國立政治大學法律學系碩士論文

指導教授：李聖傑 博士

大話雲端

—妨害電腦使用罪之法益定性與立法建議

研究生：王文成　撰

中華民國一〇一年七月

謝辭

終於在歷經千辛萬苦後，要開始寫謝辭了！雖說論文就像自己的孩子一般，讓孩子出世的最大功臣應該是身為生父母的自己，但在撰寫這本論文的時候，若未受到了許多老師同學親朋好友的支持鼓勵與幫助，也不會有悠哉坐在書桌前思考謝辭要感謝誰的一天。所以就讓我好好利用謝辭的機會，對各位老師同學親朋好友一個個致上由衷感謝之意吧。

這本論文的完成，首先要感謝的是我的父親王正斌先生與母親連素真女士，二位家長不畏家中沉重經濟壓力，仍然堅持不讓我直接到司訓所報到，而選擇咬牙苦撐以讓我順利完成學業，此恩永生難忘。再來要感謝的即是恩師李聖傑教授，俗話說千里馬也要有伯樂識，這句話常被誤會成「好貨也要配識貨者」，但個人認為這句話的意思應該是「就因為有識貨者，所以才成就了好貨」，一個人的優點或長處，在絕大多數的情形下並不是自己發現，而是被發現的，所以這種發現並培養優點的可能性，對我而言無疑是首要注重的點。要發現優點，免不了就是需要大量的溝通以及互相理解，所以在研究所論文指導教授的選擇中，我也會選擇能夠溝通以及調子相符的教授作為我的指導教授。在此不但非常慶幸，也非常感謝李聖傑老師願意在研究所給我不少次帶課輔的工作，讓我能在刑法的學問上有更多學習的機會外，也要感謝老師花了很多時間與我溝通，以找出我的長處並且指引我論文的方向。畢竟一日為師終身為父，在感謝生父母之後，首要感謝的非恩師莫屬。

除了指導教授外，本次擔任口試委員的二位教授想必是除了我與李聖傑老師外對這本論文花最多時間的人了。校內委員許恒達老師的思考敏銳實在令我嘆為觀止，在口試前所預想可能會被問到的難題，在口試中全部命中，並且老師所給的建議也非常發人深省，令我受益良多。許老師在與學生交流的態度中亦讓我感到無比溫馨，每封學生所寄出的信件無論內容為何，一定都能收到老師的回信，也代表著老師對於學生每次的交流機會都非常重視的嚴謹態度，完全就只能拿全國電子的廣告台詞來形容，真是「就甘心」。而校外委員謝煜偉老師對學生和藹可親的態度也非常讓我感動，再加上對於文獻資料要求的嚴謹度以及更新速度之

快，也著實讓學生在口試當場上了一堂影響重大的課。論文能夠順利完成，二位老師可謂功不可沒，在此深深致謝。

要能使我達到足以寫出論文的學術涵養，在研究所中的各項資源也有著不少的幫助，在這麼多資源中，法學院(尤其是刑法中心)的老師們絕對占了很大的比重。許玉秀老師在刑法的路途上引領學生入門，讓學生在大學至今都對於刑法抱有一股熱情與憧憬，也才能完成這本論文。陳志輝老師對於學術寫作以及做學問的態度要求的嚴謹度，讓我在碩一後的每一篇報告都能非常用心參與，並且多少也受到了老師積極進取的態度影響，使我不管在考國家考試或是在論文的撰寫上都能有著源源不絕的熱情。何賴傑老師在碩士班的開課時常嘗試創新，而在課程中思考以及辯證的態度，也令我能在寫論文多次「卡關」的同時屢屢出奇制勝。謝如媛老師能夠巧妙的融合有親和力的教學態度以及對於學術的嚴謹要求，並且在評分上也很能給予學生信心以及學習的動力，在寫論文感到苦悶的同時只要回想起上課的時光，瞬間就能感受到學習的快樂，對於論文的寫作動力也隨之回復。段重民老師對學生的鼓勵以及照顧，也讓學生備感溫馨。民法組的陳洸岳老師在日文方面給了我不少的指導，同時作為一個導師也非常關心學生，在老師的鼓勵下，撰寫論文的最後一個月過的也不是這麼有壓力。王千維老師則是從大學時代就非常關心學生，在寫論文的過程中也常聽到老師的鼓勵說「快畢業了、快畢業了」，對於當時還很徬徨能不能順利畢業的自己真的給予莫大信心，非常謝謝各位老師們。

除了老師們之外，學長姐對我的照顧也是沒齒難忘的。陳柏良學長從我大一的時候就對我非常照顧，無論是課輔還是研究所考試或是國考後的人生規劃上都給了我不少有建設性的建議，也為我引薦了很多厲害的學長姐。如果許玉秀老師是引起我對於刑法興趣的新芽的人，那柏良學長就是持續把這新芽給培養茁壯的人。馮聖晏學長雖是受柏良學長所託在我大四的時候來帶讀書會，但是學長幾乎是將當時讀書會的成員每個人當自己的弟妹在照顧，無論是考上前或考上後，在各方面都給了我許多的建議與幫助，令我非常感動。鍾宏彬學長因為大三時接了許玉秀老師的課輔後開始認識，進研究所之後由於學長的治學嚴謹，也解決了我不少思考上的獨斷以及盲點。陳昭龍學長的博學多聞讓我每次都很期待跟學長聊

天的時光，總會讓我學到不少知識以及人生經驗。洪兆承學長在日文的文獻提供以及各方知識的意見提供與交換在顯示出治學的硬底子外，更讓我受益良多。施家榮學長除在學術的切磋外，研究所生活的各方面也都對我非常照顧。林永瀚學長在一起上課的期間也用過來人的角度給了我們不少的機會教育。林慧君學姊不但在學術的品質上律己甚嚴，對學弟妹的照顧卻也一點不少，在研究所修課以及論文上都受到了學姐很大的幫助。任欣儀學姊與任君逸學長不但致力為剛進研究所的我指點迷津，也是常常待在刑法中心的成員之一，不管是在學術上的互動還是價值觀的交換，都給了我很大的啟發。張安婷學姊與吳中漢學長在人生哲學上給我的意見非常寶貴，整個讓我在之後的研究所生涯中提升了一個檔次，同時也讓我能夠以更多元的思考方式來思考一個問題。洪麗雯、林宛怡、蕭琬頤、卓巧琦、張建強、柯孟君、解怡蕙、郭靜儒、魏平政、陳宗佑等學長姊也在研究所以及撰寫論文的過程中給了我不少照顧、建議與幫助，在此一併致謝。

感謝完中心的學長姊後，研究所同學們對我的影響也要令我在此致謝。首先必須先行還個債履行承諾，陳鴻元在論文初稿完成當晚，願意冒舟車勞頓之累把我從政大載回家，在此於謝辭中鄭重感謝，同時也要感謝促成這樁美事的劉耀文，搭霸王車的感覺真的超爽。詹朝欽對於整本論文給予多數建議以及口試義無反顧的幫忙，讓我好生感動，真是夠義氣。闕立婷在論文是否完成關鍵的時間點上為使我完成論文而幫忙張羅研究室，並且早上面對繁重的律師實習工作，晚上還得來研究室聽我論文寫不出來的種種喇賽跟抱怨，真的也必須在謝辭中感謝。陳幽蘭願意將研究室的位子借給只見過幾次面的我，如此信賴我的人格實在感心。簡士淳除了如何帥到連正妹在公車上對自己搭訕這點之外，在許多方面都是我學習的對象，這本論文的結構也有很大一部分是受其影響。周書甫在我論文碰到瓶頸的時候，不吝犧牲自己備課的時間跟我討論他也不怎麼感興趣的刑法問題，也給了我不少建議，論文能夠順利完成當然也要算他一筆。身在日本的阿卡弟(林殷正)，雖然我一直嚷嚷著要拜託你買書結果最後都化為千風，不過就精神上也給了我不少幫助(至少在臉書上貼的日本貓咪圖片治癒效果很大 XD)。邱冠文在論文撰寫的後期進駐研究室後也排解了我許多寫論文時的苦悶。李威忠跟李昱宗(俗稱忠宗二人組？)更是在論文卡住的關鍵時刻，適時出現跟我話唬爛幾句的貴人。俗話說助人為快樂之本，希望大家都能夠往後的人生中很快樂的度過！

接下來終於要輪到身為李門子弟的各位學長姊、同窗跟學弟妹了。首先是輩份最高的阿卡利(林記弘)學長，在我研究所的過程中給我不少照顧不在話下(在我要準備國考那個學期願意編寫論文邊幫忙帶課輔實在太罩了)，特立獨行的思考邏輯以及精準快速的反應能力也讓我好生崇拜，同時這篇謝辭長度會如此與眾不同也是受其影響。既然論文的質與量皆無法與其相提並論，所以希望至少能在謝辭的量上面能夠超過阿卡利那本(誤)。小八(羅婉婷)學姊在論文寫作的過程中，由於與本論文主題有一定程度的關聯性，所以造就了大量的討論以及意見交換的機會，在此非常感謝學姊提供的不少重要文獻以及討論機會，論文能完成功不可沒。小佑(簡佑君)學姊在論文大綱要出來的那個學期，也利用帶課輔跟課的時間跟我討論論文的大綱以及論文撰寫的形式上問題，跟小八學姊一樣都是會照顧學弟妹的好學姊。大飛(朱振飛)學長非常喜歡看書與思考，最令我佩服的是 EQ 很高，跟他討論事情總是非常愉快，在論文撰寫的過程中常給我建議不在話下，口試當天也不畏自己就是下一場應試人般的幫忙也順便為我壯壯膽，真夠意思。同窗林哲安在李門聚會時都是喇賽的好對象，對於準備考試很有一套，讓我受益良多。論文互助會(對不起我還是想不出什麼帥氣的名字，如果要很中二的倒是不少個)的同窗謝孟釗與許琬婷學妹也在撰寫論文的過程中不吝給予我寶貴的建議以指點迷津，在此一併致謝。趙若傑學弟富有強烈邏輯性的思考，也在每每的討論中能夠給我反芻跟省思的機會，如果有錢的話我會趕快買一台 PSVita，揪團一起去獵綠迅龍吧！

在寫論文的過程中適時讓我打起精神的學弟妹們，也是論文完成時必須感謝的一份子。林鈺恩學妹雖然在聊天時會覺得這人兩光兩光的，但是其實她是個挺可靠的人，不論是在當中心總務的時期或是當中心總幹事的時期，也因為如此讓我能夠在擔任中心總幹事之時，將一部份的工作放心交付，專心完成論文大綱。殷子捷學弟在擔任中心文書的時候，不畏所借出的論文從此不翼而飛的風險力挺我，讓我順利借出中心數本論文作參考(當然事後立刻如數歸還)，心中甚是感動。黃俊瑋學弟雖然在我撰寫論文時已是執業律師，但每週仍會利用一兩天到校上課之餘，跟我分享一些動畫心得，讓我的宅能量能夠適度的補充(雖然今年夏番只有看 Fate/Zero)。李元棻、陳炫谷、葉書瑜、廖昱筑、傲嬌花(黃嗣芳)、陳柏安、邱筱雯、徐佩玉、邱邦傑、吳思宜、洪偉修(抱歉偉修委屈一下)、鄭欣怡、小花(許

文琪)、林道、楊喬嵐、qn123456(林永翰)、一姊(李律欣)、張喻淳、林誼勳、簡子彬、蕭一健、吳家欣等學弟妹們(如無出現者，不要懷疑一定是學長記性不好漏掉了)，也在寫論文的過程中無論是在學校或是在網路上為我打氣按讚，在此一併感謝。作為即將畢業的學長，也祝你們能夠順利完成學業，邁向人生的另一個階段。

再來要感謝的是在論文寫作過程中勉勵我的好友們，大學四年的孽緣加上國考讀書會兼週末爬山團的夥伴爾金(王泓翔)、腐姊(沈君蓉)、囧黃(黃慶輝)、ㄌㄐ(劉婕)、榔哥(劉奕榔)、囧怕翰(陳柏翰)總是能在帶給我無盡的歡樂與搞笑空間之餘，提供我知道一些重要的訊息，並且還不計代價的提供交通工具以及時間幫助我作資料的蒐集，這一路走來有你們的陪伴讓我非常慶幸。阿龐(龐笠中)、阿冏(趙均豪)、阿驢(盧柏翰)跟機歪迪(黃煒迪)也常常在臉書上相見歡，在論文遇到瓶頸時跟你們聊天總是能讓心胸開闊些。楷宅(林楷)在我寫論文的這一年來冒著被酸以及重考的風險包辦我大部分的休閒娛樂，也祝你在今年順利上榜後繼續跟兩個妹妹過著阿良良木般的同居生活，當然能藉此遇到戰場原或羽川就更好了。蕃茄(陳怡儒)在這一年間也不時的會關心一下我的論文進度(雖然通常會伴隨著對特定AV女優或是18禁遊戲的最新見解)，祝你順利尋得良妻以免出家當破戒僧(咦)。逆十字(黃遠至)在這一年間也不斷與我討論日文的文法以及給予我翻譯與檢視翻譯的機會(但通常要求翻譯的文章內容都挺糟糕的)，祝你到英國留學後不要開始懷念起台灣的食物。憶千年(姜雲馨)在板院訴輔科當替代役之餘，也會不時的告訴我各種實務經驗，令我撰寫論文的時候能夠時時刻刻的惦記著實務的難處與需求，祝你退伍後能順利找個好工作。宅匡(陳彥匡)不但平時會跟我「報告」自己的進度來激起我的競爭意識，在我寫論文而有感而發時，往往也是第一個聽我胡謅的人，祝你能夠順利畢業開拓新的人生。

最後要感謝的是我的女朋友(不論是三次元的還是二次元的)，在這25年來從未出現，讓我能專心完成這本論文。如果可以的話，希望能對未來的我溫柔一點，萬分拜託。

唉…結果頁數還是沒有超過阿卡利那本[*]，果然我還未夠班啊。

2012.07　　於現實與虛擬的狹間

[*] 林記弘，心理傷害之刑法定位，國立政治大學法律學研究所碩士論文，2010 年 7 月。

摘要

本論文共分為六章來呈現整體架構，於以下分別敘述。

第一章是緒論，就整體論文的研究動機、問題意識、研究方法以及論文結構作一個完整的交代，得以令人快速了解論文的內容以及契機。

第二章即就雲端運算的定義、發展、特色等要素，來釐清雲端運算就何所指，以及雲端運算對於現行電腦使用關係與現行電腦犯罪規範的影響。並進而指出現行電腦犯罪的規制可能因為雲端運算的到來而失去遞續性，產生了適用上的困境。

第三章的部分即是自我國電腦犯罪的發展過程作分析介紹，並且也就外國立法例的處理態度做對照，從我國電腦犯罪於妨害電腦使用罪章制定之前對於電腦犯罪規制的傳統見解，到妨害電腦使用罪章的修訂過程以及結果所呈現的整體罪章特色，以及所產生問題等皆是本章要處理的問題。並且在比較法的部分，亦詳實的呈現了當初設計規制時的該國情勢，以及修法後所遭到的批評，並且配合整體國際情勢對於我國電腦犯罪規制的去從給予一點建議。

第四章的部分則是以罪章施行後的實際面向來探討罪章所產生的適用上問題。畢竟自罪章制定施行至今已有約十年之久，於實務上的適用案例亦多達數百件，則實務上如何適用此些條文即是令人好奇之處。同時就該罪章所規制的各種行為態樣而言，在規制的設計上於現今受到何種批評，此些批評可能來自學界於分析法條後所產生的檢討聲浪，亦可能來自實務界於適用上所產生的困惑表示，更重要的則是有關行為規範的遞續性，亦即在雲端運算時代來臨後，此些行為態樣具體而言在適用上可能碰到何種困難，以及應該就何方向作改進。

第五章的部分則是對於前揭章節的分析結果的具體運用。首先必須從頭開始分析「電腦犯罪」，找出面對變動迅速的資訊科技的正確態度，並進而實踐此種態度來設計電腦犯罪的規制。在確立正確態度之後，即要基於此種態度對於電腦犯罪的規制作設計，包括罪章的保護法益、電腦概念的確定、以及細部的行為態

樣以及處罰架構等問題，以建構一個對於電腦犯罪的規制模型。並且為了確保所建構的模型不但得以解決現有問題，亦存在本文所強調的遞續性，故在建構出規制模型後，本章仍挑起了以前述章節中所提及的案例，以及雲端運算出現後可能會產生的案例為對象，以所建構的模型來適用於該些案例的擔子。

最後的章節即是結論，亦即對於上述各個章節所得出來的研究成果作一個最大的總結，其中除了彙整每章所得出的結論外，亦以一氣呵成的敘述方式來為整本論文最終所要表達的立場作一個鮮明的闡述。

關鍵字：電腦、電腦犯罪、妨害電腦使用、雲端運算、網路秩序信賴、使用空間、法益、立法建議。

簡目

詳目

國立政治大學
National Chengchi University

第一章　緒論

第一節　研究動機與問題意識

第一項 研究動機

電腦(Computer)於人類社會的發展，誠可謂影響重大。自 1946 年第一台電腦誕生，於 1970 年代後，因積體電路的引進，大幅降低電腦的生產成本，使電腦較為普及化，然此時電腦仍僅是作為商業或高科技發展的用途。於 1980 年代，個人電腦[1]開始普及於學校以及家庭。此時電腦以漸漸與大眾的生活息息相關，大多生活用品與電腦結合後，對於人類生活的便利性以及安全性影響日益增加。於 1990 年代，由於網際網路之普及，使得電腦幾乎成為人人生活中不可或缺的一大部份，舉凡購物、娛樂、金融、交友、辦公、甚至學習，大多數皆得以電腦達成。

衡諸上述發展簡史，可以發現電腦自發明至蓬勃發展，僅短短 60 餘年，但對於人類社會的影響，甚至比發明至今有 600 年以上的物品，如紙、印刷術等發展速度更快，影響更大。據此，有稱此段電腦普及的時代為「資訊爆炸」時代，亦可見電腦對於人類社會的影響程度甚鉅。伴隨著電腦快速進入並影響人類社會的現象，於社會上已產生諸多問題。於刑法上，因為電腦的發展，使行為人宛如虎添翼般獲得更快更方便的犯罪工具，亦發生行為人將電腦本身作為客體，對其之各種破壞等問題，越來越多層出不窮的案件，使得法律人不得不被迫重視此類「電腦犯罪」的問題。

從而，為因應層出不窮之電腦犯罪問題，於民國 86 年，我國刑法公布修正以及增訂 9 條關於「電腦」的條文。而於民國 92 年更追加公布增訂的第 36 章「妨害電腦使用罪」章，以顯示立法機關除惡務盡之勢。惟此項修正追加，是否真能

[1] Personal Computer，簡稱パソコン或 PC。

如立法機關所願的「除惡務盡」，從修正之後引起學術界一片撻伐聲浪的情形觀察，似乎有所疑義。除對於「電腦」本身的概念定義不清之外，妨害電腦使用罪章是否能承受未來科技型態日新月異的變動–亦即整體法條的遞續性亦具可議空間。此種疑義在近期熱門的新名詞–雲端運算的出現後，似使問題更趨明顯，且雲端運算所延伸的雲端服務已普及民間，勢必於未來會有大量、複雜的案件出現在法庭上衝擊著現行法制，亦表示此問題的急迫性以及必須重視性。

據此，本篇論文嘗試著以雲端運算為例，說明現行法上的缺失，並且試著以保護法益為出發點重新架構妨害電腦使用罪章，期能使妨害電腦使用罪章有一個合理的存在依據，並給「電腦犯罪」此一犯罪型態找到一個適當歸屬。

第二項 問題意識

自從雲端運算此一名詞出現後，意味著世界電腦發展的趨勢如同 1943 年美國 IBM 初代董事長 Thomas Watson 所預言「我認為世界電腦市場約僅五台的規模」[2]一般，正邁入了資訊計算及儲存的大一統時代。資訊計算及儲存的統合，同時也代表著將雞蛋放在同一個籃子中，資訊破壞及資訊取得之便利性顯著上升。並且，對於就被害人資訊破壞或取得之行為，是否僅係該「個人」的問題，亦不無思考之餘地。面對此種現象，觀察我國法律，於刑事上似僅得以妨害電腦使用罪處以最高五年以下有期徒刑的法律效果，行為與法律效果間是否符合罪刑相當原則即有疑義。從而，在此產生之首要問題是：刑法妨害電腦使用罪章的法律規定本身是否即有檢討餘地？

並，衡諸刑法妨害電腦使用罪章及其他相關電腦犯罪條文的研修資料，以及法律修正後學者對本次修正的評析，該些法律條文似於修訂當時即有疑義。其中較根本的爭議之一，即是本罪章的保護法益究竟為何，以及本罪章是否有獨立存在必要等問題。然就法益論者的邏輯觀察，若一罪章的犯罪皆有其獨立於其他罪

[2] 中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月，頁 4 以下。

章的保護法益，則該罪章即有獨立存在的依據。據此，本論文的首要目的，同時也是最理想的結果，即是為本罪章尋找一獨立的保護法益，使其有獨立存在的依據。

於找到保護法益，並使本罪章有獨立依據後，下一步即是環繞著此保護法益，逐一架構本罪章的各個條文，並在架構的同時也對原罪章的條文規定是否符合保護法益本旨做確認，若條文內容不符保護法益本旨，即對該條文進行修訂甚至刪除。此外，對於雲端運算出現，並造成社會上使用者使用習慣改變後所產生的新型態行為，亦應考慮如增訂新條文，或就原有條文進行增修的方式將其入罪化。

最後，亦同時要對縱向及橫向作思考。縱向思考中所考慮者，是妨害電腦使用罪章於修訂後，是否具有沿遞存續[3]的功能，亦即修訂後的新妨害電腦使用罪章縱使歷經下一次資訊科技革命，仍然對於使用者新型態的使用關係有所適用，不致再度淪落為必須再次修訂始得繼續適用的餘地。而於橫向思考的部分，則是對於「電腦」以及「電腦犯罪」等概念的釐清，並進一步思考本罪章是否僅能使用於「電腦犯罪」，抑或得擴張適用於電腦犯罪以外的行為，使刑法的法益保護功能更趨完善。此二方向的思考，皆係本論文思考的出發點，亦係本論文所欲達到的最終目的。

第二節　研究方法與論文架構

第一項 研究方法

於研究方法的部分，本文仍採用傳統的文獻分析法，輔以實務案例的整理觀察。其中文獻分析的範圍，除國內學界各論者所投書的期刊雜誌甚至專書，以及實務界流血流汗的立法過程記錄等政府出版品的文獻資料外，仍為與世界接軌並且對於電腦犯罪作更全面的分析，故亦涵蓋比較法的立法例等外國文獻資料。然

[3] 本論文稱此功能為「遞續性」。

而較遺憾之處在於，由於語文能力的不足，在此所引用的外國文獻資料僅能受限於以日文文獻為主要參考文獻。而就比較法的部分，由於一來我國是繼受法，所繼受的國家是德國與日本，從而對於該二國對電腦犯罪的處理，即是在探討我國法制的優缺後，進而思考電腦的使用行為在我國應該如何對待之前，所參考的對象，二來由於德國與日本的法體系皆屬大陸法系，與其相對的英美法系國家中亦對於電腦犯罪有所規制，或許對於思考的靈感有所啟發，並且英美法系中的美國亦是電腦發祥地，且目前仍執全世界電腦產業的牛耳，其對於資訊科技發展的反應靈敏度，絕對遠勝於德國與日本，若要檢驗規制是否有遞續性，絕對不能缺少美國對於資訊科技發展走向的敏銳觀察力，並且美國目前為主導全世界政治經濟走向的大國，在對於電腦使用的規制上，亦可能透過國際關係對於其他國家施壓，進而影響世界各國對於電腦犯罪的規制態度，若要研究此種全球性的科技犯罪，對於此種於世界上具有極大影響力國家的立法例應絕不能放過，故本文在參考德國與日本立法例之外，仍將美國立法例列為比較法參考的指標。

第二項 論文架構

在論文結構的部分，本論文共分為六章來呈現整體架構，於以下分別敘述。第一章是緒論，就整體論文的研究動機、問題意識、研究方法以及論文結構作一個完整的交代，得以令人快速了解論文的內容以及契機。

而基於本文是以雲端運算為引子，而雲端運算又是一個無論是對於社會上，或甚至對於法學上皆是一個嶄新且模糊的名詞，縱使連資訊科技業者口中所述的雲端運算可能都各有不同看法，故對於此種自電腦延伸出來的新概念勢必得做一番介紹探討。從而本文的第二章，即就雲端運算的定義、發展、特色等要素，來釐清雲端運算就何所指，以及雲端運算對於現行電腦使用關係與現行電腦犯罪規範的影響。並進而指出現行電腦犯罪的規制可能因為雲端運算的到來而失去遞續性，產生了適用上的困境。

在指出從雲端運算所看到我國電腦犯罪於遞續性上產生問題之後，於第三章之後即必須來檢視我國對於電腦犯罪的規制設計以及適用上到底出了什麼問題。

不過因對於電腦犯罪的規制設計以及適用部分所設範圍甚廣，故本文就規制的發展過程以及規制態樣的實際適用兩大部分作區分，分別於第三章及第四章作探討。在第三章的部分即是自我國電腦犯罪的發展過程作分析介紹，並且也就外國立法例的處理態度做對照，從我國電腦犯罪於妨害電腦使用罪章制定之前對於電腦犯罪規制的傳統見解，到妨害電腦使用罪章的修訂過程以及結果所呈現的整體罪章特色，以及所產生問題等皆是本章要處理的問題。並且在比較法的部分，亦詳實的呈現了當初設計規制時的該國情勢，以及修法後所遭到的批評，並且配合整體國際情勢對於我國電腦犯罪規制的去從給予一點建議。

相對於就規制制定面來檢討妨害電腦使用罪章，在第四章的部分則是以罪章施行後的實際面向來探討罪章所產生的適用上問題。畢竟自罪章制定施行至今已有約十年之久，於實務上的適用案例亦多達數百件，則實務上如何適用此些條文即是令人好奇之處。同時就該罪章所規制的各種行為態樣而言，在規制的設計上於現今受到何種批評，此些批評可能來自學界於分析法條後所產生的檢討聲浪，亦可能來自實務界於適用上所產生的困惑表示，更重要的則是有關行為規範的遞續性，亦即在雲端運算時代來臨後，此些行為態樣具體而言在適用上可能碰到何種困難，以及應該就何方向作改進。

對於前揭章節的分析結果的具體運用，即是第五章要進行的工作。第五章首先必須從頭開始分析「電腦犯罪」這個撼動世界的大怪獸，找出面對變動迅速的資訊科技的正確態度，並進而實踐此種態度來設計電腦犯罪的規制。在確立正確態度之後，即要基於此種態度對於電腦犯罪的規制作設計，包括罪章的保護法益、電腦概念的確定、以及細部的行為態樣以及處罰架構等問題，以建構一個對於電腦犯罪的規制模型。並且為了確保所建構的模型不但得以解決現有問題，亦存在本文所強調的遞續性，故在建構出規制模型後，本章仍挑起了以前述章節中所提及的案例，以及雲端運算出現後可能會產生的案例為對象，以所建構的模型來適用於該些案例的擔子。

最後的章節即是結論，亦即對於上述各個章節所得出來的研究成果作一個最大的總結，其中除了彙整每章所得出的結論外，亦以一氣呵成的敘述方式來為整

本論文最終所要表達的立場作一個鮮明的闡述。

第二章　虛擬世界之新寵兒–雲端運算

第一節　序說雲端

雲端運算，這四個聽起來帶點神秘又附有邏輯感的文字，於 GOOGLE 公司發言人暨台灣雲端運算計畫主持人葉平登高一呼後，儼然於台灣成為資訊業界數一數二「夯」的關鍵字。各個資訊業如同前一陣子生技業對奈米科技趨之若鶩一般，紛紛標榜自己所採用的服務係「雲端服務」或「軟體即服務(SaaS)」，且自家所採用的技術為「雲端技術」。然而在此仔細觀察，即會發現數項疑問。首先，每家資訊業公司口中所闡述的雲端運算定義以及功能似乎皆有出入，有表彰其發售的軟體是使用雲端運算因而免安裝、有號稱其所出租的硬碟為運用雲端運算而成的雲端硬碟，將資料存取於其上即可避免資料毀損或滅失、亦有表彰其提供的服務為雲端平台，使用者可在平台上發表他們編寫的程式，使世界各地之使用者皆得接觸使用。雲端運算的定義如此「五花八門」，不禁讓人懷疑業界所稱的雲端運算，是否僅為一個吸引肥羊入陷阱的誘餌，其實它的本質就連業界自己皆不甚理解；其次，乍聽之下，雲端運算的運算模式類似於舊時代即存在的網格運算與分散式運算技術，究竟這些技術是否有所分別？雲端運算是否就是指網格運算或分散式運算，而資訊業將它「換個包裝」即上市推廣於資訊專業知識較低的社會大眾使用？最後，縱使雲端運算不同於網格運算或分散式運算，就雲端運算是基於網際網路的運算方法這點而言，此種運算方式是否早於網際網路出現的時代即已存在並默默地開始運用，亦即雲端運算只是因為商人炒作，而舊瓶裝新酒般的將舊概念當成新興概念宣傳，實質上根本無討論的價值與必要[4]？

綜上，究竟「雲端運算」、「雲端技術」、「雲端服務」三者間的關係為何，係一同義反覆的詞彙，亦或是各有不同內涵？又，雲端運算的定義為何？是否有一個統一的定義？再者，「雲端運算」是否是個新概念，亦或僅係老調重彈？在隨

[4] 若此假設為真，則於刑法妨害電腦使用罪章修訂當時網路可謂已普及，於法律解釋上的解釋態度可能不同，且此類問題於立法當時極有可能已被提出討論，故而在此的討論價值會降低。

著時代潮流對雲端運算高談闊論，並且分析其對我國法制是否有所影響之前，似乎要先搞清楚雲端運算為何所指。

第二節　認識雲端運算

若要探討雲端運算為何所指，第一步即是對雲端運算的定義做一個探討與釐清。同時，雲端運算是一種資訊運算模式，而該模式的基本原理為何，亦是了解雲端運算時的首要工作。從而，本節即將重點聚焦於雲端運算之定義及雲端運算之基本原理，並依序於以下各項探討之。

第一項 雲端運算之定義

雲端運算本係基於網際網路的一種運算方式。透過此種方式，共享的軟硬體資源和資訊可以按需提供給電腦和其他裝置。所謂「雲端」其實即是泛指「網路」，其名稱來自工程師在繪製示意圖時，常以一朵雲來代表「網路」。因此，若將雲端運算以通俗一點的方式解釋，雲端運算就是「網路運算」[5]。舉凡運用網路溝通多台電腦的運算工作，或係透過網路連線取得由遠端主機提供的服務等，皆得稱為一種廣義的「雲端運算」[6]。據此，不同企業對於雲端運算的定義根據自己之商業應用提出了不同定義，以下提出幾個較著名的定義，並以表格整理於下供參考[7]。

定義者	定義	備註
維基百科	一種能將動態伸縮的虛擬化資源透過網路以服務方式提供予使用者的運算模式，並且使用者無需了解如何	此種定義方式較偏向服務面向，從使用者的角度定義雲端運算。

[5] 潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 10。
[6] 黃重憲，淺談雲端運算，收錄於 http://www.cc.ntu.edu.tw/chinese/epaper/0008/20090320_8008.htm。最後瀏覽日期，2011 年 10 月 8 日。
[7] 陳瀅、王慶波、金淳、趙陽、何樂、鄒志樂、吳玉會、楊林等著，雲端策略：雲端運算與虛擬化技術，初版五刷，天下雜誌股份有限公司，2010 年 12 月，頁 26 以下。

	管理那些支援雲端運算之基礎設施[8]。	
Whatis.com	一種透過網路連接以獲取軟體以及服務的運算模式，讓使用者可獲得有如使用超級電腦的體驗。	此種定義方式較偏向大量運算之面向，然網格運算與分散式運算皆可實現大量運算。
美國加州大學柏克萊分校所提出之報告	在網路上提供各種應用的服務，以及提供這些服務的軟硬體。	此種定義方式最廣也最籠統，未將雲端運算的特色指出。
Salesforce.com	一種優良的業務運行模式，在此模式中，使用者的應用程式在共通的資料中心運行，用戶只需透過登入和個人化設定，就可以使用這些資料中心的應用程式。	此種定義方式較偏向「資源共享」的服務面向，但對於雲端運算中快速運算的特色未有提及。
IBM	一種分享網路資訊服務的方式，使用者看到的只有服務本身，不用關心相關基礎的建置。	此種定義方式較偏向服務面向，從使用者的角度定義雲端運算，然較維基百科之定義更為抽象。
Gartner.com	一種將大量 IT[9]資源透過網路向多數使用者提供「服務」的運算模式[10]。	此種定義方式不僅由服務面向出發，亦有兼顧雲端運算中「大量運算」以及「透過網路提供」等特色。

[8] http://zh.wikipedia.org/wiki/%E9%9B%B2%E7%AB%AF%E9%81%8B%E7%AE%97，最後瀏覽日期，2011 年 11 月 11 日。

[9] Information Technology，中譯「資訊技術」或「資訊科技」。

[10] Gartner.com，Gartner Say's Cloud Computing Will Be As Influential As E-business，收錄於 http://www.gartner.com/it/page.jsp?id=707508，最後瀏覽日期，2011 年 11 月 11 日。

然而，過多定義反而使大眾對雲端運算失去共識[11]，又過廣的定義已包山包海，似已失去討論價值。惟在此不管採用何種定義，被廣為討論的雲端運算可謂是一種客製化產物，討論的重點應放置在使用者身上，從使用者的角度出發來定義雲端運算。從而，將雲端運算定義為「建立於『資源節省，共用共享』的概念上，令使用者捨棄既有使用習慣，改為以低成本換得高運算需求的服務，同時也會提升軟硬體資源利用效率的運算方式[12]」，似才具有討論價值。

至於雲端運算是否為「舊瓶裝新酒」的問題[13]，由於在此雲端運算所強調的重點在「使用者使用習慣的改變」，從而縱使這種運算方式是在「伺服器與客戶端」模式出現時即存在的運算方式，仍無法改變此名詞提出後造成全世界使用者使用習慣改變的事實。而此種社會現象會導致舊有的行為於法律上的重要性變更，或一些本來非犯罪之行為入罪化，並迫使我們對於現行法律的檢討。從而，在此應關注的重點應不在雲端運算本身是否係一新概念或僅係舊有概念，而是因其所造成的背後社會現象[14]。

第二項 雲端運算之基本原理

承襲自平行運算、分散式運算及網格運算的優點，並修正其缺點的雲端運算，基本原理當然會與「集體資源的集合」以及「高性能快速大量運算」有所雷同。又如前項所述，「雲端」就是指「網路」的意思，亦可初步聯想到雲端運算的思考基礎應與網際網路有關。綜合以上所述，不難聯想到雲端運算的思考基礎就是「利用網路由遠端伺服器對大量使用者進行問題的處理」這個結論。具體的運算流程為，由各使用者提出運算需求後，經由網路連接至遠端伺服器做運算處理，

---

[11] 亦有如百度提出「框架計算」此類「另立門戶」炒作之例，參王鵬，雲端運算的關鍵技術與應用實例，初版，佳魁資訊股份有限公司，2010 年 2 月，頁 1 之 5。

[12] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 3。

[13] 指雲端運算僅是商家所提出的一個噱頭，實際上了無新意，且係於「伺服器與客戶端」模式出現時即存在的運算方式的批評。

[14] 更有將雲端運算直接從使用模式的角度做定義，認為雲端運算是一種革新的 IT 運用模式。運用模式的主體是所有連接網路的實體，可以是人、設備或城市，客體就是 IT 本身，包含現在所接觸，以及將來會出現的各種資訊服務。參陳瀅、王慶波、金淳、趙陽、何樂、鄒志樂、吳玉會、楊林等著，雲端策略：雲端運算與虛擬化技術，初版五刷，天下雜誌股份有限公司，2010 年 12 月，頁 27。

再將處理結果利用網路傳回使用者方，令使用者享受結果，此結果可能是作為服務提供，亦可能是單純的運算需求。簡單來說，雲端運算的基本原理為「利用非本機或遠端伺服器(叢集[15])的分散式運算機，為網際網路使用者提供服務[16]的模型[17]。」

依照這種原理而操作所生的結果，因雲端服務提供者必須同時對於大量使用者提供服務，且使用者無需擁有太多資源即可使用雲端運算，故會導致軟硬體設備擴充、損壞以及維修等風險皆由雲端服務提供者負擔，同時多數資源皆由服務提供者擁有，並按使用者的需求來分配資源。據此，雲端運算不但能夠有效提升對軟硬體資源的利用效率，並使得非科學、數學、天文專業人士之極大數量使用者皆得透過雲端享受高效能運算所帶來的便利，亦間接提升使用者的工作效率。再者，因雲端運算著重於「對使用者端的服務」，使用者對於 IT 技術的理解程度縱使不高亦得使用，從而雲端運算模式中使用者無需了解如伺服器的位址、內部如何運作等問題，僅須透過高速網際網路即可享有並使用各種資源[18]。

綜合以上，於雲端運算興起的時代，使用者不再像過去一般必須要具備一定程度的 IT 相關知識始得使用相關產品，同時使用者亦無庸伴隨科技的進步不斷快速更新自己的硬體設備而導致大量金錢花費。惟於此時代中，使用者對於網際網路的依賴程度遽增，網際網路與人類的關聯已漸趨近於水、空氣、陽光之重要性，此種使用習慣明顯與雲端運算出現前的舊時代大相逕庭，誠可謂使用者使用習慣已有極大改變。

第三節　雲端運算之時代意義

於釐清雲端運算的定義重點在於「使用者使用習慣的改變」後，本節即從歷

---

[15] 叢集(Computer Cluster)是一硬體架構，指聯結複數電腦，視為一高運算的電腦運作的架構。雲端運算服務端中雲端主機的硬體架構亦不乏採叢集架構者。

[16] 含運算、儲存、軟硬體等服務。

[17] 在此係指「利用非本機之分散式運算機服務」或「利用遠端伺服器(叢集)之分散式運算機服務」之意，參王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 2。

[18] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 3。

史的角度探討，為何早於伺服器與客戶端模式出現時即存在的雲端運算模式，遲至今日始改變使用者的使用習慣，進而躍升成為資訊新時代的寵兒？究竟係如電信公司所推出的廣告所述「科技始終來自於人性」一般，是社會上使用者的需求帶動科技發展，抑或如 Microsoft[19]公司所出版的作業系統[20]windows 每次改版時就令大多數使用者必須改變使用方式一樣，是科技發展本身主導著社會上使用者的使用習慣？同時，本節也從時代角度探討上節的結論–究竟雲端運算造成使用者習慣改變的影響範圍有多大？被稱為「使用者」的範圍極廣，究竟受影響者，是僅限於廣大的社會大眾，抑或是就連軟硬體設備供應商本身的商業習慣亦受到了改變？

於探討方向部分，本文擬將雲端運算的來龍去脈依照「過去」及「未來」做區分，計分為「雲端運算之興起」及「雲端運算之發展」二角度分別探討，於雲端運算興起部分，預計藉由雲端運算出現的歷史，探討為何雲端運算遲至今日始成為資訊時代的指標；於雲端運算發展部分，預計藉由分析雲端運算目前所包含的類型，探討其影響的範圍。

第一項 雲端運算之興起

於雲端運算興起的部分，因是著重於雲端運算的「過去」，故首先即須了解整體運算時代發展的脈絡。然而，運算時代發展史與本文關聯較淺，從而以簡史方式表示，提出各時代的特色，達到令人大致了解的程度即可。再者即係分別對各種大力影響雲端運算的誕生，以及同時與雲端運算性質類似的運算方式[21]作介紹，以收完整認識雲端運算之效。從而，以下各款分別就運算時代發展簡史、平行運算、分散式運算、網格運算依序介紹[22]。

---

[19] 或簡稱「微軟」。

[20] Operator System，或簡稱「OS」。

[21] 計有平行運算、分散式運算、網格運算三類。

[22] 以下介紹的敘述以及所採用年代區分的方式，參考自中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月，頁 25 以下。

第一款 運算時代發展沿革

在1970年代,一般大眾對操作電腦完成生活周遭的工作仍為陌生亦不普遍。當時只有在大學、大型企業研究中心才會設置大型主機,並連結著極為大量的終端機。然而這些終端機卻未具備資料處理的能力,僅是由螢幕及鍵盤等構成的一種單純操作裝置而已。同時亦僅有少數科技菁英得以使用終端機連上大型主機,進而享用計算資源。從而,此時期的電腦運用方式,大多以一台大型主機為主,而使多數使用者同時連線,共享資源。

在 1980 年代,以蘋果電腦推出的 Macintosh[23]與 IBM 推出的 PC 為首,個人電腦開始普及。伴隨個人電腦的普及,計算方式亦從一台主機多人共用的中央處理方式,演變為家家戶戶各自有一台電腦的分散處理方式。畢竟使用者皆擁有個人電腦,即無庸如 70 年代般共享大型主機集中處理業務,從而業務處理方式轉移至使用各自所擁有之電腦處理。據此,此時期電腦的使用者從少數科技菁英擴展至多數的社會大眾,電腦的普及化也造成了社會開始對自動、高速運算的追求。

在 1990 年代,由 Internet 所構築的全球資訊網快速普及,個人電腦中的資訊,可直接透過網際網路做交換或取得,大大增加了電腦的泛用性與便利性。同時電腦的性能如處理能力及記憶容量相較以往也有著大幅度的提升。從而,此時代的電腦以及網路已非稀少資源,反而較類似如電力、自來水、瓦斯般的民生必需品。

在 21 世紀至今,因網際網路的極度發達,所使用的資訊量大幅提升,人們即開始需求更加快速、更加便利的資訊科技生活,諸如「忘記將資料儲存在他處」、「所使用軟體版本的不一致」、「單機運算速度的極限」等問題日漸浮現,從而開始雲端運算時代的拓展。

第二款 平行運算(Parallel Computing)

[23] 或簡稱「Mac」。

一、　何謂平行運算

所謂平行運算，是因人們追求更快的運算速度，並將多個電腦並聯，從而獲得更快計算速度的運算方法[24]。平行運算的基礎思想即是使用複數伺服器協同解決同一運算需求，並於多台電腦上於同一時間內進行分區操作，以達時間與空間上的「平行」。所謂分區操作，是指將同一問題劃分為若干部分，再個別將小部分分配予各獨立的處理器處理，於理想情況下，若同一問題被分成 N 部分，則解決該問題所花費的時間則係使用單機解決問題之 1/N。各個獨立的處理器，得為一台多核心電腦中央處理器[25]中的各個核心，亦得為以某種方式連接的電腦群[26]。

二、　對雲端運算之影響

連結多數伺服器處理同一問題的平行運算，其「分工合作」的核心概念為雲端運算的發展提供「大量、快速運算」此一基本訴求的出路思考，若無平行運算提供此種思維，恐怕雲端時代的來臨還會更加延緩[27]，故而認為平行運算是雲端運算發展的基石亦不為過。

第三款 分散式運算(Distributed Computing)

一、　何謂分散式運算

分散式運算的基礎思考與平行運算類似，亦是將同一大型問題分解為複數部分，其後將小部分給許多遠端電腦同時分擔處理，最後將處理結果集中綜合後，

---

[24] 王鵬，雲端運算的關鍵技術與應用實例，初版，佳魁資訊股份有限公司，2010 年 2 月，頁 1 之 2 以下。

[25] Central Processing Unit，或簡稱「CPU」。

[26] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 2。

[27] 此種核心概念亦影響至多核心 CPU 之發展。

得出問題結果的運算方式[28]。其特色為利用網際網路連接極大數量的電腦[29]，並妥適利用該些電腦閒置時的運算能力，不但使各電腦的功能物盡其用，所集合的運算量亦十分驚人，一般大型運算不在話下，甚至得以此分析來自外太空的電信號、探索外星球的智慧生命體等運算，最著名的例子莫過於 1999 年啟動的「SETI@home 計畫[30]」[31]。

二、 與平行運算之關聯

分散式運算與平行運算的基礎思考皆是「將大工作化為小工作」，將較複雜的運算需求切割為多數小部分，再交由多個處理器執行運算。惟兩者的區別在分散式運算所的各個運算部分皆為獨立，故其容許運算錯誤，並會將同一運算部分發交予多數個人電腦執行，最後驗證該些電腦執行的結果，以找到最精確的結果。然而，平行運算中，工作區與工作區間不但關係緊密，並會相互影響，所有工作區皆要求絕對正確，沒有任何浪費的分割，對運算準確性以及同步性的要求較高[32]。

三、 對雲端運算之影響

分散式運算不但具有同於平行運算般「大量、快速運算」的特色，其亦有倚賴網路連結多數個人電腦進行運算的特色，此種「利用網際網路」集合全世界使用者力量的思維，亦影響雲端運算的發想。

---

[28] 潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 36；王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 6 以下。

[29] 大約為一個或多個國家國民之個人電腦使用量，於歐美國家趨近半數使用者之電腦街加入分散式運算專案，參王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 6。

[30] 該計畫利用超過 500 萬名參與者的個人電腦的空閒時間進行分析無線電訊號的運算，以期能找出外星生物，參黃重憲，淺談雲端運算，收錄於 http://www.cc.ntu.edu.tw/chinese/epaper/0008/20090320_8008.htm。最後瀏覽日期，2011 年 10 月 8 日。

[31] 然亦有部分見解認為 SETI@home 計畫係屬網格運算之運用成果，參潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 38。

[32] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 7。

第四款 網格運算(Grid Computing)

一、 何謂網格運算

網格運算與雲端運算相同，是承襲自分散式運算的核心理念[33]，並伴隨著網際網路的進步而蓬勃發展，目前為止仍屬熱門的運算模式。網格運算的原理是利用網際網路將分散於不同地理位置的電腦閒置資源組織成一座「虛擬超級電腦」，並以此解決縱使以超級電腦皆難以解決的運算需求[34]。每一個參與網格運算的電腦皆得以一個「網點」為喻，將各個網點連接，即成為一片網格，於網格中得使用的運算資源，遠比單機電腦大量，並且運算速度亦遠高於超級電腦。

二、 與分散式運算之關聯

綜合對於分散式運算與網格運算的敘述，似可認網格運算與分散式運算極為相似，甚至欲一一區分各個系統係網格運算或分散式運算亦可能出現困難。大體而言，網格運算與分散式運算相同之處在於，網格運算係以分散式運算「將大工作分為小工作，並利用網際網路分配予各個電腦執行」的思考核心為基礎，並更進一步利用網際網路的廣泛分布性與資源分享的互助精神，活用參加網格運算電腦的閒置空間，進行大量複雜的運算模式。而相異之處在於，分散式運算須依靠運算方對於參加者的電腦做資源分配，參加者無法隨心所欲的決定是否參加，整體運算模式為靜態；惟網格運算則係將一切資源管理、資源分配皆交由網路以及使用者本身決定，使用者對於自己具最高自主管理權的資料得選擇是否分享、甚至得決定是否退出或加入網格運算，此使得網格使用的資源因而發生相應的變化，整體運算模式為動態[35]。同時，分散式運算面臨各個參加運算之電腦使用不同系統或硬體設備不均衡時如何溝通的問題，但網格運算則可將這些不同等級或不同

[33] 潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 38。
[34] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 8。
[35] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 10。

作業系統的電腦透過通訊協定互相溝通[36]。

三、 對雲端運算之影響

網格運算對於雲端運算最大的影響在於「由網路接受運算請求」之點[37]。惟網格運算的特色注重在統整各種不同類型電腦以順利進行大量運算，而雲端運算則注重在以遠端大型伺服器透過網路提供需求端大量運算的服務。並且，雲端運算更偏向使用者的服務角度，也因其沒有統整不同類型電腦始能實現大量運算的問題，於使用上較網格運算便利[38]。

第二項 雲端運算之發展

於雲端運算發展的部分，則係著重於雲端運算的「未來」面向，故在此著重者即為「雲端運算的主流發展方向」。蓋雲端運算依照國外知名分析公司 Gartner 的分類方式，又可細分為「雲端技術」與「雲端服務」，前者較著重在利用虛擬化以及自動化等技術來創造和普及電腦中的各種運算資源；而後者則專注在於藉由網路連線從遠端取得服務[39]。此種分類方式因清楚劃分雲端運算中對於一般民眾的服務面向，以及適合較專業資訊人的技術面向，二者於取向上可謂大相逕庭，想必其發展的方向亦有不同。若於討論雲端運算的發展時採用此種分類方式，即可清楚劃分其取向，而不至於互相混淆。從而，本文在討論雲端運算的發展時，即引用此種分類方式，將重點聚焦於雲端服務及雲端技術上，並於以下分別探

---

[36] 潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 38。

[37] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 12-2 之 13。

[38] 雖有認為網格運算的處理對象是複雜不易運算的大任務，適用對象為科學研究人員，而雲端運算之處理對象為簡單卻龐大的小任務，適用對象為一般大眾者，然此見解無法解釋 P2P 亦為網格運算之一環，或僅得將其作為例外。參潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 38；王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 9；鄭曄祺，處罰網路犯罪理論基礎之研究–以 P2P 為例，國立台北大學法學系研究所碩士論文，2007 年 6 月，頁 22。

[39] Jon Brodkin，Cloud computing hype spurs confusion, Gartner says，收錄於 http://www.computerworld.com/s/article/9115904/Cloud_computing_hype_spurs_confusion_Gartner_says。最後瀏覽日期，2011 年 10 月 8 日。

討。

第一款 雲端服務

於雲端服務部分，因雲端服務是以使用者的角度出發，探討藉由雲端運算得給予使用者何種服務。故若要將雲端運算的體系做區分，似乎也應從使用者的角度出發，參考其於一般單機電腦使用方式，進而分為「所使用的軟體」、「提供軟體發展的平台」、「基礎硬體設備」等三類。據此，以下即以此三方向為主，於以下分別析述。

一、 軟體即服務(Software as a Service，簡稱 SaaS)

所謂軟體即服務，是指透過網際網路，軟體供應業者向使用者提供軟體的形式。軟體供應業者將軟體統一部屬於自己的伺服器上，使用者得依自己需求向軟體供應業者提出申請，申請完畢後則根據所訂的軟體功能、時間長短支付相應費用，且軟體供應業者即會提供相應的服務[40]。使用者無須在主機內安裝全部或部分軟體，亦無須升級自家電腦以達該軟體的使用限制，只要打開瀏覽器或其他程式即可使用。並且，使用者亦無須擔心軟體更新與維護、或與其他使用者的版本相異等問題，蓋軟體的更新與維護責任皆交由軟體供應業者負擔。同時，軟體供應業者亦無須煩惱盜版及販售通路問題，可謂係使用者與軟體供應業者雙贏的局面。最後，雖然軟體同時面對多個用戶，但每個用戶感覺都是獨自享有服務[41]。現存的軟體即服務如 Twitter、Gmail、Hotmail、Google maps 等[42]。

二、 平台即服務(Platform as a Service，簡稱 PaaS)

---

[40] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 2 之 13。

[41] 陳瀅、王慶波、金淳、趙陽、何樂、鄒志樂、吳玉會、楊林等著，雲端策略：雲端運算與虛擬化技術，初版五刷，天下雜誌股份有限公司，2010 年 12 月，頁 88 至 89。

[42] 中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月，頁 15。

所謂平台即服務，係指平台提供業者利用網際網路提供開發環境平台[43]予使用者，使使用者得於其基礎架構上開發程式，並透過網際網路將所開發的程式給予他人使用[44]。使用者若是一個研發團隊時，此一研發團隊的各個成員因應用程式的開發都是基於同一個平台，故無須使用同一種作業系統進行開發，又平台本身即在雲端上，故其亦無須於同一定點進行研發，僅需連上平台提供者，即得做開發、測試、維護等工作[45]。從而軟體開發時所面臨的開發環境整合問題及開發人員聯絡問題即大幅解決，並且亦使使用者所開發的軟體能夠廣為人知，增加該軟體的能見度。現存的平台即服務如 Force.com、Google App Engine、Windows Azure 等[46]。

三、 基礎設施即服務(Infrastructure as a Service，簡稱 IaaS)

所謂基礎設施即服務，係指基礎設施提供業者提供，使使用者得以使用，以獲得更高水準的硬體設備[47]。使用者無須耗費大量金錢購買昂貴的硬體設備，即得透過網際網路使用大型企業級的硬體水準，並且其亦無須擔心硬體設備遭淘汰或損壞等問題。基礎設施即服務對於中小企業的使用者而言，係一節省成本輸出的絕佳方案，對於一般使用者而言，亦係防止其保存的資料因為硬碟損壞[48]、電腦中毒或其他意外事件而損失的良好保險。現存的基礎設施即服務如 Amazon EC2、IBM Blue Cloud、Sun Grid 等[49]。

---

[43] 包含開發所需的主機與作業系統，參潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 14。

[44] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 16。

[45] 陳瀅、王慶波、金萍、趙陽、何樂、鄒志樂、吳玉會、楊林等著，雲端策略：雲端運算與虛擬化技術，初版五刷，天下雜誌股份有限公司，2010 年 12 月，頁 88。

[46] 中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月，頁 15。

[47] 中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月，頁 9。

[48] 就租用網路硬碟儲存部分，亦有認為應將儲存空間獨立出來成為一獨立的層級–「儲存空間即服務(Storage as a service，或簡稱 STaaS)」，參潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 14。

[49] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 11。

第二款 雲端技術

於雲端技術部分，所強調者係由系統屬性及設計思想角度出發，說明軟硬體資源於雲端運算中所發揮的功能。雖自此些技術觀之，其更新與發展方向亦有可能影響未來雲端服務的型態，惟技術面向已與使用者關聯甚小，於社會上幾近無法造成影響。從而在此僅大略提及自雲端技術角度出發，將雲端運算本身所分成四部分–實體資源、虛擬化資源、服務管理中介軟體、服務介面的分類方式[50]，並不多加贅述其內容以及特色。

第三項 綜合分析

從雲端運算的興起可以得知，雲端運算造成使用者使用習慣的改變，並非單一要素影響，亦非一蹴即成。原先僅係為了進行更大型計算而構思的平行運算，伴隨著網際網路的發展以及如分散式運算、網格運算等概念的洗禮，始真正打著雲端運算的名推出於民間，並造成一股熱潮。雲端運算定義中的三大要素–「大量、快速運算」、「透過網際網路運算」、「將運算作為服務[51]」，其中大量、快速運算是繼承自平行運算以及分散式運算，而透過網際網路運算則是繼承自分散式運算及網格運算。然而，尚且不論平行運算時期網際網路之使用尚未發達，無論是分散式運算或網格運算皆未如雲端運算般造成使用者使用習慣改變，其中原因即是雲端運算的第三個要素–「服務」。縱使網格運算有借用使用者的電腦作運算，並且使用者有可能因此得到一些好處[52]，但此種好處並非即等於「服務」。所謂服務，必須是從使用者角度出發，思考使用者的需求並設法排除技術上的困難，並且因使用者的反應而改進。雲端運算架構中大幅降低使用者對於 IT 相關知識以及硬體設備需求，並且為使用者排除軟硬體版本差異以及必須攜帶主機或資料始得使用的不便利，從而始能令大量使用者改變其使用習慣。同時，因大量使用者

[50] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 12 以下。
[51] 在此所表彰之意義為「從使用者的角度出發來定義雲端運算」，使用者在雲端運算中佔有非常重要的地位。
[52] 如使用 P2P 軟體下載資料，使用者提供自己電腦內之資源。

使用習慣的改變，始會凸顯社會中本不可能實現、無重要性、或個案過少而被忽略的一些行為，並使得其有討論價值。

又，從雲端運算的發展亦可得知，雲端運算中包含了雲端服務以及雲端技術兩大分類，其中雲端服務的內容又可分為普遍一般大眾較常接觸到的軟體即服務，以及通常是企業等的程式開發者較容易接觸到的平台即服務，最後是不管是企業或一般大眾都可能接觸到基礎設施即服務。就雲端服務而言，所影響的範圍已不僅限於較專業的資訊工程師於建構程式時的使用行為，就連一般大眾都有可能在購買軟體以及儲存資料、更新電腦主機等日常使用行為因為雲端運算而有大幅度的改變。可見雲端運算影響的範圍甚廣，於日後的發展上，除非有更新的計算概念取代，否則影響範圍應只會日漸擴大而不會日漸縮小。

綜上所述，雲端運算的興起與發展，不僅表彰網際網路對於人類的重要性日益增加，亦反映出人類對 IT 相關知識以及硬體設備的多寡，與得以享受的服務逐漸不成正比，同時也使得此種利用一條條纜線所建構，連接人與人間的虛擬空間，更具研究討論的價值。

第四節　改變社會之雲端運算

於釐清雲端運算的定義以及了解雲端運算的「前世今生」後，重點仍須回歸至雲端運算的特色為何，以及雲端運算對社會的影響。雲端運算，或者更精確地說，雲端服務究竟有何種魅力，以至於劇烈改變絕大多數使用者的使用習慣？又大多數使用者改變使用習慣後，對於人類社會究竟激起何種波瀾，以致於法律學上有提及並研究的價值？蓋使用者會受雲端運算影響的理由，不外乎係屈服於其特色之下。從而，以下及先行分析雲端運算的特色，其後始討論對社會的影響。

第一項 雲端運算之特色

雲端運算與傳統電腦使用模式相較，係一截然不同的運算模式，其亦具有許多特色，令使用者拋棄舊有使用模式而進入雲端時代，同時也是使社會上出現新

法律問題的契機。其中從「使社會上出現重大改變」的角度出發，並較具重要性的特色有「依需求選擇服務」、「雲端硬體無限擴充」、「資訊安全性高」、「使用者專業需求低」、「資料及軟體使用便利性」、「高運算儲存能力」等特色，於以下分別介紹，並且在第二項對社會之影響中做連結。

一、 依需求選擇服務

因雲端時代中，雲端伺服器方擁有極大的軟硬體資源，並以按一定規則的方式分配給各個使用者。從而不同於舊時代購買軟體或硬體皆要受限於製造商提供的幾種規格，於雲端運算時代，使用者得以依喜好定制相應的服務及資源，並僅要將其需求提出於雲端，即可享受量身訂作的服務[53]。易言之，時代從「使用者必須一定程度的配合提供者」的時代變更為「提供者必須完全配合使用者」的時代。

二、 雲端硬體無限擴充

既然雲端運算時代中，雲端伺服器方擁有較大的軟硬體資源，故軟硬體的擴充也只是一種「資源分配的置換」。並且，雲端伺服器方的資源不但是全球性的，並會持續更新，且可以連結多台處理器為依使用者服務，可謂有無限擴充的可能性。據此，舊時代的個人電腦有所謂「淘汰」的概念，然於雲端運算中硬體設備係得隨時無限制擴充，以提升雲端處理能力，同時亦增加硬體使用的靈活度。

三、 資訊安全性高

同時，雲端時代中使用者的資料皆存取於雲端中，且各種應用程式亦於雲端執行，故資訊毀損滅失的風險皆會由伺服器方負擔。為防止使用者的資訊毀損滅失，伺服器方往往會採取一些安全措施。首先，運算中若出現錯誤，會透過相應的系統排除，保證運算正常執行，使用者端亦可於任意點進行恢復。同時，資料

[53] 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月，頁 3 之 7。

亦會被複製至多個伺服器備份，縱伺服器端遭意外刪除或硬體損壞，皆不因此使資料滅失。此種集中管理的安全措施對資料的安全性，相較於個人電腦時代中每個使用者必須自己為自己電腦中的資料毀損滅失負責，進而自行「構思」安全措施來的高。據此，雲端運算時代中資訊的安全性是較舊時代高的。

四、　使用者專業需求低

既然雲端運算是從使用者的角度出發，並且一般使用者大多不具備 IT 相關知識。故雲端伺服器方即會盡量降低使用者對 IT 相關知識的需求。據此，使用者在使用雲端服務時，所需的 IT 相關知識以及硬體裝置，相較個人電腦時代使用各種軟體之門檻來說降低許多。從而，使用者就算對 IT 知識極度缺乏，過去似乎只能託較懂得電腦的使用者幫忙選擇材料組裝主機以及安裝程式，然而雲端時代來臨後，使用者僅需要一台有螢幕以及上網功能的小型輸入輸出裝置即可使用如過去已安裝完畢電腦的功能。

五、　資料及軟體使用便利性

在雲端時代中，因使用者將資料及軟體皆儲存於雲端，故於需要時直接連接至雲端使用即可，使用者端所使用的硬體為何皆無影響。當使用者使用的硬體設備故障時，僅需換個硬體即得繼續作業，從而關注的重點已從硬體設備(何人所有的電腦)演變為使用權限(何人所有的使用權)。

六、　高運算儲存能力

由於雲端伺服器即係由集合多數伺服器叢集而組成，從而雲端伺服器所擁有的運算儲存能力遠大於舊時代個人電腦或超級電腦。且雲端伺服器得隨時無限制擴充，其運算及儲存能力的上限可謂無限大，亦即具有無限儲存空間以及無限運算速度。據此，相較於單機電腦，雲端伺服器所擁有的運算及儲存能力是極高的。

第二項 對社會之影響

於雲端運算對社會的影響部分，就前述雲端運算的基礎理念與雲端運算的特色綜合觀察，對現今社會的使用者最主要的影響應可歸納為二–「IT 資源之共享」以及「資訊之共同管理」。從而，以下即就 IT 資源共享及資訊共同管理為分類，並於內就前項所述的特色在社會上所造成的影響作分析。

