路入侵電腦犯罪及其證據之研究，國防管理學院法律研究所碩士論文，民國 94 年 6 月。論文方面如林宜隆、陳蕾琪，「數位證據對刑事司法的衝擊」，2002 年全國科技法律研討會，交通大學科技法律研究所，2002 年 11 月；蔡震榮、黃玥婷，「論數位證據之證據力」，刑事法雜誌，第 49 卷第 2 期，民國 94 年 4 月。惟在大陸，用語上習慣採用「數字證據」，如王芳，「數字證據的性質及相關規則」，法學雜誌，2004 年第 8 期，2004 年 8 月。

[19] 如劉滿達，「論數據電文的證據價值」，法學雜誌，1999 年第 8 期，1999 年 8 月；高富平、俞迪飛，「電子紀錄等同於紙面證據的解決方案—兼論《電子簽名法》的局限性」，法學，2004 年第 11 期，2004 年 11 月。

[20] 書籍方面如謝名冠，網路行爲犯罪之研究，臺灣臺北地方法院檢察署 89 年度研究報告，90 年 1 月；何家弘主編，電子證據之研究，法律出版社，2002 年 7 月；劉品新主編，美國電子證據規則，中國檢察出版社，2004 年 5 月；劉品新，中國電子證據立法研究，中國人民大學出版社，2005 年 5 月；皮勇，刑事訴訟中的電子證據規則研究，中國人民公安大學出版社，2005 年 3 月。論文方面如王亞林、范勝兵，「論民事電子證據」，科技與法律季刊，2002 年第 1 期，2002 年 1 月；常怡、王健，「論電子證據的獨立性」，法學，2004 年第 3 期，2004 年 3 月。

[21] 如蔡震榮、張維平，「電腦犯罪證據之研究」，刑事法雜誌，第 44 卷第 2 期，臺北，民國 89 年 4 月；高大宇等，「電腦資訊犯罪之身分追蹤驗證分析模式建立」，http://163.25.10.166/monographicStudy/network, last visited on June 8, 2007.。另外大陸用語爲「計算機證據」或「計算機數據證據」者，如游偉、夏元林，「計算機數據的證據價值」，法學雜誌，2001 年第 3 期，2001 年 3 月；丁麗萍、王永吉，「計算機取證的相關法律技術問題研究」，軟件學報，第 16 卷第 2 期，2005 年 2 月；本文亦可在 www.jos.org.cn/1000-9825/16/260.pdf 查得, last visited on June 8, 2007.。

[22] 如林一德、錢世傑，同第 1 章註 7 論文。

[23] 如宋寶宏、王靜，「電子資料證據在我國的證據地位與證明力」，西安政治學院學報，2003 年第 4 期，2003 年 12 月。

[24] 如徐巍偉，「電子文件的證據效力之研究」，中國檔案，2002 年第 2 期，2002 年 2 月。

圍亦略有不同。由相關書籍、案例及文件之豐富，可見電子證據在現實生活中甚被重視，但是在概念及定義上不論中外資訊界及司法界，共識均還在形成中。

2.2.1 電子證據之意義

目前各界對電子證據之定義並未趨於一致，參與此一領域研究之學者專家各有不同之定義，但若以對電子證據定義所描述之範疇觀察，電子證據的意義大致有以下定義方向，茲分述如下：

1、電子證據等同於電腦犯罪的證據[26]

本說將電子證據的範圍限定在電腦犯罪案件中之所有證據種類，只有在電腦犯罪中所討論之證據才是電子證據，其他案件則否。所以電子證據就是電腦犯罪之證據。

2、電子證據係與電腦相關之證據[27]

此說認為電子證據就是由電腦所生成之數據資料，其內容包括以下三種形式：

（1）電腦化的業務紀錄

有關某一行為、事件或條件之證據，亦即慣常性質的業務紀錄，例如一般公司行號的員工薪資紀錄、財務紀錄、銀行存款紀錄等，此類紀錄早期屬於必須由人工保存的各種檔案，惟現今社會中均係

[25] 例如丁秋玉，網路犯罪證據之搜索扣押研究，中央警察大學法律研究所碩士論文，民國 91 年 6 月。臺灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team，TWCERT)，「防止攻擊跳板主機的安全管理策略（二）」，http://www.cert.org.tw/document/column/show.php?key=30, last visited on June 8, 2007.。大陸亦有採用「網上證據」、「網絡證據」等詞彙者。

[26] 如蔡震榮、張維平，同前註 21，即採此種觀點。

[27] 樊崇文、溫小潔、趙燕，視聽資料研究綜述與評析，頁 170，中國人民公安大學出版社，2002 年 2 月。

以電腦化亦即數位化的形式加以處理、紀錄及保存。

（2）電腦模擬證據：

由電腦提供的計算及研究結果，包括電腦對已發生的行為、事件或條件的模擬。例如於車禍事故發生後，交通專家將車禍發生當時之各類數據及資料輸入電腦軟體中，由軟體還原車禍發生時的情形，以為責任之判定[28]；或如彈道模擬軟體，模擬還原槍擊案件發生之現場等電腦資料；又或如氣象專家使用電腦所推算出來的全球暖化數據或圖像。

（3）電腦系統運行結果

有關電腦本身各項運作的證據，例如某家一銀行 ATM 提款機伺服器對每日各提款機使用人帳號、使用項目、金額等所作自動紀錄（即稽核檔、Log File）。倘若訴訟時討論到電腦運行可能發生失誤與否，則需要提供此種稽核檔或自動紀錄以佐證系爭電腦系統性能及運作可靠與否。

[28] 例如臺灣高等法院 94 年度交上更㈡字第 1 號刑事判決：「…從而，就車損跡證所研判之撞擊位置及撞擊後行進方向，均與現場遺留之煞車痕跡及兩車翻覆位置堪稱一致。中央警察大學即為此鑑定意見（見本院卷第 100 頁），此節亦經鑑定人即本院囑託再行鑑定車禍過失責任之中央警察大學交通學系主任暨鑑識委員會召集人陳高村教授於本院審理時補充證述意見並當庭播放碰撞模擬動畫光碟明確。…」、臺灣高等法院 92 年度交上訴字第 228 號刑事判決：「…3 又經原審將全案卷證送請國立中央大學機械工程學系鑑定，鑑定之事實在於分析被告所稱並未撞及機車而係機車撞及被告自小客車右照後鏡與卷證是否相符，鑑定機關依據警員繪製之事故現場圖，利用 AutoCAD 軟體重新繪製而得出事故現場稽證之位置及尺寸圖，將 AutoCAD 所重繪之事故現場圖匯入 PC－CRASH 軟體中，進行事故碰撞模擬，所得結果為：若機車撞擊自小客車，機車在撞擊後的行駛軌跡均未撞擊電線桿，並在機車時速 50 公里、小客車時速 45 公里時，與現場機車倒地停止位置有百分之 32 之誤差；若為自小客車撞擊機車，則機車在碰撞後會先撞擊電線桿再反彈至另一端，行進軌跡與事故現場圖相當接近，在小客車時速 55 公里、機車時速 43 公里時，機車滑行距離與現場圖中機車停止位置十分接近，誤差低於百分之 2，此有國立中央大學機械工程學系於 92 年 4 月 24 日出具之鑑定報告書一份附卷可參（見本案卷第 121 至 132 頁）。因該鑑定報告係依據現場重建方法、車輛碰撞過程模擬分析之科學鑑識方法作成，藉由車輛碰撞模擬軟體對於可能存在之肇事經過進行模擬分析，鑑定之方法及過程並無瑕疵…，從而，被告所稱係被害人來撞伊之汽車與事證不符洵難採信。…」。

3、電子證據為電腦所產生及列印的證據[29]

本說認為電子證據就是紀錄在紙張上，以文書形式存在的電腦化數據的列印輸出之結果。因為作為證據的各種資料必須是能夠為人類所理解和感知的，倘若資料僅是「0」與「1」組合而為人類所無法理解或感知，法院是不會採納為證據並據以認定案件事實的。因此必須先把電腦紀錄由機器可讀形式（Machine Read Format，MRF）轉化為人類可讀形式（Human Read Format，HRF），才能使提出於法院作為認定案件事實的根據具有可理解性。職是此故，有認為將機器可讀形式的電腦紀錄列印成為紙本是該紀錄作為電子證據的惟一的合理方式，甚至有更進一步認為由電磁紀錄列印出來之紙本可以當成直接證據者[30]。

4、電子證據為當作證據之電磁紀錄[31]

本見解認為電子證據之所以與其他的證據表現形式不同，就在於它是以電氣脈衝搭配磁性或光學材料的方式紀錄在磁帶、磁碟片、USB 介面隨身碟、硬碟或是光碟片上的。其他不以電磁紀錄方式表現的證據資料，無論其是否在電腦犯罪案件中作為證據使用，也無論是否與電腦相關或是否為電腦產生，則一律排除於電子證據之外。例如經過電腦列印輸出成為紙本文件，應屬於書證而非為電子證據。

本文以為第一種定義最為狹隘，因為在現代社會中，數位化資料的應用非常廣泛，任何層面的社會生活均會運用到數位化資料，非僅有電腦犯罪始有數位化資料的使用。舉例

[29] 樊崇文等，同前註 27，頁 170。南非 1983 年電腦證據法即採此見解，容後於本文第三章說明。

[30] 王亞林、范勝兵，同前註 20，頁 98。

[31] 樊崇文等，同前註27，頁 170-171；陳家瑤、吳佳育，「數位證據於現行法律之相關問題」，頁 94，收錄於 2002 年網際空間：資訊、法律與社會學術研討暨實務研究論文集 I ，中央警察大學，2002 年。

而言，商業交易中企業對企業（Business to Business，B2B）、企業對客戶（Business to Customer，B2C）之間的電子訂單、往來郵件、各項電子形式傳送的通知與照會等等，在民事案件上亦可能被提出於法院當成證據，倘若二家公司間，海外的 A 公司透過網際網路向 B 公司訂購 RJ45 接頭網路線材一批，並在網路訂單成立後曾具體發來電子郵件指示該批網路線材細部規格，例如銅線成分、包覆銅線之橡膠材料層數及顏色等等，B 公司並回函討論及確認。詎 A 公司於 B 公司交貨後發覺規格與原先訂購者不符，則在興訟之際，將前開雙方往來之電子檔案提出於民事法院當成證據，此時電子證據即成為民事案件證據之一部分。我國民事法院中，亦有將電子郵件做為勞資薪資爭議[32]、公司法上行使歸入權案件[33]、給付買賣價金[34]等案件之證據。因此認為電子證據僅得用於電腦犯罪案件，定義過於狹隘，自不待言。對於第二種觀點本文認為過於強調電子證據的機械性質，將電子證據定義為全由電腦所生成之數據資料。然而許多電子證據的形成，會有人為的觀念、思考及操作在其中，如果滲入人為因素在內，參與製作該電子資料之人員必須到法庭接受訊問及檢驗，惟此說完全排除具有人為因素滲雜其中之電子證據，範圍亦屬狹隘。至於第三種見解，本文以為與電子資料的物理性質不符，因為電磁紀錄都是由二進位制之「0」與「1」訊號組合而成的，這樣形態的紀錄非常特殊，檢驗上具有高度技術性與困難性，所以才成為應該被特別討論的課題。如果只討論此類資料列印出來之後的文件，那麼幾乎以文書證據之角度來檢驗就可以，不需要特別討論。尤其，電子紀錄雖然需要輸出設備來呈現其內容，但是不專以列印出來的紙本為唯一的呈現方式，舉凡以聲音設備播放各種聲音檔案、螢幕呈現文件、圖像、影像以及列印為紙本等都是電子資料呈現的方式，因此第三種見解亦不無商榷之處；況且，隨著資

[32] 臺灣臺北地方法院 95 年度勞訴字第 194 號民事判決參照。

[33] 臺灣臺北地方法院 94 年度金字第 31 號民事判決參照。

[34] 最高法院 96 年度臺上字第 229 號民事判決參照。

訊科技的進步，文字與聲音之間已經可以互相轉換，例如有語音輸入法[35]，將操作者之聲音轉化成文字，亦有可以將文字自動轉成聲音讀出者[36]，本說僅考量到電磁紀錄與紙本文件之轉換性，未考量其他創新科技之可能性，亦為缺憾。

本文對於電子證據之意義認為以採取第四說為宜，亦即將電子證據定義在供為法院當成證據之電磁紀錄或電磁信息。原因如下：

1、對電子證據之概念能與我國現有法制及實務見解接軌

我國司法實務在概念上並未明確區分「充為證據前之電磁紀錄」與「當成證據時之電磁紀錄」，有討論到電磁紀錄者，即在討論電磁紀錄在訴訟過程中認定犯罪事實之應用。惟從我國歷來對電磁紀錄之討論，可知所討論者均為電磁紀錄據以認定犯罪事實者。[37]

2、與我國證據種類劃分規則接軌

各國對於證據的種類，傳統上分為「人證」、「物證」及「書證」[38]。至於電子證據，有採書證說者，有採物證說者、有採獨立證據說者，亦有採混合證據說者等等不一而足。我國雖然實務與學說之意見尚不一致，但大致上朝文書證據、準文書證據或新文書證據等方向討論。因此採第四說較能與我國證據種類的見解接軌，至於各種理論容後詳述。

3、能夠在定義中彰顯電子證據之特殊性

未來社會中，隨著資訊科技一日千里，可得數位化，並以數位儲存媒體加以儲存之資料將更加增加，而電子證據之所以與其他的證據需要區分討論之，就在於電子證據的表現形式不同於其他傳統型式的證據資料。

[35] 例如 IBM 公司之 Via Voice 語音輸入軟體即是。

[36] 例如「文字 M3」軟體即是。

[37] 關於電磁紀錄之內涵，請見 2.2.2 所述。

[38] 林鈺雄，刑事訴訟法（上冊），頁 426-427，作者自版，2005 年 9 月四版二刷。

電子證據是以電氣脈衝搭配磁性材料的方式紀錄在磁帶、磁碟片、硬碟或是光碟片上的，並且無法透過人類的感知立即理解，並且一定要透過一定的電腦處理設備處理後，才能為人類所理解。因之此說能夠彰顯電子證據需要透過一定電腦設備始能理解之特殊性。

4、採取科技中立之立法原則，容納任何新興科技的可能性

進步之速度一日千里，因此對於科技相關議題立法，各國多採取科技中立原則以應對之。科技中立原則又稱技術中立原則（Technology Neutrality），任何可確保資料在傳輸或儲存過中之完整性及鑑別使用者身分之技術，皆可用來製作電子簽章，並不以「非對稱型」加密技術為基礎之「數位簽章」為限，以免阻礙其他技術之應用發展。我國電子簽章法即考量未來科技發展的無限可能性，故立法時即採取科技中立原則[39]。此說符合科技中立的立法原則，能接納未來任何新興科技的發展。惟隨著科技的日新月異，未來是否僅以磁性載體為儲存媒介，抑或有不同之發展，誠值觀察[40]。

[39] 電子簽章法立法說明：「本法爰採聯合國及歐盟等國際組織倡議的「電子簽章」（electronic signature）爲立法基礎，而不以「數位簽章」（digital signature）爲限，以因應今後諸如生物科技等電子鑑別技術之創新發展。利用任何電子技術製作之電子簽章及電子文件，只要功能與書面文件及簽名、蓋章相當，皆可使用。」參見 http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm, last visited on June 8, 2007.

[40] 1995 年由影星基努李維（Keanu Reeves）主演的科幻電影「捍衛機密（Johnny Mnemonic）」一片，就是敘述電腦發展到可以和人腦結合的時候，人類頭腦裡有一個矽晶片介面，可以透過該介面傳輸資料進入大腦，以大腦做爲儲存資訊的載具。科幻電影所敘述之情境，往往在日後會實現，因此本片所呈現的大腦儲存數位資訊的概念，將來是否成真，尚難遽予否定。因此未來數位資料之儲存媒體，未必僅限於磁性或光學載體。

表 2-1　電子證據意義分析

意　　義	電腦犯罪之證據	與電腦相關之證據	電腦產生及列印的證據	當作證據之電磁紀錄
內　　涵	電腦犯罪案件中所有證據種類均屬之	電腦所生成之數據資料，包括： 1、電腦化的業務紀錄 2、電腦模擬證據 3、電腦系統運行結果	電子證據就是紀錄在紙張上，以文書形式存在的列印輸出之結果。	電子證據就是充為訴訟證據之電磁紀錄
問　題　點	現代社會中，數位化資料的應用非常廣泛，任何層面的社會生活均會運用到數位化資料，非僅有電腦犯罪始有數位化資料的使用，因此範圍過於狹隘。	完全排除具有人為因素滲雜其中之電子證據，範圍亦屬狹隘。	1、與電子資料物理性質不符。 2、電子紀錄不專以列印紙本為唯一呈現方式，舉凡聲音之播放、螢幕呈現等都是電子資料呈現的方式。	
本文之意見	1、與對於電子證據之概念能與我國現有法制及實務見解接軌 2、與我國證據種類劃分規則接軌 3、能夠在定義中彰顯電子證據之特殊性 4、採取科技中立之立法原則，容納任何新興科技的可能性			

資料來源：本文整理

2.2.2　電磁紀錄之內涵

電磁紀錄之內涵，各界有不同之見解，茲說明如下：

1、廣義說

聯合國國際貿易法委員會（United Nations Commission on International Trade Law，下稱聯合國貿法會）在《電子商務示範法（1996 - UNCITRAL Model Law on Electronic Commerce with Guide to Enactment）》第二條對電子數據（Data Message）定義為：「係指經由電子手段、光學手段或類似手段生成儲存或傳遞的信息，這些手段包括但不限於電子數據交換（EDI）、電子郵件、電報、電傳或傳真。」[41]

2、狹義說

加拿大統一電子證據法（Uniform Electronic Evidence Act of Canada）第一條規定：「數據（Data）係指以任何形式所表現之資料或概念」；「電磁紀錄（Electronic Record）係指存在於電腦系統或其他類似之媒介中，能夠被電腦系統或其他類似之裝置閱讀或瀏覽之紀錄。包括執行、列印、輸出。」[42]

---

[41] 法規名稱及法條譯文以聯合國貿法會簡體中文譯本爲準，以下引用均採同一出處。原文爲：「Article 2（a）"Data message" means information generated, sent, received or stored by electronic,optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;」（簡體中文出處：http://daccessdds.un.org/doc/UNDOC/GEN/ N97/763/56/PDF/N9776356.pdf?OpenElement；原文出處：http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html）, last visited on June 8, 2007.

[42] 本譯文參考郭佳玟，「談電磁紀錄證據定義與方法—比較加拿大電子證據統一法與我國刑事訴訟法相關規定」，科技法律透析，頁 13，2005 年 4 月。原文爲：

「1. In this Act,

（a）"data" means representations, in any form, of information or concepts.

（b）"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in Sub-section 4(2).」

3、我國對電磁紀錄之看法

（1）早期之實務見解

我國實務上最早提及電磁紀錄，是在民國八十一年九月八日，最高法院八十一年度第十一次刑事庭會議，時任最高法院庭長的林大法官永謀，提出一份研究報告[43]，當中提及電磁紀錄之意義及描述：

「電腦（電子計算機 electronic computer）之功能，主要在『保存』『處理』『傳遞』資訊、資料。以往被認為『可視』且『有體』之書面，於今逐漸被電腦之磁帶、磁碟等電磁紀錄物所取代。因是對於電磁紀錄物之偽造、塗改、塗去等等，是否應獲得與『文書』相同之保護，而可適用刑法偽造、變造、毀損文書之相關規定，乃成為問題。本來學說上所謂文書（包括準文書）係指使用文字或符號，在可永續的狀態中，存在於物體上所記載之意思或觀念（意識），因此德國之通說遂認刑法上之文書，必須以成為視覺之對象為限，即所謂具備『可視性』『可讀性』之要件，始屬當之（Sieber,Computerkriminalitat und Straf,§248），電磁紀錄物非特不可視、不可讀，且與文書之『必須將制作名義人表示於文書上』之另一要件亦有未合，因不認其係屬刑法上所應保護之文書。至於日本，與說上雖有爭論（仍以主張文書必須可視、可讀為多數）但實務上對於以電磁處理之汽車登記檔案，則認其相當於彼邦刑法第一五七條第一項之『公正證書之原本』，乃採肯定說（最高裁判所昭和五十八年（民國七十二年十一月二十四日）判例--刑事判例集三十七卷九號一五三八頁）。

[43] 該次會議討論問題為：『刑一庭提案：某甲強劫取得某乙在行社或郵局設立存款帳戶而發給之提款卡（或稱金融卡）後，持往行社或郵局冒領自動提（付）款機（或稱櫃員機）內之存款，除應牽連觸犯強劫及詐欺取財兩罪外，其將某乙提款卡擅自送入自動提（付）款機內，輸入提款人設定之密碼，按提款鍵及提領金額，使自動提（付）款機將款送出交付某甲之行為，是否應另成立刑法第 216 條、第 220 條、第 210 條行使偽造準私文書罪之牽連犯？有甲、乙兩說（兩說略）。決議：採林庭長所提研究意見（下略）。

電腦與財產上犯罪所關連之問題中，其以資訊之不正操作，非法獲取財物或財產上利益之行為，究係詐欺抑竊盜？亦有爭論，此則對機械（電腦）之欺騙，是否亦屬刑法上之欺罔行為之問題。大陸法系之德、日通說，認機械不可能錯誤，如藉他人之現金提取卡（提款卡）撥取款項，就電腦本身言，完全依據程式語言之指令，就一定程序予以處理，無所謂受欺罔致生錯誤，因此僅能成立竊盜罪（Schonke/Schroder/Cramer, StGB,21 Aufl , 1982 §263.、植松正『全訂刑法概論Ⅱ各論』第四一0頁）；但英美法系之立法則認機械應視同自然人之替代，其對機械之欺騙，即等於對自然人之所為，故應成立詐欺罪。如英國一九八一年七月二十七日制定之『文書及通貨偽造條例』（The Forgery and counterfeiting act）除將文書包括於『以機械、電器或其他方法紀錄或記憶資訊之磁碟、磁帶、音帶或其他裝置』外，復將機械所為之識別、運作，視同自然人所為（見該條例第八條第一項 d 款、第十條第三、四項），另美國阿拉斯加州一九八三年之立法亦然。西德（現為德國）一九八六年（民國七十五年）八月施行之經濟犯罪防止法，關於刑法一部修正為：第二六三條（關於電腦詐欺）、第二六九條（關於虛偽紀錄資訊之輸入--以此解決『文書性』問題）、第三0三條 a（關於紀錄、資料之變更）、第三0三條 b（關於電腦操作之妨害）、第二百零二條 a（資訊之不正取得）。

日本於昭和六十二年（民國七十六年）六月關於電腦犯罪亦為刑法之一部修正，其中以第一六一條之二（電磁紀錄與文書罪）、第二三四條之二（電腦資訊處理與業務妨害罪）、第二四六條之二（電腦不正操作與財產犯罪--即以詐欺論擬）為最重要。

德、日兩國因上述刑法一部修正之結果，已將電磁紀錄物以法律規定為『文書』予以處理；但德國法仍維

持『無形偽造不罰』，而『名義人之存在至少須可被判斷』。日本法則將具有『製造』『輸入』資料之權限者，視為文書之制作名義人，且主觀上限於『使人業務處理錯誤為目的』，故其立法本意，不在『保護紀錄之證明功能』，而係處罰『資訊處理之妨害』。是德、日雖以立法承認電磁紀錄物之文書性，但其著重之點並非完全相同，此乃吾人宜加注意者。至於其以資訊不正之操作，非法獲取財物或財產上利益之行為，德、日立法上均以詐欺罪論處，則無不同。我國刑法修正草案（七十九年二月十三日）第三三九條之一：意圖為自己或第三人不法之所有，以不正方法由自動付款或收費設備取得他人之物者處一年以下有期徒刑、拘役或三千元以下罰金。以前項方法得財產上不法利益或使第三人得之者，亦同。是關於本問題立法之趨勢如何，已甚為明顯。

吾人以為電磁紀錄物確係在永續狀態中記載於物體上之意思或觀念，雖其係以無形之正負磁氣存在於物體上，即由程式語言之此種電腦特有之符號予以表示，但由重現裝置印出時，即可藉其處理之機器作為文書而再生，故非不可謂電磁紀錄物亦為文書。此正如微膠捲，雖本身不能讀，但用機器即成可讀之物，亦即透過光線等，以直接之形狀放大，即能閱讀，所以可稱為『文書』之縮製版。相對於此，在電磁紀錄物之情形，固與微膠捲並非完全相同，其乃在物體上帶有無形之正負磁氣，且其再現方法為間接，必須與主記憶等電腦資訊處理組織全體為一併之運用，始能獲得再現之結果，然其雖屬如此，該磁帶所記憶之資料，只要知悉程式語言，而變換符號，經使用電腦即可為數字或文字之再現，所以其結果仍與微膠捲同，應不能謂其不具備文書性。至有謂刑法上之文書，必須以成為視覺之對象者為限，即所謂具備『可視性』『可讀性』之要件，始屬相當者；然此種附上視覺限定之說法，勿論其於盲人之點字，將難以自圓其說；且即

令其應可視、可讀，當亦非指必須為『直接』之可視、可讀之意，電磁紀錄物雖不能直接從磁帶等之本身予以解讀，但如於再生之裝置上予以印出，則資料即行再現，必要之資訊即為可讀，故吾人若以直接之可讀否定其文書性，似非妥適；況所謂可讀，亦非一般人均可解讀之意，只要關係人之間依據客觀可循之規則，均受該記號之拘束而通用者，即使對一般人言為完全不成意義，亦不足為否定文書性之理由，此正如電碼、速記符號等並非通常一般人所能知曉其意義者同。是吾人倘予採取積極說（肯定說），似亦不能謂其與『文書』之概念有所乖離；尤其社會生活不斷趨於複雜化，有關事務之處理則要求迅速化、確實化之今日，公私機構之使用電腦必將大量增加，為因應此種社會之現實，從正面予以立法，如美、英、德、日諸國然，固屬適切之途徑，但我國係一立法遲鈍之國家，為阻遏關於電腦犯罪之不法行為，基於具體妥當性之考慮，經由現行法有關之規定，『適當』運用傳統文書概念所為之論理解釋，藉司法功能之運作，以因應現實，有如日本以往所為者然，應認有其必要。

自動付款機（Cash Dispenser）係電腦之一種，提款人使用一定之機器語言，對其下一定之指令後，依自動操作系統付出一定之現款；而為提款以塑膠板所製成之『提款卡』，其與自動付款機發生一定之關係者，則係印在其上亦為吾人視覺無從察看之『磁線』，此等磁線通常除有金融機關之名稱、分支機構、存戶帳號外，為確保存款人之權益，亦儲存有『暗證號碼』（即吾人通稱之密碼），以供辨識之用，俾得確認其係該金融機關之物，以及該持卡之人係有權提款之人，並因此接受其後續之指令。故本問題所稱之『密碼』雖係一種證明之符號，然其『輸入』（即按上密碼數字）之行為，既非藉『密碼』在自動付款機軟體之磁帶、磁碟上儲存（記載）任何之

意思或觀念，故其按上密碼之本身，顯不能認係文書；且其亦非對已有之程式或資訊、資料予以變更或塗去，而僅具有辨識之作用，此正如安全鎖之密碼然，必須撥對該設定之密碼，其所用之鑰匙始能開啟該鎖，道理正同，因此亦無所謂變造文書之情事。至於鍵盤提款數字之『按上』，則是一種付款操作之指令，亦即根據　一定之程式語言命電腦依其程式所控制之自動付款系統為一定之處理，並付出與該數字相同之現款，此與一般電腦之操作，依其所欲處理之項目，須按上一定之鍵盤，發出一定之指令，其理亦屬相同，既非輸入虛偽之資訊、資料，更非變更原先儲存之紀錄，當亦不生偽造、變造文書之問題；雖其軟體之程式所支配之自動記帳系統，因接受指令後之運作，經為自動記帳之結果，而使原先儲存之資料，內容上有所變更，並輸出提款紀錄及結餘帳單，但此則係自動付款系統處理後，進而因自動記帳系統之發動，致其有關之數字前後不同。並非對程式或存儲之資料，直接予以輸入其他之資訊、資料，以變更其內容。此正如存摺之提款，經計算後，其在『帳簿』及『存摺』上所為之記載然，係付款人（金融機關）自行所記載，其『明細』應僅有『帳簿』憑證及使存款人得為核對之作用，提款人主觀上並無制作此等文書之意思，客觀上亦無此一制作之行為。茲吾人對存摺提款之上開記載，既因我國刑法無處罰使人為業務上登載不實之明文，而均不以為罪，則由自動付款機之處理，代其記帳、交付『明細』之情形，既與自然人所為者同，法律上之效果，當應從同。

實務上，部分之見解，固有將前述之密碼，以其與印章、印文、署押有相同之作用，在鑑識『人格同一性』上有類似之功能，因將之與『金額數字』結合，而視同『取款條』之情形予以處理，遂主張應成立偽造私文書罪者，甲說之思考方向諒亦如此，固非無其見地；然社會上類似、甚或相同功能之事物，法律上

亦非必須均賦予相同之評價，而仍應受所關法律概念之適當制約。茲印章、印文、署押既係表示人格同一性之記號，自仍以持續相當之時間而存在於一定之物體上為必要，其與『文書』之此一概念並無稍異，吾人倘將印章、印文、署押之概念過予擴大，認其雖非以持續之狀態而存在於一定物體上，亦屬無妨，則任何『人格同一』識別之符號，即使僅作為瞬間之辨識，而未持續存在於一定物體上者，當亦應認其為『印章』『印文』『署押』，如此，將使文書偽造罪陷於混亂，其所衍生之問題定必更難解決。實則如前之說明，本問題之密碼，僅具辨識之作用，俾電腦確認其無誤後，即聽從其後續之指令以為一定之處理，雖其不無表示一定用意之證明，但既非在永續狀態中記載一定之意思或觀念，固不能認係文書；且其按上之密碼，亦未存於一定物體上，僅供瞬間之辨識，自亦無所謂偽造印章、印文或署押。而『金額數字』則係命其付出相同數額之現款之指令，既不可能以之組成新的程式、或變更原有之程式，亦非直接更改原先儲存之資訊、資料之內容，自均無偽造、變造文書之可言。」[44]

（2）我國法律規範

A、民國八十六年十月八日修正公布之刑法第二二0條第三項：「稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。」

B、民國九十五年七月一日修正施行之刑法第十條第六款：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」

[44] 除最高法院 81 年度第 11 次刑事庭會議外，許多實務見解直接以電磁紀錄一詞用以討論電腦或相關設備所衍生之法律問題。

C、其他尚有刑法第二百０一條之一、第二百０四條、第二百０五條、第二百二十條、第三百十五條之之、第三百五十九條；刑事訴訟法第一百二十二條、第一百二十八條、第一百六十五條之一等條文亦使用「電磁紀錄」。

（3）綜上，本文對電磁紀錄之意義有以下見解：

A、修正前之舊條文有「其他無法以人之知覺直接認識之方式」等文字，較為貼切於電磁紀錄無法為人類直接判讀之特性。我國電子簽章法第二條對電子文件之定義正足以支持本文之見解，該條文規定：「電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。」

B、雖有見解認為前揭廣義說與狹義說之區分在於狹義說將照片檔、文字檔等排除於電磁紀錄之外[45]，惟就加拿大統一電子證據法第一條之文義及條文釋義[46]以觀，似未做如此區隔。

C、本文以為廣義說與狹義說之區分仍在「是否業已以擷取及固定於磁性載體之上」一點上，亦即流動之電子數據範圍過廣，有必要將之縮小範圍界定在已經電磁載體保存處理者始足當之，如此始符合電磁紀錄中「紀錄」之特點。

D、由我國實務見解及條文規定以觀，亦認係採取狹義說。蓋不論新、舊刑法條文或電子簽章法條

[45] 郭佳玟，同前註 42，頁 13。

[46] 加拿大對該條文之釋義請參見 http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2, last visited on June 8, 2007.

文，乃至實務見解上，均納入「紀錄」、「製成」及「處理」等要件，既認為有「紀錄」、「製成」及「處理」等要件，表示數位資料必須要業已「擷取」及「固定」於磁性載體之上，始得當之。

E、因此，我國均以電磁紀錄或電磁資訊之概念來看待數位化證據資料，較能符合現有法律之規定及概念，也能避免不同名詞在討論過程中產生討論者真意的耗損或誤會。

表 2-2　電磁紀錄內涵分析

	廣義說	狹義說	我國規範
意　　義	電磁紀錄指經由電子、光學或類似手段生成儲存或傳遞的信息，這些手段包括但不限於電子數據交換（EDI）、電子郵件、電報、電傳或傳真。	電磁紀錄係指存在於電腦系統或其他類似之媒介中，能夠被電腦系統或其他類似之裝置閱讀或瀏覽之紀錄。包括執行、列印、輸出。	電磁紀錄係在永續狀態中記載於物體上之意思或觀念，由重現裝置印出時，即可藉其處理之機器作為文書而再生，故非不可謂電磁紀錄物亦為文書。
依　　據	聯合國貿法會電子商務示範法（第 2 條）	加拿大統一電子證據法（第 1 條）	1、最高法院 81 年度第 11 次刑事庭會議林大法官永謀之研究報告 2、刑法第 10 條第 6 款：「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」
問　題　點	流動之電子數據範圍過廣，有必要將之縮小範圍		
本文之見解	1、由我國實務見解及條文規定以觀，認係採取狹義說。 2、由我國實務上對電磁紀錄之討論以觀，並未將電磁紀錄區分為訴訟上與訴訟外。		

資料來源：本文整理

2.3　電子證據之物理性質

電子證據是以電磁紀錄為基礎，而電磁紀錄是由電腦或電子設備，在磁性載體上以「0」與「1」的電氣訊號刻畫／紀錄而成。以此種二進位制電氣刻畫／紀錄之方式，可以紀錄文字、聲音、圖畫、影像等各種傳統形式之之資料。當此種資料因為偵查犯罪或當事人雙方因糾紛而涉訟時，被使用於訴訟活動中，即成為證據之一種，此為電子證據之概念。

本文以為應從電磁紀錄之各種物理性質或技術性質來瞭解電子證據可能會具備之特性或特徵，以便於當電子證據適用在訴訟時，能夠因應電子證據各項特性或特徵加以調整證據法則之適用。

2.3.1　電子證據之特性

1、數位性

電子證據的載體是電子元件和磁性材料等，資料的儲存，是藉由經由自動或人為操作電腦系統所產生的。但是純從物理的角度觀察，只是積體電路的電子矩陣正負電極或磁性材料磁體發生變化而已，因此蒐集、保存、展現及理解認知這些證據，均需要特殊的方式，與其他傳統證據完全不同[47]。

2、技術性

電子證據的產生、儲存和傳輸及其蒐集、分析和判斷都必須借助於電腦科學中的運算技術、存儲技術以及網路通信技術等等，所以電子證據的調查及認定具備有高度技術性、跨領域性[48]。

---

[47] 丁麗萍、王永吉，同前註 21，頁 262。

[48] 游偉、夏元林，同前註 21，頁 60；丁麗萍、王永吉，同前註 21，頁 262。

3、脆弱性

電磁資訊紀錄在磁性載體上，這些載體的設計，本來就是要易於修改以隨時儲存資料，甚至針對儲存載體之修改（儲存）速度一直在改進突破。正因為電磁紀錄及其載體容易非常被修改、刪除[49]，並且各類型電磁紀錄如文件、圖像、影音檔案等往往儲存在同一載體，因此有互相干擾或污染之疑慮。從而使得電腦資訊有脆弱而不可靠的一面。再由於電腦資料的修改與刪除都是在瞬間完成的。所以電子證據就此點而言也時遭質疑其不可靠且脆弱[50]。並且，電子證據存在於磁性載體內，即使正常讀取，每次存取時也都會改變檔案之狀態，使得電子證據之證據力受到質疑[51]。

4、依附性

電子證據不能單獨存在，必須附著於磁性（如硬碟、磁碟片、USB 隨身碟）或光學（如 MO、可錄式光碟片）等儲存媒介而存在。至於被電子證據依附之物品，在性質上係屬物證[52]。

5、多元性

電子證據本身涵蓋檔、圖形、圖像、動畫、音樂及影像等多種型態，因此電子證據本身不是單一證據種類，具

[49] 錢世傑，同第一章註 7，頁 67。

[50] 電子證據對常被挑戰者，在於電子證據極易遭篡改，且遭篡改後查證不易，此一論點幾乎成爲防禦方的標準答辯。實則，從電腦鑑識技術層面以觀，上開觀點誠屬謬誤，因爲：1、電子證據是由能借助特定工具和技術加以蒐集並分析的各種磁性物質和電磁脈衝物質形成的；2、許多法庭都承認，這種無形物可作爲證據扣押。3、電子証據同傳統物證相比具有如下優越性：（1）電子證據能夠被精確地複製，其複本能夠當作原本一樣以供質詢；由於質詢電子證據複本是十分普通的事情，因此能夠克服其原本滅失的風險。（2）如果使用合適的工具，很容易發現電子證據同其原本相比，是否遭受過篡改。（3）要想毀壞電子證據，相對而言比較困難。即使刪除，也能從計算機硬碟上恢復。（4）假如犯罪人試圖毀滅電子證據，其複本仍可能保存在犯罪人根本不知道的地方。參見 *See* Eoghan Casey, *Supra* note 17, pp.15-16。

[51] 高大宇等，同前註 18，頁 452；游偉、夏元林，同前註 21，頁 60；蔡震榮、黃玥婷，同前註 18，頁 4。

[52] 謝名冠，同前註 20，頁 173-174。

有多元性[53]。且因為表現之方式及儲存載體的多樣性，因此亦有學者爭此一特性為多媒體性或多態性。

6、人機交互性

電子證據的形成，於不同環節中有不同的操作人員參與，因此在不同程度上均可能影響電腦系統的運轉。且此種影響的層次和程度與操作人員的工作性質有關，亦即電腦管理員、網路管理員、程式師、系統分析人員以及一般的操作人員對資料資訊的影響有所不同。職故，為保證電子證據的可靠性和真實性，於檢驗電子證據時應注意分析參與操作之人員與機器兩個方面[54]。

7、隱蔽性

電子證據在存儲、處理的過程中，是以人類無法直接感知的二進位制編碼來完成。因此，一切文件和資訊都以電子數據的形式存儲於磁性載體中，具有較強的隱蔽性，因此電子證據與特定主體間的關聯性較難依照一般常規手段加以確定[55]，非透過電腦設備及相對應軟體轉換顯現方式，無法為人類了解或檢視其內容[56]。

8、不易證實完整性

電磁紀錄的製作極為容易，也因此易被複製或修改，使得在進行鑑識時不易直接將所得證據與嫌犯的關係進行連結，不利益之一方亦十分容易提出抗辯，也就是難以達到「個化」（Individualization），不如指紋或是 DNA 擁有極佳的個化能力。在易受修改的特性下，要證明其完整性，亦即未受篡改或刪除，較為困難[57]。

---

[53] 參見謝明冠，同前註 20，頁 173；游偉、夏元林，同前註 21，頁 60；丁麗萍、王永吉，同前註 21，頁 262。

[54] 丁麗萍、王永吉，同前註 21，頁 262。

[55] 游偉、夏元林，同前註 21，頁 60。

[56] 高大宇等，同前註 18，頁 452；游偉、夏元林，同前註 21，頁 60。

[57] 高大宇等，同前註 18，頁 452；蔡震榮、黃玥婷，同前註 18，頁 4。

2.3.2 電子證據之特徵

1、電子證據必須借重一定的電子媒介始得保存（儲存）

電子證據是以二進位制的形態存儲在各種電子介質上的。傳統書證主要的載體是紙張或其他可書寫物質；證人證言主要借助於人的記憶；物證可以藉助於各種物品、痕跡與物質等；而電子證據則離不開晶片、磁帶、磁碟片、硬碟、光碟、隨身碟等新型的資訊載體。這些資訊載體所存儲的數據量或資訊量很大，是傳統介質無法比擬的。此一特點也使得電子證據可以以多媒體的形式出現，可以綜合反映文件、圖像、影像、聲音等多種不同態樣之資訊內容[58]。

此外，即使是透過有線或無線網路傳輸過程中所擷取之電子證據，性質上亦必然依附於一定之儲存載體，因為：

（1）數位資料透過網路「寄送」或「移動」，其實都是「複製」之概念。對於「寄送」而言，是將來源電腦中的電子檔案，「複製」一份至目的電腦中；若是「移動」檔案，是將來源電腦中之檔案複製至目的電腦中之後，再將來源電腦中之該份檔案刪除。所以不論寄送或移動，來源電腦與目的電腦間有一台或兩台電腦儲存載體中有該檔案。

（2）透過網路「寄送」或「移動」檔案，傳輸至目的電腦時，仍須一定之儲存載體加以儲存。即使只是觀看圖片，也必須暫存於隨機存取記憶體或硬碟之中，使得觀之。

因此，從電腦的傳輸原理觀察，電磁紀錄不可能單獨存在於電腦設備之外。

[58] 何家弘，同前註 20，頁 14。

2、排除一定的物理干擾，理論上可以無限制的複製，而且每一份複本均相同

電子資料在複製的過程中，如果扣抵掉物理干擾，理論上可以無限制的複製，而且每一份複本均相同。傳統證據不論是書證或物證，複製不易，就以書證而言，即使以影印、照相等方式複製，在數次複製後，至少在細部處都會顯現出模糊、色溫落差[59]等問題，如果以人工複製，每份複本相異處會更加明顯。然而電子資料在複製過程中不會發生此種問題，甚至在硬碟中都會有針對複製過程所產生的耗損加以修補，因此各複本間不會有差異性存在。[60]

3、在傳播方式上，電子證據可以無限地快速傳遞[61]

一般來說，傳統證據只能在物理空間傳遞，因為電子證據本質上主要是一種資訊，所以可在虛擬空間傳播，並且傳遞速度驚人。傳統物證、書證、視聽資料轉移後，在原始出處就不存在了；傳統證人證言傳播開來後雖然在原始出處仍然存在，但往往會發生重大變形，由於「一傳十、十傳百」而導致面目全非。而電子證據的傳遞則不然，不僅在轉移後仍在原始出處存在，而且失真的可能性很小甚至沒有。從這個角度來說，電子證據的傳遞實質上屬於資訊的精確複製[62]。

---

[59] 色溫是指光波在不同的能量下，人類眼睛所感受的顏色變化。其標準是由英國物理學家 W.T.Kevlvin 所制定，據說是凱氏在鐵工廠內看到工人鎔鐵時，金屬由鎔化開始至最高溫度各階段間所呈現的顏色，以數據單位給予紀錄而成，後人將此單位以 K 來計算，例如正常色溫是 5000K 至 5500K。色溫最常被討論的是在照明、顯示或攝影等方面，但是近年來討論數位藝術創作之著作權保護時，常常被試圖當成保護的準據之一。當藝術家直接以電腦設備創作出數位藝術作品，合法重製與非法重製如何判別？色溫這一項基準是否可以當成管制或判斷的標準，一直是此領域討論的重點。

[60] 林一德，同第一章註 7，頁 124-126；蔡震榮、黃玥婷，同前註 18，頁 4。

[61] 此一觀點通常是被用來討論數位化時代著作權被侵害之現象，惟電子證據亦可能發生此類情形。

[62] 何家弘，同前註 20，頁 14-15。

4、在感知方式上，電子證據必須借助電子設備，且不能脫離特定的系統環境

電子證據常常被稱為「以電腦為基礎的證據（Computer-based Evidence）」，傳統書證被稱為「以紙面為基礎的證據（Paper-based Evidence）」。這兩種不同觀點表示電子證據無法離開電腦及其他電子設備或載體而單獨存在。如果沒有專門的電子設備、相應的播放、檢索、顯示設備，任何內容都只能停留在各種電子存儲載體中，不能被人類感知，也不能為法院所採認[63]。

5、電子證據易遭篡改，且不容易被發現

電子證據具有容易被修改或刪除的特點，傳統證據的原本、複本較容易識別，已如前述。而電子證據的原本與複本、真實件與偽造件則真偽難辨[64]。惟另有學者對此提出相反的觀點：傳統書證，一旦原本遭到毀損，則再難復原原始證據；而電腦硬碟上的每一次抹寫紀錄都可以被追蹤捕捉。電子紀錄任何被刪除、複製、修改的痕跡都能夠通過技術手段分析認定，也可以被復原[65]。從此一層面而言，電子證據比傳統證據更具有穩定性和安全性[66]。

[63] 林一德，同第一章註 7，頁 128-129；蔡震榮、黃玥婷，同前註 18，頁 4-5。

[64] 何家弘，同前註 20，頁 16。

[65] 發生在 94 年的南迴鐵路搞軌案中，警方將已自殺之犯罪嫌疑人李雙全電腦以電腦鑑識技術「復原」，並順利自該電腦內還原被刪除的檔案中尋獲重要線索，包括脫軌器結構圖、數據諸元；訂製臺車設計圖表、相關輪距與速度測量紀錄；化學藥品及各種有毒物劑資料等，參見東森新聞報，「南迴怪客案/范氏千萬理賠金　李雙全疑朋分共犯吃紅」，2006 年 5 月 20 日，http://www.ettoday.com/2006/05/20/138-1943820.htm#, last visited on June 8, 2007.

