電腦稽核
Computer Audit Association 民國109年08月31日 第42期
ISACA Taiwan Chapter

Opportunities and Challenges of e-Auditing in Emerging Technology Applications

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
Shodan-based IoT Security Level and Protection Mechanism

隱私資訊管理系統標準ISO27701 於GDPR適用性評估

A Win-Win Collaboration between Universities and Industry on Audit Data Analytics

The Impact of Artificial Intelligence on the Audit
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
The Study on the Legal Question of Detecting Crime by Global Position System Tracing Device

物聯網需要更好的安全性IoT Needs Better Security

區塊鏈存證應用於司法數位證據之芻議

編 輯 序

在現今數位經濟環境發展下，新興科技大大地提升了全球物聯網絡的高度連結，人工智慧在雲端技術的結合下增進了大數據的應用，而感測器、機器人、3D 列印及區塊鏈等技術也相繼成為智慧商業、智慧環境的新利器。各家企業為提升其核心競爭力，正積極發展各種相關創新服務，從導入新興科技到打造電子化營運模式、發展電子商務平台，都可以看見興新科技的發展趨勢；企業除了利用這些創新思維的服務來拓展行銷通路、滿足多元化的商業活動外，也整合內外部資源、使資源能達到最佳配置並發揮最大效益。

全球性的專業諮詢服務機構指出，隨著資訊科技的演進，新興科技的應用與發展已快速滲透到人類生活的各個領域，包括：金融、通信、零售、醫療、服務與汽車等產業，人們也愈來愈仰賴新興科技自動化與人工智慧所帶來的好處；然而，在新興科技所帶來的龐大利益下，也潛藏了無數的風險，其複雜的變化不僅改變了產業的生態結構，更是產生一連串的延伸性問題，例如：個人資料外洩、隱私侵害、網路犯罪、法規遵行、資訊安全、與非法監控 … 等。對於此類興新科技應用所衍生的風險議題，尤其是舞弊與欺詐、洗錢與避稅及資訊安全此三類是絕對不容小覷的，各產業都應持著防患未然的態度審慎面對。

綜上所述，電腦稽核期刊第四十二期以「 電腦稽核在新興科技應用的機會與挑戰 」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的論文，討論數位經濟環境下新興科技所帶來的機會與挑戰，以及思考如何運用電腦稽核技術讓風險獲得有效的控制。

本期特別邀請美國帝博大學會計系王大維教授，擔任第四十二期客座主編，共同為電腦稽核期刊帶來更加豐富精采的內容。非常感謝各位作者賜稿、各位審稿委員細心的閱稿及協會秘書處之協助，更感謝長期以來支持本期刊的各位讀者們。本期期刊若有不盡之處，敬請各位先進賜教。

張碩毅
She-I Chang
編譯出版委員會主任委員
國立中正大學 管理學院院長

王大維
Tawei (David) Wang
美國芝加哥帝博大學 (DePaul University)
Associate Professor and Driehaus Fellow

CAA 電腦稽核
Opportunities and Challenges of e-Auditing in Emerging Technology Applications
第 42 期

目 錄
CONTENTS

會務交流

發 行 人：張紹斌
總 編 輯：張碩毅
客座編輯：王大維
編輯委員：張碩毅、李順保、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：109 年 8 月 31 日
定　　價：新臺幣 250 元

Study of CIM and IoT
−Simulation for Cost Performance Analysis−
(Cost Management)

Toshifumi TAKADA
Professor, National Chung Cheng University, Taiwan
ttakada0830@gmail.com

Abstract

Research Question

This study focused on the Computer Integrated Manufacturing (CIM) of a manufacturing company producing precast concrete products using a simulation technique. CIM integrates information among segments of marketing department, manufacturing department and warehouse department. In this study, we use a virtual company (MKS Company) producing precast concrete products as the company will be sustainable if it can solve the problem of critical path. Internet of Things (IoT) can contribute to shortening the path by communicating and thus sharing information in each department simultaneously.

The result of simulation shows the cost performance of IoT is positive. Market Department collects client information and market information. The collected information is gathered together and is forwarded to Manufacturing Department. Plant manager issues a job order. As MSK must a manufacturing products by Make to Stock method. The job order must be based on the correct market information.

With IoT enables MSK to make a correct estimation of the necessary quantity of production. MSK can minimize the Opportunity Loss and Unsold Product Loss. On the other hand, MSK must be patient to suffer a large amount of Opportunity Loss in case of Without IoT. Simulation shows that MSK can decrease almost 90% of Loss by IoT.

Keywords: IoT, CIM, Simulation, Opportunity loss, Unsold product loss

Content

I.RESEARCH QUESTION

1- 1. Research Question

This study focused on the Computer Integrated Manufacturing (CIM)[1]) of a manufacturing company producing precast concrete products using a simulation technique. CIM integrates information among segments of marketing departments, manufacturing departments and warehouse departments. In this study, we use a virtual company (MKS Company) producing precast concrete products as acompany that will be more sustainable if it can solve the problem of critical path (series of tasks needed the longest time). Internet of Things (IoT)[2]) can contribute to shortening the path by communicating and thus sharing information in each department simultaneously.

This study contributes to both sides of practice and theory. In practice, many business organizations are thinking to introduce IoT but they don't know the cost-performance of IoT; how much costs they can save by introducing IoT. This study shows it by simulation. In theory, this study shows the foundations of measuring cost-performance by a simplified method. Researchers can develop this study to more realistic situations.

Prior studies in IoT are concentrating on engineering research of IoT tools or on IT architecture. This study is focusing on economic side of IoT (cost-performance) in addition to the integration with CIM. This is the difference of this study from prior studies.

1- 2. Theoretical Background

(1) Marketing Department

The marketing department of MKS needs to know the delivery date of concrete products. Clients are construction companies and they need the concrete products as soon as possible when they get a construction contract because the precast concrete products are needed at the beginning of construction. People in the

Marketing Department always contact the construction companies and civil engineering offices to get information about the construction market. When a construction company gets a contract, it orders the concrete products from MKS. If MKS has the inventories in its warehouse, the delivery can be made at the date ordered. If without inventories, as the lead time of concrete product production is usually a few months, MKS will miss the chance of sales.

(2) Manufacturing Department

If the precast concrete production is 'Made to Order'[3]) production, MKS's manufacturing department can wait for the sales invoice from the marketing department. As mentioned above, such a production method is impossible because the lead time of the delivery will be a few months and the construction companies (customers) can't wait for such a long time. If MSK doesn't have finished products inventories at the time of order, the customers will order the concrete products from another vendor.

The manufacturing department must begin the production process based on the information collected by the estimation of the marketing department. The products are made by 'Make to Stock'[4]) production. If the produced products are not ordered from a customer, the sales to another customer will become difficult or impossible and result in loss. The manufacturing department faces this difficulty. If MKS can have enough finished products inventories at any time, it is easy for them to survive but such inventories will become unsold loss.MKS must find away to minimize unsold loss. The manufacturing department needs the correct information of the market estimated by the marketing department.

(3) Warehouse Department

The warehouse department is responsible for the inventory of finished products, inventory of materials (sand, concrete, steel net), molds and logistics. This department also faces several issues to be solved, as the products when they are unmolded are not the finished products.A few months are needed to dry the products as the molds are very heavy and warehouse space is limited, and it is difficult to find a specific mold in the warehouse.Some persons in the marketing department are influential veterans among the warehouse department personnel and they can reserve products

before orders from customers and they can release reserved products when a customer does not win acompetitive bid. Such unsold products will become losses [5]).

CIM and IoT will solve these problems. We will use a simulation technique to do cost performance analysis of IoT.IoT needs sensors. New and reasonable sensors are being developed day by day. In addition, as the new sensors are sophisticated and connected to computers. In this study, we don’ t show how to integrate IoT and CIM and this will proceed our research frontier to this aspect.

II. PRECAST CONCRETE PRODUCT INDUSTRY IN JAPAN

2- 1. Precast concrete products

The precast concrete product industry in Japan developed after World War II (1945). The products consisted of fourkinds of products:U-shape gutter, box culvert, Hume pipe and pile.

(1)U-shape gutter

U-shape gutters are used for waterways along the sides of paved roads for a drain. Japan has lots of rain and paved roads cannot absorb the rainfalls. In addition, the Japanese government had a policy to increase rice production in the 1950s and 1960s. Rice fields needed the waterway, and U-shape gutters were used for that purpose.

(2) Box culvert

Large box culverts are used for having a space of wareroom or underground carparking space. Small and medium ones are used for underground multi-purpose ducts. It is widely used in big cities to hide utility poles. Urban landscape is improved by moving poles underground using a box culvert. Electricity, telephone and telecommunication lines also can be moved underground.

(3) Hume pipe

A Hume pipe is a round pipe used for waterways and drains. Ceramic pipe was used for this purpose before 1945. As heavy traffic such as trucks and buses ran on roads, such pipe was easily broken. Hume pipes substituted for ceramic pipes. Hume pipes were used for waterways, agriculture irrigation and sewage.

(4) Pile

A pile is used for the construction of tall buildings. Tall buildings are so heavy that they will sink without supports. The pile became a new product in this industry in the 1960s. Before then, tall buildings had to be built on very solid land or a big tree was used to support the building. At the time of renewal construction of the Tokyo Station building, pine trees were found beneath the old building. Now the construction of very tall buildings has become possible because piles can be used to support the building.

2- 2. Market of precast concrete product industry

(1) Construction markets

Precast concrete products are used in construction of logistics (road, highway, harbor, airport), buildings and plants, infrastructure (waterway, sewage, electricity, telephone, and Internet), agriculture (rice field irrigation), urban street (multi-purpose duct, space for stock room/ parking), etc. The market can be divided into private sector and public sector. The public sector market is large because the Japanese government, local governments, public utilities companies, and public companies have big budgets for such construction. Big general construction companies have had lots of construction work after World War II. They can get the contracts by a competitive bid from the Japanese government and local governments. Large general construction companies and small and medium construction companies attend the bid. The market is very competitive.

(2) Competitive bid and time constraint

When a company wins a bid,

the company starts the work immediately as it must finish the work before the end of fiscal year March in many cases. Very large construction contracts continue for several years but they rush to start the work because the time to finish the contracts is very severe. No one knows who will win the bid. The company who submits the lowest price will be the winner. It is said that collusions before a bid among companies are popular in Japanese public markets. Such behaviors are illegal.

Competitive bidding is ordinarily done in June or July as the Japanese government budget is to be passed at the Parliament in March. After the budget is assigned to each Ministry, the Ministry prepares the bid in April and May. A construction company that wins the bid can start the work after the bid.July or August is the beginning month of construction, and precast concrete products are to be used at the first stage of construction. For example, piling is the first work of constructing a building; that is, piles are needed prior to other work.

(3) Production process of precast concrete products

Cement, sand and pebble are materials (concrete). Steel net is set within a mold and concrete is inserted into the mold. After that, in the case of U-shape gutters and box culverts, the mold is vibrated and in case of Hume pipe and pile, the mold is rounded at high speed. In the case of pile, the mold is heated in an oven but the other three products are not heated. When the products are unmolded, the shape of the products look like finished products, but they are not completed. To get enough strength, a few months of drying process is needed under the sunshine. This means that a precast concrete product company can deliver the product to a construction company after the drying process.The construction company must wait for the process to be completed.

For the construction company, waiting for the concrete products is wasting time. Because a construction company cannot afford to waste time, the company requires the concrete products as soon as possible at the time when the company wins the bid. Well, what is the solution for this requirement?

(4) Solution

Precast concrete products can be ‘Made to Order’ production for the private sector market, but this

production method is impossible for the public sector market because of the customer requirement. The manufacturing companies solution is 'Make to Stock' production. They must have stocks of finished products and be ready to deliver the products as soon as the orders have come. This is a big risk for them because if a customer does not win the bid, the produced products for the customer will become unsold loss.

The concrete production company MSK[6])has specific customers (construction companies) and when such customers win a bid they are sure to order the concrete products from MSK. If the customer construction companies missed the bid they will not order the products, but MSK must prepare the stock; this is the 'Make to Stock' production method. Unsold finished products will result in loss for MSK. Minimizing the loss is an objective of a precast concrete product company's management. To accommodate customer satisfaction, MSK needs information from the market, manufacturing and warehouse departments. All the information must be integrated and shared with each department.

III. VIRTUAL COMPANY MSK AND CIM

3-1. Virtual company of precast concrete products

Here we have a virtual company manufacturing four kinds of precast concrete products. The name is MSK Company Ltd. (MSK). In Japan, Japan Concrete Company is the largest company specializing in the production of pile, whereas MSK produces all kinds of precast concrete products. As MSK is an all-round manufacturer in this industry, MSK has both private sector and public-sector markets.

MSK was founded in 1950 and was located in prefectures of north eastern Japan. With the Japanese government's policy of increasing rice production after World War II, lots of Hume pipes and U-shape gutters were needed for irrigating rice fields. Rice production was one of the main industries in north eastern Japan. MSK developed with this Japanese government policy. Irrigating rice fields belonged to the public sector market. On the other hand,in the 1970s, many tall buildings were constructed in big cities and piles were needed. MSK began to produce piles at that time. Construction of buildings belonged to the private sector market. Then the companies constructing big buildings needed piles.

We use a virtual company to simplify the practice. Real business is too complicated to recognize the issues to be solved. Virtual MSK Company is not a real company but it is

necessary for us to simplify and to recognize the core and essential issues and to get solution.

3- 2. Winning the competitive bid

Construction companies join the competitive bid in the public sector market. Both the Japanese government and local governments must use acompetitive bid when they order the construction of infrastructure such as rice fields, roads, bridges, highways, etc. Construction companies are required to submit the blueprint of the project and the price. The government checks the submitted documents and identifies the construction company with the lowest price. Construction companies give the job of drawing the blueprint to the civil engineering office. When a construction company wins the competitive bid it can start the construction and order the concrete products.

3- 3. Production of precast concrete products and CIM

As we have discussed, concrete manufacturing companies must produce products by 'Make to Stock' method. MSK produces the products before the time when the customer wins the bid and orders products from MSK, but MSK would like to minimize the loss from unsold stocks. How does MSK start the production for the customer?

MSK developed Computer Integrated Manufacturing (CIM) in the 1980s. CIM is a production management system that uses and shares information in three departments: marketing, manufacturing, and warehouse. Each department acquires and makes specific information for its own purpose and the computer (main frame operated by MSK headquarter office) gathers information from the local plants and offices which have three departments. The information can be shared by each department. This is the structure of CIM.

A plant manager makes the job orders (instructions) to the plant. Monthly, weekly and daily job order sheets are written. All manufacturing work must comply with the daily sheets.

Plant manager's work is subject to information from the personnel of the Marketing Department. Marketing Department personnel visit the customers and the civil engineering offices. In addition, they must read the trade papers to know the construction market. They acquire the market and customer information as precisely as possible. On the other hand, the Marketing Department needs the information of finished products and expected stocks on hand at the Warehouse Department. When they are asked the delivery date of products from the customers, they have to let them know it immediately.

The warehouse Department has the information of finished products, products in process, materials (cement, sand, puddle), and molds. The information must be shared with the Manufacturing Department and Marketing Department. Plant managers can decide the necessary amounts of production by knowing

the stock of finished products. As the molds of this industry are very heavy and large, it may take a few hours to pick them up from the warehouse. Plant managers must know the place where a necessary mold exists. In the case where a necessary mold is rented to another plant, it must be returned.

IV. IoT IN THE CIM CONTEXT

4- 1. What is IoT installed in the CIM?

Internet of Things (IoT) is one of the hot issues in IT technologies. The architecture of IoT consists of sensor, computer and Internet[7]). As the price of sensors is becoming lower and lower and many kinds of sensors are developed, the collected data by sensors is transmitted to the computer. The computer can forward the data to another computer via Internet. Thus, anyone can use the data for their own purpose. The purposes are not only for business but also for social security. For example, one of the authors visited Mainland China 25 years ago. At that time, many cars in the street were speeding. The drivers are not speeding recently because the police installed the detector sensor camera in the street. Speeding can be detected at once and the police arrest the driver soon by a face recognition system [8]).

Many business corporations have noticed the usefulness of IoT in business[9]). They analyze the business process to find the issues to be solved by using IoT. Many cases have been reported in books and journals. For example, a company specializing in boilers used IoT recently. Before using IoT, when the company received a telephone call letting them know the malfunction of the boiler the company sent the repairment team to the user company. The operation of the boiler must be stopped for a few hours until it is repaired, which causes a loss for the user. with IoT the boiler company has a contract with the user about installing several sensors in the boiler. These sensors are connected the computer of the company by Internet 24 hours per day. The boiler company can always watch the conditions of the boiler and they can fix malfunctions beforehand or they can repair them immediately after malfunction.

MSK has decided to install IoT in the CIM. CIM can be operated without IoT but the performance of CIM will be improved by installing IoT within the CIM. This is inbound IoT, within MSK. Outbound IoT connected with outside companies is also possible but this paper research is limited to inbound IoT.

4- 2. Architecture

The architecture of IoT consists of the following components [10]).

(1) Sensor

A sensor is defined as a device for collecting data in each department. Marketing Department personnel have a tablet to input customer data and to know the finished products

data, the Manufacturing Department has a camera watching the production line, and the Warehouse Department has a counting sensor at each lot or space.

(2) Edge Computer, Workstation, Cloud Computer

An edge computer is connected to the sensor and workstation to transfer data[11]). It is needed to decentralize the big data collected by the sensors. Each department has an edge computer. As MSK is using the cloud computer, the data is transferred from edge computers and stored there. MSK now doesn't have a main frame computer but uses a workstation. The workstation retrieves data from a cloud computer and makes necessary information for each department.

(3) Internet

The Internet has become a worldwide infrastructure now. No one imagined the development of the Internet when it was launched among universities. All computers on the Internet can be connected to each other by LAN cable and WiFi. Computers and other IT technologies are also developed along with the Internet. Big data can be collected by sensors and the data is transferred to computers through the Internet.

The Ministry of Internal Affairs and Communications of the Japanese government issued a White Paper Information and Communications in Japan, 2019[12]). They analyzed and forecasted IoT devices in the world and Japan as follows.

Table 4-1. IoT Devices in the industries

Military/Satellite/Airplane: IT and instruments in the cockpit, passenger transport system, monitoring system for military satellite, etc.
Automobile: control device under the hood, other monitoring devices connecting Internet
Telecommunication: networking device, cellular telecommunication system for 2G, 3G, and 4G, wireless communication infrastructure such as WiFi and WIMMAX, telecommunication terminals
Computer: computers such as note PC, desktop PC, workstation, main frame computer, super computer
Consumer goods: home appliances (white goods, digital appliances), peripheral equipment such as printers, portable audios, smart toys, sports and fitness equipment, etc.
Medical and Industrial equipment: diagnosis imaging apparatus, medical apparatus, goods, testing and measuring meters, etc. consumer healthcare equipment, automation (IA/BA), other industrial equipment such as lights, generators, security goods, testing and measuring meters, etc.

Source: Ministry of Internal Affairs and Communications, Japanese government, White Paper Information and Communications in Japan, 2019.

Table 4-2. IoT Devices (Japanese Yen: 100million) in Industries

Industry	2014	2015	2016	2017	2018	2019	2020
Total	170.7	205.1	241	274.9	310.5	354.4	403
Military/ Satellite/ Airplane	0.03	0.04	0.04	0.05	0.06	0.07	0.07
Automobile	3.8	4.7	6	7.5	9.2	11.6	14.4
Telecommunication	93.6	113.1	132.2	147.3	161.2	175.7	189.3
Computer	19.3	21.1	22	22.2	22.1	22	21.9
Consumer Goods	33.8	38.9	45.3	52	59.3	67.2	76.3
Medical	2	2.3	2.8	3.4	4.1	5	6.1
Industrial	18.2	24.9	32.7	42.4	54.5	72.8	94.9
					2018-2020 forecasted data		

Source: Ministry of Internal Affairs and Communications, Japanese government, White Paper Information and Communications in Japan, 2019.

IoT Devices in the industries

Military, Satellite, Airplane: IT and instruments in the cockpit, passenger transport system, monitoring system for military satellite, etc.

Automobile: control device under the hood, other monitoring devices connecting Internet

Telecommunication: networking device, cellular telecommunication system for 2G, 3G, and 4G, wireless communication infrastructure such as WiFi and WIMMAX,telecommunication terminals

Computer: computers such as note PC, desktop PC, workstation, main frame computer, super computer

Consumer goods: home appliances (white goods, digital appliances), peripheral equipment such as printers, portable audios, smart toys, sports and fitness equipment, etc.

Medical and Industrial equipment: diagnosis imaging apparatus, medical apparatus, consumer healthcare equipment, automation (IA/BA), other industrial equipment such as lights, generators, security goods, testing and measuring meters, etc.

Source: Ministry of Internal Affairs and Communications, Japanese government, White Paper Information and Communications in Japan, 2019.

4-3. Issues to be Solved by CIM with IoT

(1) Aim to use IoT

IoT devices have been used by many industries and the aim of using them is to identify issues in business processes or machines and to bring them to everyone concerned. This is called "visualization" by several industries in Japan. Sensors can collect data; CCD cameras collect photos, motion sensors collect body motions, smoke sensors collect smoke, thermometers collect fever and heat; etc. Such data is transferred from sensors to the edge

computer [12]).