第一款 IT 資源之共享

雲端運算除承襲了分散式運算以及網格運算「集合眾人力量尋求更高速的運算」的優點，具有「高運算儲存能力」的特色外，仍更進一步的加入了為使用者服務的性質，要讓世界上所有使用者，皆得享有如超級電腦般的運算效能。據此，服務提供者為了打造超級電腦般的規格，將世界上大部分的軟硬體資源集中起來，並且為了讓世界上所有使用者使用這台電腦而進行管理分配。從而雲端運算模式中，無論硬體設備至軟體，皆係由所有使用者所共享。於基礎設備部分，遠端伺服器叢集必須同時供應大量使用者使用，並且每個使用者皆有使用期限以及使用程度的限制；於開發平台部分亦如是；更毋庸論及表彰軟體即服務的軟體供應商。此種一份資源多數使用者共用的模式，對使用者已造成了一定程度的影響。首先，使用者無需購買大量硬體裝置，畢竟使用者已有著使用「雲端主機」這台超級電腦的資格，即無須再花大錢購置如舊時代電腦般的硬體設備，僅需擁有一個得連上網際網路的瀏覽器即可進行雲端運算，降低電腦裝置擁有的成本。同時，於軟體的使用上，使用者所使用的也非如舊時代是「屬於自己的一套軟體」，而是與其他使用者共用一套軟體。雖使用者失去了擁有實體光碟或磁碟片的感覺，然而於軟體即服務的架構下，不管是軟體更新或資料的同步[54]皆不用購買或另外下載更新檔，即可享受最新版本，並且因為雲端運算「依需求選擇服務」的特色，可以節省購買經費並去除自己完全用不到的功能。同時，對於軟體供應商而言更新資料或修正缺失亦較容易，可謂一舉兩得。最後，由於全世界共用少數幾台雲端電腦，使用者只要連上網際網路後，輸入自己的帳號密碼即得使用電腦，至於係使用何人的硬體設備皆不影響使用的效能。

[54] 如防毒軟體偵測出新病毒，必須更新病毒資料庫等。

第二款 資訊之共同管理

由於 IT 資源的共享，雲端運算使得使用者將軟體甚至硬體設備都交由服務提供業者維護保存並做管理。反面而言，服務提供業者掌握絕大多數人的資訊。無論係虛擬硬碟中所保管的資料、社交軟體如 FACEBOOK 的個人資訊，甚至連防毒軟體的使用偏好皆在供應商掌握的中。此種資訊共同管理的現象在提供予使用者莫大方便性外，同時亦造成將雞蛋置放於同一籃中的安全性疑慮。首先，就資料安全性而言，雖因雲端運算中「資料及軟體使用便利性」的特色，使用者皆將資料存取於雲端主機中，故僅需得連上網際網路，即得同步共用所有資料，無須於工作場所、住家、學校等地頻繁複製、備份正在處理或已經處理的檔案及相關工作資料，故不再依賴特定電腦存取及處理資料，然而也因為資料儲存於雲端主機中，只要雲端主機遭到毀損，則所有資料皆會遺失。縱使如雲端運算中「資訊安全性高」的特色，將資料備份於不同伺服器中，亦僅能降低資料滅失風險，並無法完全避免。同理，若雲端主機遭駭客侵入，駭客只要取得管理者的金鑰，極度大量的資料皆會暴露於駭客眼中，完全省去駭客冒著侵入不同電腦的風險。同時，也因為使用者皆將資料與作業系統儲存於雲端主機中，而使用者將透過網際網路使用該些資料以及系統，無形間使用者對網際網路的依賴性將會大幅增加，網際網路的重要性不亞於陽光、水、空氣等維持生存的要素。若網際網路功能停擺或受到干擾，即會影響社會運作甚大，並且除修復網際網路外別無他法。

第五節　本文見解–現行法之困境

於雲端運算時代下，由於雲端運算(雲端科技及雲端服務)概念已被大量的運用，導致於大多數使用者 IT 資源的共享以及資訊的共同管理，同時也因此產生了不少現行刑法妨害電腦使用罪章於適用上的問題，並於以下分別討論。

首先，由於 IT 資源的共享，導致硬體設備僅有一組或少數的數組，今同一(大)台電腦主機的規格與性能可謂係所有使用者的電腦，同時亦因每個使用者原則上皆僅得以自己的帳號密碼獲得該電腦的使用權，此時該雲端電腦亦可謂並非所有

使用者的電腦。此種電腦概念的革新會衝擊到現行刑法妨害電腦使用罪章中的「他人電腦」概念，畢竟就使用的軟硬體部分，是由所有使用者共用，然而所使用之權利範圍以及期限等則是依照個人需求而有不同，此時是否仍要強調行為客體必須要是「他人電腦」，以及如何定義「他人電腦」則有受到質疑的空間。

更進一步而言，在定義何謂「他人電腦」之前，亦存在著如何定義「電腦」，以及是否必須將妨害電腦使用罪章的「妨害」對象限定在「電腦」上？就如何定義電腦部分，因雲端運算中的軟硬體資源遍部各地，可謂係以網際網路連接各個零件而臨時湊成供使用者使用。並且雲端運算特色之一即是「使用者專業需求低」，使用者完全無法弄清楚那朵雲內部是如何運作，此時雲端電腦對於一般大眾而言就如同中國神話中的龍一般，只能被迫的已現有的動物(電腦概念)來想像牠的樣貌，但實際出現了一個很像龍(雲端電腦)的動物(科技產物)，要其判斷是否為龍(雲端電腦)時，卻因從沒看過龍而無法判斷。如此是否能如本罪章的立法理由[55]一般，將電腦概念「不予定義」，委由社會來判斷即有疑義。另，就是否須將妨害電腦使用罪章的「妨害」對象限定在「電腦」上的部分，從雲端運算的興起與發展中可以發現，電腦硬體設備已不如以往人手一機，反而漸有集中管理的趨勢，每個使用者則是以登入自己帳號的方式來區分使用的範圍以及權限，從而關注的重點已從「誰的電腦」漸變為如 1970 年代般的「誰的使用權」。又，因科技的進步，許多家電以及其他設備等不但備有微電腦，亦有標榜使用雲端技術能夠統一由使用者的雲端帳號來設定及操控，此時這個「使用權」可能不只出現在電腦上，故而若將行為客體緊咬在「電腦」範圍中，又不想將電腦的範圍過度擴大時，很可能會在解釋上產生自相矛盾的情形。

再者，就如本文「資訊之共同管理」該款內所述，絕大多數使用者的資訊係由管理者共同管理。然而一來對於此種共同管理的資訊團體作破壞或侵入遠比對多數個人電腦作侵入或內藏資訊之破壞來的容易，尤其是當駭客或快客獲得了管理者權限時，侵害所有資訊的速度既快又不易察覺。二來所造成的侵害亦遠比單

[55] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 358 條之修正說明第四點：「為因應不斷成長發展的電腦科技相關技術，所以不宜就「電腦」、「電腦系統」及「網路」等名詞予以定義。」

機時代單獨對他人電腦內的資訊做破壞或侵入他人電腦要大，並且受害者遍布全世界。三來資料備份的份數越多，被侵入者查閱或取得的可能性越大，對於重要機密的存取亦屬不利。雖我國已有訂立個人資料保護法，然該法僅限制「個人資料」的保護，並且較偏向公務機關或其他可能保有個人資料團體的處罰，對於蓄意查看或破壞資訊者似乎只能以刑法處理。從而此類行為是否是一種類似公共危險的犯罪型態即有探討空間，又配合現行法對於公務機關的電腦有加重處罰的條文，是否可對此種行為以公共危險犯的思考方向來做思考亦是問題所在。

此外，雖然台灣的資訊安全現況就微軟於 2010 年之調查發現是全球中算較危險的地區，亦即台灣的微軟用戶受到惡意程式攻擊的比率遠高於世界平均值[56]。然而，在進入雲端時代後，在資訊共同管理下，管理者對於資訊安全的要求，以及對抗惡意程式的專業性上都遠高於一般使用者，即使受到惡意程式的攻擊，要因此產生損害的機率可謂非常低。並且由於 IT 資源的共享之故，惡意程式發布者也可能因惡意程式的發布而使自己同樣受到損害。此時似乎可以預見惡意程式攻擊會日漸集中甚至可能消逝，而刑法妨害電腦使用罪章中第 362 條對於製作惡意程式的處罰必要性是否仍存在？是否符合刑法最後手段性，或是以行政罰處罰即可等問題也會浮出。同時，於刑度的部分是否符合罪刑相當原則，亦是值得思考之處。

最後也是最根本的問題，雲端運算即是網路運算，雲端運算時代的來臨無疑是象徵了「網路主宰電腦」的使用習慣漸漸的支配了整個社會。就此種現象的發展，也足以讓人思考對於電腦犯罪的規制，究竟是為了保護什麼？易言之，現行妨害電腦使用罪章的立法理由中所述的保護法益極為籠統，僅泛泛的說是「電腦使用的安全」，惟自雲端運算的發展中即會發現，世界資訊科技使用關係的重點已從「電腦」移轉到「網路」，而在此立法者所主張的保護法益是否能夠涵蓋網路的部分？以電腦為主的使用關係縱使與以網路為主的使用關係有一定程度的重疊，但二者畢竟是源自於不同出發點，思考的脈絡以及邏輯絕不相同，若未釐清電腦犯罪的保護法益為何即貿然立法適用，即會在保護的重點不在電腦本身使

[56] 潘奕萍，圖說雲端運算，初版，書泉出版社，2011 年 9 月，頁 124。

用的時候，在規制上出現了許多不合理的現象，如對於應處罰的行為因限制行為態樣而無法規制，以及對於以行政罰處罰即足的行為卻施以重刑。而會造成此種結果，一部分即是立法者對於保護法益認定的模糊，另一部分則可能歸咎於資訊科技發展的快速及難以捉模，但縱使如此，面對具有此種特色的資訊科技該以何種態度因應，亦是維持規範遞續性的一大課題。

綜合以上，現行法可能因雲端運算時代的出現，不僅出現法律適用上之問題，以及該法律本身的存廢皆有再度被探討的必要。易言之，現行刑法妨害電腦使用罪章等相關規定，似缺少法條延遞持續的性質，而於雲端運算出現後，此種「遞續性」即遭到質疑，是否此問題在電腦犯罪相關條文訂立當時就已經存在，以致可以預見隨著科技進步，這些法律遲早會遇到適用上的困境。從而，似應對我國面對此類問題的處理態度認真做一番檢視。

第三章　電腦犯罪規範之爭議及發展

在對雲端運算做了一番探究後，接下來則需審視我國以及外國對於「電腦犯罪」的處理態度，並且試圖從我國以及外國的立法態度來找出造成我國法適用困境的原因，以協助後續章節找出解決困境的方法。在 1980 年代個人電腦普及後，伴隨而來的新興名詞之一即是電腦犯罪[57]。此一名詞不但造成了當時社會的轟動，也使得不少法律學者對此做出研究，其中於當時最具代表性，也影響我國學術及實務界最深遠的學者即為林山田氏[58]，故而本章則以第一節來對林氏所研究電腦犯罪的成果做整理，然而因為林氏電腦犯罪距今已久，亦有不少學者對其研究結果有所補充。故在整理的同時，本文也對林氏電腦犯罪所產生的一些問題做討論。

又，我國於民國 92 年公布增訂之第 36 章「妨害電腦使用罪」章，似乎是唯一於章名以及主要內容在規範「電腦犯罪」的一章，其也實質被實務界拿來處理不少與電腦有關的案子，與本文的研究可謂密不可分。故在評析完林氏電腦犯罪後，接著即要在第二節中交代該章的來龍去脈。以了解立法當時立法者的思維、罪章特色以及處罰重點，進而得知立法者所想要處罰的對象，是否即是第一節所述的「電腦犯罪」，抑或是另有所指。若是另有所指，則所指為何？又第一節所述的「電腦犯罪」於立法後如何處理？若不弄清楚立法者的真意，則再多的批評很可能只是雞同鴨講。又此罪章訂立當時，引起學術界異口同聲的大加撻伐，故於釐清立法者真意後，亦應重視學界對此的回應以及評析。

最後，因為中華民國刑法是繼受法，從而在探究我國法律之外，亦應參考外國法做比較，看看其他國家是怎麼處理電腦犯罪的問題。故於本章第三節，則試著從我國刑法繼受的對象，也就是德國及日本，以及我國訂立妨害電腦使用罪章

---

[57] 同時在 1990 年代後因網際網路普及，有學者提倡討論的範圍應從「電腦犯罪」縮減至「網路犯罪」，參李茂生，我國電腦網路犯罪的虛像與實相，刑事政策與犯罪研究論文集(四)，2001 年，法務部犯罪研究中心，頁 2。

[58] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 45 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 2 以下。

時所大量參考其法制的美國等國家來看該些國家對於電腦犯罪的處理規範以作為我國處理電腦犯罪的參考。

第一節　固有見解之檢討

於 1980 年代電腦普及化後，開始出現了電腦犯罪此一名詞，並引起法律學者們的一番研究，其中於當時最有影響力的當屬林山田氏[59]，不但做為當時多數學者的論理基礎，亦對實務界修訂電腦犯罪相關條文時有所參考[60]。然而，如同電腦發展般的快速，在短短的二十餘年間，伴隨著電腦犯罪相關條文以及妨害電腦使用罪章的增訂，出現了不同的聲音。從而，在討論妨害電腦使用罪章前，似乎應對我國學界中對於電腦犯罪的風風雨雨做點回顧。據此，本章的各節排列架構，則係以林山田氏的研究架構為本，並在回顧林氏架構後，就不同的聲音以及本文見解做補充，共分為電腦犯罪之定義以及電腦犯罪之類型二類。

第一項 電腦犯罪之定義

第一款 傳統見解

林山田氏將電腦犯罪定義約略分為三大類型–廣義說、狹義說以及折衷說[61]。廣義說者認為電腦犯罪是泛指「所有與電腦科技或電腦系統有關之犯罪」[62]，此

---

[59] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 45 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 2 以下。

[60] 如管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月；謝開平，電腦犯罪之研究—我國現行法之適用與修正草案之檢討，國立中興大學法律學研究所碩士論文，1995 年 7 月；房阿生、吳振村，電腦犯罪及防治方法之研究，司法週刊社印行，1989 年 9 月；廖有祿、李相臣，電腦犯罪：理論與實務，初版，五南出版社，2003 年；洪光煊，從電腦犯罪談未來刑法修正方向，刑事法雜誌第 32 卷第 3 期，1988 年 6 月；盧文祥，電腦犯罪之研究，憲政時代第 13 卷 4 期，1988 年 4 月。

[61] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 46 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 2 以下。

[62] Lampe, Die strafrechtliche Behandlung der sog. Computer-Kriminalität, GA 1975, S. 1 ff.，轉引自林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 46。

見解將「以電腦為犯罪工具的行為」以及「以電腦為犯罪目的的行為」都包含在電腦犯罪之範疇內；然而廣義說似有牽連過廣之疑義，故狹義說者將電腦犯罪限縮至「與電子資料處理有關之故意而違法之財產破壞行為」[63]，藉由將電腦犯罪之範圍侷限在財產犯罪，以控制電腦犯罪成立之範疇[64]。惟林氏認為狹義說將電腦犯罪侷限於財產犯罪顯屬過窄，雖財產犯罪是主要類型，然其他類型中亦有可能破壞財產法益以外之其他法益[65]，從而其採行折衷說，亦即電腦犯罪是指「行為人濫用電腦或使用足以侵害電腦硬體或軟體之行為，而形成之與電腦特質有關之犯罪」[66]，其重點強調在「與電腦特質有關[67]」，至於是何種犯罪，侵害何種法益，在所不問。

第二款 問題點之呈現及本文見解

在談電腦犯罪的定義該採何說，以及林氏見解所呈現的問題點之前，必須先確定的是「定義電腦犯罪的目的」為何。一般而言在討論問題前，通常都會藉定義將問題的範圍做明確的劃分，之後才是以類型化的方式，將問題依照特徵做區隔分別細部探討。而之所以要重視定義與分類，即是為就特定事實做溝通與意見整合的工作，以避免雞同鴨講的情形產生[68]。故若電腦犯罪一詞僅係劃分出「犯罪是否與電腦特質有關」的範圍，而於刑法上仍多將此類犯罪以既有條文論處[69]，則其應是對於刑法上既有的犯罪作類型化的工作，並無新的問題產生，此種名詞

---

[63] Sieber, Computerkriminalität und Strafrecht, 1977, S. 188.，轉引自林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 46。

[64] 該見解認為「以竄改、毀損，無權取得或無權利用電腦資料或設備之違法而派壞財產法益之財產犯罪，始屬電腦犯罪」，參林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 3。

[65] 林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 3。

[66] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 47；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 3。

[67] 而所謂的「與電腦特質有關」是以「違犯、追訴或審判須有電腦專業知識」為斷，參林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 48。

[68] 李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 174。然其認為此種定義的整合其實就是主觀意義的整合，重點應置於「為何特定主觀會成為共同主觀」的問題。

[69] 林山田氏認為其定義的電腦犯罪於刑法上的處罰，除增訂電腦操縱罪與電腦間諜罪外，皆得以既有刑法論處。參林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 60 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 7 以下。

的創造在討論上的意義實則不大[70]。反之，若定義電腦犯罪的目的在於「宣示其與一般犯罪需分開處理的獨特性」，使其具有獨立於其他各罪而處罰的可能性，此定義於討論上始有意義[71]。從而有見解認為，若要將某類行為犯罪化，則應考慮行為類型以及法益的範圍，若定義本身不限定法益範疇，則有可能造成刑法的過剩規範[72]。同時亦認為林氏所採的電腦犯罪定義是犯罪學上的定義[73]，而犯罪學與刑法的關係中，犯罪學較容易著眼於較嚴重的犯罪，且會為了企圖根絕對社會有害的行為而將處罰範圍擴張[74]，並不適合做為刑法上的定義。

綜上，本文認為若要為電腦犯罪下一個定義，則應扣緊保護法益的範圍，且保護法益須與電腦的特質密切相關，以及不同於刑法分則中的各類犯罪，此定義始有獨立討論的意義，否則會造成的結果不是流於空談[75]，即是會產生刑法過剩規制[76]。

第二項 電腦犯罪之類型

第一款 傳統見解

參考自德國學者 Sieber 氏所提出的分類[77]，林山田氏將電腦犯罪的類型分為電腦操縱、電腦間諜、電腦破壞與電腦竊用四類[78]。電腦操縱是指行為人於電腦

---

[70] 同理，若認為以電腦作為犯罪場所的情形(如在網路上張貼猥褻圖片供人觀覽)亦可稱為電腦犯罪，此種定義亦無太大討論價值，參蔡美智，虛擬世界的脫軌棋子—國內電腦犯罪脫序事件簡介，律師雜誌第 228 期，1998 年 9 月，頁 53 以下。

[71] 黃榮堅，電腦犯罪的刑法問題，台大法學論叢第 25 卷第 4 期，1996 年 7 月，頁 199-201。

[72] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 179。

[73] 謝開平，電腦犯罪之研究—我國現行法之適用與修正草案之檢討，國立中興大學法律學研究所碩士論文，1995 年 7 月，頁 35。其分析多數學者對於電腦犯罪的定義，其後得出除蔡蕙芳氏外之大多數學者皆採林山田氏所提出的定義，並認該定義為犯罪學上的電腦犯罪定義。

[74] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 178-179。

[75] 最後仍回歸刑法各罪章處罰的情形。

[76] 貿然獨立立法的情形。

[77] 謝開平，電腦犯罪之研究—我國現行法之適用與修正草案之檢討，國立中興大學法律學研究所碩士論文，1995 年 7 月，頁 29。

[78] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 49 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 3 以下；房阿生、吳振村，電腦犯罪及防治方法之研究，司法週刊社印行，1989 年 9 月，頁 84-93；廖有祿、李相臣，電腦犯罪：理論與實務，

輸入、處理、輸出三階段時，故意輸入不正確的資料或程式，或竄改既有程式，使電腦產生錯誤處理結果的行為[79]；電腦間諜是指行為人以非法手段刺探、蒐集或取得電腦輸入、處理、輸出時的資料或程式的行為[80]；電腦破壞是指行為人故意非法破壞電腦軟硬體設備，使電腦系統運作失效的行為[81]；電腦竊用則是如同使用竊盜般，於未經授權則無權使用電腦之行為[82]。

第二款 問題點之呈現

有論者認為，林山田氏(以及 Sieber 氏)所提出之分類並不精確，雖此種分類方式為法律學上常用之平面式分類方法，然而此種分類方式並無法準確地掌握其於定義中強調的「電腦特質」，反而會造成分類的重複或混淆[83]。若要掌握電腦特質，則應從縱向的時間性流程中，先行區分電腦處理流程，再從各個處理流程中，分別找出應該規制的行為。其將電腦處理的流程依照電腦特質分為「合法或非法進入(簡稱 A 領域)」、「於資料處理的輸入、處理、輸出(下稱資料處理三階段)過程中進行窺視、機能干擾、破壞軟硬體或機能、複製軟體、合理操作電腦等行徑(簡稱 B 領域)」、「於脫離該當電腦或電腦系統後所為洩漏或販賣資訊、獲取具體財物或不法利益等行為(簡稱 C 領域)」三個領域，並於 A 領域中區分進入行為是否經授權，若未經授權是否處罰，若要處罰則可分為何種類型[84]；同理，於 B

初版，五南出版社，2003 年，頁 17 以下；管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月，頁 17 以下；洪光煊，從電腦犯罪談未來刑法修正方向，刑事法雜誌第 32 卷第 3 期，1988 年 6 月，頁 55 以下。

[79] 林山田氏又將其細分為輸入操縱、程式操縱、輸出操縱三類，參林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 49 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 4 以下；管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月，頁 17 以下。

[80] 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 49 以下；林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 4 以下；管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月，頁 17 以下。

[81] 在此似包含單純以物理方式破壞電腦的行為，然而物理破壞電腦並不符合林氏所定義的電腦犯罪中「與電腦特質有關」的要件，從而在此即已根本排除。

[82] 又稱「時間竊盜」或「電腦服務竊盜」，參管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月，頁 17 以下。

[83] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 180 以下。

[84] 如「竊入」與「強行進入」。

領域則應考慮該電腦之處理機能是否受到干擾[85]，若有受到干擾並認要處罰，則可依據干擾程度以及被干擾的對象做區分；至於 C 領域，由於其中之行為與電腦特質僅會有間接關係，故無法依照電腦特質加以分類。以上的分類方式若以圖像的方式表示，因為隨著時間的流動，越到後續領域時所開展的行為類型更多樣化，故會形成一個類似圓錐體的圖像[86]。然而以林氏為首的多數見解卻著重於 C 領域之分析，故會產生如瞎子摸象般，僅以實際需要而恣意區分的分類結果。

第三款 本文見解–以入侵行為為中心

與定義電腦犯罪相同，在為電腦犯罪做分類時，首當其衝的問題仍然是「分類電腦犯罪的目的何在？」。然而不同於定義電腦犯罪的目的是要劃分討論的界線，一般而言為電腦犯罪做分類的目的往往是與法規範做連結，不同類型的電腦犯罪所需要的規範程度即不同，故以下就此角度檢視林山田氏以及李茂生氏所提出的分類方式是否能達到此目的，並進而提出本文的看法。

首先，就林山田氏的分類方式而言，確如學者李茂生所批評，僅是依照實際需要而就已發生或可能發生的案件為歸納整理的分類方式，此種分類不僅粗糙且會造成概念重複，若直接將其立法化即可能造成處罰範圍的過度擴張。而既然分類本身即造成概念重複混淆不清，於反應至規範上時即無法順利作連結，應可以認為無法達到分類的目的。相對而言，李茂生氏的見解似乎較能掌握「電腦特質」，以縱向的時間流動劃分各個階段，再於各個階段中歸納出所謂「與電腦特質有關的不適切行為」的範疇，有效的限縮處罰範圍，也將電腦犯罪的圖像具體化。同時也因為其以時間性作分類，任何被劃分為電腦犯罪的行為進行皆會有著 ABC 領域的順序，不但得以因應日新月異的科技進步速度可能產生更多樣的犯罪方式，亦可以有效的對各種行為作適當評價[87]，應可以認為有達到分類的目的，本文於

[85] 在此該論者所謂「干擾」係指廣義的干擾，參李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 184-185。

[86] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 185。

[87] 例如 A 領域中有「強行侵入」以及「竊入」二種類型，而 B 領域中有「破壞軟硬體」、「單純的窺視」及「未經授權的複製檔案(刺探)」三種類型，今甲行為的流程為「竊入電腦單純窺視」，乙行為的流程為「強行侵入電腦未經授權複製檔案」，在李茂生氏的分類中此二者的類型即不相

基礎思考上亦採行李茂生教授所提出的時間性縱向分類方式。

然而，雖誠如李茂生氏所述，一般而言，電腦犯罪的行為人會先侵入系統，後於資料處理三階段中進行窺視、干擾、破壞或複製，甚至合理操作電腦，最後進而達成其與電腦特質無關之目的，從而電腦犯罪時間性流程可以切割成上述 ABC 三領域[88]。惟此種分類標準是以行為人個人的犯罪時間進程角度出發來作分析，但若將電腦犯罪的時間進程作為一個「事件」來作分析，本文認為對於電腦犯罪的規制應較為全面，畢竟電腦犯罪的發生，不一定僅是因行為人一人的不適切行為而促成。對於電腦犯罪於 C 領域部分，本即與電腦特質無關，從而無法按照電腦特質做分類[89]，故在此似無僅因為其是一般不適切行為皆具有的特徵，而特別在不適切行為的分類中歸納一領域出來討論的必要[90]。同時，某些如製作、散布或取得電腦病毒程式，以及取得或公開他人帳號密碼等行為，於時間軸上應在進入電腦之前，然此種在進入電腦時點前可能發生的行為雖非為每個犯罪流程必經的程序，然亦可能對於電腦網路的使用造成影響，在此似亦有被納入「與電腦特質有關的不適切行為」範疇的可能[91]。再者，在仔細觀察「進入電腦前的行為(下稱 T 領域)」、「A 領域」以及「B 領域」後，即會發現 A 領域中的入侵行為應是電腦犯罪規制的重點。因在「入侵」的這個時點，即是表彰著對某種應被保護利益的直接侵害，入侵後的 B 領域行為僅是擴大利益侵害的深度及廣度，而在入侵前的 T 領域亦尚未直接侵害此種需要被保護的利益。若認為空間是客體間發展出相互關係的結果，並由於科技發達，經由電腦的使用，逐漸在人類社會出現

同(惟皆在不適當行為類型範疇內)，應有受不同評價的可能，事實上單純就上述二案例觀之，亦難認為此二者應受相同評價；然於林山田氏的分類中則皆屬「電腦間諜」，進而應受相同評價，亦即「電腦間諜罪」。參李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 185 以下；林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月，頁 60 以下。

[88] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 181。

[89] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 185。

[90] 然而在確認「是否為不適切行為(電腦犯罪)」的思考上，本文亦同論者看法，應適時考慮 C 階段的分析，否則很可能會造成立法時過度犯罪化現象。然在此的分類基礎，皆是立於「以確認該些行為皆為不適切行為後，將該些不適切行為做分類」的前提下所為者。參李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 190。

[91] 自己製作病毒程式用來入侵不在話下，就連製作病毒程式提供不特定他人，而該他人拿來作為入侵電腦的用途的情形，此時行為人雖僅有「製作並提供程式」的行為，但亦間接造成電腦被入侵的結果。

了關係概念的支配空間，則 A 領域中的入侵行為無疑是破壞對他人的空間支配自由[92]；又若認為現代社會中公眾對於電腦網路使用上的安全秩序有所信賴，則 A 領域中的入侵行為亦象徵著信賴關係的破壞[93]。

據此，在此的時間性分類，本文擬以入侵行為為中心，將不適切行為流程分為三大部分–入侵前行為、入侵行為、入侵後行為。於入侵前行為的部分，主要區分為「入侵前的準備行為[94]」以及「協助入侵行為[95]」等類型；在入侵行為部分，則參考李茂生氏，區分為「竊入」及「強行進入」等類型[96]；而入侵後行為部分，亦參考李茂生氏區分為「軟硬體破壞」、「機能干擾」、「未經授權複製檔案」、「單純窺視」等類型[97]。

第二節　我國立法上面對妨害電腦使用行為之態度

在了解我國尚未訂立妨害電腦使用罪章前傳統見解對於電腦犯罪的態度後，於本章則要以妨害電腦使用罪章本身為重點作論述。於各節的鋪陳上，預計環繞著整個罪章的發展過程，敘述本罪章修法的緣由、所考慮的問題、罪章特色與處罰重點，以及修法後由各界提出的爭議。

第一項 發展沿革

第一款 初步修正電腦犯罪相關條文

由於電腦犯罪案件日漸增加，從而為回應社會大眾對於治安機關追查究辦的

---

[92] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 79 以下。
[93] 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 244 以下。
[94] 如行為人自己製作程式供自己方便入侵電腦之用。
[95] 如行為人製作一程式，然卻未善盡保護措施，而提供予他人使用，該他人將其作為入侵電腦之用。
[96] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 184。
[97] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 185。

期待，以「迎接資訊時代，防制電腦犯罪」，法務部於民國 74 年舉辦電腦犯罪問題研討會，邀請專家學者進行研究討論[98]，更於愛普生公司入侵案[99]的影響下，於民國 86 年以增修個別條文的方式，新增了刑法第 220 條、第 323 條[100]、第 339 條之一至之三等條文。本次修正的重點有三，各是電磁紀錄的準文書化、電磁紀錄的動產化，以及電腦詐欺罪的訂定。學者李茂生指出，若仔細觀察本次修法後即會發現我國實務界亦受到林山田氏的影響，電磁紀錄的準文書化實則對應林氏分類中的「電腦破壞」類型；電磁紀錄的動產化是對應「電腦間諜」類型；而電腦詐欺罪則是對應「電腦操縱」類型[101]。

本次修法通過後遭到不少批評，其中最具代表性的批評則為電磁紀錄的動產化。論者多認為刑法上所謂竊盜，必須符合「破壞他人對物的持有，建立自己對物的持有」此一要件。然而電磁紀錄有容易任意大量複製的特性，行為人在建立自己的持有時，未必會破壞他人的持有，並與同條規定的電能，熱能等能量經使用後即消耗的特性有異。從而此規定實則破壞了「竊取」一詞的傳統定義[102]。更有論者直指問題核心，認為電磁紀錄實則是一種「利益」，此規定無異承認利益竊盜，而利益竊盜為使用竊盜的變體，會與我國不罰使用竊盜的刑事政策有所衝突[103]。

第二款 增訂妨害電腦使用罪章

---

[98] 陳煥生，刑法上之電腦犯罪，刑事法雜誌第 42 卷第 3 期，1998 年 6 月，頁 2。

[99] 愛普生公司入侵案係一原任職愛普生(EPSON)公司的員工林炯碩，在因故離職後，已離職前的管理者帳號密碼登入愛普生公司的電腦，並且更改愛普生公司著作的元件資料庫佈局資料，使愛普生公司無法順利產生晶片。參林宜隆、李建廣，網路犯罪問題及其偵防機制之探討，警學叢刊第 31 卷 1 期，2000 年 7 月，頁 203 以下。

[100] 在民國 88 年、91 年的陸續修訂下，刑法第 334 條之一(搶奪、強盜罪)、第 338 條(侵占罪)及第 343 條(詐欺罪)亦準用本條，參李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 70-71；陳煥生，刑法新增妨害電腦使用罪之介紹，中華法學第 10 期，2003 年，頁 7 以下。

[101] 李茂生，我國電腦網路犯罪的虛像與實相，刑事政策與犯罪研究論文集(四)，法務部犯罪研究中心，2001 年，頁 7。

[102] 92 年中華民國刑法第 323 條修正理由說明一，法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 382。

[103] 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 236-237。

由於民國 86 年修正條文不但遭受學者大力抨擊，於實務運用上亦發現條文有漏洞、模糊不清、以及運用上困難等問題，並為有效規範日新月異的科技時代中新型態的電腦犯罪案件，使我國法律規範能符合先進國家標準[104]，故法務部於民國 90 年組成防制電腦(網路)犯罪相關法規研究小組[105]，希望一併檢討電腦犯罪問題[106]。其研討結果即係民國 92 年新制訂的妨害電腦使用罪章，號稱結合產官學代表，歷經一年多的理性辯論而成[107]。其研討過程的重點以點列方式分述於下：

一、　研討方式仍採用類型化思維

雖本次檢討的原因即是因為民國 86 年來陸續修正與電腦犯罪相關的條文有種種問題導致運用困難，而 86 年法律修正時的思維即是林山田氏於當年的時空背景下，僅能憑著稀有案例並配合想像所創造分類的實踐已如前述[108]，此種將個案類型化後即思考如何立法處罰的思維所遭到的困境似應是本次修正所應該記取教訓而根絕，甚至大膽批判的。然而於法規研究小組第一次開會時，即將此種思維再度發揮的淋漓盡致。法規研究小組於開會時，仍是以提供發生在台灣或國外的電腦或網路犯罪案例來與現行國內刑事法規範作比較，並嘗試對無法解決的案例作增修規定的作法在「檢討」電腦犯罪[109]。共計初步列出「任意讀取、移除他人電子郵件或網頁之脫序行為」、「非法入侵、讀取或攻擊他人電腦資料庫之行為」、「刺探他人密碼、蒐集他人電子信箱之行為」、「擅自使用他人電腦相關設備或身分以獲取服務之行為」、「濫發電子垃圾郵件、植入或散播電腦病毒妨害他人存取資料庫的行為」、「侵害公共使用或政府機關電腦網路之行為」、「網路服務提供(ISP)業者或其他類似之業者是否有防止使用者侵害著作權之義務」等七種態樣

---

104 葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 95。

105 以下簡稱「法規研究小組」。

106 參法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 214，葉奇鑫檢察官之發言。

107 葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 95。

108 李茂生，我國電腦網路犯罪的虛像與實相，刑事政策與犯罪研究論文集(四)，法務部犯罪研究中心，2001 年，頁 7。

109 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 9 以下。

[110]，並於第二次會議更進一步地將其分為「利用網路為犯罪客體之犯罪」以及「利用網路服務之傳統犯罪」等二大類供之後討論[111]。又，於可謂是研討尾聲的第六次會議中，所整理過去幾次會議中所關心討論的議題為四大議題–「垃圾郵件」、「嘗試入侵」、「電腦病毒」、「跳板」，並且就這些行為的防止而思考如何修法[112]的作法，仍未擺脫林氏當年面對電腦犯罪時瞎子摸象般的思維[113]。

二、　研討過程中法律學者難以傳達意見

雖本次修法「據告稱」是「結合產官學代表，歷經一年多的理性辯論而成[114]」，惟仔細觀察修法研討紀錄會發現，於法規研究小組內部研討的八次會議中，僅有國立交通大學科技法律研究所助理教授熊愛卿教授以及中央警察大學教授葉毓蘭教授兩位學者列席，且二位教授皆未八次會議均全程列席，導致法規修訂過程中，多數刑法學者幾乎無參與討論以及給予意見的空間。其中熊愛卿氏曾於法規研究小組籌備會議時似乎有考慮修法過程中過少學者參與的疑慮，而於會中建議邀請更多刑法甚至刑事訴訟法學者與會，方能對相關條文修訂有更精確的掌握[115]。然而卻遭主席以「讓學者、專家們全程參與，恐會擔誤他們太多的時間，故採因應特別主題的不同，邀請相關之學者、專家列席，參與討論[116]」為由拒絕。爾後會議亦不見因應主題而參加的學者，僅有在修法完成後的一次會議中，邀請部分學者[117]出席發表意見。

據此可想而知，於研討過程中與會學者的發言受重視的程度是偏低的。其中

---

[110] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 10 以下。

[111] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 24。類似的分類法可參照林永謀，電腦犯罪與刑事法上之問題，法令月刊第 35 卷第 7 期，頁 9；林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 85 以下；廖有祿、李相臣，電腦犯罪：理論與實務，初版，五南出版社，2003 年，頁 11 以下。

[112] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 97 以下。

[113] 然而妨害電腦使用罪章修訂時與林山田教授發表有關電腦犯罪論文的時空背景卻早已差距甚遠。

[114] 葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 95。

[115] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 3。

[116] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 3。

[117] 如陳志龍、甘添貴、靳宗立、林宜隆等學者，參法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 213 以下。

例如與會學者曾多次於會上提出因過去討論電腦犯罪的文章皆重視行為類型的分析，然此種分析僅能治標而無法治本，必須要釐清「資訊」及「資訊系統」是否能構成刑法上的法益地位，始能解決問題等直指問題核心的意見[118]，然因實務家後續討論皆著重於法律用語的定義以及犯罪類型的區分，導致幾無迴響，從而研討過程中討論到保護法益的機會趨近於無。

三、　研討內容多援引美國立法例

不同於我國刑法是繼受於德國及日本等歐陸法體系，在修訂妨害電腦使用罪章時，法規研究小組成員大量援引美國案例以及美國立法例來做為訂立新罪章的依據[119]。其中如電腦病毒[120]、網路賭博[121]等案件，以及僅因電腦犯罪行為的特殊性即應獨立於傳統犯罪訂立專章的處理態度[122]。然而，姑且不論一部刑法典內的不同章節竟是依不同法體系的概念所訂立時所造成犯罪成立及處罰上的重複與衝突，就概念本身的不一致所造成的矛盾即是一非常嚴重的問題。今法規研究小組多採行的美國法係屬英美法體系。不同於大陸法體系的是，英美法體系對於犯罪行為的處罰僅在實現刑事政策的效用，而完全不在乎處罰的依據是否具有保護法益[123]，若將一部分英美法體系之法條「移植」到大陸法體系的法典上時，即會產生刑罰無限制的前置化以及重刑化，唯有嚴重的刑罰，始能與龐大的損害相稱[124]。刑罰的無限前置及過度加重，完全違背我國刑法最後手段性的原則。同時，無法解釋保護法益為何的電腦犯罪專章，身在歐陸法系法典中，亦會面臨存在依據的質疑及挑戰。若只是因為行為的特殊性以及所造成的危害重大，即獨立於傳統犯罪處罰，於論理上可以說是站不住腳。

四、　以歐洲網路犯罪公約為重要參考資料火速訂立專章

---

[118] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 25 以下、33、58，熊愛卿教授之發言。
[119] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 65-66、100-112。
[120] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 29，林慶恆科長之發言。
[121] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 71，張紹斌檢察官之發言。
[122] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 80，葉毓蘭教授之發言。
[123] 吳文君，妨害電腦使用犯罪行法規制之分析—以保護法益為中心，國立台灣大學法律學院法律學系碩士論文，2010 年 6 月，頁 8。
[124] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 32-33，慶啟人檢察官之發言。

自第五次會議起，法規研究小組歷經人事變動，執行秘書改為葉奇鑫檢察官，而葉檢察官亦於該次會議提出歐洲議會電腦犯罪公約，並呼籲法規研究小組於該次以及第六次會議中，就此公約與我國現行相關法制作比較，以訂出修正條文草案，於期限內送立法院審議[125]。而此後的會議流程，問題的重點皆圍繞在歐洲議會電腦犯罪公約與我國法制的比較，且順利於第六次會議後送出電腦犯罪專章草案給立法院審議。審議後的第七、八次會議，討論的重點即集中在該電腦犯罪專章草案的章名、文字定義以及條文次序是否妥適等「對草案作修改」的程序，至此法規研究小組似已於大方向形成共識。

然而，自第五次會議前，法規研究小組所討論的重點仍置於就個案的歸納以及類型化，並比較類型化後的行為類型與我國現行法制是否可以處罰。由此可知，該電腦犯罪專章的草案是從第五次會議開始擬定，於第六次會議後即完成初步草案送審，擬定專章的最低限度即是參考歐洲議會電腦犯罪公約[126]。開始擬定至完成僅短短二個月餘，並且大量參考之前幾乎未引起討論的歐洲議會電腦犯罪公約以作為新增我國法的依據。姑且不論擬定草案時間過於倉促以致不禁令人懷疑草案擬定的嚴謹度以及專業度的問題，衡諸法規研究小組各研修會議紀錄，唯一可以看到對歐洲議會電腦犯罪公約與我國的連結點即在於第五次會議中，葉奇鑫檢察官所提出「…(前略)我們希望藉由此一(歐洲議會電腦犯罪公約與我國現行相關法制的)比較，使我國在電腦罪防制相關法規的修訂上能跟上世界最新潮流與趨勢，並符合國際間對防制電腦犯罪立法上之要求與標準」的發言[127]。由此可知法規研究小組之所以會選擇參考歐洲議會電腦犯罪公約作為我國法制參考的重要依據[128]，主要僅是因為「歐洲國家是引領世界潮流的先進國家，而我國法制為了跟上先進國家的腳步，故要以先進國家的法制作為重要參考資料」此一理由而已，完全未將所參考國家與我國國情、法律規範的論理基礎上是否有差異等問題作為討論重點。

---

[125] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 81-82，葉奇鑫檢察官之發言。
[126] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 86，葉奇鑫檢察官之發言。
[127] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 82，葉奇鑫檢察官之發言。
[128] 葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 95。

綜合以上四點研討過程的特色，可以得知我國妨害電腦使用罪的立法過程不但倉促並且粗糙。法規研究小組一味的追求外國法制的引入以及強調對其就現有案例所歸納出的行為態樣應該受到處罰，卻漠視處罰的依據為何，以及所引入的法制規範是否適合我國法等問題。於研討方式上亦沿襲 86 年修法時將個案類型化後再思考如何處罰的類型化思維，並且於研討過程中排除極大多數法律學者參與[129]，與會學者的聲音亦很難造成共鳴。可想而知，以此種立法態度所產生的妨害電腦使用罪，將會面臨於刑法理論上巨大的批判聲浪。

第二項 罪章特色及處罰重點

法規研究小組對於修法粗糙的處理態度已如前述，故而所研擬出來的妨害電腦使用罪章[130]條文當然精準反映了法規小組於修法上所做的努力，而具有以下特色，分別以分點方式敘述於下：

一、 專門處理狹義電腦犯罪

如同法規研究小組在第二次會議中將電腦犯罪區分為「利用網路為犯罪客體之犯罪」以及「利用網路服務之傳統犯罪」等二大類，並且於商討修正草案會議時亦有提出真正的電腦犯罪條文其實只有舊刑法第 323 條以及第 352 條第二項，其他與電腦犯罪有關的條文皆是傳統犯罪行為加上使用電腦作為工具，故並無做體系上修改移動必要的見解[131]般，修法後新增的妨害電腦使用罪章亦忠實地反映了此種見解，在其立法理由中敘明僅對「利用電腦網路為犯罪客體」的犯罪做規範，並未對利用電腦網路的傳統犯罪做更動[132]。

二、 保護法益兼及個人與社會法益

---

[129] 其中亦有認為刑法學者因無技術背景，於討論此類問題時可能產生誤解的聲音，參法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 141，張紹斌檢察官之發言。

[130] 章名於研擬時原先稱「電腦犯罪」，後改成「濫用電腦罪」，最後始改成「妨害電腦使用罪」。

[131] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 125，覃正祥檢察官之發言。

[132] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第二點。

法規研究小組在討論當時因大力參考美國法制，而漠視我國法是繼受於歐陸法體系，於以刑法處罰特定行為時，多認為應有保護法益為依據的核心問題。原則上此種態度所導致的立法結果應是一種如同英美法體系般僅是為了實現刑事政策而將犯罪行為類型化的處罰條文，並無保護法益的存在[133]。然而於新罪章制定後，其立法理由不但載明「本罪章保護法益為電腦使用安全[134]」，並該保護法益「兼及個人及社會法益[135]」外，還進一步認為目前刑法的立法體系不特別強調保護法益的種類作為章節區別，而是屬混合式的立法方式[136]，以試圖為置放於刑法最後一章的妨害電腦使用罪章排除學界可能對其作體系矛盾的批判[137]。

三、　初步嘗試以縱向時間性區分犯罪類型

法規研究小組在研擬時曾參考大量美國立法例已如前述，而美國立法例正好就電腦犯罪部分是採用縱向時間流動性的方式對於電腦犯罪作分類，進而以該些分類作為規範。而大力參考美國規範的法規研究小組，亦照單全收的將此種分類方式引入主要係以橫向平面式分類並加以規範的我國刑法中。惟於立法理由中並不見法規研究小組提及為何採用縱向時間性的方式分類，僅見因「世界先進國家立法例對於此類行為均有所處罰」的理由，即引入條文作處罰[138]。雖可據此認為新法會造成此種結果並非法規研究小組的真意，然而就算是瞎貓碰到死耗子，新法的確史無前例的跳脫了以往橫向平面性的分類方式，在刑法立法例上作了一個新的嘗試。

四、　特立獨行的規範用語

---

[133] 畢竟於法規研究小組討論當時即未對此多加著墨。

[134] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第二點。

[135] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第三點。

[136] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第三點。

[137] 其中立法理由舉出刑法第 354 條雖是置保護個人財產法益的毀損罪章，但該條中亦有出現「足以生損害於公眾或他人」的構成要件，以說明刑法並不特別強調以保護法益種類作為章節區分方式，參中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第三點。

[138] 中華民國刑法第 358 條立法理由第二點；中華民國刑法第 359 條立法理由第二點。

法規研究小組似乎認為電腦犯罪是一因應新時代資訊犯罪的新形態法律，故於法條的用語上也必須要與傳統刑法作區別，始能凸顯出其特殊性。據此，於妨害電腦使用罪章中則使用不同於傳統刑法的描述方式，如刑法第 358 條所稱「入侵」不同於刑法第 306 條所稱「侵入」、刑法第 360 條所稱「干擾」等，以及在同一條文中同時使用「電腦」、「電腦或其相關設備」、「電腦系統」等新名詞作規範。但是，在法條中使用此類新名詞的同時，法規研究小組卻未於修法時一併給予任何的解釋或定義，導致此些新名詞於未來適用上有非常廣泛且多元的解釋可能，進而使得處罰範圍更加曖昧。

五、　對公務機關為犯罪之加重處罰

於修法過程中，對於公務機關電腦為入侵、破壞或干擾時是否不同於一般電腦處理此一議題鮮少被法規研究小組所討論，亦未被加入當時的草案中，然而自草案送行政院審查通過的版本起，則於第 361 條新增對公務機關電腦犯罪的加重處罰。觀察其立法理由，最主要是為了保障國家機密，蓋政府機關電腦系統被入侵，往往造成國家機密外洩[139]，故為保護公務機關的資訊安全，參考美國對於入侵政府電腦行為加重處罰的規定，而新增本條規定。雖立法理由本身或有諸多疑義，然本條規定亦顯示了立法者有初步思考並認為「公務機關的電腦較一般電腦更需要保護」的現象。

綜合以上特色，可以發現妨害電腦使用罪章不管於保護法益上或是立法結構上都有著一點與眾不同的色彩，此種結果有弊亦有利，亦大大提供了在檢討本罪章以及思考如何處罰電腦犯罪時的不少靈感以及思考方向。

第三項 修法後出現之爭議

修法後造成了各界一股批判的浪潮。對條文抱有最多批判意見的不外乎是在修法過程中未受重視的法律學者們，於某些條文的設置上甚至連當初法規研究小

[139] 中華民國刑法第 361 條立法理由第二點。

組的內部成員亦有不同見解提出[140]。而因為意見既繁多又零散，在此本文將討論重點聚焦，統整為「保護法益」以及「科技名詞的定義」二大類，並藉由批判的意見來討論整個妨害電腦使用罪章各條文所出現的共同問題。至於個別條文的批判與疑義，則留待「妨害電腦使用罪章各行為態樣之探究」一章中探討。

第一款 保護法益

於妨害電腦使用罪章的修法理由中強調保護法益為電腦使用安全，而該「電腦使用安全」法益又兼及個人及社會法益已如前述，然而此種新型態的法益構成，正是學者們所大力抨擊的重點所在。首先，就兼顧雙重法益的犯罪類型部分，論者認為雖刑法犯罪類型中存在雙重法益的規定，但通常是一個主要保護法益搭配一輔助法益，負責輔助的法益有著限制罪責與減輕加重之功能[141]，並未如立法理由中所謂「兼及」的用法。據此，立法理由中所舉的刑法第 354 條的例子中，刑法第 354 條有規定「足以生損害於公眾或他人」之要件，是因為第 354 條所保護的個人財產法益事實上有極大多數類型皆是以民事法上侵權行為解決即可，毋庸動用到有最後手段性的刑法，但若該破壞財產法益的行為已經嚴重到足以動搖社會對財產保護秩序的信賴，始必須以刑法處罰。從而，在此該要件(社會法益)是一種區分該毀損行為應適用民事紛爭解決機制抑或是刑事制裁機制的分水嶺，並非如立法理由所述，與個人法益「兼及」。

再者，於立法過程與立法理由中可以觀察到，研擬修法的法規研究小組多次

---

[140] 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 86 以下。

[141] 詳言之，於國家或社會法益作為主要法益部分，論者認為作為輔助法益的個人法益往往擔任減輕或加重罪責的功能，以刑法第 173 條第 1 項放火罪為例，由於刑法第 173 條第 1 項所保護的社會法益包含現在住在該建築物中的人的生命與財產的危害可能性，以及鄰近或造訪該建築物的人的生命與財產的危害可能性，故會較僅有保護鄰近或造訪該建築物的人的生命與財產的危害可能性的第 174 條刑度重，然若該住在建築物中的人已放棄自身法益時，則對公共安全的危害僅剩下對鄰近或造訪者生命與財產的危害可能，其社會法益的濃稠度會因而降低，故僅成立刑法第 174 條之罪；於個人法益為主，社會或國家法益為輔的部分，論者認為輔助的社會法益往往會用來限制該個人法益被處分範圍或限縮侵害該個人法益的行為，若是重要的個人法益，若隨意處分則會造成社會對法秩序的信賴感動搖，故要以社會法益限制處分法益的範圍。而若是一般個人法益，則必須要到動搖社會對法秩序的信賴感的嚴重程度，始得成立犯罪，方符刑法最後手段性原則。參李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 240，註 9 處。

強調「社會上發生妨害他人電腦使用案件日益頻繁，造成個人生活上之損失益趨擴大，實有妥善立法之必要」。惟若只是單純以電腦的普遍性、大量使用以及龐大損害的造成，就肯認對此刑事制裁是有正當性的，即會造成處罰的恣意，若要避免此種結果，在刑法論理上尋找一個犯罪類型存在正當性的共識並對案例作檢驗思考應是個可行的方式[142]，故而若要重新審視電腦犯罪，首先應先確定者為「保護法益為何」，並非只要扯到電腦然後危害重大就要加重獨立處罰[143]。又，雖立法理由已有明示本罪章的保護法益為「電腦使用安全[144]」，然而各條間之立法理由又再度「創設」各種不同法益[145]，並且於參考草案擬訂人的意見後，發現草案擬訂人的意見又與新法立法理由有些許出入[146]。暫且不論立法理由與草案擬訂人間為何會出現對同一法條中保護法益的不同見解，不管就立法理由或草案擬訂人的版本單獨觀察，整個罪章的「保護法益」欠缺同一性[147]。由此可知應是因立法當時無法找出保護法益，而急就章似的將從擬訂的各條文中找一個相對合理的入罪化理由。會造成如此結果的原因亦如前所述，即是因為在研擬修法時大量採用美國立法例，以及參與研擬討論的法規研究小組成員多為實務工作者，於思考的重點較置於如何將修訂的新法能夠於實務上有效的適用，並能夠根絕其所觀察到各種應該處罰的「電腦犯罪」行為，對該些處罰是否有統一要保護的法益等問題則選擇性漠視所導致。然仔細分析上述二版本的「保護法益」以及條文的規範，若硬要將本罪章各條文依照保護法益的特性給放置於刑法其他各章處罰並非行

---

[142] 而此種刑法研究上廣泛的共識大多會聚焦在法益的保護上。參李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 74。

[143] 鄭逸哲，吹口哨壯膽—評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 110。

[144] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 36 章妨害電腦使用罪說明第二點。

[145] 如刑法第 358 條立法理由第二點認為本條所保護者為「電腦系統的安全性」、第 360 條立法理由第二點認為本條所保護者為「電腦及網路設備之正常運作」等。

[146] 氏認為刑法第 358 條所保護者為「電腦之使用安全」、第 359 條所保護者為「電磁紀錄之支配權」、第 360 條所保護者為「電腦系統之效能」。參葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 98 以下。

[147] 具體來說，具有同一性的例子如刑法殺人罪章(刑法第 271 至第 276 條)，此六條所保護者皆為「生命法益」，僅是侵害生命法益的態樣不同而已。反觀妨害電腦使用罪章，雖罪章的立法理由闡明本罪章保護法益為「電腦使用安全」，然而各條的保護法益有「電磁紀錄之支配權」，亦有「電腦系統效能之保障」。嚴格而言，此二者與電腦使用安全的關係甚遠，若承認此種關聯性，則本罪章最上位所闡明的保護法益—「電腦使用安全」無疑是個極度空洞的概念，將此種概念作為具有最後手段性的刑法中關鍵性的保護法益，似有導致刑罰的過度擴張之疑義。

不通[148]，因而若要思考電腦犯罪專章成立的可能性，除要找出保護法益外，該保護法益必須要是獨立於傳統法益並具有同一性，否則即應視不同的法益而個別訂立不同的專章，非僅因該些犯罪皆與電腦有關，則全部置於同一罪章之下。

第二款 科技名詞之定義

因電腦犯罪專章主要係在規範電腦犯罪，其中「電腦」、「電腦系統」、「網路」等科技名詞即會出現在法條或立法理由中，尤其是「電腦及其相關設備」一詞在該罪章的各條文中被大量使用，基於構成要件明確性原則，若對電腦一詞予以定義似乎是個理想的做法。然而科技日新月異，電腦的概念不斷快速變動，對電腦一詞作定義是否真有實益亦是個問題點。從而就是否於電腦犯罪專章中或刑法總則中加入電腦，法規研究小組於研擬法規的時候已經過不少次討論[149]，最後仍因「資訊科技發展日新月異，對於『電腦』、『電腦系統』及『網路』等科技名詞定義不易，為免掛一漏萬，或未來法律適用無法跟上科技腳步[150]」為理由而不予定義。

對此，學界亦有不少分歧的聲音。支持不予定義的論者，主要是扣緊前述立法理由的論述，認為法務部此舉是一聰明的做法，一來電腦一詞有「難以定義性」，亦即根本難以就電腦一詞予以定義[151]，若將名詞訂死即會失去法律適用的彈性[152]。亦有從電腦一詞為一流動概念的角度出發，並認為即使有要為電腦一詞為定義的必要性，也無法為電腦一詞作一定義[153]，更有論者認為除非相當明確者應予定義

---

[148] 如將第 358 條置於妨礙自由罪章、將第 359 及第 360 條置於財產犯罪各章等。類似見解參鄭逸哲，吹口哨壯膽—評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 105 以下。

[149] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 82 以下、157 以下。

[150] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 358 條之修正說明第四點。

[151] 鄭逸哲，吹口哨壯膽—評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 106。

[152] 李茂生，刑法新修妨害電腦使用罪章芻議（中），台灣本土法學第 54 期，2004 年 2 月，頁 245。

[153] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 70-71。惟其於文末亦肯認若能具體化電腦文義的輪廓，則應更具體化，參同著作，頁 75 以下。

外，似可依審判時之通念，透過解釋之方式加以解決，無庸立法訂定[154]。反之，採應予定義的論者，多係參考國外比較法，以及電腦相關業者對於電腦一詞的認識，嘗試給予電腦一詞一個定義，以符合罪刑法定原則下的構成要件明確性原則，有論者直接從電腦業界對電腦基本認識要素分析，認為電腦全名為「電子計算機」，「電腦」則係俗稱。而電腦是「一種可以解譯並執行程式命令之電子裝置，得以處理輸入、輸出、算術以及邏輯運算。其主要結構，係由輸入裝置(如鍵盤、麥克風、滑鼠等)、處理器(CPU，中央處理器之簡稱)、輸出裝置(如螢幕、喇叭、印表機等)以及儲存裝置(如軟碟、硬碟、光碟等)等四個基本元件所組成」。而除此之外，得透過連線將資料輸入或輸出電腦之輔助設備，通稱「其相關設備」(如數據機)[155]。亦有論者認為，若對電腦下最廣義的概念，則範圍必無限寬廣，故應限縮於「具有資訊處理、儲藏以及傳達功能之電腦」，始為刑法上之電腦概念[156]。同時，爭議於比較法上仍存在，採予以定義立場的有美國[157]、德國[158]、以及歐洲議會網路犯罪防治公約[159]，而採不予定義立場的有日本[160]及英國[161]，可見若從比

---

[154] 莊忠進，電腦犯罪立法之探討，刑事科學第 39 期，1995 年 3 月，頁 111。

[155] 甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌第 50 期，2003 年 9 月，頁 180-181。但在此有學者批評「認為數據機非電腦之一部分而印表機是電腦之一部分」一事過度背離社會通念，又事實上吾人無法想像單獨入侵數據機的行為。參李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 245。

[156] 蔡蕙芳，電腦犯罪和刑事立法的課題，國立台灣大學法律學研究所碩士論文，1994 年 6 月，頁 16 以下。惟其亦未說明何為「最廣義之電腦」，且將數位相機亦排除於電腦概念之外，然數位相機已具資訊處理(把數據化成圖片)、儲藏(儲存相片)、傳達(與他人手機、數位相機、電腦互相傳輸照片)等功能，依其見解似應被認為屬於電腦。

[157] 美國聯邦的定義是認為電腦是一「用以執行邏輯、算術或儲存功能的電子的、磁性的、光學的、電子化學的或是其他高速處理資料的裝置，並且包含任何與此等裝置直接相關或是連接的資料儲存設備或連線設備，但並不包含自動打字機、自動排字機、攜帶式掌上計算機或相類似的裝置，參美國聯邦法典第 1030 條(e)(1)。又因美國歷史背景以及法體系的特殊性，導致美國聯邦法與州法呈現「百花齊放」的狀態，各州對於電腦的定義皆有不同，參李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 193 以下。

[158] 然而，德國於立法時所使用形容電腦的名詞為「自動化資料處理系統(eletronische Datenverarbeitungsanlage，簡稱 EDVA)」，應可較「電腦」或「電子計算機」為明確，參莊忠進，電腦犯罪立法之探討，刑事科學第 39 期，1995 年 3 月，頁 111；蔡蕙芳，電腦犯罪和刑事立法的課題，國立台灣大學法律學研究所碩士論文，1994 年 6 月，頁 17；李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 75 以下。

[159] 其認為電腦的定義是「任何單獨或彼此相連的裝置中，有一個以上的裝置依程式運作而自動處理數據者。」，原文為「"computer system"means any device or a group of inter-connected or related devices,one or more of which,pursuant to a program,performs automatic processing of data.」。參歐洲議會網路犯罪公約第 1 章第 1 條 a。

[160] 但根據日本國會立法過程中出席眾議院法務委員會的政府代表說明：「電腦係供業務處理之用，擁有一定獨立性，能自動進行資料處理之裝置。亦即具有影響業務判斷、事務處理與控制機能之

較法的角度來看，不管採取何種看法皆有所本。

綜上，本文認為，若從規範目的角度出發，若要定義此些名詞，該定義仍應緊扣保護法益而為。從而，一般電腦相關業者對於電腦的定義[162]則可能太過於寬廣，若直接套用至刑法上即會產生過度擴張處罰範圍的困境。故在此於法學方法上有兩種定義模式，一種是直接以電腦相關業者對於電腦概念的定義作為刑法上對電腦的定義，再於立法技術上將對於特定電腦的侵害行為、以特定方式對電腦的侵害行為、或對電腦侵害至特定程度的行為等等規範要件來規定處罰。而另一種處理方式為對電腦相關業者的定義作一定程度的限縮，獨立創造出「刑法上有意義的電腦」的概念，而直接適用於刑法上。前一種定義方式雖有使刑法上的電腦與一般人所認為的電腦相符，且於法條部分處罰對象明確，不但符合構成要件明確性，對法安定性更能有所幫助，惟我國於立法上並未對特定電腦係特定罪的客體或利用工具做區分，而係一致的稱「電腦」，故而若適用第一種定義模式似勢必得走上修法一途；而第二種定義方式雖較符合我國妨害電腦使用罪的現況，然而要如何創造出「刑法上有意義的電腦」即非常困難，畢竟科技發展日新月異，若在不久的未來電腦出現了新概念，於現今下了很多工夫而創造的定義又可能立即被推翻，對於問題的解決似乎助益也不大。故若就法律規定的現況，基於電腦概念的流動性而不對其作定義的方式似乎是最佳的作法。

第三節　比較法上對於電腦犯罪之立法概況

探究完我國法的來龍去脈後，在得知我國修法過程的粗糙以及罪章本身與整部刑法體系格格不入之外，亦可以得知此種電腦犯罪的產生與規制是全球性的，

電腦始屬之。」似可認為實務上仍對電腦的定義有一定掌握。參西田典之，コンピュータと業務妨害・財產罪，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 515。

[161] 高橋郁夫，コンピューターの無権限アクセスの法の覚書―英国・コンピューターミスユース法 1990 の示唆，判例タイムズ 1006 号，1999 年 10 月，頁 92 以下；瀬川晃，イギリスにおけるコンピュータ犯罪とデータの保護，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 573。

[162] 其對於電腦之定義大多係「可以接受資料、命令，並加以分析過濾以迅速處理資料，然後輸出、對應結果的電子化設備。」，參考施威銘研究室，最新計算機概論 2010，旗標出版社，2009 年 9 月；曾憲雄、呂克明、張榮吉、廖冠捷、劉光勝、陳興忠，計算機概論，初版，東華書局，2008 年 9 月。

並非僅我國始有此類問題，且我國是繼受法國家，被繼受國對此類問題的解決方式，亦有參考價值。據此，似應在具體檢討我國妨害電腦使用罪章所可能遇到的困境之前，先行討論關於其他國家面對電腦犯罪時所採取的態度，以及若有規制時該規制的構成以及理由，以做為檢視我國法律的標準及在思考如何解決我國法困境時的參考。

但並非所有外國法律於我國皆有參考價值，一來我國於妨害電腦使用罪訂立當時，係大量參考美國立法例，二來有鑑於我國刑法是繼受德國及日本等國的規範而訂立而成，故首要探討者即是美國立法例，而後則是探討德國與日本的立法例，本節即以美國法、德國法以及日本法為順序，依次探討如下。

探討的重點部分，因對外國立法例作分析的目的在於將其做為檢視我國法律的標準及在思考如何解決我國法困境時的參考已如前述，故本節將著重於其立法背景以及規範特色的分析，從該些國家發展背景的脈絡，以及現今規範重點的角度，來給我國法律一點建議。

第一項 美國法

美國是由 50 個州以及聯邦政府組成，故而司法制度亦隨著其構成有著州法以及聯邦法等不同的規制[163]，然而在此為於討論上能聚焦，故本文將具代表性質、由國會制訂的聯邦法，以及較具重要性的州法，就立法背景的部分做區別，分別於以下各款討論。

