99 年委託研究報告

網際網路隱匿與竄改身分之行為態樣及其防制技術研究

期末報告

計畫委託機關：國家通訊傳播委員會
中華民國100年11月

99 年委託研究報告

編號：NCCB99009

網際網路隱匿與竄改身分之行為態樣及其防制技術研究

期末報告

受委託單位

義守大學

計畫主持人

楊吳泉

共同主持人

蔣麗君

王三元

研究人員

林敬皇

鄭毓芹

本報告不必然代表國家通訊傳播委員會意見

中華民國 100 年 11 月

目　次

表　次

圖　次

提　要

關鍵詞：網際網路、隱匿技術、社交工程、網路實名制

一、研究緣起

網際網路蓬勃發展，主要是其具有匿名與自由的特性，並帶動多元化的網路應用於服務與創意產業發展，但是隨之也產生越來越多不當使用網際網路的行為態樣，如目前容易透過相關隱匿技術更改來源 IP 或網路身分，以隱匿與竄改身分方式，進行犯罪行為，增加各權責主管機關對於網際網路管理之複雜度，成為網際網路正常發展的一大挑戰。為有效解決網際網路身分隱匿與竄改問題，本研究以「研析網際網路隱匿與竄改身分行為態樣」、「研析國際對網際網路隱匿與竄改身分之管制措施及分工情形」、「分析探討網際網路隱匿與竄改身分行為防制技術」及「研提執行相關防制技術與機制之配套法規修訂建議草案」等四大面向的重要議題進行。

二、研究方法及過程

本研究計畫採質性研究，從瞭解研究背景開始，其次進行文獻探討，著重於網際網路隱匿與竄改身分行為態樣分析等面向；進而瞭解網際網路隱匿與竄改身分行為態樣分析相關技術與法規；同時，進行專家學者的訪談，再進行資料整理與調查結果分析；最後，提出網際網路環境隱匿與竄改身分行為管制政策之參考。研究主軸分述如下：

1. 網際網路隱匿與竄改身分行為態樣分析：藉由蒐集國內、外不實言論或資料散布行為之現況，分析網際網路隱匿與竄改身分之行為、我國政府對此現象之管制與監督責任，提出相關管制策略與法規。

2. 研析國際對網際網路隱匿與竄改身分之管制措施及分工情形：世界先進國家對於網路管制政策及法規，因國情、風俗民情等因素，採取不同層級的管制規範，本研究將廣泛蒐集世界先進國家(包括：歐盟、美國、德國、日本、韓國等)對網路管制相關政策與法規，綜整各國相關法令與規章，做為相關權責主管機關，推動網際網路環境隱匿與竄改身分行為管制政策之參考。

3. 研提網際網路隱匿與竄改身分行為防制技術：透過蒐集與分析現有網際網路隱匿與竄改身分各項行為與技術，研提現有網際網路相關服務提供業者隱匿與竄改身分行為防制技術。

4. 研提相關防制技術與機制之配套法規修訂建議草案：檢視現有法規及所研提之防制技術，研提隱匿與竄改身分行為防制技術與機制之配套法規修訂建議草案。本研究將從社會倫理面、制度面、教育面與技術面等研提相關建議，供我國相關主管機關參考。

所選擇之訪談對象包括具科技法律背景之專家學者，透過他們的專業意見，瞭解目前網際網路隱匿與竄改身分行為所導致之網路犯罪所涉相關法規規定與處罰。此外亦針對網際網路服務業者進行訪談，探析相關業者因網際網路隱匿與竄改身分行為所導致之困擾及其能提供相關的防制與控制服務。研究團隊藉由訪談業界與專家學者，以利瞭解我國於因應網際網路之隱匿與竄改身分行為時所面臨之問題，並提出相關建議。

三、重要發現

網際網路隱匿與竄改身分之行為可以根據「技術面」與「非技術面」來進行分類。非技術面的網路隱匿行為，在日常生活中及傳統的犯罪行為也經常被採用，例如：盜用他人身分、以人頭透過架設第三地之賭博網站躲避追緝等。技術面之行為則大多透過網路的特性，改變或欺騙來源端或目的端之網路識別。

網際網路隱匿與竄改身分行為非常多樣，防制方法主要可以分成「預防」與「追查」兩大方向。大部分的防制方法為建立相關的「預防」機制，如網路設備制定安全過濾規則、加強頻寬管理與即時告警、各類伺服主機與網路設備之弱點檢測與修補等；另外，則再建立可供驗證或查驗等之「追查」機制，如保存日誌以便查詢攻擊資料、反查使用代理伺服器之使用者真實IP來源。

網際網路隱匿與竄改身分及網路犯罪行為等議題與個人隱私、商業活動、網路犯罪等三個面向相關。目前世界先進國家對於這些犯罪類型之管制與法規，因國情、風俗民情等因素，採取不同層級的管制規範，本研究蒐集歐盟、美國、德國、日本、韓國等國家，對網路犯罪相關之法規規範加以整理分析。

各國對個人隱私之保護相關法規，可歸納出幾項原則：(1)使用個人資料需告知資料擁有者；(2)確保個人資料不會被毀損或不當使用；(3)使用個人資料需具正當性與合法性；(4)韓國特別規定個人資料須以真實姓名登入，不得匿名刊登。依我國修訂後之個人資料保護法之規定，已與其他國家在個資保護規定與目的相似。

各國在網路商業行為的規範，皆著重於消費者權益、個人資料及個人隱私之保護，並且對網路服務者提出相關管制或規範；

其目的除保護消費者，也在防止違法行為產生，故對於個人資料或通信紀錄之儲存與保護，皆加以規定。網路商業行為方面，為了能有效確認使用者身分以及使用者進行之行為，各國皆制定電子簽章法規，確保使用者個人隱私，以及與網路服務者間交易行為之保護。

綜觀各國對於網路犯罪所制定相關法規，均大同小異。法律的規範，主要是用來懲罰因不法而造成他人或國家、公眾損失者，或用於維護各種法益、公平性。因此，隱匿身分之行為，如未造成他人損失，則非法律條文中所須規範的特定行為。網路犯罪行為屬於科技犯罪，即是藉由資訊科技為工具，進行犯罪之行為。目前我國偵辦此類型犯罪事實行為之主管機關為警政署。警政署於2006年4月成立「科技犯罪防制中心」，其中網路犯罪為其重要偵查項目之一。對於網際網路竄改身分行為之法律規範，特別值得一提的是美國「身分竊盜法案」，該國透過專法來規範偽冒身分之行為。我國目前對於竄改及偽冒身分行為之相關法令規範，主要是透過刑法「竄改文書罪」及「詐欺罪」等進行規範。同樣有足夠之法令規範，應不必同美國一樣，為網際網路竄改身分行為設立專法。

四、主要建議事項

分析網際網路隱匿與竄改身分行為與其防制技術與機制，本研究認為現有的機制，對於網際網路犯罪行為預防及對犯罪者追查作業，均已經有相關的法令加以規範，現階段不需要進一步新增或修訂配套法規，主要理由及其說明如下：

1. 隱匿及竄改身分行為不一定造成國家、他人之損失，但如用以做為犯罪工具，必需加以制裁，惟現有法規足以規範，不須為制訂專法或修改現行法令。
2. 防制技術與機制中，現有法令已規範追查所須的紀錄機制，並依法提供給相關執法單位，進行追查。
3. 現有法令已規範服務提供者或管理者須善盡管理之義務，增加相關安全機制，以減少偽冒動機與門檻。
4. 我國在法規規範下，已實施部分實名制的情況下，已可強化追查之相關防制技術與機制。相較之下，民眾較缺乏的是對於這些追查機制的認知與理解。
5. 電子簽章技術及身分認證技術、安全通訊協定的法令規範及技術標準成熟，但缺乏有效的宣導及教育，不需制定新法規。

6. 許多安全機制與方法均已實施，並已有相關法令規範或管理辦法，無需再制訂新的配套法規；應強化現有法規宣導與執行，使得相關防制技術與機制落實，才更具實質效益。

（一）立即可行之建議

在法律宣導方面，目前在網路犯罪之規範，需使民眾瞭解網路犯罪與一般犯罪刑責相同。在個人資料隱私與權益部分，主要以個人資料保護法為主，並有著作權法可以加以輔助規範。在商業活動部分，主要以電子簽章法來推動電子交易之普及運用，確保電子交易之安全，促進電子化政府及電子商務之發展。對於網路犯罪行為之處罰，我國刑法第36章已明文規定妨害電腦使用罪，可延伸用以規範網路犯罪。依刑法第363條之規定，第358條至第360條之罪，須告訴乃論，因此，須讓受害者瞭解自身權利，若非個人提告，治安機關亦將無法受理辦案。故對於網路犯罪行為懲處之相關規範，應加強宣導與教育，且是當務之急，針對「網路行為」之適當教育與宣導，降低網路犯罪率是可期的。

在技術面，鑒於無線網路使用頻繁之現狀，建議應使用具安全性的無線網路資料傳輸加密機制，加強資料傳輸的私密性，例如使用通道加密技術與資料加密技術，如此便可解決或降低無線網路傳輸時可能造成重要資料遭竊取或被盜用之危險。

在制度面，目前已有相關偵查制度，包含保全資料儲存與維護，在網路犯罪偵查上，可以實際破案並具嚇阻作用。由於技術因素，網路犯罪常有破案耗時且不易偵破之情形，因此，對於負責偵辦網路犯罪人員之績效考核制度，應對有功人員適度的給予獎勵，以利增加員警破案與負責之意願。此外，建立完善之培訓計畫與制度，可讓負責網路犯罪偵查之專業人力在科技專業知識與技術上，能不斷的接受學習、教育之機會，以利因應各種網路犯罪行為態樣。同時，亦應建構完備之防制網路犯罪宣導制度，讓使用者與負責人員瞭解網路犯罪之嚴重性與相關刑責，減少網路犯罪之可能性。而對於個人隱私權之合理保護，必須讓每一位網路使用者與資訊、企業負責人員瞭解隱私權基本保護原則與相關法規，以免觸法及造成被害人之損失。

本研究根據所發現網際網路隱匿與竄改身分行為可能引發之問題與現況，並參酌通傳會權責，提出通傳會在監理通訊與傳播市場時，可能執行之措施與建議：

1. 強化與其他網路主管機關、業者之合作

對於網際網路匿名與竄改身分行為所產生之犯罪追查等問

題，通傳會在行政部會與管理業界方面，可扮演積極主動的角色，透過建構跨部會會議或計畫性單位，如：由通傳會召集內政部、法務部、經濟部、交通部及金管會等組成「防制網路犯罪技術工作平台」（此工作平台雖由通傳會召集，但犯罪偵防工作仍是內政部警政署之職責），共同研議網路犯罪防制措施。建議此工作平台在必要時，除應由通傳會邀集所管電信事業參與外，仍應由其他行政機關視需要邀集ICP、IPP等相關業者共同參與，例如由經濟部邀集電子商務業者，以強化與其他網路主管機關、業者之連結與合作，共同打擊因匿名與竄改身分所導致之網路犯罪行為。同時，通傳會已經建構電腦危機處理中心(NCC-CERT)，亦可考慮強化其功能或利用其資訊分享與分析中心(NCC's Information Analysis and Sharing Center, NCC-ISAC)，強化區域聯防之合作架構與組織等，讓電信與資訊通訊服務業與政府合作，成為維護網際網路資通安全新的典範。

2. 鼓勵各類網路服務業者持續發展與採用相關防制技術

鼓勵各類網路服務業者，包括網際網路接取服務提供者(Internet access service provider, IASP)、網際網路平臺提供者(Internet platform Provider, IPP)及網際網路內容提供者(Internet content provider, ICP)，持續發展與採用相關防制技術，如：IP追查的技術、安全的傳輸協定、頻寬管理與即時告警、主動弱點管理、安全代詢伺服器名單及對其內部伺服器或使用者採行登入憑證身分認證技術(如PKI等機制)等。其中IPP、ICP部分雖非通傳會主要權責範圍，但可透過與經濟部等其他網路主管機關進行橫向連結與溝通，共同推動獎勵或鼓勵其所轄業者持續發展與採用相關防制技術，讓所轄業者能夠善盡其管理責任，並有利於警調機關、業者本身追蹤與防制隱匿身分與竄改身分所造成之網路犯罪問題。

（二）中長期性建議

在社會倫理面，網際網路提供許多不同於傳統之服務方式，如消息傳遞、購物方式等皆因網際網路蓬勃發展而轉型。因此在網際網路中也應該要有一套資訊倫理規範讓使用者遵守，這些資訊倫理規範須為能夠被網路使用者所能接受之合理規範，例如使用者利用網際網路進行活動時之相關禮儀與道德，以及對個人隱私應有之尊重。

在技術面，現行網際網路的認證方式，多以設定帳號與密碼的方式來完成。但此方法已被證實可透過封包監聽以及暴力攻擊等手法來加以破解，甚至在網路上已有公開的工具可輕鬆破解存

在於Cookie 的帳號密碼。配合民眾對於網際網路相關知識已日益提升，在無需匿名考量的情況下（例如網路報稅，並無涉及言論自由，故無需以匿名方式為之），可以鼓勵業者能夠結合電子憑證的身分認證方式來提供相關服務，必能大幅降低網際網路服務遭盜用所衍生出的犯罪問題，以及治安機關在犯罪偵查作業上較為容易實施。

在制度面，雖然因為網際網路快速發展，增加各權責單位管理上之複雜性，但制定清晰的主管機關權責劃分之標準，如以事前預防、事中偵測及事後鑑識等區分各主管機關業務所需負責之作為與工作，讓相關單位可以清楚瞭解各單位權責，以利網路犯罪偵防。以各機關須管制之犯罪行為而言，相關機關須自訂一套防制網路犯罪機制，才可真正讓網路充分發揮其正面功能。

最後在教育面部分，我們認為法律規範只能治標無法治本，唯有透過教育才能將網路犯罪防制機制落實。本研究建議透過教育部制定相關網路犯罪教育課程，從中小學開始進行相關基礎教育，如關於網路犯罪與法律之宣導等，進而推動到高等教育，避免青年學子以匿名應用網路時，在未知網路犯罪相關規定之下誤觸法規，或是不知網路犯罪法規處罰之嚴重性，而意圖犯罪。除此，教師之培訓也相當重要，唯確實儲備充足具有相關網路犯罪防制能力之優良師資，才能有效傳遞、教導相關法規、網路倫理規範及網路知能予各級學生。法務部已有個人資料保護法種子教師培訓研習會，各校應該鼓勵相關老師參與，以利培訓相關師資教導學生。透過網路犯罪防制教育之延伸與落實，將有助於降低網路犯罪之發生。

Abstract

Keywords: Internet, spoofing technique；social engineering；Internet real-name system

A. Research origin

The development of the Internet is characterized by its roots in anonymity and freedom. More recent use has seen commercialization in service and innovation industries, such as internet sales and procurement and information search. Internet has provided much convenience, but, by it's open nature, also allows inappropriate online behaviors and risk against information security. Issues of concern include anonymity, impersonation, slander, hacked websites, malicious programs which cause damages to data, and stolen personal or organizational data. The convenience and development of Internet provides a target for criminal types and increased complication for the related agencies which handle Internet issues. This research aims to explore Internet anonymity, hidden and impersonated identity behavioral styles, the regulations and protections against Internet anonymous and impersonated identity behavioral styles and suggestions to revise the related regulations. In order to examine these issues, the research purposes are (1) to collect and analyze Internet anonymous, hidden and impersonated identity behavioral styles; (2) to explore the policies and regulations for the issues related to Internet identity impersonation in other countries; (3) to explore protection technology against Internet impersonation in terms of technical means; (4) to provide relative protection technology and suggestions in accordance with prevention of Identity impersonation behaviors.

B. Research method and research flow

This research is a qualitative study, and it aims to understand the importance and reasons of the topical issues so literature reviews are related to Internet anonymous and impersonation behavioral styles. In-depth and focus group interviews are also used in this research. Finally with research results, the relative regulations and policies are provided. The research is divided into four research dimensions as follows:

1. Behavioral analysis of anonymous and falsified ID: upon gathering behavioral research regarding domestic and foreign opinions towards data security, this study analyzes Internet hidden and falsified ID behaviors and the relative laws and policies regulated and managed by the government.
2. Analysis of the international regulations and management against Internet anonymous and falsified ID: The world countries have applied different regulations and policies against Internet hidden and falsified ID because of distinct cultures and customs. This study collects their laws and regulations to provide reference for Taiwanese related agencies.
3. Study of protection technology against Internet anoymous and falsified ID: Via the collection and analysis of Internet anoymous and falsified ID behaviors and protection technology against Internet hidden behaviors, this study explores protection technology offered by current Internet services providers for the prevention of Internet hidden and falsified ID behaviors.
4. Study of drafts and suggestions for laws and regulation revisions in accordance with protection technology and mechanisms: the relative suggestions are provided in terms of the view of social ethics, institutions, education and technology for related agencies.

In-depth and focus group interviews are used in this research to understand the status quo of Internet anonymous and impersonation behavior. The interviewed include Internet service providers, experts and researchers familiar in the fields of Internet technology and cyber laws to offer their opinions and suggestion regarding the prevention of InternetIdentity issues. Finally with research results, the relative regulations and policies are provided to the related agencies as reference materials.

C. Important research finding

Internet anonymous, hidden and impersonated Identity behaviors are divided into technical and non-technical dimensions. In the non-technical dimension, Internet anonymous Identity behaviors are frequently applied in daily life and traditional criminal behaviors, for instance, stealing IDs, websites setting at another location to prevent tracing. Conversely, the behaviors in the technical dimension change or deceive source side and the

destination of Internet ID in accordance with Internet characteristics. Internet anonymous and impersonated ID behavioral styles are much diversified. Therefore, combatting malevolent behaviors is divided into prevention and investigation. The former is concerned Internet security filtering rules to assist bandwidth management and to provide real-time alerts. These rules may also reveal Internet vulnerabilities along with providing security for DNS services; the latter is related to verification or checks, for instance, record reservation, attack data, proxy IP.

This research gathers the regulations or laws related to Internet malevolent behaviors made in European Union (EU), Germany, America, Japan and Korea. These malevolent behaviors concerned individual privacy, commerce activities and cyber-crimes. Nowadays, advanced countries, such as Germany, America, have different regulations against these behaviors because of distinctive cultures and customs. In terms of individual privacy, there are several principals: (1) to inform the data owners when using individual personal data; (2) to ensure individual data is protected from inappropriate use; (3) to ensure legitimacy and justice when using individual data; (4) In Korea, the government has regulated real name log in, especially using individual data. According to Taiwan 2010 Personal Data Protection Act, the content and purpose concerning individual data protection is accordance with other countries.

The purpose of Internet criminal regulations is to punish those who have caused the nation, the public or others loss and to protect justice. Therefore, Internet anonymous or hidden identity behaviors are not specificly behavior regulated by the laws. Cyber-criminal behaviors are categorized as technical crimes, that is, criminal behaviors use information technology to do illegal activities or affairs. Nowadays, the National Police Agency (NPA) is charged with investigating these Internet crimes. In April 2006 the Technology Crime Prevention Center has been established within the NPA in order to investigate cybercrimes. Currently, Internet impersonation and counterfeit identity behaviors are regulated by the criminal law concering tampering with documents and fraud crimes. Therefore, it is unnecessary to make specific laws for punishing Internet behaviors. Further, the department of Commerce is charged with both commerce management and e-commerce related to information technology.

D. Main suggestions

In accordance with current protection technology and systems against Internet hidden and falsified ID behaviors, the study provides the suggestion that it is unnecessary to revise or increase laws or regulations to enhance the protection of Internet hidden ID behaviors or investigate. The main explanations are as follows:

1. In discussing Internet hidden and falsified ID behaviors, the unique change is the criminal tool, but not individual behaviors. Therefore, the current laws are enough to regulate the Internet malevolent behaviors.
2. In discussing protection technology and mechanisms, the current laws have already regulated to keep the records facilitate relative agencies to investigate Internet hidden and falsified ID behaviors.
3. The current laws have regulated services providers or managers to do management in order to enhance security to avoid the falsification.
4. Under the regulations and laws, part of systems use real-name enough to investigate falsification.
5. It is lack of dissemination and education of ID certificate, Internet Protocol and technical standardization for users, but not new laws or regulations.
6. Many security mechanisms and means have realized; meanwhile there are relative laws or regulations to execute them. Therefore, to enhance public exposure of laws is more important than to make new laws.

I. Instant and practical suggestions

In the perspective of law dissemination, the government has to let citizens understand the punishment of Internet crimes as well as general crimes. Regarding personal privacy and rights, Personal Data Protection Act is the main law and Copyright law is the subsidiary law to protect Internet privacy. In the perspective of commercial activities, Electronic Signature Law is the key law to realize electronic trade and ensure e-trade security in order to enhance the development of e-government and e-commerce. Concerning the punishment of Internet crimes, Penal Code Chapter 36 proclaimed in writing to regulate the crime of obstruction of computer use which can be extended to regulate Internet crimes.

From the perspective of technology, the study suggests use of more secure means to send information with encryption in order to enhance privacy of sending information. From the perspective of institutions, there is the investigation system, including maintenance of data storage which is helpful to deter internet crimes. The study suggests providing suitable systems for investigating cybercrime in order to increase the motivation of policemen to detect crimes. In addition, it is necessary to build a good system for investigating cybercrime to learn new technology and knowledge to confront various cybercrimes.

According to problems and status quo caused by Internet hidden and falsified ID behaviors and the NCC accountability, the study provides several suggestions as follows:

1. To enhance the cooperation between network units in charge and industry.

   NCC in administration departments can play an active role via cross-agencies meeting or projects, for example: NCC organizes a technology platform against cybercrimes with the Ministry of the Interior, the Minister of Justice, the Minister of Economic Affairs, the Minister of Transportation and Financial Supervisory Commission to discuss measures against cybercrimes. When it is necessary, NCC can invite the telecommunications industries, and also ICP and IPP to attend the platform. Meanwhile, NCC has already established NCC-CERT and NCC's Information Analysis and Sharing Center which can strengthen the cooperation framework and organization of regional defenses. Then, telecommunications industries have opportunities to cooperate with the government.

2. To encourage the industry to continue developing and adopting protection technology

   It is necessary to encourage industries to continue developing protection technology against Internet falsified ID behaviors, such as secure Internet protocol, bandwidth management and real-time alerts, proactive vulnerability management, and user login credentials which adopt identity authentication technology (e.g. PKI and other mechanisms).

II. Mid and long term suggestions

In the Internet, a set of information ethics should be built for users to follow. These ethic norms are reasonably accepted by online users, i.e. online users respect privacy when using the Internet.

For the dimension of technology, the industries are encouraged to use electronic certificates for ID authentication against Internet falsified ID behaviors or other cybercrimes.

For institutions, the fast development of the Internet increases the complexity of management; therefore, clear standardization to define accountability is necessary, i.e. the roles of prevention, detection and forensics are decides in advance to distinguish responsibility among administration agencies.

Finally, upon education, only education can carry out the protection mechanism against cybercrimes. This study suggests the Minister of Education draw up courses related to cybercrimes for students in primary and middle schools using a course, such as cybercrimes and laws in educate how to avoid cybercrimes. In addition, it is important to cultivate teachers who can teach laws, cyberethics and related knowledge for students to avoid malevolent Internet behaviors.

第一章　緒 論

網際網路蓬勃發展，主要是其具有匿名與自由的特性，並帶動多元化的網路應用於服務與創意產業發展。但也因此產生越來越多不當使用網際網路的行為態樣，增加各權責主管機關對於網際網路產業發展管理複雜度。在 2009 年 11 月行政院研考會的調查發現，電話與網路詐騙為民怨之首(網路票選為第二大民怨)，其原因和整個市場技術和科技快速的分工及整合有關。以下將就網際網路隱匿與竄改身分行為態樣背景與相關議題，做簡要的介紹與說明。

第一節 計畫緣起

近幾十年來隨著電腦的普及與網際網路的蓬勃發展，除改變人們的生活方式，亦帶來採購等交易的便利性。舉凡人們生活中所需的交易與資訊，皆可在網際網路上搜尋查獲相關資訊。而網際網路為人們帶來生活便利性的同時，也伴隨產生許多資訊安全隱憂，例如惡意程式的散播與攻擊，造成組織系統與資料的毀損、駭客入侵網站竄改網頁，甚至竊取個人與組織重要資料或癱瘓組織系統等。根據財團法人資訊工業策進會/經濟部技術處「創新資訊應用研究計畫」(Foreseeing Innovative New Digiservices, FIND)統計，2009 年第 2 季臺灣經常上網人口為 1,060 萬人，網際網路連網應用普及率為 46%，由於網路使用快速成長，藉由網路產生的新興犯罪行為亦不斷增加。

網路犯罪與一般犯罪並沒有差異，只是犯罪者利用網際網路做為犯罪工具，達成其犯罪目的，所以，作為工具的網際網路本身是無罪的，重點是在於使用者的行為。而欲進一步規範網際網路使用，可對網際網路進行規範，如網路交易通常會留下痕跡，而參與的廠商，如：網際網路接取服務提供者(Internet access service provider, IASP)、網際網路平臺提供者(Internet platform Provider, IPP)及網際網路內容提供者(Internet content provider, ICP)等，所留有的連線內容必須由需求單位透過執法單位發出正式請求，才能取得相關紀錄資訊。目前因應網路行為之相關規範是由各個不同之主管機關管理，更讓業者可能不服從非其目的事業主管機關之規範，進而造成犯罪追查之困難。舉例來說，商業交易行為(網路購物)就與經濟部商業司有關係，但因與網路接取服務業者管理有關，因此也和國家通訊傳播委員會的業務有關[71]。此外若是使用者不具誠信意圖，將真實自我隱匿而做出違法事情

時，將造成難以評估之傷害，如網路流氓對他人惡意攻擊事件發生於韓國，韓國電視明星鄭多彬以及流行女歌手 Yuni，因為無法忍受發布在網上論壇的匿名惡意評論和人身攻擊，憤而自殺身亡。另一個案例，一名美國女中學生旅遊回來後，發現班上沒有人願意與她聊天，原因是有人匿名使用手機簡訊，傳播她在旅途中感染上「重症急性呼吸系統症候群」(Severe Acute Respiratory Syndrome of Unknown Etiology, SARS)的流言。如此不實言論透過網路特性，對他人造成名譽傷害，可說是「網路欺凌」的行為[81]。

依據「內政部警政署警政統計通報」統計報告，可以瞭解我國網路犯罪[11][55]之現況與類型，2010 年 1-10 月電腦網路犯罪發生數共 15,115 件，其中主要亦為「詐欺案」共 7,463 件(占 59.37％)為最多，「妨害電腦使用」共 3,079 件(占 20.37％)次之；「侵害智慧財產權」主要在網路上販售大補帖、違法張貼、下載散布他人著作及販賣仿冒品等案件，共計 2,251 件(占 14.89％)為第三；「妨害名譽(信用)」:在網路上公然侮辱或誹謗他人、侮辱誹謗死者、妨害他人信用等共 874 件(占 5.78％)為第四[17]。由上述統計可知，國內網路犯罪情況仍不容忽視，犯罪手段大都是利用網際網路之匿名性、無疆界性與自由性等特性，透過網路為工具，犯罪行為雖然可以與一般犯罪行為對照，但影響層面與速度更為廣泛快速，許多犯罪行為必須跨部會協調溝通，確實是一個不容忽視的議題。

第二節　計畫目的

為有效解決網際網路身分隱匿與竄改問題，本研究以「研析網際網路隱匿與竄改身分行為態樣」、「研析國際對網際網路隱匿與竄改身分之管制措施及分工情形」、「分析探討網際網路隱匿與竄改身分行為防制技術」及「研提執行相關防制技術與機制之配套法規修訂建議草案」等四大面向的重要議題進行，主要內容分述如下：

1. 蒐集與分析目前常見網際網路環境隱匿與竄改身分行為態樣。
2. 蒐集與分析國際主要國家(包含：歐盟、美、德、日及韓國等國家)對此議題相關對策。
3. 針對網際網路隱匿與竄改身分技術(包含：「網際網路通信協定(Internet Protocol，IP)」欺騙(IP spoofing)、代理伺服器(proxy)等技術)及行為模式與防制技術，以及追查各方 IP 位址及實際所在位置技術，從技術面與法規政策

面進行完整之分析探討。

4. 綜合整理上述各項研究之成果，研提執行相關防制技術與機制之配套法規修訂相關建議。

第三節 計畫研究範圍

為進行網際網路隱匿與竄改身分之行為態樣與防制技術研究，本研究蒐集各國有關網際網路隱匿與竄改身分相關法規，並透過訪談政府機關構(例如：法務部等相關權責機關)、專家學者、ISP 業者等，此外也邀請專家學者進行座談對於此議題建議與對策作深入討論與溝通。綜整所蒐集之資料、專家學者意見、座談會意見，提出本報告作為國家通訊傳播委員會(以下簡稱通傳會)及政府相關權責機關推動網際網路產業發展及擬訂法規與管理政策規劃之參考。本研究共計訪談 9 位專家見表 1-1 所示。

表 1-1 訪談對象

訪談對象代號	服務單位	訪談時間
A-1	成功大學科技法律研究所(南部)	99 年 11 月 11 日
L-2	金石國際法律事務所(南部)	99 年 12 月 10 日
G-1	義守大學電算中心(南部)	99 年 11 月 30 日
G-2	法務部資訊處(北部)	100 年 01 月 07 日
G-3	法務部調查局(北部)	100 年 01 月 07 日
P-1	資策會科技法律中心 (北部)	99 年 11 月 19 日
P-2	國家高速網路與計算中心(南部)	99 年 12 月 03 日
P-3	中華電信公司(南部)	99 年 12 月 11 日
P-4	中華電信公司(北部)	100 年 01 月 25 日

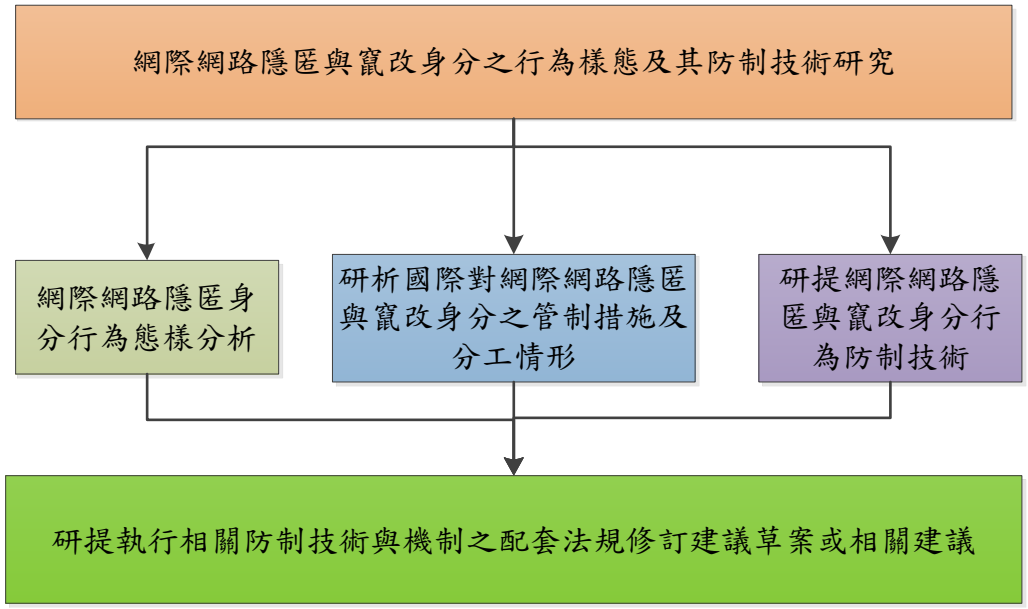
資料來源：本研究整理

第四節 研究方法與步驟

一、 研究方法說明

本研究計畫採質性研究，「網際網路隱匿與竄改身分之行為態樣及其防制技術研究」係由四個主要分項為研究主軸，如圖 1-1 所示，進行步驟分別由行為態樣現況分析、政策、法規及技術各

面向深入探討，整理分析各項研究成果，提供通傳會及各權責主管機關，推動網際網路產業發展法規及管理政策規劃參考。



資料來源：本研究整理

圖 1-1 計畫架構圖

(一) 網際網路隱匿與竄改身分行為態樣分析

藉由對於網際網路相關的行為、技術、現象之觀察與資料蒐集，分析現存於網際網路隱匿與竄改身分之行為態樣，並歸納整理成相關行為模式，作為本研究相關防制技術、法規政策面及建議之用。

(二) 研析國際對網際網路隱匿與竄改身之管制措施及分工情形

目前世界先進國家對於網路管制政策及法規，因國情、風俗民情等因素，採取不同層級的管制規範，本研究將廣泛蒐集世界先進國家(包括：歐盟、美國、德國、日本、韓國等)對網路管制相關政策與法規，綜整各國相關法令與規章，作為相關權責主管機關推動網際網路環境隱匿與竄改身分行為管制政策之參考。

(三) 研提網際網路隱匿與竄改身分行為防制技術

透過蒐集與分析現有網際網路隱匿與竄改身分各項行為與技術，研提現有網際網路相關服務提供業者因應隱匿與竄改身分行為之防制技術。

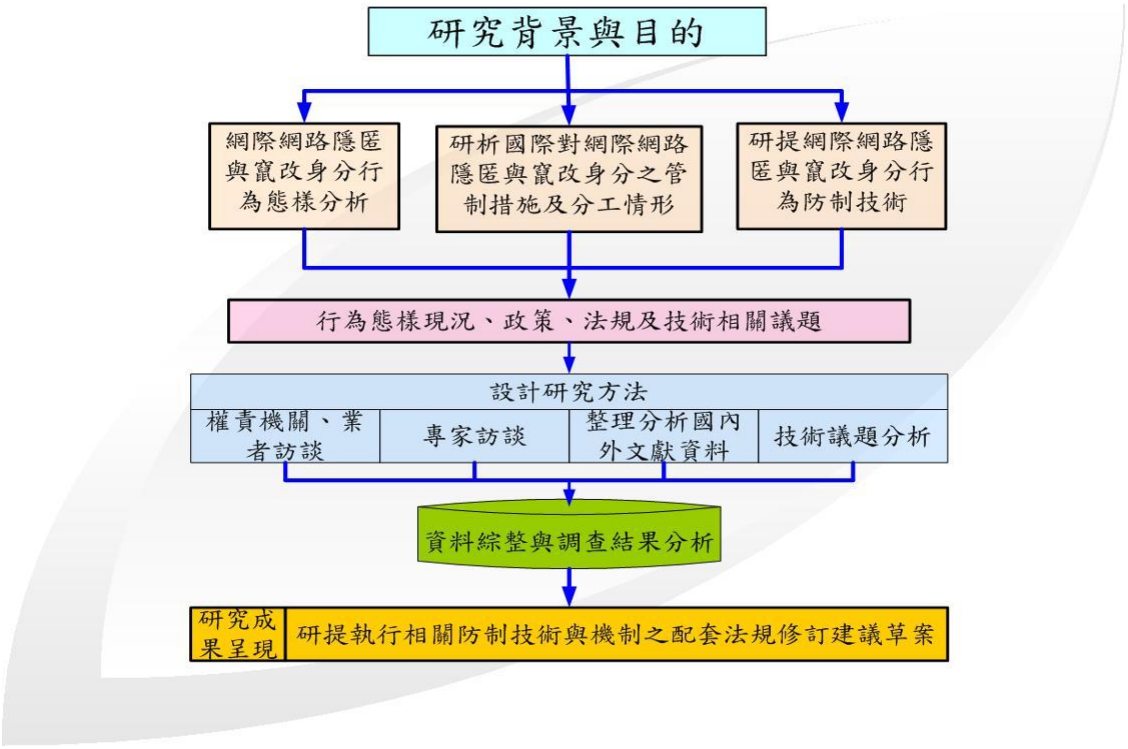
(四) 研提相關防制技術與機制之配套法規修訂建議草案

檢視現有法規及前項(三)所研提之防制技術，研提隱匿與竄改身分行為防制技術與機制之配套法規修訂建議草案或相關建議。本研究將從社會倫理面、制度面、教育面與技術面等研提相關建議，供我國相關主管機關參考。

二、 研究步驟說明

本研究流程係從瞭解研究背景開始，其次進行文獻探討，著重於網際網路隱匿與竄改身分行為態樣分析等面向；進而瞭解網際網路隱匿與竄改身分行為態樣，並分析相關技術與法規；同時，進行專家學者的訪談，並進行資料整理與調查結果分析；最後，提出網際網路環境隱匿與竄改身分行為管制政策之參考，如圖 1-2 所示。

本研究訪談對象選擇具科技法律背景之專家學者，透過專業意見瞭解目前我國對網際網路隱匿與竄改身分行為所涉網路犯罪之相關法規規定與處罰，並蒐集、汲取渠等寶貴經驗及建議。此外，研究團隊亦訪談網際網路服務業者，探析相關業者在因應網際網路隱匿與竄改身分行為所導致之困擾時，其能提供的相關防制與控制服務。研究團隊藉由訪談聽取業界與專家學者意見，並分析所蒐集相關技術及國際上先進國家之法規制度，以利瞭解面臨隱匿與竄改行為所可能衍生之犯罪問題，並提出相關管理方式與防制方法，供相關單位參考。



資料來源：本研究整理

圖 1-2 研究方法及進行步驟流程圖

第五節 報告架構說明

本研究旨在探究網際網路隱匿與竄改身分之行為態樣及其防制技術，研析目前相關網際網路隱匿與竄改身分之防制技術是否足以有效打擊可能之犯罪行為，並提出建議供通傳會及政府相關主管機關作施政參考。

本研究首先蒐集與分析國內外相關之網際網路隱匿與竄改身分行為態樣與相關防制技術研究文獻與現況資料，並經由隱匿與竄改身分行為、法規與技術的文獻回顧與評析，擬定訪談題綱，並藉由訪談結果修訂分析結果與建議；同時，列舉相關防制技術與機制及可能的配套法規修訂建議，經反覆修正後，研提最終之建議。

為滿足本計畫所研究議題，應考量之範圍涵蓋行為現況、政策、法規、技術...等，故本研究廣泛蒐集下述文獻資料，進行深入研究，作為本研究的基礎資訊：

- 國內內政部警政署所調查或統計的全國資訊調查資料。
- 蒐集世界各國對網際網路隱匿與竄改身分行為之相關對策，包含歐盟、美國、德國、韓國、日本等國家。

- 整理分析網際網路隱匿與竄改身分行為常用技術包括：各類連線欺騙行為、代理隱匿行為與會話劫持行為。
- 整理歸納各種網際網路隱匿與竄改身分之行為態樣並分析相關防制技術，包括追查各方 IP 位址及實際所在位置技術。

本報告第一章為說明研究的緣起、目的與架構。本研究將隱匿與竄改身分行為態樣分為技術面及非技術面來描述：非技術面之行為態樣主要是透過不當程序，例如：捏造假身分、使用公共電腦上網等，來躲避追蹤與偵查；技術面之行為態樣主要透過網路特性，以各種技術改變或欺騙上網來源及身分識別，如各種連線欺騙行為、代理隱匿行為、利用虛擬私密網路(Virtual Private Network, VPN)上網。本研究已完成網際網路隱匿及竄改身分相關技術、文獻資料及行為的蒐集，相關描述，請參見第二章。

網際網路隱匿與竄改身分議題牽涉到三個面向：「個人隱私」、「商業活動」以及「網路犯罪」。目前世界先進國家對於這些犯罪類型之管制與法規，因國情、風俗民情等因素，採取不同層級的管制規範，第三章蒐集先進國家，包括：歐盟、美國、德國、日本、韓國等國家，對網路犯罪相關之法規規範，分析各國常見網際網路隱匿與竄改身分之行為態樣與我國政府部門對此議題執掌與分工情形，以及世界主要國家對此議題相關對策。

網際網路隱匿與竄改身分行為非常多樣，防制方法主要可以分成「預防」與「追查」兩大方向。大部分的防制方法為建立相關的「預防」機制，如網路設備制定安全過濾規則、加強頻寬管理與即時告警、檢測主機與網路設備之弱點、DNS 服務安全檢測等；驗證或查驗之機制即為「追查」，如保存日誌攻擊資料、反查使用 proxy 之 IP 來源。這些相關防制技術會在第四章加以描述分析，研提網際網路隱匿與竄改身分所使用與可防制技術，並提出可能追查各方 IP 位址及實際所在位置之技術。

除了文獻資料蒐集之外，本研究報告完成共 9 位專家學者與業者訪談，並舉辦與 5 位專家學者的座談會，以便能將研究整理分析所得之各行為態樣、各國法規以及防制技術互相印證，進而更深入了解現狀。關於訪談與座談相關說明及分析參見第五章。

第六章則根據文獻蒐集整理、訪談及座談之專家學者建議、現有法令規章等，從社會倫理面、制度面、教育面與技術面等研提相關建議，供相關主管機關參考。我們將現有追查與預防之相關法規與規範加以整理說明，並列出現有對應之法規規範配套。據此，本研究發現在現有法令規範情況下，針

對網際網路隱匿與竄改身分行為之防制，應透過社會倫理面、制度面、教育面與技術面等著手即可，並無迫切修訂專法或修正既有法規以規範此類行為之需求，相關理由說明於第六章第二節。最後第七章綜整相關研究結論。

第二章　網際網路隱匿與竄改身分行為態樣分析

第一節 隱匿與竄改身分行為定義

「匿名性」普遍被視為是網路的基本特性之一，使用者在網路上將其真實身分全部隱藏或是部分隱藏，並可隨意使用網際網路服務，如：線上交友、線上會員註冊、線上遊戲等。學者王勝毅指出網際網路虛擬環境中有下列的行為特質[20]，包含：

(一) 無疆界性：虛擬的網際網路空間並無「領域疆界」（Territorially Based Boundaries）之限制，因為在網際網路上訊息的傳輸不會有物理所在位置上的阻隔，資訊可在有網際網路連結的地方進行傳輸與散布；

(二) 使用者匿名性：網際網路是一種開放式的網路系統，除非特定網站設置管制措施，欲進入網路空間之人，並不需要提示個人身分或輸入密碼即可進入使用或接觸資訊，因此，如果使用者不願自行提供個人的基本資料如姓名、年齡、國籍、性別或職業時，任何人很難單純從網路活動中察知其現實世界上的真實身分；

(三) 資訊公開性：網路使用者雖具有隱匿性的特質，不過對於資料的取用則是公開、無限制的共享，一旦網際網路使用者將資料上傳至網際網路上之某一位置，除非將資料加密或是在存取時要求進行身分驗證，否則會有上傳即公開之情形。

因此，王勝毅進一步指出網際網路虛擬特性已造成「主體身分的不確定性」，在網際網路上，不會有人知道使用者現實生活中之實際身分，而且也不知實際居住所在地[20]。同時也可推想出「主體身分的不確定性」兩項特質：

(一) 行為主體現實社會中的身分特徵，如姓名、住址、性別、年齡、外貌、職業、身分地位、聲音特質及行動等，在網路空間裡均無法藉由對方之網路活動確認之；

(二) 行為主體所處的位置或地理環境等場所資料，亦無法藉由網路上數位行為所展現的微弱訊息得到充分的確定性。

廣泛而言，匿名性是一種出於某種目的而不表明自己身分或者不知道其身分(個人特徵)的一種行為，使用匿名性可能是保護自己的權利，如受訪者身分或投票者身分之保護。網路匿名性的優點可以隱匿其真實世界的身分，拉開與真實世界的距離；藉著網路的匿名功能，卸下真實世界的人際關係的牽絆之後，反而能夠

促成一些在真實世界中不可能發生的人際關係。也就是說，由於身體不在場所造成的隔離功能，反而使網路空間能夠形成一些在現實社會生活中不易形成的人際關係。這是因爲網路的匿名功能使人們不必擔心身體在人際互動過程中受到侵害；其次，匿名功能使人們在網路空間中的身分和角色只是以 ID 代號的形式出現，人們不僅可以決定透露那些自己的個人資料，而且還可以控制自我呈現的方式，甚至重新塑造一個新的自我[68]。

依上述可知，因網際網路之特性為無疆界性、使用者匿名性與資訊公開性等，讓使用者可以隱匿現實生活中的真我，包括姓名、性別與年齡等，而在網路空間中可以自由發揮創意、發表言論等，享有不受限制的自由性。同樣地，也可以用來化身成另一人的身分，遂行犯罪或惡意行為，以規避偵察。在犯罪理論中有名的 M-O-P 犯罪理論所認定之三要素為：犯罪的動機(Motivation)、有犯罪的標的物(Object)以及不存在抑制犯罪發生的保護環境(Protection)三個因素。而網路匿名性符合則給予了P(Protection)這個因素，因此，網際網路的犯罪者經常使用隱匿身分與竄改身分來掩蓋所施行之犯罪行為，躲避追蹤與偵察，逃避須擔負之相關法律責任[62][69]。

網際網路使用者匿名性之特性，也造成了網路犯罪者進一步藉由身分隱匿與竄改技術來躲避追查，避免犯罪者真實身分資訊之暴露。事實上透過某些偵查技術，再配合相關日誌資料紀錄查詢，仍然能夠關聯出所欲隱匿的犯罪者真實身分，如：犯罪者在家中使用 ADSL 上網連結到線上論壇，透過論壇 ID 登入張貼辱罵他人文章，雖然該論壇 ID 並不代表個人真實身分，但可藉由原先的論壇 ID 註冊資訊以及其連結到論壇的網路位置(IP Address)，進而追蹤該 IP 的網際網路接取服務提供者（Internet Access Service Provider, IASP)，而 IASP 為了收費，存有犯罪者現實生活中的真我之資訊，所以，還是有機會透過技術層面的追蹤，找出犯罪者之真實身分。

因此，我們可以定義網際網路上之隱匿身分，是透過各種方式隱藏網際網路上所使用的身分識別與現實生活身分識別的一種行為。隱匿身分有很多種的方式達成，如：化名、冒名、偽造及竄改識別等。故隱匿身分雖包含竄改身分之行為，但是隱匿身分是網際網路的特性之一，目的可能是為了保護真實世界的自我，不一定是為了遂行犯罪或惡意之行為，而竄改身分的行為，則多是為了避免所施行的犯罪或惡意行為被追蹤或偵察。表 2-1 說明兩者間關係與異同。

表 2-1 隱匿身分與竄改身分之定義

項目	隱匿身分	竄改身分
定義	透過各種方式隱藏網際網路上所使用的身分識別與現實生活身分識別的一種行為。	利用冒用、偽造等方式，取得並使用網路或現實生活中身分識別之行為。
目的	1. 保護真實自我。 2. 保護隱私。 3. 施行犯罪或惡意行為。	施行犯罪或惡意行為。
網路常見的犯罪行為態樣	1. 化名或匿名使用網路服務，如：匿名郵件或垃圾信件等。 2. 隱匿身分執行遠端入侵攻擊。	1. 冒用身分使用網路服務，如：張貼文章、發布不實消息、偽造假網站等。 2. 盜用身分竊取隱私資料，執行遠端攻擊。

資料來源：本研究整理

第二節　網際網路隱匿與竄改身分行為態樣分析

網際網路隱匿與竄改身分之行為可以根據「技術面」與「非技術面」來進行分類。非技術面的網路隱匿行為，在日常生活中及傳統的犯罪行為也經常被採用，例如：盜用他人身分、以人頭透過架設第三地之賭博網站躲避追緝等。技術面之行為則大多透過網路的特性，改變或欺騙來源端或目的端之網路識別。相關行為態樣分析如下：

一、 非技術面之網際網路隱匿與竄改身分行為態樣分析

非技術面之分類中，並非隱匿與竄改身分之行為不需要以技術為背景進行，而是其大多為容易實行之行為，技術成分較低，主要是用以躲避追蹤與偵查之用，主要的行為態樣有 2 種：

(一) 偽冒身分及位置

冒用身分是透過雙方資訊不對等來進行欺騙或偽冒身分識別之行為，在網際網路中，許多常見的身分識別，由於匿名性的特性，讓使用者有機會利用來偽冒身分，常見的有：

1. 使用公共電腦匿名上網。
2. 改變電子郵件收件者(回覆信箱)或寄件者欄位等，寄出偽冒之電子郵件。

3. 以化名申請或租用虛擬空間、網路帳號。

4. 冒(盜)用他人之帳號，登入網路遊戲、論壇、即時通訊軟體(如MSN、ICQ、YAHOO!即時通、QQ 等)等，獲取利益或散布謠言。

5. 捏造虛偽資料、虛擬人物、公司行號以騙取他人信任。

6. 使用他人之通訊網路，如無線網路之訊號容易擷取，因此容易造成使用者藉由無線網路進入區域網路，且難以追蹤上網之位置，此一行為稱為利用無線網路溢波(沒有加密的無線網路)。

7. 取得網路交易資訊，偽冒賣方送電子郵件給買方假的付款帳號。

其中又以利用無線網路隱匿位置最值得注意，目前使用廣泛之無線網路設備為 Wi-Fi 聯盟所認證之 IEEE 802.11x 系列產品，主要有 IEEE802.11a/b/g/n 等系列。

無線網路傳遞資料之方式常見的分為兩種方式：設備對設備直接傳輸之 Ad-Hoc 方式以及利用無線存取點(Access point, AP)傳輸方式，提供給更多行動設備使用網路。為了方便，很多場所都有自行架設無線 AP 提供無線使用網際網路。

相較於有線網路，無線網路訊號是全向廣播且會穿透建築物，因此更容易被有心人士擷取使用。尤其是隨著大功率天線的應用，任何溢波的範圍都有可能成為惡意駭客的入侵點，使無線網路也可能被用來作為入侵內部有線網路，成為駭客進行攻擊的跳板。雖然可以透過安全之連線方式，如 WPA(Wi-Fi Protected Access)或 WPA2 保護，但在方便使用之考量下，許多無線網路設置者(例如：民眾在家中自行架設 AP 供自己使用)並未對無線網路採取保護措施，便容易遭受有心人士利用這些未經授權之無線網路訊號連上網際網路。

就追緝網路犯罪行為角度觀之，網路連線紀錄可以追蹤到無線 AP 連線之 IP 位址等資訊。一些犯罪行為為了逃避警方追蹤，往往特意搜尋可用之無線網路溢波或是公開無線網路訊號上網，造成犯罪調查時，只能追蹤到被盜用者身分。這類犯罪行為主要特徵為使用者上網 IP 不固定，容易達到隱匿身分之效果。偵辦上，須透過實際上網地點或是由犯罪目標逐步鎖定可疑對象[51][76]。

無線網路所具備之移動性令犯罪偵查更為艱鉅，主要原因為(1)沒有生物跡證、(2)沒有目擊者、(3)無人使用管理、(4)區域廣泛沒有實體範圍限制、(5)誤導偵辦，例如歹徒利用受害者無線溢波當跳板，須經過搜索才能確定是否有犯案動機。這些因素讓牽扯到利用無線網路所遂行之網路犯罪案件在破案上之困難[23]。

