電腦稽核
Computer Audit Association 民國110年02月26日 第43期
ISACA Taiwan Chapter

Innovative technologies and applications of smart governance in continuous auditing

智慧治理在持續性稽核之創新技術與應用

論人工智慧與隱私權保障之研究
－現代科技與資訊隱私權之拉鋸戰

探討網路寫手之偵測方法與研究

視覺化與機器學習協同整合之增強分析
—以風險視覺化為例

Evolution of Smart Governance - The Past, Present and Future of Governance and Auditing

資訊及相關技術的管理、控制與稽核(COBIT)於政府部門

資訊安全其治理稽核之落實

編 輯 序

正當全球掀起數位化、智慧化熱潮的同時，也讓急於突破現況的企業面臨了嚴峻的挑戰，而思考如何創新專業領域技術與相關應用就成為了重要的議題。智慧治理是一項新興領域，目前已在全球的銀行、零售、醫療、教育、農業、能源、科技 … 等各領域，激起前瞻性之研究與創新應用。尤其，在智慧化物聯網設施與資訊系統的整合下，更加速地催生電腦稽核新興技術之發展。智慧治理開創了電腦稽核的新應用時代，也讓內部控制與風險管理的作為有了更先進、更完善的控管機制及功能。

持續性稽核的核心目標，是強調應用數位化技術來提供即時、準確的查核作業與流程、以及產出客觀的稽核報告。持續性稽核過程強調快速、精準地呈現組織內所發生的事實、狀況、以及對潛在風險產出評估報告，其活動是確保組織內部控制、管理風險的核心作為，也是防治舞弊的重要活動。在智慧治化技術的整合下，期待能為組織及個人帶來創新與應用的契機，同時也讓稽核作業在一定規範中持續、穩健地被進行，讓組織能因適度的控管得以立足在數位化、智慧化的時代。

綜上所述，電腦稽核期刊第四十三期以「 智慧治理在持續性稽核之新技術與創新應用 」議題為主軸，邀請國內外學者與專家，提出具創新性與實用性論文，討論相關應用的機會與挑戰，以及思考如何運用智慧治理之新技術讓組織的稽核作業可以持續改善及發揮應有的成效。本期收錄文章內容理論和實務並重，包括「 論人工智慧與隱私權保障之研究 - 現代科技與資訊隱私權之拉鋸戰 」、「 探討網路寫手之偵測方法與研究 」、「 論人工智慧及電子監控之研究 」、「 視覺化與機器學習之人機協同之整合 」、「 Evolution of Smart Governance -The Past,Present and Future of Governance and Auditing」，新知分享方面則有「 應用資訊及相關技術的控制目標 (COBIT) 於政府部門 」、「 資訊安全其治理稽核之落實 」。希望透過優質文章的收錄，來啟發讀者的關注與研究興趣，進而為資訊治理與電腦稽核領域帶來更成熟之發展

此期特別邀請國立台灣大學會計系蔡揚宗名譽教授，擔任第四十三期客座主編，共同為電腦稽核期刊帶來更加精采豐富的內容。感謝各位作者賜稿及協會秘書處之協助、各位審稿委員的細心審閱。本期期刊若有不盡之處，敬請各位先進賜教。

張碩毅

國立中正大學　管理學院院長

編譯出版委員會主任委員

蔡揚宗

國立台灣大學名譽教授

CAA 電腦稽核
Innovative technologies and applications of smart governance in continuous auditing
第 43 期

目 錄
CONTENTS

編輯序

專業論壇

04 論人工智慧與隱私權保障之研究
－現代科技與資訊隱私權之拉鋸戰
- 許淑媛

25 探討網路寫手之偵測方法與研究
- 曾韵

42 視覺化與機器學習協同整合之增強分析
—以風險視覺化為例
- 孫嘉明、黃學昌

57 Evolution of Smart Governance
- The Past, Present and Future of Governance and Auditing
-TSE W K Daniel、SHI Rong

新知園地

67 資訊及相關技術的管理、控制與稽核 (COBIT) 於政府部門
- 作者：Panduranga Bichal
譯者：魏銷志

72 資訊安全其治理稽核之落實
- 余俊賢、黃榮鐘

會務交流

82 協會簡介

84 2020 年 7-12 月 CISA CISM Exam Passers

85 2020 年 9-12 月教育訓練課程
89 電腦稽核期刊前期篇名
90 近期活動報導
98 ISACA 國際證照簡介

發 行 人：葉奇鑫
總 編 輯：張碩毅
客座編輯：蔡揚宗
編輯委員：溫大民、李興漢、孫嘉明、徐立群、黃劭彥、張益誠、劉其昌、邵之美、諶家蘭
執行編輯：呂芝嫻
封面提字：林志雄
秘 書 長：黃淙澤
秘　　書：何慈雯、許秀玲

出版單位：中華民國電腦稽核協會
展 售 處：中華民國電腦稽核協會
地　　址：11070 臺北市基隆路一段 143 號 7 樓之 4
電　　話：(02)2528-8875
網　　址：https://www.caa.org.tw

視覺設計：品晟股份有限公司
印　　刷：品晟股份有限公司

發行日期：110 年 2 月 26 日
定　　價：新臺幣 250 元

論人工智慧與隱私權保障之研究
－現代科技與資訊隱私權之拉鋸戰

On the Study of the AI Regarding the Protection of the Privacy.
-The Fighting between Modern Technology and the Information Privacy Right.

許淑媛Cadalina Hsu
大洋法律事務所執行長
國立臺灣大學法學士及碩士
中正法博士候選人
C.E.O. at Da-Young attorney-at-law firm
B.A.&M.A at NTU, P.H.D. Candidate at CCU.
hsucadalina@gmail.com

摘　要

全球因為人工智慧之發達而開創了近代科技的新紀元，同時也衍生了許多耐人尋味的法律問題，隨著資訊科技的進步與網路上商業活動，各式各樣關於資訊隱私權的保障問題層出不窮，故隱私權受保護的領域有延伸之必要性。由於人工智慧日新月異，隨著數位科技的蓬勃發展，縮短了人與人間的距離，早就成為了目前的全球趨勢，而電腦資訊系統龐大的資料處理能力，也讓一切運作變得更為迅速。可是在虛擬的世界中資訊隱私權保障卻明顯不足，故又有學者稱資訊隱私是人工智慧最

為幽暗的領域之一，正因為大多數的人雖身處數位科技時代，卻在便民服務、經濟利益等力量的趨勢下，對個人資訊隱私權被侵蝕殆盡毫無所知。

目前愈來愈多的服務提供電子 E 化、電子商務等，運用了電腦科技所形成的資訊生活形態，文化素養及生活品味也更豐富化與多元化。但如何面對人工智慧科技問題，以及如何保持科技發展並兼顧資訊隱私保障，探討數位科技發展現況對於個人資訊隱私權之侵害問題則是本論文之中心，藉由美國法與歐洲指令之觀察，與多年來實務見解及實務上處理相關隱私權受侵害之解決方式，希冀在學術上得以拋磚引玉及參考借鏡。

關鍵字：人工智慧、隱私權保障、資訊隱私、個人資訊自主權。

Abstract

To embrace a new era of Artificial Intelligence(AI), the development in such a modern technology derives many thought-provoking legal questions, such as the right to privacy of information protection. With the advance of information technology and commercial activity on the internet, a wide variety of matters concerning the information privacy have raised.Therefore, the protection of the right of privacy has necessarily extended. Due to the progress of AI accompanying with flourishing digital technology development, current trend through this shortens the distance between people. The operating proficiency of the computer-based information systems is great, making everything works faster; however, the right to privacy of information protection in reality is obviously insufficient. Therefore, the information privacy is a new developing technology and standardizes in the category. Since most people live in this scientific and technological era, the very little bit of personal information would be revealed under the trend of the handy service and economic benefit without notice.

More and more services offer as electronic E, e-commerce by utilizing information lifestyle from the computer technology. Hence, cultural literacy and tastes not only enrich but also vary our lives on account of the comprehensive change and facility of AI. How to tackle with the issues of AI and keep on both technology development and information privacy is an important lesson. This paper focuses on the issues of the information infringement pertaining to the digital technology development.By analyzing those verdicts and cases in U.S.A. and Taiwan, it's essential to learn how to keep the development of AI and give consideration to the personal information protection, infringement of the right of

privacy when dealing with these problems in AI.I hope this paper can bring of tremendous devotion in the legal field.

Keywords: Artificial intelligence, The protection of privacy right, Information privacy, Information autonomy.

壹、人工智慧與隱私權之關係

一、我國隱私權之涵義[1]

隱私權就個人有無要求不受侵擾之權利，在個人生活的領域內，是否存在著一個由個人自主的空間，公共權力或他人不得任意加以干涉或侵擾。如果有的話，這個空間的內容和範圍如何？在法律體系中，對這個空間的權利應如何看待，如何定位？這是本文所欲深究的主題。個人領域不受干涉的權利，在權利體系中，原應屬於個人自由的範圍。不論從天賦人權或法律創設的立場，自由原本即是法律保留與個人的自主空間。然而自由的概念發展至今，已經十分廣泛而難以掌握，在政治事務、經濟事務，乃至於個人生活，均存在著自由的主張。而個人領域不受干涉的權利，只是自由概念下較為具體的一個部分，所以對此一部分之探討，應該有其更為特定明確之客體和概念。

首先，本文將隱私權定義為「對個人領域內事務的控制權」。以「私人的」和「公共的」區分為基礎，界定隱私為「個人領域內的事務」，表明其與公共事務或他人利益的區別。強調控制權，則在表明個人之自主性。就權利體系地位而言，隱私權屬於自由的下位概念，是對個人領域內事務的自由。其次，隱私權保障的是個人的人格和尊嚴，是精神上的利益。再次，隱私權以個人領域為範圍，所以其界限就是公共利益和他人利益[2]。本文即以上述論點為基礎建構而成。

二、美國法隱私權之涵義[3]

「隱私權」自始被界定為「不受干擾」的權利（Right to be let alone)，其內涵自最初侷限於個人資訊不被揭露的要求，逐步擴及今日個人事務的自主權，與本文所欲探究的客體尚屬相當，因此，本人仍採用「隱私權」做為探討客體的名稱，並依循美國法學上的發展做為說明探討客體的例證[4]。

首先，在內容上為隱私權的淵源及發展，包括最初概念的提出、學者的討論、在美國侵權行為法上的肯定，立法上的創設，到被提升至憲法權利的經過。其次，提到四種隱私權的保障內容，包括因非法搜索扣押造成之隱私權侵害，個人空間的隱私權、資訊的隱私權，以及對於個人事務容主要是按照案例和立法中已經出現之事實歸納而得，提出保障隱私權的基礎理論，以個人

1. 王澤鑑，人格權保護課題與展望（三）- 人格權的具體化及其保護範圍 (6) 隱私權篇（上），台灣本土法學第 96 期。
2. 王郁琦，網路上之隱私權問題，資訊法律透析第 8 卷第 10 期，88 年 10 月。
3. 邱志偉，隱私權政策現況與展望 - 以美國為中心，東海大學法律研究所碩士論文，2019 年 1 月。
4. Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920).

尊嚴為主要的保障理由，從公共利益、他人利益、和本人同意三個方面劃定隱私權的界限，並在利益衝突時提出解決的標準。最後對我國現行法律制度中有關隱私權的規定加以介紹和討論，並提出建立隱私權法制之建議。[5]同時，提供現今社會當人工智慧及隱私權發生衝突時，有法律規範可以強制處理，例如刑法上關於「秘密」之規定散見於國家及個人法益等條文中，其中妨害秘密罪所稱之「秘密」，至少包括下列3要件：**(一)資訊之非公開性：**即非一般人所知悉之事或僅有特定、限定少數人知悉之資訊；**(二)秘密意思：**本人不欲他人知悉該資訊；**(三)秘密利益性：**即從一般人之客觀觀察，本人對該秘密有財產上或非財產上保密之價值或擁有值得刑法保護之利益。換言之，妨害秘密罪章所謂之「秘密」係指依本人之主觀認知，不希望自己或特定、限定少數人以外之人能夠知悉之資訊，若此資訊受侵害時必對本人產生一定之影響力，即具有保密之價值或利益，始為刑法所保護之秘密。故除本人對於該資訊明示為秘密外，如在客觀上已利用相當環境、設備，或採取適當之方式、態度，足資確保其活動之隱密性，一般人均能藉以確認本人主觀上具有隱密性期待，而無誤認之虞者，譬如將欲保密之資訊放置於非他人得輕易查覺之處所，或將欲保密之資訊對知悉者簽訂保密條款均屬之。而刑法第317條洩漏工商秘密罪係以行為人洩漏業務上知悉依法令或契約應保密之工商秘密為其構成要件，至所謂「工商秘密」指工業或商業上之發明或經營計畫具有不公開之性質者，舉凡工業上之製造秘密、專利品之製造方法、商業之營運計畫、企業之資產負債情況及客戶名錄等均屬之[6]。

三、人工智慧之法律依據

Artificial Intelligence(簡稱AI)，中文大部分翻譯成「人工智慧」，最為人所知的可能是2014年開始，由英國倫敦Google Deep Mind開發的人工智慧圍棋軟體AlphaGo。AlphaGo贏過人類棋士一戰成名後，法律領域內對人工智慧的關注也一夕遽增。[7]目前我國法律並沒有明確的定義「人工智慧」，不過內政部依國籍法第9條第5項訂定的歸化國籍之高級專業人才認定標準中，第2條明確指出人工智慧屬於高級專業種類之一，在人工智慧方面具有獨到才能或有傑出研發設計的外國人士，可以在不提出喪失原有國籍證明的情況下申請歸化我國，所以這裡的人工智慧屬於不確定法律概念。[8]

四、AI侵害隱私權之情形

人工智慧的發展大致可以區分成三個階段，工具、協力、自主創作甚至和人類競爭。還在工具階段的AI如果造成侵權行

5. Whalen v. Roe, 429 U.S. 589 (1977).
6. 最高法院109年度台上字第2709號刑事判決參照。
7. 資策會產業情報研究所，工業機器人未來五年需求穩定看漲，2017年10月11日，取自資策會產業情報研究所官網：https://mic.iii.org.tw/IndustryObservations_PressRelease02.aspx?sqno=450，最後瀏覽日：2019年8月20日。
8. 張文貞，聯合國人權兩公約—公民與政治權利國際公約、經濟社會文化權利國際公約，財團法人台灣新世紀文教基金會，台灣聯合國研究中心，2014年8月。

為，必須要由創造或使用 AI 的自然人負責應該還算直觀，但如果是已經到達可以自主創作程度的人工智慧系統侵害他人權利，仍然要求創造或使用的自然人，為人工智慧系統的行為負起絕對責任，會不會有問題呢？舉一個例子來跟大家說明，我們先暫且不討論 AI 能不能主張言論自由，以及言論自由到底是為了保障表意人，還是閱聽大眾資訊獲知權的問題[9]，假設有一間公司發展出會自己蒐集資訊、撰寫新聞的 AI，在這個 AI 運作下產生了一篇誹謗某個公眾人物的新聞，使該名公眾人物名譽受損，可是設計 AI 的工程師可能僅僅下了「搜尋和主題相關的資料」、「撰擬新聞」等指令[10]，這時候仍然應該由設計 AI 的工程師負全部責任嗎？值得我們思考。

貳、人工智慧對隱私權之影響

一、人工智慧與基本人權[11]

史丹佛大學的研究人員曾經在《性格與社會心理學期刊》發表一份研究，研究結果顯示他們成功運用人工智慧技術，單由相片就可以辨識出相片主角是不是同性戀，當時引發軒然大波。Facebook 屢次被抨擊放任演算法運作，租屋廣告可以排除有色人種用戶、女性用戶只會接收到低薪工作的招聘廣告，造成種族、性別歧視。這些都是 AI 技術運用下可能產生的人權問題應該受到國際人權法的約束。

另外，如果 AI 可能涉及的人權問題應該由政府和法規介入管理，又應該在什麼時候、以何種程度和方式介入，如果不從開始設計 AI 時就納入相關規範，仍舊只能在造成傷害之後亡羊補牢。但 AI 業者認為如果在設計之初就管太多，會拖延 AI 技術發展，也可能會有商業機密外洩的風險。到底應該什麼時候管、管多少、如何管，考驗著政府和立法者的能力與智慧，AI 技術是未來科技趨勢所向，人工智慧在生活中的應用只會愈來愈普遍，面對新科技可能帶來的法律問題，我們的政府和立法者準備好了嗎？

(一) 問題提出

瞭解機器學習及逐漸增加的個人資料對個人自由及隱私、同意等概念可能帶來的影響為何。政府必須確保資料被儲存在正確的地方，並以適當的方式進行處理及控管。針對人工智慧所為的決策調適之概念及機制。確保 AI 系統可隨時檢核並具有合規則性，能夠被一再地、安全地被人類監督者打斷，而非學習如何避免或操縱該等介入。確保演算法決策過程之透明度、可解釋性以及數據偏見的最小化。政府應當召集業界、非官方組織及最終消費者等利害關係人共同進行對話，一方面有助於建立起公眾的信任及接受度、解決可能的誤解，另一方面亦可透過公開對話即時處理相

9. 馬興平，論資訊隱私權的保護—從釋字第 603 解釋出發，國立中正大學，2008 年。
10. 張永明，再探隱私權之自由 - 狗仔跟拍之憲法議題 - 評司法院釋字第六八九號「狗仔跟拍」之解釋，月旦法學雜誌第 197 期。
11. 陳進忠，隱私權之研究，國防大學管理學院法律學系碩士論文，2014 年 5 月。

關社會、法律及倫理議題。[12]

(二) 歷史反思

從 AI 演化過程的改變，進而勾勒出這六十年來變革體系的圖像，民主社會該如何避免成為演算法社會、黑箱社會，如何界定資訊受託者的責任，都有賴法律課予演算法使用者公共責任，讓 AI 受到法律系統的評價，針對憲法現存問題的解決與日後問題的防範。人工智慧的發展共有三個高峰 : 推理、知識、學習，今日的成果是人工智慧結合大數據與深度學習後的產物。隨著 AI 在資料科學的發展，AI 甚至可自行產出 domain knowledge (領域知識)，且只要輸入 raw data (原始資料) 就可達成目的。因為這樣高能而新穎的模式馬上就引發許多社會、倫理、法律中憲法議題相關省思。[13]

(三) 責任歸屬

最實際的問題是 AI 的存在是由種種要素構成，然而這些要素在法律上的評價亟待討論與解決。諸如，AI 如果真的有所謂智慧，就面臨到其在法律上關於人格、權利義務主體之身份定性。如果 AI 做了某項決策，要怎麼描述 AI 的意思表示、誰又要承擔 AI 決策的風險？而排除哲學層面，AI 演算法的監督與管制也箭在弦上，對智慧財產權、資訊安全，AI 的存在都有可能侵犯。而這樣資料經濟的市場轉變，或許也可能根本的改變法律的體系，與法意識。因此，政府應該再運用 AI 的同時，堅守正當法律程序的遵守，才不會侵犯人民權利。

最後市場競爭規範面臨了資料科學而啟動的競爭新局。公平交易與反托拉斯法面臨新考驗，即是有能力發展 AI 的廠商坐擁資料優勢，得以快速分析用戶資料，甚至發展出客製化定價的遊戲規則，都可能導致市場的壟斷。所以在 AI 時代中，資訊自主權的保障應該如何伸縮？個人有無主張個人資料應受國家保護之權利？以及個人是否得主張免於 AI 追蹤之權利？歐盟在對此於 2016 年通過最新的個人資料保護規則 (The EU General Data Protection Regulation，簡稱 GDPR)，特別強調數點措施，包含企業應設立資料保護長一職、資料之使用必須有明確有效同意、被遺忘權等，顯現政府在資料保護的地位更是責無旁貸。[14]

有關人工智慧關聯性相關研究，大致均分別從法律層面及科技層面加以探討。就上述之研究

12. 葉俊榮，探尋隱私權的空間意涵—大法官對基本權利的脈絡論證，中研院法學期刊第 18 期，2016 年 3 月。
13. 葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例，資訊社會研究第 31 期，2016 年 7 月。
14. 張陳弘，GDPR 關於蒐用一般個人資料之合法事由規範 – 台灣個人資料保護法遺漏的正當利益權衡條款，月旦法學雜誌第 285 期，108 年 2 月。

主題，選擇適當之研究方法，採下列研究方法：

1. 歷史分析法

最重要的目的在於讓研究者藉由檢視過去資料以便了解現在。透過文獻所提供的具體價值，能使研究者瞭解被研究者或現象的形成脈絡，同時也可以協助研究者釐清在直接的觀察或訪談時更重要的問題；而比較研究方法則是對人類在不同型態的社會中的經驗進行比較，希望透過比較了解在特殊文化、社會、經濟或政治體制下的行為模式，以求達到更宏觀的結果。

以「憲法議題」為出發點，檢視法案的立法過程，更可以了解個案的發展脈絡是否符合「基本人權」的要求。因此，本文以我國法規及法院判決判例等，國內各大報章雜誌與國內外相關文獻作為分析的基礎，反映出國內社會輿論。

2. 比較法分析法

針對外國法制與台灣不同制度之部分進行研究，以比較法分析法之方式蒐集相關國家法規加以比較研究，並對我國相關法規加以歸納分析，我國是否本已有足夠機制來保障執法人，或是應該如何增訂等，以尋求未來解決之道。以比較法分析法為例，藉由比較本國與美國、歐洲對於人工智慧之相關法規，評估本國法律是否有足夠機制來保障資料擁有者，或是應該如何參考其他國家之法律來進行增修，有利於本國對於人工智慧相關法律的進步及周延，例如以 GDPR 第 4 條之規定，自動化指以自動化方式處理個人資料的分析與預測活動，資料當事人包括工作表現、經濟狀況、位置、健度 (偏好、可信任度或者行為表現等等之判定。

3. 案例分析法

本文以各國法律為背景，參酌國外政府發展之經驗，藉由比較台灣與美國法制，以產業風險控管為問題意識，介紹各國法律之基礎概念及簡單區別後，探討此制度對公司經營之影響，及其固有架構所可能產生之優劣比較及建議。本文認為，法律有其不得不然之情形，只是要審慎面對公司經營者因所產生違法所在之疑慮，對制度健全發展所可能造成之壓制、甚至是破壞之因素有妥適之因應，更進而以臺灣各地方法院、高等法院及最高法院十幾年來所有判決判例分析該法律問題，及進一步提出法院判決及相關解決辦法[15]。

15. 葉俊榮，探尋隱私權的空間意涵—大法官對基本權利的脈絡論證，中研院法學期刊第 18 期，2016 年 3 月。

參、我國近期實務見解之整理

表 1：我國法院攸關人工智慧與隱私權侵害判決分析表（作者自行整理）

日期 / 裁判案由	法院見解	判決字號
2019 年 10 月 09 日 / 妨害名譽	被告無罪，係刑法第 309 條第 1 項所規定「 侮辱 」，係以貶損他人人格或使人難堪為目的，以言語、文字、圖畫或動作，表示不屑、輕蔑或攻擊之意思，足以對於個人在社會上所保持之人格及地位，達貶損其評價之程度，始足當之。此罪所保護者，乃個人經營社會群體生活之人格評價，而此乃法律對個人人格之保護，原則上自當以法律所承認之權利主體，始得享有。網路世界之虛擬身分，並非法律所承認之權利主體，或因該虛擬身分在網路世界中之活動，而產生類如真實世界之虛擬人格，然此種虛擬身分可隨意創建、刪除、變更、移轉，甚且隨科技進展，該虛擬身分不無可能僅為人工智慧產物，是源自此種虛擬身分之虛擬人格，與真實世界受法律保護之個人人格具有本質上差異，不能等同視之，故對於網路世界之虛擬身分公然侮辱，其行為人並不當然構成刑法第 309 條第 1 項之公然侮辱罪。	臺灣屏東地方法院 108 年易字第 737 號刑事判決
2019 年 10 月 01 日 / 返還研究費用等	原告之訴駁回，系爭契約一第 1 條二三規定：「『 本技術，或稱本組合技術 』，係指甲方（ 即被告 ）所擁有豐富高齡健康臨床照護與老化身心功能變化之判別技術；及乙方（ 即原告 ）擁有之身心功能檢測與 E 化健康管理等技術，共同組合而成之智慧財產之部分或全部 」、「『 本計畫，或稱本合作研發計畫 』，係指雙方以本組合技術為基礎，依雙方所訂定『 產官學合作研究發展計畫書 』之內容，共同為開創全新精緻化長壽健康養生與照護客製化生理監（ 檢 ）測以及 E 化健康服務模式，發展老化相關尖端研究而建立國際頂尖高齡醫學與健康服務模組 」。具體契約目的、內容至少為：因造成老化的主要關鍵在於身心功能衰退，亦即走向失能與失智的風險，而降低身心功能衰退的具體策略需要仰賴全方位的健康檢測，包括生理功能檢測與各種創新生物指標開發，並透過大數據之網路科技建立 E 化管理流程，亦即以人工智慧結合個人精準醫療與大數據的研發成果而成為具體服務模式。故系爭契約一之主要合作研發內容，即在於以被告對於老化之專業與研究成果，結合原告之生技與資訊科技技術專長，發展延緩老化對於身心健康影響之「 抗老化 」關鍵技術，並透過原告之技術建立 E 化健康服務模組；本計畫對於抗老科技的研發主體著重在延緩身心功能衰退，預計以研發成果建立延緩身心功能衰退的明確方案，證明臨床成效之後，再開發商業模式進行商品化。	臺灣士林地方法院 107 年重訴字第 386 號民事判決

2019 年 12 月 19 日 / 證券交易法等案件	原審地院判有罪，上訴人 00 上訴駁回，係因附表所示投資人 00 等人，佯稱其為美國史丹佛大學博士及美國貝爾實驗室副總裁等身分，具有光通訊專利技術，現漢唐光電公司營運良好資金充足，從事光電研發產業，已可於近年內上市櫃，或與美國思科公司洽談鉅額併購案，各投資人所購買股票於漢唐光電公司上市櫃或併購後將翻漲數倍 (徐國良佯稱事由詳如附表一「事由」欄所載) 云云，另指示不知情之漢唐光電公司員工許嘉麟將諸如「徐國良為美國加州大學洛杉磯分校 (下稱 UCLA) 電腦科學系全系第一名畢業、美國史丹福大學電腦科學博士，曾為美國朗訊科技董事長及全球總裁暨全球執行長、美國貝爾實驗室院士、研發計畫總主持人及首席執行副總裁兼美國國防部人工智慧戰略戰術超級電腦建設主持人，又為美國貝爾實驗室神經網絡部門、全光網絡部門、光纖通訊部門、光電半導部門總負責人，曾獲得美國總統科學獎、傑出科學獎 (總裁金獎)、西屋科學獎，另擁有光纖通訊 48 項、神經網絡 12 項世界專利」等不實之學經歷，及如「徐國良率領美國貝爾實驗室、美國朗訊科技公司科學家從事光電研究，漢唐光電公司為全球唯一從事光電研發之公司，擁有全球最大計畫中心」等虛假公司營運狀況及研發技術等事項登載於漢唐光電公司網頁，使投資人因徐國良口述或參看上開網頁上對一般理性投資人而言具重要性之不實資訊，而陷於錯誤並向徐國良購買其所有之漢唐光電公司股票。	臺灣高等法院刑事判決 107 年度金上重訴字第 52 號，不服臺灣臺北地方法院 107 年度金重訴字第 6 號，中華民國 107 年 11 月 26 日第一審判決提起上訴。
2011 年 07 月 16 日 / 履行契約等	(5) 一個 Unix 作業系統，程式碼約十一萬行左右，本件軟體程式碼已達三十餘萬行，甚為複雜。如鑑定書所評，欲達原告期望之高度人工智慧型排版軟體，恐為舉世所無。被告致遠科技股份有限公司為此軟體合作開發方案，工程師費用即已耗費一千零八十六萬九千九百四十元，投注心力不可謂之不多，原告迄僅支付一百二十五萬元，乃要求被告毫無底線繼續投入人力，卻不為相對之付出，實為強人所難。(6) 依該鑑定書所載，原告既認系爭軟體並未驗收，則在測試調校階段，即不應以之實施商業運轉，此為業界軟體合作之一般共識，自不得將其逕為商業使用之損失轉嫁於被告。	台灣台北地方法院 86 年度訴字 1585 號判決

2017 年 08 月 01 日 / 妨害名譽	上訴駁回。理由一、聲請簡易判決處刑意旨略以：被告甲○○與告訴人乙○○因 線上遊戲「○○○○ Online」而結識，雙方因細故生有嫌隙，詎被告竟基於妨害名譽之犯意，於民國 103 年 8 月 12 日某時許，在雲林縣○○鎮○○里○○路住處，以電腦設備連接上網，並以帳號 d 0000000、遊戲角色暱稱為「 司徒嘯天 」之名義登入線上遊戲「○○○○ Online」之「 天子 」伺服器，因對告訴人所使用之遊戲角色（ 暱稱 ）「 電因三太子 」有所不滿，竟意圖散布於眾，在不特定人得共聞共見之該遊戲區域頻道，以其遊戲角色暱稱「 司徒嘯天 」之名義，張貼內容為「 大家小心喔、電因三太子＝謎情物語是小偷、專偷別人天門倉庫的秘笈 」等文字，以此方式誹謗遊戲角色暱稱為「 電因三太子 」之告訴人，足以毀損告訴人之名譽，因認被告涉犯刑法第 310 條第 2 項之加重誹謗罪嫌等語。三、聲請簡易判決意旨認為被告涉犯刑法第 310 條第 2 項之加重誹謗罪嫌，無非係以被告供述、告訴人指訴、○○○○股份有限公司（即經營「○○○○ Online」網路遊戲之公司，下稱○○○○公司 ）103 年 8 月 29 日行管函字第 1030829002 號函文、網路遊戲畫面列印資料等，為其主要論據。訊據被告固不否認有於上開時、地，以上開遊戲角色名義，在該遊戲頻道張貼上開文字等情，惟辯稱：伊認為「 ○○○○ Online」網路遊戲之遊戲角色暱稱，無法連結到現實上之本人，不會妨害到本人之名譽等語。四、查被告於前揭時、地，以帳號 d 0000000、遊戲角色暱稱為「 司徒嘯天 」名義登入線上遊戲「 天子傳奇 Online」之「 天子 」伺服器，在該遊戲區域頻道，以暱稱「 司徒嘯天 」，張貼 內容為「 大家小心喔、電因三太子＝謎情物語是小偷、專偷別人天門倉庫的秘笈 」等文字等情，業據被告供認不諱，核與告訴人之指述情節相符，並有「 天子傳奇 Online」網路遊戲畫面列印，固堪認定；惟「 ○○○○ Online」網路遊戲無法知道遊戲角色之真實身分，遊戲帳號內只有暱稱，並無照片、Email 或其他個人資料，被告與告訴人彼此不知遊戲暱稱「 電因三太子 」、「 司徒嘯天 」本人為何人等情，亦據被告供承、暨告訴人申告陳明可按，核與中華網龍公司承辦人嚴郁欣稱：「 ○○○○ Online」玩家無法得知其他玩家之真實身分等語，互核相符，均堪認定。五、惟無法連結得知真實身分之線上遊戲角色，在網路上受有貶抑評價，是否為刑法誹謗罪規範之保護客體？論述如下：(一) 按「 人民有言論之自由 」，為憲法第 11 條明文保障之基本人權。另「 凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障 」，亦為憲法第 22 條明文，人格權植基於此，經創設列為基本權利之一，正是基於「 人性尊嚴與個人主體性之維護及人格發展之完整 」(大法官釋字第 603 號解釋參照)，即以人格尊嚴為基本權利之最高價值，中外憲法，如我國 86 年憲法增修條文第 10 條 (基本國策) 第 6 項「 國家應維護婦女之人格尊嚴 」)、德國基本法第 1 條明定「 人之尊嚴不得侵害 」，均揭明及此；然人性尊嚴之所以為最高價值，除可從自然法演變觀察外，其內涵概之體現人的主體性及自主性[16]；本此人性尊嚴觀點出發，享有基本權利中例如人格權之名譽權，其名譽的本質為人的真正價值與真實名譽，為相應於人格之客觀價值，故可曰之前於實證法 (包含憲法) 而存在之人性尊嚴，原則上應歸屬於自然存在之人（ homo)，除少許例外合於目的及性質所許之私法人或團體得享有名譽權外[17]，應以具有倫理學位格及法律上人格（ persona）為權利主體，始得享有名譽權，名譽與名譽權因之區分[18]；反之，例如人工智慧、機械人等非真實世界自然存在之人，可能具有名譽，但不擁有名譽權，人工智慧在網路遊戲經營之線上遊戲角色，亦然；惟對於無法得知真實身分之自然人在線上遊戲經營角色，是否有以名譽權保護之必要，則有歧見。	台灣高等法院台南分院 106 年上易字 256 號刑事判決

2011 年 12 月 31 日 / 違反道路交通管理處罰條例聲明異議	本院當庭比對雷達波速判讀表與違規採證照片，照片內之ＭＫ－四八〇五號及 MG- 五六〇五號二部小客車，確僅ＭＫ－四八〇五號自小客車在雷達波速範圍內，而自行動作之微電腦依現今科技，其人工智慧亦尚未達摻雜情感因素程度，於論理與經驗法則上均無刻意攀誣異議人甲〇〇可能，其所為測速結果，自有其可信之處，是異議人甲〇〇違規之事實，應堪認定，綜上查證，本件異議人甲〇〇之辯解，不足採信，原裁決機關援引首揭規定，對異議人甲〇〇裁處罰鍰新台幣二千四百元，並違規記點一點，依法洵屬有據。異議人甲〇〇猶執前詞任意指摘原處分不當，要無可採，應予駁回。	台灣桃園地方法院 90 年度交聲字 281 號刑事交通裁決

肆、人工智慧下談隱私權保護

一、個人資訊自主權

在 AI 時代裡，「個人資訊自主權」(Right to personal data/Information autonomy) 的內涵是否將有所改變個人資訊隱私受保護的程度，將有不同個人究竟有無主張個人資料應該受到國家保護的「積極權利」可言。個人可以主張免於監控與侵擾的權利。換言之，在此種情況下，個人才可以主張免於受到 AI 系統性追蹤與監控的權利。AI 時代的機器學習本質是在不斷「型塑」(Profile) 個人，這樣反覆且大量的型塑行為及其結果，即有個人資訊自主性是否受侵害的隱私疑慮，此一疑慮在歐盟最近開始施行之資料保護指令 EU General Data Protection Regulation(簡稱 GDPR) 下更加明顯。[19]

應該如何評價這類個人資料蒐集、處理與運用行為？成為型塑對象的當事人，又有哪些權利可以主張？勢必都是人工智慧時代的個人資訊爭議焦點。整體而言，GDPR 不但加強保護個人資訊自主權利，也促進了歐盟內部市場一致性的深化，同時並且將確保個資保護執法的強度得以提高，並且在簡化個資的國際傳輸之餘，建立了個資的全球保護標準。所以，為了落實並遵守 GDPR 新規定，企業的資料保護標準勢必提高，同時也必須採取新的內部管控程序，因應此一新法的要求。此一在資訊隱私方面的國際規範新趨勢，不僅是科技領域與貿易領域必須關切的發展，也是法草案研擬過程中，對於以大量個人資料經過處理而產生之「特徵描繪」或「型塑」(Profiling) 出現，在最終通過的規定中，對於基於「特徵描絕策，亦有具體規範。

二、歐洲指令對個人資料保護之規範[20]

根據 GDPR 第 4 條之規定，自動化指以自動化方式處理個人資料的分析與預測活動，資料當事人包括工作表現、經濟狀況、位置、健度 (偏好、可信任度或者行為表現等等之判定)。「特徵描繪」必須具有法

16. 王澤鑑，人格權法，第 72-74 頁。
17. 同上註，第 82 頁。
18. 高金桂，論刑法對個人名譽保護之必要性及其界限，刑事法學之理想與探索，第 184 至 186 頁。
19. See generally e.g., MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATAAND COMPETITION POLICY (2016).
20. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market，amending Directives 2002/65/EC，2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010，and repealing Directive 2007/64/EC.