第一款 聯邦法立法背景–電腦濫用修正法演變史

於 1970 年代末期，隨著電腦的普及化，美國已產生不少與電腦相關的犯罪，從而於 1979 年，美國聯邦政府有鑑於電腦犯罪的嚴重性、可能造成的巨大損失、

[163] 除 50 州與聯邦外，亦有首都華盛頓市所在的哥倫比亞特區，故共計 52 個司法管轄區，亦即有 52 種法律制度，參李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 138。

特定工作人士犯罪機會的增加、對商務有直接影響、現行法起訴此類行為相當困難等理由，對是否將電腦濫用等行為規定於聯邦法律中獨立處罰一事進行討論[164]，然而最後並未達到共識[165]。

爾後，美國聯邦於 1984 年 10 月 12 日通過「非法使用設備、電腦詐欺及濫用法[166]」該法將意圖侵害聯邦政府利益以及貿易上利益的進入電腦行為列為處罰對象[167]，並已對電腦一詞作一明確的定義[168]。然該法缺乏對許多電腦用語的定義，且無明確法院管轄權，導致立法後鮮有對電腦犯罪案件所起訴及審判者，立法效果明顯不彰[169]，聯邦政府遂於 1986 年 10 月 8 日通過「電腦詐欺及濫用法 (Computer Fraud and Abuse Act of 1986)」，大大擴充其處罰範圍[170]。然而，法律

---

[164] 此即「1979 年聯邦電腦系統保護法案(Federal Computer Systems Protection Act Of 1979)」，參房阿生、吳振村，電腦犯罪及防治方法之研究，司法週刊社印行，1989 年 9 月，頁 102 以下。

[165] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 191。

[166] Counterfeit Access Device and Computer Fruad Abuse 0f 1984，參洪光煊，從電腦犯罪談未來刑法修正方向，刑事法雜誌第 32 卷第 3 期，1988 年 6 月，頁 70；李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 139 以下；莊忠進，電腦犯罪立法之探討，刑事科學第 39 期，1995 年 3 月，頁 108。

[167] 該法將以下三種情形列為處罰對象：

(1) 意圖損害美國聯邦的利益或為外國的利益使用或足認有使用之虞，而故意無權或越權進入電腦而取得基於聯邦政府總統的命令或法律規定因國防、外交上的理由所管制的資訊，以及 1954 年原子能法案第 11 節所規定的秘密檔案(data)者。

(2) 故意無權或越權進入電腦而取得 1978 年財產上隱私權法(聯邦法典第 12 編第 3401 條以下)所規定含有金融機關財產紀錄的資訊以及公正信用報告法(聯邦法典第 15 編第 1681 條以下)所規定含有消費者信用資訊機關檔案中與消費者相關資訊者。

(3) 故意無權或越權進入電腦而使用、竄改、破壞、洩漏其內部資訊，以及妨害該電腦使用權人的使用。惟以該被進入的電腦必須是為聯邦政府運作，且以上行為對其運作產生影響之情形為限。

參 18 U.S.C.A. §1030 (a) (1)、(2)、(3) (1985)，山口厚，アメリカにおけるコンピュータ犯罪処罰法，ジュリスト 846 号，1985 年 10 月，頁 35。

[168] 該法認為電腦(Computer)是「依電氣、磁氣、光學、電氣化學或其他方法高速處理資料，具有邏輯、算數運算以及記憶機能的設備，以及與其直接連接或共同運作的資料記憶設備以及通信設備。惟自動打字機、小型計算機及其他類似裝置不在此限。」參 18 U.S.C.A. §1030 (b) (1985)，山口厚，アメリカにおけるコンピュータ犯罪処罰法，ジュリスト 846 号，1985 年 10 月，頁 35。

[169] 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 139。

[170] 擴張處罰至「故意對聯邦政府部門或機關的電腦連線(Access)，使該電腦的運作受影響」、「意圖詐欺而故意對與聯邦政府相關的電腦連線(Access)，並獲得不法利益」、「意圖詐欺而販賣密碼或相關資料，使州際或國際貿易受影響、或該些資料是用於與聯邦政府有關的電腦」等行為。參山口厚，アメリカにおけるコンピュータ・データの刑罰による保護，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 549 以下；李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 139-140。

修正後一來因限定保護對象為與聯邦利益或與貿易有關的電腦犯罪行為，二來並無州際管轄權以及主觀犯意難以認定等問題，使得實際上仍無法發揮其效果[171]。同時，美國各州州法有鑑於聯邦法規範的實質無力化，對於電腦濫用行為的犯罪化皆有所修正甚至單獨立法，反而相較於聯邦刑法在適用上有更大的彈性[172]。

於 1994 年，由於上次立法過後發生數起重大事件[173]，導致美國聯邦政府於接納 1984 年後的各種建議，將原先處罰的六種犯罪類型更加精緻化。然而本次修正亦未擴張處罰至單純無權進入的行為[174]。

在 1996 年間，美國聯邦政府為制定「國家資訊基礎保護法(The National Information Infrastructure Protection Act of 1996)」，再次修正電腦詐欺及濫用法，將規制類型擴張至 11 種類，並特別處罰入侵「被保護的電腦(protected computer)」的行為[175]。本次修法的重點除訂立與電腦病毒有關的處罰規定[176]、將「州」的範圍擴大至包含「其他共和國」以防制跨州或跨國網路犯罪[177]外，最重要的修正不外乎是處罰「單純的入侵行為[178]」，縱使該入侵被保護電腦的行為並無造成損害，或雖造成損害卻非因故意過失亦同。同時，為保障規範實施上具有成效，亦處罰如走私被保護電腦的密碼或類似資訊，以及於國際商務上散布訊息恐嚇將破壞被保護的電腦等行為[179]。

---

171 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 140；李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 191。

172 林幹人，現代の経済犯罪—その法的規制の研究—，弘文堂，1988 年 4 月，頁 192。

173 分別為刺探美國軍情的 Markus Hess 案、以自製病毒攻擊極大多數電腦的 Morris Worm 案、以及駭客集團攻擊電信公司電腦的 Legion of Doom(LOD)案等，參李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 191 以下。

174 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 192。

175 所謂被保護的電腦係指：

1. 專屬於美國政府或金融機構所使用的電腦，或雖非政府及金融機構所使用，然於其使用時為犯罪，此犯罪會導致金融機構或政府使用電腦受影響者。
2. 任何用於州際及國際商務通訊用的電腦。

參 18 U.S.C.A. §1030 (e) (2) (1996)，李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 142；李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 192。

176 18 U.S.C.A. §1030 (a) (5) (1996)

177 18 U.S.C.A. §1030 (e) (3) (1996)

178 18 U.S.C.A. §1030 (a) (1)-(a) (3)、(a) (5) (1996)

179 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁

2001 年時，美國受到 911 恐怖攻擊事件的影響，國會開始以法律來擴張國家權力，立法通過各項法案以對抗恐怖主義。其中於 2001 年 10 月 26 日通過的愛國者法案(USA Patriot Act)，其為因應預防恐怖主義，並為增加政府機關資訊系統的安全度，有效防止恐怖分子藉由破壞網站等入侵行為癱瘓美國電腦系統，而規定對於 IP 及電子郵件等通訊監聽程序[180]，並促使美國國內通過各項加重刑責的電腦(網路)犯罪規範，至此美國的整體規制有重刑化的傾向，並且美國也早於 1995 年起即已漸漸開始嘗試透過國際壓力使其他各先進國家亦制定處罰電腦(網路)犯罪的條文，以透過雙罰規定利於國際間的互助[181]。

第二款 州法立法背景–四個時期、四個階段

美國法制是秉持著實用主義為基礎，以如何才能有效使刑事政策發揮效用為目標，並不考慮任何處罰依據在理論上的基礎[182]於本文討論我國立法沿革時已有述及，而刑事政策往往與當時社會發展的歷史背景有一定程度的關聯性，故似可認美國法的立法背景即與其社會發展背景有所關聯。在此有論者即依照其立法背景與社會發展背景的交錯，將美國法的立法動向分為四個階段討論，第一及第二階段發生於 1970 年代後半至 1980 年代中期、第三階段發生於 1980 年代後半至 1990 年代中期、第四階段則約於 1990 年代後半至 2000 年代[183]。相較於聯邦法僅有一部而可以以修法時間性來做分析，州法可謂五花八門，用宏觀的立法規制趨勢來分析應較能反映其變革。故在此本文即參考論者所提出的分類架構，並在適當加上補充後，依序探討州法立法背景的沿革。

一、 第一階段–電腦資源的保護

192。

[180] 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 145。

[181] 如透過 G8 高峰會使日本制定不正連線禁止法等。参河原淳平、角野然生，サイバー空間上の犯罪対策への国際的取組み，警察学論集 53 巻 8 号，2000 年 8 月，頁 73 以下。

[182] 吳文君，妨害電腦使用犯罪行法規制之分析—以保護法益為中心，國立台灣大學法律學院法律學系碩士論文，2010 年 6 月，頁 8。

[183] 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向—無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 102 以下。

此階段中個人電腦已發明然而卻尚未普及，因此此時期的電腦本身即為稀有價值之物，通常僅有在大學或是特殊研究機關等大型機構才有設置，並由研究人員或大學學生等使用者依照時間嚴格限制輪流使用。而因為電腦本身的稀有性以及必須分享使用，故將電腦資源的侵害作為主要的處罰對象為歷史所必然[184]。據此，對於電腦系統本身以及將其所包含的電腦資源即列為此時期主要的保護法益，為達成此種目的，於美國亦不乏直接處罰「單純無權進入電腦而不具其他目的」行為的法律[185]。然而，此時認為單純無權入侵行為不應與犯罪相繩的立法例亦所在多有，但此些立法例仍不乏將「以電腦系統的妨害等目的而為的無權侵入」行為作為處罰對象者[186]。

二、　第二階段–物的財產利益的保護

進入此階段時，個人電腦已開始普及化，雖然並非非常普及，但一般公司以及個人利用電腦系統進行金融處理已如家常便飯，而電腦漸漸被認為是一種會大力影響現實世界經濟利益的「道具」。此時的電腦犯罪規制，有以下數種類型：電腦詐欺(Computer Fraud)、資訊不當更改(Unauthorised Amemmdment or Deletion of Data)、資訊竊盜(Theft of Information)、為實行以上手段而為的不正入侵[187]。由上可知，此時的電腦犯罪規制重點，並不在電腦不正使用的本身，而是在電腦不正使用的目的。因電腦的使用普遍後，常攸關巨大經濟利益，從而美國對於使用電腦危及巨大經濟利益的行為作入罪化的措施，以保護該巨大的財產利

---

[184] 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 102。

[185] 例如當時南卡羅萊州法即規定:「所謂電腦入侵(computer hacking)，係指非意圖於連接(contact)確定後為詐欺或其他犯罪行為，且非利用除連接確定時所附隨服務以外之電腦關聯服務，僅單以連接確定為為目的，所對於電腦(computer)、電腦系統(computer system)以及電腦網路(computer network)之全部或一部為連線(access)者。」

[186] 例如 1978 年亞利桑那州的電腦犯罪法(亞利桑那州法律及第 13 編第 23 章)2316 條 B 項規定將「故意無權限或逾越權限而連線(access)電腦、電腦系統、電腦網路，以及含有以上三者的軟體(software)、程式(program)與資料(data)，並將其改變、毀損以及破壞」的行為作為電腦詐欺罪處罰。此雖以電腦詐欺罪為名，實際卻是無故入侵電腦罪以及取得、刪除或變更電磁紀錄罪的合體。參夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 93、102(註 38 處)。

[187] 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 101。

益。

三、　第三階段–智慧財產權的保護

在第三階段中，美國對於智慧財產權的保護意識興起，從而此時為有效保護智慧財產權，將意圖無權限的獲得與使用智慧財產，或意圖洩漏商業機密而無權進入電腦等行為皆納入電腦犯罪[188]。此時期的特徵為，法律所保護的重點已不僅為有形的物的利益，而移動至兼及無形的財產權以及情報本身的保護上。惟，在此並非僅有州法對此有保護，聯邦法於著作權法等特別法中亦混雜著相關處罰規定，若無有條理的檢索工具，很可能會產生一罪二罰的情形[189]。

四、　第四階段–以間接的方式保護

自第一階段至第三階段觀察，法律所保護的對象皆是經由電腦為犯罪工具而所侵害的背後利益，亦即「以直接方式保護」該些利益。但在進入第四階段後，法律所保護的對象並非對該些利益的連線行為，而是「為與該些對象連線而迴避或解除電子防護」的行為，亦即「電子防護措施」本身。據此，以往的入侵後違犯其他犯罪之態樣可拆解為「破壞防護措施」、「破壞成功後的連線行為」、「連線成功後的犯罪行為」三個階段，破壞成功後的連線行為於新架構下即應理解成破壞防護措施行為的與罰後行為，而連線成功的犯罪行為則與破壞防護措施是不同的犯罪構成，在此是以一罪論或數罪論，則是競合上的問題而已[190]。據此，此階段的保護重點在於防護措施，然對防護措施的保護間接保護了保護措施背後的經濟或智慧財產等利益，故稱「以間接方式為保護」。

第三款 規範特色之分析

---

[188] 例如佛羅里達州的電腦犯罪法即明文規定將商業機密的保護做為電腦犯罪的保護對象。

[189] 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 101。

[190] 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月，頁 100-101。

綜合以上所述，可以得知美國立法例的三點特色。首先，由於美國刑法僅是為實現刑事政策，並不著墨於保護法益的問題，亦即法律保護的對象可以依照增修法甚至刑事政策的需要而變遷，可謂非常有彈性。此種有彈性的法律在延遞持續的性質上，雖從時常要以判例補充甚至修法的角度觀察可謂幾乎沒有遞續性可言，然而就其全然不在意保護法益的法體系角度觀察，在多數情形只要以判例補充即可，似可認為美國法才是很能發揮延遞持續功能的法律。

再者，就美國法的增訂修正會伴隨著社會變遷此點作分析，可以發現美國的電腦犯罪發展史，幾乎可以與社會電腦使用文化的發展史相重合，而美國是電腦發源地，現今亦是電腦發展大國，故美國法對於電腦犯罪的敏感度應是走在全球的最先端。據此，若未來對於電腦犯罪的新興問題有討論或特別立法規制的必要時，美國法應是很重要的參考指標。

最後，雖美國法並不強調保護法益的概念，但是從上述州法的分析來看，美國州法對於電腦犯罪仍然有特定的保護對象，且該保護對象變遷到最後，甚至在結論上可能跟採大陸法體系的國家相同[191]，甚至更加具有超越性。

第二項 德國法

相較於美國法，德國法則是大陸法體系立法例的代表，並在立法的思考上，與美國正好截然不同。德國同樣在 1970 年代末期開始漸漸面臨了類似於美國的電腦犯罪問題，然而一來因德國刑法本即有強烈的拘謹性格，二來因德國於電腦犯罪的定義基本上是採狹義說，已將電腦犯罪類型的範圍限縮在利用電腦而侵害財產法益的犯罪上[192]，故其對於電腦犯罪的處罰則是偏向盡量不對法律作新增或修正的保守作法[193]。而德國在因應電腦犯罪於法律上所作的措施中，最具代表性的即是第二次經濟對策法，故以下即以第二次經濟對策法為重點，輔以其他特別

[191] 都是脫離背後的經濟利益，而專對「電子防護措施」作保護。
[192] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 194。
[193] 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 43。

規定，對德國立法例作分析。

第一款 立法背景–以第二次經濟對策法為中心

由於德國法制上的拘謹緣故，導致其面臨電腦犯罪時，所思考的角度即是環繞保護法益，若此類犯罪的保護法益並不明確，則僅能考慮如何使現行法能夠適用在電腦犯罪上的問題。從而，基於德國對電腦犯罪採狹義說，似乎認為電腦犯罪僅是行為人侵害財產法益的工具，並且在找不出獨立於傳統刑法的保護法益後，進而開始檢視傳統刑法上的漏洞以及補充漏洞的手段，使現行刑法亦能解決電腦犯罪問題。經過約 10 年的討論，遂於 1986 年 5 月 15 日通過「第二次經濟對策法(Zweites Gesetz zur Bekampufung der Wirtschaftskriminalitat vom 15. 5. 1986)」，並於 1986 年 8 月 1 日施行[194]，以電腦詐欺罪(Computerbetrug，刑法第 263 條 a)以及電磁紀錄偽造罪(Fälschunggespeicheter Daten，刑法第 269 條)為中心，將現行法典上若干規定追加補充[195]。

其中電腦詐欺罪(刑法第 263 條 a)的部分，由於向來詐欺罪的構成要件必須使「被詐欺者陷入錯誤」，然而依照邏輯運算而運作的機械並不會「陷於錯誤」，故不會成立詐欺罪[196]。而若要以竊盜、侵占、背信罪來處理皆有困難，故增訂電腦詐欺罪，規定「意圖為自己或第三人得財產上之不法利益，而製作不正電腦程式，使用不正確、不完全、無權限使用的資料或以他法干涉資料處理過程，使資料處理結果受影響，而損害他人財產」的行為亦成立犯罪[197]，並使用不同構成要件要素與普通詐欺罪以示區別[198]。

---

[194] 井田良，西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 591。

[195] 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 43。

[196] 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 44。

[197] 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 164-165；井田良，西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 600。

[198] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 196 以下。

於電磁紀錄偽造罪(刑法第 269 條)部分，由於傳統刑法偽造文書罪構成要件中「文書」的要件，是以「依視覺的可讀性」為必要[199]，但電磁紀錄本身僅係磁性的排列，無法由人類肉眼直接辨識讀取，因此無法該當文書要件，而產生處罰上的漏洞。故於第二次經濟對策法中即增訂刑法第 269 條，將「意圖於法律事務往來中使用詐術，而無權偽造、變造或行使在法律事務往來中資訊處理時對於預定作為證明法律上重要事實的電氣、磁氣及其他不可視或無法直接讀取的資料[200]」的行為入罪化。於本條增訂後，意圖使他人受不利益而無權變更或隱匿作為證據的電磁紀錄行為，亦會以適用範圍較廣的第 274 條第 1 項的文書毀棄隱匿罪所處罰[201]。另一方面，德國於 1997 年 7 月通過的「資訊服務與通訊服務法規環境法(Gesetz zur Regelung der Rahmenbedingungen für Informations und Kommunikations dienste)[202]」，其中於第四章修改刑法的規定內，將刑法第 11 條第 3 項文書的概念做了相當大的擴充。據此，只要是任何電子、電磁、光學、化學或其他資料儲存物，只要含有思想內容，即與文書同義，得做為沒收以及禁用的客體[203]。

此外，關於電腦破壞(Computer sabotage)的行為，與電磁紀錄的儲存媒體為物理上的破壞相同，德國通說認為有第 303 條的器物毀損罪可以規範[204]。然而一來器物毀損罪僅有 2 年以下有期徒刑的規範，但電磁紀錄的毀損卻可能對企業造成致命性的打擊[205]，二來當電磁紀錄離開儲存媒體後則是以無體物的方式存在，

---

[199] 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 44。

[200] 井田良，西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護，刑法雜誌 28 巻 4 号，1988 年 7 月，頁 610。另法條翻譯部分參考李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 196 以下。

[201] 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 166。

[202] 謝銘洋、陳曉慧，德國對網路服務之新規範—資訊服務與通訊服務法(多元媒體法)，月旦法學雜誌第 36 期，1998 年 5 月，頁 83。

[203] 謝銘洋、陳曉慧，德國對網路服務之新規範—資訊服務與通訊服務法(多元媒體法)，月旦法學雜誌第 36 期，1998 年 5 月，頁 89；李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 198(註 19 處)。。

[204] Ulrich Sieber, Computerkriminalität und Strafrecht, 1. Auflage 1977 und 2. Auflage 1980. S. 191 f.，轉引自井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 43(註 9 處)、46。

[205] 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 43。

若對網路上傳送的資料為變更，即不可能被論以第 303 條的罪名[206]。為填補此類法律漏洞，於修正後刑法增訂第 303 條 a，規定處罰刪除、隱匿、修改電磁紀錄或致令不堪用的行為。又，有鑑於對政府或經濟部門的電腦破壞行為，很可能會造成該商號或政府機關具毀滅性的影響，此種破壞對經濟所造成的影響甚大，故刑法新增第 303 條 b，將「對他人經營的商號、公司或官署之重要資料處理，為(一)第 303 條 a 的行為，或(二)破壞、損壞、致令不堪用、刪除、變更資料處理設備或資料儲存媒體的方式以妨礙資料處理」的行為加重處罰[207]。

至於電腦間諜(Computerspionage)部分，向來是由不正競爭防止法(Gesetz gegen den unlauteren Wettbewerb)以及著作權法(Urheberrechtsgesetz)等法律保護[208]，雖不致無法可罰的情形，然為更全面的保護對他人電腦內資料的不正取得，於修法後新增電磁紀錄不正取得罪(第 202 條 a)，將「為自己或他人而無權限取得有特殊安全保護裝置的電磁紀錄」的行為納入處罰規範[209]。

第二款 規範特色之分析

綜合以上，德國立法例亦具有以下三點特色。首先，德國法所在著重者雖並非使用電腦的利益，而皆是因電腦的使用後，所帶來龐大的經濟利益。此種思維幾乎完全迴避將電腦的使用利益作為保護對象，純粹將此現象以傳統刑法做規範[210]，實則提供一個與美國立法例完全相反的衝擊性思考，就急於將電腦犯罪訂定獨立專章來處斷的台灣，似乎也應該回過頭來冷靜想想，電腦犯罪是否真有必要

---

[206] 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年，頁 166。

[207] 井田良，西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 622。另法條翻譯部分參考李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 197。

[208] 不正競爭防止法原僅對侵害業務上秘密的行為處罰，但之後 1982 年的修正草案將處罰範圍擴大。參井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月，頁 43。

[209] 在此的「取得」雖包含單純入侵以及資訊的刺探，然並不包含處分權的獲取。參李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 198。

[210] 其實從修正案的名稱即可窺知一二，修正案的名稱即是為防制「經濟犯罪」而非「電腦犯罪」，並且於修正法條的呈現上，亦無出現「自動化資料處理系統(EDVA)」等相類詞彙，可見德國刑法本次修正的目的並非處理我國或美國所謂的「電腦犯罪」，而僅是補充舊刑法，因應時代而追加文義來填補漏洞而已。

作為特別獨立處罰的犯罪。並且就遞續性的角度觀察，因德國刑法本次修正並未對電腦犯罪提出任何嶄新見解，故此些「電腦犯罪」行為仍然僅涉及傳統犯罪的保護法益，於未來即使電腦發展成任何態樣，似對於此類規制並無太大影響，故本次新修法律堪稱具有遞續性。

再者，德國刑法本次的修正完全是一類型化立法方式的呈現，而此種立法方式，論者有謂是一成功類型化電腦犯罪的法制[211]。我國電腦犯罪的立法雖亦為類型化的思維，但二者的差別即在於德國並未訂立獨立罪章，而是嚴守傳統規制模式以及保護法益，並試圖補充傳統規制所不足處；我國則是以「欲入罪化的行為」為中心，並輔以傳統刑法，且毫不考慮地將即使做補充仍無法被傳統刑法所規制的行為態樣硬是歸類到新罪章處罰。故從德國的立法模式，亦可以看出我國立法於傳統刑法體系上的缺失。

最後，德國刑法的修正條文中，有對於他人經營的商號、公司或官署重要資料處理為毀損而加重的規定，其規定理由是由於公司以及政府機關的電腦，往往掌控著大量公眾或經濟上的資訊，對於此類資訊的破壞行為無異對社會的運作或經濟上造成巨大影響，故應加重處罰。對此，我國妨害電腦使用罪雖亦有類似的規定[212]，然而立法理由竟相差甚遠。從而於具體檢討我國妨害電腦使用罪章時，本條似有極大的參考價值。

第三項 日本法

地理位置位於德國與美國之間的日本，其對於電腦犯罪的處理態度似也如同其地理位置般，介於德國與美國之間。於初期因三和銀行案而導致刑法修正時，面對電腦犯罪的態度以及規制方式類似於德國立法例，而於不正連線禁止法頒布施行後，該不正連線禁止法與之後各次修正所呈現的態度以及規制方式反而較偏向於美國法。至於為何日本立法例上會出現此種形式的轉變，以及此種轉變對日本對電腦犯罪規制的影響等，即是以下各款要分析的重點。

---

[211] 李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 198。
[212] 中華民國刑法第 361 條參照。

第一款 立法背景–三和銀行案、不正連線禁止與病毒作成罪

一、 三和銀行案所導致的刑法一部修正

在 1981 年發生震驚日本社會的三和銀行案[213]後，日本刑法界有如受到極大刺激般，開始反思刑法的修正的必要性。因三和銀行案的被告係利用電腦更改電磁紀錄，導致電磁紀錄所表彰的財產數量有變。大阪地方法院雖技術性的以「欺騙行員」以及將電磁紀錄解釋為私文書等論述，將被告以詐欺罪以及偽造私文書罪論處，但如前述德國立法例部分，就詐欺部分電腦為機器，機器不會因為行為人施用詐術而「陷於錯誤」。又，就偽造私文書部分，電磁紀錄亦不具「視覺可讀性」，從而本案被告依當時日本刑法，理應因構成要件不該當而不成立任何犯罪。惟此種結論並無法使當時的日本社會所接受，因而意味著日本刑法可能存在著處罰上的漏洞[214]。據此，日本在經過數年的討論以及意見交換後，於 1987 年對刑法進行一部份的修正，對電腦犯罪的防制做一個徹底的總檢討。

在 1987 年刑法修正前，早期學界以及實務界對於電腦犯罪的認定皆是以廣義說為主，並且試圖以歸納現有案例的方式，將電腦犯罪劃分出一個較為清晰的輪廓。其中於學界部分，有學者極度擴張電腦犯罪的範疇，認為「與電腦有關的犯罪」即是電腦犯罪[215]，而將其分為操縱電腦、危害電腦、洩漏或竊取電腦所得資料而用於不良目的三種行為類型[216]；亦有學者參考上述見解以及當時警察廳的實務見解，並加上自己補充後限縮電腦犯罪的範圍至「對電腦系統的犯罪或將電

---

[213] 三和銀行案的概略經過係 1981 年時，三和銀行某分行的女職員，操作該分行電腦於其他分行開設空頭帳號，進而竄改帳簿紀錄，導致該戶頭擁有一億八千萬日圓的存款，其後即分別提領。參李茂生，電腦犯罪與資訊政策，國家政策雙月刊第 125 期，1995 年 11 月，頁 5。

[214] 事實上，日本於 1970 年代末期-1980 年代初期時，伴隨著電腦的快速發展，除三和銀行案外亦曾發生過許多與電腦相關的案件，並造成當時社會上的恐慌，如利用電腦做假帳虛報補償金的佐藤工業案件、利用電腦製作架空借貸案以侵占銀行財產的北濱信用卡案件，以及利用電腦偽造假駕照以販賣的秋田縣警案件等，詳參鳥居壯行，コンピュータ犯罪とシステム監査，ジュリスト 834 号，1985 年 4 月，頁 34 以下；篠崎和紀，コンピュータ・セキュリティ対策の現状と課題，ジュリスト 834 号，1985 年 4 月，頁 8 以下，表 2 處。

[215] 板倉宏，コンピュータ犯罪と刑事法，ジュリスト 707 号，1980 年 1 月，頁 144。

[216] 板倉宏，コンピュータ犯罪と刑法，法学セミナー26 巻 7 号，1982 年 7 月，頁 100。

腦系統不正使用的犯罪」，並將前述學者分類加上 CD 犯罪[217]的分類[218]，更有論者將其依自己主觀的理解分為對電腦作(物理或非物理的)破壞、竊取電腦、盜用資訊、作為侵占或詐欺的手段而利用、不正利用電腦使用時間等類型[219]。其後，於 1980 年代前期開始有學者將問題作簡化以及聚焦，認為電腦犯罪是「以電腦相技術知識為必要所違犯的犯罪行為」，並僅認為僅有惡用電腦以及危害電腦兩種類型[220]；亦有學者更進一步參考前述 Sieber 氏的見解，將電腦犯罪分類成電腦操縱、電腦間諜、電腦破壞以及電腦竊用[221]。於實務界部分則大多是採用日本警察廳的定義，認為電腦犯罪是「對電腦系統的犯罪以及將其惡用的犯罪」，並且依照事例先行區分為「CD 犯罪」以及「非 CD 犯罪」[222]，在後者底下又區分為「輸入不正資料」、「以不正方法取得資料(DATA)或程式(PROGRAM)」、「電腦破壞」、「電腦不正使用」、「程式的改竄」、「磁帶等電磁紀錄物的損壞」六類[223]。然於 1980 年代早期時，實務上亦有對此種分類提出反思者，其見解亦較趨向後期學說參考 sieber 氏的四種類分類方式[224]。

綜上，將 1980 年代早期的分類與傳統分類相互比較後，傳統較著重於「與電腦相關的反社會行為」，而 1980 年代早期的分類較著重於「對電腦機能的妨害」上，而日本法制審議會於修法時即是參考後期的分類為修法[225]。

---

[217] CASH DESPENSER 犯罪的簡稱，有中譯為提款卡犯罪或金融卡犯罪者，參謝開平，電腦犯罪之研究–我國現行法之適用與修正草案之檢討，國立中興大學法律學研究所碩士論文，1995 年 7 月，頁 30；李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 228。

[218] 大谷実，コンピュータ犯罪(上)，法学セミナー363 号，1985 年 3 月，頁 21 以下。

[219] 金井浄，コンピュータ犯罪とエラー，ジュリスト 707 号，1980 年 1 月，頁 154 以下。

[220] 高石義一，コンピュータ犯罪の防止技術–メーカーの立場から，ジュリスト 834 号，1985 年 4 月，頁 39。

[221] 曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 468 以下。

[222] 會先做如此大分類，是因為當時日本除 CD 犯罪外，其他與電腦相關的犯罪被發現的數量非常少，與 CD 犯罪件數的比例相當懸殊。參伊賀興一，コンピュータの普及と刑事法の対応をめぐる諸問題，ジュリスト 846 号，1985 年 10 月，頁 54 以下；広畑史朗，コンピュータ犯罪の実態とその対策–犯罪捜査の面から–，ジュリスト 834 号，1985 年 4 月，頁 26 以下。

[223] 広畑史朗，コンピュータ犯罪の実態とその対策–犯罪捜査の面から–，ジュリスト 834 号，1985 年 4 月，頁 26 以下。

[224] 的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 7 以下。

[225] 莊凱閔，論不法侵入他人電腦系統之刑事責任–以日本法制為中心–，國立台北大學法律研究所碩士班碩士論文，2002 年 6 月，頁 69。

於 1987 年時，有鑑於伴隨金融機械化的快速[226]，電腦相關的犯罪案件數量日益增加，除可能危害多數人的生命或身體[227]外，亦可能使多數人造成財產上的損害，以及經濟秩序、社會秩序的混亂等嚴重後果[228]，故日本法制審議會為因應社會上的緊急需要，即提出了五點修正建議–偽造、變造或毀損文書罪相關修正；妨礙業務罪相關修正；財產得利罪相關修正；增訂電腦資料(DATA)的不正取得、洩漏罪；增訂電腦竊用罪[229]。然而，於正式修法的討論過程中，於電腦資料不正取得、洩漏罪增訂的建議部分，討論結果認為因要以何種觀點將其入罪化，以及要如何訂定其構成要件、保護對象的範圍以及行為類型等問題應探討的點極多，故並未新增處罰規定[230]。與此結論相同，於增訂電腦竊用罪部分，討論結果認為於行為類型應如何限縮，以及與其他機械、裝置等的竊用處罰的均衡性皆是需要妥善考慮的問題，從而於此部分亦未新增處罰規定[231]。最後，本次修正結果除對偽造、變造文書罪、毀損文書罪、妨礙業務罪以及財產得利罪作新增補充規定外，亦有新增電磁紀錄的定義[232]。

就偽造、變造文書罪增訂的部分，有鑑於修正前實務上本即有將電磁紀錄視為文書處理的見解存在[233]，本次修正即有意將一部份的電磁紀錄視為文書處理，故修改有關使公務員登載不實罪(刑法第 157 條第 1 項[234]以及第 158 條)的部分，

---

[226] 井上純夫，金融機械化システムの安全対策，ジュリスト 834 号，1985 年 4 月，頁 12 以下。
[227] 如破壞或干擾自動列車運行控制系統，或航空管制系統等。
[228] 竹内直人，コンピュータ・システム安全対策についての警察の対応，ジュリスト 834 号，1985 年 4 月，頁 20 以下。
[229] 西田典之，コンピュータと業務妨害・財産罪，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 511 以下。
[230] 曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 467。
[231] 西田典之，コンピュータと業務妨害・財産罪，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 511 以下；曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 467 以下。
[232] 日本刑法第七條之二規定：「電磁的記録とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。(電磁紀錄係指依電子方式、磁氣方式或無法憑他人知覺所能認識之方式作成之記錄，以供電子計算機處理資料用者而言。)」
[233] 大谷実、古田佑紀、西田典之，コンピュータ犯罪と刑事立法の課題，ジュリスト 846 号，1985 年 10 月，頁 19；的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 9 以下。
[234] 本項原文為：「公務員に対し虚偽の申し立てをして、登記簿、戸籍簿その他の権利若しくは義務に関する公正証書の原本に不実の記載をさせ、又は権利若しくは義務に関する公正証書の原本として用いられる電磁的記録に不実の記録をさせた者は、5 年以下の懲役または 50 万円

將使登載不實的對象延伸至「作為公證書正本之用的電磁紀錄」，以及新增電磁紀錄不正製作、行使罪(刑法第 161 條之二第 1 至 3 項)，在第 1 項規定「意圖使人錯誤處理事務，不正製作供該事務處理用之與權利、義務及事實證明相關電磁紀錄者，處五年以上懲役或五十萬元以下罰金[235]」，並在第 2 項規定不正製作公務員應製作的電磁紀錄時的處罰，以及第 3 項所規定的行使該些電磁紀錄時的處罰。

於妨礙業務罪增訂的部分，本次修正因立法者認為若侵害處理大量資料或巨額財產價值的電腦為侵害，相較於以往對人的業務妨害類型更為嚴重，而有加重處罰的必要[236]，故增訂損壞電腦妨礙業務罪(刑法第 234 條之二)，規定「損壞他人業務上使用之電腦或供其使用之電磁紀錄，對他人業務上使用之電腦輸入虛偽情報及不正指令，或以他法使電腦不為與使用目的相符之動作，及違反使用目的之動作，而妨害他人業務者，處五年以下懲役或一百萬元以下罰金[237]」。又，當時日本刑法第 234 條的行為客體，因當時的時空背景下只規定以妨礙他人的行為為主，對於以破壞電腦妨礙業務這種以物為客體的行為即會產生規制漏洞，故意增訂此規定[238]。並且，於增訂過後，實務上亦發展出「不僅是對電腦為物理的損壞，若將程式修改或刪除以致妨害業務亦成立本罪」的見解[239]。

而財產得利罪增訂的部分，由於電腦已開始介入日常生活處理各項金融業務，

以下の罰金に処する。」，在此有論者將其略譯為「公務員於關權利、義務之公證書原本之電磁紀錄為不實之記載者」，似認為本罪為公務員主動為不實登載，然「公務員に対し虚偽の申し立てをして」一句應作「對公務員作虛偽的聲請」解，並觀察此項的構成要件，應認為係使公務員登載不實為妥。參莊凱閔，論不法侵入他人電腦系統之刑事責任–以日本法制為中心–，國立台北大學法律研究所碩士班碩士論文，2002 年 6 月，頁 72；西田典之，刑法各論，弘文堂，2010 年，頁 358 以下。

[235] 原文為：「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、5 年以下の懲役または 50 万円以下の罰金に処する。」

[236] 川端博，刑法各論概要，成文堂，2007 年，頁 207 以下。

[237] 本條原文為：「人の業務に使用する電子計算機もしくはそのように供する電磁的記録を損壊し、もしくは人の業務に使用する電子計算機に虚偽の情報もしくは不正な指令を与え、またはその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、または使用目的に反する動作をさせて、人の業務を妨害した者は、5 年以下の懲役または 100 万円以下の罰金に処する。」

[238] 川端博，刑法各論概要，成文堂，2007 年，頁 95 以下；曽根威彦，刑法各論，弘文堂，2008 年，頁 74 以下。

[239] 芝原邦爾，コンピュータ犯罪，法学教室 169 号，1994 年 10 月，頁 69。

然而刑法財產犯罪中如竊盜罪、詐欺罪、侵占罪並對此些類型無法適用與前述德國立法例產生的問題類似，故而增訂使用電腦詐欺罪(刑法第 246 條之二)，規定「除前條規定外，對他人事務處理用之電腦輸入虛偽情報及不正指令，而製作與財產權得喪變更相關之不實電磁紀錄，或將該與財產權得喪變更相關之不實電磁紀錄用於他人事務處理之用，並使自己或他人獲得財產上不法利益者，處十年以下懲役[240]」。應特別注意者為，本條構成要件之一是必須輸入「不實電磁紀錄」，故若輸入他人密碼或竊用他人電腦而獲得具有財產價值的資料等情形，皆無法與本罪相繩[241]。

最後，毀損文書罪增訂的部分，修正後的刑法有限度的放寬電磁紀錄的文書性，認為在「供公務用」以及「與權利義務相關」的情形下，若將該些電磁紀錄毀損，亦成立毀損文書罪(刑法第 258、259 條)。然而若是對於處理中或傳送中的電磁紀錄為毀損，則無法成立本罪，但可能成立妨礙業務罪[242]。又，若毀壞乘載電磁紀錄的媒體(如磁片、光碟等)，則是以器物毀損罪論處[243]。並且，在此之毀損並不一定是有形的毀損，若以隱匿或其他方法讓該文書或電磁紀錄呈現無法使用的狀態即足，且該種利用上的妨害亦不論是否為一時或永續，亦無關行為人是否有日後返還的意思[244]。

然而，本次修正並非即將電腦犯罪問題一勞永逸的解決，仍在修正條文中可以看見問題點的存在。首先，就立法過程而言，雖法務省刑事局於 1986 年 5 月以及 6 月後有召集學者以及電腦業界人士進行意見的陳述，而此種意見的陳述給了當時正努力研究電腦犯罪對策，但卻尚未完全掌握濫用的實際情形的學者專家一個很好的發言平台，然而在此之後的立法過程，不但未讓學者專家參與，甚至連讓他們知道「正在進行修法」的機會都沒有，並且在短短半年餘間，修正法案

---

[240] 本條原文為：「前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報もしくは不正な指令を与えて財産権の得喪もしくは変更に係る不実の電磁的記録を作り、または財産権の得喪もしくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、または他人にこれを得させた者は、10 年以下の懲役に処する。」

[241] 西田典之，コンピュータと業務妨害・財產罪，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 522-523；西田典之，刑法各論，弘文堂，2010 年，頁 209 以下。

[242] 中森喜彦，コンピュータと文書犯罪，刑法雜誌 28 卷 4 号，1988 年 7 月，頁 509。

[243] 山口厚，刑法各論，有斐閣，2003 年，頁 348。

[244] 川端博，刑法各論概要，成文堂，2007 年，頁 378。

即通過審議並公布施行[245]。此種可以說是倉促的立法，想當然在新修正的法律條文中會引起學者們不少意見[246]。而就保護法益的觀點而言，亦有認為電腦僅是人類生活的工具，該些電腦犯罪所侵害的法益，終局而言並未跳脫傳統法益，從而不管是否使用電腦犯罪，所侵害的法益亦無不同。而若著重於電腦犯罪所造成損害的規模極大，而成為加重處罰的理由，則電腦犯罪以外的犯罪若造成大規模的損害時，亦應加重處罰，否則會違反平等原則[247]。

再者，就各條修正後的問題而言。於偽造變造電磁紀錄部分，除有懷疑是否有如此提前處罰的必要之外[248]，所受到最大的批評即是法條文字中「不正」的曖昧性。日本刑法係採形式主義，原則上僅處罰無權限製作或改寫他人文書的有形偽造、變造行為，在例外的情形下始處罰有權限者製作或改寫虛偽內容文書的無形偽造、變造行為[249]。然而修正後條文的「不正」似包含有形及無形偽造，似有偏向實質主義的味道，似與現行刑法本旨有所違背[250]。並有學者參考德國立法例，認為本條應將「不正」的用語改為「無權限」為宜[251]。在電腦妨礙業務罪的部分，有認為此種修正僅是一種「電腦特權性」的修正，僅因為透過電腦妨礙業務可能造成極大損害，即新增條文並加重刑責，如此即對未使用電腦然卻同樣達到極大損害的業務妨礙行為的評價並不公平，故即使有處罰必要，亦應於原業務妨礙罪中，以「或以他法」等概括規定中做解釋或規定較妥[252]。亦有認為本條規定太過籠統，可能使如「占據電腦室，使人無法操控電腦」等未對電腦有直接物理影響的行為都被列入處罰[253]。更有認為法條中「使電腦不為與使用目的相符之動作，

---

[245] 神山敏雄，コンピュータ犯罪立法の批判的考察，法律時報 60 巻 1 号，1987 年 1 月，頁 75 以下。

[246] 以德國為例，德國的第二次經濟犯罪對策法的修正自開始思考對策至修正法條花費約 10 年的時間，日本本次修正相對而言非常倉促。

[247] 神山敏雄，日本の経済犯罪–その実状と法的対応–日本評論社，2001 年 7 月，頁 228 以下。

[248] 神山敏雄，コンピュータ犯罪立法の批判的考察，法律時報 60 巻 1 号，1987 年 1 月，頁 78。

[249] 西田典之，刑法各論，弘文堂，2010 年，頁 348 以下。

[250] 山口厚，電磁的記録と文書犯罪規定の改正–電磁的記録の不正作出(一六一条ノ二)を中心に，ジュリスト 885 号，1987 年 5 月，頁 7 以下；的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 11 以下。

[251] 其認為無法或難以判斷作成名義人的電磁紀錄，亦僅是單純的無形不正電磁紀錄而已，完全沒有異於偽造文書規定而對其特別保護的理由。參神山敏雄，コンピュータ犯罪立法の批判的考察，法律時報 60 巻 1 号，1987 年 1 月，頁 78 以下。

[252] 神山敏雄，日本の経済犯罪–その実状と法的対応–日本評論社，2001 年 7 月，頁 260 以下。

[253] 西田典之，コンピュータと業務妨害・財產罪，刑法雜誌 28 巻 4 号，1988 年 7 月，頁 516

及違反使用目的之動作」要件的「使用目的」此一用語不但意義曖昧不明，還極有可能導致法條適用的範圍偏離當初立法目的[254]。以及有就不同角度思考，認為既然此種運作系統的破壞對於社會影響甚鉅，可能可以從社會法益角度考慮創設新型態的犯罪類型[255]。而就電腦詐欺罪部分，受到最大的質疑即是與侵占罪的關係。若今行為人受正在外國出差中的友人所託，以友人銀行帳戶支付日常生活事務，行為人卻以支付名義將錢領出後自用，此情形會成立侵占而處以五年以下懲役；然於同樣情形下，若行為人未領出該金額，而轉帳到自己帳戶下，則會成立電腦詐欺罪並處十年以下懲役。此種就同一法益侵害，僅因使用電腦而刑度差異甚大，此種結果似乎並無說服力[256]。

最後，就美國於當時主要所處罰的入侵電腦以及電磁紀錄的不正取得等問題，本次修正並無特別規定處罰，至多就將電磁紀錄列印出來或用其他媒體存取後取走該列印結果或儲存媒體時，在用來列印的紙張或該儲存媒體為被害人所有的情形下才可能以竊盜罪處罰，或在該電磁紀錄有著作物性的情形下，以違反著作權法的罰則處理[257]。然而對此已有學者開始思考是否有獨立處理的可能性，為因應資訊社會的發展變遷，似可認為「資訊」為一種新興應加以保護的法益，並進而依照保護的重要性就秘密資訊的保護、隱私的保護、具財產價值資訊的保護三個角度，並個別探討如何立法將特定行為入罪化[258]。

二、 G8 高峰會所導致的不正連線禁止法修正

以下。

[254] 芝原邦爾，コンピュータによる情報処理と業務妨害罪–改正案二三四条ノ二の検討，ジュリスト 885 号，1987 年 5 月，頁 14 以下。

[255] 的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 15。

[256] 西田典之，コンピュータの不正操作と財産犯–改正案二四六条ノ二の検討，ジュリスト 885 号，1987 年 5 月，頁 19 以下；的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 12 以下；神山敏雄，コンピュータ犯罪立法の批判的考察，法律時報 60 巻 1 号，1987 年 1 月，頁 77。

[257] 會如此迂迴的處理跟日本不完全認為電磁紀錄為動產有關，參的場純男，コンピュータに関する刑事法上の問題点–主として立法的観点から，ジュリスト 846 号，1985 年 10 月，頁 13 以下；曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 470、475 以下。

[258] 曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月，頁 467 以下。

雖日本已因應電腦的普及化而制定相關條文因應電腦犯罪，然而該些條文並未將單純無權進入電腦的行為作規範已如前述，然而一方面由於 1990 年代中期時網際網路普及，人民對網路的依存度日漸增加，同時網路犯罪數量也大幅增加[259]，使得社會上漸漸出現了處罰單純無權進入電腦的反思聲音；另一方面受到國際間強勢國美國的發展方針，日本亦開始被美國要求制訂與無權進入電腦等相關的雙罰規定，以落實國際間的互助並進而根除網路犯罪[260]，故開始了一連串的規範修訂。於日本國內方面，早於 1996 年 4 月，警察廳即發表了「有關資訊系統安全對策之中間報告書」，其中即有以行政罰的角度提出對於不正連線行為的規制方式。並在經過一番田野調查等準備措施[261]後，警察廳於 1998 年 6 月發表「高科技犯罪[262]對策重點推進計畫」，將不正連線對策法制作為重點施政的對象之一[263]，並於同年 11 月發表「不正連線法制基本思考方向」，試圖藉由增修法律的方式來達到不正連線行為的規制[264]。在幾乎同一時點，郵政省從電氣通信安全的角度亦發表「對電氣通信系統為不正連線對策法制的觀點」，然而由於思考角度的不同，使得兩者版本出現分歧[265]。最後在雙方的協議整合下，於 1999 年 1 月向國會提出關於不正連線規範的新法案[266]。於國際方面，自 1995 年 5 月的高峰會

---

[259] 據調查，於平成五年(1993 年)僅有 32 件的網路犯罪，然而於平成十年(1998 年)即暴增到 415 件，參黒澤正和，不正アクセス行為の禁止等に関する法律の制定について，警察学論集 52 卷 11 号，1999 年 11 月，頁 3 以下。

[260] 李茂生，日本不法連線行為禁止法簡介，資訊安全通訊第 8 卷第 1 期，2001 年 12 月，頁 56 以下。

[261] 依當時的調查結果，有 84%的受訪者認為應由法律規制不正連線的行為，參不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月，頁 9。

[262] High Tech 犯罪(ハイテク犯罪)是於 1997 年 1 月美國開始採用，同年 12 月的華盛頓 G8 內務、司法部長會議時因美國的主導而開始廣泛使用的用語，參河原淳平、角野然生，サイバー空間上の犯罪対策への国際的取組み，警察学論集 53 卷 8 号，2000 年 8 月，頁 73 以下；李茂生，日本不法連線行為禁止法簡介，資訊安全通訊第 8 卷第 1 期，2001 年 12 月，頁 58。

[263] 於此時期警察廳對於不正連線的規制已有分為「不正連線之禁止、處罰」、「規制助長不正連線之業務」、「為不正連線之防止、搜索而與產業界的協力」三方向的雛形，參露木康浩，不正アクセス対策法制の在り方について―不正アクセス対策法制調査研究報告書を概観― 警察學論集 51 卷 7 号，1998 年 7 月，頁 33 以下。

[264] 露木康浩，不正アクセス行為の禁止等に關する法律について，ジュリスト 1165 号，1999 年 10 月，頁 51；不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月，頁 9-11。

[265] 北村博文 ,不正アクセス行為の禁止等に関する法律の制定の経緯 警察学論集 52 卷 11 号，1999 年 11 月，頁 15 以下；李崇偉，電腦網路入侵行為之刑事立法研究，中央警察大學法律學研究所碩士論文，2003 年 6 月，頁 97 以下。

[266] 不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008

中宣言對抗國際組織犯罪後，在 1996 年 6 月的高峰會提出國際組織犯罪對策的 40 項勸告中的第 16 項勸告即提到「希望處罰現代技術的濫用行為」[267]，進而於 1997 年 1 月由美國主導設置高科技犯罪分科會，並於同年 12 月於華盛頓 G8 內務、司法部長會議使會員國就「對抗高科技犯罪之原則與行動計畫」為合意。而此行動計畫的要求實施，即是在 1998 年 5 月伯明罕高峰會的時候所要求，且於 1999 年 10 月在莫斯科舉辦的第二次 G8 內務、司法部長會議中即要求 G8 會員國同意「關於對被藏置之電腦資料為跨國連線之原則」，並要求各會員國對於與高科技犯罪相關法制現狀為報告[268]。在國內與國外的雙重壓力下，於 1999 年 8 月即通過「不正連線行為之禁止等相關法律[269]」的審查公布，並於 2000 年 2 月(其中一部分是 7 月)開始施行[270]。而在開始施行的 12 年後，亦即 2012 年 5 月，由於網路普及的進展、網路犯罪情勢漸深、釣魚(フィッシング，phishing)[271]行為的激增、使用連續自動輸入程式為入侵行為的發現[272]，以及連線管理員所實施的防制措施仍不完備等因素，對於不正連線禁止法作了一次大規模的修正，除將既有條號順序以及刑度作調整外，亦將若干行為入罪化，並擴張本法的處罰範圍，不僅限於給予帳號密碼與不正連線的情形始有處罰必要[273]。

不正連線禁止法與舊有法制最大的差異在於，不正連線禁止法一改 1987 年修正時認為電腦犯罪只是侵害傳統法益，仍未侵害新興法益的角度，於規定立法目的的第一條「本法係規定不正連線行為之禁止與罰則，以及為防止其再度發生

年 10 月，頁 9 以下。

[267] 鈴木敏夫，ハイテク犯罪に関する国際動向–国際組織犯罪上級専門家会合における取組み–，警察学論集 51 巻 7 号，1998 年 7 月，頁 86 以下。

[268] 河原淳平、角野然生，サイバー空間上の犯罪対策への国際的取組み，警察学論集 53 巻 8 号，2000 年 8 月，頁 77。

[269] 下稱「不正連線禁止法」。

[270] 不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月，頁 13-19。

[271] 釣魚行為是指，行為人偽裝成連線管理人，以 E-MAIL 寄信或在網站上公開的方式「要求」使用者輸入帳號密碼，已獲得該些帳號密碼的行為。フィッシング(phishing)此一自創語源的由來，有認為是「釣魚(fishing)」的英譯與電話線路不當使用的「飛客 phreaking」合稱者，亦有認為是「password harvesting fishing」的簡稱者，參蔵原智行，「不正アクセス行為の禁止等に関する法律の一部を改正する法律」について，警察学論集 65 巻 6 号，2012 年 6 月，頁 40，註 11 處。

[272] 特別是指同一使用者對於多數網站為了方便皆使用相同帳號密碼的情形。

[273] 四方光，不正アクセス禁止法改正の背景・経緯及び不正アクセス対策の今後の課題，警察学論集 65 巻 6 号，2012 年 6 月，頁 14-15。

而由都道府縣公安委員會的援助措施等規範，期能防止經由電氣通訊線路對於電腦之犯罪，以及維持因連線控制機制而實現的電氣通訊相關秩序，以達高度資訊通訊社會的健全發展[274]。」中，即可以觀察出該法所保護的保護法益為「社會上對連線控制機制的信賴」[275]此一社會法益。且因為該法所保護的是新興法益的緣故，對於不正連線的行為是直接視為既遂犯處罰，而非視為其他傳統犯罪的預備犯處理[276]。同時一改舊法對於特殊專有名詞不特別訂定的態度，於第二條明定各個專有名詞的解釋，如「連線管理人」、「已連接電氣通訊線路之電腦(特定電腦)」、「識別符號」、「連線控制機制」等名詞。據此，本法所處罰的對象已大大限縮，例如對單機電腦為入侵的行為，以及對連線電腦以未經過電氣通訊線路的方式入侵的行為[277]皆非本法所要處罰的對象[278]。

本法於規制的部分，大體上可以分為兩個方向。其中一個方向為不正連線禁止的處罰等對行為人的對策(不正連線禁止法第 3、4、5、6、7、11、13 條及第 12 條第 1、2、3、4 款)；另一個方向則是為使被不正連線的連線管理人能夠架構良好的防護措施，以請求都道府縣甚至國家的援助等對防禦方的對策(不正連線禁止法第 8 至 10 條及第 12 條第 5 款)[279]。就對行為人的對策方面有幾個大方向的規範—處罰不正連線的行為人(第 3 條)、處罰不正取得他人帳號密碼的行為人(第 4 條)、處罰幫助不正連線的行為人(第 5 條)、處罰不正保管他人帳號密碼的行為人(第 6 條)，以及處罰不正要求他人提供帳號密碼的行為人(第 7 條)[280]。第

---

[274] 本條原文為「この法律は，不正アクセス行為を禁止するとともに，これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより ,電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現させる電気通信に関する秩序の維持を図り ,もって高度情報通信社会の健全な発展に寄与することを目的とする。」

[275] 露木康浩、砂田務、檜垣重臣，不正アクセス行為の禁止等に關する法律の解說，警察學論集 52 卷 11 号，1999 年 11 月，頁 32-33。

[276] 園田寿，不正アクセス，法学教室 228 号，1999 年 9 月，頁 42 以下；加藤敏幸，不正アクセス，刑法雜誌 41 卷 1 号，2001 年 7 月，頁 78 以下。

[277] 如趁使用權人離開忘了登出而竊用，或直接使用該電腦強行破除安全系統等未透過網路為之的類型。

[278] 大泉雅昭，不正アクセス行為の禁止等に關する法律の概要ついて，捜査研究 576 号，1999 年 10 月，頁 13-14。

[279] 檜垣重臣，不正アクセス行為の禁止等に關する法律，法律のひろば 52 卷 12 号，1999 年 12 月，頁 29。

[280] 亦即前述的釣魚行為。

一個方向又可大致分為兩種侵害態樣—利用他人帳號密碼而不正連線(第 3 條第 2 項第 1 款)，以及利用該連線控制機制的漏洞而不正連線(第 3 條第 2 項第 2、3 款)[281]。在侵入目的部分，由於本法並非立於傳統犯罪的預備犯角度，僅是單純處罰不正連線行為，故不論侵入目的為何皆一律處罰，於刑度部分在修法前本非重刑，對不正連線的行為人處一年以下懲役或五十萬日圓以下罰金(舊不正連線禁止法第 8 條第 1 款)，對幫助不正連線者亦僅處三十萬日圓以下罰金(舊不正連線禁止法法第 9 條)；但修正後日本大幅提高不正連線行為的刑度至三年以下懲役或一百萬日圓以下罰金(第 11 條)，對幫助不正連線者亦區分行為態樣，分別論以一年以下懲役或五十萬日圓以下罰金(第 12 條)或三十萬日圓以下罰金(第 13 條)。

而對防禦方的對策方面，有鑑於不正連線禁止法的立法目的是要營造一個健全的高度資訊通訊社會，從而可以得知這個理想的營造不應僅是課與不正入侵的行為人責任即可以解決的。故該法亦課與防禦方一些防禦或協助義務，以連線控制機制的連線管理人的防範檢察以及加強防禦等管理義務(第 8 條)為首，再進一步則可請求都道府縣的公安委員會做必要的協助(第 9 條第 1 項)，且該公安委員會得將事務的一部或全部委託他人為之(第 9 條第 2 項)，而該被委託者亦有守密義務(第 9 條第 3 項)，若違反者可處以一年以下懲役或五十萬日圓以下罰金(第 12 條第 5 款)。最後是就國家援助的部分，該法亦規定國家公安委員會、總務大臣以及經濟產業大臣，每年至少須對不正連線行為的發生狀況以及連線控制機制相關技術的研究開發狀況作一次以上的報告(第 10 條第 1 項)、對於連線管理人提供必要資訊及其他援助(第 10 條第 2 項)外，並要致力普及對於防禦不正連線的方法以及知識(第 10 條第 3 項)。

然而此二次修法仍存在著遺憾之處，自立法過程角度觀察，立法至施行這段

[281] 於此部分又可以區分為「對設有存取控制機制的電腦作不正連線(第二款)」以及「對被設有存取控制機制的電腦控制的電腦作不正連線(第三款)」二類，此二款最主要是客體不同，簡單而言第二款是侵害安全系統本身，而第三款是侵害在安全系統控制下的電腦。然在此有論者將第三款譯為「以網路上的其他電腦，對特定電腦輸入可能解除使用限制的資訊或指令」，顯然理解有誤。參園田寿，不正アクセス，法学教室 228 号，1999 年 9 月，頁 44；李崇偉，電腦網路入侵行為之刑事立法研究，中央警察大學法律學研究所碩士論文，2003 年 6 月，頁 99-100。

過程可謂非常緊急，雖不致學者沒有發聲的空間，但主導立法者仍主要是警察以及政府機關，並且是一利益衡量下的結果。又若從法律條文本身的角度出發，該法所受到最大的批判即是「不正連線」用語本身的曖昧，一般認為「不正連線」亦含有「有連線權的人以犯罪目的所為的連線」，且「不正」本身即含有評價性，對於單純無權連線電腦的行為人亦有處罰的本法亦不適當，應將「不正連線」修正於「無權連線」為妥[282]。另有從警察白書中用語解說的英文 unauthorized access 的直譯[283]，以及英國立法例的參考[284]等角度，亦達到相同結論者。更進一步言，是否所有無權連線的行為都要將其與犯罪相繩亦是個應解決的大問題，在立法之初警察廳所提出的版本本即是要以行政罰為手段處罰，以及在立法過程中也曾傳出由日本律師公會(日本弁護士連合会)質疑恐會對電腦利用者的精神自由權有重大威脅、並且對於資訊流通自由有所阻礙等聲音[285]，再加上入罪化後刑度極低，對於專業犯罪者來說可謂根本沒有嚇阻效果，最後僅會適用在一些犯罪手法單純的「間歇型駭客」身上[286]。事實上，有論者在法律施行後所做的調查中，幾乎所有被以不正連線罪所起訴的案子皆非專業駭客所為，且大多是如「為免除付費線上遊戲的付費機制」或「為在某討論板上惡作劇」等犯罪目的的輕微案件[287]，可見將此行為入罪化似乎無法達到當初所預設的目的，反而使本法被用來對付另一族群的行為人。最後則係有關於幫助不正連線的部分，在前述的調查中，有一半以上的行為人皆非自己撰寫快客工具(程式)，而是由網路上或雜誌隨附的 CD 等處下載取得[288]，但由於本法僅規定在將他人的連線識別符號[289]公開或將其告知第三人時會處以三十萬日圓以下罰金，並未規範此類快客工具(程式)的散布或流通

---

[282] 園田寿，不正アクセス，法学教室 228 号，1999 年 9 月，頁 45。
[283] 加藤敏幸，不正アクセス，刑法雑誌 41 巻 1 号，2001 年 7 月，頁 82-83。
[284] 高橋郁夫，コンピューターの無権限アクセスの法の覚書–英国・コンピューターミスユース法 1990 の示唆，判例タイムズ 1006 号，1999 年 10 月，頁 88。
[285] 日本弁護士連合会，警察廳の「不正アクセス対策法の基本的考え方」及び郵政省の「電氣通信システムに対する不正アクセス対策法制の在り方について」に関するパブリックコメント公募に対する意見，自由と正義 50 巻 8 号，1999 年 8 月，頁 50。
[286] 加藤敏幸，不正アクセス，刑法雑誌 41 巻 1 号，2001 年 7 月，頁 82-83。
[287] 金澤正和，不正アクセス行為等の取締り状況及び今後の課題，警察学論集 53 巻 8 号，2000 年 8 月，頁 23-25。
[288] 金澤正和，不正アクセス行為等の取締り状況及び今後の課題，警察学論集 53 巻 8 号，2000 年 8 月，頁 26。
[289] 如 ID、密碼等資訊。

等問題，若此問題未被注意，未來很可能會產生對電腦幾乎無專業性可言[290]的行為人，但卻利用「非常人性化的快客工具(程式)」而達到不正連線結果的案例。故對於此類工具的流通規制似乎也是應檢討的點。並且，此種幫助不正連線罪的刑度僅有三十萬日圓以下的罰金，然而就動搖連線控制機制的信賴角度來看，此種行為不管連線機制再如何完備，都無法抵擋此種向第三人洩漏或公開連線識別符號的行為，故此種行為理論上對於連線控制機制安全信賴的動搖至少應與不正連線行為相同，或甚至在其之上，故對此行為的評價似也應作相關調整，始符合罪刑相當原則[291]。

三、　網路犯罪公約所導致的製作病毒罪

前述不正連線禁止法的修訂可謂是日本一次次的向資訊大國美國妥協的最佳證明，但美國對於日本的要求並不僅止於無權入侵電腦的部分。於 2001 年日本簽署網路犯罪相關條約[292]，對於國內法固須有一番修正以因應條約的要求[293]。就此，日本法務省於 2003 年以及 2004 年各以「為對應犯罪國際化及組織化之刑法一部修正案[294]」與「為對應犯罪國際化及組織化與資訊處理高度化等之刑法一部修正案[295]」為名，提出於國會接受審議，但此二次審議的結果均隨著眾議院的解散而成為廢案[296]。未通過的原因，最主要是因該次法律修正案除含有因應資訊處理高度化的問題外，亦含有國際犯罪、組織犯罪的修正案，就組織犯罪的部分，因共犯範圍不明確而可能產生處罰範圍過度擴張所致[297]。在之後數年亦多次提出

---

[290] 在現在這個時空中對於電腦的基本操作應該可以視為常識。我們對於一般僅會操作 OS 以及大眾皆在使用的軟體(如微軟的 OFFICE)的行為人，應不至於認為這種行為人叫做「懂電腦專業技術、知識」，而將其冠上「科技犯罪」或「白領犯罪」等高帽子來自我催眠。