(二)　合法掩護非法

是指犯罪人透過不相關之合法身分，申請連線遂行非法的行為。當追蹤或偵查時，只會找到合法的身分，但卻找不到真正遂行非法行為的當事人。常見的有：

1. 盜版軟體、色情網站及賭博網站架設在沒有司法互助的第三地，無法追蹤。
2. 取得假證件或以免登記資料之方式，購買 3G 網路帳號、申請郵政信箱、撥接帳號等。

此兩種不同的隱匿與竄改身分行為類別大多發生於傳統的電腦與網路犯罪行為，如：「網路賭博」、「網路詐騙」、「網路毀謗」及「電腦竊用」等。且多數的行為搭配網際網路相關技術、協定或社交工程等完成更為複雜之犯罪或惡意目的。

二、 技術面之網際網路隱匿與竄改身分行為態樣分析

網際網路服務已經深入我們的生活，隨之而來的是要如何克服在網際網路上的犯罪預防與追查等議題，其中不可避免的便是防制網際網路隱匿與竄改身分行為的技術研究。這些相關研究與網際網路基本技術[8][37][89]息息相關。本節將以技術面角度來探討，改變或欺騙來源端或目的端網路識別之行為。網路犯罪者為了獲取不法利益並且避免犯罪追蹤，常常會將網路隱匿與竄改身分行為結合遠端入侵攻擊，這些會被混合運用之行為包括隱私資料竊取、殭屍網路控制以及令 IASP 業者頭痛不已之「分散式阻斷服務攻擊」(Distributed Denail of Service, DDoS)等。本計畫研究範圍主要探討網路隱匿與竄改身分行為，因此不就遠端入侵攻擊進行探討。我們將常見之隱匿與竄改身分行為與技術分為三大類，分別為連線欺騙行為、代理隱匿行為與會話劫持行為，分別說明如下：

(一) 連線欺騙行為

透過技術或協定本身的弱點來達成連線欺騙，如：IP 欺騙(Internet protocol spoofing, IP spoofing)技術、ARP 欺騙(Address resolution protocol spoofing，ARP spoofing)技術、DNS 欺騙(Domain name service spoofing, DNS spoofing)技術等各類欺騙技術，分別說明如後。

1. IP 欺騙(IP spoofing)技術

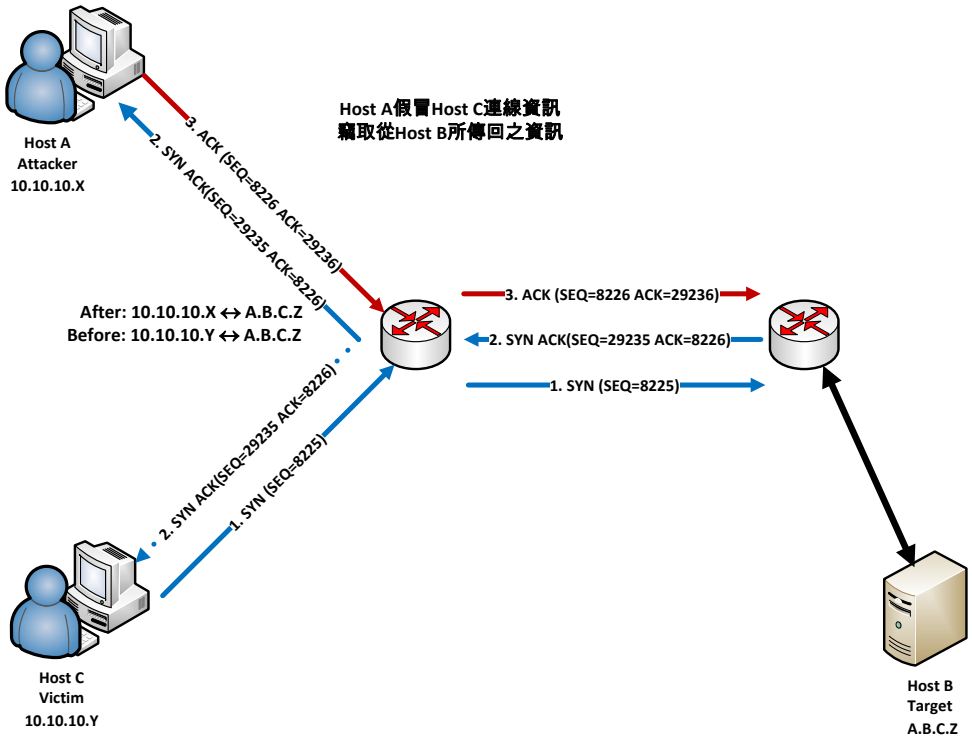
IP 欺騙攻擊是指攻擊主機藉由假冒合法之 IP 位址來欺騙受攻擊的主機，企圖讓受害主機無法追溯攻擊來源。IP 欺騙為網路通訊協定第三層之攻

擊行為，主要被駭客用來隱藏真實身分與位置，佯裝入侵者來自於可被信任網路，藉以進行後續攻擊入侵。IP 欺騙技術會更改封包來源位址，隱藏駭客真實所在位置，將來源位址更換成可信任的網路位址，讓封包看起來像是來自於可信任的網路，符合封包過濾規則(Packet Filtering)，而允許進入路由器或是防火牆； 目的地的主機收到這些封包後，會發出回應到已經被修改過的來源位址。IP 欺騙攻擊依其發生的網路環境，又可分為 Non-Blind IP 欺騙技術與 Blind IP 欺騙技術兩類。Non-Blind IP 欺騙技術通常發生在區域網路當中，亦即攻擊者可以監聽到 TCP/IP 內容；Blind IP 欺騙技術發生較常發生在廣域網路當中，攻擊者無法有效監聽到所有 TCP/IP 內容。

Non-Blind IP 欺騙技術指攻擊者可以監聽到 TCP/IP 內容，進而偽造出正確序號的 TCP 封包，達到欺騙的目的，通常發生在同一區域網路當中。攻擊者發出已經修改來源位址後的假 TCP/IP 封包，藉由攻擊者假造的 TCP/IP 封包在區域網路中建立攻擊端與目的端之間的通訊，欺騙本地端之路由器，進而監聽受害主機之通訊，竊取隱私資訊或誘導受害主機連至惡意網站，如圖 2-1 所示。Blind IP 欺騙發生在廣域網路當中，攻擊者無法監聽受害主機資訊，為了確保 Blind IP 欺騙能夠成功，攻擊者一般先將阻斷攻擊(Denial of service, DoS)結合 Blind IP 欺騙技術，藉由發生大量假冒合法 IP 的攻擊流量，癱瘓受害主機與目標主機之聯繫，以利於攻擊者後續與目標主機連線之動作。由於無法正確假造連線回應資訊，攻擊者往往會事先與目標主機正常連線，猜測網路連線協定序號增加方式，藉以取得與目標主機之連線，如圖 2-2 所示[9]。

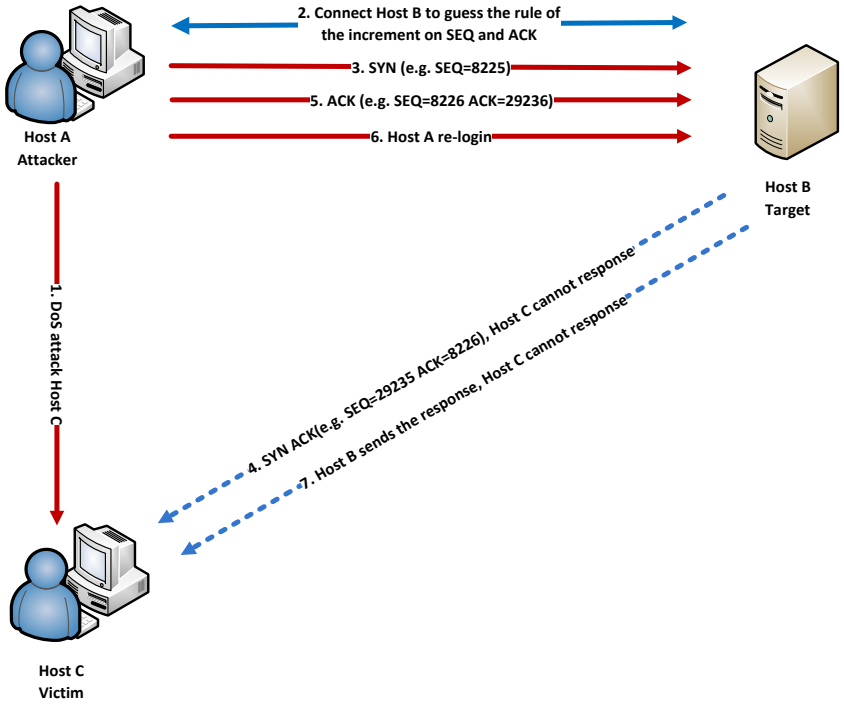
網路犯罪者常用的 IP 欺騙工具很多，這些工具的發展減低了網路犯罪的技術門檻，為網路犯罪者大開方便之門。如：2009 年美國麻省理工學院所發展的 The MIT ANA Spoofer Project 就發展了許多的 IP 欺騙工具，其中 Spoofed IP、Anonymity，最為簡單且常用：

- Spoofed IP：除了提供修改 IP 位址與 MAC 位址功能外，也支援掃描區域網路中所有存活主機的 MAC 位址與所開啟的網路埠口。
- Anonymity：幫助使用者修改、利用 Fake IP Addresses 瀏覽網站，避免由網路封包洩漏真實的網路位址。此種工具常被網路犯罪者採用躲避以網路位址為主的追蹤方式。



資料來源：本研究整理

圖 2-1 Non-Blind IP 欺騙技術示意圖

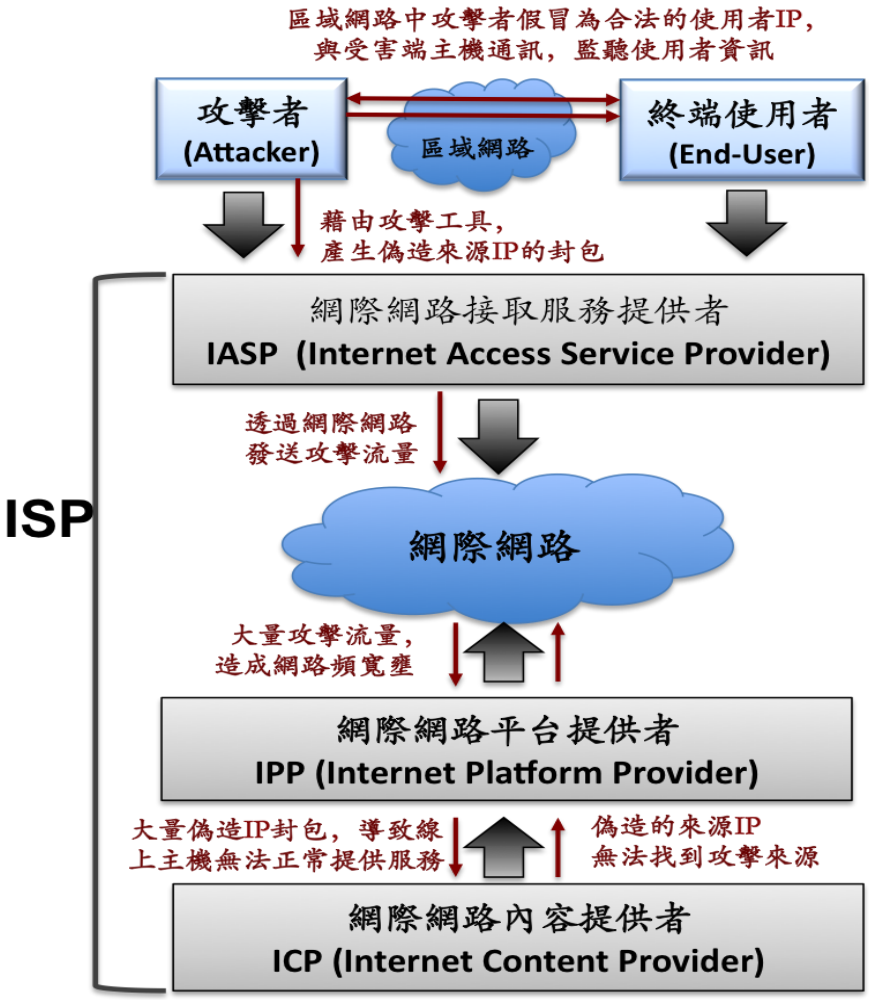


資料來源：本研究整理

圖 2-2 Blind IP 欺騙技術示意圖

網路犯罪者藉由操作 IP 欺騙工具軟體，執行 IP 欺騙攻擊，圖 2-3 為 IP 欺騙攻擊的一種範例，利用假 IP，隱匿攻擊來源來進行 DoS 攻擊。攻擊者首先利用這些工具來產生偽造來源 IP 的連線，IP 欺騙若是發生在區域網路中時，IP 欺騙最主要之目的為假冒區域網路中合法使用者，以監聽區域網路中其他使用者的資訊，此時搭配上 MAC 欺騙將會讓區域網路中其他主機認為網路犯罪者才是連線目標主機，藉此監聽區域網路中其他主機間通訊訊息。若是 IP 欺騙結合 DDoS 攻擊發生在網際網路中時，大量的攻擊流量將會造成網路設備無法負荷，造成網路頻寬壅塞，使得服務主機無法正常提供服務，受害端也因為攻擊來源位址是偽造的，因此無法成功找出攻擊位址，加以定罪。

美國麻省理工學院有鑑於 IP 欺騙犯罪問題日益嚴重，在 2009 年提出了 The MIT ANA Spoofer project，發展了一套工具稱為「Spoofer」，幫助網路管理人員有效偵測 IP 欺騙，找出網路中 IP 欺騙之真正攻擊主機位址，「Spoofer」可找出網站中哪些瀏覽者使用偽造(Fake) IP。由已被駭客攻陷的電腦稽核檔中找尋、比對出與 IP 欺騙相關之攻擊，並藉由這些資訊嘗試追蹤駭客真實 IP 所在。ANA 計畫並提供了一份報告證明 Spoofer 工具可真正幫助 IP 欺騙偵測。實際上，有很多工具都可以幫助網路管理者偵測 IP 欺騙，成功的追蹤 IP 欺騙攻擊的真實攻擊來源 IP 是非常困難的，需要搭配網際網路接取技術提供者與受攻擊者路由器日誌紀錄兩者，方可完成網路犯罪者真實身分的追蹤。

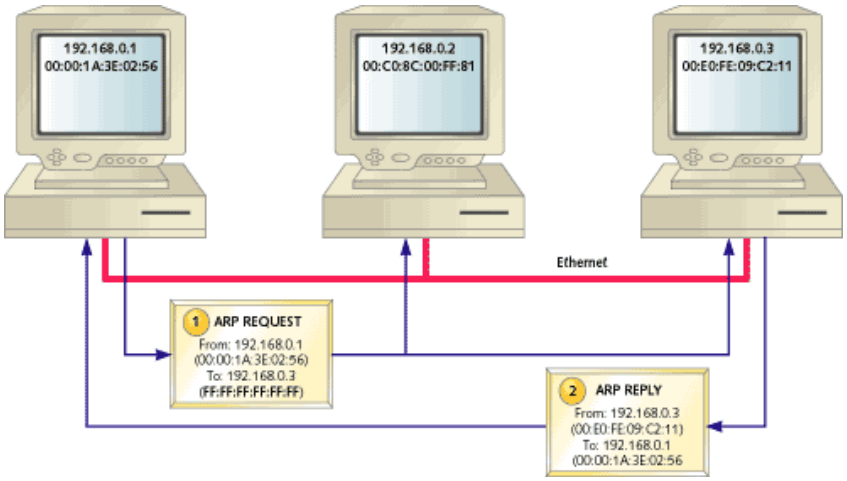


資料來源：本研究整理

圖 2-3 利用欺騙的假 IP 隱匿攻擊來源來進行 DoS 攻擊

2. ARP 欺騙(ARP spoofing)

ARP 是負責將 IP 位址轉換成 MAC 位址的一種通訊協定，當某一台電腦要傳送資料到某個 IP 位址時，會先傳送 ARP 封包詢問網路上哪台電腦的 MAC 位址對應到這個 IP 位址，當目的端的電腦接收到這個 ARP 封包之後，便會回應給來源電腦，以進行資料傳送。而在網路上的電腦與網路設備為了減少 ARP 封包對網路頻寬的影響，都存有一份暫存快取(Cache)紀錄，因此當有 ARP 封包經過時，電腦或是網路設備可儲存相對應的 IP 與 MAC 位址，這就是 ARP 暫存快取。往後可不需要再發送 ARP 封包便可直接傳輸資料，可減少對網路頻寬的影響。ARP 運作原理如圖 2-4 所示，若要查看本機的 ARP 暫存快取，可在命令模式中執行 ARP -a，如圖 2-5 所示。



資料來源：
http://www.netrino.com/images/articles/ARPRequestReply.gif

圖 2-4 ARP 運作原理示意圖

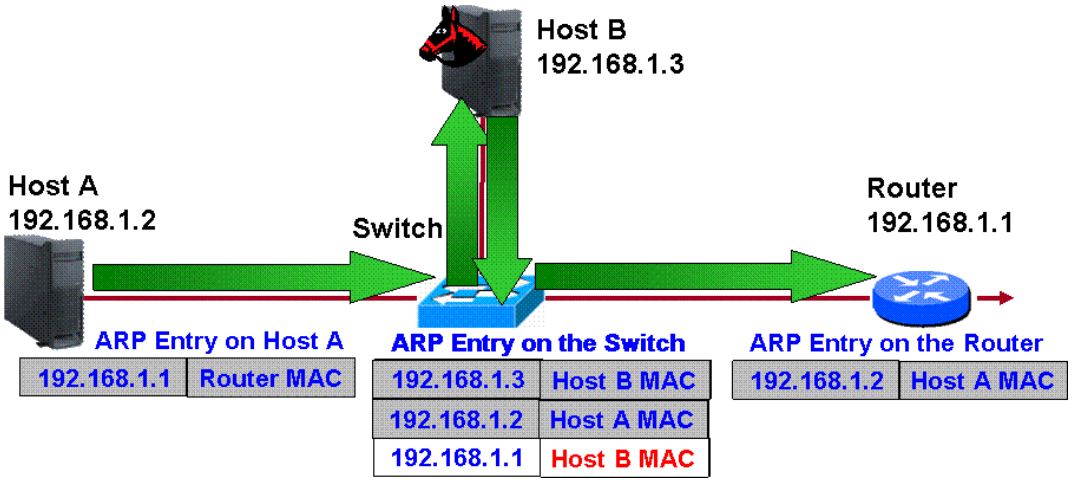
```
C:\Documents and Settings\WinXP_User>arp -a

Interface: 192.168.1.11 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0c-29-b2-88-c9     static
  192.168.1.2           00-0c-29-1e-54-e7     static
  192.168.1.12          00-0c-29-da-72-88     static
```

資料來源：本研究擷取畫面

圖 2-5 ARP 指令執行

ARP 欺騙的運作是由攻擊者發送假的 ARP 封包到網路上，尤其是送到閘道器上。其目的是要讓送至特定 IP 位址的內容被錯誤送到攻擊者所擬取代的地方。攻擊者可將這些竊取所得內容另行轉送到真正的閘道或是篡改後再轉送。由於一般的 ARP 暫存快取是根據經過的 ARP 封包變更本身的 ARP 列表，藉以查詢主機之 IP 位址與 MAC 位址對應，因此若是接收到的 ARP 封包所提供的對應資料是偽造的，就會讓資料無法傳輸到實際的目的地。有可能因為資料導向某特定電腦，駭客可利用病毒竊取封包資料或修改封包內容，如圖 2-6 所示。駭客進行 ARP 欺騙攻擊，修改了網路設備 Switch 的 ARP Cache 所記錄對應資料，如將 192.168.1.1 的 MAC 位址，指向駭客所在(HOST B MAC)，因此，當 HOST A 要傳送資料給 Router 192.168.1.1 時，所傳送的資料將會被駭客所監聽，竊取與修改。



資料來源：
http://www.trendmicro.com.tw/support/downloads/images/arp3.gif

圖 2-6 ARP 欺騙攻擊示意圖

現今 ARP 欺騙問題日益嚴重，網路犯罪者會利用 ARP 欺騙攻擊，感染內部網路某一主機後，將此主機 MAC 位址對應均指向含有惡意程式的網站，因此，所有與這台內部主機的連線都會被導向此惡意程式網站，遭受惡意程式感染，由此可知，網路管理者需特別注意網路內 ARP 欺騙情況。

常用的 ARP 欺騙工具有 SpoofMAC、ARPoison、ETTERCAP、THC-Parasite，分別簡述如下：

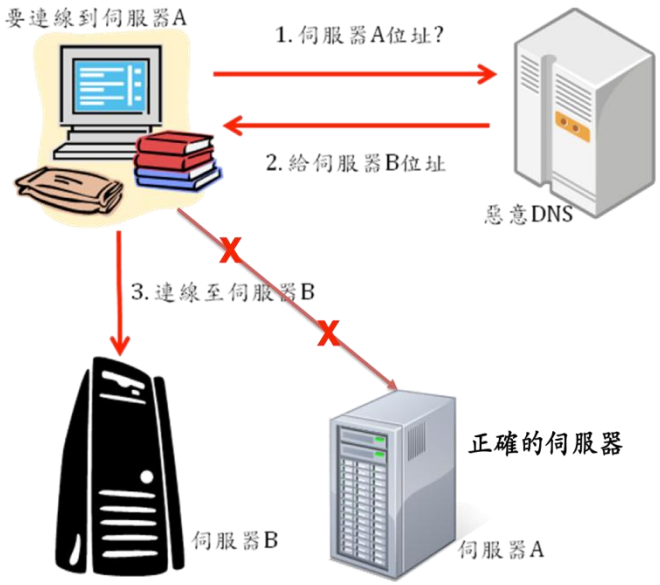
- SpoofMAC: 簡單且功能強大，為可修改網路位址與網卡 MAC 位址的工具，提供命令列模式與圖形介面模式，並具有系統日誌紀錄功能。
- ARPoison：為一輕量級命令列模式工具，能夠簡單修改本機端的 ARP 暫存快取的網路位址與 MAC 位址互相對應，藉以竊取網路傳輸資訊。
- ETTERCAP：自動化 ARP 欺騙工具，可偵測區域網路內所有 IP 位址與 ARP Table，也能夠竊取已加密的 SSH Sessions 帳號密碼，進行 ARP 欺騙攻擊與 OS Fingerprinting。
- THC-Parasite：主動式 ARP 欺騙攻擊工具，攻擊者只要設定好 ARP 欺騙資訊後，Parasite 將會對網路內所有 ARP 連線，自動回應 Fake MAC Address，一段時間後，網路內所有主機 ARP 暫存快取將會被修改。犯罪者可輕易將此工具與惡意程式站台結合，強迫受害主機瀏覽惡意程式站台。

為了要防止 ARP 欺騙攻擊的發生，建議重要網路設備啟用 Dynamic ARP Inspection 功能，檢查 ARP 訊息並拒絕假的 ARP 封包，此外可設定重要主機的 ARP 暫存快取為固定模式，ARP 欺騙病毒將無法動態修改 ARP Cache，避免區域網路內大量 ARP 欺騙攻擊的發生。網路管理者也可利用 ARP 欺騙偵測工具，偵測網路上是否有主機已遭受到 ARP 欺騙病毒的感染，常見的工具：

- Wow! ARP Protector ：為一自由軟體，可幫助保護電腦避免遭受 ARP 欺騙與攻擊，並可監聽 ARP Table 改變狀態。
- ARPCacheWatch：監控 IP 與 MAC 位址對應情形，找出多個 IP 位址對應同一個 MAC 位址，避免 ARP 欺騙攻擊發生。

3. DNS 欺騙(DNS spoofing)技術

DNS 欺騙是另一種常見之連線欺騙技巧，當傳送伺服器 A 的網址給合法的 DNS 伺服器時，DNS 伺服器會回傳一組對應到該網址的 IP 位址，好讓我們能夠正確的連上伺服器 A。攻擊者若是將該網址傳給惡意的 DNS 伺服器(被入侵的 DNS 伺服器或是攻擊者自行架設可以監聽 DNS request 的惡意 DNS 伺服器)，該伺服器可能會回傳錯誤的 IP 位址，例如是另一個伺服器 B 位址，導引我們連接到一個事前偽造、乍看下像是我們要連上的伺服器 A，實際上卻是在瀏覽伺服器 B 之網站內容，而伺服器 B 中可能放了大量的惡意連結誘使我們點擊，趁機竊取使用者資訊或是植入木馬等惡意程式，如圖 2-7 所示。

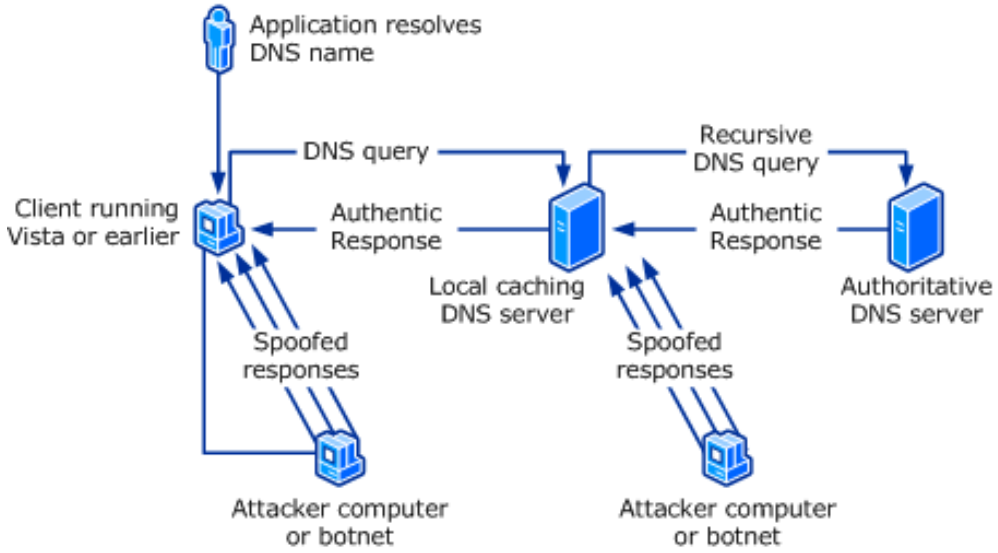


資料來源：本研究整理

圖 2-7 DNS 欺騙示意圖

DNS 欺騙攻擊工具中較著名的有 Zodiac 與 ADM DNS Tool，Zodiac 為 DNS 協定分析工具與 DNS 欺騙攻擊工具，Zodiac 能夠分析 DNS 查詢路徑，並假造惡意 DNS 封包進而影響正常的 DNS 運作。ADM DNS Tool 採用主動與被動方式攻擊 DNS 查詢封包與 DNS Server。

DNS 欺騙藉由竄改 DNS 網域名稱查詢的結果，傳回假冒的網路位址給使用者，使用者在沒有辦法判斷真假的情況下，連線到假冒的網站造成嚴重的損失；或是進入其網站首頁或網站中的不特定連結，均會被攔截轉址到某特定的惡意網站。一般人在上網時，皆透過 DNS 伺服器詢問該網域名稱所對應的 IP 網路位址，然而，DNS 通訊協定並未進行加密或身分認證，所以網路犯罪者可對 DNS 伺服器或是使用者進行欺騙連線。如圖 2-8 所示。攻擊者可假造或更改 DNS 查詢結果，以欺騙使用者對錯誤的網路位址進行連線，或是當 DNS 伺服器上沒有所查詢的網域紀錄時，DNS 伺服器向外查詢時，傳送惡意的 DNS 查詢結果給 DNS 查詢伺服器。



資料來源:

http://technet.microsoft.com/en-us/library/ee649205%28WS.10%29.aspx

圖 2-8 DNS 欺騙攻擊

綜觀 IP Spoofing，ARP Spoofing 與 DNS Spoofing 攻擊，皆與網路協定、網路結構與犯罪模式有關。由於現在通用之 TCP/IP 連

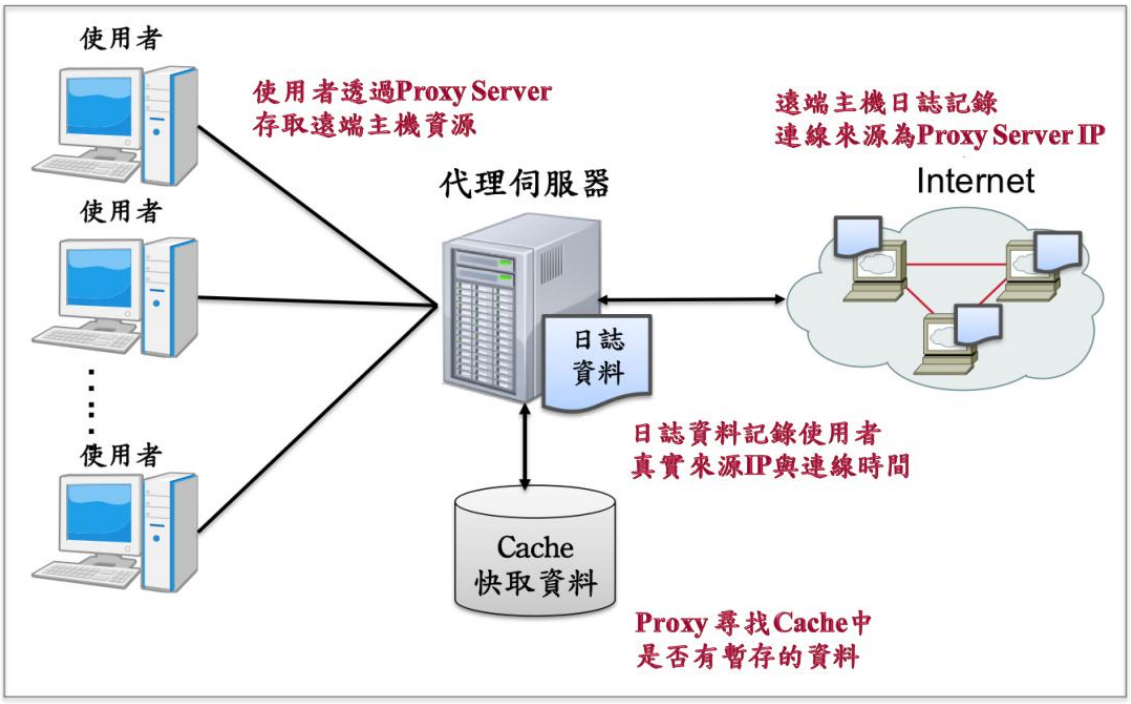
線存在許多缺點，存心不良且具有技術的人員可以藉由這些缺失欺騙連線，用來隱匿與竄改身分。這些欺騙技術隨時在增加與進步，但網路業者也有許多相對應的因應之道來防制這些行為，如：透過設備監看網路攻擊的發生等，這些防制方法主要利用紀錄檔追查，因此必須保留記錄檔與有效分析記錄檔內容所包含的欺騙行為。

(二)　代理(Proxy)隱匿行為

代理(Proxy)技術是利用轉送等方式將使用者的封包轉向成由代理伺服器所發出。因此，有心人士可以在代理伺服器掩蓋其真正的來源，透過多重轉向的方式，則真正來源的追蹤愈是困難，其行為主要用以掩蓋上網的來源與痕跡，避免追蹤。當然許多隱私保護的擁戴者及犯罪者也同樣喜歡利用這樣的方式來掩蓋追蹤。常見的技術有：代理伺服器(Proxy Server)、Tor 網路、VPN 通道技術，分述如下：

1. 代理伺服器(Proxy Server)

Proxy 就是在網路上的某一部伺服器，原先是因為要節省對外頻寬所設計，提供網路使用者作為暫存快取(cache)之用，以加快存取速度。代理伺服器會將使用者曾連線網站的網頁內容暫存在代理伺服器硬碟中，所以當有用戶透過代理伺服器上網時，代理伺服器會先檢視硬碟當中是否有暫存網頁的資料，若是硬碟中存有暫存網頁資料時，代理伺服器就會送出硬碟中的暫存網頁資料，而非真正的連線到遠端網站中；若是硬碟中沒有網頁資料時或是資料已經過期，代理伺服器才會真正連上遠端網頁取得資料，並回傳給使用者，另外保留一份副本在代理伺服器硬碟上。也就是說，使用者不論要連往哪裡，其實都是只連結到代理伺服器，再由代理伺服器向真正主機要求連線。當使用者使用代理伺服器連線到遠端主機時，是由代理伺服器連線到網際網路網站，由此可知，該被連線網站所記錄 IP 位址是代理伺服器的位址，而非使用者電腦 IP 的位址，有心人士可以利用代理伺服器的特性達到隱藏 IP 的效果。代理伺服器也是駭客獲取攻擊資源的目標，當使用者在沒有使用加密連線下，透過代理伺服器連上網路時，使用者瀏覽網頁的歷程、使用者真實連線 IP 與時間以及曾經輸入的帳號密碼等，皆會儲存在代理伺服器上。圖 2-9 為代理伺服器運作說明。

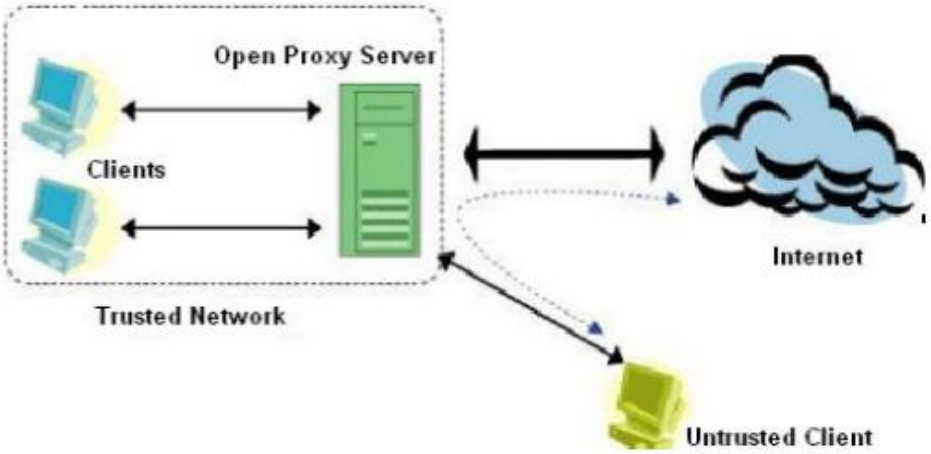


資料來源：本研究整理

圖 2-9 代理伺服器運作說明

常見用以隱匿身分與 IP (可能是犯罪行為也可能為了存取一些有所限制的網路資源等不同情節)的 Proxy 我們稱為：Open Proxy，參見圖 2-10，其種類有 Anonymizing Proxy Servers 與 Intercepting Proxy Servers。

- Anonymizing proxy servers：通常為 Web Proxy，用以代理 HTTP 協定。並搭配匿名工具，如：Privoxy、Proxify 等的使用，來隱藏真實身分。部分的 Anonymizing proxy servers 會在代理的過程中加入 HTTP_VIA、HTTP_X_FORWARDED_FOR 或 HTTP_FORWARDED 等 Header 資訊，使得來源 IP 可以被追蹤，在犯罪行為追查上較為有利。另一種 Proxy 稱為 Elite 或 High Anonymity Proxy，只有顯示 Proxy 端的 Header，因此只能追蹤到 Proxy Server 本身，除非透過 Proxy Server 的連線紀錄(Log)否則難以追查連線的真正來源，具有比較高之匿名性。
- Intercepting proxy servers：又稱為 Transparent Proxy，結合 Gateway 或 Router 甚至 NAT(Network Address Translation)等能力。具有 Socket 層或電路層代理(circuit-level proxies)等能力。同 High Anonymity Proxy，能夠完全掩蓋追蹤。許多大專院校使用此技術，來作為學校主要的 Proxy 服務。

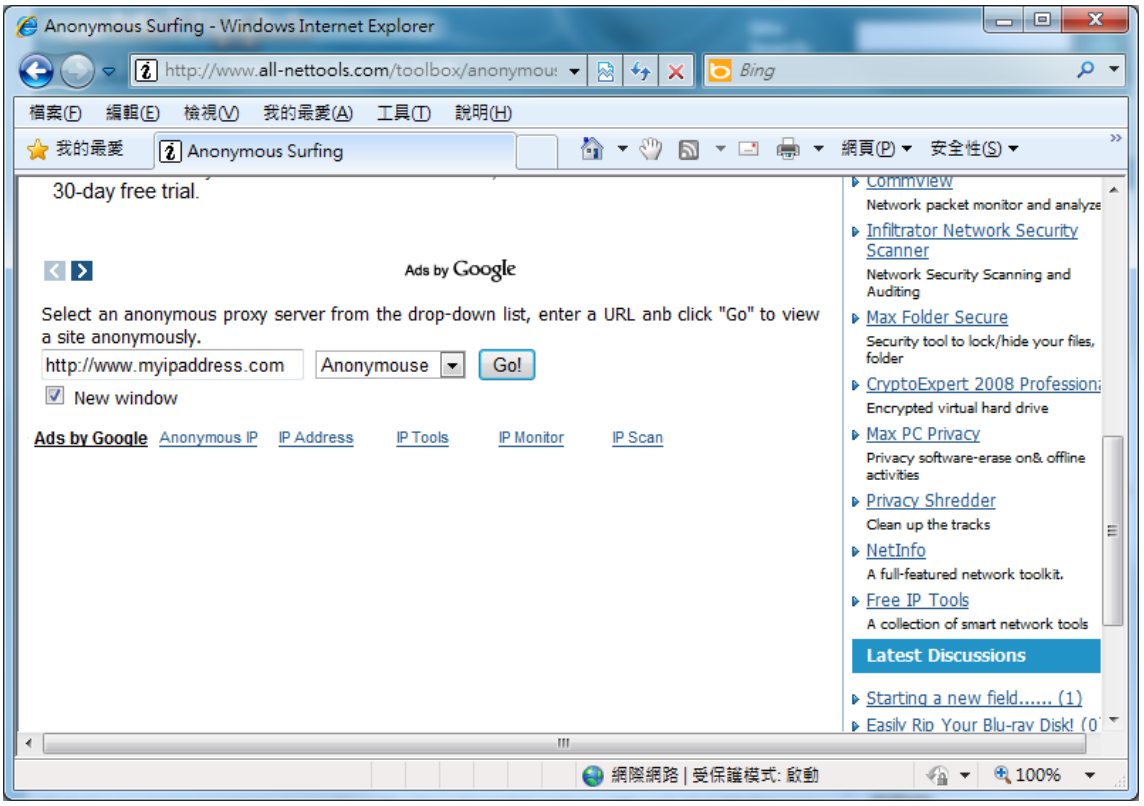


資料來源：http://www.aboutonlinetips.com/

圖 2-10 Open Proxy 機制

透過 Proxy 進行匿名上網或隱匿身分時，有主要兩種方式：

- 修改瀏覽器或應用程式設定：瀏覽器與網路應用程式多數可設定使用代理伺服器，可直接根據 Proxy 列表填入 IP 與 Port 即可使用 Proxy Server 來進行匿名上網或隱匿身分。
- 透過 Anonymous 工具：有許多免費及商用的工具，允許使用者透過該工具來隱匿 IP，如：圖 2-11 及圖 2-12 匿名瀏覽工具隱匿了連線的 IP 只能夠追蹤到 Proxy 之 IP。部分可以自動化地從 Anonymous Proxy 列表節點(圖 2-13)下載 Proxy 列表加入工具，並輪流使用這些 Anonymous Proxy，攻擊者也常用來變換不同的 IP 進行攻擊。另一種常見的工具為 Anonymous Mail 可隱匿寄件者的位址，利用代理伺服器寄信，藉以隱匿寄信來源，藉以達成寄出垃圾郵件之目的，如圖 2-14。

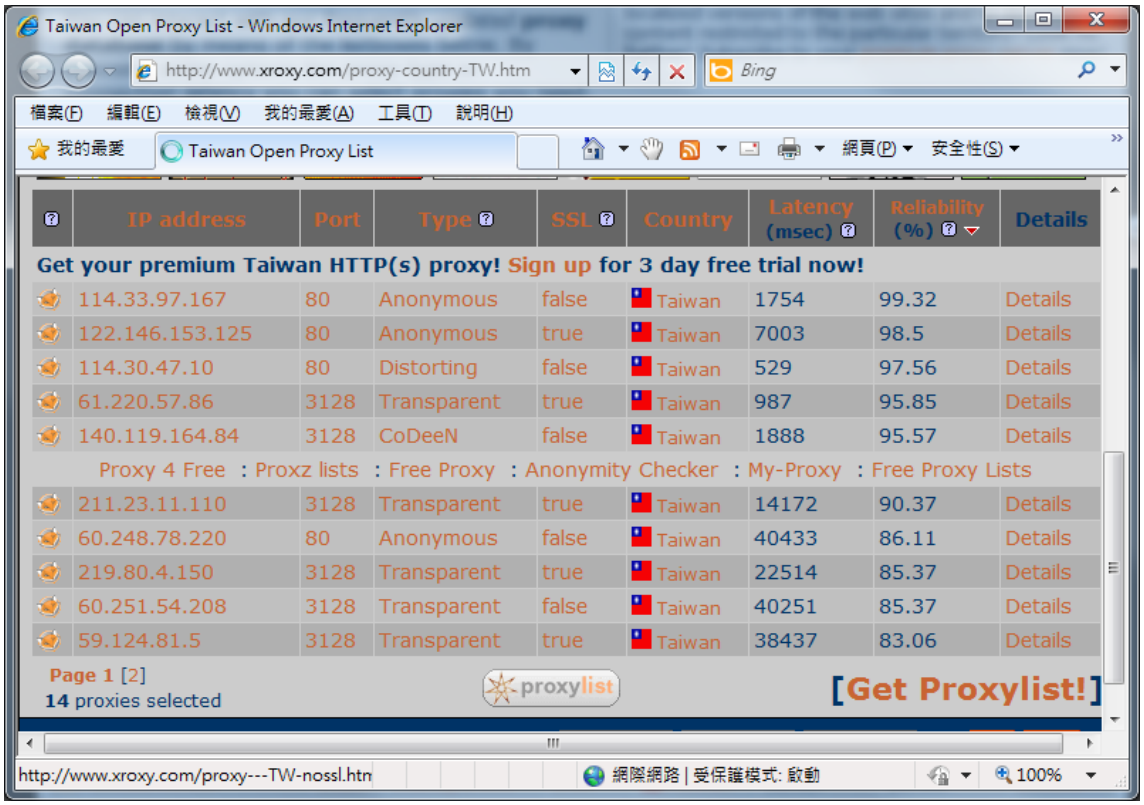


資料來源：http://www.all-nettools.com/toolbox/anonymous-surfing.php

圖 2-11 匿名瀏覽工具

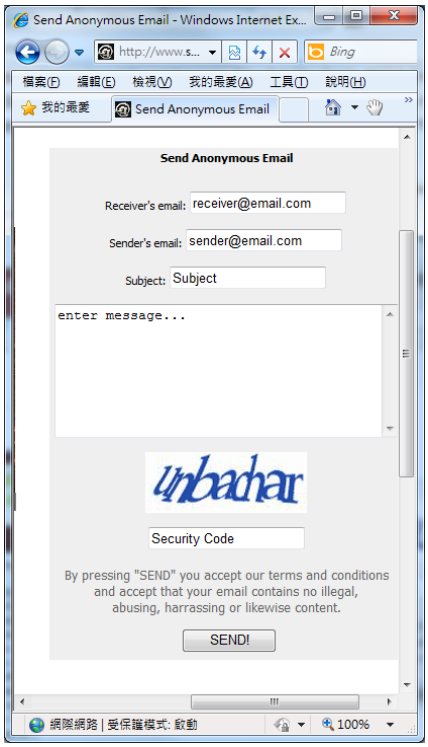
資料來源：http://myipaddress.com

圖 2-12 與本機使用的 IP 不同，呈現的是 Proxy 之 IP



資料來源：http://www.xroxy.com/proxylist.htm

圖 2-13 我國 Proxy 列表

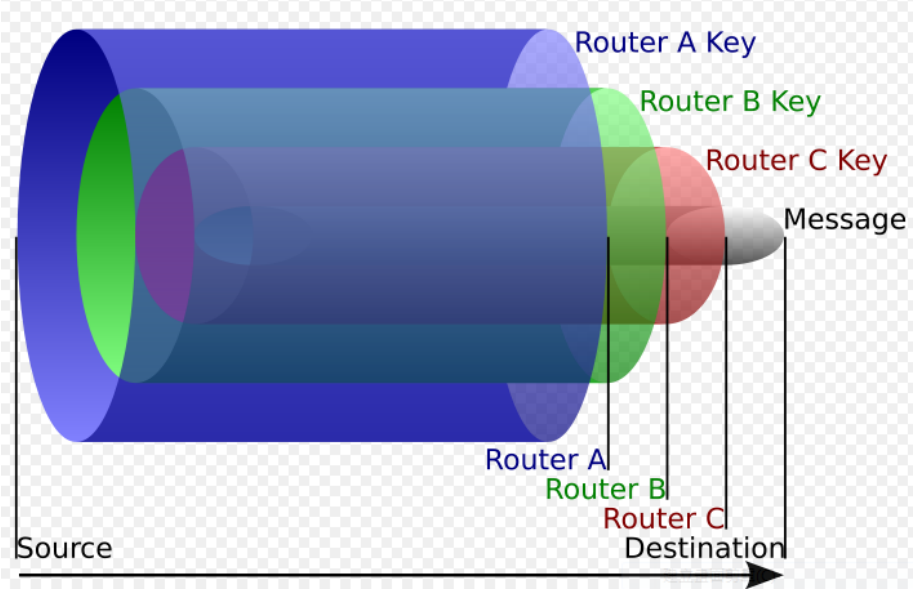


資料來源：http://send-email.org/

圖 2-14 Anonymous Mail

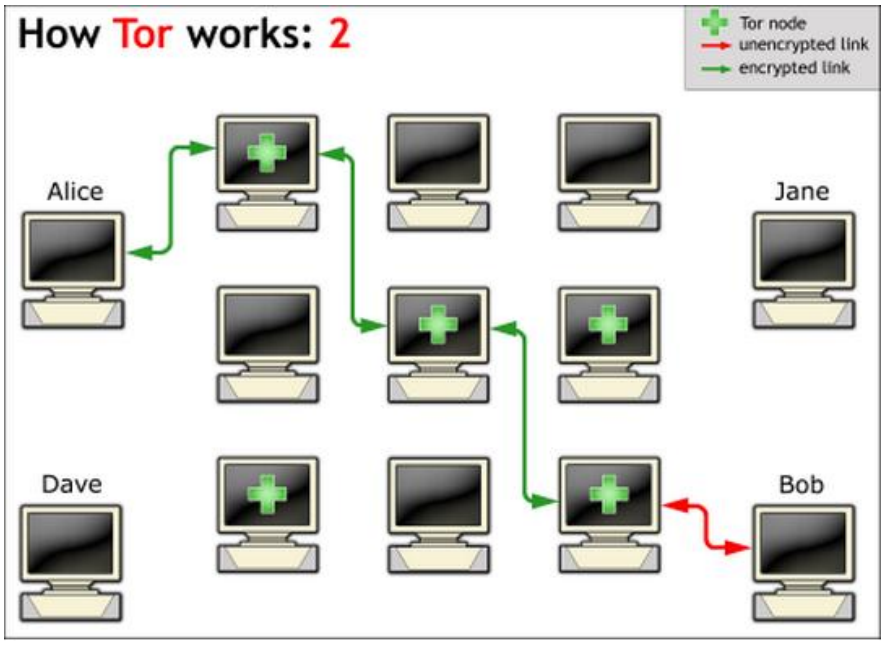
2. 洋蔥路由(The onion router, Tor)網路

Tor(The onion router)稱為洋蔥路由，Tor 工具會建構代理伺服器，透過洋蔥代理伺服器(Onion proxy)定期與其他伺服器連線，並在 Tor 網路中構成虛擬電路(Virtual circuit)。在 Tor 網路中，路由訊息會經過層層的加密，要解開訊息需要一層一層地撥開(如洋蔥一樣，圖 2-15)。Tor 網路的資料傳遞為加密傳送，離開 Tor 網路則回復明文傳送，見圖 2-16。透過 Tor 網路難以追蹤，因為經過的節點龐大，且沒有固定的路由方式。因此可以用以保護隱私，但也可被駭客用來隱匿身分及 IP 位址。



資料來源：http://en.wikipedia.org/wiki/Onion_routing

圖 2-15 Tor 網路示意圖

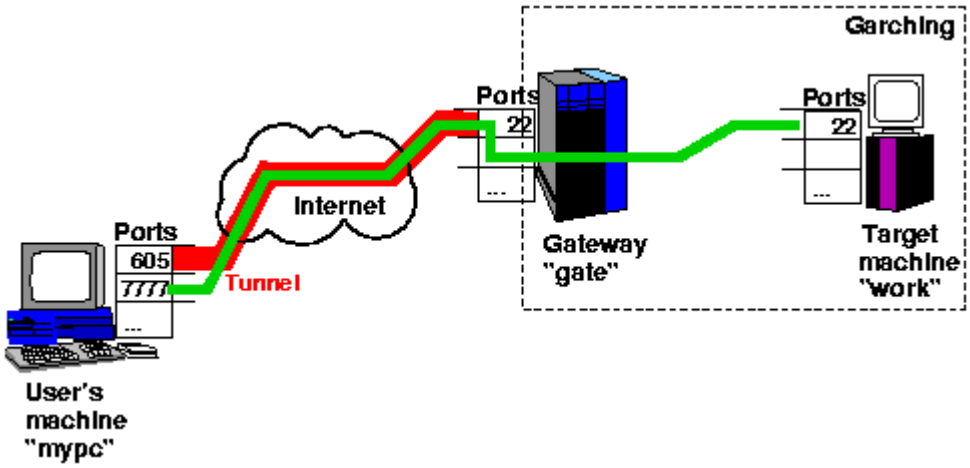


資料來源：
http://www.iusmentis.com/society/privacy/remailers/onionrouting/

圖 2-16 Tor 透過節點轉送封包，使來源位址無法追蹤

3. VPN 通道技術

VPN 通道技術(VPN tunneling)可提供安全且專屬之通訊連結網路通道，採用非實體之暫時性連線，具合法授權之使用者可透過此安全通道存取企業內部網路。VPN Tunneling 透過通道技術(Tunneling)可連接遠端不同層之網路協定，原本是用以將跨越公用網路的兩個網路連接起來的安全技術。但透過同樣的通道技術，可以將本地端網路連結端網路後，再透過遠端網路連線到目標主機(Port forwarding)，因此同樣可以用來隱藏來源 IP 及身分，見圖 2-17。最常見的是 SSL 通道技術與 SSH 通道技術，特別是 SSH 通道技術，攻擊者透過破解 SSH 伺服器的帳號與密碼，可用來建立 SSH Tunnel，就能透過通道加密方式進行封包轉送，並利用被破解的 SSH 伺服器，來隱藏來源端的 IP 與身分。雖然 SSH 伺服器可能留下紀錄檔案，但多數攻擊者可能清除該紀錄檔案，使得追蹤變得困難，進而達到隱匿身分與 IP 位址之目的。