定依據，或者獲得資料權人之同意，方得為之，而且，資料當事人必須是在補充之下，予以同意授權，方屬有效。關於敏感議題 (政治立場、宗教信仰和性傾向等) 之特徵描繪，才止之列。在限制處理權方面，GDPR 要求的是，當資料當事人提出反對時，資料控制者應立即停止處理該個人資料，而此一反對權，亦應適用於以大量個人資料所自動化產生之「特徵描繪」活動，亦即資料當事人有權理解某一特定服務究竟是如何作出特定決策，甚至拒絕加入此一特定決策，受此一特定決策拘束。可以預期的是，此一規定將會對以巨量資料基礎，以便運用於各種智慧科技、物聯網、機器學習、人工智慧等領域的資料分析與研判服務，將形成重大挑戰，例如，性質上屬於「黑盒子」決策的機器學習技術，究竟如何適用限制處理權或反對權，也是值得研究與尋求解決之道的迫切議題。如前所述，GDPR 對「自動化決策」予以限制性的規範，對於目前的科技發展趨勢來說，可能構成潛在風險。換言之，除非符合取得知情同意並明確授權同意的要件，GDPR 原則上禁止任何對歐盟公民有重大影響的自動化決策，包括評價個人研究應該深入分析與研究的重點。個人的工作表現、經濟狀況健康、個人愛好、興趣、行為、位置或運動等等。同時，GDPR 所規定的「解釋權」，也賦予個人有權瞭解某一特定服務究竟是如何作出關於其個人的特定決策的權利。這些規定可能影響到許多仰賴自動化決策的廠商所提供的服務。例如 Facebook 已經把機器學習用於廣告，這類決定的模式，應該如何調整，方能符合 GDPR 的要求，值得深入探討。更為關鍵的問題在於，機器學習及其演算法，究竟如何適用「解釋權」，也同樣值得研究。整體而言，GDPR 的規定對機器學習演算法的設計和應都帶來不少規範層面的挑戰，目前至少有兩個面向的特別值得注意，一是「禁止差別待遇」原則，一為「(獲得) 解釋權」(Right to explanation) 就禁止差別待遇來說，所謂差別待遇，是指基於個體屬於某個特定團體，例如種族和性別等，而對其予以不同的對待，而禁止差別待遇這個原則，深深地嵌入歐盟規範架構當中。為了資源分配等原因，在演算法的輔助之下進行型「特徵描繪」的應用結果，其本質就是一種差別待遇，因此，宣稱巨量資料或演算法運用都是中立的，恐怕言過其實。以人工智慧時代的特性而言，機器學習依賴的是已經蒐集篩選的資料，而社會上原本就存在的各種不公平、排除與歧視，在這些資料裡都會留下痕跡。因此，在未經考慮的情況下，仰賴資料勘探，自然會順勢產生排斥各種弱勢群體的結果，這就是探討 GDPR 的禁止差別待遇原則如何適用在人工智慧與機器學習時代之際，不得不關切的議題。[21]於缺乏存取權生效的明確日期，因此難以確定存取權解釋或系統功能解釋，在此一架構下，GDPR 可能只是賦予「系統功能解釋」的自動決策解釋包括「特定決策」的理由和情境之解釋在內。

三、歐盟下資料保護指令規範[22]

相較之下，歐盟的 1995 Data Protection Directive (歐盟一九九五年資料保護指令)

22. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC，2002/65/EC，2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

所規定的存取權，則是資料主體可以得知「資料控制者是否處理個人資料」的存取權內涵，基本上並未包括「已作成的特定解釋權」，這和 GDPR 的第 15 條與第 22 條要求不同，即使如此，在 GDPR 時代裡，我們或許可以設想幾種可能讓「特定自動決策解釋權」在實務上得以發生的情境 : 一是歐盟成員國在 GDPR 以外，制定了更多法律要求予以落實。二是基於 GDPR 第 22 條第 3 款和 Recital 71，資料控制者自願選擇提供「特定決策解釋權」。三是 GDP 未來正式施行時，廣泛解釋「自動決策的防衛機制」(第 22 條第 3 款) 已確立「特定自動決策解釋權」。四是 GDPR 未來正式施行時，將存取權 (第 15 條) 解釋成可以為「特定自動決策解釋」提供基礎。以上四種情境，以第三種與第四種最為立即可行。總而言之，嚴格說來，解釋權並沒有在 GDPR 中取得充分的規範基礎，使得透明化自動決策此一終極目的之達成，尚有距離。由於就解釋權而言，GDPR 具有「文字精確度不足」和「未能明確定義權利與防衛機制」的缺陷，同時，特定決策解釋權未能從第 22 條第 3 款防衛機制、第 13 條和 Article 14 的通知義務中，獲得明確所保障，所以未來的解釋權涵與面貌，第 22 條第 1 款的「自動決策」定義所限即限於「影響資料主體的法律效果或相似重大效果」且「純然自動處理」，方有解釋權的行使空間可言。因此，在 GDPR 正式生效之後，第 22 條的解釋適用就會變得更為關鍵 : 究竟是「禁止」(傾向保護資料主體的利益)，抑或「有權反對」(傾向維護資料控制者的利益)，因此，未來如何增加第 22 條第 3 款中解釋權的法律約束力，並且澄清第 22 條第 1 款的文字，以便確認何時自動決策為「純然自動處理」，自動決策在何種情況下會被當作「法律上或有相當重大影響」，何調第 22 條第 2 款中所規定的「為執行合約所需要」，以及確認第 22 條的規範意旨為「禁止」而非「有權反對」，都是應該持續關注的研究重點所在。同樣地，澄清第 15 條第 1 款中「existence of [...] Significance [...] envisaged consequences [...] [and] logic involved」的意義，以便確立「被通知權」，以及基於維護營業秘密的考量，如何衡量「替自動決策引入外部稽核機制」或「替資料控制者設定內部稽核要求」兩者的比重，也是重點。以上這些都是 GDPR 正式施行後的挑戰，也將是人工智慧時代的重要法律議題，值得持續密切觀察與深入研究。[23]

四、人性尊嚴分為兩個層面觀之：

積極層面，係指人類之自我決定、自我統治 ; 消極層面觀之：德國聯邦憲法法院所提出的「客體公式」。人性尊嚴的意涵，在哲理上有相當豐富的討論，但在法學領域中卻認為人性尊嚴難以從正面描述或定義。人性尊嚴表述大致上為：每一個人都是自主、自決的獨立個體，都是具體存在並且具有意義的生命。每人有權利為自己維護自己的尊嚴；每一個人在社會中，均有其一定的社會價值，每個人都有權主張自己應受到充分的尊重。

所以國家不能為了成就特定人群的目的，而將其他人當成達成目的的手段，人們

23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data，and repealing Directive 95/46/EC.

不能被貶低為單純僅受國家行為支配。然而我國憲法中並無「人性尊嚴」用語，僅有憲法增修條文第 10 條第 6 項規定：「國家應維護婦女之人格尊嚴，保障婦女之人身安全，消除性別歧視，促進兩性地位之實質平等。」人性尊嚴的憲法依據可分為 3 種說法：第一、人性尊嚴之保障是先於憲法存在，待憲法規定國家即須保障，憲法即使規定，亦僅具事後確認性質，不影響人性尊嚴之原權或固有權之地位[24]。第二、由憲法第二章所列舉之人民自由權利個別保障範圍內推演出保障人性尊嚴之內容，縱然無法從列舉之人權清單來推求，至少也可從概括保障規定憲法第 22 條中得到依據。第三、以前憲法增修條文第 10 條第 6 項為依據。我國憲法雖未像西歐各國憲法，對保障人性尊嚴之原則有明文規定，但鑒於人性尊嚴思想乃憲政國家精神根基所在，本無待憲法明示，且綜觀我國憲法中所規定之民主原則、種種基本人權保障規定，基本國策中關於社會安全之要求等，解釋上當以人性尊嚴為我國憲法當然的保障內涵，不限於憲法增修條文所規定之婦女人性尊嚴的維護。但由於人性尊嚴不在列舉權利內，而直接引基本國策的條文，尚須引憲法第二十二條為依據，使其進入憲法第二章體例內，發揮憲法第二十二條之保障媒介功能。[25]憲法第二十二條：「凡人民之其他自由或權利，不妨害社會秩序或公共利益者，均受憲法保障。」由憲法整體規範示出人性尊嚴，具有高度自然法色彩，是人所以為人當然享有之權，具有固有性、永久性和普遍性，不論何時、何地、何人，都能普遍適用，世界人權宣言中所保障者多屬此類不可侵犯與讓渡的人權。『我國此種原權層次之保障屬於憲法第二十二條概括基本權功能建構所保護之法益。』尊重並保障人性尊嚴是一種憲法價值的決定。確立國家公權力應對人性尊嚴加以尊重與保障，人性尊嚴就成為憲法秩序中最高的法律價值，非但在行政、立法及司法上應受到人性尊嚴原則的拘束，不容國家機關以任何理由、任何方式予以侵害外，甚至屬於不得經由修憲程序變更的憲法核心領域。

五、我國相關大法官解釋[26]：

大法官釋字第 372 號解釋之解釋理由書中首度明確指出：『「人格尊嚴之維護」與人身安全之確保，乃世界人權宣言所指示，並為我國憲法保障人民自由權利之基本理念。憲法增修條文第 9 條第 5 項即在揭示上開理念。』[27]此外，蘇俊雄大法官在協同（含部份不同）意見書中，更論我國應保障人性尊嚴之理由，略為：『「人性尊嚴」不可侵犯，乃是「先於國家」之自然法的固有法理，而普遍為現代文明國家之憲法規範所確認。憲法保障基本人權，對於每一組織構成社會之個人，確保其自由與生存，最主要之目的即在於以維護人性尊嚴。蓋人類生存具有一定之天賦固有權利，在肯定「主權在

24. 葉俊榮，探尋隱私權的空間意涵—大法官對基本權利的脈絡論證，中研院法學期刊第 18 期，2016 年 3 月。

25. 施啟揚，從個別人格權到一般人格權－西德戰後對人格權的加強保護及非財產上損害賠償的改進，國立台灣大學法律論叢，第 4 卷第 1 期，1974 年 10 月。

26. https://cons.judicial.gov.tw/jcc/zh-tw/contents/show/rs6d6v8wlspnmghc

27. 吳威志，國際人權兩公約有關「隱私權」規範在台灣施行的檢討與展望，科技法學論叢第 9 期。

民」之國家理念下，乃將此源諸人類固有之尊嚴，由憲法加以確認為實証法之基本人權。我國憲法雖未明文宣示普遍性「人性尊嚴」之保障，但是此項法益乃基本人權內在之核心概念，為貫徹保障人權之理念，我國憲法法理上亦當解釋加以尊重與保護。此外世界人權宣言之前言第一句即謂：「鑑於人類一家，對於人人固有尊嚴及其平等不移權利之承認確保係世界自由、正義與和平之基礎」，而第一條亦明白揭示「人皆生而自由；在尊嚴及權利上均各自平等…」世界人權宣言是會員國本身及其所轄人民均應永享咸遵之國際憲章，我國亦為簽署國之一。為維護民主憲政國家之形象，國家亦應盡保障國際人權之義務』。

釋字第 585 號解釋中提到同條例第八條第六項規定「本會或本會委員行使職權，得指定事項，要求有關機關、團體或個人提出說明或提供協助。受請求者不得以涉及國家機密、營業秘密、偵查保密、個人隱私或其他任何理由規避、拖延或拒絕」，其中規定涉及國家機密或偵查保密事項，一概不得拒絕之部分，應予適當修正。十、同條例第八條第四項前段規定「本會行使職權，不受國家機密保護法、營業秘密法、刑事訴訟法及其他法律規定之限制」、同條第六項規定「本會或本會委員行使職權，得指定事項，要求有關機關、團體或個人提出說明或提供協助。受請求者不得以涉及國家機密、營業秘密、偵查保密、個人隱私或其他任何理由規避、拖延或拒絕」，其中規定涉及人民基本權利者，有違正當法律程序、法律明確性原則。

釋字第 603 號解釋中，就戶籍法第 8 條第 2 項強制 14 歲以上國民於請領身分證時按捺指紋是否違憲，更明白論述：「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障。」[28]

釋字第 631 號解釋中，就通訊監察書於偵查中由檢察官依司法警察機關聲請或依職權核發，未要求通訊監察書原則上應由客觀、獨立行使職權之法官核發，是否違憲，亦於解釋理由書中再度重申：『憲法第 12 條規定：「人民有秘密通訊之自由。」旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利[29]。』

最後，**釋字第 791 號**解釋之解釋文揭示憲法所保障之基本權種類與範圍，亦經本院解釋而持續擴增與深化。經本院釋字第 585 號及第 603 號解釋明確肯認為受憲法第 22 條保障之隱私權即為適例。從而，系爭解釋所稱系爭規定一「為維護婚姻、家庭制度及社會生活秩序所必要…… 立法者就婚

28. 司法院大法官釋字第 585 號解釋參照。
29. 司法院大法官釋字第 603 號解釋參照。

姻、家庭制度之維護與性行為自由間所為價值判斷，並未逾越立法形成自由之空間」乙節，已非無疑；尤其系爭規定一是否仍合乎憲法比例原則之要求，更有本於憲法相關基本權保障之新觀念再行審查之必要。系爭規定一明定：「有配偶而與人通姦者，處 1 年以下有期徒刑。其相姦者亦同。」禁止有配偶者與第三人間發生性行為，係對個人得自主決定是否及與何人發生性行為之性行為自由，亦即性自主權所為之限制，按性自主權與個人之人格有不可分離之關係，為個人自主決定權之一環，與人性尊嚴密切相關，屬憲法第 22 條所保障之基本權。

系爭規定既限制人民受憲法保障之性自主權，應符合憲法第 23 條比例原則，即須符合目的正當性，且該限制有助於目的之達成，又別無其他相同有效達成目的而侵害較小之手段可資運用，而與其所欲維護法益之重要性亦合乎比例之關係。又性自主權與個人之人格有不可分離之關係，是系爭規定一對性自主權之限制，是否合於比例原則，自應受較為嚴格之審查。

系爭規定不僅直接限制人民之性自主權，且其追訴審判程序亦必然干預人民之隱私。按個人之性自主權，與其人格自由及人性尊嚴密切相關。系爭規定一處罰通姦及相姦行為，直接干預個人性自主權核心範圍之程度，堪認嚴重。再者，通姦及相姦行為多發生於個人之私密空間內，不具公開性。其發現、追訴、審判過程必然侵擾個人生活私密領域及個人資料之自主控制，致國家公權力長驅直入人民極私密之領域，而嚴重干預個人之隱私[30]。是系爭規定一對行為人性自主權、隱私之干預程度及所致之不利益，整體而言，實屬重大。況國家以刑罰制裁手段處罰違反婚姻承諾之通姦配偶，雖不無「懲罰」違反婚姻忠誠義務配偶之作用，然因國家權力介入婚姻關係，反而可能會對婚姻關係產生負面影響。是系爭規定一之限制所致之損害顯然大於其目的所欲維護之利益，而有失均衡。

30. 同前註。

表 2 司法院大法官攸關隱私權之相關解釋（作者自行整理）

司法院大法官解釋	相關隱私權之內涵
大法官釋字第 372 號解	『人性尊嚴之權利概念及其不可侵犯性，有要求國家公權力保護與尊重之地位。在個人生活領域中，人性尊嚴是個人「生存形相之核心部份」(Kernbereich privater Lebensgestaltung) ，屬於維繫個人生命及自由發展人格不可或缺之權利，因此是一種國家法律須「絕對保護之基本人權」(unter den absolutenshutz des Grundrechtes)。是此，在憲法保障之基本人權與自由價值體系中，人性尊嚴可謂是至上之價值理念，有受國家「優先保護」之地位。法理上並要求人人以自我之責任，對此固有之價值加以肯定。從而，人性尊嚴無拋棄或任意處分性；對於其侵犯行為，並不得再待審酌有無社會容忍性，而應直接以客觀評斷是否已構成傷害到人性尊嚴，決定是否加以國家保護』。惟在憲法實務上對大法官之有權解釋，無庸置疑地將直接產生影響力；對我國憲法是否承認人性尊嚴，於憲法法理上亦多有澄清作用。
釋字第 585 號解釋	「本會或本會委員行使職權，得指定事項，要求有關機關、團體或個人提出說明或提供協助。受請求者不得以涉及國家機密、營業秘密 、偵查保密、個人隱私或其他任何理由規避、拖延或拒絕」
釋字第 490 號解釋	「服兵役之義務，並無違反人性尊嚴亦未動搖憲法價值體系之基礎，且為大多數國家之法律所明定，更為保護人民，防衛國家之安全所必需，與憲法第 7 條平等原則及第 13 條宗教信仰自由之保障，並無牴觸。」揭示「人性尊嚴」之意義。
釋字第 603 號解釋	「維護人性尊嚴與尊重人格自由發展，乃自由民主憲政秩序之核心價值。隱私權雖非憲法明文列舉之權利，惟基於人性尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障。

釋字第 631 號解釋	此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利[31]。
釋字第 791 號解釋	按個人之性自主權，與其人格自由及人性尊嚴密切相關。系爭規定一處罰通姦及相姦行為，直接干預個人性自主權核心範圍之程度，堪認嚴重。再者，通姦及相姦行為多發生於個人之私密空間內，不具公開性。其發現、追訴、審判過程必然侵擾個人生活私密領域及個人資料之自主控制，致國家公權力長驅直入人民極私密之領域，而嚴重干預個人之隱私。

伍、結論

隨著 AI 的高度發展，倫理與責任的議題成為討論的核心，曾有學者提出，或許 AI 具備學習與思考演繹的能力，AI 是否能夠理解道德倫理或個人資訊保護的規範與意義？進而使 AI 成為個資保護的守門員，而非隱私侵害的麻煩製造者。隨著 AI 可透過各種感應器（Sensor）及物聯網（IoT）蒐集各種資訊，未來 AI 勢必將從被動的資料處理者，逐漸成為資料控制者，因此賦予 AI 個人資訊保護的義務就應當提高，未來 AI 的創新必須以保障個人隱私為出發點，而不是以個人資料與隱私的犧牲作為其不斷進步的代價。

人工智慧若在許多方面超越人類智慧水平的智慧、不斷更新、自我提升，進而取得控制管理權，人類是否有足夠的能力及時停止人工智慧領域的「軍備競賽」，能否保有最高掌控權，現有事實是：機器常失控導致人員傷亡，這樣的情況是否會更加擴大規模出現，歷史顯然無法給出可靠的樂觀答案。特斯拉電動車馬斯克曾稱人工智慧是「召喚惡魔」行為，英國發明家 Clive Sinclair 認為一旦開始製造抵抗人類和超越人類的智慧機器，人類可能很難生存。

2018 年 5 月 25 日歐盟的 GDPR(General Data Protection Regulation) 正式實施，是全球個人資訊隱私保護的典範法規，也給予 AI 等科技快速發展對個資隱私侵害隱憂，有一個適時平衡的契機。GDPR 針對「與個人有關的自動化決策」的規定，賦予個人有權可以拒絕「純粹以自動化方式」做成與其相關，且產生法律或類似效果的決定 (right to object)。當「純粹以自動化方式」做成個人相關決定影響當事人時，得要求資料控制者 (data controller) 之人為介入，並提供解釋 (right to explanation)。GDPR 的初步實施，大家都仍在觀望其對新興科技的隱私保護可能成效。 因此一方面新興 AI 技術仍不斷快速發展，一方面人們已逐漸驚醒個資隱私的重要性，彼此如何持續取得平衡，將會是持續發燒與關注的議題。

31. 司法院大法官釋字第 603 號解釋參照。

2020 年冠狀病毒席捲全球，人民不敢出門或是畏懼到公共場所，疫情擴散以至於口罩不夠使用、衛生紙、消毒水短缺等問題，如在此大力借助機器之功能，例如到疫區消毒，到機場當檢測人員，或是大量使用機器製造更多的口罩及消毒水等，機器以自動駕駛車輛或戰車飛機等形式出動，為國民健康安全等把關，這才是真正善用機器，並且得以獲得多贏局面，面對現代科技與隱私權保障之拉鋸戰，惟有遵循上開法令方得在發展科技之虞，對於資訊隱私權之保障臻於完善。

陸、參考文獻

一、中文文獻：

(一) 專書：

1. 曾隆興，現代非典型契約論，修訂八版，三民書局，1999。
2. 蕭文生譯，關於「一九八三年人口普查法」之判決，西德聯邦憲法法院裁判選輯 (一)，司法院印行，1991 年 5 月。

(二) 期刊 (依姓氏筆畫排列)

1. 王澤鑑，人格權保護課題與展望 (三)— 人格權的具體化及其保護範圍 (6) 隱私權篇 (上)，台灣本土法學第 96 期。
2. 王儷玲、葉淑玲、陳恩儀、汪宛臻，個資保護規範下之大數據現況運用與未來發展，資產管理人才培育與產業發展基金委託專題研究，108 年 12 月。
3. 王郁琦，網路上之隱私權問題，資訊法律透析第 8 卷第 10 期，88 年 10 月。
4. 吳威志，國際人權兩公約有關「隱私權」規範在台灣施行的檢討與展望，科技法學論叢第 9 期。
5. 施啟揚，從個別人格權到一般人格權－西德戰後對人格權的加強保護及非財產上損害賠償的改進，國立台灣大學法律論叢，第 4 卷第 1 期，1974 年 10 月。
6. 范姜真媺、劉定基、李寧修，「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案成果報告 (編號：1050224)，行政院法務部，105 年 12 月。
7. 翁逸泓，資訊委員的時代角色—以 GDPR 及英國 2018 年資料保護法為中心，月旦法學雜誌第 286 期，108 年 3 月。
8. 陳詩蘋，雲端行動支付利器－ HCE 及 Tokenization 共用平台，財金資訊季刊第 85 期，105 年 1 月，頁 3- 4。
9. 張永明，再探隱私權之自由－狗仔跟拍之憲法議題－評司法院釋字第六八九號「狗仔跟拍」之解釋，月旦法學雜誌第 197 期。
10. 張文貞，聯合國人權兩公約—公民與政治權利國際公約、經濟社會文化權利國際公約，財

團法人台灣新世紀文教基金會台灣聯合國研究中心，2014 年 8 月。
12. 張陳弘，GDPR 關於蒐用一般個人資料之合法事由規範 – 台灣個人資料保護法遺漏的正當利益權衡條款，月旦法學雜誌第 285 期，108 年 2 月。
13. 張陳弘、莊植寧，新時代之個人資料保護法制 — 歐盟 GDPR 與臺灣個人資料保護法的比較說明，新學林，2019 年 6 月。
14. 葉俊榮，探尋隱私權的空間意涵 — 大法官對基本權利的脈絡論證，中研院法學期刊第 18 期，2016 年 3 月。
15. 葉志良，大數據應用下個人資料定義的檢討：以我國法院判決為例，資訊社會研究第 31 期，2016 年 7 月。
16. 蔡柏毅，你的同意不是我的同意－淺介個資法上的「同意」，金融聯合徵信第 35 期，108 年 12 月，頁 75。
17. 劉靜怡，淺談 GDPR 的國際衝擊及其可能之因應之道，月旦法學雜誌第 286 期，108 年 3 月。

(三) 學位論文：

1. 詹文凱，隱私權之研究，國立台灣大學法律學研究所博士論文，87 年 7 月。
2. 陳進忠，隱私權之研究，國防大學管理學院法律學系碩士論文，103 年 5 月。
3. 馬興平，論資訊隱私權的保護 - 從釋字第 603 解釋出發，國立中正大學，2008 年。
4. 邱志偉，隱私權政策現況與展望 - 以美國為中心，東海大學法律研究所碩士論文，2019 年 1 月。
5. 陳之達，歐盟個人一般資料保護規則，東吳大學法律學系碩士在職專班科技法律組碩士論文，107 年 8 月。

二、英文文獻：

(一) 期刊文獻：

1. Innovations in retail payments– Report of the Working Group on Innovations in Retail Payments，2012，p 13
2. Kevin Curran，Amanda Millar，ConorMc Garvey.，Near Field Communication. ，Vol. 2 ，No. 3 . 371，371https://www.researchgate.net/profile/Kevin_Curran 4/publication/ 274532569_Near_Field_Communication/links/ 5717fbf 208aed 43f 632209b 7.pdf
3. Samuel D. Warren & Louis D. Brandies，The Right to Privacy，4 Harvard Law Review，Vol. 4，No. 5. (Dec. 15，1890)，pp. 193- 220. https://www.cs.cornell.edu/~shmat/courses/cs 5436/warren-brandeis.pdf
4. Alan F. Westen，Privacy and

Freedom(1967).
5. Thomas J. Smedinghoff，ONLINE LAW，269(1996).

(二) 判決：

1. Pavesich v. New England Life Ins. Co.- 122 Ga. 190，50 S.E. 68 (1905)
2. Joens v. Herald Post Co.，230 Ky. 227，229(1929).
3. SaratLahiri v. Qaily Mirror，295 N.Y.S.，382，388(1937).
4. Boyd v. United States，116 U.S. 616 (1886)
5. Silverthorne Lumber Co.，Inc. v. United States，251 U.S. 385 (1920).
6. Nardone v. United States，308 U.S. 338 (1939).
7. Olmstead v. United States，277 U.S. 438，456- 457 (1928).
8. Katz v. United States，389 U.S. 347 (1967).
9. Griswold v. Connecticut，381 U.S. 479 (1965).
10. Whalen v. Roe，429 U.S. 589 (1977).

(三) 歐盟法規條：

1. Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 April
   2016 on the protection of natural persons with regard to the processing of personal
   data and on the free movement of such data，and repealing Directive
   95/ 46/EC.
2. Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 April
   2016 on the protection of natural persons with regard to the processing of
   personal data and on the free movement of such data，and repealing Directive
   95/ 46/EC.
3. Directive 2007/ 64/EC of the European Parliament and of the Council of 13 November
   2007 on payment services in the internal market amending Directives 97/ 7/EC，
   2002/ 65/EC，2005/ 60/EC and 2006/ 48/EC and repealing Directive 97/ 5/EC.
4. Directive (EU) 2015/ 2366 of the European Parliament and of the Council of 25
   November 2015 on payment services in the internal market，amending Directives
   2002/ 65/EC，2009/ 110/EC and 2013/ 36/EU and Regulation (EU) No 1093/ 2010，and repealing Directive 2007/ 64/EC.

探討網路寫手之偵測方法與研究

A New framework for Astroturfing and Anti-astroturfing

曾韵
東吳大學巨量資料管理學院碩士
中央大學資訊管理學院碩士
安永諮詢服務股份有限公司 執行副總經理
guilkty@gmail.com

摘　要

網際網路已成為人們生活不可或缺的工具，根據資策會的統計，消費者獲取資訊的管道以入口網站、Facebook 所佔比例最高，此外，消費者購物前參考部落客及網紅的比例亦相當可觀，使得電子口碑除了消費者購買決策的參考之外，更是許多行銷公司或學者研究的方向，大家期望善用口碑行銷協助企業營造品牌行象與提高產品銷售，甚至利用其匿名性進行惡意的商業競爭。也有政治家掌握輿情風向控制選舉結果；這種情況在網際網路世界中稱為「 Astroturfing 現象 」。

這種欺騙行為除影響到消費者權益外，也影響網購或評論平台的信譽，因此更多企業或學者開始從不同領域切入嘗試各式方法以偵測「 Astroturfing 現象 」。然因學術領域不同、從不同角度切入，使得相關探討的文獻雖眾多但也較為複雜。本研究提出新的角度來彙總各項研究文獻所提出的偵測手法，並提出實務上可應用的實務場景供後續研究學者設計偵測手法之參考。

關鍵字：偽草根現象、虛假評論、網路欺騙、作者歸屬、作者辨識。

Abstract

Internet has play an important role in people's daily life. According to the survey of Market Intelligence & Consulting Institute(MIC), people tend to use websites, Facebook and blogs to gain information before purchasing and that makes online reviews has more influence on customer's decision making. Because of this impact, enterprises and marketing companies are highly concerned with the word-of-mouth marketing. They try to apply the WOM concept to increase sales performance and to make good reputation image to customers. Some even use the anonymity on malicious competition. There are also politicians who try to control the public opinion with WOM techniques in political elections. This is called "Astroturfing".