[291] 園田寿，不正アクセス，法学教室 228 号，1999 年 9 月，頁 45。

[292] 原文為「サイバー犯罪に関する条約」。

[293] 荒川雅行，ウィルス作成罪，法学教室 374 号，2011 年 11 月，頁 2。

[294] 原文為「犯罪の国際化及び組織化に対処するための刑法等の一部を改正する法律案」。

[295] 原文為「犯罪の国際化及び組織化並びに情報処理の高度化等に対処するための刑法等の一部を改正する法律案」。

[296] 吉田雅之 特集・情報処理の高度化等に対処するための刑法等の改正–法改正の経緯及び概要，ジュリスト 1431 号，2011 年 10 月，頁 58-60。

[297] http://ja.wikipedia.org/wiki/%E4%B8%8D%E6%AD%A3%E6%8C%87%E4%BB%A4%E9%9B%BB%E7%A3%81%E7%9A%84%E8%A8%98%E9%8C%B2%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E7%BD%AA，最後瀏覽日期，2012 年 7 月 22 日。

未果後，法務省內部進行檢討，決定將共謀罪的部分刪除後再度提出，終於在2011年的第177次國會中通過，並於同年6月施行[298]。

本次對刑法法典的修正中，含有許多部分的修正，而對於電腦犯罪的部分較具重要性的部分，無疑是刑法第19章之二─不正指令電磁紀錄罪章的新設，以及電子計算機妨害業務罪未遂犯(刑法第234條之二第2項)的新設二類。在此有探討必要者，即是不正指令電磁紀錄罪章新設的部分。本罪章僅有兩條條文─第168條之二以及第168條之三，此二條文既會被稱為罪章，即表示其具有獨立的保護法益。與不正連線禁止法相同，本罪章所保護的法益亦是一社會法益，且該法益與偽造文書罪類似，是「社會對於電腦程式(完善運作)的信賴」[299]。從而本罪並非是因電腦病毒而造成任何財產或著作權上實際損害之罪的預備犯，而是一獨立的既遂犯[300]。

如前述，本罪章共從兩個方向規範破壞電腦程式完善運作的社會信賴行為，第168條之二所規定者為作成、提供[301]與供用[302]破壞電腦程式完善運作的電磁紀錄(以下簡稱電腦病毒)的行為，第168條之三所規定者為取得與保管電腦病毒的行為。其中於作成或提供電腦病毒的規制上，除以例示概括方式列出何謂「電腦病毒」外(第168條之二第1項第1、2款)，亦對於作成與提供的行為以意圖犯的方式限縮處罰範圍，並於第3項中處罰本罪的未遂犯。而在取得與保管的部分，雖未處罰未遂犯，但亦如同前條有意圖犯的規定。值得一提的是，於前幾次提出的修正案中，並無「無故(正当の理由がないのに)」的要件，然此次提案中為了

---

[298] 杉山徳明、吉田雅之「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について，警察学論集64巻10号，2011年10月，頁4。

[299] 吉田雅之「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について，法律のひろば64巻10号，2011年10月，頁54。

[300] 渡邊卓也，サイバー関係をめぐる刑法の一部改正，刑事法ジャーナル30号，2011年11月，頁28。

[301] 在此所謂提供，係指對於明知該為不正指令電磁紀錄等資訊，並欲將其移轉到自己支配下的行為人，將該電磁紀錄移轉到其支配下的行為。參櫛清隆，「情報処理の高度化等に対処するための刑法等の一部を改正する法律」の概要，刑事法ジャーナル30号，2011年11月，頁6。

[302] 在此所謂供用，依照立法者原意，非指一般在他人電腦上運行程式的行為，而是指將程式置放在不知情的第三人的電腦中，並呈現實行可能狀態的行為。參渡邊卓也，サイバー関係をめぐる刑法の一部改正，刑事法ジャーナル30号，2011年11月，頁30。

建立程式設計工作者的信心，故加上此要件作為強調[303]。

第二款 規範特色之分析

從以上日本立法例的立法過程以及所受到的批評檢討，亦可以發現日本立法例的三點特色，也不難發現日本的這三點特色皆與台灣所發生的情況幾乎一模一樣。首先，日本推動修法是被動且倉促的，無論是 1987 年的刑法一部修正或是不正連線禁止法的推動，背後都有著巨大的國際壓力亦或是時代的情勢上壓力，在逼得日本法律不得不修正的時候，始會考慮修正。也因為兩次修正都是在壓力爆炸下產生的緣故，從擬定草案至修法通過的時間都不超過一年，甚至還有像前述為了讓立法案通過而刻意避免學者專家介入的例子在。而此種被動且倉促的修法過程，與台灣的現況非常相似。若將台灣電腦犯罪相關修法過程依照民國 86 年與民國 92 年分為兩大階段，民國 86 年的修法與日本 1987 年的修法背景類似，而民國 92 年的修法則與不正連線禁止法的修法背景相似，然而就時間點上我國整整晚了日本約十年。

再者，日本同時採納德國與美國對電腦犯罪的處理態度。在 1987 年的修法前後，由前述修法背景的介紹可以得知，雖然已有論者開始思考該次修正是否透露出一點新興社會法益的味道，然而日本主要仍是採與德國相同的「在傳統法益下追加新規範」的見解。而不正連線禁止法的增訂過程中明顯可以看到美國在國際間伸出控制國際情勢的雙手，當然日本本次以及之後的修法亦無法倖免，幾乎完全是偏向美國法的處理態度。所以相對於美國與德國這兩個極端的處理態度，日本可以說是採完全折衷的立場來處理電腦犯罪。而反觀我國對電腦犯罪的修訂過程，也可以發現 86 年的修正與德國法的處理態度類似，而 92 年的增訂專章則幾乎完全是受到美國法影響，也可謂在結論上與日本相同，是採「折衷處理態度」。然而在此與日本有稍微不同的是，我國於 92 年制訂專章時，似乎並未如同日本般因為受到美國的壓力而作修正，而僅是跟隨著「世界各國(尤其是美國)多有修

[303] 因縱使無此要件，得承諾的病毒製作或是程式 BUG 此種社會上認可的缺陷，在解釋上皆不會該當「不正電磁紀錄」的要件。參今井猛嘉，特集・情報処理の高度化等に対処するための刑法等の改正–実体法の視点から，ジュリスト 1431 号，2011 年 10 月，頁 68-69。

正的潮流」而認為對電腦犯罪應該修正而已，故若就對法律增修的嚴謹態度而言，我國可謂大大不如日本。

最後，日本可謂已為「電腦犯罪(不正連線以及電腦病毒等問題)」找出一新興法益的出路。日本在法制上是一繼受德國法的繼受法國家，從而就整體法體系而言應是如德國般採法益論，若無保護法益即無法任意對行為課以刑罰。而此種環繞保護法益建構犯罪行為的思維，在 1987 年的增訂因是參考德國對電腦犯罪的處理態度，故不致發生問題。然而問題即出現在不正連線禁止法的增訂時，因不正連線禁止法會增訂幾乎是因為美國的壓力(或謂「國際情勢」)而不得不加以規範，然而就骨子裡是繼受德國體制的日本來說，要增訂此種規範即必須要找出規範合理化的依據，亦即保護法益。而此種行為雖得以之後傳統犯罪的預備行為角度加以規範，然而對於單純不正連線即會出現規範漏洞，故此項修正對日本來說勢必有場硬仗要打。而最後不正連線禁止法修正後，可以得知日本選擇了尋找新法益的立法途徑，並且如同美國前述第四階段的精神般，將「連線控制機制」本身單獨作為一個保護對象，並藉由立法技巧得出一個新法益「社會上對於連線控制機制的信賴」以解決自美國而來的壓力所造成與繼受德國法思維的傳統刑法的衝突。反觀同樣是繼受德國法(精確來說是繼受日本法)的我國於 92 年修正時也碰上類似的問題，雖然我國並未直接受到美國的壓力[304]，但就修法過程中大量採用美國立法例來看，面臨此種問題也可謂在意料之中。並且就我國修法者的見解，他們也「找出了新興法益」來解決此問題，只不過此種「新興法益」卻是無法具體說明的「國家、社會與個人法益的集合體」而已。從而在此部分可以得知我國不僅又再一次的在立法的態度以及技巧上遠遠輸給日本外，還可以得知一個重要的訊息—對於電腦犯罪的規範態度中，找出新興法益這條路徑是可行的[305]。

第四節　小結

[304] 李茂生，我國電腦網路犯罪的虛像與實相，刑事政策與犯罪研究論文集(四)，法務部犯罪研究中心，2001 年，頁 9 以下。
[305] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 74-75。

綜合以上我國以及外國的修法過程以及規制態度並稍做統整後，不難發現對於電腦犯罪的規制態度即是由英美法系以及歐陸法系的代表，亦即美國與德國共同勾勒出兩個光譜的極端，而對於法學上並未如此引領潮流，多屬於繼受法的國家，則必須思考自己的規制態度是要在光譜的哪一個座標點上，並且要想辦法調和規制態度與被繼受法體系的衝突。在同樣面對「電腦、網路」這個時代巨輪轉動下的新產物時，無論是美國德國日本或我國皆不免在規制上會有所徬徨，然而作為英美法以及歐陸法體系代表的美國以及德國，皆以自己背後法體系的基礎為原則，在經過幾多思辨以及統整的醞釀後，始得出最後對電腦犯罪的實體規範。

然而對於身為繼受法的日本以及我國，在世界先進國家仍正在對電腦犯罪的規範作分析思考，要繼受或參考皆無所本時，社會上早已因應電腦的出現而火速產生各式各樣極待解決的亂象，可想而知此時此些國家即如同瞎子面對一頭從未見過的巨象般更加徬徨，更何況相較於我國，日本還有國際間(美國)對於法案催生的壓力在，其對於規制的渴求更甚於我國。在種種有形以及無形的壓力下，此些繼受法國家有的由於社會上需要、有的因為國際壓力、有的只為「跟上時代潮流」，自立法至施行的過程都是相當急促以及短暫的，也因此對於法律的修正或增訂難免會有不成熟或是出現問題的部分。雖然日本與我國對於電腦犯罪的規制態度的思考轉變以及面臨的處境極度類似，然而不管從日本的立法動機、立法過程甚至是最終立法成果來看，日本與我國的法制成熟度仍有相當大的差距。日本在面對受到美國壓力下而增訂的不正連線禁止法及之後的數次修正上，與其向來繼受的歐陸法系衝突中，試圖作調和而找出了新興保護法益，並且沿用至今亦不致產生體系混亂的問題。

反觀一樣是繼受歐陸法系，並且並未受到美國壓力的我國，其實是有很大機會以及相對充裕的時間可以妥善思考此問題，然而從修法態度上卻一味的認為應與世界潮流接軌，故要迅速立法，亦不管我國國內所發生的種種問題是否需要制訂新法始可解決[306]，即在「迅速」、「務實」的原則上以「先歸納所欲處罰的行為，

[306] 事實上，當年算的上是新法所規範的「電腦犯罪」的案件屈指可數，其他大多是利用電腦網路所違犯的傳統犯罪，參林宜隆、李建廣，網路犯罪抗制對策之探討，警學叢刊第 29 卷第 5 期，1999 年 3 月，頁 209 以下。

接下來則排除刑法已有規定而可順利依解釋或其他法學方法解決的行為類型，最後將排除後的剩餘行為皆置於專章規範」的大鍋炒方式制訂了妨害電腦使用罪章。與日本類似的是，雖我國不是在美國壓力下而為的修法，但在修法時也正好也大量參考了美國法作為新法的立法典範，從而我國在結果上與日本相同，亦面臨了英美法系與大陸法系的衝突要如何調和的問題。不過與日本截然不同的是，我國的立法者或謂能力不足，或謂本即認為衝突不存在，對於此種衝突近乎沒有調和，而以非常突兀的方式讓新罪章出現在刑法的最後一章。並且由於沒有進行調和的緣故，於法條的適用以及與他條的競合上亦可預見會出現不少問題。

此種從詭異的立法態度以及粗糙的立法過程中誕生的罪章，存在著根本上的缺憾，一個連保護法益都無法清楚說明的刑罰規範，就連在現代社會的適用上，都無法有效說服人民為何此類行為要以具有謙抑性的刑法來處罰，也難怪會在遞續性上觸礁，而在雲端運算時代中產生更大的問題。然縱使立法目的曖昧以及修法過程粗糙，刑法妨害電腦使用罪章仍經審議通過並公布施行至今已有十年之久，或許對於其所刻畫出的行為類型於實務上的運用狀況以及規範文字間所透露出來的一些問題點亦是一個在思考妨害電腦使用罪章應該如何修正時的一個重要指標。據此，下一章即以與本章不同，著重於實務上以及法條本身的角度來探究妨害電腦使用罪章該何去何從。

第四章　妨害電腦使用罪章各行為態樣之探究

在了解我國與外國對於電腦犯罪的面對及處理態度後，所要進而檢視的即是我國與電腦犯罪有關的各種行為態樣本身存在的爭議以及於實務上的運用情形。然而如前所述，我國妨害電腦使用罪章於立法當時，即是依照「欲處罰行為的歸納→排除刑法已有規定而可順利依解釋或其他法學方法解決的行為類型→其餘行為皆置於專章規範」的立法態度所制定，可想而知整部妨害電腦使用罪章的各條文，即是各種立法者所認為應加以規制的電腦犯罪行為類型大雜燴。故而本章即依照妨害電腦使用罪章各條文的編排順序依序探討各種立法者所擬定的行為態樣，並分析各種行為態樣間是否存在問題以及存在何種問題，以作為思考解決困境時的參考。

又，正如法規研究小組所述，在此所討論與電腦犯罪相關各種態樣的範圍應排除「以電腦為手段違犯的傳統犯罪」，而只限於妨害電腦使用罪章所規範的各罪。首先，畢竟此類犯罪所侵害者與以其他手法違犯相同，仍是該罪章所規定的傳統法益，並且其也僅是在手段上與電腦有關，實與電腦特性關係甚淺。再者，反面而言，雖就前述分析來看立法者幾乎未謹慎思考此問題，然既立法者認為為解決電腦犯罪問題應設置獨立專章，則妨害電腦使用罪章中的各罪，原則上即應要有專門的保護對象，且保護對象應該會獨立於傳統犯罪所要保護的各種對象，始有單獨建立專章的價值以及意義在。若將本章以外其他罪章的犯罪也加進來分析，實則意義不大。綜上，本章所檢視的對象，初步排除妨害電腦使用罪章以外的各條刑法上犯罪，而將分析的重點置於妨害電腦使用罪章各條文所規範的行為類型中。

第一節　規範鳥瞰

在進入妨害電腦使用罪章各條文內作細部解析之前，若先對整個罪章作一個做一個鳥瞰性質的統整工作，將要討論分析的各種行為類型、所對應在妨害電腦使用罪章的法條依據以及該法條的立法理由等做個整理，之後各項的細部解析即

可直接切入問題點，於本文體系上亦不致在討論每種行為類型時皆要個別單獨重新闡述該行為類型所依據的法條以及立法理由等概念而導致文脈過於繁雜。同時，提供法條以及立法理由的做法也會使解析時得以比較參考，於討論上較能集中重點。故而，本節的主要工作即是將妨害電腦使用罪章各罪做個鳥瞰性質的統整，並將本罪章的各條法條以及立法理由以表列式的呈現整理於下。

又，於檢討條文的角度部分，本文擬以「實務上之運用情形」、「現今所受到之批評」以及「遞續性上之困境」三個角度來檢討各個條文。所謂「實務上之運用情形」，即是就實務上所發生的案例及所作出的判決來做統整分析，同時亦會以一些實務工作者的著作資料做輔助，以探求實務界對此些規範是如何的觀察及運用，是否立法者所增訂的規範要件皆能於實務上運用自如，亦或是要件嚴苛背離常理，以致適用上窒礙難行；又是否與當初立法者所希望達到的規制目的相同，抑或是相去甚遠。而所謂「現今所受到之批評」，是指就本罪章三讀通過公布施行後，立即受到各界檢驗後，認為出現問題應予修正的問題。此類問題的產生，足以顯示本罪章雖宣稱要防制電腦犯罪，但法律訂定後卻連防制現今的犯罪皆產生疑義，於解決困境之前，應先對此些疑義做釐清甚至排除。又所謂「遞續性上之困境」，則是由妨害電腦使用罪是否能延遞持續的在未來亦可適用，亦即遞續性的角度來觀察分析，該些條文在適用上是否會產生問題、產生何種問題。即使法律條文能夠順利解決現今的法律問題，仍不代表此些法律即能因應未來層出不窮的法律問題，且資訊科技相對於傳統科技的發展速度著實迅速太多，在制定與此有關的法律時，更加應該考慮遞續性的問題。

行為態樣	條文依據	立法理由
無權進入電腦	第 358 條 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。	一、本條新增。 二、鑒於對無故入侵他人電腦之行為採刑事處罰已是世界立法之趨勢，且電腦系統遭惡意入侵後，系統管理者須耗費大量之時間人力檢查，始能確保電腦系統之安全性，此種行為之危害性應已達科以刑事責任之程度，為保護電腦系統之安全性，爰增訂本條。
取得、刪除或變更電磁紀錄	第 359 條 無故取得、刪除或變更他人電腦或其相關設備之	一、本條新增。 二、電腦已成為今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若

	電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。	電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害，鑒於世界先進國家立法例對於此種行為亦有處罰之規定，爰增訂本條。
干擾電腦運作	第 360 條 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。	一、本條新增。 二、鑒於電腦及網路已成為人類生活之重要工具，分散式阻斷攻擊 (DDOS) 或封包洪流 (Ping Flood) 等行為已成為駭客最常用之癱瘓網路攻擊手法，故有必要以刑法保護電腦及網路設備之正常運作，爰增訂本條。又本條處罰之對象乃對電腦及網路設備產生重大影響之故意干擾行為，為避免某些對電腦系統僅產生極輕度影響之測試或運用行為亦被繩以本罪，故加上「致生損害於公眾或他人」之要件，以免刑罰範圍過於擴張。
妨害公務機關電腦使用之加重	第 361 條 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。	一、本條新增。 二、由於公務機關之電腦系統如被入侵往往造成國家機密外洩，有危及國家安全之虞，因此對入侵公務機關電腦或其相關設備之犯行加重刑度，以適當保護公務機關之資訊安全，並與國際立法接軌。 三、本條所稱公務機關，係指電腦處理個人資料保護法第三條所定之公務機關。
製作並散布犯罪電腦程式	第 362 條 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。	一、本條新增。 二、鑑於電腦病毒、木馬程式、電腦蠕蟲程式等惡意之電腦程式，對電腦系統安全性危害甚鉅，往往造成重大之財產損失，致生損害於公眾或他人，一九九九年四月二十六日發作之 CIH 病毒造成全球約有六千萬台電腦當機，鉅額損失難以估計，即為著名案例，因此實有對此類程式之設計者處罰之必要，爰增訂本條。
告訴乃論	第 363 條 第三百五十八條至第三百六十條之罪，須告訴乃論。	一、本條新增。 二、刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪行為，尤其對於個人電腦之侵害行為，態樣不一，輕重有別，如受害人無告訴意願，並配合偵查，實際上亦難達到偵查成效，故採告

		訴乃論，有助於紛爭解決及疏解訟源，並可將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查，爰增訂本條。 三、至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。第三百六十二條之罪則因該行為可能造成社會重大損失，惡性較第三百五十八條至第三百六十條之罪為重大，而個別被害人往往因證據已經滅失，或不願出庭作證，以致發生被害人數雖然眾多，但卻無被害人願意提出告訴之窘境（台灣 CIH 病毒案例即無被害人願意提出告訴），影響檢察官對此類犯行之追訴，故採非告訴乃論，以有效懲處不法。

第二節　無權進入電腦—刑法第 358 條

第一項 實務上之運用情形

就無權進入電腦的行為類型部分，我國最主要運用在兩大類型的案件中—網路遊戲盜帳號以及員工對於雇主的不法行為。除此之外即是些零散如入侵他人信箱、偷取伺服器空間等案例，並且此些案例時常與同罪章其他條文於使用上出現競合的情形。以下就較具代表性的兩大類型案例以及其他案例類型，共計三種類型作分析。

首先，於網路遊戲盜帳號的部分，我國最常出現的犯罪流程即是以植入木馬程式或他法[307]得知被盜帳號方的帳號密碼後，於其他電腦輸入得知的帳號密碼而登入遊戲，將他人遊戲內的虛擬寶物作丟棄或開啟交易等動作，並另開啟自己於該遊戲的帳號去撿拾被丟棄的保護或以極低的價格甚至無價格的方式回應交易，

[307] 例如男女朋友互相認識而得知、或朋友間代為練功而告知等情形，更有甚者則是利用交易之名向被侵入方要求提供帳號而得知。

以將被盜帳號方帳號內的虛擬寶物移轉自自己帳號下的犯罪流程[308]。此種犯罪流程中皆沒有對於遊戲程式本身使用何種破解或病毒程式來做修改或破解，反而還「循規蹈矩」乖乖以輸入(他人)帳號密碼的方式登入遊戲伺服器，並且按照遊戲說明中所述的操作方式移轉物品於自己帳號。並且從該些案例亦可以發現行為人在取得帳號密碼的過程中，大多是合法得知帳號密碼然而無權或越權使用，少數使用木馬等惡意程式取得他人帳號密碼者，亦非皆是自己所撰寫[309]。從而可以得知，實務上認為應該適用刑法處理的此類行為，實際上大多不需要具備何種專業電腦知識即可能違犯。

再者，員工不法行為的部分。最常出現的犯罪流程通常是於該員工於離職前即是有權登入公司電腦並進行相關業務，而因跳槽等各種原因離職後，仍利用帳號密碼登入公司電腦或查看資料或取得資料，並將取得的資料交予現在所任職的公司，或自行使用此些資訊[310]。然就此些案例作觀察，可以發現此些案件中的行為人(員工)所需要的電腦專業知識相較於前述網路遊戲盜帳號的案例更低，僅要如離職前一般登入系統即可順利進入公司電腦並查看內部資料。又，員工於離職後能順利登入系統，管理系統的公司方未善盡管理責任，將以離職員工登入權限作限制或移除往往是造成此種結果的原因之一。從而，此種情形並非是員工「駭力高強」的突破公司安全系統的重重關卡，最後終於得到公司內部的機密資料，反而不如說往往是公司方過度輕忽自己電腦系統安全的管理，而造成就連離職的

---

[308] 參板橋地院九十一年度易字第三五八五號判決、基隆地院九十二年度基簡字第八一七號判決、板橋地院九十三年度易字第一二六六號判決、新竹地院九十三年度訴字第一七九號判決、板橋地院九十三年度簡字第一五九二號判決、宜蘭地院九十三年度簡上字第四三號判決、台中地院九十四年度中簡上字第一六一號判決、台中地院九十四年度上易字第一二三三號判決、高等法院台中分院九十四年度上訴字第一八四四號判決、台北地院九十五年度訴字第八四七號判決、台東地院九十六年度訴字第一六五號判決等。另有台北地院九十八年度訴字第一〇〇〇號判決，其事由是提供遊戲帳號予不知名人士，而該不知名人士在盜取他人帳號後將其所提供的帳號用來儲存虛擬寶物，此時法院認為提供者亦可能涉及(雖然最後認為不成立犯罪)該不知名人士所觸犯相關罪名的幫助犯。

[309] 以上述案例為例，上述案例中僅有板橋地院九十一年度易字第三五八五號判決以及台中地院九十四年度中簡上字第一六一號判決係以植入木馬程式相關，而僅有板橋地院九十一年度易字第三五八五號判決的被告是自行撰寫木馬程式。

[310] 參板橋地院九十一年度訴字第一〇二八號判決、板橋地院九十三年度訴字第二一五九號判決、台北地院九十四年度訴字第一八二三號判決、台中地院九十五年度易字第一四三七號判決、台北地院九十六年度訴字第一三〇五號判決、高等法院九十七年度上易字第一三一〇號判決、台北地院九十八年度訴字第一六八號判決、高等法院九十八年度上訴字第二八三七號判決、板橋地院九十八年度訴字第三七一八號判決、高等法院台南分院九十九年度上更(一)字第一〇號判決等。

員工都能輕易進入公司電腦。

最後於其他案件部分，有的犯罪流程是由不知名人士提供他人於 yahoo 的帳號密碼以及已安插木馬病毒在內的應用程式檔案，行為人僅輸入他人的帳號密碼，進入他人信箱或是社群網站(yahoo 奇摩家族)，並將此些含有木馬病毒的檔案或以電子郵件之方式轉寄他人，或儲存於被害人之家族網站的「檔案庫」或「酷連結」內，使更多的人能夠因而下載此病毒，該病毒發作後，可以得到該些被感染電腦使用者的 yahoo 帳號密碼[311]；有的犯罪流程是行為人架設網站，然而因為免費空間太小不敷使用，為擴充空間而進入某學校網站，並利用程式得知該學校網站中存取帳號密碼的檔案內容後，輸入前述得知的帳號密碼登入學校網站並備份資料已達擴充空間的效果[312]；有的犯罪流程則是行為人利用被害人委任其代為選課而給予學校應用系統的帳號密碼或自行猜得密碼，登入被害人於學校系統的頁面並將其中數堂課退選[313]。雖以上有些案例相較於前述二者似需要較高電腦相關知識始能違犯，然而此類行為往往也都是操作簡單的程式即能達到入侵的效果，亦無法認為需要高度的電腦專業知識始能違犯。

此外，實務上亦對本條做了許多補充性質的見解，如本條所謂的「他人電腦」應係指「他人有使用權」的電腦，並且網路遊戲或網站等註冊的帳號對使用者而言是「個人電腦的延伸」，應屬於「相關設備」[314]、以及本條所輸入的「他人」密碼與入侵的「他人」電腦或相關設備不需為同一人[315]、並且入侵行為不限於以透過通訊線路的方式為之[316]等。此些見解有些是基於立法理由而來，然有些則可能與立法理由相衝突。

第二項 現今所受到之批評

---

311 參花蓮地院九十五年度花簡字第九九六號判決、花蓮地院九十六年度簡上字第三九號判決、屏東地院九十七年度訴字第七三六號判決、高等法院高雄分院一〇〇年度上更(一)字第二十三號判決。

312 參高雄地院九十五年度易字第一三〇五號判決、高等法院高雄分院九十五年度上易字第八七二號判決。

313 參台中地院九十三年度訴字第一六六八號判決、基隆地院九十八年度訴字第九三一號判決。

314 參高等法院高雄分院一百年度上訴字第一三一〇號判決。

315 參高等法院九十五年度上訴字第二四八二號判決。

316 參高等法院九十四年度上易字第一四一八號判決。

對於入侵電腦行為，所受到最大的批評即是當初立法過程中為避免刑罰過度擴張，以符合國民法律感情，而將無權進入電腦的行為限定在「無故輸入他人帳號密碼」、「破解使用電腦之保護措施」以及「利用電腦系統之漏洞」三類的立法方式[317]。首先有實務工作者指出，此三類限定的行為中，由於條文的規制過於模稜兩可，導致實務上僅有「無故輸入他人帳號密碼」此種無權進入的態樣有規制的實益，並且得以順利解決現行「電腦犯罪」一半以上的問題[318]。蓋「破解使用電腦之保護措施」的「破解」一詞的意義存在著非常多的不確定性，無法辨識究竟是防禦措施的全部亦或是限於與該電腦有連線的防禦措施[319]；又「利用電腦系統之漏洞」的「漏洞」是相對性的概念，資訊科技在每個時間點上亦有其極限，若認達到此種「極限」後即可謂「沒有漏洞」。然而問題則出在如何對此舉證上，是要參考微軟的安全性報告？或是行政院國家資訊通訊安全會報技術服務中心的通報？抑或是外國駭客組織所發布的作業系統缺陷？論者認為此處並無客觀標準，極難有舉證可能性[320]。

再者，姑且不論此三類限定行為的法條文字規範上可能存在前述問題，就「將應處罰的無權進入電腦行為限定於三種入侵態樣」此點上，絕大多數的學者即給予嚴厲的抨擊。該些論者認為重點應環繞在「保障電腦使用的安全」，若行為人以該三種態樣以外的方式入侵電腦，並已達侵害電腦使用安全的程度，卻基於罪刑法定原則無法論以本罪，明顯存在法律上的漏洞[321]。並且衡諸美國日本等外國立法例，少有限制入侵態樣者，故採此看法者多認為應將此三種類型刪除，規定類似「無故入侵電腦或其相關設備者」即足，避免徒增適用上的困擾[322]。然反對的論者謂，將侵入行為限定在以上三種的作法，或許是立法者考量因入侵電腦此

---

317 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 358 條之修正說明第三點。

318 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 88。

319 論者舉出一個耐人尋味的例子：某甲將站在電腦室門口負責看管電腦主機的衛兵殺掉，或是將電腦室門口的大鎖打壞，並進入電腦室使用電腦的行為是否該當於「破解使用電腦之保護措施」？

320 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 89。

321 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 553-554；柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 126-127。

322 王銘勇，侵入電腦系統罪之研究，法令月刊第 55 卷第 3 期，2004 年，頁 266；蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月，頁 125 以下。

種犯罪類型在法益侵害上的輕微性，而努力就最具侵害可能性的三種類型規定為構成要件行為[323]。就以上爭議，本文認為固然此些類型是表彰較具法益侵害可能性的行為，然而如同多數論者所述，重點在於「法益是否有被侵害」而非「以何種手段為侵害」，除非是僅有此三種行為方式始能侵害法益或該些法益的侵害達到值得以刑法處罰的程度，否則藉由限定行為方式來限縮適用範圍以免濫罰，似乎不是一個較妥適的作法，並且亦有可能產生雖是以上述三種行為方式為之，但卻未侵害保護法益的情形，仍被論以本罪[324]。對於此種欲將處罰範圍限縮至較具有法益侵害性行為的立法方式，於我國立法上似可以依照概括規定的方式，以「無故輸入他人帳號密碼、破解使用電腦之保護措施、利用電腦系統之漏洞或其他相類之方法」作規範，一方面可以發揮限縮規範的效果，另一方面也不致過度限縮導致出現法律規範上的漏洞。

又，關於本罪性質的部分，有論者認為本罪的性質是一舉動犯，僅要行為結束即成立既遂犯，並不需要結果的發生[325]，但亦有不同見解認為若認本罪性質為舉動犯，即會產生與條文文義不符的情形，亦即只要不「入侵」電腦，縱無故輸入他人帳號密碼、破解使用電腦保護措施或鑽電腦系統漏洞，仍不會與本罪相繩[326]。然而，有學者認為縱舉動犯僅是一行為即會發生結果，並非「不需要有結果」，且本條的問題亦不在於不需要結果的舉動犯類型是否存在，而是此種輕微結果是否能表彰法益的侵害。首先要先確定保護法益為何，始能區分何種無權進入行為有入罪化的必要[327]。

最後，就本罪並無處罰未遂犯的部分。有論者認為雖就文義解釋而言此結論

---

[323] 李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 247 以下。

[324] 盧映潔，電腦小子鑄大錯，月旦法學教室第 57 期，2007 年 7 月，頁 18-19。氏認為縱使是單純以侵入他人電腦為娛樂，並顯示出其為電腦高手的優越感，仍會成立本罪。

[325] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 127。同時其亦認為立法者限定三種行為態樣之立法方式，會混淆本罪是結果犯或舉動犯的性質。

[326] 蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月，頁 126。然其對於「使用(access，亦即本文所謂的「連線」或「進入」)」的概念係偏向於美國學說上的「虛擬進入說」，亦即電腦系統就像是一個存在世界的另一個空間，使用電腦必須是要如同打開被害人家大門而進入家中般，處於「得以查看到電腦內部資訊的狀態」。

[327] 李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 247-248。

是當然的結果，然而與人民的感受會有落差[328]。並且亦有認為在本罪在無未遂犯的規定下，對於共犯的論處上會有極大的不合理性，在適用共犯從屬性的原則以及考慮到特別法對特定行為亦有處罰後，有可能產生僅處罰「共犯」而不處罰正犯的情形[329]。綜合以上見解，對於未遂行為的規制似有其必要性。

第三項 遞續性上之困境

在雲端時代來臨後，由於資訊的共同管理之故，大多數人的資訊都會被共同儲存於一座大型主機房內，而個人僅需使用一台小型的雲端連線裝置連線至雲端後，即可使用位於雲端內的個人作業系統。而該雲端連線裝置僅有連線功能，於開機後還須輸入雲端使用者的帳號密碼，始會連線至該使用者位於雲端的作業系統，否則內部根本空無一物。此時若依照立法者、實務以及部分學者所認為本罪所保護者除藉由通訊線路對於電腦為入侵外，就對單機電腦為入侵的行為亦應與本罪相繩的看法，可能會產生對他人上鎖的「雲端連線裝置」輸入他人密碼而開機後，再輸入自己的帳號密碼登入雲端系統的行為亦落入刑法的規範。然縱依照立法理由，在此所保護的重點亦應係後面輸入連接至雲端的該帳號密碼，而非之前的開機帳號密碼[330]。而會造成此困境，乃是因為上述論者仍立於「單機電腦」或是「可連線電腦」的角度來審視可能會發生的刑事問題，而以「單機電腦為主，連線僅是附加設備」的思維來思考電腦犯罪的規制，在未來以網路為主，單機電腦僅是附加的時代即會漸漸觸礁。故本文以為，對於個人所擁有的雲端連線裝置的保護以及對雲端電腦使用的保護應該分別論之。對於個人所持有的連線裝置作保護實則意義不大，重點在於連線到雲端後使用權限的保護，而從規制面要如何使規範能達到以上目的，則是必須思考的部分。

---

[328] 蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月，頁 127。

[329] 該論者舉出一個案例：某甲提供他人帳號予某乙，但某乙在使用此帳號密碼入侵某丙電腦時入侵失敗。此案例某乙並不成立犯罪，基於共犯從屬性某甲亦不成立妨害電腦使用罪的共犯，然某甲提供者為個人資訊，可能會成立電腦處理個人資料保護法的犯罪，而論以三年以下有期徒刑。參李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 252-253。

[330] 試想在單機電腦的主機開機鈕上裝設手動電子密碼鎖，而行為人將該密碼破解而使用電腦登入使用者為自己的作業系統介面的情形，在此僅是把主機開機鈕上的密碼鎖更換為電子鎖而已。

第三節　取得、刪除或變更電磁紀錄─刑法第 359 條

第一項 實務上之運用情形

於取得、刪除或變更電磁紀錄的部分，因實務上多數案例即與非法入侵同時成立，故可以得知於此部分案件最多的類型仍然是網路遊戲盜帳號以及員工的不法行為二類。然而就此二類而言仍有與前述無權進入電腦部分相異之處，以及此二類以外的其他類型相較於無權進入電腦部分更加多樣，故以下仍就網路遊戲盜帳號、員工不法行為以及其他類型三類作分析。

首先就網路遊戲盜帳號的部分，最常發生的犯罪流程即如同前述無權進入電腦部分，於進入遊戲前往往會有一個輸入他人帳號密碼的階段在。而輸入他人帳號密碼後，即會於遊戲內以變更電磁紀錄[331]的方式將虛擬寶物移轉至行為人或他人的帳號下。然而於此部分仍有另一種犯罪流程值得觀察，即是於網路咖啡廳等公共場所，利用他人暫時離開電腦但並未登出遊戲的空檔，使用其正在進行遊戲的電腦，並移轉其虛擬寶物的流程[332]。此種犯罪流程多發生在民國 91 至 92 年間，此時期正好是我國網路遊戲開始普及的時期，故而民眾在面對網路遊戲此一新興的遊戲型態時，並無相對的具備相關安全知識，始會導致此類案件發生。從此種流程已在 93 年後日漸減少也可以得知，在網路遊戲普及一段時間後，玩家的相關網路安全知識已有所成長。同時，此種「趁虛而入」的犯罪流程根本不需要取得被害人的帳號密碼，相較起先得知帳號密碼後輸入的犯罪流程來說，所需要的電腦專業知識更低，然而於法律適用上的結果卻等同甚至可能重於輸入帳號密碼的犯罪流程。

再者，就員工不法行為的部分。除無權進入電腦部分所述的離職員工輸入在

---

[331] 在此係指改變電磁紀錄的「磁性配列方式」，並非法條上所指的變更電磁紀錄，參李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 237-238，註 4 處。

[332] 參台北地院九十二年度易字第一六四四號判決、台北地院九十二年度簡字第三八四二號判決、台北地院九十六年度簡字第一一六八號判決等。

職時的帳號密碼登入原任職公司電腦後取得資料的犯罪流程外，在此還有行為人於任職中本即為在職公司電腦的管理者或是得以使用在職公司電腦，然而其於任職期間使用帳號密碼登入公司電腦後，取得、刪除或變更公司電磁紀錄的犯罪流程[333]。與前述流程較不同者為，此類流程的行為人雖不乏具有一定的電腦專業知識者，但在此流程中行為人使用其電腦專業知識的比率幾乎為零。然而，此類行為所造成結果的被害規模，往往會隨著行為人對電腦專業知識的了解程度而大幅的增加[334]。故由以上可以推知，此種犯罪類型行為本身雖不需要具備太高的電腦專業知識，然而有機會違犯此類犯罪者，很可能是具有一定電腦專業知識的人，並且被害程度會依照電腦專業知識的高低而有很大的不同。而就被害程度的不同與電腦專業知識的關係而言，推測極可能是因為若行為人具有高度電腦專業知識，所取得、刪除或變更的電磁紀錄更具關鍵性，並且使用的手法會更加徹底，使系統或資料的復原可能性降低，再加上若公司內部僅有行為人或少數人具有相關知識，則行為人的行為更難以及時發覺之故。

最後就其他類型部分，除無權進入電腦部分所述的無權入侵他人學校系統後將其以選上課程作退選，以及輸入他人的帳號密碼，進入他人信箱或是社群網站，並將含有木馬病毒的檔案或以電子郵件之方式轉寄，或儲存於被害人之家族網站內使更多人能夠下載犯罪流程外，仍有二個值得注意的犯罪流程。有冒名致電中華電信要求更改被害人手機語音信箱的密碼[335]者，亦有撰寫電腦程式並謊稱其為「增強元件」供人下載安裝後，反而於被害人電腦中安裝病毒元件以阻礙被害人瀏覽網頁[336]的流程。其中前者的案例，法院認為行動電話語音信箱的密碼，係一「電腦或相關設備上的電磁紀錄」，而利用致電中華電信的方式變更該密碼則會成立本罪，然而在此法院對於「行動電話是電腦或相關設備」一事並無任何的推

---

[333] 參台南地院九十五年度訴字第六九五號判決、台中地院一〇〇年度訴字第一一六二號判決、高等法院九十六年度上更(一)字第九四九號判決、最高法院一〇〇年度台上字第五二號判決、智慧財產法院九十九年度刑智上更(一)字第二三號判決、最高法院一〇〇年度台上字第三三七五號判決等。

[334] 如台南地院九十五年度訴字第六九五號判決，該案中的行為人即是負責公司電腦設備之管理維護者，並且其刪除及變更的檔案皆是於公司重要的執行檔，此些檔案一被變更或刪除，即會造成該鍍膜公司於鍍膜製程上造成重大影響，且該公司僅有該行為人具有電腦專業知識，故其刪除變更的行為更難被發現，導致該公司直至行為人離職後，始由接續其工作的員工發現。

[335] 參士林地院九十九年度訴字第一二二號判決。

[336] 參台北地院九十四年度訴字第一五一四號判決。

論或涵攝，並且對於行為人以致電的方式要求中華電信人員變更密碼是否為與電腦特質相關亦無任何解釋，即認為此種行為係一「妨害電腦使用」的行為，此種案例的論罪處罰，是否與當初立法者所欲防範的電腦犯罪相符不無可議。於後者部分，行為人僅是加裝病毒軟體在被害人等的電腦內，而該病毒軟體亦只是在使用者電腦內加裝檔案，並未取得、刪除或變更被害人電腦內的任何電磁紀錄，然本判決似乎認為「加裝檔案」亦屬「變更電磁紀錄」的一環，實與立法當時立法者所考量的適用情形相左[337]，可見就此部分實務上的適用情形與立法者所希望的規制情形完全不同。

第二項 現今所受到之批評

於本條施行後所遭受到的批評上，大多環繞在本條的構成要件中所規定的三種犯罪態樣—取得、刪除、變更上。首先就「將取得、刪除、變更」規範在同一條上等而視之的規範方式部分，有學者認為此種統包式的規定，會造成一種規範中，出現各種不同行為型態，並且各行為型態間不但無必然性前置關係或同類性關係，而會使得該條性質無法明確加以界定，亦會使得同時出現取得與刪除、變更此種破壞行為時，適用上出現困擾，從而違反罪刑法定原則下的構成要件明確性原則，並建議縱使不將取得行為及刪除、變更行為分條規定，亦應在同一條內分項規定[338]。

再者，就取得、刪除、變更電磁紀錄的文義解釋上亦出現爭執。雖有論者認為取得行為若專以電磁紀錄的隱私性角度出發，則係指行為人獲得該電磁紀錄的行為；而刪除則係指行為人將該電磁紀錄的存在抹消至無法復原的情況，並使原持有人對於電磁紀錄的支配性終局受損[339]；至於變更必須是他人電腦中本即存有

---

[337] 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年，頁 251，靳宗立教授以及葉奇鑫檢察官之發言。

[338] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 127。

[339] 若僅丟入資源回收桶而仍有復原可能者並不該當，參台南地院九十五年度訴字第六九五號判決。

該等電磁紀錄，行為人將其性質或內容轉變，而與原先不同的行為[340]。然有不同見解個別對此三種行為態樣提出了一些問題。第一，就取得行為的部分，論者認為在此的「取得行為」僅是替代修法前的刑法第 323 條於電磁紀錄的部分，至於取得與竊取間到底存在何種差別，修法前與修法後皆無法解釋清楚。同時，如在網路上瀏覽網頁時，皆會將網頁上的元件下載於自己電腦的暫存檔中，此種自動存取是否會有夠成本罪的可能不無疑義，尤其是本罪還不如竊盜罪般還設有「不法意圖」的限制，於適用上被濫用的可能性更高[341]。又，與竊盜罪密切關聯的贓物罪部分，於本罪章亦無任何類似的規定，論者認為或許可適度擴張解釋贓物罪中「贓物」的文義，然先不論是否妥適的問題，立法者宣稱本罪章是「集所有電腦犯罪於一身」一事可謂思慮不周。第二，就刪除行為的部分，雖本罪的規定解決了以往刪除非文書的電磁紀錄時無法適用刑法處罰的問題，然而本條就刪除行為籠統的規定，即會造成同樣是刪除行為，卻受到不同規制待遇的不公平結果。蓋我國於毀損文書罪的部分，係規定只要達「足以生損害於公眾或他人」的程度即會成立犯罪[342]，然本條犯罪的成立，則有「致生損害於公眾或他人」此一較嚴格的要件，此時若行為人刪除一電磁紀錄，雖該刪除行為足以生損害於公眾或他人，然尚未達到致生損害於公眾或他人的程度時，即會產生一個「視刪除的客體為何而是否成立犯罪」的詭異情形。第三，就變更行為的部分，除存在與前述刪除電磁紀錄部分在偽造(於刪除部分是毀損)文書罪的適用部分上有相同失衡現象的問題外，此部分亦存在可能會淪落至變成刑法第 339 條之三的未遂規定的問題。於草案的修正理由中，雖有特別闡述本罪與刑法第 339 條之三的不同，認為本罪並不涉及對電子化財產(金融)秩序的的順利運行的危害，故刑度較輕但處罰範圍較廣[343]，然論者認為就立法者此舉可謂非常輕率，或許立法者認為「變更他人電磁紀錄」即會「致生損害於他人」，而電磁紀錄並不限於與金融秩序有關，故在成立刑法第 339 條之三前即會先成立本罪，則在此種輕易認定「致生損害於公眾

[340] 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 101。
[341] 然論者認為此種暫存行為縱可能造成個人利益損害，仍難謂會造成公眾或特定多數人利益的損害，故若認本罪所保護者為社會法益，此種行為仍不致與本罪相繩。
[342] 參刑法第 220 條及第 352 條規定。
[343] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 359 條之修正說明第四點。

或他人」的操作下，本罪即會變成刑法第 339 條之三的未遂罪規定[344]。故論者建議既本罪與刑法第 339 條之三的關係非常密切，則在修法時即應考慮刑法第 339 條之三的定位問題[345]。

此外，就本罪的成立必須要有「致生損害於公眾或他人」的要件部分，有論者認為此種要件係一「結果性要件」，亦即在判斷行為人是否成立本罪時，除要討論行為人的行為是否造成電磁紀錄被取得、刪除或變更的結果外，還要檢討該電磁紀錄的取得、刪除或變更是否造成「致生損害於公眾或他人」的結果，成為一種「雙結果犯」的類型規定[346]。亦有類似見解的論者認為此種要件的設置無疑意味著立法者認為本罪的保護法益是一社會法益，然縱使如此，於我國刑法所規範社會法益的各種犯罪中，僅有使用「致生(公共)危險」或「足以生損害於公眾或他人」，並未曾使用「致生損害於公眾或他人」此一用語，立法者採取此種用語無疑紊亂刑法體系[347]。而在此論者認為，若本條係以增訂「足以生損害於公眾或他人」要件的方式作修正，則本要件的定位會變成對於行為侵害的「確認性佐證」，而非是結果要件，則增訂規範即得以肯定[348]。

最後，就無故取得電磁紀錄於實務上的適用部分，有實務工作者認為此項規定於實務上某些案例實則適用困難。第一，就僅得以在特定場所使用的特定資料，行為人於該場所中有使用電腦取得該些資料的權利，然其在取得該些資料後即將該些資料以 USB 隨身碟或其他存取媒體後帶離該特定場所，此種帶離的行為亦可能會危害立法理由所述的「電腦中之重要資訊遭到取得、刪除或變更，將導致

---

[344] 事實上，在臺灣高等法院暨所屬法院 91 年法律座談會的座談上，以及實務上 92 年的判決中，亦可以發現有很多網路遊戲盜帳號的情形實務上是以刑法第 339 條之三來論處，其理由往往是「339 條之三是全部性的規定，而 359 是一部性的規定，基於全部法優先於一部法原則，故僅適用 339 條之三已足。」。參臺灣高等法院暨所屬法院 91 年法律座談會刑事類提案第 11 號、基隆地院九十二年度基簡字第八一七號判決、台北地院九十二年度簡字第三八四二號判決。

[345] 李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 3 月，頁 253 以下。

[346] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 127-128。

[347] 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 243-244。

[348] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 128。

電腦使用人之重大損害」以及「電腦使用安全」的保護法益[349]。第二，就前述實務上員工於離職前對於主管不法行為的部分，亦可能發生員工在任職期間將自己有權限取得的資訊、或是公司所有，而其於任職期間有專屬使用權的電腦內部的資訊，或甚至是自己所有而帶至公司處理業務的筆記型電腦中所儲存的資訊，藉由 USB 隨身碟或 E-MAIL 等途徑給帶回家中，待離職後轉至公司的競爭對手企業底下服務後，再將此些資料提供給現任職的公司，導致原公司的重要資訊以及客戶皆被競爭對手得知。此類行為除了在極少數的情形可以用背信罪來處罰外，亦可能違反營業秘密法，然而違反營業秘密法僅負民事責任，故社會上多數受害公司皆對洩漏資訊的前員工主張本條，然而其認為就立法者所闡釋的立法目的上，應難有本條的適用，若機械式的操作法條，極可能造成以刑事手段來保護民事爭訟範圍內營業祕密的問題[350]。

第三項 遞續性上之困境

於雲端運算時代來臨後，使用者面臨 IT 資源共享的局面。在此所謂共享的 IT 資源，除硬體資源外，亦包含軟體資源[351]。就如同硬體資源的共享時，若將該共享的硬體資源為破壞，相較於僅將非共享的硬體資源破壞而言損害較大一般，若對於共享的軟體資源(電磁紀錄)為破壞，亦相較於僅將非共享的軟體資源破壞的情形，給予社會大眾的影響更大。然而本法卻未對其作區分，皆論以相同之罪，並給予執法者一樣的量刑程度，於罪刑相當原則部分即可能產生疑義。從而在軟體資源的共享部分，刪除、變更或取得電磁紀錄的部分似可以考慮做區分，分為對於多數人共用的電磁紀錄(軟體)為刪除或變更，以及對非共用的電磁紀錄為刪除、變更或取得，並給予不同程度的規制。

第四節　干擾電腦運作─刑法第 360 條

[349] 在此論者舉出國軍部隊中的案例來解釋此種情形。在部隊內如演習的簡報檔、或國外的出訪名單等資訊，得以在部隊內取得使用，雖此些資料尚未達機密程度，但也不適合流出至外部，而若有行為人將此些資料帶出部隊，是否會違反此項規定即有爭議。

[350] 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 89-90。

[351] 例如防毒軟體公司僅在其電腦內放置一套防毒軟體，而依照各個使用者與其的契約狀況提供該使用者使用該套防毒軟體的時間以及掃描病毒的程度等服務。

第一項 實務上之運用情形

實務上對於此種犯罪類型的案例非常少，除於前述取得、刪除或變更電磁紀錄的部分所提及的撰寫電腦程式並供人下載安裝後，反而阻礙被害人瀏覽網頁的尋夢園案例之外，僅有網路遊戲外掛程式、洪水攻擊以及員工離職後的不法行為等少數案例。然雖案例數量少，此些犯罪流程亦頗具有探討價值。首先是前述尋夢園案例部分，行為人之一是一電腦工程師，可謂具有高度的電腦專業知識，並且其所使用的犯罪手法以及造成的效果也是有運用到其高度電腦專業知識。然而就結果而言，植入該病毒程式後所造成電腦的效果亦只是「限制他人連結至其他聊天室[352]」此種惡作劇般的效果而已，與立法者所憂慮的「對電腦及網路設備產生重大影響」情形顯然還有很大一段差距。反面而言，從立法理由中觀察也可以發現此種僅輕微影響電腦運作的干涉行為，實則不在立法者認為應處罰的範圍內[353]，然而實務對此的判斷即認為成立犯罪，與立法者當初所期待的規制結果並不相符。

再者是於網路遊戲中使用外掛程式的部分，此案例的犯罪流程是行為人將一可獨立運作於特定網路遊戲，進行打怪練等等功能的外掛程式上傳至其架設網站，並提供該遊戲的玩家下載後使用，而該外掛程式會傳送大量封包予遊戲公司的伺服器，令角色自動打怪練等，長期或大量使用之下，會使遊戲公司的伺服器不堪負荷，以至系統資源耗盡而當機[354]。然姑且不論本案是否是因為遊戲公司所提供的伺服器效能過低，導致系統資源容易被「灌爆」，亦不論此種外掛程式如何能「致生損害於公眾或他人」，在此案例中值得注意的點是，法院認為此種外掛程式會使玩家自動打怪升級獲得大量虛擬寶物與貨幣，會有損遊戲公司「獲利」[355]。

---

[352] 若他人連接到其他聊天室網站的話，該程式也只會使系統自動連結回行為人所架設的聊天室網站，不會對其電腦內部的資源或系統運作上有任何重大危害。

[353] 中華民國刑法第 360 條立法理由第二點。

[354] 參士林地院九十三年度訴字第五三二號判決、台南地院九十四年度簡字第七四七號判決、台南地院九十四年度簡上字第三五八號判決、高等法院台南分院九十六年度上易字第一五七號判決。

[355] 參台南地院九十四年度簡字第七四七號判決、台南地院九十四年度簡上字第三五八號判決、高等法院台南分院九十六年度上易字第一五七號判決。

但該些案件內的遊戲公司所提供的網路遊戲，皆為月費制的網路遊戲[356]，虛擬寶物獲得數量的多寡根本無關遊戲公司的收益，僅有可能是在「使用外掛後，無須購買點數卡即得進行遊戲」，或「降低遊戲耐玩度」等理由上遊戲公司可能可認有所損失，然法院並未敘明遊戲公司是何種獲利受到損害，亦未區分該類外掛到底是輔助型、輕度破壞型或重度破壞型[357]，即一律認為「製作或提供外掛程式」而非「使用外掛程式」的行為人成立本罪，此種判斷的標準與立法者當初所預設的處罰對象是否相同則不無可議[358]。

又，於洪水攻擊的部分，實務上所發生的案例通常是行為人利用程式或親自發送極大量無意義的封包至被害人的伺服器，導致被害人的伺服器無法正常運作，而出現延遲甚至當機的現象[359]。然而法院於干擾行為的判斷上，或有認為本條是修正前第 352 條第二項的挪用規定，故認為本條的干擾必須「進出存取(ACCESS)他人電腦中央處理器(CPU)記憶體內之所製成電磁紀錄如軟體程式、檔案等內容，而進行變更、抹除、植入等之干擾電磁紀錄行為，致造成他人電腦當機或喪失原有處理運算資訊功能，而非指以經電腦處理後所顯示之聲音、影像或符號(OUTPUT)進行干擾」者[360]，或有認為本條立法理由中有列舉 DDoS 攻擊，從而若該當 DDoS 攻擊者即會成立本罪者[361]。然無論採以上何種見解，法院似乎多認為只要該當「干擾」行為(或只要是 DDoS 的情形)，幾乎一定會「致生損害於公眾或他人」，而對此要件採取相當寬鬆的認定標準。

---

[356] 所謂月費制係指遊戲公司提供遊戲的使用時間作為服務，而玩家必須以購買點數卡等方式換取遊玩的時間，至於在此遊玩的時間內能獲得多少虛擬寶物或成就，皆是視玩家自身遊戲技巧的服務模式，其名稱的由來是因為此類型的網路遊戲所提供一次最長的服務時段多為包月遊玩(月卡)，且亦為多數玩家所購買。

[357] 論者有謂輔助型外掛僅是針對遊戲操作的便利性所設計(如受傷自動喝水)，而輕度破壞型外掛則是會稍微影響遊戲公平性者(如自動練功)，至於重度破壞型外掛，則是會大力破壞遊戲平衡，並對於遊戲公司伺服器進行破壞者(如大量洗錢、複製限定寶物、更改人物參數等)，參盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 748-749。

[358] 雖於士林地院九十三年度訴字第五三二號判決中有提及上述問題點，然於台南地院九十四年度簡字第七四七號判決、台南地院九十四年度簡上字第三五八號判決，以及高等法院台南分院九十六年度上易字第一五七號判決中皆無論及。

[359] 參高雄地院九十三年度易字第一三一〇號判決、台北地院九十四年度易字第四八五號判決、高等法院九十五年度上易字第二五五號判決、最高法院九十七年度台非字第二一四號判決等。

[360] 參台北地院九十四年度易字第四八五號判決。

[361] 參高等法院九十五年度上易字第二五五號判決。

最後是員工離職後的不法行為部分，此案例係離職後的行為人欲取得公司營業秘密，而將其任職時所獲得的員工電子郵件信箱帳號密碼一一嘗試輸入，雖因被害人公司員工皆已更換信箱的帳號密碼而未進入成功，卻因多次輸入行為使得被害人公司發現而送法辦[362]。值得注意的是，法院對此種「嘗試入侵」的行為會認為屬於干擾行為的一種，此種作法似有將本條作為第 358 條的前階段行為或未遂行為的意味在。

第二項 現今所受到之批評

就本條於施行後所遭受到的各種批評中，除與前述取得、刪除或變更電磁紀錄罪中同有「致生損害於公眾或他人」的要件而會造成與前述相同的批評外，最主要都是環繞在「干擾」用語的不確定性。多數論者認為，本條的修正是為將舊刑法中第 352 條毀損文書罪的第二項干擾電磁紀錄罪中，構成要件「干擾」的意義實為不明確，以及干擾行為並非毀損，與有形的毀損本質並不相同等問題作有效的解決，故獨立於刑法第 360 條作增訂[363]。有論者謂此種修正的態度雖可謂正確，然而修正後的條文卻無法實現此種立法精神，還可能更會造成新的困擾，可謂立法者為德不卒之處。首先，就修正後的「干擾」行為的定義而言，因前述修正理由已經述明「干擾」不等於「(物質上的)毀損」，則立法者勢必得面對如何定義「干擾」的問題。然立法者在對干擾行為的處理上，卻採取與定義無權進入電腦行為一樣的做法—以限定行為類型的方式來確定受害的程度。立法者似乎認為在限定行為類型後，再將干擾行為中如 ping 測試或大量垃圾郵件等較輕微的情形給去除，即可給予「干擾行為」一個相對明確的概念[364]。然而此種將光譜的兩端給絕對排除的作法，並不等於干擾一詞已經被明確定義，仍要透過其他解釋結果始得確定其範圍，否則在運用上很容易出現恣意的問題，僅能期待日後司法人

[362] 參板橋地院九十一年度訴字第一〇二八號判決、高等法院九十三年度上訴字第一八八二號判決、高等法院九十八年度上更(一)字第三一二號判決等。

[363] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 352 條之修正說明，以及第 360 條之修正說明第六點。

[364] 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 360 條之修正說明第二點。

員於適用本條時能藉由判決或判例對干擾的判準明確化[365]。再者，在干擾的判準上，亦有論者提出此種干擾其實可以從類型化甚至個別化的方向思考，例如以舊型 386 電腦安裝 windows2000 的作業系統時，其系統效能本即十分有限，此時或許單純寄十封電子郵件即會使該電腦因過度運作而當機[366]，而此種寄十封電子郵件的行為是否該當「干擾」則不無疑義[367]。最後，於干擾行為於實務上的適用部分，亦有論者認為本條構成要件中不明確者除「干擾」本身外，於限制干擾的手段—「以電腦程式」或「其他電磁方式」二者亦存在不明確的問題，對於未諳電腦的法律人甚至一般人而言可謂重大障礙[368]，可能僅得如前述論者般依照個案實例予以累積[369]。

此外，就本條與第 359 條可能產生競合的問題[370]，雖有論者認為無論行為人使用何種方式，只要行為係以電磁紀錄作為攻擊對象，且有足以造成該電磁紀錄的變更或消除者，即會同時成立取得、刪除或變更電磁紀錄罪，在競合後即會成立較重的第 359 條[371]。然有不同見解認為在此因事前所設定的因果進程本即不同，故不會產生競合關係，而主張以公眾或他人的損害係導因於何者來決定成立何罪。若損害係導因於電磁紀錄的刪除或變更時，則成立刑法第 359 條之罪；反之若損害係導因於對電腦系統機能的干擾時，則成立刑法第 360 條之罪[372]。

第三項 遞續性上之困境

---

[365] 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 207 以下。

[366] 此案例看似誇張，然而此例已充分顯示出社會上各種電腦效能不一，要如何判斷干擾行為的成立，實則為一值得深刻思考的問題。

[367] 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 103。

[368] 論者舉出一例：行動電話亦會放出電磁波，而若在加護病房旁撥打行動電話，使得人工心肺機產生雜訊，按照目前法條文義解釋，亦會該當本條之罪。

[369] 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 97。

[370] 若干擾行為除造成電腦系統無法正常運作外，還另對該電腦系統內的電磁紀錄作取得、變更、刪除時，與前述第 359 條的競合關係。

[371] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 125；鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 111 以下。

[372] 該論者提出一例供思考：某甲利用會不斷複製檔案的電腦病毒來干擾他人的電腦，而某乙則是利用會刪除或變更某程式的.dll 執行檔，使程式運作產失誤差，進而干擾電腦正常運作。此二種行為在前述論者的概念下，後者即會成立第 359 條之罪，然而論者認為在此皆應論以第 360 條之罪，而使用的手法方面則僅影響刑法第 57 條的判斷而已。參李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 209。

干擾電腦運作的「干擾」一詞有很多種解釋方式，其甚不明確已如前揭現今遭受的批評部分所述。若是照立法理由所述，干擾係指「對電腦及網路設備產生重大影響，以致無法正常運作的行為」，則在雲端運算的時代中，因硬體可以大量無限擴充的緣故，要干擾此種電腦以致雲端主機癱瘓，並達「致生損害於公眾或他人」的結果可以說是幾乎不可能發生的事情[373]。故勢必要對「干擾」做其他面向的解釋，或修改「致生損害於公眾或他人」的規定，始有將干擾行為入罪化的可能。而此種面向的「干擾」既與立法理由所述者不同，則在規制的構成要件以及法律效果的設計上亦應重新考量。

第五節　妨害公務機關電腦使用之加重─刑法第 361 條

第一項 實務上之運用情形

本條自立法施行以來，少有實務判決有提及其運用。而會造成此種情形，一來很可能是實務上面所處理的電腦犯罪類型，多與個人或企業的利益有關，並無使用到本條的機會，二來亦可能是因目前實務上所查獲的案例中，行為人的電腦專業知識普遍不高，並無入侵公務機關電腦的能力，此部分可能意味著於偵防方法上，對立法理由中真正想要規制，足以威脅國防安全的高明駭客，實務上根本沒有足夠能力將其繩之以法[374]。然而無論是上述何種原因，會造成實務上的運用與立法者立法當時的期望相悖離的結果，於規範的設計或保護目的上，一定出現了一些問題。

而目前實務上有提及的運用案例中，大多是諸如盜領加班費、將警察局官方

[373] 除非以極度大量的封包將通訊傳輸的線路(如網路)的頻寬給占滿，但姑且不論網路線是屬於何人的電腦或相關設備的部分(何人有告訴權)，此種行為態樣相較於以洪水攻擊癱瘓他人主機難度更高，且假設本章所規定的刑度本即合於罪刑相當原則，就整章的刑度體系來看，以本條處罰此種將網路線灌爆的行為可能過輕。

[374] 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 210 以下。

網頁首頁的國旗改成五星旗等與國家機密等無涉的情事[375]，然而亦有少數牽涉立法理由所述的國家機密或公務機關資訊安全者，如行為人不滿任職於消防署的同事於訴訟上作對己不利的證詞，而輸入其帳號密碼進入差勤系統中，並列印公差統計以及刷卡記錄等資料者[376]，或有為將新生兒資料提供予特定公司而越權輸入向主管騙來的帳號密碼進入出生通報系統後，非法下載全國新生兒及產婦的個人資料者[377]，以及行為人為查看身為高雄市政府員工的被害人的電子郵件信箱，而在進入高雄市政府員工郵件系統後，輸入被害人的姓名、身分證字號等資料，並點選「忘記密碼」欄位，使該系統判斷錯誤而重新發給一組新密碼，並利用該新密碼進入郵件系統查看信件[378]等案例。