[66] 除前揭註 50，Eoghan Casey 採此見解之外，Alan Gahtan 亦採此說，*See Super* note 8, p.7；林一德，同第一章註 7，頁 126-128。

2.4　電子證據之法律地位

電子證據在證據規則上，其定位究竟如何，誠值討論。向來證據依物理性質與既存狀態的角度，可以區分為人證及物證及書證。相對應的證據方法，有被告、證人、鑑定人、文書、勘驗以及鑑定，其中被告、證人及鑑定人，屬於人的證據方法；文書、勘驗及鑑定屬於物的證據方法[67]。

至於電子證據，因為出現時期甚晚，概念太過新穎，甚至概念與形態都還在快速發展中，因此對於此類證據的法律地位以及證據方法，都還在討論之中。

2.4.1　歷來之見解

電子證據之法律地位，目前主要有如下各說[68]：

1、書證說[69]

（1）立論依據：

A、所謂文書，係指可閱讀的記載狀態之書面，且具有保存及傳達人的思想或意志之機能者。電子證據，尤其是電磁紀錄可以保存與傳達思想之機能，因而認為是文書，縱認以電磁記號之磁氣組合來表示思想，但尚未達到可閱讀狀態者，亦應為準文書。

B、普通的書證是將某一內容以文字符號等方式紀錄在紙張上，電子證據則是以電磁、光學等物理方

---

[67] 林鈺雄，同前註 38，頁 426；曹鴻蘭等，「電磁紀錄在民事訴訟法上之證據調查方法—民訴法研究會第 67 次研討紀錄」，頁 139，法學叢刊第 171 期，民國 87 年 7 月。

[68] 如以下各說之外，尚有準書證說，惟本文以爲與書證說差異不大，茲不納入，參見丁秋玉，同前註 25，頁 155。

[69] 蔡墩銘，刑事證據法論，頁 209，五南圖書出版公司，86 年 12 月；盧文祥，濫用電腦資訊所生法律問題之研究，國立中興大學法律研究所碩士論文，民國 74 年 1 月，頁 188；曹鴻蘭，同前註 67，頁 139。

式將同樣的內容記載在非紙張的存儲介質上而已，兩者雖然紀錄方式及載體不同，卻具有相同的功能，亦即均能紀錄完全相同的內容[70]，表達一定之意思。

C、電子證據雖然是以二進位制的形態儲存，但做為證據，其內容是用以證明案件中某一事實，且必須藉由輸出、列印到紙張上，形成列印之書面文件後，才能被人們看見、利用、理解，因而具有書證的特點，雖然亦可呈現於螢幕上，但亦無礙其書證之性質[71]。

D、不可讀對電磁紀錄之轉換過程，可以以速記文書轉換之觀念，因為速記文書是符號，也是要透過轉換才成為可瞭解意思之文書。[72]

D、電子證據係以其所紀錄之意思內容為證據資料，該項資料內容本即預定經電腦等機器列印輸出，因此儲存在磁性載體內之訊息稱為「可成文書」，而列因出來之紙本文件則為「生成文書」[73]， 故其調查方法自以書證說為妥。

E、就國際公約暨外國立法例而言

隨著電腦技術的普及以及電子商務的興起與發展，現有法律對提出原本做為證據的規定勢必會影響有關糾紛的解決或案件的調查。因此，國際公約及許多國家放寬了對訴訟中書證原本的要求，例如

[70] 何家弘，同前註 20，頁 21。
[71] 何家弘，同前註 20，頁 21。
[72] 曹鴻蘭，同前註 67，頁 145，王甲乙發言。
[73] 曹鴻蘭，同前註 67，頁 143，駱永家發言。

（A）聯合國貿易法委員會（下稱聯合國貿法會）國際商事仲裁示範法（1985 - UNCITRAL MODEL LAW ON INTERNATUONAL COMMERICAL ARBITRATION）[74]

第七條「仲裁協議的定義和形式」

「1、『仲裁協議』是指當事各方同意將在他們之間確定的不論是契約性或非契約性的法律關係上已經發生或可能發生的一切或某些爭議提交仲裁的協議。仲裁協議可以採取合同中的仲裁條款形式或單獨的協議形式。

2、仲裁協議應是書面的。協議如載於當事各方簽名的文件中，或載於往來的書信、電傳、電報或提供協議紀錄的其他電訊手段中，或在申訴書和答辯書的交獲中當事一方聲稱有協議而當事他方不否認，即為書面協議。在合同中提出參照或有仲裁條款的一項文件即構成仲裁協議，如果該合同是書面的而且這種參照足以使該仲裁條款構成該合同的一部分的話。」

[74] 本譯文採用聯合國貿法會簡體中文譯文，原文爲：

「Article 7 Definition and from of arbitration

(1) “Arbitration agreement” is an agreement by the parties to submit to arbitration all or certain disputes which have arisen or which may arise between them in respect of a defined legal relationship, whether contractual or not. An arbitration agreement may be in the form of arbitration clause in a contract or in the form of a separate agreement.

(2) The arbitration agreement shall be in writing. An agreement is in writing if it is contained in a document signed by the parties or in an exchange of letters, telex, telegrams or other means of telecommunication which provide a record of the agreement, or in an exchange of statements of claim and defense in which the existence of an agreement is alleged by one party and not denied by another. The reference in a contract to a document containing an arbitration clause constitutes an arbitration agreement provided that the contract is in writing and the reference is such as to make that clause part of the contract.」

（http://www.uncitral.org/uncitral/zh/uncitral_texts/arbitration/1985Model_arbitration.html）, last visited on June 8, 2007.

（B）聯合國國際貨物銷售合同公約（1980 - UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS ）[75]

第十三條

「為本公約的目的，『書面』包括電報和電傳。」

（C）法國民法典（Le Code civil regroupe en France）

第一三四八條第二項規定，當原本不存在時，可用確實而又耐久的複本有效地取代原本，使電子數據可以作為證據[76]。

（D）美國聯邦証據規則（Federal Rules of Evidence）

第一００一條第三項則以擴大原本解釋的方式將電腦列印輸出材料視為原本，該項規定：

第一００一條「定義」

「為本章之目的，下列定義適同之：(3）原本：文書或紀錄之『原本』，係指文書或紀錄之本身，或其製作人或發行人有意使之與原本有相同效果之相等物。照像之『原本』包括負片與其任何印製物，如資料係儲存於電腦或類似裝置，其印出物或其他輸出物得以視覺閱讀，且顯示正確反應資料者亦為

[75] 本譯文採用聯合國貿法會簡體中文譯文，原文爲：「Article 13 For the purposes of this Convention "writing" includes telegram and telex.」(http://www.uncitral.org/uncitral/zh/uncitral_texts/sale_goods/1980CISG.html）, last visited on June 8, 2007.

[76] 原文爲：「Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support.」引自 http://www.rabenou.org/code/civil/L3T03.htm, last visited on June 8, 2007.

『原本』。」[77]

F、就我國條文規定以觀：

（A）我國於民國九十五年六月十四日修正通過之刑事訴訟法第一百六十五條之一規定：

「前條[78]之規定，於文書外之證物有與文書相同之效用者，準用之。

錄音、錄影、電磁紀錄或其他相類之證物可為證據者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。」

（B）於民國九十二年六月二十五日修正通過之民事訴訟法第三百六十三條規定：

「本目[79]規定，於文書外之物件有與文書相同之效用者準用之。

文書或前項物件，須以科技設備始能呈現其內容或提出原本有事實上之困難者，得僅提出呈現其內容之書面並證明其內容與原本相符。

前二項文書、物件或呈現其內容之書面，法院於必要時得命說明之。」

---

[77] 本譯文引自崔汴生譯，美國聯邦證據法，司法院， 92 年 1 月初版。原文爲：「For purposes of this article the following definitions are applicable: (3) Original.
An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".」以下之美國聯邦證據法譯文均以此版本爲主，就誤繕之處輔以吳巡龍博士意見更正之。

[78] 按即刑事訴訟法第 165 條「卷宗內之筆錄及其他文書可爲證據者，審判長應向當事人、代理人、辯護人或輔佐人宣讀或告以要旨。前項文書，有關風化、公安或有毀損他人名譽之虞者，應交當事人、代理人、辯護人或輔佐人閱覽，不得宣讀；如被告不解其意義者，應告以要旨」

[79] 按即「第二編　第一審程序／第一章　通常訴訟程序／第三節　證據／第四目　書證」。

綜上，由國際組織、外國立法例可見各國立法上有將傳統書面形式之書證與電子證據之間拉近距離之趨勢[80]。再由我國現行民、刑事訴訟法條文之規定觀察，可認我國對於電磁紀錄採取書證說，因此電子證據亦應採此說。

（2）證據調查程序[81]

A、聲明證據時應提出法院之證據可分二種見解：

甲說：應提出電磁紀錄帶等之原本及其列印為可閱讀狀態之書面。

乙說：應提出電磁紀錄帶等之原本及列印出來之書面（即繕本）以及用以列印為書面之電腦程式外，尚須提出其以記號、符號復合化之書面。

B、訴訟當事人對電磁紀錄帶原本之存在，真正不爭執時，亦即對以繕本代替原本為證據無異議時，則可不必提出電磁紀錄帶原本。

C、法官應在法庭上朗讀所列印之文書；予以調查。[82]

本說仍以電磁紀錄帶等為證據原本，以其所列印之文書為證據繕本，且認為應向法院提出原本，繕本及其列印所用電腦程式為原則。

（3）形式證據力[83]

甲說：具有標準性能之電腦（或機器）在業務通常過

[80] 何家弘，同前註 20，頁 22。

[81] 曹鴻蘭，同前註 67，頁 139。

[82] 採朗讀見解者尚有夏井高人，裁判實務とコソピユータ一法と技術のなめぎしこ，頁 142，日本評論社，1993 年。轉引自丁秋玉，同前註 25，頁 155。

[83] 曹鴻蘭，同前註 67，頁 140。

程中，自要紀錄事項發生時起，在合理的期間內輸入電腦，有此證明即具有形式證據力。

乙說：前項外，尚須具備

A、在電腦正常機能時輸入紀錄內容日有正確的輸入原始紀錄之內容；

B、其紀錄之保存，加工及列印等管理皆有嚴格正確的實施；

C、當時電腦紀錄有繼續的在操作處理等之證明始可認其有形式證據力者。

丙說：經已列印成書面，但未經法院或公證人認證之繕本，在確認當時所使用之電腦為正常外，尚須經其書面列印人，公司相關單位負責人或律師等之連署證明後始認其有形式證據力。

（4）實質的證據力[84]

甲說：電磁紀錄內容與其所列印成書面之內容，若其同一性有問題時，法院應依聲請或依職權命鑑定，或傳喚列印人員出庭應訊，據以判斷何者為真正。

乙說：除依一般經驗法則予以判斷外；尚須慎重考慮前項形式證據力乙說所舉各款之證明者。

2、新書證說[85]

（1）立論依據[86]

A、本說又稱生成文書說。[87]

[84] 曹鴻蘭，同前註 67，頁 140。

[85] 此說爲日本民事訴訟法學者通說，參見曹鴻蘭，同前註 67，頁 144，駱永家發言。

[86] 曹鴻蘭，同前註 67，頁 139。

B、本說注重電磁紀錄之機能、存在形態及其使用目的等而認為是書證。因電磁紀錄具有保存，傳達意思之機能，雖其原狀並不能閱讀，但可列印成為可閱讀狀態之書面，所以可用「可能文書」稱之。

C、訴訟當事人把要作為證據資料之電磁紀錄內容有關部分列印成文書狀態（生成文書）作為證據原本，提出法院予以調查。當事人如無異議則只就所提出之文書（生成文書）加以調查；但如當事人對提出之生成文書與可能文書之同一性等有異議，則要進一步以勘驗或鑑定方式調查之。[88]如此既符合訴訟經濟原則，又可迅速、容易達到其調查之目的[89]。

D、若要以可能文書所保存紀錄內容為證據時，並證據調查程序要點如次：

（A）應將電磁紀錄內容列印成文書，稱此文書為「生成文書」。

（B）並由負責列印為生成文書的人員，在其書面上簽署捺印，以完成生成文書之文書形式，並以此為證據原本，提出法院調查之。

（C）本說認為生成文書是證據原本，電磁紀錄帶等本身為用以作成該原本之資料而已。

（D）惟生成文書與可能文書記載內容之同一性發生問題時，則應以鑑定方法調查之。

---

[87] 丁秋玉，同前註 25，頁 156。

[88] 夏井高人，同前註 82，頁 143，日本評論社，1993 年，轉引自丁秋玉，同前註 25，頁 155。

[89] 曹鴻蘭，同前註 67，頁 140。

（2）形式證據力[90]

此說認為以所列印呈現文書為證據原本，所以其形式證據力之證明，以與一般書證相同之證明即可。亦即有正確的輸入紀錄，且在電腦正常機能時輸入的、經嚴格的列印其紀錄為文書；並由列印人等在該文書上簽署證明等。

（3）實質的證據力[91]

A、關於輸入電腦之正確性問題，則以傳喚電腦程式設計員、操作員、管理員等予以訊問證明之。

B、至於電磁紀錄內容與其生成文書記載內容之同一性有問題時，則以在法官面前操作電腦，列印其電磁紀錄帶為畫面之鑑定方法為之。

3、物證說[92]

（1）立論基礎

A、不具可讀性的電磁紀錄帶等為非文書性質之證據原本，故應以勘驗、鑑定方法調查之。

B、電子證據係能借助特定工具和技術加以蒐集並分析的各種磁性物質和電脈衝物質形成的，雖不似其他形式之物證如指紋、DNA、槍械武器、電腦零件等具有一定形體，惟仍應屬於物證。

C、許多國家司法實務上亦承認，電子證據或電磁紀錄可予以搜索扣押，既得以實施搜索扣押，則當屬物證範疇。

[90] 曹鴻蘭，同前註 67，頁 140。
[91] 曹鴻蘭，同前註 67，頁 140。
[92] 曹鴻蘭，同前註 67，頁 139。

（2）證據調查程序要點：

書證之形式證據力得依法官之直接判斷而形成，但是由於電磁紀錄內容，法官無法以直接觀察方法加以閱讀，所以電磁紀錄之內容，如與其所列印呈現之文書同一性發生問題時，法院仍然可依職權或聲請以勘驗或鑑定方法調查而已，因而主張應依勘驗方法調查之。

（3）調查程序為：

A、法院決定勘驗後；

B、指定鑑定人並命該鑑定人製作列印紀錄內容顯現為文書之電腦程式（Program）或用由當事人提出並經鑑定人等審查認為合適之電腦程式，在法官面前列印其紀錄內容為文書；

C、且將其勘驗過程與結果作成勘驗筆錄，並將其文書附卷作為證據之一部份；

D、應以電磁紀錄磁帶或磁片等為證據原本，與電腦程式一起提出法院，供法院調查。

4、獨立證據說[93]

獨立證據說認為任何一種傳統證據都無法將電子證據完全涵涉在內，然而電子證據在司法活動地位日形重要，應用機會愈來愈多，因此應將電子證據視為一種獨立的證據類型。

5、混合證據說[94]

本說與獨立證據說的出發觀點相同，均認為電子證據

[93] 何家弘，同前註 20，頁 24。

[94] 蔣平，計算機犯罪問題研究，頁 253-254，商務印書館，2000 年 8 月。

不屬於任何一種傳統的物證。惟此說從法安定性的角度認為電子證據並非獨立的新型證據，而是若干傳統證據的組合或混合。電子證據應就相同的證明機制，歸類至傳統證據類型中的某種證據，不應另行創設證據種類及法則。

本說先設定電子證據有以下三種：

（1）電腦輸入、存儲、處理（包括統計、綜合、分析）、輸出的數據；

（2）按照嚴格的法律及技術程式，利用電腦模擬得出的結果；

（3）按照嚴格的法律及技術程式，對電腦及其系統進行測試得出的結果。

從載體性質來看，如果輸入、存儲的資訊紀錄在諸如硬碟、磁碟、光碟等介質上，即為準書證，在保證此類介質的內容能固定、不會消失或修改的情況下，電子證據可視為書證；電腦處理過的資訊如果仍儲存在上述介質上，同樣仍被視為準書證及書證；如果輸出列印到紙張上，當為書證。從輸出的形式來看，如果以紙張形式表現，即為書證；如果以聲音、圖像形式表現，即為視聽資料[95]。

又，利用電腦模擬是根據已知條件和事實，依照法律與技術之要求電腦進行演算，以確定結果發生的概然率；因此，模擬的結果可列為物證勘驗項目。

再者，對電腦及其系統進行測試，是運用軟體按照法律對電腦及系統的性能、受損情況等進行測量、測算、鑑定，從而確定犯罪的危害程度，因而可列為鑑定結論證據[96]。

---

[95] 視聽資料爲大陸獨特的證據種類，於「7、視聽資料說」說明。

[96] 蔣平，同前註 94。

6、視聽資料說[97]

此說為大陸獨特學說，大陸民事訴訟法、行政訴訟法及刑事訴訟法修正草案均規定視聽資料為獨立證據類型。且學說及實務界均認為其內涵包括錄音資料、錄像資料、電腦存儲資料和其他音像證據等。實務上大陸最高人民檢察院在「檢察機關貫徹刑訴法若干問題的意見」第三條第一款規定「電子計算機內存信息」屬於視聽資料。

採此見解之其理由主要為：

（1）視聽資料是指可視、可聽的錄音帶、錄像帶之類的資料，電子證據可顯示為「可讀形式」，因而也是「可視的」；

（2）視聽資料與電子證據在存在形式上有相似之處，都是以電磁或其他形式而非文字符號形式儲存在非紙質的介質上；

（3）存儲的視聽資料及電子證據均需借助一定的工具或以一定的手段轉化為其他形式後才能被人們直接感知；

（4）兩者的正本與複本均沒有區別；

（5）把電子證據歸於視聽資料最能反映他的證據價值。

2.4.2 本文之意見

本文以為上開各說均有未殆之處，

1、書證說之問題點

A、電子證據有時是人為輸入（Key-in）而成，若輸入後未保存原始底稿，或係在沒有底稿的情況下直接輸入的，於此種情況下，都很難認定何者係電子證

[97] 何家弘，同前註 20，頁 19-20。

據的原本[98]。

B、書面形式並不等同於書證，某一事物屬於書面形式則不一定得出其就是書證，如勘驗筆錄、鑑定結論、以及部分當事人陳述、證人證言、甚至視聽資料都可能是書面形式，但並不一定是書證[99]。

C、訴訟當事人聲明證據時，原則上應向法院提出電磁紀錄帶之原本及其繕本與程式。斯時或因原本無法或難於自電腦取出，或會將不相干而不應調查部分之紀錄內容也同時被列印成文書提出法院，是則該部分之秘密性就易遭法院或他造當事人所窺知侵害[100]。

D、電子證據原本經提出法院後，為免遭篡改，原則上以由法院保管為當。惟當事人如因業務上需要用該原本時，若不准，有妨害該當事人業務之嫌，若准許則怕被篡改[101]。

E、書證說難以圓滿回答電腦聲像資料、網絡電子聊天資料的證明機制問題[102]。

2、新書證說之問題點

該說以生成文書為證據原本，則其與電磁紀錄原本（可能文書）間成為雙重原本，有不合理之處[103]。

[98] 何家弘，同前註 20，頁 22。
[99] 何家弘，同前註 20，頁 22。
[100] 曹鴻蘭，同前註 67，頁 140。
[101] 曹鴻蘭，同前註 67，頁 140。
[102] 何家弘，同前註 67，頁 22。
[103] 曹鴻蘭，同前註 67，頁 140。

3、物證說之問題點

A、勘驗是為了認識事物之存在、性狀、形態等之調查證據方法，所以作為認識電磁紀錄內容如何之調查證據方法似不恰當[104]。

B、該說主張在法官面前操作電腦，列印電磁紀錄為畫面之調查證據方法過於繁瑣，不符合訴訟經濟及妨害訴訟指揮之流暢[105]。

C、此說之適用範圍僅涉及了電子證據的一部分，即數位式電子證據，故有一定的侷限性[106]。

D、電子證據被許可採用之前，不存在對其可信度進行判斷的問題；換言之，只有在電子證據已被採用的前提下，才需要專家就其真偽進行分析判斷，才需要法院依據專家的鑑定結論確定其是否能作為認定事實的根據[107]，此說漏未注意此等前提，自有闕漏之處。

4、獨立證據說問題點

電子證據與傳統證據相比，不需要創設一種全新的證明機制，僅以外在形式的不同遽認應創設獨立證據項目，雖在一定程度上強調了電子證據的重要性，惟有過於輕率之嫌[108]。況且，主張此說者並未說明在證據調查上應採用何種調查證據之方法。僅高唱獨立視之，未能提出具體操作方法，尚有未洽。

[104] 曹鴻蘭，同前註 67，頁 140。
[105] 曹鴻蘭，同前註 67，頁 140。
[106] 何家弘，同前註 20，頁 23。
[107] 何家弘，同前註 20，頁 24。
[108] 何家弘，同前註 20，頁 25。

5、混合證據說問題點

該觀點有關三種電子證據形式的概括性並不周延，亦未考量電資訊科技或子證據未來的可能性；況且，以輸出形式來區分書證與視聽資料的做法亦未提出理論依據[109]。

6、視聽資料說問題點

A、法律上將視聽資料與其他證據相區分，強調的是以聲音和圖像而非文字內容證明案件的真實情況，將電子證據中文字的「可視」與視聽資料中的「可視」混為一談，並無充分理由。且亦難以解釋其他文書、鑑定結論、勘驗筆錄等證據亦為「可視的」，何以未被推論為視聽資料[110]。

B、將電子證據視為視聽資料不利於電子證據在訴訟中充分發揮證據的作用。因為大陸民事訴訟法第六十九條規定，人民法院對於視聽資料，理應辨別真偽，並結合本案的其他證據，審查能否作為認定事實的依據，亦即認為視聽資料屬間證據性質，需要輔以其他證據以為判斷。因此設若某一案件只有堅強的電子證據可以作為直接證據，但因被歸類為視聽資料，造成即使該證據真實可靠，也會因無其他證據結合使用，而不能作為認定事實的根據[111]。

本文一再強調：電腦時代來臨的時間非常短，而且進步速度非常快，不僅是改變的吾人日常生活、政治、金融...等等層面，各種過往幾千年來以各種形式保存以及紀錄的資訊，也都變成可以數位化，無一例外。因此，數位化資料被當成證據，也就是電子證據出現的時間非常短，其載體、形

[109] 何家弘，同前註 20，頁 25-26。

[110] 何家弘，同前註 20，頁 20。

[111] 李學軍，「電子數據與證據」，頁 445-446，證據學論壇，第 2 卷，中國檢察出版社，2002 年 2 月。

態、呈現方式等層面也一直迅速的在變化，此時要將電子證據建立體系以及作完整的討論，是非常困難的。Alan M. Gahtan 亦稱：「在審判中使用電子證據的最大挑戰在於，不能輕易地將其劃歸傳統的證據類型。」[112]

但是另一方面，電子證據同傳統證據相比，不同之處主要在於其載體，而非證明機制方面。電子證據並非一種全新的證據，而是傳統證據以另一種形式呈現。所有傳統證據均有可能以電子證據形式之形式存在與呈現[113]。

本文之見解採取新文書證據說，惟略加修正，茲敘述理由如下：

1、文書的傳統定定義在於可閱讀的記載狀態，且具有保存及傳達人的思想或意思。因為電磁紀錄具有保存、傳達意思之機能，雖其原狀為二進位制不能直接閱讀，但可透過列印成為可閱讀狀態之書面，此為新文書證據說之觀點。

2、本文以為若就新文書證據之內涵再加推衍：

「因為電磁紀錄雖非用文字所作成而與通常之文書有異，但係利用二進位制電磁組合對於文字、圖像、聲音或影像予以紀錄，具有保存、傳達意思之機能，雖其原狀為二進位制不能直接閱讀，但可透過列印、顯示或播放等方式重現成為人類可透過感官理解之狀態，則相當於文書之閱讀，而應以修正之文書證據相應規範之[114]。」則可以滿足基於電磁紀錄特性而賦予其新意義。

---

[112] *See,* Alan M. Gahtan，*Supra* note 8，p.138，原文爲：「The biggest challenge to the use of computer-produced data as evidence at trial is that it does not fall comfortably within the traditional classification of evidence.」

[113] 何家弘，同前註 20，頁 27。

[114] 本定義係參考曹鴻蘭，同前註 67，頁 158-159，邱聯恭教授見解而擬之。

如依此標準檢討前開學說分類，

1、電子物證如在入侵電腦犯罪中，入侵者在所侵入的電腦系統中留下的關於電子痕跡（Electronic Fingerprint），因為這種痕跡是電腦自動生成的，而且是以其存在狀態來證明案件事實。而且電子痕跡可以視為數位虛擬空間的物質交換原理[115]。因此不論是以電腦自動生成紀錄之觀點或物質交換觀點來看，顯然不適用傳聞證據規則，僅主張其真實性即可。[116]

2、電子形式的「書證（Document Evidence）」，因為記載了當事人之間的意思表示。因此在被法庭採用前，除法律別有規定例外接納之情形外，本即必須接受傳聞證據法則、最佳證據法則與驗真法則的檢驗。[117]

3、數位形態的聲音、影像及圖像等證據，亦應回歸前述二種區辨方法，亦即電腦自動生成紀錄者，如便利商店監視錄影畫面、固定式超速照相機所拍攝汽車照片等，以自動生成之電子紀錄視之，僅證明其真實性即可；至於有人為因素介入者，如警員以電腦繪製之交通事故現場圖、監控時所拍攝之影像及畫面，則應以傳聞證據法則、最佳證據法則與驗真法則的檢視之。

4、各種電子聊天紀錄、電子監控紀錄等，不論為聲音或影像，均屬於典型傳聞證據（Hearsay Evidence），應當符合法定取證程序以及傳聞法則之規範。[118]

---

[115] 物質交換原理，又稱爲羅卡德物質交換原理，是法國刑事科學家 Edmond Locard 博士於 1928 年提出，後人稱爲羅卡得交換原理（Locard Exchange Principle）。此原理主張「當兩個物體發生接觸時，產生相互轉移作用，使得其中一物體上之物質轉移至另一物體上」。美國鑑識科學之父 Paul Kirk 博士進一步修正該原理爲「嫌犯不可能不遺留證據在犯罪現場，以及帶走原本於現場的證據」。在犯罪活動中，作案人不可避免地要將自身原有的物質全部或部分地遺留於犯罪現場被侵犯的客體上，同時還會從現場及被侵犯的客體上帶走某些物質，形成物質交換現象。電腦入侵犯罪中存在物證，正好表明物質交換原理同樣對虛擬犯罪空間適用。

[116] 何家弘，同前註 20，頁 28。

[117] 何家弘，同前註 20，頁 29。

[118] 何家弘，同前註 20，頁 29。

5、對電子證據之鑑定以及勘驗，回歸證據規則中相關規範即可。亦即對電子證據之真偽有爭執時，法庭可以傳統物證調查方式予以勘驗或鑑定。

6、前述生成文書為證據原本，則其與電磁紀錄原本（可能文書）間成為雙重原本之問題，本文以為係對本說之誤會。因本說認為電磁紀錄不易為人類理解，始以列印或顯示方式呈現於法庭，並非謂有另一原本產生。至於法院或雙方當事人對該生成文書提出異議，可就所提出之異議之點加以調查，或以更為精確之方式列印或顯示即可，並非有雙重原本產生。[119]

2.5 電子證據的學理分類

1、靜態電子證據與動態電子證據[120]

（1）區分依據

根據電子證據是數位化資訊處理、存儲、輸出設備中存儲、處理、輸出的證據，還是數位化資訊網絡中傳輸的證據，可以將其分為靜態電子證據和動態電子證據。

[119] 爲避免生成文書在法庭中遭質疑，實務上有一種作法是在執行搜索扣押後，將犯罪證據之電磁紀錄列印，要求犯罪嫌疑人閱覽無誤後簽名捺印，以證明列印之紙本與電磁紀錄原始內容無別。臺灣臺北地方法院檢察署 90 年度偵字第 22929 號聲請簡易判決處刑書：「…臺北縣警察局三峽分局員警於 90 年 9 月 1 日在電腦網路發現並列印上開訊息後，即撥打前述行動電話與被告聯絡佯稱性交易並相約見面，嗣經警於 90 年 11 月 9 日 11 時 10 分許，在臺北市忠孝東路、復興南路口第一商業銀行前當場查獲，並扣得行動電話一支行動電話一支（內含門號 0917xxxxxx 號ＳＩM卡一枚）等情，業據被告於警詢及偵查中陳述無訛，核與證人即查獲本案之員警陳○○於偵查中之證述互核一致，證人陳○○於偵查中到庭證稱「該信息列印資料確於警詢中提示被告確認後始由被告簽名 、捺印」等語明確…」。警察偵查犯罪規範，第 4 章第 17 節，第 232 點規定：「執行電腦搜索應注意事項：（四）電腦檔案之證據應當場列印，並請受搜索人簽名按指印。」，內政部警政署，民國 92 年 8 月 12 日。

[120] 皮勇，同前註 20，頁 9-11。

（2）意義

靜態電子證據，是指數位化信息處理、存儲、輸出設備中儲存、處理、輸出的證據，包括電腦系統中存儲的電腦文件、影音檔案等。其他被保存在電腦外部儲存設備中，如硬碟、軟碟、光碟中，這些存儲介質上的電磁紀錄亦屬於靜態電子證據。

動態電子證據，是指數位化信息網路中傳輸的電子證據，包括數位化資訊網絡中傳輸的電子郵件和數據電文、下載中的電腦文件、瀏覽中的網頁、網路播放串流式（Streaming）影像及音樂檔案。這類電子證據的共同特點是沒有固定附著於某一電磁介質上，而處於數位化資訊網絡的通信傳輸中，其傳輸的途徑可以有多種，既可以是有線數據通信線路中傳輸，也可能是中間通過無線通信線路傳輸，甚至完全通過無線通信線路傳輸。

（3）區分實益

靜態電子證據因為已經固定，因此，在蒐集這些電子證據時可以使用搜查、扣押等調取書證、物證所使用的偵查措施。且於提出靜態電子證據時，若這些靜態電子證據自形成之後沒有因人為因素發生變動，並且電腦資訊系統的正常運作沒有影響其完整性，或者相應存儲設備沒有受外界因素影響而損壞，應推定這些證據具有真實性。

至於動態電子證據，因為是處於數據傳輸過程中，在通信網絡中保存的時間很短，如果不能在電腦數據通信過程中即時截收，可能無法獲取這種電子證據，因此，蒐集動態電子證據具有即時性。此外，動態電子證據之蒐集不阻礙數據通信正常進行，而係以技術方法對往來數據以複製之方法截留之，此舉可能過度侵犯人民通信自由與隱私權利，因此蒐集此種動態電子證據需要嚴格的限制條件，如適用的犯罪範圍、有關權利保障條

件等，法院在採用動態電子證據前應更加注意蒐集動態電子證據方法的合法性。[121]

2、類比式電子證據與數位式電子證據[122]

（1）區分依據

根據攜帶資訊方式的不同，電子證據可分為類比式電子證據與數位式電子證據。

（2）意義

類比式電子證據是透過資訊中的某些特徵的具體數值或量（如電壓信號的幅度、降位、頻率、脈衝信號的幅度或持續時間等）來記載電子信息的內容，如第一代類比式行動電話、有線電話所錄下的各種通話內容基本上屬於此。

數位式電子證據則是通過信號的離散狀態的各種可能組合所賦予各種數值或其他資訊的方法來承載電子資訊的內容，如第二代行動電話（GSM）所錄下的各種通話內容。

（3）區分實益

由於藉助電子技術的性質不同，類比式電子證據與數位式電子證據之間存在著一些明顯差異：

A、前者在複製時有一定的損耗，其複本與正本相比有一定的區別，而後者的正本與複本則基本完全一致；

[121] 我國新修正之通訊保障及監察法規定自民國 96 年 12 月 11 日起，進行通訊監察需取得法院核發之通訊監察書，該法第 5 條及第 6 條規定非法通訊監察所取得之證據資料須經法院審酌一定之情況下始有證據能力，否則應予排除。第 7 條則對非法取得之證據資料完全排除其證據能力。民國 96 年 7 月 20 日司法院大法官會議解釋第 613 號亦揭明：「爲制衡偵查機關之強制處分措施，以防免不必要之侵害，並兼顧強制處分目的之達成，則經由獨立、客觀行使職權之審判機關之事前審查，乃爲保護人民秘密通訊自由之必要方法。是檢察官或司法警察機關爲犯罪偵查目的，而有監察人民秘密通訊之需要時，原則上應向該管法院聲請核發通訊監察書，方符憲法上正當程序之要求。」均係採相同之概念。

[122] 何家弘，同前註 20，頁 31-33。

B、前者在技術上剪輯較為困難，若刪改後必然會破壞資訊的連續性，這樣刪改痕蹟很容易被識別，而後者是以離散的電磁或光學信號等物理形式存在的，可被輕易地改變或刪除，且不易被發覺。

類比式電子證據與數位式電子證據在證據價值方面各有優劣：

1、在真實性方面，類比式電子證據更容易防止偽造，優於數位式電子證據；

2、在證明力方面，數位式電子證據的複製件更為精確，其證明力一般大於類比式電子證據。

3、數據電文證據、附屬信息證據與系統環境證據[123]

（1）區分依據

此係由檔案學與鑑定學之觀點所提出的分類。依檔案學之觀點，對於電子檔不僅要保存數據本身，還要保存「元數據」，即該檔產生的時間、地點、形成者及形成機構的職能背景、業務活動的經過表述、數據形成及存儲方式等。

依照鑑定學，任何電子數據都離不開特定的系統環境，雖然從理論而言較高版本的軟體應能相容較低版本的軟體，但特定電子數據只有借助其原始的系統軟硬體環境才能得到最真實的顯現，所以電腦鑑識專家必須蒐集並使用原始系統環境尤其是軟體系統環境才能正確開展鑑定工作多如果將這些原理適用於電子證據，就會發現電子證據實際上包括數據電文證據、附屬資訊證據與系統環境證據。

[123] 何家弘，同前註 20，頁 33-34

（2）意義

數據電文證據，是指表達一定意思表示之電磁紀錄本身，即記載法律關係發生、變更與滅失的數據，如 E-Mail、EDI 的正文。

附屬信息證據，是指對表達一定意思表示之電磁紀錄生成、存儲、傳遞、修改、增刪而引起的紀錄，如電子系統的日誌紀錄、電子檔的屬性資訊等，它的作用主要在於證明電子數據的真實性，即證明某一電子數據是由哪一電腦系統在何時生成的、由哪一電腦系統在何時存儲在何種介質上。由哪一電腦系統或 IP 地址在何時發送的以及後來又經過哪一電腦系統或 IP 位址發出的指令而進行過修改或增刪等。