This kind of deceptive action affects the reputation of online shopping platform and consumers' rights as well. Since not all online reviews are truth worthy, more and more researchers are developing techniques to detect astroturfing. However, because of the dynamic application in astroturfing, there have been discussed in different literature domains but less survey of the whole picture. In this paper, we propose a new framework to summarize the researches and put forward practical applications of anti-astroturfing techniques for future study.

keywords：Astroturfing, Fake review, Deceptive review, Astroturfer, Authorship attribution.

壹、前言

由於新興科技的發展，企業採用網路口碑方法傳播，透過電子郵件、新聞群組、網路討論區、部落格、社群媒體等進行口碑傳播。Hanson（2007）[1]認為網路口碑行銷的行為在人際間的影響非常快速且廣泛，因此不論是正面或負面的評論，對於消費者的購買意願都有絕對的影響力，甚至在短時間內對企業形象造成極大的影響。為此，企業開始僱用網路寫手，發表產品使用的正面體驗評論，使消費者相信產品進而刺激購買慾望。但在競爭激烈的商業環境，企業甚至希望寫手間能互相幫忙，拉抬相關文章或評論的人氣，使其運作更有效率。

然而，許多產品誇大不實的新聞引發消費者對於明星或網紅發文的置入性行銷產生不信任感；因此，為搏取更多的信任，網路寫手從以往的部落客開始隱藏成為網路素人一時有感的評論，對於身份的隱藏手法更加細膩，且從以往的好評文章轉向攻擊對手的

1. Hanson, W. A. (2007).Principles of Internet Marketing. South-Western College.

負評文章。

三星寫手門事件就是其中著名的例子：2013年三星台灣分公司委託同集團中的鵬泰顧問公司進行產品宣傳，除了監控知名網站討論區的記錄，還指派員工假裝顧客發表購買心得分享或撰寫文章「自問自答」，影響網路輿論並打擊競爭對手（特別是HTC）的品牌形象。全案由公平交易委員會判罰款台灣三星電子1千萬元，受委託的鵬泰公司處300萬元，並以此案例討論公平交易法的相關條文，同時修訂薦證者（即網路寫手）若傳播或刊載錯誤的廣告訊息，將與廣告主負連帶損害賠償責任。

綜觀全球，假新聞、假評論的議題造成許多層面的影響，其中亦包含許多平台或社群媒體的公信力，因此眾多網路平台業者近年來開始重視這個議題。維基百科創辦人亦於2017年4月創《維基論壇報》欲打擊假新聞[2]，Google及臉書也不約而同地同時發佈對付網路上的假新聞的各項作法[3]。

值此之際，許多研究早已針對網路寫手之偵測方法進行探討，期望協助找出網路上的不實言論，或者刻意經營的帳號，維持網路秩序。

本研究協助大家瞭解網路寫手（或稱「Astroturfing」現象）以及相關偵測手法，最後再提出應用場景以及適合的偵測手法（領域方向）提供參考。

貳、Astroturfing 的偵測方法

Astroturfing原本是從AstroTurf演變而來，原意指的是人工草皮的表面。由於其原意代表的是”假”的意思，因此用於在網路上發表一些言論，製造大多民眾都喜歡某種產品或支持某種東西的假象。

網路時代下，Astroturfing變得更加難以發現，企業或行銷公司為了利益，大量產出帶有偏見或不實的資訊。Liu、Mukherjee及Glance（2012）[4]估計在今日所有的網路顧客評論中，有三分之一是假的。所有大型的使用者推薦網站，包含亞馬遜網路書店、TripAdvisor、專門推薦商家的Yelp等，幾乎都曾被指控刊出假評論。

本研究參考實際商業應用情況，彙整目前可能的Astroturfing使用情境如「表1」。

2. 趙安平。謊言年代，如何對假新聞展開逆襲。2017年5月12日。取自：https://theinitium.com/article/20170512-taiwan-fake-news/
3. 陳曉莉。Google及臉書雙雙出招再打假新聞。2017年4月26日。取自：http://www.ithome.com.tw/news/113701
4. Liu, B., Mukherjee, A. & Glance, N.（2012）. Spotting Fake Reviewer Groups in Consumer Reviews. International World Wide Web Conference Committee.

表 1：Astroturfing 分類與使用情境

領域	操弄者	被影響者	目的	情境
政治用途	政府 / 政黨 / 利益團體	民眾	製造輿論	利於某項政策推動、公關危機轉移話題
		特定人物	誤導	遊說支持或反對政策
	個人政客	民眾	製造輿論	利於政策推動、自我行銷取得民意支持、打擊政敵
商業用途	行銷公司	民眾 / 消費者	製造輿論	行銷公司產品或服務、塑造企業形象、打擊特定公司
			欺詐行為	騙取點擊率以提高績效、騙取點擊以取得授權蒐集個資
	一般企業	民眾	製造輿論	行銷公司產品或服務、塑造企業形象、打擊競爭對手
			誤導	公關危機轉移話題、商業併購前後刻意炒作
		客戶	製造輿論	行銷產品、維持客戶忠誠度
	部落客 / 網紅	民眾 / 粉絲	製造輿論	行銷特定產品或服務、打造粉絲人氣、打擊對手
其他	詐騙集團	民眾	欺詐行為	於粉絲團發文吸引消費者付錢卻未能購買到商品

一般來說，Astroturfing 的需求起點通常為某些公司或集團，透過雇用特定人員作為寫手，為達到影響力且確保隱匿性，他們於不同平台註冊不同帳號並刻意經營之。最後這些帳號再透過協作的方式，發表各式評論或回應，以達到最終目的。

本研究以「圖 1」描述 Astroturfing 關係結構，整理出各類文獻的偵測方向：

一、分析文章是否為虛假評論（Fake Review）：

目前偵測文章是否為虛假文章，主要

是透過文字探勘及分析文章特徵的方法來進行。文字探勘係透過分析文章相似度來判定是否為同一作者所為，進而發現可能存在的寫手。而透過文章特徵來判斷則是分析虛假評論本身的特性（如文章圖文並茂陳述某些特定產品等），藉以判定文章是否為虛假評論。

二、分析帳號是否為寫手帳號（Fake Account）：

分析帳號為主的方法，主要係透過帳號本身的行為（如登入時間、發文及回文數量等）來判定是否為寫手刻意經營的帳號。此外，依據行銷公司雇用寫手的特徵也可發現，單一寫手可能擁有多個帳號，因此多透過帳號間的發文、回文相互回應方式以有效經營帳號。故亦有研究透過社群網路分析的方式，偵測帳號間的關聯，以偵測寫手帳號群。

三、分析是否為 Astroturfing 現象：

近幾年也開始有文獻探討偵測 Astroturfing 的現象，甚至進而希望揪出跨平台間不同帳號的幕後寫手。此類偵測方法，多半採以綜合前兩項方法來進行。

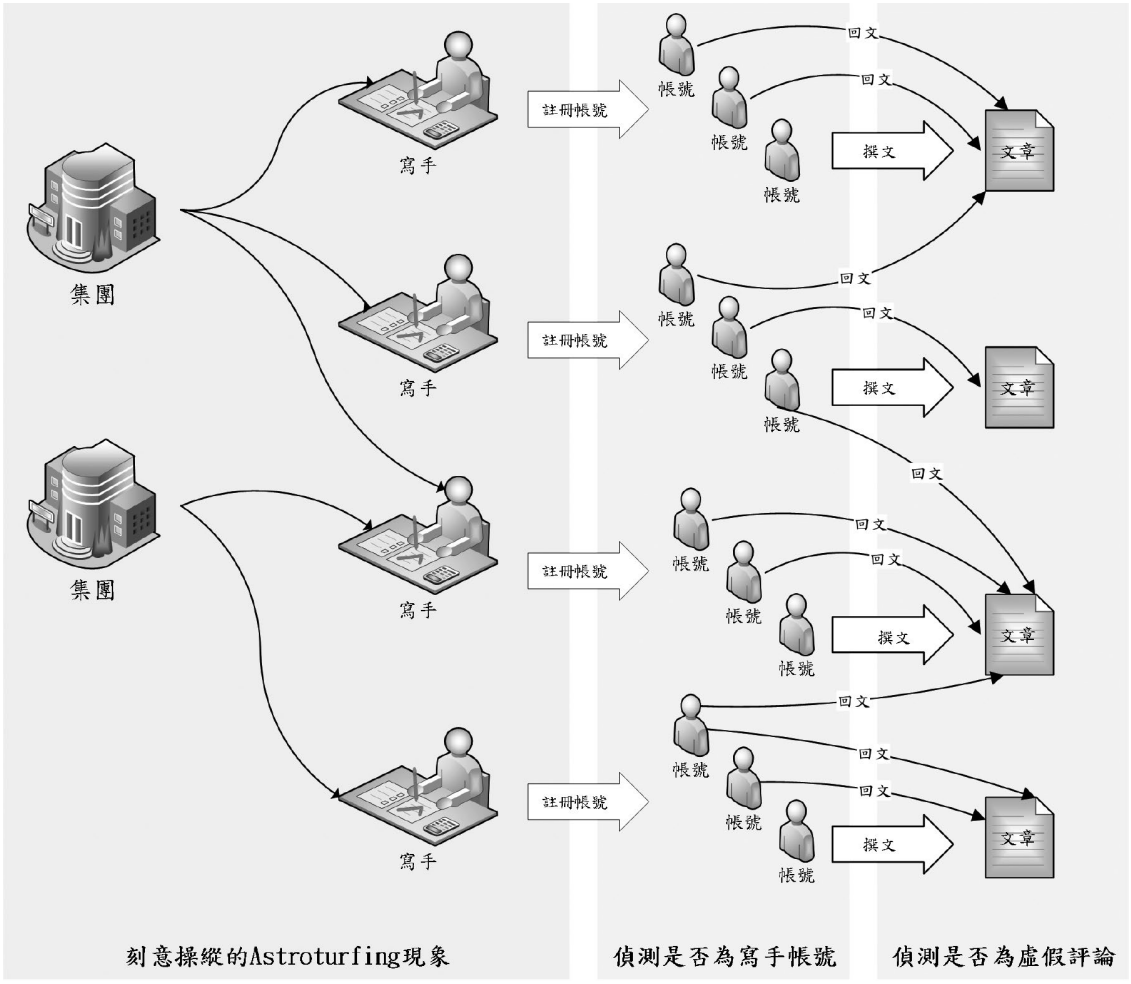


圖 1 集團與網路寫手關係圖

參、綜合整理與方法比較

本研究經過大量的文獻探討，除了將相關研究依文章、寫手、寫手間關係等角度歸納為虛假評論（ Fake Review）偵測以及寫手帳號（ Fake Account）偵測等兩大類外，再依分析與文章內容相關性與否分為文章特徵分析、文字探勘、帳號特徵分析、以及社群網路分析等偵測方法，根據本研究的整理，將各種偵測方法的優缺點條列於「表 2」:

表 2: 各項偵測方法優缺點

領域	作法說明	優點	缺點
偵測虛假評論			
文章特徵	依據文章本身的特性進行分析。	執行較方便簡單。透過爬蟲程式可輕易取得資料集。	精準度不足，大多研究採用混合的方式提高精準度。此外，文章本身特性也將依不同的網站所能取得的資訊而有所限制。
文字探勘－相似度比較	透過不同的方法比對寫作風格以確認是否為同一人撰寫。	針對文章相似度或意見內容進行方析，較為明確。甚至可以根據文章內容進行跨網站的分析，可協助辨識出不同帳號的同一寫手。	斷字詞的方式容易對結果造成極大差異影響。且語言差異將影響分析。文章若屬回應類的短文，較難判斷。
文字探勘－意見探勘	透過分析文章的情感或意見傾向，辨識是否為虛假評論文章。	除了偵測特殊意見外，可以用於偵測刻意隱藏寫作風格的文章。	斷字詞的方式以及採用的詞庫容易對結果造成極大差異影響。且語言差異將影響分析。
偵測寫手帳號			
帳號特徵	透過發文者的基本資料或相關行為進行偵測。	從內文以外的特徵進行分析，因此可跨越語言限制。	帳號特徵依不同的網站所能取得的資訊而有所限制。
社群網路分析	透過社群網路分析技術，分析帳號發文與回文的關係，辨識是否為刻意操作的議題。	可以找出網寫手的社群關係，發掘多個帳號。	透過社群網路可辨識出寫手刻意經營的關聯，但難以定義到個人。

根據 Ma,Y.,&Li,F.（2012）[5]的整理，認為偵測虛假評論的挑戰主要有資料取得以及行為模式兩項，主要係因為多數情況為了使大眾誤認為相關評論文章為一般民眾的有感發文，因此使用各種方法隱藏身份，加上各網站平台所能提供之資訊並不相同，因此對於研究學者而言著實困難。

為方便未來學者快速進入此領域，本研究將相關探討文獻根據資料分析各個階段彙總成「表 3」，並於後續各節進行說明偵測 Astroturfing 從資料取得到實驗設計等各階段的執行重點。

表 3: Astroturfing 研究架構

作者	偵測類別					實驗設計(資料分析各階段)				
	偵測虛假評論			偵測寫手帳號		資料準備			分析方法	結果驗證
	文章特徵	相似度分析	意見探勘	帳號特徵	社群網路分析	人工標記	既有資料集	刻意製作		
Ott, M., Choi, Y., Cardie, C., & Hancock, J. T. （2011）[42]	V	V	V	V				V	統計分析、監督式學習(Naïve Bayes、SVM)	透過刻意操作的事前答案進行驗證
Jindal, N., & Liu, B. （2008）[30]	V			V		V			監督式學習(Logistic Regression)	以人工標記的結果驗證(真實情況為何不確定)
Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V. （2010）[17]	V			V		V			監督式學習(SVM)	以人工標記的結果驗證(真實情況為何不確定)
Chen, C., Srinivasan, V., Zhang, X., & Wu, K. （2011）[23]	V		V	V		V			1. 一般統計方法 2.監督式學習(SVM)	以人工標記的結果驗證(真實情況為何不確定)
Li, F., Huang, M., Yang, Y., & Zhu, X. （2011）[34]	V					V			監督式學習(SSVM, Naïve Bayes, logistic regression)、非監督式學習(bootstrapping method)	以人工標記的結果驗證(真實情況為何不確定)
宋海霞、严馨、余正涛、石林宾、苏斐 （2013）[2]	V					V			非監督式學習(K-Means)	以人工標記的結果驗證(真實情況為何不確定)
Afroz, S., Brennan, M., & Greenstadt, R. （2012）[15]	V		V				V		監督式學習(SVM、K nearest、Naïve Bayes、決策樹)	以既有資料的結果驗證
Liu, B., Mukherjee, A. & Glance, N. （2012）[37]		V		V		V			監督式學習(SVM)	以人工標記的結果驗證(真實情況為何不確定)
Lau, R. Y., Liao, S. Y., Kwok, R. C. W., Xu, K., Xia, Y., & Li, Y. （2011）[33]		V	V			V			非監督式學習	分類結果透過人工檢查(真實情況為何不確定
Zheng, R., Li, J., Chen, H., & Huang, Z. （2006）[48]		V	V				V		監督式學習(決策樹、SVM、類神經網路)	以既有資料的結果驗證
Iqbal, F., Hadjidj, R., Fung, B. C., & Debbabi, M. （2008）[29]		V					V		監督式學習(決策樹、SVM)	以既有資料的結果驗證
Peng, J., Detchon S., Choo, K. R., and Ashman, H. （2016）[43]		V						V	監督式學習(KNN)	1.同一作者的前後文相互比較確認模型 2.控制之已知帳號的文章
Chen, Y. R., & Chen, H. H. （2015）[24]			V	V			V		監督式學習(SVM)	以既有資料的結果驗證
林昱叡（2016）[3]				V	V		V		統計分析、非監督式學習(K-means)、監督式學習(SVM)	以既有資料的結果驗證
Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A., & Menczer, F. （2011）[45]			V		V	V			監督式學習(AdaBoost, SVM)	以人工標記的結果驗證(真實情況為何不確定)
Burgoon, J., Blair, J., Qin, T., & Nunamaker, J. （2003）[21]			V					V	統計分析(F-test)監督式學習(決策樹)	透過刻意操作的事前答案進行驗證
Mihalcea, R., & Strapparava, C. （2009）[39]			V					V	監督式學習(Naïve Bayes、SVM)	透過刻意操作的事前答案進行驗證
Montes-y-Gómez, M., & Rosso, P. （2013）[40]			V					V	半監督式學習(PU-learning)	透過刻意操作的事前答案進行驗證(使用Ott等人製作之資料集)
Rout, J., Dalmia, A., Choo, K. K. R., Bakshi, S., & Jena, S. （2017）[46]			V					V	半監督式學習(Co-training,PU learning)	透過刻意操作的事前答案進行驗證(使用Ott等人製作之資料集)

5. Ma, Y., & Li, F.（2012）. Detecting review spam: Challenges and opportunities. In Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on (pp. 651-654). IEEE.

一、資料準備

(一) 監督式學習法

大多數學者偵測虛假評論或寫手帳號多將其視為分類問題，幾乎在所有現有的檢測嘗試中都被採用，學者們採用各式的監督式方法進行虛假評論或寫手帳號的判定，而學習過程的基礎是資料。然而，此類問題最大的挑戰為實驗資料的取得，尤其是已確認為寫手或虛假評論的文章資料。可以想見，大多數的寫手或虛假評論會採用各式方法隱匿，使其看起來就像是一般的評論文章或者消費者。另一方面，訓練資料集的品質也影響了分類演算法的結果，因此對欲探討 Astroturfing 偵測的學者們，如何取得已知寫手帳號或虛假評論之資料勢必成為重要課題。

1.人工標記法：此為最常見的方法，大多文獻決定研究的網路平台後，通常會透過爬蟲程式取得該網路平台之資料。接下來，以人工方式進行文章是否為虛假文章的標記，有些嚴謹的研究團隊，在其文獻中會特別說明標記的方法。在進行標記時，首先較嚴謹的團隊會先定義虛假評論的特性，特別參考相關文獻或網路消費者指引等資訊，提供執行標記的組員瞭解虛假文章可能的特徵，以供其參考。

2.既有資料集：人工標記的方法因為採用人為處理，因此多半會有數量過少，或者是人工判讀的不準確性，畢竟無法驗證虛假文章是否真的是寫手所為。因此，部份學者則是採用既有的資料集進行實驗驗證。最簡單的方式就某次事件所取得資料進行細部研究，三星寫手門事件於 2013 年爆發並遭公平會裁罰後，網路上即流出相關的虛假評論及寫手資料（ HHP-2011.xlsx 及 HHP-2012.xlsx），此提供了各研究一個極佳的訓練測試資料集。林昱叡（2016）[6] 以及 Chen 及 Chen（2015）[7] 等，都以此資料集進行實驗。此種方法有一個缺點，即現實世界資料較難取得，當取得後會發現確認為虛假評論或寫手筆數遠遠少於一般情況，如「表 4，三星寫手門事件資料集中確定為虛假評論僅佔整體資料的 4. 99%。

6. 林昱叡（2016）。這是業配文嗎？網軍的貼文型態與網絡分析。國立臺北大學資訊管理研究所碩士論文。

7. Chen, Y. R., & Chen, H. H.（2015）. Opinion spam detection in web forum: a real case study. In Proceedings of the 24th International Conference on World Wide Web (pp. 173-183). ACM.

表 4：Chen（2015）實驗所用之三星寫手門事件資料集

Type	#posts	#spams	%spams
First Posts	10, 951	546	4. 99%
Replies	148, 481	1, 337	0. 90%
All Posts	159, 432	1, 883	1. 18%

3.刻意產生資料集：除了人工標記以及利用既有資料集外，Ott、Choi、Cardie 及 Hancock（2011）[8] 使用 Amazon Mechanical Turk（AMT）[9] 結合 TripAdvisor 製作了一個新的資料集。他們找了一群人針對特定酒店撰寫了 400 個正面的虛假評論（5 星級評等），並且從同一酒店中的 TripAdvisor 網站收集了 400 則「真實」的 5 星級評論，以此彙整成為 800 則正面的評論文章。除此之外，在之後的研究，他們依此概念建立了第二個資料集，但這次是以星級評等為 1、2 的負面評論。將兩次的資料集結合在一起，聲稱這是第一個已知的、用來審查虛假評論的「黃金標準資料集」。透過人工扮演寫手的方式來實際撰寫虛假評論，不失為一種方式，然需留意的是，該研究的資料集係學者外包人員撰寫，用於學術用途。雖請撰寫者模擬自己是飯店員工被要求撰寫虛假評論，但意圖係用於研究而非影響消費，因此此類資料集訓練出的分類器，是否真能在真實世界發揮效果，還有待觀察。

(二) 非監督式學習法

由於難以生成準確標記的虛假評論資料集，所以使用監督學習並不一定適用所有情況。非監督式學習為此提供了解決方案，因為它不需要標記資料。Lau、Liao、Kwok、Xu、Xia 及 Li.（2011）[10] 開了一種非監督式的文字探勘模型，並整合進語義模型中，用以偵測虛假評論，並將結果與監督式學習的方式進行比較。他們認為衡量「不誠實」（或欺騙）概念是不實際的，因為電腦無法評斷

8. Ott, M., Choi, Y., Cardie, C., & Hancock, J. T.（2011）. Finding deceptive opinion spam by any stretch of the imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1 (pp. 309-319). Association for Computational Linguistics.
9. Amazon Mechanical Turk（AMT）,Retrieved from: https://www.mturk.com/mturk/
10. Lau, R. Y., Liao, S. Y., Kwok, R. C. W., Xu, K., Xia, Y., & Li, Y.（2011）. Text mining and probabilistic language modeling for online review spam detection. ACM Transactions on Management Information Systems (TMIS), 2(4), 25.

作者的感受；他們提出另一種類似的方法，估算評論內容重疊的情況，如果對不同產品的評論卻使用同樣的文章內容（如「圖 2」），表明這兩篇文章內容應該不會出自作者的真心（意即作者有意欺騙）。

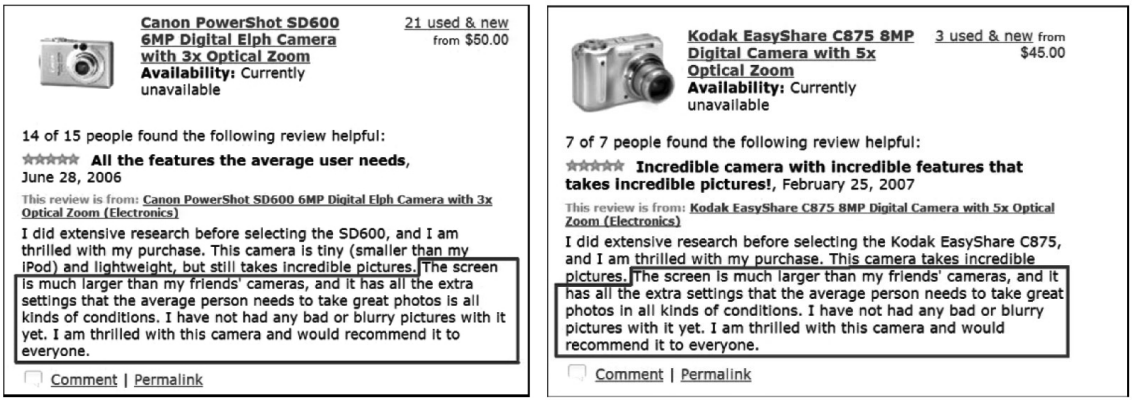


圖 2：兩篇針對不同產品之評論相似度極高

雖然非監督式學習的好處是不用標記資料集，但在分析結果的判讀上，仍需要驗證模型是否能準確衡量。Lau 等人（2011）將執行後結果，透過人工的判斷，以確認是否該模型的確能有效將虛假評論偵測出來。

（三）採取半監督式學習法

在其他研究領域已經發現，與監督式的方法相比，Crawford（2015）[11] 使用未標記的數據結合少量的標記數據可以顯著提高機器學習準確度。協同訓練（co-training）是半監督式學習法一個重要的演算法，係由 Blum 及 Mitchell（1998）[12] 所提出的，是一種使用既有標籤來遞增地將其他未標記的資料進行標記的方法。它將兩組獨立且不同的特徵集各自訓練成兩個分類器。再將未標記的資料用兩個分類器各別進行預測，再把這些樣本加到另一個分類器的訓練集中，讓兩個分類器相互學習。這方法可以有效地在大量的資料集上產生有標記的資料，降低人工參與標記的需求。

二、特徵選取

（一）文章特徵彙總

文章特徵部份，主要著重於與內文分析較無關聯的屬性。本研究除提

11. Crawford, M., Khoshgoftaar, T. M., Prusa, J. D., Richter, A. N., & Al Najada, H.（2015）. Survey of review spam detection using machine learning techniques. Journal of Big Data, 2(1), 23.

12. Blum, A., & Mitchell, T.（1998）. Combining labeled and unlabeled data with co-training. In Proceedings of the eleventh annual conference on Computational learning theory (pp. 92-100). ACM.

出相關文獻的屬性特徵外，亦針對台灣較常見的 Facebook 與 PTT 所提供較特殊之屬性進行整理如「表 5」。

表 5: 各文獻使用過之文章屬性

平台	文章屬性	說明
一般屬性	文章 ID	
	發文者 ID	
	發文時間	
	文章標題	
	文章內容	
	回文與否	判定新發文章或僅為回文
	回文數	
	回其文章的帳號數量	
	文章後第一篇回文時間	
	文章出現數字的比例	
	文章出現驚歎號或問號等特殊符號的比例	
	出現虛假評論常見用語比例	網路上許多提醒消費者辨識虛假文章的常見用語
	文章發送 IP	此部份訊息通常僅限於網站管理者才有
	文章發送位置	此部份訊息通常僅限於網站管理者才有
Twitter	Hashtag 與文章字數的比例	twitter 用「 #」強調主題，寫手多半會用此功能強調主題
	Mention 與文章字數的比例	twitter 用「 @ 」提及某位使用者，寫手多半透過此種方法散布訊息
	URL 與文章字數的比例	透過 URL 的方式將使用者導到寫手想要的地方
	Retweet 次數	文章被轉發的次數

Facebook	心情標籤	哈哈、小花、按讚數等
	文章被分享次數	
PTT	推文種類	推 / 噓
	URL	
	版主標記	版主註記「M」

三、實驗設計與驗證結果

根據本研究的觀察，除了一般研究進行的模型比較外，部份文獻研究方向係以文章相似度判定是否為同一寫手所為，因此使用的資料集則有更多元的取得方式。以 Peng 等人（2016）[13]等人來說，透過各種方式來確認實驗結果，包含：

1. 將同一作者的前半段與後半段進行比對，驗證所提之方法確實測得出高相似度。
2. 於不同網站上找尋三組帳號，根據其帳號相似度或自我揭露之資訊確認是同一人後，取得其文章作為測試並驗證所提方法能用於不同帳號與網站的偵測。惟，此種情況比較不適用寫手，因為帳號沒有在避諱或隱匿寫作風格。
3. 取得三組控制帳號（已知寫手的資訊），經過一段時間後，將帳號的發文結果進行比對，驗證其方法。
   將方法用於實際偵測，找到 3 個帳號，此些帳號較符合真實的寫手情形（會隱匿、不讓人知道是同帳號）。雖然偵測結果顯示，且經作者人工確認，認定某些帳號是同一人，但仍舊無法確定真正答案為何。

肆、Anti-astroturfing之應用與建議

由於有關 Astroturfing 的相關文獻，其所橫跨的領域廣泛，可應用的面向亦非常多元，本研究根據各文獻探討以及觀察將相關應用面向之分類整理如下：

一、一般使用者過濾資訊

根據國家通訊傳播委員會所發布的「105 年民眾申訴廣電媒體內容案件數統計」，52%的申訴案件係與電視廣告不實有關、26% 的申訴案件與廣播電台廣告不實有關。在網路社會中，更頻傳相關糾紛，行政院公平會早於 2010 年即表示，網路廣告不實比重日益增加，2003 年至 2010 年間，有 33. 8% 廣告不實案件為透過網路散布。

對於消費者而言，不實廣告或虛假評論可能對其造成損失，因此已有許多網站如 Consumerist，提供相關判斷準則供消費者參考。

13. Peng, J., Detchon S., Choo, K. R., and Ashman,H.（2016）.Astroturfing Detection in Social Media: a binary n-gram-based approach. Concurrency Computat: Pract. Exper.

二、網站經營者維護信譽

除國外履見不鮮的裁罰案例外，行政院公平會也曾表示，網路商品廣告不實，除供貨商要負責，網路平台、線上購物網站及網拍賣家，雖然不是製造商，但「提供商品」或「服務銷售」，因此須負擔責任[14]。有此考量，亞馬遜提供驗證評論文章真偽的服務（Verified Purchase Review），以確認評論發表人真的是透過 Amazon 購買產品後所撰寫的評論文章，以此作為資訊提高評論文章的可信度。

Google 身為知名的業者，早已透過各種演算法來過濾不當內容，避免人為的輿論操作。近期更在自動搜尋建議及精選摘要中加入了用戶回饋機制，讓用戶舉報不當內容，甚至回饋到偵測演算法中。

三、企業危機管理

危機可能是單一的重大事件，或可能是多重議題的組合，而造成對於營運上的威脅。從三星寫手門事件可以發現，企業除雇用寫手推銷產品或提升形象外，亦可能雇用寫手抹黑競爭對手。對於企業而言，如何在危機事件爆發時，掌握輿論情況，並且辨識相關負面評價是否真為其利害關係團體的看法，勢必成為決策的重要考量。

四、訴訟

在鑑識科學領域中，司法語言學（Forensic linguistics），是司法語言學家利用其語言學的背景為有語言爭議的案件，從語音、語意、語體以及話語結構等角度提供意見甚至專家證據，以協助司法審判的進行。與訴訟有關的司法語言學的，其中一個應用即在為有爭議的書寫文字或作品鑑定作者身份（Author identification），另外還有寫作時間與場合之認定、語料特徵之分析等。最常舉的案例為：1950 年代在英國曾經發生一個 19 歲低智商且文盲的青年 Bentley 因涉嫌教唆朋友開槍打死一名警察而被處死。多年之後，語言學家 Malcolm Couthard 分析了 Bentley 對警察的口供筆錄，發現筆錄中經常出現的一些句法結構不大可能出自 Bentley 之口，而可能有部份是由審訊的警察所編造。此一發現協助促成英國上訴法庭於 1998 年推翻對 Bentley 的指控[15]。

由於網路的可匿名性，許多網路犯罪事件數量在近幾年內成長驚人，犯罪者可能透過匿名電子郵件或網路論壇等，散播對個人或企業不實的言論。對於執法機關而言，如何揪出相關人等，並在現行法治體系下提出相關證明將犯罪者繩之以法，也將是一個重要的應用領域。

伍、結論與未來研究建議

採用文字探勘手法用以偵測 Astroturfing 現象之文獻探討眾多，本研究觀察應已進入成熟期，已有學者開始探討跨網站間不同文章是否為同一寫手所為；此外，近來許多研究開始採用基本的社群網路分析手法，透過分析發文帳號間之關聯以發掘協同運作的寫

14. 曹逸雯。廣告不實案件網路購物就占 1/3 部落客、網拍都要小心。2010 年 11 月 8 日，取自：https://m.nownews.com/news/616858。

15. Derek Bentley case. Retrieved from wiki web site: https://en.wikipedia.org/wiki/Derek_Bentley_case.

手群，成果已相當豐碩。然而，仍有許多社群網路分析技巧可用於分析，未來研究方向可往此方向更加深入。此外，未來方向也可朝結合文字探勘以及社群網路分析兩種方法來進行 Astroturfing 偵測，結合兩種方法的優點，預期將使準確度更加提升。

陸、參考文獻

1. 北京新浪網。大眾點評重拳出擊虛假評價半年處理違規評價近 600 萬條。2017 年 4 月 24 日。取自：http://news.sina.com.tw/article/ 20170424/ 21795810.html
2. 宋海霞、严馨、余正涛、石林宾、苏斐（2013）。基于自适应聚类的虚假评论检测。南京大学学报 : 自然科学版 , 49(4), 433- 438。
3. 林昱叡（2016）。這是業配文嗎？網軍的貼文型態與網絡分析。國立臺北大學資訊管理研究所碩士論文。
4. 翁頌舜、李唯菁（2012）。探索電子口碑對購買意圖影響之研究。國立臺北科技大學資訊與運籌管理研究所碩士論文。
5. 國家通訊傳播委員會。105 年民眾申訴廣電媒體內容案件數統計 (依性別區分)。2017 年 3 月 27 日，取自：http://www.ncc.gov.tw/Chinese/news_detail.aspx?site_content_sn= 1153&is_history= 0&pages= 0&sn_f= 37172
6. 張筱祺（2016）。台灣網購消費者調查分析－整體族群行為。財團法人資訊工業策進會。
7. 張筱祺（2017）。台灣網購消費者調查。財團法人資訊工業策進會。
8. 曹逸雯。廣告不實案件，網路購物就占 1/ 3，部落客、網拍都要小心。2010 年 11 月 8 日，取自：https://m.nownews.com/news/ 616858。
9. 郭旭、祁瑞华（2016）。作者身份识别中不规范文本特征选择方法的研究。现代图书情报技术，(11), 27- 33。
10. 陳曉莉。Google 及臉書雙雙出招再打假新聞。2017 年 4 月 26 日。取自：http://www.ithome.com.tw/news/ 113701
11. 趙安平。謊言年代，如何對假新聞展開逆襲。2017 年 5 月 12 日。取自：https://theinitium.com/article/ 20170512-taiwan-fake-news/
12. 鄭天澤、楊亨利、陳麗霞（2016）。2016 台灣寬頻網路使用調查報告。台灣網路資訊中心。
13. 蘋果日報專案組、法庭中心。蘋果臥底揭網路寫手滲透 56 論壇。2013 年 7 月 5 日。取自：http://www.appledaily.com.tw/appledaily/article/headline/ 20130705/ 35128572/
14. 30 Ways You Can Spot Fake Online Reviews（2010）. Retrieved from Consumerist web site: https://consumerist.com/ 2010/ 04/ 14/how-you-spot-fake-online-reviews/
15. Afroz, S., Brennan, M., & Greenstadt, R.（2012）. Detecting hoaxes, frauds, and deception in writing style online. In Security and Privacy (SP), 2012 IEEE Symposium on (pp. 461- 475). IEEE.
16. Amazon Mechanical Turk（ AMT）,

Retrieved from:

https://www.mturk.com/mturk/

17. Benevenuto, F., Magno, G., Rodrigues, T., & Almeida, V.（2010）. Detecting spammers on twitter. In Collaboration, electronic messaging, anti-abuse and spam conference (CEAS) (Vol. 6, p. 12).