其中值得注意的案例者為，行為人為提再審，而連結至法務部的書狀例稿區，並誤開啟「再議」的書狀並填妥個人資料後回存。然因該系統老舊，允許將置於該網站上的文件修改後回存的指令，導致法務部的再議例稿被改成已填寫被告個人資料的版本[379]，而行為人回存後發現法務部竟「無故刊登」其個人資料於網頁上而大為驚訝，遂找記者將此事大肆宣揚，導致法務部長公開致歉。於歷經數次審判的此案例中，法院多依公訴例旨認為行為人的行為不但該當於「變更他人電腦內的電磁紀錄」外，還達到「致生損害於法務部對於書類空白例稿電子檔案管理之正確性」的結果[380]。在此一方面再度顯示實務上對於「致生損害」要件的操作非常寬鬆之外，此案例中行為人教育程度僅有國中畢業，並且從其辯稱其根本不知道會回存檔案一事也可以看出其或許連電腦作業系統的基本使用能力都不具備，其此種「烏龍行為」若亦成立本罪，似與立法者當初預設的處罰範圍有一段不小的差異。

第二項 現今所受到之批評

---

[375] 參高等法院台中分院九十七年度上訴字第三一〇八號判決、高等法院九十九年度上訴字第三七〇六號判決等。

[376] 參高等法院九十五年度上訴字第七六五號判決。

[377] 參台北地院九十三年度訴字第一一五七號判決。

[378] 參高等法院高雄分院九十五年度上訴字第一五八九號判決。

[379] 參台北地院九十五年度訴字第一一一七號判決、高等法院九十五年度上訴字第四四一七號判決、台北地院九十六年度訴更(一)字第一號判決、高等法院九十六年度上訴字第一三一三號判決、最高法院九十七年度台非字第二八五號判決。

[380] 雖各審級多認為本條為告訴乃論之罪，因欠缺告訴而不受理。

於本條現今所受到的批評上，就立法意義部分，學者認為本條的立法表彰了兩種意義—重視對政府機關電腦的保護，以及對於金融、商業用的電腦或相關設備不刻意的保護。然而就前者的部分，學者指出本條立法背景正值中國大陸利用「網軍」攻擊我國政府機關網站，使得國防等機密受威脅，此種考量自立法理由中亦可以窺知一二[381]。然而一來此種威脅往往來自國外而無法逮捕規制，二來目前重要的訊息往來因考量網路的脆弱性，亦不會透過電腦網路傳遞。故學者推測本條並非是如立法理由所述為保障的國防機密，而是由第二種意義下的推測，亦即為掩飾藉全面性的嚴罰而保障資本家利益的現象[382]。

此外，就公務機關的定義上亦產生爭議，多數見解即認為公務機關的相關公務資料亦可能委託民間電信業者保管，或向其租用或借用主機，甚至公務機關的電腦本身亦有可能完全不涉及公務資料者，此種以公務機關為分類基準，於運用上可謂徒增困擾[383]。同時，國內亦有部分機關雖非政府機關，但其執行相當於政府事務，如亞東關係協會或證券交易所等，如對該些機構的電腦違犯電腦犯罪所造成的危害似較對公務機關為之更大，故論者建議將犯罪客體部分擴大為除公務機關之電腦外，亦包含公務機關使用之電腦[384]。

第三項 遞續性上之困境

首先就本罪加重的理由部分，國防機密這點在前述現今所受到的批評部分已經有論者點出其矛盾之處，故本條加重的理由應不是為保護國防機密，且前述論者亦有提及商業以及金融企業的問題，商業以及金融企業除有營業秘密之外，會涉及與民眾相關者即是其保有社會大眾的大量重要資訊，無論是個人資料或是財產亦或是使用習慣等等，若因有心人士入侵該些企業的電腦而將該些資訊交到其

---

381 中華民國刑法第 361 條立法理由第二點。

382 易言之，學者認為本罪章的刑度皆過高，立法者更設立一個更加嚴罰的規定吸引民眾注意力，而使其忽略本罪章的刑度皆過高的事實。而本罪章的保護客體，實質上會限縮於金融或商業網路上的電腦，然金融或商業界為掩飾自己大量引進電腦系統又不致力於安全維護的行為，即會贊同政府的嚴罰，以推卸自己責任。參李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 210 以下。

383 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 98。

384 王銘勇，侵入電腦系統罪之研究，法令月刊第 55 卷第 3 期，2004 年，頁 266-267。

手上，社會整體運作即會大亂。故綜合以上可以得知，本條要加重的理由應是「保有大多數人重要資訊的電腦更加不可以被侵害」這點，而非如立法理由所述是國防機密。

同時，在雲端運算出現後，除了公務機關的電腦外，保有大多數人的重要資訊的私人企業亦會更加增長[385]，並且所持有的重要資訊亦會更多，對於侵害這種保有大多數人重要資訊的私人企業電腦亦應考慮是否加重處罰，以符合本條的加重理由。若認亦應加重處罰，於要件的設計以及考量上可能必須注意是否可能使本條成為私人企業怠於增強自己網路安全措施的最佳理由。

第六節　製作並散布犯罪電腦程式—刑法第 362 條

第一項 實務上之運用情形

與干擾電腦運作的犯罪態樣類似，本條幾乎很少出現在修法後的實務判決中，亦成為實務上的冷門條款之一。然而耐人尋味的是，我國實務上所出現的各種判決中，使用犯罪電腦程式[386]的案例非常多[387]，而其中雖大多數是非行為人所撰寫者，然亦不乏行為人親自撰寫犯罪電腦程式並使用的情形[388]。可見犯罪電腦程式的使用在現行實務上的電腦犯罪態樣中，仍是佔了重要的一環。但實務上對於此些自己撰寫犯罪電腦程式並使用的案例，皆無判斷是否成立犯罪，甚至連是否有成立犯罪的可能都尚未提及。姑且不去考慮實務判斷上疏忽的問題[389]，會造成此

---

385 就現階段而言 facebook 即持有大多數人許多重要的個人資訊。

386 或我們可以從立法理由中得知，此種「犯罪電腦程式」，可以理解成包含電腦病毒、木馬程式、電腦蠕蟲程式等惡意的電腦程式。參中華民國刑法第 362 條立法理由第二點。

387 參板橋地院九十一年度易字第三五八五號判決、台中地院九十四年度中簡上字第一六一號判決、台北地院九十四年度訴字第一五一四號判決、花蓮地院九十五年度花簡字第九九六號判決、花蓮地院九十六年度簡上字第三九號判決、屏東地院九十七年度訴字第七三六號判決、高等法院高雄分院一〇〇年度上更(一)字第二十三號判決等。

388 參板橋地院九十一年度易字第三五八五號判決及台北地院九十四年度訴字第一五一四號判決。

389 事實上，實務於自己撰寫犯罪電腦程式並使用的案例並不僅有一例，而於該些案例中皆未提及本條的適用，故要以「實務集體忽視本條文」為理由來解釋實務上的此種現象，恐怕過於牽強。

種情形有極大的可能是法律條文本身即存在著解釋或適用上的問題，以致實務上根本難以適用。

於實務上有討論到本條的案例中，除前述外掛程式的案例[390]外，僅有撰寫程式取得大量網路銀行的帳號密碼進而惡用以及撰寫程式進入他人公司後取得客戶資料等案例[391]。而此些案例均有一個共同特徵—撰寫者皆自己使用該程式。或許可以從此角度推知僅撰寫並散布程式而未使用的行為人根本難以繩之以法，然亦可就法院量刑以及競合的部分，發現實務上對本罪的定位往往是刑法第 358 條至第 361 條的預備犯，此是否與立法者所設定的定位相同，亦是值得討論的部分。

第二項 現今所受到之批評

於製作並散布犯罪電腦程式罪現今所受到的批評中，最主要是集中在三個部分—本罪的定位、「專供犯本章之罪之電腦程式」此一構成要件的解釋，以及「致生損害於公眾或他人」此一結果要件的妥適性上。首先，就本罪的定位而言，多數論者皆認為本罪是刑法第 358、359、360 條的實質預備犯，並進而認為在本章各罪皆無處罰未遂犯的情況下，將實質預備犯獨立處罰將違反罪刑法定原則[392]。更有甚者，認為本罪的刑度較同法第 358 以及第 360 條要重，亦會產生預備行為處罰較重的不合理行為[393]。然在此有不同見解試圖將現行法的規制合理化，將本罪的處罰重點置於「提供」行為而非製作行為，認為當行為人製作出一具有危險性的電腦程式時，該製作行為即是「前行行為」，此時行為人本身即被賦予一「管理」的義務，若此時行為人積極的提供予他人，或雖未積極提供，但卻置放於網

---

390 參士林地院九十三年度訴字第五三二號判決，然本判決似認為該外掛程式並非「專供犯本章之罪」的程式。

391 參高等法院台中分院九十八年度上更(一)字第三五號判決、高等法院台中分院九十八年度上訴字第一一九二號判決等。

392 盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 752-753；鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 113；林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 107；柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 128。

393 盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 752-753。

路空間讓人任意下載，即會成立本罪。據此，其認為本罪的定位係一「具有實質預備犯性質的正犯」，而合理解釋了本罪的刑度較前述各罪為重，以及未處罰未遂犯卻處罰實質預備犯的不合邏輯規制體系[394]。

再者，就「專供犯本章之罪之電腦程式」此一構成要件的解釋部分，大多數見解均認為若單純按文義解釋，本條幾乎無適用餘地。蓋並無任何電腦程式是除用來犯罪外沒有其他用途，此項構成要件於實務的運用上，無異鼓勵行為人作「無恥抗辯」而非「無罪抗辯」，亦即僅要行為人告訴檢調單位其所製作的程式，是不只拿來犯「本章之罪」，還欲拿來犯「其他各章之罪」，即不會成立本罪[395]。故除提倡將「專供犯本章之罪」要件刪除者外[396]，以下各種見解均是設法為「專供犯本章之罪之電腦程式」的意義作一個合理的解釋。其中有見解認為自立法理由觀之，所謂「專供犯本章之罪之電腦程式」是指該電腦程式「主要的」用途是拿來作為犯本章之用，並舉出如系統監控程式等工具程式，主要是拿來作為系統監控，故非本條所指稱者[397]。然而有學者從不同角度思考，認為立法者之所以會如此規定，是導因於立法者試圖以「專供」的客觀事實來證明行為人的主觀「惡意」，然而一來「惡意」的範圍較「專供」廣，有些立法者想處罰的行為無法有效規制；二來因「專供」、「惡意」等詞彙的意義皆難以確定，在實務上很可能會以實際發生的損害結果來反推程式的有害性，然而此即會發生邏輯倒置的矛盾；三來若試著將「專供」的意義給移至第二行為要素作討論，即可能會產生構成要件行為類型化危險性空洞化的結果，使得前述限定電腦犯罪功效門檻的效用化為烏有[398]，從而導出將製作與提供行為分開處理的結論，在製作部分僅判斷所製作者是否為一「危險的電腦程式」，而將規制重點置於之後的提供行為[399]。然在此亦有論者持反對意見，認為前述見解會使得製作程式者戰戰兢兢，進而引發寒蟬效應，造

394 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 212 以下。
395 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 99。
396 鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 114。
397 黃仲夫，刑法精義，修訂廿六版，元照出版有限公司，2010 年 8 月，頁 767；盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 751。
398 其認為原始的危險仍係發生在製作行為上，提供行為僅是將該危險具體化而已。
399 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 212 以下。

成電腦程式發展的後退，故而採取「不法意圖說」，認為本罪所指的「專供」是指「意圖專供犯本章之罪」的意思，一方面限縮解釋可能造成的法律漏洞，另一方面亦使電腦程式免於過早被評價[400]。

最後，就「致生損害於公眾或他人」此一結果要件的妥適性的妥適性部分，有見解認為此項規定顯然將行為人犯罪的成立與否繫於他人是否使用其製作的犯罪電腦程式，同時反觀使用病毒而對電腦為侵入等行為本即有刑法第 358 條至第 361 條可規範，故可認為本條應係主要規定製作犯罪程式者，然立法者卻使用「不完全是對於製作電腦病毒行為之處罰」的構成要件作規制，將製作行為與使用行為混合規定在同一構成要件內作為一種行為類型，實不恰當[401]。同時，亦有論者認為此種實害犯的構成要件，會產生本條與本章其他各條幫助犯的競合問題，雖於本章大多數條文的解釋上不致出現問題，然於刑法第 358 條與本條的競合關係部分，若行為人製作一有害電腦程式，並提供與他人或自己用來入侵他人電腦時，若未造成公眾或他人損害，即無法與本罪相繩。然刑法第 358 條並無「致生損害於公眾或他人」此項構成要件，故若是提供自己入侵，則僅成立該條正犯，若提供他人入侵，則僅成立該條幫助犯。此時會出現「散布給他人」此一較嚴重的情形卻僅成立共犯，並獲得「得按正犯之刑減輕」法律效果的不公平狀態。故論者認為，在現階段即應注意在此時刑法第 30 條第二項的操作[402]。

---

[400] 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 106。然而，其批評李茂生氏「此說(「專供」係指意圖專供犯本章之罪的見解)本係學者所不採者，其理由基於解釋範圍寬廣而不符立法者「真意」。」的部分，由於李茂生氏所謂的「真意」，是立法者「想處罰卻礙於客觀規定過於狹隘而處罰不到」的真意，與林冠宏氏所解讀的「因為不想處罰範圍如此寬廣，但卻使用了如此寬廣的構成要件」截然不同；且於其批評「然，其於該文前述部分提及，程式在功能上並非「單一」；卻又在文後指出：「製作」與「『提』供」會使電腦程式輕微的危險性，足以確定構成要件的類型化危險性，求諸於製作行為所形成電腦程式本身的「客觀有害性」；一則，前後對於程式本身的工具性，以及製造行為本身是否即帶有客觀有害性，此一評價介入點十分奇特」的部分，蓋李茂生氏於呈現本段文字時的推論是從「無法利用第一個行為要素(製作)來界定「專供」的意義時，所嘗試使用第二個行為要素(提供)來界定」而來，其中並試圖以「或謂如果有「製作」與「『提』供」的行為，則縱或該電腦程式僅具有輕微的危險性，此際仍可藉此而確定構成要件該當行為的類型化危險性。」來作為其嘗試使用第二個行為要素來界定的正面論述，且最後的結論亦認為「構成要件行為所蘊含的類型化危險的定型仍舊是應該求諸於『製作行為』所形成的電腦程式本身的客觀有害性。」。從而，林冠宏氏對此為批評的部分，顯然是未充分理解李茂生氏的論述而導致的錯誤批評。

[401] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 128。

[402] 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁

值得附帶一提者是，對於第 360 條的加重部分，有見解認為電腦犯罪程式亦可能是專門針對公務機關電腦或相關設備犯之者，並參酌第 361 條的立法理由，認為應將本條置於第 361 條之前，以使本條有加重空間[403]。

第三項 遞續性上之困境

在雲端運算出現後，系統的安全性通常是交給雲端服務提供方來負責，此時即會產生是否處罰撰寫電腦病毒等惡意程式行為的問題。或謂雲端時代中講求 IT 資源共享，此即意味著若對於「他人」電腦系統施加病毒，該病毒很可能亦會作用到自己身上，並且雲端服務方對於系統安全性的保護，原則上應會比一般個人電腦強，撰寫病毒的行為實質上的「殺傷力」可能大幅降低，而認為此種行為不應以刑法處罰。然而惡意程式並不僅限於病毒程式，又縱使於雲端時代，不同使用者仍有不同使用的空間，在該個人使用的範圍內仍可能出現病毒，同時病毒程式所造成的惡害與雲端服務方對於系統安全保護的程度係屬二事，不能因為雲端服務方對於系統安全保護程度高，而否定行為的不法性，故似仍有必要處罰與惡意程式有關的行為。但是，就實務上的分析來看，通常使用惡意程式者皆較撰寫者為多，且使用者往往對於電腦安全性的危害更大，同時亦要考慮在雲端運算出現後，網路流通的方便性大增，使得此類惡意程式的取得更加容易。故規制的角度似乎應該考慮要擴張至對使用惡意程式者為處罰，甚至考慮變更處罰對象，以處罰使用者為原則，處罰製作者為例外。

第七節　告訴乃論─刑法第 363 條

第一項 實務上之運用情形

本條雖非電腦犯罪的行為態樣，然於實務上可謂是整個妨害電腦使用罪章中

215。

[403] 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 561。

最常運用到的一個條文，並且就實務上的運用情形，亦可以觀察出我國實務中對於電腦犯罪法條適用上的處理態度。我國實務上向來的電腦犯罪判決，僅有少部分的告訴人事後撤回告訴，致法院於該部分下不受理判決，多數案例的告訴人仍不願意撤回告訴[404]。然而，法院於該些告訴人未撤回告訴的案件所做的有罪判決中，所認定的刑度皆不高，多處於得以易科罰金的程度。此種現象顯示，縱法院認為此類案件大都為輕微案件，告訴人仍多不願撤回告訴。就以上觀察可以得知，立法理由中認為於罪章中設置告訴乃論的制度所具有「將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪」的功能，於實務的操作上顯然無法有效發揮，反倒是部分未該當非告訴乃論態樣的重大電腦犯罪，可能因被害人不願提出告訴而成為犯罪黑數[405]。

另外，本條僅規定第 358、359、360 條之罪須告訴乃論，然而於第 361 條對公務機關為第 358、359、360 條的行為時的加重處罰，是否須告訴乃論亦不失為一爭議，若根據立法理由似應認為是非告訴乃論[406]，而實務上雖素有爭議，然最高法院已於判決中明確表示本罪非屬告訴乃論[407]。

第二項 現今所受到之批評

本條於運用上最主要所遭受到的批評即是本條自身，亦即「立法者設定告訴乃論訴訟要件的理由」。從立法理由可以得知，本罪章規定告訴乃論的理由主要有二—在被害人無意配合偵查時，實際上難以達到偵查效果，以及為將國家資源集中於處理較嚴重之電腦犯罪[408]。然此二項理由多遭學者批評，有論者即認為是否能收偵查實效並非犯罪是否應設定告訴乃論的原因，且參照外國立法例，美國

---

[404] 就同樣是網路遊戲盜帳號的類型為例，雖有部分案件告訴人已撤回告訴，然亦有多數案件的告訴人不願撤回告訴，然而參考撤回告訴與未撤回告訴的犯罪手法以及未撤回告訴的情形法官的量刑輕重等，會發現二者幾乎如出一轍的是小型案件，由此可見將是否訴追的門檻交由被害人掌握，與將司法資源集中於重大案件的目的實現二者之間根本無正相關。參板橋地院九十九年度訴字第一八二一號判決、台北地院九十六年度簡字第一一六八號判決。

[405] 於我國早期以林山田為代表研究電腦犯罪的見解中，電腦犯罪的特色之一即是「高犯罪黑數」，參盧文祥，電腦犯罪之偵防實務，律師雜誌第 228 期，1998 年 9 月，頁 27。

[406] 中華民國刑法第 363 條立法理由第三點。

[407] 參最高法院九十七年度台非字第二八五號判決。

[408] 中華民國刑法第 363 條立法理由第二點。

及日本等國家於電腦犯罪部分皆無告訴乃論的規定，又於涉及第三人的情形[409]要判斷告訴權人實有困難，縱認相關人員均為被害人，亦可能會發生被害人不知被害而未告訴，等到發現被害事實而提出告訴時，相關證據已滅失導致偵查困難等問題[410]。另有學者從規定告訴乃論的角度做觀察，歸納出一般告訴乃論的規定，通常若不是因為追訴會增加被害人的痛苦，故基於尊重被害人意願的角度而設，即是因犯罪情況過於輕微，而不宜由國家直接發動追訴權之故。然而反觀本罪章的犯罪態樣以及法定刑，應可認為本章所規定的犯罪不僅有輕微的犯罪，進而推斷重點可能出在被害人的痛苦部分。然而論者舉出金融、商業電腦系統的問題，並認為作為「第一使用人」的金融業者基本上會因可能引起「第二使用人(客戶)」的恐慌而多不願提出告訴[411]，甚至還可能幫助掩飾被侵害的事實，私底下填補第二使用人的損害。故在此若以「金融機關提出告訴即會『非常痛苦』」為理由設置此規定，無疑扭曲告訴乃論的設置理由。但若將告訴權的行使重點置於第二使用人身上時[412]，在協助偵查的意義上即無效果，蓋如前述第二使用人本即可能不知道自己被侵害，要其協助偵查更加困難[413]。綜上所述，論者多主張將本條給廢除。

此外，關於刑法第 362 條與本條的關係部分，有論者認為若自刑法第 362 條是刑法第 358 條至第 360 條的實質預備犯角度出發，則刑法第 362 條亦應具有告訴乃論的性質，故若能說明第 358 條至第 360 條與第 362 條的差異，否則不應分別處理[414]。

第三項 遞續性上之困境

---

[409] 如線上遊戲的遊戲公司與玩家、金融業的金融業者與客戶等。

[410] 王銘勇，侵入電腦系統罪之研究，法令月刊第 55 卷第 3 期，2004 年，頁 267。

[411] 試想自己存錢的銀行或金融機構若發生系統被駭客入侵的案子，自己是否會對將財產置於該金融機構底下一事感到不信任。

[412] 論者有認為被害人是電腦的「使用權人」而非「所有人」者，參甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌第 50 期，2003 年 9 月，頁 185。

[413] 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 216-217。

[414] 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 108。

正如前述現今受到批評部分的論者所言，本條表現出整個妨害電腦使用罪章規制態度的曖昧，若謂刑法第 359 條的「取得」電磁紀錄是刑法第 323 條電磁紀錄部分的「還魂」條文，該條於修法前的竊取電磁紀錄罪亦屬非告訴乃論之罪，為何於當時的適用上並未出現立法理由中所述「對於個人電腦之侵害行為，態樣不一，輕重有別，如受害人無告訴意願，並配合偵查，實際上亦難達到偵查成效」以及「有助於紛爭解決及疏解訟源，並可將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查」等問題？同時，亦可從前述實務的運用情形以及現今所受批評部分觀察出，本條縱使設計了告訴乃論的條文，於偵查上不見得成效頗彰，同時亦無發揮將國家有限司法資源拿來偵察較嚴重的電腦犯罪的功用[415]。此外，在雲端運算出現後，「網路無國界」的現象更趨明顯，雲端主機的各個部位有可能散落在世界各地[416]，此意味著涉及跨國的犯罪亦會增加[417]，此時如果仍認為需要告訴乃論才能使行為人接受刑事規制，於實務上可以預見幾乎無法達到規制的效果[418]。從而，本罪章設計告訴乃論的規定，在未來雲端時代來臨後，很可能會成為本罪章各條文皆成為具文的元凶。

第八節　小結

就以上各罪的實務運用情形中稍加觀察，可以發現一個有趣的情形—實務上主要運用案例中，絕大多數的行為人不是沒有電腦專業知識，就是縱使具備電腦專業知識，卻在犯罪時並未運用。並且該些犯罪所造成的損害，有壓倒性的多數是對於「特定個人或企業」的損害，而少有涉及國家或社會的損害者。會造成此

---

[415] 除非認為立法理由中所謂「重大電腦犯罪」即是指案件數最多的「網路遊戲盜帳號」類型。

[416] 例如運算的機房在台灣，但儲存的機房卻在印度，或運算與儲存的機房同時存在台灣與印度，但使用者所使用的是台灣儲存機房內的硬碟以及印度運算機房內的處理器。

[417] 無論是此種將電腦網路作為客體的攻擊行為，亦或是利用電腦網路為傳統犯罪的行為，皆會有「跨國化」的現象，參渡邊卓也，電脳空間における刑事的規制，成文堂，2006 年 9 月，頁 1 以下。

[418] 有學者認為電腦犯罪所保護者為「使用空間的支配」法益，並認若侵害雲端電腦管理者的主機，並獲取該主機內大多數人個資的情形(並未對任何管理者以外任何人的使用空間為侵入)，僅會侵害該管理者的使用空間支配法益，但是這種主機管理者往往係外國人，則我國是否能期待該外國人於我國提出告訴，則是值得思考之處。參李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 77 以下。

種現象，有可能是因為該些行為依照法條構成要件容易成罪，又有造成「特定個人」的損害這個冠冕堂皇的理由，故即大量運用來「彰顯司法威信，打擊電腦犯罪」。又，在比較立法理由中所討論「欲防止的電腦犯罪類型」後也可以發現，立法者所預設的重大案件於實務上起訴者可謂寥寥無幾，同時從案件審判的刑度角度觀察，目前實務上所出現的案件中，法院所論處的刑度相較於該些案件所違犯法條的最高本刑而言皆非常低。此現象是否可以解讀成立法者預設的該些重大案件在台灣發生率極低或有一定發生率但是皆無法偵破，所以僅能抓小案件來「交差」不無疑義，但應可以認為本罪章在實際運用上可能無法有效規制立法者所預設的行為態樣，而且還可能導致將本無庸處罰的行為硬是要與該些罪名相繩。

再者，在我國學者以及實務工作者的眼裡，妨害電腦使用罪章的各條文規定可謂漏洞百出，除因創設新品種「涵蓋個人、社會、國家法益」的綜合型態保護法益，導致牽連過廣而使得規制態度曖昧外，從章節的編排到條文的設計、構成要件的設定以及訴訟要件的要求，皆與立法當時所欲達成的目標迴不相牟並且漏洞百出，使得該些條文中的多數構成要件皆不會在實務上有妥適運用的空間。除某些構成要件行為於實務上因為規範文義不明確而根本無法適用外，亦存在某些條文與罪章外的條文呈現競合現象的結果[419]，同時也因為其中某些條文的規定，使得案件縱使爭論到最高法院，審檢辯三方皆尚未對該犯罪的實體事實作判斷與釐清[420]。由此可見，本罪章在修訂後不僅是在實務的運用上，或是論理的探討上，都顯示出了相當的問題。

最後是本罪章從遞續性上的角度的觀察，由本罪章於構成要件中使用的詞彙以及規範的行為態樣皆可以發現，本罪章於立法當時所設定的處罰型態即是「以單機電腦為主，連線電腦與網際網路為輔」的規制模式，加上曖昧不明的保護法益，使得處罰範圍忽大忽小，雖有些條文因此會看似非常有「前瞻性」，連國外

[419] 參臺灣高等法院暨所屬法院九十一年法律座談會刑事類提案第一一號、台南地院九十二年度簡字第四六三號判決、板橋地院九十二年度簡字第一九三九號判決、
[420] 參最高法院九十七年度台非字第二八五號判決。

仍在猶豫的問題皆以明文規範處罰[421]，然而在探討立法過程以及立法理由與實務上的運用情形後，會發現此種具有「前瞻性」的條文只不過是瞎貓碰到死耗子而規定出來的結果，亦即僅有「條文規定本身」具有前瞻性，條文背後的理由以及實務的運作情形等仍顯示此類問題於我國還有一些討論的餘地。在雲端時代來臨後，社會對資訊科技的焦點已不如以往在單機電腦及連線電腦與網際網路間擺盪，而移轉至以網際網路為主，單機或連線電腦為輔的新體系。而面對網際網路的漸受重視，除可以據此認為以單機電腦規制為主要思考模式而訂立的妨害電腦使用罪章「過時」了，或不符合「遞續性」了之外，亦可以從中嗅出一點對於所謂「電腦犯罪」或「妨害電腦使用罪」規制態度的端續。究竟應如何面對我國對於此些行為的規制，是如德國般回歸至各傳統罪章論處，亦或是如美國般獨立於專章或以專法處罰，而構成要件以及條文編排應呈現什麼樣的圖像，則係接下來要討論的重點。

[421] 如刑法第 359 條對無故取得電磁紀錄的處罰等。

第五章　以法益為中心重新建構妨害電腦使用罪

在從立法過程、比較法、學理以及實務的角度探討完我國對於電腦犯罪規制的來龍去脈之後，於本章即是要展現出本文對電腦犯罪規制的態度，並且嘗試以此態度為電腦犯罪尋求一個妥適的規制方式，以達本文解決電腦犯罪規制遞續性問題，以因應時代變遷的最終目的。據此，於體系的編排上，本章分為「處罰電腦犯罪應設置專章」、「入罪化行為之篩選」、「建構電腦犯罪專章模型」以及「實務上問題之解決」四大部分。首先，於處罰電腦犯罪應設置專章的部分，會先探討應以何種方式與態度規制電腦犯罪較為妥適，而在得出要重新修法訂立專章結論後，即會產生如何劃分犯罪行為的問題。故接下來於入罪化行為之篩選部分，即會處理各種行為態樣的劃分，以及於構成要件的規制上要如何區分出犯罪行為，以與規制態度相呼應。建構電腦犯罪專章模型部分的工作，則是在確定各種行為態樣後，就整體電腦犯罪專章的顯現上做一個完整性的統整工作，並建構出一個規制模型，此時新的電腦犯罪專章雛型即已呈現。最後於實務上問題之解決部分，則係就新的電腦犯罪專章對於前述實務上發生的案例，以及雲端運算來臨後會產生的案例作適用，已收實用之效。

第一節　處罰電腦犯罪應設置專章

本節主要是對於電腦犯罪規制大方向的確立，亦即要以何種態度面對此種處於流動狀態、會以極快的速度以及無法預測的走向而「進化」的犯罪態樣，並就此一態度進而推導出，對此種犯罪態樣而言適當的規制模式究竟是要除罪化或是回歸至傳統刑法處理，抑或是仍以制定專章的方式為規制。從而，本節共要處理三個層次的問題：第一，先行論證對於已經來臨的「雲端運算時代」中，法律規範對此的因應態度，並導出若要將電腦犯罪設專章處罰，勢必要論證其特殊性的結論。第二，我國刑法目的之一為保護法益，若要論證電腦犯罪存在與傳統刑法中的保護對象與眾不同的特殊性，立證新興保護法益存在的方式應是一個足以將

討論聚焦，以及足以認定刑事制裁正當性的方法[422]。故在此部分的討論中，即集中在新型態保護法益的探尋，並確立處罰的核心基礎。第三，在確認電腦犯罪的保護法益後，則進而考慮是否可圍繞著保護法益對於以往產生問題的一些詮釋，如是否需定義何謂「電腦」以及如何定義，與是否應繼續使用「電腦犯罪」一詞來代表此類犯罪等問題。據此，就體系編排上，為符合本文思考的脈絡，故會依照前述三個層次的問題，依序分為三大部分於以下分別作探討。

第一項 面對資訊時代之應有態度

資訊科技日新月異，自 1970 年代的大型主機時代，到 1980 年代的個人電腦時代以及 1990 年代的網際網路時代，直到現今的雲端運算時代，只不過短短四五十年，然而在 1970 年代中，誰也沒料想到資訊科技會在四五十年後發展出雲端科技的運作體系，然而資訊科技就在大眾不知不覺下，以飛也似的速度正持續進步中。據此，我們可以知道資訊科技發展的特色，除難以推知發展以及難以掌握動向外，「進化」的速度還非常快。而單是資訊科技此種難以掌握動向的特性，本即會使法律界焦頭爛額的思考，若有心人士利用此類資訊科技的特色或優勢，對個人、社會或國家等造成負面的影響或傷害時該如何規制，再加上其飛快的進化速度，往往造成當法律界就單一使用關係總算費盡心思勾勒出規制體系後，另一種新的使用關係又悄悄「後浪推前浪」的取代了前一種使用關係變成了主流，從而造成了許多與電腦網路使用相關的法律，於增訂後即面臨必須要再思考修正或補充的殘酷情況。姑且不論身處英美法系代表大國的美國法中給予大量法官造法空間的特例，就國情以及立法過程都激似我國的日本，都在位於個人電腦時代的 1986 年刑法修正後，進而於所謂網際網路時代的 1999 年增訂不正連線禁止法[423]。同時，我國在民國 86 年(1997 年)增訂電磁紀錄文書化、動產化以及電腦詐欺罪後，也同時在民國 92 年(2003 年)增訂電腦犯罪專章。然而，仔細觀察後會發現，我國的兩次「增訂」時點明顯落後整個資訊科技發展的一個世代。據此，

[422] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 74 以下。

[423] 雖說是受到「國際」間的壓力而定，然而此種「國際」間的壓力究竟是從何而來，則應可以理解成是「世界大國」在極快速的時刻嗅到了資訊科技的推進，而「促使」法律層面亦要向資訊面跟進，以妥善保護該國的利益。

在參照我國的修法過程以及立法理由後，似乎可以認為我國對電腦犯罪的處理態度就是如同前述般已經對於資訊科技的變化多端感到束手無策，而在時代轉瞬而過後，才推出以前一個時代的思維與現處時代的「表徵」融合下的產物作為規制準則的典型[424]。

而要避免落入此種「修法→不適用→再修法→又不適用」的無盡迴圈中，首當其衝者即是要分析為何於現行法的所有規制中，唯獨在電腦犯罪的規制上會造成此種情形。固然一方面諸如前述是資訊科技發展的特性使然，然而在另一方面，法律界在面對社會現象時所採取的一貫態度亦是造成無盡迴圈的一大原因。有論者認為，台灣的法學教育有強調「詮釋法學」為基礎能力的傾向，導致面對資訊科技此種新社會現象時對應能力貧弱，一方面必須小心審理案件，以給與自己有更能了解該現象的機會，另一方面則矛盾的必須明確執法，以緩和新興社會現象與傳統秩序間的差距[425]。而此種貧弱的對應能力恰巧碰上了難以捉摸並且變遷快速的資訊科技，使得法律規制與科技變遷的差距越來越大。據此，對於此種變遷快速又難以捉摸走向的社會現象，一味的追隨其腳步做分析歸納後制定規範的規制態度顯然行不通且所制定的規範也許亦已不合時宜，在無法改變身為造成法律規制與科技變遷差距日漸增加的首要原因的資訊科技本質時[426]，要解決此種困境僅能從身為第二原因的法律界態度面下手。亦即必須重建法律人在面對資訊時代時所應有的規制態度，以順利拉近法律規制與科技變遷的差距。

至於何謂「法律人在面對資訊時代時所應有的規制態度」，有論者舉美國為例，在美國已有學者就對應態度(manners)作一番研究，並以歸納的方式整理出美國實務上對於以既有法律來面對資訊時代的新問題時的兩種處理態度—廣泛適用的定義性處理(broad/definitive approach)以及限縮範圍的臨時性處理

---

[424] 具體而言，我國正好在網際網路時代的末期，幾乎都快轉變至雲端時代的時間點上，提出了以前一世代單機電腦思維並配合當下(網際網路時代)表徵的「妨害電腦使用罪章」，雖然就研討過程以及立法理由都有提及甚至可以認為是重視「網路」犯罪，然而最後修正的法條中皆未提及「網路」二字，僅能依賴學者從「相關設備」部分推導而出。又縱使認為本法亦有處理到網路部分的問題，網際網路在該罪章中所佔地位仍遠遠不如立法者據以為思維的單機電腦。參李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 245 以下。

[425] 范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 27-28。

[426] 實際上，我們也無法想像要如何改變資訊科技那難以捉摸又變遷快速的本質。

(narrow/tentative approach)。詳言之，前者係以規範(rule)的建置來處理問題，意味著在之後對於類似案件的處理時，法院能有的判斷空間較小；而後者及偏向標準(standard)的建立，與前者不同的是，縱使建立了判斷標準，於之後的案件法院仍有相同的判斷空間[427]。同時，論者亦提出美國學者 Sunstein 的見解，認為法院在面對科技案件時，應採司法極簡主義(Judicial Minimalism)[428]，亦即僅在支持判斷結果的必要範圍內做處理，盡可能就其餘部分不加決定[429]，並進而主張我國對於面臨資訊時代快速變遷時所應有的規制態度為「面臨問題時優先採用限縮原則，例外採用規範原則」[430]。具體來說，該主張的中心思維認為，面對科技的變遷，法律人應盡可能的「不要干涉」，而在不過度干涉的前提下，尋求規制的可能性，故會得出首先於面臨問題時優先採用限縮原則的結論。但我國是大陸法系，法官於判斷上不如英美法系的法官有如此寬廣的空間，論者為解決此類問題，即提出我國判例制度[431]來做補充，認為若優先活用判例制度作事前處理，相較於事後發現問題所在而聲請釋憲來的有實益[432]。然而我國刑法受罪刑法定原則拘束，行為時若法律無明文規定處罰即不應處罰之，刑法第一條尚有明文[433]，並且我國是大陸法系國家已如前述，法官造法的空間有限，若無一全面性質的規範則執法者會失去論罪的依據，已不是僅依靠判例制度就有辦法解決的問題。從而，在此似應開始思考論者所謂的「例外」，亦即已設立規範的方式來全面性的對應此類情形。但縱使符合例外情形，論者亦主張必須在設立規範時思考下列數個要素：第一，該規範必須是針對資訊科技而為的立法；第二，該規範所處理的問題必須是具同質性(with common elements)的重複性問題；第三，該規範必須是屬於相似行為的一般性禁止，並無關權益歸屬或涉及利益權衡；第四，該規範於關係到

---

[427] Lee, supra note 18, at 1293. 轉引自范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 31 以下。

[428] 原文譯為「司法限縮主義」。

[429] 原文是「say no more than necessary to justify an outcome, and leave as much as possible undecided」參 Sunstein, Cass R., The Supreme Court 1995 Term-Foreword: Leaving Things Undecided, 110 HARV. L. Rev. 4,4-18(1996). 轉引自范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 32。

[430] 范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 32 以下。

[431] 此即是指我國實務上最高法院所做出的判例，會在實質上對於下級審法院為拘束的制度。

[432] 范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 35 以下。

[433] 林東茂，刑法綜覽，六版，一品文化出版社，2009 年 9 月，頁 1 之 82。

法規匯流[434]時，必須不會導致與舊有規範的無法融合，或甚至出現管轄範圍的外溢(extraterritorial spillover effects)；第五，規範必須不會因為資訊科技的快速變遷而受實質上的影響[435]。從以上五點考慮要素作分析，可以歸納出於面對資訊科技的規制時的一個思考方向—「跳脫資訊科技的快速變遷，並尋找與現實社會上的連結點」。若一味基於對新科技的恐懼以及社會的迫切需要而不斷的訂立新法，本即會導致該些新法在制定後立即因為資訊科技的再度變遷而失去沿遞存續的功能又面臨必須修正的問題，故此時應探求的是，對於資訊科技的發展，現實社會中人民所「害怕」的是什麼？而在找出人民所「害怕」的東西後，接下來的重點才是本著對於該「害怕」的東西做防制或避免而思考立法的問題。而將此種態度套用至刑法的規制上可以發現，刑法中所規範的各條條文，皆是對於人民所害怕的東西，亦即「具有社會損害性(破壞法益)的行為[436]」為保護而制定的規範，從而可以得知在找出「破壞法益的行為」之前，邏輯上必須先找出「法益(保護法益)」為何。同時在找出保護法益為何之後，對於規制的模式亦幾乎迎刃而解。若保護法益的結論是一新興法益，則基於保護法益的特殊性，此類犯罪必須獨立規制處罰，反之若保護法益的結論仍是傳統法益，則此類犯罪即必須回歸至既有傳統罪章中嘗試以補充規定的方式規制[437]。

就獨立規制究竟是如同日本一般以訂立附屬刑法的方式為之，抑或如我國妨害電腦使用罪章般置於刑法分則下的一個罪章處理較妥的問題，本文認為從附屬刑法的定義觀察，所謂附屬刑法，是指該規定本係以如民事、商事或行政等其他法律領域為主要規範，然而於其中的部分規定設有刑責，並將違反者視同犯罪人的法律而言[438]。而從日本的不正連線禁止法立法背景以及規定本身來看，可以發現該法的產生本即含有濃厚的行政法色彩，不但在提倡修法之時本僅是以行政法

---

[434] 所謂法規匯流，係指法律為跟隨科技的腳步而制定新規範的現象。
[435] 范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月，頁 33。
[436] 亦即「破壞人類和平共同生活」的行為，參林鈺雄，新刑法總則，三版，元照出版有限公司，2011 年 9 月，頁 9。
[437] 在此或許必須為了使討論聚焦而限縮討論的範圍，技術性的忽略法益論與規範論的爭執，以及我國刑法的規範目的應採法益保護說或規範維護說的問題。關於法益概念的流變以及與規範論的衝突，可參考許恒達，刑法法益概念的茁生與流變，月旦法學雜誌第 197 期，2011 年 10 月，頁 147 以下。
[438] 陳子平，刑法總論，二版，元照出版有限公司，2008 年 9 月，頁 6 以下。

的方式呈現,條文本身亦參雜了許多國家或都道府縣如宣導或加強安全控管等的協助義務[439],故日本將不正連線禁止法以附屬刑法的方式呈現實有其理由,而除非認我國政府與日本相同有在國家的指導下建立安全網路秩序的打算,並建構細緻的行政法規定並以之為構成要件解釋的前提,始有選擇以行政法的附屬刑法方式為規範的可能,否則在欠缺主體領域下的處罰規定,本應回歸至刑法分則內的獨立罪章作規範[440]。

綜合以上,在面對瞬息萬變的資訊科技,並在要加以規制的情形下,首當其衝要思考者即是保護法益的問題,從而以下的討論會聚焦於電腦犯罪的保護法益的探尋,試圖來為電腦犯罪的何去何從找到一條通往解決大道上的路標。

第二項 電腦犯罪之保護法益

第一款 實務見解

實務上在民國 92 年修法過後至今,對於電腦犯罪的保護法益可以說是眾說紛紜[441]。就侵入電腦行為(刑法第 358 條)的保護法益,有認為是屬「社會大眾」對登入機制安全性之信賴[442]、「被害人」登入控制機制之信賴[443]或電腦系統的登入控制機制[444]此種「信賴」類者,有認為是屬資訊安全[445]、電腦使用安全[446]或系統安全[447]的「安全」類者,有認為是屬密碼管理正確性[448]、電子信箱管理正確性

---

439 不正アクセス対策法制委員会,不正アクセス行為の禁止等に関する法律,立花書房,2008 年 10 月,頁 9 以下。

440 黃榮堅,基礎刑法學(上),三版,元照出版有限公司,2006 年 9 月,頁 11,註 8 處。

441 以下關於保護法益的整理,主要參考自妨害電腦使用的法益思考,行政院國家科學委員會專題研究計畫成果報告,計畫編號:NSC 98-2410-H-004-124-,計畫主持人:李聖傑,並對於民國九十九年後較新的實務見解作追加補充。

442 九十四年少年法院(庭)庭長法官業務研討會法律問題提案第二十號。

443 高雄地院九十八年度審簡字第一七一七號判決。

444 台北地院九十四年度易字第一五九〇號判決。

445 高等法院高雄分院九十五年度上易字第八七二號判決。

446 南投地院九十三年度簡字第一六一九號判決。

447 板橋地院九十四年度簡字第一六三號判決。

448 高等法院高雄分院九十五年度上訴字第一五八九號判決。

[449]、電子商務管理正確性[450]或線上遊戲合法運作管理正確性[451]的「管理正確性」類者，亦有認為是屬個人祕密[452]或商業秘密[453]的「秘密」類者。而實務上較早期的見解，多認為侵入行為的保護對象是準私文書或準動產[454]。

而就取得、刪除、變更電磁紀錄行為(刑法第 359 條)的保護法益的意見分歧更是五花八門，有認為是智慧財產權的保護[455]，有認為是屬網路遊戲秩序[456]、網路遊戲管理[457]、電子財產秩序[458]此種「秩序本身」，有認為是屬線上遊戲管理正確性[459]、電磁紀錄管理正確性[460]、資訊管理正確性[461]、客戶資料管理正確性[462]、帳號資料管理正確性[463]等「管理正確性」類，有認為是屬電腦系統安全性之信賴[464]或電磁紀錄管理之安全信賴性及機密性[465]的「信賴」類，有認為是屬被害人的商譽[466]、信用[467]、商業競爭能力[468]一類，亦有認為是屬被害人的隱私[469]、客戶資料管理隱密性[470]、資料私密性[471]等「隱私權」相關一類。與侵入行為相同，早期

---

[449] 台中地院九十八年度易字第一〇〇五號判決。
[450] 高雄地院一〇〇年度審訴字第九五九號判決。
[451] 台中地院九十九年度訴字第一四四號判決。
[452] 高等法院高雄分院九十五年度上訴字第一五八九號判決。
[453] 高等法院九十七年度上易字第一三一〇號判決、台北地院九十六年度訴字第一三〇五號判決。
[454] 連江地院九十三年度訴字第四號判決、台北地院九十二年度訴字第一一〇八號判決等多數。
[455] 智慧財產法院九十七年度刑智上訴字第四十八號判決、智慧財產法院九十八年度刑智上訴字第一號判決、智慧財產法院九十八年度刑智上訴字第十一號判決。
[456] 高雄地院九十三年度簡字第五四七號判決。
[457] 高雄地院九十六年度簡字第三八七二號判決。
[458] 南投地院九十五年度訴字第八〇一號判決。
[459] 花蓮地院九十二年度花簡字第一七一號判決。
[460] 台北地院九十六年度訴字第八八一號判決、台北地院九十三年度訴字第三二六號判決等多數。
[461] 宜蘭地院九十六年度訴字第二四號判決。
[462] 金門地院九十六年度簡上字第一號判決、士林地院九十九年度訴字第一二二號判決、南投地院九十九年度訴字第七三號判決。
[463] 台北地院九十六年度訴字第六四〇號判決。
[464] 台北地院九十四年度易字第一五九〇號判決。
[465] 台北地院九十六年度訴字第五七八號判決。
[466] 高雄地院九十四年度訴字第一四七號判決。
[467] 高等法院九十八年度上訴字第三二四六號判決。
[468] 桃園地院九十六年度訴字第一二九〇號判決。
[469] 台北地院九十六年度訴字第五七八號判決。
[470] 台中地院九十五年度易字第一四三七號判決。
[471] 雲林地院九十四年度訴字第七八八號判決。

實務見解亦多認為此類行為的保護對象是準動產[472]。

就干擾電腦行為(刑法第 360 條)的保護法益，由於案例不多的緣故，實務見解在保護法益的部分意見相對集中，僅大體上分為二種見解，一種認為是電腦記錄處理效能[473]或電腦處理運算資訊功能[474]等「效能」類，另一種認為是電腦與網路正常運作[475]或電腦連線機能正常運作[476]等「運作正常」類。

就侵害公務機關電腦行為(刑法第 361 條)的保護法益部份，實務上多認為係屬公務機關對於電磁紀錄管理正確性等「管理正確性」類[477]，僅有少數見解認為是公務機關人員對於電腦系統安全性之信賴的「信賴」類[478]，或政府機關資訊安全等「安全」類[479]，以及遭洩漏者的個人隱私權等「隱私」類[480]。

就製作並散布犯罪電腦程式(刑法第 362 條)的保護法益部分，由於實務上案例本即不多，有提及保護法益的案例更少，大多數見解皆認為係屬被害人檔案資料管理一類[481]。

而就此些判決所呈現的保護法益態樣做整理及分析，會發現乍看之下無法將各種行為態樣的所有保護法益闡釋(具體的保護法益呈現)歸納至一個更上位的概念(罪章的保護法益)下，但若參考前述本罪章的立法過程以及立法理由可以發現，此些概念都可以歸納在立法者所創造的「電腦使用的安全」此一「包含國家、社會、個人法益」的新興法益之下。更精確的說，就是因為立法者(幾乎也可以說是實務界本身)在立法時所闡述的法益概念涵蓋面向非常廣泛，在實務上幾乎只

---

472 台北地院九十五年度訴字第八四七號判決、台北地院九十四年度易字第九一九號判決等多數。
473 南投地院九十四年度簡字第七四七號判決。
474 台北地院九十四年度易字第四八五號判決。
475 台中地院九十七年度訴字第一四九四號判決。
476 台北地院九十四年度訴字第一五一四號判決。
477 高雄地院九十四年度訴字第一七一四號判決、台中地院九十八年度易字第一〇〇五號判決、台北地院九十六年度訴字第五七八號判決、高等法院九十九年度上訴字第三七〇六號判決。
478 台北地院九十四年度易字第一五九〇號判決、高等法院九十四年度上訴字第七六五號判決。
479 高雄地院九十三年度易字第一三〇五號判決。
480 台北地院九十三年度訴字第一一五七號判決。
481 高雄地院九十三年度易字第一八八二號判決、高等法院台中分院九十八年度上更(一)字第三五號判決。

要稍微提出一個相對有說服力的法益概念，即可以將任何看似與構成要件該當的行為入罪化[482]。在歸納出此結論的同時，除顯示出了電腦使用安全這種被立法者所創設的新興法益其內涵的空洞性外，還可以顯示出實務工作者對於行為的入罪化以及處罰基礎並不是因為行為人「侵害保護法益」，反而較類似於德國學者賓丁(Karl Binding)所提出的規範理論(Normentheorie)概念，是因為行為人對於(刑法)規範的「不服順(Ungehorsam)」[483]。從而在此概念下，法益僅是規範的「客體」，故邏輯上在任何刑法規範中，都可以找的到法益概念。換句話說，此種法益概念的選擇以及決定，即委由創設規範的立法者決定。然而，此種「法益」概念，充其量僅能說是「法條益(Gesetzesgut)」而已，與刑法所保護的法益概念內容仍有差距[484]。並且，姑且不論賓丁所提出的規範論是否即是其本意，有論者認為在法治國體制下的刑法，若本身僅是為了保護體制而忽略人的存在，將會違反憲法對於基本權保障的基本精神[485]。據此，我們可以認為就實務見解中所提出的「法益」概念部分，或許就制裁規範層面有參考的價值，然事實上在行為規範層面的討論上，是較不具參考價值的。

第二款 學說見解

在學說見解部分，由於本罪章立法過程中並未使多數學者參與立法，並且立法者在條文構成要件的內容以及行為的入罪化選擇中，亦僅是將與電腦有關的犯罪行為態樣去除以傳統刑法即可解決的「以電腦作為犯罪工具或平台」一部分行為態樣後全部置於該罪章內處罰的緣故，於法律施行後，未在立法過程中參與的學者們一方面本於法學研究的嚴謹態度，必須釐清各罪章的行為態樣並對於立法整體的草率態度採取批判；但另一方面又要設法維護立法者根本的尊嚴以及建立

[482] 事實上，綜合本文前述對實務界的分析整理部分，亦可以看出本罪章各罪的構成要件本身即含有不少問題，其中亦不乏「缺乏明確性」此一與罪刑法定原則相左的瑕疵，然而就立法過程以及立法理由觀察，立法者於立法當初所要表達的處罰態度似與現行條文的實際適用有些出入。故在此本文使用「看似與構成要件相當」來表現構成要件的不明確以及處罰態度與實際扞格的現象。

[483] Binding, Normen I, S. 185.，轉引自陳志龍，法益與刑事立法，自版，1990 年，頁 11。

[484] 陳志龍，法益與刑事立法，自版，1990 年，頁 127 以下。

[485] 鍾宏彬，法益理論的憲法基礎，初版，公益信託春風煦日學術基金， 2012 年 4 月，頁 194-195。關於對賓丁所提出的規範論的細部解讀可參照同書第 236 頁以下。

人民以及執法者對於新法適用上的信心，以使耗費大量社會資源而訂立的新法能順利在社會上發揮效果，故亦出現眾說紛紜的現象[486]。然而，雖說學說上對於電腦犯罪的保護法益眾說紛紜，但仍可以就大方向上作幾個不同出發點的區分。故而本文將學說見解就論者所採取的解釋態度分為四大類，於以下作較詳細的論述。

一、　不具獨立保護法益

主張不具獨立保護法益的學者，通常對法務部的修法抱有疑義且大力批判，多認為電腦犯罪專章所保護的法益，其實根本與刑法其他罪章無異。至於特定侵害行為所侵害的法益為何，則應視該侵害行為的態樣決定。在現時提倡此主張的論者中最具代表性者認為，電腦犯罪的「新花樣」，並非該些犯罪所侵害的法益，而是使用電腦或網路來竊盜、侵占、恐嚇、偽造文書、甚至致人於死的犯罪手法[487]。其進而解釋立法者訂立專章的理由或許在於現行刑法的理論架構是建立於十九世紀快速進步之物理學研究成果上，惟現今資訊爆炸，儼然已進入一個「數位」的時代，使得「物理的刑法」似乎對於社會欠缺了「適應力」或「理解力」，因而導出有立法規制的必要。然而其亦從並非所有電腦犯罪都不得以現今刑法直接適用[488]，以及電腦犯罪僅是「手段」電腦的方向做觀察，認為要使「物理的刑法」獲得適應力，並非將該些行為獨立作立法，而是應著眼於有些物理性的行為難以套用轉化至數位刑法。畢竟讓立法者所困擾的並不是電腦犯罪本身，而是含有物理性構成要件要素用語的構成要件[489]。若能成功的將「物理性的」構成要件要素用語轉換成「物理–數位雙棲性的」，「物理的刑法」即亦將成功轉型為「物理的–數位的」刑法，以解決電腦犯罪造成刑法無法適用的問題[490]。亦有論者持類似見

---

[486] 除有學者盡力「幫忙」立法者尋找罪章的保護法益之餘，亦有學者好意為立法者開啟一道台階，使立法者發覺應將該些規範回歸至傳統犯罪時也能有所依據。參李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 243 以下；李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 79。

[487] 鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 104-105。

[488] 如以 E-MAIL 教唆殺人，一樣可以殺人罪之教唆犯處罰之。

[489] 例如刑法第 320 條第一項的「動產」以及刑法第 210 條的「文書」等。

[490] 鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁

解認為，電腦犯罪專章所保護的法益，雖其中某些罪亦有輔以保護傳統的社會法益，主要仍於傳統個人法益範疇之下。然同前述論者般，電腦犯罪專章所保護的法益並無「新意」，亦即並無超脫現行刑法保護之個人法益的各種法益。於第 358 條部分，其認為仍是在保護使用人對電腦內部訊息的隱私利益；於第 359 條部分，其認為保護者為隱私利益以及財物支配等利益；於第 360 條部分，其認為所保護者類似刑法第 304 條「他人行使權利」的利益。又，其認為第 361 條是一加重性質的處罰；第 362 條係一預備犯或幫助犯的加重處罰明文化[491]。

此類見解較類似於前述德國對於電腦犯罪的規制所採取的處理態度，畢竟如論者駁斥批評使用「電腦犯罪」一詞會混淆視聽者的一段話：「電腦犯罪仍是人在犯罪，並非電腦本身會犯罪[492]」一般，電腦僅是行為人利用的工具，跟電話、手槍或螺絲起子並無不同。而對於妨害電腦使用罪章的制定，論者多認為從我國於民國 86 年亦曾經對電腦犯罪有類似的增訂看來，我國的規制態度應本是如同德國般，從傳統罪章的構成要件下手作修正，然而立法者卻未經思考，將本已增訂的部分條文刪除，另行制定妨害電腦使用罪章。如此立法簡直「欠缺刑事立法的整體性規劃」，不但不依循前例，還進而破壞立法體例，造成刑法規制上的謬誤，是一個極其失敗的立法[493]。而對現況能想的到的解套方式似乎只有將該罪章廢除，重新修正傳統刑法一途[494]。

二、 涵蓋個人、社會、國家法益的集合體

此類見解本文於以下簡稱「修法派」，因其並未對電腦犯罪的保護法益一事做較深入性的思考，反而是認為「法律本有隨社會變遷的動能」，進而認為既然社會上對於電腦犯罪的防制有迫切的渴求，則法律為回應社會的需要，對於電腦犯罪亦顯示出了其規制態度，則不妨放下既有的分類標準，思考新的法益概念來

105-106。

[491] 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 97 以下。

[492] 林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年，頁 2。

[493] 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 549-550。

[494] 鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 115。

詮釋此種社會現象[495]。亦即改變固有保護法益的概念，來接受「電腦使用的安全」此一橫跨國家、社會、個人法益界限的初生巨嬰。故而在保護法益的認定上，誠如採取此類見解的論者所言：「在節制電腦使用安全與秩序的要求下，似乎宜對於法律所保護的法益，重新思考，不應依個人法益或是社會安全法益的分類方式作為規範保護的指標，而應對於新制定的新興犯罪類型，思考新的保護法益概念，否則將陷入新制度舊思維的謬誤[496]。」一般，修法派學者幾乎完全接納修法理由的意見，並認為電腦犯罪的保護法益為「電腦使用的安全」，並有認為此種保護法益屬於「競合性或重疊性法益」，除在保護社會大眾資訊安全外，並兼及個人秘密及財產安全的見解。並且在專章內各罪具體保護法益的闡釋中，該論者一致認為該罪章所有犯罪類型的保護法益具體闡釋皆無二致，皆是「社會大眾資訊安全及個人秘密及財產安全」[497]。

簡言之，此類見解有如前述實務見解般較偏向規範論者的思考邏輯，然而法益概念之所以會產生，本即帶有「基於刑法的謙抑性而限縮行為入罪化範圍」的思維[498]，若反而依照社會上的需要，在未思考該些「利益」是否可以轉變，或是否需要轉變為新的「保護法益」以及如何轉變等問題時，即一概因為所造成行為的損害甚鉅以及社會上對於電腦使用安全規制的迫切需要而逕以「法律隨社會變動」的理由認為其屬於一新興法益[499]，除在邏輯思考上本末倒置外，很可能因此造成刑法體系枝節旁生，進而因為大量重複處罰使得整部刑法肥大化，產生體系紊亂的問題。更有可能因為將行為大量入罪化，使得刑法的處罰範圍大量擴張，淪為僅為實現刑事政策的工具[500]。而實務界完全不在意保護法益的作法固有其技術上的壓力以及理由，而對於刑法謙抑性的嚴格把關似應是學術界的工作，如在

---

[495] 徐振雄，網路犯罪與刑法「妨害電腦使用罪章」中的法律語詞及相關議題探討，國會月刊第 38 卷第 1 期，2010 年 1 月，頁 62-63。

[496] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 129。

[497] 甘添貴，體系刑法各論，修訂再版，2004 年 2 月，頁 539 以下。並且其將社會大眾資訊安全與個人秘密財產安全就「危險性」作排序，認為應以前者為「主要保護法益」，而後者為「次要保護法益」。

[498] 許恒達，刑法法益概念的茁生與流變，月旦法學雜誌第 197 期，2011 年 10 月，頁 139 以下。

[499] 事實上有如前述實務保護法益部分，此種「法益」根本僅是「法條益」而已。

[500] 有論者有使用「過剩的刑事規制」來描述此種「刑法違反謙抑性」的入罪規制，參李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 173 以下。

此竟與實務界採相同的規制態度，無疑是造成我國規制體系紊亂的元兇。

三、　以集體(社會)法益為保護

此類見解多是基於憲法賦予人民的「溝通權」延伸思考而來，認為電腦網路，特別是網路是人類使用來溝通的工具，而為保護溝通的順暢，所以需要對於電腦的使用方式作規制[501]。然而依照細部見解以及思考流程的不同，亦可以分成兩大類的見解—保護資訊處理程序的安全以及社會上對於網路安全的信賴。

主張電腦犯罪的保護法益是保護「資訊處理程序的安全」者，主要是著眼於溝通權的直接發展，而從「電腦最重要的功能在於處理資訊」作思考的出發點。電腦在現代社會所扮演的角色即為一個資訊通路的起點與終點[502]，而此種資訊通路的安全就如同交通安全般，只是現代人的溝通不一定要親自出門，僅要傳送資訊即可。而為了維持人與人溝通的順暢，則必須保障此種資訊處理的安全性[503]。更有論者將此思維更加深入的探討，認為電腦的資訊處理即是溝通順暢的基石，而在資訊處理的保護中，無論該電腦是否具有溝通性質，亦即無論單機電腦或連線電腦，只要電腦具備有資訊處理的性質，則應該保障「資訊處理程序的安全」。雖此種資料處理的「目的」，很可能是涉及國家社會或個人法益，且對於資料處理的過程作保護，最終對於資訊處理目的所涉及的各項法益亦間接的保護到，然而「資料處理的目的」與「資料處理的過程(程序)」係屬二事，不能混為一談。對於資料處理程序的安全，論者認為其本身也是一個實體的利益，並以「正當法律程序」原則作比喻，謂正當法律程序本身即是為了落實基本權，但發展至現在，其本身亦變成一個被主張的「實體權」。故雖說資料處理程序的安全相對其他實體權利而言是程序性質，其本身亦為一實體法益[504]。然其卻因資料處理程序的安全是衍生自個人使用資訊處理工具為由，將其性質歸類於個人法益下，而後又以交通安全為喻，認為若個人資料處理程序安全能確保，則人與人往來間的資料處

---

501 參第十四屆政大刑法週會議紀錄，2007 年 3 月，頁 20-22，許玉秀教授與李茂生教授的發言。

502 實則在此可以從網格運算中得出一點靈感，將「起點與終點」簡稱為「網點」。

503 第十四屆政大刑法週會議紀錄，2007 年 3 月，頁 20-21，許玉秀教授的發言。

504 陳憲政，電腦犯罪之法律適用與立法政策–保護法益之遞嬗–，國立政治大學法律學研究所碩士論文，2006 年 12 月，頁 57-58。

理安全也可以獲得保障，故資料處理程序的安全亦屬集體(社會)法益[505]。在此本文以為論者似有誤解，若同樣以交通安全為比喻，保障個人的交通安全，是為了維持整體交通秩序，然並不代表交通安全此一法益即是「既屬個人法益，又屬集體(社會)法益」的「競合或重疊性法益」。若著眼於資料處理程序是人與人往來的基石，則資料處理程序的安全法益應屬集體(社會)法益為是。