(2) Issues to be solved by IoT at MSK

Issues to be solved depend on each company. In case of MSK, we identify the following issues to be solved by IoT in the CIM context.

(a) Watching manufacturing process in real time: Three elements are needed to make precast concrete products: concrete (cement, sand, and puddle), mold, and steel net. MSK has eight lines of production; two lines for each product (U-shape gutter, Hume pipe, box culvert, and pile). Plant managers send a weekly instruction sheet to line managers. Each line manager must have prepared mold and its steel net by the day prior to production. A mold with a steel net is set under the concrete inserter of each line. Concrete is liquid but it doesn't flow like water, so a U-shape gutter and box culvert must be vibrated and a Hume pile and pile must be turned around in order to release air from the concrete. CCD cameras are installed to watch the process above and AI makes judgments about the timing of completing the insertion of concrete. Experienced workers used to be responsible for this judgment. After they retired from MSK, AI is doing this job.

(b) Capturing unidentified market information: Each person in the Marketing Department of MSK (market personnel) has a tablet with application software for customer management. MSK's customers are the companies purchasing concrete products from MSK. Market personnel collect market information about specific construction from trade papers, civil engineering office personnel, and customer companies and input the collected information in the tablet. All the tablets are connected to the edge computer by Internet and the data is transmitted to the plant manager.

(c) Sharing inventory information among each department: the Warehouse Department is responsible for inventory management. Inventories for the precast concrete company are materials (cement or liquid concrete, sand, puddle), molds, steel wire, unmolded products to be dried, and finished products. These inventories are

stored in a warehouse and stock yard. The warehouse and stock yard have slots (spaces) where inventories are stored. Plant managers need the information about materials, molds and steel wire. Personnel in the Marketing Department need the information about finished products. The information kept by the Warehouse Department is shared by other departments.

V. SIMULATION FOR COST PERFORMANCE OF IoT

5- 1. Objective

The objective of the simulation is to confirm the IoT cost performance by comparing Opportunity Loss and Unsold Product Loss between With IoT and Without IoT[13]). We focus on IoT about the market information collected by the Marketing Department. If IoT contributes to decrease the loss amount, it is performance of IoT. We use a simulation technique because it has advantages for this kind of research. Opportunity Loss is defined as the loss which accrues when MSK has missed the customer order in case the stock of finished product is zero. Customers cannot wait for the lead time of production, so they will order products from another company. IoT of CIM context may minimize Opportunity Loss.

If MSK has enough inventories of products, Opportunity Loss will decrease but Unsold Product Loss will increase. MSK must use Make to Stock production method and it may have some amounts of unsold products at the term end. Such amounts will become losses. Unsold Product Loss and Opportunity Loss is in a trade-off relationship.

By using a simulation technique, we will calculate these losses and costs and compare these amounts in both with IoT and without IoT situations. Simulation has a big advantage over an empirical study because we can get as much data as we wish. We cannot get enough data in an empirical study because there is not enough available data in the real business. In addition, the data in business fluctuates by many factors, especially human factors. Simulation is done in a computer without bias and fluctuations by human factors.

5- 2. Initial conditions

Simulation starts from the initial conditions. We need to simplify the initial conditions of MSK as follows.

(1) Four kinds of concrete products: MSK producesmany kinds of precast concrete products.For example, there are about 50 different sizes of U-shape gutter produced by MSK. In addition, the construction company, MSK’s customer, might ask for a special feature to the product.But we simplify that MSK is producing just

four kinds of products as U-shape gutter (Product 1), Hume pipe (Product 2), box culvert (Product 3), and pile (Product 4). The numbers 1, 2, 3, and 4 are assigned because of the simulation technique.

(2) 500 stocks for each product at the beginning of the term. Simulation starts with the initial stocks of each product as 500. When 5 Product 1 were delivered to the customer, the residual stocks of Product 1 became 500- 5= 495. Delivery is made according to the invoice issued by personnel of the Marketing Department. The quantity of delivery varies from 1 to 5 randomly and the Marketing Department issues 200 invoices in a term. When the residual stock is estimated to zero, the Plant Manager issues the production order sheet. This estimation is made according to the report of the market forecast made by the Marketing Department. The Line Manager starts the production according to the order sheet. The lead time of the production is zero in the case with IoT,and a term in the case without IoT. The quantity of production of a production order is 100 for the case of With IoT and 500 for the case of Without IoT.

(3) Opportunity Loss: If the delivery invoice is issued when the residual stock is zero, the order becomes an Opportunity Loss. Recovery of stock is made at the average delivery invoice issued at the time of 166, which is the time when the residual stock becomes zero on average.

(4) Unsold Product Loss: As the Plant manager issues the production order sheet according to the estimated residual number of stocks. This estimation is made from the market forecast information by personnel of the Marketing Department. The forecast information is not the delivery invoice. Unsold products will remain at the end of a term in the case of With IoT. This stock

Table 5-1. Initial Conditions of Simulation

Product	u-shape gutter	Hume pipe	box culvert	pile
Product #	1	2	3	4
Price	100	120	150	200
Cost	60	72	90	120
Beginning	500	500	500	500

becomes Unsold Product Loss.

5-3. Calculation of loss and comparison between with IoT and without IoT

(1) Calculation of Opportunity Loss

MSK will miss the opportunity of a sale in the case when orders come but there is no stock of finished product. Suppose a Product 1 order comes with the quantity of order as three and the number of order in a term is 200. If the sale price of Product 1 is 100 per piece, then the Opportunity Loss is 3 x 100 = 300. The Plant manager issues a production order sheet when the estimated stock is zero and supposes that the lead time is zero in the case of With IoT and the lead time is a term in the case of Without IoT. MSK suffers the Opportunity Loss till the stock recovered on the next term in the case of Without IoT. The Opportunity Loss will be accumulated in a term.

(2) Unsold Product Loss

If MSK has some amounts of stocks at the end of a term, Unsold Product Loss accrues. Suppose the residual quantity of Product 1 is 60 at the end of a term and the cost is 60 per piece of Product 1, then the Unsold Product Loss is 30 x 60 = 1800. Unsold Product Loss is inevitable with the Make to Stock production method but in the case of Without IoT, Unsold Product Loss does not accrue because Stock on Hand becomes zero during the term.

Table 5-2. Calculations of Losses Example: Product 1

Term	Loss	Opportunity Loss		Unsold Product Loss	
	IoT	With IoT	Without IoT	with IoT	without IoT
Term 1	Beginning Stock	500	500	500	500
	Price	100	100	100	100
	Cost	60	60	60	60
	Loss number	60	200	30	0
	Realized Loss	6,000	20,000	1,800	0
Term 2	Beginning Stock	500	500	500	500
	Loss number	60	200	30	0
	Realized Loss	6,000	20,000	1,800	0
Term 3	Beginning Stock	500	500	500	500
	Loss number	60	700	30	0
	Realized Loss	6,000	20,000	1,800	0
	Total Loss	18,000	60,000	5,400	0

Table 5- 2 shows an example of Loss calculation. Loss with IoT from Term 1 to 3 is 18, 000 + 5, 400 = 23, 400; Loss Without IoT is 60, 000 during the same three terms. IoT performance is 60, 000 – 23, 400 = 36, 600. IoT has a positive performance in this example.

5- 4. Result of simulation

5- 4- 1. Additional conditions

We did a simulation for Product 1 (U-shape gutter). "With IoT" is the case in which the Marketing Department has collected enough information to estimate the time when the stock on hand becomes zero. On the other hand, "Without IoT" is the case in which the Marketing Department cannot collect market information and MSK cannot produce the products until the next term. We will compare the result of simulation between With IoT (Opportunity Loss and Unsold Product Loss) and Without IoT (Opportunity Loss only). If Loss of With IoT is less than Loss of Without IoT, then the difference amount is the performance of IoT.

The initial condition of this simulation is as shown in Table 5- 1. We will add the following conditions.

(1) Conditions in Table 5- 1: (a)sales price: 100, (b)cost of product: 60, (c)initial holdings: 500

(2) Sales opportunities in a term: 200 times

(3) Sales amounts of each sale: 1 to 5 randomly

(4) Addition of Stocks on Hand for With IoT: 166th sale, 100 stocks; No addition to Without IoT

(5) Recovery of Stocks on Hand at the next term: 500 stocks

5- 4- 2. Simulation of With IoT

We tried simulation of With IoT for 10 slots. Each slot has 10 terms. A term consists of 200 sales and 100 stocks are added at the 166th sale. As each sale delivery invoice has one to five products randomly, the average of delivery is three. Theoretical estimation of Stock on Hand will become zero will be 500 / 3 = 166. 67. The result of simulation is shown in Table 5- 3.

100 products are added to Stock on Hand at the 166th sale. This means that Opportunity Loss will be accrued if Stock on Hand becomes zero before the 166th sale. Table 5- 3 shows that the average Opportunity Loss is 600 in 10 slots with 10 terms in a slot. 600 Opportunity Loss will be accrued in a term.

Table 5-3. Opportunity Loss With IoT till 166 Sales

Sales	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9	Slot10		
#1	0	-31	0	-30	0	0	-22	0	0	-7		
#2	0	0	0	-3	-15	-5	-10	0	0	-9		
#3	0	-27	-14	-7	0	0	-12	-5	-3	-19		
#4	0	-13	-8	0	-22	0	-20	-11	0	-2		
#5	0	0	0	0	0	0	0	0	0	-3		
#6	-10	0	-18	0	0	0	0	0	0	0		
#7	-2	-31	0	0	0	-6	-16	0	-12	0		
#8	-2	0	0	0	0	0	0	0	-31	-47		
#9	0	-21	0	0	-21	0	-29	0	0	0		
#10	-5	-25	0	0	0	-5	0	0	-1	-8		
	-19	-148	-40	-40	-58	-16	-109	-16	-47	-95	-588	-58.8
	-2	-15	-4	-4	-6	-2	-11	-2	-5	-9	-60	-6
	-200	-1500	-400	-400	-600	-200	-1100	-200	-500	-900		-600

Table 5- 4 shows the simulation after the addition of 100 products at the 166th sale; 167th to 200th 33 sales in a term and 10 slots.

Table 5-4. Opportunity Loss and Unsold Products Loss With IoT 167-200

Sales	Slot 1		Slot 2		Slot 3		Slot 4		Slot 5		Slot 6		Tern 7		Slot 8		Slot 9		Slot 10		
	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	OC	UPL	
#1	4	0	0	6	0	13	8	0	0	7	0	10	0	4	0	1	10	0	3	0	
#2	6	0	0	5	0	0	8	0	6	0	0	13	0	2	0	0	0	0	0	12	
#3	0	0	1	0	0	2	0	0	0	3	8	0	0	7	0	4	0	4	8	0	
#4	0	12	0	5	0	15	0	15	1	0	3	0	0	6	0	2	0	22	0	3	
#5	0	2	2	0	12	0	0	6	0	5	1	0	3	0	7	0	0	1	0	2	
#6	0	4	4	0	5	0	3	0	0	5	1	0	0	4	0	1	0	3	1	0	
#7	4	0	0	1	0	9	0	4	0	23	0	14	0	5	0	0	3	0	0	0	
#8	3	0	1	0	0	0	0	1	0	2	0	10	3	0	2	23	2	0	16	0	
#9	0	2	0	1	11	0	0	9	0	10	0	7	2	0	21	0	1	0	0	14	
#10	7	0	2	0	0	6	0	3	10	0	16	0	0	14	10	0	0	9	0	11	
	24	20	10	18	28	45	19	38	17	55	29	54	8	42	40	31	16	39	28	42	
	2	2	1	2	3	5	2	4	2	6	3	5	1	4	4	3	2	4	3	4	
	200	120	100	120	300	300	200	240	200	360	300	300	100	240	400	180	200	240	300	240	
Opp Loss	200	0	100	0	300	0	200	0	200	0	300	0	100	0	400	0	200	0	300	0	230
US Loss	0	120	0	120	0	300	0	240	0	360	0	300	0	240	0	180	0	240	0	240	234

As 100 products are added at the 166th sale, either Opportunity Loss or Unsold Product Loss will be accrued at the end of a term. Table 5- 4 shows that the average Opportunity Loss is 230 in a term and the average Unsold Product Loss is 234 in 10 slots with 10 terms.

The average Opportunity Loss from 1st to 166th sales in a term is 600. 230 Opportunity Loss and 234 Unsold Product Loss from 167th to 200th sales in a term. The total loss With IoT is 1, 064 in a term.

5- 4- 3. Opportunity Loss Without IoT

Stock on Hand is to be recovered at the next term. Theoretically, Stock on Hand will become zero at the 166th sale. After that from the 167th to 200th sale, MSK will miss the sale. MSK must be patient with the Opportunity Loss in the case of Without IoT. Theoretical amount of the loss is 3 x 33 x 100 = 9, 900. Table 5- 5 shows the result of simulation of Opportunity Loss Without IoT.

Table 5-5. Opportunity Loss Without IoT 1-200 Sales

Sales #	Slot1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7	Slot8	Slot9	Slot10	
#1	66	141	97	100	83	109	77	91	110	117	
#2	89	103	86	101	67	125	87	121	102	127	
#3	66	123	71	87	121	108	90	84	104	113	
#4	80	91	117	110	101	100	45	115	90	87	
#5	96	101	80	98	129	129	98	87	92	98	
#6	113	74	98	113	112	85	72	68	78	108	
#7	62	93	94	122	88	127	93	118	108	152	
#8	88	116	77	153	140	105	72	94	89	89	
#9	90	143	111	112	104	86	119	151	102	100	
#10	101	120	109	79	100	82	93	85	106	83	
	851	1105	940	1075	1045	1056	846	1014	981	1074	
	85	111	94	108	105	106	85	101	98	107	
	8500	11100	9400	10800	10500	10600	8500	10100	9800	10700	100000
											10000

The result of simulation about the average Opportunity Loss in the case of Without IoT is 10, 000. It is very near the theoretical amount of 9, 990.

5- 5. Cost performance of IoT

We have done 10 slots x 10 terms simulations. Table 5. 6 shows the Loss Table.

Table 5-6 Average Loss Talbe

IoT	Opp Loss 1-166	Opp Loss 167-200	sub Total	UP Loss	Total
With	600	230	830	234	1,064
Without	-	-	9,990	0	9,990
Performance					8,926

The average loss in the case of With IoT is 1, 064; Without IoT is 9, 990. The difference amount of 8, 926 shows the performance of IoT. Our simulation is done just for Product 1. The result will be almost the same as Table 5. 6, but it depends on the cost of IoT. As we neglect this cost to install IoT, we should consider that amount in future research.

VI. CONCLUSION

The result of simulation shows that the cost performance of IoT is positive. The Marketing Department collects client information and market information. The collected information is gathered and is forwarded to the Manufacturing Department. The plant manager issues a job order. As MSK must manufacture products by the Make to Stock method, the job order must be based on correct market information.

With IoT enables MSK to make a correct estimation of the necessary quantity of production. MSK can minimize the Opportunity Loss and Unsold Product Loss. On the other hand, MSK must be patient to suffer a large amount of Opportunity Loss in the case of Without IoT. Simulation shows that MSK can decrease almost 90% of Loss by IoT.

As we pointed out, we ignore the cost of installing IoT (sensors, computers, and training expenses). We need to continue the research to consider the cost of IoT.

REFERENCES

1. Brogi, A. and S.Forti, QoS-Aware Deployment of IoT Applications Through the Fog, IEEE Internet of Things Journal, Vol. 4, No. 5, October 2017, pp. 1185-1192.
2. Chen, S., et al., A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective, IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014, pp. 349- 359.

3. Ding, W., Study of Smart Warehouse Management System Based on the IoT, Du, Z. (Ed): Intelligence Computation and Evolutionary Computation, AISC 180, Springer, 2013, pp. 203- 207.
4. Farris, I., et al., Federated Edge-assisted Mobile Clouds for Service Provisioning in Heterogeneous IoT Environments, IEEE, Working Paper, 2015, pp. 1- 6.
5. Gubbi, J., et al., Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 29, 2013, pp. 1645- 1660.
6. Jun, C., Application of Core Technologies for Smart Manufacturing: A Case Study of Cost Benefit Analysis Based on Modeling and Simulation for Sustainability, Proceedings of the 2017 Winter Simulation Conference, IEEE, 2017, pp. 4454- 4455.
7. Lee, K., et al., Application of IoT to Inventory Management in the Tire Industry, INFORMATION, Vol. 19 No. 11(A), pp. 5001- 5005.
8. Mahmud, B., et al., Internet of Things (IoT) for Manufacturing Logistics on SAP ERP Applications, e-ISSN: 2289- 8131, Vol. 9 No. 2- 6, pp. 43- 47.
9. Ministry of Internal Affairs and Communications, Japanese government, White Paper Information and Communications in Japan, 2019.
10. Mourtzis, D., et al., Industrial Big Data as a result of IoT adoption in Manufacturing, Elsevier, pp. 290- 295.
11. Teneja, M., et al., Resource Aware Placement of IoT Application Modules in Fog-Cloud Computing Paradigm, IFIP/IEEE IM 2017 Special Track on Management of IoT, pp. 1222- 1228.

FOOTNOTES

1. Computer Integrated Manufacturing (CIM) was one of the computerized manufacturing technologies proposed in the 1980s. The main objective of CIM is to find a solution tooptimize the quantity of production by integrating information in the market, inventory, and production. At that time, as the Internet was not available it was difficult to integrate information.
2. Internet of Things (IoT) is one of the hot challenges in IT. Everything can be connected to computers through the Internet. Sensors are implemented to everything and collect data. Big data, edge and fog computing, AI, cloud, and related technologies have been developed recently. Sensors are one of the key technologies.
3. ‘Made to Order’ production is possible in case the supply side (manufacturer) is stronger than the demand side (user, consumer, customer). We can easily find such markets. For example, mask production cannot satisfy demand because of COVID- 19. Governments around the world have invested money to the production lines of mask manufacturers to increase production.
4. ‘Make to Stock’ production is an ordinal situation in those markets and supply side

manufacturers are competing in the market. Demand side consumers can choose one of the commodities at the shop. Supply side manufacturers must show their products at a shelve of the shop. If they cannot do that they will miss the sale and suffer loss.

5. Din, W., Study of Smart Warehouse Management System Based on the IoT, Intelligence Computation and Evolutionary Computation, AISC 180, Springer, 2013, pp. 203- 207. The Warehouse Department is responsible for information of finished products, products-in-process, materials, equipment for production, and logistics.

6. The precast concrete products manufacturing companies developed rapidly after World War II in Japan because Japan needed to increase rice production and to construct infra-structure. Almost everything was destroyed by bombing during the war and as the army was dissolved, lots of people returned home tono food.

7. Brogi, A. and S. Forti, QoS-Aware Deployment of IoT Applications Through the Fog, IEEE Internet of Things Journal, Vol. 4, No. 5, October 2017, pp. 1185- 1192.

   Farris, I., et al., Federated Edge-assisted Mobile Clouds for Service Provisioning in Heterogeneous IoT Environment, IEEE, Working Paper, 2015, pp. 1- 6.

   Because of big data collected by sensors, it is difficult to deal with such data by a peer computer or a workstation. New computation technologies are needed such as fog, edge, and cloud.

8. Chen, S., et al., A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective, IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014, pp. 349- 359.

   Chinese society has changed dramatically since 2000. As the Chinese government adopted the open economic policy, many foreign companies moved their plants to China. China has become Plant of the World where airlines, highways, and rapid trains are developed. Lots of money have been invested in the research and development, and IT industries are also developed.

9. Lee, K., et al., Application of IoT to Inventory Management in the Tire Industry, INFORMATION, Vol. 19, No. 11(A), pp. 5001- 5005.

   Mahmud, B., et al., Internet of Tings (IoT) for Manufacturing Logistics on SAP ERP Applications, e-ISSN: 2289- 8131, Vol. 9, No. 2, pp. 43- 47.

   Many applications of IoT have been introduced by academic journals, books, and websites.

10. Gubbi, J., et al., Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 29, 2013, pp. 1645- 1660.

11. Teneja, M., et al., Resource Aware Placement of IoT Application Modules in Fog-Cloud Computing Paradigm, IFIP/IEEE IM 2017 Special Track on Management of IoT., pp. 1222- 1228.

    Mourtzis, D., et al., Industrial Big Data as

a result of IoT adoption in Manufacturing, Elsevier, pp. 290- 295.Resource management is needed for IoT because of big data.

12. Ministry of Internal Affairs and Communications, Japanese government, White Paper Information and Communications in Japan, 2019.

    The Japanese government enacted IT BASIC Act of 2015. IT policies have been executed according to this act.

13. Jun, C., Application of Core Technologies for Smart Manufacturing: A Case Study of Cost Benefit Analysis on Modeling and Simulation for Sustainability, Proceedings of the 2017 Winter Simulation Conference, IEEE, 2017, pp. 4454- 4455.

    Simulation is a useful technique for the analysis of IoT as real data is difficult to get.