18. Blum, A., & Mitchell, T.（1998）. Combining labeled and unlabeled data with co-training. In Proceedings of the eleventh annual conference on Computational learning theory (pp. 92- 100). ACM.

19. Bonabeau, E.（2004）. The perils of the imitation age. Harvard Business Review, 82, 99- 104.

20. Brennan, M. R., & Greenstadt, R.（2009）. Practical Attacks Against Authorship Recognition Techniques. In IAAI..

21. Burgoon, J., Blair, J., Qin, T., & Nunamaker, J.（2003）. Detecting deception through linguistic analysis. Intelligence and security informatics, 958- 958.

22. Byers, J. W., Mitzenmacher, M., & Zervas, G.（2012）. Daily deals: Prediction, social diffusion, and reputational ramifications. In Proceedings of the fifth ACM international conference on Web search and data mining (pp. 543- 552). ACM.

23. Chen, C., Srinivasan, V., Zhang, X., & Wu, K.（2011）. Battling the Internet Water Army: Detection of Hidden Paid Posters (No. arXiv: 1111. 4297).

24. Chen, Y. R., & Chen, H. H.（2015）. Opinion spam detection in web forum: a real case study. In Proceedings of the 24th International Conference on World Wide Web (pp. 173- 183). ACM.

25. Crawford, M., Khoshgoftaar, T. M., Prusa, J. D., Richter, A. N., & Al Najada, H.（2015）. Survey of review spam detection using machine learning techniques. Journal of Big Data, 2(1), 23.

26. Derek Bentley case. Retrieved from wiki web site:

https://en.wikipedia.org/wiki/Derek_Bentley_case.

27. Gelb, B. D., and Sundaram, S（2002）. Adapting to word of mouse. Business Horizons (45: 4), 2002, pp. 21- 25.

28. Hanson, W. A.（2007）. Principles of Internet Marketing. South-Western College.

29. Iqbal, F., Hadjidj, R., Fung, B. C., & Debbabi, M.（2008）. A novel approach of mining write-prints for authorship attribution in e-mail forensics. digital investigation, 5, S 42-S 51.

30. Jindal, N., & Liu, B.（2008）. Opinion spam and analysis. In Proceedings of the 2008 International Conference on Web Search and Data Mining (pp. 219- 230). ACM.

31. Kamakura, W. A., Basuroy, S., & Boatwright, P.（2006）. Is silence golden? An inquiry into the meaning of silence in professional product evaluations. Quantitative Marketing and Economics, 4(2), 119- 141.

32. Kovic, M., Rauchfleisch, A., & Sele, M.

（2016）. Digital Astroturfing:

Definition, typology, and countermeasures.. Retrieved from osf.io/preprints/socarxiv/ 7ucsh

33. Lau, R. Y., Liao, S. Y., Kwok, R. C. W., Xu, K., Xia, Y., & Li, Y.（2011）. Text mining and probabilistic language modeling for online review spam detection. ACM Transactions on Management Information Systems (TMIS), 2(4), 25.

34. Li, F., Huang, M., Yang, Y., & Zhu, X.（2011）. Learning to identify review spam. In IJCAI Proceedings-International Joint Conference on Artificial Intelligence (Vol. 22, No. 3, p. 2488).

35. Liu, B.（2012）. Sentiment analysis and opinion mining. Synthesis lectures on human language technologies, 5(1), 1- 167.

36. Liu, B., Dai, Y., Li, X., Lee, W. S., & Yu, P. S.（2003）. Building text classifiers using positive and unlabeled examples. In Data Mining, 2003. ICDM 2003. Third IEEE International Conference on (pp. 179- 186). IEEE.

37. Liu, B., Mukherjee, A. & Glance, N.（2012）. Spotting Fake Reviewer Groups in Consumer Reviews. International World Wide Web Conference Committee.

38. Ma, Y., & Li, F.（2012）. Detecting review spam: Challenges and opportunities. In Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on (pp. 651- 654). IEEE.

39. Mihalcea, R., & Strapparava, C.（2009）. The lie detector: Explorations in the automatic recognition of deceptive language. In Proceedings of the ACL-IJCNLP 2009 Conference Short Papers (pp. 309- 312). Association for Computational Linguistics.

40. Montes-y-Gómez, M., & Rosso, P.（2013）. Using PU-Learning to Detect Deceptive Opinion Spam. WASSA 2013, 38.

41. Ott, M., Cardie, C., & Hancock, J. T.（2013）. Negative Deceptive Opinion Spam. In HLT-NAACL (pp. 497- 501).

42. Ott, M., Choi, Y., Cardie, C., & Hancock, J. T.（2011）. Finding deceptive opinion spam by any stretch of the imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies-Volume 1 (pp. 309- 319). Association for Computational Linguistics.

43. Peng, J., Detchon S., Choo, K. R., and Ashman, H.（2016）.Astroturfing Detection in Social Media: a binary n-gram-based approach. Concurrency Computat: Pract. Exper.

44. Pennebaker, J. W., Booth, R. J., & Francis, M. E.（2007). LIWC 2007: Linguistic inquiry and word count. Austin, Texas: liwc.net.（註：已改成 http://liwc.wpengine.com/）

45. Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A., & Menczer, F.（2011）. Detecting and Tracking Political Abuse in Social Media. ICWSM, 11, 297-304.

46. Rout, J., Dalmia, A., Choo, K. K. R., Bakshi, S., & Jena, S.（2017）. Revisiting semi-supervised learning for online deceptive review detection. IEEE Access, 5(1), 1319- 1327.

47. Senecal, S. & Nantel, J.（2004）. The influence of online product recommendations on consumers' online choices. Journal of Retailing, Volume 80, Issue 2, 2004, Pages 159– 169.

48. Zheng, R., Li, J., Chen, H., & Huang, Z.（2006）. A framework for authorship identification of online messages: Writing style features and classification techniques. Journal of the American society for information science and technology, 57(3), 378- 393..

視覺化與機器學習協同整合之增強分析—以風險視覺化為例

The Augmented Analytics Integrated with Visualization and Machine Learning: Illustrated by Risk Visualization

孫嘉明
國立雲林科技大學會計系
黃學昌
國立雲林科技大學會計系

摘　要

近年來人工智慧蔚為風潮，機器學習可以加速資料分析或提高決策結果準確度，但如何才能有效提升人類決策能力呢？機器學習是否可能成為決策黑箱，造成決策的盲點，或是導致使用者的抗拒？

為了彌補機器學習在解釋上的不足，本研究將機器學習所挖掘之繼續經營疑慮法則，進一步以學者提出的視覺化分析知識生成模型及結合杜邦分析法之財務指標，並以風險視覺化儀表板呈現分析結果；後續則透過使用者訪談，評估與回饋視覺化介面的決策效益。研究目的在於評估系統使用者在分析財務報表過程中，藉由操作互動式視覺化圖表是否有利於理解及驗證機器學習模型所辨識之財務危機決策規則。目的之二則是探討使用者如何結合視覺化工具與機器學習模型，達到兼俱正確性與可解讀性之綜合效果。

本研究經過使用者評估發現，應用視覺化與機器學習協同整合之視覺化分析知識生成模型，所產製的財務預警儀表板，確實有助於使用者增強理解機器學習分析

結果，並可深入分析各指標變動趨勢，促使提升分析人員對資料之敏感度，提供證據以即時採取相應之措施。

關鍵詞：增強分析、機器學習、視覺化分析、財務預警、風險視覺化。

Abstract

Artificial intelligence has become a trend in recent years. Machine learning can accelerate data analysis or improve the accuracy of decision-making results. But how can it effectively improve human decision-making capabilities? Is it possible that machine learning can become a decision-making black box, causing blind spots in decision-making, or causing users' resist?

In order to make up for the deficiencies of machine learning in explanation, this research applies the rule of continuous operation doubts excavated by machine learning process, and adopts the theory of Knowledge Generation Model for Visual Analytics combined with the financial indicators of DuPont analysis method, and present them with financial risk dashboard; follow-up through user interviews to evaluate and feedback the decision-making benefits of the visual interface. The purpose of the research is to evaluate whether system users can understand and verify the financial crisis decision-making rules identified by the machine learning model by operating interactive visual dashboards in the process of business analytics. The second purpose is to explore how users can combine visualization tools and machine learning models to achieve a comprehensive effect of correctness and interpretability.

Through user evaluation, this research found that the application of the Knowledge Generation Model for Visual Analytics that integrates visualization and machine learning to produce financial risk dashboards does help users to enhance their understanding of the results of machine learning analysis and can provide in-depth analysis. The trend of changes in various indicators urges analysts to increase their sensitivity to data and provide evidence to take immediate measures.

Keywords: Augmented analytics, Machine learning, Visual analytics, Financial warning, Risk visualization.

壹、人工智慧與人機協同整合

近年來人工智慧蔚為風潮，帶動了新一波工業 4. 0 的科技發展，人工智慧的核心發展與應用在人臉及圖像辨識、語音辨識、大數據資料分析、機器翻譯、機器學習等面向蓬勃發展，這些技術對許多產業未來的發展有著顛覆性的影響。其中機器學習結合了強大的電腦運算能力及大數據，可針對特定的問題，運用複雜的數學計算建立預測模型，將不同數據間的關聯特徵顯現出來，有助於日後快速有效地處理類似問題（孫嘉明，2018）。

機器學習可以加速資料分析或提高決策結果準確度，但如何有效提升人類決策能力呢？機器學習是否可能成為決策黑箱，造成決策的盲點，或是導致使用者的抗拒 (孫嘉明，2019) ？因此，可解讀性 (interpretability) 與準確性 (accuracy) 之間的取捨成為使用機器學習演算法的基本問題；因為對人們易於理解的演算法，其準確性通常低於相對較難理解的演算法 (Goodrum, 2016)。

可解讀性的挑戰在於其為主觀的模型評估，在於對人類而言，該模型是否易於解釋，與使用者對於目標問題之背景知識、資料來源內容、演算法程序以及分析結果之解讀能力等有關。相較而言，模型的準確性則為可量化的客觀指標，易用於評估模型是否能夠正確預測結果。所以目前人工智慧的研究發展上，所提出的演算法大多以「準確性 」為衡量優劣的標準，但如何提高模型的「 可解讀性 」，過去一直被忽略，近來才逐漸受到關注 (孫嘉明，2019)。

如同產業 4. 0(或稱工業 4. 0) 在各種不同領域引入人工智慧的應用，其中與過去自動化應用的最大差異在於利用產業 4. 0 技術打造「 人機協同 」的工作環境，而不是取代人力。如最早提出「 擴增智能 」概念的 Engelbart(1963) 所指出 :「 不主張用人工智慧取代人類的思考，而是主張人類心靈的直覺天賦，應該要和機器處理資訊的能力整合，才能把人類的預感、即時反應、同理心等，與高效能電子產品裡運作異常複雜的嚴謹邏輯，以及精簡的術語、符碼等，共同組合成完整實用的知識領域 」(Engelbart，1963)。因此人與電腦運算之間的關係已由傳統的人員主導分析的「 操作模式 」(如圖 1a)，逐漸演進為人員自資訊系統擷取所需資訊的「 協助模式 」(如圖 1b)、或進一步發展為由電腦系統先進行資料前置處理以提供人員評估所需資訊及評估後續分析與決策方向的「 增能模式 」(如圖 1c)。

如將資訊系統類型與上述三種不同的人機模式相互類比，傳統交易處理系統或管理資訊系統偏向為「 操作模式 」; 早期的商業智慧系統（ BI：Business Intelligence）偏向為「 協助模式 」; 目前結合機器學習、視覺化分析 (visual analytics)、文字探勘等進階分析技術，一般統稱為增強分析（ Augmented Analytics），即趨向「 增能模式 」發展，更加著重電腦分析能力，Gartner 公司提出將成為未來數據分析的重要發展趨勢（ Gartner, 2019）; 但顯然人員也需要不同於傳統資訊系統的分析技能，人機協同的互動介面及分析程序，也與以人員為主導的操作或協助模式有所不同。

人類主要以領域知識來解讀資訊系統分析處理所產出的資訊，決策者更是需要資訊系統能夠提供決策支持證據，或是協助其

思考推論過程。但一般的機器學習分析結果並未提供與領域知識相關的決策資訊。因此，本研究所期望探究的第一個研究問題為：機器學習分析程序，由來源資料、建立模型到分析結果，如何提高其可解讀性，轉換為具領域知識意涵的決策資訊？

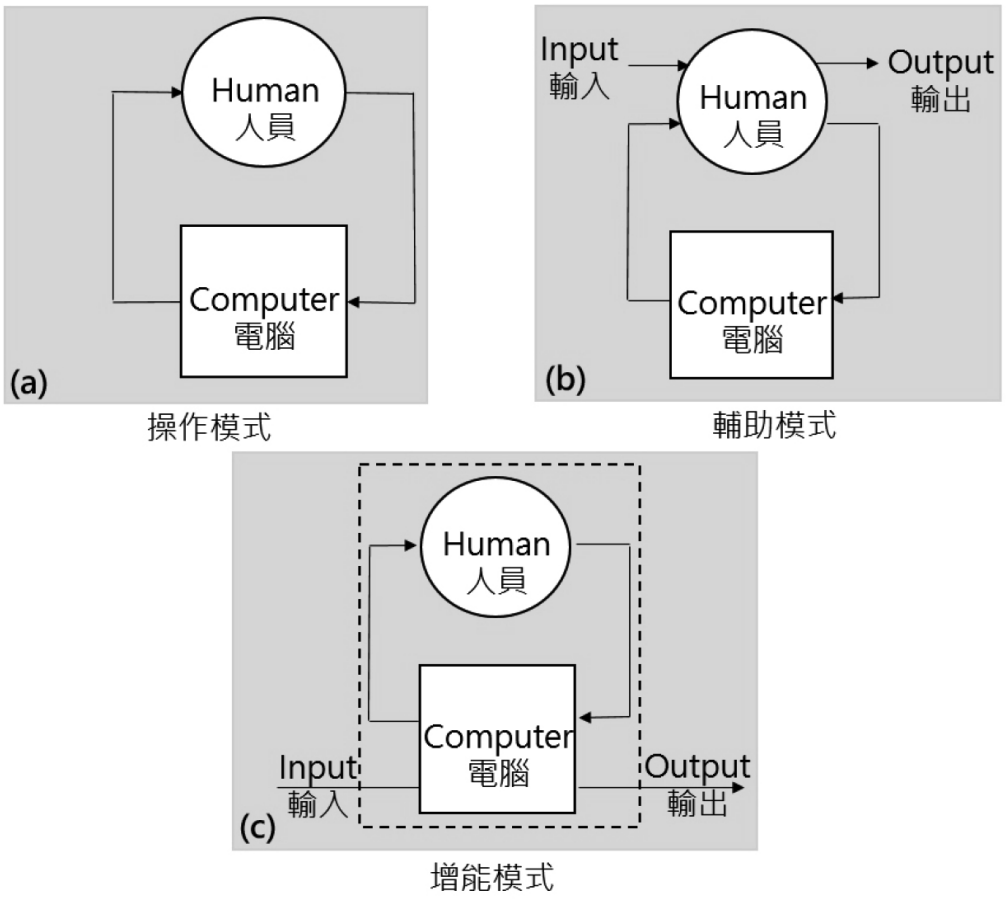


圖 1：三種不同的人機協同模式

近年來，以視覺化分析技術（visual analytics）解讀機器學習分析結果已成為重要的新興實務與研究領域。因為，視覺化分析技術不單只是如傳統視覺化方法（visualization）將資料結果以靜態的圖形加以表達；視覺化分析強調結合動態可操作之視覺化圖表，考量人員因素與資料分析技術，所進行的互動決策程序。因此，多位學者也提出視覺化分析與機器學習兩者可相互彌補其不足之處：視覺化分析有助於更直觀地檢視機器學習的分析結果，機器學習則以電腦的快速運算能力客觀地探索與驗證資料間的潛在關係 (Fayyad et al., 2002; Yeh, 2006)。

因此，如利用易於解讀的領域知識以表達機器學習模型的決策規則，並透過視覺化分析呈現其分析或預測結果，將可以提高資訊接受者對於分析結果的信任程度，並且幫助決策者以其所熟悉的領域知識，驗證評估模型決策規則或預測結果的正確性。故本

研究所將探究的第二個研究問題為：如何結合視覺化分析工具，以幫助決策者更能直觀地驗證或評估機器學習模型所提供的決策資訊？

貳、視覺化分析與機器學習

視覺分析是一門由互動式視覺化介面所支持的分析推理科學。許多問題的複雜性質使得在資料分析過程中需加入人類智慧判斷。視覺化分析方法可以使決策者結合人類的靈活性、創造力和背景知識與電腦能大量儲存及處理的能力去洞察複雜的問題（Cook & Thomas，2005）。使用先進的視覺化介面，人類可以直接與電腦資料分析的功能互動，使他們在複雜情況下做出明智的決定（Keim, et al., 2008）。

資訊視覺化 (data visualization) 的設計特性是利用人類解決問題的感知與認知能力去創造資訊的互動式視覺表達方式（Ware, 2004），而資訊視覺化的目標是讓使用者能更簡單的了解和解釋大量且複雜的資訊。為什麼視覺化表達，可以提高理解呢？因為對於多數人而言，將資料間的關係，以各種圖形結構（如：叢集、階層、分散程度、差異幅度）等不同表達方式，相對於大量的原始表格資料或是抽象的數學模型，都較容易解讀。在閱讀圖形所表達的結構或關係時，不但可幫助決策者找出資料間的潛在關係，也有助於理解或驗證電腦系統的計算結果是否可靠而值得信賴。

可見，適當地結合視覺化分析技術與機器學習，將得到互補的效果。例如 : 在資料前置處理階段，資料視覺化將有助於選擇相關聯的資料屬性以及偵查出異常值（outlier）；在資料分析階段，則可提供選擇適當演算方法的參考訊息；在資料分析結果的整理活動中，視覺化分析將有助於分析結果中找尋潛在的洞見（insight）與意涵 (Witten and Frank, 2000)。

機器學習結合視覺化分析已成為人機協同整合應用重要的發展方向，如：Sacha、Sedlmair、Zhang、Lee、Weiskopf、North 與 Keim（2016）即認為視覺化分析的目標是集結自動化的數據分析（例如機器學習）與互動式視覺化，來解決複雜的問題。在資料的範圍過於複雜且龐大，且不容易查看原始數據情況下，分析數據問題的本質是很困難的；因此透過機器學習分析探勘資料是不可避免的。但其應用的關鍵在於將人們的知識、見解和反饋過程納入分析之中，不僅可以調整模型並且可以改進修正人們現有的知識與前先的分析假設。如下圖 2 階段 A，資料分析人員可以對資料進行清理、編輯或增加數據；階段 B 主要為了預先對下一階段 C— 模型選擇與建立，對資料進行轉換或標準化；階段 D 為探索與直接操作，此步驟可以進行簡單的互動式視覺化，並對先前的相關設定進行更動調整合；最後階段 E 強調由資料分析人員透過易於了解的視覺化圖表介面進行互動與驗證，如此可更有效的驗證機器學習結果或探索確認視覺化分析所得到的洞見，再次進行模型調整或驗證。

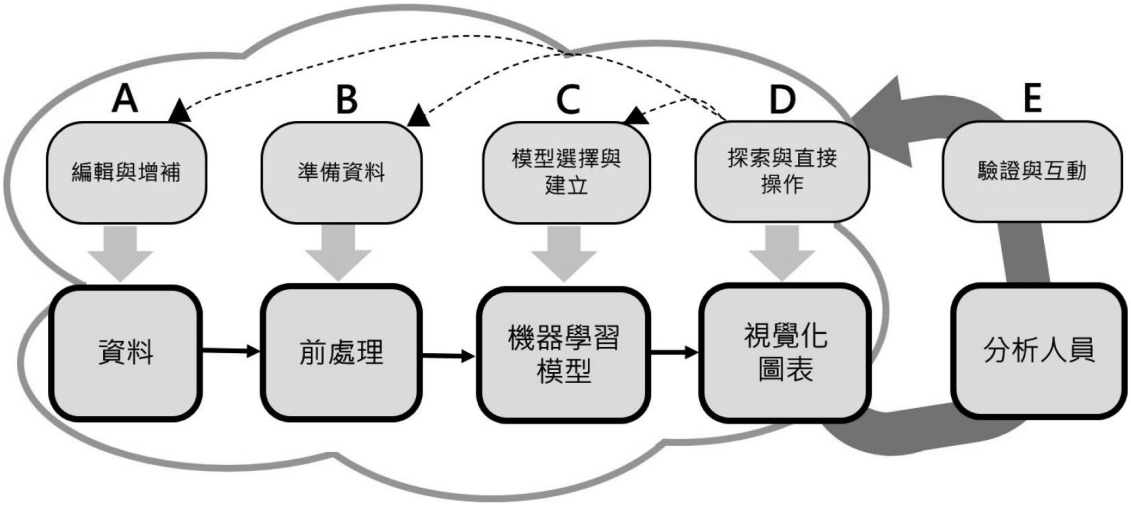


圖 2: 以人為中心的機器學習架構

（修改自：Sacha 等人，2016）

叁、風險視覺化分析

風險視覺化為在組織的風險管理中，使用互動的風險視覺化圖像，以提高整個風險管理過程的風險分析和溝通品質（ Eppler &Aeschimann，2009）定義。風險視覺化採用圖表、概念圖、視覺隱喻和製圖技術，以提高對風險的理解和後續管理。其制定風險視覺化框架的目標可分為三大層面：首先，展示風險視覺化的範圍；換言之，強調風險視覺化在何處和何時可以提供效益，並應被風險管理人員視為有用的工具；第二，提供一個視覺化風險或風險相關訊息時需考慮的關鍵因素清單；第三，展示風險視覺化的互補資訊，以應用於風險管理、治理及溝通當中，有效進行與風險相關的決策。

Shneiderman 在 1996 年即提出視覺資訊探索過程的重要程序：「瀏覽、聚焦、篩選，然後針對需要的部分再詳細探索 」。視覺化的起點通常僅提供比較高階的瀏覽資訊，再使用互動介面展現部分的明細內容，再剔除不感興趣的部分，以及增加需求項目的資訊。為此，視覺化的資訊揭露過程，有很大部分是來自人員操作的媒介，不但能提昇風險資訊相關的互動交流，也促進大數據的視覺呈現。Husdal（2001）則提出應用視覺化技術及編製圖形的過程，有助於自在地探索風險和促進相關人員的溝通。風險事件的視覺化，透過展現不確定性和風險因子的變異程度，可以提高對這些事件的認識。可用的視覺化技術，例如：資料剖析、風險移轉分析、歸因 / 分解，以及與歷史、規章、同業等的比較，這些功能皆有利於改進風險分析和強化洞察力。

近年來視覺化儀表板已成為商業智慧（ Business Intelligence）解決方案的一部份，且提供組織所關切的關鍵績效指標資訊（ Gannholm，2013）。「儀表板 」是一個圖表化的動態操作介面，可以呈現出一個或多個視覺化之重要資訊目標，將其編排至同一視窗，藉此一目了然監測資訊（ Few，2013）。隨著視覺化分析技術與風險管理之普及，以風險視覺化方式呈

現之儀表板也逐漸成為監理機關監督控管以及組織與內外部進行風險溝通的基本工具（Sarlin，2016）。

肆、結合人機整合之風險視覺化應用實例

Sacha、Stoffel.A、Stoffel.F、Kwon、Ellis與 Keim（2014）提出視覺化分析的知識生成模型（如圖 3）。此模型由左半部為以電腦為核心的資料處理活動，以及右半部之人員邏輯思考活動所組成。在左半部的電腦處理活動中，又包含了兩大流程；分別為下方的「資料庫知識探索」（Knowledge Discovery in Databases，KDD）流程，以及上方的「資訊視覺化」流程。「資料庫知識探索」，包含了 Fayyad 等人（1996）針對資料探勘程序所提出著名的五階段模型：分別是選擇（selection）目標資料，經過初步的資料前處理（preprocessing）再轉換（transfer data）為易於分析處理的資料型態，接著探勘出資料的特徵（patterns）最後經由專家評估獲得知識。上方則是結合 Keim 等人（2008）所提出「資訊視覺化」流程，主要將以符號為主的文數資料轉為更具體易於理解的視圖。值得注意的是：先前文獻大多未能明確說明人們如何理解與互動操作這些數據分析結果並且採取決策與行動。然而電腦缺少人員分析解讀就無法在數據間推論出令人耳目一新的重要問題；反之，人們也無法如同電腦一樣高效能處理計算大量的數據。所以此一知識生成模型的優點在於：解析了在人機協同互動當中，人與電腦之間如何倚靠著互動式操控介面與持續挖掘問題與驗證假設的「意義建構」（sense making）過程。該過程主要包含了探索循環、驗證循環、知識產出循環等三個不同的互動層次。茲簡述如下：

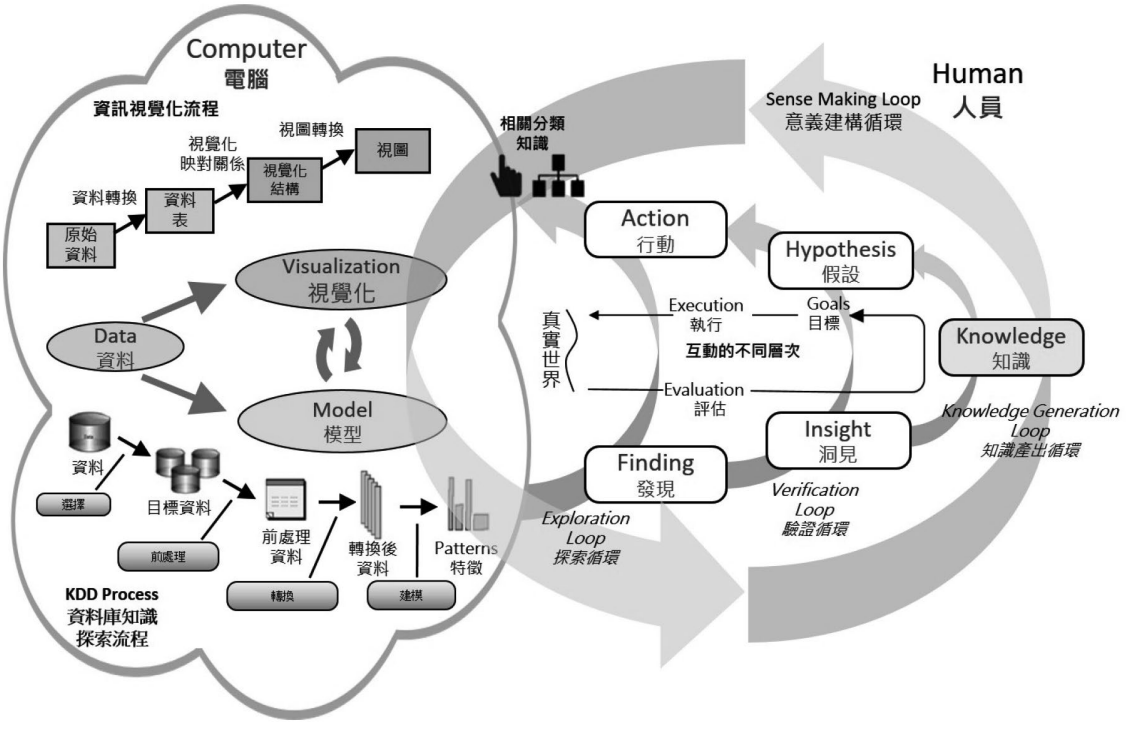


圖 3：視覺化分析之知識生成模型
（修改自：Sacha 等人，2014）

一、**探索循環（Exploration Loop）：**此部分為使用者與電腦系統間的直接互動，閱讀及操作已產生的視覺化圖表或模型並分析數據。使用者通常針對某一具體的目標進行探索，以找尋所期望的回饋資訊，雖然系統所產出的結果不一定符合預期。Bertin 等人（2011）提到回饋可以幫忙人員的感知和理解，對當前的狀態與行為進行調整，以改變現狀，並可以補強增進電腦系統兩大流程：知識探索和視覺化之間的互補與修正。在下一個驗證循環中，更是可以運用所發現得到的回饋作為基礎以進行驗證。

二、**驗證循環（Verification Loop）：**為了驗證具體的假設，使用者試圖從圖表中探索出支持或牴觸假設的證據，透過收集足夠的證據獲得新知識。Sacha 等人（2014）認為在解讀機器學習或視覺化分析結果所啟發的洞見（insight），仍可能因為證據不足，可能存在偏誤不能直接做為知識，所以需要針對與洞見相關的假設進行驗證。

三、**知識產出循環（Knowledge Generation Loop）：**分析人員可以依其個人專業知識或與不同領域專家進行討論，由收集到的證據識別是否接受洞見成為新知識或進一步調查。視覺化分析能夠使我們分析大量的資訊，藉此支持複雜的決策和數據探索（Sacha et al.，2014）。

以下示例係以主計總處「中華民國行業標準分類」中的電子產業為分析對象，並利用自臺灣經濟新報資料庫（Taiwan Economic Journal, TEJ）中所收集證交所公開資訊重大訊息，所標註發生財務危機事件企業樣本資料作為訓練資料集，財務危機類別亦採用 TEJ 之分類原則定義[1]，並加註於表 1。本研究建立機器學習所使用之企業財報資料範圍取自 TEJ 資料庫，研究樣本係以「TEJ IFRS Finance- 國際會計準則」資料庫下的「IFRS 以合併為主財務（累計）- 一般產業 IV」作為選取對象，選取條件為：（一）公司別：所有上、市櫃公司；（二）資料期間：2008 年 1 月 1 日至 2015 年 12 月 31 日之財務資訊（含公司基本資料）；進一步將機器學習所歸納之分類法則（如表 1；機器學習模型之建置流程細節可參考：蔡賢民，2016），結合視覺化分析以展示知識生成模型之人機協同整合流程，透過不同層次分析循環反覆驗證機器學習成果法則之合理性，以協助使用者評估標的公司之財務概況，及時採取對應之策略。

1. 本研究從 TEJ 的公司屬性資料庫中之項次 82 整理出企業的發生危機事件，數種不同類別之危機事件雖可能同時或相繼發生，該資料庫此處欄位僅註記最近一次的事件類別。