而主張電腦犯罪的保護法益為「社會上對於網路安全的信賴法益」者，是著眼於電腦網路，或直接指明是「網路」本身在人類社會所建立起一個「溝通制度」的地位為出發點來思考。雖論者在修法後技巧性的從罪章條文中的「致生損害於公眾或他人」構成要件作體系解釋而得出應創設一個「信賴關係」令其使用，而能想的到的信賴關係僅有「社會上對於網路安全的信賴法益」的結論[506]，然而此種推論畢竟是本著為修法者補破網的心態而出發所作的論述。若要論證電腦犯罪的保護法益，必須從論者於前述對於電腦犯罪的分類加以說明，論者認為法益保障的規制，若依照時間的流動來觀察，亦可以整理成陰謀、預備、著手、既遂等階段，在各個階段中，對於規制的要求會越趨嚴格，同時在越重要的法益的保護中，保護的時點會越前置。從而在隨著時間的流動，空間型規制的複製不會完整的複製，而會隨著時間的發展適當限縮，故亦會產生一個圓錐型的圖像。論者認為此種圓錐型圖像與電腦犯罪分類圓錐型圖像的結構應屬相同，且於將二圓錐重合後，會得出一個結論：「原則上只有對於貫穿到圓錐底部的不適切行為，始有迫切的犯罪化需要」[507]。論者並進而闡述，以文書保護為例，若某項財產法益有表彰其存在或價值的文書存在，而該文書是一個可以被侵犯的客體時，對於財產法益的圓錐上，文書被侵犯的時點應會存在於圓錐的中心點上，此時若立法者特別重視對文書的保護，則很有可能會額外創設一新法益保障文書，而會在舊有圓錐體的中間點產生一個新的圓錐體[508]。而就電腦犯罪的情形，有論者即依上述邏

---

[505] 陳憲政，電腦犯罪之法律適用與立法政策–保護法益之遞嬗–，國立政治大學法律學研究所碩士論文，2006 年 12 月，頁 58。

[506] 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 244。

[507] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 187 以下。

[508] 李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988 年 5 月，頁 187。

輯試導出電腦犯罪的保護法益，認為若社會上的某種秩序遭到破壞時，進而會導致社會大眾的恐慌，則該秩序即應由刑法保護。如同前述的文書制度以及政府所宣導「網路即馬路」一詞所表彰的交通制度一般，在網際網路的使用上亦會出現一個「安心使用網路」的秩序，以及附麗於其上的「社會上對於安心使用網路空間的信賴感」此一集體(社會)法益，此即為電腦犯罪所要保護的法益[509]。同時，論者並就我國社會上對於網路空間的使用是否呈現一種秩序，以及民眾是否對其產生信賴感，且該信賴感是否夠穩固以至於作為保護法益看待等問題作了一番探討，最後仍認為我國此一社會法益仍存在，並且有日益壯大的可能，然現行情形此一社會法益看似仍不足以用刑法加以保護，若仍要以刑法加以保護的情況下，則刑度應全面性的降低，以不違反刑法謙抑性原則[510]。此外，亦有學者從交易制度來例證相同的結論，認為因社會的複雜化，本來從以物易物的交易制度已不足以滿足人類日趨複雜的交易結構，從而建立了貨幣制度，此後在資訊化社會下，傳統的貨幣交易制度亦不足以滿足人類的交易結構時，又會有新制度的建立，即是利用電腦網路而生的「電子化付款機制」，從而如同對於貨幣制度的信賴般，對於電子交易制度的信賴亦是必須要保護的人際關係制度，並考量到社會成員對於電腦與網路系統有高度信賴，並且電腦系統從不是單一個體獨立享有的私人利益，而是由特定的網路社群共同享有等因素[511]，認為應將社會對於網路安全的信賴此一社會法益作為電腦犯罪的保護法益。

最後，學者亦對於現行妨害電腦使用罪的重刑化部分呼籲，假使本來就僅是一個圓錐的情形，原則上越上層的處罰即應該越輕微，若行為已經達到最底層的情形，則應利用法條競合的吸收關係直接處罰最底層的行為。但於新圓錐的情形，吸收關係即會在新圓錐的底部造成中斷，假使要在新圓錐的底部設立一個更嚴重的規制(指刑度很重的電腦犯罪)時，對於越往圓錐頂端的部分即應為更嚴格的審

---

509 吳文君，妨害電腦使用犯罪行法規制之分析–以保護法益為中心，國立台灣大學法律學院法律學系碩士論文，2010 年 6 月，頁 67 以下。

510 吳文君，妨害電腦使用犯罪行法規制之分析–以保護法益為中心，國立台灣大學法律學院法律學系碩士論文，2010 年 6 月，頁 86 以下。

511 許恒達，資訊安全的社會信賴與刑法第三五九條的保護法益–評士林地方法院九十九年度訴字第一二二號判決，月旦法學雜誌第 198 期，2011 年 11 月，頁 241-242；同樣概念的運用另可參照許恒達，洩露使用電腦知悉秘密罪的保護射程－－評臺中高分院九十八年度上訴字第一三一九號刑事判決，月旦法學雜誌第 190 期，2011 年 3 月，頁 202。

查[512]。

四、　以個人法益為保護

採取此類見解的論者認為，對於電腦犯罪主要應該考量者，不是行為人阻礙了「電腦」此一科技產物的使用利益，而是經由電腦特性所表現的使用利益以外的保護法益[513]。使用電腦行為本身是一連串動作流程，除使用目的不同外，不同的行為階段中亦可能被分析出不同的使用利益。而依照前述學者所提出的圓錐型法益規制模型以及行為類型模型中，亦可以觀察出對於不同階段使用利益的判斷。若圓錐頂端是到達底部的不變條件，則只要例證圓錐頂端的使用利益有保護的必要，則從此種必要條件出發的後續行為，則皆有保護必要，並且可依照利益侵害的不同發展成各種行為類型。而就圓錐頂端的利益，亦即電腦犯罪的保護法益部分，論者從空間的概念出發，認為空間的概念雖於早期是一靜止、絕對的狀態，被表現為像是充滿許多客體的容器，並可以用長、寬、高來測量，惟今日空間概念已轉趨為動態、關係的理解，認為空間是客體之間發展出相互關係的結果[514]。而由於科技的發達，經由電腦的普遍使用，於人類間漸出現了一個「關係概念」的支配空間，對此空間無法以傳統之長、寬、高的容器形象來理解，應以空間中客體的互動關係來理解，亦即人類把對於傳統空間的概念經驗，延續到使用電腦的經驗。並以家族相似性的哲學概念為基礎，例證刑法電腦犯罪專章的法益應有理解為獨立新法益的可能[515]。以刑法第 358 條的保護法益為例，如同刑法第 306 條的保護法益是住居的安寧一般，住居的安寧只不過是另一種形式的安心領域呈現，於電腦的使用中，人們仍對於使用電腦的空間亦產生同樣安心領域的期待，不論是資訊擁有、隱私甚或財產利益。而第 358 條所述者為電腦犯罪的原型，之後可能發展出各種不同的類型，雖各種類型可能侵害該罪所輔助保護的其他法益，

---

[512] 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月，頁 190。

[513] 李聖傑，開啟電子門鎖算什麼？，月旦法學教室，2011 年 4 月，頁 25。

[514] Martin Dodge、Rob Kitchin 著、江淑琳譯，網際空間之圖像，2005 年 1 月，頁 53。轉引自李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 78。

[515] 李聖傑，「家族相似性」探尋刑法典範之應用–以法益為核心，刑事法學的新視野，元照出版有限公司，2011 年 5 月，頁 149 以下。

惟至少對於使用空間的安全皆有所侵害。從而認為依照現行法，電腦犯罪專章所保護的法益則是「使用空間的支配性」[516]。

然而採此見解的學者在最後的結論上，仍未一律揚棄如同前述德國立法例的處理方式般將電腦犯罪的規制直接以使用利益作為基礎的分類思考，並結合既有的傳統刑法罪章的結構規制方式的可能性，反倒是認為在立法者給予立法的空間時，應採取較傾向於德國立法例的處理方式為當[517]。

第三款 本文見解

對於以上四種學說見解，首先就修法派見解的部分，修法派見解會造成我國刑法體制崩毀，而導致濫刑化的結果已如前述，並從比較法的角度來看，連與我國處境類似的日本，在保護法益的闡釋上亦沒有如此「先進」的見解，且對於電腦犯罪的問題，其仍有試圖找出「社會上對於網路使用安全的信賴」此一社會法益，並未如修法派見解般直接棄守法益理論，而試圖為保護電腦犯罪的某項利益反過來質疑法益的區分方式，故本文在思考電腦犯罪保護法益的最初，即排除採取修法派見解的可能性。

而對於認為不具獨立保護法益的見解(下稱第一種見解)對於最後兩種見解的最大質疑，即是「虛擬空間只不過是現實空間的延伸」，例如在電腦裡面『偷走』電磁紀錄跟在現實社會上偷東西應該要相同以竊盜罪處理，僅是構成要件規範用語的不同而已[518]。後兩種見解皆是著眼於對電腦系統侵害的階段(手段)的規制，而對於該手段或許能找出各種不同的理由來架構規制的圖像，然而對於傳統法益的保護仍然未置一詞，並依照其邏輯會得出「處罰在網路遊戲上竊取他人的虛擬寶物的行為，是因為行為人『破壞了被害人使用空間的支配』或『破壞了社會上對於網路使用安全的信賴』，而非因為行為人『竊取了被害人的東西』。」的結論，反面而言，持此類見解的人即會認為「只有在現實社會上的『偷』，才有以刑法

[516] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 78-79。
[517] 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 79。
[518] 鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 106。

處罰其行為的必要；而在虛擬空間中的『偷』則不會處罰其『偷』的行為，而是透過其他角度來評價該行為為犯罪。」，然而此種結論似乎不合邏輯。故認為電腦犯罪的保護法益是傳統法益以外的新法益者，僅是逃避問題而非解決問題。

此種批評看似有理，且命中了後兩說見解的心臟，然而在仔細思考後會發現，此種批評其實是一種誤解。首先，就電磁紀錄的財產性問題，於民國 86 年修正時即將電磁紀錄動產化，然而在動產化後即會在「竊盜」的規制出現問題，故於民國 92 年將刑法第 323 條部分刪除。所謂「竊盜」，係指破壞他人對物(電磁紀錄)的支配管領，而建立自己對物(電磁紀錄)的支配管領而言[519]，然而就電磁紀錄的「竊取(剪下貼上)[520]」行為做觀察，此種「竊取」行為卻是先將同樣的資料進行複製後，再將原本的資料刪除的行為，此即電磁紀錄的「可複製性」[521]。若要以現實社會上的行為來比擬，最類似者應是「甲將乙桌上的文件以完全模仿該文件筆跡的方式照抄於一份與記載該文件的紙張相同品質的紙上，並在抄寫完成，得出一個外觀上一模一樣的文件後，將原文件銷毀」的行為。而此種行為雖然在結論上也得到了「一消一長」的結果，但在現行刑法上並不會被評價為竊盜，反倒是在足以生損害於公眾或他人的情形下會成立偽造文書罪以及毀損罪[522]。就此類行為，社會上的評價描述與法律上的評價描述本即有落差，社會上會認為「行為人把我的文件(電磁紀錄)給偷走了」，是因外見上以及結論上似乎是一個「行為人動手腳，最後結果是一消一長」的關係，而此項關係與竊盜罪具有很高的相似性，但是就該行為的分析上，反而較類似於偽造文書[523]以及毀損。故僅從外見結論上的一消一長情形以及社會上的用語，即論證此類行為應屬竊盜，而反過來質疑相同事件為何不相同處理，此種思考脈絡似乎稍嫌率斷。

---

519 林東茂，刑法綜覽，六版，一品文化出版社，2009 年 9 月，頁 2 之 120 以下。

520 在此應非指電磁紀錄的實體物(載體)，而是指電磁紀錄內部的抽象價值，畢竟電磁紀錄的實體物本即屬於刑法上的物，將其竊取的行為本即該當刑法第 320 條第一項竊盜罪，沒有增訂第 323 條的必要，參黃榮堅，刑法增修後之電腦犯罪問題，刑罰的極限，初版，元照出版有限公司，1999 年 4 月，頁 309-310。

521 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表第 323 條刪除說明第一點。

522 在此會評價為偽造以及毀損而不評價為竊盜，是因為取得自己支配管領行為跟喪失他人支配管領的行為間並不具因果關係，而是兩個獨立的行為。

523 有些電磁紀錄還不具有文書性。

然而，似乎不是不能將竊盜的處罰重點放置於「得」的部分，亦即將竊盜的定義修正為「建立自己對於物(電磁紀錄)的支配管領」，而不論是否破壞他人對於物的支配管領。畢竟在竊盜罪的立法當時，並未想到可能會有破壞他人對物支配管領以外的方式來建立自己對於物的支配管領，而在時代進步後，法律也應跟隨時代腳步作修正，將不破壞他人對物支配管領，僅建立自己對物支配管領的行為態樣也歸納於竊盜罪之下[524]。此種見解看似可行，但實際上卻可能會造成竊取電磁紀錄罪遭到被架空的待遇，有論者認為在此要處罰者既是「透過複製的手段取得他人無形的抽象價值(智慧財產)」，本條即會變成著作權法的基本規定，亦即本條是規定「任何動產的取得」，而著作權法是特別規定「智慧財產(電磁紀錄)的取得」的處罰。一旦行為人竊取了電磁紀錄，基於特別法優於普通法的原則，仍會依照著作權法處理，刑法第 323 條形同架空。或有認為著作權法的限制嚴格，在不符合著作權法限制的情形仍可以回歸本條處理[525]。然論者仍認為電磁紀錄的價值本即在抽象的智慧財產價值，若電磁紀錄內容並無原創性，則從著作權法的要求看來，立法者本即認為此種著作並無被保護的價值，而行為人所竊取者是「不值得保護的財產利益」，故不應以竊盜罪論處[526]。

從以上分析看來，似乎一面倒的應該認為竊取電磁紀錄的行為並不能該當竊盜罪，而論述重點即在電磁紀錄的「可複製性」，然而此種論述理由即會在實務上最常見的案例—「網路遊戲盜帳號[527]」的情形上碰到困難。虛擬寶物被偷會對被害人造成現實社會上的物被偷一樣的感覺，是因為虛擬寶物跟一般電磁紀錄的稍微不同點—「(假的)不可複製性」。會稱呼(假的)不可複製性，是因為該些虛擬寶物仍屬於電磁紀錄，本即具有可複製性，然該些電磁紀錄是屬遊戲公司所有且受其管理，在實務上發生的大量案例並非對其為複製而言[528]。現今大部分網路遊

---

524 黃榮堅，刑法增修後之電腦犯罪問題，刑罰的極限，初版，元照出版有限公司，1999 年 4 月，頁 312。

525 如電磁紀錄的內容並無原創性，或屬於合理使用範圍的情形。

526 黃榮堅，刑法增修後之電腦犯罪問題，刑罰的極限，初版，元照出版有限公司，1999 年 4 月，頁 313。

527 或謂「竊取虛擬寶物」，因在前述實務分析時使用「網路遊戲盜帳號」的用語來表彰「被盜用的是帳號」的重點，故在此為了用語統一而沿用。

528 若行為人是以破除遊戲公司的管理營運機制，直接複製大量虛擬寶物的方式來取得虛擬寶物，即仍是以複製方式為之，故事實上是可以複製的。

戲偷虛寶的案例皆是「行為人輸入他人帳號密碼→進入遊戲中操縱該他人的遊戲角色→以遊戲公司預設的遊戲制度將該角色內的虛擬寶物『移轉』至其他帳號內」此種行為流程，故基於在此的未複製而「移轉」，即可能造成行為人受到自己的支配物被竊盜的感覺。同時，該些虛擬寶物亦是玩家苦心經營遊戲，經過各種任務而取得，並可在遊戲內依照遊戲規則任意使用的，看似與現實社會上受自己支配管領的動產並無不同，若認為竊取虛擬寶物不是竊盜，似乎仍可能違反相同事件相同處理的平等原則。

從而，在此即與前述竊取電磁紀錄的部分相同，首要分析者即是此種行為是否跟竊盜的行為流程相同，而只不過竊盜的客體從實體的物變成虛擬寶物而已。首先是破壞他人對(虛擬寶)物的支配部分，要破壞他人對虛擬寶物的支配的前提，則是「虛擬寶物必須本即在該他人的支配底下」。然而衡諸多數遊戲公司的遊戲規章，以及行政院消費者保護委員會在民國 94 年 3 月所草擬的「線上遊戲定型化契約範本」中的第 14 條，皆有提到「遊戲內的所有電磁紀錄所有權屬於遊戲公司方」的所有權歸屬問題[529]，故玩家對於虛擬寶物的支配來源，應不會是因為所有權而來。然而同條的後段卻有提到「玩家依照本契約以及遊戲管理規則之規定，對於電磁紀錄有支配的權利」，就此部分似乎可以認為玩家基於契約對於虛擬寶物得以支配管領，然而姑且不論玩家所支配管領的對象是該電磁紀錄本身或是該電磁紀錄的內容(虛擬寶物)，亦不論玩家如何支配儲存在官方伺服器上的虛擬寶物，依照該條玩家「支配管領」的前提是「依照該契約以及遊戲管理規則」，玩家並非如竊盜罪的支配管領一般，對於物有完全的支配以及監督權[530]，僅是能在契約或遊戲管理規則的允許下，在網路遊戲中使用此些虛擬寶物進行遊戲而已。

---

[529] 就現今玩家數量較多的幾個大型多人網路(MMO)遊戲、連線遊戲或網頁遊戲為例，晴空物語客服管理與規章第二條，收錄於 http://gd.x-legend.com.tw/08service/service_06.php、聖境傳說客服管理與規章第二條，收錄於 http://fn.x-legend.com.tw/08service/service_06.php、幻月之歌遊戲服務管理規章第十九條，收錄於 http://tw.beanfun.com/divina/www/7_gm_3.html、「SD 鋼彈 Online」線上遊戲服務使用者合約書第十五條第一項，收錄於 https://member.wasabii.com.tw/WA_liscence/liscence_sd.html、《信喵之野望》線上遊戲服務使用者合約書第十五條第一項，收錄於 https://member.wasabii.com.tw/WA_liscence/liscence_cat.html、暴雪公司 battle.net 使用條款第 5 條 G.及第 8 條，收錄於 http://tw.blizzard.com/zh-tw/company/about/termsofuse.html，以上最後瀏覽日期皆為 2012 年 5 月 29 日。

[530] 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 304 以下。

故在此與其說是一種支配，毋寧說只是一種「使用」的權利，亦即依照遊戲規則，玩家向遊戲公司申請「使用」該些虛擬寶物(更精確的說，是虛擬寶物所表彰在遊戲中的「差別待遇」)來進行遊戲的權利[531]。會造成此種規制用語謬誤現象，或許是因為在訂立範例當時的思維，是以該虛擬寶物是一個「物」的前提下，將既有的現實社會關係作連結而產生的結論。惟在此本文要提供一種不同的思維，來解構網路遊戲盜帳號的現象。

首先可以確定的是，遊戲內的所有電磁紀錄所有權屬於遊戲公司方的事實，包含玩家向遊戲公司所申請的帳號密碼、所創立的角色以及所獲得的虛擬寶物。而遊戲公司所提供的則是「遊戲服務」，亦即在玩家付出消費的時數後，在時數內提供玩家「使用」遊戲內容的服務，該服務當然包含存檔以及遊戲的進行[532]。再者，在遊戲內玩家會完成如打怪、交易等等「任務」，而獲得一定的虛擬寶物，此種虛擬寶物僅是一種「遊戲內成就以及差異性(利益)的表徵」，亦即遊戲公司本身在遊戲的設定上，認為此些「任務」是一種「遊戲內差異性的篩選措施」，篩選出完成任務的玩家，給予與其他玩家在遊戲內的「差別待遇(利益)[533]」[534]。此種差別待遇除了包含該虛擬寶物所設定的能力[535]外，還包含虛擬寶物的電磁紀錄本身[536]。從而只要在完成任務後，玩家縱使親自打電話告知遊戲公司自己已完成任務，遊戲公司在查證後，仍然必須給予其在遊戲內的差別待遇。然而面對大量客戶的遊戲公司，根本無法期待所有完成任務的玩家都要一一打電話確認，故其

---

[531] 相似見解可參考顏邦峻，從「竊取」線上遊戲的虛擬財物探討刑法上的電腦犯罪罪章之適用，國立政治大學法律研究所碩士論文，2006 年 7 月，頁 14。然該論者最後仍認為線上遊戲的虛擬財物屬刑法竊盜罪章上應保護的動產，參同論文，頁 26。

[532] 在此專指「月費制」的網路遊戲，而「商城制」的網路遊戲限制更加寬鬆，玩家建立帳號遊玩是完全免費的，亦即遊戲公司是免費提供遊戲內容的服務，故就論述上不致產生問題。

[533] 在商城制的網路遊戲中，還可能因為花現金向遊戲公司購買虛擬寶物而獲得，然而此種花現金購買的虛擬寶物基於遊戲公司獲利問題皆在程式設計上不會開放玩家間直接交易，僅可能依照類似「買抽獎券進行抽獎(任務)→抽獎得到虛擬寶物→遊戲內交易系統做交易(任務)」的間接流程提供玩家交易，故亦不會產生被偷竊的問題。且縱使在未來出現不同的商業型態而出現直接交易的遊戲類型，在此亦可以解釋成「由現金購買此種篩選機制而得來的差別待遇」，重點在於「該玩家具有差別待遇」，而非差別待遇從何而來。

[534] 相似見解可參考張繼圃，線上遊戲中虛擬財產在犯罪判斷上定位之研究，私立東海大學法律研究所碩士論文，2006 年 1 月，頁 54 以下。然該論者最後卻認為線上遊戲的虛擬財物屬刑法財產罪章上應保護的利益，參同論文，頁 50。

[535] 如「+7 大馬士革刀」此一虛擬裝備會使遊戲中角色的攻擊力增加 100 個單位。

[536] 如「娘娘蝴蝶結」此一虛擬裝備沒有任何特殊能力，但男性角色裝備上去後會在外觀上感覺非常娘。

在完成任務時，設置了一個「虛擬寶物」來表彰該玩家完成了任務，而必須在遊戲中獲得差別待遇[537]。據此，受差別待遇的重點在於「完成任務的玩家」，而非「擁有寶物的玩家」，縱使該些玩家的寶物受到他人給「移轉」，仍不變其是「完成任務的玩家」的地位，此時其致電遊戲公司要求遊戲公司在遊戲內要給予其差別待遇，遊戲公司仍應該給予。簡言之，虛擬寶物僅是「簡化」了「玩家向遊戲公司申請給予差別待遇」的流程而已[538]，將該簡化流程的表徵給「移轉」，並不改變該玩家本身應給予差別待遇的事實。故在此若將此流程與竊盜罪作連結，會發現該「偷虛寶」者所為的行為根本沒有「移轉支配管領」，就「遭竊」的玩家角度來看，該玩家仍然不會改變具有差別待遇的事實，而就遊戲公司的角度來看，行為人將虛擬寶物轉移到自己「在遊戲公司管領下」的帳號，無疑是把一個人左邊口袋的東西放到其右邊口袋，完全不生「破壞原有支配管領並建立新支配管領」的效果，從而此種行為應該跟竊盜的本質並不類似[539]。反而是行為人本身並非「完成任務的玩家」，而其卻在「完成了交易」或「完成了撿拾」等需要其他玩家共同完成的任務中，違反其他玩家意思而登入其帳號完成該任務，並佯裝成合於遊戲規則的方式完成該些任務，以致遊戲公司陷於錯誤，而誤給予其在遊戲中的差別待遇(服務)，並造成遊戲公司的損失(給予服務)，更類似於詐欺的本質，並且詐欺的對象是遊戲公司。

然而，在此可能會遭受與現實連結比較上的批評，謂現實上的物也是一種「價值的表彰」，該價值本即包含對於物本身的支配管領以及對物背後所表彰利益的

---

[537] 在此可以以一個比喻來說明：某一豪門打算舉辦宴會，而發給主人想邀請的好友一人一張邀請函，但一來因為主人必須忙著主持宴會，二來因為邀請人數眾多而無法一個一個認臉，所以主人就囑咐僕人站在宴會門口，以「認邀請函」的方式來辨認與會者的身分，並在邀請函上註明請攜帶出席。但此時所邀請的重點在於「主人的好友」，而非「持有邀請函的人」，邀請函的功能只是在於「節省主人認人的時間」而已。故縱使受邀的某甲並未攜帶邀請函出門，其仍然只要要求主人出來「認人」一樣可以進宴會。

[538] 基本上，玩家每次上線玩遊戲的讀取各種檔案的行為，本身就是一個個跟遊戲公司請求「我要在遊戲中做某某事了，請給我專屬於我的差別待遇」的過程，而遊戲公司的伺服器依照玩家的請求，才會給予其在遊戲中的差別待遇。

[539] 然而以前述宴會的例子，若某乙將某甲的邀請函偷走，仍然會成立竊盜罪，然而其原因不在於該邀請函所表彰的利益，而在於邀請函本身是一個「物」(當然在此的重點應不是邀請函本身，就像前述竊取電磁紀錄的案例重點不是在電磁紀錄的載體本身一般，只是邀請函剛好也被「物」的概念涵蓋，故對於邀請函本身的竊取也必須以刑法加以保護)。但於虛擬寶物的場合，雖然此些電磁紀錄看起來也像是虛擬的「物」，然實際上其只是一種「利益(差別待遇)的表徵」而已，此時是否要將此種利益的表徵硬是解釋成物，則是耐人尋味之處。

支配管領[540]，而在現實中將物偷走的行為本身亦是一個背後所表彰利益的支配被破壞的行為，從而偷虛寶的犯罪流程在現實生活中竊盜行為的解釋運用上亦無不同，故對於現實上的物跟虛擬寶物為竊盜的行為似應該等同而論。然而，架構網路遊戲的虛擬世界與現實世界存在著根本性的差異—在虛擬世界中，我們可以知道有「神(遊戲管理者)」的存在，並且在遊戲內部我們可以直接跟「神」溝通，「神」也有顯示「真理(價值的歸屬)」給我們知道的能力。從而，縱使我們移轉了「價值的表彰」，全知全能的神仍然可以判別出誰是擁有該價值者。具體而言，縱使玩家的虛擬寶物遭竊，仍不影響玩家向遊戲管理者要求「使用」該寶物所表彰在遊戲中差別待遇的此一利益，而遊戲管理者去調查 IP 記錄以及使用履歷的行為，即是確認玩家是否本即應受差別待遇，且該差別待遇的表彰亦非由該玩家完成「交易」或「拋棄」等「任務」而移轉[541]。若在調查 IP 記錄與使用履歷後確認屬實，即可確認該玩家仍應給予差別待遇[542]。然而現實社會中我們無法得知是否有神存在，並且我們也無從知道「真理(價值的歸屬)」，而僅得由「客觀的情況」來推知「接近真理的事實」。在此種「無從得知真理」的世界中，人類又矛盾的追求「真理」，故只好藉由刑事的手段來盡力維護價值的歸屬，而唯一能證明價值歸屬者，就是身為「價值的表彰」的財物本身，故刑法上會對侵害財產法益的行為作處罰的規定。然而在價值的歸屬得以直接確認，價值的表彰存在與否並不影響價值歸屬判斷的時候，對於「移轉」價值表彰的行為似乎就沒有理由再以擁有最後手段性的刑法來論處。

即使如此，此類行為在社會上仍造成一種「不平衡」的錯置感，亦即該盜帳號且擁有虛擬寶物的人若將該寶物拿去賣掉換成現實生活上的貨幣時，仍然獲得了大量的「現實」金錢，並顯出該些所謂「價值的表彰」在社會上仍有一定的經濟價值，但此種經濟價值本不應該由該行為人所享有，是其利用盜帳號並移轉虛擬寶物的手段而獲得。惟此種不平衡其實是個假象，而此種假象是由兩個不同階段的行為所組成。前階段的「偷虛寶」行為應解釋為詐欺行為已如前述，而後階

[540] 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 328。
[541] 亦即被盜帳號，由不同 IP，甚至與之後取得該寶物的玩家同一 IP 完成該任務的情形。
[542] 此種作業流程可參考暴雪(BLIZZARD)公司 battle.net 使用條款的處理方式，網址為 http://tw.blizzard.com/zh-tw/company/about/termsofuse.html，最後瀏覽日期：2012 年 5 月 29 日。

段的現金交易(Real Money Trade，下稱 RMT)行為應獨立觀察，畢竟亦有可能用來 RMT 的虛擬寶物是玩家自己依照遊戲規則達成任務而得來的成就。同樣如前所述，在 RMT 在遊戲部分的流程中，亦為一個建立在雙方玩家的合意上所共同達成的「交易任務」或「撿拾任務」，任務的內容通常是賣方提供虛擬寶物，買方提供極少量的虛擬資源(包含虛擬貨幣或虛擬道具)或甚至不提供任何資源而進行，或是賣方將虛擬寶物依遊戲規則「拋棄」，而買方將該寶物為撿拾。賣方為了達成任務，所要消耗者即是「虛擬道具所表彰的差別待遇」，反觀買方通常不會在遊戲中付出任何資源。而此種「賣方自願消耗其差別待遇而協同買方完成任務」的對價，則是現實世界中的金錢。故在此應可認為 RMT 在民法上應較類似承攬的關係，該金錢並非是虛擬寶物的對價，而是「完成任務」此一工作的對價。至於就是否禁止 RMT 的部分，我國絕大多數遊戲公司因考量到 RMT 會產生大量法律問題以及變相助長電腦犯罪的發生，故多在遊戲規章中明文禁止此類行為[543]。然在最近的遊戲公司中，亦不乏嘗試克服此類問題，在嚴格的控管下允許並管理 RMT 行為者[544]。

此外，就此種 RMT 行為的遏止可以從兩個方面著手。首先，就遊戲公司方面，前述的線上遊戲定型化契約範本第 14 條中，本即認為玩家在「依照本契約以及遊戲管理規則之規定」時，始對於電磁紀錄有支配(使用)的權利，然而事實

---

[543] 就現今玩家數量較多的幾個大型多人網路(MMO)遊戲、連線遊戲或網頁遊戲為例，晴空物語客服管理與規章第十四條，收錄於 http://gd.x-legend.com.tw/08service/service_06.php、聖境傳說客服管理與規章第十四條，收錄於 http://fn.x-legend.com.tw/08service/service_06.php、幻月之歌遊戲服務管理規章第十七條，收錄於 http://tw.beanfun.com/divina/www/7_gm_3.html、瑪奇遊戲管理規則第十一條，收錄於 http://tw.beanfun.com/mabinogi/8_customer2.aspx、「SD 鋼彈 Online」線上遊戲服務使用者合約書第十五條第三項，收錄於 https://member.wasabii.com.tw/WA_liscence/liscence_sd.html、《信喵之野望》線上遊戲服務使用者合約書第十五條第三項，收錄於 https://member.wasabii.com.tw/WA_liscence/liscence_cat.html、暴雪公司 battle.net 使用條款第第 2 條 B.(c)、(d)及第 8 條，收錄於 http://tw.blizzard.com/zh-tw/company/about/termsofuse.html，以上最後瀏覽日期皆為 2012 年 5 月 29 日。

[544] 參暗黑破壞神三官方網站，收錄於 http://tw.battle.net/d3/zh/blog/462199/%E3%80%8A%E6%9A%97%E9%BB%91%E7%A0%B4%E5%A3%9E%E7%A5%9EIII%E3%80%8B%E7%8F%BE%E9%87%91%E6%8B%8D%E8%B3%A3%E5%A0%B4%E7%BE%8E%E6%9C%8D%E5%B0%81%E6%B8%AC-2011-12-2，最後瀏覽日期：2012 年 5 月 29 日。然而此種 RMT 拍賣市場亦僅於美國伺服器開放，並且有限定 IP 或使用特定銀行的信用卡付帳等等嚴格限制。

上多家遊戲公司的遊戲規章內皆有規定「禁止在遊戲中買賣、轉讓任何電磁資料成為現金或實體物品」已如前述，故可以認為玩家若將遊戲內寶物作 RMT 時，本即違反遊戲規則，而既然違反遊戲規則，意味著不論買方或賣方遊戲帳號內的電磁資料，遊戲公司皆可以在違反遊戲規則的範圍內做變更或刪除，而通常從遊戲的履歷或交易的對價等資料亦可以看出是否有RMT的跡象，一旦認為是RMT，則遊戲公司當然可以對該些帳號作變更[545]。再者，從買賣雙方的角度觀察，就賣方所獲得現實生活上的金錢貨幣部分，則在由買方於有民事請求權基礎時，向賣方為請求。然而此時除非賣方有為特殊的「保證」行為，否則通常明知有風險仍為交易的買方，在賣方為「服務的給付(在遊戲內移轉寶物，與買方共同完成任務)」後，所產生被遊戲公司對電磁紀錄作變更的風險本應由買方自負。

必須附帶一提的是，若「偷虛寶」的行為人並未將該寶物作 RMT，反而是依照網路遊戲規則中的交易任務，將該些寶物與不知情的第三人換成虛擬貨幣或其他寶物時該如何處理的問題[546]。此時因涉及不知情第三人對遊戲中遊戲規則及任務制度安全運作的信賴感的關係，故可能必須考慮由遊戲公司以制定遊戲規章或與玩家的定型化契約中載明等方式處理，而處理方式亦具有彈性，在一般情形可能可以以「雙贏」的方式，使第三人與被害人都能擁有該差別待遇，然而在「雙贏」的情況可能重大影響遊戲平衡的情形下[547]，可能會必須考慮以「變更後補償」的方式，在變更第三人帳號內的電磁紀錄後，給予其相當的補償。必須強調的是，就之後涉及 RMT 的部分，皆是以民事即可處理的問題，更何況在遊戲公司禁止 RMT 的情況下，對於支付現金交換虛擬寶物的買方來說，令其負有對賣方為金錢返還請求的訴訟壓力實則適得其所，也有助於遏止此類行為。

但縱使經過以上論述，仍然無法消弭社會大眾的法感情中對於「偷虛寶」的行為人感到「可惡」、「利益被侵害」的情緒。在無法從「破壞他人對虛擬寶物的

---

[545] 同時在 RMT 的情形，除交易可能取消外，該些玩家還可能會遭到強制取消帳號或是強制沒收寶物等遊戲規則的處罰。

[546] 若是知情的第三人或甚至是該偷虛寶玩家的分身帳號，遊戲公司亦可依其「明知」該虛擬寶物是「贓物」，而對其帳號內的電磁紀錄作變更，然而事實上極有可能大部分都以不知情來處理，故在此不知情的情況較具討論價值。

[547] 例如該虛擬寶物是整個遊戲中只能有一件，而若為同時保護被害人以及第三人的利益，勢必使遊戲中出現兩件該寶物，而會破壞遊戲本身的平衡時。

支配管領」以及「建立自己對於虛擬寶物的支配管領(RMT)」中獲得解釋時，所注重的點即存在於「為什麼行為人可以隨意輸入我的帳號密碼而登入本來只有我或我授權的人才能登入的遊戲帳號？」上，而此種「登入控制機制」的破壞，背後所表彰的利益侵害似乎才是社會大眾產生「不平衡」的源頭。在此即回歸到前述學說或實務上對於保護法益的爭執，而就此問題不論是採取以個人保護的角度或以集體保護的角度皆足以解決，故第一種見解認為「認為電腦犯罪的保護法益是傳統法益以外的新法益者，僅是逃避問題而非解決問題」的批評，實際上應是一種誤解，問題不是沒有解決，是此類問題若加以拆解，本身即以傳統刑法即得以解決，然而縱使以傳統刑法加以解決，仍無法解釋人民受到某種利益被侵害的感覺，故在此即可能要討論是否有新興保護法益的產生[548]。

而就新興法益討論的後兩種見解，則是完全以不同面向的角度來觀察同一種社會現象。認為以個人法益為保護的見解(下稱使用空間支配說)是基於傾向消極面的「若行為人侵害我的電腦，我會受到什麼損害？」為思考的出發點，以所有電腦犯罪一概會有的特性─使用空間支配的破壞作論述，認為規範重點應是「因行為人的行為，被害人會受到損害」，而不論該電腦是否有連線機制，亦即縱使對單機電腦為侵害，或對連線電腦為侵害，所侵害的法益皆同為使用空間的支配。而在此見解下，由於侵入電腦是表彰使用空間支配的破壞，因此所有電腦犯罪一定必須要有「入侵電腦」的行為始會該當，故採取本說者對於入侵電腦的定義操作即會極度寬鬆，縱使被害人就站在行為人旁看著行為人使用其授權使用的電腦，若其僅授權行為人上網收信，而行為人卻未經同意在收信之前先上 FACEBOOK 看看有沒有好友在其塗鴉牆上留言，此一看塗鴉牆留言的行為本即該當入侵電腦的行為，以及寄送含有病毒的電子郵件讓對方收下的行為，亦屬一種入侵電腦的行為[549]。

反之，就認為以社會法益為保護的見解(下稱網路安全信賴說)，則是基於偏

---

[548] 事實上，法益不可能會「產生」，只可能會被「發現」，參陳志龍，法益與刑事立法，自版，1990 年，頁 102-103。而在此使用「產生」的用語，是相對於第一種見解認為「電腦犯罪沒有獨立的新法益」而言，表示從「無」到「有」的過程。

[549] 然而以上二行為依照現行法，因未該當限定行為的構成要件(輸入他人帳號密碼、破解使用電腦之保護措施、利用電腦系統之漏洞)而不成立入侵電腦罪。

向積極面的「若行為人侵害我的電腦，我會失去什麼機會？」為思考的出發點，而以社會上對於網路安全秩序的信賴作為保護網路此一溝通機制的法益。此種信賴關係可以作為法益保護，實與德國的經濟犯罪概念類似[550]。決定一個不法行為是否能歸類於經濟犯罪，最重要的標準即是「整體經濟秩序的危險或侵害」[551]，而此種整體秩序的維持可以作為保護的對象，即是因國家的任務有所改變的緣故。不若 19 世紀的夜警國家，20 世紀的德國是朝向社會國發展，亦即國家有保障與促成個人自我實現的任務，國家不但要保護社會弱勢，同時也要提升全民生活水準。而隨著國家介入的事項越來越多，維持制度運作的正常亦為實現國家任務的一大要素[552]。如同德國學者郝斯曼(Hassemer)所述：「因為人類是社會性的存在，只有在與他人共處的共同體當中，其利益才能確保與實現。對這些制度的保護，就是為了生活在這些制度中的人類的間接利益而進行的法益保護[553]。」，故德國就對於制度的保護上，亦有限度的肯認可以作為法益保護，而其中的一種類型即是「對於制度的信賴」。對於制度的信賴是制度運作的基石，當制度中的每個人都能互相信賴時，每個人僅需要負責自己所負責的部分，相較於每個人必須對自己以外的部分傷腦筋的制度來說，前者顯然可以將自己負責的部分作的較好，而每個人都可以將自己負責部分做好的同時，也意味著整體會更好[554]。而此種信賴關係即意味著要以「違背信賴」作為是否成罪的判斷基準，從而採此說學者多認為，並非單純的入侵電腦或其他不適切行為即會成立犯罪。同時，由於其著眼點是在於電腦網路的溝通機能，從而對於不具連線機能的單機電腦的入侵或刪除資料等行為，似乎皆會因為「未違背社會上對於網路安全秩序的信賴」而皆不成立犯罪。

而此二見解的兩相比較之下，會發現不但雙方的見解皆有理由，且各執一詞

[550] 在前述的第二次經濟對策法中，即有對電腦犯罪的修正。參林東茂，德國近年來的經濟刑法發展趨勢，危險犯與經濟刑法，初版，五南圖書出版股份有限公司，2002 年 11 月，頁 117 以下。

[551] 林東茂，經濟犯罪之研究，初版，中央警官學校犯罪防治學系發行，1986 年 4 月，頁 205 以下。

[552] 鍾宏彬，法益理論的憲法基礎，初版，公益信託春風煦日學術基金， 2012 年 4 月，頁 245 以下。

[553] NK/Hassemer/Neumann, vor § 1 Rn. 138=AK/Hassemer vor § 1 Rn. 281. 轉引自鍾宏彬，法益理論的憲法基礎，初版，公益信託春風煦日學術基金， 2012 年 4 月，頁 246-247。

[554] 鍾宏彬，法益理論的憲法基礎，初版，公益信託春風煦日學術基金， 2012 年 4 月，頁 261 以下。

沒有交集，呈現一種非常微妙的關係。然仔細觀察會發現，看似互斥的兩種見解，其實有並存的可能—兩說見解根本是在就不同的面向論其法益。就如同放火罪的「燒燬」可以表現出他人所有物的毀損，但也同時可以表現出周圍的人因此而擔心害怕自己的人身或財產安全受到損害一般，對於入侵電腦的行為，雖然表現出了空間支配的破壞，但同時也因為一個被害人的空間支配受到破壞，而造成大多數人對於網路安全秩序的信賴感遭到破壞[555]。既然對於法益面向的論述角度不同，所論述的目標(法益)也不同，理論上兩個見解應該是不足以解決對方的問題。從而，採取網路安全信賴說的論者非常認份的僅將適用範圍限縮於「網路」的部分，因唯有網路才有溝通的可能性，故採類似保護法益的日本不正連線禁止法亦於構成要件的設計上限定要「透過通訊線路」而不正連線的行為，才可能依照該法處罰；採取使用空間支配說的見解，亦僅著眼於空間支配的破壞，而不管是否為連線電腦，以及入侵行為態樣的輕重等問題。

但是，問題的癥結點就在於我國對於電腦犯罪專章的規制上，「電腦犯罪」的範圍可大可小，在前述即已有分為兩種(個人以及集體)法益作論述的空間，然而立法者完全無視此類問題，一概把此種可大可小的犯罪完全規範在同一個罪章中，且給予非常重的刑度。先撇除立法者所設定的刑度以及立法理由中欲規制者幾乎皆是網路安全信賴說所欲防止的「大型」電腦犯罪的部分[556]，無論是網路安全信賴說或使用空間支配說，皆是採取對電腦犯罪尋找一個「適當的保護法益」來令其能夠順利適用。若將電腦犯罪全部解釋成社會法益，頂多會造成單機電腦的規範部分無法規制的結果[557]，但是不少問題即會發生在將電腦犯罪皆解釋成個人法益的情形。

首先，就入侵行為的部分，採取使用空間支配說的論者是以家族相似性作為論理依據，將入侵電腦以及侵入住宅的行為作論證後，得出入侵電腦亦呈現出一個使用空間支配的侵害的結論[558]。然此結論可能會導致過擴張處罰範圍的問題，

---

555 第十四屆政大刑法週會議紀錄，2007 年 3 月，頁 31-32，李茂生教授的發言。

556 參中華民國刑法第 358、359、360、361、362、363 條立法理由第二點。

557 然而此種無法規制現象對於採取網路安全信賴說者來說應是限縮處罰後必然的結果，與其說是缺陷，不如說已達到限縮處罰的目的，反倒是個好處。

558 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月，頁 78。

在比照入侵電腦跟侵入住宅的時候，除觀察到入侵電腦在與侵入住宅類似，亦呈現使用空間支配破壞的特性之外，還必須要注意入侵電腦與侵入住宅最大的差別—侵入住宅目前似無法找到對社會有益之處，但入侵電腦對於資訊科技的發展有一定的助益。資訊科技除包含硬體設備外，亦包含軟體設備。而軟體設備不外是程式的撰寫，而程式的撰寫表彰出程式設計師的一貫邏輯概念，此種邏輯概念或可能來自於設計師本身的自身經驗，亦可能來自於資訊工程教育的傳承。但邏輯終將會有漏洞，而此種漏洞，絕大多數都是依靠駭客等專門破解程式的人而發現。正如論者所謂：「無故入侵電腦的行為有時僅是造成輕微的、微不足道的個人損害而已，甚至有時是一個健康的行為，因為其可促使掌管電腦的人注意的系統的漏洞等，並因此而能及早採取一些必要的補救措施[559]」，雖有謂此種破解應在專門的場合(如研究室等處)進行，然而此種分權分職的「中心式論述」正忽略了網路「去中心化」的最大特色，亦即在網路中並無所謂何為中心何為端末的問題[560]。如同著作權保護與資訊分享的權力拉扯部分，在此資訊科技能有辦法能如此快速的發展，有一大部分也是因為全世界有如此多數多樣的入侵手法以及病毒問世，接著引發世界各地對於系統安全的精進，此種發展是一種世界性、體制性的，故為了不讓刑法阻礙資訊科技的發展，對於法益衡量以及優越利益衡量[561]即是在此的重點[562]。而通常法益與利益衡量的結果，大多會對於構成要件的成立條件作一點限縮，在此可能想的到較有效的限縮方式即是如同毀損罪般的「足生損害於公眾或他人」此一要件，以社會法益作為個人法益成罪的門檻[563]。然而此時即會發現一個有趣的現象，對於純粹單機電腦的入侵行為，幾乎無法例證能達「足生損害於公眾或他人」的程度。從而縱使採取個人法益的保護，最後仍然很難規範到

---

[559] 李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 250。

[560] 李茂生，我國電腦網路犯罪的虛像與實相，刑事政策與犯罪研究論文集(四)，法務部犯罪研究中心，2001 年，頁 3。

[561] 要保護的對象不是侵害他人的駭客(嚴格來說是快客)，而是整個資訊發展的體制。

[562] 尤其是採本說見解者的「入侵」概念非常寬鬆，會導致刑罰權的大力擴張。

[563] 在此所謂的門檻，係指「縱使行為人的行為為侵害保護法益的行為，仍須就資訊科技發展的利益與被破壞的法益作利益權衡」的門檻，而非「判斷行為人的行為是否侵害保護法益」的門檻。由於個人空間支配法益的侵害依照論者的論述可能遠較社會對網路秩序安全信賴法益的侵害可能性要高很多，故若如同社會法益般僅依照是否侵害法益來權衡利益是否需要保護可能會使利益的保障造到嚴重限縮，而必須在侵害法益之後仍要考慮利益問題。又，刑法第 358 條限定行為態樣的限縮方式已遭到不少批評，故在此未援引此種方式作為門檻。

純粹單機電腦的入侵行為。

再者，在告訴乃論的設定上，運用家族相似性而得出個人法益的見解亦會產生一些疑義，與入侵電腦相似的侵入住宅罪，是有告訴乃論此一訴訟要件的設定的，而似乎對於入侵電腦罪，似亦應具備告訴乃論此一訴訟要件[564]，然而此一要件會因為網路的發展而導致的資訊國際化，使得對於重大跨國案件的侵害，實務上刑罰權的發動皆受阻礙[565]，間接使得本罪章主要條文皆成具文[566]。然若僅是要單純解決問題並非困難，蓋告訴乃論的規定與不法行為本無關聯，若因電腦犯罪國際化的特性，而不設定告訴乃論的作法亦無不可，但若如此，則更要注意前述可能造成刑罰權過度擴張的現象。

最後才回到立法者所設定的刑度以及立法理由作觀察，立法理由中所使用的「DDoS 攻擊」、「CIH 病毒」、「系統管理者須耗費大量之時間人力檢查」或「較嚴重的電腦犯罪」等語詞，以及最重本刑三年或五年以下的重刑度，雖然仍可以解釋成該些行為皆侵害個人法益[567]，然而如何說服破壞使用空間支配的個人法益足以用同是「破壞他人安心領域支配」的侵入住居罪的三倍以上刑度來處罰，亦是個困難的問題。而若僅是要解決此問題似也不困難，只要主張此種不合理刑度的表現即是立法者思慮欠佳之處，故應主張將刑度全面降低即可。

可是，反觀整體對於構成要件行為的設置、訴訟要件的設置、以及刑度的設置，主張以個人法益為電腦犯罪保護的論者皆得出「是立法者思慮欠佳，故應修正」的結論，但一整個罪章中，除了構成要件、法律效果(刑度)以及(有時候會設置)的訴訟要件外，似乎什麼都沒剩下了。此種結果不禁令人懷疑兩個問題：第一、立法者在制定妨害電腦使用罪章時，所預設的保護法益是個人法益嗎？第二、採取使用空間支配說的論者，真的是要為立法者所訂立的妨害電腦使用罪章找到

---

564 刑法第 363 條亦規定本章之罪，除第 361 條及第 362 條之外皆須告訴乃論。

565 無論是我國對國外，或是國外對我國。

566 若依照採網路安全信賴說論者的意見，此種告訴乃論之罪本即理所當然的應刪除，問題的處理相較於採使用空間支配說論者來的簡單明瞭。

567 以放火罪的例子來看，各種放火行為皆包含物的「燒燬」，似亦皆得以個人法益作解釋，在此即呈現了保護法益不同而應有不同規制的問題，不能因為刑法已規定了放火罪，對於毀損罪只要適用「放火罪的較低刑度」而不另行規定。

一個適用歸屬嗎？第一個問題的解答很可能是「有」的，但同時也可能是「沒有」的，畢竟立法者(也就是實務)本身根本沒有保護法益的概念，若要認真探究的話會發現正如修法理由所述「兼及保護國家、社會、個人法益」。至於第二個問題的解答，很可能也是「有」的，然卻由於立法者在立法時考慮太多關於社會法益的部分，導致在個人法益的規制上左支右絀，若要打造一個純保護個人法益的電腦犯罪專章，的確幾乎要將整個罪章「砍掉重練」。於保護社會法益的情形亦然，但主張網路安全信賴說者因為在條文上受到立法者的「恩惠」較多，故若硬是要用現行法來解決問題，需要修正的部分以及碰到的問題就會較少。

又，參考前揭章節對於雲端運算的敘述來看，雲端運算的核心其實就是網路運算，網路運算名符其實，網路在體制的運作占了很大的要素，並且在導致使用者使用型態的改變上，也可以發現「IT 資源的共享」以及「資訊的共同管理」其實也就宣示著「網路(集中資源)為主、單機(分散資源)為輔」的時代已經來臨，而作為溝通機制的網路，似也應是未來的保護重點。

綜合以上，似可以認為立法者對於妨害電腦使用罪章的規制上，應主要是想規制破壞採取網路安全信賴說的論者所主張的社會法益的行為，故在刑度的使用以及構成要件的規制上皆課以重刑以及嚴格(？)限制構成要件的該當。並且從雲端運算時代的來臨也可以發現社會上對於網路安全秩序的信賴日漸增加，故而在此應可以認為妨害電腦使用罪章的保護法益應以社會上對於網路安全秩序的信賴為妥。至於個人的使用空間支配，仍應如所主張的論者所述，嘗試回歸傳統刑法條文作規制，亦或如同放火罪與毀損罪的關係，再以另一個獨立罪章作專門規制是一個較適當的作法。據此，同時也限於篇幅，以下的論述即僅聚焦於以社會上對於網路安全秩序的信賴為保護的電腦犯罪專章作論述，而先擱置對保護個人的使用空間支配的電腦犯罪專章部分的建構。

第三項 其他爭議問題之解決

在確定了妨害電腦使用罪章以及電腦犯罪的保護法益後，在此即要解決前揭章節所提出與保護法益有關的各種爭議問題，包含電腦犯罪的定義、電腦犯罪的

名稱使用、以及電腦本身的定義問題。故以下就依序就電腦犯罪的定義、電腦犯罪的名稱使用、以及電腦的定義三個方向作分析。

首先是就電腦犯罪的定義部分，前揭章節對於電腦犯罪的定義爭執，最後得出的結論是「從保護法益的角度出發思考」，但在此所遇到的困難，即是於保護法益的探討上，竟然得出一個社會法益以及一個個人法益的結論，雖然可以再次證明電腦犯罪概念的攏統以及涵蓋範圍過廣的問題，然而要如何對如此廣泛涵蓋的犯罪範圍下一個不空洞的定義即是個具有挑戰性的工作。反射性可以想到的方式是，如同公共危險罪跟毀損罪一般，由於個人法益以及集體法益性質以及規制範圍的不同，對於「電腦犯罪」下兩種不同定義，對於侵害社會上對於網路秩序安全信賴的部分，即是要定義成「行為人濫用電腦或使用足以侵害電腦硬體或軟體之行為，而造成由電腦網路所架構的溝通秩序紊亂之犯罪」，而對於侵害個人使用空間支配的部分，則要定義成「行為人濫用電腦或使用足以侵害電腦硬體或軟體之行為，而造成他人失去使用空間支配之犯罪」。不過，此種區分式並且分別圍繞保護法益所作的定義，可謂完全未解決電腦犯罪定義的問題。若在未來又因科技發展導致再度發現需要保護的法益時，關於電腦犯罪的定義即會越來越多，並且此些犯罪皆有一個共同的特徵，即是「行為人濫用電腦或使用足以侵害電腦硬體或軟體之行為」。同時，在保護法益的探討後，可以發現無論是採取網路安全信賴說或使用空間支配說的論者，所得出的保護法益結論跟電腦本身關聯性已漸行漸遠，「濫用電腦」為犯罪行為儼然僅成為此些保護法益的前提概念。惟繼續對此更深入的作思考，會發現重點應在此些行為所保護的法益是否被破壞，而破壞此些法益是否一定要使用電腦，儼然根本不是重點了，故與其認為此些犯罪類型皆為電腦犯罪的下位概念，毋寧認為電腦犯罪僅是引導論者思考而得出保護法益的一個契機而已。此種結果與德國對電腦犯罪的處理態度非常類似，亦即電腦犯罪根本不是「新」的犯罪，其所謂「新」，僅是「新」在犯罪的過程中會使用電腦或網路的行為方式而已。據此，即可以大膽說出「電腦犯罪本身即非常空洞，沒有下定義的必要性，若硬要為其下定義，應僅採取最寬鬆的定義方式即可」此一結論，電腦僅是發現此些法益的共同特徵(同時也會包含傳統法益的部分)，

並非一定要透過電腦始能侵害此些法益[568]。

再者即會導出電腦犯罪的名稱使用問題，既然已經找到電腦犯罪的保護法益，並可就保護法益來限縮部分行為的入罪化，且已導出所謂「電腦犯罪」其實是一個空洞的概念，則會進一步產生的問題即是「是否仍要稱呼此類犯罪為『電腦犯罪』？」的問題。實務上對於電腦犯罪的稱呼，從一開始基於犯罪工具都是透過電腦而使用的電腦犯罪，到依照行為人行為態樣的共通性而使用的濫用電腦罪，以及最後定案依照被害人所受到的不利益而使用的妨害電腦使用罪，皆是依照該些犯罪的共通性來作為稱呼的基準。若依照此種命名標準，對於前述兩種電腦犯罪的命名很可能會是「破壞使用空間罪」以及「妨害網路秩序罪」。雖然結論邏輯正確，但幾乎無法在社會上獲得共鳴，後者的妨害網路秩序罪可能還有些許連結點，然而使用空間破壞罪如同前述跟電腦本身其實已經沒有強烈的連結性了，此刻似乎要回到問題的原點—「對於要求電腦犯罪『正名』的目的為何？」來作思考。依前述，因一個犯罪的名稱所表彰的即是其保護法益的反射，如同殺人罪表彰生命法益的侵害、傷害罪表彰身體法益的侵害、妨害電腦使用罪即表彰(實務認為的)電腦使用安全法益的侵害，但於電腦犯罪定義的部分已得出電腦犯罪本身即是一個空洞的概念，僅具有引導人類思考並尋找出相對於傳統法益的新型態保護法益的時代意義，故在此對於此種僅具時代意義的空洞概念，本即無法就名稱來表彰保護法益，反而在其具有引導出人類尋找新型態保護法益的功能上，似應於名稱中表示「為何人類會開始尋找新型態保護法益」的特色。而人類會開始尋找新型態保護法益，即是因為當初被納入此種犯罪類型的行為皆有「使用電腦為犯罪行為」的共通特色，故在電腦犯罪的名稱使用部分，本文依然主張使用「電腦犯罪」此一名詞來作為此些犯罪類型的總稱，縱使總稱在犯罪討論的面向上極為空洞且不具討論價值，然而其仍有引導人類尋找新型態保護法益的時代意義，然而本文所得出新型態保護法益是使用空間的支配以及社會上對於網路秩序安全的信賴，並聚焦於後者來建立獨立罪章時，對於所建立的罪章名稱即應使用

[568] 然而，若要嚴格來說，真正可能符合電腦犯罪的定義者，應該是採取網路安全信賴說的論者所架構下的犯罪類型。畢竟其保護的即是「由多數電腦的連線所架構的網際網路通訊制度」，若在未來可能發展出電腦以外的更新型通訊制度，則並非其所保護的對象，然而在此即會產生如下述的電腦定義問題。

「妨害網路秩序罪」。

最後要處理的問題即是「電腦」的定義，由於無論學說或實務僅有極少部分論者在例外情形容許刑法上對電腦為定義[569]，並且在前揭章節本文亦認為在現行法的規定之下似以不為定義為較妥適的作法，然於前述本文最後得出了必須修法的結論，在修法的前提下，是否需要對於電腦作定義的問題即再度浮現出來。認為不予定義的多數見解，所採取的主要理由即是電腦的不可定義性(流動性)概念，因科技日新月異，若於未來出現了更新型的使用型態，則依據舊型態所訂定的法律又會失去遞續性。以此為理由雖實有幾分道理，但在本文前述對於電腦犯罪的定義作分析時即有提及，目前找出的各項保護法益與電腦的關聯已經甚淺，雖然有可能是於時代上要侵害此些法益即必須使用電腦，惟不表示在未來侵害此些法益亦必須使用電腦，若在構成要件中規定如「須使用電腦始能違犯本罪」的構成要件，而在電腦的定義上又以遞續性為理由「交給社會決定」，可能會產生因微電腦以及雲端大量介入人類生活時，社會大眾無法判斷什麼是電腦，亦或以最寬鬆的方式去判斷電腦，前者的情形很可能即會造成法官恣意，並使得判決的歧異率高；後者的情形即會造成刑罰權範圍不當的變動，並在社會大眾皆不認為此是電腦，偏偏利用該物亦能侵害使用空間支配的情形時，亦會造成與其所批評「定義電腦之後出現新產品而導致舊法失去遞續性」相同的情況。比較妥適的作法，應該是在構成要件的設計上，充分顯示出對法益的保護，而非執著於「使用電腦」的行為，若構成要件充分顯示出對法益的保護，則縱使不規定使用電腦的行為會成立該罪，在涵攝的過程中亦會將使用電腦的行為涵攝入內。此種作法因無須提及電腦，故也不會涉及電腦的定義。然而，此種方式對於妨害網路秩序罪可能反而會出現適用上的問題，畢竟網路秩序的建構，即是對於使用電腦的資訊時代中，由多數電腦所架構的網際網路所形成的秩序，其對於電腦仍有一定程度的關聯，而如同貨幣制度般，網路制度的使用亦會有其壽命，而其壽命本即是遞續性的尾端，縱使運用家族相似性尋找出類似的可罰行為，基於罪刑法定原則仍必須進行法律的修訂，故對於此種會隨著人類生活的時代而變遷的共同生活利益，亦僅能

[569] 蔡蕙芳，電腦犯罪和刑事立法的課題，國立台灣大學法律學研究所碩士論文，1994 年 6 月，頁 16 以下。

限制於其「主宰」人類生活的那段時間中具有重要性而已。從而，若今天人類又發展出一套新的溝通系統，而此種系統的運作又更加超越現行的網路系統，並連最寬鬆的電腦概念都無法包含時，法律所應該作的，不是利用電腦概念的流動性硬是認為其是「電腦」而適用相關條文規制，而是必須如本文般繼續思考是否又是一個新型態法益可能被發現的徵兆，或是必須利用家族相似性來找出處罰的依據。據此，因妨害網路秩序罪對於網路秩序解釋的實質需要，對於電腦下一定義於刑法上仍有必要性，並為刻畫出遞續性的最大範圍，本文認為應對於電腦(嚴格來說，應是「電子計算機」)下一最寬鬆的定義，亦即採用美國聯邦法、州法、我國資訊科技業以及認為應予定義的學者所採用的定義—「一種可以解譯並執行程式命令之電子裝置，得以處理輸入、輸出、算術以及邏輯運算。其主要結構，係由輸入裝置、處理器、輸出裝置以及儲存裝置等四個基本元件所組成[570]」。在下了最寬鬆的定義之後，接下來的工作即是為了不讓處罰範圍過廣而作一定程度的限縮，此種限縮本文即認為應是在構成要件設置時要作的工作，亦即「侵害何種電腦需要處罰」、「侵害電腦到何種程度需要處罰」或「以何種方式侵害電腦需要處罰」的問題。就此些構成要件的限制，即是本文在確立以上問題的解答後，於下一節中所主要探討的標的。

第二節　入罪化行為之篩選

在確認妨害網路秩序罪的保護法益，並得出必須以獨立罪章處罰的大方向後，接下來在本節要劃定以法益為核心應該要處罰的行為態樣作為罪章法條的基礎。此些行為有可能是前揭章節已討論過的舊有法條本身既有規範的行為態樣，亦有舊有法條並未規範，但因為涉及保護法益故亦應列入處罰的新行為態樣。並且在劃分何種行為態樣需要處罰後，本節也必須要為劃分出來的行為態樣做構成要件上的限縮，以免偏離以保護法益為中心的處罰宗旨。

---

[570] 甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌第 50 期，2003 年 9 月，頁 180-181。然在此僅是參考論者對於電腦定義最寬鬆的敘述，本文仍不認同論者對於實際判斷部分所認為「數據機不是電腦的一部分，而印表機是」等分析。

如前所述，「電腦犯罪」涵括範圍廣泛，各種行為態樣的評價不一，同時某些行為仍具有保護必要，而不能過度擴張處罰範圍，縱使社會法益比起個人法益，法益侵害的可能性較低，可以作為限縮處罰範圍的門檻，然而在過了處罰範圍門檻後仍存在行為處罰嚴重性評價的各種問題，如刑法第 320 條普通竊盜罪與刑法第 321 條加重竊盜罪的關係一般，若行為該當於幾個要件，所受到的評價即會不同於單純侵害法益的行為，故本節仍一概須處理此些問題。

最後，就將行為入罪化的分類部分，本文採用前揭章節所歸納整理的電腦犯罪時間型分類來就各階段作是否入罪化的探討，亦即將行為依照時間的進程切割為「入侵行為」、「入侵後行為」、「入侵前行為」三類，並依序於以下探討。而就刑度的設定部分，因涉及立法技術部分，且社會上對於網路秩序安全的信賴是一相對於傳統法益來說的全新法益，故不能使用家族相似性作刑度的比擬，原則上本文應僅涉及構成要件的建議，而不就刑度的輕重作探討。但由於行為有輕有重，若僅以相對的「比較輕」或「比較重」來敘述，幾乎沒有任何實益，故在此仍必須要有一相對的標準，來具體化刑度的輕重，以體現罪責的輕重，並因此反映不法內涵的輕重。此一相對的標準，本文擬「借用」保護法益同是社會上對於網路秩序安全信賴的日本不正連線禁止法的處罰規定，亦即「不正連線(入侵)行為處以一年以下懲役(類似我國一年以下有期徒刑)或五十萬日圓以下罰金(類似我國五萬新台幣以下罰金[571])[572]」為基準，而就行為評價的不同再對刑度部分作輕重的調整，相較於空泛的指出輕重關係，有個刑度為基準應較為具體。此外，日本不正連線禁止法對於侵害社會上對於網路秩序安全信賴行為(不正連線行為)的評價，也可以給我國作參考，此種社會上對於網路秩序安全信賴法益大概「值多少錢」，對於刑度的拿捏上也可以有所依據。