Shodan為基礎的IoT安全等級與防護機制

Shodan-based IoT Security Level and Protection Mechanism

賴森堂
實踐大學資訊科技與管理學系助理教授
stlai@g2.usc.edu.tw

摘　要

資訊與網路技術持續演進，促使 IoT 的應用不斷擴增且融入民眾日常活動，大幅提升民眾生活品質與便利性。IoT 架構透過感測器大量蒐集民眾活動與消費行為，傳至雲端分析，可提升企業與組織的營運績效與服務品質，不過，業者未針對資訊安全善盡保護責任，勢必衝擊民眾個人與敏感性資料安全。政府單位與國際安全機構無法具體管制與規範 IoT 裝置的安全性，使得 IoT 安全議題成為安全威脅。在 IoT 年代，為了保護民眾個人與敏感性資料安全，本文以 IoT 網路搜尋引擎 Shodan 為依據，識別特定網域的 IoT 裝置型號與製造商，再透過多項安全事證剖析裝置的安全等級，主動確認 IoT 裝置的安全性，擬定一套 IoT 資訊安全防護措施，適時提醒民眾採取安全防範措施，以保護關鍵個人與敏感性資料安全。

關鍵詞：IoT、Shodan、安全標章、安全等級、個人與敏感性資料安全。

Abstract

The continuous evolution of information and network technologies has promoted the continuous expansion of IoT applications and integration into people's daily activities, which has greatly improved people's quality of life and convenience. The IoT architecture collects a large number of people's activities and consumption behaviors through

sensors, and transmits them to the back-end analysis, which can improve the operational performance and service quality of enterprises and organizations. However, if the industry fails to fulfill its protection responsibility for information security, it will inevitably impact the personal data and sensitive data security. Government units and international security agencies cannot specifically regulate and regulate the security of IoT devices, making IoT security issues a security threat. In the IoT era, in order to protect the personal and sensitive data of the people, this paper uses the IoT network search engine shodan as the basis to identify the IoT device types and manufacturers in specific domains. And combines several IoT security evidences to determine the security levels of IoT device. Draw up the IoT information security precautions, concretely confirm the security levels of IoT devices, and promptly remind the people to take security precautions to protect key personal data and sensitive data security.

Keywords: IoT, Shodan, IoT devices, Security levels,Personal and sensitive data security

壹、前言

IoT 技術與應用大幅提升企業與組織的營運效率與服務品質，增強市場的競爭優勢，也為人們帶來高度便利性與優質的生活，不過，IoT 運作環境卻存在許多待克服的挑戰，包括數據品質、處理效能、網路傳送速度、持續擴充能力及資訊安全等議題 (Sharma, 2018;Spofford, 2019)，其中，又以資訊安全議題衝擊最大也是民眾最關注的項目 (Maple, 2017; Chen, 2016)。因為 IoT 運作架構涉及感知層、網路層及應用層等三個技術層面，而且每一層面都存在多項安全問題與危機，感知層的 IoT 裝置或設備出廠前，廠商必須規範一套正確性與安全性的完整檢測程序，以確認產品已符合安全準則。網路傳輸作業經常是資訊被竊取的關鍵，加入密碼學的安全性應用演算法，可以降低網路層的安全風險。應用層除了必須導入資訊安全管理制度，也要遵循個資法的規範。此外各層級整合後的 IoT 運作架構更需要進行全面性的安全檢核且通過嚴格的滲透測試，以善盡保護用戶的個人資訊安全。不過，IoT 裝置、資訊設備及網路技術持續快速演進，政府相關單位與國際安全機構無法全面配合 IoT 環境演進，制定出新的安全條款與規範，很難有效檢測與具體管控 IoT 裝置的安全性，使得 IoT 運作環境存在難以克服的資訊安全危機。

一般民眾申請銀行帳號、手機門號、信用卡或是學校入學都必須提供完整的個人資料，以便確認客戶或學生的真實身份。這些個資可以協助檢、警、調處理相關犯罪事件的調查作業，不過，「個資保護法」對於個資與敏感性資料蒐集、處理及利用有嚴格的規範，甚至要求蒐集民眾個資與敏感性資料的組織或機構必須導入一套資訊安全管理系統 (ISMS) 如 ISO 27001, BS 7799，且善盡保

護個人資料安全的責任，以避免個資與敏感性資料外洩，遭到濫用，造成民眾的困擾與危機。現今 IoT 技術廣泛運作的環境下，許多民營企業或組織為了提升市場競爭力且增加營利，在未明確告知的情況下，大量取得民眾的個資與敏感性資料，未獲得民眾同意，即不當使用個資與敏感性資料，且未善盡保護個人資料敏感性資料安全的責任，造成民眾極大的困擾與恐慌。IoT 的安全問題與缺失，對一般民眾可能造成的衝擊與影響：

- 個人行蹤隱私：個人的行蹤一旦被他人隨時掌握，無法隱密，即喪失個人行蹤的隱私權，對於個人人身安全造成很大的威脅。
- 個人樣貌隱私：個人的照片一旦外洩，可能被搜索、誤用或濫用，對於個人造成生活起居上的困擾。
- 個人生活習性：一般聯營或量販店會記錄消費者的購買習性，再透過各種管道發送促銷廣告，影響個人的生活習慣且浪費多項資源。
- 個人健康狀態：個人健康資訊是關鍵隱私，一旦外流，不僅會影響找工作或就業的機會，且經常收到不需要的藥物廣告或詐騙的簡訊與電話，造成生活上極大的困擾。
- 個資與敏感性資料：個資與敏感性資料包括身分證號、生日、住址、信用卡號、帳戶密碼、病歷、樣貌等重要資料項目，因蒐集單位的疏失而被盜用，勢必造成民眾難以預期的損失。

IoT 的應用越來越多元，民眾個資、敏感性資料與日常生活的各項活動都是企業與組織蒐集對象，這些資料未能妥善管理，一旦被有心人士竊取且不當利用，勢必會對民眾造成極大的衝擊。最嚴重的情況是當裝置或設備被駭客入侵後，一般民眾根本無法立即察覺，企業或組織更不會主動告知，直到民眾發現個資或敏感性資料被不當利用，為時已晚。為此，本文以 Shodan 為基礎，規劃 IoT 裝置安全評估機制，進而提出一套 IoT 資訊安全防範措施，主動確認 IoT 架構的安全性，適時提醒 IoT 民眾採取安全防護機制，以保護民眾個人資料安全。第二節針對 IoT 架構與安全問題及 IoT 安全制度之建立進行探討。第三節討論 IoT 裝置安全評等的擬訂方式以及應採取的安全防護措施。第四節以網路設備清查工具 Shodan 為依據，提出 IoT 安全防護作業流程。第五節評估 IoT 安全防護措施的限制與效益評估。第六節再次強調 IoT 個人資料安全的重要性，及 IoT 安全防護流程的貢獻，且針對本主題作結論。

貳、IoT裝置安全議題

IoT 技術與應用面臨許多急待克服的挑戰，而安全缺失問題的影響力則是多項挑戰最受關注的項目之一，值得深入探究。

一、IoT 架構與安全問題之探討

IoT 架構以雲端運算為核心 (Jiang et. al., 2014；陳響亮等，2017)，架構分為應用層、網路層感知層三個階層 (鄭逸寧，2011)。IoT 三層架構運作與面臨的安全威脅說明如下 (參閱圖 1)：

(1) 應用層：企業與組織將 IoT 感知器搜集到大量資料進行篩選、分析、分類與處理，以協助企業與組織規劃

商業活動與提升營運效益，這些資料大都涉及個資與敏感性資料，企業與組織對於用戶的個資與敏感性資料必須善盡保護責任，應用層的安全漏洞經常造成資安事件且導致個資與敏感性資料外洩，將為民眾帶來生活上的困擾與安全危機：

- 應用層對於客戶的個資與敏感性資料未規範一套安全保護措施。
- 應用層缺乏一套嚴謹的存取權限管控與身份確認機制。
- 應用層使用的應用軟體本身存在安全漏洞與缺失。

(2) 網路層：在 IoT 的運作環境中，網路層是連接感知層與應用層的傳輸介面，負責 IoT 裝置蒐集的資料與應用層之間數據的傳送，網路層的安全控管相當重要，一旦傳送的資料被駭客截取或竄改，都可能造成難以預期的後果，網路層的安全威脅如下：

- 缺乏無線通訊安全的管制作業。
- 數據在網路中傳輸易遭受外部截取。
- 資料加密、安全認證、安全管理及入侵檢測等技術不足。
- 大功率無線設備可直接干擾其訊號。

(3) 感知層：感知層是由端點設備所組成，也因此其安全著重於訊息蒐集的安全與設備的安全。感知層對終端設備需要制定一套安全標準，從晶片設計、電路設計到系統及軟體都要符合安全規範，對於使用的安全應包含用戶認證、數據儲存安全及權限管理等。感知層的安全威脅說明如下：

- 設備無人監控、機器容易被破壞盜取或冒名使用。
- 為降低成本，硬體結構簡單、缺少加密性與安全性、容易被偽造，訊息容易被推算。
- 裝置的傳輸及安全標準不同。

不過，隨著技術與環境持續的演進，網路層結合 5G 的網路技術提升數據傳輸的效率，應用層將人工智慧的學習能力與推論能力融入 IoT，有學者提出四階層的 IoT 架構用以改善資訊安全與個人隱私的議題 (Chen, 2016)，也有業者將 IoT 平台加入網路層與感知層之間 (Lueth, 2019)，大幅提昇 IoT 的運用領域，且有效減少人力資源。此外為了改善 IoT 運作的安全危機，應該從製造商、企業與組織及一般使用者等三方面各自承擔其責任：

(1)IoT 裝置製造商的責任 :IoT 設計初期，就必須將安全性納入考量，參與產品設計與開發的團隊必須接受資訊安全訓練課程，且具備安全開發經驗。產品在上市前，除了進行各項功能性、品質、效能等測試外，還必須完成高安全性的滲透測試。

(2) 蒐集 IoT 資訊的企業與組織的責任：應導入資訊安全管理制度，對蒐集的資訊須善盡保護個資與敏感性資料安全的責任，且嚴格管控使用的 IoT 設備，若是無法修補的設備，應考慮隔離於主要網路之外。防護措施需將整個網路架構納入資安考量，並在採購時，要求廠商確保設

備安全性。

一般使用者的責任：使用 IoT 裝置前，應了解使用裝置的風險，如果不確定設備的功能，最好就不要使用。使用時，要將預設密碼更換成高度複雜的密碼。

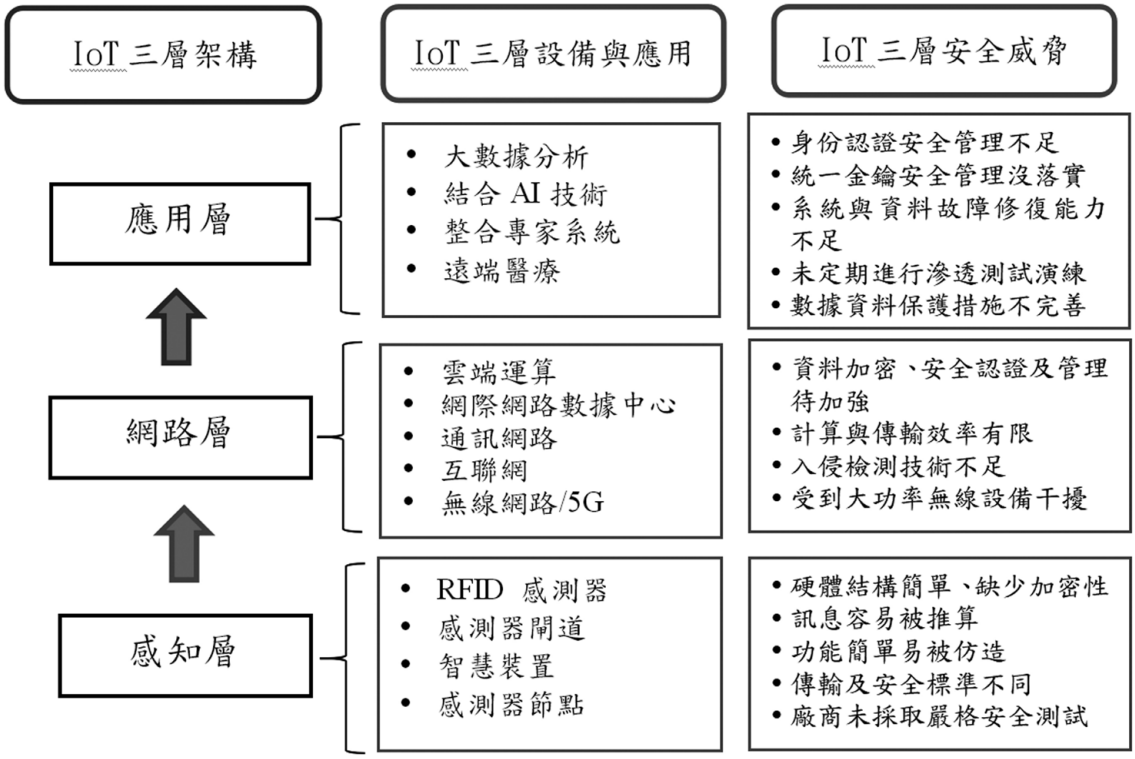


圖 1. IoT 三層架構的任務與安全威脅示意圖（本研究整理）

二、IoT 裝置安全規範與安全標章之探討

2018 年 9 月加州州長簽署了「 SB- 327 資訊隱私：連網裝置 」的法案，成為第一個 IoT 裝置安全法，此一法案將於 2020 年 1 月 1 日開始執行，要求製造商為 IoT 裝置提供合理的安全功能，以保障裝置及其資料的安全，不受非授權存取、破壞、濫用、修改或洩露 (林妍湊，2018)。為了改善 IoT 安全的風險，各國政府開始重視 IoT 的安全政策，也對此進行一些政策上的規範，例如：歐盟推行的「 歐盟 GDPR 和歐盟網路安全法案 」、2020 年即將實施的「 加州及奧勒岡州 IoT 裝置安全法案 」、美國國會提出的「 美國 IoT 網路安全改善法 」草案、中國提出的「 中國物聯網安全國家標準 」等等 (薛正，2019)。而在近期，領先全球的安全科學公司 UL(優力國際安全認證有限公司) 建立了一套標準 IoT 安全評等 (IoT Security Rating)，藉此定義 IoT 設備的資安防護能力，且將 IoT 安全性區分為鑽石、白金、金、銀、銅等五等級 (薛正，2019)。安全評等機制大幅減輕製造商對於產品評估與監測所投入的測試成本與時間，有效改善資訊安全漏洞的風險，除了讓大眾可以更直接了解產品的安全性，更讓廠商從產品設計與

維護製程，進一步了解產品本身的缺失與不足。在國內，UL 今年與台灣政府相關單位及企業共同合作成立物聯網資安聯合檢測中心，為台灣的 IoT 資安把關。2018 年 12 月 NCC(國家通訊傳播委員會) 與經濟部攜手推動「物聯網設備資安檢測制度及認證標章」，除了激勵相關設備製造商更重視資通安全、爭取認證外，也可提供消費者選購時的參考。在此之前，台灣資通產業標準協會也制定一套影像監控系統資安產業標準，為消費者在網路攝影機使用過程的資訊安全與個人隱私進行把關。選擇導入資安管理制度的製造商且通過安全認證或安全標章的 IoT 裝置，可以保障民眾個人資訊與隱私安全。表 1 為資安管理制度與 IoT 裝置安全標章機構彙整表。

表 1. 資安管理制度與 IoT 裝置安全標章機構彙整表（本研究整理）

資安管理制度 / IoT 安全標章 / IoT 安全認證	發起組織 / 機構	安全識別方式
GDPR	歐盟	公司或組織取得資安證照
ISO 27001/BS 7799	ISO/BSI	公司或組織取得資安證照
IoT 裝置安全等級	UL 安全認證公司	IoT 裝置取得安全等級
NCC 1. 1 IoT 安全檢查制度	NCC	IoT 裝置取得安全標章
影像監控系統資安產業標準	台灣資通產業標準協會	IoT 裝置取得安全認證

叁、IoT裝置安全評等與防護措施

有效確認 IoT 裝置的類型與劃分安全等級，可以規劃出較為具體的安全防護措施。

一、IoT 裝置的類型劃分

IoT 裝置的種類繁多，用途、功能與特質也有很大的差異，且不斷有新的產品推出，所以不可能針對個別的 IoT 裝置提出不同的防護措施，此外不同用途的 IoT 裝置對於民眾的安全威脅也不盡相同，因此必須先了解 IoT 裝置的功能與特性，才能採取適當的安全防護措施。本文以一般民眾較常接觸的 IoT 裝置進行特性分類，將 IoT 裝置分成網路監控裝置、無限通訊裝置及行動支付裝置等三大類型，且針對不同類型 IoT 裝置的定義與安全防護措施說明如下：

(1) 網路監控裝置：一般透過網路攝影機、網路監視器等 IoT 裝置，可以即時取得遠端或重要關卡的影像，協助防範犯罪或遏止違法的行為。不過，IoT 裝置缺乏安全保護設施，一旦被駭客入侵，監視影像將被截取且在網路上傳播，若配合人臉辨識的應用軟體，更會暴露民眾的行蹤，對於個人資料安全造成極大的影響，須慎選廠牌與產品型號才能降低此類型的安全風險。

(2) 無線通訊裝置：短距離的網路通訊設備 (如 WiFi, 藍芽、RFID、紅外線等)，已經取代許多實體的連線裝置。不過，這些裝置需要取得連線者資料才能運作，例如：WiFi 印表機須先存取接收到的資料再執行列

印的動作，基地台須取得行動裝置的帳號才能進行連線。無線通訊 IoT 裝置缺乏安全保護機制，可能會遭到惡意程式攻擊，使得用戶的個資與敏感性資料被盜用或濫用，造成難以預期的損失。應該避免使用曾經發生資安事件的產品型號與廠商之設備。

(3) 行動付款裝置：為了提升服務品質與交易的便利性，超商、速食店與許多飲料店都紛紛推出行動支付的付款方式，支付行為又分為 LINE PAY、APPLE PAY、手機信用卡、行動 SD 卡、QR Code 等，可直接使用行動裝置、RFID 或信用卡支付，接收各種付款方式 IoT 的裝置，必須具備高度的安全防護能力，有效保護消費者個資與敏感性資料，營運的公司與組織對於後端的運作環境與設備也必須導入資訊安全管理制度，善盡保護用戶的個資與敏感性資料的責任。使用者應該進一步確認此類型裝置的安全性，以保護個人資料與敏感性資料安全。

二、網路 IoT 裝置搜尋工具

「知己知彼 , 百戰百勝 」，對於 IoT 裝置的關鍵屬性有深入的了解，才能針對個人資料安全採取適當的防護措施，本節剖析幾項使用率較高的網路 IoT 搜尋工具，包括 Shodan, Censys,BinaryEdge 及 ZoomEye 等 (耿浩然，2017; OSINT, 2019)，整理說明如下：

(1) Shodan 是由程式設計師 John Matherly 於 2009 年推出的，早在 2003 年，Matherly 就已提出搜索與 Internet 鏈接設備的想法。Shodan 受到關注的能力就是可搜尋到與 IoT 有關聯的連網設備。Shodan 主要是針對伺服器、網絡攝影機、交換機、路由器等網絡基礎設備做掃描。Shodan 創建帳號是免費的，可以取得基本的設備資料，申請 Shodan 會員，可以取得更完整的服務。

(2) Censys 是由密歇根大學和 Rapid 7 公司共同合作完成，當初建製的目的主要是用於學術研究上，並被定義為一個非營利項目，所以 Censys 不收取任何費用項目，且所有數據都可提供免費下載。

(3) BinaryEdge 是一家瑞士公司，創建於 2015 年，提供一整套的數據安全解決方案，包括適時防火牆的守護掃描及整個網絡安全，在開放平台方面邁出巨大一步，已發展為一套具有廣泛搜索、過濾和下載功能的 OSINT(Open Source Intelligence) 工具，現在似乎能與 Shodan 匹敵，是一套著重於網路安全防護的工具。

(4) Zoomeye 被多數人認為是中國版本的 Shodan，也是中國第一個半開放式的網路搜索引擎，其功能能夠讓用戶快速查閱搜索設備在全球的分部情況。雖然 Zoomeye 針對普通用戶是免費的，但是在商業版也有自己的收費項目。

其中 Shodan 開發的時間最早、用戶數最多、網路上最多人討論，不僅提供多種程

式語言的 API，產品品質與安全性也獲得使用者的認同，是市占率最高的網路 IoT 裝置搜尋工具。至於其他工具也是常用的 IoT 搜尋引擎，他們跟 Shodan 之間的差異大概就是搜尋方式不同、掃瞄工具不同，或是收費模式不同等，基本上是各有優劣，請參閱表 2 網路設備搜尋引擎關鍵特性比較表。

表 2. 網路設備搜尋引擎關鍵特性比較表（本研究整理）

網路設備搜尋引擎 比較關鍵特性	Shodan	CenSys	BinaryEdge	ZoomEye
設計 / 開發國家	美國	美國	(歐洲) 瑞士	中國
對一般民眾具可用性	V	-	-	V
提供多種程式 API	V	V	-	V
基本功能不收費用	V	V	-	V
產品品質與安全性	V	-	V	-
用戶多且易取得支援	V	-	-	-