系統環境證據，是指表達一定意思表示之電磁紀錄運行所憑藉的硬體和軟件環境，即某一電子數據在生成、存儲、傳遞、修改、增刪的過程中所依靠的電子設備環境，尤其是硬體或軟體名稱和版本。

（3）區分實益

這三種證據所起的證明作用不同。

數據電文證據主要用於證明法律關係或待證事實，它是主要證據；

附屬資訊證據主要用於證明數據電文證據的真實可靠，它像用於證明傳統證據保管環節的證據一樣，必須構成一個完整的證明鎖鏈，表明每一數據電文證據自形成直到獲取、最後到被提交法庭，每一個環節都是有據可查的，也構成一個證據保管鏈條；

系統環境證據則主要用於在法院審理時或鑑定時顯示該電磁紀錄的證據，以確保該數據電文證據以其原始面目展現在人們的面前。

此種分類顯示理想之電子證據應當具有此三大部分，於蒐集電子證據時應當同時蒐集此三部分，以確保得以構成完整資訊。

4、電腦生成證據、存儲證據與混成證據[124]

（1）區分依據

參考國外學者關於電子證據分類得出的結論，亦即按照電子證據形成的方式進行的分類。

（2）意義

電子設備生成證據，是指完全由電腦設備自動生成的證據。這一種電子證據的最大特點是，它是完全基於電腦設備的內部命令運行的，其中沒有摻雜人的任何意志，亦即毫無人為陳述滲雜其間[125]。例如以提款卡在自動提款機（ATM）上提款時，自動取款機對所輸人密碼是否正確、取款的時間、數額、交易流水序號等的紀錄，即屬此類，又如 ISP 服務商的伺服器對登入者所留下之紀錄。[126]

電子設備存儲證據，是指純粹由電腦設備錄製人類的資訊而得來的證據，如對他人電話交談進行秘密錄音得來的證據，又如由人將法律條文輸入電腦形成的證據等。

---

[124] *See* Alan M. Gahtan，*Supra* note 8, p.138，原文爲：「Computer-produced Evidence means：1、documentary evidence which originates from a person, and where the computer is primarily being used as an electronic filing cabinet；2、electronic data corresponding to events monitored and recorded by the computer without human intervention (for instance, long distance telephone calls made by hotel guests)；3、and data generated by the computer where the computer is used to interpret or analyze data supplied directly by external sensors (such as a breathalizer or a radar speed gun).」

[125] 張斌著，視聽資料研究，頁 186，中國人民公安大學出版社， 2005 年 11 月。

[126] 同前註。

電子設備混成證據，即電腦儲存兼生成證據，是指由電腦等設備輸入資訊後，再根據內部指令自動運行而得來的證據。如財務人員將收支各項明細輸入電腦後，電腦再自動計算收支總額，最後得出當天、當次的收支明細表以及帳面餘額等，即屬此類證據。[127]

（3）區分實益

就電子設備生成證據而言，無須進一步核實該調查結果的準確性，它至少告訴我們兩點：其一，電子設備生成證據是準確性相當高的證據；其二，影響電子設備生成證明力大小的因素主要是其準確性。

至於後兩類證據，就證明力大小的判斷，除了要考慮電腦設備的準確性外，還要考慮輸入時是否發生了影響輸入準確性等人為的因素。因此有傳聞證據規則、最佳證據規則與驗真規則的適用。

（4）類似見解

本說第二存儲證據與第三混成證據間似無區別之實益，因均具有共同的特徵，亦即有人為因素、意思或操作介乎其中，因此亦有將之合併而為「電腦儲存紀錄（Computer-stored records）」及「電腦產生紀錄（computer-generated records）」二種者，此二種之意義及區辨已如前述，茲不贅述。

5、原本電子證據與複本（派生）電子證據

因為文書原本具有較高的證明力，所以法院較易接納為認定待證事實之依據，文書複本必須在原本滅失或難以取得、其與原生證據吻合、且採用它不會導致對當事人不公平等情況下，方能採用之[128]。提出文書複本之一方必須對於原本

[127] 張斌，同前註 125。

[128] 何家弘，同前註 20，頁 39-40。

滅失或難以取得、與原生證據吻合、不會導致對當事人不公平等一一舉證說明外，法院採證上的證明力也不會高於文書原本。

惟電子證據係以「0」與「1」之二進位制形態存在於磁性或光學載體上，人類直觀知覺難以理解判斷，必須以列印、顯示等方式呈現後，始得為人類所理解及判斷。又電子證據可以大量、無誤差的複製，因之電子證據何者為原本、何者為複本，又複數複本間各複本之證據力如何，均有研究之必要。

（1）區分依據

電子證據究竟在什麼情況下可以認定是來自於原始出處之為原本或複本？在討論採認電磁紀錄為證據之過程中一直迭為學者所爭執，已如前述。且由技術層次以觀，電子證據在電腦系統中生成、複製及傳送等層面也滋生許多問題，

A、若電腦設備自動生成之電子證據，此時在訴訟過程中必須列印或顯示出來才能為人類所認知及理解，則究竟是電腦內部電子形式之數據是電子證據原本，抑或是電腦列印輸出者為原本，或是由電腦螢幕（顯示器）所顯示之資料才是電子證據原本？

B、又若某一電子證據屬於電子設備紀錄證據或混生證據，則是否應將紙本底稿或操作及輸入之有關人員內心意思視為原本，將其他證據均視為複本[129]？

C、網路上的電腦系統運作所產生的電子證據，其原本與複本又當如何加以區分？例如賣方以電子郵件形式向買方發出要約，此時該電子郵件會在要約人電腦、要約人郵件伺服器（Mail Server）內、承諾人

[129] 何家弘，同前註 20，頁 40。

郵件伺服器[130]內及買方電腦內均有內容相同之該份電子郵件，則何者應視為電子郵件之原本？

目前區分電子證據原本複本之學說如下：

A、傳統文書證據規則之觀點[131]

電子證據之原本係指電子數據首先初次固定於磁性載體上者。亦即若該電子證據首先固定於某電腦設備硬碟上，則該硬碟上之電子形式證據即為原本電子證據；若電子證據首先固定於磁帶、軟碟片或光碟上者，則磁帶、軟碟片或光碟上的電子形式證據即為原本。除此之外任何由此原本複製、列印或顯示之電子證據均為複本。[132]

本說符合傳統文書證據之見解，惟此說將原本界定為首次固定於磁性載體者，則在有電磁紀錄收受對造之一方將永遠無法在訴訟中提出電子證據之原本。以前開電子郵件要約與承諾之例，買受人將永遠只能提出系爭電子郵件之「複本」，在訴訟上未盡公平。

B、同一性說[133]

本說認為從電腦信息裏面只有標準化、構造化的資料（Data），沒有與紙文書相同的原本性因素存在。電子數據雖然無可讀性、可視性，但依照當事

[130] 就技術角度來形容電子郵件之收受，電子郵件寄至收件人郵件伺服器後，當收件人以 POP3 形式（例如 Outlook Express）接收電子郵件時，電子郵件收件軟體連結至郵件伺服器，核對帳號密碼無誤後，會將電子郵件已複製之方式下載至收件人電腦端。此時，郵件伺服器中之電子郵件仍然存在，必須收件人設定將電子郵件在接收後刪除存在伺服器中之郵件，伺服器始會將存於其內之郵件刪除。以 Outlook Express 爲例，該選項設置在「帳號／進階／遞送／在伺服器保留郵件備份」。許多窺探他人電子郵件妨害秘密之案件，即是利用此一特點，再未經授權接收他人郵件後保留伺服器端之電子郵件，則原收件人因爲沒有「漏信」、「掉信」等情形，將不易發覺自己電子郵件被他人接收。

[131] 馮大同編，國際貨物買賣法，頁 304，對外貿易教育出版社，1993 年 5 月。

[132] 蔡墩明，同前註 69，頁 211。

[133] 何家弘，同前註 20，頁 45。

人的意思，若透過轉換方式變為可讀的、可視的，此時應視為該電子證據與列印出的紙本文件一起構成原本。亦即原本電子證據是電子形式證據與列印出來的證據具有同一性，且二者均為原本。[134]

惟本說不適用於電子證據量大無法列印之情形，也無法依此而界定電子證據複本為何。

C、擬制原本說

(A) 學說

從電子證據之特性觀察：

a、電子證據須藉由列印或顯示方式始能為人類所感知理解，其不與傳統證據可直接為人感知理解有別，故而列印或顯示之行為應非界定電子證據原本與否之標準；

b、電子證據之移轉是以複製方式為之，不似傳統證據僅有一份，在轉移後中會造成在原處的滅失之情形。職故，以電子證據是否源於原始出處一節來判斷電子證據原本亦未盡妥適；

c、電子證據欲長時間保存，須以複製的方式為之，是故電子證據很難永遠保存在所謂「首先固定於其上的磁性載體」上，以此觀點而論，即使是電子證據之原本亦可能是複製而來的。

故而以此等特點以觀，欲界定電子證據之原本或複本，傳統觀念均有改變之必要[135]。

---

[134] 安富潔，ハィテク犯罪與刑事手續，頁 261 以下，慶應義塾大學法學研究會， 2000 年 7 月。轉引自丁秋玉，同前註 25，頁 145。

[135] 何家弘，同前註 20，頁 46。

（B）立法例

a、聯合國貿法會之觀點

聯合國貿法會在前述電子商務示範法第八條「原本」中規定：

「1、如法律要求資訊須以其原始形式展現或留存，倘若情況如下，則一項資料電文即滿足了該項要求：

（a）有辦法可靠地保證自資訊首次以其最終形式生成，作為一項資料電文或充當其他用途之時起，該資訊保持了完整性；和

（b）如要求將資訊展現，可將該資訊顯示給觀看資訊的人。

2、無論本條第 1 款所述要求是否採取一項義務的形式，也無論法律是不是僅僅規定了不以 原始形式展現或留存資訊的後果，該款均將適用。

3、為本條第 1 款（a）項的目的：

（a）評定完整性的標準應當是，除加上背書及在通常傳遞、儲存和顯示中所發生的任何變動之外，有關資訊是否保持完整，未經改變；和

（b）應根據生成資訊的目的並參照所有相關情況來評定所要求的可靠性標準。

4、本條的規定不適用於下述情況：[...] 」[136]

[136] 原文爲 Article 8：「Original

1. Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) Where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

2. Paragraph 1 applies whether the requirement therein is in the form of an obligation or whether the

準此，只要該數據電文具完整性、且可以顯示，即可視為符合法律對原本的要求。換言之，若該數據電文

（1）係直接輸入於電腦中，

（2）自首次成為電子形式起即保持完整未予改動，且

（3）後來可顯示為人們可知的形式，則不違反原本的要求；

即便該數據電文最初為書面形式，惟事後符合前開三項要件，亦承認其為原本而不違反原本的要求。

聯合國貿法會的觀點維護電子證據原本之真實可信度，然學者以為此種區分標準有其侷限性，僅可視為區分電子書證原本與複本之方法，不能適用於一切電子證據[137]。

b、美國之觀點

美國聯邦證據規則第一００一條第三款規定：

「原本文書或紀錄之「原本』，係指文書或紀錄之本身，或其製作人或發行人有意使之與原本有相同效果之相等物。照像之「原本』

law Simply provides consequences for the information not being presented or retained in its original form.

3. For the purposes of subparagraph (a) of paragraph 1:

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

4. The provisions of this article do not apply to the following: [...].」

[137] 何家弘，同前註 20，頁 43。

包括負片與其任何印製物，如資料係儲存於電腦或類似裝置，其印出物或其他輸出物得以視覺閱讀，且顯示正確反應資料者亦為「原本』」[138]。第 4 款規定：「『複本』係指以原本之同一版本或從相同之模體所製作，或以照像之方法，包括放大縮小，或以機械或電子重複錄製，或以化學再製，或以能精確翻印原本之其他相同技術所製作之相等物。」

依前開規定，電子證據於以下兩種情況下屬於原本：

（1）當有關之電磁資料係存儲在電腦內，且該電磁資料所產出能以視覺閱讀，並能準確反映資料之印出物或其他輸出物；

（2）製作者或發行者有意使複本之電子證據具有同文書本身具有同等效力。

美國立法例擴大了傳統對於原本的界定，亦即不限於自然意義上的原本證據，而且擴大至擬制意義上的原本證據。

學者以為聯合國貿法會與美國聯邦證據規則等立法

[138] U.S. Federal Rules of Evidence, Rule 1001. Definitions

「For purposes of this article the following definitions are applicable:

(3) Original. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

(4) Duplicate. A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.」

例，對於原本證據已推衍至不以自然意義上之原本為限，亦可能是人為擬制之原本。本文亦採此見解，並認為此見解與前述修正式之新文書說相契合。

表 2-3　電子證據原本與複本之區分標準

	文書說	同一性說	擬制原本說
意義	電子證據之原本係指電子數據首先初次固定於磁性載體上者。除此之外任何由此原本複製、列印或顯示之電子證據均為複本	電子證據原本是電子形式證據與列印出來的證據具有同一性，且二者均為原本。	電子證據之原本係指該電子數據本身；或製作者或發行者有意使其具有同等效力的複本；至以電子的再錄制方法，或以其他能正確複製原件的相應技術而產生者，則為複本
依據	由傳統文書證據見解衍生而來		聯合國貿法會電子商務模範法第 8 條、美國證據規則第 1001 條
問題點	此說將原本界定為首次固定於磁性載體者，則在有電磁紀錄收受對造之一方將永遠無法在訴訟中提出電子證據之原本，在訴訟上未盡公平。	本說不適用於電子證據量大無法列印之情形，也無法依此而界定電子證據複本為何。	
本文之見解	1、對於原本證據已推衍至不以自然意義上之原本為限，亦可能是人為擬制之原本。 2、此見解與前述修正式之新文書說相契合。		

資料來源：本文整理

（2）意義

採聯合國貿法會與美國聯邦證據規則之區分標準，可以得知：

電子證據之原本係指該電子數據本身；或製作者或發行者有意使其具有同等效力的複本；不侷限於資訊首先固定所在之磁性載體，而係對當事人而言具有法律效力、具最終完整性之數據資料。任何直接源於該電子數據的列印輸出或其他可感知之輸出物，設若能準確地反映該紀錄內容，均可視為原生電子證據。

電子證據複本指以電子複製之方法，或以其他能正確複製原本的相應技術而產生者，則為複本[139]。

（3）區別實益

若以美國證據制度之角度以觀，電子證據是否為「原本」涉及該國最佳證據法則（The Best Evudence Rule）之問題，在該證據法則之要求下，訴訟中充為證據之文書，除法律別有規定得以複本代之外，必須提出文書之原本以供檢閱。[140]

我國未有如最佳證據法則之規定，惟訴訟中是否提出原本以供檢閱，將會影響法院對該文書證明力之判斷。此部分於第五章敘述之。

6、其他分類

按法律上對相同之事務，應為相同之處理；不同之事務，則應為不同之處理。因此對於各種法律概念的區分，必須要有區分之實益，亦即不同的的法律概念，必須有不同之法律效果，否則及無區辨之意義。

[139] 何家弘，同前註 20，頁 47。

[140] 丁玉秋，同前註 25，頁 148。

關於電子證據之文獻上尚有如下三種分類，為本文以為在法律上並無區別之實益，亦即法律效果上並不明顯，惟亦可作為概念之釐清，故一併列出以述之。

（1）封閉系結中的電子證據、開放系統中的電子證據與雙系統中的電子證據[141]

A、區分依據

根據運行環境對電子證據進行的分類，由於電子證據對載體形態的依賴性較大，不同的系統環境往往決定了證據的本質差別。從系統環境的角度考慮，可將電子證據分為「封閉系統中的電子證據」、「開放系統中的電子證據」與「雙系統中的電子證據」。

一般而言，依電腦網路的作用範圍，可以將其分為「局域網（Local Area Network，LAN）」和「廣域網（Wide Area Network，WAN）」。

局域網係指較小範圍內的電腦網絡，主要特點可以概括為以下幾個方面：

（A）局域網是由若干獨立的設備連成一體，直接進行通信的網絡；

（B）局域網具有數據傳輸快且誤碼率低的特點；

（C）局域網用戶通常是固定的，彼此一般可以明確判斷網絡對方是現實生活中的具體某個人。廣域網，通常由兩個或兩個以上的局域網組成，利用公用線路傳輸數據，作用範圍廣。

廣域網特點可以概括為：

（A）通信介質、通信方式複雜。局域網的通信介質一般是同軸電纜、雙絞線和光纖等數據專線，以數位通信方式進行傳輸，而廣域網則採用公

[141] 何家弘，同前註 20，頁 35-37。

用電話線、衛星通信系統、遠程光纖等，以模擬通信、微波通信、光纖遠程高速等方式進行傳輸。

（B）廣域網需要借助網絡軟件和通信協議實現傳輸，因而資訊的誤碼率高於局域網。

（C）廣域網同時在線用戶數以萬計，資訊的來源不確定，因此在數位的安全保密性方面、防止非法用戶使用、查找網絡犯罪主體等方面，廣域網的要求及難度都要高得多。[142]

B、意義

所謂「封閉系統」，係指由獨立的一台電腦或多台以局域網方式連接的電腦所組成的系統。其特點是電腦系統不向外界開放，用戶相對固定，即便多台電腦同時介入數據交換過程，借助監測手段也可以迅速跟蹤查明電子證據的來源。如銀行內部管理系統網路、企業內部網路、檢察官內部網路等等。

「開放系統」則可概括為由多台電腦組成的廣域網和校園網系統，其特點是證據來源不確定。

「雙系統」，則是「封閉系統」與「開放系統」的合稱，並不是說某一電子系統有時是封閉系統，有時又變成了開放系統。

此三者所產生之電子證據，則區分為封閉系結中的電子證據、開放系統中的電子證據與雙系統中的電子證據。

[142] 亦有在「局域網」及「廣域網」間另行區分「城域網」者，例如跨越數城市、地區之校園網路屬之。然本文以爲此亦屬於「局域網」之一種，不需另行分類。

C、區分實益

將電子證據區分為封閉系統中的電子證據、開放系統中的電子證據與雙系統中的電子證據，最重要的意義在於確定了證據調查的思路。由於封閉系統的相對人是確定的，故案件發生後可以直接追查行為人，即誰實施了篡改數據的行為或者發出要約的行為等；而開放系統的相對人是不確定的，故必須首先根據開放系統的電子證據，查出是哪一台電腦或哪一個 IP（Internet Protocol）位址發出了實施了篡改數據的行為、或者發出要約的行為等，而後才能對應找行為人。此外，封閉系統下電子證據以電腦本身存儲、顯現的證據為主，開放系統下的電子證據，往往主要體現為第三方即網絡服務器所存儲、顯現的證據，雙系統下的電子證據則要視具體的系統環境而定。顯而易見，開放系統與雙系統中的電子證據，在可採性與證明力方面，都要較封閉系統中的電子證據複雜得多。從這個角度來說，這一分類最大的優點在於簡化人們對電子證據的認識。

D、本文認為無證據規則上區別實益之理由

（A）本分類只是在釐清證據在調查時之思路，對於法庭活動中實際操作證據排除法則、傳聞證據法則或認定證據能力、證明力等方面並無實益。

（B）對於電子證據調查階段，任何可能性均不能被排除，況且不論被告被指控在封閉、開放系統中犯罪，均可能會有相仿之答辯，例如帳號被冒用、電腦被冒用等等。單純因為所涉系統的不同而排除某些犯罪手法或可能性，在實務上執法人員不太可能會因此而排除任何調查的可能性。

（C）現在網際網路發達，企業內部網路與外部網路雖然會以子網路遮罩（Mask）區隔，但是都在同一台電腦上，轉換容易。例如行為人透過內部管制網路查得商業機密報告，旋即利用電子郵件或其他方式將該報告傳送出去，此情形不難想像，因之很難嚴格區分封閉系統或開放系統，更遑論所產生之電子證據。

（D）即便在法庭活動證據調查環節中，檢察官亦需要舉證證明被告涉嫌犯罪，使法院產生有罪之確信，因此檢察官會善盡舉證責任，不至於發生因為所涉系統不同而降低舉證標準。

（2）依通訊協定不同區別來電子證據

A、依據

電腦發展之初，都是單機作業，彼此並無聯結，其後美國國防部為了軍事目的，在一九六九年開始發展 ARPANET 計畫，希望透過網路相互連結，達到風險分散、隨處指揮之目的。計畫開始時有四部主機，到了一九八三年已經有三二０部主機了。要統合不同電腦間硬體、作業系統、軟體等之運作，必須建立一套通訊協定，讓電腦之間可以對話與協調。最早在 ARPANET 上所使用的之通訊協定為 Network Control Protocol（NCP），其後到了一九七０年代末期為 TCP/IP（Transmission Control Protocol/Internet Protocol）通訊協定所取代[143]。

TCP/IP 通訊協定包含有以下服務

（A）連線服務：

運作於網路最底層，指示資料如何自一台電腦經由網路連線媒介傳遞到另一台電腦。連

[143] http://squall.cs.ntou.edu.tw/bcc/NetworkApplications/InternetAndTCPIP.html、http://lips.lis.ntu.edu.tw/ytchiang/study/others/tcpip/TCPIP.htm#TCP/IP 的歷史發展，last visited on June 8, 2007.

線服務並不保證資料能以正確的順序抵目的地，甚至無法保證資料能到達目的地。

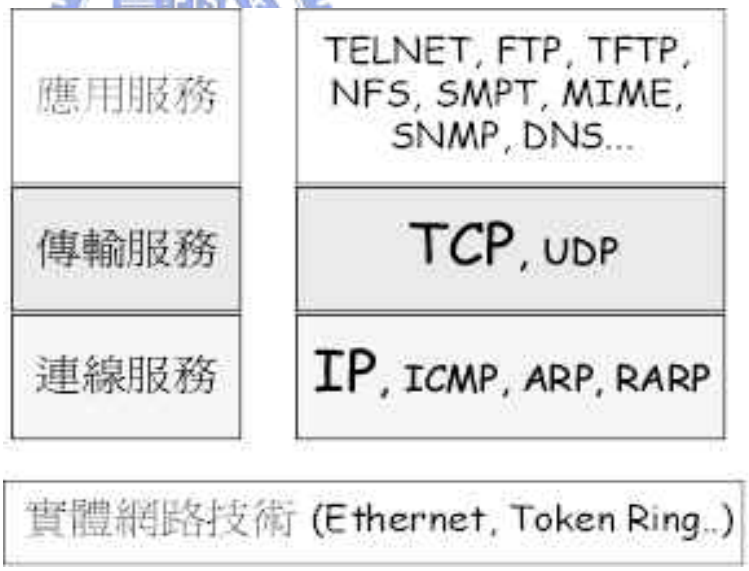
（B）傳輸服務：

運作於網路中間層，可增強上述的連線服務，以提供完整可靠的通訊品質。

（C）應用服務：

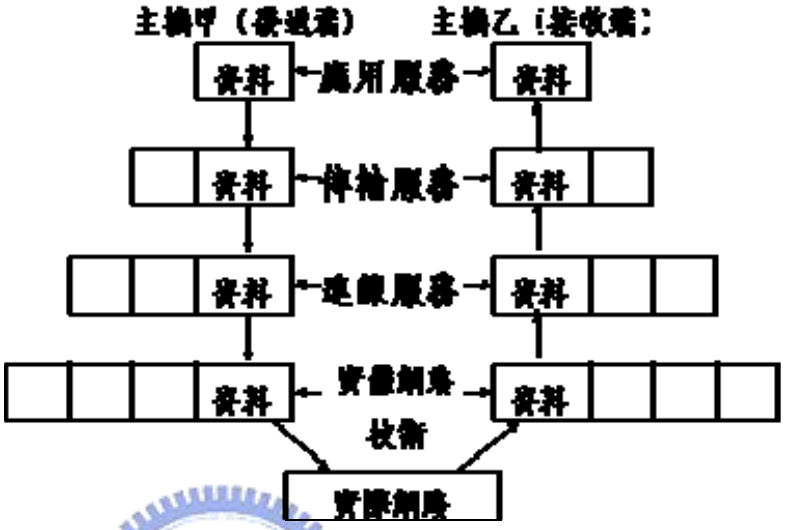
位於網路最高層，可讓一台電腦上的應用程式與另一台電腦上類似的程式交談，執行如檔案拷貝、上傳下載等工作。應用服務必須靠連線服務和傳輸服務來達到可靠而有效率的服務品質。

圖 2-1　TCP/IP 劃分階層架構與相關協定[144]



[144] http://lips.lis.ntu.edu.tw/ytchiang/study/others/tcpip/TCPIP.htm#TCP/IP 的階層架構與協定, last visited on June 8, 2007.

圖 2-2　TCP/IP 資料傳輸程序[145]



一九八０年代開始，國際標準組織（Internetational Standard Organization，ISO）開於著手於另一套通信協定標準化之研擬。於 1984 年頒布了 OSI 基本參考模型，訂定七個層次之功能標準、通信協定及服務種類[146]。

OSI 的 7 層通訊協定分述如下[147]：

（A）實體層（Physical Layer）

用來規定種種電氣規格和訊號處理之方式。實體層主要是利用電子訊號（如電壓、頻率等）透過傳輸媒體（如電纜、光纖、無線電、衛星等）傳送最基本的 0 與 1 的資訊。實體層定義了介面的實體特性，如機械元件、連結器等，以及實際連接的設定與維護等層面。

[145] *Id.* , last visited on June 8, 2007.

[146] http://lips.lis.ntu.edu.tw/ytchiang/study/others/tcpip/OSI.htm, last visited on June 8, 2007.

[147] http://lips.lis.ntu.edu.tw/ytchiang/study/others/tcpip/OSI.htm, last visited on June 8, 2007.

（B）資料鏈結層（Data-Link Layer）

資料鏈結層定義兩個透過實體連線的系統資料傳送與接收，有時也提供偵錯與控制的服務。

（C）網路層（Network Layer）

為了讓彼此不在同一條傳輸媒介上的節點，能透過中間其他節點進行通訊，OSI 因此故設立了網路層來規範資料在網路中的尋徑（Routing）功能，讓封包能依最短的路徑傳送到目的地。網路層讓資料有效率地送達到正確的地點，亦能提供錯誤控制的功能。

（D）傳輸層（Transport Layer）

傳輸層用以控制資料在起始點和目的節點之間可靠無誤的傳輸，具有連接導向的特性，提供高品質的服務與精確傳輸。它的主要工作包括控制封包順序、資料流量控制、偵測重複的封包、緊急資料的傳送、複雜的錯誤與回復處理、以及安全方面等。

（E）交談層（Session Layer）

兩台電腦在實際傳輸資料之前，必須先建立一個交談，交談層即是負責建立、主控一個交談，利用會話技巧或對話，協調系統之間的資料交換。

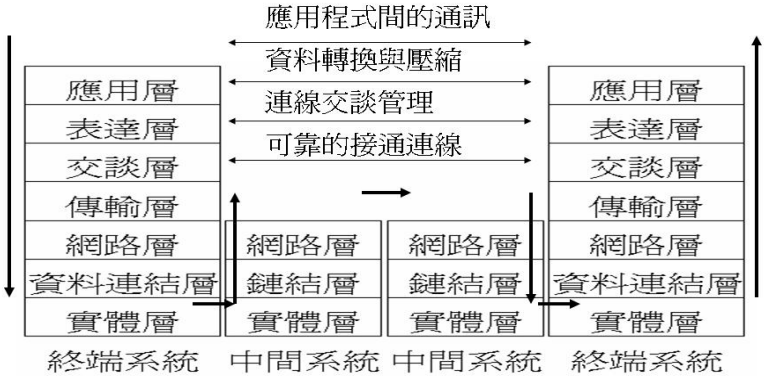
（F）表現層（Presentation Layer）

表現層讓不同廠牌及使用不同資料格式的各種機器得以相互通訊，亦即用來處理不同資料格式之間的轉換。

（G）應用層（Application Layer）

應用層是一般使用者執行工作的地方，用來規範各類應用之使用介面和運作程序，以提供使用者統一、有效的網路應用服務，也確保任何遵循此一規定的使用者得以相互通信。

圖 2-3 OSI 的七層架構與相關協定[1]

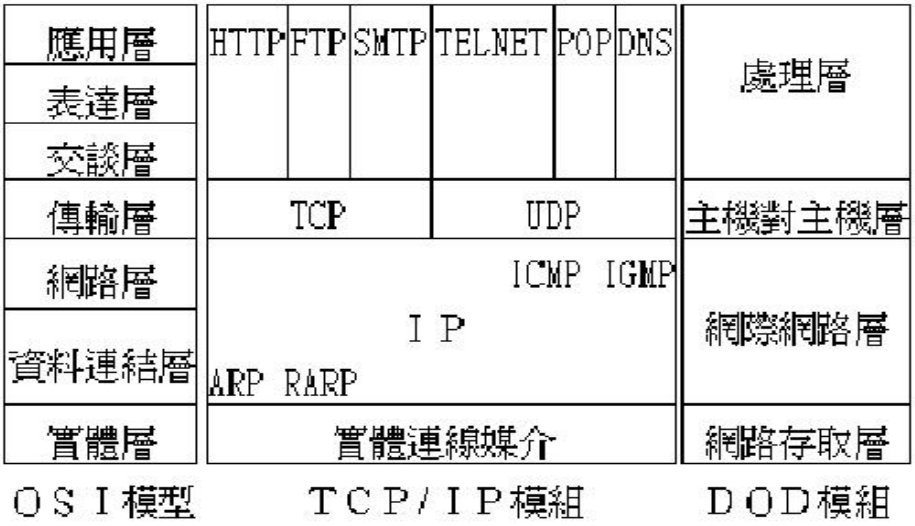


40

圖 2-4 TCP/IP 與 OSI 分層架構的對應[148]

[148] 高大宇等，同前註 18，頁 57。

圖 2-5 OSI 模型、TCP/IP 協定及 DOD 模組的關係圖[149]



B、意義

以 TCP/IP 通訊協定為區分，各階層網路通訊協定之層次所獲得之電子證據來討論，主要可以分為：

(A) 實體層[150]

由於在此階層，資料是以「0」與「1」之二進位制來傳送，必須透過特殊的軟、硬體設備始能加以辨識理解。此協定中最常見之電子證據為網路卡卡號（MAC address），因為每一張網路卡在製造過程中會配發具有獨一無二性之序號，且理論上無法篡改，因此可藉由追溯網路卡之卡號而查知該網路卡所配置之電腦及所在地。

[149] 高大宇等，同前註 18，頁 5。

[150] 林宜隆、陳蕾琪，同前註 18，頁 715。

（B）IP 層

電腦要連結上網，需要有一個 IP 位置，如同住家之門牌號碼一般。如果有 IP 位置，可以透過臺灣網路資訊中心（TWNIC）查出某一段網址由哪一家公司或機關所擁有，這是屬於靜態網址的部分。相較於靜態網址的是動態網址，當一台電腦要連上網際網路的時候在網路層會新給一個網址，目前是由網路服務提供者（lSP）來做這項服務。若要追查動態網址的電腦，可向 ISP 尋求找出在某一時段內，哪一個使用者取得這個網址，或可查出其撥接的電話號碼以便找尋使用者的位置。但是此種數位證據，會因技術較高的入侵者更改網址，而無法找到真正的電腦所在位置。

（C）TCP 層

一般伺服器提供各種系統資源服務，如電子郵件通訊協定（SMTP），藉由路徑的指令，可以得知指向哪一個通訊埠（Port），因此在可透過伺服器的紀錄檔（log file），察看哪些通訊埠與伺服器的通訊埠通訊，分析伺服器過去與現在系統資源的使用情形，這些都可作為數位證據。

（D）應用層

電子郵件系統、網站的網頁等皆屬於應用層，例如網玷上的色情圖片、非法販賣光碟的資訊等，可藉由搜尋引擎（search engines）來加以監控。但是電子郵件的標頭容易刪改，亦可能利用轉址郵件伺服器[151]或匿跡郵件伺服器

[151] 例如在 www.bigfoot.com 網站或 GMail 網站申請電子郵件帳號，他人將電子郵件寄至該帳號後，該帳號再將電子郵件轉至使用者其他電子信箱收受電子郵件。

[152]寄發電子郵件，因而無法得知真正的電子郵件發送者；或是特洛伊木馬（Trojan horse）[153]的程式，除了必須藉由防制程式查知外，尚還需要對此種程式熟悉，否則同樣屬於被侵害者。

以 OSI 之七層通訊協定來區分，各階層網路通訊協定之層次所獲得之電子證據來討論，主要可以分為：

（A）實體層

實體層為七層通訊協定中最低層級，只有各種規格或介面之定義，因此在此層級中並無電子證據[154]。

（B）資料連結層

每一張網路卡均會有一個製造序號，即所稱之 Mac adderss，[155]此項序號在電腦透過網路卡連結至網路時，均會留存在資料連結層。惟

[152] 例如在 www.ghostmail.com 網站申請帳號後，透過該網站郵件伺器寄發郵件，事後僅能追溯查至 ghostmail 網站郵件伺服器相關資訊，該網站會以保護隱私為由拒絕提供實際發信人相關資訊。例如臺灣臺北地方法院 89 年度訴字第 929 號刑事判決「一、王○○與新加坡籍人黃◎（DAVID NG GEE）…除申請免費電子郵件 oldbig54@yahoo.com、oldbig54@hotmail.com、vcdqueen@hotmail.com 外，並以 Ghost mail V5.1 版程式，在 tw.bbs.comp. hacker、tw.bbs.comp.hardware、tw.bbs.comp.network、tw.bbs.rec. entertainment、tw.bbs.comp.movie、tw.bbs.comp.tv、tw.bbs.comp.tv.x- files 等新聞群組以「光碟女王」名義，散佈隱匿電子郵件寄件人資料之販賣盜版光碟片之交易訊息…」或自行安裝發信郵件伺服器軟體，發信完畢後即行移除，如此亦難查知實際發信人資訊。

[153] 特洛伊木馬又稱木馬，起源於古希臘神話，傳說希臘人圍攻特洛伊城，久攻不下，後來設計建造數匹巨大的木馬，讓士兵藏匿其中。軍隊佯裝撤退而將木馬丟棄於特洛伊城外，令該城誤將之作為戰利品而拖入城內。木馬內的士兵則乘夜晚敵人慶祝勝利、放鬆警惕的時候從木馬中爬出來，與城外的部隊裏應外合而攻下了特洛伊城。電腦被植入木馬入侵的主要途徑為：電子郵件、下載及安裝不明來源的軟體（例如.賀卡、小遊戲等）、利用系統漏洞（例如微軟 IIS 服務器漏洞）等等方式。

[154] 錢世傑、錢世豐、劉嘉明、張紹斌，電腦鑑識與企業安全，頁 6-21，文魁資訊股份有限公司， 2004 年 10 月。

[155] Mac Address 又稱 Physical Address，是指網路卡上面一個由 6 組 16 進位之數字組成的 48 位元之序號，理論上沒有兩張卡的 Mac Address 是相同的。這個位址其實分為兩個部份：前面三組數字為 Manufacture ID，也就是廠商 ID；而後面的三組是 Card ID。

需注意者，Mac Adress 亦有軟體可以將之更改變造[156]，進行網路蒐證時應加以注意比對。

（C）網路層與資料傳輸層

電腦上網時會留下 IP（Internet Protocal）位置在網路層及資料傳輸層，可以當作鑑別連結電腦之資訊，惟需注意假 IP 及透過 IP 分享器上網時，犯罪嫌疑人真實身分之認定。

（D）交談層與表現層

通常此二通訊層不會留下電子跡證供為電子證據。

（E）應用層

應用層提供使用者與網路溝通的介面，基本上其常見之服務有網頁瀏覽、電子郵件、新聞群組及網路通訊的服務等。為正因為使用廣泛，犯罪者也得藉由各種網路服務，進行犯罪行為，因此會有大量的電子證據。例如瀏覽器中紀錄（History buffer）、我的最愛等各種紀錄的功能，會將近所瀏覽的網頁內容或網頁連結加以保留，網路通訊軟體也通常提供保存談話內容的設定，這些歷史紀錄檔提供執法人員相當豐富的電子證據[157]。

C、區分實益

此類電子證據應視為執法人員蒐集電子證據來源分析之用，具有管制上之意義，惟無證據規則上

[156] 例如 Macshift 軟體即可更改網路卡之卡號，參見 http://devices.natetrue.com/macshift/, last visited on June 8, 2007.