資料來源：
http://www.rzg.mpg.de/networkservices/ssh-tunnelling-port-forwarding

圖 2-17 Tunneling 技術用以隱藏使用者 IP

常見的 VPN 技術可分為兩類，PPTP VPN 與 SSL VPN：

(1) PPTP VPN

PPTP(Point-to-Point tunneling protocol)通道技術由於其容易設定的特性，而且是撥接網路(Dial-up networking)第一個支援的 VPN 協定，因此被廣泛採用。PPTP 將網路協定資料段封裝(encapsulated)在 IP 封包中，然後透過網際網路傳送。經過包裝之後的封包，會被網路上任何路由器或機器視為一般 IP 封包般傳送，直到抵達通道的另一端之後，才將傳送端封裝上去的 IP 表頭取下。此種 IP 封裝的好處是可以讓許多不同協定的資料能夠經由僅支援 IP 的網路媒介(例如，網際網路)傳送。當使用者與 PPTP VPN 伺服器建立 PPTP 連線後，使用者即可取得 PPTP VPN 所綁定的 IP 位址，透過此 IP 位址作為存取各項服務，並隱藏使用者真實的來源 IP 位址。

(2) SSL VPN

相對於以 PPTP 通道技術提供的 VPN 服務，SSL VPN 的運作是在網路的應用層上進行，是一種利用 HTTPS 通訊協定的 VPN 架構。由於現今的電腦作業系統大多皆搭載支援 HTTP 及 HTTPS(SSL-based HTTP)通訊協定的網頁瀏覽器。SSL(Secure socket layer)安全協定是網頁伺服器和瀏覽器之間以加解密方式溝通的安全技術標準。可保障使用者通訊間之私密性與完整性。SSL VPN 的運作方式是由遠端使用者連線到 SSL VPN 閘道，進行相關之驗證與認證後，再經由 SSL VPN 閘道連接另一網路，確保連線間的安全性，常被企業組織間用來提供遠端使用者成功存取組織

內部的網路資源，採用 VPN 機制時，需先經過身分認證後，才能夠連上 VPN 閘道器，相對代理伺服器來說，在身分追查確認上是較為簡單的。

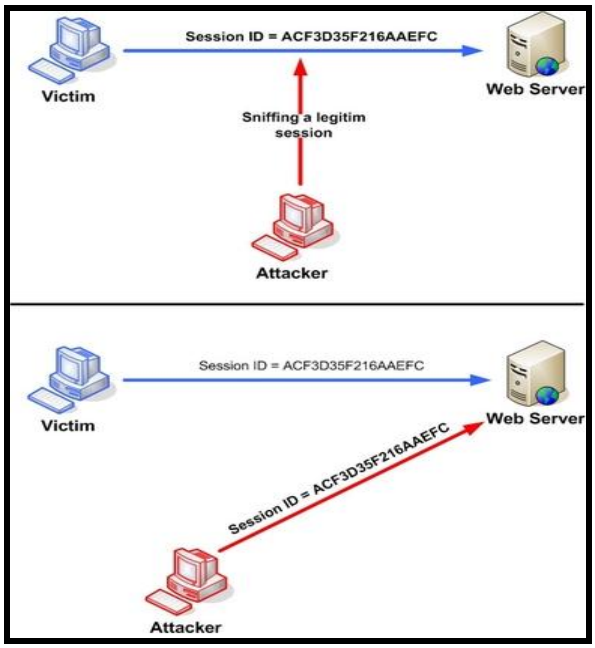
綜觀來說，VPN 通道技術可保障通訊安全，除了保證資訊的隱密 (Confidentiality)，避免第三者「竊聽」到通訊內容，同時還須確保網路傳送內容不被篡改破壞，亦即所謂資料的一致性/完整性 (Integrity)；另外就是資料來源的驗證(Authentication)，確定資料並非來自網際網路上第三者所偽造[84]。這些資訊安全服務可能被用以隱匿身分，也可用在正向上，確保個人隱私防止資料被窺視。

(三) Session Hijacking 攻擊與 Cookie 欺騙

Session Hijacking 攻擊與 Cookie 欺騙此兩種竄改身分之技術主要為攻擊網頁應用程式，取得網頁應用程式認證用的 Token，來進行偽冒及竄改身分之行為，通常需要搭配如 ARP 欺騙、代理等方式來達成竊取身分識別之行為。

1. Session Hijacking 攻擊

會話劫持(Session Hijacking)為網路犯罪者結合了竊聽和欺騙的手段來達到身分假冒與資料竊取的目的。會話(Session)所指的是兩台主機之間的一次通訊，例如當使用者利用 HTTP 瀏覽網站時，這樣的方式就稱之為 HTTP Session。網路犯罪者將會在使用者與遠端網站主機通訊時，中途攔截具有使用者身分資料辨識的 Session ID 或是竊取存在用戶端電腦的 Session ID，之後藉由挾持 Session ID 與修改連線資訊，達成冒用使用者身分及進入遠端網站竊取資訊。下圖 2-18 說明會話挾持攻擊。此類技術主要為攻擊網頁應用程式，網路犯罪者透過 Session Hijacking 攔截伺服器主機和用戶端主機之間傳送的訊息與 Session ID，然後駭客會變更伺服器主機傳送的訊息內容並傳給用戶端主機。而當用戶端主機收到訊息後，仍然會相信訊息來源來是自於伺服器主機，然後會依照訊息指示進行動作。當用戶端主機將訊息回傳給伺服器主機時，此時駭客仍然會中途攔截，並加以修改，然後再傳回給伺服器主機。而伺服器主機和用戶端主機則永遠都不知道通訊內容曾經被攻擊、修改過，會話劫持(Session Hijacking)將會導致網路攻擊者成功的冒用網頁使用者的身分進入該使用者所使用的的網站，竊取重要的資料或利益。而在 Session Hijacking 的防範上，可採用安全的通道加密以及監控 Web 伺服器主機日誌資料，來杜絕會話挾持的發生。



資料來源：
http://www.owasp.org/index.php/Session_hijacking_attack

圖 2-18 Session Hijacking 說明

2. Cookie 欺騙

有一些網站會以寫入使用者端小型文字檔的形式，在使用者電腦中儲存一些資訊，用以辨識使用者身分，或是記錄一些使用者的資料與喜好(如：IP 位址、瀏覽過哪些網頁...) 等。當使用者再度進入該網站時，網站便可以利用這些資訊提供您個人化的內容，而這種小型文字檔就稱為 Cookie。Cookie 記錄著使用者的帳戶 ID、密碼之類的訊息，如果在網上傳遞，通常使用雜湊函數(Hash Function)編碼，如：MD5 或 Base 64 等方法處理或加密。這樣經由加密處理後的訊息，即使被網路上一些別有用心的人截獲，也無法看懂。Cookie 在商業網站上的功用，綜觀來說包含 (1) 追蹤和管理使用者狀態、喜好設定、業務資料及用戶提供的其他資料，(2) 出於安全目的，(3) 以不記名方式理解使用者在網站上的使用情況以及 (4) 評估某些廣告措施的有效性。通常 Cookie 有兩種類型，分為 Persistent Cookie 與 Session Cookie。Persistent Cookie 可以設定存在 Browser 一段時間，亦即明確指定 Cookie 的有效時間，如果設定時間夠長，即便 Browser 關閉後或是重開機依然還是會存在；Session Cookie 只存在於連線狀態下，當過了 Timeout 時間或是瀏覽器關閉，其 Cookie 資訊就會被消失。

一般來說，Cookie 是儲存在客戶端，因為 Cookie 當中會記錄具有隱私性的資料，如：帳號、密碼、身分證字號等。所以 Cookie 安全性須要額外重視，應用程式撰寫者對於 Cookie 應經過加密後再存放於使用者端，Cookie 欺騙是利用截獲使用者之 Cookie，並將該 Cookie 再一次送給伺服器，若能夠通過驗證，就可以冒充使用者的身分登入網站。因此，亦須要設定 Cookie 的 Timeout 時間或透過多層的驗證來避免攻擊者利用類似重送攻擊(Re-Play attack)之方式取得使用者的身分登入網站。

三、 小結

網際網路隱匿身分與竄改身分讓網路犯罪行為變得更不易偵查，並且難以找到真正的犯罪者。根據上述行為態樣與分析結果，網際網路隱匿身分與竄改身分可區分為非技術面與技術面兩大類，如表 2-2 所示。非技術面用的是類似於傳統的犯罪手法進行隱匿身分與竄改身分，即使沒有相關網際網路技術，還是可能使用傳統的方法進行。而技術面的隱匿行為，則透過網際網路協定本身的弱點或特性進行隱匿與竄改身分，多數的網路隱匿技術本身是用以保護隱私並非用來進行犯罪，但是卻被有心人利用來遂行犯罪行為。因此，對於相關技術使用之證據留存規範與偵辦技術值得重視。

表 2-2 網際網路隱匿身分與竄改身分行為態樣

項目	非技術面	技術面
特性	使用傳統犯罪手法來隱匿或偽冒身分，有時不需要網路技術同樣可以成功。	透過網際網路協定、技術之特性或弱點來達成欺騙、偽冒甚至隱匿身分或 IP 或位置。 技術本身是用來保護隱私或安全性，被誤用於進行犯罪行為。
行為態樣	1.偽冒身分及位置 2.合法掩護非法	1. 連線欺騙(Spoofing)行為 2. 代理(Proxy)行為 3. Session Hijacking 攻擊與 Cookie 欺騙

資料來源：本研究整理

第三節　網際網路隱匿與竄改身分行為態樣與犯罪行為

自從網際網路盛行以來，傳統的犯罪，也開始透過網路做為媒介。網際網路隱匿身分行為態樣，除了為保護個人隱私外，許多非法之行為亦透過此一行為進行掩飾。而竄改身分之行為，則是為了獲取不法利益或進行破壞而為之。除了網路原有的隱匿性外，透過隱匿身分與竄改身分行為就變成了犯罪行為中的一環。雖然並非每種的犯罪行為都存在隱匿身分與竄改身分行為，但多數的犯罪行為為避免被追蹤與偵察，大多會採用不同程度的隱匿行為。如同前述 M-O-P 理論，這些隱匿技術能提供犯罪者免於洩漏真實世界的身分，以逃避科罰責任，所以只要有犯罪行為，則隱匿身分與竄改身分行為就會永遠存在。

(一)　網路犯罪

在資訊通信網路快速成長之際，部分資料因安全整備不足而遭他人侵害的事實也時有所聞，例如透過電腦病毒破壞電腦及網路系統的正常運作、駭客入侵他人電腦從事不法行為、以及利用網路為犯罪工具或場所等行為。依警政署統計 2010 年 1-11 月電腦網路犯罪發生數 3,514 件，而依犯罪方式觀察，以無故取得、刪除或變更他人電腦或電磁紀錄 304 人占 54.29%最多。

2001 年 11 月在布達佩斯由歐洲理事會的 26 個歐盟成員國以及美國、加拿大、日本和南非等 30 個國家的政府官員共同簽署《網路犯罪公約》(Cyber-crime Convention)成為全世界第一部針對網路犯罪行為所制訂的國際公約[82]。於公約中並明訂 9 類網路犯罪行為(表 2-3)以刑法處罰。

表 2-3 網路犯罪公約 9 類網路犯罪行為

犯罪行為	公約定義
非法存取	指任何故意威脅或攻擊電腦系統及電腦資料的行為，如電腦駭客等行為
非法截取	包括非法截取電腦傳送的「非公開性質」電腦資料
資料干擾	包含任何故意毀損、刪除、破壞、修改或隱藏電腦資料的行為
系統干擾	任何電腦資料的傳送，只要其傳送方法足以對他人電腦系統構成「重大不良影響」時，將會被視為「嚴重妨礙」電腦系統合法使用。所以在此原則下，利用電腦系統傳送電腦病毒、蠕蟲、特洛伊木馬程式或濫發垃圾電子郵件，都符合「嚴重妨礙」電腦系統，即構

犯罪行為	公約定義
	成「系統干擾」的行為
設備濫用	包含生產、銷售、發行或以任何方式提供任何從事各項網路犯罪的設備
偽造電腦資料	包括任何虛偽資料的輸入、更改、刪改、隱藏電腦資料，導致相關資料喪失真確性
電腦詐騙	包括任何有詐騙意圖的資料輸入、更改、刪除或隱藏任何電腦資料，或干擾電腦系統的正常運作，為個人謀取不法利益而導致他人財產損失
兒童色情的犯罪	包括一切在電腦系統生產、提供、發行或傳送、取得及持有兒童的色情資料
侵犯著作權及相關權利的行為	包括數條保障智慧財產權的國際公約列為侵犯著作權的行為

資料來源: http://zh.wikipedia.org/wiki/網路犯罪公約

曾百川以近年來國內外司法警察所偵破的各類型網路詐欺犯罪案件及相關文獻資料進行分析，依網路使用目的區分為網路拍賣、網路購物、商業金融、網路遊戲、色情網站及其他類型六類網路詐欺型態[65]。

目前，在網路空間所犯的罪行可分類為幾種：(1) 以網路空間為犯罪場所(被動)，如網路色情、網路援交；(2)以網路為犯罪工具(特定目標)，如網路恐嚇、網路誹謗；(3)以網路為犯罪客體(為攻擊目標)，如網路入侵(駭客)、散播電腦病毒，如表 2-4 所示。

表 2-4 網路犯罪之分類及其常見類型

分類標準	特　點	常見型態	犯罪事實易知悉程度	偵查難度
以網路空間為犯罪場所 (被動)	被動性質，引誘吸引一般人進入	1.網路色情 2.網路援交 3.販賣盜拷 4.網路賭博 5.網路遊戲 6.販賣槍械 7.教授製仿炸彈	高	低

分類標準	特　點	常見型態	犯罪事實易知悉程度	偵查難度
以網路為犯罪工具(特定目標)	針對特定目標予以侵害性質，藉由網路作為犯罪工具	1.網路恐嚇 2.網路誹謗 3.網路詐財	中	中
以網路為犯罪客體 (為攻擊目標)	對網路或電腦系統的攻擊性或破壞性	1.網路入侵(駭客) 2.散播電腦病毒 3.網路竄改 4.資料隱碼(SQL Injection)	低	高

資料來源：林宜隆等著，我國網路現況分析與對策—以刑事警察局網路犯罪偵查案例作分析[31]。

網路犯罪具有以下特性：散布迅速、身分易藏、證據有限、毀證容易、適法困難、全球性、偵查不易、行為與結果之時間和地點分離、持續性，各國法律與實務對於某些行為是否違法的判斷標準不同，也使得跨國性網站的非法行為，在偵查上相當困難[29][51][76]。

(二)　網路犯罪與隱匿行為

我國目前並無推行「實名制」，網路身分(帳號)登記之資料無法確認，因此犯罪者可遂行網路隱匿身分之行為。網路隱匿身分或竄改身分行為助長了網路犯罪行為，在表 2-5 我們分析整理網際網路隱匿與竄改身分行為之分類及其常見類型之關聯。

表 2-5 網路隱匿身分或竄改身分行為與網路犯罪常見類型

面向	隱匿行為	網路犯罪常見類型	說明
非技術面	1.偽冒身分	1　網路色情 2　網路援交 3　販賣盜拷 4　網路賭博 5　網路遊戲 6　販賣槍械 7　教授製仿炸彈 8　網路恐嚇 9　網路誹謗 10　網路詐財	以網路空間為犯罪場所之網路犯罪類型較易使用非技術面的隱匿行為。其主要的偵察方式也非找到其偽冒之身分，而是追蹤金

面向	隱匿行為	網路犯罪常見類型	說明
	2.合法掩護非法	1 網路色情 2 網路援交 3 販賣盜拷 4 網路賭博 5 教授製仿炸彈 6 網路恐嚇 7 網路詐財	流。
技術面	1.連線欺騙(Spoofing)行為	1 網路入侵(駭客) 2 散播電腦病毒 3 網路竄改 4 網路詐財	以網路為犯罪工具(特定目標)及以網路為犯罪客體(為攻擊目標)之類型為隱藏其身分與引誘使用者上當等，會使用技術面的隱匿行為，透過網路技術提升追蹤之困難度。
	2.代理 (Proxy)行為	1 網路色情 2 網路援交 3 販賣盜拷 4 網路賭博 5 網路遊戲 6 販賣槍械 7 教授製仿炸彈 8 網路恐嚇 9 網路誹謗 10 網路詐財 11 網路入侵(駭客) 12 散播電腦病毒 13 網路竄改 14 SQL Injection	
	3.Session Hijacking 攻擊與 Cookie 欺騙	1 網路入侵(駭客) 2 散播電腦病毒 3 網路詐財 4 網路竄改	

資料來源：本研究整理

網際網路隱匿身分與竄改身分之行為，雖存在許多相關的技術議題，但就隱私保護與網路犯罪類型來看，非技術面的部分，只需有較強的犯罪動機，而不一定需要技術的支持也可遂行，亦是影響網路犯罪偵察的重要隱匿行為之一。因此本研究針對此兩面向之隱匿行為進行分析，並於本研究報告後續章節說明社會、法律與技術等議題之有效因應方法，供作未來對於隱匿行為態樣研究與網路犯罪防制之參考。

第三章　國際對網際網路隱匿與竄改身分之管制措施及分工情形

網際網路隱匿與竄改身分及網路犯罪行為等議題，皆與三個面向相關：一是「個人隱私」牽涉到隱匿身分與個人資料的維護與隱密性規定可能相牴觸[78]，例如獲取個人隱私資料危害網路使用者之匿名性；二是「商業活動」與網路交易行為需確認交易雙方身分，同時，透過網路匿名性特性，犯罪者遂行相關犯罪交易活動，如網路販賣違禁、管制物品、盜版光碟、贓物、侵犯他人著作權及商標權[35]；三是「網路犯罪」是以電腦與網路為一般犯罪之通訊連絡工具或場所或犯罪工具，例如駭客侵入與散布電腦病毒等，常透過網際網路隱匿與竄改身分行為來規避追查。目前世界先進國家對於這些犯罪類型之管制與法規，因國情、風俗民情等因素，採取不同層級的管制規範，本章節蒐集先進國家，包括：歐盟、美國、德國、日本、韓國等國家，對網路犯罪相關之法規規範，特別綜整各國有關隱匿與竄改身分相關法令與規章，作為網路犯罪等相關權責主管機關推動網際網路環境隱匿與竄改身分行為管制政策之參考。

第一節　個人隱私

一、 隱匿身分與個人隱私

在前一章已界定隱匿與竄改身分行為之意義。廣泛而言，匿名性是一種出於某種目的而不表明自己身分或者讓他人不知道其身分(個人特徵)的一種行為，網路使用者採取匿名性可能是為了保護自己的權利或言論自由。如受訪者身分或投票者身分，不願意公開自己的真實姓名或身分，因此隱匿其真實世界的身分。在藉由網路的匿名功能卸下真實世界人際關係的牽絆之後，反而能夠自由自在建立人際關係，如交友或聊天等。換言之，因爲網路的匿名功能，促使使用者不必擔心在人際互動過程中身心可能受到侵害；再者，匿名功能亦使使用者在網路空間中的身分與角色只是以身分代號的形式出現，使用者不僅可以決定透露那些自己的個人資料，如姓名、地址或相片等，同時亦可以決定自己是否要在網路空間中讓別人瞭解某些私人面向，更進而還可以控制自我呈現的方式，甚至重新塑造一個新的自我[38][68]。

因此，網路使用者可以在自由意願選擇下，自由自在遨遊於網路空間中，甚至可以在網路中創造一個新的自我。對大多數網

路使用者而言，現實生活中的壓力、沉悶、苦惱，都可以藉上網而得到紓解與排遣，有些使用者也想逃避到網路空間中，避開現實世界中的責任與不悅[77]。故此，對多數使用者而言，採用網路匿名性而隱匿自己真實身分，或許只想自由自在交友、與人聊天或抒發自己的意見，不一定具有違法、傷人或犯罪的意圖。

吳庚大法官於大法官釋字五○九號解釋理由中之協同意見書指出[35]：

■「...言論自由既攸關人性尊嚴，此項憲法核心價值的實現，在多元社會的法秩序理解下，國家原則上理應儘量確保人民能在開放的規範環境中，發表言論，不得對其內容設置所謂『正統』的價值標準而加以監督。從而針對言論本身對人類社會所造成的好、壞、善、惡的評價，應儘量讓言論市場自行節制，俾維持社會價值層出不窮的活力；至如有濫用言論自由，侵害到他人之自由或國家社會安全法益而必須以公權力干預時，乃是對言論自由限制的立法考量問題，非謂此等言論自始不受憲法之保障。...準此，吾人固不否定言論自由確實具有促進政治社會發展之功能，但是應注意並強調憲法保障言論自由之意旨，並不受此項工具性思考所侷限，更不應為其所誤導。」

網路上言論自由應予以捍衛，不容隨意侵犯，然對於基本權利與社會公益有所衝突時，應予以「實益考量」。亦即希望一方面能保有言論自由之基本權利，另一方面對於言論自由下的網路資訊是否傷及社會公益應加以審慎計算[35][80]。故此，在網路世界中難以將使用者採用隱匿身分方式就與一定會犯罪畫等號[78]，若網路使用者不是將隱匿身分當作是犯罪工具，只是用於個人資料的隱藏或言論自由的保護時，做為保護個人權益的用途，則應該給予適當保護。但如果將隱匿身分當作犯罪工具或手段損害他人權益，則須加以處罰。由於各國文化與法規不同，則對於個人隱私的法律上保護亦將有所不同。以下說明美國、德國、歐盟、日本、韓國與我國在個人資料保護方面法規之規定。

二、 依各國法規探析個人隱私保護之規定

(一) 美國

美國是一個極重視個人隱私與權益的國家，1974 年通過的「隱私權法案」(Privacy Act)規範聯邦政府所蒐集的個人資料公布於眾時，應該通知當事人該情事[52]。而按上開法律之規定，所謂的「個

人資料」意指，包含個人之教育、金融交易、醫療紀錄、犯罪前科及受雇紀錄之中關於個人之姓名、識別號碼、象徵或其他足以辨識個人如指紋、聲紋或相片之資料[64]。「隱私權法」特別強調「公平使用原則」，其認為：「在尚未通知當事人並獲得其書面同意以前，資訊擁有者不得將人民為某種特殊目的所提供之資料，使用在另一個目的上」，在隱私權法施行後，更陸續於 1986 年推動電子通訊隱私權法、1987 年通過電腦安全法等，以保護個人資訊之隱私。除此為保障網路上自由通訊，2009 年 7 月美國眾議員 Ed Markey 和 Anna Eshoo 提出「網路自由保護法案」交由國會討論。該法案主要在建立網路中立性的標準，規範網路的使用機會，確保能給每人使用網路機會；換言之，在不用獲得他們的 ISP 服務供應商的同意下，在網路上分享個人的看法。美國聯邦通訊傳播委員會(The Federal Communications Commission，簡稱 FCC)主席 Julius Genachowski 宣布制訂網路中立性這項法規的計畫，其主要效力是在致力於保護網路的根本開放性。

在美國除政府立法保障使用者個人使用網路的權利，網路自治團體也提供相關個人隱私權的解決辦法，包括：(1) TRUSTe：此非營利團體成立於 1996 年，參與這個團體的網站都會獲得一個標誌，用以保證不濫用網路使用者的個人資料。知名的網站如 AT&T、IBM 等都有參與本組織。(2) The Platform for Privacy Preferences：由 Open Profiling Standard 與 Original Platform for Privacy Preferences 所共同組成，簡稱 P3。P3 之目的是要讓網路使用者能夠自行控制資訊之流向，什麼樣的資料可以上傳，什麼樣的資料不能提供，都可以經由 P3 獲得控制。1995 年發布《個人隱私與國家資訊基礎結構》白皮書，這個以“保護與電信有關的個人隱私”為主題的白皮書是美國國家電信與資訊管理局(NTIA)根據上面所提到的指導原則和公共調查而發布的。文中提出電信(網路)環境下保護個人隱私的兩大原則：(1)告知：應當事先告知客戶，他們可以蒐集何種個人的資料或數據及如何使用這些資料。只有在客戶同意以後，蒐集者才能按照事先宣布的用途自由地使用這些數據(一般的個人數據，只要客戶默許即可。但是對於較為敏感的個人數據，則需要客戶的明確同意)。(2)消費者由於被不當使用或披露個人資訊，或由於被提供了不準確、過時的、不完整的或無關的個人資訊而受到傷害時有權要求賠償。以下法規是美國政府對個人隱私保護相關法規(依最近年度到最遠年度排列)包括：

1. 個人資料隱私與安全法案（Senate Bill S.495）
2. 網際網路自由保護法草案（Global Online Freedom Act, H.R.275）

3. 加州網路隱私保護法（California Online Privacy Protection Act）
4. 電子通訊隱私法（Electronic Communications Privacy Act, H.R. 5018）
5. 兒童網上隱私保護法（Children's Online Privacy Protection Act）
6. 發布《個人隱私與國家資訊基礎結構》白皮書（1995 Privacy and the NII）
7. 電腦濫用法修正案(Computer Abuse Amendments Act of 1994)
8. 電腦匹配和隱私權保護法修正案(Computer Matching and Privacy Protection Amendments Act of 1990)
9. 電腦安全法案(Computer Security Act of 1987)
10. 電腦欺詐與濫用法(Computer Fraud and Abuse Act of 1986)
11. 電子通信隱私法(Electronic Communications Privacy Act of 1986)
12. 隱私保護法案(Privacy Protection Act of 1980)
13. 隱私法案(Privacy Act, Public Law No. 93-579 of 1974)

(二) 德國

德國是全球第一個制定網際網路成文法的國家。為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，德國於 1977 年 1 月 27 日即制定「資料處理個人資料濫用防制法」(Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung)，又稱「德國聯邦個人資料保護法」(Bundesdatenschutzgesetz)，並行之有年。後因歐洲聯盟成立，為轉置歐盟指令、保障個人資料及資訊自由流通，而於 2001 年 5 月 18 日修正其內容。最近一次修正日期為 2003 年 1 月 14 日，修法目的旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令。

1. 德國聯邦個人資料保護法(Bundesdatenschutzgesetz, DSG)

德國「聯邦個人資料保護法」於 1977 年頒布生效（當時法規名稱為「資料處理個人資料濫用防制法」），2001 年 5 月 18 日再次進行修法，其修法目的在轉化 1995 年歐盟個人資料保護訓令並保障個人資料及資訊自由流通；目的乃在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之訓令[40]。最近一次修正

日期為 2003 年 1 月 14 日，修法目的旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令。此法計有 6 章共計 60 條條文，條文規範包括與資料保護相關之各項原理原則，例如限制蒐集原則(又稱直接原則，如第 4 條第 2 項、第 13 條第 2 項)、內容完整正確原則(如第 20 條第 1 項前句、第 35 條第 1 項)、目的明確原則(或稱目的拘束原則，如第 14 條、第 28 條第 1 項)、限制利用原則(如第 31 條)、安全保護措施原則(如聯邦資料保護專員制度措施及第 9 條之附件明確規定之安全措施)、公開原則(第 13 條第 2 項前句之資料應向當事人蒐集、第 33 條關於告知之規定)及個人參與原則(如第 19 條至 21 條、第 33 至 35 條)及責任原則(如第 7 至 8 條之損害賠償與罰則)等[40]。此外由於聯邦制，德國各州也有自己的資訊保護法，例如 1970 年制定的黑森州資訊保護法是世界上首部此類法律。相較於其他國家，德國為貫徹個人資料之保護而創設聯邦資料保護專員(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)制度，是德國聯邦個人資料保護法的一大特色[19][41]。

2. 著作權法(Urheberrechtsgesetz)

德國著作權法的全稱為著作權及相關保護權法(Gesetz über Urheberrecht und verwandte Schutzrechte)，制定於 1965 年 9 月 9 日。當網際網路越來越普及，傳統紙本時代的著作權規範面臨新科技所帶來的許多新挑戰。聯邦眾議院遂於 2003 年 4 月 11 日及 2007 年 7 月 5 日通過二次所謂的資訊社會著作權改革，使法令規範跟上現代化的腳步。2003 年的改革重點是增訂第 52a 條，允許老師、教授或研究人員得透過電腦螢幕或內聯網(intranet)，提供受著作權保護之著作的一部分或片段，讓特定範圍的學生和研究人員閱讀，以滿足教學或研究目的。這類使用必須給付合理費用，但費用求償權只能透過著作權管理團體行使。52a 條訂有實施期限，期滿之前再依據實務經驗檢視成效並訂定新的有效期限。2007 年通過的資訊社會著作權第二次規範法已於 2008 年元旦開始實施，其重點如下：

(1) 私人複製：舊法原已明定非法取得之著作不得複製。此規定維持不變，只是將數位時代的音樂和電影等產物亦納入所謂的著作項目。網路使用者如果明知 P2P（Peer to Peer）網路平台上供下載之音樂或電影屬於非法取得，即不得複製。為自用目的而私人複製受著作權保護之著作並不違法，但著作權所有權人有權透過保護裝置限制自用目的之複製。破解保護裝置乃違法行為。

(2) 總額付費以補償私人複製：私人合法複製亦須付出合理費用。

(3) 學術與研究之限制：公共圖書館、博物館和檔案機構得將館藏出版品以電子方式於閱覽區公開呈現。圖書館亦得在法律允許範圍內為讀者複製受著作權保護之著作，但為保護著作權，複製數量須與館藏數量一致。此一規定係為保護作者及出版者之智慧財產權。

(4) 未知的使用方式：為使著作人之著作權在新興科技出現後依然受到保障，新法規定，每當著作透過一種新型技術重製時，著作人即有權收取著作權費。出版者在開始利用新技術重製著作前，應告知著作人。著作人被告知後，得在三個月內撤銷其權利。此規定亦適用於檔案儲存技術。

上述相關法規主要強調個人對資料使用之權利與義務，以利確保資料合法且正當的被使用。

(三) 歐盟

在 1996 年 11 月歐盟所舉行的電氣通信大臣理事會，依據「有關網際網路上違法有害內容之特別作業小組報告書」，通過有關網際網路使用之決議。其決議之概略內容為(1)獎勵促進由網路提供者與利用者代表團體共同建立自主規範之制度、以及獎勵促進建立有效的網路行為規範與國民報案專線之制度，(2)提供利用者的過濾系統及獎勵依據 PICS(Platform for Internet Content Selection)設定評價系統，(3)促進國際性閣僚會議的積極參與及相關各界代表的參與[66]。在 2008 年 6 月更提出報告，建議歐盟立法要求所有部落格(Blog)應取得官方的認證標記。

在 2007 年 11 月里約熱內盧「網路治理論壇」 (Internet Governance Forum，IGF)時，由義大利和巴西政府發起的網路權利憲章(Internet Bill of Rights)運動，無疑具有成為全球規範的潛能。在 2010 年歐盟推出《歐盟範圍內個人資料數據全面保護實施辦法》(A Comprehensive Approach on Personal Data Protection in the European Union，簡稱「實施辦法」)填補歐盟範圍內個人隱私保護方面的空缺。該「實施辦法」賦予用戶可告知網站必須永久刪除其註冊的個人資料的權利，並且規定公司在以任何形式使用用戶資料或對用戶的個人資料進行編輯前必須獲得用戶的明確授權。這份長達 20 頁的「實施辦法」同時還指責網際網路公司目前

的隱私保護政策極不透明。該「實施辦法」被認為是 1995 年數據保護法案的修訂版，其預示著隨著網際網路科技的飛速發展，保護用戶隱私法案也應該跟上新一代網際網路的發展需求。該「實施辦法」中指出：目前通過網際網路蒐集個人資料數據的方法變得越來越隱蔽，且極不易被發現。該「實施辦法」中建議，對於侵犯其個人隱私權的公司，消費者應該具有追訴權，甚至提起刑事訴訟的權利[91]。以下是保護個人隱私相關法規：

1. 2010 歐盟範圍內個人資料數據全面保護實施辦法，簡稱「實施辦法」(A Comprehensive Approach on Personal Data Protection in the European Union)。
2. 2002 電子通訊中個人資料處理與隱私保護指令(隱私及電子通訊指令)。（Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications）

(四) 日本

隨著電腦處理資料技術發達，攸關個人隱私等足夠資訊辨識個人之資料可簡單利用電腦儲存、流通、加工、編輯，且因網路普及，個人資料可瞬間傳遞至全世界，如能善用電腦處理個人資料，有助提升行政效率，甚至促進經濟發展。但個人資料經電腦處理後，因可輕易彙整獲悉個人資料全貌，如遭濫用或不當利用，有侵害個人權益之虞，若處理不當，導致個人資料外洩，即使未對個人造成實質傷害，亦可能引發個人對其個人資料保管、使用之疑慮。個人資料電子化雖促成社會繁榮進步，惟個人資料之處理亦攸關個人權益，應於尊重個人人格之理念下慎重處理。近年來電子科技日益精進，在邁向網路資訊化社會之同時，電腦處理個人資料之保護更形重要，故日本於 2003 年制定「個人資料保護法」，俾謀求個人隱私可確切獲得保障[21]。

1. 個人資料保護法（個人情報の保護に関する法律）

日本之個人資料保護法於 2003 年制訂，在日本個人資料保護法案中，不論是行政機關或是民間機構，只要有利用個人資料者，都受到此法之規範。此外，特別是對於使用電腦或資料庫等儲存利用個人資料之相關單位(個人資料利用事業者)，亦設定「個人資

料利用事業者之義務」規定，訂定具體且明確之規範。以公務機關之個人資料處理而言，日本早在在 1989 年就已制定「行政機關電腦處理個人資料保護法」，然而為配合「個人資料保護法」之制定，因此 2003 年於國會中提出相關之個人資料保護法案，除對原先「行政機關之電腦處理個人資料保護法」之修正案外，另提出「獨立行政法人資料保護法案」、「資料公開與資料保護審查會設立法案」、「行政機關之個人資料保護法施行相關法律準備之法案」等，以加強個人資料保護法之完整性，目前日本使用施行的為 2008 年新修正之「個人資料保護法」。在尊重個人人格之理念下，慎重處理暨利用個人資料，係為制訂日本個人資料保護法案之基本考量；因此(1)資料利用目的之限制、(2)資料之適當取得、(3)確保資料正確性、(4)確保資料安全性、(5)確保資料之透明度，即為本法案之五項基本原則。為保護所有個人、團體、法人以及機關個人資料，依據上述五項基本原則，個人資料保護法案朝向制定適當處理及利用個人資料之方向而努力，且實務上何種資料之處理與利用始可視為恰當，以及對於公益活動或正當事業活動之必要性亦加以評估後，於個人資料保護之必要範圍內予以判斷，為制訂本法案之相關考量因素。

(五) 韓國

大約在 2008 年 1 月下旬，Google 才正式推出韓語版本的 YouTube 影音網站，一年後 Google 卻因為必須遵守韓國法律的緣由，而不得不暫時取消 YouTube 韓國站匿名用戶的上傳與留言權利；換言之，唯有以真實姓名登記註冊的網友，方能繼續上傳影音檔案到 YouTube 韓國站，或是進行留言、評論。2009 年 10 月傳出韓國知名女星崔真實(최진실)自殺身亡一案，雖然警方無法確認其自殺原因，但據傳網路謠言和惡意的誹謗，可能是造成女星自殺的關鍵因素。為此，韓國積極著手修訂《信息通信網法施行令修正案》(簡稱修正法)，以防止匿名網友任意發布流言。韓國廣播通信委員會(Korea Broadcasting Commission)聲稱，為預防以匿名方式產生的網際網路負面效果，計劃從 2008 年 11 月，增加適用「限制性本人確認制」的網站。「限制性本人確認制」是指一項在網站等進行網上留言時通過身分證確認本人的程式[28]。在《修正法》之後，網站日用戶數量超過 10 萬的所有營運商都受此確認制之規範，因此幾乎所有韓國網站都受此規定限制，即是使用者須採用本身的真實姓名登入入會，亦稱為「實名制」。

在《情報通信網法施行修正案》中，於第 60 條第 2 項新設網路侮辱罪的處罰規定，條文如下：不論任何人如利用資訊通信網

對於他人有侮辱行為者，處 3 年以下徒刑或 3,000 萬元以下罰金。實施前項犯罪裁罰時，應尊重被害人的意思。2008 年 10 月 3 日，由政黨所主導針對網路侮辱罪處罰及網路實名制的《情報通信網利用促進及情報保護法修正案》(別稱崔真實法)。此法案立法審查時韓國「民主黨」、「民主勞動黨」及「自由先進黨」等發表反對的意見。2008 年 10 月 6 日被害人家屬請求該法案不要使用該名稱來立法。同日在「國政監督」中朝野政黨間經過激烈的言詞辯論後，考慮被害人家屬和其他相關人所經歷的苦痛，達成在訂立法案名稱時不使用真名的共識。事實上，韓國在網路隱匿身分情況下所造成網路名譽毀損事件在 2004 年就有 837 件，2009 年則增加到 2,106 件，增加 2.6 倍。「韓國傳播通信審議委員會」(類似我國通傳會，但通傳會不負責受理網路辱罵審議之權責。)所接受到的網路辱罵情報審議事件的速度也從 2006 年 2,074 件，增加到 2009 年的 35,288 件，增加 17 倍以上。目前重要相關法規有二：

1. 情報通信網法施行修正案（사이버 모욕죄）
2. 情報通信網利用促進及情報保護法修正案(別稱崔真實法)（정보통신망 이용촉진 및 정보보호 등에 관한 법률）
3. 促進使用信息通信網路及信息保護關聯法(정보통신망 이용촉진 및 정보보호 등에 관한 법률)

(六) 我國

1995 年 8 月 11 日我國即已制定「電腦處理個人資料保護法」，公布全文共 45 條。2010 年 5 月 26 日修正公布名稱「個人資料保護法」(以下簡稱為「個資法」)與修正為全文共 56 條。個資法主要的立法目的，在於規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。本法依第 53 條規定所定特定目的及個人資料類別，由法務部會同中央目的事業主管機關指定之。依第 55 條規定本法施行細則，由法務部定之。施行日期依第 56 條規定由行政院定之，但現行電腦處理個人資料保護法條文第第 19 條至第 22 條及第 43 條之刪除，自公布日施行。

個資法規定在向當事人蒐集個人資料時，須明確告知蒐集之目的、類別利用期間、地區、對象及使用方式，且當事人得自由選擇提供個人資料(第 8 條)。公務機關或非公務機關違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。如被害人人不易或不能證明其實際損害額時，每人每一事件新臺幣 500 元以上 2 萬元以下(第 28 條與第 29 條)。意圖為自己或第三人不法之利益或損害他人之利益，而對於

個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 100 萬元以下罰金(第 41 條與第 42 條)。

1. 我國現行法規定

電腦處理個人資料保護法第 3 條第 6 款及第 7 款所規範之主體，包括公務機關及非公務機關。而非公務機關依據該法第 3 條第 7 款，係指公務機關以外之事業、團體或個人，包括：

(1). 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。

(2). 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。

(3). 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。

對於非公務機關的範圍，除了上述第 3 條第 7 款第 1 目、第 2 目所明確規定的徵信業、醫院、學校等行業外，目前實務上，採第 3 條第 7 款第 3 目經法務部會同中央目的事業主管機關之指定，及由法院判決解釋的方式，用以確認是否為電腦處理個人資料保護法所規範之行為主體[73]。目前，已被指定的事業、團體或個人，如下：

(1) 百貨公司業

(2) 零售式量販業

(3) 私立就業服務機構

(4) 證券業

(5) 期貨業

(6) 不動產經紀業

經法務部會同中央目的事業主管機關之指定後，依電腦處理個人資料保護法第 43 條第 2 項規定，該受指定之事業、團體或個人，應於指定之日起 6 個月內，辦理登記或許可。

2. 個人資料保護法擴大主體適用範圍

依照現行電腦處理個人資料保護法第 3 條第 7 款第 3 目規定，「其他經法務部會同中央目的事業主管機關指定之事業、團體或

個人」，係為電腦處理個人資料保護法之規範對象，而未經指定之事業、團體或個人，則非為該法所規範之行為主體。「個人資料保護法」修正擴大適用規範對象，納入所有行業為規範之行為主體。換言之，現行法原本只有適用於特定行業，於個資法通過後，將擴大到蒐集個人資料的所有公、民營事業，不再侷限於現行的八大行業，而網路商店等電子商務業者，也將成為電腦處理個人資料保護法的規範對象。個人資料保護法修正之後，對於電子商務活動與個人資料保護法適用之影響，主要分為保護客體與行為主體二方面：(1)保護客體方面，個人資料保護法修正擴大客體適用範圍，不再僅限於電腦處理之個人資料，而將擴大到處理、蒐集及利用非經電腦處理之個人資料，且其將護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式等直接或間接方式識別該個人資料的保護，列為適用範圍。(2)行為主體方面，有關電子商務活動業者，例如網路商城、線上遊戲、部落格網站、線上影音等各式各樣之產業態樣，皆非現行法所明文規範之行業，因此，在電腦處理個人資料保護法中，為保護電子商務態樣中消費者之個人資料，只能採用指定或法院判決解釋的方式，將電子商務活動業者納為規範範圍。而於個資法通過後，將適用於所有行業，擴大行為主體的適用範圍，是以，網路商城、線上遊戲等電子商務業者，均為適用之規範對象[68]。

法務部 2011 年 2 月完成個資法施行細則草擬會議，最快 2011 年 5 月公布細則條文，預計新版個人資料保護法的正式適用施行，最快將從原本的 2012 年 1 月再延期到 2012 年 6 月左右。公布施行細則的同時，行政院便可同時公布新版個資法和施行細則正式適用的時間。參考原本的電腦處理個人資料保護法的公布到適用中間有一段適應期，加上新版個資法將適用於各行各業，一般預計至少會提供 1 年的適應期，因此，新版個資法正式適用的時期可能從原本的 2012 年 1 月延至該年 6 月。目前我國因個資法施行細則還在法務部研擬過程中，故實行個人資料保護時，採行部分仍使用電腦處理個人資料保護法中之規定，待個資法實行細則制定完成公布實施之後，才會全面取代原先舊法。

三、 隱匿身分與個人隱私分析與討論

對個人隱私之保護並不與網際網路隱匿身分之行為相牴觸，在特定的範圍內，個人的隱私資料受到保護，不論其是否有隱匿身分行為(即便是需要表明身分，也須保護個資)。但是當網際網路隱匿身分行為之行為造成重大的事件或影響時，如：韓國女星因

網路留言影響而自殺之事件、透過網路隱匿身分之行為遂行重大犯罪且難以追查等。故從韓國政府開始實行所謂的「網路實名制」，希望透過此一機制，讓網際網路隱匿身分之行為消失，每一位使用者使用網際網路時均透過真實的身分，藉以杜絕可能借用隱匿身分的行為進行謾罵、惡意留言或難以追查的犯罪者。

韓國多位影星因網友惡意的留言，再加上個人本身患憂鬱症，導致看到這些負面留言之後心情低落自殺。基於這些負面影響，韓國國內民眾，尤其網友，認為網路上惡意留言應該受到規範。自 2007 年 7 月起，韓國網路使用者不再允許匿名留言。此規定是基於 2007 年韓國資訊通訊部通過《促進使用信息通信網路及信息保護關聯法》規定，為淨化網路文化，引用“網路實名制”。主要目的是為整治韓國網路社會的惡習，改善惡意留言與利用網路匿名侵犯個人隱私現象，其適用對象為上網人數超過十萬人次的網站與公部門機關之網站。若想在這些使用率旺盛之網路上留言，就必須先以真實姓名加入會員，才得以被允許使用之。韓國政府希望藉由此規定能遏止日益嚴重的匿名與惡意網路留言之現象，避免再有人因此而身心受傷或自殺身亡。

網路實名制的實行，對企圖透過網路從事不法活動的人來說是一種威懾。特別是在不適宜青少年瀏覽的網站，由於規定使用者瀏覽前必須填寫正確的身分證號碼和姓名，進而在一定程度上將這些網站與未成年人隔離，也讓那些在網上發布有害訊息的網友三思而行。網路實名制是韓國網路管理最大的特點，成為網路安全的基礎。但也有人指出，過多使用身分證或實名認證制度，勢必增加居民身分證號碼洩露的危險。很多網路犯罪正是利用在網上獲得的真名和身分證號碼進行的。因此，這是實行網際網路實名制時值得注意的議題[57]。

推動實名制的理由可分為主要四項：第一、網路犯罪偵防，包括恐嚇、詐欺、毀謗、色情言論、和對於著作權的侵犯。第二、保護公共利益，為避免網友在論壇任意張貼不實訊息，損害廠商信譽或誤導消費者，或用不實訊息煽動群眾。第三、釐清網路業者的責任，透過實名制的管理，讓作為中介者的網路服務商可以排除和言論發表者的共同責任。第四、打擊恐怖活動，用實名制防止恐怖組織運用網路聊天室傳遞訊息，從事恐怖活動。對於非犯罪行為的言論，實名註冊會產生兩種效果，一種是嚇阻效果，對於所有言論只要對他人有所影響，無論其是否構成犯罪，都戒慎恐懼，因此，不負責任的言論和單純的個人想法抒發都將大幅減少。另一種效果是，處於臨界地位的言論一旦出現，網路業者

馬上面臨是否要提供言論發表人真實資料的兩難。業者提供資料會損害個人隱私，而不提供則須與言論發表人承擔共同責任。

我國民情是極重視個人言論自由之保護，若仿韓國實施實名制，恐招網路使用者與多方相關團體的抗議與反彈。為確保使用者之言論自由與個人隱私，學者專家傾向政府可採用「記名制」，若是使用者有不當留言或使用時，相關主管單位也可以查核到真實姓名。不但可顧及到言論自由與網路使用權，同時也可以適當保護個人隱私。

依上述各國對個人隱私之保護相關法規，可歸納出幾項原則：(1)使用個人資料需告知資料擁有者；(2)確保個人資料不會被毀損或不當使用；(3)使用個人資料需具正當性與合法性；(4)韓國特別規定個人資料須以真實姓名登入，不得匿名刊登個資(見表 3-1)。依我國 2010 年個人資料保護法之規定內容，事實上目前皆已與其他國家在個資保護規定與目的相符合，況且個資法規實行細則仍未確定，故此法仍未完全實施，待有朝一日實施後，瞭解其成效再進一步探討修正與否。

表 3-1 各國個人資料保護相關法規目的

國家	法 規	主要目的
美國	1980 年隱私保護法案 1986 年電子通信隱私法	(1) 告知：應當事先告知客戶，他們可以蒐集何種個人的資料或數據及如何使用這些資料。 (2) 消費者由於被不當使用或披露個人資訊，或由於被提供了不準確、過時的、不完整的或無關的個人資訊而受到傷害時有權要求賠償。
德國	1977 年「資料處理個人資料濫用防制法」(聯邦個人資料保護法)。 2003 年修正聯邦個人資料保護法	(1) 為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損。 (2) 修法目的旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令。 (3) 聯邦資料保護專員制
歐盟	2010 年《歐盟範圍內個人資	用戶可告知網站必須永久刪

國家	法　規	主要目的
	料數據全面保護實施辦法》簡稱「實施辦法」	除其註冊的個人資料的權利，並且規定公司在以任何形式使用用戶資料或對用戶的個人資料進行編輯前必須獲得用戶的明確授權。
日本	2003 年個人資料保護法	(1)資料利用目的之限制 (2)資料之適當取得 (3)確保資料正確性 (4)確保資料安全性 (5)確保資料之透明度，即為本法案之五項基本原則。
韓國	2008 年情報通信網利用促進及情報保護法修正案	限制性本人確認制 (實名制)即是一項在網站等進行網上留言時通過身分證確認本人的制度。
我國	2010 年個人資料保護法	個資法規定在向當事人蒐集個人資料時，須明確告知蒐集之目的、類別利用期間、地區、對象及使用方式，且當事人得自由選擇提供個人資料(個資法第 8 條)。

資料來源: 本研究整理

第二節　　商業活動

商業交易雙方，須要能夠確保交易的對象身分，以確保買方可取得貨物，賣方可已收到貨款。而網際網路透過電子商務進行交易的過程中，因網路匿名的特性，身分確認是困難的，所以需要特別設計交易方式或公正第三方等機制來進行。因此，在討論網際網路隱匿身分與竄改身分之行為時，相關透過網路之商業活動，包含：電子商務、傳統的商品透過網路交易等行為與規範法規等，均應納入議題檢視之。

一、　電子商務定義

電子商務(E-Commerce, EC)意指透過網際網路、企業內部網(Intranet) 和增值網(Value Added Network, VAN)以電子交易方式進行交易活動和相關服務活動，替代傳統商業活動，將各環節電

子化與網絡化之商業交易行為。電子商務包括電子貨幣交換、供應鏈管理、電子交易市場、網絡營銷、線上事務處理、電子資料交換(EDI)、存貨管理和自動數據收集系統等。在此過程中，利用到的資訊技術包括：網際網路、外部網絡、電子郵件、資料庫、電子目錄和行動電話等[15]。電子商務依交易方式不同，可分為企業對顧客、企業對企業、顧客對企業與顧客對顧客等方式。因此，過去傳統產業(如旅遊與保險業等)的經營方式都因電子交易的發展，而產生根本性的變革；換言之，因網路整合創造新的交易市場，減輕經營成本與提升服務品質，此皆賴於網路交易特質—互動性、立即性、溝通簡易性與精準回應性[50]。

由於電子商務的潛藏商機廣泛，包括行銷、廣告等項目。若被用於不當用途或被濫用，將構成網路經濟體的危機，其損失可能難以估計，包括商譽與消費者的信心度之損失。故此歐盟認為網路的規範應以促進經濟發展，同時兼顧正當的社會整體需求(公共利益)為目的；而後者是歐盟介入管制網路內容的主要因素[50]。因此為防弊電子商務的弊端，各國紛紛制定相關法規，用於規範廠商與消費者之責任與義務，以圖維護電子交易市場之公平、正當與合法性[72]。