三、IoT 裝置安全評等方式

一般民眾缺乏 IoT 相關技術也沒有資訊安全的關鍵知識，因此對於 IoT 裝置的安全性很難適時進行有效評估，本文蒐集 IoT 裝置四個層面的安全事證做為 IoT 裝置安全評等的依據：

(1) IoT 裝置本身的安全標章或安全認證是關鍵且重要的事證：雖然目前提供 IoT 裝置安全標章或安全認證的機構並不多，不過，通過具公信力機構安全認證的 IoT 裝置，應該可確定 IoT 裝置的安全性。目前國內的 IoT 裝置安全標章與安全認證的機構有：

- UL 公司制定之 IoT 安全評等標章
- 台灣資通產業標準協會制定之影像監控系統安全認證標章

(2) IoT 裝置本身是否設定嚴謹的安全管理機制：網路上許多設備為了管理方便而忽略了安全性，完全沒有設定使用者權限，缺乏安全的管制措施，任何人都可以登錄使用，有心人事也可以利用安全管制不足的設備進行資料竊取、竄改與濫用等不法的惡意行為。因此，應該避免使用缺乏安全管制的 IoT 裝置。

(3) 製造商是否導入資訊安全管理制度：製造商取得安全標準認證，勢必直接或間接影響產品的安全品質，國際及國內資訊安全管理制度包括 ISO/IEC 27000 系列標準、英國標準協會 BS 7799、CNS 27000 系列標準，可藉由網路搜尋確認製造商是否已取得任一種安全標準認證，用以判斷的 IoT 裝置的安全等級。

(4) 資安事件的報導是值得注意的安全評等項目：俗話說壞事傳千里，因此當有某一項 IoT 裝置或某一家製造商發生被入侵、被濫用或資料被竊取等資安事件，造成個資與敏感性資料外洩，勢必在網路迅速傳遞，以

提醒民眾小心防範，因此，資安事件也是安全評等的項目。本文引用具高可靠度的兩項網路資安事件資訊，其中國家資通安全通報應變網站 (https://www.ncert.nat.gov.tw/#) 會不定期公布國內外發生的資安 (事件) 新聞，iThome 新聞網每一或兩個月發布十大資安新聞 (羅正漢，2020)。

本文依上述的四項安全事證，對 IoT 裝置的安全等級進行評估，將 IoT 裝置分成 4 個等級，劃分的方式說明如下 (參閱表 3 所示)：

優質等級：IoT 裝置取得安全標章、製造廠商取得資訊安全制度證照、裝置具安全管理機制且未發生任何資安事件者屬於優質等級，可安心使用。

良好等級：IoT 裝置取得安全標章或製造廠商取得資訊安全制度證照、裝置具安全管理機制且未發生任何資安事件者屬於良好等級，可使用。

尚可等級：IoT 裝置未取得安全標章或製造廠商未取得資訊安全制度證照，裝置缺乏安全管理機制，也未發生資安事件者屬於尚可等級，需小心可使用。

劣質等級：IoT 裝置曾發生資安事件者都屬於此等級者屬於劣質等級，不推薦使用，不須再判斷是否取得安全標章或製造廠商是否取得資訊安全制度證照，裝置是否缺乏安全管理機制。

表 3. IoT 裝置分成 4 個安全等級（本研究整理）

安全等級	產品取得安全認證或標章	製造商通過 ISMS 認證	具安全管理機制	發生資安事件	使用建議
優質	V	V	V	-	可安心使用
良好	至少取得一項證照		V	-	可使用
尚可	至少取得一項證照		-	-	小心使用
劣質	-	-	-	V	不推薦使用

肆、Shodan為基礎的安全防護流程

了解周遭網路環境 IoT 裝置，才能採取適當的 IoT 安全防護措施，本節以網路設備清查工具 Shodan 為依據擬訂 IoT 個人資料安全防護流程。

一、網路設備清查工具 Shodan 的應用

為了快速清查周遭網路環境的 IoT 裝置與設備是否具備安全性，首先必須採用網路裝置搜尋工具，清查連結特定網路區域的 IoT 裝置，且識別出 IoT 裝置的型號與製造商，再進行安全性的確認。本文以 Shodan 搜尋引擎清查特定 IP 範圍的 IoT 裝置 (林宜進，2019; TACERT, 2019)，以下分三個步驟說明 Shodan 運作方式：

(1) 設立 IP 範圍：於 Shodan 網頁登錄帳號後，設定要搜尋的 IP 範圍：49. 158. 197. 244」(搜尋指定的 IP 位置或是網段)，工具搜尋後呈現網頁內容如圖 2(a) 所示。

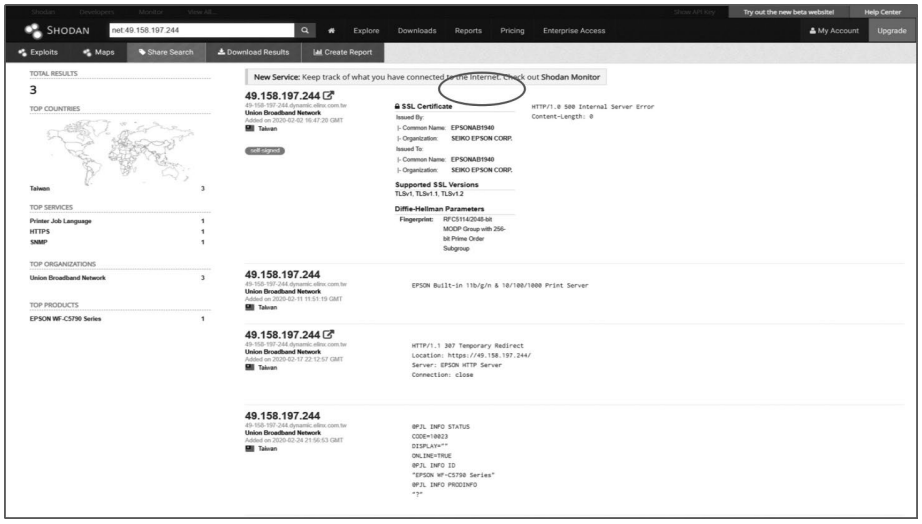


圖 2(a)．Shodan 工具搜尋後呈現網頁

(2) 點選取搜得的 IoT 裝置：點選搜得的第一筆資料後，發現可以直接進入列表機伺服器網站，並無任何密碼設置可以直接進入網站內部查詢相關列印歷史資料 (如圖 2(b) 所示)。

(3) 識別出裝置的製造廠商與產品型號：查看產品詳細資料的 Product 欄位找到該 IP 位置的聯網設備為 EPSON WF-C 5790 再加上藉由 Nmap 查詢 9100 埠的連線狀態為開啟 (如圖 2(c) 所示)，可能被有心人士利用，所以綜合以上敘述，此產品可能有網路安全性的疑慮。

以 EPSON WF-C 5790 為例，此產品並未取得或無安全標章，製造商已取得 ISMS 證照，使用時缺乏安全管理機制，且未發生過資安事件，依前一節 IoT 裝置安全評等方式，此產品只能被評為「尚可」等級，建議小心使用。

圖 2(b) 列表機伺服器的列印歷史資料

圖 2(c). Nmap 查詢 9100 埠的連線狀態

經由搜尋且識別的 IoT 設備，可以剖析該裝置的製造廠、產品用途、完整的型號與安全管制措施等關鍵安全屬性，這些屬性是確認 IoT 設備安全性的依據。Python 是一套功能強大且易學的物件導向程式語言，且具有免費的開發環境與套裝模組 (軟體)，可以在不同平台上安裝，完成的應用程式可以跨平台。Shodan 官方提供多項 Python 套件，提供使用者可選用 CLI(命令列) 或是撰寫 Python 程式呼叫 Shodan 支援的模組套件，引用 Python API 不僅可以取得更完整的資訊，而多種免費 Python 套裝模組也可協助快速撰寫一套網路爬蟲的程式，針對特定 IoT 設備的網路資料快速搜尋且進行安全事證分析。透過路爬蟲的程式搜尋作業，可以確認設備製造商是否建制資訊安全管理制度、IoT 裝置是否取得安全標章或通過安全認證等，如 NCC 推動之「物聯網設備安全認證標章」。匯集 IoT 裝置的製造廠、產品用途、完整的型號與安全管制措施等關鍵安全屬性，可以蒐集 IoT 裝置的安全事證且協助判斷 IoT 裝置的安全等級。

二、IoT 安全防護流程

瞭解 IoT 裝置的用途、功能、安全措施、型號與製造廠等關鍵屬性，才能判斷其安全等級，且針對有安全顧慮的 IoT 裝置採取適當的防護措施。本文設計的 IoT 安全防護流程分為五個步驟 (參閱圖 3)，說明如下：

步驟 1. 以 Shodan 工具搜尋設定網域的 IoT 裝置：

以網路設備的 IP address 可以設定周遭網域，再透過 Shodan 搜尋工具所提供的 Shodan Filters • net 指令可以清查出特定網域的 IoT 裝置與設備，如 product: 產品 / 軟體 (product:mongodb) version: 版本等。

步驟 2. 識別 IoT 裝置與設備的廠商與產品型號：

結合 Shodan API 進行搜尋後的分析與處理，不僅可以取得更完整得數據，而且能夠配合相關的應用或處理程序實現自動化分析效益。本步驟將撰寫 Python 程式引用相關模組，針對 Shodan 工具搜尋結果進行進階的分析作業，除可快速獲得特定網域內的 IoT

裝置與設備，更可具體識別出 IoT 裝置與設備的製造商與產品型號，以及設備的安全管理措施。

步驟 3. 搜尋 IoT 製造廠商、產品型號與安全事件等關鍵的安全事證

以網路爬蟲搜尋關鍵 IoT 型號、IoT 製造商的安全管理制度及安全事件等事證，包括：

- 利用網路的查詢確認裝置是否已通過安全認證或取得安全標章。
- 檢視製造廠商是否建制一套 ISMS。
- 確認 IoT 裝置或設備廠商是否曾發生資安事件。

步驟 4. 剖析 IoT 裝置與設備的安全等級

依 3. 3 節 IoT 裝置安全評等方式，以四項安全事證區分裝置的安全等級，且建議使用優質與良好等級之 IoT。具體判斷裝置的安全性，且列出存在安全質疑的 IoT 裝置與設備。

步驟 5. 採取適當的安全保護措施

針對 IoT 資訊安全風險的威脅，可以分為兩方面的保護與防範措施：

(1) 主動式安全保護措施：

- 識別 IoT 裝置與設備的安全性。
- 判斷 IoT 設施歸屬企業與組織的資訊安全制度。
- 勿主動連結有安全疑慮的 IoT 裝置與設備。
- 勿主動連結未導入資訊安全管理系統的企業與組織所架設的 IoT 設施。

(2) 被動式安全保護措施：

- 設定避免行動裝置被定位之功能。
- 設定避免被不明 IoT 裝置或設備連結之功能。
- 在未知的環境下，盡可能關閉藍牙、WiFi 及可被連結之功能。

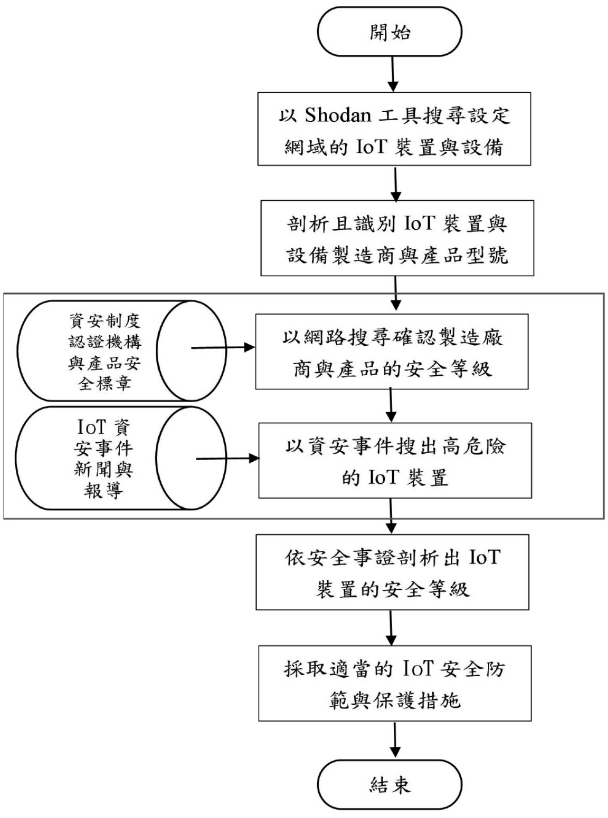


圖 3. IoT 安全防護作業流程圖（本研究整理）

伍、IoT安全防護措施的限制與效益評估

本文以網路設備清查工具 Shodan 為基礎，搜尋特定網域的 IoT 裝置，識別 IoT 裝置的型號、製造商與裝置安全管理措施，再從多項安全事證確認 IoT 裝置的安全等級，進而提出一套 IoT 安全的防護措施，採取主、被動方式防範 IoT 運作環境的安全風險。不過，環境的變遷，資訊技術持續演進，IoT 設備製造商不斷推出新的 IoT 產品或型號，受限於現實的條件，IoT 設備的安全認證機制與安全標章都屬於規劃或擬訂過程的起步階段，IoT 設備型號的安全事證並不易取得，因此，初期先以 IoT 裝置的安全管理措施、是否曾經發生資安事件、製造商的信譽，及製造商是否導入資訊安全管理制度為評估 IoT 安全等級的關鍵項目。當輿論與民眾對 IoT 安全有進一步的認識與要求後，將促使政府單位與國際機構制定標準的 IoT 安全規範，此階段將帶動各種 IoT 設備的安全標章與認證制度，對本研究提出的 IoT 安全防護措施勢必帶來更具體且完整的效益。本文規劃的 IoT 資訊安全防範措施，初期展現的成果說明如下：

- 探討 IoT 運作環境對個人安全的影響
- IoT 裝置安全認證與安全標章制度建立之探討
- 適時清查周遭環境之 IoT 裝置並識別 IoT 裝置的安全性
- 採取主、被動方式防範 IoT 架構的安全風險
- 具體提高民眾對 IoT 安全議題的重視與認知
- 保護民眾關鍵資訊安全與個人隱私

陸、結論

隨著資訊技術與網路環境的持續演進，促使 IoT 的多項應用已完全融入人們的日常生活，如行動支付、無線上網、GPS 定位、人臉辨識、網路點名等，大幅提升民眾生活品質與便利性。不過，IoT 環境的快速發展，也帶來許多的挑戰，特別是個人資料安全方面的問題，IoT 裝置製造廠為了降低開發成本與加快上市時間，並未將關鍵性的安全品質融入裝置中，也未考量使用者與一般民眾的隱私安全，而政府單位也無法適時擬定 IoT 設備的安全規範，對於民眾個人資料安全造成極大的威脅。為了保護民眾的個人資訊安全與隱私，本文以網路設備清查工具 Shodan 結合 IoT 安全等級評估，列出一般使用者 IoT 安全防護機制，藉由 Shodan 清查出周遭網域的 IoT 裝置與製造廠商，再利用網路爬蟲蒐集 IoT 裝置的安全事證，具體評估 IoT 裝置的安全等級，且依據 IoT 裝置的特質，適時提醒民眾採取適當的 IoT 安全防護措施，以保護關鍵個人資料安全。

參考文獻

1. 陳響亮，沈彥成，& 馮盟翰，2017，基於雲端與邊際運算架構之嵌入式居家環境品質偵測系統，TANET 2017 臺灣網際網路研討會，pp. 183- 188。
2. 鄭逸寧，2011，物聯網技術大剖析，iThome，2011 年 12 月。 https://www.ithome.com.tw/news/ 90461
3. Chen, C. W., 2016，以四層式物聯網架構提昇物聯網環境之安全與可用性，朝陽科技大學資訊管理系學位論文。

4. 薛正，2019，物聯生活不給「駭」UL IoT 安全評等大揭密，Taiwan, UL。https://taiwan.ul.com/blog/ 201912_ iotsecurityrating/
5. 林宜進 (2019)，Shodan 簡介與應用，NASOC。http://www.tp 1rc.edu.tw/tpnet 2019/ 2019meeting 1_ 5_ 1.pdf
6. TACERT, 2019，IoT 設備資安防護指南 , 臺灣學術網路危機處理中心團隊 (TACERT) 製 2019 年 4 月 30 日。
7. 林妍溱，2018，加州通過第一個 IoT 裝置安全法 , ithomehttps://www.ithome.com.tw/news/ 126165
8. 耿浩然，2017，網絡空間搜索引擎全方位評測，合天網安新聞 (FreeBuf.COM)https://www.itread 01.com/articles/ 1489723261.html
9. 羅正漢，2020，2020 年 6 月十大資安新聞，ithome 網安新聞 (iThome.COM) https://www.ithome.com.tw/news/ 138602
10. Sharma, R., 2018, Top 10 Challenges Enterprises Face In IoT Implementation, finoit, 2018. https://www.finoit.com/blog/enterprise-challenges-in-iot/
11. Spofford, D., 2019, The Top 6 Problems When IoT Products Hit the Real World,verypossible, June 4, 2019.
12. Lueth, K. L., 2019, The 25 best IoT Platforms 2019 – based on customer reviews, iot-analytics, July 10, 2019. https://iot-analytics.com/the- 25-best-iot-platforms- 2019/
13. Maple,C., 2017, Security and privacy in the internet of things, JOURNAL OF CYBER POLICY, 2017 VOL. 2, NO. 2, 155– 184.
14. OSINT, 2019, New Kids On The Block (Part I), 16 June 2019 https://www.secjuice.com/new-kids-on-the-block/

隱私資訊管理系統標準ISO27701於GDPR適用性評估

魏銷志Yu-Chih Wei
國立臺北科技大學資訊與財金管理系助理教授
vickrey@mail.ntut.edu.tw

洪韻茹Yun-Ru Hung
國立臺北科技大學資訊與財金管理系專任助理
ollie@mail.ntut.edu.tw

陳昇智Simon Chen
環奧國際驗證公司技術經理
simon@mail.tcicgroup.com

祝亞琪Ya-Chi Chu
中華電信研究院資通安全研究所
gyh2211@cht.com.tw

摘 要

歐洲隱私權法規 - 一般資料保護規定 (EU General Data Protection Regulation, 簡稱 GDPR) 於 2016 年正式發布並以於 2018 年 5 月 25 日生效，ISO 標準組織為因應 GDPR 合規及加強隱私保護完整性，在內容上以隱私保護為核心並進行全面性的規範，以確保組織內隱私保護、資料的安全性、完整性及可用性，並且有效進行管控，著手起草 ISO/IEC 27552，後以 ISO/IEC 27701: 2019 進行發布。為瞭解 ISO/IEC 27701: 2019 以及 ISO/IEC 275522nd CD 內容差異進行比對，對照 GDPR 於 ISO/IEC 27701: 2019 以及 ISO/IEC 275522nd CD 中，所列項目完整度是否無對應上的缺漏。 也同時比較 ISO/IEC 27001: 2013、ISO/IEC 27002: 2013、ISO/IEC 29100: 2011、ISO/IEC 29151: 2017 與 ISO/IEC 27018: 2019 完整度及對應上項目差異。

關鍵詞：隱私保護、資訊安全、ISO、PII、GDPR

Abstract

The EU General Data Protection Regulation (GDPR) was officially released in 2016, and took effect on May 25, 2018. The International Organization for Standardization (ISO) considered improving privacy protection a core subject in the new GDPR compliance. To ensure adequate privacy protection, data security, integrity, availability and effective management and control within an organization (the "Items"), ISO began the drafting of ISO/IEC 27552, and then ISO/IEC 27701: 2019 was released. In order to understand the differences between ISO/IEC 27701: 2019 and ISO/IEC 27552 2nd CD, we further compared the incorporation of GDPR provisions in ISO/IEC 27701: 2019 and ISO/IEC 27552 2nd CD to find out whether the protection provided by these two ISOs for the Items was adequate. In this paper, we also discuss and compare ISO/IEC 27701: 2019 with other standards, such as ISO/IEC 27001: 2013, ISO/IEC 27002: 2013, ISO/IEC 29100: 2011, ISO/IEC 29151: 2017 and ISO/IEC 27018: 2019, to find the differences in their protection of the Items.