[157] 錢世傑等，同前註 154，頁 6-20。

之實益。因為政府部門在制訂網路管理政策時，為資訊安全及追查犯罪之考量，法令及稽查規範上應注意要求涉及各通訊協定層之網路業者保留相關資訊。例如要求 ISP 公司保留 IP 紀錄、要求政府機關及金融業者要保留伺服器稽核檔（Log File）均需達一定之年限，甚或應保留哪些項目等等，因此本文以為此種技術層次的分類，意義應在於管制而非在證據層面。

第三章　電子證據立法方向與範圍

3.1　國際間對電子證據重視之原因

電腦發明之初多半應用在大型實驗室裡[1]，純粹是為了龐大計算或模擬推導等理工軍事用途。電腦體積在縮小、普及之後，逐漸安裝在各大學裡，當時操作電腦，幾乎還是專屬於電腦工程師的權力，可是因為電腦普及，不需要全時運算提供各種實驗數據，剩餘的運算空文件，被電腦工程師利用在私人研究及測試，因此產生了駭客（Hacker）[2]、病毒（Virus）及散布蠕蟲（Worms）[3]等犯罪行為。同一時間，電腦也逐漸進入銀行、保險公司、電話公司、證券交易所及監理單位、戶政單位，在商業交易及行政管理上也逐漸扮演重要的角色。[4]

[1] 同第二章註 2，頁 90 頁以下。

[2] 駭客（Hacker）原是指電腦功力深厚、頭腦靈活，可以利用最基礎的定義或演算解決電腦問題的高手。Hack 是小斧頭之意，Hacker 原意是指手藝精巧，能單以一柄小斧頭就製作出精美木工用品的人，逐漸演變爲類電腦領域高手的尊稱。然而有一些高手恃才傲物、或爲求向自我挑戰而做出一些入侵或破壞他人系統的行爲，Hacker 一詞遂逐漸被形容成帶有犯罪的色彩。然而在電腦領域中，Hacker 仍然是一種尊稱，故而有人希望以 Cracker（中譯爲劊客或黑客）或 Punk（中譯爲叛客）來形容以電腦犯罪者，還給 Hacker 一詞清白。

[3] 電腦病毒與電腦蠕蟲的產生究竟何者爲先，二者之間實際定義應該如何區分，迄今仍無定論。電腦病毒的觀念，早在 1949 年起即陸續出現在科幻小說中，1980 年，德國多特蒙（Dortmund）大學 Jürgen Kraus 寫了一篇「自我複製程序（Selbstreproduktion bei programmen）」的學位論文（http://vx.netlux.org/lib/pdf/Selbstreproduktion%20bei%20Programen.pdf, last visited on June 8, 2007.）有認爲是第一篇討論電腦病毒觀念的學位論文，惟亦有認爲應屬於電腦蠕蟲領域者。到了 1982 年出現過蘋果 2 號（Apple Ⅱ）電腦病毒，1986 年初巴基斯坦的 Amjad 與 Basit 兄弟所撰寫的「巴基斯坦病毒（又稱 Brain 病毒）」通說被定義爲第一隻個人電腦上的病毒。至於非實驗室理論上的蠕蟲，當屬 1988 年麻省理工學院學生由 Robert Tappan Morris 所撰寫並散布的 Morris 蠕蟲（或稱 I.Worm）。附帶一提的是，Robert Tappan Morris 的父親 Robert Morris 也是電 腦高手，曾經利用單純的數學運算原理撰寫出正確率極高的拼字檢查程式。

[4] 同第二章註 2，頁 128 以下。

駭客、入侵、病毒等「專業」的行為剛開始沒有被社會所瞭解及重視，因為發生的區域都是在專業領域中，如研究機構、大學等。即使是發生，電腦專業領域的是也未必認為是應該受到規範的犯罪行為，甚至有可能引為趣事。況且因為此領域太過專業，法律界未意識到、亦無能力加以追查及規範。然而這類行為逐漸擴及到商業或公共領域，被認定有可能造成嚴重的金融、隱私及安全問題之後，各國才對此類行為所衍生出之電腦犯罪類型加以立法規範；也因此才體會到蒐集電腦犯罪相關證據的必要性。在查獲此類犯罪並將被告起訴後，電子證據在法庭活動中之適用開始與傳統證據規則之間發生挑戰與討論。此外，商業交易上透過電腦完成者日益增加，對各交易環節中所留下的「電子意思表示」，亦逐漸在發生糾紛後，被以證據之角色提出於法庭之中，不論民事或刑事訴訟，討論此類電子化商業行為所產生／遺留之跡證者，日漸增加。

隨後，網際網路普及[5]，電腦犯罪已由一國之內、單機的犯罪形態，逐漸轉變為跨越國界、多機串連的犯罪形態，電腦犯罪以現今的眼光視之，已經變成是無國界、跨國界的犯罪，電腦犯罪者以各個國家的電腦或網路為跳板，以規避追查；或與全球罪犯違犯意聯絡，共同遂行犯罪；或以其他國家的電腦為攻擊傷害的對象，此類行為已成為吾人日常生活中經常聽聞之消息。網路金融、跨國電子商務亦日益發達，全球幾乎已經形成單一市場，近日來對此已有「地球是平的」的形容。凡此種種，促成了國際組織及世界各國對於電腦及網際網路的重視焦點，不在侷限於規範電腦犯罪，而改為重視電子證據的保存、提取、證據規則的調整、內外國電子證據的法庭應用以及全時（Full Time）/即時（Real Time）的跨國合作[6]等方面。

---

[5] 關於網際網路的發展歷史，相關論述眾多，本文建議可參見全球資訊網路的發明人 Tim Berners-Lee 所著，張介英、徐子超譯，一千零一網 WWW 發明人的思想構圖，臺灣商務印書館，臺北，88 年 12 月。

[6] 即 24/7 合作網路，此一觀念對於國際合作偵辦電腦犯罪非常重要，我國亦爲「24/7 Computer Crime Network」第 35 個會員國。關於 24/7 之概念，參見下述「歐洲議會電腦犯罪公約（Convention on Cybercrime）」第 35 條。

3.2　國際組織所訂規範分析

國際組織對於跨國際之電子商業活動與網路電腦犯罪，非常重視，為建立國際兼商務行為與電腦犯罪間之秩序與規則，各國際組織自二十世紀晚期開始，從民刑事的角度制訂相當多的示範法與公約，強調各國應在國際間及國內對電子商務規範與電腦犯罪之防制與合作，應有齊一的步調與標準，各國在內國訴訟制度雖有不同，但是對於電子證據之屬性及其法律地位均應透過立法及案例加以確認。

3.2.1　聯合國

3.2.1.1　貿法會

1、聯合國貿法會最早在規範電子商務時，試圖通過擴大「書面形式」、「簽名（名）」和「原本」等概念的範圍、把以電腦為基礎的技術也包括進去來解決國內法中的這種規定給使用電子商業造成的障礙。

（1）「聯合國國際貨物銷售合同公約」（1980 - United Nations Convention on Contracts for the International Sale of Goods (CISG)）

貿法會於一九八０年四月十一日通過本公約，確立了關於訂立國際貨物銷售合同、買賣雙方義務、違約的補救措施以及合同的其他方面的一整套法律行為規則。並於一九八八年一月一日生效。該公約第十三條規定「為本公約的目的，『書面』包括電報和電傳。」亦即承認電子文件具有書面之效力。

(2)「聯合國貿法會國際商事仲裁示範法」(1985 - UNCITRAL Model Law on International Commercial Arbitration，簡稱「國際商事仲裁示範法」)

聯合國大會於一九八五年十二月十一日通過批准該示範法的決議，該示範法之宗旨是協調和統一世界各國調整國際商事仲裁的法律，建議各國從統一仲裁程序法的願望和國際商事仲裁實踐的特點出發，對該示範法予以適當的考慮。[7]該示範法承前揭聯合國國際貨物銷售合同公約對於書面之解釋，認為仲裁協議中之書面包含電傳形式之電子文件。

國際商事仲裁示範法第七條第二款「仲裁協議的形式」

「(2) 仲裁協議應是書面的。協議如載於當事各方簽名的文件中，或載於往來的書信、電傳、電報或提供協定紀錄的其他電訊手段中，或在申訴書和答辯書的交換中當事一 方聲稱有協議而當事他方不否認即為書面協議。在合同中提出參照載有仲裁條款的一項文件即構成仲裁協議，如果該合同是書面的而且這種參照足以使該仲裁條款構 成該合同的一部分的話。」

2、「關於電腦紀錄法律效力的建議 (1985 - Recommendation on the Legal Value of Computer Records)」

[7] http://big5.mofcom.gov.cn/gate/big5/training.mofcom.gov.cn/video2.asp?ClassID=663&action=-ifbase4-base44-yczO8bDZv8YmQ2xhc3NuYW1lPbn6vMq+rcOzyr63treo, last visited on June 8, 2007.

貿法會於一九八五年提交與 EDI 有關的「關於電腦紀錄法律效力的建議（Recommendation on the Legal Value of Computer Records）」，其中對於 EDI 等電腦紀錄或資料，建議各國政府在各自許可權範圍內審查與自動資料處理有關的規則，並加以適度調整，以便消除國際貿易中使用自動資料處理方法不必要之障礙。[8]

3、「電子商務示範法」、「電子商務示範法頒布指南（Guide to Enactment）」；以及「電子簽名（字）示範法（2001 - UNCITRAL Model Law on Electronic Signatures）」[9]及「電子簽名示範法頒布指南（Guide to Enactment）」。[10]

貿法會後來在一九九六年十二月十六日通過「電子商務示範法」、「電子商務示範法頒布指南（Guide to Enactment）」；以及「電子簽名（字）示範法（2001 - UNCITRAL Model Law on Electronic Signatures）」[11]及「電子簽名示範法頒

[8] 該建議已爲「電子商務示範法」及「電子簽名（字）示範法」所取代，參見 http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/1985Recommendation.htm, last visited on June 8, 2007.

[9] 聯合國貿法會網站網頁稱「2001 - UNCITRAL Model Law on Electronic Signatures」爲「電子簽名法」（http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/2001Model_Signatures.html, last visited on June 8, 2007.），惟於簡體中文條文中，稱爲「電子簽名法」（http://daccessdds.un.org/doc/UNDOC/GEN/N01/490/25/PDF/N0149025.pdf?OpenElement, last visited on June 8, 2007.），以下均已電子簽名法稱之，至於我國立法用語則爲「電子簽章法」。

[10] http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/2001Model_signatures.html, last visited on June 8, 2007.

[11] 聯合國貿法會網站網頁稱「2001 - UNCITRAL Model Law on Electronic Signatures」爲「電子簽名法」（http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/2001Model_Signatures.html, last visited on June 8, 2007.），惟於簡體中文條文中，稱爲「電子簽字法」（http://daccessdds.un.org/doc/UNDOC/GEN/N01/490/25/PDF/N0149025.pdf?OpenElement, last visited on June 8, 2007.，以下均已電子簽名法稱之，至於我國立法用語則爲「電子簽章法」。

布指南（Guide to Enactment）」。[12]電子商務示範法及電子簽名示範法，對於電子證據做出更明確的規定，並附帶有詳細的說明，其立場如下：

（1）運用功能等同方法（The functional-equivalent approach）解決數據電文的書面形式、原本與簽章問題。

A、功能等同法之意義

功能等同法是指立足於分析傳統的書面要求的目的和作用，以確定如何通過電子商務技術來達到這些目的和作用。[13]

在「在電子商務示範法頒布指南」簡介第E點中，對功能等同方法有詳細說明[14]：

「15、示範法係針對傳統的書面文件的法律規定是發展現代通信手段的主要障礙。在擬訂示範法時，曾考慮能否通過擴大『書面形式』、『簽名』和『原本』等概念的範圍、把以電腦為基礎的技術也包括進去來解決國內法中的這種規定給使用電子商業造成的障礙。一些現有法律文書就採用了這種辦法，例如『貿易法委員會國際商業仲裁示範法』第七條和『聯合國國際貨物銷售合同公約』第十三條。其後考量到：應允許各國將其國內立法加以修改以適應用於貿易法的通訊技術的發展，而不必全盤取消書面形式的

[12] http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/2001Model_signatures.html, last visited on June 8, 2007.

[13] 皮勇，同第二章註 20，頁 30。

[14] 英文版：http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, last visited on June 8, 2007.；中文版：http://www.uncitral.org/pdf/chinese/texts/electcom/MLEC_C_V05-89449_Ebook.pdf, last visited on June 8, 2007.

要求或打亂這些要求所依據的法律概念和做法。況且，通過電子手段滿足書面形式要求在某些情況下可能需要制定新的規則。這是因為電子資料交換電文與書面單證之間的許多區別之一是後者可用肉眼閱讀，而前者除非使其變為書面文字或顯示在螢幕上，否則是不可識讀的。

16、因此，示範法依賴一種有時稱作『功能等同辦法』的新方法，這種辦法立足於分析傳統的書面要求的目的和作用，以確定如何通過電子商業技術來達到這些目的或作用。例如，書面文件可起到下述作用：提供的文件大家均可識讀；提供的文件在長時間內可保持不變；可複製一文件以便每一當事方均掌握一份同一資料副本；可通過簽名核證資料；提供的文件採用公共當局和法院可接受的形式。應當注意到，關於所有上述書面文件的作用，電子紀錄亦可提供如同書面文件同樣程度的安全，在大多數情況下，特別是就查明資料的來源和內容而言，其可靠程度和速度要高得多，但需符合若干技術和法律要求。然而，採取功能等同辦法不應造成電子商業使用者須達到較書面環境更加嚴格的安全標準（和相關費用）。

17、就數據電文本身來看，不能將其視為等同於書面文件，因為數據電文具有不同的性質，不一定能起到書面文件所能起到的全部作用。這就是為什麼示範法採用了一種靈活的標準，考慮

到採用書面文件的環境中現行要求的不同層面：採用功能等同辦法時，注意到形式要求的現有等級，即要求書面文件提供不同程度的可靠性、可查核性和不可更改性。例如，關於應以書面形式提出資料的要求（構成『最低要求』）不應混同於較嚴格的一些要求，例如『經簽署的文書』、『經簽署的原本』或『經認證之法律文件』。

18、示範法並不打算確定一種相當於任何一種書面文件的電腦技術等同物。相反，示範法只是挑出書面形式要求中的基本作用，以其作為標準，一旦數據電文達到這些標準，即可同起著相同作用的相應書面文件一樣，享受同等程度的法律認可。應當指出，示範法第六至八條內含的功能等同法是針對『書面形式』、『簽名』和『原本』等概念的，並不針對示範法內涉及的其他法律概念。例如，第十條並沒有為現行的貯存要求創立其功能等同物。」

B、採用功能等同方法之條文例如

（A）電子商務示範法

a、第六條「書面形式」[15]

「1、如法律要求資訊須採用書面

[15] Article 6「Writing」

「1. Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

2. Paragraph 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

3. The provisions of this article do not apply to the following:[...].」

形式，則假若一項數據電文所含資訊可以調取以備日後查用，即滿足了該項要求。

2、無論本條第一款所述要求是否採取一項義務的形式，也無論法律是不是僅僅規 定了資訊不採用書面形式的後果，該款均將適用。

3、本條的規定不適用於下述情況：[...] 」

b、第七條「簽名」[16]

「1、如法律要求要有一個人簽名，則對於一項數據電文而言，倘若情況如下，即滿足了該項要求：

（a）使用了一種方法,鑑定了該人的身份，並且表明該人認可了數據電文內含的資訊；和

（b）從所有各種情況看來,包括根據任何相關協定，所用方法是可靠的，對生成或傳遞數據電文的

[16] Article 7「Signature」

「1. Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement therein is in the form of anobligation or w hether the law simply provides consequences for the absence of a signature.

3. The provisions of this article do not apply to the following: [...].」

目的來說也是適當的。

2、無論本條第一款所述要求是否採取一項義務的形式，也無論法律是不是僅僅規定了無簽名時的後果，該款均將適用。

3、本條的規定不適用於下述情況：[...]」

c、第八條「原本」[17]

「1、如法律要求資訊須以其原始形式展現或留存，倘若情況如下，則一項數據電文即滿足了該項要求：

（a）有辦法可靠地保證自資訊首次以其最終形式生成，作為一項數據電文或充當其他用途之時起，該資訊保持了完整性；和

（b）如要求將資訊展現，可將該資訊顯示給觀看資訊的人。

2、無論本條第一款所述要求是否採取一項義務的形式，也無論法律是不是僅僅規定了不以原始形式展現或留存資訊的後果，該款均將適用。

3、為本條第一款（a）項的目的：

（a）評定完整性的標準應當

[17] 原文參見第二章註 136。

是，除加上背書及在通常傳遞、儲存和顯示中所發生的任何變動之外，有關資訊是否保持完整，未經改變；和

（b）應根據生成資訊的目的並參照所有相關情況來評定所要求的可靠性標準。

4、本條的規定不適用於下述情況：[…]」

（B）電子簽名示範法[18]

第六條「符合簽名要求」[19]

「1、凡法律規定要求有一人的簽名時，如果根據各種情況，包括根

[18] 法規名稱及法條譯文以聯合國貿法會簡體中文譯本爲準，以下引用均採同一出處。

[19] Article 6. 「Compliance with a requirement for a signature」

「1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].」

據任何有關協定，使用電子簽名既適合生成或傳送數據電文所要達到的目的，而且也同樣可靠，則對於該數據電文而言，即滿足了該項簽名要求。

2、無論第一款所述要求是否作為一項義務，或者法律只規定了無簽名的後果，第一款均適用。

3、就滿足第一款所述要求而言，符合下列條件的電子簽名視作可靠的電子簽名：

（a）簽名製作資料在其使用的範圍內與簽名人而不是還與其他任何人相關聯；

（b）簽名製作資料在簽名時處於簽名人而不是還處於其他任何人的控制之中；

（c）凡在簽名後對電子簽名的任何更改均可被覺察，以及

（d）如果簽名的法律要求目的是對簽名涉及的資訊的完整性提供保證，凡在簽名後對該資訊的任何更改均可被覺察。

4、第三款並不限制任何人在下列任何方面的能力：

（a）為滿足第一款所述要求的目的，以任何其他方式確立某一 電子簽名的可靠性；或

（b）舉出某一電子簽名不可靠的證據。

5、本條規定不適用於下列情形：[…]。」

（2）遵循平等對待原則處理電子證據的可採性（證據能力）和證明力[20]

A、平等對待原則之意義

承襲前揭功能等同法之精神，認為數據電文之證據能力與證明力，其標準應該與對傳統書面證據之檢驗採取齊一之標準。

在電子商務示範法第九條之釋義中提及：「資料電文在法律訴訟中作為證據的可接受性，同時確立其證據價值。對於可接受性，第一款規定，在法律訴訟中，不得僅僅以資料電文是採用電子形式而否定其作為證據的可接受性，這再次強調了第4條所述的總原則，明確地使它適用於證據的可接受性，因為在某些法域，這方面可能會發生特別複雜的爭議。『最佳證據』一語是普通法系某些法域容易理解的用語，也是必要的用語。但是，對於尚未熟知這一規則的法律系統，『最佳證據』概念有可能產生很多不確定性。凡這一詞語會被認為毫無意義甚至會產生誤解的那些國家，在頒佈實施『示範法』時，似宜避免提及第一款中的『最佳證據』規則。

關於一項資料電文的證據力的評估，第二款對於如何評估資料電文的證據價值，提供了有用的指導（例如，考慮到資料電文的生成、儲存或傳遞方式是否可靠）。」[21]

[20] 皮勇，同第二章註 20，頁 30。

[21] 同前註 14。

B、採用功能等同方法之條文例如

（A）電子商務示範法

a、第五條「數據電文的承認」

「不得僅僅以某項資訊採用數據電文形式為理由而否定其法律效力、有效性或可執行性。」[22]

b、第九條「數據電文的可接受性和證據力」

「1、在任何法律訴訟中，證據規則的適用在任何方面均不得以下述任何理由否定一項數據電文作為證據的可接受性：

（a）僅僅以它是一項數據電文為由；或

（b）如果它是舉證人按合理預期所能得到的最佳證據，以它並不是原樣為由。

2、對於以數據電文為形式的資訊，應給予應有的證據力。在評估一項數據電文的證據力時，應考慮到生成、儲存或傳遞該數據電文的辦法的可靠性，保持資訊的完整性的辦法的可靠性，用以鑒別發端人的辦法，以及任何其他相關因素。」[23]

[22] Article 5「Legal recognition of data messages」

「Information shall not be denied legal effect, validity or enforce ability solely on the grounds that it is in the form of a data message.」

[23] Article 9「Admissibility and evidential weight of data messages」

3.2.1.2　聯合國第十屆預防犯罪和罪犯待遇大會

聯合國二０００年十二月四日之第十屆預防犯罪和罪犯待遇大會，對高科技與電腦犯罪的預防、偵查、國際合作等，揭櫫了許多重要的方針。[24]

這些方針包括對電腦犯罪行為之定義、刑事程序立法、跨國犯罪證據之蒐集與協助等方向。其具體內容為：

1、就高科技犯罪和與電腦犯罪等問題所發表之「維也納宣言」，第十八段即揭櫫：「成員國決定就預防和控制電腦犯罪制定著眼於行動的政策建議，並承諾致力於增進各國預防、調查和檢控高技術犯罪及電腦犯罪的能力。」

2、第五/六三號「關於執行『關於犯罪與司法：迎接二十一世紀的挑戰的維也納宣言』的行動計畫第 11 項「打擊高技術和電腦犯罪的行動」

「34、為了實施和落實《維也納宣言》第十八段中所作的承諾，即兼顧其他論壇正在進行的工作，就預防和控制高技術和電腦犯罪制訂著眼於行動的政策建議，並增進偵查、預防、

「1. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
(a) On the sole ground that it is a data message; or
(b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
2. Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.」

[24] 參見 http://www.un.org/chinese/documents/decl-con/docs/a-conf187-4-rev-3.pdf、http://www.un.org/chinese/documents/ecosoc/2001/r2001-47.pdf。, last visited on June 8, 2007.

調查和起訴這類犯罪的能力，建議採取下列具體措施。

A、國家行動

35、各國將酌情單獨或集體地努力支持下列行動：

(a)根據國家法律酌情將濫用資訊技術定為犯罪，包括在必要時審查欺詐等犯罪的情況，以確保其適用於利用電腦和電信媒體和網路實施這些犯罪的情況；

(b)制訂和實施各項規則和程序，包括行使管轄權的規則和程序，確保能在國家一級有效地偵查和調查與電腦和電信有關的犯罪，並在多國案件中得到有效的合作，同時照顧到國家主權、有效執法的需要及有效保護隱私權和其他有關基本權利的需要；

(c)確保對執法人員進行培訓和裝備，以便能夠有效快捷地對有關跟蹤通信的援助請求和為偵查和調查跨國高技術和電腦犯罪所需其他措施的請求作出回應；

(d)就採取行動打擊高技術和電腦犯罪以及技術變化的影響而與涉及開發和部署電腦、電信設備、網路軟硬體和其他有關產品和服務的產業進行國內和國際討論。這些討論可包括關鍵的領域，例如：

㈠有關國內和國際技術與網路管理的問題；

㈡有關將旨在預防犯罪或便利偵查、調查或起訴犯罪的要素納入新技術的問題；

(e)酌情以雙邊方式和通過國際和區域組織，包括與私營部門合作，特別是以技術專門知識的形式，作出自願捐贈，以便協助其他國家制定和執行有效打擊高技術和電腦犯罪的措施，包括上文(c)項和(d)項所提及的措施。

B、國際行動

36、國際預防犯罪中心將依照大會第 56/…號決議在酌情同其他有關的國際和區域組織合作的情況下：

(a)支持開展國家和國際研究活動，以認定新的電腦犯罪形式，並評估這類犯罪在可持續發展、保護隱私權和電子商務等關鍵領域的影響，以及所採取的對策；

(b)傳播國際議定的材料，如準則、法律和技術手冊、最低限度標準、經驗證的做法和示範立法，以協助立法人員和執法當局及其他當局制定、採取和適用在一般和特定案件中有效打擊高技術和電腦犯罪和罪犯的措施；

(c)酌情促進、支援和執行技術合作和援助專案。此類專案將使預防犯罪、電腦安全、刑事立法和訴訟程序、起訴、調查技術和有關問題方面的專家與尋求這些方面的資訊或援助的國家匯合在一起。」

3.2.2 歐洲議會（Council of Europe）

歐洲議會早在一九八九年就提出報告，請各成員國注意電腦及網路犯罪問題，其後經歷多次的修改，在二００一年十一月八日推出「網路犯罪公約（Convention on Cybercrime）」[25]，後經會員國的簽署，在二００四年七月一日生效。該公約之主要目標是希望簽署會員國之間可以制訂打擊網路犯罪的共同刑事政策以及國際合作。

其中與電子證據與跨國合作有關的重要條文主要為

1、第二章「國家層級」第十四條至第二十一條規定電子證據之保全、強制處分、截留及提出等。

（1）第十四條　程序規定的運用範圍[26]

「1、締約方應制定必要的國內法或者其他規定，為本部分特殊的刑事偵查和起訴規定權力和程序。

2、除第二十一條的特別規定外，締約方應實行本條第一款規定的權力和程序。

a、本公約第二條至第十一條規定的犯罪；

b、其他通過電腦系統實施的犯罪；

c、電子形式的犯罪證據的蒐集。

3、 a、締約方可以保留權利，如果這些犯罪或者類犯罪不比適用第二十一條規定措施的類犯罪更為嚴格，第二十條規定的措施僅對保留所指定的犯罪或者類犯罪適用。締約方應考慮嚴格限制這一保留的使用，以使第二十條的規定得到更廣泛的實行。

b、當締約方由於國內法律在調整適應本公約

[25] CETS No.: 185，http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, last visited on June 8, 2007.

[26] 網路犯罪公約中譯參考自皮勇翻譯之版本，載於皮勇，同第二章註 20，頁 286-307。英文原文請參見前註網站，以下條文均同。

期間的限制，而不能將第二十條、第二十一條的規定適用於服務提供商的電腦系統中傳輸的通信，而這些系統是：

(i) 為一封閉用戶群體的利益運作；

(ii) 沒有使用公用通訊網絡，並沒有連接其他的電腦系統，無論是公用的還是私人的。

該締約方可以保留不對這些通信使用本公約的權利。締約方應考慮限制這一保留，以使第二十條、第二一條的規定得到更廣泛的實行。」

(2) 第十五條　條件和保障

「1、締約方應保證將本部分規定的權力和程序的建立、執行和適用，置於國內法的適用條件和保障下，它們應為人權和自由提供足夠的保護，包括承擔國際公約義務而引起的人的權利：「一九五０年歐洲理事會人權及基本自由保護公約」、「一九六六年聯合國公民權利和政治權利國際公約」和其他生效的國際人權公約，它們應與相稱性原則相一致。

2、這些條件和保障應適當考慮相關權力和程序的性質，包括司法或者其他適當的監督、有權解釋的應用，以及這些權力和程序的適用範圍和期間的限制。

3、為了與公共利益相一致，特別是為了司法公正，締約方應考慮本部分規定的權力和程序對權力、責任和第三方正當利益的影響。」

(3) 第十六條　儲存的電腦數據的快速保護

「1、締約方應制定必要的國內法或者其他規定，確保有權機關能提取或者相似的實現指定電腦數據的快速保護，包括往來數據，它一般儲存在某電腦系統中，特別是那些有理由相信的易被

修改或者丟失的電腦數據。

2、當締約方適用第一款，以命令方式要求個人保護個人所有或者控制下的特定的儲存的電腦數據時，締約方應制定必要法律或者相關規定，要求個人保護並維持電腦數據的完整性必要長的一段時間，最長可達九十天，以使有權機關能調查案件事實。締約方可再次命令，以使保護期延長。

3、締約方應制定必要的國內法或者其他規定，要求保護電腦數據的管理人或者其他人，在依據國內法向有權機關提供以上協助期間保守秘密。

4、本條規定的權力和程序應遵守第十四條、第十五條的規定。」

（4）第十七條　往來數據的快速保護和部分提交

「1、針對依第十六條進行保護的往來數據，各締約方應調整必要的國內法或者規定：

a、無論是一個或者多個服務提供商，參與了通信的傳輸，必須保證能對往來數據進行快速保護。

b、保證快速提供給締約方有權機關或者該機關指定的個人足夠的往來數據，使締約方可以識別服務提供商及通信傳輸的途徑。

2、本條規定的權力和程序應遵守第十四條、第十五條的規定。」

（5）第十八條　提交指令

「1、各締約方應調整必要的國內法或者規定，授權其有權機關可以指令：

a、個人在其控制範圍內提交個人所有或者控制的特定電腦數據，這些電腦數據儲存在一電腦系統中，或者是某電腦數據存儲媒

體中；

b、在締約方國內提供服務的服務商在服務商所有或者控制範圍內，提交與這些服務相關的用戶信息。

2、本條規定的權力和程序應遵守第十四條、第十五條的規定。

3、本條中的『用戶資訊』，是指以電腦數據或任何其他形式包含的任何資訊，這些資訊由服務商所持有，與服務用戶相關，往來數據、內容數據以外的信息。通過用戶資訊可以建立：

a、用於通信服務、技術規則、服務期間的一類信息；

b、用戶身份號、郵政編碼或者位址、電話或者其他訪問號碼，帳單或者支付資訊的，在服務條款或者協定中可以得到的；

c、安裝通信設備地點的任何其他資訊，這些資訊是在服務協定或者安排的基礎上可獲得的。」

（6）第十九條　搜查和扣押存儲的電腦數據

「1、各締約方應調整必要的國內法或者規定，授權有權機關搜查或者相似地進入其境內的：

a、一個電腦系統或者其中某部分和存儲在其中的電腦數據；

b、可能存儲電腦數據的電腦數據存儲媒體。

2、各締約方應調整必要的國內法或者規定，保證如果有權機關搜查或者類似地進入第一款 a 之規定的特定的電腦或其部分，並有理由相信要搜尋的電腦數據存儲在領域內另一電腦系統中或者某部分中，而且，這些數據對起始系統是公開的或者可以合法進人的，有權機關應能夠。快速展開搜尋或者類似地進入其他系統。

3、各締約方應調整必要的國內法或者規定，授權

有權機關扣押或者採取相似的安全措施，保護第一款、第二款規定的電腦數據。這些措施應包括以下權力：

a、扣押或者使用相似的安全措施保護電腦系統或者其一部分，或者一個電腦數據存儲媒體；

b、製作或者獲取這些電腦數據的備份；

c、保持相關的存儲的電腦數據的完整性；

d、使其不可訪問或者將其從可訪問的電腦系統中移走。

4、各締約方應調整必要的國內法或者規定，授權有權機關指令任何知道電腦系統功能或用於保護其中電腦數據的應用措施的人，提供合法的、必要的資訊，確保第一款、第二款規定的實施。

5、本條規定的權力和程序應遵守第十四條、第十五條的規定。」

（7）第二十條　電腦數據的實時蒐集

「1、各締約方應調整必要的國內法或者規定，授權有權機關：

a、在締約方境內應用技術手段蒐集或者紀錄；

b、強令服務提供商在其技術能力範圍內：

（i）通過技術手段方式在締約方境內蒐集或者紀錄；或者

(ii)與有權機關合作並協助有權機關蒐集或者紀錄在締約方境內的通過電腦系統傳輸的特定通信的實時的往來數據。

2、當締約方由於國內法體系中確定的原則，不能適用第一款 a 中的規則，它可以替代採用法律規定或者其他必要的規則，來保證其境內傳輸的與特定通信相關的往來數據的蒐集或者紀

錄。

3、各締約方應調整必要的國內法或者規定，要求服務提供商對本條規定的執行和任何與此相關的資訊保守秘密。

4、本條規定的權力和程序應遵守第十四條、第十五條的規定。」

（8）第二十一條　內容數據的截取

「1、各締約方應調整必要的國內法或者規定，就國內法規定的一類嚴重犯罪，授權有權機關：

a、在締約方境內應用技術手段蒐集或者紀錄；

b、強令服務提供商在其技術能力範圍內：

（i）通過技術手段方式在締約方境內蒐集或者紀錄；或者

（ii）與有權機關合作並協助有權機關蒐集或者紀錄在締約方境內的通過電腦系統傳輸的特定通信的實時的內容數據。

2、當締約方由於國內法體系中的確定的原則，不能適用第一款 a 中的規則，它可以替代採用法律規定或者其他必要的規則，來保證其境內傳輸的與特定通信相關的往來數據的蒐集或者紀錄。

3、各締約方應調整必要的國內法或者規定，要求服務提供商對本條規定的執行和任何與此相關的資訊保守秘密。

4、本條規定的權力和程序應遵守第十四條、第十五條的規定。」

2、第三章「國際合作」第二十九條至第三十五條則係前開保全、強制處分等規定國際合作之作法與規範

（1）第二十九條　儲存的電腦數據的快速保護

「1、締約方可以要求另一方指令或者以其他方式對位於該方境內的，請求方提交相互協作請求要求對其進行搜查或相似快速進人、扣押或採取相似的其他安全措施或者進行數據披露的電腦系統中存儲的數據進行快速保護。

2、第一款規定的保護請求應指明：

a、有關機構扣押保護的數據；

b、作為刑事調查對象的犯罪和相關事實的主要目錄；

c、被保護的存儲的電腦數據和與違法的關系；

d、認定存儲的電腦數據的管理人或者電腦系統的位置的任何資訊；

e、保護的必要性；和

f、締約方提交相互協作的請求，以搜尋或其他相似的進入、扣押或者採取相似的安全措施，或者對存儲的電腦數據的披露。

3、在接到另一締約方的請求後，被請求方應依照其國內法律，採取適當措施相似地保護指定的數據。為了對請求作出反應，雙重犯罪地不應成為提供數據保護的條件。

4、把雙重犯罪地作為以搜尋或其他相似的進人、扣押或採取相似的安全措施或者披露存儲的電腦數據以響應相互協作請求的條件的締約方，當其有理由相信在提出請求的時候，雙重犯罪地條件未被滿足，則該締約方可對於本公約第二條至第十一條規定的犯罪保留拒絕根據本條提出的保護請求的權利。

5、此外，扣押僅能在以下條件下拒絕保護：

a、請求的犯罪是被請求方視做政治犯罪或者與政治犯罪相關的犯罪，或者

b、被請求方認為請求的執行可能損害其主權、安全、公正或者其他重要利益。

6、當被請求方相信保護將不能保證未來可以得到數據，或者將危及其保密性或者損害請求方的調查，它應快速告知請求方，由請求方決定是否該請求仍然執行。

7、作為第一款規定的請求的任何保護應持續至少六十天，以使請求方可以請求搜尋或其他相似的進人、扣押或者採取相似的安全措施或者披露存儲的電腦數據。該請求被接受後，數據應繼續被保護，直至對該請求作出決定。」

（2）第三十條　受保護的往來數據的快速提交

「1、當在依據第二十九條保護特定通信相關的往來數據的請求執行中，被請求方發現他國的服務提供商涉及了通信的傳輸，被請求方應快速向請求方提交足夠多的往來數據，以確認服務提供商以及通信傳輸經由的路徑。

2、第一款規定的往來數據的提交可以由於以下條件而保留：

a、請求的犯罪是被請求方視作政治犯罪或者與政治犯罪相關的犯罪，或者

b、被請求方認為請求的執行可能損害其主權、安全、公正或者其他重要利益。」

（3）第三十一條　與相互協作相關的訪問存儲的電腦數據

「1、締約方可以要求另一方搜尋或其他相似的進入、扣押或者採取相似的安全措施，或者提交位於被請求方境內存儲的電腦數據，包括依據第二十九條保護的數據。

2、被請求方應通過第二十三條規定的國際文件、協定、法律，以及本章其他規定的應用，對請求作出響應。

3、在以下情況下應對請求作出快速響應：

a、有理由相信有關數據特別容易丟失或者被修

改；或

b、本條第二款規定的文件、協定、法律提供的快速協作。」

（4）第三十二條　跨境進入經同意或公開存儲的電腦數據

「締約方可以不經另一方的允許

a、進入可公開獲取的（開放數據源）存儲的電腦數據，不考慮這些數據在地理上出於何處；或

b、如果締約方獲取的是合法的和自願提供的個人數據，該個人獲得法律授權提供電腦系統中的公開數據，則該締約方可以進人或者接收處于另一方領域內存儲的電腦數據。」

（5）第三十三條　相互協作實時蒐集往來數據

「1、締約方應相互提供往來數據的實時蒐集，該往來數據與其領域內電腦系統中傳輸的特定通信相關。依第二款規定，這種協助應遵守國內法要求的條件和程序。

2、締約方至少應對這類犯罪提供協作，即在相似的國內案件中這些犯罪可以獲得往來數據的實時蒐集。」

（6）第三十四條　相互協作實時蒐集內容數據

「締約方應在生效的條約和國內法律範圍內，對電腦系統傳輸的特定通信中的內容數據提供實時蒐集和紀錄的相互協作。」

（7）第三十五條　24／7 網路

「1、各締約方應指定一個一天二十四小時，一周七天的有效聯繫點，以保證對與電腦系統和數據有關的犯罪調查和處置，或電子形式的犯罪證據蒐集快速協助的規定得以執行。如果其國內法和司法允許的話，該協助應包括有助於直接

執行以下規定：

a、技術建議的規定；

b、第二十九條、第三十條規定的數據保護；

c、證據蒐集、法律規定的資訊和犯罪嫌疑人的位置。

2、 a、一方的聯絡點有能力執行與另一方快速通信。

b、如果一方指定的聯絡點不是該方負責國際協作或者引渡罪犯的有權機關，該聯絡點應保證它能夠和這些機構，快速協調。

3、任何締約方應保證有良好訓練的、裝備齊全的人員，以促進該網絡的正常發展。」

3.2.3　八大工業國組織（Group of Eight）

八國工業國組織（下稱「8 國峰會」）係指現今世界八大工業領袖國的聯盟。該議始創於英國、美國、法國、西德、日本及義大利在一九七五年所舉行的的六國峰會，加拿大於一九七六年加入，改稱七國峰會，俄羅斯於一九九七年加入，故現稱八國峰會。

一九九七年十二月，八國峰會通過了有關網絡犯罪的十點行動計劃，該行動計劃包括商定司法援助協議時應審議電腦犯罪問題、審議電子證據的保存及在外國刑事訴訟中提供這類證據的方法、關於電腦安全的司法標準及其他技術標準、在法律訴訟中使用電子證據等。一九九九年八國峰會更進一步通過了執法機構尋求查閱外國儲存的電子數據所應遵循初步的基本原則。[27]

[27] 皮勇，同第二章註 20，頁 35-36。

3.2.4 小結

以上各國際組織法律及公約中之各種項目及方針誠值參考，國際組織也帶領電腦犯罪、高科技犯罪之偵查及司法程序，由內國行為走向國際合作。

惟國際組織所制訂的公約或法律不具有強制力，僅具有概括性、原則性的綱領性質，希望世界各國可以通過移植和吸收其精華而轉換為國內立法，成為具有強制力的國家法律。[28]

此類國際性公約或法律對於電子證據規則主要規範了數據電文原本與複本的界定及效力、證據能力、證明力原則及證據蒐集與保存原則等等。

3.3 各國立法例

3.3.1 各國立法態度

對於電子證據，各國目前態度都予以承認其證據效力，惟各國間在對於電子證據立法模式、檢視與接納等方面還是有所差別[29]。

1、大陸法系國家對證據採認之架構

大陸法系國家如我國，因為是以專業法官進行審判，故而對於證據的要求主要表現在證據蒐集措施方面，對於認證規則如驗真法則、傳聞法則等較少著墨[30]。對於電子證據的認證，只要是依照法律規定的程序蒐集

[28] 皮勇，同第二章註 20，頁 35。

[29] 皮勇，同第二章註 20，頁 36-37。

[30] 例如早年我國的說學及實務見解，是不承認我國有傳聞證據的，僅黃東熊教授認爲刑事訴訟法第 159 條屬於傳聞證據之規定，即是一例。而在新修訂刑事訴訟法中，則明文規定傳聞證據的排除與例外。

與提出，都可以被採納，而由法官基於自由裁量、自由心證等原則判斷該項證據之證據力。

例如法國、日本等國家，並沒有為因應電子證據而特別立法，而是將相關法制規定在刑事訴訟法等法律中。例如對於電子證據的證據種類，我國與法國、日本等大陸法系國家多半依照傳統證據類型如書證或者擴展的書證的認證規則來處理。例如，在法國民法典中「書面證據」一章之中，第一三一六條規定，當證據是由一系列文字、字母、數字或其他任何具有可理解的內容的符號或標誌組成的，不論其載體和傳輸方式如何，均為書證。第一三一六條之一規定：以電子形式做成的文書與書面載體的文書一樣被視為證據，前提是做成該文書的人能夠正式地得以識別，該文書的製作與保管的條件應能保證其完整性，簽名應與簽名人相一致，並代表當事人對由該行為所產生義務的同意。這一規則既適用於書面載體的證據，也適用於電子形式的電子簽名[31]；在日本，亦援用文書的認證規則。[32]

2、英美法系國家對證據採認之架構

英美法系國家，因為採非專業的陪審團對於證據與待證事實之關係加以判斷，所以對於證據的前期取證與後期認證，均有非常嚴謹的規定。

英美法系如美國，法庭活動中對於所有的證據，都區分為取證方法與所取得之證據資料，不論是證據方法或證據資料都先受到證據排除法則之規範，亦即先有合法之取證方法，始能得出合法證據資料，若方法被排除

[31] 參見法・達尼埃爾.馬丁、弗雷德里克-保羅.馬丁合著，盧建平譯，網絡犯罪-威脅、風險與反擊，頁 148，中國大百科全書出版社，2002 年 12 月。

[32] 參照本文第二章之文書說。

（例如違法搜索、扣押），則因之而取得之證據資料即不能被採用；其後，合法的取證方法所取得之證據資料，再一次受到證據排除法則之規範，倘被排除，則縱然取證方法合法，證據資料亦不能被採納，例如雖合法傳喚及宣示之證人，在作證時所說的話卻屬於傳聞或臆測，則其縱然在法庭作證，但證詞亦因此無法被採用。是以不論是一般證據或電子證據，均要考慮證據法則中可採性與證明力、傳聞法則、違法證據排除法則、驗真法則及最佳證據規則等。

相對於前開國家儘可能維護暨有法制的完整性，希望透過解釋或小幅度修正證據調查方法的方式取代專門立法之方式解決社會演進中所衍生的法律問題。許多英美法系國家的證據法的最大特點是擁有詳細的證據採納和排除規則，故而此等法系國家對於電子證據接納之方式，往往以立法方式加以處理，致力於建立完善電子證據認證規則。許多英美法系國家制定了專門調整電子證據的法律，例如南非一九八三年電腦證據法（Computer Evidence Act 57 of 1983 of South Africa）、加拿大一九九八年統一電子證據法（1998 – Uniform Electronic Evidence Act of Canada）、菲律賓二００一年電子證據規則（2001 – Rules on Electronic Evidence of Philippines）；也有透過修改證據法或判例法的方式，對電子證據進行詳細的規定，例如美國聯邦證據規則、一九九九年統一證據規則即是，茲分述之。