二、 各國規定對電子商業活動之個人隱私規定

(一) 美國

關於消費者個人資料保護的法律規定，美國 1970 年的「公正信用報告法案」(Fair Credit Reporting Act，簡稱 FCRA)旨在避免消費信用報告機構(Consumer Reporting Agencies)將其所有消費者個人資料的揭露之不正確性與恣意性。於是該法規定關於上開單位於揭露所有之消費者個人資料於第三人時，必須經本人書面的同意。而所謂「得揭露於第三人」之情形，係指除非受揭露之第三人用於信用、受雇及保險調整評估、政府機關核發證照或福利，以及其它適法的商業用途時[64]。除此，美國為了有效解決電子商務行為與網路法律問題，除引用原有電腦相關法律外，先後廣徵產、官、學及研意見發表 NII 白皮書及全球電子商務架構(A Framework for Global Electronic Commerce)，對傳送(Transmission)的法律意義、侵害責任的歸屬等問題提出意見；並提出五個原則與九項建議，就關稅、電子付款、電子商法、智慧財產權保護、隱私權、安全性、通訊基礎建設、內容(Content)及技術標準等，做出原則性規範。

在商業活動方面，美國政府制定以下三項重要法規，確保網路交易之安全性，確保消費者的個人權益。

1. 全球暨國家商務電子簽章法(Electronic Signatures in Global and National Commerce Act，簡稱 ESIGN)

為保證電子商務行為之安全、合法及有效，由各州訂定數位簽章法(Digital Signature Act)並建立認證制度，以利遏止商務詐欺則儘量適用電腦犯罪相關法律。如美國猶他州在 1995 年 5 月便通過數位簽章法，該法利用「數位簽章(Digital Signature) 之安全技術以期保障網際網路上陌生人與陌生人的交易(Stranger to Stranger Business or Transactions between Parties Having no Prior Relationship)，並促進電子交易之流通。之後，美國各州於其後之立法，便逐漸轉向於制定以「技術中立」及「市場導向」為原則的電子簽章立法(Electronic Signature Legislation)，並在立法技術上以「紀錄(Record)」與「身分確認(Authenticate)」來取代傳統法律中「書面(Writing)」及「簽名(Signature)」的字眼。「統一州法全國委員會議」(National Conference of Commissioners on Uniform State Laws)為統一美國各州電子商務法律，於 1999 年提出建議各州採用的「統一電子交易法」(Uniform Electronic Transaction Act, 簡稱 UETA)，該法之第五條(b)項中，便明文規定該法僅適用於當事人均已同意以電子方式進行交易的情形。

此外，美國聯邦政府於 2000 年通過之「全球暨國家商務電子簽章法」，該法第 101 條(c)項(1)款中亦規定，如依法令規定與交易有關之資訊應以書面為之者，於取得消費者明確同意時，得以電子紀錄滿足法律規定必須做成書面之要求，其主要目的，均在保護交易當事人，使其不致因利用電子文件為溝通方法，而反遭受不利益的結果，故此法目的在開啟新的經濟契機，並保障美國消費者權利。電子簽章法規只規定原則性的定義，該法依據幾項原則制訂：a.自由市場和行業自律；b.技術中立原則；c.廣泛的當事人自治原則；d.外國不得干涉私營工業標準；此法具有幾項特點：a.法律承認電子紀錄、電子簽名，但是不要求使用電子紀錄或者電子簽名；b.如果要求提供給消費者書面通知，電子文本的通知就算符合要求，前提是消費者已同意接受並能取得該電子信息；c.如果州已採納了 UETA，或州法是符合技術中立的，州法有優先適用權。依據 ESIGN 第 102 條規定，ESIGN 原則上是鼓勵各州依 UETA 制定州級立法，並在確保技術中立的原則下，給予各州極大的裁量權去決定採用何種身分辨識技術。即一旦各該州依 UETA 制定或修改其成文制定法或法則，各該州即可依 UETA 的解釋，優先於聯邦的 ESIGN 而適用；反之若該州並未接受 UETA

時，聯邦 ESIGN 為確保技術中立原則，將依 ESIGN 相關規定解釋有關電子交易的法律爭議，以避免州法獨惠於特殊技術標準，而阻礙了電子商務的州際或跨國發展[27]。

2. 管制濫送色情及行銷之侵擾法（Controlling the Assault of Non-Solicited Pornography and Marketing Act, CAN-SPAM Act of 2003）

美國政府早在 1988 年便針對濫送商業電子郵件問題，由聯邦貿易委員會 Federal Trade Commission(FTC) 責成美國業界與民間團體，組成「未經邀約商業電子郵件專案工作小組」(The Ad-Hoc Working Group on Unsolicited Commercial Email)，就未經邀約之商業電子郵件(Unsolicited Commercial Email, UCE)氾濫問題，提出政府因應政策以及國會應行立法因應報告。美國國會歷年來曾提出不少與商業電子郵件相關規範法案，為兼顧人民隱私權、消費者保護與言論自由，如何因應未經邀約之商業電子郵件氾濫問題，向來為立法過程所爭執之重點。州立法對未經邀約之商業電子郵件問題較聯邦立法為早，自內華達州(Nevada) 1997 年 7 月通過 13 號州參議院法案開始，迄今已有三十餘州針對未經邀約之商業電子郵件進行立法管理；而聯邦立法則於 2003 年 12 月 16 日由美國布希總統簽署管制濫送色情及行銷之侵擾法（Controlling the Assault of Non-Solicited Pornography and Marketing Act, CAN-SPAM Act of 2003），並於 2004 年 1 月 1 日生效。

3. 數位千禧年著作權法 （Digital Millenium Copyright Act of 1998）

美國總統柯林頓於 1998 年 10 月月 28 日批准「1998 年數位化千禧年著作權法案(The Digital Millenium Copyright Act of 1998」，修正美國現行著作權法。「1998 年數位化千禧年著作權法案」[56]除履行「世界智慧財產權組織」所通過之「世界智慧財產權組織著作權條約(World Intellectual Property Organization Copyright Treaty, WCT)」及「世界智慧財產權組織表演及錄音物條約(WIPO Performances and Phonograms Treaty, WPPT)」之規定外，尚包括如下重點：

(1) 網路服務業者責任之限制。

(2) 允許維修過程中對於電腦程式之暫時性重製。

(3) 釐清美國著作權局對相關政策之職權。

(4) 延伸數位化廣播之暫時性錄製之例外。

(5) 要求美國著作權局向國會提出有關透過數位化科技促

進遠距教學之建議。

(6) 延伸現有對於圖書館與檔案機構之例外規定。

(7) 延伸錄音著作演出之法定授權至數位化傳輸。

(8) 引進有關集體談判協議下電影著作權利轉讓契約之相關推定。

(9) 船舶設計之著作保護。

依前述重點可知，「1998 年數位化千禧年著作權法案」事實上要規範之範圍，較「世界智慧財產權組織著作權條約(WCT)」及「世界智慧財產權組織表演及錄音物條約」(WPPT)之規定更廣。其內容再分為五項法案：

第一案「世界智慧財產權組織著作權及表演及錄音物條約執行法案」。（WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998）

第二案「網路著作權侵害責任限制法案」。（Online Copyright Infringement Liability Limitation Act）

第三案「電腦維修競爭確保法案」。（Computer Maintenance Competition Assurance Act）

第四案「綜合規定法案」。（Miscellaneous Provisions）

第五案「船舶設計保護法案」。（Vessel Hull Design Protection Act）

(二) 德國

根據 Global Industry Analysis 統計，2008 年德國電子商務市場中企業對企業(B2B)市場規模為 5,620 億歐元，佔全球份額的 10.4%。企業對顧客(B2C)市場規模為 750 億歐元，佔據全球份額為 9.9%。可見德國電子商業交易是非常蓬勃發展[90]。為維護使用者個人權益保護，德國於 1997 年 8 月 1 日開始實施「資訊與通信服務架構建置法規」(Gesetz zur Regelung der Ranhmenbedingungen für Informations-und Kommunikationsdienste)，國內多簡稱「多媒體法」(Informations-und Kommunidationsdienste Gesetz-IuKDG)，整套法規內容包括隱私權保護、著作權保障、青少年保護等議題；其中就網路服務提供者(Internet Service Provider, ISP)之法律責任規則規定於「電信服務法」(Teledienstengesetz, TDG)，後再依據歐盟電子商務指令(E-commerce Directive)關於網路服務提供者之責任規範，於 2001 年修正電信服務法網路服務提供者之相關條文[58]。TDG 該法於

2007 年 3 月國會通過第二次修正案，將法規名稱修正為電子媒體法(Telemediengesetz, TMG)，並將網路服務提供者之資訊提供義務等加以修正[58]。如電信法第 10 條規定，訊息儲存服務提供者對他人所儲存之訊息如有下列情況，則不負責任：(1)對於違法行為或訊息無知悉；或於民事損害賠償請求情況下，對於造成權利侵害之明顯情事無所知悉；(2)在知悉該違法情事存在後，立即除去該訊息或阻礙該訊息之接取。但前者免責規定不適用在訊息儲存服務提供者與訊息提供者間有隸屬、監督關係。如於知悉該違法行為或違法訊息後，立即移除該訊息或阻礙該訊息之接取，訊息儲存服務提供者仍有免責規定之適用[58]。

「多媒體法」中的第 3 條「數位簽章法」堪稱全世界最早賦予「以個人身分為根據且無法私自偽造的數位簽名」全國性法律效力的法律架構。此外德國並通過「數位簽章法」(Gesetz Zur Digitalen Signatur)僅就數位簽章而為立法，並未兼及其他電子簽章。為因應資訊、電信科技之發展，並配合歐盟於 1999 年 12 月 13 日公布之「共同組織電子簽章架構指令」，復於 2001 年 5 月 16 日通過「電子簽章架構條件法」(Gesetz über Rahmenbedingungen für Elektronische Signaturen)，2001 年 5 月 22 日開始生效。不同於傳統的資訊傳遞方式，使用網際網路傳遞資訊，需經過平台提供者(Host-provider)所提供網路空間將資訊發布，因網路的特性—快速與無國境—故訊息的傳遞若是違法將造成難以估計的損傷，如隱私短片揭露。基於此，德國政府對於網路提供者是否需直接或間接對這些違法負責加以規範，以下是德國政府規範商業活動違法行為之重要法規，分述如下：

1. 電子媒體法(Telemediengesetz, TMG)

該法是準電子商務法，於 2007 年 3 月生效，用來規範電子商務經營者的商業行為。TMG 共 16 條，主要內容有：(1)法律主體可以不經申請自行開設網站主頁；(2)但主頁必須包括經營者的有關詳細資訊，例如名字、聯繫方式、稅務登記號等；(3)經營者需披露所提供產品或服務的詳細資訊；(4)經營者對於消費者的個人資訊保護義務；(4)歐盟一國內註冊的經營者開展歐盟內業務時只需按照該國法律行事，無須符合其他成員國的法律規定。

2. 民法典(Burgerliches Geselzbuch, BGB)

主要涉及電子商務合同的訂立和電子簽名效力等問題。隨著民法典債權編的改革，原來的《遠程銷售法》已經取消，其規定已納入民法典。如法規第 13 條明文規定消費者之定義：消費者係

指，自然人中，非出於營業行為之目的，亦非出於獨立之職業行為之目的，而締結法律行為者[36]，故網路消費者也包含於其中。

3. 不正競爭防止法(Gestez gegen den unalutere Wettbewerb, UWG)

此法針對商業電子郵件規範，規範電子郵件廣告的發送行為。如第 18 條明文規定文件資料之利用規範，為競爭之目的，或圖利自己，對於營業交易中受託之技術文件資料，尤其是圖案、模型、樣版、配方，無權加以利用或洩漏他人者，處 2 年以下有期徒刑或科處罰金。

4. 電子簽名法(Gesetz über Rahmenbedingungen für elektronische Signaturen)

1997 年制定，2001 年頒布的《電子簽名條例》。在德國刑法、商標法、反不正當競爭法、著作權法、價格標注法、各州廣播合作法中也有關於電子商務的規定。

5. 電子服務法(Teledienstgesetz, TDG)

所謂「網路上的服務提供者」(ISP)一般分為接取服務提供者(Internet Access Provider, IAP)、平台服務提供者(Internet Platform Provider, IPP)與內容服務提供者(Internet Content Provider,ICP)。對於一般責任原則，依此法的規定，服務提供僅就自己所提供的資訊負責，亦即服務提供者對自己本身所為之資訊內容(包括編輯)，如有違反德國相關法規規定，則依法應負其相關責任；如 TDG 第 9 條至第 11 條規定，對於在其網路上傳輸之他人所提供之資訊，僅作傳輸的連線服務提供者、伺服器提供者、主機代管業者或搜尋引擎者雖不必負責，但仍負有被動注意義務或移除封鎖資訊的義務[59]。

(三) 歐盟

歐盟法規原則上不能在成員國直接適用，因為歐盟法一般以方針政策形式出現，僅規定了框架條件，還需各國透過國內法加以轉化執行。在電子商務方面重要的歐盟法規有歐盟委員會的《電子商務指令》和《準入監督指令》以及歐洲議會規範電子簽名的《1998/48/EG 指令》和《1999/93/EG 指令》等。

在歐盟同樣採取建置電子商務法制環境基礎下，建設資訊社會工程，如 1997 年的《歐洲電子商務行動方案》(A European Initiative in Electronic Commerce)，即在謀求建立一個安全可靠的電子商務法律體系，跨越國家主權壁壘，建立線上消費者信心。

1997 年 12 月，歐盟委員會提交《關於資訊社會著作權及鄰接權的指令草案》(Proposal for Directive on Copyright and Related Rights in the Information Society)；1998 年 8 月，歐盟頒布《關於資訊社會服務的透明度機制指令》(Directive on a Transparency Mechanism form Information Society Services)；1998 年 12 月，歐盟執委會通過歐盟《內部市場電子商務資訊社會服務法律框架指令》(Proposal for a Directive on certain Legal Aspects of Electronic Commerce in the Internal Market)，2002 年 7 月，歐洲會議與歐盟理事會通過《電子通訊中個人資料處理及隱私保護指令》(Directive on privacy and electronic communications)

1997 年之《電信事業個人資料處理及隱私保護指令》(Directive 97/66/EC)，議題廣泛包括網路隱私權的保護、電子商務的稅收、消費者權益保護、電子貨幣與電子支付、智慧財產權及著作權、資料與軟體的保護、電子簽章等。1999 年 12 月，歐盟委員會又提出《電子歐洲：為所有人建造的資訊社會》(eEurope: an Information Society for All)，同月，歐盟頒布《關於建立電子簽章共同法律架構指令》(Directive on a Community Framework for Electronic Signatures)。2000 年 5 月，歐盟議會通過電子商務有關的法律問題指令，即是電子商務指令(Directive on Electronic Commerce)，內容涉及網路服務、電子簽章、消費者權益、司法管轄、關稅與稅收、電子貨幣、著作權保護等。2000 年 6 月，歐盟與美國為解決有關個人資訊隱私的保護問題，特別簽訂安全港協議，使個人資訊受到跨國同等的保護[46]。

在商業行為中最重要法規即是「電子簽章共同法律架構指令」。1999「電子簽章共同法律架構指令」於 1999 年歐盟通過「電子簽章共同法律架構指令」，即「電子簽章指令」(Directive 1999/93EC of the European Parliament and of the Council of 13 December, 1999 on a Community Framework for Electronic Signatures)，承認電子簽章之法律效力，採取技術中立原則，對於電子簽章之服務提供者推定一系列之義務，為提供認證服務確立基本之行為規範。該指令目的是方便電子簽名的使用並使其法律效力得到承認。指令主要內容包括：(1)確定電子簽名效力的原則；(2)給電子簽名及相關概念加以定義；(3)確定成員國國內及國際電子簽名認證服務的市場許可；(4)對電子簽名數據的保護；(5)在指令附件中對於電子簽名認證提供商、電子簽名的產生裝置、電子簽名的安全核對提出了技術上和法律上的具體要求等 15 條正文以及 4 個附件。

此外，歐盟為能有效掌握恐怖主義份子與重大犯罪人的通聯與行蹤，於是透過制定規範，強制並延長電信與網路服務提供者

保存用戶通聯紀錄，以利檢警進行犯罪工作調查。在此背景下，「資料保存指令」(Directives on the Retention of Data)於 2005 年 12 月正式經歐盟議會表決通過，並在 2006 年 2 月經歐盟部長理事會(European Council of Minister)批可而正式生效。「資料保存指令」之規範內容之目的，主要是統合歐盟會員國賦予其內國電信業者，或網路服務提供者對所擁有通訊資料的保存義務，以確保這些通聯資料能及時被用於協助檢警進行重大犯罪偵察與起訴。適用範圍包含所有自然人或法人之通聯資料與位置資料，以及其他用來識別發話者與受話者所必須的資料；但不得適用於通訊實質內容之保存[54]。在資料保存內容部分，依其保存項目之不同，主要分為 6 大類：(1)追查與識別通訊之資料；(2)識別通訊地點之資料；(3)識別通訊日期、時間與通聯時間長短之資料；(3)識別通訊類型之資料；(5)識別用戶所使用之溝通器材及可能使用器材之資料；以及(6)識別行動通訊位置之資料等。依據此指令第 6 條之規定，各會員國需確保上述資料得保存 6 個月以上(但最多不得超過 24 個月)，並確保被保存之資料可隨時配合執法單位調查而提出，以協助調查時的參考利用[54]。

(四) 日本

日本政府鼓勵 ISP 的業者使用過濾軟體和標籤系統。1997 年 2 月網路的新聞報導指出，日本通產省與 ENC 共同合作發展過濾系統，此系統能防堵有關於犯罪(Crime)、色情(Sex)與暴力(Violence)的網站。報告中提到聰明晶片(Smart Chips)的發展，這種晶片好比電視的 V 晶片，能自動地防止接觸到不適宜的網站，使用者必須鍵入密碼才可以進入[66]。

1. 電子簽章暨認證業務法（電子署名及び認証業務に関する法律）

為確保順利推動電子簽章，以促進電子通訊之流通及處理，故須就電子簽章及電子紀錄真正成立之推定、特定認證業務之認定制度、其他相關必要事項詳加規定，日本總理府於 2000 年 5 月 31 日頒布本法，定 2001 年 4 月 1 日施行。

2. 著作權法（著作権法）

因應網路時代來臨，1997 年修法，明定公開傳輸應取得著作權人許可，於 LAN 或 Intranet 使用時，亦須取得著作權人同意。此外，學術機構或教育機構以研究或教學為由存取他人資料時，雖有須輸入帳號及密碼之限制，亦逾個人使用範圍，應獲得著作權人同意。順應數位時代潮流，日本逐次修法，強化著作權之相關規範，惟鑒於亞洲諸多國家其物價低於日本，為防止國外合法

生產之音樂光碟回流至日本，以較低價格販售，掠奪相關權利人之經濟利益，2004 年修法，就「明知僅限國外散布之商業性音樂光碟卻故意輸入日本販售」列入侵權行為，以俾匡正此陋習；2006 年亦修法嚴格取締輸出侵害著作權之商品，且強化侵權行為之刑事罰則，力求著作權保護至臻至善。最新修正 2008 年 6 月 18 日法律第 81 號增定對於兒童、學生之教科書、殘障使用等特定圖書之著作保護。

3. 不正競爭防止法（不正アクセス禁止法）

日本在 2002 年對不正競爭防止法中有關營業秘密保護問題進行修正研議，並於 2003 年立法通過修正建議，2004 年實施，即是日本對於營業秘密的保護規定在其不正競爭防止法中，依其於 1993 年所修正的不正競爭防止法第 2 條第 4 項的規定，所謂「營業秘密」，係指作為秘密而予以管理之生產方法、販賣方法以及其他對事實活動有用的技術上或營業上的情報，而不被公眾所知悉者。日本將營業秘密侵害之行為，具體規範在不正競爭防止法中，都當作是「不正競爭行為」，故就侵害營業秘密之行為，可依不正競爭防止法第 3 條規定，對於因不正競爭行為對營業上利益產生侵害或有侵害之虞時，請求其停止侵害行為或防止其為侵害行為；可依同法第 4 條規定，請求因故意或過失為不正競爭行為所生之損害賠償；若無法證明損害數額，則可依第 5 條規定決定之[86]。

(五) 韓國

韓國政府乃於 1999 年 7 月 1 日制定施行「電子商務基本法」（Basic Law on Electronic Commerce）。依據該法政策目標乃設定於對電子商務最低程度的政府管制，因此政府部門應有的作為，乃是民間主導、政府誘導或輔導（第 19 條）。依據該法規定，政府應訂定電子商務推展計畫，由產業能源部為主管機關，綜理政府全體有關計畫之推動事宜，設置於產業能源部內的政策委員會（Policy Committee）負責推展計畫之擬定，而其最終案之決定，則由「資訊化委員會」（Informationization Committee）負責（法第 21 條）。根據該基本法第 22 條規定，電子商務推展計畫的具體執行機關為「韓國電子商務機構」（Korean Institute for Electronic Commerce, KIEC），該機構為一獨立公益法人，其除為一技術研究機關外，並於國際標準化之事項上，為韓國對外協商之負責機關，一般網際網路服務提供事業，負有對 KIEC 之運作基金繳交一定款項之義務。另外一個依據電子商務基本法應設置之機構為「電子資料交換委員會」（Korean Electronic Data Interchange, KEDI），

統合相關事項的標準化作業（第 23 條）。最後，依據該基本法第 26 條規定，另有一「電子商務服務中心」（Electronic Commerce ）負責電子商務的教育、研修等事宜。

除此，韓國政府於 1999 年宣布「Cyber Korea 21」計畫，倡導以知識經濟為發展基礎的國家政策，並於 1999 年立法通過「電子商務架構法」(Framework Act on Electronic Commerce，或譯為 Basic Act on Electronic Transaction)，以基本法方式，讓行政機關的政令宣導及國內的電子商務基礎環境之建構有明確的法源依據。與「電子商務架構法」同為韓國電子商務核心法律者為「數位簽章法」(Digital Signature Act)，該法之立法目的是為完備電子商務安全與憑證服務之法制環境。由於數位簽章法將電子簽章的範圍限縮至「數位簽章技術」，無法與持續發展的各項電子簽章及憑證技術相銜接，韓國政府有鑑於此，於是將數位簽章的定義做擴張解釋，並基於全球化趨勢下國際交易日益頻繁，須對外國憑證在韓國之效力加以規範，於是韓國「數位簽章法」更名為「電子簽章法」（Electronic Signature Act）。為保證安全數位化的發展，2006 年韓國政府修正了關於商業票據法與支票的法律。其中的修正法案包括：「商業票據法」、「支票法」、「電子商務商業票據法」，及「電子支票法」等，目前皆已頒布實施。

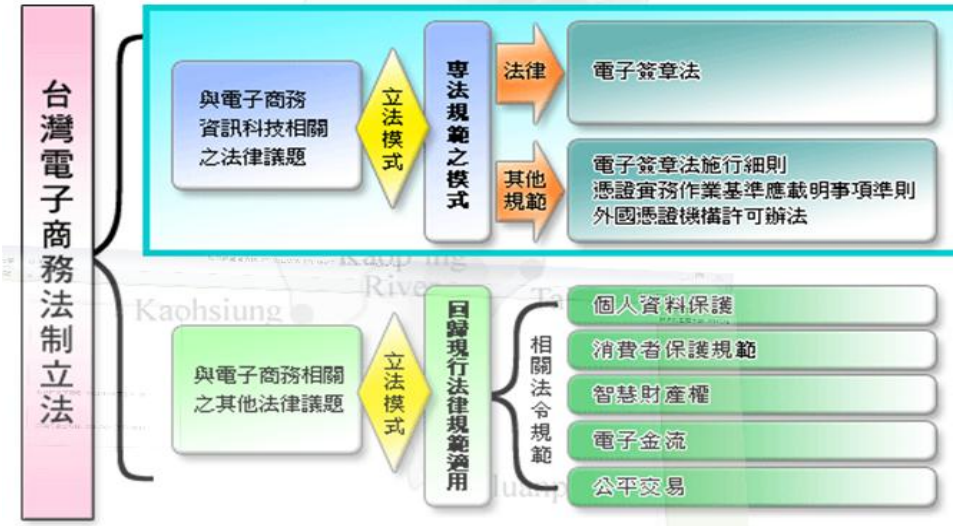
2006 年 4 月 28 日通過的「電子銀行交易法」，已於 2007 年 1 月 1 日施行。又為將電子化文件的檔案處理取得法源依據，並改善電子憑證文件管理系統(the eCertified E-document Authority System，簡稱 CEDA)，新修正的「電子商務架構法」規劃電子商務之新的國家電子化交易系統特以專章處理，而該新修正的 CEDA 法制部分亦於 2007 年開始施行[74]。在商業活動方面，主要相關重要法規如下：

1. 電子商務商業票據法（Electronic Signature Act）
2. 電子金融交易法（Electronic Financial transaction Act）
3. 電子商務架構法 (Framework Act on Electronic Commerce，或為 Basic Act on Electronic Transaction）
4. 計算機程序保護法（Computer Programs Protection Act）

(六) 我國

我國對於電子商務法制之立法，對於資訊技術性之特殊部分，採取專法規範之模式，如「電子簽章法」及「電子簽章法施行細則」、「憑證實務作業基準應載明事項準則」與「外國憑證機構許可辦法」等子法之制定。然而其他相關電子商務交易之所

產生的其他相關法律議題如交易行為之法律關係、消費者保護、智慧財產權的保護等，則回歸以現行法律為基礎規範，以調合傳統法律與科技新興法律所帶來的衝擊，並充實電子商務法制環境之發展方式[73]。我國電子商務法制立法方式如圖 3-1 所示，相關法規列舉說明如下。



資料來源：http://gcis.nat.gov.tw/eclaw/tjk/chinese/tjk_tw_body.asp?PageCode=tw_page2。

圖 3-1 我國電子商務法制立法方式

1. 光碟管理條例

光碟管理條例實施後，國內的「影音光碟」（Video Compact Disc，VCD）與「數位化多功能光碟」（Digital Versatile Disc，DVD）製造業者，將必須申請核發許可證與識別證方可進行製造，若未經許可製造光碟、未壓印來源識別碼、未經許可輸入製造機具等，將處以刑事罰與行政罰，透過此法案國內將可依此法規打擊光碟盜版業者。例如，未來若未經申請許可進行生產光碟的業者，一經查獲，政府依法可下令停工，並處以新臺幣 150 萬以上，新臺幣 300 萬元以下的罰鍰，並可連續處罰，最高處罰金額可達新臺幣 600 萬罰鍰；再不遵從者，處 1 年以上 3 年以下有期徒刑，得併科新臺幣 300 萬元以上 600 萬元以下罰金。(第 15 條)。依本條例第 3 條規定主管機關為經濟部。

2. 營業秘密法

2006 年實施營業秘密法，主要目的在於保障營業秘密，維護產業倫理與競爭秩序，調和社會公共利益。依此法第 2 條規定，「營業秘密」係指方法、技術、製程、配方、程式、設計或其他

可用於生產、銷售或經營之資訊，且符合下列要件者：(1)非一般涉及該類資訊之人所知者；(2)因其秘密性而具有實際或潛在之經濟價值者；(3)所有人已採取合理之保密措施者。依此法第 10 條之規定之一：以不正當方法取得營業秘密者。所謂「不正方法」，包括竊盜、詐欺、脅迫、賄賂、擅自重製、違反保密義務、引誘他人違反其保密義務或其他類似方法。營業秘密法僅規定民事損害賠償責任，但依個案情形，仍可能觸犯刑法之洩露業務上知悉工商秘密罪、竊盜罪、侵占罪、背信罪或違反公平交易法之相關規定。

3. 電子簽章法

此法於民國 90 年 11 月 14 日公布，主要目的在建立安全及可信賴之網路環境，確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，且能鑑別交易雙方之身分，並防止事後否認已完成交易之事實，乃電子化政府及電子商務能否全面普及之關鍵。該法主要以透過法律規定之方式，承認電子文件、電子簽章與實體書面、簽章有等同之效力，並對於數位簽章應用中，扮演「被信賴的第三人」（Trusted Third Party）角色簽發憑證，以證明簽章人身分的憑證機構加以規範。國內首於 1997 年由經濟部委託資策會科技法律中心進行數位簽章法之研究，並建議政府應儘速制訂數位簽章法，以律定電子簽章及電子文件之法律地位，建立電子憑證機構之管理制度，界定「憑證機構」（Certificate Authority，CA）與使用者之權責，建立跨國認證之機制。為推動安全的電子交易系統，政府及民間企業利用現代密碼技術，建置各領域之電子認證體系，提供身分認證及交易認證服務，以增進使用者之信心，並解決現有法令規範不足或不確定之處。此法第 2 條界定「電子文件」，意指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。「電子簽章」意指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。此法第 12 條規定，憑證機構違反規定者，主管機關視其情節，得處新臺幣 100 萬元以上 500 萬元以下罰鍰，並令其限期改正，逾期未改正者，得按次連續處罰。其情節重大者，並得停止其一部或全部業務。

4. 著作權法

著作權法可以更有效、更快速的保護著作權人的權益。此法第 90-4 條中明文規定網路服務提供者以契約、電子傳輸、自動偵測系統或其他方式，告知使用者若有三次涉有侵權情事，應終止全部或部分服務。對於用戶往往產生極大的影響，尤其我國的「通

知/ 取下」程序只要權利人單方發動即可，無須等待法院或行政機關之裁定或同意，業者即須執行取下涉及侵權的網頁（第 90-6 條第 3 款、第 90-7 條第 3 款、第 90-8 條第 3 款）。

我國電子商務產業之推動以行政院為最高政策指導單位，而相關政策、計畫之研擬與推動則由主管商業管理業務之「經濟部」為中央目的事業主管機關。目前經濟部商業司主管確認電子文件與電子簽章之法律效力之「電子簽章法」，並以「電子商務法制及基礎環境建構計畫」各項計畫來推動電子商務相關產業發展工作。至於與電子商務相關之其他事宜，則按各法規內容由各主管機關規範與管理之[73]。

資料來源：
http://gcis.nat.gov.tw/eclaw/tjk/chinese/tjk_tw_body.asp?PageCode=tw_page3

圖 3-2 我國電子商務法治推動機構

從 1999 年 7 月開始，經濟部商業司將「推動電子簽章法計畫」之法制相關推動工作正式委託「財團法人資訊工業策進會科技法律研究所」負責執行，以加強對國際立法發展趨勢之研究與比較，期對電子商務之立法制定、及其他各項相關規範方案之提出因應對策，促使完成我國電子商務法制化的立法推動工作。其他經濟部所負責與電子商務相關之工作有幾項：(1)智慧財產局所負責之國內智慧財產權之保護；(2)工業局則負責國內電子商務相關工業發展與推動；(3)關於電子商務之國際合作則由專司貿易推動的國貿局負責；(4)其他相關事項之各主管機關，如法務部所負責個人

資料之保護，行政院消費者保護委員會所負責消費者保護事宜等皆與電子商務法制推動相關[73]。

依上述對於消費者或相關主管單位，我國對於電子商務法規已有明確法律規定與職掌機關分工。若能有效整合跨機關合作，與各機關能確實執行相關法規，將有利於保護網路消費者權益。

三、 各國規定對電子商業活動與資料保護、存取分析與討論

為預防不當使用網路資料，造成消費者或使用者之損失，對於電信資料的保存，我國電信法第 7 條規定，除依法律規定查詢或是電信事業用戶查詢本人之通信紀錄之情形外，「電信事業或其服務人員對於電信之有無及其內容，應嚴守秘密，退職人員，亦同。」、「電信事業處理有關機關（構）查詢通信紀錄及使用者資料之作業程序，由電信總局訂定之。」與「電信事業用戶查詢通信紀錄作業辦法，由電信總局訂之。」。前電信總局根據上述法律之授權，於 2002 年 12 月 26 日制定「電信事業處理有關機關查詢電信通信紀錄實施辦法」（以下簡稱實施辦法），要求電信業者應保存電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼、通信日期、通信起迄時間等紀錄，並以電信系統設備性能可提供者為原則。同時，實施辦法第 5 條規定，對於電信事業通信紀錄之保存期限，市內通信紀錄應保存 3 個月，而國際、國內長途通信及行動通訊紀錄均應保存 6 個月[54]。

進行電子商務行為時，網際網路身份辨識部分可以分成網際網路連線及電子交易行為兩部分探討：在網際網路連線部分，對於撥接用戶識別帳號、通信日期、上下網時間紀錄與免費電子郵件信箱、網頁空間線上申請帳號時之來源 IP 位址，以及當時系統時間等紀錄，保存期間均為 6 個月；ADSL 用戶與纜線數據機用戶之識別帳號、通信日期與上下網時間；網際網路接取服務業者提供其用戶張貼於留言版、貼圖區或新聞討論群組之內容來源 IP 位址及當時系統時間，應保存 3 個月；網際網路接取服務業者提供電子郵件服務時，其通信紀錄之最少保存期間則為 1 個月[54]。對於違反本條規定之第二類電信業者，依據電信法第 64 條第 2 項，處新臺幣 20 萬元以上 100 百萬元以下罰鍰，並通知限期改善，屆期仍未改善者，則廢止其許可。另外，電子交易行為部分必須在兼顧交易安全及確保消費者權益與隱私權，因此對於網路平台及其上使用者，包括供應商與物流商，皆有必要加以規範[80]。經濟部電子商務資安通報服務中心在 2011 年公布了一系列在電子商務

交易安全規範[75]，包括電子商務資安通報機制規範及作業準則與對於網路平台、供應商、物流商等安全規範。其中在個人身分保存方面，主要要求須依照 ISO27001 制定安全作業管理，其中對於紀錄檔存查方式，業者可以依據電子商務交易風險管理需求或是實際執行情形自訂執行標準。

以歐盟為例，依「資料保存指令」第 6 條之規定，各會員國需確保上述資料得保存 6 個月以上（但最多不得超過 24 個月），並確保被保存之資料可隨時配合執法單位調查而提出，以協助調查時的參考利用。由於資料保存指令的訂定，明顯增加電信與網路服務提供者的負擔，若政府單位未提供補助或透過租稅減免的方式提供協助，這些成本勢必會轉嫁至電信及網路使用者身上，造成用戶費用的提高，進而引起民眾之反彈。故為使「資料保存指令」推動更為順利，歐盟學界與實務界均建議，歐盟會員國將本指令落實於該國法律時，應考量到如何對業者進行補助，避免業者將額外之費用轉嫁到用戶身上，增加用戶之負擔。

反觀我國，雖賦予電信業者於接受查詢時可收取查訊費用之規定（實施辦法第 7 條），但礙於查詢機關經費不足，實務上電信業者常無法依規定收取查詢費用，使電信業者將增加之成本轉嫁於消費者。此外，不同於我國目前僅規範電信業者保存之義務，但未要求業者在保存期限屆至後，應將資料去名化或刪除之作法，歐盟「資料保存指令」要求保存期限屆至後，各會員國必須要求其國內之業者將所保存之資料刪除，以確保資料安全並保障人民之隱私不受侵害。歐盟國家在思考資料保存之議題時，同時也考慮到人權與資料保護之議題[54]。相對於我國則採用配合個人資料保護法來考慮到此一議題。

依上述各國在網路商業行為的規範，皆著重於保護消費者之權益與個人資料隱私之保護，並且對網路服務者提出相關管制或規範；其目的除保護消費者，也在防止違法行為產生，故對於個人資料或使用紀錄之儲存與保護，皆加以規定以利日後相關單位處理。為達此些目的，各國皆制定電子簽章法規，確保使用者個人隱私，以及與網路服務者間交易行為之保護。

表 3-2 各國規定對電子商業活動之個人隱私規定

國家	法 規	主要目的
美國	(1) 全球暨國家商務電子簽章法 (2) 數位千禧年著作權法	(1) 如依法令規定與交易有關之資訊應以書面為之者，於取得消費者明確同意時，得以電子紀錄滿足法律規定必須做成書面之要求，其主要目的，均在保護交易當事人，使其不致因利用電子文件為溝通方法，而反遭受不利益的結果，故此法目的在開啟新的經濟契機，並保障美國消費者權利。 (2) 主要涉及電子商務合同的訂立和電子簽名效力等問題。
德國	(1) 電子媒體法 (2) 民法典 (3) 電子服務法 (4) 電子簽名法 (5) 不正競爭防止法	(1) 規範電子商務經營者的商業行為 (2) 主要涉及電子商務合同的訂立和電子簽名效力等問題。 (3) 對於一般責任原則，依此法的規定，服務提供僅就自己所提供的資訊負責，亦即服務提供者對自己本身所為之資訊內容(包括編輯)，如有違反德國相關法規規定，則依法應負其相關責任。 (4) 此法針對商業電子郵件規範，規範電子郵件廣告的發送行為。

國家	法　規	主要目的
歐盟	(1)電子商務指令 (2)電子簽章指令 (3)資料保存指令	(1)內容涉及網路服務、電子簽章、消費者權益、司法管轄、關稅與稅收、電子貨幣、著作權保護等。 (2)該指令目的是方便電子簽名的使用並使其法律效力得到承認。 (3)主要是統合歐盟會員國賦予其內國電信業者，或網路服務提供者對所擁有通訊資料的保存義務，以確保這些通聯資料能及時被用於協助檢警進行重大犯罪偵察與起訴。
日本	(1)電子簽章暨認證業務法 (2)著作權法 (3)不正競爭防止法	(1)為確保順利推動電子簽章，以促進電子通訊之流通及處理，故須就電子簽章及電子紀錄真正成立之推定、特定認證業務之認定制度。 (2)嚴格取締輸出侵害著作權之商品，且強化侵權行為之刑事罰則，力求著作權保護至臻至善。 (3)對於因不正競爭行為對營業上利益產生侵害或有侵害之虞時，請求其停止侵害行為或防止其為侵害行為。
韓國	電子商務基本法	依據該法政策目標乃設定於對電子商務最低程度的政府管制，因此政府部門應有的作為，乃是民間主導、政府誘導或輔導。
我國	電子簽章法	主要目的在建立安全及可信賴之網路環境，確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，且能鑑別交易雙方之身分，並防止事後否認已完成交易之事實，乃電子化政府及電子商務能否全面普及之關鍵。

資料來源：本研究整理

第三節　電腦與網路犯罪

一、　電腦與網路犯罪與隱匿、竄改身分

電腦網路犯罪案件，皆具有幾項的特性：散布性、身分易藏、證據難採、毀證容易、適法困難、偵查不易。目前網路犯罪類型大約可分為九種，即是網路性交易、網路盜拷、網路賭博、網路遊戲、網路詐欺、網路恐嚇、網路毀謗、駭客入侵與電腦病毒。這九種類型網路犯罪牽涉到技術面與非技術面兩種，前者是以網路為犯罪工具(特定目標)及以網路為犯罪客體(為攻擊目標)之類型，為隱藏其身分與引誘使用者上當等，會使用技術面的隱匿及竄改身分之行為，透過網路技術提升追蹤之困難度，其主要行為牽涉到連線欺騙(Spoofing)行為、代理 (Proxy)行為、Session Hijacking 攻擊與 Cookie 欺騙，主要犯罪行為是網路色情、網路援交、販賣盜拷、網路入侵（駭客）、散播電腦病毒、網路詐財與網路竄改等不法行為；後者是以網路空間作為犯罪場所之網路犯罪類型，較易使用非技術面的隱匿行為，其主要的偵查方式也非找到其偽冒之身分，而是追蹤金流，其牽涉到隱匿行為以偽冒身分與合法掩護非法居多，主要犯罪行為是網路色情、網路援交、販賣盜拷等居多[16][33][63][67]。

二、　各國法規對竄改身分之犯罪行為規範

(一) 美國

美國消費者聯盟(Consumer Union)在 2010 年 1 月進行「消費者報告（Consumer Report）網路狀況」調查 2,000 名美國成年網友，發現有 9%的社交網路用戶在過去一年曾遭遇惡意軟體入侵、詐騙、身分或騷擾等各種形式的傷害。根據該報告的估計，過去兩年內美國人因為網路犯罪而導致的損失高達 45 億美元，其中也包括因惡意程式入侵而置換 210 萬台電腦的費用。針對那些曾遭受過身分竊盜的使用者進行調查發現，有 67%的使用者表示他們應該知道個人資訊是如何洩漏的，其中有 20%認為是在進行其他網路活動時被攫取的，有 11%認為是因網路購物，有 5%認為是因網路金融交易，只有 1%認為其資料是從社交網站外洩的。因此，在網路犯罪方面，使用者個人身分與資料之保護途徑顯得格外重要。

網路犯罪申訴中心(Internet Crime Complaint Center, IC3)是美國 FBI 與美國國家白領犯罪中心（National White Collar Crime Center）所共同設立的網路詐騙申訴機構。根據 IC3 的統計 2008

年的申訴案件從 2007 年的 206,884 件，增加到 275,284 件，足足增加 30%以上，這也是繼 2005 年 231,493 件案例之後再創新高。事實上，美國的網路犯罪申訴案例自 2005 年之後原本開始逐年下降，2006 年與 2007 年皆微幅減少。不過詐騙金額則一直維持增加的趨勢，2008 年總計達 2 億 6459 萬美金，較 2007 年的 2 億 3909 億增加一成。在申訴類別中，以未送貨/未付款最高（32.9%），其次則是拍賣詐騙（25.5%）、信用卡詐騙（9%）及諸如「龐茲騙局」（Ponzi Schemes）一類的所謂「機密詐騙」（Confidence Fraud，7.9%）。而平均每個案例的被騙金額，最高者則是支票詐騙（3000 美元），其次則是機密詐騙（2000 美元），奈及利亞郵件詐騙（1650 美元）；金額最少的則是信用卡詐騙（223 美元），拍賣（610 美元），以及詐騙案例最多的未送貨/付款（800 美元）[60]。為此，美國於 1998 年通過「身分竊盜與僭越威攝法(Identity Theft and Assumption Deterrence Act)」，2004 修正身分辨識的定義，將姓名、社會安全碼、電話、指紋、聲紋等生物辨識資訊、電信設備辨識碼均納入為身分的一部分，違反者為聯邦重罪最高可處以 30 年有期徒刑、罰金與財產沒收。為「身分竊盜行為」之專法，用以規範現實社會與網路之偽冒身分之行為，亦是第一個也是目前唯一將「身分竊盜行為」以專法規範之國家，其餘國家，大多將偽冒身分之行為納入於個人資料保護、詐欺等法令中[85]。

美國聯邦法(Code of Federal Regulations)有其他相關規定，如未經授權或超出授權範圍故意進入使用電腦系統，意圖欺詐而未經授權或超出授權範圍故意進入使用被保護的電腦，以及意圖從事欺詐性交易、走私，而故意使用未經授權的密碼來進入使用政府電腦系統，或是州際、國際的商業電腦系統。(見表 3-3)以下是美國政府規範網路犯罪相關法規：

1. 美國愛國者法案(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001)
2. 計算機濫用修正案（Computer Abuse Amendments Act）
3. 海外情報監聽法（Foreign Intelligence Surveillance Act）。

「美國愛國者法案」（USA Patriot Act）是 2001 年 10 月 26 日由美國總統 George W. Bush 簽署頒布的國會法案（Act of Congress）[43]。正式的名稱為「Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001」，中文意義為「使用適當之手段來阻止或避免恐怖主義以團結並強化美國的法律」，此法案的目的是為防止恐怖主義，進而擴張美國警察機關的權限。根據法案的內容：

(1)警察機關有權搜索電話、電子郵件通訊、醫療、財務和其他種類的紀錄；(2)減少對於美國本土外國情報單位的限制；(3)擴張美國財政部長的權限以控制、管理金融方面的流通活動，特別是針對與外國人士或政治體有關的金融活動；(4)並加強警察和移民管理單位對於居留、驅逐被懷疑與恐怖主義有關的外籍人士的權力。此法案也延伸恐怖主義的定義，包括國內恐怖主義，擴大警察機關可管理的活動範圍。

在 70 年代，尼克遜政權濫用情報蒐集權力，白宮利用國家安全局（National Security Agency，簡稱 NSA）和聯邦調查局作為監視反越戰者、共產黨同情者等異己的工具，終於在 1978 年，國會通過《海外情報監聽法》（Foreign Intelligence Surveillance Act），同時設立隸屬司法部的「海外情報監聽法庭」（Foreign Intelligence Surveillance Court），規定情報機構如要在美國本土進行竊聽和搜查，必須先獲由 11 名聯邦法官組成的海外情報監察法庭批准，不經此法庭允許，國家安全局於法無據，不能對國內任何“外國勢力代理人”進行竊聽。《海外情報監聽法》草擬初衷，是要防範無孔不入監視民眾，以強而有力的立法制衡未來行政機關進行竊聽。在《海外情報監聽法》下，最受影響的是國家安全局。美國遭受 911 恐怖攻擊後，2002 年布希總統簽署秘密行政命令，授權國安局竊聽境內的美國國民、外國人與海外疑似恐怖分子的電話、電郵及其他通訊，行動審查權握在當時的白宮法律顧問手上。

表 3-3 美國聯邦法規內容列舉

法規	條(項)次	條文內容
聯邦法	第 1028 條	創設新的犯罪態樣-「身分竊盜」，禁止未經授權故意移轉或使用「用以辨識他人身分的方法」（a means of identification），違反者最高可處 15 年的有期徒刑、罰金與沒收財產的處罰。
	第 1028 條(a)(7)	「辨識身分的方法」定義擴張及於「單獨存在，或與其他資訊（如姓名、社會安全碼、電話、指紋、聲紋等生物辨識資訊、電信設備辨識碼等）連結存在，可供辨識特定個體的數字」，禁止移轉、持有或使用。
	第 1030 條(a)(1)	未經授權或超出授權範圍故意進入使用電腦系統，並藉此獲取受美國政府保護的國防和外交方面的資訊，或 1954 年原子能法所規定的受限制的資料。
	第 1030 條(a)(2)	未經授權或超出授權範圍故意進入使用電腦系統，並藉此獲取金融機構或美國聯邦法第 1602

法規	條(項)次	條文內容
		（n）條中所規定的信用卡發行者的金融資訊，或有關於誠信紀錄的消費者資訊，或美國政府任何部門或機關的資料，或涉及州際、國際通訊，而來自任何被保護的電腦內的之資料。
	第 1030 條(a)(3)	未經授權或超出授權範圍，故意進入使用美國政府機構或代理機構之任何非公用且供政府專用的電腦，或是該電腦雖非在供美國政府專用，但若為美國政府使用，該行為會影響被美國政府所使用的電腦或為其服務的電腦的運轉。
	第 1030 條(a)(4)	意圖欺詐而未經授權或超出授權範圍故意進入使用被保護的電腦，並藉由電腦使用獲取某種有價值的東西。
	第 1030 條(a)(5)	故意傳送程式（Program）、資訊（Information）、代碼（Code）或指令（Command），因而造成被保護的電腦的損壞；未經授權進入使用被保護的電腦，不論故意、輕率或是鹵莽而導致被保護的電腦的損壞。
	第 1030 條(a)(6)	意圖從事欺詐性交易、走私，而故意使用未經授權的密碼來進入使用政府電腦系統，或是州際、國際的商業電腦系統。
	第 1030 條(a)(7)	意圖勒索金錢或其他有價之物，故意於州際或國際商務中傳送含有任何威脅損壞受保護電腦的資訊。
	第 1030 條(a)(1)	未經授權或超出授權範圍故意進入使用電腦系統，並藉此獲取受美國政府保護的國防和外交方面的資訊，或 1954 年原子能法所規定的受限制的資料。
	第 1030 條(a)(2)	未經授權或超出授權範圍故意進入使用電腦系統，並藉此獲取金融機構或美國聯邦法第 1602（n）條中所規定的信用卡發行者的金融資訊，或有關於誠信紀錄的消費者資訊，或美國政府任何部門或機關的資料，或涉及州際、國際通訊，而來自任何被保護的電腦內的之資料。
	第 1030 條(a)(3)	未經授權或超出授權範圍，故意進入使用美國政府機構或代理機構之任何非公用且供政府專用的電腦，或是該電腦雖非在供美國政府專用，但若為美國政府使用，該行為會影響被美

法規	條(項)次	條文內容
		國政府所使用的電腦或為其服務的電腦的運轉。
	第 1030 條(a)(4)	意圖欺詐而未經授權或超出授權範圍故意進入使用被保護的電腦，並藉由電腦使用獲取某種有價值的東西。
	第 1030 條(a)(5)	故意傳送程式(Program)、資訊(Information)、代碼（Code）或指令（Command），因而造成被保護的電腦的損壞；未經授權進入使用被保護的電腦，不論故意、輕率或是鹵莽而導致被保護的電腦的損壞。
	第 1030 條(a)(6)	意圖從事欺詐性交易、走私，而故意使用未經授權的密碼來進入使用政府電腦系統，或是州際、國際的商業電腦系統。
	第 1030 條(a)(7)	意圖勒索金錢或其他有價之物，故意於州際或國際商務中傳送含有任何威脅損壞受保護電腦的資訊。

資料來源: 本研究整理

(二) 德國

目前德國網路犯罪型態，以無權取得或利用資料、資訊竄改與資訊破壞居多(見表 3-4)。基本上，德國電子簽章法制（資訊與通信服務法）對此些犯罪行為加以規範與處罰，此法規係架構於特定的技術標準－公開金鑰基礎建設 (PKI)之上，並認為「數位簽章」技術之利用是目前最臻成熟的身分辨識安全機制。德國在 1997 年提出「資訊與通信服務法」，此法為綜合性的法案，用來解決經由網際網路傳輸的違法內容，包括猥褻、色情、惡意言論、謠言、反猶太人等宣揚種族主義的言論，更嚴格規範有關納粹的言論思想與圖片等相關信息。德國也採用「德國刑法典」(Strafgesetzbuch)加以規範相關網路犯罪行為，如未獲授權而取得，或使他人取得受保護的資料，意圖偽造或使用作為證據的重要資料等相關竄改個資或文件違法行為，造成他人財產損失。在德國刑法典第 303 條 a 項明文規定網路隱匿與竄改資料行為之規範與處罰，即是「不法刪除、隱匿、使不能使用、或改變資料內容者，處以 2 年以下有期徒刑或罰金。本罪之未遂犯，處罰之。」(見表 3-4)以下是德國規範網路犯罪之重要法規：

1. 德國刑法典（Strafgesetzbuch）

2. 住宅監聽法（Gesetz zur akustischen Wohnraumüberwachung）
3. 資訊與通信服務法（Informations und Kommunikationsdienste-Gesetz，簡稱 IuKDG）