Keywords: Privacy protection, Information security, ISO, PII, GDPR

壹、緒論

歐洲隱私權法規 - 一般資料保護規定 (EU General Data Protection Regulation, 簡稱 GDPR) 於 2018 年 5 月 25 日生效，只要核心業務直接或間接與歐洲民眾個資的蒐集、處理和利用有關，不論擁有的歐洲民眾個資多寡、組織規模大小，皆須從控制制度到內部系統進行調整與修正，使之合規於 GDPR 對於個資保護的規範與要求。為提供組織在隱私資訊管理系統上，有國際一致的管理系統驗證機制，ISO 標準組織為了再強化 ISO/IEC 27001 標準與 GDPR 合規及加強隱私保護的完整性，著手起草 ISO/IEC 27552。

基於各類型管理系統要求大都以 ISO XXX 01 命名，例如 :ISO 9001, ISO 27001 等等，ISO/IEC 27552 於正式公告前更名為 ISO/IEC 27701(27701 2019)，本研究以 ISO 27552 標準草案合規 GDPR 之研究 (洪韻茹、魏銪志、杜雨儒 2018) 為基底，對照 ISO/IEC 275522 nd CD 與 ISO/IEC 27701 合規於 GDPR， 及 ISO/IEC 27001: 2013、ISO/IEC 27002: 2013、ISO/IEC 29100: 2011、ISO/IEC 29151: 2017 與 ISO/IEC 27018: 2019 對照 ISO/IEC 275522nd CD 與 ISO/IEC 27701 之情形與差異。

對於歐盟所發布 GDPR 所適用的單位而言，ISO/IEC 27701: 2019 提供一個具體的管理系統框架，可以有效建置、維運、驗證、稽核及持續改善個資管理系統，進行個資法遵循提供對應表，以盡防護工作避免個資當事人的個人資料遭到不法的蒐集、處理及利用。為確認 GDPR 及 ISO/IEC 27701: 2019 兩者的差異、缺漏事項，以及

與 ISO/IEC 275522nd CD 標準中的條款進行對應，確保項目均被列入 ISO/IEC 27701: 2019，避免以 ISO/IEC 27701: 2019 進行建置個資管理系統的單位，無法有效的合規於歐盟所發布 GDPR 而被裁以高額罰款。

貳、文獻探討

ISO/IEC 27701: 2019 為針對歐盟所發布的 GDPR 進行合規所發展出的一套標準，為了更好的進行標準整合及提供更完善的實施，除了 ISO/IEC 27701: 2019 本身的標準之外，包含相關標準指引比較與分析 ISO/IEC 27001: 2013、ISO/IEC 27002: 2013 外，亦整合了 ISO/IEC 27018: 2019 公用雲個資處理者控制措施、ISO/IEC 29151: 2017 個資控制者控制措施、ISO 29100: 2011 隱私框架，提供參照及實施指引 (黃明達、梁日誠 2019)。

一、ISO/IEC 27001: 2013 資訊技術－安全技術－資訊安全管理系統－要求事項

ISO/IEC 27001: 2013 為國際通用資訊安全管理制度，提供在任何組織環境中建立、實作、維護與持續改進資訊安全管理系統 (Information Security Management System, ISMS) 的要求事項而建構，組成包括組織之資訊安全政策、資訊安全之組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、運作安全、通訊安全、系統獲取開發及維護、供應者關係、資訊安全事故管理、營運持續管理之資訊安全層面、遵循性等 14 個領域，35 項控制目標，114 項控制措施。

並藉由運用風險管理過程，保持資訊機密性、完整性及可用性，防止資訊遭竊取、濫用、遺失或各種災害將影響降至最低，且適用於各型式的組織，無論組織類型、規模或性質均適用此標準 (27001 2013)。

二、ISO/IEC 27018: 2019 公用雲個人可識別資訊 (Personally Identifiable Information, PII) 處理者保護 PII 之作業規範

ISO/IEC 27018: 2019 為 ISO/IEC 27001 資訊安全管理系統的延伸標準，此標準為第一個針對雲端服務供應商在公有雲上個人資料保護的國際標準，主要由兩部分組成，第一部份為擴充 ISO/IEC 27002: 2013 的 16 個控制措施的實作指引，第二部份依據 ISO/IEC 29100: 2011 的隱私框架原則的 11 項新增 25 項具體的控制措施，對個人資料保護通訊方面提供治理框架，並適用於所有類型的組織，確保個人資料在雲端上獲得適當保護。

根據客戶 PII 的雲服務，供應商須以滿足保護雙方 PII 的法律和法規要求的方式提供其服務。客戶同意下針對資料生命週期，各階段採用適當的防護措施，確保個人資料得到更適當的保護，使得客戶對於雲端服務更加信任。並且幫助提供商提供高層次的個資保護措施、降低事件的發生率、有效的管理資安風險並強化競爭力以保護組織的名譽。然而在 PII 控制者的角色與職責在 ISO/IEC 27018: 2019 標準中並未有明確的控制措施。2019 年版本主要針對舊版標準附錄 A 中的文字疏漏進行修訂 (27018 2019)。

三、ISO/IEC 29100: 2011 資訊技術－安全技術－隱私權框架

ISO/IEC 29100: 2011 提供資訊及通訊技術系統 (Information and Communication Technology, ICT) 保護人可識別資訊 (PII) 之框架，包含隱私保護要求技術及隱私防護原則，有隱私防護框架，為識別相關於個人資訊之作業互動、角色、隱私保護控制、隱私保戶需求與政策，並定義與 PII 相關的隱私保護事項，協助處理和保護 PII 的 ICT 系統的設計，實施、運行、維護和推動創新解決方案，組織收集或處理 PII 將越來越需要保護 PII 的指引，以降低發生隱私洩露的風險，利用組織、技術和流程建置於整體隱私保護框架，以保護 ICT 系統內的 PII，通過使用實踐改進組織的隱私規劃 (29100 2011)。

四、ISO/IEC 29151: 2017 資訊技術－安全技術－個人可識別資訊保護之作業規範

ISO/IEC 29151: 2017 建立控制及實施控制指引，由 ISO/IEC 27002: 2013 提供指引，考量在組織的資訊安全風險環境中可能適用的處理 PII 的要求，並處理 PII 監管要求，包括控制的選擇，實施和管理，同時考慮到組織的資訊安全風險環境，且適用於 PII 控制者的所有規模與類型的組織當中 (29151 2017)。

ISO/IEC 發展出 ISO/IEC 29100: 2011 隱私保護框架後，逐漸發展出多種標準，諸如 ISO/IEC 27002: 2013(27002 2013) 控制措施之作業規範、ISO/IEC 29151: 2017 個人可識別資訊保護實務、ISO/IEC 27018: 2019 雲端系統的資料保護和 ISO/IEC 27701 資訊安全控制措施以保護個資，而 ISO/IEC 27701 為因應 GDPR(General Data Protection Regulation)(2016/ 679 2016) 而生。

依照 GDPR 訂定之 99 條條款對照至 ISO/IEC 27701 之範圍、規範性引用文件、定義、架構、ISO/IEC 27001: 2013 與個人資料管理系統 (Personal Information Management System, PIMS) 相關要求、ISO/IEC 27001: 2013 與 PIMS 具體指導相關、針對 PII 控制者的附加 ISO/IEC 27002: 2013 指引、附加的 ISO/IEC 27002: 2013 指引中，並擴充於標準 ISO/IEC 27001: 2013 與 ISO/IEC 27002: 2013 相關標準，且涵蓋 ISO/IEC 27018: 2019 與 ISO/IEC 29151: 2017 標準。

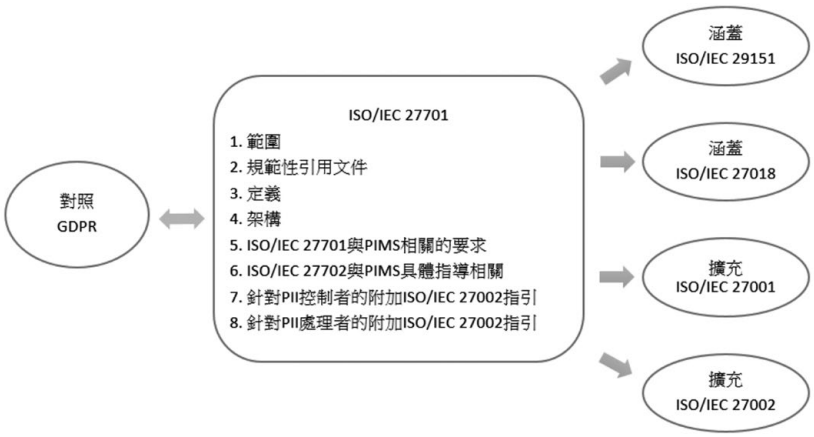


圖 1ISO/IEC 27701 架構圖

叁、ISO/IEC 27701相關指引比較與分析

ISO/IEC 27701: 2019 於標準附錄中，補充 PII 控制者及 PII 處理者可對應參考之控制目標及措施，並對應 ISO/IEC 27001: 2013、ISO/IEC 27002: 2013、ISO/IEC 29100: 2011、ISO/IEC 29151: 2017 與 ISO/IEC 27018: 2019 對照 ISO/IEC 275522nd CD 與 ISO/IEC 27701 之間差異，盡量以客觀的角度進行標準間的分析、描述及比較，並確認合規於 GDPR 之項目是否吻合。

一、ISO/IEC 27001 新增個人識別資訊控制措施

ISO/IEC 27001: 2013 中，將個人識別資訊 (PII) 分為 PII 控制者與 PII 處理者，依據收集和處理的條件、對 PII 當事人的義務、隱私設計與預設及 PII 分享、傳輸與揭露等四個控制目標進行擴增。附錄 A 為 PII 控制者所新增的控制措施，附錄 B 為 PII 處理者所新增的控制措施，兩附錄共計新增 49 項控制措施 (如下表 1 所示)。ISO/IEC 275522nd CDPII 控制者共計 32 項，而 ISO/IEC 27701: 2019 PII 控制者共計 31 項，ISO/IEC 27701: 2013 相較 ISO/IEC 275522nd CD 對於 PII 控制者少一項新增指引。

表 1ISO/IEC 27701 的個人識別資訊新增控制措施

控制目標	PII 控制者			PII 處理者		
	附錄 A	ISO/IEC 27552 控制措施	ISO/IEC 27701 控制措施	附錄 B	ISO/IEC 27552 控制措施	ISO/IEC 27701 控制措施
收集和處理的條件	A. 7. 2	8	8	B. 8. 2	6	6
對 PII 當事人的義務	A. 7. 3	10	10	B. 8. 3	1	1
隱私設計與預設	A. 7. 4	10	9	B. 8. 4	3	3
PII 分享、傳輸與揭露	A. 7. 5	4	4	B. 8. 5	8	8
總計	-	32	31	-	18	18

ISO/IEC 27701 PII 控制者新增控制措施皆與 ISO/IEC 275522nd CD 相同，其中 A. 7. 4. 4 PII 最小化與去識別化的目標及 A. 7. 4. 5 PII 最小化及去識別化，於 ISO/IEC 27701 合併為一項 A. 7. 4. 4PII 最小化目標，A. 7. 4. 5 之後項目往前遞補，即 A. 7. 4 有項由 A. 7. 4. 1 至 A. 7. 4. 9 共 9 個項目。PII 處理者新增控制措施，在 ISO/IEC 27701 及 ISO/IEC 275522nd CD 皆相同，無新增或刪除項。

表 2ISO/IEC 27701 PII 控制者新增控制措施

控制目標	PII 控制者			
	附錄 A	控制措施	ISO/IEC 27552 數量	ISO/IEC 27701 數量
隱私設計與預設	A. 7. 4	A. 7. 4. 1 限制蒐集 A. 7. 4. 2 限制處理 A. 7. 4. 3 準確性和品質 A. 7. 4. 4 PII 最小化目標 A. 7. 4. 5 PII 在處理結束時去識別與刪除 A. 7. 4. 6 暫存檔案 A. 7. 4. 7 保存 A. 7. 4. 8 汰除 A. 7. 4. 9 PII 傳輸控制	10	9

PII 控制者及 PII 處理者各有多項控制目標及控制措施，部分控制措施於 PII 控制者及 PII 處理者中相同，包含 A. 7. 2. 8 B. 8. 2. 6 處理 PII 相關之紀錄、A. 7. 4. 6 B. 8. 4. 1 暫存檔案、A. 7. 4. 9 B. 8. 4. 3 PII 傳輸控制、A. 7. 5. 2 B. 8. 5. 2 可能傳輸 PII 的國家和國家組織、A. 7. 5. 4 B. 8. 5. 3 向第三方揭露 PII 的記錄，共 5 項控制措施相同。

表 3 ISO/IEC 27701 PII 控制者及 PII 處理者相同控制措施

	PII 控制者		PII 處理者		
控制目標	附錄 A	控制項	附錄 B	控制項	控制措施
收集和處理條件	A. 7. 2	A. 7. 2. 8	B. 8. 2	B. 8. 2. 6	處理 PII 相關之紀錄
隱私設計與預設	A. 7. 4	A. 7. 4. 6	B. 8. 4	B. 8. 4. 1	暫存檔案
		A. 7. 4. 9		B. 8. 4. 3	PII 傳輸控制
PII 分享、傳輸與揭露	A. 7. 5	A. 7. 5. 2	B. 8. 5	B. 8. 5. 2	可能傳輸 PII 的國家和國家組織
		A. 7. 5. 4		B. 8. 5. 3	向第三方揭露 PII 的記錄

二、對照 ISO/IEC 29100

於 ISO/IEC 27552 對照 ISO/IEC 29100 項目中 1. 同意權和選擇內 A. 7. 3. 2 確定並履行對 PII 當事人的義務、A. 7. 3. 3 提供 PII 當事人資訊，7. 公開、透明和通知中 A. 7. 3. 8 提供已處理的 PII 副本，及 8. 個人參與和存取中 A. 7. 3. 10 自動化決策，皆於 ISO/IEC 27701 中剔除新增相關控制項目。

此外，於 ISO/IEC 27701 新增原 ISO/IEC 27552 無編列之項目共七項，包含 2. 合法性和規範的目的中 A. 7. 3. 10 自動化決策，5. 使用、保存和揭露限制中 A. 7. 4. 6 暫存檔案、A. 7. 4. 7 保存、A. 7. 4. 8 汰除與 A. 7. 5. 1 識別 PII 國際傳輸的基礎，8. 個人參與和存取的 A. 7. 3. 8 提供已處理的 PII 副本與最後 9. 責任歸屬的 A. 7. 5. 1 識別 PII 國

際傳輸的基礎，皆是原 ISO/IEC 27552 中未編列，在此版 ISO/IEC 27701 中新增修改項。

ISO/IEC 27552 中新增 10 項 PII 控制者相關控制項，於 ISO/IEC 27701 中新增 11 項 PII 控制者相關控制項，其中包含原有的 A. 7. 4. 4 PII 最小化與去識別化的目標及 A. 7. 4. 5 PII 最小化及去識別化，合併為 A. 7. 4. 4 PII 最小化目標，及 A. 7. 4. 5 PII 在處理結束時去識別與刪除。

表 4PII 控制者相關控制措施差異

ISO/IEC 29100	ISO/IEC 27552 PII 控制者相關控制措施	ISO/IEC 27701 PII 控制者相關控制措施
1. 同意權和選擇	A. 7. 3. 2 確定並履行對 PII 當事人的義務 A. 7. 3. 3 提供 PII 當事人資訊	
2. 合法性和規範的目的		A. 7. 3. 10 自動化決策
5. 使用、保存和揭露限制		A. 7. 4. 6 暫存檔案 A. 7. 4. 7 保存 A. 7. 4. 8 汰除 A. 7. 5. 1 識別 PII 國際傳輸的基礎
7. 公開、透明和通知	A. 7. 3. 8 提供已處理的 PII 副本	
8. 個人參與和存取	A. 7. 3. 10 自動化決策	A. 7. 3. 8 提供已處理的 PII 副本
9. 責任歸屬		A. 7. 5. 1 識別 PII 國際傳輸的基礎

ISO/IEC 27701 包含原 ISO/IEC 27552 對照 ISO/IEC 29100 所有相關控制項目，並且新增 PII 處理者之控制項，包含 B. 8. 2. 1 合作協議、B. 8. 3. 1 對 PII 當事人的義務、B. 8. 3. 1 對 PII 當事人的義務及 B. 8. 4. 3 PII 傳輸控制共 4 項。

表 5ISO/IEC 27552 未包含之 ISO/IEC 29100 對照 ISO/IEC 27701 PII 處理者新增相關控制項

ISO/IEC 29100	ISO/IEC 27701 PII 處理者新增相關控制項
2. 合法性和規範的目的	B. 8. 2. 1 合作協議 B. 8. 3. 1 對 PII 當事人的義務
8. 個人參與和存取	B. 8. 3. 1 對 PII 當事人的義務
10. 資訊安全	B. 8. 4. 3 PII 傳輸控制

三、對照與 ISO/IEC 27701 及 GDPR 之差異

比照 ISO/IEC 27552 標準草案合規 GDPR 之研究 (洪韻茹、魏銷志、杜雨儒 2018) 於此篇論文中對照方式，比對結果為 ISO/IEC 27701 對 GDPR 涵蓋率為

48. 78%，並且發現於 ISO/IEC 27552 標準草案合規 GDPR 之研究論文中，ISO/IEC 27552 誤將 GDPR 中的 (12)(5)(a)、(12)(5)(b)(2016/ 679 2016)「考量所要求提供之資訊或溝通或採取行動之行政成本，收取適當費用；或拒絕該請求。控管者應就該請求之明顯無理由或過度性負舉證責任。」列為應包含但未包含之項目，更正為不應包含，並且在 ISO/IEC 27552 與 ISO/IEC 27701 對到 GDPR 中皆未列入。

(6)(2)(2016/ 679 2016)「會員國得維持或採用更具體之規範，使其與本規則所定本條第 1 項第 c 點及第 e 點之適用相符，為處理及用以確保處理合法性與公正性之其他措施，包括為第九章所規定之其他特定處理情形，訂定更具體化之特定規範。」在 ISO/IEC 27552 標準草案合規 GDPR 之研究中列為未包含並且不應包含，並在 ISO/IEC 27701 對照表中包含，因此此項應列為應包含但未包含項。

ISO/IEC 27552 應包含 (12)(4)、(12)(5)、(12)(6)、(36)(2)(2016/ 679 2016) 這四項但未包含，於 ISO/IEC 27701 將 ISO/IEC 27552 漏列之項目列進標準中，使標準更符合 GDPR 之規範。

(12)(4)(2016/ 679 2016)「如控管者不同意資料主體之要求者，該控管者應立即且最遲於收到資料主體要求之一個月內附具理由告知該資料主體，並敘明向監管機關提出申訴及尋求司法救濟之可能性。」、(12)(5)(2016/ 679 2016)「第 13 條及第 14 條所定應提供之資訊及第 5 條至第 22 條及第 34 條所定任何溝通及採取之任何行動，應無償提供之。如資料主體之請求明顯無理由或過度者，尤其是基於該等請求過於重複者，控管者 」、(12)(6)(2016/ 679 2016)「在不影響第 11 條規定之情況下，如控管者對於當事人依照第 15 條至第 21 條提出請求之資料主體身分有合理懷疑者，控管者得要求提供為確認該資料主體身分所必要之額外資訊。」、(36)(2)(2016/ 679 2016)「當監管機關認為第 1 項所稱之處理將違反本規則，尤其是當控管規則指令者未能完全指出或減低風險時，監管機關應於收受諮詢請求後 8 周內，提供書面意見予控管者並視情形予處理者，並得行使其於第 58 條所載之任何權力。該期間可因處理之複雜程度再延長 6 周。監管機關應於收受諮詢請求後 1 個月內通知控管者並視情形通知處理者上開延期情況及延期原因。該等期間得中止至監管機關取得提供諮詢所需之資訊。」

其餘 51. 22% 請參考 ISO/IEC 27552 標準草案合規 GDPR 之研究表 6 ISO/IEC 27552 未涵蓋 GDPR 之條款，ISO/IEC 27701 對照 GDPR 未完全涵蓋之條款，及章節未涵蓋數量列表，並扣除誤列之第二章原則 6 處理之合法性數量 1，未完全涵蓋數量為 60 項，未涵蓋的部份屬於 GDPR 適用範圍與定義或監管機關相關要求或罰則。

四、對照與 ISO/IEC 27018 及 ISO/IEC 29151

ISO/IEC 27552 中對照 ISO/IEC 27018 的項目中有 22 項無資料，ISO/IEC 29151 對照有 29 項無對照資料，ISO/IEC 27701 對照 ISO/IEC 27018 及 ISO/IEC 29151 對照，相較於 ISO/IEC 27552 對照完整。ISO/IEC 27552 缺漏多並且受限於篇幅不在此進行比較，僅針對 ISO/IEC 27701 對照 ISO/IEC 27018 及 ISO/IEC 29151 項目進行說明。

ISO/IEC 27018 對應 ISO/IEC 27701 27 項，並列出 35 項以對應 ISO/IEC 27701，其中 6. 6. 2 用戶存取管理就對應了 A. 9. 2. 1 用戶申請和取消、A. 11. 8 唯一的用戶識別、A. 11. 9 用戶授權的紀錄及 A. 11. 10 用戶 ID 管理四個項目。

ISO/IEC 29151 對應 ISO/IEC 27701 35 項，並列出 35 項以對應 ISO/IEC 27701，其中 A. 13. 2 在某些司法管轄區的跨境資料傳輸限制項，同時對應到 7. 5. 1 PII 傳遞識別、7. 5. 2 國家和國際組織的 PII 可以轉讓及 7. 5. 3 技術轉讓給 PII，對應 3 個項目。