3.3.2 制定專門法律適用於電子證據

1、南非一九八三年電腦證據法

南非是最早針對電腦證據立法之國家，在一九八三年即有此舉。但是該國對於電腦證據之意義，採本文第二章

之第三種見解，將電子證據界定為電腦產生及列印的證據。該法共有六條，主要是就電腦列印輸出紙本之驗真、驗真方式、驗真主體資格、驗真內容、經驗真的電腦列印輸出文件可採性和證據力等方面進行了規定，惟該法僅適用於民事訴訟案件。[33]

2、加拿大一九九八年統一電子證據法[34]

加拿大電子證據法對於電子證據之觀念已進步到瞭解電子證據是一種磁性紀錄，非列印紙本。並且與南非電腦證據法僅適用於民事案件不同，對於民、刑事案件均能一體適用之。該法共有九條，規範方向為:

（1）對電子證據意義做出規定

該法第一條將電子證據界定在以電腦數據為基礎的證明材料。證明材料是否屬於電子證據的標準在於是否保存或紀錄在一套電腦系統或類似裝置中。[35]

（2）對於最佳證據法則之規定

第四條規定，輸出數據形式的電子紀錄，如果已經明地、經常地發揮作用，並且被依靠、或用來作為存儲在輸出數據中的資訊的紀錄，那麼它就是符合最佳證據規則的紀錄。[36]

（3）建立推定原則

第五條規定，沒有相反的證據，可以推定產生或存儲紀錄的電子紀錄系統的真實性。

（4）建立電子證據交互詰問原則

第八條規定對於以具結方式將電子證據引入法庭之他方當事人，有權利對該證人進行交互詰問。

---

[33] 詳細之評述，請參見何家弘，同第二章註 20，頁 332-336。

[34] 加拿大統一電子證據法原文請參見 http://www.ulcc.ca/en/us，中文譯本請參見何家弘，同第二章註 20，頁 494-502。

[35] 本條中文譯本亦可參見郭佳玟，同第二章註 42。

[36] 何家弘，同第二章註 20，第 338 頁。

3、菲律賓二００一電子證據規則

菲律賓電子證據規則共十二條，對於電子證據常見的爭議作出了許多規範：

（1）最佳證據規則

電子證據，尤其是電子文件，往往是以列印輸出的形式向法庭提交，這時就很難依據傳統的方法區分何者為原本，何者為影本，因此應認最佳證據法則中「提供原本」的要求於此應加以調整。故該規則第四條規定：如果某一電子文件是借助視覺或其他形式可能讀取的列印輸出或其他輸出，並有證據證明其準確地反映了數據內容，則應將其視為符合最佳證據規則的原始文件相當物（Equivalent）。[37]

（2）傳聞規則

根據「無歧視原則」、「平等原則」之觀點，以電子、光學或其他相似手段製作的這些業務紀錄並不應因其是電子形式而被認為非屬傳聞規則之例外，應一體適用傳聞法則對於業務紀錄之例外規定。[38]

（3）驗真法則

同上之觀點，對電子證據的可採性不應予以特別的限制，但電子證據確實具有一些獨特之處：

A、極易受到篡改或破壞，且可能不留下任何痕跡；

B、它在技術上具有複雜性，可能會涉及不同軟硬體組成的電腦系統；

C、電子證據在儲存媒體中可能與大量的無關資訊雜存在一起，有遭污染之可能。

[37] 何家弘，同第二章註 20，頁 347。

[38] 何家弘，同第二章註 20，頁 347-348。

因此，該規則第五條規定：在任何法律程序中，擬引入電子文件的當事人負有依照本證據規則規定的方式證明其真實性的責任。[39]

（4）關於電子文件的證明力

為保證電子文件的真實性，不但需要對其驗真以保證其可採性，在評價其證明力時也要考慮其生成、存儲、傳達的方法或方式等因素以保證該文件資訊的準確性和完整性，從而評價其證明力。[40]

（5）證明的方法

由適格證人採用具結的方法，即有關電子文件可採性和證明力的一切事項，均可以通過適格證人之證言加以證明，並接受他方當事人交互詰問。[41]

3.3.3　修訂現有法律規範適用於電子證據

例如美國聯邦證據規則與一九九九年修訂之統一證據規則（Uniform Rules of Evidence of USA）。美國聯邦證據規則對於電子證據之規定將在第四章詳述，至於美國一九九九年統一證據規則以「紀錄（Record）」一詞替代原先使用的「文書（Writings）」、「錄音（Recordings）」、「照片（Photographs）」等詞，並規定「紀錄」是指通過有形方式記下的資訊，包括存儲在電子媒介和其他媒介中，並且可通過可察覺的形式獲知的資訊。實際擴展了「文書」、「錄音」、「照片」的內涵，使得電子證據得以適用與「文書」、「錄音」、「照片」等證據相同的證據規則。[42]

---

[39] 何家弘，同第二章註 20，頁 348。

[40] 何家弘，同第二章註 20，頁 349。

[41] 何家弘，同第二章註 20，頁 349。

[42] 美國統一證據法則原文請參見 http://law.upenn.edu/bll/ulc，中文譯文請參見何家弘，同第二章註 20，頁 506-517。

3.3.4 透過擴大對書證之解釋來處理之國家

例如上述法國於民法典中第一三一六條規定，當證據是由一系列文字、字母、數字或其他任何具有可理解的內容的符號或標誌組成的，不論其載體和傳輸方式如何，均為書證。再於第一三一六條之一規定將電子形式之文書與書面文書為相同之處理。或如我國刑事訴訟法仿效民事訴訟法第三百六十三條[43]及日本刑事訴訟法第三百零六條第二項之立法例，增訂第一百六十五條之一，規定準文書得為證據方法及其開示、調查之方法，以概括地規範將來可能新生的各種新型態證據。[44] 此外，我國亦有類此之規定。

[43] 民事訴訟法第 363 條：

「本目規定，於文書外之物件有與文書相同之效用者準用之。

文書或前項物件，須以科技設備始能呈現其內容或提出原件有事實上之困難者，得僅提出呈現其內容之書面並證明其內容與原件相符。

前二項文書、物件或呈現其內容之書面，法院於必要時得命說明之。」

該條例法理由：

「二　隨科技之進步，利用磁碟片、磁帶、錄音帶、縮影膠片等科技設備作成文書或保存文書、資訊等之應用，日漸廣泛；於訴訟中，舉證人以前開科技設備所保存之內容作爲證據資料，聲請調查時，如未顧及該等證據方法之特異性，一律依原條文準用本目之規定，令持有人必須提出原件時，恐有窒礙難行之處；爰增設第二項，規定證據方法須以科技設備始能呈現其內容或提出原件有事實上之困難者，提出人得僅提出呈現其內容之書面並證明其內容與原件相符，以代原件之提出。」

[44] 刑事訴訟法第 165 條之 1：

「前條之規定，於文書外之證物有與文書相同之效用者，準用之。

錄音、錄影、電磁紀錄或其他相類之證物可爲證據者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。」

該條立法理由：

「一　本條係新增。

二　隨著現代科學技術之進步與發展，不同於一般物證和書證之新型態證據，例如科技視聽及電腦資料已應運而生，我國刑事訴訟法原規定之證據種類中，並未包含此類科技視聽及電腦資料在內，爰參考我國刑法第 220 條及民事訴訟法第 363 條第 1 項之規定，暨日本刑事訴訟法第 306 條第 2 項之立法例，增訂準文書得爲證據方法及其開示、調查之方法，以概括地規範將來可能新生的各種新型態證據。」

3.4　立法例上之觀察

國際組織與各國對於電子證據之認識理解與調整適用，恰與一般人對電子證據理解認識之過程若合符節。電腦發明之際，除具專業知識之電腦工程師之外，一般人對其認識不深，此時具有法律專業之學者及實務界對電腦之瞭解與一般人無異。因此對於電子證據，因為商業交易之須要必須面對時，先認為與文書無異，或引用列印紙本為證據即可，並不瞭解電子證據之性質與傳統書證間仍有不同之處。

迨法律與資訊專業領域相互瞭解之後，發現書證與電子證據在性質上仍有不同，因此在分析之後，以等同功能法之角度，透過解釋而適用書證之相關規定，亦將電子證據擴大適用於刑事案件。

1、由電子證據之證據類型與調查方法角度觀察

（1）國際組織之角度

電子證據之證據類型，從聯合國貿法會歷次立法上來看，認為應採取「功能等同方法」處理之；亦即建議各國訴訟制度上應以評估傳統書證之相同標準對電子證據之「書面形式」、「簽名」及「原本」等議題加以認定。例如電子商務示範法第六條、第七條及第八條。

但是國際組織中的各種示範法，都只是認為以傳統書面形式的基本要求作為標準，一旦電子證據達到這些標準，即可同起著相同作用的相應書面文件一樣，享受同等程度的法律認可，惟證明力部分則應由各國依具體案件認定之。

（2）各國立法例之觀點

本文所參酌之立法例，皆以各種形式認定電子證據之性質屬於或頃向於書證性質，再依各國證據規則中對於書證之調查證據方法加以討論。例如南非、加拿大、美國聯邦證據規則、美國統一證據規則及我國刑事訴訟法第一百六十五條之一等規定。

2、由證據能力與證明力之角度觀察

（1）國際組織之角度

電子證據之證據能力及證明力，經過分析，認為應採取「平等對待原則」處理之；亦即法院應以評估傳統證據之證據能力及證明力之相同標準對電子證據加以認定。例如電子商務示範法第五條及第九條。

此外，網際網路發達之後，不論民事或刑事之電子證據均具有跨國性、國際性之特徵；因此國際組織特別針對電子證據跨國蒐證、取得、保全等程序作出規範，以求即時保全證據，並避免提出於內國時被法院以不具證據能力或證明力而摒除於訴訟外。

（2）各國立法例之觀點

各國對於電子證據之證據能力及證明力多半為直接於刑事訴訟法或證據規則中直接做出規範。英美法系國家因為採行當事人進行主義，各項證據法則除別有規定外均一體適用於民、刑事案件，因此違反各項證據法則，會被法院以無證據能力排出之。直於大陸法系國家，對於證據能力之認定亦如我國一般日益嚴格，違反法律對於證據能力之規定者，將無證據能力而排除之。

至於電子證據的取得、蒐集或保全是否符合程序，各國執法機關均有相關之規定，惟此類規定多半屬行政規則或手冊，例如美國司法部之 Searching

and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 及 Electronic Crime Scene Investigation－A Guide for First Responders[45]，或我國內政部警政署警察偵查犯罪規範對於電腦犯罪案件之處理原則及應注意事項[46]等是。

[45] The Technical Working Group for Electronic Crime Scene Investigation, Department of Justice, U.S.A., 2001.

[46] 關於我國警方實施電腦犯罪之偵防，作業規範請參見本文附錄。

第四章　電子證據的證據能力與證明力

4.1　前言

我國刑事訴訟程序中，對於證據能力與證明力之觀念，雖然教書均有提及，然而因為我國是以具法律專業之法官來審理案件，非以不具法律專業之陪審團為之，因此並未嚴格將不具證據能力的證據排除在審判外。亦即一切證據均得以進入訴訟程序中為審判之參考，由法官認定是否應予採認為認定犯罪事實之依據。

因為在實務操作上並未加以重視，因此證據能力與證明力之觀念並問落實於對刑事證據之採認上。即使是判例或判決，亦往往有對證據能力與證明力混淆不清之情形發生。[1]

我國新制刑事訴訟法，本來對於證據能力，並無明確規定，僅有修正前刑事訴訟法第一百五十九條：「證人於審判外之陳述，除法律有規定者外，不得做為證據。」有學者將之解釋為對於傳聞證據排除之規定[2]，倘採此見解，該條文可視為屬於對證據能力之規定，除此之外，並無其他條文對於證據之證據能力作出規定。

民國九十二年刑事訴訟法修正，修正後第一百五十五條第二項規定：「無證據能力、未經合法調查之證據，不得作為判斷之依據。」係首次將證據能力之概念明訂於條文之中。

---

[1] 對於證據能力與證明力產生混淆之實務見解，請參見第一章註 8；並請參見黃朝義，「證據基本概念與舉證責任」，警察法學第 5 期，頁 329-332，內政部警政署，2006 年 10 月。新制刑事訴訟程序實施後，亦有發生法院在進行準備程序時，被告對於各項證據不討論證據能力，及一概加以否認其證明力之情形發生。足認我國往昔對證據能力與證明力並未強調才會有這種情形發生。

[2] 早期僅學者黃東熊主張我國修正前之刑事訴訟法第 159 條「證人於審判外之陳述，除法律有規定者外，不得做爲證據。」之規定爲傳聞法則，參見黃東熊，刑事訴訟法研究，第 222 頁，自版，民國 70 年；刑事訴訟法論，頁 451-452，三民書局，88 年 3 月。

證據能力之證明方式須採嚴格的證明，亦即據以判斷作為認定犯罪事實依據之證據，必須在法律規定所准許的證據方法範圍內，並且依法律規定的調查程序踐行之，兩者同時俱備，才取得證據能力。[3]符合嚴格證明之要求，法院始得引為判斷犯罪事實之依據，反之則否。刑事訴訟法第一百五十五條第二項立法理由二：「本條第二項規定無證據能力之證據，與未經合法調查之證據，不得作為判斷之依據，正足以表示『嚴格證明』之要求」 即為此意。

至於證明力，因為採自由心證主義，由法院自行認定，因此往往造成民眾誤會法院對證據之認定係恣意為之，修正後刑事訴訟法第一百五十五條第一項特為規定：「證據之證明力，由法院本於確信自由判斷。但不得違背經驗法則及論理法則。」立法理由亦再加說明：「本法就證據之證明力，採自由心證主義，將證據之證明力，委由法官評價，即凡經合法調查之證據，由法官依經驗法則及論理法則以形成確信之心證。惟一般社會大眾對於所謂「自由」二字每多曲解，誤以為法官判斷證據之證明力，無須憑據，僅存乎一己，不受任何限制，故經常質疑判決結果，有損司法威信。爰參考德國刑事訴訟法第二百六十一條之規定，及最高法院五十三年台上字第二０六七號及四十四年台上字第七０二號判例之見解，修正本條第一項，以明法官判斷證據證明力係在不違背經驗法則、論理法則之前提下，本於確信而自由判斷。」

證據能力與證明力之觀念，因為在此次刑事訴訟法明文規定以確立其觀念，因此本文認為對於電子證據之適用或調整，有必要在此作一探討。

[3] 林鈺雄，「嚴格證明法則與直審理原則」一文，收於氏著嚴格證明與刑事證據一書，頁 8-9 ，學林文化事業有限公司出版，2002 年 9 月。

4.2　證據能力與證明力概說

1、證據能力

證據能力又稱證據之可採性（Admissibility）、證據容許性、證據資格、證據適格等等。「Admi-」字源即有「允許」、「容許」之意。證據能力係指提交於法院的證據能夠被法院所接受，亦即證據有一定之資格能夠在法庭上被允許提出。

證據能力為英美證據法則上的核心問題，旨在保證法院採納之證據是可信任、可靠及符合法定程序之證據。[4]因為英美法系國家採取陪審團審判制度，由陪審團成員為事實之判斷，為防止不具法律專業的陪審團產生偏見或感情用事，所以英美證據法則上對可以使用為證據之範圍加以限制，此即為證據需具備證據能力之要求。

證據能力較少有正面的規範，多半是以數個證據排除法則如違法證據排除法則、傳聞法則、自白排除法則等等來加以形塑其內涵。[5]

證據的可採性與嚴格證明密切相關。可採性法則適用於為確定被告是否有罪之嚴格證明過程[6]，其他程序中則不適用之。

2、證明力

證明力係指證據對於案件所欲調查或證明之事實是否有證明作用及其作用之程度，故又稱為證據價值、證據力。證據證明力之英文為「Probative Value」，由此可知證據證明力在討論證據對於案件或待證事實之「價值」、「份量」，凡此皆屬於

[4] 郭志媛，刑事證據可採性之研究，頁 24，中國人民公安大學出版社， 2004 年 4 月。

[5] 同前註。

[6] 同前註 4，頁 26。

事實問題；證據證明力是指證據在證明待證事實上所體現之價值大小及強弱狀態或程度而言。[7]

3、證據關聯性、證據能力與證明力之比較

（1）證據關聯性是邏輯與經驗之問題，對於關聯性之判斷，有賴於人類的生活經驗與邏輯；而證據可採性是法律問題，對於可採性之判斷，完全取決於證據法則所預先設立的規定。因此對於證據關聯性僅能做原則性之規範。例如聯邦證據規則第四０一條至第四０三條。

我國非採陪審團制度之國家，新修正之刑事訴訟法雖於第一百六十三條之二第二及第三款規定：

「當事人、代理人、辯護人或輔佐人聲請調查之證據，法院認為不必要者，得以裁定駁回之。

下列情形，應認為不必要：

一　不能調查者。

二　與待證事實無重要關係者。

三　待證事實已臻明瞭無再調查之必要者。

四　同一證據再行聲請者。」

然而此規定非等同於聯邦證據規則前開條文之規定。由法院依邏輯與經驗判斷證據與待證事實間之關聯性。至於證據可採性我國與美國均是以法律明訂之方式形塑其範圍。

（2）證據能力指的是依法可被容許和可被採作證據的資格，也被稱之為證據資格或證據適格性。亦即符合法律之規定而得到法律之承認而具有證據能力；反之則不具證據能力。由此可之，證據能力產生於法律上的規定，它是「外掛（Plug-in）」於證據上，並非證據本身所固有者。至於證據證據力隨證據的產生而產生，隨證據的存在而存在，其意義是「內建（Build-in）」的。

[7] 何家弘，同第二章註 20，頁 134。

（3）證據證明力是從實質上考察證據，係屬於客觀、自然之範疇。證據能力則是人類法律制度對證據之認定，屬於主觀、人為之範疇。從順序上觀察，證據能力之產生應以證據／證據證明力為前提。沒有證據／證據證據力存在，則證據能力失其存在的基礎。

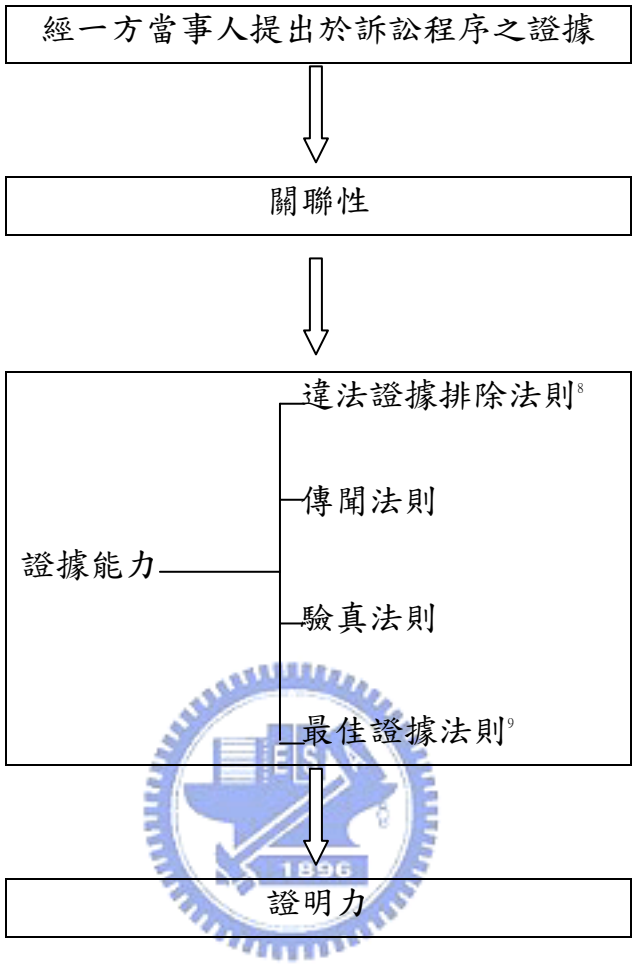
證據證明力應先於證據能力，但是人類基於人權保障、程序正義等等考量，透過法律制度相反操作。規定任何證據，必先滿足

A、於法律所准許之證據方法範圍內，且

B、依法律規定的調查程序踐行之

必二者同時俱備，方能取得證據能力。反將對自然、客觀存在之證據證明力之考量，至於人為、主觀之證據能力之後。

圖 4-1　證據能力與證明力與刑事證據法則對應關係



[8] 本文違法證據排除法則在檢驗順序上應優先於傳聞法則，因爲在美國制度上，前者之規範多爲美國聯邦憲法（修正案）位階，傳聞法則規範之相對位階較低。此外，若證據之取得爲違法遭排除，則不會進行其他證據規則之檢驗。至於在我國，雖然同規範於刑事訴訟法內，然而本文考量爲保障程序正義與避免公權力遭濫用，仍應強調違法證據排除法則優先於其他證據法則被檢驗，惟如此排序純爲本文之觀點。

[9] 在美國證據規則下最佳證據法則屬於證據能力，我國刑事證據法則中並無最佳證據法則之規定，法院會列爲證明力之範圍。

4.3　電子證據之證據能力

電子證據的證據能力是用以決定何種電子證據能夠進入訴訟程序或應予排除之機制。為進行訴訟活動所蒐集之任何電子證據，均必須符合法律規定的程序並經過法院就合法性所為之判斷，才能提出於訴訟之中，證明該電子證據本身欲待證明之事項。

4.3.1　美國

4.3.1.1　證據能力對於電子證據適用之爭議

美國屬陪審團制度之國家，電子證據要在訴訟活動中被採納，須不被各種排除法則如違法證據排除法則、傳聞證據法則、驗真法則及最佳證據法則等所排除[10]，始足當之。其中又以傳聞證據法則及最佳證據法則是欲將電子證據採為證據最主要之障礙。

基此，有學者認為電子證據是否具有證據能力，應注意兩方面：

1、電子證據合法性之問題

隨著社會資訊化、數位化之發展，電子資訊與人類的生活、工作有著密切的關聯性，電子證據之蒐集過程極易造成人民通信、隱私等方面權利之侵害，若關於蒐集電子證據之過程違法，則該證據在訴訟中之資格將會受到挑戰質疑，甚至喪失。因此，電子證據合法性之要求是其證據之適用上首要討論者。[11]

[10] 皮勇，同第二章註 20，頁 53。

[11] 皮勇，同第二章註 20，頁 53。

2、電子證據真實性之問題

電子證據容易被刪除、篡改而難以驗真辨偽。[12]因此，如何其真實性之問題即成為重要議題之一。[13]

4.3.1.2 證據能力對於電子證據適用之調整

美國聯邦證據法則並無對電子證據在可採性方面，作出特別規定，因此對於訴訟活動中日益增加的電子證據，端賴司法實務，亦即具體案例中累積建構其法則。

電子證據要能取得證據資格，須要判斷是否符合法定程序，得以通過嚴格證明之考驗。應從以下層面加以考量與判斷：

1、蒐證主體的合法性

刑事偵查案件中蒐集證據的責任是由司法警察機關及檢察機關為之，於電子證據之蒐集方面亦不例外。倘若有司法警察機關或檢察機關違法蒐證之情形，則其所取得之證據自不得為訴訟活動中所採用。

此外，實際執行業務之蒐證人員也必須具備調查取證資格，其身分必須是具有法律賦予其權力之法定人員。惟由於電子證據是高科技產物，一般的蒐證人員很難具備相關的專業知識，因此，被授權具有電子證據取證資格的電腦專家、第三方機構在案件需要的情況下也可作為合法的蒐證主體。[14]非具有法定身分之人員所調查取得的電子證據，不具有證據能力。

---

[12] *See,* J. Shane Givens, "*THE ADMISSIBILITY OF ELECTRONIC EVIDENCE AT TRIAL: COURTROOM ADMISSIBILITY STANDARDS*", 34 Cumb. L. Rev. 95,2003. (http://www.lexis.com/research/retrieve?_m=8e87e3acb4c42f7157dfed93d537837a&csvc=bl&cform=bool&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=d21507ef554b1a33e00a464344debdc8) ,last visited on June 10, 2007.

[13] 皮勇，同第二章註 20，頁 53。

[14] 蔣平，同第二章註 94，頁 166-167。

2、蒐證程序的合法性

執法人員違反法定程序擅自侵入他人電腦或網路系統中所獲得之電子證據不具有證據能力，理由在於若容認執法人員以違法手段獲取證據，會鼓勵偵查人員的違法行為，縱容對人民隱私、住宅和人身等權利之侵害。因此，要採取法定措施保證蒐證的合法性。[15]

倘若符合各項合法性之規範，則該項電子證據就適法性層面具有證據能力，得以被法院採納；反之則應受違法證據排除法則之規範加以排除之。

至於在電子證據真實性方面，應注意到以下三個層面之問題：

1、電磁紀錄是否遭到偽造、變造

因為電腦紀錄具有脆弱性，往往遭提出系爭電子證據之他方當事人質疑該電子證據遭到篡改，通常法院不否認電磁紀錄確有可能遭到修改，但若質疑之一方沒有舉證證明遭到篡改，則不會影響證據之真實性。[16]

2、產生電磁紀錄之電腦軟體或硬體出錯不可靠

對造當事人亦往往爭執產生系爭電磁紀錄之電腦軟體或硬體不可靠，有可能出錯，並要求測試或送鑑定。

法院見解認為認為提出證據之一方必須證明該資料之可靠性(reliability)作為合適的基礎(proper foundation)，合適的基礎必須是在日常業務活動有規律的實施中所記錄與保存的資料，並且由管理人或其他有資格的證人出面作證，而這些資料還必須符合

[15] 蔣平，同第二章註 94，頁 167。

[16] *See*, e.g. United States v. Whitaker.

連續性及負責盡職性(conscientiously)。政府部門只要提出足夠的事實證明該紀錄值得信賴(trustworthy)，且賦予相對人交互詰問權即為已足。[17]

3、電磁紀錄製作人真實身分之確認

傳統文書可藉由筆跡鑑定判斷製作人之身分，但電磁紀錄則否。此外，許多電腦技術足以讓人以匿名或冒名方式使用電腦或上網[18]。因此，當檢察官提出電子證據欲證明被告涉嫌犯罪時，被告往往質疑該電子證據之真實性，辯稱電子證據係他人所製作。[19]

通常法院對於此種非常態之抗辯，均會要求抗辯之一方盡舉證責任，自不待言。

4.3.2 我國

4.3.2.1 證據可採性對於電子證據適用之爭議

電子證據就證據能力部分，仍然應著眼於前述電子證據合法性與真實性之層面。目前在訴訟中竟證據能力部分經常發生爭執之點，主要有以下幾種情形：

1、電子證據形成時，電腦軟硬體是否正常

電子證據形成時電腦機械、作業系統或應用程序等電子軟硬體是否處於正常狀態下運作，若運作不正常，是否會進而影響電子證據之正確性？

[17] 錢世傑，同第一章註 7，頁 73。

[18] 例如本文前所提及之僞冒網路卡序號（Mac Address）、或以下所提及發送匿跡郵件等行爲。

[19] 林一德，同第一章註 7，頁 128。

例如被告可能抗辯某伺服器所採用中央處理器（Central Process Unit，CPU）浮點運算單元有瑕疵[20]，或所使用之作業系統不穩定、有漏洞[21]，或有外力干擾[22]，以致於所生成之稽核檔電磁紀錄中錯誤紀錄其 IP 位置，至令被告遭誤會未經許可無故侵入該伺服器。

2、蒐證程序違法

執法人員於執行電磁紀錄蒐證時是否符合法令之規範[23]、是否以違法侵入他人電腦之方式取得電磁紀

[20] 浮點數是屬於有理數中某特定子集的數的數字表示，在電腦中用以近似表示任意某個實數。這個實數由一個整數或定點數（即尾數）乘以某個基數（電腦中通常是 2）的整數次冪得到，這種表示方法類似於基數爲 10 的科學記數法。至於浮點運算則是指浮點數參與的運算，這種運算通常伴隨著因爲無法精確表示而進行的近似或捨入。電腦採二進位制運算，對於二進位浮點數算術標準，以電氣電子工程師協會（Institute of Electrical and Electronics Engineers，IEEE）所制訂之 IEEE 754 爲最廣泛使用之運算標準，大多數 CPU 或浮點運算器（Floating-Point Unit，FPU）均遵循標準。最早浮點運算器是一顆在主機板上獨立負責處理有關於浮點數值運算之晶片，到了 INTEL 公司推出 Pentium 處理器之後，由於電晶體體積一直縮小，便將浮點運算器直接內建於 CPU 中，不透過橋接晶片傳輸數據，以增加運算時的效能。然而初期因爲技術未臻成熟，故發生浮點運算單元瑕疵，會發生計算錯誤之情形。

[21] 例如臺灣高等法院 95 年度上易字第 2214 號刑事判決：「一、訊據被告○○○固坦承伊曾侵占告訴人 XX 公司永吉分銷店收入之現金款項，惟否認伊自 87 年 7 月 20 日起即以上開方式侵占告訴人款項達 1550 萬 2893 元，辯稱伊係於 88 年 3 月起始爲侵占犯行，侵占款項僅爲 204 萬 5 千元，且因告訴人之電腦系統存有瑕疵，伊每月所列印出之科目餘額表中『應收票據』欄均爲零，故伊係利用此漏洞將「庫存現金」科目之款項改列於『應收票據』以侵占告訴人之款項，但從未將『庫存現金』科目款項列於『應付各費』、『暫收業務款』等科目云云。」

[22] 例如臺灣臺北地方法院 94 年度交聲字第 288 號交通裁定：「三、異議人即受處分人之異議意旨略以：經分析二張採照片可知，兩張照片之時間相隔 0.6 秒，兩張照片行車距離約少於 8 公尺，因此行車速應該是 48 公里左右，又測速雷達測出速度有誤之主因是發射之電波被車旁之大卡車干擾產生錯誤結果。」

[23] 例如臺灣板橋地方法院 91 年度訴字第 1028 號刑事判決：「『…又本案搜索聲請、執行及扣押之進行等程序，乃由未具司法警察官或司法警察權限之調查局人員爲之，顯已違反前揭刑事訴訟法第 128 條之 1、之 2、第 136 條規定而不合法，本案全部扣案物均無證據能力。』、『又告訴人所提出之光碟係未經合法的採證，且係事後製作，認無證據能力。』、『本件搜索票載明之搜索範圍只有電腦、光碟片及磁片，不包含上述範圍以外之文書，故扣案之帳號密碼表爲違法取得之證據，不具證據能力』」本案被告就電子證據可供抗辯之爭點提出甚多，頗值由電子證據各角度加以研究。

錄、在網路上截留他人電子郵件或聊天紀錄之適法性，甚至所承辦或移送之案件類型是否符合機關執掌[24]等，均為討論之重點。

3、合法保存及提出之認定

電磁紀錄於案發時或案發後有無予以妥適合法保存，並以適切之形態提出於法院。又電磁紀錄若為被害人或告訴人所提出，則是否遭篡改或偽造。

4、實際製作（犯罪）人身分之認定

由於電腦紀錄等電子證據表現為「0」與「1」數位化之電磁紀錄，除非使用者使用了特定的身份鑑別方式，如公私密鑰加密、電子簽章等，否則僅從電子證據本身無法直接證明其製作者的身份。[25]

反之，現今傳播媒體發達，駭客植入木馬以他人電腦為跳板遂行犯罪之新聞屢聞不鮮，因此訴訟當事人一方往往抗辯其電腦遭駭客入侵植入木馬，被當成犯罪工具之跳板；[26]或駭客入侵後利用其電腦散發妨害

[24] 同前引刑事判決：「一、被告○○○之辯護人抗辯本案◎◎實業股份有限公司以違反電信法、通信保障與監察法等妨害祕密所提之告訴，均非在法務部調查局組織條例第 2 條規定所職掌之範圍內，尤本件為告訴乃論之罪，其保護者僅屬個人法益，更不應論為『重大』之經濟犯罪，準此，調查局既非『依法令關於特定事項，得行司法警察官之職權者』，該局自不屬於刑事訴訟法第 230 條第 1 項所定之『司法警察官』，則告訴人於 90 年 6 月 6 日以聲請函提出本件告訴，於告訴當時，既非以『檢察官或司法警察官』為提出的對象機關，該告訴程序於法未合，且告訴人受任人 XXX 固於 90 年 11 月 2 日於檢察官偵訊時以言詞提出告訴，但其當時未經合法委任而提出委任狀，且由偵查卷內可知告訴人乃至遲於 90 年 5 月 16 日即知悉本件事實，XXX 提出告訴之時日已逾越 6 個月告訴期間，其告訴亦於法未合。」

[25] 皮勇，同第二章註 20，頁 60。

[26] 例如臺灣高等法院 94 年度上訴字第 564 號：「被告○○○抗辯伊公司電腦 IP 位置 211.21.176.xxx 遭人以木馬程序入侵申設 Email 帳號，發上開攻擊信函・・・」、臺灣臺北地方法院 93 年度訴字第 588 號刑事判決：「被告辯稱：右揭犯行均係他人所為，與被告無關，被告既未冒用○○○、◎◎◎名義申請電子郵件信箱，亦未上網出售 COACH 包包，復未通知 XXX、◎◎◎匯款至其中興銀行中山分行帳戶，更未寄電子郵件給 XXX、◎◎◎，遑論冒用◎◎◎名義申請帳號、散布◎◎◎援交郵件，右揭犯罪事實可能係遭他人以木馬程式進

他人名譽電子郵件；或無線網路未加密而遭人盜用。

5、電子證據是否遭到篡改

若法院或訴訟他方能證明電子證據形成後遭到篡改，則此種電子證據必須被排除。[27]惟若僅能證實電腦系統存在有被篡改之可能性，則尚不足以認為此一電子證據不具有可採性而應被排除。[28]

行遠端遙控侵入其電腦所為，依其日常生活作習，於午夜 12 時前均已就寢，故無法察覺電腦遭人侵入，何況起訴書所指ＩＰ位址：「163・21・183・XXX」為臺北市立師院附小之固定ＩＰ，且 92 年 2 月 22 日為被告任職之建國高級中學學校日，被告當時在學校內與學生家長 AAA 聊天，豈可能分身至臺北市立師院附小上網連線？況被告並不認識在超商提款機提款之人，被告從未使用中興銀行中山分行帳戶金融卡，故未查覺該金融卡已遺失云云。被告否認有於 92 年 2 月 4 日至同年月 25 日間，於如附表一所示時間使用電腦以 wang8xxxx、chumimixxx 帳號連結上網至雅虎公司，而辯稱如事實欄所示之行為，係遭人以木馬程序侵入其電腦，以遠端搖控方式所為，因其平常於未使用電腦時，雖未關機，但均關閉電腦螢幕，所以未查覺電腦已遭人入侵控制云云。」

[27] 同前引刑事判決：「告訴人提出之郵件伺服器紀錄檔光碟片，其所載內容係隨時可編輯更動，且該光碟片係告訴人於 90 年 6 月 6 日隨同○○公司之聲請函提出予市調處，惟依本院 93 年 1 月 12 日之勘驗筆錄，該光碟片目錄檔中卻可看出其內載之紀錄日期包含 90 年 6 月 7 日，是該光碟片之來源（提出時間、提出人）及內容均有疑問，顯無證據能力。」、臺灣臺北地方法院 92 年度訴字第 1411 號刑事判決：「惟辯稱：學校網頁會公布帳號即學號・・・，學號則可自當時之准考證號碼查得，・・・此外，告訴人○○○所提出之電子郵件非為自伺服器直接列印之正本，而為影本，有可能遭篡改、增刪，・・・況依 XXX 於 93 年 4 月 13 日庭訊時證稱其並不確定偵卷第 12 頁之電子郵件是否係從其電子郵件信箱中直接列印等語，而該頁之電子郵件亦未經郵件空間提供者之驗明，則該郵件是否為真實，或已經篡改、增刪，顯有疑問，自不能僅憑真實性並不確定之電子郵件影本即論斷該郵件係由被告所發。・・・若非有人予以篡改，該郵件即屬偽造而成，該頁電子郵件應欠缺本案之證據能力。」、臺灣板橋地方法院 91 年度易字第 2968 號刑事判決：「（5）、辯護人雖以被告張○○無使用遠端撥入（RAS）及備份操作員（Backup Operators）權限之必要；就上揭 XX 公司佐證資料光碟片中之「Johns」帳號使用者權限圖示而言，在「不隸屬於」一欄中如「Acc、Account Operators、Adm、Administrators」等權限，可輕易點選其中一項，並按「新增」鈕而加入「隸屬於」欄，成為該帳號使用者之權限，容易進行篡改，而任意增加「Backup Operators」備份操作員之權限；況且偵查卷所附檔案資料夾名稱為「John」，與被告張○○設立之「Johns」目錄夾有別，而建立時間或為西元 2002 年 2 月 19 日，或西元 2001 年 12 月 7 日，皆與公訴人起訴之 89 年底有別，且在被告張○○離職（90 年 3 月 28 日）離職後，顯見該「Johns」使用者權限有遭人更動之虞云云。」

[28] 該電腦系統存在遭篡改可能性之大小，雖不影響證據可採性，惟得由法院以之權衡判斷其證據證明力之價值程度。參見皮勇，同第二章註 20，頁 61。

6、電磁紀錄經顯示後可能產生意義上之誤差

電磁紀錄為「0」與「1」之磁氣組合，儲存於載體時，無法為人類透過感知而瞭解其意義，此時將之顯示於電腦螢幕或列印為紙本以供閱讀，一般咸認係較妥適之方式。惟電磁紀錄在此轉換之過程中，需與顯示卡、螢幕電腦、記憶體、儲存載體、CPU、印表機等硬體及作業系統、應用程序等軟體間發生互動交集。因此電磁紀錄於轉換成螢幕顯示或紙本文件時有可能發生誤差。例如欲將網頁列印，卻出現亂碼或方格[29]；或如在螢幕上觀看 PDF 檔案正常，列印時卻在某些地方出現亂碼[30]等均是一般電腦使用者常見之情形。

4.3.2.2 證據可採性對於電子證據適用之調整

對於電子證據之證據能力，本文認為除依刑事訴訟法對證據能力之各項規範外，於有裁量權限可得審酌是否有證據能力時，除可依新制刑事訴訟法第一五八條之四立法理由「三」所提供之參考事項[31]外，若專就電子證據之特性加以考量，尚可就以下各點加以參考：

1、以違反法律強制或禁止之規定所取得之電子證據，例如違反通訊保障及監察法[32]、違法搜索扣押或其他不正方式取得之電子證據、違反傳聞法則之電子證據等，均應予以排除之。

---

[29] 參見 http://blog.bs2.to/post/EdwardLee/566 ,last visited on June 10, 2007.

[30] 參見 http://anais.fang.free.fr/forum/viewtopic.php?id=891,last visited on June 10, 2007.