表 3-4 德國網路犯罪型態

類型	犯罪行為	法規
無權取得或利用資料	未獲授權而取得，或使他人取得受保護的資料	德國刑法典第 202 條 a 資料不正取得罪，處以 3 年以下有期徒刑或罰金。 所稱之資料，僅指以電子、磁性或其他非可直接以感官辨識之方式所儲存或傳送者。
資訊竄改	意圖為自己或第三人之非法利益，無權的影響資料處理，因而造成他人財產損害	德國刑法典第 263 條 a 電腦詐欺罪，處 5 年以下有期徒刑或罰金。
	意圖偽造或使用作為證據的重要資料	德國刑法典第 269 條資料偽造罪，處 5 年以下有期徒刑或罰金。 本罪之未遂犯，處罰之。
資訊破壞	非法刪除、隱匿、使不能使用、或改變資料內容	德國刑法典第 303 條 a 資料變更罪，處以 2 年以下有期徒刑或罰金。 本罪之未遂犯，處罰之。
	毀損或妨害與其他商業、企業、或官署上具有重要性之資料處理	德國刑法典第 303 條 b 電腦破壞罪，處 5 年以下有期徒刑或罰金。 本罪之未遂犯，處罰之。

資料來源：本研究整理

(三) 歐盟

歐盟於 2001 年 11 月由歐洲理事會的 26 個歐盟成員國以及美國、加拿大、日本和南非等 30 個國家的政府官員在布達佩斯共同簽署《網路犯罪公約》（Cyber-Crime Convention），此法成為全世界第一部針對網路犯罪行為所制訂的國際公約。而《網路犯罪公約》制定的目標之一是期望使國際間對於網路犯罪的立法有一

致共同的參考標的，也希望國際間在進行網路犯罪偵查時有一個國際公約予以支持，而得以有效進行國際合作。網路犯罪公約除序言外，本文分為 4 章，共計 48 個條文。序言是說明《網路犯罪公約》的功能、目標；第一章為術語的使用，即是對網路犯罪涉及的術語進行名詞定義其中包括有電腦系統（Computer System）、電腦資料（Computer Data）、服務提供者(Service Provider)與通訊資料（Traffic Data）等都有一明確之定義；而第二章為國家層面上的措施，包括有刑事實體法、刑事程序法和管轄權三個部分，其目的為要求各簽約國於各國國內應採取的措施，且在程序法部分規定了有關電子證據調查的特殊程序法制度，而值得注意的是在規範非法存取（Illegal Access）的行為方面，《網路犯罪公約》要求各國應立法明定非法存取為犯罪行為並應予處罰；第三章為國際合作，包括一般原則和特殊規定兩個部分，在一般原則中包含規範引渡及相互合作等相關問題，而特殊規定則係有關電腦證據取得的問題，簽約國應建立一週七天且一天 24 小時皆能聯絡合作機制的網路，各國也要對於相關人員加強訓練，並配予必要的裝備以配合各國合作事項的進行；第四章為最後條款，主要規定《網路犯罪公約》的簽署、生效、加入、區域應用、公約的效力、聲明、聯邦條款、保留、保留的法律地位和撤回、修訂、爭端處理、締約方大會、公約的退出和通告等事項。網路犯罪公約在第二章自第 2 條至第 10 條中制定了簽署國需要對九類網路犯罪行為以刑法處罰，見表 3-5。

在網路犯罪方面，歐盟主要規範法規是「2001 年網路犯罪公約」。「2001 年網路犯罪公約」要求各國應立法明定非法存取為犯罪行為並應予處罰，並透過國際合作建立聯絡合作機制的網路。網路犯罪公約在第二章自第 2 條至第 10 條中制定簽署國需要對九類網路犯罪行為以刑法處罰 ，分述於下[44][53]：

1. 非法存取（Illegal access）：指任何故意威脅或攻擊電腦系統及電腦資料的行為，如電腦駭客等行為，這些行為不僅帶給電腦系統及合法使用者極大困擾，更是影響電腦系統的正常運作，且若電腦系統因此故障，更需耗費人力、物力等資源去修復，故此類行為應予懲罰。(請參照《網路犯罪公約》第 2 條) 。
2. 非法截取（Illegal interception）：此類行為包括非法截取電腦傳送的「非公開性質」電腦資料，此項規定是用以保障電腦資料的機密性。根據歐洲理事會說明，如果電腦資料在傳送時，沒有意圖將資訊公開時，即使電腦資料是利用公眾網路進行傳送，也屬於「非公開性質」

的資料。(原文請參照《網路犯罪公約》第 3 條) 。

3. 資料干擾（Data interference）：包含任何故意毀損、刪除、破壞、修改或隱藏電腦資料的行為，此項規定乃是為了確保電腦資料的真確性和電腦程式的可用性。 (原文請參照《網路犯罪公約》第 4 條)。

4. 系統干擾（System interference）：此項規定與第四條的「資料干擾」不同，此項規定乃是針對妨礙電腦系統合法使用的行為。根據歐洲理事會的說明，任何電腦資料的傳送，只要其傳送方法足以對他人電腦系統構成「重大不良影響」時，將會被視為「嚴重妨礙」電腦系統合法使用。所以在此原則下，利用電腦系統傳送電腦病毒、蠕蟲、特洛伊木馬程式或濫發垃圾電子郵件，都符合「嚴重妨礙」電腦系統，即構成「系統干擾」的行為。(請參照《網路犯罪公約》第 5 條) 。

5. 設備濫用（Misuse of devices）：包含生產、銷售、發行或以任何方式提供任何從事上述各項網路犯罪的設備。由於進行上述網路犯罪，最簡便的方式便是使用駭客工具，因此間接催生了這些工具的製作與買賣，因此有需要嚴格懲罰這些工具的製作與買賣，從基本上杜絕網路犯罪行為。 (原文請參照《網路犯罪公約》第 6 條) 。

6. 偽造電腦資料（Computer-related forgery）：包括任何虛偽資料的輸入、更改、刪改、隱藏電腦資料，導致相關資料喪失真確性。目前歐洲理事會各成員國法律，偽造文件都是犯罪行為，需要接受刑事制裁，故此規定只是將無實體存在的電腦資料也納入「偽造文書」的文書範圍。(原文請參照《網路犯罪公約》第 7 條) 。

7. 電腦詐騙（Computer-related fraud）：包括任何有詐騙意圖的資料輸入、更改、刪除或隱藏任何電腦資料，或干擾電腦系統的正常運作，為個人謀取不法利益而導致他人財產損失，這是需要予以刑事處罰的犯罪行為。 (請參照《網路犯罪公約》第 8 條) 。

8. 兒童色情的犯罪（Offences related to child pornography）：包括一切在電腦系統生產、提供、發行或傳送、取得及持有兒童的色情資料，此項規定是泛指任何利用電腦系統進行的上述兒童色情犯罪行為。(請參照《網路犯罪公約》第 9 條) 。

9. 侵犯著作權及相關權利的行為（Offences related to

infringements of copyright and related rights）：此項規定包括數條保障智慧財產權的國際公約列為侵犯著作權的行為，《網路犯罪公約》也規定這些行為必須為故意、大規模進行，並使用電腦系統所達成的。（請參照《網路犯罪公約》第 10 條）

表 3-5 歐盟網路犯罪相關法規內容

法規	條(項)次	條文內容
網路犯罪公約	第 2 條	「非法進入」 各締約方應針對蓄意威脅或攻擊電腦系統及電腦資料的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 3 條	「非法截取」 各締約方應針對非法截取電腦傳送的「非公開性質」電腦資料的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 4 條	「資料干擾」 各締約方應針對蓄意毀壞、刪除、破壞、更改或隱瞞電腦資料的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 5 條	「系統干擾」 各締約方應針對電腦資料傳送方法足以對他人電腦系統構成「重大不良影響」的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 6 條	「不正當使用設備」 各締約方應針對以任何方式提供任何從事各項網路犯罪的設備的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 7 條	「偽造電腦資料」 各締約方應針對不誠實輸入、更改、刪改、隱瞞電腦資料，導致有關資料失去真實性的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 8 條	「電腦詐騙」 各締約方應針對意圖詐騙的輸入、更改、刪除或隱瞞任何電腦資料，或干擾電腦系統的正常運作，導致他

法規	條(項)次	條文內容
		人財產損失以謀取個人利益的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 9 條	「兒童色情相關犯罪」 各締約方應針對在電腦系統生產、提供、發行或傳送、取得及持有兒童的色情資料的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。
	第 10 條	「侵犯版權及相關權利」 各締約方應針對從事被保障智慧財產權國際公約列為侵犯著作權的行為，採取必要的立法和其他措施，規定該行為為刑事罪行。

資料來源: 本研究整理

(四) 日本

在日本學者與民間團體常批評，資訊社會中網路犯罪相關法規尚未趕上網路科技發展的腳步。因此日本在 1990 年代就開始配合網路科技的發展實施相關法規，為避免發生網路犯罪發生，同時保護一般民眾的個人資料。日本政府於 2007 年底公布的調查報告，則是建議立法要求所有網路內容（包括傳統媒體的網路版以及由使用者自行生產的部落格和網站），都應採取適度過濾，避免十八歲以下青少年接近有害內容。因網際網路科技發達，日本藉由行動電話或個人電腦連線上網的族群遽增，上網收發電子郵件儼然成為日常生活或社會經濟活動不可或缺之一部分。此方面重要法規如下：

1. 特定郵件傳送標準化法（特定電子メールの送信の適正化等に関する法律）

利用電子郵件聯繫者雖日趨增多，但非收信人要求或未經收信人同意擅自透過網路大量寄發廣告或宣傳電子郵件之行為已是不容小覷之社會問題。此種濫發電子郵件即俗稱之「垃圾郵件」不僅造成網際網路資源浪費，妨礙網際網路使用人收發電子郵件，因處理垃圾郵件而耗損之人力、物力，亦可能傷害經濟發展。有鑑於濫發商業電子郵件情事日益猖獗，為遏止垃圾郵件繼續泛濫，日本於 2002 年 4 月 17 日制定「特定電子郵件傳送標準化法」，並於 2003 年 7 月 24 日修正，希冀此法之施行，可使網際網路使

用人免於垃圾郵件騷擾，建構良好的電子郵件使用環境，俾促進高度資訊化社會健全發展。

2. 犯罪法規移轉防止法第 26 條(インターネット上への違法な情報へのガイドライン)

此法主要是因為利用網際網路之詐欺增加許多，特別是有關金融機關的相關犯罪率快速提升，為保護民眾的權益，除網際網路之外將內容擴大至一般狀況，所有有關此類犯罪者，一律處分。按規處分網際網路中不正當尋求對方的金融機關相關資訊者。在此不正當一詞包括恐嚇、匿名、假企業、身分盜用等。此一法規除網際網路之外對於一般情況下亦適用。

(五) 韓國

2010 年 4 月 1 日起，韓國新的網路誹謗法(即新修正之《情報通信網利用促進及情報保護法》)正式上路，明確規範韓國境內所有每天不重複造訪人數超過 10 萬的網站經營業者，都必須要求用戶提供其真實姓名和身分證號碼。事實上，韓國許多的入口網站或中大型網站早在這之前，便已要求網友必須以真實的身分證字號來註冊，因此這項法規的施行，對於韓國國內的網路產業影響並不大；但是對於非韓國國內的企業或崇尚言論自由的公司，如 Google 而言，雖然手上握有會員的基本檔案，未來勢必也得從善如流，對於網路實名制建立一個新的查核制度。

在韓國有關網路犯罪主要主管機關：韓國資訊通訊部(MIC)、韓國電子商務資源中心(CRC)與網路爭議調解中心與韓國資訊安全署(KISA)。目前韓國現行針對網路侮辱罪相關法律，如下：

1. 憲法第 309 條 (於出版物等所為之名譽毀損罪)

(1) 以毀謗他人為目的，於新聞、雜誌及收音機等其他出版物中違犯 307 條第 1 項之罪者處 3 年以下徒刑、禁錮或 700 萬元以下的罰金。

(2) 以第 1 項之方法違犯第 307 條第 2 項之罪者，處 7 年以下的徒刑、10 年以下的褫奪公權或 1500 萬元以下的罰金。第 311 條 (侮辱)公然侮辱他人者處 1 年以下徒刑、禁錮或 200 萬元以下的罰金。

2. 情報通信網利用促進及情報保護法第 60 條(損害賠償等)

(1) 網路服務提供者(ISP)於提供網路服務時，如對於網路服務使用者有發生損害之情形時，應負損害賠償

責任。但如該損害的發生是因網路服務使用者之故意或嚴重過失，則不在此限。

(2) 如有發生第 1 項以外之損害賠償時，須與受損害賠償者達成協議。

(3) 如在第 2 項其他損害賠償有關的協議中，有無法達成協議或無法進行協議之情形，當事者可向傳播通信審議委員會申請裁定。

其他相關重要法規如下：

1. 電信事業法（전기통신사업법시행령）
2. 促進使用信息通信網路及信息保護關聯法(정보통신망 이용촉진 및 정보보호 등에 관한 법률)
3. 1948 年國家保安法（국가보안법）

韓國政府決定在 2005 年 10 月起實行網際網路實名制，即在網路上發帖(發布訊息)、跟帖(回覆訊息)以及上傳照片和動態影像時需要確認居民身分證和本人真名的制度，以糾正網路不良行為猖獗，如在網上侵犯人權、詆毀名譽、侮辱謾罵等現象。韓國人的上網活動目前已比較接近實名化了。在韓國的很多網站，發布訊息的條件是必須成為會員，在加入會員時必須留下身分證號碼等個人資料。在韓國上網獲得增(加)值服務前，也必須提供身分證號碼。而韓國已開設的身分證號碼網上認證系統，可以即時驗證個人身分。對於 17 歲以下沒有身分證的青少年，網站在獲取青少年詳細訊息後，會通過行動電話發送密碼的方式確認使用者身分。由於韓國行動電話在銷售時必須有身分證明，網路管理部門在需要時可以通過向行動電話運營商合作，追查上網者的真實身分，對未成年者加強管理，提供保護。

(六) 我國

依內政部警政署之「警政統計通報」統計報告我國在 99 年 1 至 10 月電腦網路犯罪概況，99 年 1 至 10 月電腦網路犯罪發生數 15,115 件，較 98 年同期減少 7,608 件(-33.48％)，破獲率 77.74％，較上年同期減少 6.83 個百分點，呈現發生數減少、破獲率減少情形，惟發生數減少幅度大於破獲率。依據資策會(FIND)統計，近 5 年經常上網人口或網際網路連網應用普及率均呈逐年增加趨勢，至 98 年底，上網人數達 1 千萬餘人以上，網路應用普及率達 46％ (見表 3-6)。99 年 1 至 10 月電腦網路犯罪發生數主要為詐欺 7,463 件最多、妨害電腦使用 3,079 件次之、侵害智慧財產權 2,251 件居第三。依案類別觀察，本期發生數以「詐欺」(7,463 件，占 49.37％)最多、「妨害電腦使用」(3,079 件，占 20.37％)次之、「侵

害智慧財產權」(2,251 件，占 14.89%)居第三，此三類共占電腦網路犯罪 84.64%；破獲率除「妨害電腦使用」因多為網路遊戲，偵辦時發現上網來源端為中國大陸、香港等地，追查不易，破獲比例較低(19.32%)外，其餘案類破獲率約有 7 成或以上。(見表 3-6 與表 3-7)

表 3-6 近5年電腦網路上網人數及犯罪概況

年別	經常上網人口(萬人)	網路應用普及率(%)	發生數(件)	破獲數(件)	破獲率(%)	嫌疑人(人)(A)	被害人(人)(B)	倍數關係(B)/(A)
94年	959	42	24,479	5,768	23.56	5,350	22,209	4.15
95年	976	43	22,711	10,900	47.99	10,430	19,487	1.87
96年	1,003	44	29,285	21,260	72.60	18,917	22,545	1.19
97年	1,046	45	26,523	20,840	78.57	18,952	21,179	1.12
98年	1,067	46	26,479	22,289	84.18	18,757	24,620	1.31

資料來源：內政部警政署，警政統計通報（99年第50號）[17]。

表 3-7 2010 年 1-10 月電腦網路犯罪概況-依類別

項目別	發生數				破獲數			破獲率	
	本期(件)	結構比(%)	與上年同期比較		本期(件)	與上年同期比較		本期(%)	與上年同期增減(百分點)
			增減數(件)	增減率(%)		增減數(件)	增減率(%)		
總計	**15,115**	**100.00**	**-7,608**	**-33.48**	**11,751**	**-7,467**	**-38.85**	**77.74**	**-6.83**
詐欺	7,463	49.37	-4,977	-40.01	6,975	-4,770	-40.61	93.46	-0.95
妨害電腦使用	3,079	20.37	-398	-11.45	595	-405	-40.50	19.32	-9.44
侵害智慧財產權	2,251	14.89	-479	-17.55	2,245	-475	-17.46	99.73	0.10
妨害名譽(信用)	874	5.78	64	7.90	604	23	3.96	69.11	-2.62
一般妨害風化	421	2.79	-1,466	-77.69	418	-1,469	-77.85	99.29	-0.71
違反兒童及少年性交易防制條例	228	1.51	-215	-48.53	228	-215	-48.53	100.00	-
賭博	288	1.91	137	90.73	288	137	90.73	100.00	-
其他	511	3.38	-274	-34.90	398	-293	-42.40	77.89	-10.14

資料來源：內政部警政署，警政統計通報（99 年第 50 號）[17]。

1. 刑法第 36 章妨害電腦使用罪

在此章中明文規定網路犯罪刑責與罰金，分述如下：

- 第 358 條規定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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。

- 第 359 條規定無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。
- 第 360 條明定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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。
- 第 361 條規定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。
- 第 362 條明定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 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。
- 第 363 條明定第 358 條至第 360 條之罪，須告訴乃論。

2. 通訊保障及監察法

依通訊保障及監察法第 1 條規定：「為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，特制定本法」，該法立法目的係為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序而制定。因此，該法不僅是為偵查犯罪而設，更在於保障人民秘密通訊之自由。因之該法名稱中，「保障」尚在「監察」之前。又該法第 5 條規定：有事實足認被告或犯罪嫌疑人有下列各款罪嫌之一，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，得發通訊監察書[39][87][88]。

3. 行政單位執掌

網路科技進步，使得犯罪行為更趨複雜，網路犯罪行為有許多類型，不同類型行為各有其主管機關。例如：網路販賣醫療藥品屬於衛生署主管、網路發表內容違反著作權法屬於智慧財產局等，因此牽涉到的主管機關眾多。針對網路犯罪行為偵辦與防制上，主要以內政部警政署主管犯罪防制與偵查、經濟部商業司主管網路身分認證法規與通傳會主管網路接取紀錄規範等三者為主要管制單位，分述如下。

(1) 內政部警政署（包含相關警察機構）

網路犯罪行為屬於科技犯罪，偵辦以警政署為主管機關。警政署於 2006 年 4 月成立「科技犯罪防制中心」，網路犯罪為其中不可忽視之重要項目。各類網際網路隱匿與竄改身分犯罪行為，

包含前述非技術面及技術面之行為均屬於警政署防制與偵辦之範圍。

觀察 2005-2008 年警察機關受（處）理妨害電腦使用案情況，以 2005 年最為嚴重。自 2005 年刑事警察局成立「科技犯罪防制中心」，並於各警察機關成立「科技犯罪偵查專責組」加強偵查作為，妨害電腦使用案發生數從 2005 年最高點 18,296 件逐年遞減，破獲率自 2005 年最低點 3.57%逐年遞增，被害人數亦從 2005 年 18,323 人大幅下降至 2008 年 4,224 人，顯示警察單位偵防作為對遏止犯罪已有顯著成效。

(2) 經濟部商業司

經濟部商業司主要職掌分為數項，其中「商業管理」與「電子商務」等兩項與資訊科技相關，內容包含全國商業行政資訊系統、電子工商、電子遊戲機、商業科技、電子商務與物流等項目。涉及利益之商業行為經常需要認證身分，因此網路身分認證重要法源：電子簽章法，目前是經濟部商業司所主管。

(3) 國家通訊傳播委員會

通傳會依通訊傳播基本法及國家通訊傳播委員會組織法規定掌管電信法、廣播電視法、有線廣播電視法及衛星廣播電視法等原隸屬交通部、新聞局、交通部電信總局之相關通訊傳播法規。在網際網路隱匿與竄改身分犯罪行為中，涉及網際網路接取服務經營者對於電信通信紀錄保存期間之規範由通傳會所主管。

以上三者可說是網際網路隱匿與竄改身分行為態樣與防制犯罪偵辦、身分認證法規管理、網際網路接取服務法規管理之重要單位。因此，三者功能之發揮與否將牽涉到國內網路犯罪增減與管制之重要關鍵。

表 3-8 我國網路犯罪行為模式與法規

類型	犯罪行為	法規
網路色情	散布或販賣猥褻圖片的色情網站	➢ 兒童及少年性交易防治條例第 33 條「電腦網路散播色色情廣告」罪。 ➢ 刑法第 235 條「散布猥褻圖畫影像」罪。 ➢ 如果所提供的是未滿 18 歲之人的猥褻圖片，則觸犯了兒童及少年性交易防制條例第 28 條第 1 項。
	在網路上媒	➢ 刑法第 231 條第 1 項「意圖營利，引誘或容留良家婦女，與他人姦淫者」。

類型	犯罪行為	法規
	介色情交易	➢ 刑法第 231 條第 1 項「意圖使男女與他人為性交或猥褻之行為者，而引誘、容留或媒介以營利者」。 ➢ 刑法第 233 條第 1 項「意圖使未滿 16 歲之男女與他人為性交或猥褻之行為者，而引誘、容留或媒介之者」。 ➢ 社會秩序維護法第 80 條，媒合暗娼賣淫者，處 3 日以下拘留或新臺幣 3 萬元以下罰鍰。
電腦駭客	未經授權進入他人之系統	➢ 刑法第 358 條規定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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。 ➢ 第 360 條規定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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。
	偷窺檔案	➢ 如果駭客所偷窺的是封緘的信函、文書或圖畫，則可構成刑法 315 條的妨害書信秘密罪(部分情況不適用)。 ➢ 刑法 359 條規定無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。
	複製檔案	➢ 電腦駭客入侵系統，複製他人檔案，可能構成刑法 320 條竊盜罪 (部分情況不適用)。 ➢ 刑法 359 條規定無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。 ➢ 著作權法 91 條的重製罪。
	更改、刪除檔案	➢ 如果所更改或刪改的檔案具有「表示其用意之證明」的功能，亦即其屬文書的話，則可能構成偽造文書罪，也可能構成刑法 352 條的毀損文書罪
	盜用他人網	➢ 電信法第 56 條第 1 項規定，「意圖為自己

類型	犯罪行為	法規
	路	或第三人不法之利益，以有線、無線或其他電磁方式，盜接或盜用他人電信設備通信者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 15 萬元以下罰金。」
	盜用他人密碼	➢ 刑法第 358 條規定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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。
	電腦病毒	➢ 刑法第 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罪。 ➢ 刑法第 362 條製作專供妨害電腦使用之電腦程式罪。
網路詐欺	竊取虛擬寶物	➢ 刑法第 339 條普通詐欺罪 ➢ 刑法第 323 條竊盜罪
	詐騙帳號	➢ 刑法第 158 條(冒充公務員行使職權) ➢ 刑法第 339 條普通詐欺罪 ➢ 個人資料保護法第 42 條(販賣個人資料)
	虛設行號	➢ 刑法第 339 條普通詐欺罪
	網路情人	➢ 刑法第 339 條普通詐欺罪
	網路老鼠會	➢ 刑法第 339 條普通詐欺罪
傳統犯罪	網路販毒	➢ 毒品危害條例相關規定
	網路上販賣槍枝 網路上教製炸彈	➢ 槍砲彈藥刀械管制條例 ➢ 刑法第 153 條第 1 款之以文字公然煽惑他人犯罪
	網路誹謗與公然侮辱	➢ 刑法 309 條第 1 項的公然侮辱罪 ➢ 刑法 310 條第 2 項的加重誹謗罪
	網路恐嚇	➢ 刑法 305 條恐嚇危害安全罪
	冒用他人名義	➢ 刑法 217 條第 1 項偽造署押罪

類型	犯罪行為	法規
	網路販賣禁藥	➢ 藥事法第 22 條(禁藥之定義) ➢ 藥事法第 83 條(明知偽藥或禁藥而販賣) ➢ 毒品危害防制條例第四條(製造、運輸、販賣第一、二、三級毒品) ➢ 毒品危害防制條例第 5 條(意圖販賣而持有毒品)
	網路賭博	➢ 刑法第 266 條(普通賭博) ➢ 刑法第 267 條(已刪除) ➢ 刑法第 268 條(供給賭場圖利或聚眾賭博罪) ➢ 惟因網路賭博有虛擬特性，「公眾得出入場所」、「聚眾」等概念在解釋上可能有疑問。
	侵害商標	➢ 商標法第 81 條(侵害他人商標專用權之處罰) ➢ 商標法第 80 條(證明標章準用商標之規定) ➢ 著作權法第 91 條第 1 項(重製他人著作罰則)
	竊取股市交易秘密	➢ 刑法第 318 之 1 條洩露利用以電腦設備而知悉之秘密罪 ➢ 刑法第 320 條竊盜罪 ➢ 刑法第 323 條竊盜罪

資料來源：本研究整理

表 3-9 我國相關法規內容

法規	條(項)次	條文內容
電信法	第 56 條第 1 項	意圖為自己或第三人不法之利益，以有線、無線或其他電磁方式，盜接或盜用他人電信設備通信者，處五年以下有期徒刑、拘役或科或併科新臺幣 15 萬元以下罰金。
個人資料保護法	第 42 條	意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 100 萬元以下罰金。
商標法	第 80 條	證明標章、團體標章或團體商標除本章另有規定外，依其性質準用本法有關商標之規定。
	第 81 條	未得商標權人或團體商標權人同意，有下列情形之一者，處 3 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金： 一、於同一商品或服務，使用相同之註冊商標或團體商標者。 二、於類似之商品或服務，使用相同之註冊商標或團體商標，有致相關消費者混淆誤認之虞者。 三、於同一或類似之商品或服務，使用近似於其註冊商標或團體商標之商標，有致相關消費者混淆誤認之虞者。
兒童及少年性交易防治條例	第 33 條	廣告物、出版品、廣播、電視、電子訊號、電腦網路或其他媒體，散布、播送或刊登足以引誘、媒介、暗示或其他促使人為性交易之訊息者，由各目的事業主管機關處以新臺幣 5 萬元以上 60 萬元以下罰鍰。 新聞主管機關對於違反前項規定之媒體，應發布新聞並公告之。
	第 28 條第 1 項	散布、播送或販賣前條拍攝、製造之圖片、影片、影帶、光碟、電磁紀錄或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處 3 年以下有期徒刑，得併科新臺幣 500 萬元以下罰金。

法規	條(項)次	條文內容
著作權法	第 91 條	擅自以重製之方法侵害他人之著作財產權者，處 3 年以下有期徒刑、拘役，或科或併科新臺幣 75 萬元以下罰金。 意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處 6 月以上 5 年以下有期徒刑，得併科新臺幣 20 萬元以上 200 元以下罰金。 以重製於光碟之方法犯前項之罪者，處 6 月以上 5 年以下有期徒刑，得併科新臺幣 50 萬元以上 500 萬元以下罰金。 著作僅供個人參考或合理使用者，不構成著作權侵害。
	第 91 條 第 1 項	擅自以移轉所有權之方法散布著作原件或其重製物而侵害他人之著作財產權者，處 3 年以下有期徒刑、拘役，或科或併科新臺幣 50 萬元以下罰金。 明知係侵害著作財產權之重製物而散布或意圖散布而公開陳列或持有者，處 3 年以下有期徒刑，得併科新臺幣 7 萬元以上 75 萬元以下罰金。 犯前項之罪，其重製物為光碟者，處 6 月以上 3 年以下有期徒刑，得併科新臺幣 20 萬元以上 200 萬元以下罰金。但違反第 87 條第 4 款規定輸入之光碟，不在此限。 犯前二項之罪，經供出其物品來源，因而破獲者，得減輕其刑。
槍砲彈藥刀械管制條例	第 7 條	未經許可，製造、販賣或運輸火砲、肩射武器、機關槍、衝鋒槍、卡柄槍、自動步槍、普通步槍、馬槍、手槍或各類砲彈、炸彈、爆裂物者，處死刑、無期徒刑或 7 年以上有期徒刑；處徒刑者，併科新臺幣 3000 萬元以下罰金。 未經許可，轉讓、出租或出借前項所列槍砲、彈藥者，處無期徒刑或 5 年以上有期徒刑，併科新臺幣 1 千萬元以下罰金。 意圖供自己或他人犯罪之用，而犯前二項之罪者，處死刑或無期徒刑；處徒刑者，併科新臺幣 5000 萬元以下罰金。 未經許可，持有、寄藏或意圖販賣而陳列第 1 項所列槍砲、彈藥者，處 5 年以上有期徒刑，併科新臺幣 1000 萬元以下罰金。

法規	條(項)次	條文內容
		意圖供自己或他人犯罪之用，以強盜、搶奪、竊盜或其他非法方法，持有依法執行公務之人所持有之第 1 項所列槍砲、彈藥者，得加重其刑至二分之一。 第 1 項至第 3 項之未遂犯罰之。
	第 8 條	未經許可，製造、販賣或運輸鋼筆槍、瓦斯槍、麻醉槍、獵槍、空氣槍或第 4 條第 1 項第 1 款所定其他可發射金屬或子彈具有殺傷力之各式槍砲者，處無期徒刑或 5 年以上有期徒刑，併科新臺幣 1000 萬元以下罰金。 未經許可，轉讓、出租或出借前項所列槍枝者，處 5 年以上有期徒刑，併科新臺幣 1000 萬元以下罰金。 意圖供自己或他人犯罪之用，而犯前二項之罪者，處無期徒刑或 7 年以上有期徒刑，併科新臺幣 1000 萬元以下罰金。 未經許可，持有、寄藏或意圖販賣而陳列第 1 項所列槍枝者，處 3 年以上 10 年以下有期徒刑，併科新臺幣 700 萬元以下罰金。 第 1 項至第 3 項之未遂犯罰之。
	第 9 條	未經許可，製造、販賣、轉讓、出租或出借魚槍者，處 1 年以下有期徒刑、拘役或新臺幣 50 萬元以下罰金。 意圖供自己或他人犯罪之用，而犯前項之罪者，處 2 年以下有期徒刑、拘役或新臺幣 100 萬元以下罰金。 未經許可，持有、寄藏或意圖販賣而陳列魚槍者，處 6 月以下有期徒刑、拘役或新臺幣 50 萬元以下罰金。 第 1 項及第 2 項之未遂犯罰之。
毒品危害條例	第 4 條	製造、運輸、販賣第一級毒品者，處死刑或無期徒刑；處無期徒刑者，得併科新臺幣 2000 萬元以下罰金。 製造、運輸、販賣第二級毒品者，處無期徒刑或七年以上有期徒刑，得併科新臺幣 1000 萬元以下罰金。 製造、運輸、販賣第三級毒品者，處五年以上有期徒刑，得併科新臺幣 700 萬元以下罰金。 製造、運輸、販賣第四級毒品者，處 3 年以上 10 年以下有期徒刑，得併科新臺幣 300 萬元以下罰金。 製造、運輸、販賣專供製造或施用毒品之器具者，處

法規	條(項)次	條文內容
		1年以上7年以下有期徒刑，得併科新臺幣100萬元以下罰金。 前五項之未遂犯罰之。
刑法	第5條	意圖販賣而持有第一級毒品者，處無期徒刑或十年以上有期徒刑，得併科新臺幣700萬元以下罰金。 意圖販賣而持有第二級毒品者，處5年以上有期徒刑，得併科新臺幣500萬元以下罰金。 意圖販賣而持有第三級毒品者，處3年以上10年以下有期徒刑，得併科新臺幣300萬元以下罰金。 意圖販賣而持有第四級毒品或專供製造、施用毒品之器具者，處1年以上7年以下有期徒刑，得併科新臺幣100萬元以下罰金。
	第153條第1項	以文字、圖畫、演說或他法，公然為左列行為之一者，處2年以下有期徒刑、拘役或100元以下罰金：一、煽惑他人犯罪者。
	第158條	冒充公務員而行使其職權者，處3年以下有期徒刑、拘役或500元以下罰金。 冒充外國公務員而行使其職權者，亦同。
	第217條第1項	偽造印章、印文或署押，足以生損害於公眾或他人者，處3年以下有期徒刑。
	第231條	意圖使男女與他人為性交或猥褻之行為，而引誘、容留或媒介以營利者，處5年以下有期徒刑，得併科10萬元以下罰金。以詐術犯之者，亦同。 公務員包庇他人犯前項之罪者，依前項之規定加重其刑至二分之一。
	第231條第1項	意圖營利，以強暴、脅迫、恐嚇、監控、藥劑、催眠術或其他違反本人意願之方法使男女與他人為性交或猥褻之行為者，處7年以上有期徒刑，得併科30萬元以下罰金。 媒介、收受、藏匿前項之人或使之隱避者，處1年以上7年以下有期徒刑。 公務員包庇他人犯前二項之罪者，依各該項之規定加重其刑至二分之一。 第一項之未遂犯罰之。

法規	條(項)次	條文內容
	第 233 條 第 1 項	意圖使未滿 16 歲之男女與他人為性交或猥褻之行為，而引誘、容留或媒介之者，處 5 年以下有期徒刑、拘役或 5000 元以下罰金。以詐術犯之者，亦同。
	第 235 條	散布、播送或販賣猥褻之文字、圖畫、聲音、影像或其他物品，或公然陳列，或以他法供人觀覽、聽聞者，處 2 年以下有期徒刑、拘役或科或併科 3 萬元以下罰金。 意圖散布、播送、販賣而製造、持有前項文字、圖畫、聲音、影像及其附著物或其他物品者，亦同。 前二項之文字、圖畫、聲音或影像之附著物及物品，不問屬於犯人與否，沒收之。
	第 266 條	在公共場所或公眾得出入之場所賭博財物者，處 1000 元以下罰金。但以供人暫時娛樂之物為賭者，不在此限。 當場賭博之器具與在賭檯或兌換籌碼處之財物，不問屬於犯人與否，沒收之。
	第 268 條	意圖營利，供給賭博場所或聚眾賭博者，處 3 年以下有期徒刑，得併科 3000 元以下罰金。
	第 305 條	以加害生命、身體、自由、名譽、財產之事，恐嚇他人致生危害於安全者，處 2 年以下有期徒刑、拘役或 300 元以下罰金。
	第 309 條 第 1 項	公然侮辱人者，處拘役或 300 元以下罰金。
	第 310 條 第 2 項	散布文字、圖畫犯前項之罪者，處 2 年以下有期徒刑、拘役或 1000 元以下罰金。 對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。
	第 315 條	無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或 3000 元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。
	第 318 條 第 1 項	無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處 2 年以下有期徒刑、拘役或 5000 元以下罰金。

法規	條(項)次	條文內容
	第 320 條	意圖為自己或第三人不法之所有，而竊取他人之動產者，為竊盜罪，處 5 年以下有期徒刑、拘役或 500 元以下罰金。 意圖為自己或第三人不法之利益，而竊佔他人之不動產者，依前項之規定處斷。 前二項之未遂犯罰之。
	第 323 條	電能、熱能及其他能量，關於本章之罪，以動產論。
	第 339 條	意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處 5 年以下有期徒刑、拘役或科或併科 1000 元以下罰金。 以前項方法得財產上不法之利益或使第三人得之者，亦同。 前二項之未遂犯罰之。
	第 339 條 第 1 項	意圖為自己或第三人不法之所有，以不正方法由收費設備取得他人之物者，處 1 年以下有期徒刑、拘役或 3000 元以下罰金。 以前項方法得財產上不法之利益或使第三人得之者，亦同。
	第 339 條 第 2 項	意圖為自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處 3 年以下有期徒刑、拘役或 1 萬元以下罰金。 以前項方法得財產上不法之利益或使第三人得之者，亦同。
	第 339 條 第 3 項	意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處 7 年以下有期徒刑。 以前項方法得財產上不法之利益或使第三人得之者，亦同。
	第 352 條	毀棄、損壞他人文書或致令不堪用，足以生損害於公眾或他人者，處 3 年以下有期徒刑、拘役或 1 萬元以下罰金。
	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 3 年以下有期

法規	條(項)次	條文內容
		徒刑、拘役或科或併科 10 萬元以下罰金。
	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 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

資料來源: 本研究整理

依上述分析，我國目前對網路犯罪有明文規定，依犯罪行為不同，可採用不同法規處罰之，列舉如下:

1. 網路上散播色情圖畫影像（可能成立散播猥褻物品罪）。
2. 網路上辱罵他人或黑函中傷他人(可能成立公然侮辱罪或刑法第 310 條的誹謗罪）。
3. 網路上傳播足以破壞他人經濟信用的消息(可能成立妨害信用罪）。
4. 侵入國防機密系統（可能刺探或蒐集國防秘密罪或刑法第 111 條刺探或收集中華民國國防應秘密之文書罪）。
5. 「網路上教人製造炸彈」（煽惑他人犯罪）。
6. 寄送電子郵件恐嚇他人（可能成立恐嚇罪）。
7. 未經授權侵入他人的系統檔案或窺看電子郵件(妨害書信或文書秘密罪)。使用電腦病毒擾亂或毀壞他人的系統檔案(毀損文書）。
8. 假冒他人名義，發送涉及權利義務的電子郵件，例如訂購書本（偽造文書罪）。
9. 偽造金融卡（偽造文書罪）。

三、 各國規定對電腦與網路犯罪及隱匿與偽造身分之分析討論

科技的發展日新月異，於是影響網路上的犯罪手段及手法也不斷更新變化，其相關待解決之網路犯罪問題錯綜複雜，除國內負責單位須有技術能力，還須了解法規相關規範，才能適時遏止網路犯罪。例如管轄權的問題：網路活動或交易發生範圍可能是國內，也可能是跨國，若國內網路犯罪行為，我國執法單位即可

偵查與破案；若是跨國不法問題，就牽涉到國際法規與外交關係，國內主管機關可能因跨國無邦交關係，而導致無法繼續偵查與破案，這是亟待解決的外交及跨國合作問題。

網路犯罪防制為確保國家網路能正當合法發展，其整體網路犯罪防制體系之各權責單位應緊密結合，避免多頭馬車事權不一，以發揮防制網路犯罪的最大效果[70]。目前我國防範網路犯罪的三個層次為犯罪偵查、政策研擬與技術研發，分由內政部警政署、法務部與通傳會，以及教育部等單位負責。不同單位間如可良好的溝通聯繫，更能夠達成防制網路犯罪各層次相互整合支援之功能。若網路犯罪已經發生，則網路業者是否能保存相關資料並提供作為偵察與證據使用，更顯得重要。針對國內網路服務業者，有個人資料保護法上的限制，需由司法機關申請調閱特定範圍內之資料，較不易引發爭議，例如用戶連線 IP，但如調閱使用者的資料傳輸內容，則恐有侵害個人秘密問題，例如調閱電子郵件信箱內容。針對國外網路服務業者，在無國際邦交、合作關係、法令限制下，要求配合偵查困難度將更高[18][71]。

綜觀各國對於網路犯罪相關法規，均大同小異，且法律規範主要是懲罰造成他人、國家或公眾損失者，或維護公平性。因此，隱匿身分之行為並非法律條文中所規範的特定行為，故現有法令規章對於一般網路身分隱匿行為沒有規範限制。對於網際網路竄改身分行為之法律規範，所蒐集之各國法案大多沒有特別規範，特別值得一提的是美國「身分竊盜法案」，透過專法規範偽冒身分之行為。我國目前對於竄改及偽冒身分之行為之相關法令規範主要透過刑法「竄改文書罪」及「詐欺罪」等進行規範。同樣有足夠之法令規範，應不必同美國一樣，為網際網路竄改身分行為設立專法。

表 3-10 各國對網路犯罪之主要法規規定

國家	法　規	主要目的
美國	(1) 美國愛國者法案 (2) 聯邦法第 1030 條 (3) 身分竊盜法案（聯邦法第 1028 條）	(1). 此法案的目的是為防止恐怖主義，進而擴張美國警察機關的權限。 (2). 意圖從事欺詐性交易、走私，而故意使用未經授權的密碼來進入使用政府電腦系統，或是州際、國際的商業電腦系統。 (3). 專為身分竊盜行為制訂之專法。

國家	法　規	主要目的
德國	(1).資訊與通信服務法 (2).德國刑法典	(1). 解決經由網際網路傳輸的違法內容，包括猥褻、色情、惡意言論、謠言、反猶太人等宣揚種族主義的言論，更嚴格規範有關納粹的言論思想與圖片等相關信息。 (2). 規範相關網路犯罪行為，如未獲授權而取得，或使他人取得受保護的資料，意圖偽造或使用作為證據的重要資料等相關竄改個資或文件違法行為，造成他人財產損失。
歐盟	網路犯罪公約	期望使國際間對於網路犯罪的立法有一致共同的參考標的，也希望國際間在進行網路犯罪偵查時有一個國際公約予以支持，而得以有效進行國際合作。
日本	犯罪法規移轉防止法	此法主要是因為利用網際網路之詐欺增加許多，特別是有關金融機關的相關犯罪率快速提升，為保護民眾的權益，除網際網路之外將內容擴大至一般狀況，所有有關此類犯罪者，一律處分。
韓國	(1). 情報通信網利用促進及情報保護法第60條 (2). 通訊保障及監察法	(1). 明文規定網路犯罪刑責與罰金 (2). 為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序而制定。
我國	2003 年刑法第 36 章	網路服務提供者(ISP)於提供網路服務時，如對於網路服務使用者有發生損害之情形時，應負損害賠償責任。但如該損害的發生是因網路服務使用者之故意或嚴重過失，則不在此限。

資料來源: 本研究整理

第四章　網際網路隱匿與竄改身分行為防制技術

網際網路隱匿與竄改身分行為態樣可以依據「非技術面」及「技術面」進行分類。防制技術也可依據這兩種方式進行。

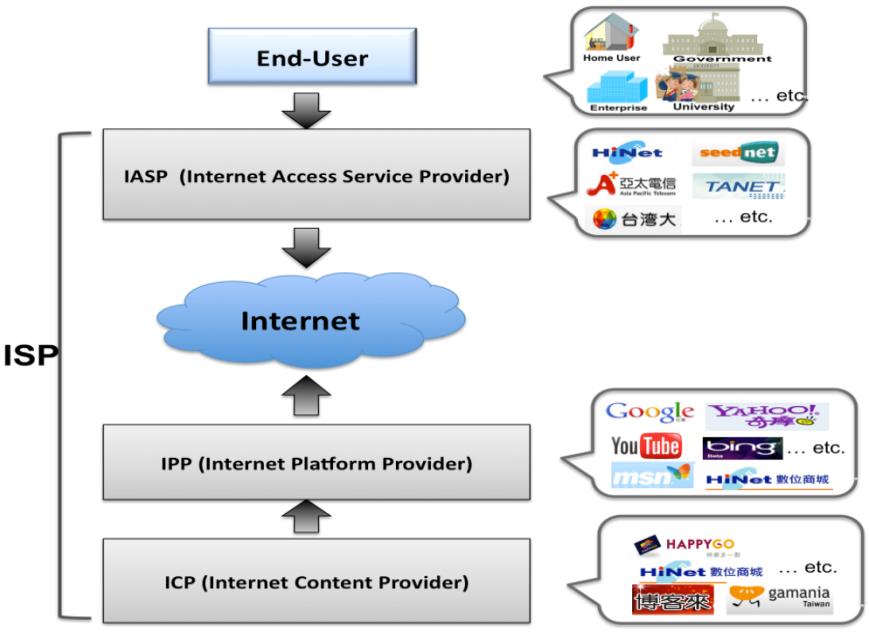
第一節　非技術面隱匿與竄改身分行為防制技術進行方向

非技術面隱匿與竄改身分行為主要包括：偽冒身分及位置與合法掩飾非法等兩種主要態樣。這些行為屬於容易進行之方式，技術需求低。如同傳統隱匿與竄改身分之犯罪行為一般，非技術面相關犯罪行為之防制技術進行方向可以分成減少偽冒動機以及提高偽冒門檻兩個方向進行，分別敘述如下：

一、　減少偽冒位置與身分之動機

網際網路使用過程中，所經過的各類伺服器會留下網際網路連線使用紀錄，這些連線紀錄可以協助調查網路使用來源。根據「電腦網路內容分級處理辦法」定義，電腦網路服務提供者(Internet Service Provide, ISP)依據範圍再細分為網際網路接取服務提供者(Internet Access Service Provider, IASP)提供連線服務給使用者連上網路，例如 Hinet、Seednet、我國學術網路(TANET)…等；網際網路平臺提供者(Internet Platform Provider, IPP)則是提供上網後各項網路相關服務的業者，例如 YAHOO!電子信箱服務、提供檔案傳輸服務的 FTP 業者或提供資料檢索與搜尋引擎的業者；以及網際網路內容提供者(Internet Content Provider, ICP)，主要係指提供多媒體內容的網路業者，其對於所播放的內容有決定權，通常也有在經濟或通訊面上加以監督或控制的可能性，圖 4.1 呈現三者彼此之間之關係。有些業者因其業務會同時扮演多個角色，如中華電信除提供網際網路接取服務(屬 IASP)，使用者可利用其線路連接網際網路，亦提供一個平台提供各式各種商務服務(屬 IPP)，如：購物商城、伺服器租賃(Hi-Cloud)、電子郵件申請、影片選取…等，且在多媒體影片平台上購物商城上提供影片播放(屬 ICP)。ICP 及 IPP 屬於網路應用的層次，其中 ICP 上使用者的法律責任在於所提供的內容，IPP 負責平台管理維護，可以檢視所管理網頁內容，若所提供之內容違反法律需追查違法人員身分。這兩類提供者針對相關服務使用人身分認證，部分重要網路服務，例如網路轉帳，必須認證使用者真實身分，許多應用服務，包括網路論壇及社交網路則未硬性要求使用真實姓名身分，這兩部分會依照業務屬性會有相關專業認定，因此由相關專業部門主

管，如醫藥部分由衛生署所管理。至於 IASP 負責網路接取服務部分，可以確認使用者連線部分，依照「第二類電信事業管理規則」規範，IASP 電信通信紀錄依屬性必須保存 1 至 6 個月，這些紀錄在犯罪調查或是蒐集證據，可以用來協助確認使用來源，可以降低偽冒位置與身分並遂行犯罪動機。



資料來源：本研究整理

圖 4-1 IASP、IPP、ICP 關係示意圖

依據圖 4-1，IASP 業者可以得知用戶資訊以及連線紀錄，因此 IASP 業者連線紀錄通常可以提供連線上網位置，但實際上一個用戶連線往往會有許多人共用，因此偵辦犯罪行為時，必須進一步偵查實際上網情形。另外因應網路族群增加，需要增加數位鑑識人員的員額及鑑識人員加強數位鑑識能力訓練。

無線網路與有線網路之最大差異是網路信號傳輸媒介為無線電波，容易被截取訊號使用。如果用戶自行架設無線網路 AP 提供上網且未做好適當安全防護時，無線溢波會讓未經許可之使用者盜用，在偵辦上確認使用者比較不容易。這部分防範要從教育面著手 良好的資訊安全教育教導民眾維護自身資訊安全，例如無線網路 AP 務必加上安全之防護協定，如 WPA 與 WPA2 等。同時要求 AP 製造業者在快速上手的手冊中加入啟動加密功能並做好登錄密碼設定。如果業者依照規定留下連線紀錄，加上數量充足且技術純熟的數位鑑識人員確實偵辦犯罪行為，配合良好的資訊安全教育，可以減少偽冒身分與位置之動機。

二、 提高偽冒身分之門檻

IPP 及 ICP 提供服務屬性是針對特定使用者，因此連線紀錄除了上網位址外，也可以留下使用者上網內容，包括發表內容或是線上交易等。目前一般 IPP 對其使用者的身分檢查，通常不會要求確認使用者之真實身分，即可提供服務。至於身兼 IASP 角色之 IPP，因為整合收費原因，可以利用使用者註冊之電子郵件查明真實身分。如果在 IPP 或 ICP 領域內發生涉及犯罪行為時，往往必須配合犯罪者上網之位址來逐步偵查使用者身分。

為了避免網際網路隱匿與竄改身分行為，而提高偽冒身分之門檻，第一個必須重視的是認證身分中個人帳號及密碼保護之問題，許多網路釣魚便是以竊取使用者帳號及密碼為目的。這部分的防制措施，可透過教育使用者使具有良好之網路使用習慣，例如：不隨意下載即時通訊或是電子郵件附件，尤其是可以執行的附檔，以防止帳號密碼被竊。執行帳號密碼傳輸之連線，要改用具加密技術之安全連線，例如：SSL 連線，以防止傳輸過程中被竊聽。依此觀點來看，傳統之檔案傳輸協定(File transfer protocol, FTP)、電子郵件收信協定(Post office protocol 3, POP3)等，原本都未對帳號密碼傳輸加以保護，這些都必須加上安全防護，以確實提高偽冒身分之門檻。

另外一個比較嚴謹之避免偽冒身分方式是使用憑證(Certificate)認證身分，這部分國內已具有良好之建設[24]。依照 ITU-T X.509 標準，目前政府已經建置良好之政府公鑰基礎建設(Government Public key infrastructure, GPKI)，GPKI 為一個階層式(Hierarchy)公開金鑰基礎建設，GPKI 所屬各憑證機構(Certification Authority, CA)包含政府憑證總管理中心(Government Root Certification Authority, GRCA)以及各政府機關所設立的下屬憑證機構(Subordinate CA)所組成，目前相關組織如圖 4-2 所示。各相關憑證機構認證服務對象與主管單位如表 4-1 所示。依照電子簽章法規定 CA 應製作憑證實務作業基準(Certificates Practice Statement, CPS)，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。這部分經過多年努力，在網路身分認證上，我國已具有良好之技術基礎。對於許多電子化政府之業務具有良好之助益。

資料來源: http://grca.nat.gov.tw/

圖 4-2 政府公鑰基礎建設架構

為了兼顧方便與安全，許多網站會採用比較基本之帳號密碼以及憑證之身分認證方式，例如國家科學委員會之入口，如圖 4-3 所示，其中 MOICA 即為使用自然人憑證登入之畫面。因為許多憑證機構之憑證實務作業基準會要求憑證申請時，認證真實身分。因此使用憑證是網路實名制施行之重要步驟，也是確認使用者身分，避免隱匿與竄改身分之重要技術。但是網路匿名文化以及言論隱私權等議題造成網路實名制是個充滿爭議的議題，這部分，我們認為依據網站性質來規範是一個適當之作法[79]。如網路所得稅申報、網路銀行轉帳等這些攸關權益，在原本行為中，便規範必須認證身分之行為，在網路上還是得按照原本要求實施實名認證。上述之所得稅申報、銀行轉帳等行為，在原本規範中即必須確認身分，具有比較高的偽冒身分門檻。