表 6 ISO/IEC 27701 對照 ISO/IEC 27018 及 ISO/IEC 29151

ISO/IEC 27701	ISO/IEC 27018	ISO/IEC 29151
5. 4 規劃	N/A	4. 2 要求對 PII 的保護
5. 5 支援	N/A	7. 2. 3 認識資訊安全、教育和培訓
6. 2 資訊安全政策	5. 1. 1 資訊安全政策	5 資訊安全政策
6. 3 資訊安全組織	6. 1. 1 資安全角色和職責	N/A
6. 4 人力資源安全	7. 2. 2 信息安全意識，教育和培訓	N/A
6. 5. 1 資產責任	N/A	8. 1 資產責任
6. 5. 2 資訊分類	N/A	8. 2 資訊分類
6. 5. 3 媒體掌控	A. 11. 4 保護資料裝置遺失 A. 11. 5 使用未加密的行動儲存裝置和設備	8. 3 媒體掌控
6. 6. 2 用戶存取管理	A. 9. 2. 1 用戶申請和取消 A. 11. 8 唯一的用戶識別 A. 11. 9 用戶授權的紀錄 A. 11. 10 用戶 ID 管理	9. 2 用戶存取管理
6. 6. 3 用戶責任	N/A	9. 3 用戶責任
6. 6. 4 系統和應用流程存取控制	N/A	9. 4 系統和應用流程存取控制
6. 8. 1 安全區域	N/A	11. 1 安全區域
6. 9. 1 操作流程和責任	N/A	12. 1 操作流程和責任
6. 9. 2 保護免受惡意軟體	N/A	12. 2 保護免受惡意軟體
6. 9. 3 備份	N/A	12. 3 備份
6. 9. 4 記錄和監控	12. 4. 1 事件日誌 12. 4. 2 日誌資訊的保護	12. 4 記錄和監控
6. 10. 1 網路安全性管理	N/A	13. 1 網路安全性管理

6. 10. 2 資訊傳輸	13. 2. 1 資訊傳遞的政策和程序 A. 11. 10 用戶 ID 管理	13. 2 資訊傳輸
6. 11. 1 資訊系統的安全性需求	A. 11. 6 PII 的加密過的公開的數據傳輸網絡傳送	N/A
6. 11. 3 測試資料	12. 1. 4 開發、測試和運行環境的分離	N/A
6. 12. 1 資訊安全的供應商關係	A. 11. 11 合約措施	N/A
6. 13 資訊安全性事件管理	16. 1. 1 涉及 PII 數據洩露通知 A. 10. 1 涉及 PII 資料洩露通知	N/A
6. 15. 1 遵守法律和合約要求	A. 10. 2 保留期限管理的安全策略和指南	N/A
6. 15. 2 資訊安全審查	18. 2. 1 資訊安全的獨立審查	18. 2 資訊安全審查
7. 2. 1 目的合法性和規範	N/A	A. 4 目的合法性和規範
7. 2. 2 根據法律依據	N/A	A. 4. 1 目的合法性
7. 2. 4 獲取和記錄同意書	N/A	A. 3. 1 承諾
7. 2. 5 隱私影響評估	N/A	A. 11. 2 隱私影響評估
7. 2. 6 與 PII 處理器合約	N/A	A. 11. 3 承包商對 PII 處理器隱私要求
7. 3. 1 確定履行 PII 負責人義務	N/A	A. 10 PII 主要參與和使用
7. 3. 3 提供訊息 PII 負責人	N/A	A. 9 公開、透明和注意
7. 3. 6 存取、新增或刪除	N/A	A. 10. 1 PII 負責存取
7. 4. 1 限制收集	N/A	A. 5 限制收集
7. 4. 3 準確度和品質	N/A	A. 8 準確度和品質
7. 4. 5 PII 去標識和刪除處理	N/A	A. 7. 1 使用、保留和披露限制
7. 4. 6 臨時文件	N/A	A. 7. 2 安全刪除臨時的文件
7. 4. 7 保留	N/A	A. 7. 1 使用、保留和披露限制
7. 5. 1 PII 傳遞識別	N/A	A. 13. 2 在某些司法管轄區的跨境資料傳輸限制
7. 5. 2 國家和國際組織的 PII 可以轉讓	N/A	A. 13. 2 在某些司法管轄區的跨境資料傳輸限制
7. 5. 3 技術轉讓給 PII	N/A	A. 13. 2 在某些司法管轄區的跨境資料傳輸限制
7. 5. 4 PII 透露給第三方的記錄	N/A	A. 7. 4 PII 披露的記錄

8. 2. 2 組織目標	A. 3. 1 公共雲 PII 處理者的目的	N/A
8. 2. 3 市場行銷和廣告使用	A. 3. 2 商用的公共雲 PII 處理者	N/A
8. 3. 1 PII 負責人合約	A. 2. 1 PII 負責人有義務及權利共同工作	N/A
8. 4. 1 暫存檔案	A. 5. 1 安全刪除臨時文件	N/A
8. 4. 2 退貨、轉讓或出售 PII	A. 10. 3 PII 回報、轉讓和處置	N/A
8. 4. 3 輸控制	A. 12. 2 PII 的預定目的	N/A
8. 5. 2 國家和國際組織的 PII 可以轉讓	A. 12. 1 PII 的地理位置	N/A
8. 5. 3 向第三方揭露 PII 的紀錄	A. 6. 2 記錄您的 PII 揭露	N/A
8. 5. 4 通知要求 PII 揭露	A. 6. 1 PII 揭露通知	N/A
8. 5. 5 揭露具有法律 束力 PII	A. 6. 1 PII 揭露通知	N/A
8. 5. 6 公布承包商處理 PII	A. 8. 1 承包 PII 揭露處理	A. 7. 5 承包 PII 處理的公開內容
8. 5. 7 承包商參與處理 PII	A. 8. 1 承包 PII 揭露處理	N/A
8. 5. 8 變更承包商處理的 PII	A. 8. 1 承包 PII 揭露處理	N/A

肆、結論

根據 ISO/IEC 27701 進行探討，對照及比較 ISO/IEC 27001: 2013 資訊安全管理系統為底，ISO/IEC 27002: 2013 資訊安全管理實作指引作為延伸補強原先的不足，涵蓋 ISO/IEC 29100: 2011、ISO/IEC 29151: 2017 及 ISO/IEC 27018: 2019 使其標準結構更完整。並確認 GDPR 及 ISO/IEC 27701: 2019 兩者的差異、缺漏事項，以及與 ISO/IEC 275522nd CD 標準中的條款進行對應，確保項目均被列入，避免無法有效的合規於歐盟所發布 GDPR 而被裁以高額罰款。

以及對照 ISO/IEC 27552 與 GDPR 兩者標準之條款差異，計算出對 GDPR 涵蓋率為 48. 78%。扣除 GDPR 訂定的適用範圍與定義或監管機關相關要求或罰則相關條款及細項，ISO/IEC 27701 涵蓋其他所有規定及細項。其餘未涵蓋的部份屬於 GDPR 訂定的適用範圍與定義或監管機關相關要求或罰則相關條款及細項，扣除這些項目得到涵蓋率為 100%，本研究的分析顯示 ISO/IEC 27701 在規定及細項中包含了 GDPR 所有項目。

未來將研究符合 ISO/IEC 27701 及 ISO/IEC 27701 的 ISMS 與 PIMS 的系統管理平台，以有效執行 ISMS 及 PIMS 所需要的 PDCA 管理循環，除此之外，亦將研究符合 ISO/IEC 27005 及 ISO/IEC 29134 的資訊安全與個人資料方法論，並進一步研發評鑑系統，以有效降低執行資訊安全與個人資料風險評鑑與管理的難度。

參考文獻

1. 2016/ 679, E. 2016. "General Data Protection Regulation." from https://gdpr-info.eu
2. 27001, I. I. 2013. "Information Technology-Security Techniques-Information Security Management Systems-Requirements." pp. 1- 23.
3. 27002, I. I. 2013. "Information Technology-Security Techniques-Code of Practice for Information Security Controls." pp. 1- 80.
4. 27018, I. I. 2019. "Information Technology-Security Techniques-Code of Practice for Protection of Personally Identifiable Information (Pii) in Public Clouds Acting as Pii Processors." pp. 1- 23.
5. 27701, I. I. 2019. "Security Techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management-Requirements and Guidelines." pp. 1- 66.
6. 29100, I. I. 2011."Information Technology-Security Techniques-Privacy Framework-Amendment 1: Clarifications." pp. 1- 4.
7. 29151, I. I. 2017. "Information Technology-Security Techniques-Code of Practice for Personally Identifiable Information Protection." pp. 1- 39.
8. 洪韻茹、魏銪志、杜雨儒 . 2018. "ISO 27552 標準草案合規 GDPR 之研究 ." Cyberspace 2018, pp. 1- 12.
9. 黃明達、梁日誠 . 2019. " 整合資安與個資管理系統的國際標準 -ISO/IEC 27701 簡介與應用 ," 國土及公共治理季刊 (7: 4), pp. 92- 101.

A Win-Win Collaboration between Universities and Industry on Audit Data Analytics

王大維Tawei (David) Wang
DePaul University
david.wang@depaul.edu

Abstract

The author has arranged seven joint internal audit data analytics projects with Chicagoland companies in the past four years. These 8 to 10 week long projects have exposed students to business practices and have helped companies leverage the talents in universities by exploring different data analytics possibilities. The author shares several project arrangement insights and encourages more win-win collaborations between universities and industry on audit data analytics projects.

Keywords: Audit data analytics, Collaboration between universities and industry,Curriculum innovation

中文摘要

筆者於過去四年間，安排了多次與芝加哥企業界合作的審計數據分析 (Audit data analytics) 專案，透過這些專案經驗在此探討產學合作所帶來的益處。這些產學專案長達八至十週，而在這樣長期密切互動與交流下，不僅能使學生獲取企業運用審計數據分析的實務經驗，更能幫助企業探索不同的審計數據分析應用層面。為鼓勵更多學校能與企業界進行產學合作，筆者於本文也進一步討論產學合作的可能步驟與流程，期望能幫助產學雙方達到雙贏局面。

關鍵字 : 審計數據分析、產學合作、課程創新

1. INTRODUCTION

With the belief that universities and professionals can work closely to bring business practices to the classroom and to bring new thoughts and ideas back to the companies, I have arranged seven joint projects with companies in audit data analytics in the past four years based on two analytics related courses at DePaul University. These 8 to 10 week long projects are featured with intensive interactions between the sponsoring companies and student teams.Through the interactions, on one hand, the projects help companies explore different audit data analytics initiatives and possibilities, such as automation and predictions, and execute planned analytics procedures with student groups. These projects allow companies to leverage the talent in universities to implement different analytics projects and to explore possible benefits without sacrificing internal resources. Companies also have a chance to work closely with students. By interacting with students, companies may bring potential job candidate to the company. On the other hand, student groups are able to learn by doing a real project, which provides a great environment that cannot be replicated in a classroom setting and is featured with all the key factors when learning analytics. It is also important for the student team to have the networking opportunity with businesses for their future careers.

In this article, I would like to share several planning and coordination strategies when arranging these projects. Possible ways to reduce the concerns of using confidential data and operational information are also presented. I hope that this article will encourage more win-win collaborations between universities and companies or audit firms on audit data analytics and potentially improve audit practices and accounting data analytics curriculum.

2. WHY COLLABORATE?

Using data analytics in auditing has drawn a lot of attention in recent years. Audit firms have highlighted how they have leveraged data analytics in audit engagements in order to improve audit quality (Deloitte n.d.; KPMG 2015; Cohn 2015; EY Reporting 2015). Companies' internal audit teams have also attempted to use analytics to make the audit more efficient and more effective (Protiviti 2015; Aristiguieta 2020). Though there seem to be benefits coming along with the incorporation of data analytics in audit (e.g., Tysiac 2020), many challenges remain (e.g., Aristiguieta 2020). For example, talents with technical training and business as well as accounting skills are not common in the job market. Where to start and how to start with analytics as well as different possibilities that can be brought by analytics may not be clear either not to mention the justification of the value of all the additional investments in all aspects around data analytics.

Accounting programs are facing similar

challenges (Wang 2017). With the increasing need of having basic analytics skills and the accreditation requirements, accounting programs have attempted to bring new curriculum that aims to help students be equipped with the critical thinking skills and data analysis capability that can tie closely to business operations. However, designing the curriculum and meeting the expected learning objectives are not straightforward since it is much more than teaching a specific software. In addition to the design of the learning outcomes and the corresponding in-class and take-home activities, learning activities also have to reflect or mimic a more real analytics project. First, audit data analytics projects are often ambiguous and uncertain, which are very different from what accounting major students used to work with. Specifically, traditional accounting courses often have one best solution and the questions asked are very specific. For analytics projects, the questions can be open-ended and require students to narrow down the scope, identify information needed and may have to change the scope as the project moves on. In addition, data analytics projects focus on the connections between business operations or business issues and the analyses as well as the interpretations. Without a good understanding of the underlying business operations, the analyses and the interpretations may not provide additional value. However, the connection between the analysis and the underlying business operations are not commonly emphasized in the accounting curriculum due to the time limit of accounting courses and the goal of preparing students for the CPA exam. Third, the data itself is often noisy without perfect documentations. Learn how to live with all the noisy datasets and still perform the analysis can be challenging for accounting students. Last, translating analytics techniques or terminology to business languages then make actionable recommendations can also be challenging. That is, how to appropriately communicate the analyses and findings effectively to the executive team and to provide suggestions require practices in order to make the findings relevant and to provide values.

With these challenges in mind, these audit data analytics projects were arranged in the past four years with the support from DePaul University and the sponsoring companies.[1] School of Accountancy and MIS at DePaul University currently has three different masters programs: Master of Science in Taxation (MST), Master of Science in Accountancy (MSA) and Master of Science in Audit and Advisory Services (MSAA). The accounting or auditing data analytics courses are included in the MSAA program. The MSAA program is aimed for students with accounting undergraduate degrees and has the objective of training students with higher level skills, such as judgement, communication, etc.

1.Due to confidentiality issues, I am not able to discuss projects or sponsoring companies in details in the article.

That is, given students' accounting background, the program can help students further develop their capabilities. The program has nine required courses including one internal audit, three fraud and forensic accounting courses, four IT related courses (including two data analytics courses) and one statistics. Currently, the program has about 100 to 125 students every year. Students can be experienced professionals or recent graduates from colleges.

The projects are based on these two data analytics courses, which are designed based on the maturity level of data analytics. The first course "audit data analytics" emphasizes on descriptive analytics and diagnostic analytics in the context of auditing (mainly internal audit), which shows the patterns that have already happened in the past and/or is happening and links the findings to business operations in order to make interpretations and actionable recommendations. The second course "data analytics and data mining" emphasizes on predictive analytics and prescriptive analytics also in the context of audit, which focuses on predictive modeling and how we can achieve the predicted target. These two courses cover a wide variety of scenarios, such as assertion testing, forensic/fraud detection, risk assessment, compliance issues, operational audit, etc. Though both courses emphasize on different analytics skillsets, the main goal is still about critical thinking skills and interpretations of findingsas well as providing actionable recommendations. Specifically, building on students' solid training in accounting and business, the additional data analytics skills can help students broaden their career opportunities and further develop their capabilities. More importantly, these students are more likely to be able to communicate with the information technology service group or data analysts in the future.

3.PROJECT ARRANGEMENTS

3. 1. Initial Discussion of the Project, Data and Timeline

The initial discussion generally centers around the possibility of the collaboration and potential topics that may fit with both parties' timeline and objectives. For example, the university' s program may run in a 10-week, 12-week or a 16-week time frame while the sponsoring company may have an audit plan for a specific objective from March to May. In this case, the timeline may fit for both parties. Ideally, we attempt to arrange the project one semester ahead of time.

There are several different possible projects that can be discussed. The student team may (1) perform an existingaudit data analytics procedure for the sponsoring company (e.g., test vendor management, fraud detection, risk assessment, compliance, etc.) or shadow an engagement, (2) design an analytics procedure (e.g., list the steps required, provide the algorithm or the program and proof of concept), (3) explore some possible analytics such as more advanced predictive analytics (e.g., deep learning) or the involvement of

different external datasets, or (4) perform other analytics related tasks based on the arrangement.

After the initial discussion, the sponsoring company and the instructor will work separately to move the project forward. The sponsoring company may have to discuss internally. Such discussion may include the chief audit executive, director of internal audit, the executive team, the legal/risk department and the human resources, for instance. The company may also want to assign a manager or senior manager to be in charge of the project. Meanwhile, the instructor can seek additional support from the department if needed and to form student teams of 3 to 5 depending on the number of students the sponsoring company is willing to take. One or two teams are more feasible for this kind of projects. It also depends on the student team's availability during the project period as the project may take 80 to 100 hours for the whole team in an 8- to 10-week period. The instructor can collect students' resume for the sponsoring company to form the team or pre-filter for the company. Note that if students have full-time or part-time jobs, potential conflict of interests should be avoided.

In this step, there may be a back-and-forth process between the sponsoring company and the instructor to narrow down the scope of the project and to secure the datasets. Note that it is perfectly fine to have a not-well-defined project. The ambiguity and uncertainty are normal and are part of the learning processes.

The confidentiality of the data and the operational procedures are always the priorities for the project. The data can be reduced to include only those fields needed for the project. The data can always be anonymized and the analyses are still meaningful. In the extreme case, the sponsoring company can set up a terminal for the student team so the access and the use of data can be constrained. The sponsoring company can also create dummy data for the student team to perform a proof of concept. Based on the proof of concept, the company can replicate the procedures and analyses with the complete dataset. The confidentiality of the data and operational information should be emphasized with the student group so more attention will be given when handling the information.

Once we have a draft for the project and have secured the data, several documents or training may be arranged before the project can be initiated. A non-disclosure agreement is always required, which may be signed by the student team, the instructor, the college or the university. For data accessing, security and privacy training may be required as well. A kick-off meeting can be scheduled as the next step.

3. 2. Kick-Off Meeting

The kick-off meeting brings the student team and the sponsoring company together for the first time. It's a good time to introduce the company, people that will be involved in the project, the operational processes related

to the project and the corresponding policies and regulations if any. The company may also explain or demonstrate the datasets with access instructions during the meeting. The company and the student team can set up a contact window for further communications. Note that the instructor should be involved in all communications but only as a quiet participant. The student team leader is the person who coordinates with the team and the company as coordination and project management are also part of the learning objectives. The instructor may choose to review all materials before anything goes out to the sponsoring company in order to ensure everything goes smoothly.

3. 3. Check Points and Mid-Project Review

There are two sets of check points: one for the sponsoring company and the other for the instructor and the student team. For the sponsoring company's check points, it can be a regular weekly meeting or a more touch-based meeting. However, it is expected that there may be more questions and meetings at the beginning of the project as the student team is trying to understand business operations, the datasets and the connection between the two.

On the instructor and the student team side, it should be more structured with three pre-defined deliverables. An initial audit planning can help the student team set the direction and to ensure the student team has an initial plan laid out. Though the purpose is for the student team to drive the project by themselves as much as possible, the instructor can meet regularly with the student team to answer questions and to ensure everything is still on track. The student team should also submit a mid-project review. This mid-project review document can be shared with the sponsoring company and an oral presentationis encouragedto ensure the project is going in the correct direction and to solve any foreseeable issues. The last check point is the final presentation and deliverables, which will be discussed in the next sub-section.

3. 4. Final Presentation and Deliverables

Due to the confidential nature of the project, it is suggested to have the final presentation in the sponsoring company's office. Such arrangement can also increase the interactions between the student team and the sponsoring company's employees. In addition to the final presentation, several deliverables may be required depending on the types of the projects. A report that includes an executive summary and major findings is always preferred. Some other deliverables may involve additional data files, computer programs, algorithms, and visualizations, for example. These files allow the sponsoring company to replicate the findings or to customize the program for future tests.

4. CONCLUSIONS

With the increasing need in using data

analytics skills in audit in recent years, it brings a great opportunity for companies and universities to work together to initiate and explore different possibilities in audit data analytics. The collaboration has been shown to benefit both the sponsoring companies and the students involved. This article outlines the steps when arranging these projects and encourages companies and instructors to reach out for possible collaboration opportunities that can move the field forward.

REFERENCES

1. Aristiguieta, F. 2020. "The analytics journey: Finding the right direction," retrieved on June 29, 2020 from https://iaonline.theiia.org/ 2020/Pages/The-Analytics-Journey-Finding-the-Right-Direction.aspx
2. Cohn, M. 2015. "PwC transforms audit practice with data analytics," retrieved on June 29, 2020 from https://www.accountingtoday.com/opinion/pwc-transforms-audit-practice-with-data-analytics
3. Deloitte. n.d. "Audit analytics – Getting it right," retrieved on June 29, 2020 from https://www 2.deloitte.com/ch/en/pages/audit/articles/audit-analytics-getting-it-right.html
4. EY Reporting. 2015. "How big data and analytics are transforming the audit," retrieved on June 29, 2020 from https://www.ey.com/en_us/assurance/how-big-data-and-analytics-are-transforming-the-audit
5. KPMG. 2015. "Audit data &analytics: Unlocking the value of audit," retrieved on June 29, 2020 fromhttps://home.kpmg/xx/en/home/insights/ 2015/ 02/audit-data-analytics-unlocking-value-of-audit.html
6. Tysiac, K. 2020. "How firms are delivering value with audit data analytics," Journal of Accountancy, retrieved on June 29, 2020 from https://www.journalofaccountancy.com/news/ 2020/jan/cpa-firm-value-audit-data-analytics- 22751.html
7. Protiviti. 2015. "Changing trends in internal audit and advanced analytics," retrieved on June 29, 2020 from https://www.protiviti.com/sites/default/files/united_states/internal-audit- data-analytics-whitepaper-protiviti.pdf
8. Wang, T. 2017. "The development of audit analytics curriculum at DePaul University: Challenges and opportunities," 2017 International Conference on Computer Auditing, London,UK.