[31] 該條例法理由三：「法官於個案權衡時，允宜斟酌(一)違背法定程序之情節。(二)違背法定程序時之主觀意圖。(三)侵害犯罪嫌疑人或被告權益之種類及輕重。(四)犯罪所生之危險或實害。(五)禁止使用證據對於預防將來違法取得證據之效果。(六)偵審人員如依法定程序有無發現該證據之必然性及(七)證據取得之違法對被告訴訟上防禦不利益之程度等各種情形，以為認定證據能力有無之標準，俾能兼顧理論與實際，而應需要。」本文認為法院審酌之標準「包括但不限於」上開 7 項標準，以免對法官裁量權限有不當限制。

[32] 甫修正後經總統公布，將於 96 年 12 月 11 日施行之通訊保障及監察法第 5 條、第 6 條及第 7 條均有規定違法進行通訊監察所取得之證據應相對或絕對排除之。

2、非處於常態狀況下之電腦設備所生成之電子證據，例如電腦設備非於正常運作之狀態；提出證據之一方所交付之電子證據不完整、片段、不連續；未經合法保存、無法證明該電子證據為真實等情形，該電子證據應認為無證據能力。反之，則應認為有證據能力。

4.4　電子證據之證明力

電子證據證明力主要指電子證據與其他形式的證據相比較時所體現出的證明力的大小問題，有時則指證據本身的說明力，與電子證據證據能力屬於法律問題不同，電子證據證明力是屬於事實問題。[33]

4.4.1　美國

4.4.1.1　證據證明力對於電子證據適用之爭議

證據證明力的證明方式主要是基於通常的經驗或常識，而非基於既定的法律法則，亦即我國所稱的自由證明。這種證明方式是根據法官或陪審團成員對證據與待證事項的觀察與經驗所做出的符合常識的決定，即二者間存在多大或多少之因果關聯。[34]此一點於判斷電子證據之證明力亦同。

目前為止，不論美國或我國，多數法官及陪審團成員對於電子技術或資訊技術，均非專家，縱使法官具有法律上或證據方面之專業，亦缺乏資訊或電子之專業，而足堪能對「電子」與「證據」的結合之電子證據正確的判斷或指示。[35]

---

[33] 蔣平，同第二章註 94，頁 168。

[34] 何家弘，同第二章註 20，頁 134。

[35] 我國法學教育與大陸法系國家如德國、日本相同，高中畢業考取大學後選擇就讀法律學系

4.4.1.2 證據證明力對於電子證據適用之調整

美國聯邦證據法則對於電子證據之證明力並無特殊規定，因此仍應認為對於電子證據證據力之認定，回歸到自由心證之傳統。

無論是電子證據還是傳統證據都有自身的不安全或不可靠因素，隨著電子技術尤其是電腦技術的成熟和廣泛應用，人類對電腦之可靠性也應逐步提高。因此，學術界及實務界均賦予電子證據與傳統證據以平等待遇，不因不信任而不願意使用電子證據、或者不敢賦予電子證據以足夠的證明力，亦即給予電子證據與傳統證據相同之待遇。[36]只要能證明電子證據之真實性，則證明力之份量或價值由陪審團判斷之。[37]

（Department of Law），完成 4 年法學教育後通過司法考試而成爲檢察官、律師或法官，然後就（執）業。開始工作後因爲業務繁重、照顧家庭等因素，較少有機會對於資訊科技等加以進修，以作爲工作上之輔助。英美法系國家如英國、美國、澳洲等，大學不設法律學系，係在完成學士課程後至專業法學院（Law School）深造 3 年後通過考試投入就（執）業。法學院招收學生範圍甚廣，理工醫農文史法商兼而有之，資訊系畢業學生在大學 4 年學得資訊專業，待完成法學院學業後，對法律與資訊均能有所掌握。近年來世界快速變動，單一法律專業漸漸不足以因應社爲需要，因此有倡議將我國法學教育改採學士後法學院制度者。惟具雙重專業者在中外就（執）業市場均甚受重視，是否願意屈就薪資較低之政府體系，猶有疑問，美國公務部門司法人員流動快速，充實經驗後即轉任至大型律師事務所之情形，向爲該國政府所苦惱。又，英美國家法官多半爲執業多年、素富聲譽之律師或檢察官轉任，惟資訊科技發展一日千里，半導體中摩爾定律（半導體晶圓上可容納的電晶體數目，約每隔 18 個月便會增加 1 倍，性能也將提升 1 倍，而價格下降 1 半）於資訊業均能適用，因此執業多年後擔任法官者，是否仍保持最先進、充分之資訊專業得以對電子證據做出正確指示，亦待觀察。再，未來各種類型之案件中均有可能提出電子證據，承審法官縱具其他如建築、金融專業，對於電子證據之瞭解亦與常人無異。

[36] 何家弘，同第二章註 20，頁 138-139。

[37] *See* MARK D. ROBINS, "*Evidence at the Electronic Frontier: Introducing E-Mail at Trial in Commercial Litigation*", 29 Rutgers Computer & Tech. L. J. 219, 2003. (http://www.lexis.com/research/retrieve?_m=8b8da1766c656334d7ceff46a76452fc&docnum=22&_fmtstr=FULL&_startdoc=21&wchp=dGLbVtb-zSkAl&_md5=48b24ec02a24252e95c125ab05d8664b) ,last visited on June 10, 2007.

4.4.2　我國

4.4.2.1　證據證明力對於電子證據適用之爭議

電子證據縱然通過可採性之檢驗，認為具有證據能力，但該項電子證據是否得以證明待證事實，或對於欲證明待證事實有多大價值，亦即電子證據之證明力如何，往往成為訴訟過程中攻防雙方爭論之重點，亦深居於中立審判地位之法院所困擾。

本來，證據之證明力概由法院依自由心證加以判斷，時至今日仍然是最基本的見解。然而對於數位資料及電腦資訊的不熟悉，以及相對於法律體系是「緩慢而穩定」的演進，電子資訊科學卻高唱「摩爾定律」、「十倍速時代」，以目不暇給的速度在成長。因此要使參與訴訟活動之各方對電腦資訊、電子證據能夠有所掌握與瞭解，並進而精準適切的予以檢驗適用，不論中外均為十分困難之挑戰。相對的，對電子知識無法充分掌握，亦往往為抗辯電子證據之一方展現了絕佳的辯護戰場。

例如在臺灣臺北地方法院八十九年度訴字第九二九號案件中，檢察官認為被告林某與新加坡籍人黃 X 明知「駭客任務 The Matrix」等視聽著作，分別係美商時代華納娛樂公司（TIME WARNER ENTERTAINMENT COMPANY, L.P.，下稱美商華納公司）、美商迪士尼企業股份有限公司（DISNEY ENTERPRISE,INC，下稱美商迪士尼公司）之著作，惟共同基於意圖銷售營利及意圖為自己不法所有之概括犯意，自八十八年三、四月間某日起，在住處先後多次以該處所裝設之二三○六 XXXX 號電話，向網中華電信申請之 XXXXX 撥接帳號，在 tw.bbs.comp.hacke 等新聞群組以「光碟女王」名義，散佈隱匿電子郵件寄件人資料之販賣盜版光碟片之交易訊息，迨不特定人上網以發送電子郵件之方式下單訂購後，即未經前揭著作權人之同意，連續擅

自以 CD-R 重製上開視聽著作，再透過不知情之郵差寄送交付前開盜版光碟片予訂購之人，檢察官經過偵查後，以八十八年度偵字第二０九五四號提起公訴。

1、檢察官認為被告林某涉嫌犯罪，理由中有二項：

（1）網路撥接帳號為被告林某所申請。

（2）扣案電腦中林某所撰寫之「博士論文 3」與盜版光碟「訂單」二文件之系統最後一次儲存時間相同，因認係同一人即林某所編輯為其依據。

2、惟法院判決認為林某無罪，其理由為：

（1）被告王某、林某雖均供承前開 XXX 撥接帳號係被告林某所申請，惟亦於警訊時陳稱其等回系爭查獲地點使用電腦時，曾將帳號密碼儲存在電腦中以利撥接，使用被查扣電腦之人即可能以該帳號撥接上網等語，衡情亦不違常理，是要難以「光碟女王」曾有藉由該撥接帳號連接上網，即認被告王某、林某亦參與本件犯行。

（2）又依偵查卷附扣案電腦Ｃ硬碟中 MY DOCUMENT 資料夾內檔案全覽列印資料所示（第二六－一頁），WORD 文件「博士論文草稿 3」與 WORD 文件「訂單」之最後存檔時間均為西元一九九九年五月九日上午九時七分，而 WORD 文件「訂單 0511」之最後存檔日期為西元一九九九年五月九日上午十時十七分，另「訂單」及「訂單 0511」文件經開啟後，內容均為客戶訂購盜版光碟之訂單，有偵查卷附列印資料可佐（第二六－七至二六－九頁），又「博士論文草稿 3」文件確係被告林某所繕打，固經被告林某所是認；惟查，上揭所述僅顯示「博士論文草稿 3」與「訂單」二文件曾同時或在相差不到一分鐘之內之時間 存檔，然編輯文件時間與存檔時間並無必然關聯

> 性，如被告林某所辯「此種二文件存檔時間相同之情形，或係其在編輯「博士論文草稿 3」時，因照顧幼女而中斷工作，但未存檔，而後有人編輯「訂單」文件，在編輯完成後，將 WORD 程序關閉，此時 WORD 會提醒使用者將未存檔之文件存檔，如此存檔後二文件之儲存時間即會相同」，亦非絕無可能，又「博士論文草稿 3」與「訂單 0511」之最後存檔時間不同，亦難謂係同一人所編輯，是在無其他積極證據佐證之下，徒以「博士論文草稿 3」與「訂單」二文件之存檔時間相同，即推論該二文件係同一人所編輯，尚嫌速斷。[38]

因此，對於電子證據證明力認定，本文相信比一般證據有更多討論之空間，隨伴而來之挑戰亦因而增加。

4.4.2.2　證據證明力對於電子證據適用之調整

關於證據之證明力，固得由法院依自由心證加以判斷之，依修正後刑事訴訟法第一五五條第一項之規定，輔以違背經驗法則及論理法則。

在斟酌電子證據證明力時，應採取以下方向：

1、在形式證據力層面，考量電子證據之真實性時，應審酌電子證據之準確性及完整性，例如該項證據在形成、儲存、複製或傳輸、蒐集等方面是否受到影響及其影響程度的大小等因素。

2、在實質證據力層面，應由法院根據事實和法律，基於自由心證，在經驗法則及論理法則之輔助下，衡量電

[38] 本案經檢察官提起上訴後，臺灣高等法院以 91 年度上訴字第 3607 號刑事判決採取與一審法院相同之見解而駁回檢察官上訴。

子證據之證明力。

3、電子證據作為認定犯罪事實之依據，主要在於與犯罪行為相關事實部分，例如圖片內容是否達到猥褻之程度；電子郵件內容是否達到恐嚇、寄送流傳程度是否達到妨害名譽等，至於其他事實，如行為人身份之確認、郵件內容有無遭偽造及變造，均應由其他證據補強之。[39]

[39] 謝明冠，同第二章註 20，頁 182。

第五章　刑事證據法則對於電子證據之適用

5.1　前言

隨著吾人日常生活日趨數位化，過往訴訟活動中傳統證據所扮演的各種角色，逐漸為各種類型的電子證據所取代。時至今日，各國法院皆不可能對電子證據視而不見或拒絕採納為裁判之依據。如果法院拒絕適用電子證據，反而會造成訴訟無法順利進行，甚至因此可能造成法院無法發現真實，而有審判結果不公之疑慮。因此，各種國際組織率先在公約或示範法中一再敦請各國採認電子證據，應等同於其他證據而賦予平等之地位。

不論英美法系或是大陸法系，各項證據法則的演進，均已有堅實的學理及實務基礎。而電子證據出現於訴訟活動中，即使在電腦發明的國家—美國，仍然在一九七０年代中期才開始出現，其他國家則視電腦化、數位化的程度而有所不同。

因此如何將電子證據採納於訴訟活動中，電子證據如何符合既有證據法則，或應該另行獨立建構專屬證據法則，一直都是各國學術界及實務界感到非常困難艱鉅的挑戰。尤其，法律專家對於電腦或數位資料的理解有限，甚至有許多誤解，跨領域之專業隔閡，更形成電子證據為法庭採納之門檻。

另一方面，我國為建構更為公平正義的訴訟制度，切合社會之實際需要，於民國九十二年二月六日，大幅度修正通過刑事訴訟法，此次修改與新訂條文共達一百三十三條，為刑事訴訟法自民國十七年公佈施行以來修改幅度最大的一次。此次修法，對於支配刑事訴訟最重要的證據法則，亦在此次修改中大幅增訂翻修，對刑事偵查及審判活動產生重大且深遠的影響[1]。此次就證據

[1] 蔡碧玉，同第一章註 1。

法則修改的重點包括：檢察官舉證責任之具體化、違法取證之證據排除、傳聞法則之建立、準備程序與審判期日明確區分、詰問法則之明定、明定共同被告之證人地位、鑑定留置及鑑定採樣程序、證據保全程序之建立、簡式審判程序之新訂及自訴強制律師代理制等均係有別於過往之重大修正。[2]

新修訂之刑事訴訟法雖稱由「職權主義」改向「改良式的當事人進行主義」[3]，惟實際上大部分的修正方向，多是朝美式刑事訴訟制度方向修改[4]。尤其在證據法則方面，是更朝向美國法制之方向加以制訂。雖然在修訂過程中引起許多學者專家以及司法實務界人士表示許多不同的意見[5]，惟終究還是完成立法[6]。因此，本

[2] 蔡碧玉，同第一章註 1。

[3] 刑事訴訟法第 31 條修正理由（一）。

[4] 論者往往有謂我國法制係繼受自德國，例如呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規爲例，頁 47，中正大學電訊傳播研究所碩士論文，89 年 6 月。惟究其起源，不得不追溯至日本明治維新時期，彼時日本國內爲究應採行法國法制抑或是德國法制，爭論不休。同一時間德國在 1896 年頒布新民法，並規定將於 1900 年 1 月 1 日，也就是二十世紀的第一天起開始實施。因爲其內容豐富，結構嚴謹，集羅馬法體系之大成，再創新猶，並採行「從一般到具體、從抽象到特殊」之方式建構法律體系，極富科學性、邏輯性，日本遂決定採用德國法律體系，並著手將該部德國民法翻譯、轉植到國內，從而更進一步繼受德國其他法律及體系。我國則是於清末圖強之際，有鑑於日本富強迅速，關鍵應在社會制度而非船艦槍礮，又考量兩國文化、文字的差距較小，在沈家本等法學先進之帶領下，將日本民法及相關法律體制加以採用。因此，考我國法制之繼受方向，應稱「直接」繼受自日本法制而「間接」繼受自德國法制，始爲正辨。然而，自第二次世界大戰末期起，我國受美國援助日深，影響亦日深。其後我國法制，於創設或修正時參考自美國者亦愈多，如動產擔保交易法、證券交易法、著作權法等是。因此對於不同法系間基礎思考邏輯與架構之不同，往往成爲學者及實務界深感扞格之處。其實在各國間趨同現象日益加速之今日，各國之間的法律移植與融合應爲常態，不應斷予排斥。惟在研修之際，應保持開放之心胸、做充分之討論，以求其完善，並能將修訂後之法律，以最順暢之步調推行運作，社會及司法成本亦降至最低，如此方爲司法之幸、人民之福。

[5] 例如吳巡龍，「兩造對抗制 檢方起訴均不能事先將卷宗證據送法院 而我們卻自相矛盾 司改修法 非驢非馬」，聯合報第 15 版，2001 年 12 月 23 日、「《刑事訴訟制度大變革》看看檢察官濫權、訴訟曠廢時日等缺失 當事人進行制 美國在檢討 台灣卻躁進」，聯合報第 15 版，2001 年 10 月 30 日。宋伯東，「刑訴交互詰問制 學者反對倉促修法立院週三討論修正草案 施慶堂指目 前『一國五制』有待『統一』」，聯合報第 12 版，2001 年 10 月 21 日。

[6] 現今法律的修改，本文認爲已經不必過於執著在繼受自大陸法系或英美法系一節上。當前世界經濟全球化、高科技的發展，特別是網路化的進步更促進各國交往的廣泛，各國之間的趨同現象也將有所增加，各國之間的法律移植與融合也出現前所未有的新形勢。這種技術、經

文於討論刑事證據法則時，專以民國九十二修正之刑事訴訟法參酌美國證據法制之立法例加以討論，進而檢討新制刑事證據法則對於電子證據之適用範圍。[7]

美國聯邦證據規則（Federal Rules of Evidence）之體例分為第一章「通則」、第二章「司法認知」、第三章「民事訴訟與程序之推定」、第四章「證據關聯性與其限制」、第五章「拒絕證言權」、第六章「證人」、第七章「意見及專家證言」、第八章「傳聞」、第九章「真正之證明與辨認」、第十章「文書、紀錄與照片之內容」及第十一章「其他規定」。

至於美國證據學的討論上，將證據法則主要區分為以下領域[8]討論：一、審判構成方式與準備；二、證據的關聯性、證明力；三、品行與傾向四、證人；五、非法證據的排除；六、傳聞法則；七、文書證據與最佳證據法則；八、外行意見與專家證人；九、證人拒絕證言權；十、展示性證據之處理；十一、司法認知、證明與推定等範圍。

本文對電子證據的法律性質，係採取本文修正後之新文書證據說，基此，在適用證據法則方面，本文認為電子證據在違法證據排除法則、傳聞法則、書證之驗真法則與最佳證據法則應加以一一討論。

濟一體化進程的加快，便利交通所造成的時間、空間距離的收縮或「時空收斂」（time-space convergence），促使人類活動越來越趨向於一種機械式的標準化運動，這在客觀上強化了法律制度的整合與趨同性，也使西方的法治傳播呈現出某種慣性。職故，大陸法系已有逐漸個案化，甚至是先由法院對某一類問題展出看法之後，再將之成文化的趨勢，並且許多法律的體系與概念，也漸漸傾向於普通法體系；相對的，普通法體系亦將相當多案例法上所發展出來的概念的，將之成文化、法典化，使法院於裁判時，有一定的標準，關於此部分的發展趨勢，請參見 Guido Calabresi, A Common Law for the Age of Statutes, Harvard Univ. Perss,1982 一書。惟在立法技術上，倘若透過現行法律的解釋或相同體系立法例的參考修正而能完足現代社會之需要，則應以此爲優先考量，俾將社會及司法成本降之最低。又，即便參考其他法系制度較不相同之立法例，亦應廣納雅言、多方徵詢意見，始能求其周延。

[7] 刑事訴訟法於民國 92 年修正後，93 年、95 年與 96 年之修正，對證據法則均未再有所更動。

[8] 此處對於美國證據法學之區分係參考 Allen、Kuhns & Swift, EVIDENCE－Text, Problems And Cases, 3rd Ed.，Aspen Pub-lishing Inc.,2002；及 John W. Strong, McCORMICK ON EVIDENCE, 5th Ed.,WEST Publishing Co.,1999。

表 5-1　電子證據適用之證據法則

有＊號之證據法則應討論電子證據之適用

關聯性法則[9]
違法證據排除法則（＊）
傳聞法則（＊）
文書認證（驗真法則、最佳證據法則）（＊）
證人作證資格
證人免除證言權
專家證人與科學證據
司法認知
證明與推定

資料來源：本文整理

5.2　違法證據排除法則對於電子證據之適用

5.2.1　違法證據排除法則之意義

我國早期對於違法證據之排除，並無特別強調。因為某項證據如果屬於違法取得，縱然納入訴訟程序中，法官仍會摒棄納入認定事實或形成心證之證據項目中。反之，在採取陪審團訴訟制度之國家，因為對於事實之認定，係由不具法律專業之陪審團為之，為避免陪審團成員被誤導、受污染，

[9] 美國證據法則中關聯性法則（Relevance）雖於電子證據有適用之餘地，但是該法則係指訴訟中所提出之證據係用以證明證據與待證事實間具有無聯繫因素，討論關聯性原則不是在討論證據本身的內涵意義，而是以之看待證據與待證事實間的一種聯繫關係。關聯性法則也是訴訟經濟的篩選器（Filter），沒有關聯性法則對證據加以篩選過濾，則必然引起訴訟過程中湧進難以數計、良莠不齊的證據，讓訴訟無法順利進行，因此關聯性是現代證據法律制度的基本原則，且關聯性法則的基礎是建立在邏輯（logic）與一般經驗（general experience）之上，旨在避免無謂之證據資料進入訴訟活動中延滯訴訟之進行，此方面不論為受請求調查之客體是否為電子證據均會受到關聯性法則之規範，關聯性法則在電子證據之領域並無例外或需要調整之情形，因此在此不予討論，合先敘明。

因此特別強調依法行政（Due Process of Law）、程序正義等觀念。

5.2.2 美國

非法證據排除法則有狹義和廣義之分。狹義的非法證據排除法則係指法院在審判時不得採納違反聯邦憲法第四條修正案[10]禁止違法搜索、扣押之保護性規定獲得的證據，稱為「Exclusionary Rule」。廣義的非法證據排除法則還包括依據聯邦憲法第五修正案而來之正當程序排除法則、自證有罪排除原則（5th Amendment Exclusionary Rule – Due Process Exclusionary Rule、Self-incrimination Exclusionary Rule）及依據第六條修正案而來之未經辯護證據排除法則（6th Amendment Exclusionary Rule）等等。此處所討論者為狹義說，亦即討論不當搜索、扣押所取得之電子證據。

5.2.2.1 違法證據排除法則對於電子證據適用之爭議

電子證據在形態上的無形性以及取證方式上的特殊性、技術性，使得法院在適用違法證據排除法則時，必須對傳統定義下之違法證據排除法則加以重新檢視與形塑。

例如本來違法證據排除法則是適用在傳統物品之違法搜索與扣押行為與執行人員物理性的入侵行為。但是如果進行電子監聽所取得的證據，應否排除之？另外，在網際網路傳輸之數據，是採用廣播（Broadcast）技術，則在

[10] 美國聯邦憲法第四修正案（Amendment IV: Warrants and searches.）規定：「人民的人身、住宅、文件和財產不受無理搜查和扣押的權利，不得侵犯。除依據可能成立的理由，以宣誓或代誓宣言保證，並詳細說明搜查地點和扣押的人或物，不得發出搜查和扣押狀。（The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.）」

網際網路上所截留之證據，是否可以用於法庭之中？是否對隱私有所侵害，或應認為被告對在網路上傳輸之資訊有被侵害之預見？凡此均為對於相關之爭議。

5.5.2.2 違法證據排除法則對於電子證據適用之調整

美國對於電子證據取得之規範，就搜索、扣押電腦之行為，主要是從聯邦憲法第四修正案、聯邦刑事訴訟法則及電子交易隱私法案（ECPA）建構而來；電子資訊攔截與竊聽由綜合治理犯罪與街道安全法以及愛國者法案來規範。

電子證據在形態上的無形性以及取證方式上的特殊性，使得美國傳統定義下之違法證據排除法則受到很大的衝擊。[11]

1、在搜索、扣押方面

傳統蒐證規範僅在限制物理意義上有形物之違法搜索與扣押行為，以及執法人員因此種搜索扣押所產生的物理性侵入行為。然而電子證據之搜索、扣押，往往不會有物理性質的侵入行為，或因為電子證據是磁性紀錄，所以不算是取得有體物，不受前開憲法修正案或相關法律之規範。

對此，實務上各級法院以判決刑事對於電子證據之搜索、扣押，作出詮釋及規範，茲分述如下：

（1）無令狀搜索、扣押

A、原則

基於美國聯邦第四修正案之規定，無令狀搜索限於：

[11] 劉品新主編，同第二章註 20，頁 236。

（A）搜索行為沒有違背被告「對隱私的合理期待（Reasonable Expectation of Privacy）」；

（B）該項搜索雖違背被告對隱私的合理期待，但符合法律所允許之情況。

始得為之。茲分述如下：

（A）搜索行為沒有違背被告對隱私的合理期待

電磁紀錄並非物理上有實體、具象之物品，且可以輕易複製、傳輸，製造或儲存電磁紀錄之工具即電腦設備又往往容易為多人共用，因此是否應認為電磁紀錄仍有「對隱私之合理期待」所保護？

美國聯邦最高法院在 United States v. Ross[12]、 United States v. Barth[13]等案件中，認為可以把電腦裏儲存的數據比擬為放置在一個關閉容器（a closed container）裏的物品，對被告控制下的個人電腦進行搜索好比打開一個關閉的容器。因此，被告對其個人電腦中儲存的資料之管控，就好比對其控制下的一個關閉容器裏的物品一樣，都具有合理的隱私期待。在此種情況下進行搜索，與打開被告掌控的關閉容器需要的搜索條件一致。[14]

[12] 456 U.S. 798,822-823（1982）

[13] 26 F. Supp 2d 929,936-937（W.D. Tex. 1998）

[14] 張斌，同前註 7，頁 213。

不過，被告對其個人電腦裏的數據具有的合理隱私期待，在一些情況下不受聯邦憲法第四修正案之保護。主要情況有以下三種：[15]

a、被告自行開啟電腦

在 United States v. David[16] 一案中，執法人員站在電腦後面，透過螢幕看到被告在其筆記型電腦中輸入通行密碼。法院認為執法人員在此情形下所獲得之密碼並不違反第四修正案，因為在這種情況下，即使在自己家裏或者辦公室，對自己意圖暴露給公眾的資訊即顯示在螢幕上的內容，不具有隱私的合理期待，不受第四修正案之保護。

b、被告自己將電腦交給他人[17]

被告自己將所持有之電腦交給第三人的行為，視為自願放棄其對隱私之合理期待。

例如在 United States v. Poulsen[18] 案件中，被告 Poulsen 是一名駭客，他將一個載有其侵入他人電腦系統之磁碟片丟在其所有的一個公共場所寄物櫃中，並且很大意地將此寄物櫃出租他人，執法

[15] 張斌，同前註，頁 214-215。

[16] 756 F. Supp. 1385（D. Nev. 1991）

[17] 張斌，同前註 14，頁 214。

[18] 41 F. 3d 133（9th Cir. 1994）

人員對此寄物櫃進行無證搜索時發現此張磁碟片，以此作為起訴 Poulsen 之證據。雖經被告抗辯，惟法院認為搜查沒有違背 Poulsen 的隱私期待，因為 Poulsen 自己的疏忽行為已經表明他對該磁片不再具有憲法權利。

c、私人搜索

在 United States v. Hall[19] 一案中，被告將電腦送修，維修人員發現電腦裏有許多兒童色情圖片，便將此情況告之警方。上訴法院否決了被告要求排除專業人員私人無證搜索所獲證據違反聯邦憲法第四修正案的申請，因為電腦維修人員的私人搜索是基於其自身行為性質的要求，對電腦的搜索行為以及隨後對有罪證據所做的紀錄，並沒有違反第四修正案。

在 United States v. Kennedy[20]一案中，聯邦法院再次重申了私人搜索合法性原則，認為 ISP 的匿名管理者對被告存放在網際網路上的資訊進行搜索，政府公權力沒有介入，因而不受聯邦憲法第四修正案的保護。

[19] 142 F 3d 988（7th Cir. 1998）

[20] 81 F. Supp. 2d 1103,1112（D. Kan. 2000）

為避免政府執法人員藉助私人搜索法則而規避違法證據排除法則，濫用搜索權力，聯邦法院在 United States v. Runyan[21]一案中指出，政府部門執法人員運用私人搜索法則是否合法，取決於政府部門執法人員對特定電腦文件搜索範圍是否超過私人無證搜索的範圍。如果超過了私人搜索範圍，則必須申請搜索票，否則即是違法搜索。

（B）法律規定之例外情形況[22]

a、同意搜索（consent search）[23]

被告出於自願同意，則不論出於明示或暗示，都能使執法人員實施無令狀搜索。

b、緊急搜索（Exigent Circumstance）

證據之保全遇有迫切危險，例如當電腦證據面臨被刪除或消磁之危險時，執行搜索之人員可以進行緊急搜索，惟何種情形構成緊急搜索，應由法院依個案認定之。[24]

[21] 275 F. 3d 449,464-465（5th Cir. 2001）

[22] 張斌，同前註 14，頁 217-219。

[23] 張斌，同前註 14，頁 216。

[24] 張斌，同前註 14，頁 218。

c、一覽無遺（Plain view）

聯邦法院在某些案件中認為在電腦搜索案件中，一覽無遺條款沒有授權執法人員擅自打開他們沒有得到允許的電腦文件。

對於一覽無遺法則，法院於此處有不同見解

（a）肯定說

電腦是一個整體，執法人員有權對電腦某一部分的搜索，則可以通過一覽無遺條款的適用，對整台電腦甚至其附屬設備，如磁碟、光碟進行搜索。[25]

（b）否定說

電腦系統不能看做一個整體，不同的部分具有不同的隱私期待權利，對電腦某一部分的搜索，不能通過一覽無遺條款來對整個系統進行搜索。[26]

d、逮捕附帶搜索（Search Incident to a Lawful Arrest）

警員在逮捕嫌犯時，可對其

[25] *See* United States v. Runyan、United States v. Slanina（283 F. 3d 670 680（5th Cir. 2002））

[26] *See* United States v. Carey（172 F. 3d 1268,1273-1275（10th Cir. 1999））、United States v. Walser（275 F. 3d 981,986（10th Cir. 2001））

人身及其周圍有限的環境進行無證搜索。則嫌疑人在被拘捕時，身上也許有電子設備或儲存載體，則逮捕嫌疑人時可以附帶搜索之。[27]

e、國境搜索（Border Searches）

邊境搜索是美國聯邦最高法院特許的、對發生在邊境上的案件進行無證搜索，其目的是為了打擊走私和其他財產型態之犯罪。

只要在邊境上或者與邊境功能類似的地點，進行例行搜索（routine searches），並不需要事實理由或者合理懷疑，均可以無證進行。

例如在 United States v. Roberts[28]案中，執法人員得知被告某日將攜帶大量兒童色情電腦圖片，從德州飛往法國巴黎。執法人員在德州休斯頓機場專門設置一檢查區，被告到達後，執法人員以正在檢查不能違法運出境外的現金及高科技產品及數據，後來在被告物品中發現一台筆記型電腦和六張 ZIP 磁碟片，被告簽署書面同意搜索，結果執法人員發現了數千張兒童色情圖片。一審時被告要求排除兒童色情圖

[27] 張斌，同前註 14，頁 218。

[28] 86 F. Supp. 2d 678（S.D. Tex. 2000）

片證據，法院否決，認為對被告行李之搜索屬於例行搜索，不需要搜索票及合理懷疑。上訴法院維持一審法院之見解。[29]

（2）有令狀搜索、扣押[30]

執法人員向法院聲請搜索票，均需依照聯邦憲法第四修正案為宣誓或者簽署代誓言，保證書確立搜索依賴的可信理由（Probable cause），同時法院在搜索票上應詳細載明被扣押的物品。

但「詳細載明」之要求對於電腦搜索而言非常困難，因為電腦文件不像一般搜索中的有形物品，它是以電磁紀錄之形式存在，可以儲存在極小的一個儲存載體之上，且在極短時間內透過網際網路向全球傳播。執法人員在執行搜索以前，無法知道其所需要的電腦文件表現為什麼樣的形式，藏在電腦或者網路上。[31]因此，法院在

[29] 惟亦有法院認爲執行邊境無令狀搜索，倘若是在沒有合理懷疑之情況下爲之，逾越海關條例的立法目的以及憲法第 4 修正案的合理性標準。美國洛杉磯海關在 2004 年 7 月間，要求一位自菲律賓返國旅客打開筆記型電腦，並在其中發現許多兒童色情照片。2006 年 10 月間，洛杉磯聯邦法院法官普利格森基於「搜索電腦或電子儲存設備中的內容，比搜索隨身餐盒或其他具體物件更具侵略性；此種在沒有合理懷一下進行的搜索，逾越海關條例的立法目的以及憲法第 4 修正案的合理性標準。」、「電子儲存裝置的功能即是人類記憶的延伸。這些儲存設備可以儲存我們的思想，不論這些思想多麼不值一提或多麼深奧…因此，政府侵入人民的思想與侵犯人民的身體一樣，都不爲憲法第 4 修正案所容」，因而排除該筆記型電腦內容之證據能力。惟美國國土安全部業已對該判決提出上訴。參見林少予，「全民公敵 美國反恐反到誰？」，聯合報第 A13 版，95 年 12 月 4 日。

[30] 張斌，同前註 14，頁 222-224。

[31] 例如現在 Google 所提供之電子郵件 GMail 容量高達 2GB，雅虎（Yahoo！）宣稱其所提供之電子郵件容量沒有上限。就筆者最近之執法經驗發現，被告十分容易將電腦犯罪事證藏放在此種電子郵件信箱中，只要被告不怕麻煩，不讓電腦自動紀錄電子信箱之帳號密碼，則執法人員要查獲電子信箱之內容物相當困難。

United States v. Reyes[32]一案中，進一步認為，在當今技術與經濟高度發展的時代，特定紀錄可能以任何形式出現，因而不可能期待搜索票能夠精確地描述所需紀錄的存在方式，這是對於電子證據令狀聲請所採取比較寬容之態度。[33]

2、電子監聽

美國傳統觀念上違法證據排除法則僅適用於物理意義上的違法搜查與扣押行為，以及執法人員因此而生之侵入行為，因此對於不具物理性質之監聽行為，並無相關之規範。一直到一九六七年，Kates v. United States[34]一案，聯邦最高法院才調整了既有的違法證據排除法則的適用範圍。

Kates v. United States 案中警方在被告經常使用傳遞簽賭訊息之公共電話亭安裝竊聽器，聯邦最高法院認為聯邦憲法第四修正案所要保護的客體是「人」，而非「地方」，公用電話亭雖非被告之住所，但使用時談話人主觀上對其隱私會有合理之期待，客觀上社會亦會認為該期待屬於合理範圍，因此監聽前應取得法院之許可，否則屬於違法取證，監聽所取得之證據不具有證據能力，應予排除。[35]自此，違法證據排除法則自此也適用到無形的電子證據上。

---

[32] 798 F. 2d 380,383（10th Cir. 1986）

[33] 相對於電子證據有令狀搜索採取比較寬容之態度，無令狀搜索則採取比較嚴格之態度，例如在 United States v. Carey 一案中，法院認爲被告同意搜索之書面，僅載明「同意扣押被告人控制任何財產」或「同意在被告住處徹底搜查場所和財產」，搜索被告之財產並不必然包括同意搜索電腦，且即便能夠搜索被告住所內之電腦，亦不能及於被告所有而放在他處的電腦。在 United States v. Turner 案中，執法人員得到被害人鄰居簽署同意搜索住處與私人物品之書面同意，在搜索該鄰居電腦時，發現裏面有許多兒童色情圖片，檢察官以擁有兒童色情圖片罪起訴鄰居。聯邦法院認爲，對電腦的搜索已超越了同意的範圍，爲此搜查所獲的兒童色情圖片不具有可採性。

[34] 389 U.S. 347（1967）

[35] 吳巡龍，「得通訊一方同意竊聽錄音之證據能力」，收於氏著刑事訴訟與證據法實務，頁 199-200，新學林出版股份有限公司，2006 年 11 月。

至於對網際網路發展之後各項電子證據蒐證合法性之討論也層出不窮，例如電子郵件、網頁內容、電子文件等。在 United States v. Golonel James A. Maxwell,Jr.[36]一案中，法院認為電子信箱與傳統郵箱可堪類比，將對電子信箱之搜查納入搜索扣押的法律體系中。

考察美國有關電腦證據違法排除的規定，可得出以下結論：

1、電子證據違法排除之目的在於限制政府執法人員搜索權力之濫用，保護人民對電磁紀錄隱私合理期待之權利。侵犯此項人民憲法上權利所獲得之電子數據，不具有證據能力，應予排除。[37]

2、電子證據與其他實體證據同受聯邦憲法第四修正案的平等保護。法院對於電子證據以功能等同物品之概念，即把電子證據類比傳統物件，再以相關法律加以保護。[38]

3、對於人民有隱私合理期待之電子證據，在同意、緊急情況、逮捕時、國境管制等情況下，可以執行無令狀搜索。

4、有令狀搜索電腦應區分實物與電磁紀錄，並詳細載明搜索範圍，若搜索票上載明的範圍名不符實、過寬或過窄，都有可能使所獲得之電子證據被認定為違法取得沒有證據能力。

[36] 42 M.J. 568（1995）

[37] 張斌，同前註 14，頁 225。

[38] 張斌，同前註 14，頁 225。

5.2.3 我國

5.2.3.1 違法證據排除法則對於電子證據適用之爭議

我國對於違法證據排除之規定，並非如美國一般建立在憲法層級與具體案例上，而係在民國九十二年修法後列於刑事訴訟法及相關法規中。

我國與美國，乃至於世界各國所面臨對違法電子證據排除之挑戰，均應相同。原因在於：

1、電磁紀錄是技術性、規格性之無體物，全世界對於電磁紀錄之製作標準均相同，亦即為二進位制磁氣矩陣排列。尤其電磁紀錄或電腦設備及各種計量單位均為全球規格化，各國使用之設備與電磁紀錄均相同，所面臨之問題雖然隨著資訊化程度不同而有先後之別，但是最後均為相同。

2、網際網路無遠弗屆，各國網路間溝通之通訊協定採用相同規格，而不論原因起於商業或犯罪，發生爭端需要透過司法體系解決時，所提交之電子證據均為相同規格，因此針對電子證據所產生之爭執或討論亦趨於一致。

5.2.3.2 違法證據排除法則對於電子證據適用之調整

1、非法取供

違反刑事訴訟法第一百五十六條第一項規定，以違法、違背自由意志及其他不正方法取得被告之自白，再因此而取得之電子證據，因認為違反法定程序而不得作為證據。

例如前揭註三十一之情形，倘若執法人員以不正

方法對被告刑求，訊問出被告在 GMail 電子信箱之帳號及密碼，進入該信箱所取得之電子證據，應認為不具有證據能力，必須排除之。

惟如係非法取得被告以外之人之非任意性供述時，再進而取得之電子證據，其證據能力如何？

按我國刑訴法第一百五十六條第一項業已明文規定因非法取供而無證據能力者，僅限於被告之自白，故於被告以外之人，其非任意性之供述而取得不利於被告之電子證據，即不能適用第一百五十六條第一項之絕對排除規定，僅得依第一百五十八條之四規定判斷其有無證據能力。[39]

2、違反法定障礙事由期間或夜間訊問禁止規定取得之被告或犯罪嫌疑人之自白或其他不利陳述

違反刑事訴訟法第一百五十八條第一項前段規定，取得被告自白或其他不利陳述，並進而取得之電子證據，依本條之規定亦應予以排除其證據能力。至於對於但書所規定之情形，必須由提出該項電子證據之檢察官負舉證責任，就其違背之非出於惡意，依個案情節主張之。

3、檢察事務官或司法警察（官）詢問受逮捕拘提之被告或犯罪嫌疑人時，違反第九十五條第二款、第三款之告知義務

違反刑事訴訟法第一百五十八條之二第二項規定，於逮捕被告或犯罪嫌疑人時違反告知義務未告知被告或犯罪嫌疑人權利，因此而取得相關之電子證據，亦應予以排除之。

[39] 蔡碧玉，同第一章註 1，(三) 文，第 2-3 版。

4、刑事訴訟法第一百五十九條第一項規定，傳聞證據不得作為證據

就電子證據與傳聞法則間所生之相關問題，如下節所述。

5、刑事訴訟法第一百五十八條之三規定，證人或鑑定人應具結而未具結者，其證言或鑑定意見不得作為證據

證人或鑑定人對於電子證據若有未經具結之情形則其證言或鑑定意見不得予以採納，應予排除之。

6、刑事訴訟法第一百六十條規定，證人之意見證據不得作為證據

證人對電子證據之各人意見無證據能力，法院應予排除之。

7、違反甫經修正後總統公布，將於民國九十六年十二月十一日施行之通訊保障及監察法第七條第一項及第二項之規定，並因而取得之電子證據，應予排除不得採為證據。

8、違法搜索、扣押所取得之電子證據

違反刑事訴訟法第一百五十八條之四之規定，違法搜索、扣押所取得之電子證據或電磁紀錄，除有法律明文排除之情形外，允許法官審酌人權保障及公共利益之均衡維護，對該項電子證據之證據能力取捨有裁量權。另外刑事訴訟法第四百十六條第二項之規定，亦同此意旨。

9、違反甫經修正後總統公布，將於民國九十六年十二月十一日施行之通訊保障及監察法第五條及第六條之規定，利用違法通訊監察所衍生取得之電子證據，其證據能力之有無，概由法院視情節重大與否決定是否採納之。

10、私人違法取證之法律效果

至若我國法制上對於私人違法取得之電子證據，是否適用證據排除法則？

刑事訴訟法第一百五十八條之四之規定，係僅限於「實施刑事訴訟程序之公務員因違背法定程序取得之證據」始有其適用；另同法第一百五十六條之違法取供、第一百五十八條之二之違反法定障礙事由及夜間禁止訊問規定及違反第九十五條告知義務之規定，亦專指檢察事務官及司法警察等執法人員，均未包含私人之違法取證在內。按文義解釋，私人違法取得之證據，自不能適用上開證據排除法則而認定其無證據能力。[40]

此觀點與美國法院之意見，認為對違法證據之排除旨在限制具有公權力之政府人員或私人以違法方式取得證據之意旨相一致。

5.3　傳聞法則對於電子證據之適用

5.3.1　傳聞法則之意義

傳聞法則本是英美法系陪審團訴訟制度下特有之證據法則，主要目的在用以之證明證人在法庭外所為之口頭、書面或肢體語言等陳述均不具有可採性，亦即不具有證據能力，不得提交法庭作為陪審團認定事實之依據。然而此一甚具理想性質之證據法則，受限於訴訟活動中千變萬化之情形，在美國判例法上做出許多例外允許採納傳聞證據之案例，隨後這些案例逐漸整理而成文化，因此現行美國聯邦證據法則有多達二十三款之例外規定以及概括採納條款。

[40] 蔡碧玉，同第一章註 1，(三) 文，第 4 版。

5.3.2 美國

5.3.2.1 傳聞法則對於電子證據適用之爭議

隨著電磁紀錄的發展和應用範圍不斷擴大，各類型電磁紀錄被當成證據而提交至法院的情形也日益普遍。若每份電子證據均需有之情或製作之人到法庭結證亦將會嚴重影響這從事這些業務之人的日常工作，也會大大言滯法院訴訟的順暢程度。例如信用卡的刷卡紀錄、銀行存款或支票帳戶明細、ATM 提款機紀錄等，均屬於傳統定義下之傳聞證據。若不將之以例外規定予以排除，則社會不僅無法享受因為電子化、數位化帶來的便利，反而將會因龐大的電磁紀錄被當成傳聞證據而使整個社會蒙受無以名狀之訴訟災難。

因此電子證據必須檢討是否能以各種傳聞法則之例外加以採納，倘若可以，則電子證據即具有可採性。但是傳聞法則之定義，在於只有當出證之一方所提供之證據，且該項證據是要用以證明其所主張事實之真實性時，此項證據才屬於傳聞法則的範疇，於電子證據之適用，只有當電子證據用於證明其紀錄資訊所反映事件的真實性時，始為傳聞證據。[41]

5.3.2.2 傳聞法則對於電子證據適用之調整

美國司法實務上將電子證據分為三種，即電腦生成紀錄（Computer-generated Records）、電腦存儲紀錄（Computer-stored Records）以及前開二種之混和形式（both Cpmputer-generated and Computer-stored Records）。

[41] United States v. Cestnik, 36 F.3d 904, 909-10（10th Cir. 1994）

電腦生成紀錄由於完全是電腦自行運作後制作出來的，因此無庸以傳聞法則加以檢驗，只需要進行驗真程序即可。至於後二者，由於包含人類的陳述，必須接受傳聞法則的檢驗，並對其進行驗真程序後，才能用於證明事實。[42]

對於電腦生成紀錄，美國大部分的法院允許電腦紀（computer records）得以引用聯邦證據法則第八０三（6）條「商業紀錄」為傳聞證據例外採納之法源依據[43]，例如 United States v. Salgado、United States v. Cestnik、United States v. Goodchild、United States v. Moore、United States v. Briscoe 及 United States v. Catabran[44]等案例均採此見解。在這些案件中法院認為，倘若此類電腦紀錄係依照日常例行性之程序所留存之紀錄，則可以被承認為商業紀錄。[45]另外也有法院認為雖然電子證據得以例外的被採納，但法源依據不應是前揭第八０三（6）條「商業紀錄」，而應為第八０三（8）條「公務紀錄與報告」[46]，此外亦有法院引用第八０三（9）條「生命統計紀錄」或第八０七條「其他概括規定」者。總此，可知美國實務及學說上均能接受第一類電腦生成紀錄不受傳聞法則之規範，屬於傳聞之例外，只是適用條文時會視該項電子證據之性質而適用不同之規定。

有一些法院在適用聯邦證據法則第八０三（6）條時，加以引伸，訂定一些標準，如 United States v.