表 1：決策樹模型的財務預警分類法則

電子產業	
法則 1	被預測為非財務危機公司的法則
1	if D 2 股東權益報酬率 >= - 12（ %）
法則 2	被預測為財務危機公司的法則
2- 1	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 < - 30（ %）and C 5 固定資產週轉率 < 0. 88 ）then 重整公司 (註 1)
2- 2	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 < - 30（ %）and C 5 固定資產週轉率 >= 0. 88 and D 9 營業利益率 < - 34（ %））then 繼續經營疑慮公司 (註 2)
2- 3	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 >= - 30（ %）and D 7 毛利成長率 < - 26（ %）and A 3 長期資金適合率 >= 55（ %））then 紓困公司 (註 3)
2- 4	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 >= - 30（ %）and D 7 毛利成長率 < - 26（ %）and A 3 長期資金適合率 < 55（ %））then 重整公司
2- 5	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 >= - 30（ %）and D 7 毛利成長率 >=- 26（ %）and D 6 每股盈餘 >= - 1. 2 ）then 繼續經營疑慮公司
2- 6	if（ D 2 股東權益報酬率 < - 12（ %）and D 9 營業利益率 >= - 30（ %）and D 7 毛利成長率 >= - 26（ %）and D 6 每股盈餘 < - 1. 2 ）then 淨值為負公司 (註 4)

註： 以下財務危機分類之定義，主要依據經濟新報資料庫的定義說明（參考網址如下：http://www.tej.com.tw/webtej/doc/wind1.htm），其中又分為 9 類實質財務危機事件與 7 類準財務危機事件共計 16 類。在本資料模型分析期間中，電子產業只有出現以下 4 類：

1. 重整：公司聲請重整。
2. 繼續經營疑慮：會計師對公司之繼續經營假設提出疑慮、就重大科目作保留、出具無法表示意見或否定意見等。
3. 紓困公司：向財政部申請紓困；向銀行要求展延、減息並掛帳；個別要求或召開債權人會議。以上三者只要發生其一即是。
4. 淨值為負：公司淨值為負數且經營層無增資打算。

一、探索循環（Exploration Loop）

1. 建構模型（Modeling）

此處使用前一系列研究蔡賢民（2016）的機器學習分析結果作為示例，該研究以歷史資料進行學習建立企業財務危機預警模型，並經由決策樹分析建立了電子產業財務危機的分類法則。

2. 視覺化（Visualization）

此階段使用經濟新報資料庫下載之原始資產負債表、綜合損益表，依據視覺化分析程序將原始的財務報表資

料整理並轉換為視覺化軟體可接受的資料格式。後續使用視覺化分析軟體，將資料以歷年趨勢折線圖、直條圖、圓餅圖等，製作為財務預警之風險儀表板，以利使用者進行探索與驗證循環。

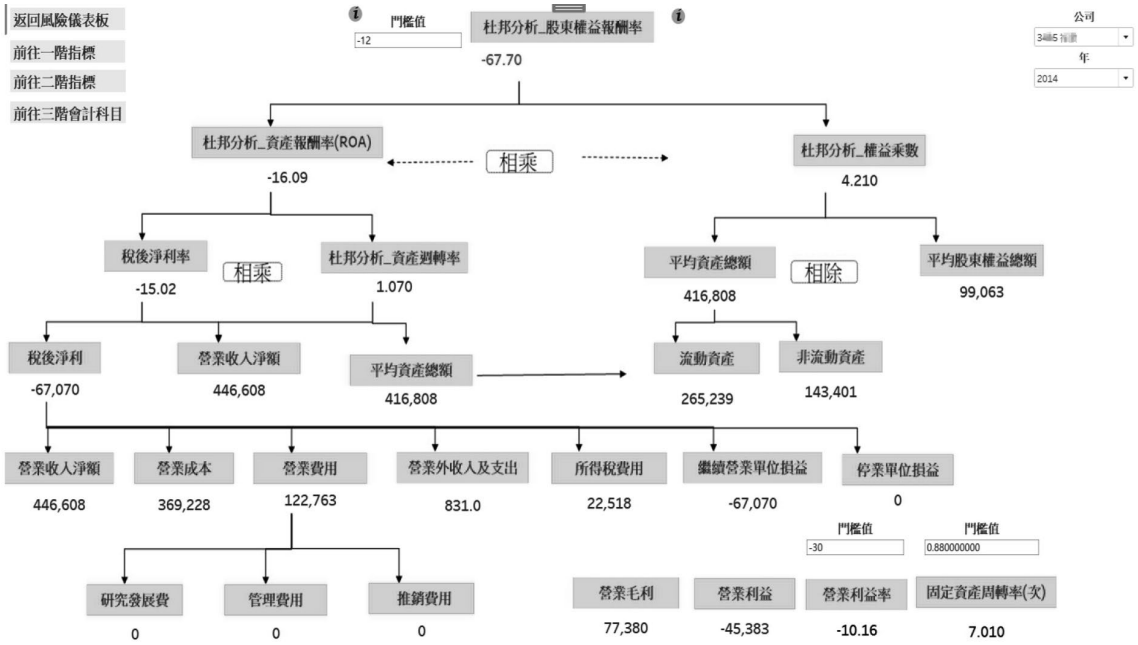


圖 4 結合杜邦分析與機器學習結果之風險儀表板

圖 4 為以杜邦分析為基礎呈現架構之財務風險儀表板，該儀表板可主動依據上述機器學習分析結果所歸納的多項危機公司預測法則以顏色進行預警標示，例如：依據其中的一項法則，如果股東權益報酬率 >- 12% 則預測非財務危機公司，數值會呈現黑色，反之 < - 12% 呈現紅色。因此使用者可依據紅色預警指標項目進一步檢索前先所定義的一、二、三階指標相關數據，反覆進行探索循環及驗證循環，以評估此公司是否的確為財務危機公司。

二、驗證循環（Verification Loop）

驗證循環與探索循環彼此緊密相依，在驗證的過程中可能意外發現其他相關資訊而進行探索循環，經由發現（ finding）或觀察再次的回到驗證循環建立假說並洞察出薄弱證據所在，以此不斷的循環直至收集足夠證據，進入知識循環。

1. 假設（Hypothesis）

此階段依據使用者在先前探索循環所得到的回饋，進行問題探索及建立假設。在本示例中以先前決策樹分析結果中權重佔比最高的前兩項重要預警指標，分別為股東權益報酬率及營業利益率，作為動態圖表分析面向，以比較財務危機公司與同業非財務危機公司之間的軌跡變動差異。

2. 洞察（Insight）

透過杜邦分析的資訊結構，可便於使用者遵循著財務知識框架，理解財務報表的經營成果，藉由互動介面發

展推理過程；例如：使用者可由比率的變動幅度、歷年趨勢、會計科目的組成比例，經由驗證循環的假設並獲得證據，最後建構成為新發現的領域知識。如圖 5 中可明顯看出在 2015 年發生財務危機的個案公司在前三年的股東權益報酬率持續下滑，營業利益率甚至到了 2015 年跌到 - 47. 95%。右邊股東權益報酬率及營業利益率的表格深淺圖可明顯看出個案公司分析期間在這兩項指標的績效表現明顯低於同業。

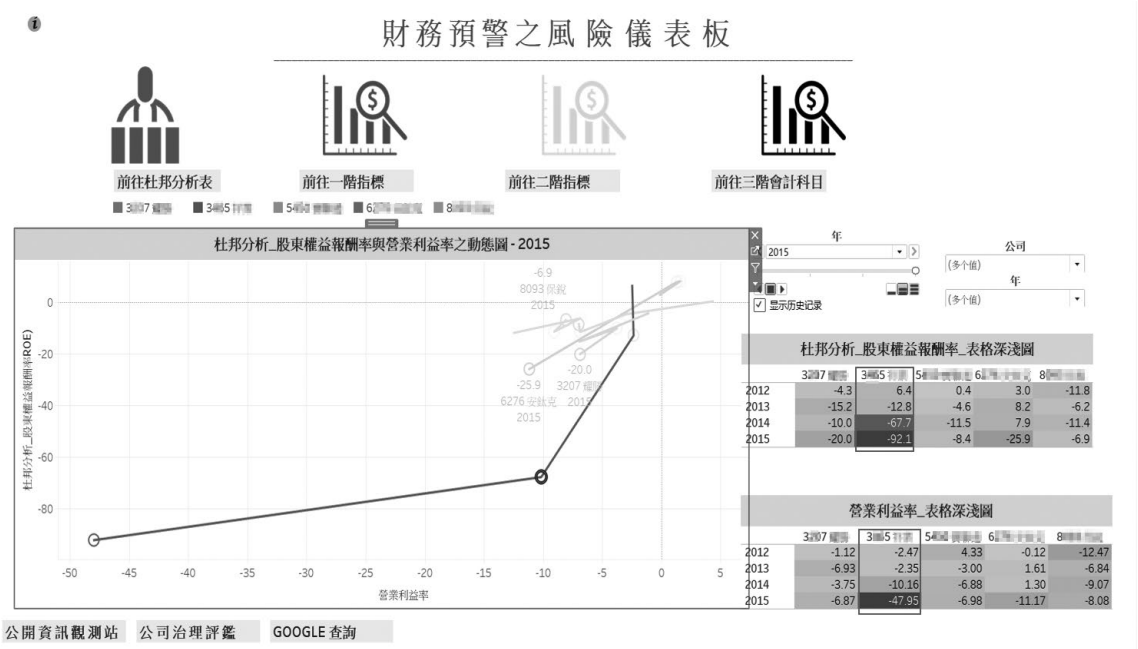


圖 5: 基於機器學習所挑選財務預警指標之風險視覺化呈現

在本示例中應用 Sacha 等人（2014）所提出的視覺化分析之知識生成模型理論，透過視覺化儀表板中以機器學習所探索出的財務危機公司分類法則找出高風險的公司；進一步以分類法則中的重要指標：股東權益報酬率及營業利益率，以折線圖呈現給使用者直觀的視覺分析結果，一眼即可判斷異常公司之變動軌跡。

另一方面，也可透過基於杜邦分析的儀表板（如圖 4），針對超過門檻值之異常指標，依據杜邦分析的指標組成關係，分階層以有邏輯的方式將不同財務資訊依序向下展開探索問題所在。例如：本示例中將杜邦分析架構圖中的股東權益報酬率、總資產報酬率、權益乘數歸類為一階指標，將稅後淨利率、資產周轉率歸類為二階指標，接著將資產負債表之科目歸類為三階指標。依據各階層指標的組成相關資訊，各再細部提供各層次的財務指標風險分析儀表板。例如：於前次驗證循環得知個案公司在 2015 年被預測為財務危機公司，為此需要更多的證據。可將股東權益報酬率、資產報酬率、權益乘數等以歷年折線圖一同觀察同業狀況 (如圖 6 一階指標同業比較圖)，評估個案公司是否因經濟環境的波動與同業間發生一致的情況，亦或是個案公司可能未及時改善經營策

略或個別錯誤決策，而遭受較大的財務衝擊。經由圖 7 三階指標負債趨勢圖中，明顯得知個案公司在 2014 年確實有大量的發行公司債，以充盈資金，進而導致 2014 的權益乘數達到歷年新高。(註：此處受限於篇幅僅能以上述部分圖表簡述其設計理念，並未能完整呈現各項指標資訊組成關係以及意義建構循環中透過探索、驗證及知識產出的反覆過程；細部展現過程可參考：黃學昌，2018。)

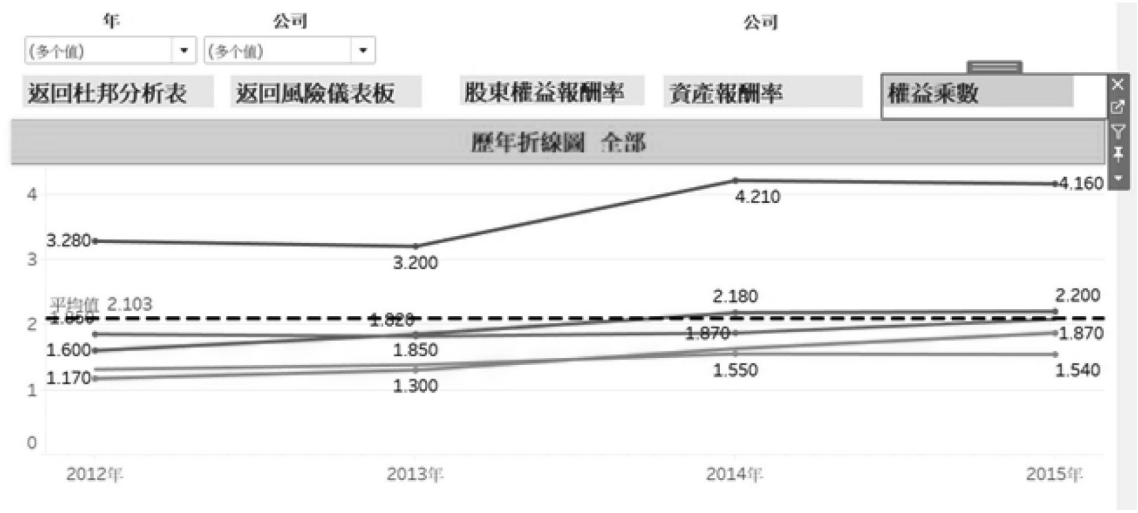


圖 6：一階指標同業比較圖－權益乘數折線圖

圖 7：三階指標－負債趨勢圖

伍、結論與建議

如同本文前文所提到：如何兼顧機器學習之可解讀性與準確性，才能有效輔助使用者有效進行決策。隨著產業界各領域均積極於擴展使用各種基於機器學習演算法的智能決策分析系統的當下，更是應當考量應用新興科技背後的決策風險與黑箱效應。如：歐盟 2018 年所實施的通用資料保護規則（ General Data Protection Regulation, GDPR）中即明定：當人們的權益受到與演算法相關的決策所影響時，當事者有權要求執行者提出解釋（ Goodman & Flaxman, 2016）。另外一項要求則是：與演算法相關的決策必須是可供測試評估的（ contestable），亦即應當要基於可測試的假設進行明確的推論；或是提供簡易的方式，以測試模型的執行結果或決策是否有可能受到不當的操控或偽造（孫嘉明，2019）。

為了擴展機器學習在財務資訊之風險評估應用，本文建議可將一般人認為複雜難懂的機器學習模型建構過程，加入更為直覺易懂的風險視覺化圖表分析。過去研究中，多位學者也提出視覺化分析與機器學習兩者可相互彌補其不足之處：視覺化分析有助於更直觀地檢視機器學習的分析結果，機器學習則以電腦的快速運算能力客觀地探索與驗證資料間的潛在關係。對於非機器學習領域專長的一般使用者而言，更是可以透用簡單快速的視覺化互動分析工具（ Visual Analytic Tools）以動態圖形分析、理解並解釋其分析結果。

在視覺化分析工具選擇上，雖然 Python 或 R 語言提供了各種視覺化圖表元件，然而對於不善於程式語言的一般使用者而言，並不容易自行使用或調整這些視覺化程式元件。因此，本文建議就使用者端的資料呈現與規則探索驗證方面，可結合一般使用者容易自主使用的自助式企業智慧分析工具（ Self-Service BI Tools）。其優點為：分析人員或決策主管無需等待資訊人員協助，即可隨時彈性依需求與分析考量，自行進行即時分析、建立或動態改變所需報表。因此，資訊人員無需隨時支援各單位臨時性報表需求，可以更專注於資訊策略發展或系統維護；如此，使用者與資訊人員將可各自發揮專業與所長。

另外，建議可運用視覺化分析之知識生成模型，以利於引導財務風險視覺化儀表板設計及讓使用者在操作互動式視覺化圖表時快速呈現及探索由機器學習所預警的潛在財務風險。如有效運用知識生成模型中三個循環的分析流程，將有助於系統使用者，以具有邏輯結構且熟悉普及的財務指標呈現其變動趨勢，驗證風險發生的可能性；並且依循多階細部指標向下展示其細部資訊，將能直觀地從中了解比率變動的細部原因。如此，便可透過機器學習與視覺化分析之人機協同整合應用，提高決策效益且減低機器學習黑箱效應所產生的負面影響。

參考文獻

中文部分

1. 孫嘉明，2018，雲端運算環境下審計數據分析之發展趨勢與挑戰，月旦會計實務研究，2018/ 07(7)，54- 61。
2. 孫嘉明，2019，可解讀性：人工智慧技

術在會審產業應用的關鍵因素？，月旦會計實務研究，2019/ 03(15)，13- 26。

3. 蔡賢民，2016，採領域驅動資料探勘方法進行財務預警分析，國立雲林科技大學會計系研究所碩士班論文。
4. 黃學昌，2018，財報分析之風險視覺化效益評估，國立雲林科技大學會計系研究所碩士班論文。

英文部分

1. Bertini，E.，Tatu，A.，&Keim，D.（2011). Quality metrics in high-dimensional data visualization: An overview and systematization. IEEE Transactions on Visualization and Computer Graphics，17(12)，2203- 2212.
2. Cook，K. A.，& Thomas，J. J.（2005）. Illuminating the path: The research and development agenda for visual analytics.
3. Engelbart, D.C. ,“A Conceptual Framework for the Augmentation of Man’s Intellect,”Vistas in Information Handling, P.D. Howerton and D.C. Weeks, eds., Spartan Books,Washington,D.C., 1963, pp. 1– 29.
4. Eppler，M. J.&Aeschimann，M.（2009）. A systematic framework for risk visualization in risk management and communication. Risk Management，11（2），67- 89.
5. Fayyad，U.，Piatetsky-Shapiro，G. & Smyth，P. (1996). From data mining to knowledge discovery in databases. AI magazine，17(3)，37.
6. Few，S. (2013). Information Dashboard Design: Displaying data for at-a-glance monitoring. Analytics Press.
7. Gannholm，L. (2013). A Comparative Evaluation Between Two Design Solutions for an Information Dashboard.
8. Gartner, (2019), How Augmented Analytics Will Transform YourOrganization: A Gartner Trend Insight Report,
9. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. AI Magazine, 38(3), 50- 57.
10. Goodrum, W. (2016). Finding Balance: Model Accuracy vs. Interpretability in Regulated Environments. HP.
11. Husdal , J .（2001）. Can it be really that dangerous? Issues in visualization of risk and vulnerability, http://www.husdal.com/ blog/ 2001/ 10/can-it-really-b.html, accessed 26 June 2008.
12. Keim，D. A.，Mansmann，F.，Schneidewind，J.，Thomas，J.，& Ziegler，H. (2008). Visual analytics: Scope and challenges. In Visual data mining (pp. 76- 90). Springer，Berlin，Heidelberg.
13. Sacha，D.，Sedlmair，M.，Zhang，L.，Lee，J. A.，Weiskopf，D.，North，S.，&Keim，D.（2016，August）. Human-centered machine learning through interactive visualization. ESANN.
14. Sacha，D.，Senaratne，H.，Kwon，B. C.，Ellis，G.，&Keim，D. A.（2016）. The role of uncertainty，awareness，and trust in visual analytics. IEEE transactions on visualization and computer graphics，22（1），240- 249.

15. Sacha，D.，Stoffel，A.，Stoffel，F.，Kwon，B. C.，Ellis，G.，&Keim，D. A.（2014）. Knowledge generation model for visual analytics. IEEE transactions on visualization and computer graphics，20（12），1604- 1613.

16. Sarlin，P.（2016）. Macroprudential oversight，risk communication and visualization. Journal of Financial Stability，27，160- 179.

17. Shneiderman，B.（1996）. The eyes have it: A task by data type taxonomy for information visualizations. In Visual Languages，1996. Proceedings.，IEEE Symposium on 336- 343. IEEE.

18. Ware, C. (2012). Information Visualization: Perception For Design. Elsevier.

19. Witten, I. H., & Frank, E. (2005). Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.

20. Yeh, R. (2006). Visualization techniques for data mining in business context: a comparative analysis. Proceedings from Decision Science Institute, 310- 320.

Evolution of Smart Governance – The Past, Present and Future of Governance and Auditing

TSE W K Daniel
City University of Hong Kong, Instructor
SHI Rong
City University of Hong Kong, Postgraduate student

Abstract

With the rapid booming of modern businesses, huge volume of transactions is generated in shorter period. In addition, because of the business globalization which involves more than one party in a transaction, the transaction information has become more complicated than before. Besides, the high popularity of big data analytics has made the huge amount of data processing more complicated. All these have affected the effectiveness or efficiency of governance substantially. In this paper, the topics of smart governance and continuous auditing are discussed in terms of their past and current aspects.

Keywords: Smart governance,Continuous auditing,Modern businesses,Globalization, Big data analytics

1. Introduction

In the past few decades, the rapid booming of modern businesses and globalization as well as the adoption of big data analytics has increased the complexities and volume of business transactions. This would in turn affect the efficiency and effectiveness of governance. Because of this, the need for improving corporate governance becomes important.

The World Bank first mentioned the concept of "governance crisis" in "Sub-Saharan Africa: From Crisis to Sustainable Growth" (1989). Since then, research on governance began to arouse widespread attention.However, it was not until the "Our Global Partnership" issued by the Global Governance Council in 1995 that governance was defined as "the sum

of the many ways in which various public or private individuals and institutions manage their common things", which is currently the most representative explanation.

Because of modern rapidly changing technologies, Sriram et al. (1992) claimed that auditors could no longer effectively use conventional audit techniques which were suitable for manual environment. On the other hand, auditors had to develop audit techniques to improve audit efficiency. This started the need for continuous or concurrent auditing.

2. The Past of Governance and Auditing

With the development of society, Stephen Goldsmith and William D. Eggers began to propose the concept of network governance in "Network Governance: A New Form of Public Sector". Network governance (without involvement of information technology) is a governance model in which non-profit organizations, for-profit companies, etc. participate extensively in the provision of public services through the cooperation of corporate departments.

Primarily, auditing is a kind of assurance attesting the integrity of all accounting records. Because of the governance issues, auditing has included all aspects relating to the assets of an organization. Nowadays, nearly all organizations are using computer systems for their businesses. Thus, traditional manual auditing has been largely transformed into information systems auditing or computer auditing. In fact, the names of information systems auditing, computer auditing and traditional auditing have been used interchangeably.

3. Present situation of Governance and Auditing

Warren et al. (2006) considered that business is dynamic and change is constant. Technology continues to change and become more complex. Thus, companies seek new technologies to enhance their business processes. In fact, technology is a driving force for positioning businesses in the global market. Besides, big data analytics is one of the critical success criteria in modern business and such big data should have excellent data governance. This gives rise to the need of smart governance which can effectively and efficiently monitor the whole business operations.

Scholars such as M Holzer, ST Kim (2006) and ME Milakovich (2012) began to propose the concept of digital governance. Digital governance is to promote the interactive relationship between government and non-governmental organizations through the use of information technology, and to improve the democratization of public governance.

Although the concept of smart governance was proposed shortly after digital governance, its definition is still vague until now. Smart governance is a multi-faceted research content; the most basic content includes two

aspects, smart and governance. Therefore, scholars' research on smart governance is also multifaceted. Based on information and communication technology, Schuurman et al. (2012) believe that smart governance is the process of collecting and processing information in the process of public governance. Giffinger (2007) and Giuffre et al. (2012) believe that providing citizens with new communication channels is a good way of smart governance. Gil-Garcia (2012) believes that smart governance is a new type of electronic governance that uses complex information technology to integrate and process information between organizations and provide better services to citizens.

Based on research on external cooperation and participation, Giffinger et al. (2007) also proposed that smart governance is a service that improves democratization. Batagan (2011) believes that it is to improve inter-departmental cooperation for economic growth and improve the quality of services for citizens. Kourtit et al. (2012) believe that an open governance structure can improve the efficiency of urban operations. Willke (2007) proposed that smart governance is a cross-departmental collaborative communication to achieve governance purposes.

Based on the research of internal collaboration, Batty et al. (2012) proposed that smart governance is a stronger inter-departmental collaboration method to strengthen the links within the government or within the business. Willke (2007) also pointed out that smart governance is to strengthen the collection of principles, factors, and capabilities in response to emergencies. Gil-Garcia (2012) also believes that integrating the information within the enterprise and better processing this information is the primary task of smart governance.

Based on the decision-making process, Walravens (2012) proposed that smart governance is a technological means of decision making and decision making. Barrionuevo et al. (2012) believe that smart governance is the way that the smart governance system recognizes the current situation and proposes a strategic plan and finally implements it. Willke (2007) believes that smart governance is a comprehensive assessment of principles, factors and capabilities and provides a structure for decision-making.

Based on e-administration, Giffinger et al. (2007) proposed that smart governance constitutes an updated administrative management method that allows more citizens to participate in politics. At the same time, they believe that the e-administration brought about by smart governance, e-democracy provides Better communication channels to citizens. Nam (2012) believes that it improves the possibility of smart cities, and that with a smart governance framework; smart cities can be created more actively. Batty (2012) believes that smart governance is only the improvement of government management. Willke (2007) believes that smart governance brings more

possibilities for social contact with electronic administration. Odendaal (2003) believes that e-governance gives government agencies the opportunity to deliver services and information to the public online.

Based on the purpose of smart governance, Batagan (2011) believes that smart governance will ultimately enhance citizens' sense of being served and economic growth. Caragliu et al. (2009) believe that the ultimate goal is to improve the quality of social public services for citizens. Kourtit et al. (2012) believe that the goal is to increase the economic and urban ecological performance in response to negative externalities and historical growth path dependence.

Due to the eruption of smart governance, information systems auditing has to be transformed. Shah (2020) considered that the concept or the vision of auditing has been subject to many changes during the recent decades. Shah (2020) also suggested that since the environment is constantly changing, the principles and methods on which the essentials of audit focus need to change, so as to produce robust and efficient results which can be relied upon by all. The output of the transformation is called continuous or concurrent auditing. By definition, there is a slight difference between continuous auditing and concurrent auditing: Concurrent auditing are the techniques which can be run continuously or periodically depending on whether the expected losses associated with the exceptions identified are low or not. Thus, the two terms can be used interchangeably. Broadly speaking, Everythingwhat (2020) mentioned that concurrent auditing techniques are tools that auditors use to collect audit evidence on the reliability of a computer-based application system at the same time as the application system carries out live operational processing of transaction data. It involves the ongoing automated examination of business processes. This is achieved by embeddingauditsub-routines into the application systems used by employees to process transactions. The system then flags unusual transactions for review by theaudit staff.

Clark et al. (1989) defined concurrent auditing techniques as the tools that auditors use to collect audit evidenceon the reliability of a computer-based application system at the same time as the application system carries out live operational processing of transaction data. They are implemented via program instructions that are embedded within the application software or within the system software, such as the database management system, that supports the application system. According to Putra (2020), such techniques can address the problems of:i) disappearing paper-based audit trail because of the use of computer systems; ii) difficulties of performing transaction walkthroughs because of outsourcing or proprietary software (without the source code) used; iii) the need for timing identification of errors and irregularities for immediate response to the adverse environment especially in big data analytics; iv) presence of

entropy in systems due to the normal wear or outdated technologies; v) increased exposures when errors and irregularities found due to rapid proliferation of incorrect information; vi) increased incidence of distributed information systems because of advanced technologies like internet of things; vii) increased integration of information systems due to the increasing complexity of business process and viii) the need for more effective and efficient audits because stakeholders have various information needs. All the above problems appear in smart governance arena.

4. The Future of Smart Governance

At present, the application of smart governance is mainly reflected in the following five aspects: smart healthcare, smart agriculture, smart education, smart energy, and smart transportation.Information technology began to be used in medicine in the 1950s. During the next sixty years of development, it has developed into an independent discipline, medical informatics. At the very beginning, Ledley (1959) mentioned the process of using computer technology to assist medical diagnosis in "Science". Ledley (2006) proposed Hospital Information System (HIS), Laboratory Information System (LIS) and Picture Archiving and Communication Systems (PACS). In recent years, smart medicine has undergone further research. In the research of smart hospitals, Fuhrer et al. (2006) proposed to carry RFID technology in the entire hospital for rapid identification and recording of patient information. Yu et al. (2012) proposed a smart hospital framework based on the Internet of Things to solve the inflexibility of traditional hospital information systems. On the other hand, in the research of telemedicine, AkinobuUchikubo (2001) designed a set of practical application patents of telemedicine system, which is used to connect the information interaction between patients and remote doctors. Jurik et al. (2008) in the research of remote medical monitoring proposed the combination of computer software and hardware, so that remote monitoring of the patient's physical condition can be achieved. The latest application research, in the research of wearable mobile devices, Cox et al. (2018) uses wearable and mobile sensors to monitor the real-time status of cancer, which is helpful for doctors to detect the patient's physical abnormality in time. Boysenet al. (2017), Kaib et al. (2016) are mainly focused on the practical research of smart wearable devices, such as research on waterproof and power supply methods, so as to make better use of these devices.

In terms of smart agriculture, McKEE et al. (2018) applied for a patent on an animal collar system to monitor the state of animals at all times to achieve the purpose of scientific breeding. Gondchawar et al. (2016) proposed IoT-based smart agriculture, which monitors the data of cultivated land in real time through the series connection of various sensors and

mobile devices. Opara et al. (2001) proposed the concept of food traceability. The latest research by Badia-Melis et al. (2016) proposes to connect the current food traceability information to other information systems to make the smart governance ecology more perfect.

Smart education means that teachers and students can complete teaching tasks through mobile devices, no longer limited to traditional teaching models, and at the same time integrate campus work, study and life governance on the basis of the Internet of Things. Sharples et al. (2005) put forward the concept of mobile education, and Sharples et al. (2009) proposed the integration of all aspects of mobile education to form an overall system Smart governance program. Alghamdi et al. (2016) proposed the application of IoT to smart campuses in order to provide better services and better evaluate teaching quality.

Smart energy mainly includes two aspects: improving daily electricity consumption and electricity consumption in public facilities. The book of Y Strengers (2013) proposed a smart energy management system suitable for the home for energy use feedback, smart pricing and other aspects. Mathiesen et al. (2015) proposed intelligent monitoring in the traffic process to intelligently control the energy use of public facilities.

The current main application scenarios of intelligent transportation include traffic management, personal travel, environmental protection, and future application research such as unmanned vehicle technology. Q Yang, HN Koutsopoulos proposed a set of dynamic intelligent traffic management system as early as 1996, which is used to evaluate traffic conditions and make route suggestions. Vaid et al. (2002) proposed the application of traffic management system in intelligent traffic control. Golob et al. (2001) proposed the application of information technology in personal travel to solve the choice of transportation and cost control during personal travel. Al-Sakran (2015) proposed an intelligent transportation information system to monitor pollution emissions and provide better smart governance solutions. Burke et al. (1992) put forward the factors that need to be considered in the future of unmanned vehicle technology. Jarrell (2015) designed a patent on information exchange, monitoring and congestion management between urban vehicles.

On the basis of existing applications in multiple fields, future development will pay more attention to how to aggregate the existing separate smart governance applications to bring out the greater use of smart governance. Atzori (2015) put forward the idea of decentralized governance in the future, and explored whether the government still needs to exist in the case of using multiple information technologies (mainly blockchain technology) to create decentralized political governance in the future. Hill et al. (2006) proposed that a multi-party governance model and multiple governance frameworks will be implemented in the future

to deal with increasingly complex governance issues. Pereira et al. (2018) studied the infrastructure of smart cities based on smart governance in the future through a literature review. Kulkarni et al. (2020) analyzed how smart governance translates into various aspects of good governance in smart cities.

5. Future aspect of Continuous Auditing

Warren et al. (2006) considered that a continuous audit should focus on all processes including those that are not a component of the financial report and also be akin to a supervisory review more than the traditional 'after-the-fact' review as well as relying on analysis that cross corporate business processes and address risks. Besides, it should also focus on anomalies and can include models that perform analytic procedures. However, Warren et al. (2006) also claimed that there are some impediments to continuous auditing. Such impediments can fall into three categories, namely, people, process and technology. People impediments include lack of client resources to provide audit schedules and lack of appropriate auditor skill set, therefore staff retention is very important. Process impediments include client control environment and closing process not adequate and the issues with current audit model. Technology impediments include client systems not adequate or properly integrated and also better technology audit tools required. All those impediments require time for adoption. However, the most important impediment is the investment required to develop and implement a continuous auditing process and also the difficulty to cost-justify or calculate a return on investment. In addition, under globalization, business practices and culture of each country differ.