The Impact of Artificial Intelligence on the Audit

人工智慧對於審計實務之影響

Miklos A. Vasarhelyi
KPMG Distinguished Professor of Accounting Information Systems
Director of Rutgers Accounting Research Center
Director of Continuous Auditing & Reporting Lab (CAR Lab)
Rutgers Business School
Rutgers, the State University of New Jersey
miklosv@business.rutgers.edu

Sheng-Feng Hsieh
Ph.D. Candidate in Accounting Information Systems
Rutgers Business School
Rutgers, the State University of New Jersey
shengfeng.hsieh@rutgers.edu

Acknowledgment: We highly appreciate the invitation from the guest editor, Dr. Tawei (David) Wang, of the journal to write this commentary article.

Abstract

Artificial intelligence (AI) and other emerging technologies are evolving and impacting audit practice. This paper briefly discusses the impact of AI in terms of the viewpoint from the regulatory bodies, the current academic research status, the current practical AI applicationsin accounting firms, the ethical issues of AI implementation, the evolving CPA certification,and the reform of accounting education. Auditors in the digital era are to have a different mindset and skills that include AI and other emerging technologies.

JEL Classification: M 42
Keywords: Artificial Intelligence (AI), Audit

中文摘要

人工智慧與新興科技正在改變審計實務之運行。本文將簡短由審計準則制定機關之觀點、相關學術研究、現行會計師事務所之人工智慧應用、人工智慧運用之倫理議題、以及變革中的會計師認證制度與會計教育等不同層面來探討人工智慧對於未來審計實務之影響，也提倡身處數位時代的審計從業人員應該具備人工智慧以及新興科技的能力。

關鍵字：人工智慧、審計

1.INTRODUCTION

A wide range of technologies has been emerging that are loosely called Artificial Intelligence (AI). Among these Machine Learning, Expert Systems (Vasarhelyi 1988; Vasarhelyiand O' Leary 1989), Computer Vision, Voice Recognition, Cognitive Computing, Neural Networks, and others have emerged in applications in many industries, and are slowly being adopted in the accounting and auditing domain. Expert Systems, also called rule-based systems, got much attention by large firms in the late nineties but was progressively abandoned by the beginning of this century. Now with computational and storage capabilities enhanced by dimensional factors, it can be associated with new AI techniques like image recognition and become potentially viable. This area of research and application has not yet been adequately explored but presents great potential as it can incorporate rules of audit judgment into automated processes now with much better technologies.

Essential to an intelligent environment is available data streams that can be integrated into a usable data source for more intelligent applications. This data ecosystem (Cho, Vasarhelyi, and Zhang 2019) requires considerable preparation and manipulation as the sources are not designed to work together. Auditing will progressively use a large number of exogenous variables (Brown-Liburd and Vasarhelyi 2017). This integration of heterogeneous data streams that may include social media, weather, Internet of Things (IoT), aerial photography, news pieces, and others linked to data from internal sources will be of great importance to the profession as well as for many other areas of endeavor. Many startups are now creating "linkage" algorithms and databases to provision for this integration.

Regulatory bodies are carefully

monitoring the development and implementation of AI in the audit practice. For example, the Public Company Accounting Oversight Board (PCAOB) established the Data and Technology Task Force to attain insights of data analytics and emerging technologies, including AI, from academia and practice. In the latest research update (PCAOB 2020), PCAOB shared observations on the current AI implementation in assessing and identifying risks of material misstatement and generating audit evidence. Similarly, the Technology Working Group of the International Auditing and Assurance Standards Board (IAASB) issued a document, emphasizing on how the audit documentation would be affected when auditors use automated tools and techniques during an audit engagement(IAASB 2020).Moreover, the Association of Chartered Certified Accountants (ACCA) held an event[1] on the impact of digital and artificial intelligence on audit and finance professionals. The conference discussed how auditing standards would evolve,how technologies would strengthen audit quality, and how to educate and train audit and finance professionals.

2.ACADEMIC RESEARCH ABOUT THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE AUDIT

Omoteso (2012) reviewed the research on the pros and cons of AI system implementation in the audit industry and depicted the future direction of application development and research. Issa, Sun, and Vasarhelyi (2016) raised 24 different research ideas related to the AI implementation in auditing and discussed whether AI would become a workforce replacement or supplementation to encourage scholars to research on the practical AI-driven auditing transformation.Kokina and Davenport (2017) explained how AI capabilities and applicationstransform audit practice and interaction with human auditors. Potential biases, either data-driven bias or human-machine interaction bias, should be further studied (Kokina and Davenport 2017).These papers all share a positive perspective on the AI implementation in audits.

In terms of AI application in audit research, Zhaokaiand Moffitt (2019) proposed a "Contract Analytics Framework (CAF)" to guide auditors when they utilize text analytics to analyze or extract information from a massive amount of contracts. The results also supported the feasibility of the framework and the technique to audit a full

1. The event report of "The impact of Digital and Artificial Intelligence on audit and finance professionals: harnessing the opportunities of disruptive technologies" is available at: https://www.accaglobal.com/gb/en/technical-activities/technical-resources-search/2018/december/impact-of-digital-and-ai-on-audit-.html

population of contracts.Appelbaum and Nehmer (2017a and 2017b) discussed how "dronnovation," including drones, mechanical robots, and robotic processes (bots),be adopted to the automation of accounting. Sun and Vasarhelyi (2017)focused on how to implement deep learning to generate supplementary audit evidence, support auditors' judgment,and enhance the efficiency and effectiveness of audit automation.

AI-based application and its usage by auditors, however, are not always perfect. Commerford, Dennis, Joe, and Ulla (2020) experimented with 170 subjects and investigated the impact of source of firm-provided evidence, either from the AI specialist system or from the human specialist, on the auditor judgment.They concluded that "the implementation of advanced specialist systems could alter auditor judgments in a way that inadvertently undermines audit quality."

3.CURRENT APPLICATION OF ARTIFICIAL INTELLIGENCE IN AUDITSFROM BIG FOUR FIRMS

Big four accounting firms have injected significant investments in the exploration of AI applications in the audit practice (Bowling and Meyer 2019;Commerford et al. 2020; CPA.com 2019;Kokina and Davenport 2017). For example, PricewaterhouseCoopers (PwC) cooperated with H 2O.ai company and built an innovative bot, called GL.ai, and named the "Audit Innovation of the Year" by the International Accounting Bulletin in 2017, with AI and machine learning functions[2] . It helps auditors to understand companies and detect fraud and anomalies by analyzing large amounts of data in a short time, impossible to be achieved by manual inspections. "GL.ai has been successfully trialed on 20 audits in 12 countries including Canada, Germany, Sweden, and the UK.[3] "EY also has a cloud-based platform, EY Atlas, to integrate AIinto a supportive environment for auditors(EY 2016). Specifically, EY AtlasincorporatesAI "and speech recognition capability, to bring a leading class research experience to our people and clients (EY 2016)." Furthermore, EY has used drones with AI in inventory observations in audits[4] , allowing more frequent and accurate inventory data collection.

KPMG associated with Microsoft and IBM Watson to launch KPMG Clara (KPMG 2018), a new "automated, agile, intelligent, and scalable" audit platform, integrating various functions in predictive analytics and cognitive technologies. It enables users of

2. PricewaterhouseCoopers (PwC). 2019. Harnessing the Power of AI to Transform the Detection of Fraud and Error. Available at: https://www.pwc.com/gx/en/about/stories-from-across-the-world/harnessing-the-power-of-ai-to-transform-the-detection-of-fraud-and-error.html
3. PwC. 2019. Harnessing the Power of AI to Transform the Detection of Fraud and Error. Available at: https://www.pwc.com/gx/en/about/stories-from-across-the-world/harnessing-the-power-of-ai-to-transform-the-detection-of-fraud-and-error.html
4. EY scaling the use of drones in the audit process, June 2017. Available at: https://www.ey.com/gl/en/newsroom/news-releases/news-ey-scaling-the-use-of-drones-in-the-audit-process

KPMG Clara to analyze entire populations and to implement data-driven risk assessment (KPMG 2018). Deloitte has GRAPA to assist auditors with obtaining the knowledge and experience in the pool of previous audits when they formulate the risk strategy for audits (Deloitte 2018). In this way, an auditor not only relies on his/her own experience but also benefits from the knowledge pool from all colleagues worldwide to support risk evaluation. Moreover, Deloitte' s Argus, an intelligent tool that can analyze, search, and locate amendments in documents, mainly aids auditors in identifying minor differences in contracts. The previously time-consuming and labor-intensive identification would become efficient and effective with the assistance of Argus.

4.THE ETHICS OF ARTIFICIAL INTELLIGENCE ON AUDITS

When auditors are implementing more and more AI-related technologies into practice, they should carefully consider and keep the ethical guidelines in their minds, especially in the highly regulated industry. Jobin, Ienca, and Vayena (2019) investigated and analyzed guidelines about AI ethics and identified a convergence on a set of principles, including transparency, justice, fairness and equity, non-maleficence, responsibility, and accountability, and privacy. This result underlined "highlight the importance of integrating guideline-development efforts with substantive ethical analysis and adequate implementation strategies (Jobin et al. 2019)."

Focusing on the audit domain, Munoko, Brown-Liburd, and Vasarhelyi (2020) raised the capabilities and challenges of AI applications and identified ethical principles at risk with AI. Munoko et al. (2020) also analyzed and elaborated elements of three aspects of the audit practical ethics, including individual, institutional, and socio-political levels, listed in Table 1.

Table 1 Elements of practical audit ethics

(summarized and modified from Munoko, Brown-Liburd, and Vasarhelyi 2020)

Individual (auditor) level	Due care
	Professional skepticism and judgment
	Auditor competence
	Independence
Institutional (audit firm) level	Confidentiality and data security
	Data quality (inclusion/exclusion)
	Non-isolation
Socio-political (profession and societal) level	Audit quality across the profession
	Beneficence
	Transparency
	Deprofessionalization

5.EVOLVING CPA LICENSURE MODEL AND CURRICULUM DESIGN

Facing the increasing potential and usage of AI, CPAs may grasp this opportunity to provide clients with new services related to cybersecurity management and IT controls and risks(Tysiac 2019).Hence, CPAs in the digital era need to know data and audit analytics, business intelligence, risk management in IT, cybersecurity, etc. Meanwhile, the contents in the CPA examination needs to be reconsidered to enable innovation in the audit practice.In January 2020, the National Association of State Boards of Accountancy (NASBA) and the American Institute of Certified Public Accountants (AICPA)proposed a new "core plus discipline" CPA evolution licensure model[5] (Coffey 2020). In the proposed model, each CPA candidate is required to (1) pass all subjects from the "core," related to accounting, auditing, tax, and technology, and (2) select and pass one of the three "disciplines," including information systems and controls, business reporting and analysis, and tax compliance and planning. Advanced themes about information systems, such as the security and privacy of information and cybersecurity, would be covered in the discipline of information systems and controls. In May 2020, the AICPA Council "overwhelmingly" voted to support the proposed CPA exam model, expecting to launch the new CPA examination by January 2024[6].

The design of the curriculum at the undergraduate and graduate levels should be restructured to make accounting students equip with the essential knowledge to become CPAs in the next generation. In the 2018 Accounting Accreditation Standards, the Association to Advance Collegiate Schools of Business (AACSB) updated the guidance about "Information Technology Skills, Agility, and Knowledge for Accounting Graduates (A 5)[7]." Specifically, the standard clearly states that accounting programs should incorporate curriculum related to emerging technologies, such as data management/ security and data analytics (statistical modeling, text analysis, predictive analytics, or data visualization, etc.) (AACSB 2018). The concept, capabilities,and implementation of AI methodologies could be integrated into courses in accounting programs.It's essential for auditors in the digital era to equip with the mindset and skills of AI and other emerging technologies (Drew 2019).

5. More information about the proposed CPA licensure model could be obtained from the webpage, CPA EvolutionInitiative from NASBA and AICPA. Available at: https://www.evolutionofcpa.org/

6. "Another Step Close to Evolving CPA Licensure," posted by AICPA Communications on May 21, 2020. Available at: https://blog.aicpa.org/2020/05/another-step-closer-to-evolving-cpa-licensure.html#sthash.y2xRwDAE.eGhWJgJh.dpbs

7. The Association to Advance Collegiate Schools of Business (AACSB) Accounting Standards. 2018. Available at: https://www.aacsb.edu/accreditation/standards/accounting

6.CONCLUSIONS

"Artificial intelligence is the science and engineering of making computers behave in ways that, until recently, we thought required human intelligence," according to the interview with Andrew Moore[8] (High 2017). The World Economic Forum[9] indicated that Artificial Intelligence is seen as the engine of the Fourth Industrial Revolution. While business applications of AI are widespread in many areas, the audit profession has been slow in its adoption due to several reasons, including restrictive standards and conservatism. Although several of the large firms have developed applications containing some AI technology, as described earlier in this paper, these are still not close to being used in the mainstream of external auditing. At least two tools have been launched to compete with traditional audit tools that contain elements of AI (Mindbridge[10]and Caseware AI [11]), and several cases have been published with examples.

In general, expensive and comprehensive applications, tend to be constraining and limiting as well as not very scalable and challenging to apply in different contexts. However, narrow domain apps that can count, classify, understand voice, parse semantics, identify errors, etc. can be inserted in a progressively more automated robotic process automation (RPA) (Huang and Vasarhelyi 2019; Rosario and Vasarhelyi 2019). Blending basic keystroke replacement applications that will substantially reduce manual labor in auditing with narrow AI applications is called Intelligent Process Automation (IPA) (Berutti et al. 2017) and presents great promise for accounting and auditing.

The aforementioned drone-based inventory counts of cattle being performed by EY uses a "count" AI application associated with pictures. This combination of narrow apps that can be currently classified as AI within new methods of performing accounting and auditing functions will probably be prevalent in the coming years.

In conclusion, usage of AI in the accounting and auditing field is still incipient with both experimentation mainly by the large firms and the emergence of tools focusing on accounting markets or tools from other fields (e.g., legal discovery). However, the potential is immense and undoubtedly will be the future of the profession.

8. Andrew Moore is the former Dean of the School of Computer Science, Carnegie Mellon University

9. Shaping the Future of Technology Governance: Artificial Intelligence and Machine Learning. World Economic Forum. Available at: https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-artificial-intelligence-and-machine-learning

10. https://www.mindbridge.ai/

11. https://www.caseware.com/us/analyticsai

REFERENCES

1. Appelbaum, D., and Nehmer, R. 2017a. "The Coming Disruption of Drones, Robots, and Bots: How Will it Affect CPAs and Accounting Practice?" CPA Journal (87: 6), pp. 40- 44.
2. Appelbaum, D., and Nehmer, R. 2017b. "Using Drones in Internal and External Audits: An Exploratory Framework," Journal of Emerging Technologies in Accounting (14: 1), pp. 99- 113.
3. Association to Advance Collegiate Schools of Business (AACSB). 2018. 2018 Eligibility Precedures and Accreditation Standards for Accounting Accreditation. Tampa: AACSB. Available at: https://www.aacsb.edu/-/media/aacsb/docs/accreditation/accounting/standards-and-tables/ 2018-accounting-standards.ashx?la=en&hash = 8DCDA 6CE 3B 0CEF 6AB 82D 39CBF 53995 DA 96111196
4. Berruti, F., Nixon, G., Taglioni, G., and Whiteman, R. 2017. "Intelligent Process Automation: The Engine at the Core of the Next-Generation Operating Model," Digital McKinsey.
5. Bowling, S., and Meyer, C. 2019, "How we Successfully Implemented AI in Audit," Journal of Accountancy (227: 5), pp. 26- 28.
6. Brown-Liburd, H., and Vasarhelyi, M. A. 2015. "Big Data and Audit Evidence," Journal of Emerging Technologies in Accounting (12: 1), pp. 1- 16.
7. Coffey, S. S. 2020. Our Proposal to Evolve CPA Licensure. Available at: https://blog.aicpa.org/ 2020/ 01/our-proposal-to-evolve-cpa-licensure.html#sthash.M 7OhU 8cA.dpbs
8. Commerford, B. P., Dennis, S. A., Joe, J. R., and Ulla, J. 2020. "Man Versus Machine: Complex Estimates and Auditor Reliance on Artificial Intelligence." Available at SSRN: http://dx.doi.org/ 10. 2139/ssrn. 3422591.
9. Cho, S., Vasarhelyi, M. A., and Zhang, C. (2019). The Forthcoming Data Ecosystem for Business Measurement and Assurance," Journal of Emerging Technologies in Accounting (16: 2), pp. 1- 21.
10. CPA.com. 2019. "The Rise of Artificial Intelligence: A Critical Inflection Point for the Accounting Profession." Available at: https://www.cpa.com/sites/cpa/files/media/resources/whitepapers/the-rise-of-artificial-intelligence-cpacom-report.pdf
11. Deloitte. 2018. "16 Artificial Intelligence Projects from Deloitte: Practical Cases of Applied AI." Rotterdam: Deloitte Netherland. Available at: https://www 2. deloitte.com/content/dam/Deloitte/nl/Documents/innovatie/deloitte-nl-innovatie-artificial-intelligence- 16-practical-cases.pdf
12. Drew, J. 2019, "What's 'Critical' for CPAs to Learn in an Al-Powered World," Journal of Accountancy (227: 5), pp. 20- 24.
13. Ernst & Young (EY). 2016. "Leading-Edge Digital Technology Powering the

EY Audit. London: EY Global. Available at: http://cdn.ey.com/echannel/gl/technologypoweringtheEYaudit-v 9/download/Leading-edge% 20digital% 20technology% 20 powering% 20the% 20EY% 20audit.pdf

14. High, P. 2017. “Carnegie Mellon Dean of Computer Science on the Future of AI,” Forbes. Available at: https://www.forbes.com/sites/peterhigh/ 2017/ 10/ 30/ carnegie-mellon-dean-of-computer-science-on-the-future-of-ai/# 793d 5f 812197

15. Huang, F., and Vasarhelyi, M. A. 2019. “Applying Robotic Process Automation (RPA) in Auditing: A framework,” International Journal of Accounting Information Systems (35), 100433.

16. International Auditing and Assurance Standards Board (IAASB). 2020. Non-Authoritative Support Material Related to Technology: Audit Documentation When Using Automated Tools and Techniques. New York: International Federation of Accountants. Available at: https://www.ifac.org/system/files/publications/files/FINAL-Non-Authoritative-Support-Material_Audit-Documentation-When-Using-Automated-Tools-And-Techniques.pdf

17. Issa, H., Sun, T., and Vasarhelyi, M. A. 2017. “Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation,” Journal of Emerging Technologies in Accounting (13: 2), pp. 1- 20.

18. Jobin, A.,Ienca, M., and Vayena, E. 2019. “The Global Landscape of AI Ethics Guidelines,” Nature Machine Intelligence (1: 9), pp. 389- 399.

19. Kokina, J., and Davenport, T. H. 2017. “The Emergence of Artificial Intelligence: How Automation is Changing Auditing,” Journal of Emerging Technologies in Accounting (14: 1), pp. 115- 122.

20. KPMG. 2018. “KPMG Clara — a smart audit platform.” Amstelveen: KPMG International. Available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/ 2017/ 05/ kpmg-clara-a-smart-audit-platform.pdf

21. Munoko, I., Brown-Liburd, H., and Vasarhelyi, M. A. 2020. “The Ethical Implications of using Artificial Intelligence in Auditing,” Journal of Business Ethics.

22. Omoteso, K. 2012. “The Application of Artificial Intelligence in Auditing: Looking Back to the Future,” Expert Systems with Applications (39: 9), pp. 8490- 8495.

23. Public Company Accounting Oversight Board (PCAOB). 2020. “Data and Technology Research Project Update Spotlight. Washington, DC: PCAOB. Available at: https://pcaobus.org/Documents/Data-Technology-Project-Spotlight.pdf

24. Rozario, A. M., and Vasarhelyi, M. A. 2018. “How Robotic Process Automation is Transforming Accounting and Auditing,” The CPA Journal(88: 6), pp. 46- 49.

25. Sun, T., and Vasarhelyi, M. A. 2017. “Deep

Learning and the Future of Auditing: How an Evolving Technology could Transform Analysis and Improve Judgment," CPA Journal (87: 6), pp. 24- 29.

26. Tysiac, K. 2019. "NASBA and AICPA Seek Input on Evolving Licensure Model," Journal of Accountancy. Available at: https://www.journalofaccountancy.com/news/ 2019/jun/cpa-licensure-model-input- 201921411.html

27. Vasarhelyi, M. A., and O' Leary, D. 1989. "Artificial Intelligence in Accounting and Auditing: Creating value with AI" (Vol. 5). Markus Wiener Publishers.