---

[42] *See,* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, pp.142-143.

[43] *See,* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, p.142。採此種分類最重要的案例是 People v. Holowko。

[44] United States v. Salgado, 250 F.3d 438, 452（6th Cir. 2001）、United States v. Cestnik, 36 F.3d 904, 909-10（10th Cir. 1994）、United States v. Goodchild, 25 F.3d 55, 61-62（1st Cir. 1994）、United States v. Moore, 923 F.2d 910, 914（1st Cir. 1991）、United States v. Briscoe, 896 F.2d 1476, 1494（7th Cir. 1990）及 United States v. Catabran, 836 F.2d 453, 457（9th Cir. 1988）

[45] *See,* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, p.142.；*Supra* note 24.

[46] *See* ,e.g. Hughes v. United States,953 F. 2d 531 ,540（9th Cir. 1992）

Sanders[47]一案中，法官對於電腦業務紀錄是否可以被採納提出了三項評判標準：

1、關於產生源頭：即必須產生於正常的業務行為，不屬於傳聞的簡單堆砌。

2、關於產生過程：必須產生於正常的業務進行過程中，製作的目的可以確保其具有準確性。

3、關於保管與紀錄：必須是出於正常業務活動而對結果按照慣常程式所進行的紀錄，其製作程式必須保證資訊內容的真實性。

其後，在 United States v. Cestnik[48]一案中，法官認為：如果電腦業務紀錄符合以下三項條件，即

1、它們是按照確保準確性的慣常程式進行保管的，

2、製作它們的目的中本身帶有確保準確的因素（如非為訴訟目的而製作），以及

3、它們不屬於傳聞的簡單堆砌，則具有可採性。

則可以加以接受。

在 United States v. Briscoe[49]一案中，法院認為：「如果電腦紀錄的保管者或其他適格證人能夠證實，該紀錄是在業務活動中按照慣例保管的，並且在這種業務活動中存在著製作紀錄的一般慣例，則該紀錄具有可採性」。

在正常業務活動中保管的紀錄，指的是電子數位形式的數據，而非該數據的列印輸出物，因為實際列

[47] 749, F 2d. 195, 198（5th Cir. 1984）

[48] 同前註 41。

[49] 896 F.2d 1476, 1494 （7th Cir., 1990）

印輸出物不可能符合「業務紀錄」的範疇，不能以之作為傳聞證據的例外。[50]但為了電子證據的方便為人類所理解，而將之以列印或顯示之方式呈現電腦紀錄。此種列印或顯示之狀態只是電腦紀錄的外在表現形式，藉此增強證據資訊的易讀性及易理解性，實質上之電子證據仍應指數位形式之電腦紀錄，而非其列印或顯示，只要系爭之電磁紀錄符合「正常的業務活動中形成」或者其他要件，則可以接納此種列印或顯示形式之證據能力。[51]

從美國學者及法院意見，可以瞭解：

1、在確定某一電子證據是否適用傳聞法則加以排除，或視為例外予以採納，應審酌其是否完全由機器生成，或有人為陳述在內。

例如 People v. Huehn[52]一案，檢察官主張即便銀行自動提款機（ATM）的數據及其機器狀態紀錄均屬於自動生成數據，是由銀行自動提款機自動生成的，但實際上也需要相關人員的監管、保管，所以法院最終將其作為傳聞證據，再依照業務紀錄例外之規定加以而加以採納。

2、電子證據適用傳聞法則的主要方式是作為業務紀錄，依聯邦證據法則第八０三（6）條，以傳聞例外處理，但亦有適用其他傳聞例外者，[53]例如

（1）Hughes v. United States[54]案件中，法院認為國稅局製作之電子稅單符合聯邦證據法則第八０三（8）條有關公共機關或代理機構以任

[50] *See,* United States v. Sanders；*Supra* note 3；劉品新主編，同第二章註 20，頁 119

[51] 劉品新主編，同第二章註 20，頁 120。

[52] 53,P.3d 733,（Colo.App. 2002）

[53] 劉品新主編，同第二章註 20，頁 174。

[54] 951, F.2d 531（9th Cir. 1992）

何形式製作的、闡述下述內容的紀錄、報告、陳述或者數據匯編之規定，因此可以作為傳聞證據之例外而被可以被採納。

（2）在 United States v. Blackburn[55]一案中，聯邦調查局探員在銀行搶犯遺留在被丟棄汽車上的眼鏡，旋即請驗光人員使用自動鏡片測試儀對這副眼鏡欲矯正之項目及度數等進行檢測；一審法院對檢測數據適用聯邦證據法則第八０三（6）條而認為該電子紀錄為業務紀錄，得以排除傳聞證據之限制而有證據能力，並據此將被告定罪；被告上訴主張提出該紀錄是聯邦調查局的調查活動和針對蒐集被告犯罪事證所得，不屬於業務紀錄。二審法院支持此見解，惟認為檢驗眼鏡之數據屬於聯邦證據法則第八０三（24）條之概括例外規定，仍以之判決被告有罪。

3、電子證據的傳聞法則有許多特殊限制[56]

例如 United States v. Sanders[57]一案中，法官對於電腦業務紀錄是否可以被採納提出了三項評判標準；United States v. Cestnik[58]一案中，法官也提出三項條件。而前述 People v. Huehn 一案，法院認為若要適用聯邦證據法則第八０三（6）條「業務紀錄之例外」而採納電子證據，須符合五要件：

（1）該紀錄是在正常的業務過程中產生；

[55] 992, F.2d 666（7th Cir. 1993）

[56] 劉品新主編，同第二章註 20，頁 175。

[57] 749, F 2d. 195, 198（5th Cir. 1984）

[58] 同前註 41。

（2）參與該紀錄產生過程的人都在依業務的慣常流程行事；

（3）輸入程式無誤；

（4）輸入程式在業務活動發生的合理時間內完成；

（5）資訊由對紀錄事項知情的可靠人員傳輸。

足見電子證據在傳聞法則之適用上有許多限制。

5.3.3　我國

我國對於傳聞法則之瞭解，歷史並非久遠，除對此問題有專門研究之學者外，大多數法律學者及實務界多半停留在學校教學時之粗淺概念上。民國九十二年修正刑事訴訟法前，始引起討論與關注，因此對傳聞法則之研究尚難稱深入廣泛，案件之累積不多，更遑論對於電子證據適用傳聞法則之討論。

5.3.3.1　傳聞法則對於電子證據適用之爭議

傳聞法則對於電子證據之適用時機為，只有當電子證據用於證明其紀錄資訊所反映事件的真實性時，始為傳聞證據。電子證據是否應認為屬於傳聞證據之例外而應加以排除？法源依據何在？此二議題應屬於我國刑事訴訟法所應討論之課題。

5.3.3.2　傳聞法則對於電子證據適用之調整

我國法制中不論是學界或實務界，對於傳聞法則、電子證據等概念累積之研究與案例均非成熟，因此並未有如美國傳聞法則中將電子證據予以分類成電腦生成紀

錄（Computer-generated Records）、電腦存儲紀錄（Computer-stored Records）以及前開二種之混和形式（both Cpmputer-generated and Computer-stored Records）等三種，並賦予不同證據法則上之效果。

我國司法實務上對於電磁紀錄是否適用於傳聞法則，有無證據能力，有不同之見解：

1、肯定說—電腦紀錄不屬傳聞證據，具有證據能力

（1）「本件檢察官所提出雅虎公司所提供ＩＰ稽核資料、使用者會員資料、中華電信數據通信分公司ＩＰ通聯紀錄資料均係電腦數位資料檔案之再現，其性質屬電腦自動紀錄，不含人之供述要素，非屬供述性證據，無庸受刑事訴訟法第一五九條第一項所定傳聞證據排除法則之規範。又核上開文書係分別由雅虎公司、中華電信數據通信分公司所提供，具備形式與實質之真實性，得為證據使用。」[59]

（2）「雅虎奇摩公司電子郵件列印資料（同上偵查卷第一四七頁）：此份列印資料，乃電信警察隊第一中隊回覆台北地檢署之附件資料，為被告以外之人在審判外之書面陳述，依刑事訴訟法第一百五十九條第一項之規定，原則上不具證據能力；惟被告及選任辯護人對於此附件資料，資料上所顯示網址為：http://home.kimo.com.tw/long_lived2002/chinese/index.htm 之虛擬網頁空間之ＩＰ登錄時間為二００三年九月及十月間，表示此乃於檢察官偵訊後，胡○○才上網將網頁

[59] 臺灣板橋地方法院 93 年易字第 638 號刑事判決。

移除，但對於檢察官將其作為證據使用並不爭執，僅爭執不能以此證明網頁由誰所製作等證明力之問題（當日審判筆錄參照），而上開附件資料內容為「上述網址會員登錄帳號、登入時間及登錄ＩＰ」，與檢察官主張之事實有關聯性，且上開資料之製作過程，亦無任何不適當之情形，依刑事訴訟法第一五九條之五規定而有證據能力，至於得否由上開資料證明出檢察官所主張之事實則為該份文書證據之證明力問題，應先敘明。」[60]。

（3）「查偵查卷第四０頁至第四六頁之數位聯合電信股份有限公司、中華電信股份有限公司數據通信分公司分別為覆臺北市調查處九十年六月十二日（九十）肆字第九０四二五四二、九０四二五四一號函及九十年七月十一日（九十）肆字第九０四三０三四號函（該三份函附於本院審理卷可查）詢事項所傳真回覆之電信使用者資料查詢回覆單，乃係從事業務之人於業務上製作之紀錄文書，而被告並未釋明數位聯合電信股份有限公司、中華電信股份有限公司數據通信分公司就該函覆之文書資料有何顯不可信之情況存在，則上開文書依前揭條文所規定，均有證據能力。」[61]。

（4）「惟刑事訴訟法第一五九條之四第二款及第三款規定『除顯有不可信之情況外，從事業務之人於業務上或通常業務過程所須製作之紀錄文書、證明文書；除前二款之情形外，其他於可信之特別情況下所製作之文書，亦得

[60] 臺灣臺北地方法院 93 年度易字第 1338 號刑事判決。

[61] 臺灣板橋地方法院 91 年度訴字第 1028 號判決，法院之見解。

為證據』，工作站電腦資料檢視備忘錄電腦歷程資料，係連續性由機器所製作之文書，如同銀行提存款紀錄無從增刪，自得為本案之證據。」[62]。

(5)「本判決下列所引用之發卡銀行信用卡或現金卡帳單部分，均為銀行承辦人員於業務上或通常業務過程中所須製作之紀錄文書或證明文書，查無其他顯有不可信之情況，且為被告所不爭執，故依刑事訴訟法第一五九條之四第二款之規定，亦有證據能力。」[63]

(6)「(七)松青超市八十八年三月七日、三月十七日、九月十二日發票三紙：此係松青超市收銀員所製作，為被告以外之人在審判外之書面陳述，依刑事訴訟法第一百五十九條第一項之規定，原則上不具證據能力；惟此係超商內從事業務之人依據顧客 購買交易之資料製作而與以列印之業務過程不間斷、有規律而準確之記載，正確性較高，依刑事訴訟法第一五九條之四第二款之規定，該發票三紙具有證據能力。」[64]

(7)「(一)被告將其所申辦之新海郵局、上海商業銀行帳戶資料交予李○○等詐欺集團使用，

[62] 臺灣臺北地方法院 92 年度訴字第 2083 號刑事判決。

[63] 臺灣臺北地方法院 95 年度訴字第 79 號刑事判決；同只尚有如臺灣臺北地方法院 93 年度訴字第 1088 號刑事判決：「(四)花旗信用卡八十八年八月一日消費帳單明細表：此係花旗銀行臺北分行所製作，用以表示告訴人黎○○每月之消費紀錄資料等情，為被告以外之人在審判外之書面陳述，依刑事訴訟法第 159 條第 1 項之規定，原則上不具證據能力；惟此係銀行內從事業務之人依據公司電腦先前交易之資料製作而與以列印，此項資料係根據信用卡交易之業務過程不間斷、有規律而準確之記載，正確性較高，依刑事訴訟法第 159 條之 4 第 2 款之規定，該等消費帳單明細表具有證據能力。」

[64] 臺灣臺北地方法院 93 年度訴字第 1088 號刑事判決

並由該集團成員，冒充法院、檢察署書記官等名義，以上揭方式詐騙告訴人戴晏溱、林雲華財物後，再由被告填寫提款單據，向銀行、郵局提領詐得之款項等事實，為被告所不否認，並據告訴人等於本院審理時結證明確，且有本院卷附上海商業銀行九十五年十一月十三日上華字第○九五○○○二四四號函、十二月十五日上華字第○九五○○○二六六號函及所附客戶資料、對帳單、活期性存款取款憑條，中華郵局政股份有限公司板橋郵局九十六年一月十日板營字第○九六○二○○○四一號函及所附客戶歷史交易清單、郵政存簿儲金提款單足按，上揭單據，均為從事業務之人對於業務上或通常業務過程中所須製作之文書，並無顯不可信之情況，依刑事訴訟法第一五九條之四第二款之規定均有證據能力，是此部分事實堪以認定。」[65]

2、否定說—電腦紀錄屬於傳聞證據，不具證據能力

（1）「數位聯合電信股份有限公司、中華電信股份有限公司數據分公司針對法務部調查局函覆之電信使用紀錄表，屬傳聞法則不具證據能力」[66]

（2）「刑事訴訟法新制採改良式當事人進行主義，為保障被告防禦權及維護直接審理與言詞審理原則，固於第一五九條第一項規定：『被告以外之人於審判外之言詞或書面陳述，除法律有規定者外，不得作為證據。』酌採英

[65] 臺灣板橋地方法院 95 年度易字第 1837 號刑事判決。

[66] 臺灣板橋地方法院 91 年度訴字第 1028 號判決，被告之主張。

美法之傳聞法則，是以，倘某項證據並非『被告以外之人於審判外之言詞或書面陳述』因非屬傳聞證據，自無傳聞法則之適用；而上開法文中之言詞或書面陳述即指供述證據而言，至所謂供述證據係指以一定事實之體驗或其他知識而為報告者，除此之外則為非供述證據；故此傳聞法則之規定，須供述證據始有其適用之餘地，而屬非供述證據者，即不受傳聞法則之拘束與排除，自不待言。本件檢察官所舉定存單、活期儲蓄存款取款憑條、活期存款收入傳票、放款本金（利息）收入傳票、歷史交易明細表等，固均由金融機構之職員於職務上所製作，然並非以其立場或地位，就特定之事實所為之書面陳述，核其性質，乃分別就存提款、匯款、定期存款、貸款清償等交易事實，將存款人、匯款人、受款人、存提款、匯款時間、金額、幣值、存匯帳戶之號碼等事實，經由機器設備予以機械式紀錄，並列印於交易認證欄之文書，是其待證事實並非以交易申請人所填具之各式文書所對象，而係著眼於此項記載匯款人、受款人、匯款時間、金額、幣值、匯入帳戶號碼之事實，即機械設備列印於交易認證欄上所呈現之事實，並非被告以外之人於審判外之陳述，即非屬供述證據，自不受傳聞法則排除之限制。」[67]

（3）「按刑事訴訟法新制採改良式當事人進行主義，為保障被告防禦權及維護直接審理與言詞審理原則，固於第一五九條第一項規定：『被告以外之人於審判外之言詞或書面陳

[67] 臺灣高雄地方法院 94 年度訴字第 1498 號判決。

述，除法律有規定者外，不得作為證據。』酌採英美法之傳聞法則，是以，倘某項證據並非『被告以外之人於審判外之言詞或書面陳述』因非屬傳聞證據，自無傳聞法則之適用；而上開法文中之言詞或書面陳述即指供述證據而言，至所謂供述證據係指以一定事實之體驗或其他知識而為報告者，除此之外則為非供述證據；故此傳聞法則之規定，須供述證據始有其適用之餘地，而屬非供述證據者，即不受傳聞法則之拘束與排除，自不待言。本件高雄市政府警察局楠梓分局刑案偵查卷宗所附之通聯調閱查詢單、臺灣高雄地方法院檢察署於 95 年 2 月 7 日雄檢博棉 94 蒞 22040 字第 9761 號函附之雙向通聯紀錄查詢資料，前者係針對行動電話發話、受話之有關電話號碼、發（受）話基地台位置、發（受）話之日、時、分、秒及其耗費時間等事項予以紀錄，而此之資料乃於使用該門號之　行動電話撥打或接收時，由電信公司之機房電腦自動以電磁紀錄加以儲存，後者原則上亦針對相同之背景資料予以紀錄，僅其設定之條件，非以門號為之，而係以各行動電話本身之序號為查詢條件，將與該行動電話有所通聯之電話號碼、發（受）話之時間、發（受）話基地台位置及該行動電話所搭配使用之門號，均詳細予以臚列，換言之，二者性質上均係就相關通聯資料經由機房電腦予以機械性紀錄，或列印供收取電話費之用，或作為證明電話發（受）話之紀錄之用，均非任何人就特定事項之體驗所為之供述，非屬供述證據，即非傳聞證據，自不受傳聞法則排除之限制，合先敘明。」[68]。

[68] 臺灣高雄地方法院 94 年度易字第 1930 號判決。

（4）「辯護人李○○律師質疑 XX 公司Ｒ／Ｄ專用工作站電腦資料檢視備忘錄、電腦歷程資料影本無證據能力」[69]。

由我國條文與實務見解觀察，可知：

1、從美國與我國文獻及案例中可以發現：除電子設備生成紀錄外，傳聞法則主要對電子設備存儲紀錄（第二類）與混和衍生紀錄（第三類）有適用的必要和法律效力，亦即有「人為」因素介入其中的電子證據，始應受傳聞法則之規範；至於電子設備生成的紀錄，因為實際上是實物證據，不含有「人為」因素，故不應以傳聞則加以規範，僅得以物證標準檢驗之。此與傳聞法則向來之定義與範圍一致，堪予肯定。

2、目前為止我國接受電腦自動生成紀錄不屬於傳聞證據之法源依據，多半引用刑事訴訟法第一百五十九條之四第二款：「除顯有不可信之情況外，從事業務之人於業務上或通常業務過程所須製作之紀錄文書、證明文書」，另外亦有引用第三款「除前二款之情形外，其他於可信之特別情況下所製作之文書，亦得為證據」之概括條款者，可見我國對於電子證據在傳聞法則上之見解，與美國 尚屬一致。至於前開否定說

3、對於電腦自動成紀錄是否屬於傳聞證據，有無證據能力一節，本文認為以採肯定說為當。惟美國聯邦證據規則第八０三條各款規定，認為各款屬「傳聞證據」之例外，亦即認為該條各款所列情形，仍屬傳聞證據，只是例外予以採納為認定事實之基礎。至於我國法院所引用之第一百五十九條之四，其所

[69] 臺灣臺北地方法院 92 年度訴字第 2083 號刑事判決。

列各款非屬傳聞證據之例外採納條款，因此電腦自動生成紀錄在我國屬非屬傳聞證據。

5.4　書證與驗真法則對於電子證據之適用

5.4.1　書證之意義

書證係指以書面之存在或內容所欲表示之意思為證據者。書證可分為廣義與狹義，廣義之書證指文書證據及證據文書二種；狹義之文書則單指證據文書一種。

文書證據係指以外觀、形狀及型態做為證據者，本質上屬於物證之一種，調查方法依刑事訴訟法第一百六十四條第二項之規定，為由法院向被告提示，令其辨認。若被告不解其義，應告以要旨。

至於證據文書，係指以文書之內容做為證據資料者，本質上屬於人的證據方法。調查方法依刑事訴訟法第一百六十五條之規定，法院應向被告宣讀或告以要旨，至若有關風化、公安或有毀損他人名譽之虞者，應交付閱覽，不得宣讀。被告不解其義者，應告以要旨。

本文對於電子證據之立場係採新文書證據說，以如前述。因此對於書證方面證據法則之探討，自應對書證所需要之驗真法則加以討論，亦即需要討論書證之證據調查方式。

5.4.2 書證與驗真法則

5.4.2.1 美國

5.4.2.1.1 書證與驗真法則對於電子證據適用之爭議

訴訟進行中提出電子證據之他方當事人往往會先對該證據移出偽造或變造之質疑，並進一步要求對系爭電子證據進行驗真，對於電子證據之驗真應與對於其他紀錄驗真之標準無異。[70]

對電子證據實施驗真之困難主要在於提出該項電子證據之他方當事人：

1、對電腦生成紀錄與存儲紀錄在形成後是否遭到過篡改、處理或毀損，提出質疑或異議[71]

在 United States v. Whitaker[72]案件中，檢察官指控被告非法銷售毒品，指控的證據是從另一名共犯福斯特的電腦中恢復得來的電子文件，這些文件詳細紀錄了他們以三個化名實施的毒品交易：一個化名是「Me」，推測可能是福斯特自己；一個化名「Gator」，係被告之綽號；另一個化名「Cruz」者為另一個毒品交易商之綽號。起訴之前檢察官許可福斯特協助從其電腦中找回了上述電子文件當成證據。訴訟中被告之辯護人提出，那些通過綽號牽連其當事人的電腦文件未能得到合理驗真，因為福斯特只需快速敲入幾個鍵，便能輕而易舉地將被告所代表之「Gator」添加進去，製作出一份看起來對檢察官有利之電腦文件。法院駁回此項主張，認為儘管存在著相

[70] CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, p.144.

[71] CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, pp.144-145.

[72] 127 f. 3d 595,601（7th Cir. 1997）

當大的懷疑，但仍不足以支持這些電腦紀錄已遭篡改；在缺乏明確證據證明發生了篡改的情況下，僅存在篡改可能性並不影響作出電腦紀錄符合驗真要求的結論。法庭認為，這種所謂的電腦文件遭篡改的主張「不過是一種臆想……沒有任何證據支持這種假想」，所以它並不影響對電腦紀錄具有可採性的裁定。

後來亦有法院採取相同之見解，並認為若抗辯之一方無法提出更進一步之證據證明系爭電子證據遭到篡改，則篡改的可能性之主張僅得影響證據之證明力，不能影響其證據能力。[73]

2、對電腦生成紀錄所依賴的作業系統或應用程式之可靠性提出質疑[74]

電腦生成紀錄之真實性會牽涉到作業系統或應用程式是否可靠之抗辯，若生成電腦紀錄之程式本身即含有嚴重設計錯誤，則該紀錄就有不真實之可能。此外，若程式輸出不正確，則其輸出之結果亦不得引為認定事實之依據。

訴訟程序中被告常試圖透過挑戰電腦程式之可靠性，藉以否定由該程式生成紀錄的真實性。對此法院認為只要檢察官能夠提供充足的證據，使陪審團確信這些紀錄是可信賴的、而被告擁有足夠的機會就準確性問題進行調查，則檢察官所提之該項電子證據具有證據能力。[75]

---

[73] United States v. Bonallo,858 F.2d 1427,1436（9th Cir. 1988）

[74] *See* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, pp.144-145.

[75] 同前註。

在證明方法上，通常提出電子證據之一方會以該程式用於正常的業務活動中，並因此得到系爭電磁紀錄以為證據之方式，用以證明電腦程式該程式可靠。[76]若該電腦程式不是應用於正常業務活動中，則舉證之一方必須說明該電腦是如何依指令運行，以及電腦準確地收到何種指令。一旦舉證之一方已經證實使用該程式具有基本的可信賴性，則對於電腦程式運行所產生之電磁紀錄錄準確性之質疑，僅是證明力問題，而不是可採性問題。[77]

3、會對電腦存儲紀錄的製作者身份，提出質疑[78]

電腦之可共用性、網際網路之匿名性，往往造成電腦存儲紀錄制作者身份之識別及確認具有很大的爭執空間，往往成為法庭中攻防之焦點。

實務上舉證方式通常是提供間接證據來證實該電磁紀錄製作者之真實身份。例如，在 United States v. Simpson[79]一案中，為證明被告曾與一名 FBI 探員在某一網路聊天室（Chat Room）討論過兒童色情之事，檢察官向法院提出該探員與一名自稱為「Stavron」之人進行網路聊天之列印輸出物，並意圖證明「Stavron」就是被告。一審法院採納該證據，判決被告有罪。被告在上訴中主張由於檢察官無法通過筆跡、文風和聲音證明那些網路聊天室中的陳述是他作出的，因此關於這些陳述之列印輸出物未經驗真，應予排除。聯邦上訴法院認為有大量的間接證據表明

[76] United States v. Moore, 923 F.2d 910,915（1st Cir. 1991 ）

[77] United States v. Catabran,836 F.2d 453,458（9th Cir. 1988）

[78] *See* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, pp.144-145.

[79] 152F.3d 1241（10th Cir. 1998）

「Stavron」就是被告，因此檢察官已經舉出了充足的證據，足以證明被告就是「Stavron」，那些列印輸出物也得到了驗真。並進而駁回被告之上訴。

5.4.2.1.2　書證與驗真法則對於電子證據適用之調整

1、電子證據之驗真必須遵循平等原則[80]

例如在 United states v. Vela[81]一案中，被告上訴主張將電磁紀錄與正常業務活動紀錄加以區別處理，並對電磁紀錄提出了更高的驗真標準，惟法院認為「電腦數據的匯編...應該與業務行為製作的其他紀錄一樣受到同等的對待」；在 United States v. Whitaker 一案中，辯方提出共犯福斯特操作電腦，可能對紀錄的完整性和準確性產生影響，法院認為辯護人的主張雖有一定的道理，但並沒有確實的證據證明存在這種情況，故認定檢察官的證明已經符合了對紀錄的驗真要求。

2、電子證據的驗真主要考察其是否具有形式上之真實性[82]

驗真是指形式上的真實性，而非實質上的可靠性。前者是可採性問題，後者屬於證明力問題。法院對這樣的觀念在 United States v. Whitaker、United States v. Bonallo 等案件中均一再出現。

[80] 劉品新主編，同第二章註 20，頁 109。

[81] 673 F2d.86,90（5th Cir. 1982）

[82] 劉品新主編，同第二章註 20，頁 110。

3、電子證據的驗真方法主要是側面認定方式，即自認、證人作證、推定與鑑定方式完成[83]

電子證據在產生、存儲、傳輸與取證等各個階段都有可能出現人眼不能察覺的差錯，對這些差錯只能通過間接方式加以辨別。在 United states v. Simpson 一案中即是採此方式。被告 Simpson 辯稱執法人員所查獲之兒童色情照片下載時間與 FTP 端的紀錄檔時間不同，無法確認兩者是相同的檔案；此外復辯稱執法人員將 Simpson 在網路聊天室之聊天內容印出之紙本文件無法比對筆跡，故無法證明此證據之真實性，法院不得採為證據。檢察官舉證從被告 Simpson 於網路聊天的談話內容中，可得知其真實姓名、個人的地址與電子郵件帳號。對 Simpson 住處搜索之結果，也找到能佐證談話內容的資料，故種種情況證據皆可佐證談話內容的印出物具有真實性，因此法院認為可採為證據。另外對於下載檔案時間與 FTP 伺服器時間不一致，檢方說明一般人下載檔案時，若發現本身已有此內容之檔案，往往會將新下載的檔案刪除，因此雖然有留下存取記錄，但電腦中的檔案並非下載的檔案，所以才會發生所持有的檔案紀錄之下載時間與 FTP 端紀錄檔之時間不同的結果。ISP 伺服器管理者作證表示，被扣押電腦中之 log 檔，指出 doit007.jpg 及 kk-a0021.jpg 兩個檔來自於 Boston 的網站，此二檔案並不會突然被下載，換言之，使用者無論是否知悉檔案內容，但明知其正下載檔案。此說法亦為法院所接受，因此認為被告前開二項抗辯均不足採，系爭證據仍有證據能力，最後據以將被告定罪。

[83] 劉品新主編，同第二章註 20，頁 111。

有學者認為對於電子證據之驗真，除傳統驗真法則之規定外，尚得就以下標準加以檢驗：[84]

1、電腦設備保存紀錄與產生列印物之可靠性；

2、基本資料最初存於電腦紀錄保存系統之方式；

3、一般商業運作模式之資料存取方式；

4、對於事件之發生有所認知的個人所記錄之事件，在事件發生後合理時間內資料之存取方式；

5、確保資料存取正確性之機制；

6、資料儲存的方法及避免在儲存過程中發生遺失之預警方式；

7、電腦程式處理資料之可靠性；

8、認證程式精確性之機制；

9、印出物準備的時間與方式。

[84] *See* Donald M. Zupanec, "*Annotation, Admissibility of Computerized Private Business Records*", 7 A.L.R.4th 8, 1981.,轉引自 J. Shane Givens, "*THE ADMISSIBILITY OF ELECTRONIC EVIDENCE AT TRIAL: COURTROOM ADMISSIBILITY STANDARDS*", 34 Cumb. L. Rev. 95, 2003.
（ http://www.lexis.com/research/retrieve?_m=bc6faa26c22b5742fd79764531df2933&docnum=2&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=6c966bc7fde4101b9817c35536c854fc，last visited on June 9, 2007.）

5.4.2.2 我國

5.4.2.2.1 書證與驗真法則對於電子證據適用之爭議

我國法定之證據方法分為人證、物證及書證三種，各有不同之調查方法。惟對於電子證據究竟屬於何種種類之證據，一直未有深入之探討，學說及實務上亦未有一致之見解。也正因為有一致之看法，所以衍生對於電子證據應適用物證或書證調查方法，調查方法有無應予調整或改進之處等討論，即未曾多見。

本文於第二章即先就電子證據之屬性，從資訊技術及法律上先加以分析，待認定電子證據屬於調整定義後之新文書證據，則以之對於現行制度下書證調查方式提出討論。

5.4.2.2.2 書證與驗真法則對於電子證據適用之調整

1、我國刑事訴訟法原規定之證據種類中，原未包含錄音帶、錄影帶及電腦資料在內，民國九十二年刑事訴訟法增訂第一百六十五條之一：

「前條之規定，於文書外之證物有與文書相同之效用者，準用之。

錄音、錄影、電磁紀錄或其他相類之證物可為證據者，審判長應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。」

（1）本條文概括規範現有各種形態證據如錄音、錄影及電磁紀錄，亦包含將來可能新生的各種證據，並明文以「適當之設備，顯示聲音、影像、符號或資料」為錄音、錄影、電磁紀錄或其他相類之證物的調查

方法。[85]考量未來科技的可能性，預留發展之空間，誠屬進步富有彈性之修法。

（2）現代社會，提出錄音帶、錄影帶、電磁紀錄為證據方法已經非常普遍，因此等物品之外觀並無可讀性，不應僅以「提示」為調查方式，但我國舊法對此既無明文規定，實務界見解復莫衷一是，新法第一百六十五條之一第二項規定此類證據審判長應以適當之設備，顯示聲音、影像、符號或資料，均屬正確之修法。[86]

2、我國現行刑事證據制度有待商榷之處：

（1）我國未要求書證是否應提出原本，書證是否提出原本，僅影響法院對該書證證明力之價值判斷，此點與修正後刑事訴訟法區分證據能力與證明力之觀點未趨一致。因為證據之提出，應該先考量證據能力上真實性如何，才進一步討論該項證據之證明力。因此我國法院審理案件習慣上將證據一概納入後再判斷證明力，今後應加以改善。

（2）證據的提出，法院理應確定其真實性後，才能審酌實質的內容，但我國刑事訴訟法對於書證之驗真並未作明文規定，致實務上缺乏依循的標準。[87]

---

[85] 該條立法理由強調：「隨著現代科學技術之進步與發展，不同於一般物證和書證之新型態證據，例如科技視聽及電腦資料已應運而生，我國刑事訴訟法原規定之證據種類中，並未包含此類科技視聽及電腦資料在內，爰參考我國刑法第 220 條及民事訴訟法第 363 條第 1 項之規定，暨日本刑事訴訟法第 306 條第 2 項之立法例，增訂準文書得爲證據方法及其開示、調查之方法，以概括地規範將來可能新生的各種新型態證據。」

[86] 吳巡龍，「我國刑事訴訟法關於物證、書證調查方式修訂之檢討」，頁 354，收於氏著新刑事訴訟制度與證據法則，學林文化事業有限公司，2003 年 9 月。

[87] 吳巡龍，同前註，頁 325。

5.5 最佳證據法則

5.5.1 最佳證據法則之意義

美國的證據制度，繼受自英國，英國古老司法程序中有文書審（trail by Charters）制度，亦即由起訴之原告將與爭議事實有關，並由被告所製作之文書遞交給法院，以便由法院裁定原告之主張是否有足夠之依據。[88]當時文書審有三要件：一、必須提供原始文書；二、必須由輔證證人證明文書制作過程；三、不能以言詞修正或變更文書之內容。[89]逐漸發展之後形成了今日的最佳證據法則。

最佳證據法則通常適用於文字材料或文書證據，即指為了證明文書的內容，要求提供原始文書，而不能提供複本。美國在訴訟上為防止出現欺詐和錯誤，以致於影響陪審團對事實之判斷，一直以來均遵循最佳證據法則。現今雖在聯邦證據法則中因應案件實際情況而有所調整，但仍為該國重要證據法則之一。

5.5.2 美國

5.5.2.1 最佳證據法則對於電子證據適用之爭議

電子證據的出現和運用，對最佳證據法則的挑戰在於如何判斷其原本。訴訟過程中，雙方當事人均會爭執電子文件之輸出列印輸出物，是否屬於最佳證據法則所稱之「原本」；如何適度調整許可使用電子證據複製件的範圍；以及如何區分電腦列印輸出物與聯邦證據法則第一００六條稱之「摘要」。

[88] 郭志媛，同第四章註 4，頁 252。

[89] 郭志媛，同第四章註 4，頁 252。

聯邦證據規則為因應新形態之文書證據或電子證據，在兩方面擴大了最佳證據法則的適用範圍：

1、最佳證據法則不僅適用於書面文件，也適用於錄音及照片。傳統上最佳證據法則只適用於書面文件，因此電話錄音、照片等形態之證據不在最佳證據法則適用的範圍內。但是，聯邦證據法則第一００二條擴大了最佳證據法則的適用範圍，根據本條，最佳證據法則不僅適用於書面文件，也適用於電話錄音、照片等。[90]

此外，聯邦證據法則第一００一條規定，所謂「書面」，包括以手寫、列印、印刷、影印等方式固定下來的字母、文字、數字或者其他具有相似功能的符號等。因此，電腦輸出列印之紙本文件、磁碟以及嵌有標誌文字的動產，如路標或者商品標簽等都應適用最佳證據法則。「錄音」包括以機械或者電子方式紀錄下來的字母、文字、數字或者其他具有相似功能的符號等。「照片」包括普通的靜止照片、X 光片、錄影帶和電影等。

2、在需要適用最佳證據法則時，傳統上一般只允許出示「原本」，但聯邦證據法則第一００三條擴大規定到也可以出示文件複本。

5.5.2.2　最佳證據法則對於電子證據適用之調整

1、電子證據的最佳證據法則的適用前提是為證明電子紀錄的內容[91]

[90] *See* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, p.152.

[91] 劉品新主編，同第二章註 20，頁 229。

最佳證據法則於電子證據之適用，前提在於為證明電子紀錄的內容，若非如此，而是為了證明其他內容，則並無適用最佳證據法則之問題。例如在 United States v. Gonzales – Ambrosio Hernandes – Coronel[92]一案中，法院指出最佳證據法則是尋求對文書與錄音紀錄的證據內容獲得最佳證實，本案中檢察官要證明的是談話內容，故可以採納證人證言，如果檢察官之目標是要探詢錄音帶紀錄的內容為何時，那麼錄音帶才會成為最佳證據。

2、判斷電子證據原本、複本之標準是人為擬制的，非自然標準[93]

例如在 Donald Gene Burleson v. the State of Taxas[94]一案中法院指出，電磁紀錄顯示物是通過電腦顯示的而非列印的，是通過視覺可讀的，並且是數據的準確反映，屬於原本之列。在 Doe v. United States[95]一案中法院認為，威阿軍事研究中心提交的程式性資料能夠證明其列印表確實屬於電腦數據的準確列印物，採納這樣的列印表作為證據雖不是典型地符合最佳證據法則，但不構成有違此法則。

有學者因此認為美國解決電子證據在最佳證據法則方面遇到的法律障礙的做法，概括為擴大解釋法，即通過擴大對原本的解釋，來解決在適用最佳證據法則時難以判斷何為電子證據原本的問題。[96]

---

92 537 F.2d 1051 (9th Cir. 1976)

93 劉品新主編，同第二章註 20，頁 229。

94 802 S. W.2d 429; 1991 Tex. App.