第一項 入侵行為

[571] 在此考量日幣約為我國幣值的三分之一，且日本人的平均所得約為我國人的三倍以上，從而日本人消費一千日圓(約新台幣三百元)對其的感覺，約如我國國民消費三百日圓(約一百新台幣)對我國國民的感覺，故在此取大概的數值，即是三分之一日圓並換算台幣(再乘以三分之一)後的處罰金額。

[572] 參日本不正連線禁止法第 8 條第一款。

第一款 侵害行為之特定

所謂入侵行為，依照現行多數學說以及實務見解應解為「無權進入電腦」的行為，故前揭章節所討論的「有權進入」部分及不屬之。對於入侵行為所保護的具體法益內涵應是「社會上對於網路系統中登入控制機制完善運作的信賴」，登入控制機制是負責判斷網路系統中登入伺服器的使用者是否為特定人，判斷的方式目前大多是用帳號密碼的方式作判斷。故可能影響登入控制機制完善運作，進而使得社會上對於網路系統中登入控制機制完善運作失去信賴的行為，即是以各種方法破解或迴避登入控制機制、以及以其他手段「欺騙」登入控制機制的這些行為[573]。仔細觀察可以發現，我國妨害電腦使用罪章於入侵行為部分的規範，本已顯示出如此區分的端倪。破解登入控制機制的行為即類似於刑法第 358 條的破解使用電腦的保護措施構成要件行為，迴避登入控制機制行為即類似於刑法第 358 條的利用電腦系統之漏洞構成要件行為，欺騙登入控制機制行為即類似於刑法第 358 條的輸入他人帳號密碼構成要件行為，僅是第 358 條的構成要件規定非為顯現出該條的目的在於對登入控制機制完善運作的保護，故對於構成要件的敘述非常籠統，但是在侵害行為的劃分上則提供了本文思考的基礎方向。同時，若依照本文前述的分類方式，此三種行為皆屬「強行進入」，蓋會在網路系統上設置登入控制機制者，即表示對於該些伺服器已作了防護機制，對於防護機制動各種手腳而進入的行為，本即是一種強行進入的行為。如此一來，「竊入」的行為態樣應僅限於無權進入未設置登入控制機制伺服器的情形，然而縱使無權進入，此種進入仍不會損及社會上對於網路系統中登入控制機制完善運作的信賴[574]，故以下即排除竊入行為的可罰性，僅對於此三類強行進入的行為態樣，作構成要件規制的分析討論。

第二款 構成要件規制之設定

---

[573] 須注意者是，入侵行為並非是後續行為的預備犯，其所保護的是「社會上對於登入控制機制完善運作的信賴」這個獨立法益內涵。參加藤敏幸，不正アクセス，刑法雜誌 41 卷 1 号，2001 年 7 月，頁 81。

[574] 雖可能會侵害該伺服器相關權利人的使用空間支配性，但即非在此所要規制的情形。

在構成要件的規制上，首要討論的問題即是就保護法益範圍的限縮處罰。既本罪的保護法益具體內涵為「社會上對於網路系統中登入控制機制完善運作的信賴」，在構成要件行為的判斷上，不能僅因該行為是一個破解、迴避或欺騙登入控制機制的行為，即認定該些行為皆必須納入處罰範圍，反而縱使未破解、迴避或欺騙登入控制機制，而可能造成社會上對於網路系統中登入控制機制的完善運作不信賴[575]時，應認定該行為必須納入處罰範圍，故在此即要依照保護法益的範圍而劃分處罰的界線。此種界線的劃分，本文認為可以參考危險犯中所出現的「足以生損害於公眾或他人」要件來做標準，將本罪定位成一個「適性犯[576]」的概念，不致使處罰範圍如抽象危險犯般過度擴張，亦不會與刑法第 359 條或第 360 條一般因需要「致生損害」的具體危險要素而使得犯罪的成立過於困難。在「足以生損害於公眾或他人」此一要件的判斷上，所要判斷的具體要素即是「是否造成社會上對於網路系統中登入控制機制完善運作的不信賴」，因「足生損害」的該「損害」，從保護法益的觀點出發，即是因保護法益的被侵害推導出可以將行為給予足以使公眾或他人造成損害的評價，進而成立本罪。

再者，於「足以…」要件之前的構成要件行為態樣部分，有鑑於前揭章節對於限制特定行為此一作法的批評，在此擬以概括規定的方式規定行為態樣為「破解、迴避電腦網路的登入控制機制，或輸入他人帳號密碼等使電腦網路的登入控制機制無法有效運作的其他相類行為」，一方面以此些行為態樣為例來顯示入罪行為的嚴重程度，另一方面亦開放概括條款來因應未來可能出現的新型態電腦網路使用關係。同時，由於本罪是要保護社會上對於網路秩序安全的信賴關係，從而於構成要件行為的設定上，亦要限制入侵行為必須要以「透過通訊線路」的方式為之，在此所謂通訊線路，即包含有線或無線的任何網路傳輸型態，故縱使行為人透過無線網路入侵他人電腦，仍然會該當本罪。此外，就行為的「結果[577]」部分，亦有必須討論的空間。雖此種行為在分類上以及稱呼上多數論者甚至本文

[575] 雖然很難想像此種情形。

[576] 關於適性犯的探討，可參考蔡蕙芳，危險概念與各種犯罪類型－「足以」要件危險犯之討論，發表於「2006 年刑法分則共同議題之探討」研討會，2006 年 5 月，頁 1 以下。

[577] 在此並非指構成要件結果，蓋本罪的性質是行為犯，在此的結果是指因果上的結果。例如「拿起杯子」的因果上結果是「杯子被拿起了」。

皆以「入侵行為」為稱呼，但於本罪中此種行為的結果並非「電腦被入侵」，而是「登入控制機制無法正常運作」[578]，僅是往往在登入控制機制無法正常運作後，行為人進而侵入電腦而已。據此，於構成要件上不能設置「而入侵他人電腦」此種「結果」性規定[579]。

最後是有關未遂犯的規定，由於本罪若僅處罰既遂行為，對於未遂行為並未處罰。雖前揭章節有論者以社會觀感以及共犯處罰的角度來論述未遂行為處罰的必要性[580]，但一來個人資料保護法與本罪所保護的對象本不相同，二來此種行為在未遂階段可能涵蓋到尚且無法判斷是否足以生損害於公眾或他人行為的部分[581]，若規定未遂犯很可能會因牽連過廣而與要維護資訊科技發展空間的權衡理念相違背，從而在此為限縮處罰，本文仍認為無庸規定未遂犯。須特別說明的是，同前述「結果(行為完成)」的部分，在此的未遂行為應是指「已著手開始嘗試癱瘓登入控制機制，但未癱瘓成功」而言，並非指「已著手開始嘗試癱瘓登入控制機制，且已癱瘓登入控制機制，但未入侵成功」的情形。

第三款 刑度之設定

於刑度的設定上，雖然日本不正連線禁止法所規範的行為態樣中，並不包含迴避登入控制機制的行為態樣[582]，然而就「登入控制機制無法完善運作」的角度出發，無論是迴避、破解或欺騙登入控制機制，皆會使得登入控制機制無法完善

---

[578] 有見解認為依照刑法第 358 條的文義解釋，若僅無故輸入他人帳號密碼、破解使用電腦保護措施、或利用電腦系統漏洞，而未侵入他人電腦時，仍不會成立本條之罪。參蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月，頁 125-126。

[579] 但若從保護使用空間支配性的角度，則結果應以「他人使用空間的支配被破壞(電腦被入侵)」為必要，與本罪的規定範圍完全不同。

[580] 蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月，頁 127；李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 252-253。

[581] 例如在登入控制機制的帳號密碼欄中胡亂輸入一些數據，嘗試尋找該控制機制漏洞的行為，若最後未找出該機制的漏洞，不但未使得社會上對於登入控制機制正常運作的信賴受到損害，反而更加建立社會上對於登入控制機制安全性的信賴。

[582] 在此的迴避是指，該電腦設有登入控制機制，然而該登入控制機制卻因設計者的過失或其他因素未全面對各種登入手段作控制，行為人利用此種空檔而以其他登入方式登入該電腦而言。該登入控制機制未被破解，行為人仍處於得以隨時進入他人電腦的狀態，此種結果亦屬於登入控制機制無法完善運作的一種。

運作，其中迴避與破解行為皆得以加強登入控制機制系統安全性的方式來降低可能發生的情形，然就欺騙登入控制機制的情況，並無法以上述方式來降低發生可能性[583]。而日本不正連線禁止法將欺騙行為與破解行為以相同的刑度規範，故在此就迴避行為看來亦應以相同刑度規範即可。

又，雖日本不正連線禁止法相較於本法的處罰範圍較廣，但該法的處罰範圍過廣本是其施行後所遭到的批評之一[584]，故若從保護法益相同的角度看來，在此給予相同的刑度或許才是正確的作法。據此，也基於本罪是整個妨害網路秩序罪的規制重點及基礎，同時考量到日本不正連線禁止法修正後增加對不正連線行為的刑度，但一來我國社會的資訊化程度不如日本，二來刑度增加的修正時日尚淺，可謂未有足夠時間經過實務上檢驗是否合於罪刑相當原則，故在此本文較保守的參考日本不正連線禁止舊法的刑度，論以一年以下有期徒刑、拘役、科或併科五萬元以下罰金的刑度。

第二項 入侵後行為

第一款 侵害行為之特定

於入侵後行為的部分，因涉及較多的面向，故以下即就各種面向分別討論。首先是與電磁紀錄的變更、毀損、取得等相關行為的部分，其所保護的具體法益內涵應是「社會上對於電腦與網路系統中電磁紀錄儲存安全性的信賴」，蓋在使用網路系統的同時，人們所擔心的即是是否會因身處不安全的網路秩序，而使得自己所信賴，儲存在電腦網路系統中的資訊遭到破壞、取得或窺視[585]。因此在保障社會上對於網路秩序安全的信賴下，亦必須保障社會上對於電磁紀錄儲存正確

---

[583] 園田寿，不正アクセス，法学教室 228 号，1999 年 9 月，頁 45；李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月，頁 251。

[584] 日本弁護士連合会，警察廳の「不正アクセス対策法の基本的考え方」及び郵政省の「電氣通信システムに対する不正アクセス対策法制の在り方について」に關するパブリックコメント公募に対する意見，自由と正義 50 巻 8 号，1999 年 8 月，頁 50；加藤敏幸，不正アクセス，刑法雜誌 41 巻 1 号，2001 年 7 月，頁 82-83。

[585] 此亦為採取使用空間支配說的論者所著眼的地方。

性的信賴。又，對於「儲存於電腦系統中」的「儲存媒體」部分，應解為「包含行為當時的所有已接續的儲存媒體」，除了接續在主機內的 HDD 或 SSD 硬碟外，舉凡 3.5 吋磁碟片、可複寫的 CD 或 DVD 或 BD 光碟片、以 USB 接頭隨插即用的隨身碟或具隨身碟功能的 MP3 播放器、甚至外接式硬碟等，只要是在行為當時已接續在電腦上者皆屬之[586]。再者，就「動手腳」的部分，即如前述分類方式，區分為變更電磁紀錄的排序以及取得電磁紀錄二種類，變更電磁紀錄的部分意指對電磁紀錄的磁性配列方式作變更[587]，包含將其刪除以及將其變更兩種類；而取得電磁紀錄即不涉及原電磁紀錄磁性配列方式的變更，僅是單純將原有電磁紀錄的磁性配列方式複製到其他載體而已。若以現行刑法第 359 條來比喻，變更電磁紀錄的種類即類似「無故刪除、變更他人電腦或相關設備之電磁紀錄」的構成要件，而取得電磁紀錄的種類即類似「無故取得他人電腦或相關設備之電磁紀錄」的構成要件。

再來必須要討論者，即是關於使電腦運作機能受減損或直接喪失的行為部分，其所保護的具體法益內涵應是「社會上對於電腦與網路系統中電腦機能完善運作的信賴」，在使用網路系統時，除擔心所儲存的電磁紀錄是否安全外，人們亦會擔心是否會因身處不安全的網路秩序，使得自己所信賴並使用的電腦網路系統本身運作效能遭到影響。因此在保障社會上對於網路秩序安全的信賴下，亦必須保障社會上對於電腦機能完善運作的信賴。故行為人雖未涉及電磁紀錄的變更或取得，但卻利用惡意程式甚至以手動[588]等方式降低電腦運作的效能，仍然應考慮由刑法規制。若以現行刑法第 360 條來比喻，此種行為即屬於「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備」的構成要件行為。

同時，雖行為人未對電磁紀錄為變更或取得，而僅單純窺視電腦內資訊的行為，亦可能破壞社會上對於網路秩序安全的信賴感。此種單純窺視部分所保護的

---

[586] 此種結論亦可以用「最寬鬆的電腦概念」得出，電腦具有輸入、運算、儲存、輸出的要素，故只要具有此四種要素，並具解譯並執行程式命令功能電子裝置都叫做電腦，故就儲存媒體而言，縱使儲存媒體是透過外接或是臨時儲存的方式為之，該電子裝置在該當下仍具有儲存功能。

[587] 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 237-238，註 4 處。

[588] 雖然很難想像行為人會選擇以手動方式來干擾電腦運作。

具體法益內涵應是「社會上對於電腦與網路系統中電腦內部資訊私密性的信賴」，在使用網路系統時，人們會擔心是否會因身處不安全的網路秩序，使得自己所信賴的電腦網路系統中的電腦內部資訊暴露在他人的眼中。從而在保障社會上對於網路秩序安全的信賴下，亦必須保障社會上對於電腦內部資訊私密性的信賴。雖現行刑法並未對此為保護，但此種行為亦透過前述論證具有應保護的社會生活共同利益，從而似應納入侵害行為的一種中，但此種行為態樣所侵害的法益著實輕微，也許可以考慮僅以行政法處罰即可。

最後要再次提及的是，要對於儲存於電腦系統中的電磁紀錄為變更或取得、影響電腦機能運作，以及單純窺視等行為，必以進入電腦此一行為為前提[589]。並且此種進入行為，依照保護法益的範圍來看，雖可能是「有權進入」的行為[590]，但不能是以「未透過通訊線路」方式進入的行為，由於以未通過通訊線路的方式的進入行為，本不涉及網路秩序的問題，故在此並非本罪要規制的對象。據此，以變更電磁紀錄的行為態樣為例，對於借用他人單機電腦使用時，將對方電腦內的資料一掃而空的行為，應不在本罪處罰範圍內；反倒是透過網路以合法授權的方式連線到對方的電腦時，趁機將對方電腦正以 USB 接頭所接續的 USB 隨身碟內的資料一掃而空的行為，應在本罪處罰範圍內。

此外，就前揭章節的分類中，亦含有軟硬體破壞此一類型，然而就軟體部分而言，軟體即是程式，而程式即屬於電磁紀錄的一種，故對於軟體的破壞部分已歸納在前述變更電磁紀錄的種類中。而硬體部分的破壞，極難想像如何透過通訊線路入侵電腦後對於硬體作破壞，可能想的到的方式中，大概僅有「發送大量封包使得電腦運算過熱而降低使用壽命」的情形，然而此種過度使用的部分除可以涵蓋在前述降低效能或使功能喪失的部分外，硬體設備因不斷使用而降低使用壽命的部分，由於電腦硬體設備在今日已屬普及，並無特別保護必要，從而以傳統刑法的毀損罪來規範即已足夠，故在此未將此種類型作獨立區分。

---

589 畢竟此類別即稱為「入侵後行為」，若未進入(入侵)則不會規範於此類別中。

590 雖「有權進入」並非「入侵」，然而此種分類是「電腦犯罪」的分類，若依照使用空間支配說的論者，有權進入後作變更或取得電磁紀錄等行為，在變更或取得行為著手的瞬間，其即認為同時該當入侵行為，故在此仍然使用「入侵後行為」的用語。

第二款 構成要件規制之設定

在構成要件的規制上，由於此行為在絕大多數情形皆會與入侵行為同時發生，亦即行為人意圖變更或取得儲存於電腦系統中的電磁紀錄、減損電腦運作效能或單純窺視而入侵該電腦並實現其不法意圖，而對於此種意圖為該些行為而入侵電腦後並實現其意圖的部分，應更屬於刑法應保護的範圍，從而於該類行為的規制中，會以較特殊的規制模式於下述章節呈現，在此以及下款刑度設定的部分，即聚焦於非於該情形的情況下進入電腦後，在未授權的情況下為此類行為的情形作探討，合先敘明。

首先必須處理的是變更或取得電磁紀錄的部分，是否要將變更以及取得皆並列在同一個構成要件內為處罰。因現行法將變更(含刪除)、取得置於同一構成要件下論處，即遭到論者以「會造成規範中出現各種不同行為型態，並且各行為型態間無必然性前置關係或同類性關係，會違反罪刑法定原則下的構成要件明確性原則」為理由大力批評[591]。或許此種批評在依據個人法益保護的使用空間支配說建立罪章時是必須要參考的，但在此所保護者為社會上對於電腦與網路系統中電磁紀錄儲存安全性的信賴，無論是將電磁紀錄變更或取得，皆會破壞此種信賴關係，應可認為具有同類性關係，至於依照行為型態的不同可能造成損害範圍相異的部分，應僅是破壞信賴關係實際損害上的問題而已，並不會影響被破壞的信賴程度，故本文仍主張將此變更與取得行為規範於同一條內。

其次要處理電腦運作機能受減損或直接喪失的行為部分，與此種行為態樣作比擬的刑法第 360 條，本有受到「干擾」一詞定義不明確的批評，故本文於構成要件的制定上，不使用較具爭議的「干擾」一詞作規範，而依照具體保護法益的「減損電腦運作效能」作為構成要件行為規範。又，刑法第 360 條對於行為的方式限定於「以電腦程式或其他電磁方式」，本文認為若確認此種行為必須要透過

[591] 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 127。

網路為前提時，其所有可能的「干擾」方式一定是透過「電磁方式」[592]，故沒有必要重覆對於構成要件的行為方式作規定，同時也能避免「其他電磁方式」可能產生的其他解釋方式而造成處罰範圍的不當擴張[593]。同時，雖謂在雲端運算來臨後，對於電腦效能的減損可能會因為雲端硬體的無限擴充性而失去處罰必要，並對於此種社會上對於網路秩序安全信賴的具體信賴法益，亦可能隨著時代而失去適用的可能性，但此種行為在目前仍有可能發生，且現代社會仍信賴此種情形不會因為使用網路而發生，故對於此種破壞信賴的行為仍有規制必要。

再者要處理者即為單純窺視的部分，此種行為因刑法並無處罰規定，故在構成要件的設置上即無從參考。然而「窺視」是現實社會上的用語，於電腦世界中應為「瀏覽電腦內部資訊」的行為，故應以此作為構成要件行為規範。

最後所必須處理者，即是此三種類型的行為皆會出現的問題。第一，處罰此三類行為的前提，是此三類行為皆是以「非屬意圖入侵的情形而進入電腦，並在未授權的情況下為該些行為」的方式違犯；第二，此種「進入電腦」的方式亦必須透過通訊線路為之，以緊扣保護法益的範圍。從而在構成要件的規制中皆必須加上「對於前條以外透過通訊線路而連線的電腦」以及「無故(未經授權)」的構成要件要素，以解釋諸如「將他人滑鼠或鍵盤拿走是否為一種干擾行為」等疑問。第三，如同前述入侵行為一般，為了不使刑罰過度擴張，亦要設置「足以生損害於公眾或他人」此一限縮要件來限定處罰範圍，以切合信賴法益的保護範圍。

第三款 刑度之設定

就以上三種行為類型的刑度設定上，首先就單純窺視的部分，因只要一進入電腦，無論是對於電磁紀錄的變更或取得，或是影響電腦運作效能的行為，甚至不作任何事，皆會包含窺視的行為，再加上窺視行為所侵害的法益非常輕微已如前述，故對於窺視行為的處罰，於刑度部分應會遠低於其他二者。再來是於影響

[592] 縱使是用雙手操控滑鼠一個封包一個封包寄送，亦是透過「通訊線路」此種電磁方式來干擾。

[593] 例如在加護病房旁撥打行動電話，使得人工心肺機產生雜訊的行為，因行動電話亦會放出電磁波，故亦該當干擾電腦的解釋方式，參張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月，頁 97。

電腦效能的部分與變更或取得電磁紀錄的部分的刑度輕重問題，變更或取得電磁紀錄所涉及者為電磁紀錄本身的安全性問題，電磁紀錄本身的安全則有賴電磁紀錄儲存管理機制來維持，此種資訊儲存管理機制的正確運行，相較於電腦本身運作效能的完整來說，應更需要仰賴人與人之間的信賴關係支撐。故在兩相比較之下，應認為影響電腦效能的部分的刑度應較變更或取得電磁紀錄的部分為輕。

又，關於刑度最重的變更或取得電磁紀錄部分該如何評價，本文認為因變更或取得電磁紀錄的行為所侵害者為社會上對於電腦與網路系統中電磁紀錄儲存安全性的信賴，此種信賴從大方向上觀察亦是對於一種對於「(電磁紀錄儲存管理機制的)正確性」的信賴，與社會上對於網路系統中登入控制機制完善運作的信賴應同是「正確性」的信賴，故似應給予相同的評價。從而，對於電磁紀錄的變更或取得，應處以一年以下有期徒刑、拘役、科或併科五萬元以下罰金的刑度。在得出電磁紀錄的變更或取得行為的刑度後，亦可以比擬出影響電腦效能的行為以及單純窺視行為的刑度，影響電腦效能的行為處罰，約是電磁紀錄的變更或取得行為的二分之一，即是六月以下有期徒刑、拘役、科或併科三萬元以下罰金的刑度；而單純窺視行為的處罰，更是影響電腦效能的行為的三分之一，即是拘役、科或併科一萬元以下罰金。

第三項 入侵前行為

第一款 侵害行為之特定

電腦犯罪與傳統犯罪的差別之一，即在於電腦犯罪具有專業性的特質[594]，並且電腦犯罪是對於電腦程式的對抗行為，亦非僅透過肉身即可違犯，故在入侵行為發生的時點之前，行為人多會作一些「準備」，而在此時點上的各種行為即是「入侵前行為」部分所要規制者。然而此些行為多種多樣，並且包山包海，何種行為始有規制的必要即是件難事。若參考我國刑法與日本不正連線禁止法的規定，

[594] 盧文祥，電腦犯罪之研究，憲政時代第 13 卷 4 期，1988 年 4 月，頁 63。

似乎可以找出一些端倪，就我國刑法的部分，於入侵階段前的規制，僅有製作並使用犯罪電腦程式的行為必須要處罰，且細部又分為「自己製作自己使用」與「自己製作他人使用」兩部分，而有害程式的使用會有效的促進使用者犯罪成功的可能性，而製作程式並提供於他人甚至不特定多數人者即造就了絕大多數犯罪成功的可能，就此可以發現有害程式的製作或使用似乎是一個必須規制的重點；而就日本不正連線禁止法的部分，於第 9 條中對於將他人的帳號密碼公開或告知第三人者會處以三十萬日圓以下罰金，就此種告知或公開帳號密碼的行為，由於輸入帳號密碼而進入伺服器的行為，無法透過安全系統的更加完備來減少犯罪成功的可能性已如前述，並且此種帳號密碼系統的設置目的即是為了要快速且方便的判斷是否為當事人，若得到該人的帳號密碼，即意味著能破除一切的登入控制機制，故對於將他人帳號密碼告知第三人或公開的行為，無疑大幅增加了輸入他人帳號密碼而入侵電腦行為的成功率，故在此亦有規制的必要。

然而，問題即會發生在保護法益上面，就製作或使用惡意程式的行為，似乎仍可以認為其所侵害的法益為「社會上對於網路安全秩序的信賴」，由於所謂惡意程式即是強調其具有擾亂現行網路運作秩序功能的程式，若使用或製作，的確對於網路秩序安全有所威脅，進而會動搖社會上的信賴。惟就將他人的帳號密碼公開或告知第三人的行為，其所侵害的法益是否為社會上對於網路安全秩序的信賴即有疑義，蓋帳號與密碼的建立，往往是帳號密碼持有人自行設定，且僅有持有人、該服務的管理人[595]、持有人授權得知者可能得知，此三類人以外者要得知持有人的帳號密碼，除純粹猜測得知，與使用各種如入侵電腦、設置病毒或偷看等方式探知的方式外，僅剩下由該三類人告知的方式。先不論以強暴脅迫等方式迫使該三類人告知的強盜得利情形，其中持有人的告知本即有授權的意味，但就在持有人外的後兩類人告知的情形上即出現疑義。服務管理人與被授權得知帳號密碼者皆有共同的特性—若未受到得將帳號密碼告知第三人的授權時，負有保密的義務，並僅能在授權人授權底下使用此些帳號密碼。而由於帳號密碼的私密性與安全性即如同鑰匙一般，應可推知在持有人未明示得告知第三人此些資訊時，推定持有人未為授權。故原則上服務管理人與被授權得知帳號密碼者對於帳號密

[595] 在金融方面即是銀行，在網路遊戲方面即是遊戲公司。

碼持有人負有一種保密義務，此種保密義務與妨害秘密罪章所保護的秘密法益應較為類似，若行為人將帳號密碼告知第三人或公開時，所侵害的並非是社會上對於網路安全秩序的信賴，而是帳號密碼持有人對於該行為人的信賴。同理，在該行為人未告知他人，但卻在授權時段外仍輸入該帳號密碼而進入伺服器的情形，所侵害的亦僅是帳號密碼持有人對於該行為人的信賴，而非社會上對於整個網路安全秩序運作的信賴。可是，在維護網路安全秩序運作的前提下，必須適度保障運用帳號密碼來辨認身分的此種登入控制機制，在此固然會涉及與洩漏秘密或背信行為相似等問題，然若著眼於帳號密碼機制中只要一得知帳號密碼即可破除所有安全措施的脆弱面，以及帳號密碼在此是與惡意程式類似的「促進犯罪成功率的工具」等面向，則可認為若認為製作散布並使用惡意程式的行為要受到規制，對於散布並使用帳號密碼的行為亦應受到規制。於使用帳號密碼部分於入侵行為已有規範，而散布帳號密碼的行為在此即可認為會侵害社會上對於整個網路安全秩序運作的信賴，而有規制的必要性。

第二款 構成要件規制之設定

於構成要件規制部分，首先要處理的問題即是與入侵行為的預備犯與幫助犯問題。首先是問題較小的幫助犯，前述如告知第三人他人帳號密碼以及給予他人惡意程式等行為，的確於某一部份的情況下應論以入侵行為的幫助犯。故在此所要規定者，即是去除入侵行為幫助犯的部分，亦即行為人並未具備幫助故意以及既遂故意的情形，始有特別設置處罰的必要[596]。

再者是對問題較大的預備犯而言，於前揭章節對於我國刑法第 362 條現今所受批評部分已有提及，多數論者皆將該條定位為刑法第 358、359、360 條的實質預備犯，並進而產生在該些犯罪皆未處罰未遂犯時，獨立處罰實質預備犯可能違反罪刑法定原則的疑慮[597]。本文認為，未處罰未遂行為即處罰預備行為會產生違

[596] 不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月，頁 87-89。

[597] 盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 752-753；鄭逸哲，吹口哨壯膽–評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月，頁 113；林

背罪刑法定原則的疑慮誠屬當然，然此些行為是否皆為預備行為卻有疑義，其中部分行為因本身即會破壞社會上對於網路安全秩序信賴，從而具有處罰的必要性，故該些行為本身應具有獨立保護法益，並非與入侵行為處於著手與預備的關係，故其並非是實質預備犯的地位，而應是正犯的地位。據此，在前述某些侵害行為的處罰上，即應緊扣此一原則來設計構成要件，將屬於預備行為的部分給排除於處罰範圍之外。

接著即是要處理惡意程式以及散布帳號密碼此二種行為態樣的構成要件規制問題。於惡意程式的部分，首先必須對於惡意程式作定義，畢竟如論者所批評，程式皆含有各種不同功能，要如何定義惡意程式實有困難[598]。本文認為每個程式皆有被拿來惡用的可能，要以構成要件區別是否屬惡意程式極為困難，不如朝著「將一個程式的惡意面作表彰」的方向作思考，若該程式具備多種用途，而僅利用該程式得以入侵他人電腦的用途來入侵電腦，在此該程式即為惡意程式。再者才是所處罰行為的問題，雖現行法是處罰製作並使用的行為，並且從立法理由可以觀察出立法者本想處罰的行為應是製作行為，而其他構成要件僅是限縮處罰範圍而已[599]。惟真正會造成侵害行為較容易成功的，應是使用或散布該些程式之人才是，同時惡意程式亦屬於一種程式，程式的撰寫本有助於資訊科技的發展，基於不能以刑法限制資訊科技發展的立場，對於程式的撰寫本身原則上無處罰必要性，而應將處罰重點放置於惡意程式的使用或散布[600]。在使用惡意程式入侵他人電腦時，無疑增加了入侵行為的成功率，相較於未使用惡意程式的情形對於網路安全秩序的威脅更加嚴重，在此應考慮以如竊盜罪與加重竊盜罪或洩漏秘密罪與加重洩漏秘密罪的關係一般，是一入侵電腦行為的加重要素，而以「利用特定電腦程式所具備之破解、迴避電腦網路登入控制機制或其他使電腦網路的登入控制機制無法有效運作之功能而犯之者」的構成要件規定在入侵行為的部分；於散布

冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月，頁 107；柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月，頁 128。

598 黃仲夫，刑法精義，修訂廿六版，元照出版有限公司，2010 年 8 月，頁 767；盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 751。

599 中華民國刑法第 362 條立法理由第二點。

600 同時程式的撰寫本身於現行法即可能被認為是入侵行為的預備行為，在此一併解決預備犯與罪刑法定原則的問題。

惡意程式部分，因惡意程式的無法定義，故僅有在如同刑法第 292 條公然介紹墮胎罪般，在「介紹特定電腦程式的犯罪功能並主動散布」的情形，始能處罰該行為人。不過有些電腦程式可能非常普及以致於無庸散布，行為人僅需介紹該犯罪功能並「強烈建議」社會大眾可以使用此方法犯罪，即可達到散布的目的，並且所造成的效果相較於介紹並散布的行為態樣而言更強，在此似亦有規制必要，惟此種行為本即可被現行刑法第 153 條的射程範圍涵蓋，故於此不另為規定。

至於散布帳號密碼的部分，在此即參考日本不正連線禁止法，在「無故公開他人的帳號密碼及該帳號密碼所利用之電腦，或依知該帳號密碼所利用電腦之第三人之請求而告知」時，始有處罰必要。不過由於不正連線禁止法本身含有大量的行政法色彩，處罰的範圍較廣，與我國國情不盡相同，故在此應限於「足生損害於公眾或他人」，亦即此種公開或告知第三人的情形足以使社會上對於使用帳號密碼的登入控制機制的信賴崩毀的情形下，始需要以刑法處罰公開帳號或告知第三人的行為[601]。

第三款 刑度之設定

在刑度的設定上，以惡意程式入侵電腦的行為，因不法內涵相較於未以惡意程式入侵電腦的行為為重，故在刑度上應考慮對此類行為的加重處罰[602]。散布惡意程式或他人帳號密碼行為的部分，雖散布他人密碼會造成帳號密碼持有人在使用該帳號密碼作為登入控制機制的部分完全被「破解」，相較於散布惡意程式對於入侵行為的成功率提升有較大的深度，但散布惡意程式卻相較於他人密碼僅能「破解」一個登入控制機制，具有對於各種登入控制機制皆可能危害的廣度，二者可謂互有長短，並由於二者皆是「增加入侵行為的成功率」的行為，就此角度出發似論以相同刑度即足。而就散布他人密碼部分的刑度即有日本不正連線禁止

[601] 於告知第三人的部分雖有極大部分是會構成該第三人的幫助犯，但就保障運用帳號密碼來辨認身分的此種登入控制機制的角度而言，該告知行為亦是一個會加速此種制度崩潰的源頭，故在此無論是否會成立幫助犯(若該第三人得知後並未為犯罪行為的情形)，皆有處罰必要。參不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月，頁 88-89。

[602] 但此種行為因牽涉到規制設計上的問題，故量刑部分於後述章節處理。

法得以參考，，故對於散布惡意程式與散布他人密碼皆參考自該法第 13 條，處以三萬元以下罰金的刑度[603]。

第三節　建構妨害網路秩序罪章模型

在釐清所有應處罰的犯罪類型後，在本節所必須呈現的，即是一個完整而有體系的妨害網路秩序罪專章。要建構一個罪章的必要條件，除前揭章節所述的獨立保護法益以及入罪化行為的規制外，還包括各條文呈現的處罰架構。畢竟就妨害網路秩序的行為評價部分仍然有輕有重，此時的處理究竟是如同現行法般制定一個極高的刑度上限，並給予執法者依照個案裁量的空間，或是否可以思考從行為的態樣再進行更細緻的區分，將不法內涵較大的行為作有效的處罰，而就不法內涵較小的行為給予較低的刑度上限，以彰顯法益的破壞程度。但要在罪章內呈現如此的區分，作為前提的要件即是要區分何謂「不法內涵較大」的行為。在確定不法內涵較大的行為後，始能進一步思考該如何在罪章中區分出不法內涵較大的行為並給予適當的處罰。據此，於以下即分為「確認重點規制行為」以及「設計規制模型」兩大部分，並依序探討之。

第一項 確認重點規制行為

在確認重點規制行為的部分，必須要注意到的一點是，在時間型的分類上，每個時間階段的行為可能是一連串的，只是在規制上依時間進程的方式作切割，從而對於此種「一連串」的犯罪流程，理論上相較於單純違犯其中一個時間進程中的情形更應該給予規制。據此，在時間進程中「理想」的犯罪流程，應是行為人意圖變更取得電磁紀錄、降低電腦運作效能或僅單純窺視，而使用惡意程式透過網路入侵電腦後，再進而實現其意圖的流程。此種流程侵害社會上對網路秩序安全信賴法益的程度，應是所有犯罪流程中最大的，故刑法應極力防止此類行為的發生，列為最主要的重點規制行為。其次，若前述理想的犯罪流程中欠缺了其

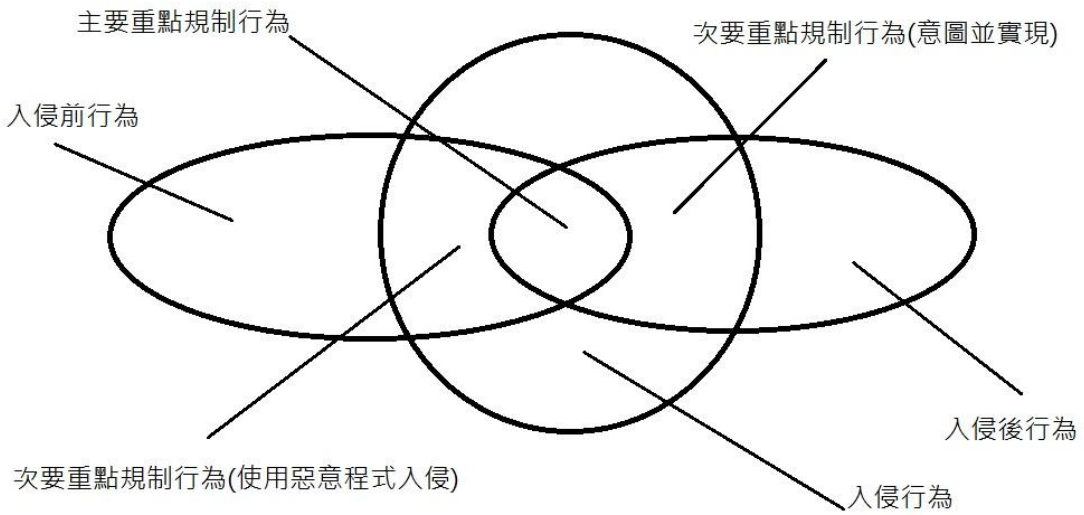
[603] 不正連線禁止法第 13 條的刑度本是三十萬日圓的罰金，經過換算後約為新台幣三萬元。

中一個要素，例如行為人使用惡意程式透過網路入侵電腦後，另行起意變更取得電磁紀錄、降低電腦運作效能或單純窺視，以及行為人意圖變更取得電磁紀錄、降低電腦運作效能或僅單純窺視，但未使用惡意程式透過網路入侵電腦後，再進而實現其意圖等情形，此種流程侵害社會上對網路秩序安全信賴法益的程度雖不若第一種流程，但是仍相較於單純入侵或單純有權進入後變更取得電磁紀錄、降低電腦運作效能或單純窺視的情形，故在此應列為次要的重點規制行為。若再度將前述次要重點規制行為拿掉一個要素，即會發現以一般刑法上的理論(如競合論等)即可給予妥適評價，無列為第三重點規制行為的必要。

在確認過主要與次要的重點規制行為後，剩餘的行為則單獨依照前述的規制運作即足，而此二種重點規制行為，或許也就是我國立法當時真正所欲以重刑規制的「重大電腦犯罪」類型，並且其對於法益的侵害著實較剩餘行為大，故在對此些行為的論處上，僅單純使用刑法總則中的理論並不足以評價，應思考並設計較特殊的方式來做規制。據此，以下即是對於為了有效劃分處罰重點規制行為與其他行為，而設計一個規制的體制來架構妨害網路秩序罪。

第二項 設計規制模型

在規制體系的設置上，首先即要設法區分主要以及次要重點規制行為與其他行為所不同的特徵點，並就該特徵點作區分。如同前述在確認重點規制行為時所思考的脈絡一般，主要的重點規制行為與其他行為最大的不同點在於兩個要素—「不法意圖並實現」和「惡意程式的使用」。在確認主要行為的不同點後，亦可以得知次要的重點規制行為與其他行為的不同點，即是「不法意圖並實現」和「惡意程式的使用」二者的其中之一。其中不法意圖並實現的部分與入侵後行為會出現部分的重疊，而惡意程式的使用部分則會與入侵前行為有相關，重點規制行為與前述的行為分類上的關係，即如下圖所示。



綜上所述，可以發現若對於「不法意圖並實現」和「惡意程式的使用」此兩個要素作規制上的設計，整體上無論是對於主要重點規制行為或次要重點規制行為都能有效區分，故以下即要討論如何規範此兩個要素，始能有效篩選出重點規制行為並處罰。首先是對於不法意圖並實現的部分，於競合論上本即應依照「不完全的多行為犯」來解決，亦即行為人雖該當了兩個不同的構成要件，但因其主觀上僅出於同一意圖，故應將其整體僅作一個評價[604]。但此種不完全的多行為犯所出現的形式，多是後行為的不法內涵重於前行為，或對於法益的侵害重點在於後行為的情形[605]，然而在此正好相反，對於社會信賴破壞的規制重點應是以入侵行為為主，其後的入侵後行為本僅是加重信賴破壞的程度而已，亦即相較於偽造並行使文書的情形，應更接近於擄人勒贖的情形。擄人勒贖本身含有擄人與勒贖的兩大部分，且擄人與勒贖之間具有意圖並實現的關係，又依照法條文義、實務見解以及多數學說見解，本罪的成立僅要「意圖勒贖而擄人」即足，並不以勒贖行為為必要[606]，故可以認為擄人行為才是侵害法益的重點，其後的勒贖行為僅是

[604] 亦有稱「意圖犯之前、後實現行為」者，參林鈺雄，新刑法總則，三版，元照出版有限公司，2011 年 9 月，頁 585。
[605] 如意圖行使而偽造文書，而其後行使的情形。
[606] 盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月，頁 712。

法益侵害程度的加重而已[607]。此外，擄人勒贖行為同時也是「妨害自由」與「恐嚇取財」行為的實質結合[608]，屬於結合犯的一種，並從刑度遠重於前述二罪看來，本罪的出現即是在刑事政策上基於對於此類行為的特別規制，因縱使將妨害自由與恐嚇取財的行為數罪併罰，其刑度仍不足以評價擄人勒贖的行為，故設計特別加重的結合犯規定論處。然而，擄人勒贖罪並無更加重處罰實現意圖的行為，是與本文所述應處罰侵入後實現意圖的情形不同之處，但縱使如此仍不表示即沒有考慮設置處罰實現意圖行為規範的空間[609]。

據此，對於意圖並實現的部分可以朝兩個方向考慮規制的設計，其中一個方向即是設置(實質或形式)結合犯的方式，將此種行為整體作加重的特別規制，另一種即是對於意圖為入侵後行為的入侵行為加重處罰，並利用競合理論不另處罰實現意圖的入侵後行為。此二種方法從處罰入侵後行為與否的部分看似互斥，但仍有共存的可能，第二種規制模式中具有不法意圖的入侵行為加重處罰的理由，應是該入侵行為不僅是單純使登入控制機制無法正常運作而已，並必然會更進一步就社會上對於電磁紀錄、電腦系統效能以及電腦內部資訊的私密等信賴關係為侵害，相較於一般的入侵行為對於法益侵害可能性的程度更大。惟此種加重處罰的程度是否能大到涵蓋對於意圖行為的實現亦有包含即是問題所在。在傳統刑法因不法意圖而加重的規定中，無論是擄人勒贖罪、公然猥褻罪或刑法第 233 條媒介幼童性交猥褻罪，皆未對實現意圖的行為作更進一步的加重，故似可就此認為若刑法上以意圖犯的方式作為加重處罰的要素時，於量刑的考量上往往已涵蓋實現意圖的部分。不過，就設置結合犯的法理觀察，無論是形式或實質結合犯，會設置結合犯的規定即是因為對於特定二罪名的違犯特別嚴重，基於刑事政策的考量必須要論以更重的刑度而言[610]。而既是因刑事政策的考量，對此種「特定二罪名」的認定上，應不會就該二罪名是否有意圖與其實現的關係而為不同判斷，故

---

607 同時從刑法第 347 條第五項未經取贖而釋放被害人必減其刑的部分，亦可以得出此結論。參黃仲夫，刑法精義，修訂廿六版，元照出版有限公司，2010 年 8 月，頁 745-746。

608 學界多稱此為「實質結合犯」，參林鈺雄，新刑法總則，三版，元照出版有限公司，2011 年 9 月，頁 583-584。

609 對此有論者即認為擄人勒贖罪從刑度觀之，應是對「擄人行為+勒贖行為」的行為評價才是，參甘添貴，體系刑法各論，修訂再版，2004 年 2 月，頁 412。

610 林鈺雄，新刑法總則，三版，元照出版有限公司，2011 年 9 月，頁 584。

而在此仍有在意圖加重後對於意圖的實現另以結合犯的方式更加加重的規制設計可能性。但必須要注意的是，若要以結合犯加重意圖並實現的行為，於意圖行為的加重部分應僅能彰顯「只有意圖而未實現」行為的評價，否則會造成刑罰過度的加重，而違背罪刑相當原則。

然而，也因為結合犯的設置僅是因重刑化的刑事政策[611]，行為人對於法益的侵害並無較僅使用數罪併罰的情形嚴重，故在結合犯的設置上必須非常小心，除在具有充分理由的時候始能夠有限度的使用外，原則上應盡量排除使用[612]，更何況是在行為已有特別加重的情形下，又要以結合犯更加重處罰，所要說明的理由必須更加充分。在不法意圖並實現的情形，既有依加重事由而處罰的方式可以規制，並且亦極度難以說明對此類行為的評價何以需要使用比數罪併罰後的最高刑度更加嚴重的刑罰來規制，故縱使二種方式存在並存的可能性，本文仍不採取結合犯的設計方式。

從而，於不法意圖並實現的部分，本文擬僅就具不法意圖的入侵行為中的不法意圖作為加重處罰事由而設置一加重構成要件，並依照不法意圖的不同，而決定規制的刑度。首先是意圖變更、取得電磁紀錄而入侵的行為，此種入侵的意圖，衡諸立法理由以及立法過程的意見，似才是妨害電腦使用罪中所欲規定的「情節較重大的入侵行為[613]」，故其刑度即參考刑法第 358 條，論以三年以下有期徒刑、拘役、科或併科十萬元以下罰金的重刑度。就意圖影響電腦效能的入侵行為部分，則依照前述入侵後行為刑度設定上的不法內涵關係，論以二年以下有期徒刑、拘役、科或併科七萬元以下罰金的刑度[614]；就入侵後僅單純窺視的行為部分，亦依照前述的不法內涵關係，論以一年六月以下有期徒刑、拘役、科或併科五萬元以

611 黃仲夫，刑法精義，修訂廿六版，元照出版有限公司，2010 年 8 月，頁 255 以下。

612 在法益論者所架構下的刑法，理論上應是不能出現僅因刑事政策而特別加重的情形，故若認為刑法是為保護法益而存在，對於此種侵害法益相同但卻因刑事政策必須要重罰的條文設計應該採取盡量揚棄的態度。

613 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第 358 條之修正說明第三點。

614 雖衡諸我國刑法規定，並無以「七萬元以下罰金」方式規制的刑度，然在此僅表彰一種量刑的比重而已，故仍維持七萬元以下罰金的刑度。

下罰金的刑度[615]。

就惡意程式的使用問題即較為單純，因惡意程式使用僅是犯罪手段上的問題，並未涉及如前述般競合理論與刑事政策的概念，故原則上僅要設計加重規定即可適當評價。惟對於加重的設計上有兩種設計方式，第一種設計方式是如同前述意圖犯的規定，將使用惡意程式的行為與不法意圖同列為加重要素，整體的呈現即如同竊盜罪與加重竊盜罪的關係，而意圖犯與使用惡意程式僅要成立其一，即能評價為「重大的入侵行為」；第二種設計方式則是如同刑法第 318 條之二對使用電腦加重妨害秘密行為的加重般，以原刑度的倍數加重方式呈現。

在此二種設計方式的選擇上，若選擇第一種設計方式時，似乎必須說明使用惡意程式入侵電腦所反映的不法內涵與意圖為入侵後行為而入侵電腦所反映的不法內涵相當，並且在主要重點規制行為的部分，亦即「惡意程式的使用」與「不法意圖並實現」二要素皆具備的電腦犯罪類型中，若不法意圖並實現部分的規制設計即是如同前述般以加重構成要件與形式結合犯的方式規範，在此又將惡意程式的使用也作為一個與不法意圖相當的加重構成要件時，由於加重構成要件間是屬擇一關係，亦即行為僅要該當其一即會加重，在行為該當複數加重要件時，僅是單一的加重行為，並僅成立一個加重入侵罪[616]。如此一來即會使主要重點規制行為與不法意圖並實現的次要重點規制行為所論處的刑度相同，進而無法區分主要重點規制行為與次要重點規制行為的差別，似乎不是個妥適的作法。或可認為在嘗試獨立論證使用惡意程式入侵行為的不法內涵後，可以以同條不同項的規定方式呈現加重規定的態樣，但因前述對不法意圖的規制是依照不同的意圖而作區分，於評價上更是如同其態樣般的五花八門，若又因此必須再重新設計規制態樣，未免使規範的呈現上出現非必要的過度繁雜。故與其如此大費周章的思考以加重構成要件規定後對於整體規制體系的維持應如何變更或追加條文的設計，不如嘗試考慮第二種設計方式是否能有效解決問題。

第二種設計方式可能呈現的規範模式，即是「在基本構成要件與加重構成要

[615] 雖衡諸我國刑法規定，並無以「一年六月以下有期徒刑」方式規制的刑度，然在此僅表彰一種量刑的比重而已，故仍維持一年六月以下有期徒刑的刑度。
[616] 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 356-357。

件後，設置一特別加重條款，規定基本構成要件與加重構成要件若該當該條款中的規定情形，即加重一定比例的刑罰」。具體而言，即是在入侵電腦罪、加重入侵電腦罪之後，規定「利用特定電腦程式所具備之破解、迴避電腦網路登入控制機制或其他使電腦網路的登入控制機制無法有效運作之功能而違犯以上三罪時，加重其刑至二分之一」。據此，對於如何將使用惡意程式的要素融入處罰體系中的問題似乎即能妥善的解決，亦不會造成處罰規定的多餘及混亂，故而似應選擇第二種設計方式來作規範。

不過，第二種設計方式亦會在對於公務機關電腦的部分產生問題，由於現行刑法第 361 條，對於公務機關電腦犯罪的加重，即是採用本文所述的第二種設計方式，若在此本文亦在對公務機關電腦犯罪的部分採用此種加重方式時，可能會發生整部傳統刑法前所未有的「加重後加重」情形。但此種問題的解決相較於前述第一種設計方式所產生的問題而言容易許多，原則上此種加重規定的呈現方式，亦僅是刑事政策上的考量，在未導致規制體系紊亂或適用上以及刑度計算上的不便利時，以「加重後加重」的方式呈現並無不可。況且會使用概括加重的其中一個理由，即是所加重的罪名涉及甚廣，若依照每條的情形個別設計加重構成要件以及刑度，會使得法條的呈現上過於繁雜，從而可以認為此種概括加重的設計反而是為了維持規制體系而設計的方式，在有助於體系維持的情形下，似應採取雙重概括加重較妥。

綜上所述，本文在使用惡意程式的加重規制上，擬採用第二種設計的方式作規範的呈現，亦即若使用惡意程式入侵電腦時，該些入侵行為的處罰刑度各加重至二分之一。

第三項 解決其餘問題

在確立重點規制行為的區分及處罰後，罪章的架構實則呼之欲出，但在組織罪章架構前，仍存在幾項前揭章節已提及而有待解決的問題，計有對於公務機關的加重處罰以及告訴乃論的設置二項，故以下即對此二項問題為分析探討後，始著手於進行罪章架構的組織。

首先是對於公務機關的加重處罰問題，對此種行為的加重理由已如前述應是「保有大多數人資訊的電腦更加不可以被侵害」，若侵害此種電腦，除從個人法益保護的角度看來，一次會侵害極大多數人的資訊甚至使用空間的支配性[617]外，從本罪保護法益的角度觀察，亦會嚴重影響社會上對於電腦網路此種溝通制度安全性的信賴，使得社會上對於將資料以電子化的方式集體儲存於伺服器中一事感到惶恐與不安，故對此種電腦的侵害必須加重規制。而加重規制的方式，則如前述參考現行刑法第 361 條，以概括加重的方式處罰，亦即規定「對於公務機關、金融機構、商業機構或其他保存多數人資訊之機構之電腦，違犯前述之罪者，加重其刑至二分之一」。

至於將處罰範圍擴張至金融或商業機構的規定方式是否會因而導致該些機構不積極增強自己網路安全措施的問題，本文認為一來設置此種加重處罰所注重的點應是社會上對於網路制度的信賴關係可能因此遭受更加嚴重的破壞，而非是否「圖利」私人企業，二來私人企業具有同業競爭的壓力，如同前揭章結論者所述，金融、商業等私人企業往往非常懼怕企業內的電腦遭到入侵一事被大眾(嚴格來說，是「客戶」)得知[618]，因此種資訊安全亦屬於社會上在選擇服務企業時所注重的考量之一，若企業因刑法有加重處罰而怠於增強自己網路安全措施，即會流失大量客戶，與企業利益相背反，故如此規定應不至於產生此類問題。

再者是對於告訴乃論此種訴訟要件設置的問題，一來本罪章所保護的法益是社會法益，而社會法益的保護在原則上不會交由實質上遭到侵害的個人來決定是否發動訴追[619]；二來基於告訴乃論本身既與偵查實效無關，且亦無助於將稀少的訴訟資源完善的分配到「較嚴重的電腦犯罪」上，並且還有可能因此種規定使得「較嚴重的電腦犯罪」於實質上無法被規制。並且從雲端運算時代的發展也可以發現，以網路為主而建構的溝通秩序時代已漸漸來臨，此種時代的特色之一即是

---

[617] 如 WEBMAIL 等提供多數人使用的網路服務，該多數人於服務中得使用的範圍內亦存在使用空間。

[618] 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月，頁 216-217。

[619] 現行刑法內有關社會法益的條文中具告訴乃論規定的僅有四條，亦即第 230 條血親性交罪、第 238 條詐術結婚罪、第 239 條通姦罪、第 240 條第二項和誘有配偶之人脫離家庭罪。然此四個條文存廢的爭議性皆重大，應可認為是社會法益中例外設有告訴乃論規定的情形。

「國際化」，面對此種國際化的時代特色，告訴乃論的規定很可能會造成犯罪的實際追訴可能性大打折扣，故在此本文主張於本罪章內不設置告訴乃論此一訴訟要件。

第四項 呈現罪章架構

在處理完所有的問題之後，於此即是要呈現出妨害網路秩序罪章的整體規制架構。首先就章節排序的部分，多數學者皆認為章節的排序具有特定法益的表彰[620]，並非如妨害電腦使用罪章的修法理由中所述「並不特別強調以保護法益之種類作為章節的區別[621]」，故在此既確定本罪章所保護的法益為一社會法益，為體現刑法分則各章中所區別的保護法益，則應將本章置於社會法益的部分始為妥適。但現行刑法中社會法益的罪章亦有排序，要將本章置於社會法益的何處亦是問題所在，若就本章所保護的法益是一種「社會上對於制度妥善運作的信賴」角度出發，似將其置於同是對於制度運作信賴的偽造文書印文罪章之後較適得其所。而關於罪章排列順序的問題，既刑法已容許章節序號以「之一」的方式表示[622]，則在此要將該章訂為「第十五章之一」亦無不可。而章名的部分即參考前揭章節，訂以「妨害網路秩序罪」。綜上所述，此一新罪章的名稱及順序即為「第十五章之一妨害網路秩序罪」。

就罪章內部條號的編排部分，由於本罪章是以入侵行為為規制中心，故對於入侵行為的規制即是放在首要條文中規定。對於入侵行為的規制分為普通入侵行為以及加重入侵行為，並分別以不同條文規定。在入侵行為規制後，其次即是入侵後行為的規制，並僅限於前條以外的情況下進入電腦後為之的情形。再者即為關於使用惡意程式的加重規定，並僅涵蓋以惡意程式入侵電腦的情形。其後是入

---

620 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月，頁 43 以下；李聖傑，「家族相似性」探尋刑法典範之應用–以法益為核心，刑事法學的新視野，元照出版有限公司，2011 年 5 月，頁 145-146；李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月，頁 239-240。不同見解參許恒達，資訊安全的社會信賴與刑法第三五九條的保護法益–評士林地方法院九十九年度訴字第一二二號判決，月旦法學雜誌第 198 期，2011 年 11 月，頁 240。

621 參行政院、司法院會銜送立法院審議之關於電腦網路犯罪部分之刑法部分條文修正草案中之中華民國刑法部分條文修正草案對照表於刑法第三十六章之修正說明第三點。

622 如刑法第十六章之一的妨害風化罪章即是一例。

侵前行為的規制，最後才是對於保有大多數人資訊的電腦為前述犯罪的更加重處罰。

而就是否要於總則的立法解釋部分規定「電腦」一詞的定義問題，本文認為雖依照本文前揭章節的結論似乎認為有必要作規定，但此一結論是建立在「刑法中所有條文的訂立基礎皆與本章相同」的前提下而得出，然刑法分則中有許多條文涉及電腦，若貿然將電腦以最寬鬆的定義規定於刑法總則上，即會造成該其他行為處罰範圍的混亂。並且對於最寬鬆的定義上，縱使未於總則規定，於實際適用上因僅可能產生限縮處罰而不可能產生擴張處罰的情形[623]，並且於本罪章構成要件的設計上，是否為「電腦」的爭議所造成的影響亦已有限，故在此應認無庸特別於現行刑法第 10 條對於「電腦」作定義。

綜合以上，對於各條文的構成要件設計以及條號排序等要素所呈現的整體規制架構，即於以下用表列的方式呈現[624]。

章名：第十五章之一妨害網路秩序罪	
條號	條文內容
220-1	**第一項**[625] 透過通訊線路，無故輸入他人帳號密碼、破解或迴避電腦登入控制機制，或其他相類之方法，使該電腦之登入控制機制失效，足生損害於公眾或他人者，處一年以下有期徒刑、拘役、科或併科五萬元以下罰金。
220-2	**第一項** 意圖變更或取得儲存於電腦系統中之電磁紀錄，對該電腦犯前條之罪者，處三年以下有期徒刑、拘役、科或併科十萬元以下罰金。 **第二項** 意圖減損電腦運作效能，對該電腦犯前條之罪者，處二年以下有期徒刑、拘役、科或併科七萬元以下罰金。 **第三項** 意圖瀏覽電腦內部資訊，對該電腦犯前條之罪者，處一年六月以下

623 且限縮處罰的可能性，依照現行實務對電腦犯罪的論處方式可謂微乎其微。

624 以下法條呈現的文字型態參考自羅傳賢，立法程序與技術，三版，五南圖書出版股份有限公司，2002 年 7 月，頁 149 以下。

625 原則上在法條的呈現上是不應該在僅有一項(款)的情況下標註「第一項(款)」，然在此為方便確認故特別標明，以下相同。

	有期徒刑、拘役、科或併科五萬元以下罰金。
220-3	**第一項** 對於前條以外透過通訊線路而連線的電腦，無故變更或取得儲存於該電腦系統中之電磁紀錄，足以生損害於公眾或他人者，處一年以下有期徒刑、拘役、科或併科五萬元以下罰金。 **第二項** 對於前條以外透過通訊線路而連線的電腦，無故減損該電腦運作效能，足以生損害於公眾或他人者，處六月以下有期徒刑、拘役、科或併科三萬元以下罰金。 **第三項** 對於前條以外透過通訊線路而連線的電腦，無故瀏覽該電腦內部資訊，足以生損害於公眾或他人者，處拘役、科或併科一萬元以下罰金。
220-4	**第一項** 利用特定電腦程式所具備之破解、迴避電腦登入控制機制或其他使電腦的登入控制機制無法有效運作之功能，而犯第二百二十之一條、第二百二十之二條之罪者，加重其刑至二分之一。
220-5	**第一項** 下列各款行為，處三萬元以下罰金： **第一款** 以文字、圖畫或他法，公然介紹特定電腦程式的犯罪功能，並散布該程式者。 **第二款** 無故公開他人的帳號密碼及該帳號密碼所利用之電腦，或依知該帳號密碼所利用電腦之第三人之請求而告知該帳號密碼，足生損害於公眾或他人者。
220-6	**第一項** 對於公務機關、金融機構、商業機構或其他保存多數人資訊之機構之電腦犯前五條之罪者，加重其刑至二分之一。

第四節　規制之實際運用

在呈現出妨害網路秩序罪的規制架構後，在此即是要實際驗證此罪章是否能足以解決問題。由於從前揭章節實務分析部分可以發現，問題範圍極度廣泛，故在此大略的將問題依照時間點區分為「現今實務問題的處理」以及「雲端時代來

臨後所產生問題的處理」二大部分。在現今實務問題的處理部分，則依照問題的發生頻率以及涉及前揭章節所述重點的契合度，選擇發生頻率較高或較值得一提的行為態樣來探討處理方式，計分為帳號密碼盜用、員工不法行為、洪水攻擊、外掛程式、施放電腦病毒、以及侵入公務機關員工郵件系統等情形。而在雲端時代來臨後所產生問題的處理，則是集中於前揭章節中對於雲端運算的特色適用於現行法時可能產生問題的部分作探討，以證明本罪章具有足以在未來面對雲端運算時代來臨的遞續性，計分為入侵雲端主機、刪除或變更雲端主機內之電磁紀錄、降低雲端主機運算效能、以及物理性質的破壞雲端主機或主要通訊線路的行為。就以上行為處理的論述方式，本文採用重點式的論述，直接點出新罪章與現行刑法處理方式的差別，以將討論重點聚焦，並且更能凸顯新罪章相對於現行刑法妨害電腦使用罪所變更的不同之處，以說明新罪章的完整性。

第一項 現今實務問題之處理

第一款 帳號密碼盜用

帳號密碼盜用的情形，是我國實務上所查獲的電腦犯罪中最多數的一類，因此種行為態樣極度單純，並不需任何電腦相關專業知識即可違犯，且由於法條中限定行為態樣的緣故，現行實務上只要一確認行為人具有輸入他人帳號密碼而侵入他人電腦的行為時，即認為會成立刑法第 358 條之罪。然而在妨害網路秩序罪章的涵攝下，此類行為是否一概有處罰的必要即有疑義，易言之，此類行為不一定都侵害法益，只有就侵害法益的行為而言始有處罰必要。而此種類型即是刑法第 220 條之一[626]所規範的入侵行為，本條所保護的法益為登入控制機制的妥善運作，而在此的登入控制機制類型是以帳號密碼來控制，而此種以帳號密碼來控制的登入控制機制，有一部分是要靠設定帳號密碼的人，亦即「被盜用的人」來合作維持運作。若帳號密碼的設定者並不在乎其帳號密碼被任何人知道而廣泛告知

[626] 此為上節結論而擬制出的建議修訂法條，現行刑法並不存在本條文，以下若出現刑法第 220 條之一至之六的條文亦同，皆不再贅述。

他人甚至公開，就輸入其帳號密碼而登入的行為即不會動搖社會上對於此類登入控制機制的信賴。從此情形可以推出，當密碼設定者僅告訴其身旁的少數人(例如男女朋友)其帳號密碼時，即表示該密碼設定者對於所告知之人為授權，就該些人依授權內容輸入帳號密碼而登入系統時，亦不會動搖社會對此種認證機制的信賴[627]。更進一步而言，若此些被授權的人自己不自重的在未經授權的時段仍使用帳號密碼登入時，帳號密碼設定者雖會感到遭受背叛以及不安，但此種不安不是來自於對於利用帳號密碼的登入控制機制不妥善的運作，而是其授權的人「不被信任」，故此種情形所關係到的信賴關係應是「被害人對於行為人的信賴」而非「社會大眾對於登入控制機制妥善運作的信賴」。同理，在該行為人進入電腦後的入侵後行為，如變更密碼或刪除資料等行為，亦是破壞「被害人對於行為人的信賴」，縱使社會大眾皆不會容許此類行為[628]，然此種不容許僅是對於「行為人不能破壞被害人對其的信賴」此一命題的認同，並非認為因此即會對於網路運作的安全秩序感到不信賴[629]。畢竟社會大眾根本沒有對電腦或網路系統能夠無懈可擊的辨認來者是否有權的功能一事抱有任何期待與信賴，既無期待與信賴則不會出現信賴被破壞的問題[630]。