6. Conclusion

Governance is one of the cornerstones of successful modern businesses. To have more effective and efficient governance, smart governance has to be adopted. Without proper continuous auditing techniques implementation, smart governance cannot be achieved. In other words, to have smart governance, proper continuous auditing is required and such implementation requires management support, availability of appropriate skills, the clear baseline criteria and aligned technology infrastructure.

7. References

1. Alghamdi, A. and Shetty, S., (2016),August.Survey toward a smart campus using the internet of things.In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)(pp. 235- 239).IEEE.
2. Al-Sakran, H.O., (2015), Intelligent traffic information system based on integration of Internet of Things and Agent technology. International Journal of Advanced

Computer Science and Applications (IJACSA), 6(2), pp. 37- 43.

3. Atzori, M., (2015), Blockchain technology and decentralized governance: Is the state still necessary?.Available at SSRN 2709713.
4. Badia-Melis, R., Mishra, P. and Ruiz-García, L., (2015), Food traceability: New trends and recent advances. A review.Food control, 57, pp. 393- 401.
5. Barrionuevo, J.M., Berrone, P. and Ricart, J.E., (2012), Smart cities, sustainable progress.IESE insight, 14(14), pp. 50- 57.
6. B t gan,L., (2011), Smart cities and sustainability models Informatica Economic , 15(3), pp. 80- 87.
7. Batty, M., Axhausen, K.W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G. and Portugali, Y., (2012), Smart cities of the future.The European Physical Journal Special Topics, 214(1), pp. 481- 518.
8. Boysen III, L. and Vaughan, M.W., Sol Cuff Technologies, LLC, (2017),Wearable mobile device charger.U.S. Patent 9, 553, 475.
9. Burke, S.A., Liang, C.Z. and Hall, E.L., Tennant Co, (1992), Guiding an unmanned vehicle by reference to overhead features. U.S. Patent 5, 155, 684.
10. Caragliu, A., Del Bo, C. and Nijkamp, P., (2009), Smart cities in Europe, series research memoranda 0048.VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics, pp. 2009- 48.
11. Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J.R., Mellouli, S., Nahon, K., Pardo, T.A. and Scholl, H.J., (2012), Understanding smart cities: An integrative framework. In 2012 45th Hawaii international conference on system sciences(pp. 2289- 2297).IEEE.
12. Clark, Groomer & Murthy (1989), “An empirical analysis of the accounting information systems course”, Journal of Information Systems, Fall, 10(2), pp 103-127
13. Cox, S.M., Lane, A. and Volchenboum, S.L., (2018), Use of wearable, mobile, and sensor technology in cancer clinical trials. JCO Clinical Cancer Informatics, 2, pp. 1-11.
14. Everythingwhat (2020), https://everythingwhat.com/why-do-auditors-use-concurrent-audit-techniques
15. Fuhrer, P. and Guinard, D., (2006),Building a smart hospital using RFID technologies: use cases and implementation. Fribourg, Switzerland: Department of Informatics-University of Fribourg.
16. Giffinger, R., Fertner, C., Kramar, H. and Meijers, E., (2007), City-ranking of European medium-sized cities.Cent.Reg. Sci. Vienna UT, pp. 1- 12.
17. Gil-Garcia, J.R., (2012), Towards a smart State ? Inter-agency collaboration,information integration, and beyond.Information Polity, 17(3, 4), pp. 269- 280.
18. Giuffrè, T., Siniscalchi, S.M. and Tesoriere,

G., (2012), A novel architecture of parking management for smart cities.Procedia-Social and Behavioral Sciences, 53, pp. 16-28.

19. Goldsmith, S. and Eggers, W.D., (2005),Governing by network: The new shape of the public sector. Brookings institution press.

20. Golob, T.F. and Regan, A.C., (2001), Impacts of information technology on personal travel and commercial vehicle operations: research challenges and opportunities.Transportation Research Part C: Emerging Technologies, 9(2), pp. 87-121.

21. Gondchawar, N. and Kawitkar, R.S., (2016),IoT based smart agriculture. International Journal of advanced research in Computer and Communication Engineering, 5(6), pp. 838- 842.

22. Hill, M. and Hupe, P., (2006), Analysing policy processes as multiple governance: accountability in social policy.Policy & Politics, 34(3), pp. 557- 573.

23. Holzer, M. and Kim, S.T., (2006), Digital governance in municipalities worldwide (2005): a longitudinal assessment of municipal websites throughout the world.

24. Huang C., Peng G., Su J. (2017). Smart Governance. China: Tsinghua University Press.

25. Jarrell, J.A., (2015), Unmanned aerial vehicle communication, monitoring, and traffic management. U.S. Patent 9, 087, 451.

26. Jurik, A.D. and Weaver, A.C., (2008), Remote medical monitoring.Computer, 41(4), pp. 96-99.

27. Kaib, T.E., Volpe, S.S. and Clark, J.G., ZOLL Medical Corp, (2016), Water resistant wearable medical device.U.S. Patent 9, 427, 564.

28. Kourtit, K., Nijkamp, P. and Arribas, D., (2012), Smart cities in perspective–a comparative European study by means of self-organizing maps.Innovation: The European journal of social science research, 25(2), pp. 229- 246.

29. Kulkarni, P. and Akhilesh, K.B., (2020), Big Data Analytics as an Enabler in Smart Governance for the Future Smart Cities. In Smart Technologies(pp. 53- 65).Springer, Singapore.

30. Ledley, R.S. and Lusted, L.B., (1959), Reasoning foundations of medical diagnosis.Science, 130(3366), pp. 9- 21.

31. Mathiesen, B.V., Lund, H., Connolly, D., Wenzel, H., Østergaard, P.A., Möller, B., Nielsen, S., Ridjan, I., Karnøe, P., Sperling, K. and Hvelplund, F.K., (2015), Smart Energy Systems for coherent 100% renewable energy and transport solutions. Applied Energy, 145, pp. 139- 154.

32. McKEE, J.T., Basone, M.A. and Heberto, J., Smart Pet Technologies LLC, (2018), Smart animal collar system. U.S. Patent Application 15/ 258, 635.

33. Milakovich, M.E., (2012), Digital governance: New technologies for

improving public service and participation. Routledge.

34. Odendaal, N., (2003), Information and communication technology and local governance: understanding the difference between cities in developed and emerging economies.Computers, Environment and Urban Systems, 27(6), pp. 585- 607.

35. Opara, L.U. and Mazaud, F., (2001), Food traceability from field to plate.Outlook on agriculture, 30(4), pp. 239- 247.

36. Pereira, G.V., Parycek, P., Falco, E. and Kleinhans, R., (2018), Smart governance in the context of smart cities: A literature review. Information Polity, 23(2), pp. 143- 162.

37. Putra Lie Dharma (2020), http:// accounting-financial-tax.com/ 2009/ 10/ concurrent-auditing-techniques/

38. RamSriram, Glenn Sumners (1992), “Understanding Concurrent Auditing Technqiues”, TheEDP Audit, Control, and Security Newsletter, July 1992 Vol. XX, No. 1

39. Schuurman, D., Baccarne, B., De Marez, L. and Mechant, P., (2012), Smart ideas for smart cities: Investigating crowdsourcing for generating and selecting ideas for ICT innovation in a city context.Journal of theoretical and applied electronic commerce research, 7(3), pp. 49- 62.

40. Shah C J Jimil (2020), http://cajimilshah.weebly.com/traditional-vs-modern-techniques-of-auditing.html

41. Sharples, M., I., Arnedillo-Sánchez, M. Milrad, &G. Vavoula,(2009). Mobile learning: Small devices, big issues. Technology-Enhanced Learning, pp. 233-249.

42. Sharples, M., Taylor, J. and Vavoula, G., (2005), October.Towards a theory of mobile learning.InProceedings of mLearn(Vol. 1, No. 1, pp. 1- 9).

Strengers, Y., (2013), Smart energy technologies in everyday life: Smart Utopia?.Springer.

43. Uchikubo, A., Olympus Corp, (2008), Remote medical supporting system.U.S. Patent 7, 386, 730.

44. Vaid, A., Putta, S. and Rakoshitz, G., Micro Focus Software Inc, (2002),Directory enabled policy management tool for intelligent traffic management. U.S. Patent 6, 502, 131.

45. Walravens, N., (2012), Mobile business and the smart city: Developing a business model framework to include public design parameters for mobile city services.Journal of theoretical and applied electronic commerce research, 7(3), pp. 121- 135.

46. Warren Donald, Smith Murphy (2006), “Continuous Auditing: An Effective Tool for Internal Auditors”, Internal Auditing, 21(2), pp 27- 35

47. Willke, H., (2007),Smart governance: governing the global knowledge society. Campus Verlag.

48. Yu, L., Lu, Y. and Zhu, X., (2012), Smart hospital based on internet of things.Journal of Networks, 7(10), p. 1654.

資訊及相關技術的管理、控制與稽核（COBIT）於政府部門

Using COBIT in Government Departments

作者：Panduranga Bichal
COBIT建置人員ISO 27001 LI、ITIL專家、
PRINCE2 Practitioner執業人員、TOGAF

譯者：魏銷志
國立臺北科技大學 資訊與財金管理系助理教授
CISM,CISA,CRISC,CISSP

印度政府注重提供有效率的政府服務予客戶。政府的客戶包含市民、商業機構、遊客或任何在日常活動中需要與不同階級政府部門互動的個體。印度政府的目標是，除了透過科技應用外，能做更多來改善市民的生活。

印度總理目前以透過利用任務的方式來解決公共衛生、醫療保健及都市化問題。例如：普惠金融，即以平民化的價格提供金融服務予廣大的弱勢及低收入群體。普惠金融含多項任務，如表 1 所示。

表 1：政府達成普惠金融的方案

任務	目標	對象
人民財富計畫方案 (JDY)	藉由普惠金融提供金融服務予印度各社會階層	確保所有印度家庭至少有一個銀行帳號
社會福利 — 事故保險方案 (PMSBY)	幫沒有保險的窮困及弱勢人士設置全民社會保險制度	提供 20 萬印度盧比的意外死亡暨傷殘保險予 18- 70 歲人士
社會福利 — 人壽保險計畫方案 (PMJJBY)	特別針對沒有保險的窮困及弱勢人士制定全民社會保險制度	提供 20 萬印度盧比的人壽保險予 18- 50 歲人士

養老保險金方案 (APY)	解決老人社會保障的需求	18- 40 歲人士於滿 60 歲後每月可領一筆固定金額的退休金
微型企業發展和融資機構方案 (Mudra)	提供資金給小型或微型企業以鼓勵其創業	提供簡易貸款予 5 千 7 百萬個小型企業
為所有人提供住房計劃方案 (PMAY)	解決都會區窮人對住宅的需求	讓 2 千萬個都會區窮人於 2022 年以前能擁有自己的住宅

資料來源：www.narendramodi.in。已取得同意在此轉載。

為了達成這些目標，各政府部門會利用 IT 來建立可執行這些任務的各種活動的系統，並藉由該系統來監督執行成果以追蹤進度，繼而回報給負責這些任務的高級管理階層。IT 很明顯地在執行這些任務的各個層面均扮演了很重要的角色以促使各階層政府部門官員能達成和完成這些任務的目標。

政府部門裡的各個領域專家們，有些並無或只有些許的 IT 知識。他們大多仰賴於外部顧問（ IT 公司 ）來滿足他們的 IT 需求。因此，企業與 IT 間的溝通便有了隔閡，進而造成 IT 創造出對企業利害關係人而言低價值或無價值的 IT 產品的情形。最終，造就了一群不滿意的 IT 產品使用者。

對IT治理的需求

IT 治理的主要目標在確保在 IT 上的投資能產生商業價值並減少 IT 風險。這可以透過建立一套組織結構來達成。這組織結構應賦予各個負責資訊、業務流程、應用及基礎架構的人員一個明確的角色。

IT 治理應被視為是 IT 可創造出與企業組織整體策略並容的價值，而非別樹一幟。如此一來，企業組織利害關係人均應參與 IT 決策過程。藉此，大家對關鍵性系統所作的決策均負共同責任，並可確保所有與 IT 有關的決策均係因企業組織需求而為。

儘管軟體業者致力於認定並採取一套適用於發展 IT 項目的最佳實務規範，然而實務上仍有很高的失敗率及未達標的情形。大多數的 IT 項目均無法達成企業組織的目標。

最佳實務規範的要點在採用一個組織結構。這個組織結構必須具有高效率的治理架構，且對 IT 利害關係人的角色和責任有明確規範。這樣的架構始可確保在 IT 上的投資能符合並達到組織的目標及策略。

如果沒有這個架構，IT 項目就會比較容易失敗。然而，許多企業組織仍然不正視 IT 治理的重要性。他們在開始執行 IT 項目時並不完全了解企業組織對該項目的需求及該項目與企業組織目標的關聯性。

如果要成功，企業組織需要考慮以下所有的要素：高層次架構、獨立保證、績效管理報告機制、資源管理、風險管理、策略一致性及價值傳遞。這些要素均包含於最佳實務規範裡。

在所有適用於 IT 治理及管理的架構裡，COBIT 5 架構特別適合，因為它幫助管理階層拉近介於控制需求、技術挑戰及商業風險之間的差距。COBIT 藉由組織結構讓政策發展更明確化，且讓 IT 控制更能符合

最佳實務規範。COBIT 注重合規、協助企業組織強化由 IT 得到的價值、一致性並將企業 IT 管理及控制架構的應用簡單化。

COBIT 的 5 個原則如圖 2 所示。這些原則協助企業組織用不同於常態的方式來使用 IT。也就是說，IT 常被視為一個僅為管制成本的中心，對協助企業組織達成他們目標僅能提供些許幫助或完全沒有幫助。

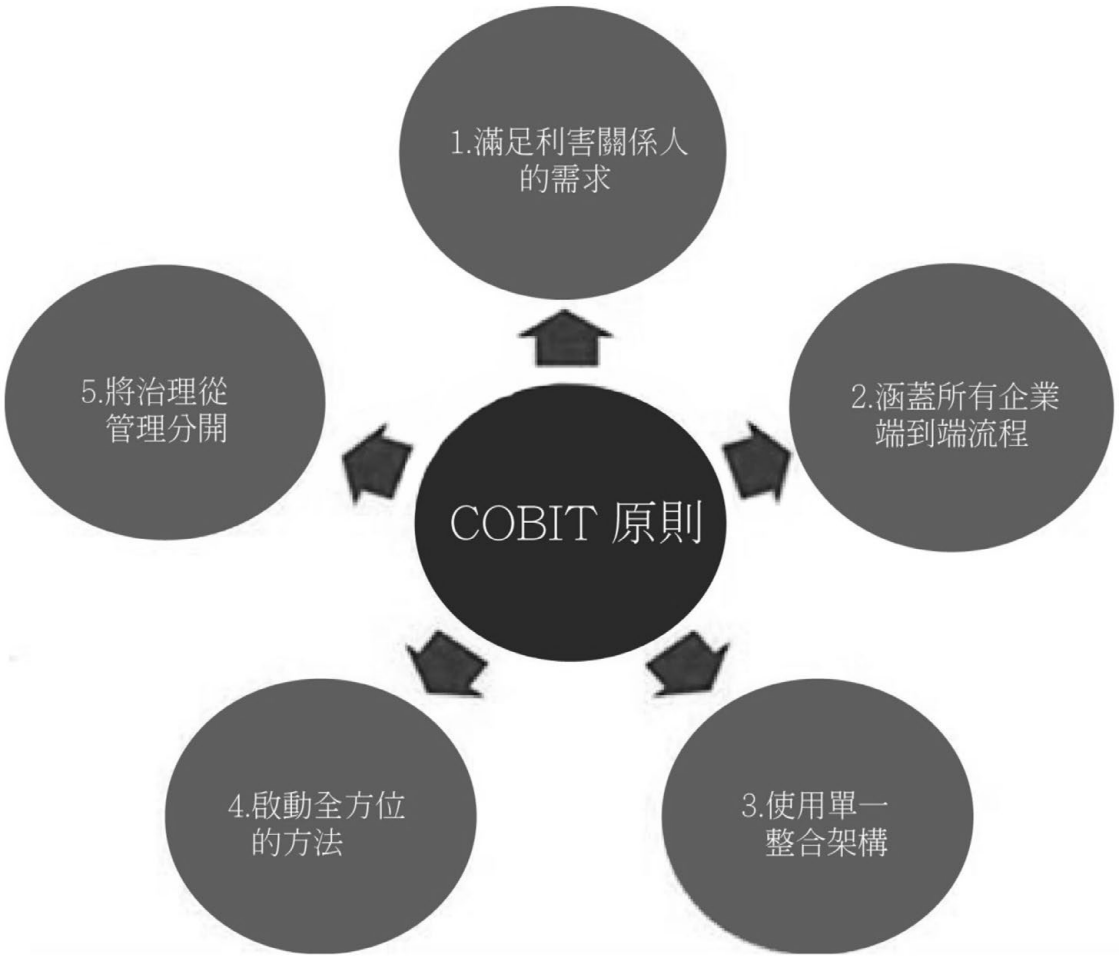


圖 2 - COBIT 5 原則

資料來源：國際電腦稽核協會（ISACA),COBIT 5, 美國，2012

滿足利害關係人的需求

政府部門的主要利害關係人係政府本身、其他部門、市民和政府部門職員。

所有利害關係人的需求，均需透過 COBIT 5 的目標級聯 (Goals Cascade) 加以分析。利害關係人需求必須連結到IT需求，然後再連結到治理促成因素（ Enablers）需求。如此的話，這些需求才能被轉換成一個比較具實際性和可行性的策略。COBIT 可

協助透過評估相關風險來保持資源利用及利益實現間的平衡。

這個原則針對有利害衝突的利害關係人間的不同需求，加以治理、談判及做決策。

涵蓋企業所有端到端流程

資訊在政府決策過程中扮演重要的角色。即時取得資訊可協助制定法律的架構，進而造福市民。

COBIT 涵蓋了企業所有部門對資訊及 IT 的使用，而不僅限於 IT 功能而已。

COBIT 整合了 IT 治理及企業治理，且涵蓋了所有管理資訊及科技須用到的流程。

應用一個單一的整體架構

科技不斷的變化及利害關係人與供應商所施加的壓力讓政府部門員工的工作變得複雜。對科技所知有限的政府員工必須面對管理與治理資訊及相關科技的艱難任務。

COBIT 5 與其他許多框架及方法有極高的一致性，例如資訊技術基礎架構庫（ ITIL）和國際標準化組織（ ISO）/ 國際電工委員會（ IEC）ISO/IEC 27001 標準。它能提供企業一個涵蓋性及一致性兼備的單一整合架構，且能透過客製化來滿足各部門的需求。

就算政府部門的職員僅有極少的 IT 知識，亦能透過採用 COBIT 以取得具 IT 產業水準的 IT 解決任務中獲益。

啟動全方位取向方式

對政府部門員工與受益人有很大影響力的決策會由政府部門的高級管理階層決定，進而藉由這些決策來達成政府的目標。為了達標，管理階層必須對政府部門有全面的認識，包含管理與治理的結構與過程。

COBIT 5 能協助藉由治理促成因素（ Enablers）來有效率地管理與治理跨部門的 IT。所謂治理促成因素係指會影響與治理與管理相關活動成果的因素。

治理促成因素的應用可以跨越整個部門，包含所有內部及外部與 IT 治理與管理相關的資源。

COBIT 5 有 5 個治理促成因素：

- 原則、政策與架構 — 將日常所需的行為轉換成符合邏輯的指引
- 流程 — 含應用所需 IT 來達成企業目標，再藉此達成與 IT 相關的目標
- 組織結構 — 負責利用取得的資訊來替企業做決策
- 資訊 — 企業本身的重要產品；讓企業能維持完善的治理及成功地運作
- 人員、技能與專長 — 分派適合的工作給有適合技能的人員，並採取更正措施及決策

將治理從管理分開

治理與管理不同。治理著重於需要做的事，而管理著重於要如何執行；負責治理與管理的團隊也不同。他們必須界定他們的責任範圍，但又必須一起合作來達成企業的目標。

所謂治理，係指了解企業的需求，依優先順序及制定決策來決定其方向，並監督是否符合目標。所謂管理，係指一種機制，並

藉由該機制來制定符合企業目標的執行計畫。

COBIT 5 釐清了治理與管理各自都有其不同的目的、責任，且需要不同形式的活動及組織結構來支持。

COBIT 5 使用評估（Evaluate）、引導（Direct）、監督（Monitor）的資安治理標準（EDM）來執行治理過程，而使用規劃（Plan）、建置（Build）、執行（Run）、監督（Monitor）（PBRM）的流程來執行管理過程。

治理過程（或 EDM）透過指定及同意欲達成的企業目標的活動來落實評估利害關係人的需求。這是種排定優先順序的活動，也是一種用來監督執行成果是否符合目標的活動。管理過程（或 PBRM）則落實監督這些活動的執行，並確保符合治理過程。

結論

任何組織、公司或政府均可建置COBIT來改善 IT 的表現。它有這些彈性是因為它可依組織的需求客製化。它從了解利害關係人的需求及商業挑戰開始，然後利用目標級聯當指標（從企業目標，到 IT 目標，再到治理促成因素目標 ）。這個過程，不僅重要，而且非常有用及很有成效。透過展示 COBIT 架構可帶來的商業利益，來取得資深管理階層的認可，是永遠都很重要的任務。

選擇所需要的控制因素（實務的關鍵 ），而非盲目地跟從架構及執行程序，是 COBIT 5 其中一個能成功的主要因素。除此之外，確保企業組織內各個角色及責任分配有明確的區分，且與各個團隊分享（透過負責者（Responsible）、當責者（Accountable）、事先諮詢者（Consulted）、事後告知者（Informed）方式（RACI））亦是重要的一環。國際電腦稽核協會（ISACA）COBIT 5 的建置（COBIT 5 Implementation）能協助將改善計畫分成數個小階段來執行，且能讓組織在計畫進行中持續獲益。

ISACA 提供了很多採用 COBIT 架構的指引，但若有需要，仍需尋求專家的協助。重點在人，而不是文件。文件並非執行者。這個過程是在訓練人採取新的行為模式。

註：作者是一位在治理、風險管理與合規、風險管理、IT 服務管理、資訊系統安全管理 ISO 20000 稽核、及 COBIT 5 建置方面的資深顧問。

原文出處：ISACA/Resource/News and Trends/Industry News/2017/Using COBIT in Government Department

資訊安全其治理稽核之落實

Practice of the Governance Audit of Information Security

余俊賢
互聯安睿資通(股)公司 CEO
Jack@arcran.com

黃榮鐘
互聯安睿資通(股)公司 資安服務處長
Pato@arcran.com

壹、觀念釐清篇

一、前言

資訊安全不太像是傳統的自然科學、數位邏輯等課程，這門學問其實較複雜，因為它要解決的不是自然界的問題、邏輯閘的問題，而是「人」製造出來的問題；凡是人製造出來的問題都不容易解決，人往往也是最大的資安議題，故「以終為始」到「資訊安全 (即資安)」，企業必須要確認達成 (資安) 目標所要做的事，才能逐步完成。透過管理，強化效率，領導企業才能達到既定的目標及方向。

二、風險與資安目標

記得以前在 PC 的時代，一人一台機器，很少能夠連上網，現在則變成沒有什麼東西不連上網，Uber Eats、Foodpanda 外送團隊也在網際網路上提供點餐服務，什麼東西都放到網路上面，這就是所謂的雲端。我們的資料基本上都放在雲端上，每個人都脫離不了 Apple、Google 等的世界，因此問題相對會變得更加複雜，尤其在 2018、2019 臉書個資外洩事件，更是引起大眾對資訊安全的重視。

各位先進在談資安目標時，應清楚的明白「沒有目標就沒有風險」，影響目標達成的不確定因素所帶來的衝擊叫風險。

我們常在談資安，當然資料經過處理即成有用的資訊 (Information)。但，何謂安全 (Security) ？事實上「安全」就是資安的目標，資訊的管理必須達到「安全」這個目標。而安全的目標就是 CIA(機密性、完整性、可用性)。(The FISMA defines three security objectives for information and information systems - Confidentiality, Integrity, Availability)

所以，資訊安全是用來保護電腦系統、網路和資料等各類資訊技術的機密性、完整性、可用性，以避免遭受攻擊、毀損或未經授權的存取動作。

貳、資安防疫篇

一、如何做好資安防護

資訊安全防護的內在到底有哪些？資訊安全工作應如何推展？這樣的問題不論政府機構或各企業向來十分重視，但相關的主機安全、網路安全，甚或是 Internet 安全等資安議題，很少提出較有效的方法論點作為參考或依據。

軍隊在建軍備戰時，常提到「安全是一切的基礎，沒有安全就沒有一切」，這句話，各位先進應是耳熟能詳，但它同時也可適用於資訊安全的知識領域，本篇我以較從管理者的觀點切入，從資訊安全需求面、資訊安全政策面及安全機制三方面，淺談資安防護所應具備的內容，提供使大家對資訊安全防護工作有更進一步的體認。

(一) 資訊安全需求面

資訊的特徵，縱然在保護資訊之 CIA(機密性、完整性與可用性)，但企業組織與軍方單位會因需求不同而使得要求重點相異，如一般企業組織採用資訊系統之目的在使其員工能有效率作業傳遞資訊，因此資訊存取與分享至關重要，所以可用性 (Availability) 的確保為第一要務；但若是在軍方單位，必強調機密性 (Confidentiality) 與完整性 (Integrity)，因為機密資訊若遭未授權人員讀取 (如 : 部隊部署、武力配置) 而導致洩漏，將危及國防安全體系，因此 CIA 裡資安目標裡，它更注重 CI，亦即寧願檔案無法讀取或遭刪除，而不是被偷走使可以利用之，因此明確的定義所屬單位之資訊安全需求，應是落實資安防護工作的首要之務。

(二) 資訊安全政策面

何謂「資訊安全政策」，即是指導組織資訊安全的最高原則及指導方針，資訊安全政策為建構資訊安全管理制度與資訊安全防護技術二者的基礎建設，其意義在於必須為組織設定如何安全的使用資訊，以及安全的優先順序及達成組織目標，在符合組織的目標下，規範「資訊安全」的範圍，且以資訊安全為基礎的資訊管理與資源使用原則。

在「資訊安全政策」之目的與功能面，應對資訊資產安全的需求，提供指導方針與規範，具體呈現高層管理者對資訊安全的支持與承諾及定義有關部門與人

員對資訊安全管理的角色與責任，並指引資訊安全服務產品的選擇與技術的引進。接著在「資訊安全政策」的制定，應初步評估，並促使高階主管提升資訊安全敏感度及意識，並做安全需求分析，諮詢相關專家或顧問意、核定發布資訊安全政策，最後實施安全政策教育、建立資訊安全意識及做政策內外部宣導，以作為資訊安全基礎建設及資訊安全信賴。

(三) 資訊安全機制

若只依賴資訊安全政策就認為可貫徹始終做到資訊安全，那是不夠的、不可能的，需以資訊安全機制相互配合，方能落實安全政策；為什麼呢？因為資訊安全機制可以保證系統不會進入所謂的不安全狀態 (亦即可能被入侵的狀態)；安全機制可以是技術，也可以是控管的程序，資料加密 (Data Encryption)、防火牆 (Firewall)、入侵偵測系統 (IDS)、入侵防禦系統 (IPS) 的運用，屬於資安技術；又如機敏資訊分開持有、最低權限之設計、資料攜出入之控管，則屬於控管程序。

但各位先進可想而知，有時候技術性的機制並無法滿足政策的規定或需求，如企業內雖禁止使用非法的 mp 4、mp 3 影音及音樂 MIS 人員 (資訊系統管理人員) 會經常實施盤查，但往往還是免不了一些較懂資訊的員工去加密、修改副檔名、甚至使用隱藏等其他方法。實際上，即使 MIS 人員使用一般的搜尋工具仍無法有效的盤查 (當然較先進的工具還是可以的，我這邊只是舉例)，可想而知，這時您用技術是無法達成資安控管目標的，您必須輔以程序或政策才能有效的加以禁止之。

由上述的概要分析應可以清楚地了解到，事實上沒有任何一種機制或方法可提供系統絕對安全的保證，但也不能因此就不做；需認知瞭解到，不同的方法必能提供不同程度的防衛、抵禦的能力，依照單位需求，綜合運用，整體安全防護目標才能確保達成。

另外，評估或衡量安全性時，一定不能僅依賴系統本身所採用或擁有的機制或方法及顧慮到使用者環境，因它也是影響安全成敗的重要因素之一，必須納入考量而為之。

我做個小總結 :

資訊安全的構成元素包含資訊安全需求、資訊安全政策及資訊安全機制等三面向，「需求用來定義安全的目標」，它說明什麼樣的安全是你所預期的；「政策定義安全的意義或內涵」，它說明你要達成安全目標的步驟有哪些；而「資訊安全機制則能強化政策」，也就是說您應採用什麼樣的 (軟體) 工具、程序或方法才可以有效的保

證達成資安防護目標，因此三者相輔相成。

建議政府機構或企業組織在建構資訊系統時，除必須優先考量作業系統本身的安全性之外，更應將上述資安的三個元素整合在整個軟體發展生命週期 (System Development Life Cycle, SDLC) 的每一階段中，使得安全機制可有效強化政策的執行，而且安全政策也能滿足組織的需要需求，如此一來，才能在安全無虞的環境下使用資通網路的環境，去構築及達成想要的目標。

二、資安治理成熟度評估

我國於 2014 年起，始推動資安治理制度，首先建立政府資安治理架構，包含 4 大面向與 18 個流程面，以及政府機關資安治理成熟度評估機制和自動化評估的工具，協助各機關、企業去完善資安防疫的作為。

再者，行政院國家資通安全會報技術服務中心、經濟部工業局等單位，在推動資訊安全管理制度已有一段時間，大多數政府機關業已導入資訊安全管理系統（ Information Security Management System；ISMS），並通過公正第三方之驗證，各機關單位亦可參考 ISMS 相關控制措施以達其防疫目標。

資通發展面向，為因應所謂的資通訊科技發展及資安威脅趨勢，許多較先進國家已將「 資安管理 」提升至「 資安治理 」層次，大家必須認知，資安風險為組織重要風險之一，資安目標亦為組織重要目標之一，管理高層必須加強對於資安防護工作之重視，同時亦應反映在組織資安相關人力配置與經費等資源的投入，才能有效的以降低資安風險。

整個資安治理成熟度評估架構，應參考及網羅集資安治理相關國際標準與最佳實務，包含 ISACA COBIT 5、ISO/ IEC/ CNS 27014、ISO/ IEC/ CNS 27001、ISO/ IEC 33020、ISO/ IEC 33004 及 NIST CyberSecurity Framework 等等，並結合我國資安推動之「 策略面 」、「 管理面 」及「 技術面 」3 大面向，發展適合我國之資安治理成熟度架構。(參閱圖 1)

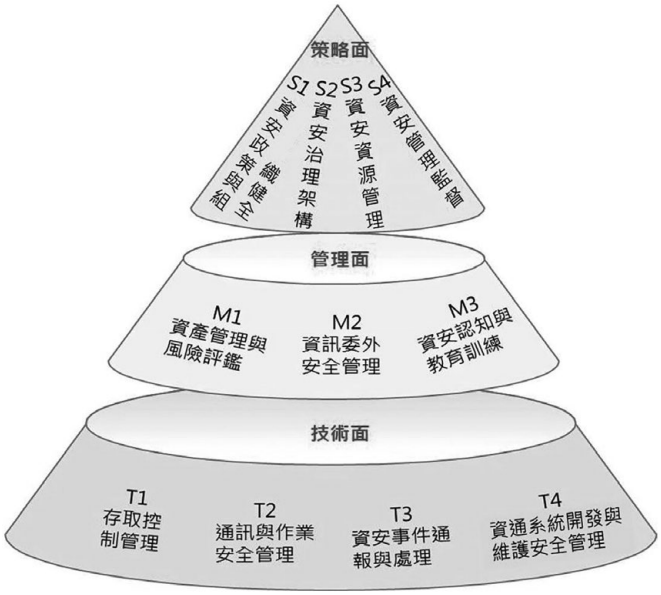


圖 1: 資安治理成熟度架構

（資料來源：行政院國家資通安全會報技術服務中心整理）

評估當然就要確保它的可信度與適用性，故相關單位也參考能力度、成熟度評估相關國際標準，包含 ISO/ IEC 33004 與 ISO/ IEC 33020 等。(參閱圖 2)