表 4-1 政府公鑰基礎建設架構

交互認證憑證	憑證使用對象	註冊窗口	主管機關
GCA 憑證	政府機關(構)及單位	行政院研究發	行政院研究發

		展考核委員會	展考核委員會
MOEACA 憑證	公司、分公司及商號	經濟部商業司、各縣市政府公司及商號登記機關	經濟部
MOICA 憑證	一般民眾	內政部資訊中心及各縣市戶政事務所	內政部
XCA 憑證	學校、財團法人、社團法人、行政法人、自由職業事務所、其他組織或團體	各類憑證用戶之主管機關	行政院研究發展考核委員會
HCA 憑證	醫事人員、醫事機構及其所屬應用於醫事專門用途的伺服器應用軟體	全國衛生局所	行政院衛生署
GTestCA 憑證	GCA、MOEACA、MOICA、XCA 之測試憑證	無	行政院研究發展考核委員會

資料來源: http://grca.nat.gov.tw/02-01.html

資料來源: http://web1.nsc.gov.tw/

圖 4-3 國家科學委員會入口身分認證

第二節　技術面隱匿與竄改身分行為防制技術進行方向

技術面隱匿與竄改身分行為態樣，往往與作業系統、網路協定、網路結構有密切關聯。犯罪行為也會包含技術成分，如連線欺騙、駭客攻擊等。本節就技術面之網際網路隱匿與竄改身分攻擊行為，共三種行為類型分別對應七種攻擊態樣，分別研究其追查與防禦方法，並就 IASP、IPP、ICP 角度加以探討其可能實行之防禦措施。下表說明隱匿與竄改身分行為類型與攻擊態樣：

表 4-2 技術面之隱匿與竄改身分行為

行為分類	攻擊態樣
欺騙行為	IP 欺騙(IP Spoofing) ARP 欺騙(ARP Spoofing) DNS 欺騙(DNS Spoofing)
偽裝行為	代理伺服器(Proxy Server)、Tor Network 虛擬私有網路通道(VPN Tunneling)
劫持行為	會話劫持(Session Hijacking) 、 Cookie 欺騙 (Cookie Hijacking)

資料來源: 本研究整理

一、 IP 追查技術與 IP 欺騙之追查與防禦

網際網路隱匿與竄改身分行為追查與防制技術上，就是要找出網路犯罪者的真實身分。本節主要探討網際網路隱匿與竄改身分行為態樣防制方法，亦即找出網路犯罪者所使用的 IP 位址，進而找出網路犯罪者真實身分，在開始探討行為態樣防制技術之前，讓我們先探討該如何查詢判定連線 IP 的擁有者之方法。

當我們已經取得 IP 位址後，可透過 WHOIS 服務來協助查詢所屬的擁有者，WHOIS 服務主要用意為協助網路管路人員保持網路的穩定性、安全性及排除網路問題所用，便於協調各相關之網路管理人員，相互合作以達到其目標，國際的 IP 由 NIC 管理，國內由 TWNIC 管理；可到下列網站查詢各段 IP 分配給何單位：

(一) TWNIC 查詢 http://www.whois.twnic.net.tw。

(二) 由 WHOIS 資料庫查 IP，http://whois.mintac.net/b5/。

(三) IPNetInfo 反查工具，使用者能夠透過它所提供功能來查詢某一個 IP 位址的擁有者，使用者只需要輸入 IP 位址，程式就會自動連結到網路上的資料庫去查詢該 IP 位址的擁有者、電話、FAX 號碼、電子郵件等資訊。

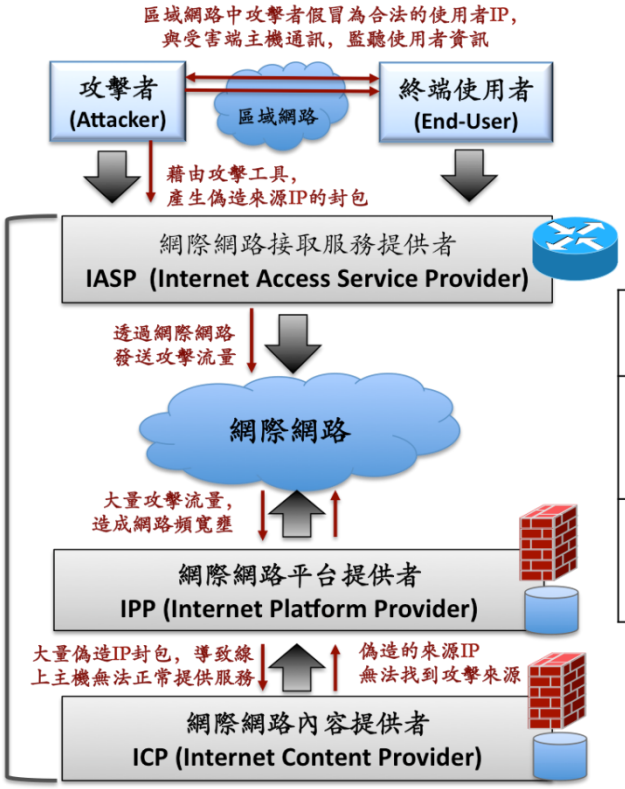
很多時候當執法單位找到網路犯罪者之犯罪歷程時，透過 WHOIS 系統去做查詢，大部分可以發現 IP 所屬的管理者是 IASP 業者，這時要再詳細的知道犯罪者的資料，必須尋求 IASP 幫助找出犯罪者真實身分。

網路攻擊者為了隱藏自己的行蹤與身分進行非法活動，則會運用 IP 欺騙技術來假冒 IP，導致受害主機無法成功的進行反追蹤，駭客常將 DDoS 結合 IP 欺騙，產生大量攻擊流量，癱瘓受害主機，使之無法正常提供服務，也無法追查其來源。圖 4-4 為 IP 欺騙攻擊與防禦說明，IP 欺騙若是發生在區域網路中時，其最主要之目的為假冒區域網路中合法使用者，監聽區域網路中其他使用者的資訊。若是 IP 欺騙結合 DDoS 攻擊發生在網際網路中時，大量的攻擊流量將會造成網路設備無法負荷，造成網路頻寬壅塞，使得服務主機無法正常提供服務，受害端也因為攻擊來源位址是偽造的，因此無法成功找出攻擊位址，加以定罪。

為了降低 IP 欺騙所造成的威脅，就 IASP、IPP、ICP 分別提供下列防禦建議措施:

(一) IASP 可採行邊界路由器入口過濾(Ingress Filtering)機制來減緩 IP 欺騙所造成的影響。IASP 的邊界路由器為網際網路的進出口，當接收到從其他邊界路由器所發出的攻擊時，如：駭客從日本主機對我國進行 IP 欺騙，則可利用入口過濾機制來進行防禦。入口過濾(Ingress Filtering)是路由器上的一個功能，可以用來檢查進出的網路內容，若是邊界路由器收到從其他邊界路由器所來的流量時，可先進行 IP 的檢查，若是發現來源位址是受到管制來源的情況下，則可進行阻擋，否則則直接往下傳送，邊界路由器入口過濾機制可視為防禦的第一道防線，以阻擋假冒 IP 的流量。然而，入口過濾機制需要購買昂貴的高階路由設備，造成實現上的困難度。再者，路由器上的紀錄保存也提供了攻擊來源追查的其中一個管道，IP 欺騙在追查上並無有效之攻擊來源追蹤方法，唯有透過不同國家不同 IASP 的合作， 提供路由器的日誌紀錄，才有機會找到真正發動攻擊的來源位址。

(二) IPP 與 ICP 在 IP 欺騙的防制上，可採用下列三種建議措施，網路設備制定安全過濾規則、加強頻寬管理與即時告警、保存日誌攻擊資料。為避免 IP 欺騙流量造成網路壅塞影響到線上服務品質，可使用網路安全設備制定安全過濾規則，檢查來源 IP 位置的有效性，阻擋無效網路位置的連線；監控網路頻寬亦是另一個方法，當發現網路流量異於往常時，應主動發出警告，執行下一階段的安全政策；網路設備或是服務主機遭受到攻擊時，日誌紀錄都會存有相關的資訊，因此，藉由不同日誌的保存與分析也能夠讓我們關連、判斷攻擊 IP 欺騙的軌跡。



IASP	• 實行邊界路由器入口過濾機制（Ingress Filtering)
IPP	• 網路設備制定安全過濾 • 加強頻寬管理與即時告警 • 保存日誌攻擊資料
ICP	• 網路設備制定安全過濾 • 加強頻寬管理與即時告警 • 保存日誌攻擊資料

資料來源：本研究整理

圖 4-4 IP 欺騙攻擊流程與防禦建議

二、 ARP 欺騙之追查與防禦

ARP 欺騙對區域網路具有極大的威脅，因為當區域網路中某一台電腦遭受病毒感染時，中毒的電腦會在區域網路中進行 ARP 欺騙攻擊，發布偽造的 ARP 通訊，將區域網路中其他電腦或是路由器所有的通訊都轉向已中毒的電腦，已中毒的電腦將會有竊取

密碼、影響網路連線主機對應關係、攔截資料或加以側錄、...等許多非法行為。最新的 ARP 欺騙攻擊手法也會與惡意網頁結合，內部主機遭受 ARP 欺騙病毒感染後，將會修改受感染主機的 MAC，將受感染主機之 MAC 指向惡意網站，當其他主機要求與受感染主機連線時，將會被導向惡意網站，造成大規模感染，由此可知，ARP 欺騙將會對企業內部網路安全造成很大的影響。為了有效追查 ARP 欺騙的攻擊來源，建立完善的 IP/MAC 以及網路授權存取的對應表，將有助於當 ARP 欺騙發生時，有效追查攻擊來源，亦能幫助管理者檢視區域網路內，是否有發生未被授權主機存取區域網路之情形。

為了有效偵測防禦 ARP 欺騙攻擊，本研究提出建立 ARP 欺騙偵測與告警機制、提升網路設備安全性及檢測主機與網路設備之弱點等三項解決方案，分別說明如下，IASP、IPP 以及 ICP 都應正視 ARP 欺騙之問題，導入解決方案於現行架構之中：

(一) 建立 ARP 欺騙偵測與告警機制：區域網路管理者可利用 ARP 欺騙軟體監聽網路上之 ARP 回應與重要主機之 ARP Cache，如：Arpwatch、Wow! ARP Protector、XArp v2、ArpDefender 等。若偵測出 ARP Cache 有不正常變動時，即時通知網路管理者進行處理。此外，部分 ARP Spoofing 攻擊會製造出大量的 ACK/DATA 封包，管理者監控網路狀態過程中，也能夠偵測出 ARP Spoofing 攻擊行為。

(二) 提升網路設備安全性：採用 DHCP Snooping 建立區域網路上服務伺服器與合法主機的 IP/MAC 對應表，如：網路閘道口(Gateway)、WWW 伺服器、Mail 伺服器等，並開啟網路設備路由交換器之 Dynamic ARP Inspection 功能，紀錄與檢視合法的 IP/MAC 對應表，避免 ARP Spoofing 病毒修改 IP/MAC 對應表，即時偵測並攔截區域網路中 ARP 欺騙之惡意攻擊行為。許多網路設備中都已實現此種安全機制。

(三) 檢測主機與網路設備之弱點：大規模 ARP 欺騙的發生常來自於區域網路主機遭受惡意程式感染所致，檢測並修補區域網路中系統主機與網路設備之弱點，將有助於防禦 ARP Spoofing 之發生。

三、 DNS 欺騙之追查與防禦

隨著網路服務與電子商務的快速發展，在網路族群透過打開瀏覽器輸入網址連上網站的同時，網域名稱伺服器(DNS)正在為我

們提供網址轉換的基本服務，最常用方式是將網際網路之網域名稱(Domain name)對應到實際的網路位址(IP)。然而，DNS 通訊協定並未進行加密或是身分認證，因此攻擊者可以假造或是更改 DNS 回應，造成所傳遞的資訊常常發生被竄改、惡意欺騙...等資訊安全事件，例如：DNS 欺騙竄改 DNS 網域名稱查詢的結果，傳回假冒的網路位址給使用者，使用者在沒有辦法判斷真假的情況下，連線到假冒的網站造成嚴重的損失；或是一進入其網站首頁或網站中的不特定連結，均會被攔截轉址到某特定的惡意網站。

DNS 伺服器設計上是採用分散式資料庫的方式及主從式(Client-Server)架構，控管網路重要資訊，因而延伸出與授權網域註冊中心網域資料同步化、網域資料更新、轄區傳送...等問題，再加上軟體設計可能存在的缺失，這些是防護 DNS 安全正常運作所需注重的重點。IASP 為提供使用者進行網域名稱之查詢會架設 DNS 伺服器。但對 IASP 而言，在確保 DNS 伺服器正常運作無誤外，亦需強化 DNS 主機的安全性，確認網域名稱資料的正確性，避免 DNS 被攻擊者當成攻擊的利器。追查 DNS 欺騙攻擊來源可透過檢查 DNS 系統服務日誌紀錄，判斷是否有異常事件發生，日誌紀錄包含查詢來源、查詢的網域名稱、查詢結果、DNS 系統登入存取紀錄、DNS 服務相關的訊息等。

IASP 在防禦 DNS 欺騙攻擊上，可透過 DNS 服務安全檢測與 DNSSEC(DNS Security Extensions)安全驗證來達成。DNS 安全檢測重點包括不良委任關係(Lame Server)、授權錯誤(Delegation Error)、DNS 容錯能力、轄區傳送(Zone Transfer)與 DNS 版本弱點修補等五項。有效之安全檢測技術，可避免因 DNS 系統設定錯誤而影響網域查詢效能、洩漏網域資訊及為駭客大開方便之門。至於 DNSSEC(DNS Security Extension)技術，則為另一有效防禦措施。DNSSEC 主要是增強 DNS 服務的驗證，在 DNS 主機之間彼此資料傳遞時，利用數位簽章來驗證 DNS 來源與訊息內容的可信度。透過密碼學的技術，對於相互通訊的 DNS 主機間，利用單向雜湊函數(One-way Hash Function)檢視訊息內容並產生一組雜湊值，接收端將數位簽章解密，再利用雜湊值驗證訊息是否遭受竄改。DNSSEC 藉由數位簽章的簽署與驗證過程，確保 DNS 網域名稱解析的真實性與完整性，是目前公認為防止 DNS 攻擊與降低假冒詐欺安全風險的最有效方式。雖然 DNSSEC 已獲得各領域專家學者的支持，網路設備廠商也都積極投入 DNSSEC 之研發，也被定義為下一代 DNS 服務的必要規範，預計在未來十年之內取代現有的 DNS 系統架構，但對於 DNSSEC 的推廣與布署，仍存有許多瓶頸尚待克服，其令人望之卻步的兩個主要原因為，DNSSEC 將會影響服務效能以及設定維護上之困難度。

資料來源：本研究整理

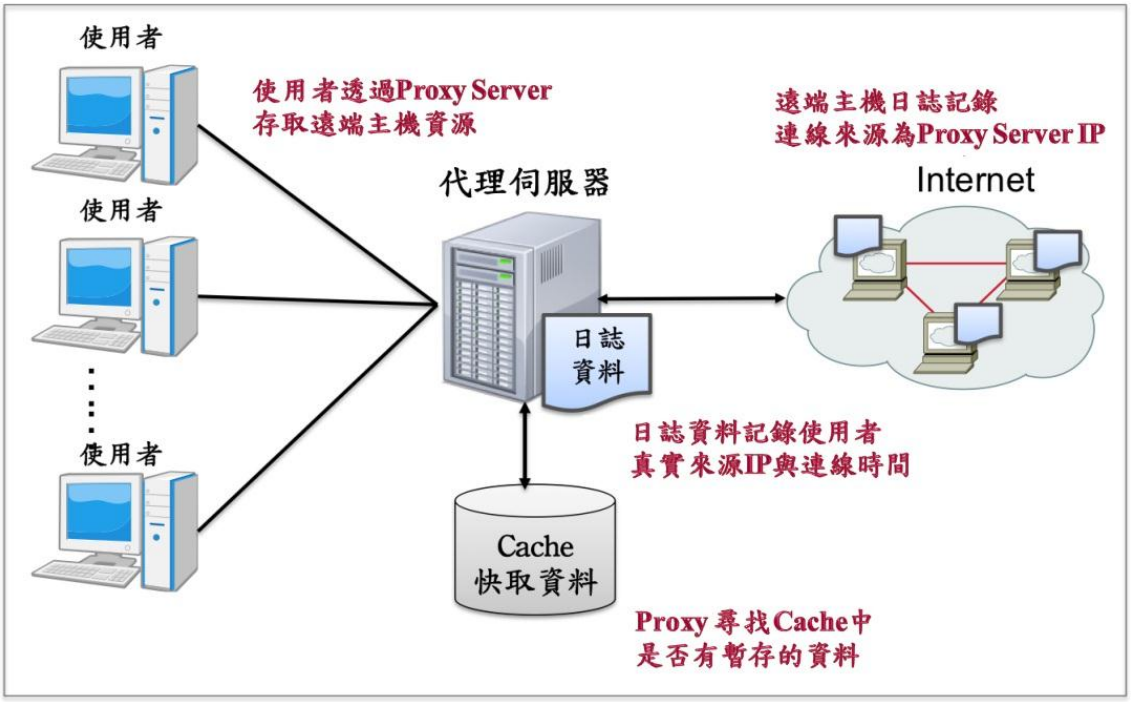
圖 4-5 DNSSEC 示意圖

ICP 與 IPP 也會架設經過合法授權之 DNS 伺服器，提供網路主機使用，在經費、現行架構與人力維護技術充足的條件下，採用 DNSSEC 防禦是一個最佳的選擇。IPP 與 ICP 在防禦 DNS Spoofing 上，亦需對 DNS 服務完成安全檢測，其檢測重點如上所述包含不良委任關係(Lame Server)、授權錯誤(Delegation Error)、DNS 容錯能力、轄區傳送(Zone Transfer)與 DNS 版本弱點修補。此外，在重要服務主機上，建立具名的網域名稱與網路位址配對存取控制清單(ACLs)，並於出現本機無法解析到網域名稱查詢時，將查詢轉送到特定的代詢伺服器，如：IASP 所提供可信任的 DNS 伺服器，也有助於避免遭受 DNS Spoofing 之危害。至於一般使用者之家用電腦，亦需常常注意本機的網域名稱與網路位址配對存取控制清單，是否有被惡意程式修改成將特定網域名稱對應到惡意伺服器之情形。

四、 代理伺服器服務(Proxy Sever)之追查與防禦

代理伺服器(Proxy Server)是一種網路服務，原先是因為要節省對外頻寬所設計，各家 IASP、機關、較具規模公司或是大專院校都會提供代理伺服器服務。代理伺服器會將使用者連線網站的網頁內容暫存在代理伺服器硬碟中，所以當有用戶透過代理伺服器上網時，代理伺服器會先檢視硬碟當中是否有暫存網頁的資料，若是硬碟中存有暫存網頁的資料時，代理伺服器就會送出硬碟中的暫存網頁資料，而非真正的連線到遠端網站中；若是硬碟中沒有網頁資料時或是資料已經過期，代理伺服器才會真正連上遠端網頁取得資料，回傳一份給使用者，另外留一份在代理伺服器硬碟上。當使用者使用代理伺服器服務且需連線到遠端主機時，是由代理伺服器連線到網際網路網站，由此可知，該網站所記錄連線者之 IP 位址是代理伺服器的位址，而非使用者電腦 IP

的位址。有心人士可以利用上述代理伺服器的特性，達到隱藏 IP 的效果。另外，當使用者在沒有使用加密連線下，透過代理伺服器連上網路時，使用者瀏覽網頁的歷程、使用者真實連線 IP 與時間，以及曾經輸入的帳號密碼等，皆會儲存在代理伺服器上，所以代理伺服器也是駭客獲取攻擊資源的目標。下圖 4-6 為代理伺服器運作說明。

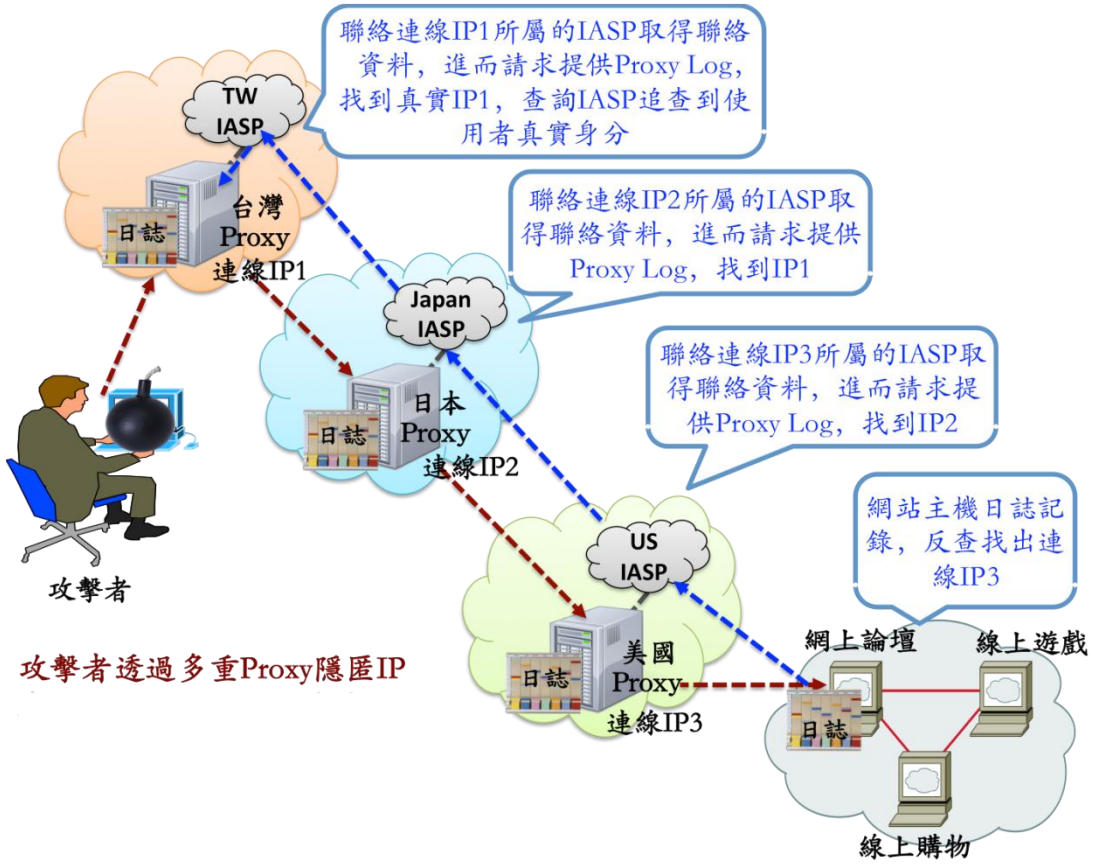


資料來源：本研究整理

圖 4-6 代理伺服器運作說明

目前有很多的免費代理伺服器可供使用者使用，這些代理伺服器有些位於國內，但大多數位於世界各地。當需要追查犯罪者的真實身分時，必須回溯追查犯罪者的網路連線歷程，透過與代理伺服器服務業者進行聯繫，以類似調閱通聯紀錄之手法，取得代理伺服器的日誌紀錄，將得知犯罪者的連線 IP 與時間，進而追查到提供犯罪者網際網路接取服務之業者，找出犯罪者的真實身分。圖 4-7 為代理伺服器身分追查說明，追查日誌紀錄可找出具犯罪情事之 IP 位址，利用 WHOIS 技術，可查詢出一個域名或是一個網際網路 IP 位址的擁有者資訊與聯絡方式，當相關 IP 經追蹤辨識後，判定為代理伺服器時，當代理伺服器位於國內，犯罪偵辦單位可請求該代理伺服器業者提供日誌紀錄，以便進行更詳盡之網路歷程追查；若該代理伺服器是位於國外時，則除了可發信

請求國外代理伺服器提供日誌紀錄外，尚可以請我國電腦網路危機處理暨協調中心(TWCERT/CC)協助與國外電腦網路危機處理暨協調中心聯繫(CERT/CC)，請求其協助犯罪歷程的調查。電腦網路危機處理暨協調中心主要負責安全事件相關通報與處理，也是國際上深獲信任且承認的安全組織。代理伺服器服務所造成身分隱匿問題必須藉由連線紀錄逐步追查，因此 IASP、IPP 與 ICP 業者若是有提供代理伺服器服務時必須保存伺服器日誌紀錄，提供犯罪事實偵查之用。



資料來源：本研究整理

圖 4-7 代理伺服器身分追查說明

五、 VPN 通道(Tunneling)之追查與防禦

隨著網際網路的普及與全球化趨勢的影響下，網路無國界已不再是一個口號，企業組織也分佈在全球各地，建立一個具有加密保護之安全通道，讓合法使用者遠端存取企業內部資料，已成為重要的課題。VPN 通道可提供安全且專屬之通訊連結網路通

道，採用非實體之暫時性連線，具合法授權之使用者可透過此安全通道存取企業內部網路。

當使用者透過 VPN 通道連接到公眾網路上的網路服務時，如：論壇發表文章、網路銀行轉帳等，支援這些網路服務的主機設備，必定會有日誌紀錄功能，日誌中所記錄的連線來源並非是使用者真正的網路位置，而是 VPN 主機的網路位址，當有犯罪事實發生時，網路服務業者需反查出使用者真實身分時，透過日誌紀錄能夠得知使用者所使用的連線 IP、連線時間、網上服務登入資料...等資訊，將日誌資料中連線來源位址，也就是 VPN 主機 IP，透過 WHOIS 查詢得知連線 IP 的所屬管理單位，管理單位必定有 VPN 帳號使用者真實身分資料，成功的追查出使用者真實身分。

比較代理伺服器服務與 VPN 服務兩者間的差異性，使用者使用代理伺服器服務並不需要經過身分認證與授權，而使用 VPN 服務則先取得授權後，才能夠透過帳號與密碼使用服務；再者，代理伺服器服務大多不是採用安全傳輸，因此代理伺服器端可收集到使用者資料，易造成隱私安全上的問題，VPN 通道多有安全加密傳輸機制，如: SSL VPN，可確保使用者在傳輸上的資料的安全隱私性。

相較於網際網路上眾多的 Proxy 服務，免費的 VPN 服務相對來說是比較少的，如：UltraVPN、AlonVPN、PacketiX、ProXPN...等免費 VPN 服務，使用者仍須到 VPN 網站，填寫個人資料註冊取得帳號後才能使用，使用者註冊時所填寫的使用者身分資料的真實性將會影響到身分追蹤的成效。而在企業組織內部所提供的 VPN Tunneling 服務，因為有合法有效的身分授權，相對來說將會對身分追蹤判定有所助益。

六、 會話劫持(Session hijacking)之防護

會話劫持為網路犯罪者結合了竊聽和欺騙的手段來達到目的身分假冒與資料竊取的目的。會話所指的是兩台主機之間的一次通訊，網路犯罪者將會在使用者與遠端網站主機通訊時，中途攔截具有使用者身分資料辨識的 Session ID，之後藉由挾持 Session ID 與修改連線資訊，達成冒用使用者身分進入遠端網站竊取資訊。會話劫持攻擊分為兩種形式：(1)被動劫持，網路犯罪者在使用者與遠端主機之間監視兩方的通訊，從中監聽竊取資訊，(2)主動劫持，停止使用者端對遠端主機網站的連線，網路犯罪者利用所竊取的 Session ID 取而代之與遠端主機進行會話連線，冒充使

用者的身分取得網站使用者的重要資料，如：金融交易資料，進一步從事危害使用者的行為 。

預防會話劫持的因應對策包括了下列兩種:

1. 建立身分認證與會話加密機制：會話劫持起因為 Session ID 被駭客所劫持，而網路犯罪的掌握了 Session ID 後，為何可以為所欲為？最主要的原因在於 Session ID 中夾帶了使用者帳戶與密碼資訊，因此，對於敏感的會話通訊，選用一個有密碼認證功能的工具，把整個通訊內容加密，可防範會話劫持的發生，如：Secure Shell (SSH)、SSL VPN，HTTPS 替代 HTTP。
2. 教育使用者基本安全觀念：使用者經常因為不良使用習慣，讓網路犯罪者有機可趁，造成損失，因此，購買昂貴的資訊安全設備，不如落實使用者的基本安全觀念，如：調整網頁瀏覽器安全設定、禁止以非加密通道存取公眾電子信箱、加強密碼強度..等。

七、 Cookie 劫持(Cookie hijacking)之防護

Cookie 是一種儲存在使用者端的資訊，用來讓 Web Server 能夠追蹤使用者資訊，如使用者帳號、密碼等紀錄，如果在網上傳遞，通常使用的是 MD5 方法加密，經由加密處理後的訊息為一串無意義的字母與數字；Cookie 在商業網站上的功用，綜觀來說包含 (1) 追蹤和管理使用者狀態、喜好設定、業務資料及用戶提供的其他資料，(2) 出於安全目的，(3) 以不記名方式理解使用者在網站上的使用情況以及 (4) 評估某些廣告措施的有效性。通常 Cookie 有兩種類型，分為 Persistent Cookie 與 Session Cookie。Persistent Cookie 可以設定存在 Browser 一段時間，亦即明確指定 Cookie 的有效時間，如果設定時間夠長，即便 Browser 關閉後或是重開機依然還是會存在；Session Cookie 只存在於連線狀態下，當過了 Timeout 時間或是瀏覽器關閉，其 Cookie 資訊就會被消失。

如同會話劫持一般，網路犯罪者可以利用當前網路上一些用戶管理系統將用戶登錄信息儲存在 Cookies 中這一不安全的做法進行攻擊，一般的 Cookies 用戶系統至少會在 Cookies 中儲存用戶名與用戶等級兩個變量，Cookie 欺騙也就是截獲 Cookie 的人不需要知道這些字串的含義，當瀏覽器每次造訪頁面時都會把 Cookies 傳輸過去，而包含密碼的 Cookies 一旦被他人獲取並向伺服器提交，通過驗證後，就可以冒充受害人的身分登錄網站。

防範 Cookie 劫持上，我們提出了三大類的防護方法：

(一)、 良好網路使用習慣的教育：Cookie 中記錄重要的個人資料，為了避免因為系統遭受 Cookie 劫持，應隨手刪除電腦裡的 Cookie 紀錄，重要帳號與密碼避免儲存在 Cookie 當中，注意系統的安全性，安裝系統修補程式。

(二)、 規範網站的隱私權政策：當使用者連上網站時，應注意並詳讀每個網站的隱私權政策，尤其是 Cookie 所蒐集的使用者資訊用途，以避免個人資料被濫用。

(三)、 使用電子簽章發送電子郵件: 使用者電腦中的 Cookie 遭受到網路犯罪者劫持後，常會被網路犯罪者利用的方式是登入電子郵件帳號，亂發廣告信，有鑑於此，個人電子郵件應採用電子簽章簽署，以確認電子郵件的正確性、完整性與有效性。

第三節　隱匿與竄改身分防制方法分析與建議

網際網路隱匿與竄改身分行為非常多樣，防制方法主要可以分成預防與追查兩大方向。預防方法主要在於確認使用者或設備本身的身分，並確保設備及網路連線安全性；追查部分主要在於保留連線紀錄，以便必要時能夠檢查分析。綜合以上所得，網際網路隱匿與竄改身分行為態樣與防制方法歸納如表 4-3。

表 4-3 網際網路隱匿與竄改身分行為態樣與防制方法

面向	行為分類	攻擊態樣	防制方法
非技術面	偽冒身分行為	竊取帳號密碼 使用無線溢波上網	保存網際網路連線使用紀錄(追查) 使用安全連線傳輸帳號密碼(預防) 使用安全無線網路傳輸協定(預防) 使用憑證身分認證技術(預防)
	合法掩飾非法		
技術面	欺騙行為	IP 欺騙	網路設備制定安全過濾規則(預防) 加強頻寬管理與即時告警(預防)

面向	行為分類	攻擊態樣	防制方法
			保存日誌攻擊資料(追查)
		ARP 欺騙	建立偵測與告警機制(預防) 提升網路設備安全性(預防) 檢測主機與網路設備之弱點(預防)
		DNS 欺騙	DNS 服務安全檢測(預防) DNSSEC 安全驗證(預防) 建立安全代詢伺服器名單(預防)
	偽裝行為	代理伺服器 虛擬私有網路通道	反查使用 proxy 之 IP 來源(預防) 使用者帳號認證(追查)
	劫持行為	會話劫持	建立身分認證與會話加密機制(預防) 教育使用者基本安全觀念(預防)
		Cookie 欺騙	良好網路使用習慣的教育(預防) 規範網站的隱私權政策(預防) 使用電子簽章發送電子郵件(預防)

資料來源: 本研究整理

許多網路產品支援安全功能，但大多數使用者為求方便，卻使安全功能失去其原有功用。在安全防制上，我們提出以下建議：

一、 加強教育，建立民眾基本安全觀念

一般民眾為求方便，都存在著「只要網路可以通就好了」，並未考慮到安全的問題。要建立起民眾的安全觀念，應宣導網際網路若未經嚴格管控會讓犯罪者有機可乘的觀念，讓民眾養成開啟相關安全機制的習慣，以防止上網服務遭盜用的情形發生。

二、 推行憑證的運用於網際網路的認證程序上

現行網際網路的認證方式，多以設定帳號與密碼的方式來完成，但已被證實可透過封包監聽以及暴力攻擊等手法來加以破解，甚至在網路上已有公開的工具，可讓人輕鬆破解存在於 Cookie 的帳號密碼。若業者提供服務時能夠結合電子憑證的身分認證方式，必能大幅降低網際網路服務遭盜用所衍生出的犯罪問題，追查上也較為容易。

三、 使用安全的無線網路資料傳輸安全加密機制

使用通道加密(如：WEP、WPA、WPA2 等)或資料加密(如：AES、DES 等)等技術，才是解決無線網路傳輸可能造成重要資料遭竊取的根本之道。

四、 與網際網路業者協調，嚴格審查使用者身分的真實性

隨著行動電信業者推展手機上網服務，期望行動電信業者能夠嚴格審查使用者身分後再行提供服務。目前，要成為行動通信業者之用戶，必需使用雙證件才能登錄成為用戶，相當於實名制，在此所謂的嚴格審查議題，即是需要業者對於辦理相關服務時，需仔細核對與審查用戶之身分與證件。不要等到通傳會進行行政檢查時，或發生犯罪情況時調閱資料才發現用戶登錄時有問題，導致犯罪追查無法進行。

第五章　座談會及訪談專家意見整理

在本研究中，為了解專家學者對於此一議題在法律領域、科技領域之看法與意見，我們舉辦一場專家座談會與訪談 9 位專家學者。本章說明訪談設計及方法，並綜整專家學者意見。

第一節　專家座談會說明

一、 專家座談會之設計

本研究所舉辦專家座談會，主要是採用焦點團體座談的方法，對於特定受訪者以小團體方式，進行主題聚焦討論與凝聚共識為目的。由研究團隊成員依據已設計的議題，引導參與者說出其對於隱匿身分與竄改身分相關問題的看法並進行討論，以提出相關意見、建議與解決方法。因此，焦點團體座談的內容及進行方式如下：

(一) 舉辦焦點團體座談邀請北中部地區五位專家學者參與，針對設定議題進行討論，以利本研究提出相關防制隱匿身分與竄改身分所造成網路犯罪之可行性建議與規範。（此次座談未邀請南部專家學者北上，主因是考量經費有限，為彌補此問題，本研究之專家訪談以南部專家學者為主，來瞭解其相關意見與建議。)

(二) 本次專家座談時間為 99 年 12 月 24 日(五)下午 02:00 ~ 03:30，於行政院國家資通安全會報技術服務中心富陽辦公室 2 樓大會議室舉行。受訪專家學者包括公共政策與資訊技術專長之學者與業界專家。

此次專家座談會議之議題，主要有兩大議題，一是討論有關隱匿身分與竄改身分相關網路犯罪行為之主要主管機關與相關法規；二是瞭解我國實施如韓國之網路「實名制」之可能性，相關議題分述如下。

(一) 就隱匿與竄改身分角度來看，網路犯罪行為與一般犯罪行為在偵辦上有何差異？依這個角度來看，在網際網路隱匿與竄改身分犯罪行為，對於政府各部門分工有何建議？相關法規應該朝向那個方向修改？

(二) 依照目前社會現況包括在網路上各式各樣之行為，如網路論壇、網路遊戲、電子交易、電子化政府等行為，如何在網路“實名制”、“匿名性”及“言論自由”取得一個平衡點？

二、 專家座談會之相關意見與建議

根據所設定之議題，參與專家學者對於隱匿身分與竄改身分相關網路犯罪行為，提出相關意見與建議，分述如下：

(一) 網路犯罪牽涉範圍廣泛，難以由單獨機關負責

由於網路犯罪牽涉範圍廣泛，難以由單一機關獨力負責，因為網路犯罪的技術在網路上並不特別，只是在制度上的偵辦程序與執行面困難些，尤其在網路上發生的犯罪行為，其偵測處理通常是跨越很多不同權責之部門。譬如說，一般民眾可能認為網路的部分就應該由通傳會做為主管機關，但實務上，倘若犯罪發生的層次是在金融方面，透過金融網路遂行之犯罪行為，則與金管會有關，應歸屬金管會之業務管轄，又如一般網路網路交易之商業行為，則由經濟部商業司所管轄。因此在廣泛使用網路的情況下，變成發生犯罪的行為的場所雖然是在網路的虛擬社會中，但仍應依據現實社會中該行為所違法令之原主管機關負責（例如現實社會中，販賣槍枝由內政部《警政署》主管，則發生有利用網際網路進行槍枝販售之不違行為時，仍應由內政部負責查處）。此外處理網路犯罪行為仍與現實社會一樣，可能發生在橫跨多個政府主管部門之情況，除了負責偵察的司法部門(可能為內政部警政署亦可能為法務部調查局等執法/司法部門)外，更多時候，在犯罪的預防需要政府的主管部門訂定相關的規範，來協助網路犯罪的預防及偵查。再者由於現行的通報制度，通報資訊只止於主管之機關，在相關通報資訊交換不暢之情況下，跨部門偵辦網路犯罪變得更困難。

(二) 犯罪行為的偵辦上，檢調、警政還是主要的負責單位

目前我國在政府機關為解決網路犯罪負責權責，已有相關的規定，政府在 2001 年就已經成立行政院「國家資通安全會報」，是行政院層級的一個跨部會部門，主要由政府各部會參與，譬如像法務部、經濟部（商業司）、研考會等。研考會主要負責的是政府體系相關機關的資安事件通報和應變，有關資安事件由技服中心協助處理。目前研考會已經要求所有的政府機關都要有兩個以上的資安聯絡人，政府機關的內部網路發生資安事件，由該機關先行處理，如果沒有辦法處理，再透過技服中心協助。如果入侵的電腦來自民間單位，可以透過會報的機制，也可由法務部調查局和刑事警察局處理(皆為國家資通安全會報成員)。

在網路犯罪行為的偵辦上，檢調、警政還是主要的負責單位，因其為執法單位，當犯罪發生時，責無旁貸。但偵辦的過程中，對於網路犯罪行為的追查，並非如偵辦一般的犯罪一樣，僅需單純的透過事後採證即可進行。由於網路的特性使然，若沒有足夠的事前保護措施，如紀錄機制等，網路犯罪追查將變得相當的困難。

(三) 犯罪偵辦執行面的之問題與政府各部門分工建議

網路犯罪無法偵破並不一定是技術上無法解決所造成，反而有些是整個結構性的問題，其實調查網路犯罪跟調查一般犯罪一樣，都是要靠犯罪時所留下的痕跡加以追查。現在已經解決網路犯罪偵查的技術問題，即以法令加以規範網路設備和服務的紀錄保存機制。譬如民眾利用網路銀行進行轉帳等金流作業時，該銀行負有保留相關網路交易紀錄之義務。而通傳會是主管網路接取服務的機關，便須規範 IASP 業者必須要存有紀錄的機制，目前第二類電信事業管理規則在這部分有詳細規範，其相關 IP 核配紀錄亦可協助提供治安機關偵辦相關網路犯罪時之間接證據。透過有效的紀錄管理機制與檢調、警政單位負責事後的偵查工作相互配合，可以有效地防範隱匿與竄改身分之網路犯罪行為。當網路犯罪發生在非政府機關時，如犯罪者使用跳板，且跨國網路犯罪，經過層層調查之後，發現犯罪行為者是在國外架設網站，則必需建立國際網路犯罪偵查合作機制。當然，網路不法行為有許多類型，且牽涉到眾多政府部門，相關部門必須重視網際網路這個被非常普遍使用的工具。

(四) 現有法規足以處理網路犯罪行為，但執行面的能力或標準仍不足

至於在制約網際網路隱匿和竄改身分所涉不法行為這方面，現有的法條是否足夠？如果從技術上來看，例如入侵他人的電腦，不論其目的是作為跳板再去攻擊他人，或者是竄改網路的封包這樣的行為，目前刑法對兩種犯罪行為已經足夠處理。與會的專家學者均認為現在的法律對於處理目前的網路犯罪問題是足夠的。

網際網路興起，造成人際交往與交易方式之改變，在過去設計法規時，並沒有考量到犯罪的工具。而如果網際網路這個工具需要被提到的話，在修法的過程中可以在某個條文上多加「網際網路」這四個字。同時，可依在偵辦過程中的便利性加以考量修法，如對紀錄檔的保存規定等。這些細則如要從不同的角度去做規範，恐有相當的難度，特別在跨部會合作時會有一定的障礙，

但如果各部會能達成共識，進行修法則不是很困難。如果從行政單位的角度，倘全面研究後認為有修法必要時，把這些法規放在一起然後整個送審，透過包裹的方式修法比較可行。

再則，如個資法對企業來說，最困難問題是舉證，目前企業不曉得個人資料保護需要做到怎樣的程度，害怕會需要投入大量的資金都還不夠，所以在法律方面制訂後，還需要主管機關給企業一個可依循的標準或者配套措施。譬如參照日本，訂定一個認定的標準或者是採用如 ISO 這種國際認證的方式。若主管機關設立或授權有一個驗證單位，並訂定類似高標、中標與低標之級距，根據企業的規模程度決定其需要達到的標準，像是金融、電信等特別產業就需要更高的要求。只要企業通經過驗證單位驗證通過後，就代表企業具有個人資料保護能力。

此外，與會資安業者也提出其看法，資訊安全在中國大陸視為國防產業，視同武器，希望我國可透過法規鼓勵國內資安廠商投注更多經費製作良好產品的依據。譬如以個資法來講，政府應要求相關行業之業者必須通過國家公測單位檢定，而這些公測單位必須是已被國家以更嚴謹的機制驗證過的，而資安業者則要取得此標章。如此政府就有依據及標準去要求廠商的個資保護機制需要達到甚麼樣的資安程度，同時，根據建立之資安分級，也可以將相關產業所需的安全程度進行分級，業者就可以知道投入多少錢可以做多少生意，如果要進入更高風險的就需要投入更多的錢，而資安產業的潛力是很大的，如果有一個主要的檢測標章，就有主要的參考方向。

(五) 實名制施行應依照實際應用情形決定

有關實名制之施行，應依應用上需要與否來決定，否則實名制到最後是懲罰守法的人，因為違法的人還是可以透過隱匿和竄改的方式去破壞實名制的作法，所以實名制應該依應用在甚麼地方來決定，且應該由政府和企業來決定是否實施之。同時，若是以應用、服務或交易等功能為主，要做到實名制，那就要確保實名制的安全強度是足夠的。譬如說網路銀行，只需要輸入帳號及密碼，像這樣的交易，確實牽涉到民眾重大權益，確實應該考慮實名制。在涉及到使用者重大權益時，確實需要實名的制度，然而在一般的使用上，則沒有必要去做強制性的規範。

(六) 可利用記名制來替代實名制

在討論使用實名制時，參與者反映出，在網路上除了匿名與實名，還有一種前虛後實的 ID 設計方法，稱為「記名制」。記名與實名之間有些許差異，「記名制」之 ID 與其本人個資間一對一

的真實程度，可依其 ID 賦予程序之嚴謹度不同而有所影響。所以設計上，當 ID 的取得比較容易時，該 ID 能夠使用的服務應是屬於低風險的。而當服務之風險提高時，前虛的虛（亦即使用之 ID）會趨近於實，甚至是需要去跟國家的 ROC ID、內政部 ID、護照 ID 有所對應，如果跨境的話，還需透過跨部門的協調，所以在 ID 的取得方面沒有著墨太多，反而是花很多時間在認證的機制上。而在記名制之技術上，對企業來說是以成本為考量，其嚴謹度將依成本為調整方向。但是如果企業是使用高強度之認證，而其在資訊科技上很弱，則其強認證就打很深的折扣。所以企業可就應用的環境和所處的環境風險程度，來建立記名制度，以利使用者 ID 之確認與保護。同時，還是要讓網路的自由保存著，才會有活潑性。

遊戲產業業者有提出一個想法，就是 Authentication Hub，這個 Hub 是由多家遊戲業者合力出資，請電信業者做身分認證，因為遊戲裡的 ID 雖然是虛擬的，但是卻是有價的，所以遊戲廠商提出 Authentication Hub 概念。除此，在與業界討論時他們也提供一個意見，即是 ID Provider 的概念。在政府的體制之下，用自然人憑證去 ID Provider 申請一個真實的身分，假設民眾要去銀行開一個網路帳戶，必須要有一個 ID，而這個 ID 就是向 ID Provider 取得，而且 Authentication 也是由這個 Provider 所提供，並不是由銀行去做，所以所有的 Authentication 的紀錄會保留在 ID Provider 那裏。如果某個 ID 發生犯罪要追查，就必須由法官依法請 ID Provider 提出證據，且這個證據是足夠的。而如果還有遺漏的話，則另需有保險來承擔損失，倘仍有損失，再由國家單位對這個風險負責，並把錢賠給因遭偽冒或被盜用的被害人。由政府主管機關或業界合作建立 ID Provider 之機制，也可說公正之第三者，以確立在網際網路身分確認之安全機制。

綜合上述相關建議，以利防制因隱匿身分與竄改身分所造成之網路犯罪行為，與會之專家學者仍建議現有政府單位及企業以個資保護為主，並期盼建立完備的制度面，更甚於法規之規範。

第二節　專家訪談說明

經文獻分析與比較各國政府有關隱匿身分與竄改身分相關網路犯罪之規定，本研究為實際瞭解我國在此方面相關法規之規範是否符合目前社會需求，再進一步進行專家訪談，以利瞭解我國在網際網路有關個人隱私、商業活動與網路犯罪三方面之現行相

關法規是否需考量進行修法，以符合民眾之期待與現行網路社會之需要。

一、 專家訪談方式

「專家深度訪談法」(In-Depth Interview)主要是採用較不具結構性的訪談方式，可說是一種非結構式訪談。在訪談的過程中，研究者無須按照預定的訪談結構和機械式提問問題，受訪者也無須按照問題做出回答，此一方式是研究者就某一主題與被研究者進行自由、深入的交談。專家深度訪談法主要在於瞭解受訪者對問題之態度、專業或價值觀。藉由訪談過程可以探詢到問題的核心，是一種透過雙向溝通方式，擷取個人較為內隱性知識的一種方法，如個人的經驗、觀念等，這類存在於腦海中的知識、實證知識、高級技能、私有知識，係經由長期工作所累積的經驗知識；換言之，專家深度訪談法主要著重於受訪者在某一個領域中的專業能力，其代表著一群具有特殊專業能力的專家團體。

在進行專家訪談過程，本研究設計訪談時間為 1 小時或 1 小時 30 分鐘，為有效掌握訪談時間，本研究提供一份訪談大綱。此訪談大綱設計目的主因一是讓研究者不要表現得像個無法勝任的與談者，須能夠清楚地表達自己訪談的主題；二是為了確保訪談不要失焦偏離主題；三是避免讓專家受訪者不要陷入即興敘述與主題不甚相關的個人見解或個人議題。訪談大綱是依據文獻分析與委託單位所提供之研究目標而設計，訪談問題皆與隱匿身分與竄改身分議題相關，分為全面性與法律面兩面向，分述如下：

二、 專家訪談問題

(一)、全面性議題：

主要目的在瞭解國內目前因隱匿身分與竄改身分所造成違法行為態樣，包括個人隱私、商業活動與網路犯罪三面向。由受訪者專業說明國內因隱匿身分與竄改身分相關整體問題，並瞭解在個人隱私、商業活動與網路犯罪三方面防制方式。本面向提問三個問題如下：

1. 從法治觀點，目前有那些行為態樣是國內社會因網際網路隱匿與竄改身分而形成之行為方式？最嚴重是何種行為態樣？

2. 請問有那些法規是用於因應這些網際網路隱匿與竄改身分之行為態樣?其防制效果如何？
3. 請問這些網際網路隱匿與竄改身分行為態樣之相關法規是否有一致性防制規範指標或相關判斷原則？

(二)、法律面向議題：

主要目的在瞭解國內目前對隱匿身分與竄改身分所造成違法行為態樣所做規範與相關法律，包括個人隱私、商業活動與網路犯罪三面向；並瞭解相關法規是否足以因應規範目前網路違法行為，以及瞭解目前法規是否需要修正，以利因應目前網路社會所需之法規。本面向提問四個問題如下：

1. 目前國內大多引用那種法規因應於防範網際網路隱匿與竄改身分之行為態樣？
2. 請問國內是否需有專屬於規範網際網路隱匿與竄改身分之行為態樣之特定法規？
3. 目前國內是否須修改網際網路隱匿與竄改身分行為態樣之相關法規？若是,請問應該朝向那個方向修改？修改標準為何？應該重視何項行為態樣？
4. 目前國外那個國家對網際網路隱匿與竄改身分之行為態樣相關法規最值得作為國內參考？為什麼?