從而，本文認為僅有在「帳號密碼設定者未告知行為人帳號密碼」，而行為人得知該帳號密碼並輸入的情形下，始會讓人產生「此種機制不足以保障我的安全」的不信賴感，始能該當「足生損害於公眾或他人」的要件而成立本罪。就實際運用的案例中，以網路遊戲盜帳號為例，若該帳號密碼是行為人去偷看或利用

---

627 縱使是遭強暴脅迫而交出帳號密碼，亦是一種授權，只是授權的來源「有問題」而已。

628 應該沒有人會容許自己授權的人背叛自己，故本文在此武斷的使用「皆」。

629 惟應注意有不同見解認為，於告知男女朋友帳號密碼而被其拿去惡用的情形時，無異使個人對於具有親密關係之人不得主張任何隱私利益，故認為可以產生對於通信資訊安全的信賴破壞。參許恒達，資訊安全的社會信賴與刑法第三五九條的保護法益–評士林地方法院九十九年度訴字第一二二號判決，月旦法學雜誌第 198 期，2011 年 11 月，頁 248。惟本文認為論者會採如此見解，一定程度上是要為實務上的條文適用尋找一個合理的解套方式，其論述重點仍是「實務對於本罪的適用，必須考量是否破壞社會大眾對於資訊安全的信賴，而非一概成罪」，此種結論即為本文所採。

630 對於將帳號交與他人暫時保管一事，現行社會上對於此種情形應皆會有所警覺而會暫時的更換密碼(至少筆者即會)，而就非短期共同生活的伴侶(如男女朋友關係)的情況，可能會因實際生活需要而共用同一組密碼，但在關係中斷後亦應會立即更換密碼的才是，而就此種可以說「因自己的怠惰」所造成的不幸結果，還要將責任歸咎給其本來就不期待具有此種功能的電腦網路登入控制機制或資料儲存機制，坦白說網路系統何其無辜。

木馬程式得知[631]，此些輸入帳號密碼的行為仍會成立刑法第 220 條之一之罪，但若是如前述是好友共用，或是代為練功等情形，即因不足生損害於公眾或他人而不成立本罪。

第二款 員工不法行為

於員工不法行為的部分，若依前述區分為離職前為之與離職後為之，於離職後為之的部分基本上絕大多數是該員工發現自己離職前的帳號密碼能使用，並輸入該帳號密碼進入公司電腦的情形，而此種情形並不足以生損害於公眾或他人已如前述，故在此不再贅述，而將重點置於離職前為之的情形。而在離職前為之的情況，多半是利用自己的員工帳號密碼登入公司系統後，將公司規定不得攜帶出公司的文件資料給帶出公司，或是不得瀏覽公司主機的某些區域但卻瀏覽，而最多數的情況則是將公司內部的重要資料全數刪除的情形。現行實務上對於此三種情形皆認為會成立刑法第 359 條之罪，但在此本文認為應將行為態樣作區分而分別判斷。就第一種情形，仍與離職後為之的情形相同，行為人所破壞的是被害人對其的信賴，故仍不足以生損害於公眾或他人。

第二種情形必須區分該些不得瀏覽的區域是否有施以任何安全措施隔絕[632]，或僅是以契約或使用規則來規制，若是後者固然會成立本罪，然若是前者，行為人在破除安全措施的同時，仍可能另該當刑法第 220 條之一之罪，而破除後的後續行為，所破壞的已非被害人對其的信賴，已屬社會上對於網路安全秩序的信賴問題，畢竟社會上就對於一個未授權連線的電腦進行連線後為入侵後行為的情形，應會認為「既然都不允許他人進入並設置安全措施，但安全措施竟被破壞並且內部的資訊受損，感覺網路好像不太安全」，故可認已動搖社會上的信賴而成立犯罪。

至於第三種情形，仍必須區分所刪除的資料中是否包含行為人「沒有權限刪除」的。因刪除的手段有很多種，最激烈的刪除手段即是將整個硬碟格式化，若

[631] 於利用木馬程式的部分，則於以下「施放病毒」的行為部分詳述。
[632] 若此種安全措施仍允許員工使用其帳號密碼登入，即與沒有設置無異。

今天行為人僅是在其登入後「有權」使用的部分進行刪除或變更電磁紀錄，則仍屬被害人對其的信賴的問題，但若行為人是以格式化或是施放病毒將整個系統全面破壞，或將其「無權」使用的部分局部破壞時，若無權使用的部分設有安全措施，此種破壞行為首先會因「其他相類方式[633]」而使登入控制機制失去效用，而成立刑法第 220 條之一之罪，並且就刪除電磁紀錄的部分可能會成立刑法第 220 條之三之罪[634]。惟此種行為應可認為破壞登入控制機制是意圖破壞儲存於內部的電磁紀錄[635]，而成立刑法第 220 條之二之罪，此時由於刑法第 220 條之二是刑法第 220 條之一的特別規定，故不另論刑法第 220 條之一之罪，而刑法第 220 條之三之罪亦是實現意圖的行為，基於不完全的多行為犯概念亦不另為處罰。

第三款 分散式阻斷攻擊(DDoS)

此種洪水攻擊依實務上認為成立刑法第 360 條的行為態樣，可概略分為二類，第一類是傳送大量封包來癱瘓他人電腦主機，另一類是未為連線，但不斷傳送欲連線的封包來「嘗試連線」，而造成他人電腦主機的癱瘓。前者的部分，由於其傳送的封包往往是經過被害人所認證始能進入[636]，故基於前述法理在此的效能減損亦不足以生損害於公眾或他人，故不成立本罪章的犯罪，但其行為可能會因破壞他人對於使用空間的支配，而成立破壞使用空間罪章內的條文。然而在「偷偷進入並傳送封包」的情形，則會視情形成立刑法第 220 條之一、第 220 條之三或甚至第 220 條之二之罪。而後者的部分，即是一連串的「以嘗試進入來造成他人電腦效能的減損」，然而此種嘗試進入會造成電腦效能減損，即是因該電腦的登入控制機制連續正常運作所致，此種行為不但不會破壞社會上對於網路安全秩序的信賴，反而還一次次的建立社會上對於登入控制機制妥適運作的信賴，故在此

---

633 在此並非破解而是破壞，亦非規避登入控制機制所涵蓋的登入方式。

634 認為「可能會」是因刑法第 220 條之三限制該些行為必須要於已連線的狀態下為之，在此有沒有辦法解釋成已連線即可能產生爭議，但無論最後是否成立，此種情形於競合的時候幾乎不會另論本罪，故在此討論的實益較小。

635 若要破壞內部的電磁紀錄，必須先過登入控制機制這關，故行為人乾脆連登入控制機制都一啟破壞。

636 如寄送大量垃圾信件來灌爆他人信箱的情形。

亦不成立本罪章的犯罪[637]，不過該行為仍可能因為破壞他人對於使用空間中完整的空間支配，而成立破壞使用空間罪章內的條文[638]。

第四款 外掛程式

外掛程式的使用原則上是為了補足原程式的不足之處，但由於資訊科技的發展，外掛程式亦出現了鑽原程式漏洞或造成原程式不足的類型。而就補足原程式不足的外掛程式，原則上僅會在單機上運行，縱使在有些時候會與網路有所相關，其與原程式所在的電腦為連線亦僅在於補足原程式的不足，應不會使得社會大眾對於網路安全秩序失去信賴感，故此種外掛程式的使用不會成立本罪章中的犯罪。但就鑽原程式漏洞以及使原程式失去部分機能的程式部分，若僅在單機上運行，則僅可能涉及著作權的問題，於本罪章無涉，惟在與網路相關的情形下，該些程式可能會傳送封包來達成鑽原程式漏洞或使原程式失去部分機能的目的，此時則必須視具體情形來判斷該封包的傳送是否足以構成入侵行為，若不足以構成入侵行為則成立刑法第 220 條之三之罪，若足以構成入侵行為，在此即因不法意圖而成立第 220 條之二之加重入侵罪。

第五款 施放電腦病毒

所謂電腦病毒(惡意程式)亦是一個相當籠統的概念，與其如現行法般概括式的規定使用病毒必須處以極刑，不如依照其所造成的效果來區分可能成立的犯罪。據此，若該電腦病毒的效果僅是單純的惡作劇，如點下去後會讓整個螢幕出現一個巨大的豬頭圖案後立刻回復正常，並無造成電磁紀錄的變更取得、電腦機能的

---

[637] 或許在此會有認為此種情形會讓社會大眾覺得「今天我使用網路卻可能被不明人士如此對待，網路的使用著實不安全」，而認為有影響社會對於網路安全秩序的信賴感。此種見解看似合理，然而在一般人使用網路並且認可登入控制機制有存在必要的同時，亦意味著允許登入控制機制在每個處理過程中所耗費的少許系統資源，若從此觀點出發下，此種情形應仍是在網路機制完善運作下所產生的結果，行為人僅是惡用此種機制來達到使行為人受到損害的目的而已。此種行為就類似不斷對被害人打電話，在被害人接起時立刻掛斷重打，使得其他人無法打電話連絡被害人的惡作劇一般，被害人應不會覺得使用電話來溝通不安全，只會覺得行為人非常的令人厭煩而已。

[638] 但由於此種行為根本未進入他人電腦，故縱使以破壞使用空間罪章來處理，亦有很高機率屬例外處罰的情形。

減損或系統被瀏覽等結果，則此種惡作劇的行為不應由刑法規制，故不成立犯罪。但若電腦病毒的效果是會造成電腦機能的減損或電磁紀錄的變更，即可能會成立犯罪。此時則必須思考該病毒的來源，若病毒是行為人入侵電腦後施放，則依照行為人意圖的有無，以及入侵行為的程度，可能會成立刑法第 220 條之一至之三之罪。而若該病毒是被害人允許行為人對電腦連線後所施放，此時仍會回歸如經授權進入的情形一般，所侵害的應是被害人對行為人的信賴而不成立本章之罪，但可能成立破壞使用空間罪章之罪。又若該病毒是會使電腦自動連線並傳送封包給行為人的電腦[639]，此時即是一種迴避登入控制機制的連線行為，自該病毒傳送封包(連線)給行為人的電腦時，即會成立刑法第 220 條之一不正連線罪以及刑法第 220 條之三之取得電磁紀錄罪，又此種病毒施放的同時行為人應有不法意圖，故最後會論以刑法第 220 條之二的加重不正連線罪，並因該不正連線是透過惡意程式而為，依照刑法第 220 條之四更加重刑度至二分之一。

較值得一提的是特洛伊木馬型病毒，此種病毒往往透過郵件或其他方式進入他人電腦而自動或手動施放，然無論是自動或手動施放，該病毒要發作，必須在信件的傳輸中，通過信箱對於危險信件的過濾系統。而此種過濾系統亦屬登入控制機制的一類，此種將惡意程式偽裝成一般程式或信件，而導致信件過濾系統無法判斷是否危險而使接收該信件的行為，無疑是迴避登入控制機制的判斷而與他人電腦進行連線。故此種迴避登入控制機制的行為，應會成立刑法第 220 條之一之罪。並且會依照該病毒的目的，而解釋成行為人具備各種不法意圖，進而成立刑法第 220 條之二的加重不正連線罪。

第六款 入侵公務機關員工郵件系統

此種案例與前述帳號密碼盜用的案例最大的不同點，即在於此種入侵行為的客體是公務機關。但入侵的並非公務機關中所涉及保管大多數人資訊的系統，而僅是為了方便員工作業，或甚至僅是員工福利性質的免費網路信箱系統。現行實

[639] 如行為人為了取得他人個資，而施放病毒，該病毒發作後會於電腦上網期間連線到行為人的電腦，並傳送含有他人個資的封包給行為人。

務上對此類行為的判斷，完全不區分是否為涉及保管大多數人資訊的系統，即皆依刑法第 361 條給予加重處罰。然若依照此種加重處罰的設置理由，對於與保存大多數人資訊的系統無關者為入侵或為入侵後行為，原則上應排除於加重範圍外。但行為人在入侵公務機關電腦時，原則上並不會刻意去區分何部分系統有涉及保管大多數人資訊，僅在例外情形如明知自己所入侵的僅是未涉及保管大多數人資訊的員工郵件系統，才有區分的可能性。從而，本文認為對於此類型案例必須做區分，若客觀上該系統未保管大多數人資訊，且主觀上行為人亦明知其入侵的對象顯然不涉及保管大多數人資訊的系統時，依照刑法第 220 條之六的歷史解釋，應例外的無適用本條加重的餘地。反之，若客觀上該系統是作保管大多數人的資訊之用，或行為人不知其入侵的對象是否涉及保管大多數人資訊的系統時，即應適用本條加重其刑至二分之一。據此，於此案例中客觀上員工郵件系統應非屬保管大多數人資訊的系統，若行為人亦明知此事而侵入，則無庸依刑法第 220 條之六加重，反之若行為人並不知，僅是為了侵入公務機關的電腦系統時，仍應適用第 220 條之六加重其刑。

第二項 雲端時代來臨後所產生問題之處理

第一款 入侵雲端主機

入侵雲端主機看似是一個清楚的概念，實際上仍有一定程度的模糊。由於雲端時代來臨後所造成的資訊共同管理特色，使得一個雲端主機中，除了管理者得以使用的部分外，仍涵蓋世界各地的使用者所能使用的部分。故入侵雲端主機的行為，還可以再區分為入侵管理者的部分以及入侵使用者的部分。在入侵使用者的部分，雖然各個使用者因為 IT 資源的共享緣故，所使用的都是同樣的硬體設備，但一來網路秩序妨害罪章的不正連線罪本不限於進入「他人」電腦的情形[640]，在此可以省去何謂「他人電腦」的解釋問題；二來由於本文採取最廣義的電腦概

[640] 就「未經授權而使登入控制機制失效」的構成要件看來，邏輯上不可能對自己的電腦為之，因一旦對於自己電腦為之，即代表已經過授權。

念，故在此只要該電子運算的機具具有輸入、輸出、儲存、運算的功能，即可稱為電腦，故就算實現此些功能的硬體設備因雲端運算全球化的特色而四散各地，依照最廣義的電腦概念仍可以認為其為電腦。而此種僅入侵使用者的部分，雖所入侵的是保存多數人重要資訊的雲端主機，然客觀上其入侵的部分未保存多數人重要資訊，主觀上行為人亦明知此事，故亦無法以刑法第 220 條之六加重其刑。其行為的評價，即相當於現今藉由網路入侵個人電腦的情形。

而就入侵管理者的部分，則相當於現今藉由網路入侵公務機關的情形。管理者的主機內除了管理者自身的資料外，亦保存大量使用者的資料，若對於此主機為入侵，即會直接對該雲端主機中的使用者造成恐慌與不安，故在此即是實務上所要處罰的「典型電腦犯罪」，而有加重處罰的必要。在構成要件的涵攝上，客觀上管理者的主機應有保存大量使用者的資料，並且會入侵管理者的行為人主觀上原則上亦明知此事，故此種入侵行為即會以刑法第 220 條之六加重其刑。

第二款 刪除或變更雲端主機內之電磁紀錄

如同前述入侵雲端主機的部分，在此由於 IT 資源的共享，亦應區分為共用電磁紀錄以及非共用電磁紀錄而應有不同論處。而區別的方法即如同前述對於公務機關加重的判斷要素相同，以主客觀綜合的方式判斷。

必須注意的是，通常雲端主機的管理者為了讓使用者感到安全，會將使用者的電磁紀錄作非常多份的備份，以防止各種可能遺失的狀況。而此種防止的遺失狀況，除了人為的刪除外，還可能因為天災使機房滅失，或是因機器使用的老舊而使得資料遺失的情形。據此是否得以認為行為人刪除的資料通常多有備份，就刪除此些資料而言，因使用者對於管理者有備份一事亦明知，故應不會對於此種行為造成對於網路系統的不信賴，而認無處罰的必要性即有疑義。然而在此本文仍認為，或許因管理者有將使用者的資料備份會降低使用者對於資料遭刪除而導致對於網路安全秩序的不信賴，但此種不信賴並未完全根除，僅是降低比率而已，更何況如同前述因法律的處罰可能會造成企業怠於加強網路安全一般，不能因企業已加強網路安全，法律即將社會上對網路安全秩序的信賴全權交給企業負責，

從而或可考慮在此種情形降低宣判時的刑度，不得認因此種行為並無處罰必要，故不足生損害於公眾或他人，而不成立犯罪。

第三款 降低雲端主機運算效能

雲端運算時代中的雲端電腦具有硬體資源無限擴充的特色已如前揭章節所敘明，從而實際上對於降低雲端主機本身的運算效能應可認為是邏輯上不可能的事情。雖然邏輯上無法降低雲端主機本身的運算效能，但對效能是接受自雲端服務提供者流動性分配的各使用者而言，仍有降低效能的可能。由於雲端運算的特色之一是依需求訂制設備，故對於訂制內硬體規格的使用，仍相當於現今個人電腦的概念。據此，在雲端運算時代來臨後，降低運算效能的行為雖無法存在於對雲端主機的侵害，但仍可能會存在於對雲端使用者的侵害，故關於降低電腦運算效能的規制不會因為雲端運算的到來而失去適用餘地。

然而就前述傳送大量嘗試連線封包的行為態樣中，在雲端運算時代中雖仍有可能發生，惟要完全實現雲端資訊社會，所需的網路管線流量即是遠超過現今的網路流量，就現今的網路流量而言要以此種嘗試連線的封包塞爆網路，已有一定困難度，更遑論就雲端時代中要以更加大量的封包塞爆網路。而就塞爆伺服器的部分，即如同前述雲端主機一般的無限擴充特性，要將其塞爆仍有困難，不過若是要塞爆雲端使用者的伺服器仍有可能性，但無論是否可能，就現行法的情況下此種惡作劇般的行為即非本罪章所要規制者，從而縱使在雲端運算時代中，此種行為的不法內涵評價只會隨著科技的越進步而越降低，故仍無以本罪章處罰的必要。

第四款 物理破壞雲端主機或主要通訊線路

此種行為態樣本身並非是本罪章所規制的範圍，更甚言之亦非破壞使用空間罪所要規制的範圍。此種行為態樣與本罪章的關係，如同刑法第 185 條之三醉態駕駛罪以及第 185 條之四肇事逃逸罪相對於刑法第 184 條妨害舟車航空行使安全罪以及第 185 條妨害公眾往來安全罪的關係。簡言之，無論是妨害網路秩序罪或

破壞使用空間罪，皆是對於該電腦網路系統的使用面的規制，而物理破壞雲端主機或主要通訊線路的行為則是對於電腦網路系統的建構面的規制。在仍身處網際網路時代的現今台灣社會，單純物理破壞主機或單純切斷網路線的行為，或許僅會對於該個人電腦或該網路線可能連接到的電腦有影響，但會得出此種結論是因為現今社會中個人電腦配合網路使用仍是最普遍的使用關係，且個人電腦並非是稀有價值之物，縱使個人電腦遭物理性質的損壞，至多可能該當刑法上的毀損罪而已。然而在雲端運算時代來臨後，由於雲端運算中 IT 資源共享以及資訊共同管理的特性，使得人類與電腦的關係又回到 1970 年代與中央處理器的關係，亦即雲端主機與主要通訊線路對於人類而言是非常重要且稀有價值之物，除了雲端主機中儲存著絕大多數人的重要資訊外，主要通訊線路亦是如現今的交通幹道般是人類在未來使用電腦的必需品。若無網路即無法到達雲端，若無法到達雲端即無法碰觸到自己所儲存的資訊，若無法碰觸到自己所儲存的資訊即無法處理事務，故可認為此二者在雲端運算社會中對於人類的影響非常重大。更可以推知在未來有更高階的技術發展後，此種集體溝通的基礎建設對於人類的重要性可謂必然日趨重要，故是否可從此些情形中尋找出如同刑法第 184 或第 185 條的交通基礎建設法益亦是值得探究之處。

雖然可以預見在雲端運算時代的人類社會中，此種法益概念可能成為規制的重點，然而一方面由於現行社會似乎無法嗅出此種法益的端倪，在制定規範時難免會參雜過多想像的成分，使得規範制定的實質意義不大。另一方面縱使有辦法透過論證來說明此種新興法益的發現，此種新興法益與本文所述的妨害網路秩序罪或破壞使用空間罪所保護法益的面向皆有不同，若要設計以此種法益為中心，並環繞法益而制定相關構成要件的規範，似仍必須以獨立罪章方式建構，無法歸納於妨害網路秩序罪或破壞使用空間罪之下。從而本文在此僅提出論證此種行為態樣所表彰新興法益的可能性，並未能更深一步的去探討法益的內涵以及規制的設計。

第六章　結論

資訊科技變遷的速度著實非我們可以想像的，從電腦稍為普及的 1970 年代至 2012 年的今日，僅短短四十餘年，其中已歷經了中央電腦時代、個人電腦時代、網際網路時代、始至今日的雲端運算時代的四大使用型態革命。有趣的是，在每一個時代中，人類與電腦及網路的關係皆有不同。在中央電腦時代，由於電腦是稀有價值，人類對電腦的關係是建立於電腦本身的使用，且人與人必須互相讓步(遵守秩序)的重點在於使用電腦的權利，亦即電腦的使用時間。然而在進入個人電腦時代後，因電腦的普及化，其再也不是稀有價值之物，反倒是因個人電腦的獨佔性與專屬性，使得人手一台的個人電腦成為每個人可支配的一塊領域，從而人類對電腦的關係轉變為透過電腦所營造的使用空間，而所遵守秩序的重點即在於未經允許不得觸碰對方的使用空間。在網際網路的普及後，人類堂堂邁入網際網路時代，此時的電腦不僅是個人可支配的一塊領域，並且還具有用來溝通的功能，此時人類與電腦的關係區分出一塊給予了人類與網路的關係—亦即溝通的橋樑，而所遵守秩序的重點除了原本的使用空間支配外，也因網際網路的崛起而畫出了一塊名為網路安全秩序的新生地。在往後的發展中，隨著雲端運算時代的來臨，網際網路對於人類的影響力早已遠遠超越單機電腦，並且進一步的欲將單機電腦所帶給人類的利益給吞噬。在此時代的單機電腦對於人類而言，已幾乎僅是一個像手機一般的溝通硬體設備，真正具有價值的反而是當初剛崛起，如今發展至有如巨大怪獸般的網際網路，故雲端運算時代所象徵的意義即在於網路漸漸取代電腦在人類心中的地位。

對於此種溝通機制在社會上的日顯重要，相對的亦有不少人類打算利用此種溝通機制所相關的專業知識，來達成一些會侵害社會上共同生存利益的行為，更有甚者可能會造成社會上的巨大恐慌，以及對於資訊科技使用的恐懼以及不安。而此種恐懼以及不安即會造成世界上整體對於資訊科技的不信任，進一步亦會造成資訊科技發展的延滯，更加造成人類的不利益。若謂刑法的功能在於保護社會上共同生存的利益，則對於此類行為，刑法似乎必須想辦法因應，然而就如何因應的部分，即產生不小的問題。

基於資訊科技時代的變動是全球性的，想當然會產生的問題也是全球性的，世界各地都在因應電腦網路的出現，以及人類對於電腦或網路因時代變遷而導致的使用關係變遷所產生的問題做思考。然於世界上法學先進國家率先思考後而得出的結論中，依照英美法系與大陸法系的不同，而產生了偌大的歧異。身為大陸法系代表國的德國，基於嚴謹的法益理論以及富有邏輯的法學方法，認為此種利用電腦而侵害社會上共同生存利益的行為，並非是新型態的犯罪，所侵害的仍屬傳統刑法中所保護的法益，僅是因使用的手段新穎，而使得傳統刑法捉襟見肘，故主張僅就傳統刑法內的構成要件作修正，使構成要件能夠涵蓋利用電腦而為犯罪行為的部分。相對的，號稱海洋法系代表國的美國，基於實用主義下的實用法學理念，並不以保護法益作為行為規制的界線，而以刑事政策作為規範設置的唯一判準，同時也因為是電腦發展大國的緣故，美國能夠精準的嗅出資訊科技發展的每個階段中人類與電腦網路的關係，並立即作出規制變更的判斷，以及對世界各國合力編織處罰密網的提倡。就在二個背後有不同法體系支撐的世界大國你來我往的互相影響下，對於時代中身處較於弱勢地位的亞洲國家無疑更加深了對資訊科技發展所帶來社會現象的懼怕，以及設法規制電腦犯罪的躊躇。

其中相較於其他亞洲國家先進不少，甚至可以說是全亞洲國家的指標也不為過的日本，在此種世界潮流的衝擊之下，仍然必須俯首稱臣的著手進行電腦犯罪的規制。在設法規制的過程中，可以看見日本一方面懼怕美國所提及的資訊危害會在國內社會中蔓延，而必須對於新的使用習慣作規制，另一方面亦擔心繼受於德國的大陸法系法典，可能會因為此種規制的設計而使得刑法體系崩毀的忐忑，不過畢竟不愧對於當時亞洲大龍的稱謂，在百般猶豫後日本仍在兩位世界級的法學教師交叉轟炸下，交出了漂亮的成績單—不正連線禁止法。不但順利達成了美國所需要的雙罰規定以及對於電腦網路犯罪的規制依據，也同時顧及了繼受自德國的傳統刑法體系，並未使整體崩盤。

同樣是身為亞洲國家，並曾被稱呼為亞洲四小龍之首的我國，亦在電腦犯罪的規制上面臨了此種困境，雖然並未直接受到自美國而來的國際壓力，但我國仍自力從社會上對於資訊科技的互動以及國際情勢中，得出了必須規制的結論。並且於規制的思考脈絡上，亦與日本非常類似，是先就德國法對於電腦犯罪的處理

態度為依歸，而以修訂傳統犯罪中的構成要件的方式來達到規制的效果，其後受到美國法的影響，又再度思考是否必須就現行的使用關係作更進一步的規制。但我國的各方面水準仍不若躋身已開發國家的日本，無論是規制設計的時間點，或規制設計的品質，皆連日本的車尾燈都無法見到。此種規制設計所產生的缺失，具體而言即是出因於面對電腦犯罪態度的草率，以及對規制建立基礎的疏忽所導致，故無論是民國 86 年的修訂或民國 92 年的罪章增訂，皆產生了相當多的問題，同時也使得我國的刑法，因妨害電腦使用罪章的訂立，而成為亞洲立法的壯舉—既破壞既受自德國以及日本的大陸法系刑法，又因構成要件的規定不清不堪使用而無法達成如美國般的規制效果，並且還附帶前述任何先進國家都望塵莫及的重刑度，在連 G8 中最後一個訂立網路犯罪規制條文的日本都已制定訂立不正連線禁止法之後，又經過了三年的時間點上，始姍姍來遲的降臨於台灣社會。

然而，乍看之下經過草率修法，並且於規範條文所呈現的規制模型中問題百出的妨害電腦使用罪，竟然在這個奇蹟之島上能夠順利的給予我國實務界約近十年的恩惠，在感嘆此種莫名其妙的發展簡直是破格的超展開之餘，仍不免對於實務上的運用情形產生極大的好奇心。但如同俗話所述「好奇心會殺死貓」一般，在了解實務上運用法條的實態後，又必須無奈感嘆台灣實務界曲解立法原意的高超程度，否則會對不起天地良心，也同時對於因違反此罪章的條文而被以過重的刑度所「招呼」的行為人感到悲哀與惋惜，如果行為人不是生在台灣，就不會遭到如此對待。同時也因為修法的草率加上實務上的大力「活用」，導致電腦犯罪在台灣似乎成為了一個重大犯罪課題，不同於日本的不正連線禁止法是要靠該法的規制令政府企業與人民攜手合作建立良好的網路秩序，並進而營造先進且安全的資訊社會，我國的妨害電腦使用罪無疑是動用重刑威嚇以及實務上的大力「宣導」的詭異方式，來營造黑影幢幢的網路秩序與充滿著恐懼與不信感的資訊社會。

此外，基於修法的草率原因除一部分是因為立法者面對電腦犯罪規制的態度不佳，另一方面則是完全忽視學術研究的貢獻，而在修法過程中幾乎無學者能夠參與討論。縱使在日本，此種忽略學者參與的立法方式於修法過後亦會有學者撰文批判，想當然我國的情形，在修法結果公布後，立即遭受學術界排山倒海而來

的批評聲浪，除在罪章體系以及保護法益等基礎要素上修法者充分展現其兄弟獨到之創見外，充滿與立法理由的矛盾以及隨處可見的規制漏洞絕對是對於規範逐條進行批判論者的最愛，如在入侵電腦罪中限制行為態樣，在取得、刪除或變更電磁紀錄罪與干擾電腦罪中詭異的「致生損害於公眾或他人」要件，在干擾電腦罪中不明確的「干擾」和「其他電磁方式」構成要件，以及在製作惡意程式罪中設計「專供犯本章之罪」的構成要件此些致命性的問題，甚至還基於風馬牛不相及的理由設定了完全背離世界潮流的告訴乃論訴訟要件。就此種滿面瘡痍的電腦犯罪規制，幾乎可以斷言面臨已悄悄到來的雲端運算世代，完全失去沿遞存續的性質，而勢必在實務上或社會上面臨衝擊而發現問題所在後，又必須重新修訂法律，然而若我國立法的水準仍然沒有成長，此種悲慘的輪迴只會不斷持續。

若要使得電腦犯罪的規制具有遞續性，最重要的一點即是面對此問題的態度。既我國的規範體制是承襲於德國及日本此種大陸法系的體制，則在面臨問題時，似必須依照此種規範體制的脈絡來作思考。電腦犯罪亦僅是一種基於人類對於未知高科技所產生的恐懼感以及疏離感，而將具有此種特徵的不適切行為一股腦兒的統統塞入此種概念下而生的產物，但重點並不在電腦犯罪的危害甚大或新穎多變的使用關係，而在於從此些新穎多變的使用關係以及所造成的危害中能看出什麼端倪，亦即對於掌管論罪科刑的刑法而言最重要的「保護法益」為何。若保護法益真如德國刑法界多數意見所主張，僅是侵害傳統的保護法益，而無法論證有新興法益的存在時，則我國的規制設計上即應該如同德國般回歸至傳統構成要件的增訂，而並非硬是參考美國法制，將規制給移植至我國刑法中制定獨立專章；然一旦發現新興法益的存在，基於新興法益的獨立性，則勢必得訂立專章來處理此種新興法益的規制。

而我國對於此類犯罪保護法益的探討中，實務見解與修法派一度棄守法益理論，或甚至心中本即不存在法益概念，試圖以其所精心營造的恐怖電腦犯罪來說服社會大眾此種新興法益應是社會上共同生存的利益，並且不要在意其定位。而堅守德國法制的論者隨即道破實務見解與修法派的迷思，認為根本無所謂「兼及國家、社會、個人法益的綜合體」，電腦犯罪完全不是侵害新法益的犯罪，而是使用新興手段的傳統犯罪。除以上二種見解之外，仍有學者向日本精神看齊，努

力的尋找可能是解藥的新興法益，來為已經公布施行的妨害電腦使用罪章作一點亡羊補牢。皇天不負苦心人，在一番努力之下，論者終於從「層出不窮」的電腦犯罪案例中，尋找出新興的保護法益，但令人驚訝的是，電腦犯罪之所以在保護法益的問題上產生困境，即是因為其是一種對於資訊科技恐懼的集合體，而此種集合體經過分析後，依照面向的不同，所找到的新興法益亦有不同，故「電腦犯罪的保護法益不只一個」這個敘述應該為真。就如同毀損罪跟放火罪的關係一般，若著重於他人之物的毀棄損壞，則在放火行為中會看到毀損罪的影子；而若著重於社會上可能因為此行為而感到恐慌與不安，則會在放火行為中嗅出放火罪的端續。從電腦犯罪這個籠統的概念中，若聚焦於他人電腦的使用空間被入侵，則在電腦犯罪中會認為保護法益的所在是使用空間支配的破壞；若著眼於社會上會因此對於網路安全產生不安感，即會認為電腦犯罪的保護法益在於社會上對於網路秩序安全的信賴。

而在釐清所謂電腦犯罪其實只是個僅具歷史意義的海市蜃樓後，即沒有必要再在刑法上使用電腦犯罪一詞，應回歸保護法益來對其為稱呼，就目前所尋找出的新興法益，區分為破壞使用空間罪與妨害網路秩序罪，而就電腦的定義部分，由於使用空間支配的破壞實則與電腦沒有太大的關聯，縱使不是使用電腦，也可能會因為人與該機制的使用關係，而營造出一個使用空間，然而網路秩序是建立在電腦間所連線而成的網路系統，故在此原則上仍需要電腦概念的輔助。並且由於遞續性的考量，該電腦概念應盡量做最寬鬆的定義方式，以使得此種法益的保護體系能夠趨於完善。

在從電腦犯罪的案例中找出新興保護法益後，則必須圍繞該保護法益建構一個獨立的專章。在專章的建立上，除了要考量規制的重點以及條文的設計外，最重要的仍是要考慮價值的衡量，以免造成刑罰過度干涉資訊科技的發展，而反而與不規制的情形殊途同歸，使得資訊科技的進步遭受阻礙。此外仍然必須考量該當構成要件所論處的法律效果，應不得超過其所侵害的法益，否則即會違背罪刑相當原則。並且在規制體系設定完成後，亦要提出該規制體系的運用，對於目前社會上所產生的電腦犯罪問題，以及雲端運算時代到來後可能會產生的問題作解決，以對於遞續性的部分，以及規制應如何運用的部分作一個合理的說明。

最後的最後，仍必須衷心的祈禱台灣的法制運作以及社會水準能夠日趨成熟，在面對因資訊科技大量介入人類社會後所導致社會快速變遷而產生的各種問題時，能夠以更健全的態度面對，並以更完善的思考處理問題，天佑台灣。

參考文獻

壹、 中文文獻

一、 教科書

1. 甘添貴，體系刑法各論，修訂再版，2004 年 2 月。
2. 林山田，刑法總論，增訂十版，2004 年 1 月。
3. 林山田，刑法各罪論(上)，增訂五版，2005 年 9 月。
4. 林鈺雄，新刑法總則，三版，元照出版有限公司，2011 年 9 月。
5. 林東茂，刑法綜覽，六版，一品文化出版社，2009 年 9 月。
6. 陳子平，刑法總論，二版，元照出版有限公司，2008 年 9 月。
7. 黃榮堅，基礎刑法學(上)，三版，元照出版有限公司，2006 年 9 月。
8. 黃仲夫，刑法精義，修訂廿六版，元照出版有限公司，2010 年 8 月。
9. 盧映潔，刑法分則新論，修訂四版，新學林出版有限公司，2011 年 9 月。
10. 羅傳賢，立法程序與技術，三版，五南圖書出版股份有限公司，2002 年 7 月。

二、 專書

1. 王鵬，走進雲端運算，初版，佳魁資訊股份有限公司，2009 年 11 月。
2. 王鵬，雲端運算的關鍵技術與應用實例，初版，佳魁資訊股份有限公司，2010 年 2 月。
3. 中田敦、小林雅一、石田愛、浦本直彥、高橋秀和、松尾貴史、岩上由高、酒井達明、西片公一、森正彌、太田一樹著，鄧瑋敦譯，雲端運算大解密，初版，城邦文化事業股份有限公司，2010 年 2 月。

4. 林東茂，經濟犯罪之研究，初版，中央警官學校犯罪防治學系發行，1986年4月。

5. 房阿生、吳振村，電腦犯罪及防治方法之研究，司法週刊社印行，1989年9月。

6. 施威銘研究室，最新計算機概論2010，旗標出版社，2009年9月。

7. 陳志龍，法益與刑事立法，自版，1990年。

8. 陳瀅、王慶波、金淳、趙陽、何樂、鄒志樂、吳玉會、楊林等著，雲端策略：雲端運算與虛擬化技術，初版五刷，天下雜誌股份有限公司，2010年12月。

9. 曾憲雄、呂克明、張榮吉、廖冠捷、劉光勝、陳興忠，計算機概論，初版，東華書局，2008年9月。

10. 潘奕萍，圖說雲端運算，初版，書泉出版社，2011年9月。

11. 廖有祿、李相臣，電腦犯罪：理論與實務，初版，五南出版社， 2003年。

12. 鍾宏彬，法益理論的憲法基礎，初版，公益信託春風煦日學術基金， 2012年4月。

三、 專書論文

1. 李茂生,我國電腦網路犯罪的虛像與實相,刑事政策與犯罪研究論文集(四)，法務部犯罪研究中心，2001年，頁1-20。

2. 李茂生，資本、資訊與電腦犯罪，權力、主體與刑事法，翰蘆出版社，1988年5月，頁169-300。

3. 李聖傑,「家族相似性」探尋刑法典範之應用—以法益為核心，刑事法學的新視野，元照出版有限公司，2011年5月，頁142-163。

4. 林東茂，德國近年來的經濟刑法發展趨勢，危險犯與經濟刑法，初版，五南圖書出版股份有限公司，2002年11月，頁105-147。

5. 黃榮堅，刑法增修後之電腦犯罪問題，刑罰的極限，初版，元照出版有限公

司，1999 年 4 月，頁 301-344。

6. 葉奇鑫，我國刑法電腦犯罪修正條文之立法比較及實務問題研究，刑事政策與犯罪研究論文集(六)，2003 年，頁 95-107。

四、 期刊論文

1. 王銘勇，侵入電腦系統罪之研究，法令月刊第 55 卷第 3 期，2004 年。

2. 甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌第 50 期，2003 年 9 月。

3. 李茂生，刑法新修妨害電腦使用罪章芻議(上)，台灣本土法學雜誌第 54 期，2004 年 1 月。

4. 李茂生，刑法新修妨害電腦使用罪章芻議(中)，台灣本土法學雜誌第 55 期，2004 年 2 月。

5. 李茂生，刑法新修妨害電腦使用罪章芻議(下)，台灣本土法學雜誌第 56 期，2004 年 3 月。

6. 李茂生，電腦犯罪立法模式的比較法學分析，台灣法學會學報第 19 輯，1998 年 11 月。

7. 李茂生，日本不法連線行為禁止法簡介，資訊安全通訊第 8 卷第 1 期，2001 年 12 月。

8. 李茂生，電腦犯罪與資訊政策，國家政策雙月刊第 125 期，1995 年 11 月。

9. 李崇偉，美、日、德三國網路犯罪相關法制之探討，警大法學論集第 9 期，2004 年。

10. 李聖傑，使用電腦的利益，月旦法學雜誌第 145 期，2007 年 6 月。

11. 李聖傑，開啟電子門鎖算什麼？，月旦法學教室，2011 年 4 月。

12. 林山田，電腦犯罪之研究，政大法學評論第 30 期，1984 年 12 月。

13. 林山田，論電腦犯罪，軍法專刊第 30 卷第 8 期，1984 年。

14. 林永謀，電腦犯罪與刑事法上之問題，法令月刊第 35 卷第 7 期。

15. 林宜隆、李建廣，網路犯罪抗制對策之探討，警學叢刊第 29 卷第 5 期，1999 年 3 月。

16. 林宜隆、李建廣，網路犯罪問題及其偵防機制之探討，警學叢刊第 31 卷 1 期，2000 年 7 月。

17. 林冠宏，刑法妨害電腦使用罪章之研究，刑事法雜誌第 50 卷第 6 期，2006 年 12 月。

18. 洪光煊，從電腦犯罪談未來刑法修正方向，刑事法雜誌第 32 卷第 3 期，1988 年 6 月。

19. 范建得，重行檢視網際時空應有之法律規範，月旦法學雜誌第 130 期，2006 年 3 月。

20. 柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第 11 期，2003 年 9 月。

21. 徐振雄，網路犯罪與刑法「妨害電腦使用罪章」中的法律語詞及相關議題探討，國會月刊第 38 卷第 1 期，2010 年 1 月。

22. 莊忠進，電腦犯罪立法之探討，刑事科學第 39 期，1995 年 3 月。

23. 張紹斌，刑法電腦專章及案例研究，軍法專刊第 54 卷第 4 期，2008 年 8 月。

24. 陳煥生，刑法新增妨害電腦使用罪之介紹，中華法學第 10 期，2003 年。

25. 陳煥生，刑法上之電腦犯罪，刑事法雜誌第 42 卷第 3 期，1998 年 6 月。

26. 黃榮堅，電腦犯罪的刑法問題，台大法學論叢第 25 卷第 4 期，1996 年 7 月。

27. 許恒達，洩露使用電腦知悉秘密罪的保護射程－－評臺中高分院九十八年度上訴字第一三一九號刑事判決，月旦法學雜誌第 190 期，2011 年 3 月。

28. 許恒達，刑法法益概念的茁生與流變，月旦法學雜誌第 197 期，2011 年 10 月。

29. 許恒達，資訊安全的社會信賴與刑法第三五九條的保護法益—評士林地方法院九十九年度訴字第一二二號判決，月旦法學雜誌第 198 期，2011 年 11 月。

30. 管高岳，電腦犯罪，法學叢刊第 41 卷第 1 期，1996 年 1 月。

31. 蔡美智，虛擬世界的脫軌棋子—國內電腦犯罪脫序事件簡介，律師雜誌第 228 期，1998 年 9 月。

32. 蔡榮耕，Matrix 駭客任務：刑法第 358 條入侵電腦罪，科技法學評論第 5 卷第 1 期，2008 年 4 月。

33. 蔡蕙芳，〈危險概念與各種犯罪類型－「足以」要件危險犯之討論〉，發表於「2006 年刑法分則共同議題之探討」研討會，2006 年 5 月。

34. 鄭逸哲，吹口哨壯膽—評刑法第三十六章增訂，月旦法學雜誌第 102 期，2003 年 11 月。

35. 盧文祥，電腦犯罪之研究，憲政時代第 13 卷 4 期，1988 年 4 月。

36. 盧文祥，電腦犯罪之偵防實務，律師雜誌第 228 期，1998 年 9 月。

37. 盧映潔，電腦小子鑄大錯，月旦法學教室第 57 期，2007 年 7 月。

38. 謝銘洋、陳曉慧，德國對網路服務之新規範—資訊服務與通訊服務法(多元媒體法)，月旦法學雜誌第 36 期，1998 年 5 月。

五、 碩士論文

1. 李崇偉，電腦網路入侵行為之刑事立法研究，中央警察大學法律學研究所碩士論文，2003 年 6 月。

2. 吳文君，妨害電腦使用犯罪行法規制之分析—以保護法益為中心，國立台灣大學法律學院法律學系碩士論文，2010 年 6 月。

3. 莊凱閔，論不法侵入他人電腦系統之刑事責任—以日本法制為中心—，國立台北大學法律研究所碩士班碩士論文，2002 年 6 月。

4. 陳憲政，電腦犯罪之法律適用與立法政策—保護法益之遞嬗—，國立政治大學法律學研究所碩士論文，2006 年 12 月。

5. 張繼圃，線上遊戲中虛擬財產在犯罪判斷上定位之研究，私立東海大學法律

研究所碩士論文，2006 年 1 月。

6. 蔡蕙芳，電腦犯罪和刑事立法的課題，國立台灣大學法律學研究所碩士論文，1994 年 6 月。

7. 鄭曄祺，處罰網路犯罪理論基礎之研究—以 P2P 為例，國立台北大學法學系研究所碩士論文，2007 年 6 月。

8. 謝開平，電腦犯罪之研究—我國現行法之適用與修正草案之檢討，國立中興大學法律學研究所碩士論文，1995 年 7 月。

9. 顏邦峻，從「竊取」線上遊戲的虛擬財物探討刑法上的電腦犯罪罪章之適用，國立政治大學法律研究所碩士論文，2006 年 7 月。

六、 政府出版品

1. 法務部，刑法有關電腦(網路)犯罪研修資料彙編，2002 年。

七、 其他書籍

1. 第十四屆政大刑法週會議紀錄，2007 年 3 月。

貳、 日文文獻

一、 教科書

1. 大谷実，刑法講義各論，成文堂，2007 年。

2. 川端博，刑法各論概要，成文堂，2007 年。

3. 曽根威彦，刑法各論，弘文堂，2008 年。

4. 西田典之，刑法各論，弘文堂，2010 年。

5. 山口厚，刑法各論，有斐閣，2003 年。

二、 專書

1. 神山敏雄，日本の経済犯罪―その実状と法的対応―日本評論社，2001 年 7 月。

2. 林幹人，現代の経済犯罪―その法的規制の研究―，弘文堂，1988 年 4 月。

3. 不正アクセス対策法制委員会，不正アクセス行為の禁止等に関する法律，立花書房，2008 年 10 月。

4. 渡邊卓也，電脳空間における刑事的規制，成文堂，2006 年 9 月。

三、 期刊論文

1. 荒川雅行，ウィルス作成罪，法学教室 374 号，2011 年 11 月。

2. 伊賀興一，コンピュータの普及と刑事法の対応をめぐる諸問題，ジュリスト 846 号，1985 年 10 月。

3. 板倉宏，コンピュータ犯罪と刑事法，ジュリスト 707 号，1980 年 1 月。

4. 板倉宏，コンピュータ犯罪と刑法，法学セミナー26 巻 7 号，1982 年 7 月。

5. 井田良，西ドイツにおけるコンピュータ犯罪への対応，ジュリスト 846 号，1985 年 10 月。

6. 井田良，西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月。

7. 井上純夫，金融機械化システムの安全対策，ジュリスト 834 号，1985 年 4 月。

8. 今井猛嘉，特集・情報処理の高度化等に対処するための刑法等の改正–実体法の視点から，ジュリスト 1431 号，2011 年 10 月。

9. 大泉雅昭，不正アクセス行為の禁止等に關する法律の概要ついて，捜査研

究 576 号，1999 年 10 月。

10. 大谷実，コンピュータ犯罪(上)，法学セミナー363 号，1985 年 3 月。

11. 大谷実、古田佑紀、西田典之，コンピュータ犯罪と刑事立法の課題，ジュリスト 846 号，1985 年 10 月。

12. 加藤敏幸，不正アクセス，刑法雑誌 41 巻 1 号，2001 年 7 月。

13. 金井浄，コンピュータ犯罪とエラー，ジュリスト 707 号，1980 年 1 月。

14. 金澤正和，不正アクセス行為等の取締り状況及び今後の課題，警察学論集 53 巻 8 号，2000 年 8 月。

15. 神山敏雄，コンピュータ犯罪立法の批判的考察，法律時報 60 巻 1 号，1987 年 1 月。

16. 河原淳平、角野然生，サイバー空間上の犯罪対策への国際的取組み，警察学論集 53 巻 8 号，2000 年 8 月。

17. 北村博文，不正アクセス行為の禁止等に関する法律の制定の経緯，警察学論集 52 巻 11 号，1999 年 11 月。

18. 櫛清隆，「情報処理の高度化等に対処するための刑法等の一部を改正する法律」の概要，刑事法ジャーナル 30 号，2011 年 11 月。

19. 黒澤正和，不正アクセス行為の禁止等に関する法律の制定について，警察学論集 52 巻 11 号，1999 年 11 月。

20. 蔵原智行，「不正アクセス行為の禁止等に関する法律の一部を改正する法律」について，警察学論集 65 巻 6 号，2012 年 6 月。

21. 四方光，不正アクセス禁止法改正の背景・経緯及び不正アクセス対策の今後の課題，警察学論集 65 巻 6 号，2012 年 6 月。

22. 篠崎和紀，コンピュータ・セキュリティ対策の現状と課題，ジュリスト 834 号，1985 年 4 月。

23. 芝原邦爾，コンピュータ犯罪，法学教室 169 号，1994 年 10 月。

24. 芝原邦爾，コンピュータによる情報処理と業務妨害罪–改正案二三四条ノ二の検討，ジュリスト 885 号，1987 年 5 月。

25. 杉山徳明、吉田雅之，「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について，警察学論集 64 巻 10 号，2011 年 10 月。

26. 鈴木敏夫，ハイテク犯罪に関する国際動向–国際組織犯罪上級専門家会合における取組み–，警察学論集 51 巻 7 号，1998 年 7 月。

27. 瀬川晃，イギリスにおけるコンピュータ犯罪とデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月。

28. 曽根威彦，コンピュータとデータの保護，刑法雑誌 28 巻 4 号，1988 年 7 月。

29. 園田寿，不正アクセス，法学教室 228 号，1999 年 9 月。

30. 高石義一，コンピュータ犯罪の防止技術–メーカーの立場から，ジュリスト 834 号，1985 年 4 月。

31. 高橋郁夫，コンピューターの無権限アクセスの法の覚書—英国・コンピューターミスユース法 1990 の示唆，判例タイムズ 1006 号，1999 年 10 月。

32. 竹内直人，コンピュータ・システム安全対策についての警察の対応，ジュリスト 834 号，1985 年 4 月。

33. 露木康浩，不正アクセス行為の禁止等に關する法律について，ジュリスト 1165 号，1999 年 10 月。

34. 露木康浩，不正アクセス対策法制の在り方について—不正アクセス対策法制調査研究報告書を概観—，警察學論集 51 巻 7 号，1998 年 7 月。

35. 露木康浩、砂田務、檜垣重臣，不正アクセス行為の禁止等に關する法律の解說，警察學論集 52 巻 11 号，1999 年 11 月。

36. 鳥居壯行，コンピュータ犯罪とシステム監査，ジュリスト 834 号，1985 年 4 月。

37. 中森喜彦，コンピュータと文書犯罪，刑法雑誌 28 巻 4 号，1988 年 7 月。

38. 夏井高人，アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆，判例タイムズ 1008 号，1999 年 10 月。

39. 西田典之，コンピュータの不正操作と財産犯–改正案二四六条ノ二の検討，ジュリスト 885 号，1987 年 5 月。

40. 西田典之，コンピュータと業務妨害・財産罪，刑法雑誌 28 巻 4 号，1988 年 7 月。

41. 日本弁護士連合会，警察廳の「不正アクセス対策法の基本的考え方」及び郵政省の「電氣通信システムに対する不正アクセス対策法制の在り方について」に関するパブリックコメント公募に対する意見，自由と正義 50 巻 8 号，1999 年 8 月。

42. 檜垣重臣，不正アクセス行為の禁止等に關する法律，法律のひろば 52 巻 12 号，1999 年 12 月。

43. 広畑史朗，コンピュータ犯罪の実態とその対策―犯罪捜査の面から―，ジュリスト 834 号，1985 年 4 月。

44. 的場純男，コンピュータに関する刑事法上の問題点―主として立法的観点から，ジュリスト 846 号，1985 年 10 月。

45. 山口厚，電磁的記録と文書犯罪規定の改正–電磁的記録の不正作出(一六一条ノ二)を中心に，ジュリスト 885 号，1987 年 5 月。

46. 山口厚，アメリカにおけるコンピュータ・データの刑罰による保護，刑法雑誌 28 巻 4 号，1988 年 7 月。

47. 山口厚，アメリカにおけるコンピュータ犯罪処罰法，ジュリスト 846 号，1985 年 10 月。

48. 吉田雅之，特集・情報処理の高度化等に対処するための刑法等の改正–法改正の経緯及び概要，ジュリスト 1431 号，2011 年 10 月。

49. 吉田雅之，「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について，法律のひろば 64 巻 10 号，2011 年 10 月。

50. 渡邊卓也，サイバー関係をめぐる刑法の一部改正，刑事法ジャーナル 30 号，2011 年 11 月。

附件：建議修法及理由對照表。

現行條文	修　正　條　文	說　　明
第三十六章 妨害電腦使用罪	刪除	一、本章刪除 二、目前刑法之立法體系，本即強調以保護法益之種類作為章節之區別，並非屬混合式之立法方式，又依照我國刑法之修法歷程，於章名以及條文名本即容許以「之一」、「之二」等方式增列(刑法第十六章之一規定參照)，並無更動條次或條文之問題，故應依照本章之罪之保護法益而將本章置於適當之章節。 三、刑法之保護法益依學理可區分為個人法益、超個人法益或個人法益、社會法益或國家法益，並原則上特定犯罪類型應僅有保護特定單一法益，僅於加重減輕或限制罪責之情形下，始會以其他法益作為輔助判斷標準，例如在保護個人財產法益之毀損罪章(刑法第三十五章)中，所出現以社會法益作為判斷標準之「足以生損害於公眾或他人」之構成要件(刑法第三百五十四條規定參照)。然衡諸本章之罪，所保護之法益繁雜，可認僅係將與電腦相關之不適切行為類型化而成之規定，故此些規定應依照該規定之保護法益而回歸傳統刑法中保護該些法益的罪章內，並無獨立設置專章之必要。

—	**第十五章之一** **妨害網路秩序罪**	一、本章新增 二、基於為連接數台電腦而架構的網際網路已成為社會上的重要溝通機制，此種溝通機制的順利運作，已成為刑法上應予保障之重要利益。機制順利運作的基礎，即建立於使用此機制之社會大眾對於此種溝通機制之信賴，若要保護此種溝通機制，即必須要保護社會對於此種溝通機制之信賴，亦即社會對於網路安全秩序之信賴，故本章之保護法益即為社會對於網路安全秩序之信賴，而此種信賴關係之保護，與現行刑法分則各罪章均有不同，應有獨立設章之必要，爰新增本章。 三、本章所定之罪，其保護法益為社會法益，從而依刑法之立法體系，應將其列為社會法益之章節下，又此種對於溝通機制信賴之法益，與偽造貨幣、偽造有價證券及偽造文書罪章之保護法益相類似，故將本章列於偽造文書罪章之後。
—	**第二百二十條之一** 透過通訊線路，無故輸入他人帳號密碼、破解或迴避電腦登入控制機制，或其他相類之方法，使該電腦之登入控制機制失效，足生損害於公眾或他人者，處一年以下有期徒刑、拘役、科或併科五萬元以	一、本條新增 二、網路系統之使用，必須由電腦對於其他電腦作連線，於連線過程中，縱使使用者本身設有登入控制機制，亦可能遭到未經授權之他人以破壞或迴避等方式癱瘓，而與使用者電腦為不當之連線，並造成使用者對於網路秩序安全之不信賴，此種行為之危害性應已達科以刑事責任之程度，為保護社會對於網路系統中登入控制機制

	下罰金。	妥善運作之信賴，爰增訂本條。 三、本章之保護法益，係社會對於網路安全秩序之信賴，從而僅有在行為涉及網路機制使用時，始有處罰必要，故在此設置「透過通訊線路」之要件，以限制處罰範圍。此種通訊線路即係有線以及無線網路的總稱。 四、蓋登入控制機制亦屬一種電腦程式，電腦程式亦屬資訊科技的一環，資訊科技之發展會如此迅速，極大部分係因全球性、去中心化之檢視程式漏洞以及安全性測試行為，此些行為絕大多數未經授權，若刑法一概處罰，無疑是以刑法限制資訊科技發展。從而癱瘓登入控制機制之行為並非全部必須處罰，惟有會影響社會對於網路安全秩序信賴之行為始有處罰必要，故在此加上「足以生損害於公眾或他人之行為」之要件，以免刑罰範圍過度擴張。 五、由於本章之保護法益係社會基於電腦網路而生之通訊秩序安全之信賴，在此似有必要對於電腦或網路等資訊科技名詞下定義，然而一來若要完善保障此種通訊秩序，對於電腦網路等名詞應採最寬鬆之定義，並於構成要件中限制僅有足以建立此種通訊秩序者使得成為本條規範之對象，故縱未規定電腦之定義，對於適用最廣義定義之本條而言，亦不生太大影響。二來刑法體系中並非僅有本章使用電腦等名詞，若貿然採取最寬鬆之定

		義，則會造成其他罪章適用上之混亂，故本條對於上開名詞不特別另予定義。
—	**第二百二十條之二** 意圖變更或取得儲存於電腦系統中之電磁紀錄，對該電腦犯前條之罪者，處三年以下有期徒刑、拘役、科或併科十萬元以下罰金。 意圖減損電腦運作效能，對該電腦犯前條之罪者，處二年以下有期徒刑、拘役、科或併科七萬元以下罰金。 意圖瀏覽電腦內部資訊，對該電腦犯前條之罪者，處一年六月以下有期徒刑、拘役、科或併科五萬元以下罰金。	一、本條新增 二、社會上對於電腦網路使用產生不信賴之原因，即係若使用該溝通機制，即會使自己所使用的電腦系統遭到不利益，故對於意圖令使用者所使用之電腦遭到不利益之未經授權而破壞登入控制機制行為，對於造成社會上對於電腦網路使用不信賴之程度更加嚴重，應有加重處罰之必要，爰增訂本條。 三、然而對於使用者所造成之不利益亦有程度之分，故本條亦就所造成不利益之程度區分為意圖變更或取得儲存於電腦系統中之電磁紀錄、意圖減損電腦運作效能，及意圖瀏覽電腦內部資訊三類，並論以不同刑度。
—	**第二百二十條之三** 對於前條以外透過通訊線路而連線的電腦，無故變更或取得儲存於該電腦系統中之電磁紀錄，足以生損害於公眾或他人者，處一年以下有期徒刑、拘役、科或併科五萬元以下罰金。 對於前條以外透過	一、本條新增 二、除第二百二十條之二之情形外，在網路系統之使用中，縱經授權登入電腦，或未經授權但亦未至成立犯罪程度而登入電腦之情形，亦可能因無故變更或取得儲存於該電腦系統中之電磁紀錄、減損該電腦運作效能或瀏覽該電腦內部資訊而造成使用者對於網路秩序安全之不信賴，此種行為之危害性應已達科以刑事責任之程度，為保護社會上對於電腦網路系統

	通訊線路而連線的電腦，無故減損該電腦運作效能，足以生損害於公眾或他人者，處六月以下有期徒刑、拘役、科或併科三萬元以下罰金。 對於前條以外透過通訊線路而連線的電腦，無故瀏覽該電腦內部資訊，足以生損害於公眾或他人者，處拘役、科或併科一萬元以下罰金。	中電磁紀錄儲存安全性、電腦機能完善運作，及電腦內部資訊私密性之信賴，爰增訂本條。 三、本章之保護法益，係社會對於網路安全秩序之信賴，從而僅有在行為涉及網路機制使用時，始有處罰必要，並由於第二百二十條之二之情形已依該條規定加重處罰，故在此設置「對於前條以外透過通訊線路而連線的電腦」之要件，以限制處罰範圍。 四、又，無故變更或取得電磁紀錄、減損電腦運作效能或瀏覽電腦內部資訊等行為，並非皆會使得社會對於網路安全秩序失去信賴，若刑法一概處罰，即會過度擴張處罰範圍。從而僅在足以影響社會對於網路安全秩序信賴之行為時，始有處罰必要，故在此加上「足以生損害於公眾或他人之行為」之要件，以免刑罰範圍過度擴張。
—	**第二百二十條之四** 利用特定電腦程式所具備之破解、迴避電腦登入控制機制或其他使電腦的登入控制機制無法有效運作之功能，而犯第二百二十之一條、第二百二十之二條之罪者，加重其刑至二分之一。	一、本條新增 二、惡意程式之使用，足以使得登入控制機制之癱瘓更加快速且便利，並使得本不具電腦專業技術之行為人亦得以為此類行為，對於社會上就網路安全秩序之信賴感危害甚大，故對於使用惡意程式而不正連線之行為，應予加重處罰，爰增訂本條。 三、基於並無電腦程式係專供犯罪之用，且任何電腦程式皆可能用來犯罪之故，本條僅規定「利用特定電腦程式所具備之破解、迴避電腦登入控制機

		制或其他使電腦的登入控制機制無法有效運作之功能」之要件，而未對於「惡意程式」或「病毒程式」作定義。
—	**第二百二十條之五** 下列各款行為，處三萬元以下罰金： 一、以文字、圖畫或他法，公然介紹特定電腦程式的犯罪功能，並散布該程式者。 **二、**無故公開他人的帳號密碼及該帳號密碼所利用之電腦，或依知該帳號密碼所利用電腦之第三人之請求而告知該帳號密碼，足生損害於公眾或他人者。	一、本條新增 二、行為人雖未對於電腦為不正連線或連線後之不正行為，但對於使社會大眾輕易得以對特定電腦為不正連線之行為，仍可能對社會上就網路安全秩序之信賴感造成危害，故對於此類行為仍具處罰必要，爰增訂本條。 三、基於並無電腦程式係專供犯罪之用，且任何電腦程式皆可能用來犯罪，又惡意程式亦屬電腦程式，若貿然將製作程式之行為列為處罰規定，可能會造成以刑法限制資訊科技發展之情形，故若要抑止惡意程式之濫用，應就使用以及散布為規制之重點，故參考刑法第二百九十二條，設有「以文字、圖畫或他法，公然介紹特定電腦程式的犯罪功能，並散布該程式者」之要件，而未處罰製作程式之行為。 四、除惡意程式外，就以帳號密碼之輸入作為控制辦法之登入控制機制而言，帳號與密碼為最重要之判斷因素，若將帳號密碼以及該帳號密碼所使用之電腦公開或告知他人，無疑會使得該登入控制機制的正常運作全面崩毀，此種行為破壞社會上對於網路安全秩序信賴感之程度不亞於散布惡意程式之行為，故本條於處罰散布惡意程式行為外，亦處罰將帳號密

		碼以及該帳號密碼所使用之電腦公開或告知他人之行為。 五、將帳號密碼以及該帳號密碼所使用之電腦公開或告知他人之行為，雖於告知第三人的部分有極大部分會構成該第三人之幫助犯，然就保障運用帳號密碼以辨認身分之登入控制機制的角度言之，該告知行為亦為一加速此種制度崩潰之源頭，故無論是否會成立幫助犯，皆有處罰之必要。
—	**第二百二十條之六** 對於公務機關、金融機構、商業機構或其他保存多數人資訊之機構之電腦犯前五條之罪者，加重其刑至二分之一。	一、本條新增 二、由於公務機關等保存多數人資訊機構之電腦系統內部儲存大量多數人重要資訊，如被入侵即會造成社會恐慌，進而對於網路安全秩序之信賴減損甚大，因此對公務機關或保存多數人資訊之機構電腦之犯行加重刑度，以適當保護公務機關等保存多數人資訊機構之資訊安全，進而維護社會上對於網路安全秩序之信賴感。 三、本條所稱公務機關，係指電腦處理個人資料保護法第三條所定之公務機關。