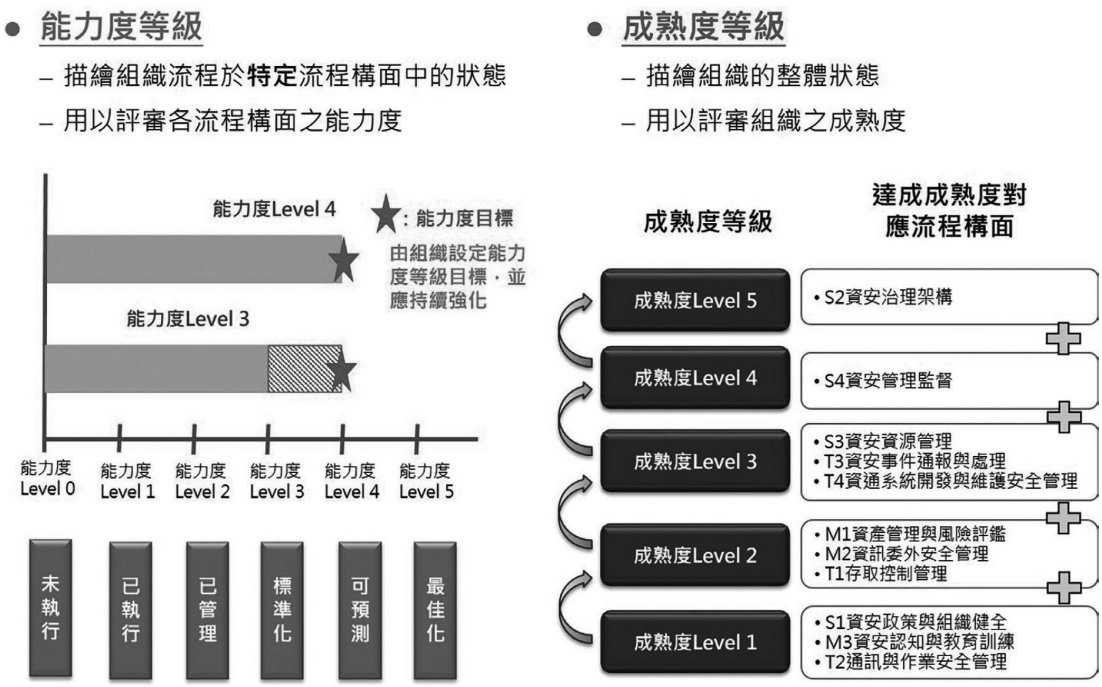


圖 2: 能力度與成熟度之評估方法

（資料來源：行政院國家資通安全會報技術服務中心整理）

依據資安治理成熟度架構之運作模式，選定成熟度之評估標的，並建立能力度（Capability）與成熟度（Maturity）分級定義與評估原則，設計完整的資安治理成熟度評估方。

在能力度設計上，為有效評估各流程構面之執行程度，使能力度評估結果能與後續之成熟度計算方式結合，各單位及企業亦參考國際標準 ISO/IEC 33020 設計，應將能力度等級由低至高分為 6 級。(參閱圖 3)

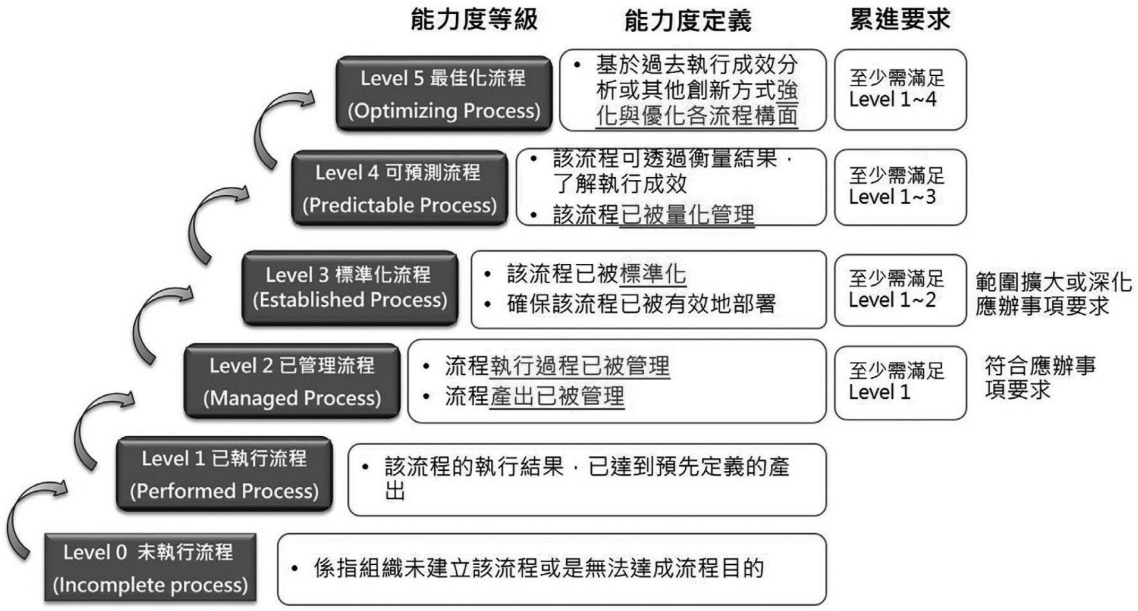


圖 3: 資安成熟度能力等級

（資料來源：行政院國家資通安全會報技術服務中心整理）

透過資安治理成熟度評估機制之推動，政府期能掌握整體資安防疫之情形 (當然也可適用於企業參考)，並加強管理階層對於資安管理工作之更加重視，同時如前述所提及，必須增加資安人力與經費等資源之投入，以降低資安風險。

參、落實資安篇

一、資訊安全稽核與認證

本篇以資安稽核的視野，讓各位先進了解資安稽核的目的及其可帶來的效益，並透過資安意識的宣導、強化，實實在在地去確認資訊安全系統的存在，引進相關的稽核管理制度 (如 :ISO/IEC 27001，CNS 27001) 並落實資訊安全。

接著「稽核」這兩個字，想必大家一定聽過、看過，但何謂稽核呢？

ISO 8402 定義：品質稽核係一項系統化及獨立性之審查，以確定品質活動及相關結果是否符合計畫之安排，且此項安排是否被有效執行並適合於達成目標。

ISO 9000 定義：品質稽核係系統的、獨

立的與文件化的過程，用以獲得證據及客觀的評估，以確定稽核準則所達成的程度。

所以「稽核」應是由有能力且獨立之人員客觀取得與評估證據，以支持其聲明是否符合報告的系統化過程。而我們所要提及的資安稽核之目的在於：

- 檢查、評估資安控制措施之缺失及衡量
- 資訊安全管理制度 (ISMS) 對 ISO 27001 之符合性、有效性和適切性
- 適時提供改進之建議，以合理確保及保證該制度得以持續有效的實施，以符合合約的要求及驗證需要。

再著眼觀之，資安稽核的效益主要是在於可驗證：

- 是否符合資安標準及法令的要求
- 可評估資訊安全管理制度的有效性
- 減少資訊安全管理系統失效之風險
- 為管理階層審查，提供訊息
- 提升資安意識及改善之機會
- 落實資訊安全的最後一道防線

另外，在落實資安稽核面，主要在稽核類型分為三類，以下簡略做說明之 :

第一方稽核：內部稽核

由組織對自身系統及程序所做的稽核，目的在確保組織資訊安全系統的實行與改進。

第二方稽核：外部稽核

組織對其供應商或分包商所做的稽核，目的在驗證供應商或分包商的績效是否適切。

第三方稽核：外部稽核

由具有公信力且獨立於被稽核組織及其供應商與客戶的團體所執行，通常會依據公認之資訊安全系統標準進行，去驗證組織的 ISMS 是否符合特定標準，如 :SGS、TUV、BSI 等驗證機構。

二、資安意識安全教育

資安意識的培養與建立，絕對是吃力不討好的資安工作，且因其涵蓋面向非常廣泛，單位必須不斷勸導、說服，甚至要強迫使用者，改變原本操作以及存取應用系統與資料的種種不良習慣，因此，在推動的過程當中，會遇上許多接踵而至的阻礙，不過，這種作法對於提升資安的有效性，仍然倍受肯定。

美國系統網路安全協會 (System Administration,Networking and Security；SANS) 的 2016 財務面向安全與風險調查報告中，特別提到，金融服務業當中，絕大多數的公司以防火牆 (Firewall)、網路入侵偵測與防禦系統 (NIPS)、端點防護系統 (EDR/MDR)，作為減輕風險的主要控制措施，與此同時，他們對於實施員工資安意識的教育訓練所能帶來的防護效果，也給予了高度的肯定。

當組織在推動資安意識的過程中，其實會經歷幾個階段 (參閱圖 4)，SANS 特別提出了安全意識成熟度模型 (Security Awareness Maturity Model)，來呈現不同時期具有的重點發展目標，有助於組織瞭解及判斷目前組織的資安意識是處於何種階段。

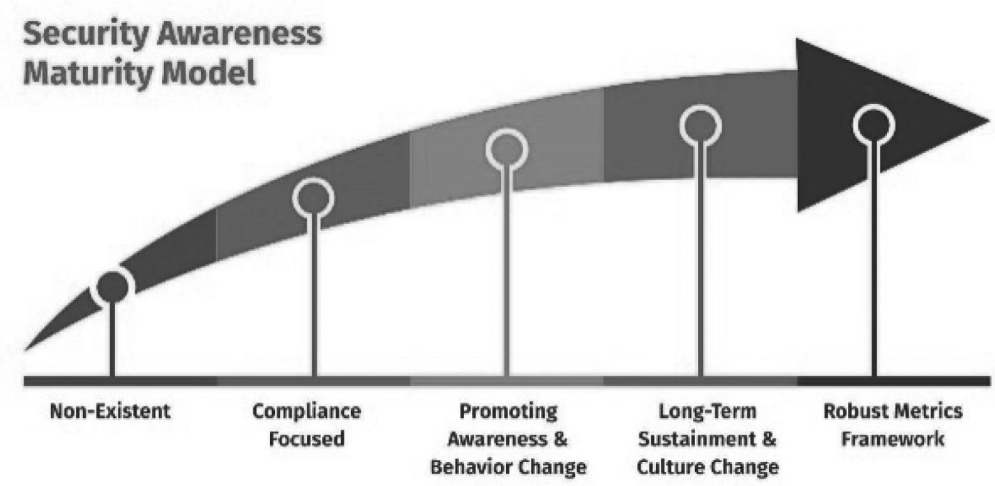


圖 4：安全意識成熟度模型（圖片來源：SANS）

而在 SANS 的安全意識部落格 (Security Awareness Blog) 當中，他們建議推動資安意識計畫的負責人員，可從溝通、協同運作、文化這三個層面加以著手：

(一) 溝通

資安意識的養成，終究都關乎組織之間能否進行有效溝通，建議組織推動資安意識的人員在一開始的時候就要先鼓勵大家多去了解資訊安全這項議題，並且向他們解釋為何要關心資訊安全。

根據 SANS 的建議，最好透過簡單的方式，描述應該要做的事情，並且設法讓大家能夠展現並實現這些行為。

(二) 協同運作

資安意識的好與壞，牽涉到使用單位裡面每個成員的認知，為了要讓這樣的觀念普及，推動者必須要與許多人一起合作，不僅限於單位內成員，可與其他單位部門或國家地區協同運作。

SANS 建議，可以成立一個資安諮詢委員會（ Security Advisory Board）的組織，成員來自各部門的代表。透過他們的參與，可以促使資安意識的計畫得以成形，並且能夠持續維護、進展及追蹤之。

(三) 文化

要做好資訊安全，除了針對行為層面的落實，相關風俗文化的培養更需注意，因為這牽涉到後續能否維繫之。

對文化的建立，SANS 認為當中包含了觀念、態度、信念的形成與確立，有了這些，才能更有效地推動組織想要資訊安全。同時，文化也包含了情感的表達與交流，而這對技術人員來說，可能會有些困難，所以，以文化為基礎來進行組織內部的溝通與協

同運作，對於推動資安意識將有重大的突破。

肆、結語

(以下內容部份參考行政院政策與計劃之重要政策)

在國家公務體系中，上至行政院資通安全會報，下至各縣市政府 D 級機關，透過經費、人力、技術與教育訓練等四項元素，塑造出資安防護機制，雖無法百分之百的防堵漏洞、去除威脅，但實質上已增強各機關自我的防護能力，並降低資安事件危害。此時此刻，就讓我們從政府資安政策－「資訊安全管理系統（Information Security Management Systems；ISMS）」的執行開始學習，並在工作中落實。

推動資安防護為各機關、企業不可缺少的工作，可參考行政院落實資安防護之作為，如 :

(1) 推廣認知教育：各機關每年辦理 1 次通報演練及 2 次電子郵件社交工程演練。

(2) 參考相關法規辦法 :《資通安全管理法》立法 (註：已於 107 年 5 月 11 日經立法院三讀通過)，完善各項資安法制環境。

(3) 提升防禦技術 : 透過攻防演練、資安健診、DDoS、弱點掃描等機制，主動發現網站 / 系統之弱點，始能即時完成弱點修補。另外，亦可結合大數據分析及人工智慧技術 (AI)，預測資安攻擊之趨勢。

最後，我們面對複雜多變的資安威脅及挑戰，政府極力建構國家資安聯防體系，提升整體資安防護機制，培育優質資安人才，打造台灣成為安全及可信賴的數位國家，皆有賴於全體國人的同心協力去維護及強化。

參考文獻

1. 我國推動資安治理之建議
http://www.bas-association.org.tw/catalog/arts/ 010202034.pdf
2. 經理人 - 成功學大師柯維，用 4 個字教你活出不後悔的人生
https://www.managertoday.com.tw/articles/view/ 47218
3. 什麼是 ISO 認證第三者稽核？
https://www.isoleader.com.tw/home/iso_news_detail/ 1317
4. 如何做好資訊安全防護工作
http://www.cyepb.gov.tw/edit/attached/file/ 20150812/ 20150812172650_ 2130.pdf
5. 2019 資安十大趨勢－提升資安治理成熟度
https://www.ithome.com.tw/news/ 128034
6. 微軟提出四大資安應變措施 - 協助企業資安防疫
https://news.microsoft.com/zh-tw/cyber-security-enterprise 4/
7. 行政院 : 落實資安防護作為
https://www.ey.gov.tw/Page/ 5A 8A 0CB 5B 41DA 11E/ 39af 7a 8a- 19cd- 411d- 9d 80-c 236c 69bee 49
8. 政戰資訊服務網 - 認識駭客攻擊趨勢，落

實資安防護作為 (103 年 5 月第 3 週)

https://gpwd.mnd.gov.tw/Publish.aspx?cnid= 513&p= 3362

9. 聯合新聞網 - 名家觀點：落實資安治理官民當務之急

https://udn.com/news/story/ 7238/ 4625022

10. 資通電子報 : 資安防疫新思維：什麼病毒都一樣，防疫沒捷徑！

https://marketing.ares.com.tw/newsletter/ 2020- 03-cyber-security/focus

11. 科技部建置之新版「 科技大觀園 」科普網站 : 資訊安全威脅與防護

https://scitechvista.nat.gov.tw/c/sTVN.htm

12. 行政院國家資通安全會報 - 技術服務中心 : 資安治理成熟度評估機制暨工具說明會

http://icstwebstorage.blob.core.windows.net/attachfilenew/%E 8%AD%B 0%E 9%A 1% 8C 2_%E 8%B 3% 87%E 5%AE% 89%E 6%B 2%BB%E 7% 90% 86%E 6% 88% 90%E 7% 86% 9F%E 5%BA%A 6%E 8%A 9% 95%E 4%BC%B 0%E 6%A 9% 9F%E 5% 88%B 6.pdf

13. 105 年國家資通安全防護整合服務計畫資安治理成熟度評審使用手冊

https://download.nccst.nat.gov.tw/attachfilehandout/%E 8%B 3% 87%E 5%AE% 89%E 6%B 2%BB%E 7% 90% 86%E 6% 88% 90%E 7% 86% 9F%E 5% BA%A 6%E 8%A 9% 95%E 5%AF%A 9% E 4%BD%BF%E 7% 94%A 8%E 6% 89% 8B% E 5% 86% 8A_v 1. 0_ 1051204.pdf

14. iThome: 趨勢資安教育訓練，達 80/ 20 之效

https://www.ithome.com.tw/node/ 39328

15. 工業技術研究院資訊技術服務中心 : 資訊安全簡介與資訊安全政策

http://cc.web 2.ncut.edu.tw/ezfiles/ 26/ 1026/img/ 140/information(950504).pdf

16. iThome: 威脅就在眼前！找回面對資訊安全的危機感

https://www.ithome.com.tw/news/ 112742

17. RedHat: 什麼是資訊安全？

https://www.redhat.com/zh-tw/topics/security

18. 中華技術電子書 / 中華技術雜誌 :ISO 內部品質稽核作業探討

http://www.ceci.org.tw/book/ 53/ch 53_ 5.htm

中華民國電腦稽核協會

中華民國電腦稽核協會（ CAA）自民國 83 年成立，舉辦過無數次有關資訊安全管理與電腦稽核等相關學術研討與實務運用之座談會，並舉辦各項資訊安全與電腦稽核講習課程，提供會員與外界人士一個提升專業知識及能力與分享經驗的場所。民國 85 年 ISACA TAIWAN CHAPTER 成立，為全球第 142 個支會，成為引領台灣與世界電腦稽核之先河，長期推廣國際電腦稽核師證照 (CISA)、國際資訊安全經理人證照 (CISM)、國際企業資訊治理師 (CGEIT)、國際資訊風險控制師認證 (CRISC)。民國 90 年與 BSI 開始合辦主導稽核員訓練及建置實務 … 等課程，例：資訊安全管理系統主導稽核員證照 (BS 7799/ISO 27001 Lead Auditor)、IT 服務管理系統主導稽核員證照 (ISO 20000 Lead Auditor)、營運持續管理系統主導稽核員證照 (ISO 22301 Lead Auditor)… 等，並配合政府各階段 ISMS 的推動計畫，承辦國家資通安全標準的翻譯專案，且已成為證券期貨局、銀行局銀行業、銀行局票券商、投信投顧公會及保險局認可之內部稽核人員專業訓練機構暨公務人員終身學習訓練機構。

協會簡介

願 景

願景：持續為資訊科技治理與電腦稽核之先導機構。

宗 旨

一、推動電腦稽核及系統控制安全之學術研究發展。
二、協助制訂電腦稽核、控制、安全之標準。
三、協助企業強化電腦系統之控制與電腦稽核功能。
四、與國際電腦稽核相關組織作資訊及技術之交流。
五、協助保護個人資料等事項。

任 務

一、舉辦有關電腦稽核、控制、安全之研討會、講習會。
二、舉辦企業及機關團體之教育講習，以推廣有關電腦稽核控制，安全之實施。
三、出版電腦稽核、控制、安全之刊物及著譯叢書。
四、聯繫企業、學術界及政府機構，以促進電腦稽核理論與實務之交流。
五、接受企業、政府機構委託協助建立電腦稽核功能與電腦安全及控制制度或辦理電腦稽核之研究。
六、舉辦對電腦稽核有貢獻之表揚事項。
七、接受政府相關機關之委託舉辦電腦稽核人員資格檢定。
八、聯繫國際電腦稽核組織、進行合作。
九、辦理其他為達成本會宗旨之必要事項。

沿革

- 1994 年 7 月 14 日正式創立，由朱寶奎擔任第一屆理事長。秘書長由林秀玉會計師擔任。
- 1996 年 7 月由朱寶奎續任第二屆理事長。秘書長由林秀玉續任。
- 1998 年 7 月由魏忠華接任第三屆理事長。秘書長由陳瑞祥擔任。
- 2000 年 8 月由魏忠華續任第四屆理事長。秘書長由黃涼澤擔任。
- 2002 年 9 月由蔡蜂霖接任第五屆理事長。秘書長由莊盛祺擔任。
- 2004 年 9 月由吳琮璠接任第六屆理事長。秘書長由吳素環擔任。
- 2006 年 9 月由吳琮璠續任第七屆理事長。秘書長由許林舜擔任。
- 2008 年 9 月由黃明達接任第八屆理事長。副理事長由林宜隆擔任。秘書長由徐敏玲擔任。
- 2010 年 8 月由黃明達續任第九屆理事長。副理事長由林宜隆續任並暫代秘書長。
- 2012 年 8 月由林宜隆接任第十屆理事長。副理事長由楊期荔擔任。秘書長由黃涼澤擔任。
- 2014 年 8 月由林宜隆續任第十一屆理事長。副理事長由楊期荔續任。秘書長由黃涼澤續任。
- 2016 年 8 月由張紹斌接任第十二屆理事長。副理事長由蘇庭興擔任。秘書長由黃涼澤續任。
- 2018 年 9 月由張紹斌續任第十三屆理事長。副理事長由蒲樹盛擔任。秘書長由黃涼澤續任。
- 2020 年 9 月由葉奇鑫接任第十四屆理事長。副理事長由蒲樹盛續任。秘書長由黃涼澤續任。

會員權益

一、可免費參加本協會定期舉辦之例會活動 (含台北、新竹、南區)，並獲得 CISA、CISM、CRISC 及 CGEIT 持續進修 (CPE) 學分。

二、參加 CISA、CISM 國際證照考試複習課程及本協會舉辦之課程可享有會員折扣價。

三、會員得以優惠價格購買協會出版品。

四、可免費獲得協會出版之《電腦稽核期刊》(一年兩期)。

五、透過電子郵件方式，可取得電腦稽核相關領域之最新訊息。

六、輔導會員取得國際電腦稽核師 (CISA)、國際資訊安全經理人 (CISM) 、國際資訊風險控制師認證 (CRISC) 及國際企業資訊治理師 (CGEIT) 證照並提供會員專業認證管道。

七、參加協會各種活動、擔任協會委員會委員及出席會員大會等，並享有發言權、表決權、選舉權、被選舉權；團體會員得由五位代表人出席本協會會議並行使權利義務。

八、可進入協會會員專屬網站瀏覽各期刊物及下載各類電子文檔，如歷年期刊文章、ISACA 摘譯期刊、例會講義、職業道德規範、及提供各項查核指引等資料。

會員義務

- 本協會會員有繳納會費及遵守本會章程與決議事項之義務。

July-December 2020 Certification Exam Passers

ISACA Taiwan Chapter

	Exam Type	ID No.	Name	Top 3
1	CISA	1079439	Kuang-Tzung Chiang	
2	CISA	1171310	Tao-Chien Chang	
3	CISA	1221619	Chia-Hsiang Liu	
4	CISA	1262955	Yong-Chih Huang	
5	CISA	1282084	Chien-Chin Kao	No.1
6	CISA	1288264	Fang-Chi Wang	
7	CISA	1296155	En-Wei Ning	No.2
8	CISA	1312859	Wan-Chun Chang	
9	CISA	1336562	James Tu	No.3
10	CISA	1338915	Chien Hung Li	
1	CISM	230893	Yun Tseng	No.3
2	CISM	1262955	Yong-Chih Huang	
3	CISM	1296155	En-Wei Ning	No.1
4	CISM	1301256	Yu-Hung Chen	
5	CISM	1327880	Chien-Ming Chen	No.2
6	CISM	1338915	Chien Hung Li	

※ 以上資料來源： ISACA總會202101更新。

2021 年度教育訓練課程列表

電腦稽核協會為證期局公發公司、銀行局金控公司及銀行業、信用卡業務機構、電子支付機構、保險局保險業、保險代理人/經紀人公司、投信投顧公會認可之內稽人員訓練機構及董監進修課程辦理機構及公務人員終身學習訓練機構

課程類別	課程主題	時數	預定開課時間	課程費用
ISACA 國際證照系列	CISA 國際電腦稽核師認證研習班_平日班	30	**4/19-23** **9/8-10, 15-16**	NT$ 40,000
	CISA 國際電腦稽核師認證研習班_假日班	30	**5/8, 15, 22, 29, 6/5** **10/2, 16, 23, 30, 11/6**	NT$ 40,000
	CISM 國際資訊安全經理人認證研習班_假日班	24	**3/6, 13, 20, 27** **7/3, 10, 17, 24**	NT$ 32,000
ISO 系列(與 BSI 合辦)	ISO 27001:2013 資訊安全管理系統 CQI & IRCA 主導稽核員訓練課程 ※日期標註「底線」者，為前 **2** 天採線上課程，後 **3** 天採實體課程	40	**1/18-19, 2/22-26、3/8-12、4/12-16、5/10-14、6/7-11、7/12-16、9/13-17、10/4-8、11/15-19、12/6-10** 假日班：**8/13-14, 19-21** 高雄班：**4/12-16、9/13-17**	NT$ 53,000
	ISO 27001:2013 資訊安全管理系統 內部稽核員訓練課程	16	**5/13-14、9/23-24**	NT$ 21,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	**5/12-14、10/19-21**	NT$ 36,000
	ISO 20000-1:2018 服務管理系統 CQI & IRCA 主導稽核員訓練課程 ※日期標註「底線」者，為前 **2** 天採線上課程，後 **3** 天採實體課程	40	**3/15-19、6/21-25、8/30-9/3、12/6-10**	NT$ 55,000
	ISO 20000-1:2018 服務管理系統 CQI & IRCA 稽核員/主導稽核員轉版訓練課程	16	**2/1-2、5/6-7、8/5-6、11/4-5**	NT$ 22,000
	ISO 20000-1:2018 服務管理系統 內部稽核員訓練課程	16	**2/1-2、8/16-17**	NT$ 20,000
	ISO 20000-1:2018 服務管理系統 建置實務課程	24	**3/17-19、9/14-16**	NT$ 35,000
	ISO 22301:2019 營運持續管理系統 CQI & IRCA 主導稽核員訓練課程 ※日期標註「底線」者，為前 **2** 天採線上課程，後 **3** 天採實體課程	40	**2/22-26、6/21-25、8/9-13、11/8-12**	NT$ 55,000
	ISO 22301:2019 營運持續管理系統 轉版課程	8	**5/10、8/20**	NT$ 11,000
	ISO 22301:2019 營運持續管理系統 基礎課程	16	**3/15-16、6/17-18、9/2-3、12/13-14**	NT$ 21,000
	ISO/IEC 29100:2011+A1:2018(CNS 29100)隱私框架 主導稽核員訓練課程	36	**2/22-26、5/17-21、9/6-10、12/20-24**	NT$ 55,000
	ISO/IEC 29100:2011+A1:2018(CNS 29100)隱私框架 國際標準基礎課程	8	**2/8、5/3、9/17**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準基礎課程	8	**4/9、8/3、11/26**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準建置課程	16	**5/27-28、9/23-24、12/13-14**	NT$ 15,000

課程類別	課程主題	時數	預定開課時間	課程費用
內稽系列	內部稽核實作基礎班(初任課程)	12	4/6-7	NT$ 6,600
	NEW!編碼有原則－管理無缺口上機設計操作	7	2/24、3/24、4/14、5/26、7/28、8/25、9/29、10/27、11/24、12/15	NT$ 3,850
	NEW!十秒內飆速編製損益表與合併報表	7	2/25	NT$ 3,850
	查核人資假勤及薪資管理分析報表實作班	7	6/22	NT$ 3,850
	NEW!設計紙本內控合理化表單(初任課程)	7	7/27	NT$ 3,850
	範例設計五大組成要素之自行評估問卷(初任課程)	7	10/26	NT$ 3,850
	應用商業簡報視覺化技巧呈現經營分析與稽核報告	7	11/23	NT$ 3,850
	以電腦控制關鍵點查核舞弊實務案例	7	11/25	NT$ 3,850
	一例一休加班特休目前法規真實範本	7	12/24	NT$ 3,850
	NEW!稽核不出門，能知天下事－後疫情時代的稽核利器：風險智能儀表板★	6	1/14	NT$ 3,300
	NEW!如何打造誠信經營企業★	6	1/15	NT$ 3,300
	內部稽核做人做事成功的實務作法	6	2/212	NT$ 3,300
	新興科技下之「稽核轉型」及「數據分析」實務案例解析★	6	3/15	NT$ 3,300
	資料分析軟體應用技巧與查核實務	6	3/18	NT$ 3,300
	內部稽核有效應用財務報表實務班(初任課程)★	6	5/3	NT$ 3,300
	內部稽核「工作達標」有效作法	6	7/5	NT$ 3,300
	內部稽核「協助組織達標」有效作法★	6	9/6	NT$ 3,300
	內控 2.0：統計預測、數據分析、資訊安全與舞弊偵防★	6	10/1	NT$ 3,300
IT Audit與資訊治理系列	核決權限制定原則與執行稽核風險管控機制(初任課程)	7	9/28	NT$ 3,850
	電腦稽核規劃實務(初任課程)★	6	3/9、9/7	NT$ 3,300
	資訊系統與通信傳輸查核★	6	3/10、10/6	NT$ 3,300
	NEW!從新修正公司治理評鑑指標看智財管理★	6	3/16	NT$ 3,300
	突破稽核抽樣的海量數據蒐證技術★	6	3/25、8/31	NT$ 3,300
	NEW!從新修正公司治理評鑑指標看智財管理★	6	3/30	NT$ 3,300
	國際標準 ISO 22301 營運持續管理系統稽核實務－以稽核活動檢視組織韌性與復原力★	6	4/12	NT$ 3,300
	數位時代電腦稽核實務(初任課程)★	6	4/13、10/5	NT$ 3,300
	NEW!智慧製造資安趨勢與應用★	6	4/27	NT$ 3,300
	網站安全與稽核簡介(Ⅰ)★	6	4/28、9/13	NT$ 3,300
	網站安全與稽核簡介(Ⅱ)★	6	5/5、9/24	NT$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	5/13、11/11	NT$ 3,300
	NEW!雲端世代之科技風險發展趨勢★	6	5/27	NT$ 3,300
	網路風險控制與網路安全稽核	6	5/28	NT$ 3,300
	NEW!ZERO TRUST－管理及內控的跨界治理★	6	5/31、11/29	NT$ 3,300
	資料存取於稽核與行為分析之應用	6	6/3	NT$ 3,300
	有效成本管控設計與分析★	6	6/4	NT$ 3,300
	雲端服務管理稽核★	6	6/8	NT$ 3,300

課程類別	課程主題	時數	預定開課時間	課程費用
IT Audit與資訊治理系列	行動應用 APP 安全檢測與實務★	6	6/11	NT$ 3,300
	ERP 系統控制測試與稽核★	6	6/17	NT$ 3,300
	稽核分析在銷售收款循環稽核個案演練(Arbutus 操作)	6	6/24	NT$ 3,300
	數位時代的採購流程控管與查核實務★	6	6/25	NT$ 3,300
	大數據分析對有效風險管理作業及內控三道防線的因果關係看知行合一哲學★	6	7/15	NT$ 3,300
	NEW!數位身分(Digital Identity)風險與挑戰★	6	7/16	NT$ 3,300
	ISMS 資訊安全管理系統內部控制與稽核	6	7/29、12/28	NT$ 3,300
	Excel 結合大數據分析(Ⅰ)：Power BI 資料擷取與多元資料分析	6	7/22	NT$ 3,300
	Excel 結合大數據分析(Ⅱ)：Power BI 視覺化分析與風險評估	6	8/12	NT$ 3,300
	稽核分析在採購付款循環稽核個案演練(Arbutus 操作)	6	8/19	NT$ 3,300
	數位轉型與新興科技應用下，企業資訊治理架構實務分享★	6	8/26	NT$ 3,300
	ERP 系統控管與查核實務★	6	10/8	NT$ 3,300
	稽核分析在金融業以風險為導向內部稽核個案演練(Arbutus 操作)	6	10/14	NT$ 3,300
	應用系統導入 PKI 安全機制與檢查	6	10/21	NT$ 3,300
	談資安事件應變機制及稽核重點★	6	10/22	NT$ 3,300
	NEW!雲端服務委外之安全管控與稽核要點★	6	10/29	NT$ 3,300
	網路與系統安全實務查核★	6	11/19	NT$ 3,300
	數位時代下的稽核變革及實務案例分享★	6	12/6	NT$ 3,300
舞弊稽核與數位鑑識系列	企業舞弊最常使用在採購作業範例解析(初任課程)	7	3/23	NT$ 3,850
	企業舞弊最常使用在銷售作業範例解析(初任課程)	7	4/15	NT$ 3,850
	存貨與固定資產作業舞弊查核(初任課程)	7	5/25	NT$ 3,850
	查核資料庫(Database)舞弊造假資料匯集案例實作班	7	8/24	NT$ 3,850
	案例分享－舞弊手法與查核技巧	6	2/23、8/30	NT$ 3,300
	保全企業數位證據－資訊環境的自行舉證操作實務★	6	3/5	NT$ 3,300
	打造風險智能組織－從舞弊風險預防、偵測、調查到危機處理★	6	3/12	NT$ 3,300
	NEW!以稽核角度看資安事件應變及數位鑑識★	6	3/19	NT$ 3,300
	網路與系統日誌分析實務操作	6	4/9	NT$ 3,300
	NEW!數位鑑識軟體入門操作實務★	6	4/16	NT$ 3,300
	不實財報的各種作假手法與鑑識資料分析(FDA)細察技術★	6	4/29、11/30	NT$ 3,300
	防範及稽核薪資作業舞弊的 31 個妙招★	6	5/7	NT$ 3,300
	事件應變處理與數位鑑識整合實務★	6	5/14	NT$ 3,300
	舞弊調查實務★	6	5/21	NT$ 3,300