二、 專家訪談樣本

本研究範圍因涉及政府制度、企業與法律三個面向，故在選取樣本時著重於此三方面的選擇，並且為顧及南部與北部的樣本數目平衡，選取 4 個位於南部的單位與 5 個位於北部的單位，總共訪談 9 個單位之專家學者，以利協助本研究目標之完成。受訪名單基於受訪者姓名與身分保密原則之規定，故以代號處理之，如表 5-1 所示。訪談時間從 99 年 11 月中旬至 100 年 01 月 07 日止，共訪談 9 次。

表 5-1 受訪者單位與受訪日期說明

訪談代號	服務單位	訪談時間
A-1	成功大學科技法律研究所(南部)	99 年 11 月 11 日
L-2	金石國際法律事務所(南部)	99 年 12 月 10 日
G-1	義守大學電算中心(南部)	99 年 11 月 30 日

訪談代號	服務單位	訪談時間
G-2	法務部資訊處(北部)	100 年 01 月 07 日
G-3	法務部調查局(北部)	100 年 01 月 07 日
P-1	資策會科技法律中心 (北部)	99 年 11 月 19 日
P-2	國家高速網路與計算中心(南部)	99 年 12 月 03 日
P-3	中華電信公司(南部)	99 年 12 月 11 日
P-4	中華電信公司(北部)	100 年 01 月 25 日

資料來源：本研究整理

三、 專家訪談意見與建議

本研究經過訪談 9 位專家學者，針對隱匿身分與竄改身分所造成相關網路犯罪行為態樣進行討論，訪談內容結果分析將從兩大類型討論：一是技術面；二是非技術面：就制度面與法律面提出相關意見與建議，分述如下：

(一) 技術面

在偵查因隱匿身分及竄改身分所造成之網路犯罪行為時，技術大多不會是問題或瓶頸。凡走過必留下痕跡，透過事後痕跡的追查，如紀錄（Log），大多能夠重建或釐清犯罪經過。但追查時可能出現的瓶頸有二：一為沒有適當的機制，能夠在事發時留下紀錄，作為後續犯罪追查之用。二為跨越國界時，沒有司法互助，無法取得事後的痕跡，這並非技術上能夠解決之問題。

基本上，電信業者所提供的網際網路服務，都可透過上網時間、來源及目地 IP 來反查犯罪來源，由於網際網路活動非常頻繁，業者保留網際網路連線使用紀錄明顯有成本考量。

具有電腦專業技術的犯罪者，透過修改來源端封包、在被害者電腦植入木馬操控或破解無線網路登入，來達到犯罪目的，此類行為不易追蹤。配合偵辦使用者犯罪動機，並解析網際網路連線使用紀錄，包括各類電腦及網際網路連線使用紀錄，可以追查來源。

現有相關防制方式是在重要交易時，透過電信網路(行動電話及市話)或個人認證輔助裝置(自然人憑證、IC 金融卡、OTP)來對網路交易行為再作進一步身分認證，所造成的問題為增加交易成本及使用上比較不方便。

(二) 非技術面

受訪專家學者之意見與建議，傾向於透過非技術面來解決網際網路匿名與隱匿身分所造成之問題。訪談之專家學者對於此部分依個人隱私、商業活動及網路犯罪等面向所提意見與相關建議之結果，分述如下：

1. 個人隱私部分

若單純看網際網路隱匿，一般常見的行為是利用網路上公開的 VPN 或 Proxy 主機，隱藏自己真正的 IP 後進行網路瀏覽行為；或是利用職務之便，如使用者本身就是學校某主機管理者，可使用學校主機當跳板，來隱藏自己的來源 IP 位置、隱藏真實之身分。當一般使用者利用此等方式進行正當的網頁瀏覽行為時，其實並無違法。因此，若僅單純透過公開的 Proxy 與 VPN 或是公共空間的 WiFi 無線網路，來進行網頁瀏覽、收發信件等行為，並未違反相關的法規或須擔負任何違法責任。

對竄改身分來說，比較嚴重的行為態樣是透過作業系統或軟體的漏洞，在對方未知的情形下，破解對方的網路與電腦，取得該電腦使用者或管理者身分之後，再利用對方的網路與電腦，進行網路攻擊或犯罪行為，這些行為會觸犯到刑法及其他相關法律。這些利用入侵他人網路或電腦，再進行他人個人資料散布等行為，將可能造成妨害秘密、名譽、通信秘密、侵害著作權及侵入他人電腦等行為，即有違反刑法、個人資料保護法、著作權法及商業秘密法或其他相關法律責任，舉例如下：

(1) 妨害秘密會觸犯刑法第 318 條之 1。

(2) 網路侮辱及誹謗等妨害名譽行為會觸犯刑法第 309 條至第 314 條。

(3) 分散式阻斷攻擊(DDoS) 會觸犯刑法第 352 條第 2 款之規定等。

(4) 若在未經他人許可之下，透過入侵方式侵入他人網路或電腦，就會觸犯刑法第 358 條--無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。

(5) 若對政府公務機關電腦進行入侵等犯罪行為則依刑法第 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。

(6) 竄改身分之冒用者可能觸犯個資法及刑法相關法條。

■ 個人資料保護法第 3 條：

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

a 查詢或請求閱覽。
b 請求製給複製本。
c 請求補充或更正。
d 請求停止蒐集、處理或利用。
e 請求刪除。

- 個人資料保護法第 5 條

  個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。當負責機關違反規定，致個人資料被竊取、洩漏、竄改依第 12 條應負起責任主動通知當事人。

- 刑法第 358 條

  無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。

- 刑法第 359 條

  無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

- 刑法第 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 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。

事實上，目前我國法律並未有直接針對隱匿與竄改身分定義之特定法規，既有法規僅就損害或侵害公眾或他人之行為進行定義，如：刑法第 360 條規定以電磁方式"干擾"他人電腦或其相關設備，致生損害於公眾或他人者，是有刑責的；並未定義在過程中所進行之隱匿或竄改身分之行為。依目前刑法第 358~360 條相關法條來說，「隱匿行為」本身並非犯罪，侵害他人電腦或利益之行為才是犯罪。

在我國對類似的網路匿名或竄改身分之攻擊手法進行偵查時，通常需要執法機關發函至該網段之註冊單位索取調閱相關資

料，經該單位網路管理人員的配合，協助執法人員經由相關的網路日誌(Log)找到真正的來源 IP，才有辦法查出相關的犯罪者。所以，犯罪偵察過程中，跨單位的合作與協調情形，將影響資料的取得與辦案的速度。

匿名身分的特色可讓網際網路服務呈現活潑多樣化，讓使用者能扮演不同角色，網際網路許多社群服務如同是個人內心世界的交流溝通，若只考慮少數人的犯罪問題，而將大多數人所享用之匿名方式取消，將嚴重打擊網際網路感性的一面。所以屬於服務社群交流者採用自由心證方式來認證，這方面有賴網友與業者自律。但屬於理性實務的服務，如拍賣、金融交易、公司管理網站等服務，如有犯罪問題發生，將造成經濟財產損失，故需要較嚴謹的認證程序來確認身分，確認身分的相關資訊有賴個人資料保護法規範保護個人隱私。

2. 商業活動部分

站在網際服務提供者立場，為維持合法的網際網路環境，除使用者與 ISP 自律之外，仍需相關法令的配合執行，德國的通訊服務法即對網站的經營者訂有相關處罰的規範，如進入一個網站，把對他人侮辱性的言論貼到網站上面，該網站業者是要為這個言論負責的，德國政府賦予網站業者相關義務，但沒有對匿名行為做規範。依目前法規，以下幾項問題是國內業者困擾之處，分述如下。

(1) 主動過濾非法行為及內容是業者自律的表現，但「主動」一詞所帶來的人力及設備成本也是屬於業者之服務成本;故往往造成業者無法得知須付出多少成本才夠負擔此「主動自律」行為之義務。
(2) 若是其網站發生非法事件，要立即作刪除還是向權責機關舉報，現行法令無較明確的分界。業者擔心若主動舉報給主管機關，是否將違反個人資料保密原則。
(3) 配合法令儲存週期(大部分為 6 個月)的儲存通信紀錄，其設備與維運人力將是業者之成本考量。
(4) 協助通訊監察所涉及的客戶隱私權問題。
(5) 協助搜索扣押所涉及的服務中斷問題。
(6) 協助作證之額外負擔。
(7) 防制技術可能涉及專利侵權問題。

現有防制方式可在重要交易時，透過電信網路(行動電話、市話)或個人認證輔助裝置(自然人憑證、IC 金融卡、OTP)來對網路交易行為再作進一步身分認證，而其所造成的困擾為增加交易成本與使用上的不便。目前國內在重大的電子商務交易方面，包括

股票買賣一定要求要用電子簽章，就由金管會要求買賣者使用電子簽章，由法律規定此類活動一定要留下使用者的行蹤，使用者不能夠隱匿身分，若不留的話就無法交易。由金管會訂定規定，故若有不法行為發生，發動偵辦作業時，即可從使用者行蹤這點著手。其實現在所有的法規為了避免發生箝制言論自由之虞，都是從要求相關業者留下使用者行蹤，再由相關單位追查到違法位置。故針對商業活動這個議題，建議從記錄行蹤下手。一般而言，如果談到隱匿身分，一定講言論自由；反之如果是討論竄改身分，因為其行為者有可能把其行蹤抹掉，甚至換到別的身分去栽贓嫁禍，所以採行措施應以方便追查使用者行蹤者較好。

當使用者要交易時，由行業的規範去要求業者一定要留下顧客的交易紀錄，如透過第二類電信事業管理規則要求電信業者所有的號碼都必須是真實的，而且不能夠繞話務；如此，有利於追查電話網路之違法行為。網路服務業者服務項目，如拍賣、金融交易、公司管理網站等，這些服務可能因為犯罪問題造成經濟財產損失，因此均需較嚴謹的認證程序來確認身分：

(1) 透過通訊裝置如行動電話或市話。
(2) 透過個人、金融認證裝置(自然人憑證、IC 金融卡)。
(3) 透過其他個人認證裝置(OTP)。
(4) 使用 SSL 加解密技術，避免傳輸過程中資料遭受攻擊或封包竊聽等問題。

也就是說，在商業活動部分，對於隱匿與竄改身分之問題，將視行業別而有所不同。對於商業、金融之交易，因其涉及金流，所以需要確認交易雙方之身分，故需採用身分驗證機制，來確認交易雙方。而交易雙方當然也可隱匿其身分，但需透過代理等方式取得另一身分，來進行交易，而此代理機制是有紀錄、可供追蹤的。對於在網際網路上提供服務而言，均透過網際網路連線服務提供商，因此，部分的連線紀錄是留存在網際網路連線服務提供商，但是其他平臺或內容之服務提供業者，倘若未實施實名制，則可能不知道其使用者的真實身分，而僅能記錄使用者所使用之代理身分。因此，在相關主管機關進行管理時，就須分別就各行業加以規範，使其業者能夠留存相關紀錄。也就是說當使用者要交易的時候，應由各該行業的法規或規範去要求業者，一定要留下交易的紀錄。

3. 網路犯罪部分

網路匿名行為，從法律制裁的角度來看，是否需針對這樣的行為做制裁、提出懲罰是一個很大的問題。通常就刑事法來看，

網路匿名行為只是一種現象而已，但透過這個現象可能會產生很多犯罪行為，譬如像是網路詐欺、散播猥褻資訊、侵害著作權等。實務上，現在對於不法行為之偵辦程序，通常是有侵害行為發生後，再由警方或是檢調單位進行所謂的偵查，如：追查 IP。等於是說，須先有侵害行為發生之情形，再追查幕後的主導者與共事者；但是匿名行為是使用者於侵害行為之前，先改掉自己的名字或是隱藏身分，既有法規是沒有明確定義與規範的。欲對匿名行為規範時，較適當之作法應是透過私人訂約的方式。換言之，網路服務業者會在其網站訂定相關約定事項，要求欲使用其網站的人，形式上要保證個人真實姓名。網路上常發生的違法行為如侵害著作權、公然侮辱，尤其在 PTT 更是常發生。但要在 PTT 限制每個網路使用者要提出他的真實姓名，不提出真實姓名要被處罰，在法律上不易站得住腳。

依外國法規資料，特別是德國，在網路犯罪部分亦沒有針對匿名行為做出規範，所以在比較法的立場上來看的話，目前找不到一個先例，在國內確實也沒有類似規定是針對匿名行為做處罰的。若匿名行為須規範，則政府須制定一個標準，即是在某一個特定動作或是特定場合，如雙方訂合約（民事諦約），此類必須確認對方身分行為之活動，不能有匿名的動作。從現在法理與法律來看，其實目前是可以做到的，國內不需要再透過一套法規來處理。

匿名行為是一個點，而匿名後造成的侵害事實上又是另外一個點，現在法律都是針對後面侵害事實做規範，若要管制前面這塊，法理上是有問題的，縱然這是一種很普遍的現象，但因匿名行為牽扯到言論自由。故若針對網路侵害行為，現今我國相關法規已足夠規範，不需一個專門的法規，因為這些犯罪行為事實上與傳統的犯罪行為雷同，只是使用工具不同，即利用網際網路進行犯罪，故實務上，目前並無新的犯罪態樣產生，所以不需修法或進一步制定新的法規來規範網路犯罪。除非有新的行為態樣產生，才有需要新的法規來規範新的行為，如電子簽章法，因為有網路簽章問題，這是過去沒有的行為態樣，因此政府須制訂新的法規規範此類行為。除此，匿名行為牽涉到資訊自由的問題或是網路犯罪的問題，法理上無法把每個上網的人都想像成一個潛在的犯罪者，因為上網可能只是查資料，若是規範使用者一定要據實陳報個人的真實身分，就好像把個人變成潛在犯人，在法治國家來說當然會有一些問題。因此，其解決方法不是針對匿名行為直接做規範，而是宜要求相關網路業者擔負應有之義務，如當某些業者的網站發生很多犯罪行為的時候，則該業者在刑法和行政法兩方面都會有責任。因為已有損害發生，故各該業者即具有刪

除掉違法言論與網頁的責任，主管機關可以加以監督與處罰，以刑法的基礎原理原則就可以解釋到這點。我國可以參照德國電信服務法第 9 條，對於網路提供者訂出一些行為規範，亦即當業者經營網頁的時候，必須對於自己經營的網頁負責。總之，依目前的整個發展，我國是沒有修法的問題，就刑法而言，因為刑事訴訟法已修改，例如可以針對有關之電磁紀錄進行扣押，其實這是修法上的一大躍進，以前根本沒有想到電磁紀錄，目前刑法已經賦予偵查人員一定的權限，如果執法人員具有完善技術能力，便可落實偵查網路犯罪行為。

目前影響面較大且較嚴重的網路犯罪態樣是「網路釣魚」，因為網路釣魚的手法一直在演變，技術上很難防，甚至法律上也很難防，如僵屍病毒（Botnet）用一大堆木馬程式，然後透過封包進行阻斷服務攻擊，全部指向一個 IP 進行攻擊，其實這在技術上是很難防的。因為網路釣魚會牽涉到後端的詐欺行為，當網路釣魚的受害者個資被竊取之後，永遠不知道其資料被拿去做什麼事。目前大概只能用刑法規範此類型網路犯罪態樣，換言之，妨害秘密或涉及竊取他人的資料，只要能夠證明犯罪事實，刑法就都可以處理，是沒有問題的。

除網路釣魚之犯罪行為，還有其他如利用偽造身分申請免費 EMAIL，再利用此 EMAIL 申請拍賣網站帳號，進行拍賣詐欺或販售非法軟體等，或利用偽造身分登入社群工具，對被害者發布有損名譽的言論，或入侵遊戲網站盜取虛擬寶物等不法行為，以及其他如散播猥褻物品、詐欺、公然侮辱、誹謗、便利窺視竊聽及散布竊聽內容（如偷拍影片之上傳）、洩漏營業秘密、散布兒童及青少年猥褻資訊、侵害著作權等網路犯罪行為。對這些網路犯罪行為通常是以刑法去處理，但囿於網路環境的關係，所以處理的效果其實是有限的，有限性不是說這個法本身訂得不周全，而是事後的偵查有困難性。

4. 相關建議

現今對於網際網路的觀念需要轉變，不可只是當作工具，也必須以策略為觀點。因為有策略概念之後，裡面就牽涉到管理、人、教育訓練。如果只是當作工具就會變得比較被動，這部分受訪的專家學者在制度面與法律面提出相關建議如下：

(一)、 制度面

1. 歐盟針對網路犯罪方面，整合各國檢舉及宣導網站，成立歐洲網路熱線提供協會與歐洲安全教育網站，此方式值得

國內參考。歐洲網路熱線提供協會，使用網路檢舉熱線，對於違法的使用和內容做出快速回應。

(1) 建立全球性的檢舉熱線。
(2) 交換資訊。
(3) 交換專業知識。
(4) 教育決策。
(5) 掌握網路犯罪之新趨勢及發展解決之道。
(6) 鼓勵將孩童電腦從臥房移至客廳，增加父母與子女互動機會。
(7) 與 ISP 業者保持連繫，尋求防護措施。

2. 歐洲安全教育網站提供教育及宣導資訊給一般民眾，使其瞭解網路的不當資訊。讓民眾可以瞭解如何安全地與有效地使用網路。家長可透過此網站來學習如何監督與追蹤不適合青少年的影像及資訊，提升對網路資訊警覺性及對違法內容的了解，並可立即向檢舉熱線回報。
3. 建議與其他國家建立犯罪偵查協定，協助處理跨國網路犯罪行為。
4. 從教育著手，規範學生須修讀「資訊科技與法律」相關課程，以利培養學生瞭解網路犯罪嚴重性與相關法規處罰。

(二)、 法律面

1. 如現行法規已明確界定那些行為是隱匿身分、藏匿身分與竄改身分之行為，則若有違反這些行為者就應依法處罰。如果現行法規沒有明確界定之隱匿身分、藏匿身分與竄改身分之行為，則這些行為是屬未命題，可以不用處理。如韓國與大陸推行實名制，規定某種網路行為須採用實名制。但縱使已立法明確界定那些行為是隱匿身分、藏匿身分與竄改身分之行為，但上開行為僅是屬於犯罪之過程，法律規範應以犯罪結果為管理之標的，故不建議由法規明確界定那些行為是隱匿身分、藏匿身分與竄改身分之行為。
2. 朝加強警察追查網路犯罪者可能性之方向修改法規，包括提供接取服務之電信業者或其他網路服務提供業者，由法規明訂配合追查之項目，因這是符合國家安全與公共利益的概念。
3. 美國憲法支持人民有匿名發言的權利，其最高法院認為匿名是避免受到多數暴政的盾牌，法律也規定行為只要不違反法律，允許人們以匿名方式交流互動。該國明確定義匿名的合法性，值得作為國內參考[7][12]。

4. 建立類似檔案法概念，規範網際網路服務提供者保留資料，並將資料分級，資料保留期限將依分級而有所不同，如根據業務性質訂立紀錄檔案分級，第一級需要保留 3 個月、第二級保留 6 個月、第三級就保留 1 年。

第三節　小結

綜整本研究訪談專家學者及舉辦座談會專家對於隱匿身分與竄改身分之行為態樣與防制技術等觀點分述如下：

- 隱匿身分與竄改身分行為，是兩種行為態樣，隱匿身分並不一定違反現有法令，因此法律宜規範所屬之犯罪行為。而竄改身分利用他人身分所遂行之行為，相對於「文書」之規範，會構成「偽造文書罪」。
- 我國現有法令，對於隱匿身分與竄改身分行為並無特別進行規範，而是透過因隱匿身分與竄改身分行為所遂行的犯罪結果進行處罰。接受本團隊訪談之法律專家或學者多數認為現有的法令，已足以規範透過隱匿身分與竄改身分行為所遂行的網路犯罪行為，不需要特別為「隱匿身分與竄改身分行為」製作專法或特別加註於法條中加以規範。僅有一位資訊技術專業的專家學者認為，須要於法條中特別加以規範，但本研究在分析與彙整相關學者專家意見後，認為現有法條規範的範圍較為廣泛，若特別加註，則將使得法條規範範圍限縮於特定範圍中，反恐不利於其他法益之保護，故未將此一意見作為研究結果產出參考。
- 隱匿身分與竄改身分所可能進行的行為，不論是正常或犯罪行為，在技術上均可能發展或找到對應的解決方案。但這個解決方案的可能成本高或需要國際上其他國家的配合。再者透過一項技術解決了一個問題，可能再衍生其它問題，因此，參與座談與訪談的專家學者均認為目前應朝透過法律宣導及管理制度，如偵查制度、網路犯罪破案考績制度、專業人力培訓制度等，避免因網路隱匿身分與竄改身分行為所造成的問題。
- 因為網路匿名所導致的問題，而欲採用「網路實名制」來解決此一議題。參與座談與訪談之專家學者則有兩項主要的觀點與主張。一為「網路實名制」將限制人民的自由，所以無論如何均不應採用，而可考慮如：「記名制」等技術或方式，透過公正第三方來進行類似實名制，但又不會直接侵害人民自由之方式。另一主張採用「網路實名制」在特定的

應用場景中是必須的，而且現在也具有相關規範並經執行，如：網路報稅，透過自然人憑證存取的系統等，因此維持現有之情況即可，不須再有新法或強制規範一定要使用「網路實名制」。

- 當透過隱匿身分與竄改身分所遂行的電腦與網路犯罪行為發生時，如何進行有效的追蹤是座談與訪談之專家學者較為關心的議題，由於網路本身所存在的特性，可透過網路位置及數位鑑識等技術來進行追查。但是犯罪偵查機關，如警方、檢調等單位所要面臨的，卻是跨國無法繼續往下追查及沒有留存適當紀錄或痕跡等困難，因此參與座談與訪談之專家學者建議短、中期可透過建立跨國合作之機制，與透過主管機關要求業者留存適當紀錄、改進現有偵查制度等作為，長期則透過社會倫理、教育來改善與解決此類問題，才是政府各部會面對此一情況應有之作為。

第六章　研提執行相關防制技術與機制之配套法規修訂建議

第一節　相關防制技術與機制之現況

根據研究與分析網際網路隱匿及竄改身分行為態樣，本研究發現由於網際網路特性使然，此類行為並不是絕對違反法令規範。犯罪者得以透過此類行為躲避追查。而一般使用者，也因為不了解其所需要償付的責任，而肆意的利用相關的技術，使自己遊走於法律的邊緣或灰色地帶。

「隱匿身分」行為，本即為網際網路的特性之一，在網際網路中，使用者間由於無法直接面對面，故需透過間接的方式來證明或確認彼此間的身分。但也因此一特性，許多的犯罪者透過「隱匿身分」行為來躲避犯罪後被追緝，獲取不法利益，如：透過網路入侵他人電腦竊取網路銀行密碼，盜取存款。甚至透過「隱匿身分」以規避在網路上應負擔的行為責任，如：在 BBS 上發表謾罵貼文等。除了透過 IP 位置追查外，若要防制在網際網路上「隱匿身分」的犯罪或不法行為，則恐須要透過身分確認機制，如：韓國所實施之「實名制」、業界者所提之『記名制」等，將現實身分直接對應至網際網路使用者之身分。然而透過這些身分確認機制卻可能損害網路的匿名性及自由，同時，對於使用者個人資料保護亦可能造成某種程度的侵害。因此，在使用者普遍要求個人隱私資料保護意識下，各國紛紛制定個人資料或隱私保護相關法令規範。本研究所訪談之專家學者也認為『實名制」所需之法規、登記等條件，現階段在我國實施較為困難，甚或造成民眾的反彈。

「竄改、偽冒及竊盜身分」之行為是竊盜與盜用他人身分所遂行之行為，不論是受訪談的專家學者意見及國內外之法律規範均將其視為違法之行為；既然是違法的行為，則必定需要追(查)緝與避免因其行為所造成的損失。就法令上規範而言，除美國將「身分竊盜」行為明訂為專門之罪名外，我國及其他國家之法律僅就犯罪結果加以規範，並未在法律條文中，明訂「竊盜身分行為」之罪名。在實務上，我國多以因「竊盜身分之行為」後所進行之相關證明文書偽冒作為起訴之罪名(竄改或偽冒文書罪)加以規範。

商業相關法規規範各類商業活動的進行，網際網路上的商業活動亦同樣受到「隱匿身分」行為之影響。從技術的角度來看，網路服務提供者在提供服務時，所設計的商業流程，必然能夠記錄及留存相關交易資訊，以利計費，即使有些服務為免費提供予使用者，但仍會透過伺服器加以記錄，這些紀錄雖無法直接對應使用者的真實身分，但透過間接方式，如：網路連線服務提供業者對於 IP 位址與使用者的綁定。在商業活動中對於身分確認的要求更為嚴謹，則更可保障交易雙方之利益。我國之電子簽章法，即是對於身分確認機制的專法之一，用以確認電子簽章之合法地位。

隨著資訊科技之發展，電腦與網路技術日新月異，在資訊社會中藉由電腦與網路產生的犯罪行為也逐漸增加。網路具有普遍性、開放性、互通性、隱匿性、多樣性、即時性及跨區域性等特性，而透過網路所犯罪刑也具類似特性。有鑑於此，目前各國政府如美國與歐盟等國家，皆積極在尋求方法縮短科技與法律兩者間的差距，以利減少或遏止網路犯罪之可能性。如美國於 1994 年已通過電腦濫用修正法(Computer Abuse Amendment Act of 1994)，與 1996 年對於電腦詐欺及濫用法之修訂建立針對網路犯罪之規範。美國司法部於 1989 年對電腦犯罪態樣依其在犯罪的角色，分為三種類型：一是以電腦作為犯罪客體之行為，例如對於電腦硬碟或是軟體的偷竊行為；二是以電腦作為主體的犯罪行為，包含各類電腦病毒、網路之攻擊或入侵之行為；三是以電腦作為傳統犯罪工具行為，如電信詐欺或侵害著作權等行為[83]。

網路犯罪可說是電腦犯罪之延伸，因網路犯罪是一種電腦系統與通訊網路相結合之犯罪，偏重於網際網路之應用，具有網際網路特性之犯罪，如隱密性與匿名性，亦即犯罪過程中透過網際網路方能進行其犯罪意圖之行為[30][34]。因此援用電腦犯罪分類，輔以網路犯罪之定義，依網路在犯罪中所扮演角色，將其犯罪行為分為三類：一是以網路空間作為犯罪場所，如網路色情、網路賭博等行為；二是以網際網路作為犯罪工具，如網路上散布誹謗、網路詐財與網路釣魚等行為；三是以網際網路為犯罪客體之行為，如網路入侵或散布電腦病毒等行為[83]。將網際網路隱匿與竄改身分行為用以遂行網路犯罪時，難以追蹤犯罪之人。故此，從應用實務而言，網際網路與傳統犯罪相比較，網路犯罪具有匿名性、隱密性、即時性與跨域性之特性，而再加上電腦犯罪之可遙控性與自動複製性之特性，使得網路犯罪比傳統犯罪之成本可能更低廉，其所造成傷害可以跨域延伸，突破地理環境與國家疆

域之限制，因此，增加刑事程序上對於犯罪者之追蹤、逮捕與定罪之困難度，特別是犯罪偵查、蒐證與資料保全等問題更難處理。

本研究第四章研提之網際網路隱匿及竄改身分行為防制技術與機制，現有的防制技術與機制可概分為兩大類，一類為「追查」，主要用來對抗因隱匿及竄改身分行為與技術所遂行的犯罪行為。另一類為「預防」，主要用來預防因隱匿及竄改身分行為與技術進行犯罪行為。

這些防制技術與機制的實施及成效，有賴於網際網路服務提供商及網際網路使用者之配合。政府所扮演的角色為透過相關的法令、管理辦法及規範，提供網際網路服務提供商及使用者對抗利用隱匿及竄改身分行為所進行的犯罪或作為之損害。根據所研提的防制技術與機制，分析現有法令、管理辦法及規範如下：

一、 追查類之防制技術與機制現況

追查類之防制技術與機制，須克服隱匿及竄改身分行為會導致犯罪行為不易追查之特性，所以需要透過紀錄、日誌等機制協助執法單位找出犯罪者及其犯罪事實。如：透過連線紀錄，能夠協助追查犯罪者來源 IP，協助防制偽冒身分、合法掩護非法、欺騙、偽裝及劫持等行為態樣所進行的犯罪行為。追查類之防制技術與機制現況，可從各類紀錄機制之規範及網際網路實名議題來看：

1.各類紀錄機制之規範

防制隱匿與竄改身分行為技術中，保存相關的連線紀錄或登入日誌是最為基礎的作法之一，透過系統或網路的各類紀錄，可利用來追蹤使用者，追查在系統或網路中發生的犯罪行為。網路犯罪的追查，必須要有相關的紀錄留存以作為證據，執法單位是否能夠取得相關的連線紀錄，將是最為重要的關鍵。現有電信相關法規(固定通信業務管理規則、行動通信業務管理規則、第三代行動通信業務管理規則、第二類電信事業管理規則、無線寬頻接取業務管理規則等)均已規定須保留相關通信紀錄及使用者資料，可提供辦案機關相關犯罪偵查方向及證據參考。

商業活動部分，雖然電子商務業者並未具有 IASP 業者的身分，不必遵守相關電信管理規則，也未必有保存客戶交易紀錄的義務。但基於保障消費者與避免爭議的考量下，電子商務業者均會保存客戶交易資料，且網路上之交易紀錄仍屬適用民法有關契約之規定，由交易雙方負保存之義務。顯示現有法規中，對於連線紀錄、交易紀錄等均有明文規範。

依據「第二類電信事業管理規則」第 27 條則規定，電信業者對於有關機關調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供其資料。業者對屬於網際網路接取服務相關紀錄或是虛擬行動網路服務通信紀錄，應保存 1 個月至 6 個月。另外，依據「電信事業處理有關機關查詢電信通信紀錄實施辦法」、警察機關查詢電信通信紀錄及使用者資料管制作業要點，以及通訊保障及監察法等規定，執法單位依其權限及相關規範，即可調閱這些連線紀錄或通訊紀錄，以利犯罪偵察。依據警政署所發布的統計數據來看，現有網路犯罪除跨國之犯罪外，破獲率約有 7 成或以上(參見表 3-6 與表 3-7)。顯見在現有環境下，透過對於相關紀錄的追蹤，找到網路犯罪者頗有成效。

此外，對於透過相關紀錄的追查，執法單位透過法律程序，調閱國內各行業或單位之相關紀錄，以追查網路犯罪。但對於在追查過程中，涉及需取得國外伺服器或網路等紀錄，則無法透過法律來加以規範，而是需要透過外交或其他協商管道進行，面臨跨國無法繼續往下追查及國外沒有留存適當紀錄或痕跡等困難。

2.網際網路實名議題

網際網路實名制似可從源頭避免隱匿身分與竄改身分之行為，但事實上，其仍無法完全遏止竄改或隱匿身分之行為，其僅具遏止網際網路匿名之可能。本研究受訪談之專家也認為，網路實名制的施行，可能侵害網路自由。同時，實名制的實施，甚至可能因為沒有適當配套機制或面臨無法克服之技術問題，反而變成懲罰守法的人。

找到使用網路或連線的人，是追蹤隱匿及竄改身分行為的重要部分。現階段，我國為避免詐騙的發生，使用者欲申請電信或網路連線時，依「固定通信業務管理規則」第 49-2 條、「第三代行動通信業務管理規則」第 77 條、「無線寬頻接取業務管理規則」第 75 條及「第二類電信事業管理規則」第 27 條等規定，電信用戶申請服務須採用實名登記，並留存相關紀錄，供有關機關依法查詢。顯見我國現有之制度，事實上已採取部分實名制。當使用者透過國內 IASP 連線至網際網路時，不論是透過 ADSL、CABLE、無線網卡、智慧型手機或 WIMAX 等各種終端或技術接取網路時，均可透過此一部分實名制，綁定其現實身分與使用之 IP。當網路犯罪追查時，虛擬 ID，最終也將對應至其使用之 IP，故執法單位可連結犯罪行為所使用之 IP 與其現實身分。

當然，根據本研究所進行的學者專家座談與訪談，參與座談與訪談之專家學者則有兩項主要的觀點與主張。一為「網路實名

制」限制人民的自由，所以無論如何均不應採用，而可考慮如：「記名制」等技術或方式，透過另外公正第三方來進行類似實名制，但又不會直接侵害人民自由之方式。另一主張採用「網路實名制」在特定的應用場景中是必須的，而且現在也具有相關規範並經執行，如：網路報稅，透過自然人憑證存取的系統等，因此維持現有之情況即可，不須再有新法或強制規範一定要使用「網路實名制」，可以由各應用需求來規範，這種在特定應用引用實名制之方式符合網路自由精神與重要場景需辨明身分之需求。這部分可以搭配 IASP 連線服務申請必須以真實身分申請之規範，可以營造一個比較自由且安全的網際網路環境。

二、 預防類之防制技術與機制現況

預防類之防制技術與機制，主要是著重於提高隱匿與竄改身分行為之門檻或降低利用隱匿及竄改身分行為之犯罪作為及損失，讓隱匿與竄改身分行為不易施行。此類之防制技術與機制包含企業（使用者）應建立資通安全觀念及政策，並透過採取足適之安全機制，如：使用安全無線網路傳輸協定、網路設備制定安全過濾規則、建立偵測與告警機制、檢測及修補檢測主機與網路設備之弱點、DNSSEC 安全驗證、建立身分認證與會話加密機制等。說明如下：

1.安全機制

資訊安全意識抬頭，多數網際網路服務提供者，已開始採用相關的安全技術與機制進行防護作為。如：安全傳輸協定、身分認驗證技術、加解密技術、偵測與告警技術及弱點檢測與修補管理等，避免造成經營者或客戶之損害。這些安全技術與機制，除了有利於資安事件或網路犯罪的追蹤外，對於隱匿與竄改身分行為的施行，亦造成適當的遏阻及門檻，如：使用憑證身分認證技術，使用者就不易進行偽冒身分；提升網路設備安全性，就不易被進行 ARP 欺騙行為等。當大眾普遍熟悉此類安全技術之優點後，即產生使用誘因，各網際網路服務提供者及使用者始有意願採用相關安全技術與機制。

再者，在網路的傳輸過程中，網際網路服務提供業者扮演著非常重要的角色，負責提供傳遞資訊的網路線路並保持其暢通。因此，也必須肩負起相關責任，提供安全的服務如：電信法第 6 條規定電信事業應採適當並必要之措施，以保障其處理通信之秘密，保障使用者之安全。「行政院所屬機關電腦設備安全暨資訊機密維護準則」第 28 條規定各機關應視業務需要，採行有關資訊

安全之保險措施；「電腦網路內容分級處理辦法」第 10 條規定，應依我國網際網路協會訂定之網際網路服務業者自律公約，採用內容過濾或身分認證等措施機制，防制兒童或少年接取不良之資訊；「電子票證應用安全強度準則」第 2 條規定電子票證發行機構之安全需求與設計，建立安全防護措施，以確保電子票證應用之安全強度。此外，通傳會基於監督管理電信事業營運之職責，要求電信業者參照 ISMS(Information Security Management System) 精神，對資訊安全採嚴格之管控，進而取得 ISO27001 之資訊安全認證，並要求相關電信業者加強對設備遠端管理功能之安全管控，以維護消費者權益並確保資通訊安全。雖非強制要求電信業者通過 ISO27001 之資訊安全認證，但已讓提供電信及網路服務之業者將相關的安全技術與機制納入其服務中。而這些安全技術與機制有助於提高隱匿與竄改身分行為之門檻。

個人資料保護法中第 11 條規範公務機關或非公務機關應維護個人資料之正確，同時，第 18 條公務機關及第 27 條非公務機關應有安全機制防止個資遭竊竄損漏，且第 28 條及第 29 條規範損害賠償之責與第 48 條第 4 款明定未訂資安維護計畫罰則。規範在處理相關個人隱私及身分資料時，不論公務機關或非公務機關均須維護、及保護相關資料，並制訂相關保護計畫及措施，避免違法或洩漏個人隱私及身分資料。消費者保護法第七條也規定服務提供者須確保商品或服務，要符合當時科技或專業水準可合理期待之安全性。這些透過法規明定之作為（公務機關或非公務機關遵循法令所執行的制度或採用相關保護技術）有助於在追查時，利用這些保護或安全機制所產生之紀錄進行追蹤及預防個人資料的洩漏或被利用來進行竄改身分之行為。

隱匿與竄改身分防制技術中，部分的技術是跟隨國際腳步，如 DNSSEC 安全驗證，係由國際同步對於 DNS 機制施行才能發揮效益，隨著國際上對於 DNSSEC 技術的採用，我國 TW 網域亦將同步配合國際上 DNSSEC 技術之部署。目前我國雖未公布相關導入的時間表，但由於國際上已於 2010 年開始進行 DNSSEC 技術之部署，預計在未來 10 年將可替代現有 DNS 系統架構。

2.觀念及政策

隱匿與竄改身分行為的防制，除了可採行相關技術外，尚可從加強教育及改善使用者的安全觀念與使用習慣著手。主要的原因，這些隱匿與竄改身分之行為的發生，大多是因為使用者不了解其背後的運作技術，而認為「於網路使用匿名的 ID，所以別人不知道我是誰」進而發生一些違法行為，如：對事件的爭執或看

法歧異時，因一時氣憤便在線上留言或透過電子郵件攻訐對方，甚至辱罵及毀謗，並認為其在網路上發布之留言或言論係以匿名為之，所以其真實自我及位置無法被追蹤。或以為蓄意透過技術隱匿其 IP 位置，即可躲避追查等，其次，在網路上張貼援交訊息也是現在網路犯罪的大宗，多數被查獲的被告都表示不知道這樣的行為構成兒童及性交易防制條例第 29 條之規定，更顯示網路犯罪者對自己犯罪行為的無知，顯見這部分需要法治教育的宣導來彌補。

另外，在身分認證技術中最有效率的方案為電子簽章技術，我國自 2002 年起就開始使用自然人憑證機制，為一有效的身分認證技術，且電子簽章法於 2001 年 1 月公布用以律定電子簽章及電子文件之法律地位。這些技術與法規均已完備，可用於隱匿與竄改身分行為之防制技術或機制中。但目前看起來成效仍有限，許多民眾仍不知何謂電子簽章或自然人憑證。根據資策會(FIND)統計截至 2011 年 3 月，我國網際網路用戶數為 2,555 萬，但自然人憑證發卡量尚未超過 250 萬，且大多集中於大都會區，顯見仍待宣導及教育民眾對於此類身分認證技術之應用。

三、小結

本研究研提之網際網路隱匿及竄改身分行為防制技術與機制現況與現有相關法規及規範現況整理如表 6-1。

表 6-1 網際網路隱匿及竄改身分行為防制技術與機制現況

類型	防制技術與機制	相關法規及規範現況與問題
追查	1. 保存網際網路連線使用紀錄 2. 使用憑證身分認證技術 3. 保存日誌攻擊資料 4. 反查使用 proxy 之 IP 來源 5. 使用者帳號認證 6. 建立身分認證與會話加密機制	1. 竄改身分有可能觸犯刑法偽造文書罪。 2. 隱匿身分為受到網路自由之保護，與隱私權有關。同時現有法規如：刑法電腦犯罪專章或其他傳統犯罪等處罰是犯罪行為，而非過程的行為，故隱匿與竄改身分之行為，若未損及國家、他人利益或公平正義，則不違反法令規定。 3. 隱匿與竄改身分之行為可能造成

類型	防制技術與機制	相關法規及規範現況與問題
		難以追查犯罪行為，但現有法令規範連線行為是需要紀錄的，並且可提供執法單位申請調閱。如：「第二類電信事業管理規則」第 27 條、「固定通信業務管理規則」第 49-1 條、「電信事業網路互連管理辦法」第 25 條、「無線寬頻接取業務管理規則」第 74 條、行動通信業務管理規則第 72 條及第 72 之 1 條、第三代行動通信業務管理規則第 75 條及第 76 條之規定。 4. 網際網路實名制看似可從源頭避免隱匿身分與竄改身分之行為，但卻無法完全遏止竄改或隱匿身分之行為，其僅遏止網際網路匿名之可能。
預防	1. 使用安全連線傳輸帳號密碼 2. 使用安全無線網路傳輸協定 3. 網路設備制定安全過濾規則 4. 加強頻寬管理與即時告警 5. 建立偵測與告警機制 6. 提升網路設備安全性 7. 檢測主機與網路設備	1. 網際網路服務提供業者扮演重要的角色，需提供相對應安全機制，相關法規如：電信法第 6 條、電腦網路內容分級處理辦法第 10 條、行政院所屬機關電腦設備安全暨資訊機密維護準則第 28 條、電子票證應用安全強度準則第 2 條。 2. 個人資料保護法第 11 條維護資料正確性、第 18 條公務機關及第 27 條非公務機關應有安全機制防止個資遭竊竄損漏、第 28 及第 29 條損害賠償、第 48 條第 4 款

類型	防制技術與機制	相關法規及規範現況與問題
	之弱點 8. DNS 服務安全檢測 9. DNSSEC 安全驗證 10. 建立安全代詢伺服器名單 11. 教育使用者基本安全觀念 12. 良好網路使用習慣的教育 13. 規範網站的隱私權政策 14. 使用電子簽章發送電子郵件	未訂資安維護計畫罰則及消費者保護法第 7 條服務及商品提供之可合理期待之安全性等。公務機關或非公務機關遵循法令所執行的制度或採用相關保護技術，有助於預防個人資料的洩漏或被利用來進行竄改身分之行為。 3. 現有參照 ISMS(Information Security Management System)精神或導入安全管理標準之要求，實作強化安全之機制，並提高隱匿與竄改身分之行為之門檻。 4. 部分防制技術與機制，如：DNSSEC。會隨著國際上通用服務而隨之導入。不需強制規範。 5. 隱匿與竄改身分之行為的發生，大多是因為使用者不了解法規及不清楚網路背後的運作技術與機制，而造成誤解或無知，並不是政策或法律沒有規範，因此，教育與宣導才是更有效的解決方式。 6. 防制技術或機制、法規多數是完備的，顯見其仍待宣導及教育民眾。

資料來源: 本研究整理

雖然現有的法令已可處罰透過網際網路隱匿及竄改身分所進行之犯罪，且對於相關的防制技術與機制，亦有法規與辦法等加以支持，但是對於追蹤網路犯罪仍須強化其執行面。網際網路隱匿與竄改身分行為無法透過技術完全的解決與防制，畢竟部分隱

匿身分之技術就是用來保護個人隱私之用，所以經由管理制度、教育等方式，才是更有效的方式，而非完全透過技術與法規之規範。

第二節　尚不需配套法規之理由

分析網際網路隱匿與竄改身分行為與其防制技術與機制，本研究認為現有的機制已經有相關的法令規範足以協助追查及預防，現階段不需要進一步透過配套法規來強化其機制，而是需要透過社會倫理、法律宣導、技術、制度與教育等來強化其防制技術與機制。主要理由及其說明如下：

1. 隱匿及竄改身分行為不一定造成國家、他人之損失，但被當成工具進行犯罪行為，現有法規足以規範，不須為制訂專法或修改現行法令。
2. 防制技術與機制中，對於追查所須的紀錄機制，現有法令已規範需留存，並依法提供給相關執法單位，進行追查。
3. 現有法令（如個人資料保護法第 27 條、第 28 條、第 29 條及第 48 條第 4 款）已規範服務提供者或管理者須善盡管理之義務，增加相關安全機制減少偽冒動機與門檻。
4. 我國在法規規範下，已實施部分實名制（如雙證件申請電信服務、自然人憑證進行所得稅申報）的情況下，已可強化追查之相關防制技術與機制。相較之下，民眾較缺乏的是對於這些追查機制的認知與理解。
5. 電子簽章技術及身分認證技術、安全通訊協定的法令規範及技術標準成熟，但缺乏有效的宣導及教育，而非新法規。
6. 許多安全機制與方法均已實施，並存在法令規範或管理辦法，無須在制訂新的配套法規，強化現有法規宣導與執行，並落實相關防制技術與機制，更具實質效益。

一、 不須為「隱匿及竄改身分行為」制訂專法或修改現行法令

專法的修訂為針對特定之行為結果，因其促使不公平之情況產生，故對於加害或侵害之一方進行處罰，促使社會公平維護正義。從應用實務而言，網際網路與傳統犯罪相比較，網路犯罪具有匿名性、隱密性、即時性與跨域性之特性，而再加上電腦犯罪之可遙控性與自動複製性之特性，事實上網路犯罪內容與傳統犯罪內容並無太大差異，例如詐欺罪，不論在傳統的犯罪與網路犯罪中均可能遂行，其手段與本質未變，而是犯罪工具改變。法規

為維護公平，因此規範侵害他人權利之結果，而非其過程之行為，因此，無須特定的法規(專法)規範網際網路隱匿與竄改身分行為。

「網際網路隱匿身分行為」可能無過失或侵害他人利益，如：在網路論壇中使用 ID 發表對於新聞事件的個人意見，不涉及謾罵或損害他人名譽，只是抒發自己的意見，未侵害他人權利或利益，且受憲法保障其言論自由，故不應透過專法規範或處罰其行為。但涉及謾罵或損害他人名譽，損及他人權益或利益時，則應依其所觸犯之「妨害名譽」等加以處罰，而非處罰其使用 ID 來隱匿身分之行為。

「網際網路竄改身分行為」是為冒用或竄改他人之身分，進而損害他人之利益，雖現有法律中並未明確定義這樣的行為。但現有法律中對於冒用或竄改他人之身分所導致之結果早有明文規定，舉例來說，在網站登錄填入假的身分證統一編號，依刑法第 210 條規定「偽造、變造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。」屬偽造文書罪。在一份用以表彰身分的資料中，填入假的身分證字號(冒用他人身分)，客觀上構成以他人名義製作文書、或是表彰他人名義於文書上(竄改他人身分)，主觀上使用者也知道自己填入假的資料，故此當屬偽造行為。若利用假造之身分證字號進行不法行為，例如網路上之詐欺行為、逃避不法追訴、社交工程身分偽造等，將以具體之不法行為事實所涉之法規論處（如刑法：詐欺、竊盜、背信等），偽變造文書僅係過程之一，同樣可能構成刑法競合一罪的情形。因此現有法規中，對於「竄改身分行為」事實上已經有相關的法規加以規範，無須再重覆另立一專法規範其行為。

由於國內已有用以規範保護個人隱私與權利及商業活動行為之相關法律規定，可以規範網路犯罪。本研究就個人隱私、商業活動及網路犯罪部分，提出幾項法規，說明現有「網際網路隱匿與竄改身分行為」事實上均有現行之法規，分述如下：

(一) 個人隱私部分

因應隱匿身分與竄改身分行為所遂行的犯罪結果，我國在個人資料保護法中，已有相關的規定。例如個資法第 42 條規定，意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 100 萬元以下罰金。

再者，個人資料保護法的實施，也促使在網際網路上的電子商務交易愈趨於保護消費者，因此，許多電子商務業者，透過現有法令規範(個資法、經濟部提供的網路平台交易安全規範等)的遵循，提高消費者個人隱私資料的安全性。

匿名牽涉到言論自由，採用匿名並非一定是有意圖進行犯罪行為；但竄改身分則是犯罪行為，目前已有著作權法、個資法、電子簽章法、偽造文書與刑法第 36 章妨害電腦使用罪之規範，故已足夠規範相關犯罪行為。

(二) 商業活動部分

根據民法 153 條第 1 項，契約是雙方當事人合意而生法律上效果之行為。又自 2011 年起生效的「零售業等網路交易定型化契約應記載及不得記載事項」也明訂個人資料保護、帳號密碼被冒用之處理及消費爭議處理等內容。顯示在網路上之交易行為，為保障交易雙方權利與義務，其各自須負責留下交易紀錄或記載於契約中。對於商業活動的交易雙方而言，其活動過程均透過契約加以約束及規範，並受到現有之相關法令(如：民法、消費者保護法等)保護，已無須為其行為再修訂專法。

(三) 網路犯罪部分

事務上，不當之網際網路隱匿與竄改身分行為，並未造成新形態之犯罪行為產生，與傳統犯罪行為比較，僅是犯罪工具改變，所使用的是一個強大且快速的工具，但其犯罪結果與現實世界間仍有相當的對應，基本的法益體系沒有改變，刑法原本即有相關處罰規定，所以刑法大部分的條文如妨害風化、妨害名譽、詐欺、竊盜、賭博等在網路世界仍可適用。 如刑法第 358 條無故輸入他人帳號密碼，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金，此乃屬告訴論，若受害者提告，主管機關或負責人員可能須耗時證明之，這就有賴相關人員的負責態度與願意破案的積極度，故執行面是較須受重視之因素。

網路犯罪及網際網路隱匿與竄改身分行為日新月異，難以使用單一專案法規規範所有新的犯罪態樣與技術，故透過現有法規與判例加以規範，其效果將大於制訂專法。

綜整上述，「網際網路隱匿與竄改身分行為」僅是網路犯罪中的可能行為，而「網際網路隱匿與竄改身分行為」也能用在隱私權保護並非一定造成犯罪，故無須修訂專法來特別規範「網際網路隱匿與竄改身分行為」。對於經由「網際網路隱匿與竄改身分行為」所遂行之犯罪行為，依我國現行法律來看，均有相關的

法規用以管理及處罰相關的侵害及犯罪行為(可參考表 3-8 及表 3-9)，故亦無須為因「網際網路隱匿與竄改身分行為」修訂專法來規範之。此外，「網際網路隱匿身分行為」，亦為隱私議題之一，現有的法令也保護個人隱私(如：個人資料保護法等)，故同樣無須再為其另訂專屬法規條文來定義及規範之。

二、 現有法規已規範犯罪追查與連線紀錄保存機制

網路犯罪的追查，必須要有相關的紀錄留存以作為證據。而其中最重要的是連線紀錄的追查與保留。執法單位是否能夠取得相關的連線紀錄將是此一議題最為重要的關鍵。現有通訊類相關法規如：固定通信業務管理規則、第二類電信事業管理規則、行動通信業務管理規則、第三代行動通信業務管理規則、無線寬頻接取業務管理規則等均已透過明文規範須保留相關紀錄以供有關機關查詢，電信事業基於協助立場，提供上開資料可間接證明犯罪事實及提供警方擬定辦案方向之參考。商業活動部分，雖然電子商務業者並未具有 IASP 業者的身分，不必遵守電信事業相關管理規則，也未必有保存客戶交易紀錄的義務。但基於保障消費者與避免爭議的考量下，電子商務業者均會保存客戶交易資料，且網路上之交易紀錄仍屬適用民法有關契約之規定，由交易雙方負保存之義務。另為引導電子商務正向發展，目前經濟部刻正辦理「網路平台安全及通報機制建置計畫」亦委託資策會制定「電子商務交易安全規範」供作積極輔導電子商務業者強化平台業者、商品供應商、物流商等之資訊安全管理之行政指導文件，相關行政措施已逐步展開。

同時，依據相關電信業務管理規則保留用戶一定期間通信紀錄之規定，及「電信事業處理有關機關查詢電信通信紀錄實施辦法」、警察機關查詢電信通信紀錄及使用者資料管制作業要點與通訊保障及監察法等規定，除了電信業者須保留相關連線紀錄外，執法單位可依其權限及遵守相關規範下，亦即可依法調閱這些保留下的連線紀錄或通訊紀錄，以利犯罪偵察。由表 3-6 與表 3-7 警政署所發布的統計數據來看，現有網路犯罪除跨國之犯罪外，破獲率約有 7 成或以上，顯見在現有環境下，執法單位透過連線或通訊紀錄的追蹤，找到網路犯罪者頗具成效。

個人資料保護法第 11 條、第 18 條、第 27 條、第 28 條及第 29 條及第 48 條第 4 款與消費者保護法第 7 條，規定要建立保護及相關的安全措施，來保護處理的個人資料、身分資訊或服務。有助於預防個人資料的洩漏或被利用來進行竄改身分之行為。同