95 805 F. Supp. 1513,1517（D. Hawaii. 1992）

96 劉品新主編，同第二章註 20，頁 230。

3、法院在特定條件下可以允許採納電子證據之複本[97]

例如聯邦證據法則有規定證據數量太大不便於舉證的七種情況下，可以允許採納電子證據之複本。[98]

5.5.3　我國

5.5.3.1　最佳證據法則對於電子證據適用之爭議

我國現行法律，並無類似美國最佳證據法則之規定。對於電磁紀錄供作證據者，僅在刑事訴訟法法第一百六十五條之一規定，審判長對於電磁證據可為證物者，應以適當之設備，顯示聲音、影像、符號或資料，使當事人、代理人、辯護人或輔佐人辨認或告以要旨。惟規定主要目的在於透過特定的呈現方式證物，讓當事人能瞭解證物之內容，並非「最佳證據法則」之規定。[99]

惟同樣的困境，如電子證據如何判斷其為原本？訴訟過程中，雙方當事人均會爭執電子文件之輸出列印輸出物，是否屬於「原本」、是否有誤差？又如何適度調整許可使用電子證據複本之範圍？凡此亦均為我國檢視電子證據時之挑戰。

5.5.3.2　最佳證據法則對於電子證據適用之調整

我國並無最佳證據法則之規定，刑事訴訟法對書證及物證之調查，仍採職權主義，法院負有調查證據之義務。且依刑事訴訟法第一百六十一條第一項規定：「檢察官就被告犯罪事實，應負舉證責任，並指出證明之方

[97] 劉品新主編，同第二章註 20，頁 232。

[98] *See* CCIPs, Department of Justice, U.S.A., *Supra* note 8. Ch2, p.153.

[99] 錢世傑，同第一章註 7，頁 78。

法。」故對於電子證據之真實性，仍應由法院與檢察官於訴訟過程中加以調查及證明，期能協助法院發現真實。

本文認為電子證據是否為原本之判斷，可參考本文第二章對於電子證據原本與複本之區分標準定之。本文建議以美國聯邦證據規則第一００一條之規定為標準，電子證據於以下兩種情況下屬於原本：

A、當有關之電磁資料係存儲在電腦內，則該電磁資料產出能以視覺閱讀，並能準確反映資料之印出物或其他輸出物；

B、製作者或發行者有意使複本之電子證據具有同文書本身具有同等效力。

C、專利法第一三０條第二項

「前項專利檔案，得以微縮底片、磁碟、磁帶、光碟等方式儲存；儲存紀錄經專利專責機關確認者，視同原檔案，原紙本專利檔案得予銷燬；儲存紀錄之複製品經專利專責機關確認者，推定其為真正。」雖僅在規範電磁形式之專利文件真正性之推定標準，但亦應可作為我國電子證據書證原本概念之參考。

另外，因為傳統書證原本之概念實不容易不容易應用到電子證據或電磁紀錄上，因此通過以其他替代方式滿足最佳證據規則的目的，以證明「電腦系統真實性」來取代「電腦紀錄真實性」的證明，亦即以系統的真實性可以替代紀錄的真實性；究其實質，是以環境證據取代直接證據[100]，本文前開由 Donald M. Zupanec 所提出之應參考前開美國九項標準，即是從此觀點出發之標準，亦有可資參考之處。

[100] 何家弘，同第二章註 20，頁 341-342。

第六章　結論

近年來，由於資訊普及、數位化生活之蓬勃發展，人類既有溝通模式與商業市場的交易習慣大幅改變，社會生活中紛爭解決機制，尤其是訴訟證據，在此潮流衝擊下，亦不可或免的面臨前所未有的發展機會與重大挑戰。隨著各類型電子證據提出於法院者日增，訴訟當事人對於此類型證據將會衍生之證據法則上之爭執可預期地也將逐漸增多，面對此一新興之爭執態樣，相關之法制建立也就愈形重要，法院亦有必要對電子證據基本性質及原理加以留意，亦免造成審判錯誤或遲滯。是以，傳統的刑事證據法則是否仍然適用於電子證據所產生之爭議？我國既有之刑事證據法制相關規定，對於此類證據形態所衍生之紛爭解決是否足夠？均值得吾人進一步加以探討，這也是本文研究目的之所在。茲就本文所設定之研究議題即電子證據與新制證據法則間之關係、法律問題及爭議解決，歸納結論整理如后：

一、電子證據之意義：

本文認為電子證據是供為法院當成證據之電磁紀錄或電磁痕跡。因為採此定義能與我國現有法制及實務見解接軌；亦能與我國證據種類劃分規則接軌；能夠彰顯電子證據之特殊性；且採取科技中立之立法原則，能容納任何新興科技的可能性。

二、電子證據之法律地位：

電子證據之的法律地位以及證據方法，歷來有書證說、新書證說、物證說、獨立證據說、混合證據說、鑑定結論說及視聽資料說等見解。本文採新書證說而加以修正，認為其法律地位為「電磁紀錄雖非用文字所作成而與通常之文書有異，但係利用『0』與『1』二進位制電磁組合對於文字、圖像、聲音或影像予以紀錄，具有保存、傳達意思之機能，雖其原狀為二進位制不能直接閱讀，但可透過列印、顯示或播放等方式重現成為人類可透過感官理解之狀態，則相當於文書之閱讀，而應以修正之文書證據相應規範之。」故而調查證據之方法應以書證方法為基礎而調整之。

三、電子證據之分類：

學者專家對於電子證據雖然分類甚多，惟本文以為僅靜態電子證據與動態電子證據；類比式電子證據與數位式電子證據；數據電文證據、附屬信息證據與系統環境證據；電腦生成證據、存儲證據與混成證據；原本電子證據與複本（派生）電子證據等五種分類有證據法學上區別之實益。至於封閉系結中的電子證據、開放系統中的電子證據與雙系統中的電子證據；通訊協定不同區別電子證據等電子證據之分類，或許有其他意義上之區別實益，惟不具有證據法學上區別之實益。

四、電子證據立法例規範方向：

電子證據經規範屬於書證範疇，不論國際組織或其他國家，在採取等同功能法作為判斷之後，認為電子證據在證據類型上等同於書證，應以調查書證之方法調查之。至於採用傳聞法則、最佳證據法則與驗真法則之國家，認為電子證據於此等證據法則中應予調整適用。另外電子證據之證據能力與證明力應採取平等對待原則處理；亦即法院應以評估傳統證據之證據能力及證明力之相同標準對電子證據加以認定。

五、電子證據於刑事證據法則之適用：

本文對電子證據的法律性質，係採取修正後之新文書證據說，亦故應以修正之文書證據相應規範。基於認為電子證據屬於新文書證據的前提之下，在適用證據法則方面，本文認為電子證據應有證據能力與證據證明力、傳聞法則、違法證據排除法則、書證與最佳證據法則、驗真法則等證據法則之適用。

六、電子證據於證據能力與證明力之適用：

對於電子證據之證據能力，本文認為在有法定事由之其況下，應依刑事訴訟法對於證據能力之各項排除規範加以排除外；至於有得由法院斟酌之情形，於審酌是否有證據能力時，除新制刑事訴訟法第一五八條之四立法理由「三」所列之參考事項加以考量外。專就電子證據之特性加以考量，本文認為可就以下各點加以參考：「1、就合法性而言，以違反法律強制或禁止之規定所取得之電子證

據，例如違反通訊監察法、違法搜索扣押或其他不正方式取得之電子證據、違反傳聞法則之電子證據等，均應予以排除之。2、就真實性而言，不具有真實性的電子證據，例如電腦設備非於正常運作之狀態；提出證據之一方所交付之電子證據不完整、片段、不連續；未經合法保存、無法證明該電子證據為真實等情形，該電子證據應認為無證據能力。」在斟酌電子證據證明力時，應採取以下方向：「1、基於形式證明力即證據真實性之考量，應審酌電子證據之準確性及完整性，例如該項證據在形成、儲存、複製或傳輸、蒐集等方面是否受到影響及其影響程度的大小等因素。2、基於實質證明力之考量，由法院依據事實和法律，基於自由心證衡量電子證據之證明力。」

七、電子證據於傳聞法則之適用：

由美國與我國學說及實務中可以發現：除電子設備生成紀錄外，傳聞法則主要對電子設備存儲紀錄（第二類）與混和衍生紀錄（第三類）有適用的必要和法律效力，亦即有「人為」因素介入其中的電子證據，始應受傳聞法則之規範；至於電子設備生成的紀錄，因為實際上是實物證據，不含有「人為」因素，故不應以傳聞則加以規範，僅得以物證標準檢驗之。目前為止，我國接受電子證據屬於傳聞證據例外項目之法源依據，多半引用刑事訴訟法第一五九條之四第二款：「除顯有不可信之情況外，從事業務之人於業務上或通常業務過程所須製作之紀錄文書、證明文書」，另外亦有引用第三款「除前二款之情形外，其他於可信之特別情況下所製作之文書，亦得為證據」之概括條款者，可見我國對於電子證據在傳聞法則上之見解，與美國尚屬一致。

八、電子證據於違法證據排除法則之適用：

本文認為因非法取供；違反法定障礙事由期間或夜間訊問禁止規定取得之被告或犯罪嫌疑人之自白或其他不利陳述；檢察事務官或司法警察（官）詢問受逮捕拘提之被告或犯罪嫌疑人時，違反告知義務；傳聞證據；證人或鑑定人未經具結所出具之證言或鑑定意見；證人之意見證據；違反立法院於九十六年六月十五日，第六屆第五會期第十八次會議通過之通訊保障及監察法第七條第一項及第

二項之規定所衍生取得之電子證據等等，均應予排除不得採為證據。另外，對於違法搜索、扣押所取得之電子證據；違反立法院於九十六年六月十五日，第六屆第五會期第十八次會議通過通訊保障及監察法第五條及第六條規定所衍生取得之電子證據，除有法律明文排除之情形外，允許法官審酌人權保障及公共利益之均衡維護，對該項電子證據之證據能力取捨有裁量權。至於私人違法取得之電子證據，依刑訴法第一五八條之四之規定，私人違法取得之證據，自不能適用上開證據排除法則。

九、電子證據於書證及驗真法則之適用：

我國刑事訴訟法於民國九十二年刑事訴訟法增訂第一六五條之一，概括規範現有各種形態證據如錄音、錄影及電磁紀錄，亦包含將來可能新生的各種證據，並明文以「適當之設備，顯示聲音、影像、符號或資料」為錄音、錄影、電磁紀錄或其他相類之證物的調查方法。該條文考量科技未來可能性，預留發展之空間，誠屬進步富有彈性之規定。惟刑事訴訟法對於書證之驗真並未作明文規定，實務運作時缺乏依循之標準。又現代社會，提出錄音帶、錄影帶、電磁紀錄為證據方法已經非常普遍，此等物品之外觀並無可讀性，不應僅以「提示」為調查方式，新法第一六五條之一第二項規定此類證據審判長應以適當之設備，顯示聲音、影像、符號或資料，亦屬正確之修法。

十、電子證據於最佳證據法則之適用：

我國刑事訴訟法並無如美國聯邦證據規則中最佳證據法則之類似規定，對於提出文書繕本或影本作為證據的條件亦無任何規範。惟刑事訴訟上所使用之文書不可能皆能提出原本，有時乃有使用繕本或影本之必要，應仿美國立法，規定繕本或影本之使用時機，或明文規定準用民事訴訟第三五三條之規定。又因我國並無最佳證據法則之規定，復以法院對書證及物證之調查，仍採職權主義，法院負有調查證據之義務。再按刑事訴訟法第一六一條第一項規定：「檢察官就被告犯罪事實，應負舉證責任，並指出證明之方法。」故對於電子證據之調查，本文以為應由法院與檢察官於訴訟過程中共同加以調查及證明，期能協助法院為實質真實之發現。

參考文獻

一、中文著作

1.1 書籍

1. 王兆鵬，搜索扣押與刑事被告的憲法權利（國立台灣大學法學叢書124），元照出版有限公司， 2003 年 3 月。
2. 王旭正、柯宏叡、ICCL-資訊密碼暨建構實驗室，資訊與網路安全安全，博碩文化， 2007 年 3 月。
3. 內政部警政署，警察偵查犯罪規範，民國 92 年 8 月 12 日。
皮勇，刑事訴訟中的電子證據規則研究，中國人民公安大學出版社，2005 年 3 月。
4. 何家弘主編，電子證據之研究，法律出版社，2002 年 7 月。
5. （美）Rolando V. Carmen，李正峰等中央警察大學教授合譯，美國刑事偵查法制與實務（Criminal Procedure law and Practices），五南圖書出版有限公司，2006 年 8 月。
6. 林世懿，「國內電子商務經營現況及發展趨勢分析」，92 年度電子商務環境整備及企業對個人電子商務推動計畫，經濟部商業司，民國 92 年。
7. 林俊益，傳聞法則之研究，收錄於司法研究年報第 23 輯第 7 篇，司法院，民國 92 年 11 月。
8. 林鈺雄，嚴格證明與刑事證據，學林文化事業有限公司出版，2002 年 9 月。
9. 林鈺雄，刑事訴訟法（上冊），自版，2005 年 9 月四版二刷。
10. 吳巡龍，新刑事訴訟制度與證據法則，學林文化事業有限公司，2003 年 9 月。
11. 吳巡龍，刑事訴訟與證據法實務，新學林出版股份有限公司，2006 年 11 月。
12. 高大宇、王旭正、資訊密碼暨建構實驗室，資訊安全，博碩文化，2003 年 6 月。

13.高忠智，美國證據法新解，法律出版社， 2004 年 4 月。
14.郭志媛，刑事證據可採性之研究，中國人民公安大學出版社， 2004 年 4 月。
15.（美）Martin Campbell-Kelly、William Aspray 著，梁應權、胡頂立譯，我的名字是電腦（Computer：A History of the Information Machine）一書，天下遠見出版股份有限公司， 1999 年 6 月。
16.（日）石井一正著，陳浩然譯，日本實用刑事證據法，五南圖書出版有限公司，民國 89 年 5 月。
17.張斌，視聽資料研究，中國人民公安大學出版社， 2005 年 11 月。
18.陳樸生，刑事證據法，海天文化事業有限公司，民國 86 年 5 月重訂四版。
19.馮大同編，國際貨物買賣法，對外貿易教育出版社， 1993 年 5 月。
20.黃東熊，刑事訴訟法研究，自版，民國 70 年。
21.黃東熊，刑事訴訟法論，三民書局，民國 88 年 3 月。
22.（美）Tim Berners-Lee 著，張介英、徐子超譯，一千零一網 WWW 發明人的思想構圖，台灣商務印書館，民國 88 年 12 月。
23.（美）崔汴生譯，美國聯邦證據法，司法院，民國 92 年 1 月初版。
24.（日）土本武司著，董璠輿、宋輝英譯，日本刑事訴訟法要義，五南圖書出版有限公司，民國 86 年 5 月。
25.樊崇文、溫小潔、趙燕，視聽資料研究綜述與評析，中國人民公安大學出版社， 2002 年 2 月。
26.蔡墩銘，刑事證據法論，五南圖書出版公司， 86 年 12 月。
27.錢世傑、錢世豐、劉嘉明、張紹斌，電腦鑑識與企業安全，文魁資訊股份有限公司， 2004 年 10 月。
28.謝名冠，網路行為犯罪之研究，臺灣臺北地方法院檢察署 89 年度研究報告，民國 90 年 1 月。
29.劉品新主編，美國電子證據規則，中國檢察出版社， 2004 年 5 月。
30.劉品新，中國電子證據立法研究，中國人民大學出版社， 2005 年 5 月。
31.劉曉丹，美國證據法則，中國檢察出版社， 2003 年 2 月。
32.蔣平，計算機犯罪問題研究，商務印書館， 2000 年 8 月。
33.（法）達尼埃爾.馬丁、弗雷德里克-保羅.馬丁合著，盧建平譯，網絡犯罪-威脅、風險與反擊，中國大百科全書出版社， 2002 年 12 月。

1.2 期刊報章論文

1. 丁麗萍、王永吉，「計算機取證的相關法律技術問題研究」，軟件學報，第 16 卷第 2 期， 2005 年 2 月。
2. 王芳，「數字證據的性質及相關規則」，法學雜誌， 2004 年第 8 期，2004 年 8 月。
3. 王亞林、范勝兵，「論民事電子證據」，科技與法律季刊，2002 年第 1 期， 2002 年 1 月。
4. 李學軍，「電子數據與證據」，證據學論壇，第 2 卷，中國檢察出版社， 2002 年 2 月。
5. 宋伯東，「刑訴交互詰問制 學者反對倉促修法立院週三討論修正草案 施慶堂指目 前『一國五制』有待『統一』」，聯合報， 2001 年 10 月 21 日。
6. 宋寶宏、王靜，「電子資料證據在我國的證據地位與證明力」，西安政治學院學報，2003 年第 4 期， 2003 年 12 月。
7. 林少予，「全民公敵 美國反恐反到誰？」，聯合報，民國 95 年 12 月 4 日。
8. 林鈺雄，「嚴格證明法則與直審理原則」一文，收於氏著嚴格證明與刑事證據一書，學林文化事業有限公司出版， 2002 年 9 月。
9. 吳巡龍，「得通訊一方同意竊聽錄音之證據能力」，收於氏著刑事訴訟與證據法實務，新學林出版股份有限公司，2006 年 11 月。
10. 吳巡龍，「我國刑事訴訟法關於物證、書證調查方式修訂之檢討」，收於氏著新刑事訴訟制度與證據法則，學林文化事業有限公司， 2003 年 9 月。
11. 吳巡龍，「《刑事訴訟制度大變革》看看檢察官濫權、訴訟曠廢時日等缺失 當事人進行制 美國在檢討 台灣卻躁進」，聯合報， 2001 年 10 月 30 日。
12. 吳巡龍，「兩造對抗制 檢方起訴均不能事先將卷宗證據送法院 而我們卻自相矛盾 司改修法 非驢非馬」，聯合報， 2001 年 12 月 23 日
13. 高富平、俞迪飛，「電子紀錄等同於紙面證據的解決方案—兼論《電子簽名法》的局限性」，法學， 2004 年第 11 期，2004 年 11 月。
14. 徐巍偉，「電子文件的證據效力之研究」，中國檔案，2002 年第 2 期，2002 年 2 月。

15. 郭佳玟，「談電磁紀錄證據定義與方法—比較加拿大電子證據統一法與我國刑事訴訟法相關規定」，科技法律透析， 2005 年 4 月。
16. 常怡、王健，「論電子證據的獨立性」，法學，2004 年第 3 期， 2004 年 3 月；
17. 曹鴻蘭等，「電磁紀錄在民事訴訟法上之證據調查方法—民訴法研究會第 67 次研討紀錄」，法學叢刊第 171 期，民國 87 年 7 月。
18. 游偉、夏元林，「計算機數據的證據價值」，法學雜誌，2001 年第 3 期， 2001 年 3 月。
19. 張斌，「美國非法計算機證據排除之規定及啟示」，證據學論壇第 12 期，法律出版社， 2007 年 1 月。
20. 黃朝義，「證據基本概念與舉證責任」，警察法學第 5 期，內政部警政署，2006 年 10 月。
21. 錢世傑，「論刑事證據上關於數位資料證據資格之檢討」，月旦法學雜誌第 143 期， 2007 年 4 月。
22. 蔡碧玉，「2003 年刑事訴訟法新刑事訴訟法簡介（一）」，法務通訊，第 2137 期，民國 92 年 5 月 29 日。
23. 蔡碧玉，「2003 年刑事訴訟法新刑事訴訟法簡介（二）」，法務通訊，第 2138 期，民國 92 年 6 月 5 日。
24. 蔡碧玉，「2003 年刑事訴訟法新刑事訴訟法簡介（三）」，法務通訊，第 2139 期，民國 92 年 6 月 12 日。
25. 蔡碧玉，「2003 年刑事訴訟法新刑事訴訟法簡介（四）」，法務通訊，第 2141 期，民國 92 年 6 月 26 日。
26. 蔡震榮、張維平，「電腦犯罪證據之研究」，刑事法雜誌，第 44 卷第 2 期，民國 89 年 4 月
27. 蔡震榮、黃玥婷，「論數位證據之證據力」，刑事法雜誌，第 49 卷第 2 期，民國 94 年 4 月。
28. 劉滿達，「論數據電文的證據價值」，法學雜誌，1999 年第 8 期，1999 年 8 月。

1.3 會議論文集

1. 林宜隆、陳蕾琪，「數位證據對刑事司法的衝擊」，收錄於 2002 年全國科技法律研討會，交通大學科技法律研究所， 2002 年 11 月。
2. 陳家瑤、吳佳育，「數位證據於現行法律之相關問題」，收錄於 2002 年網際空間：資訊、法律與社會學術研討暨實務研究論文集Ⅰ，中央警察大學， 2002 年。

1.4 學位論文

1. 丁秋玉，網路犯罪證據之搜索扣押研究，中央警察大學法律研究所碩士論文，民國 91 年 6 月。
2. 呂雅文，探討通訊隱私範圍之變遷-以美國、德國和台灣法規為例，中正大學電訊傳播研究所碩士論文，民國 89 年 6 月。
3. 林一德，電子數位資料於證據法上之研究，臺大法研所碩士論文，2000 年 1 月
4. 潘建民，網路入侵電腦犯罪及其證據之研究，國防管理學院法律研究所碩士論文，民國 94 年 6 月。
5. 盧文祥，濫用電腦資訊所生法律問題之研究，國立中興大學法律研究所碩士論文，民國 74 年 1 月。

1.5 實務案例

最高法院

19 年上字第 1222 號判例

89 年度台上字第 6963 號刑事判決

96 年度臺上字第 229 號民事判決

高等法院

臺灣高等法院 88 年度上易字第 4209 號刑事判決

臺灣高等法院 92 年度交上訴字第 228 號刑事判決
臺灣高等法院 94 年度上訴字第 564 號
臺灣高等法院 94 年度交上更（二）字第 1 號刑事判決
臺灣高等法院 95 年度上易字第 2214 號刑事判決

地方法院

臺灣臺北地方法院 94 年度金字第 31 號民事判決
臺灣臺北地方法院 95 年度勞訴字第 194 號民事
臺灣臺北地方法院 89 年度訴字第 929 號刑事判決
臺灣臺北地方法院 92 年度訴字第 1411 號刑事判決
臺灣臺北地方法院 92 年度訴字第 2083 號刑事判決
臺灣臺北地方法院 93 年度訴字第 588 號刑事判決
臺灣臺北地方法院 93 年度訴字第 1088 號刑事判決
臺灣臺北地方法院 93 年度易字第 1338 號刑事判決
臺灣臺北地方法院 94 年度交聲字第 288 號交通裁定
臺灣臺北地方法院 95 年度訴字第 79 號刑事判決
臺灣板橋地方法院 91 年度訴字第 1028 號刑事判決
臺灣板橋地方法院 91 年度易字第 2968 號刑事判決
臺灣板橋地方法院 93 年易字第 638 號刑事判決。
臺灣板橋地方法院 95 年度易字第 1837 號刑事判決。
臺灣高雄地方法院 94 年度訴字第 1498 號判決。
臺灣高雄地方法院 94 年度易字第 1930 號判決。

1.6 網路文獻

1. Jürgen Kraus,「自我複製程序（Selbstreproduktion bei programmen）」
http://vx.netlux.org/lib/pdf/Selbstreproduktion%20bei%20Programmen.pdf
（last visited on June 8, 2007.）
2. 類比形式之介紹
http://cmca.mis.ccu.edu.tw/book/IEC/Questions/IEC_QCH15.doc；
http://www.sunfar.com.tw/ecsfweb/dictionary/dirdesc.aspx?dict_no=D0081
（last visited on June 8）

3. 數位形式之介紹
http://mypaper.pchome.com.tw/news/joehank/3/1265941409/20060311184056/；
http://www.sunfar.com.tw/ecsfweb/dictionary/dirdesc.aspx?dict_no=D0081
（last visited on June 8）

4. 東森新聞報，「南迴怪客案/范氏千萬理賠金　李雙全疑朋分共犯吃紅」，2006 年 5 月 20 日
http://www.ettoday.com/2006/05/20/138-1943820.htm#
（last visited on June 8, 2007.）

5. 高大宇等，「電腦資訊犯罪之身分追蹤驗證分析模式建立」，
http://163.25.10.166/monographicStudy/network
（last visited on June 8, 2007.）

6. 臺灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team，TWCERT)，「防止攻擊跳板主機的安全管理策略（二）」
http://www.cert.org.tw/document/column/show.php?key=30
（last visited on June 8, 2007.）

8. 聯合國貿法會國際商事仲裁示範法
簡體中文出處：
http://daccessdds.un.org/doc/UNDOC/GEN/ N97/763/56/PDF/N9776356.pdf?OpenElement
英文出處：
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
（last visited on June 8, 2007.）

9. 聯合國貿法會電子商務示範法
簡體中文出處：
http://www.uncitral.org/uncitral/zh/uncitral_texts/electronic_commerce/1996Model.html
英文出處：
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
（last visited on June 11, 2007.）

12.「《聯合國國際貿易法委員會國際商事仲裁示範法」簡介》
http://big5.mofcom.gov.cn/gate/big5/training.mofcom.gov.cn/video2.asp?C

lassID=663&action=-ifbase4-base44-yczO8bDZv8YmQ2xhc3NuYW1lPbn6vMq+rcOzyr63treo
（last visited on June 11, 2007.）

13. 聯合國貿法會電子簽名法
簡體中文出處：http://www.uncitral.org/uncitral/zh/uncitral_texts.html
英文出處：http://www.uncitral.org/uncitral/en/uncitral_texts.html
（last visited on June 8, 2007.）

14. 我國電子簽章法立法說明
http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm
(last visited on June 8, 2007.)

15. 加拿大統一電子證據法
http://www.ulcc.ca/en/us
（last visited on June 8, 2007.）

16. 美國統一證據法則
http://law.upenn.edu/bll/ulc
（last visited on June 8, 2007.）

17. 美國憲法中文譯文本
http://www.yihuiyanjiu.org/yhyj_readnews.aspx?id=4645&cols=13.
(last visited on June 8, 2007.)

18. 網頁列印出現亂碼之討論
http://blog.bs2.to/post/EdwardLee/566
（last visited on June 10, 2007.）

19. PDF 列印出現亂碼之討論
http://anais.fang.free.fr/forum/viewtopic.php?id=891
（last visited on June 10, 2007.）

二、英文著作

2.1 書籍

1.Alan M. Gahtan, Electronic Evidence, Thomson Canada Limited, 1999

Allen、Kuhns & Swift, EVIDENCE–Text, Problems And Cases, 3rd Ed.，Aspen Pub-lishing Inc.,2002.

2.Computer Crime and Intellectual Property Section Criminal Division（CCIPs）, Department of Justice, U.S.A., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 2002.

3.Eoghan Casey, Digital Evidence And Computer Crime, 2nd Ed., P.668, Academic Press, 2004。

4.Eoghan Casey, Investigating Child Exploitation and Pornography, Elevsier Academic Press, 2005。

5.John W. Strong, McCORMICK ON EVIDENCE, 5th Ed.,WEST Publishing Co.,1999。

6.Technical Working Group for Electronic Crime Scene Investigation, Department of Justice, U.S.A., Electronic Crime Scene Investigation－A Guide for First Responders, 2001.

2.2 期刊報章論文

1.Adam Wolfson,,” *“Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay* ”, Michigan Law Review,,104 Mich. L. Rev. 151，October, 2005.

(http://www.lexis.com/research/retrieve?_m=9f19dd1806e9a1092816c5ad374dfdff&docnum=2&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=0b5b9a81266a707b24d5b3c65975de5c , last visited on June 9, 2007.）

2.J. Shane Givens, “THE ADMISSIBILITY OF ELECTRONIC EVIDENCE AT TRIAL: COURTROOM ADMISSIBILITY STANDARDS”, 34 Cumb. L. Rev. 95, 2003.

（http://www.lexis.com/research/retrieve?_m=bc6faa26c22b5742fd79764531df2933&docnum=2&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-

zSkAl&_md5=6c966bc7fde4101b9817c35536c854fc，last visited on June 9, 2007

3.Jeffrey J. Norton & Noah P. Barsky, "*MANAGEMENT CONTROL ISSUES AND LEGAL CONCERNS SURROUNDING BUSINESS-TO-BUSINESS E-COMMERCE: TRANSACTIONS IN THE ELECTRIC UTILITY INDUSTRY*", University of Pittsburgh-The Journal of Law and Commerce, 2002
（http://www.lexis.com/research/retrieve?_m=92af733708afc0d3b48b63d4ebc4d335&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-SkAl&_md5=84d52e74afde656f7d7ce0da4e539c21,last visited on June 8, 2007.）

4.J. Shane Givens, "*THE ADMISSIBILITY OF ELECTRONIC EVIDENCE AT TRIAL: COURTROOM ADMISSIBILITY STANDARDS*", 34 Cumb. L. Rev. 95,2003.
(http://www.lexis.com/research/retrieve?_m=8e87e3acb4c42f7157dfed93d537837a&csvc=bl&cform=bool&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=d21507ef554b1a33e00a464344debdc8 ,last visited on June 10, 2007.）

5.Mark A. Johnson，" *Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?* ", 75 Marq. L. Rev. 439, rquette Law Review, 1992.
(http://www.lexis.com/research/retrieve?_m=a5c3fbd567f542231242d3453315e87a&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=12afbda7a64c850f82910de2d5178d60 , last visited on June 9, 2007.)

6.MARK D. ROBINS, "*Evidence at the Electronic Frontier: Introducing E-Mail at Trial in Commercial Litigation*", 29 Rutgers Computer & Tech. L. J. 219, 2003.
(http://www.lexis.com/research/retrieve?_m=8b8da1766c656334d7ceff46a76452fc&docnum=22& _fmtstr=FULL&_startdoc=21&wchp=dGLbVtb-zSkAl&_md5=48b24ec02a24252e95c125ab05d8664b ,last visited on June 10, 2007.)

7.Mark N. Cooper, "*SYMPOSIUM BRIDGING THE DIGITAL DIVIDE: EQUALITY IN THE INFORMATION AGE: INEQUALITY IN THE DIGITAL SOCIETY: WHY THE DIGITAL DIVIDE DESERVES ALL THE ATTENTION IT GETS* ", Yeshiva University Cardozo Arts & Entertainment Law Journal, 20 Cardozo Arts & Ent LJ 73，2002。
（http://www.lexis.com/research/retrieve?_m=4f3cd7388765bec5777ba57b8c108b2f&csvc=bl&cform=2758.-2&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVtb-zSkAl&_md5=46ba71a77de00048855980bf6abb526a, last visited on June 9, 2007.）

8.Orin S. Kerr, "*DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE*", 105 Colum. L. Rev. 279, January, 2005.

（http://www.lexis.com/research/retrieve?_m=6e7ca8e2547e33442a8e42472e865062&docnum=100& _fmtstr=FULL&_startdoc=91&wchp=dGLbVtb-zSkAl&_md5=a7047eb8cf3f598de2e9450f7d7aa777, last visited on June 8, 2007.）

2.3 實務案例

Alderman v. United States, 394 U.S. 165（1969）

Doe v. United States, 805 F. Supp. 1513,1517（D. Hawaii. 1992）

Donald Gene Burleson v. the State of Taxas, 802 S. W.2d 429; 1991 Tex. App.

Hughes v. United States, 953 F. 2d 531, 540（9th Cir. 1992）

Kates v. United States, 389 U.S. 347（1967）

New York v. Quarles, 467 U.S. 649（1984）

Norman A. Harris v. United States Department of Agriculture and Linda Jones , 124 F.3d 197（6th Cir. 1997）

People v. Holowko, 486 N.E.2d 877,878-89（Ill. 1985）

People v. Huehn, 53, P.3d 733,（Colo.App. 2002）

Rawlings v. Kentucky, 448 U.S. 98（1980）.

Silverthorne Lumber Co. v. United States, 251 U. S.385（1920）

Taylor v. Alabama, 457 U.S. 687（1982）

The People v. Timothy Ray Ward, 037718, Court of Appeal of California（5th Appllate District 2002）

United States v. Barth, 26 F. Supp. 2d 929, 936-937（W.D. Tex. 1998）

United States v. Blackburn, 992, F.2d 666（7th Cir. 1993）

United States v. Bradley Joseph Steiger, D. C. Docket No. 00-0017-CR-N（2003）

United States v. Bonallo, 858 F.2d 1427, 1436（9th Cir. 1988）

United States v. Briscoe, 896 F.2d 1476, 1494（7th Cir. 1990）

United States v. Carey（172 F. 3d 1268,1273-1275（10th Cir. 1999））

United States v. Catabran, 836 F.2d 453, 457（9th Cir. 1988）

United States v. Criminal Triumph Capital Group, Inc. ET AL., 211 F.R.D. 31; 2002 U.S. Dist., United States,（District Court for The District of Connecticut, 2002）

United States v. Cestnik, 36 F.3d 904, 909-10（10th Cir. 1994）

United States v. David, 756 F. Supp. 1385（D. Nev. 1991）

United States v. DeGeorgia, 420 F.2d. 893（9th Cir. 1969）

United States v. Golonel James A. Maxwell, Jr., 42 M.J. 568（1995）
United States v. Gonzales – Ambrosio Hernandes – Coronel, 537 F.2d 1051 (9th Cir. 1976)
United States v. Goodchild, 25 F.3d 55, 61-62（1st Cir. 1994）
United States v. Hall, 142 F 3d 988（7th Cir. 1998）
United States v. John L. Fueero（106 F. Supp. 2d 921;U.S. Dist.（2000））
United States v. Kennedy, 81 F. Supp. 2d 1103,1112（D. Kan. 2000）
United States v. Moore, 923 F.2d 910, 914（1st Cir. 1991）
United States v． Poulsen, 41 F. 3d 133（9th Cir. 1994）
United States v. Reyes, 798 F. 2d 380,383（10th Cir. 1986）
United States v. Robert, 86 F. Supp. 2d 678（S.D. Tex. 2000）
United States v. Ross, 456 U.S. 798,822-823（1982）
United States v. Runyan, 275 F. 3d 449,464-465（5th Cir. 2001）
United States v. Sanders, 749, F 2d. 195, 198（5th Cir. 1984）
United States v. Salgado, 250 F.3d 438, 452（6th Cir. 2001）
United States v. Slanina（283 F. 3d 670 680（5th Cir. 2002））
United states v. Simpson, 152F.3d 1241（10th Cir. 1998）
United States v. Vela, 673 F2d.86,90（5th Cir. 1982）
United States v. Vincent Franklin Bennett, 363 F.3d 947; 2004 U.S. App. 64 Fed. R. Evid. Serv.（Callaghan）467（9th Cir. 2004）
United States v. Walser, 275 F. 3d 981,986（10th Cir. 2001）
United States v. Weinstock, 153F.2d 272,278（6th Cir. 1998）
United States v. Whitaker, 127 f. 3d 595,601（7th Cir. 1997）
Walder v. United States, 347 U.S. 62（1954）

附錄　我國警方實施電腦犯罪偵查規範

摘自　內政部警政署，警察偵查犯罪規範，第 4 章第 17 節，臺灣，民國 92 年 8 月 12 日。

第四章 實施偵查

第十七節　電腦犯罪案件之處理

228、電腦犯罪係指利用電腦、網路及其周邊設備為主要工具或目的所從事之犯罪行為。

229、偵辦電腦犯罪案件，必要時得請求各直轄市、縣（市）警察局刑警（大）隊電腦犯罪專責組協助偵辦；涉及系統入侵、網路洗錢等重大案件者，得會同刑事警察局偵九隊協助偵辦。

230、各警察機關可依據電腦處理個人資料保護法及相關法令之規定，向網際網路服務業者、學校或相關業者查詢用戶個人資料或紀錄。

231、執行電腦犯罪案件搜索前置作業應注意事項：

（一）依據民眾檢舉或主動上網發現非法網站，蒐集相關資料。

（二）調閱搜索對象基本資料：運用警察資訊系統、刑事資訊系統（如刑案知識庫）或其他資訊系統調閱搜索對象基本資料。

（三）決定搜索地點、對象與時間：依據搜索對象上網時間及地區，決定搜索地點。

（四）勘察搜索環境：

１、確定搜索地點是否正確。

２、確定搜索地點電腦設備及其數量。

（五）擬訂搜索計畫。

１、勘察現場、畫現場圖：確定有那幾種型式的電腦及其數量、使用的系統、媒體、周邊設備等以決定搜索警力。

２、擬定搜索成員及其任務：依據現場勘察結果，估計搜索所需警力，並分配每位人員任務。

3、訂定搜索計畫：搜索計畫應含：

（1）現場狀況：現場人數、電腦數量及其系統。

（2）任務：搜索何種犯罪型態網站，如色情、盜賣非法光碟網站等。

（3）搜索項目：依據搜索之網站型態，擬訂搜索項目。

（4）交通：前進與離開路線。

（5）通信：回報搜索結果或請求支援。

（六）技術勤前講習：說明搜索任務、項目，模擬現場搜索狀況，講解人員示範如何操作電腦，自電腦內部取出犯罪證據，並由搜索人員親自實際操作演練。

232、執行電腦搜索應注意事項：

（一）網路上身分極易偽造、變造、匿名及被冒用，搜索應審慎為之，以免影響受搜索人權益。

（二）應讓受搜索人與電腦保持適當距離，避免受搜索人接觸電腦刪除檔案、證據。

（三）勿安裝或拷貝任何程式、檔案至受搜索人的電腦中。

（四）電腦檔案之證據應當場列印，並請受搜索人簽名按指印。

（五）搜索對象如為學校，應會同該校主任秘書或相當職務人員執行之，搜索時應注意態度與技巧。

233、執行電腦扣押應注意事項：

（一）執行扣押時以扣押整套電腦設備為宜，包含電腦主機、螢幕、鍵盤、電源線等設備。

（二）扣押電腦應符合比例原則，尤其網路公司應特別注意其影響層面。

（三）扣押物品時最好使用原扣押物的包裝或紙箱以免扣押證物受損，影響其證據力，尤其是電腦主機內含所有重要證據，更須小心拆裝搬運。

（四）磁碟片、光碟片等電腦輔助記憶體之數量應確實清點，並詳載於扣押物品目錄表。

234、電腦犯罪案件證物處理應注意事項：

（一）電腦：使用原設備包裝或紙箱避免受損影響其證據力，並小心拆裝搬運。

（二）磁碟片、光碟片：避免置於強光、高溫、磁場附近及灰塵場所。

235、電腦犯罪案件電腦鑑識應注意事項：

（一）重大特殊案件之電腦證物遭毀損、刪除、格式化或經加密無法解讀，得將證物送刑事警察局偵九隊鑑識解析。

（二）鑑識前應先將重要資料備份，以完整保存證據，必要時可全部備份。

（三）電腦鑑識時應於備份資料執行非破壞性鑑識，必要時得於原始資料鑑識解析。

（四）電腦資料、檔案或證據已遭刪除或格式化，應還原被刪除或格式化的資料、檔案或證據。

（五）電腦資料、檔案或證據被隱藏，應還原隱藏電腦資料、檔案或證據。

（六）電腦資料、檔案或證據被設定密碼，應將所設定之密碼解密。運用搜尋工具，輸入檔案名稱或檔案內容可能出現之數字、姓名或文字串，搜尋電腦內部重要檔案或證據。

236、電腦犯罪案件訊問重點：

（一）平常如何上網（何時、地、使用何電話、何帳號）。

（二）擁有、使用網路服務公司之撥接帳號。

（三）擁有、使用電子郵件帳號（含國、內外及電子布告欄網站）及代號（名稱、化名）。

（四）擁有、使用網路服務公司網頁之網址。