課程類別	課程主題	時數	預定開課時間	課程費用
舞弊稽核與數位鑑識系列	內部稽核舞弊偵查應用技巧實作(初任課程)★	6	**6/7**	NT$ 3,300
	營業秘密法實務案例解析與證據攻防★	6	**7/2**	NT$ 3,300
	數位鑑識於機密資料外洩稽核應用實務★	6	**7/9**	NT$ 3,300
	資料導向的舞弊偵測與查核實務	6	**7/23**	NT$ 3,300
	以數位鑑識協助舞弊稽核的運用實務	6	**8/6**	NT$ 3,300
	💻利用數位鑑識分析人員不當行為	6	**9/17**	NT$ 3,300
	資安事件與資料外洩鑑識調查實務分享★	6	**10/15**	NT$ 3,300
	資安持續稽核與監控：組態安全管理之應用★	6	**10/28**	NT$ 3,300
	認識數位鑑識技術基礎與實務	6	**11/5**	NT$ 3,300
	結合系統資料與網路資源透析潛在舞弊事件	6	**11/12**	NT$ 3,300
	數位證據與實例分享★	6	**12/17**	NT$ 3,300
個資外洩與保護系列	資料庫稽核與個資保護★	6	**1/21、10/7**	NT$ 3,300
	個人資料保護建置★	6	**6/18**	NT$ 3,300
	歐盟 GDPR 合規與個人資料保護★	6	**7/6**	NT$ 3,300
	個人資料保護稽核★	6	**12/10**	NT$ 3,300
	💻個資法導入與查核內控循環作業管理規範(初任課程)	7	**12/16**	NT$ 3,850
數位金融與電子支付系列	PCI DSS 基礎訓練課程(與 BSI 合辦) ※採線上課程	8	**3/9**、**6/18**	NT$ 8,000
	NEW!數位轉型與資訊安全★	6	**3/22**	NT$ 3,300
	行動支付稽核實務班★	6	**6/2**	NT$ 3,300
	PCI DSS 資料安全標準與電腦稽核實務★	6	**8/4**	NT$ 3,300

※ 本會保有課程安排及師資調整異動之權利，實際課程請依本會網站公告為準。
※ 本會會員課程費用另有優惠。
※ 「💻」為上機操作課程，學員需自備有 USB 孔的筆電。
※ 「★」為上市上櫃公司董事、監察人進修課程。
※ 「初任課程」僅限證期局(公開發行公司)之內稽人員可申報，銀行局、保險局不適用。
※ 可申報進修時數：實際可申報時數請依本會網站公告為準

- ■ 證期局公開發行公司內部稽核人員訓練時數
- ■ 證券期貨局內部稽核人員初任職前訓練時數
- ■ 證券期貨局內部稽核人員在職或替代訓練時數
- ■ 銀行局金融控股公司及銀行業內部控制及稽核人員在職訓練時數
- ■ 銀行局信用卡業務內部稽核人員在職訓練時數
- ■ 銀行局電子支付機構內部稽核人員相關專業在職訓練時數
- ■ 保險局保險業內部稽核人員在職訓練時數
- ■ 保險局保險代理人及保險經紀人內部稽核人員在職訓練時數
- ■ 投信投顧公會內部稽核人員訓練時數
- ■ 公務人員終身學習時數(限 ISACA 證照及 ISO 課程)
- ■ CISA、CISM、CGEIT、CRISC、CIA 學習時數
- ■ 上市上櫃公司董事、監察人進修時數

※ 歡迎企業包班，為您量身訂做所需課程。
※ 詳細課程規劃請上本會網站 www.caa.org.tw 查詢，或來電(02)2528-8875 洽詢。

電腦稽核期刊前期篇名整理

第四十二期_電腦稽核在新興科技應用的機會與挑戰

- Study of CIM and IoT-Simulation for Cost Performance Analysis-Cost management
- Shodan 為基礎的 IoT 安全等級與防護機制
- 隱私資訊管理系統標準 ISO 27701 於 GDPR 適用性評估
- 人工智慧對於審計實務之影響
- 論全球衛星定位系統於偵查中使用之合法性及立法制度發想
- 物聯網需要更好的安全性
- 區塊鏈存證應用於司法數位證據之芻議

第四十一期_5G時代來臨之稽核創新與AIoT應用

- 人工智慧對產業之影響 - 擁抱 AI，戰勝趨勢
- 運用 IoT 平台評估程序改善 IoT 運作效益
- 企業整併異質企業資源規劃系統流程 - 以銷貨退回與折讓 e 化為例
- 編碼有原則、管理無缺口 - 編碼選單設計成功經驗談
- 機器學習稽核 -CRISP-DM 架構

訂購詳見電腦稽核協會網站https://www.caa.org.tw/publish.php

近期活動報導

台北例會

2020.07.20

【 以 ISO 27701 標準為框架建立在既有資訊安全管理系統中架構之個人隱私管理系統 】

當前科技的發展，已讓社會大眾、企業等機關習慣將個人隱私相關文件、機密文件存放在雲端。而只要對罪犯來說是有利可圖的，就有犯罪的可能性，大型雲端遲早會遭受到攻擊，故評估風險時，若沒評估出風險，就是一件危險的事情。「不怕一萬，只怕萬一」，我們必須及早做好防範的措施及相對應的準備，例如：存取控制、資訊備份、事件日誌的存錄、確保資訊傳送的程序及政策、測試資料之保護、安全事故管理等等。

◆以 ISO 27701 標準為框架建立在既有資訊安全管理系統中架構之個人隱私管理系統專題演講 -BSI 英國標準協會台灣分公司驗證部門 - 章鈺經理

本次例會邀請到 BSI 英國標準協會台灣分公司驗證部門產品經理 - 章鈺，為大家介紹 ISO/IEC 27701 隱私資訊管理系統標準，內容主要分為 4 個主題：ISO/ IEC 27701 隱私資訊管理系統標準緣由、與 ISO/ IEC 27001 相關的 PIMS 特定要求介紹、與 ISO/ IEC 27002 相關的 PIMS 特定指引簡介、控制者與處理者的隱私管理強制要求說明，讓學員們能夠對此議題有更加深刻的理解。

2020.08.27

新竹例會

【 內部稽核如何發現公司重要風險之實務 】

◆安永聯合會計師事務所諮詢服務部 - 吳欣倫協理

本次邀請到安永聯合會計師事務所諮詢服務部 - 吳欣倫協理來為大家做新竹例會演講，演講主題為「內部稽核如何發現公司重要風險之實務」，吳協理詳細地介紹了企業風險之來源、辨識方法 / 管道、評估，及內部稽核人員之職能要求。讓各位對稽核領域有興趣的學員能夠更清楚地內部稽核人員所應具備、培養的技能以因應未來趨勢。

2020.08.15

【「後疫情時代的資訊治理與稽核」專業論壇暨第 14 屆第 1 次會員 (代表) 大會及第 14 屆理監事選舉 】

◆左起中華民國內部稽核協會理事長趙曉慧、行政院資通安全處處長簡宏偉、中華民國電腦稽核協會第十三屆理事長張紹斌、安永諮詢服務股份有限公司總經理張騰龍、安侯企業管理股份有限公司副總經理邱述琛、勤業眾信風險管理諮詢股份有限公司資深執行副總經理林彥良。

本年度會員大會邀請了業界專家學者們共襄盛舉，並由中華民國電腦稽核協會第十三屆理事長張紹斌、行政院資通安全處處長簡宏偉、安永諮詢服務股份有限公司總經理張騰龍、勤業眾信風險管理諮詢股份有限公司資深執行副總經理林彥良、安侯企業管理股份有限公司副總經理邱述琛、中華民國內部稽核協會理事長趙曉慧，以上貴賓共同揭開序幕。

本次因應疫情，以「後疫情時代的資訊治理與稽核」為主題，為大家帶來三大主題的演講：由資通安全處處長簡宏偉，為大家講述主題一「後疫情時代應有的資安思維」、中華民國電腦稽核協會理事長葉奇鑫，為大家講述主題二「個資法修法與資安稽核」，綜合座談「後疫情時代應有的資安思維」則由安永聯合會計師事務所朱家德執行副總經理、安侯企業管理股份有限公司林軒宇經理、勤業眾信聯合會計師事務所陳威棋副總經理，以「善用資訊治理與稽核的優勢，化危機為轉機」為主軸分別講述三個不同的子題：「後疫情時代的舞弊風險與偵防」、「以資訊治理達成數位轉型及高階風險管理策略」、「全面啟動企業韌性」為大家帶來演說，現場也因英國標準協會台灣分公司暨東北亞區總經理蒲樹盛、淡江大學資訊管理系榮譽教授黃明達兩位主持人的對談，而產生更多的思考激盪。

◆「後疫情時代的資訊治理與稽核」專業論壇與會學員

為感謝這一年來各位理監事、各委員會主委、委員們不斷協助推廣協會事務及證照，也於會上公開進行表揚。與此同時，也感謝各位努力的學員們在工作之餘也不斷持續進修並考取 CISA、CISM、CRISC、CGEIT 證照，為此，本會進行了 2019 年前三名的新科頒獎，以激勵更多想考取證照的學員們能夠繼續向自己的目標邁進。

台北例會

2020.09.25

【 稽核轉型與價值提升－從大數據稽核到風險智能儀表板 】

現今日益月新的新興科技，諸如：人工智慧、機器自動化、物聯網、大數據分析、區塊鏈技術、雲端運算等都對稽核產生了一定的影響，本次例會邀請到勤業眾信張益紳執行副總經理以主題「 稽核轉型與價值提升－從大數據稽核到風險智能儀表板 」來為大家演講、帶著大家去思考如何透過稽核流程智慧化及大數據資料分析來為企業提供更具附加價值的服務。張副總經理提到若想擺脫經濟衰退、提高獲利成長，個人、企業、甚至公部門就應加速智慧轉型，否則在這樣快速成長的環境下將會被淘汰。期望透過這次「 大數據稽核實務 」、「 風險智能儀表板 」及「 風險智能儀表板應用實例 」的介紹，讓學員們了解如何應用風險智能儀表板去協助企業集團管理風險及其可帶來的效益。

◆勤業眾信聯合會計師事務所執行副總經理 - 張益紳副總經理

2020.10.20

新竹例會

【 美國規矩，全球適用－針對美國新秩序，企業營運面臨的持續衝擊及因應方式解析 】

◆安侯法律事務所執行顧問 - 翁士傑顧問、孫欣顧問

科技趨勢的發展，影響的不僅為個人層面，更是與國家發展息息相關，而其中也延伸出了許多國家安全問題。本次新竹例會邀請了安侯法律事務所執行顧問 - 翁士傑顧問、孫欣顧問，以「 美國規矩，全球適用－針對美國新秩序，企業營運面臨的持續衝擊及因應方式解析 」為主題來講述美國為保護國家安全，政府及相關單位所實施的經濟制裁及技術、軟體出口控制措施。

兩位顧問首先帶來案例解說，例如：美國封殺華為集團、中興通訊案、伊朗制裁案、法國興業銀行案、孟晚舟案，再從案例一步一步帶入到當前的法規趨勢議題，最後提出企業因應之道。

顧問提到風險辨識、建立內部合規遵循機制（ EMCP）之重要性，同樣是涉及違反規範的企業，未建立合規遵循機制的企業會受到更重的制裁。有建立遵循機制、透過遵循機制找出並主動接露違規是減輕責任的重要因素。建立合規遵循的機制、辨識風險，此類超前布署將能使企業在發展的道路上更加穩健。

2020.10.16

南區例會

【內部控制理論與實務】

本次南區分會長特別邀請到東華大學會計系張益誠主任到中正大學，分享關於內部控制的經驗以及心得，透過舉例讓同學更能理解內部控制理論、如何將理論運用到實務上，會上與同學們一起討論許多個案，例如 : 高鐵提出的優惠補助案、保險業務的缺失、銀行行員偷搬 1600 萬、銀行收到假美鈔 ... 等不同的案例，在這些案例當中也提到可利用數位鑑識分析 (FDA) 的輔助來發現舞弊風險，使同學提高對內部控制的認知並與生活做連結。

◆內部控制理論與實務專題演講 - 國立東華大學會計系張益誠主任

台北例會

2020.10.22

【「數位轉型下資訊治理、風險管理、與持續稽核新作為」實務研討會】

◆左起互聯安睿資通股份有限公司執行長余俊賢、ISACA 台灣分會副會長陳政龍、兆益數位股份有限公司莊盛祺總經理、財星 500 大企業駐美稽核經理高智敏、中華民國電腦稽核協會理事長葉奇鑫

◆「數位轉型下資訊治理、風險管理、與持續稽核新作為」實務研討會與會講師、學員

近年來，企業為因應科技潮流，不斷地求新求變、朝著數位轉型的方向發展，而數位轉型勢必會延伸出相關資訊治理、風險管理、持續稽核的新作為，本次 10 月例會演講主題即以此為主軸，為大家帶來相關議題的演說。

本次例會一開始由 ISACA 台灣分會副會長 / 財團法人國家實驗研究院正工程師陳政龍為大家介紹、推廣「接軌 ISACA 國際觀點及發展 6C 專業人士的主流趨勢」(6C：CISA、CISM、CRISC、CGEIT、CSX-P、CDPSE) 讓大家了解目前最新的趨勢。接下來則是分別由互聯安睿資通股份有限公司執行長余俊賢來為與會學員們做「網路安全攻防實作展示」、財星 500 大企業駐美稽核經理的高智敏經理講解「如何透過誠信企業文化防弊」。最後的綜合座談由兆益數位股份有限公司莊盛祺總經理主持，同時與三位講師及學員們進行與會對談，使各方論點能產出更多智慧的火花。

2020.11.27

台北例會

【數位化時代－企業內部資訊安全防護及管理機制】

◆安永企業管理諮詢服務股份公司 - 曾品媛資深經理

數位化時代下，網路攻擊手法也越來越多變化，從勒索病毒，機密資料外洩，到惡意程式攻擊；尤其因應疫情關係，許多工作已轉型為遠距工作，其中所面臨的挑戰除了遠距查核使查核困難度提升、企業所受到的攻擊、威脅也更加日益猖獗。本次例會邀請到安永企業管理諮詢服務股份公司資深經理曾品媛以「數位化時代 - 企業內部資訊安全防護及管理機制」來為大家介紹未來十年之全球資安發展趨勢、網路安全與風險管理、組織如何面對挑戰及疫情期間日常作業的防禦方法。曾經理提到「雖然工作可委外，但責任無法委外」期望學員在往後能加強對委外廠商的監督與查核。

[協辦] 勤業眾信聯合會計師事務所

2020.12.17

【「身份識別存取管理趨勢與策略藍圖 」研討會 】

◆左起中華民國電腦稽核協會理事長葉奇鑫、勤業眾信聯合會計師事務所風險諮詢服務部營運長吳佳翰、CyberArk Software Ltd. 大中華區技術顧問黃開印、勤業眾信聯合會計師事務所風險諮詢服務部副總經理陳鴻棋、勤業眾信聯合會計師事務所風險諮詢服務部資深執行副總林彥良

隨著新興科技的發展，企業因帳號與權限的管理機制強度不足而造成機敏資料外洩的事件層出不窮，除此之外也屢屢遭受到惡意的網路攻擊，由此可見，數位身分識別與存取管理儼然已成為企業須面對的重要課題。本會協辦此次勤業眾信聯合會計師事務所主辦之研討會，即是以「身分識別存取管理趨勢與策略藍圖 」為主題，來為大家講解最新的趨勢話題。

會上，由勤業眾信聯合會計師事務所風險諮詢服務部營運長吳佳翰、資深執行副總林彥良、副總經理陳鴻棋分別為大家剖析身份管理三道防線－特權帳號管理、身份治理、客戶身份識別與存取管理，帶領大家一同深入了解如何透過數位身分識別存取管理、策略來達到安全治理與法規遵循之目標。

這兩年，因疫情關係使得遠距工作變成常態，CyberArk Software Ltd. 大中華區技術顧問黃開印指出，在這樣的工作型態下，有近八成遠距工作員工使用不安全、未受管理的個人裝置存取公司系統的問題發生；CyberArk Idaptive 為其提供了解決方案，透過 Idaptive 生命週期管理，在員工生命週期的每個階段簡化應用程式存取請求管理、建立應用程式帳戶及終止存取權限以達到保護作用。

中華民國電腦稽核協會葉奇鑫理事長則是從資安及營業秘密訴訟攻防案例來談身份識別與存取管理重要性，向大家分享過往訴訟攻防經驗。葉理事長提到，過去便有刑事判決案例中的企業，因嚴格控管員工的資訊存取權限、建立機密資料保護的相關規範，而取得勝訴判決，建議企業應正視身份識別與存取管理，此議題不僅重要甚至會與營業秘密之訴訟勝敗習習相關。

透過各位業界專家們的介紹，期望能讓各企業了解到此議題的重要性，並做出應對措施以達到降低風險的作用。

新竹例會暨聯誼會

2020.12.18

【 遵循風險管理智能化－以新興科技輔助三道防線強化遵循風險管理 】

法令遵循風險是什麼？法令遵循風險是當公司為遵循法令規範、公司內部政策及程序時，可能產生法令事故的風險，其中常見的有：存在造假之風險、管理階層選擇性偏差、不尋常或複雜之交易 …… 等等。

當企業未能遵循法令法規時，要面對的不僅是裁罰、調查、訴訟，更會對企業產生聲譽之損害，降低品牌的信任度。年末新竹例會即由勤業眾信聯合會計師事務所協理李介文，以「 遵循風險管理智能化－以新興科技輔助三道防線強化遵循風險管理 」為主題，為學員介紹當前遵循風險之趨勢、管理時會遇到的困境與挑戰及要如何以三道防線落實遵循風險管理、提醒企業可以透過強化法遵能力來維持市場競爭力及保護公司聲譽。

◆勤業眾信聯合會計師事務所 - 李介文協理

2020.12.29

台北例會

【 營業秘密保護實戰面面觀 】

◆合盛法律事務所主持律師 - 張紹斌律師

2020 年度最後一場月例會，邀請到合盛法律事務所主持律師張紹斌，以「 新修正營業秘密法 」為主題來演講，過程中張律師以生動活潑、淺顯易懂的描述方式舉了各種不同的例子來幫助大家釐清常見的問題、使學員能對營業秘密的基本觀念及其商業價值有更深一步的認識。會中張律師提醒學員們應留意的問題，例如：商標要有顯著性、識別性，且須登記並主張其使用範圍，若商標被外界使用，必須及時提出應對措施，避免商標淡化成為一種通用名詞而喪失原有的權益。除此之外，也介紹了中、美、日、韓關於營業秘密之相關法規、讓學員能了解各國法規的不同之處。

ISACA
Taiwan Chapter

證明您的能力足夠帶領企業面臨新時代的挑戰

資訊化是21世紀重要的時代特性，大量的資訊與相對應的技術支援，雖將能促進企業的成功，但在此環境下，卻同時也增加了許多原本沒有而複雜且具有挑戰性的新管理議題。

ISACA®國際電腦稽核協會是一個屬於世界領先地位的全球性組織，提供資訊專業人士能以卓越的途徑進行個人專業的成長與發展。同樣的，全球資訊專業人士也認為，ISACA對於他們的職業生涯發展與企業價值的提升均提供了實質的幫助。

將 CISA、CISM、CGEIT或CRISC的認證名稱放置在您名字後面，將能證明您的專業能力、經驗與推廣。這可認定您是一位專業的資訊人才，擁有全面性的資訊系統視野，並關係到企業能透過價值傳遞(value delivery)且獲得成功的關鍵因素。

隨著現代企業越來越依賴資訊系統(IS)，對於技術與資訊系統專業人員的需求快速的上升，並且更著重於資訊與治理的能力。企業需要合格的資訊專業人才的實務知識與專長，來幫助確認關鍵性問題與制定具體作法以支持資訊與相關技術的治理作為。ISACA的認證將滿足企業如此的迫切需求。ISACA以全球公認的認證讓企業能識別具備豐富經驗與知識的專業人才。

在國際的獨立研究報告中指出，ISACA名稱代表著：

- 高階資訊專業人士的薪資報酬
- 可信賴的專業能力與認可
- 招募程序中的高點選率與優先面試

如何取得更多的資訊

訪問ISACA認證網站：**www.isaca.org/certification-success**
ISACA認證部門：**certification@isaca.org**

CISA Certified Information Systems Auditor®
An ISACA® Certification
國際電腦稽核師

CISM Certified Information Security Manager®
An ISACA® Certification
國際資訊安全經理人

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification
國際企業資訊治理師

CRISC Certified in Risk and Information Systems Control™
An ISACA® Certification
國際資訊風險控制師

國際電腦稽核師(CISA)在稽核領域
如同註冊會計師(CPA)與公認會計師(CA)在會計領域一般

組織越來越依賴複雜的資訊作業來協助內部業務運作與控制措施的執行，企業需要擁有知識與技能的稽核專業人才，幫助企業找出關鍵問題與解決方案，以確認資訊系統的可信賴性與價值。

國際電腦稽核師證照(Certified Information Systems Auditor® , CISA®)是毋庸質疑的認證，當您擁有CISA證照，您的專業將立即得到理解與認同，CISA證照將讓您在國內與國際上對於使用標準、確認管理缺失、法規符合性，提供解決方案、發展控制措施以提供企業價值的專業知識、技能、經驗與可信賴的認可。

CISA認證是世界知名對於企業系統的稽核、控制、監控與資訊技術評估的標準。事實上在許多獨立的研究中指出，如資訊安全媒體集團(Information Security Media Group, ISMG)的每年就業趨勢調查，CISA始終是排名資訊證照中最搶手與薪資最高的認證。

歷經38年發展，現今CISA證照已是國際認可標準的具體實現，並且在162個國家有超過 100,000 位的專業人士獲得此項認證。

右表介紹CISA的專業工作活動項目，並指出每一專業領域的分配率。

說明
專為資訊科技/資訊系統稽核師，以及控制、保證與資訊安全專業人士設計。

資格要求
五(5)年(含)以上資訊系統/資訊科技稽核、控制、保證或安全工作經驗。

經驗最多可抵減三(3)年。

考試範圍領域(%)
1.資訊系統稽核流程 (21%)
2.資訊科技治理與管理 (17%)
3.資訊系統的取得、開發與建置 (12%)
4.資訊系統的營運及企業靈活性 (23%)
5.資訊資產的保護 (27%)

證實您的資訊安全專業知識–提升競爭優勢

具備資訊安全管理專業人士的需求正呈現逐步上升的趨勢，國際資訊安全經理人(Certified Information Security Manager® , CISM®)是一項在資訊安全管理上全球公認的標準，現代企業必須保護自己免受網路犯罪與越來越多的惡意攻擊等問題，CISM以獨特並專注於資訊安全管理為著重點，提供資訊安全具體的實務做法。不同於其他的安全認證，CISM識別出個別的企業資訊安全管理、開發與佈建階段。

取得CISM的專業人士瞭解企業的需求，他們知道如何去管理和適應他們企業與行業的安全需求。CISM將不僅是具備資訊安全的專業知識，同時也在資訊安全的系統開發與管理上具有可靠的經驗。

CISM 驗證意涵著更高的收入潛力與職業發展。例如在最近的獨立研究2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™ ,ITSCPI)中指出，CISM持續被列為高報酬與最受歡迎的資訊認證之一。

走過第13個年頭，目前已有超過21,300位專業人士取得CISM證照。

右表介紹CISM的專業工作活動項目，並指出每一專業領域的分配率。

說明
專為管理、設計、監督和評估企業資訊安全的人員設計。

資格要求
五(5)年(含)以上資訊安全管理工作經驗。

經驗最多可抵減兩(2)年。

考試範圍領域(%)
1.資訊安全治理 (24%)
2.資訊風險管理 (30%)
3.資訊安全計劃開發與管理 (27%)
4.資訊安全事故管理 (19%)

展現您良好治理的能力
–對於您的企業與職業發展發揮廣大的影響力

避免發生意外(例如難以處理的資訊數據侵害)，對於企業來說是至關重要的，良好的治理將建立檢查與平衡機制，並對於發生意外事件能進行敏捷的反應。而當企業雇用了CGEIT，將可以確保具有良好的治理能力。

國際企業資訊治理師(Certified in the Governance of Enterprise IT® ,CGEIT®)認可的專業人士具備對於企業資訊治理的原則與實踐有廣泛的知識與經驗。作為一位CGEIT的專業人士，您將證明您具有在一個組織中資訊治理的能力，由整體面掌握複雜的議題，並因此而提升對企業的價值。

CGEIT專業人士具備公認可信賴的資訊治理與策略定位等關鍵議題的知識與實務經驗，其所提供的公信力將使CGEIT的專業人士晉升成為「C-suite」高階經理人。

自2008年以來，已有超過5,000位專業人士取得CGEIT認證。

右表介紹CGEIT的專業工作活動項目，並指出每一專業領域的分配率。

說明
CGEIT對各種專業人員的資訊科技治理原則和實務知識及其應用進行認證。

資格要求
五(5)年(含)以上顧問或監督角色，支援企業資訊科技相關治理的經驗。

經驗最多可抵減一(1)年。

考試範圍領域(%)
1.企業資訊科技治理 (40%)
2.資訊科技資源 (15%)
3.效益實現 (26%)
4.風險最佳化 (19%)

個人事業與企業組織未來的試煉

對於改善公司治理、營運績效與安全基礎設施的需求不斷的增長，意味著資訊風險管理對於要能適應未來發展的企業是至關重要的。

國際資訊風險控制師(Certified in Risk and Information Systems Control™ , CRISC™)是唯一針對資訊風險管理專業人士未來職業發展的驗證，其定位於有效連結資訊風險管理與企業風險管理，以成為企業戰略合作的夥伴。

CRISC是最新且經過嚴格評核，具備識別資訊技術風險與評估資訊業務與風險管理的專業人士。CRISC證照將使您在企業內部資訊運作的未來發展上，提供更好的諮詢機會，並且使您在組織中的角色更顯重要；資訊風險將成為企業整體風險重要的組成部分，並使您在組織的資訊風險議題上成為知識型的領導者與內部規則變更的推動者。

2012年Foote Partners的資訊技能與證照報酬指數(IT Skills and Certifications Pay Index™ ,ITSCPI)，CRISC已擠身前10名薪資最高的認證之一。

自2010年以來，已有超過16,000位專業人士取得CRISC認證。

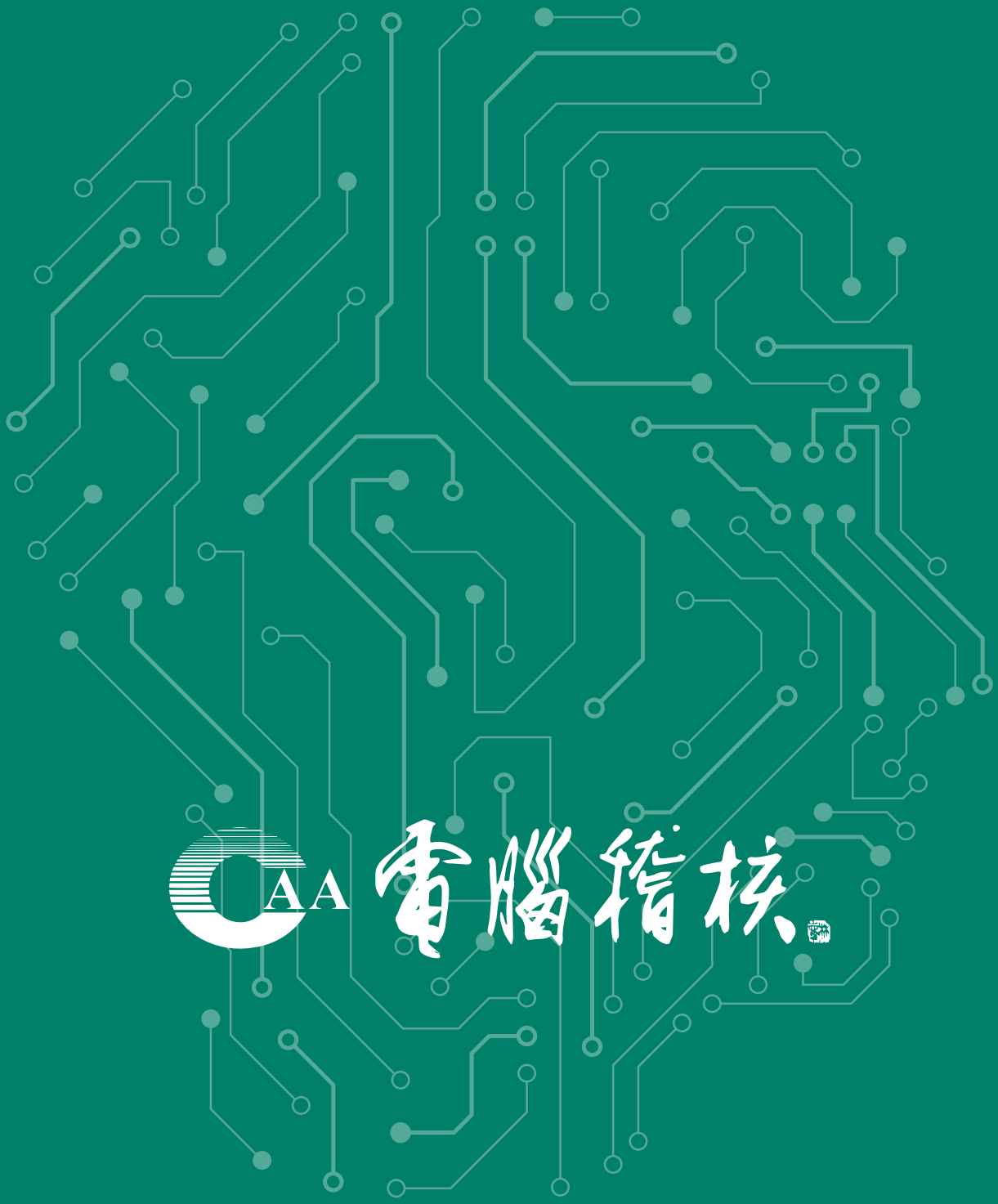
右表介紹CRISC的專業工作活動項目，並指出每一專業領域的分配率。

說明
專為具有資訊科技風險管理經驗，並具有資訊系統控制、設計、實施、監督和維護經驗的人員設計。

資格要求
三(3)年(含)以上資訊科技風險管理與資訊系統控制工作經驗。

無工作經驗抵減或替代方案。

考試範圍領域(%)
1.資訊科技風險識別 (27%)
2.資訊科技風險評估 (28%)
3.風險回應與移轉 (23%)
4.風險和控制監控與報告 (22%)



ISACA
Taiwan Chapter

中華民國電腦稽核協會
11070台北市信義區基隆路一段143號7樓之4
7F.-4, No.143, Sec. 1, Keelung Rd., Xinyi Dist., Taipei City 11070, Taiwan (R.O.C.)
886-2-2528-8875 Fax : 886-2-2528-8876
Web : www.caa.org.tw www.isaca.org.tw