時，執法單位進行犯罪偵察時，也可利用這些安全機制，進一步釐清隱匿與竄改身分之情況，有利於找到真正的犯罪者。

由此看來，犯罪追查與連線紀錄的保存，現有法規已規範。在本研究第四章中所說明之各項防制技術與機制，可依據連線紀錄來追查犯罪，本研究認為尚無須修改現有之配套法規。

三、 現有法規已規範管理者須善盡管理之義務

如上一節所述，電信法第 6 條、個人資料保護法第 18 條、第 27 條、第 28 條、第 29 條及第 48 條第 4 款及電腦網路內容分級處理辦法第 10 條、行政院所屬機關電腦設備安全暨資訊機密維護準則第 28 條、電子票證應用安全強度準則第 2 條等多項法規及管理辦法，均已規範需採用相關安全機制。經濟部商業司「網路平台安全及通報機制建置計畫」，為提升電子商務平台業者之資訊安全管理，委託電子商務資安通報服務中心制訂包含：網路平台、物流商、供應商等一系列電子商務交易安全規範，以作為我國電子商務產業相關業者之行政指導文件。事實上，採用這些相關的法規、安全機制與業者或管理者所面臨的營運風險有關，當其認為隱匿與竄改身分之行為態樣足以造成營運風險的因素時，就可能將資源投入於防制技術或機制中。技術在不斷地演進中，防制技術或機制也可能不斷地推陳出新，現有法規及行政措施已足以規範相關業者應採行有關資訊安全之保險措施，而不須規範或或新修定配套法規，來確保其使用之技術與機制。

四、 民眾較缺乏的是對於這些機制的認知與理解

為了避免詐騙，相關電信業務之管理規則均已明定各該業務經營者應查核、登載其用戶資料，如《固定通信業務管理規則》第 49-2 條「經營者應核對及登錄其用戶之資料，經載入經營者之系統資料檔存查後始得開通，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。前項用戶之資料包括姓名、身分證統一編號、第二證件號碼、地址及所指配號碼等資料。」

此法規的實施，讓我國對於網路實名制，有了很大的進展，透過此一法條之規定，當使用者申請相關電信或網路服務時，就留下了實名的資料，在配合上述之紀錄保存規範，透過連線紀錄找到實際的使用者不再是難題，也就是說目前我國是屬於「部分網路實名制」之情況。雖然此法只規範包含通信網路的固定通信業務，但事實上，網際網路上的追查動作，均透過 IP 的追查，能夠查詢到特定時間使用的 IP，則能夠透過此一法規找到對應的用

戶或使用者實體位置。但是這些機制，卻不為大多數的民眾所認知及理解。許多民眾有錯誤的觀念，仍認為網路上的行為受到匿名的保護，所以別人不知道我是誰。疏不知藉由相關電信法規規定所留存之紀錄，執法單位即可連結犯罪行為所使用之 IP 與其現實身分。此一部分需透過對於法令的宣導與教育讓民眾認知與了解，有助於提高合法掩護非法等行為態樣之防制機制門檻。

五、 法令規範及技術標準成熟，但缺乏有效的宣導及教育

本研究所研提的防制技術與機制，大多為現今安全管理主流使用之技術與機制，如：憑證身分認證技術、偵測與告警機制、安全過濾規則及檢測主機與網路設備之弱點等。且如電子簽章法、及本節第三項所描述之善盡管理義務之法規規定等，顯見現有電子簽章技術及身分認證技術、安全通訊協定的法令規範及技術標準成熟。但是這些防制技術與機制的使用情況卻仍在緩慢起步中，顯示缺乏有效的宣導及教育，促進相關技術與機制的使用。另外，部分技術與機制，如：DNSSEC。隨著國際上之部署，我國亦順勢更新及實施，並不須要制訂相關配套法規或規範。

六、 強化現有法規宣導與執行，使得相關防制技術與機制落實才更具實質效益

綜論上述，許多安全機制與方法已可實施，並已有相當完備之法令規範或管理辦法，這些法令規範與管理辦法已敷運用。因此無須再為執行防制技術與機制特別制訂新的配套法規。事實上，我國目前比較缺乏的是宣導及教育民眾，使瞭解相關的法規規範及隱匿與竄改身分的防制技術與知識。

舉例來說，許多民眾上網向各大入口網站申請帳號時，為隱匿自己的真實身分，故意在認證欄內，胡亂填上一個自己瞎掰的身分證統一編號，若該身分證統一編號確實存在，則就已觸犯刑法偽造文書罪。依刑法規定，偽造文書屬於公訴罪，被害人事後可以向犯罪嫌疑人提出名譽損害賠償。在許多被破獲的網路犯罪案例中，執法單位就指出有許多人申請帳號時，故意填具不實身分資料，而這種行為之比率，竟然高達 50%以上，顯見違法行為非常普遍。另外，許多犯罪者也會蓄意地隱匿身分，認為執法單位無法追查。有一販賣盜版軟體及色情光碟的案例，嫌犯利用網路容易隱匿身分不易查察的特性，以人頭資料申請架設網站、郵政信箱及承租套房，使得執法單位在追查時連連受阻。後來從 IP 位址查出這個網站登記在台中縣龍井鄉一棟大樓內，進而將嫌犯逮捕。此類的案例，不勝枚舉，顯示目前許多民眾對於現有的法

規及隱匿與竄改身分防制技術與知識的欠缺，因此誤觸法網或異想天開地認為其行為可躲避追查。故宣導及教育民眾，使瞭解相關的法規規範及隱匿與竄改身分防制技術與知識，才是當務之急。

七、 小結

根據上述，本研究建議，目前尚無須對於「網際網路隱匿及竄改身分行為」制訂專法或修法，同時，在現有法令規範下，尚不須對於執行網際網路隱匿及竄改身分行為之防制措施與機制制訂特別之配套法規，而是應透過社會、法律宣導、技術、制度與教育等方式，來強化防制措施與機制之執行，並預防因網際網路隱匿及竄改身分行為所導致的網路犯罪及損失，進一步說明請參見下節。分析整理相關隱匿或竄改身分行為之防制措施與機制與現有法規規範配套如下表 6-2。

表 6-2 防制技術與機制與現有法規規範配套

類型	防制技術與機制	現有法規規範配套	
追查	1. 保存網際網路連線使用紀錄 2. 使用憑證身分認證技術 3. 保存日誌攻擊資料 4. 反查使用 proxy 之 IP 來源 5. 使用者帳號認證 6. 建立身分認證與會話加密機制	個人資料保護法	第 10 條公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。 第 18 條 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 第 22 條 中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。 第 23 條 對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入

類型	防制技術與機制	現有法規規範配套	
			之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。 第 27 條 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏；中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法；前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。 第 28 條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 第 29 條非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
		固定通信業務管理規則	第 49-1 條經營者對於市內通信之通信紀錄，應至少保存三個月；對於國際及國內長途通信之通信紀錄，應至少保存 6 個月。經營者因用戶本人查詢之申請，應提供依前項規定保存之通信紀錄。 第 49-2 條經營者應核對及登錄其用戶之資料，經載入經營者之系統資料檔存查後始得開通，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。 前項用戶之資料包括姓名、身分證統一編號、第二證件號碼、地址及所指配號碼等資料。

類型	防制技術與機制	現有法規規範配套	
			前項證件號碼，於法人申請時，指營利事業登記證號及代表人身分證號；於自然人申請時，指身分證號及足資辨識身分之證明文件證號。第一項用戶資料之載入，應於經營者受理申請2日內完成之。
		第二類電信事業管理規則	第27條　經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。 前項電信內容之監察事項，依通訊保障及監察法規定辦理之。 經營者對於第一項電信通信紀錄應至少保存期間如下： 一、語音單純轉售服務通信紀錄應保存六個月。 二、網路電話服務通信紀錄應保存六個月。 三、網際網路接取服務： (一)撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。 (二)非固接式非對稱性數位用戶迴路(ADSL)用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。 (三)纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。 (四)張貼於留言版、貼圖區或新聞討論群之內容來源IP位址與當時系統時間應保存三個月。 (五)免費電子郵件信箱及網頁空間線上申請帳號時之來源IP位址及當時系統時間應保存六個月。 (六)電子郵件通信紀錄應保存一個月。 四、虛擬行動網路服務通信紀錄應保

類型	防制技術與機制	現有法規規範配套	
			存六個月。 經營者應核對及登錄其用戶之資料並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。虛擬行動網路服務經營者或 E.164 用戶號碼網路電話服務經營者應將使用者資料載入其系統資料檔存查後始得開通；以預付卡或其他預付資費方式經營虛擬行動網路服務者或 E.164 用戶號碼網路電話服務者，亦同。 前項用戶之資料包括使用者姓名、國民身分證統一編號、第二證件號碼及住址等資料，且虛擬行動網路服務經營者或 E.164 用戶號碼網路電話服務經營者另應包括所指配號碼。用戶如為政府機關、公立學校及公營事業機構，得以該機關(構)公文書作為識別用戶身分之證明文件。 前項證件號碼，於外國人申請時，指護照號碼及護照外之其他足資辨認身分之證明文件證號；於法人申請時，指公司登記統一編號及代表人國民身分證統一編號；於自然人申請時，指身分證號及足資辨識身分之證明文件證號。 主管機關得限制經營者受理民眾以同一身分證統一編號申請電信服務之用戶號碼數。經營者應依主管機關公告之限制條件及執行方式辦理。 第四項之虛擬行動網路服務經營者或 E.164 用戶號碼網路電話服務經營者應於受理申請二日內完成其使用者資料之載入。 第 27 條之 1 虛擬行動網路服務經營者或 E.164 用戶號碼網路電話服務經營者以預付卡或其他預付資費方式提供服務者，應每週複查其用戶資料，

類型	防制技術與機制	現有法規規範配套	
			如有使用者已經啟用服務而無使用者資料之情事，經營者應暫停其通信。 前項規定，經營者應於其營業規章及服務契約內定之。
		行動通信業務管理規則	第 72 條 經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。 前項電信內容之監察事項，依通訊保障及監察法規定辦理之。 經營者對於第一項之電信通信紀錄應至少保存六個月。 第 72 條之 1 經營者對於通信紀錄，應至少保存六個月。 經營者因使用者本人查詢之申請，應提供依前項規定保存之通信紀錄。 第 73 條 經營者應核對及登錄其使用者之資料，經載入經營者之系統資料檔存查後始得開通，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之。以預付卡或其他預付資費方式經營本業務之服務者，亦同。 前項使用者之資料包括使用者姓名、身分證或護照之證號、身分證或護照外之其他足資辨識身分之證明文件證號、住址及所指配號碼等資料。 第一項使用者資料之載入，應於經營者受理申請二日內完成之。
		第三代行動通	第 75 條 經營者對為調查或蒐集證據依法律程序查詢電信之有無及其內容時，應提供之。 前項電信內容之監察應依通訊保障及監察法之規定辦理。 經營者對於第一項之通話紀錄應至少

類型	防制技術與機制	現有法規規範配套	
		信業務管理規則	保存六個月。 經營者建設或新設、新增、擴充第三代行動通信系統時，其通訊監察相關設備應依通訊保障及監察法及其施行細則相關規定辦理。 第 76 條 經營者對於通信紀錄，應至少保存六個月。 經營者因使用者本人查詢之申請，應提供依前項規定保存之通信紀錄。 第 77 條 經營者應核對及登錄其使用者之資料，經載入經營者之系統資料檔存查後始得開通，並至少保存至服務契約終止後一年，有關機關依法查詢時，經營者應提供之；以預付卡或其他預付資費方式經營第三代行動通信業務之服務者，亦同。 前項使用者之資料包括使用者姓名、國民身分證或護照之證號及國民身分證或護照外之其他足資辨識身分之證明文件證號、住址及所指配號碼等資料。 第一項使用者資料之載入，應於經營者受理申請二日內完成之。
		無線寬頻接取業務管理規則	第 74 條 經營者對為調查或蒐集證據依法律程序查詢電信之有無及其內容時，應予提供。前項電信內容之監察，應依通訊保障及監察法之規定辦理。經營者對於第一項之通話紀錄，應至少保存 6 個月。經營者建設或新設、新增、擴充無線寬頻接取系統時，其通訊監察相關設備應依通訊保障及監察法及其施行細則相關規定辦理。經營者對於通信紀錄，應至少保存 6 個月。經營者因使用者本人查詢之申請，應提供依前項規定保存之通信紀

類型	防制技術與機制	現有法規規範配套	
			錄。
		電子簽章法	第 1 條　為推動電子交易之普及運用，確保電子交易之安全，促進電子化政府及電子商務之發展，特制定本法。 第 11 條　憑證機構應製作憑證實務作業基準，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關核定後，並將其公布在憑證機構設立之公開網站供公眾查詢，始得對外提供簽發憑證服務。其憑證實務作業基準變更時，亦同。 憑證實務作業基準應載明事項如下： 一、足以影響憑證機構所簽發憑證之可靠性或其業務執行之重要資訊。 二、憑證機構逕行廢止憑證之事由。 三、驗證憑證內容相關資料之留存。 四、保護當事人個人資料之方法及程序。 五、其他經主管機關訂定之重要事項。 本法施行前，憑證機構已進行簽發憑證服務者，應於本法施行後六個月內，將憑證實務作業基準送交主管機關核定。但主管機關未完成核定前，其仍得繼續對外提供簽發憑證服務。 主管機關應公告經核定之憑證機構名單。
		電子簽章法施行細	第 7 條　本法第 11 條第 1 項所稱對外提供簽發憑證服務，係指憑證機構簽發之憑證，可供憑證用戶作為其與憑證機構以外之第三人簽署電子文件時證明之用者。

類型	防制技術與機制	現有法規規範配套	
		則	
預防	1. 使用安全連線傳輸帳號密碼 2. 使用安全無線網路傳輸協定 3. 網路設備制定安全過濾規則 4. 加強頻寬管理與即時告警 5. 建立偵測與告警機制 6. 提升網路設備安全性 7. 檢測主機與網路設備之弱點 8. DNS 服務安全檢測 9. DNSSEC 安全驗證 10. 建立安全代詢伺服器名單 11. 教育使用者基本安全觀念 12. 良好網路使用習慣的教育 13. 規範網站的隱私權政策 14. 使用電子簽章發送電子郵件	電信法	第 1 條「保障通信安全及維護使用者權益」 第 6「條電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。 電信事業應採適當並必要之措施，以保障其處理通信之秘密。」 第 7 條「電信事業或其服務人員對於「電信之有無及其內容」，應嚴守秘密；退職人員亦同。」
		個人資料保護法	第 11 條 公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。 第 18 條 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 第 27 條 非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏；中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法；前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。 第 28 條 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。 第 29 條 非公務機關違反本法規定，

類型	防制技術與機制	現有法規規範配套	
			致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。 第 48 條　非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 1.違反第 8 條或第 9 條規定。 2.違反第 10 條、第 11 條、第 12 條或第 13 條規定。 3.違反第 20 條第 2 項或第 3 項規定。 4.違反第 27 條第 1 項或未依第 2 項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
		消費者保護法	第 7 條　從事設計、生產、製造商品或提供服務之企業經營者，於提供商品流通進入市場，或提供服務時，應確保該商品或服務，符合當時科技或專業水準可合理期待之安全性。
		兒童及少年性交易防制條例	第 9 條「醫師、藥師、護理人員、社會工作人員、臨床心理工作人員、教育人員、保育人員、村里幹事、警察、司法人員、觀光業從業人員、網際網路服務供應商、電信系統業者及其他執行兒童福利或少年福利業務人員，知悉未滿 18 歲之人從事性交易或有從事之虞者，或知有本條例第四章之犯罪嫌疑者，應即向當地主管機關或第六條所定之單位報告。 本條例報告人及告發人之身分資料應予保密。

類型	防制技術與機制	現有法規規範配套	
		行政院所屬機關電腦設備安全暨資訊機密維護準則	第 28 條「各機關應定期或不定期實施資訊保密及安全防護教育訓練。各機關應視業務需要，採行有關資訊安全之保險措施」
		電腦網路內容分級處理辦法	第 10 條「電腦網路服務提供者應自本辦法施行之日起 18 個月內，完成電腦網路分級之相關準備措施，並進行分級。期限屆至前，應依我國網際網路協會訂定之網際網路服務業者自律公約，採用內容過濾或身分認證等措施機制，防制兒童或少年接取不良之資訊。」
		電子票	第 2 條「發行機構應依本準則規定之安全需求與設計，建立安全防護措施，以確保電子票證應用之安全強

類型	防制技術與機制	現有法規規範配套	
		證應用安全強度準則	度，保護消費者之權益。」

資料來源：本研究整理

第三節　對於防制隱匿與竄改身分行為之相關建議

網路犯罪行為屬於科技犯罪，即是藉由資訊科技為工具，進行犯罪行為，目前我國偵辦此類型犯罪事實行為以警政署為主管機關。警政署於 2006 年 4 月成立「科技犯罪防制中心」，其中網路犯罪為其重要偵查項目之一。各類網際網路隱匿與竄改身分犯罪行為均屬於警政署防制與偵辦之範圍。再則，經濟部商業司主要職掌分為數項，其中「商業管理」與「電子商務」等兩項與資訊科技相關。因我國已通過電子簽章法，依法規定是由經濟部商業司所主管，涉及企業認證單位相關業務時，即由該部門負責。最後，通傳會依通訊傳播基本法及國家通訊傳播委員會組織法規定掌管電信法、廣播電視法、有線廣播電視法及衛星廣播電視法等原隸屬交通部、新聞局、交通部電信總局相關通訊傳播法規。在網際網路隱匿與竄改身分犯罪行為中，涉及網路接取經營者(IASP)之規範由通傳會所主管。除此三單位，因個資法之規定，由法務部草擬個資法施行細則，故法務部也是重要防制網路犯罪之重要單位。事實上，各單位內皆有統籌資訊業務或網際網路相關主管機關，若要有效防制因匿名或竄改身分所造成網路犯罪行為，各相關主管機關應善盡監督之職。除此，在社會、法律宣導、技術、制度與教育等面向亦皆須配合，分述如下：

一、 社會倫理面

網際網路應用提供許多不同於傳統服務方式，如消息傳遞、購物方式等皆因網路而轉型。在過去傳統社會中，強調面對面互動過程中彼此之信任、禮貌與尊重等基本道德或倫理，常因網路匿名與隱匿特性而被忽略，造成使用者在網路上對自己傳遞消息

真實性不負責或透過網路報復或謾罵其他人，如罵人腦殘或張貼不雅照片等。此些不當情形雖可經由法律途徑處理，但對被害人而言，名譽傷害已造成，受害人之心理創傷實非法律懲處可以彌補。故此，資訊網路社會中為防制網路犯罪，也應該要有一套資訊倫理規範讓使用者遵守，這些資訊倫理規範須能被網路使用者所接受之合理規範，如使用網路之相關禮儀與道德，與對個人隱私之尊重。

二、 法律宣導面

目前在網路犯罪之規範，我國在個人資料隱私部分，主要以個人資料保護法為主，雖施行細則，法務部尚未發布，但是已明確說明相關規範，讓個人使用網路權利受到適當保護。除此，仍有著作權法可以加以輔助規範之。在商業活動部分，主要以電子簽章法為主，此法主要目的是為推動電子交易之普及運用，確保電子交易之安全，促進電子化政府及電子商務之發展。依該法第 2 條規定，主管機關為經濟部。此法亦規定憑證機構由經濟部負責管控，因此在我國未採取實名制之現況，對於網路使用交易時，憑證機構之認證與管理將是重要任務，經濟部應對憑證機構有一套明文的資訊安全規範，以確保使用者之權益。在網路犯罪處罰部分，我國刑法第 36 章已明文規定妨害電腦使用罪，可延伸規範網路犯罪。依刑法第 363 條之規定，第 358 條至第 360 條之罪，須告訴乃論，因此，須讓受害者瞭解自己的權利，若非個人提告，治安機關亦將無法受理辦案，故對於網路犯罪懲處之規範，宣導與教育是當務之急，適當網路教育與宣導可以降低網路犯罪率。

三、 技術面

對於技術層面建議主要有二：

(一)、推行憑證的運用於網際網路的認證程序上

現行網際網路的認證方式，多以設定帳號與密碼的方式來完成。但此方法已被證實可透過封包監聽以及暴力攻擊等手法來加以破解，甚至在網路上已有公開的工具可輕鬆破解存在於 Cookie 的帳號密碼。若業者提供服務時能夠結合電子憑證的身分認證方式，必能大幅降低網際網路服務遭盜用所衍生出的犯罪問題，以及追查上較為容易。

(二)、使用安全的無線網路資料傳輸安全加密機制

加強資料傳輸的私密性，如使用通道加密技術(WEP、WPA 等對於無線網路通道進行加密保護)與資料加密技術(使用 AES、DES

加密演算法對資料加密後才傳送)，以解決無線網路傳輸可能造成重要資料遭竊取及被盜用之可能。

四、 制度面

由於網路犯罪偵查過程牽涉到保全證據，故刑事程序上之搜索與扣押等強制處分有其必要性。因網路資料與證據易被毀損或銷毀，故此在制度上需有周詳之偵查規定，以利偵查人員取得相關證據。如歐盟之「網路犯罪公約」第 16 條規定電腦儲存數據之立即保全，可以使該負責儲存電腦數據資料者有維護與保存完整資料之義務，在最多不超過 90 天之必要期限內，遞交由主管機關取得。各締約國應採取必要的立法和其他措施，以責成電腦儲存數據資料之保管人或其他人，於國家所規定之訴訟期間內保守秘密。這規定不但牽涉到主管機關與負責人之權責，也涉及負責人員之專業性與對資料隱私保密之認知。電腦維護負責人須瞭解個人對資料保存與維護之重要性，與其須遵守之保密原則。故此在主管機關或相關機關人員專業與業務之「執行力」將是重要關鍵，有待相關機關重視與培訓。

既然保全資料儲存與維護是偵查過程重要的關鍵，其儲存與維護之成本將是主管單位與提供資料單位之重要考量因素之一，尤其私人企業網路服務提供業者。若為偵查之便利以法律規範資料保存與維護所需之基本期限，如六個月或一年期限等不同期限，將造成業者成本升高，因其包含設備、人力資安成本等，故若主管單位強調資料儲存與保護之時效重要性時，可能也需考量如何協助相關單位成本付出之代價，所以目前法律上對於不同資料之保存期限，會有不同等級之規定。這些分級依照不同等級資料設計出（如：系統登入紀錄、系統存取紀錄等）不同保存期限與所需基本人力之科技技術，以利降低網路服務提供業者在資料儲存與保全之成本，當然隨著網路科技發展，有需要時這些期限可以依照實際需求與情況來修訂。

再者，網路犯罪相關主管機關權責需分明，目前網路犯罪難以由單一機構完全解決，常需跨部會合作，甚至需跨國合作，因此在權責分配需有一套基本標準或法規，如個資法執行細則依法規定由法務部研擬，法務部可能須考量業者與政府機關不同角色與權限，加以明文規定不同機關之權責，以利日後推動個資法之執行。若已有網路犯罪事實，毋庸置疑將由檢調機關處理。負責主管機關除對於網路犯罪工具、場所需有一定之認知與專業技能之外，其處理案件之態度與觀念亦應隨資訊科技變遷而更新與進步。故此，相關人員培訓與職場再教育將是主管單位需要考量之

議題，這部分尤其需要重視在身分隱匿與竄改行為之預防以及證據之保留與確認。這些訓練與教育行為可讓大家認知網際網路便利性是一種工具與過程，而不是結果。也因此，不管政府、產業或是相關單位才不至於將把所有網際網路相關行為歸類給網際網路管理單位。例如各大學放置在網路的學生資料，一般由電子計算機中心相關單位維護，但管理學生資料權限需由教務處註冊單位負責。此外隨著科技進步以及使用方式，陷入犯罪者技術或手段是主管機關無法解決之現象，尤其目前網路犯罪往往牽涉到跨國之合作，因網路犯罪可跨國界，故相關業務執行者的外語能力將是不可或缺之條件，故主管機關在培訓人才或徵聘人員時，需將此外語能力列入考量合格專業人員資格之一。

在網路犯罪過程中，個人隱私權之保護是一重要項目。美國聯邦最高法院法官 Harlan 曾在 Katz v. United States 一案中的協同意見書中指出，所謂「隱私權的合理期待」包含兩部分：一是當事人之行為須反映出對隱私權真實(主觀)之期待(actual expectation of privacy)；二是該當事人對隱私權的主觀期待，須為社會上認為合理的 (society is prepared to recognize as “reasonable”)。雖然判斷兩者區分有困難，但其已兼顧到個人的期待與社會的觀感或合理認知與標準之間的相配合。例如專責電腦犯罪的刑事局偵九隊偵查員李昀儒表示，我國大小聊天室非常多，包括 UT 聊天室、尋夢園、豆豆聊天室、雅虎奇摩聊天室等，除雅虎奇摩等網站須先註冊個人資料才能登入，其他聊天室只要輸入暱稱即可進入，根本沒有認證與管控，導致歹徒可用匿名犯罪。因此，為避免青少年被騙，使用網路聊天室是否需制定認證制度值得思考，如韓國採取實名制度。我國在處理網路個人隱私時，也須兼顧到個人期待與社會觀感之合理性。

依上述，在制度面網路犯罪防制機制，可分為幾項：

1. 完善偵查制度：包含保全資料儲存與維護。
2. 完備網路犯罪破案考績制度：由於網路犯罪破案耗時且不易偵破，對於負責網路犯罪人員之績效考核制度，應有條件加以獎勵，以利增加員警破案與負責之意願。
3. 完善培訓計畫與制度：讓負責專業人力能在科技專業知識與技術能再教育，以利因應網路犯罪行為態樣。
4. 制定清晰的主管機關權責劃分之標準，如以事前預防、事中偵測及事後鑑識等區分各主管機關業務所需負責之作為

與工作，讓相關單位可以清楚瞭解各單位權責，以利網路犯罪偵防。

5. 個人隱私權之合理保護：讓使用者與負責人員瞭解隱私權基本保護原則與相關法規，以免觸法，造成被害人之損失。
6. 建立完備網路犯罪宣導制度，讓使用者與負責人員瞭解網路犯罪之嚴重性與相關刑責，減少網路犯罪之可能性。
7. 各機關須自訂一套防制網路犯罪機制，如法務部內部對透過網路向部會提出建言時，基本上是採非實名制，但若出現不當言論或毀謗時，經機關彙整並開會討論屬實時，將透過合法程序找出實際使用者 IP 位置，讓使用者對自我言論負責，並給加害者一個合理合法處罰，其制度兼顧保護使用者言論之自由與個人使用網路權利不受損害。

目前法規已足以因應匿名或竄改身分所導致相關網路犯罪行為，惟仍須在制度面強化，使整體防制犯罪體系更臻完備。如保全資料儲存與維護制度之建立；由於網路犯罪破案耗時且不易偵破，對於負責網路犯罪人員之績效考核制度，應有條件加以獎勵，以利增加員警破案與負責之意願。再則，訂定一套網路犯罪偵查人員培訓制度，以利讓負責處理網路犯罪專業人員能在科技專業知識與技術能再教育，以利因應網路犯罪行為態樣。這一部分配合主管機關以及相關管理單位人員之培訓，期在預防方面可以減輕偵查人員之負擔，在證據保留方面亦可以更有效率提供給偵查人員。除此，讓使用者與負責人員瞭解隱私權基本保護原則與相關法規，以免觸法致造成被害人之損失。政府須建立防制網路犯罪之宣導制度，讓使用者與負責人員瞭解網路犯罪之嚴重性與相關刑責，以減少網路犯罪之可能性。

五、 教育面

法律規範只能治標無法治本，唯有透過教育，才能根本地將網路犯罪防制機制落實。本研究建議透過教育部制定相關網路犯罪教育課程，從基礎教育如中小學開始進行「網路犯罪與法律」教學與網路犯罪防制之宣導，進而推動到高等教育，避免青年學子以匿名應用網路時，在未知網路犯罪相關規定之下誤觸法規，或是不知網路犯罪法規處罰之嚴重性，而意圖犯罪。除此，教師之培訓也相當重要，唯具有熟悉防制網路犯罪知能且深具教導能力之師資，才能有效傳遞、教導相關法規。法務部已有個人資料保護法種子教師培訓研習會，各校應該鼓勵老師參與，以利培訓相關優良師資以教導學生。透過網路犯罪防制教育之延伸與落實，將有助於降低網路犯罪之發生。

第四節　對於通傳會相關之建議

通傳會是我國通訊傳播的中央目的事業主管機關。依「國家通訊傳播委員會組織法」第 3 條條文指出通傳會掌理通訊傳播專業管制性業務，包含通訊傳播監理政策之訂定、法令之訂定、擬訂、修正、廢止及執行等事項，此外也包含通訊傳播事業營運之監督管理及證照核發等業務，通傳會扮演通訊與傳播市場的監督管理及執行相關政策之角色，主管第一、二類電信事業。就一般民眾所認知的網際網路中各服務提供者來說，通傳會主管 IASP，而 ICP、IPP 並非第一、第二類電信事業，是由各權責機關(如：經濟部、金管會、內政部警政署等)管理，故網際網路相關議題應視議題性質，由各權責機關主政。

根據本研究發現網際網路隱匿與竄改身分行為所引發之問題與現況及通傳會權責，提出通傳會在監理通訊與傳播市場之可能執行措施與建議：

(一)　強化與其他網路主管機關、業者之合作

對於網際網路匿名與竄改身分行為所產生之犯罪追查等問題，通傳會在行政部會與管理業界方面，可扮演積極主動的角色，透過建構跨部會會議或計畫性單位，如：由通傳會召集內政部、法務部、經濟部、交通部及金管會等組成「防制網路犯罪技術工作平台」（此工作平台雖由通傳會召集，但犯罪偵防工作仍是內政部警政署之職責），共同研議網路犯罪防制措施。建議此工作平台在必要時，除應由通傳會邀集所管電信事業參與外，仍得由其他行政機關視需要邀集 ICP、IPP 等相關業者共同參與，例如由經濟部邀集電子商務業者，以強化與其他網路主管機關、業者之連結與合作，共同打擊因匿名與竄改身分所導致之網路犯罪行為。同時，通傳會已經建構電腦危機處理中心(NCC-CERT)，亦可考慮強化其功能或利用其資訊分享與分析中心(NCC's Information Analysis and Sharing Center, NCC-ISAC)，強化區域聯防之合作架構與組織等，讓電信與資訊通訊服務業與政府合作，成為維護網際網路資通安全新的典範。

(二)　鼓勵所轄業者持續發展與採用相關防制技術

鼓勵業者持續發展與採用相關防制技術，如：IP 追查的技術、安全的傳輸協定、頻寬管理與即時告警、主動弱點管理、安全代詢伺服器名單及對其內部伺服器或使用者登入憑證身分認證技術(如 PKI 等機制)等。此一部分雖非通傳會主要權責範圍，但可透過與經濟部等其他網路主管機關進行橫向連結與溝通，共同推動獎勵或鼓勵其所轄業者持續發展與採用相關防制技術，讓所轄業者能夠善盡其管理責任，並有利於警調機關、業者本身追蹤與防制隱匿身分與竄改身分所造成之網路犯罪問題。

第七章　結論

本研究透過蒐集國際各國對於網際網路隱匿與竄改身分相關法律規範、專家學者對於此一議題相關意見與建議，彙整與分析後結論如下：

- 目前隱匿與竄改身分相關網路犯罪行為並無新的犯罪行為產生，而只是犯罪工具改變。因此，一方面在技術上必須注重各類系統與連線安全性，另一方面需保留連線紀錄提供追查。進一步具有認證身分之法規規範。國內已有相關法規規範網路犯罪行為，故本研究不建議針對此類行為修訂專法。現有法令中，亦不須要特別規範此類行為。因此在執行上，必須更加重視身分隱匿與竄改行為之預防，以及證據之保留與確認的培訓與教育，一方面可以讓執行單位能夠了解與使用網際網路相關科技，讓科技的進步能夠應用到好的方向；另一方面可讓大家認知網際網路便利性是一種工具與過程，因此不管政府、產業或是相關單位才不至於把所有網際網路相關行為歸類給網際網路管理單位。
- 現有網際網路隱匿與竄改身分行為之防制技術僅能局部地解決其行為所衍生的安全問題，故須配合相關的法律規範或管理規範，才能全面的解決隱匿與竄改身分相關網路犯罪行為。但這些法律規範或管理規範卻可能造成其他的問題，如侵害隱私、網路自由等。認證使用者身分方式，如實名制，可以妥善防制隱匿與竄改身分行為。但卻可能部分侵害網路自由與個人隱私，民眾接受意願低。且實施「實名制」時除須改變現有網路機制外，對於實名的登記機制，成本偏高；且在申辦網路連線的過程中，採用登記制，也促使我國實施部分實名制，故專家學者及研究結果均認為現階段我國不適合實施。
- 本研究所提之相關防制技術與機制，現有法令已足夠配合與協助執行相關機制，惟對於相關機制與法令的宣導及執行面，仍須強化。
- 利用隱匿與竄改身分所遂行的網路犯罪行為會對追緝造成困難，其困難點來自追緝的過程中，所留存的紀錄痕跡不足，造成無法持續追緝犯罪者。而解決方案可透過對於紀錄留存的要求及服務提供者資安技術的採用等來強化追蹤

痕跡及避免紀錄的不足。另一困難點，為追緝犯罪者的過程，遇到跨國法治管轄的問題，此一部分，有賴透過跨國合作之方式，由政府相關單位主動建立相關合作管道，才能有效解決此一問題。

- 網路犯罪相關主管機關權責需分明，目前網路犯罪難以單一機構可以完全解決，常須跨部會合作。網路犯罪的偵查，尚須完善培訓計畫與制度，讓負責專業人力能在科技專業知識與技術能力再教育，以利因應網路犯罪行為態樣。
- 現有的網際網路隱匿與竄改身分行為與其防制技術與機制已經有相關的法令規範足以協助追查及預防，且民眾較缺乏的是對於這些追查機制、配套法規的認知、理解與執行，而非新法規。因此，本研究認為尚不須制訂或修訂相關的配套法規，而是透過社會、法律宣導、技術、制度與教育等來強化其防制技術與機制。(請參見第六章說明)
- 法律規範只能治標無法治本，唯有透過教育才能將網路犯罪防制機制落實。本研究建議透過教育部制定相關網路犯罪教育課程，從基礎教育如中小學開始進行「網路犯罪與法律」教學與網路犯罪防制之宣導，進而推動到高等教育，避免青年學子以匿名應用網路時，在未知網路犯罪相關規定之下誤觸法規，或是不知網路犯罪法規懲處之嚴重性，而意圖犯罪。
- 建議通傳會強化與其他網路主管機關、業者之合作，這部分通傳會在行政部會與管理業界方面，可扮演積極主動的角色，透過建構跨部會會議或計畫性單位，如：由通傳會召集內政部、法務部、經濟部、交通部及金管會等組成「防制網路犯罪技術工作平台」，共同研議網路犯罪防制措施。建議此工作平台在必要時，除應由通傳會邀集所管電信事業參與外，仍得由其他行政機關視需要邀集 ICP、IPP 等相關業者與主管機關共同參與。同時，通傳會已經建構電腦危機處理中心(NCC-CERT)，亦可考慮強化其功能或利用其資訊分享與分析中心(NCC's Information Analysis and Sharing Center, NCC-ISAC)，強化區域聯防之合作架構與組織等，讓電信與資訊通訊服務業與政府合作，成為維護網際網路資通安全新的典範。此外也能藉此鼓勵業者持續發展與採用相關防制技術，方能建構更能夠安全的網際網路環境。

參考文獻

[1] “18 U.S.C. § 1030 : US Code - Section 1030: Fraud and related activity in connection with computers”, http://codes.lp.findlaw.com/uscode/18/I/47/1030 。 (瀏 覽 日 期:2011/01/15)

[2] “Open Proxy Server Mechanism”, http://www.aboutonlinetips.com。(瀏 覽 日 期:2010/11/08)

[3] “The Cybersecurity Series”, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm。(瀏 覽 日 期:2010/12/02)

[4] “The MIT ANA Spoofer Project”, http://spoofer.csail.mit.edu/index.php。(瀏 覽 日 期:2010/11/08)

[5] “The Platform for Privacy Preferences”， http://www.w3.org/P3P。(瀏 覽 日 期:2010/12/02)

[6] “Tor Project: Anonymity Online”, http://www.torproject.org. (瀏 覽 日 期:2010/11/10)

[7] Anonymous speech, http://itlaw.wikia.com/wiki/Anonymous_speech 。 (瀏 覽 日 期:2011/01/08)

[8] D. E. Comer, D. L. Stevens: Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture, 4th edition, Prentice Hall, 2000.01.

[9] E. Maiwald: Fundamentals of network security, McGraw-Hill, 2003.11.

[10] L. E. Cohen and M. Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach”, American Sociological Review, 44: pp:588-608, 1979.

[11] MediaWiki：電腦犯罪， http://www.pmsh.tnc.edu.tw/~wiki/98106/index.php/電腦犯罪。 (瀏 覽 日 期:2010/10/30)

[12] Speech: Anonymity, http://ilt.eff.org/index.php/Speech:_Anonymity。 (瀏 覽 日 期:2010/11/10)

[13] TREND MICRO: ARP Spoofing 攻擊示意圖, http://www.trendmicro.com.tw。(瀏 覽 日 期:2010/11/08)

[14] TRUSTe，http://www.truste.org。(瀏覽日期:2010/11/10)

[15] United Nations：UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, New York: United Nations Publication, 1999.

[16] 丁秋玉：網路犯罪證據之搜索扣押研究，中央警察大學法律研究所碩士論文，2002/06。

[17] 內政部警政署：警政統計通報，http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=54699&ctNode=11393&mp=1。(瀏覽日期:2010/10/20)

[18] 內政部警政署刑事警察局：犯罪預防寶典，第七篇第三章 電腦與網路犯罪預防，http://www.cib.gov.tw/crime/Crime_Book_Content.aspx?chapter_id=0000007&rule_id=0000003，2010/12。

[19] 王怡惠：德國電信服務法下訊息儲存服務提供者之法律責任。科技法律透析，7月， 15-21頁，2008。

[20] 王勝毅：網際網路上犯罪行為之研究，中國文化大學法律學研究所碩士論文，2000/12。

[21] 立法院國會圖書館：外國法案介紹-著作權法，http://npl.ly.gov.tw/do/www/billIntroductionContent?id=39# 日本。(瀏覽日期:2010/11/15)

[22] 全國法規資料庫：http://law.moj.gov.tw/index.aspx。

[23] 行政院國家資通安全會報：無線網路網路安全會議紀錄，http://www.nicst.nat.gov.tw/include/getfile.ph?pfid=22，2005。(瀏覽日期:2010/10/30)

[24] 行政院國家資通安全會報技術服務中心：建立我國通資訊基礎建設安全機制計畫，2007。

[25] 行政院國家資通安全會報技術服務中心：資通安全法律案例宣導彙編第6輯，2008。

[26] 行政院經濟建設委員會：網際網路法制計畫，2002。

[27] 余啟民：國際電子簽章法相關立法發展趨勢之淺析：http://gcis.nat.gov.tw/eclaw/e28_Body.asp?PageCode=docu_2_06。

[28] 李永峰：韓國明星崔真實自殺引爆爭議-實名上網打擊謠言也限制自由，亞洲週刊。

http://www.iasiaweekly.com/archives/650 ， 2008 。 (瀏 覽 日 期:2010/10/30)

[29] 李 茂 生 ： 我 國 電 腦 網 路 犯 罪 的 虛 像 與 實 ， 刑 事 政 策 與 犯 罪 研 究 論 文 集 （ 四 ） ， 法 務 部 犯 罪 研 究 中 心 編 印 ， 2001/11 。

[30] 林 宜 隆 、 李 璘 昱 、 劉 金 和 、 莊 育 秀 、 許 盛 凱 ： 不 當 資 訊 防 治 政 策 與 管 理 策 略 之 初 探 ， 台 灣 網 際 網 路 研 討 會 論 文 集 (二) ， 2003 。

[31] 林 宜 隆 、 賀 宙 才 、 張 翔 舜 、 林 子 豪 ： 我 國 網 路 現 況 分 析 與 對 策 — 以 刑 事 警 察 局 網 路 犯 罪 偵 查 案 例 作 分 析 ， 網 址 ： http://jitas.im.cpu.edu.tw/2007-1/1.pdf 。

[32] 林 宜 隆 、 黃 讚 松 ： 網 路 使 用 問 題 分 析 與 犯 罪 預 防 之 探 討 ， 資 訊 、 科 技 與 社 會 學 報 ， 第 2 卷 2 期 (3) ， 2002 。

[33] 林 宜 隆 : 網 路 犯 罪 之 案 例 分 析 ， 中 央 警 察 大 學 學 報 ， 第 37 期 ， 2000 。

[34] 林 宜 隆 ： 網 路 使 用 犯 罪 問 題 與 網 路 安 全 管 理 之 探 討 ， 中 央 警 察 大 學 學 報 ， 第 32 期 ， 1998 。

[35] 林 承 宇 ： 網 際 網 路 有 害 內 容 管 制 之 研 究 。 廣 播 與 電 視 ， 第 十 八 期 ， 91-114 頁 ， 2002 。

[36] 林 易 典 ： 德 國 民 法 債 編 修 正 之 重 點 ， 政 大 法 學 評 論 ， 第 七 十 九 期 ， 116-149 頁 ， 2004 。

[37] 林 長 毅 、 蔣 大 偉 ： TCP/IP 網 路 管 理 (第 二 版) ， 美 商 歐 萊 禮 圖 書 ， 2000/09 。

[38] 林 建 中 ： 隱 私 權 概 念 之 再 思 考 — 關 於 概 念 範 圍 、 定 義 及 權 利 形 成 方 法 ， 國 立 臺 灣 大 學 法 律 研 究 所 碩 士 論 文 ， 1999 。

[39] 林 富 郎 ： 通 訊 監 察 法 制 化 之 研 究 ， 國 立 中 正 大 學 法 律 研 究 所 碩 士 論 文 ， 1999 。

[40] 邱 琳 雅 ： 財 團 法 人 金 融 聯 合 徵 信 中 心 法 務 小 組 ， 德 國 聯 邦 個 人 資 料 保 護 法 (BDSG) ， 財 團 法 人 金 融 聯 合 徵 信 中 心 ， 97/10, http://www.jcic.org.tw/publish/2009m08_12.pdf

[41] 邱 琳 雅 ： 德 國 聯 邦 個 人 資 料 保 護 法 （ BDSG ） ， 金 融 聯 合 徵 信 雙 月 刊 ， 第 八 期 ， 60-65 頁 ， 2009 。

[42] 柯 立 明 、 林 峻 立 ： 網 路 釣 魚 問 題 之 研 究 ， 資 通 安 全 專 論 ， 2008 。

[43] 美國愛國者法（USAPA）：http://news.findlaw.com/hdocs/terrorism/hr3162.pdf。(瀏覽日期:2011/01/10)

[44] 胡惠生：全球首條網上犯罪國際公約，資料來源：http://www.gamez.com.tw/viewthread.php?tid=74710，2001。(瀏覽日期:2010/10/20)

[45] 計世網：國外網際網路管理經驗分析，http://www.lanecat.tw/news/20071224.asp，2007。(瀏覽日期:2011/01/10)

[46] 徐振雄：電子商務政策與法律理論初探，通識研究集刊，第14期，頁73-92，2008。

[47] 財團法人台灣網路資訊中心：IPv6 安全技術，新一代網際網路協定互通與認證計畫，2009。

[48] 財團法人台灣網路資訊中心：個人應用之網路安全，網際網路趨勢研討會，2008。

[49] 財團法人金融聯合徵信中心：日本個人資料保護法案介紹，http://www.jcic.org.tw/publish/020603.doc。(瀏覽日期:2011/01/25)

[50] 高玉泉：歐盟有關網路內容管制之政策及原則，傳播與管理研究，第一卷第一期，南華大學傳播管理研究所，http://www.nhu.edu.tw/~media/_periodical/0101/010101.pdf，2011/03/30。

[51] 張志宗：我國高科技犯罪偵查能量之研究-以網路犯罪為例，華梵大學資訊管理學系碩士論文，2009。

[52] 張錦俊：美國與歐盟個人資料隱私政策差異與整合，資通安全專論，2007。

[53] 張錦俊：歐洲理事會網路犯罪公約檢析，資通安全專論T98021，國家實驗研究院科技政策中心，2009。

[54] 張耀中：從歐盟「資料保存指令」看我國資料保存之規範，http://www.ithome.com.tw/itadm/article.php?c=39970，2006/10/19。(瀏覽日期:2010/11/10)

[55] 教育部教育 wiki：網路犯罪，http://content1.edu.tw/wiki/index.php/網路犯罪。(瀏覽日期:2010/09/12)

[56] 章忠信：美國一九九八年數位化千禧年著作權法案簡介，萬國法律，http://www.copyrightnote.org/paper/pa0010.doc，第107期，1999。

[57] 郭戎晉：網路實名制與電子商務安全機制之法制研究，資通安全專論，2009。

[58] 郭佳玫、陳人傑：從德國法談濫發商業電子郵件之規範，科技法律透析，23-60頁，2008/08。

[59] 郭佳玫：從德國判決談網路言論經營者對他人言論責任之轉變，科技法律透析，31-45頁，2009/01。

[60] 郭和杰：08年美國網路犯罪增加三成，IThome Online, http://www.ithome.com.tw/itadm/article.php?c=54208。(瀏覽日期:2010/11/08)

[61] 陳韋金：IP 追蹤教學，財團法人台灣網站分級推廣基金會，http://www.ticrf.org.tw/chinese/download/IPteach.pdf。(瀏覽日期:2010/12/24)

[62] 陳欽賜：網路犯罪與偵防對策之研究，逢甲大學公共政策研究所碩士論文，2007/08。

[63] 陳憲政：電腦犯罪之法律適用與立法政策，國立政治大學法律學研究所碩士論文，2006/12。

[64] 彭開英：從美國消費者個人資料保護法規看我國消費者個人資料保護之法律規定(上)，http://proj3.moeaidb.gov.tw/nmipo/content/viewcontent.aspx?sn=DDED5F28E25C41338E705E5A26143CB5#Scene_1。(瀏覽日期:2011/03/30)

[65] 曾百川：網路詐欺犯罪歷程之質化研究，中央警察大學犯罪防治研究所碩士論文，2005。

[66] 馮震宇：網路犯罪與網路犯罪公約（上）、（下），月旦法學教室，第4期、第5期，2003。

[67] 黃育勳：電腦之搜索扣押，國立臺北大學法律研究所碩士論文，2001。

[68] 黃詣翔：網路匿名性的研討分析，http://www.shs.edu.tw/works/essay/2009/03/2009033112244675.pdf，2009。(瀏覽日期:2010/12/24)

[69] 黃讚松：從情境犯罪預防理論探討網路犯罪預防對策之研究，中央警察大學碩士論文，2009年。

[70]楊永年、楊士隆、邱柏嘉、李宗憲：網路犯罪防治體系之政府職能與角色分析，行政院研究發展考核委員會委託研究報告，2009/12。

[71]楊永年：網路犯罪防治體系之政府職能與角色分析。行政院研考會委辦臺灣公共治理研究中心，2009。

[72]經濟部：台日韓電子商務法治資訊網，http://gcis.nat.gov.tw/eclaw/tjk/chinese/tjk_tw_body.asp?PageCode=tw_page3，2008/08/15。(瀏覽日期:2011/01/10)

[73]經濟部：電子商務活動之個人資料之保護，台日韓電子商務法治資訊網，http://gcis.nat.gov.tw/eclaw/tjk/chinese/tjk_tw_HotNewsView.asp?sno=OX%5DP。(瀏覽日期:2010/12/05)

[74]經濟部全國工商行政服務入口處：韓國電子商務法治環境-電子商務法治推動過程，http://gcis.nat.gov.tw/eclaw/tjk/chinese/tjk_tw_body.asp?PageCode=kr_page1。(瀏覽日期:2010/11/15)

[75]電子商務資安通報服務中心檔案下載服務，http://ec-cert.org.tw/content/application/eccert/document/guest-cntgrp-browse.php?vars=3e83390f4d53e5353ca24c84e2b17eeeff397a170683a9f99f622444a9d0e3e3965c77b144ca17a466983a7d0cece4ca99156d20814a3624226c3b5abf23e3427b05ccdf0f672ff0504322542eb2d0aa。(瀏覽日期:2011/04/25)

[76]電腦及網路犯罪分析：電腦及網路犯罪分析，http://www.internet-recordor.com.tw/crime.html。(瀏覽日期:2010/10/30)

[77]翟本瑞：逃到網中：網路認同形成的心理機制研究，第四屆資訊科技與社會轉型研討會，2001。

[78]劉敏慧：個人隱私系列之一-網路安全與隱私權的衝突，國家資通安全會報技術服務中心，2008。

[79]劉敏慧：個人隱私系列之五-個人隱私資料保護與實務建議，國家資通安全會報技術服務中心，2009。

[80]劉靜怡：網際網路時代的資訊使用與隱私權保護規範：個人、政府與市場的拔河，資訊管理研究，第 4 卷，第 3 期，2002。

[81]數位時代：韓國網路誹謗法上路 YouTube 韓國站取消匿名者上傳與留言的權利，

http://www.bnext.com.tw/focus/view/cid/1/id/1834，2009/04/12。

[82]歐盟網路犯罪公約（Convention on Cybercrime），http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm。

[83]潘維大、成永裕、葉奇鑫、法思齊、徐育安：網路犯罪「數位證據」蒐集保全程序與相關證據法則之探討，法務部委託研究案，2008。

[84]蔡宛宜：保護個人隱私從修改瀏覽器設定做起，國家資通安全會報技術服務中心，2010。

[85]蔡懷卿：電腦犯罪問題－美國刑事立法之參考，刑事政策與犯罪研究論文集(二)，法務部犯罪研究中心編印，1999/05。

[86]賴文智、顏雅倫：第七講:日本不正競爭防止法。益思科技法律出版，http://www.is-law.com/old/OurDocuments/BOOK1000-8.pdf ，2010/03/12。

[87]錢世傑：網路通訊監察法制與相關問題研究，中原大學財經法律系碩士論文，2002。

[88]謝立功：通訊保障及監察法第五條之探討，http://www.npf.org.tw/post/1/901，2007/02/07。

[89]簡榮宏、廖冠雄：無線區域網路，全華科技圖書，2007/01。

[90]嚴書貞：德國的電子商務市場，http://218.246.21.135:81/gate/big5/gjdzsw.drcnet.com.cn/gjdzsw/DocView.aspx?docid=2429870&leafid=14480&chnid=1070，2010/12。

[91]騰訊網：歐盟推網際網路隱私保護新規 針對 Facebook 等，http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/internet/2010-11/05/c_12743253.htm，2010/11。