28. Vasarhelyi, M. A. 1988. Expert Systems in Accounting and Auditing. Artificial Intelligence in Accounting and Auditing. Markus Wiener Publishing.

29. Zhang, C. A., Dai, J., and Vasarhelyi, M. A. 2018. "The Impact of DisruptiveTechnologies on Accounting and Auditing Education: How Should the Profession Adapt?" The CPA Journal(88: 9), pp. 20- 26.

30. Zhaokai, Y., and Moffitt, K. C. 2019. "Contract Analytics in Auditing," Accounting Horizons (33: 3), pp. 111- 126.

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

The Study on the Legal Question of Detecting Crime by Global Position System Tracing Device

許淑媛 Cadalina Hsu
台灣大學法學士/碩士，中正法博士候選人，大洋法律事務所執行長
B.A./M.A at NTU, P.H.D.Candidate at CCU,
C.E.O. at Da-Young attorney-at-law firm.

摘　要

近來，隨著科技的不斷創新與日新月異，犯罪手法日趨組織化、國際化與科技化，進而增加查緝難度，國內之檢、警、調、海巡、憲兵等司法警察機關，於執行公權力時，已無法完全利用傳統之偵查技巧蒐集獲得相關資料，故多需仰賴及運用高科技定位技術來維護國家安全或進行犯罪偵防，例如透過衛星定位系統、通訊監察設備所顯示之基地台位置及監視錄影系統等方式，對人民進行追蹤和監控，藉此蒐集相關不法犯罪事證，然上述高科技設備之運用過程中對部分之善意第三人，於憲法上所賦予的居住遷徙自由、秘密通訊自由或隱私權等基本權利造成侵害，但近年來之犯罪手法及手段不斷精進，將上述科技設備運用於犯罪偵查中，即不見得搜尋所需的資料，更何況予以摒除，然而，對於運用這些科技設備進行犯罪偵查的要件與程序為何？現行法律有無明文規定？現行法規所訂定之要件與程序是否完整，相關司法警察機關因如何在公益與私利間取得平衡，即為本文所欲探討之重點。

關鍵詞 : 科技設備、犯罪偵查、證據排除、通訊監察、衛星定位。

Abstract

Recently, with constantly changing and innovative technology, technique of perpetration has become more organized, internationalized and technologized which increases the difficulties of investigation and arrest. Judicial and police institutions such as prosecutor, police, coast guard, gendarme, and etc. can't obtain relevant information by using the traditional investigative techniques while executing authority. Therefore, it's necessary to utilize highly technical positioning techniques to maintain national security or crime investigation. For instance, via GPS and communications monitoring system which reveal the locations of base stations or surveillance system to track and monitor civilians in order to collect relevant illegal evidence. However, the utilization of those technical equipment may violates some fundamental rights such as the right to live and migrate, the right to secret communication and privacy of the friendly third party in the meantime. Nevertheless, the techniques of perpetration have forged ahead vigorously. It won't guarantee to obtain the information by using the technologies mentioned above during the investigation, not to mention to dismiss it. Yet, what are the conditions and procedures to use this equipment to investigate crime? Is it clearly regulated in the ordinance? Are the conditions and procedures drawn up in the legislation completed? And how do judicial and police institutions strike a balance between non-profit and profit is the key point of this essay.

Keywords:
Technical Equipment, Crime Investigation, Evidence Elimination, Communication Monitoring, Global Position System.

壹、前言

自民國 (下同) 103 年海巡署王姓士官長為查緝私菸而安裝衛星定位系統追蹤器於他人車輛底盤後，有關偵查機關以衛星定位系統取得他人位置資訊行為定性之爭議甚囂塵上，其本質究竟屬於任意偵查抑或強制處分，若係後者則現行法是否存在可適用之相關規定，又或者於立法論上應以如何之體制建構等等爭議卻並未隨著最高法院表明立場而消失。[1]

全球衛星定位系統除廣為人知之美國 GPS(Global Positioning System) 系統外，尚有俄羅斯之 GLONASS 系統 (ГЛОНАСС) 以及歐盟之伽利略

1. 歷審判決參照：高雄地院 104 年度聲判字第 81 號、105 年度易字第 110 號，高雄高分院 105 年度上易字第 604 號、最高法院 106 年度台上字第 3788 號。

(Galileo) 系統等，惟台灣現行多數定位系統仍以美國 GPS 系統之訊號為主，故本文就以全球衛星定位系統產生座標回傳之偵查方式，仍以 GPS 偵查代稱之，主旨在探討 GPS 系統於偵查中使用之合法性及立法制度發想，探討重點包含現行法規所訂定之要件與程序是否完整，以及相關司法警察機關因如何在公益與私立間取得平衡，此文從定性的角度切入，探究增訂立法之位置、基本決定機關之架構、第一線之司法警察、司法警察官使用 GPS 系統於偵查中的權限等。

然而，我國司法警察（官）於偵查犯罪時，為了蒐集相關證據或特定犯罪嫌疑人之位置而進行各式之個人資料蒐集，若賦予司法警察（官）可隨意進行此種偵查作為之權限，確可加強偵查之效率，但人民之行動軌跡、通話記錄及各式記錄（如病歷紀錄及金融記錄等）便會因此運作而無所遁形。

依刑訴法第 230 條、231 條是否得作為使用 GPS 定位追蹤器之依據？如無，則是否能在目前刑事法或通訊及保障監察法上找到其他可資運用之條文，或應以何令狀方式為之，其發動門檻及賦予何種程序保障，一併為討論，俾使偵察機關利於因應日新月累的犯罪手法而發展新興偵查犯罪手段，得以發現犯罪真實，及兼顧人權之保障。

貳、定性

一、以侵害基本權利與否作為強制處分與任意偵查之區分：

對於強制處分與任意偵查之區隔，已不再侷限於物理性手段施強制力限制人民基本權利，一般係以該作為是否侵害憲法所保障之基本權利為標準。

二、是否侵害隱私權：

首先，必須先說明的是，隱私權的侵害及活動是否公開，應為兩個獨立的分別要素，即便這兩個概念在多數時候十分相似，彼此之間也具有高度的正相關，然而，卻是個別存在的兩個不同概念，不應混為一談；在刑事實體法的層次，由於刑法第 315 條之 1 條文明文「非公開」的構成要件，因此不可避免的，非公開的活動勢必是成罪的待證前提，而在刑事程序法的層次，如上開之述，對憲法上基本權利的侵害將會進一步衍生法律保留以及比例原則的誡命，此時是否侵害了人民的隱私權或其他權利即屬關鍵。

對隱私權的侵害不應單純理解為存在侵害與否，處於交際往來之社會中，任何人實然皆或多或少地遭受隱私的侵害與剝奪，他人能夠獲知吾人公開、表露於外的一切資訊，無論被獲知者是否願意，然而，這是我們所應該能要預見以及接受的，當我們踏進這個社會成為其中的一份子，這就是我們所預料到將付出的代價。

因此，隱私權事實上應該是以不同程度區分，只有在當被窺見的程度已經大於我們所預見、一般認為會被侵害的程度時，此時才該當對隱私權的侵害。

由是觀之，道路乃開放空間，開車行駛在公開場合上應當能夠合理預見並且接受此時任何人皆能窺視探測該車此時之位置所在，因此難謂此種情形之下隱私權受到侵害。

然而從學說到實務見解[2]，許多意見都在此時援引美國法上的「馬賽克理論」(或稱「鑲嵌理論」)，認為縱然個別瞬間之位置資訊係屬公開，亦不具有合理隱私期待，然而藉由大量、長時間的密集拼湊，將能夠由點而線，由線而面的獲知鉅量資訊，對於被定位者的隱私權將造成嚴重危害。

學說見解對此產生的批評是，既然實務也承認，路人均可見到被害人的車輛於某時經過某處，亦即，對於每個路人來說，車輛在該時點從他的眼前經過這件事，無疑是公開的。既然每一小段的行駛經過都是公開的活動，我們就很難理解，為什麼累積加總在一起就會導致質變？[3]

然而本文認為，首先在量的層面，即便如前所述，當我們行走活動在公開空間時，勢必已然認知到並接受自己的活動被探測窺見的事實，然而這並不代表我們認知並接受自己 24 小時無時無刻的活動位置都被縝密詳實沒有遺漏地記錄下來；此外在質的層面，若行為人駕車前往無人的野外山區又或者停留於自家封閉車庫，此時是否代表相對地因為並非公開而無法為位置偵查？

以 GPS 持續發送訊號以及無論公開或非公開皆一併監錄的特性觀之，往往能夠在一定時間內取得大量確實的位置資訊，並且系統化地歸納整理為可再現之資訊，存在調閱分析之可能，此外由於其不可控性亦如通訊監察可能造成本案外之不必要侵擾之危險[4]，因此在一般的情形下會構成對於隱私權的侵害，僅在少數的短期、公開監看的例外情形並不會造成隱私權侵害。

我國最高法院於 106 年度台上字第 3788 號刑事判決中強調「是個人縱於公共場域中，亦應享有依社會通念得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主，而受法律所保護，此觀司法院釋字第 603 號、第 689 號解釋意旨自明。故而隱私權屬於憲法所保障之權利，殆無疑義。而有無隱私權合理保護之期待，不應以個人所處之空間有無公共性，作為決定其是否應受憲法隱私權保障之絕對標準。個人身處公共場域中，仍享有私領域不被使用科技設備非法掌握行蹤或活動之合理隱私期待。」

最高法院又於該判決中，根據前述理解及 GPS 偵查之性質為下開判斷：「又偵查機關為偵查犯罪而非法在他人車輛下方底盤裝設 GPS 追蹤器，由於使用 GPS 追蹤器，偵查機關可以連續多日、全天候持續而精確地掌握該車輛及其使用人之位置、移動方

2. 高等法院 104 年上易字第 352 號判決：「即如馬賽克拼圖一般，乍看之下微不足道、瑣碎的圖案，但拼聚在一起後就會呈現一個寬廣、全面的圖像。個人對於零碎的資訊或許主觀上並沒有隱私權遭受侵害之感受，但大量的資訊累積仍會對個人隱私權產生嚴重危害。是以車輛使用人對於車輛行跡不被長時間且密集延續的蒐集、紀錄，應認仍具有合理之隱私期待。」

3. 蔡聖偉，私裝 GPS 跟監與刑法第三一五條之一—評臺灣高等法院一〇〇年度上易字第二四〇七號判決，月旦裁判時報，32 期，頁 35，2015 年 2 月。

4. 通訊保障及監察法第 18 條之 1：「依第五條、第六條或第七條規定執行通訊監察，取得其他案件之內容者，不得作為證據。但於發現後七日內補行陳報法院，並經法院審查認可該案件與實施通訊監察之案件具有關連性或為第五條第一項所列各款之罪者，不在此限。依第五條、第六條或第七條規定執行通訊監察所取得之內容或所衍生之證據與監察目的無關者，不得作為司法偵查、審判、其他程序之證據或其他用途，並依第十七條第二項規定予以銷燬。違反第五條、第六條或第七條規定進行監聽行為所取得之內容或所衍生之證據，於司法偵查、審判或其他程序中，均不得採為證據或其他用途，並依第十七條第二項規定予以銷燬。」

向、速度及停留時間等活動行蹤，且追蹤範圍不受時空限制，亦不侷限於公共道路上，即使車輛進入私人場域，仍能取得車輛及其使用人之位置資訊，且經由所蒐集長期而大量之位置資訊進行分析比對，自可窺知車輛使用人之日常作息及行為模式，難謂非屬對於車輛使用者隱私權之重大侵害。而使用 GPS 追蹤器較之現實跟監追蹤，除取得之資訊量較多以外，就其取得資料可以長期記錄、保留，且可全面而任意地監控，並”無跟丟”可能等情觀之，二者仍有本質上之差異，難謂上述資訊亦可經由跟監方式收集，即謂無隱密性可言。」

前開立論與立法趨勢應值贊同，惟刑事訴訟法制至今仍未對 GPS 偵查為任何規範。前引我國最高法院判決，即是前海巡署士官長為查緝販毒，因無法律授權、亦未立案調查或報請長官書面同意下逕為 GPS 偵查，是以不能認有法律上之正當理由而侵害受偵查人之隱私，被法院認定犯妨害秘密罪；該判決作成後，第一線偵查犯罪之人員運用 GPS 偵查頓時面臨觸法之風險。

然相關機關對於刑事訴訟法制不備使第一線人員面臨風險之處境，迄今未有正確之認識與立法準備作業。第一線偵查人員無法律依據所致觸法風險，不因法務部及相關機關怠於提案有所緩解，爰依據前引我國最高法院判決及各法制先進國之規範精神，並參照同為偵查具隱密性或組織性、且難以使用他法偵查之犯罪之通訊監察法制立法例，於刑事訴訟法新增相關法規，俾使第一線偵查人員辦案時有法可循，安心辦案，亦使受偵查人之權益受正當法律程序之保障。

三、作為強制處分，應有法律保留原則之適用。

(一) 侵害隱私權之前提下即有法律保留之適用

如前所述，既然 GPS 監察於一般情形下會造成隱私權侵害，屬於強制處分，亦即刑事訴訟上基本權干預[5]之性質，據此受有法律保留原則及比例原則之拘束。

(二) 依現行法律之適用空間

1. 通訊保障及監察法

基於秘密對於隱私權的侵害特性、擷取人民資訊之性質，或有認為應以通訊保障及監察法 (下稱通保法) 之規範作為 GPS 之適用依歸，然而由通保法本身之條文[6]觀之，其所稱之通訊乃指：「①利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信、②郵件及書信、③言論及談話。」此外，多數學說亦認為通保法之通訊乃指通訊雙方含有思想表示之內容[7]，蓋單純位置標點之發送並不包含其思想之內

5. 林鈺雄，刑事訴訟法，頁 302-303，7 版，2013 年 9 月。
6. 通訊保障及監察法第 3 條第 1 項各款參照。
7. 林裕順，GPS 偵查法治化研究，月旦裁判時報，68 期，頁 22，2018 年 2 月。
8. 李榮耕，科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展，臺灣大學法學 論叢，44 卷 3 期，頁 933，2015 年 9 月。

涵，因此不屬於通保法之通訊，亦無相關規範之適用[8]。

2. 警察職權行使法

由於警察職權行使法第 11 條明文警察於特定情形為防止犯罪，認有必要，得經由警察局長書面同意後，於一定期間內，對其無隱私或秘密合理期待之行為或生活情形，以目視或科技工具，進行觀察及動態掌握等資料蒐集活動；GPS 偵查是否於此範圍內遂成重大爭議。然而首先該條款之適用，乃被動對犯罪之防止、預防而非主動積極之犯罪偵查追緝，不應混為一談。

此外，實務上之 GPS 偵查往往亦未取得警察局長之書面同意，如此情況之下其所自為之 GPS 偵查，自亦有違法。而值得思考的是，最高法院及學說理所當然地論證人力跟監及 GPS 跟監二者之不同，乃係建立在人力跟監合法，而 GPS 跟監僅只係以科技設備取代人力所實行之偵查追緝手段，此時自然應論理 GPS 為何不能該當人力跟監之規範，惟有學者提出如此地思考或有未全之處，GPS 乃獨立之型態，應單獨就此型態之偵查獨立分析[9]，且就跟監本身之合法與容許性部分，亦並非全無疑問[10]，從我國新修正刑法 344 條之 1 加重重利罪以及日本糾纏騷擾行為罪[11]觀之，也能夠發現對於單純跟蹤所造成的侵害以及保護必要日漸升高。

退萬步言之，縱然人力跟監偵查係屬合法，於以 GPS 替代人力跟監之場合，一來人力有時而窮，反之 GPS 卻能精密確實地將每一瞬間之位置資訊客觀紀錄，對隱私權之侵害不可同一而論，二來若於人力不可至之偏遠或非公開位置，GPS 亦能追蹤之，不可否認 GPS 所能偵查之範疇確實較諸人力跟監更深且廣；此時 GPS 已然逸脫跟監所能及之預想及授權範圍，縱然合於跟監之發動，不代表得以之作為 GPS 合法之根據。

3. 刑事訴訟法規定 :

(1) 刑事訴訟法第 230、231 條

傳統實務曾主張跟監雖侵害隱私權，惟乃不具強制性之任意偵查方法，刑事訴訟法第 230、231 條既然規定司法警察、司法警察官知有犯罪嫌疑則應開始調查，則得依據上開規定獲得授權[12]。

然而該規範事實上應僅具組織法之意義，揆諸法律保留之根本精神，作為授權基本權干預之法律亦應符合明確性之要求，以概括條款作為授權依據實乃謬誤，實務亦於後續判決[13]中更正其立場。

(2) 刑事訴訟法第 122 條

9. 薛智仁，GPS 跟監、隱私權與刑事法—評最高法院 106 年度台上字第 3788 號刑事判決，月旦裁判時報，70 卷，頁 44-45，2018 年 4 月。

10. 對跟監的質疑，參見李錫棟，跟監對基本權利之干預，中央警察大學法學論集，第 9 期，2004 年 3 月；范里，跟監應屬刑事訴訟上之基本權干預—評最高法院 102 年度臺上字第 3522 號判決，刑事法雜誌，58 卷 2 期，2014 年 4 月。

11. 對於日本糾纏騷擾行為罪，參見黃士軒，概觀日本糾纏騷擾行為罪的處罰現況，刑事法評論，第 5 期，2017 年 6 月。

12. 最高法院 102 年度台上字第 3522 號判決參照。

13. 最高法院 106 年度台上字第 3788 號判決參照。

於刑事訴訟法中，更有作為GPS授權依據之可能者乃搜索之相關規定，事實上，隨著科技日新月異的發展，對於隱私的侵害可能衍生各種不同的態樣，此時亦非不許適用關於搜索之授權條款，而不必執著於是否係屬物理上獲取有形證據的形式。然而有認為GPS偵查真正無法適用搜索規定之原因在於，搜索於法律上基於立法者所賦予的公開性原則，存在其極限而不能適用於諸如通訊監察及GPS偵查等無法對當事人公開之搜索方法，故而因為其執行方法欠缺公開性而不符合現行法的搜索定義，換言之，刑事訴訟法第122條並非GPS跟監的法律依據[14]。

(3) 應以針對特定類型之法制規範

就現行可能適用之法律而言，皆未有可行之規範條款，故而較妥適之作法應為以獨立類型規劃設計GPS之授權依據。

參、法制建構之發想

一、增訂之位置

法務部對於GPS偵查立法之修法草案，擬將其納入現行之通保法中，規定司法警察要使用GPS監控辦案，需先取得檢察官同意[15]，學界方面則有以通保法增訂[16]以及於刑事訴訟法中增訂[17]等不同意見。

本文認為較為妥適之作法乃係於刑事訴訟法另闢專章又或另修專法，由於通訊保障監察法乃針對含有意思思想表示內容之監聽，所可能侵害者以及應規範之密度、嚴格程度與GPS應有所別，兩者間之發動條件若堅持一致則將有過度僵化之疑慮，不應一概而論。

二、二分模式為基本決定機關之架構

而GPS偵查發動之決定者，本文認為由於其並未達到如搜索、通訊監察等之隱私權侵害程度，且為求偵查中之效率，應以二分模式作為決定之依歸，亦即偵查中由檢察官決定，而審判中由法官決定，惟大部分發動之情形為偵查中，檢察官乃一般情況下之決定者，乃屬當然。

三、允許司法警察、司法警察官緊急情況下之無令狀例外

囿於檢察官與員警之人數相差懸殊，縱然檢察官為具有權限之偵查主體，然而事實上執行第一線勤務者絕大多數情況下皆為司

14. 薛智仁，同註9，頁48、49。
15. 姜宜菁、廖炳棋，科技辦案法制化／緝凶蒐證，頁68，2018年9月。
16. 朱志平，GPS定位追蹤於刑事偵查程序之運用及其授權基礎—從臺灣高等法院高雄分院105年度上易字第604號刑事判決出發，法令月刊，68卷9期，頁128-129，2017年9月。
17. 薛智仁，同註9，頁57-59。

法警察或司法警察官，此時若如前述以檢察官之令狀為必要，則勢必將大為妨害偵查之效率及機能，產生如刑事訴訟法第 131 條第 2 項之弊，將架空 GPS 偵查，故本文以為應允許司法警察、司法警察官於必要時得於若不及時架設 GPS 則勢難取得架設之時機又或被監控人即將離去之例外情形，自行先為裝設 GPS，該當無令狀之急迫例外。惟前開情形中，先行無令狀 GPS 偵查之司法警察及司法警察官事後亦應有數日內須陳報檢察官並取得其審查許可之事後陳報義務。

四、同通保法存在最長期間之限制

此外，如通保法之規定[18]，GPS 偵查作為當事人不知自己受監察之型態，亦應有最長期間之限制，因如前述，隱私權的侵害乃如光譜般的存在，隨著連續監控的時間越長，也隨之造成越大的隱私權侵害，存在最大限度的監控極限，並於例外情形得釋明具體理由繼續之（惟此時應由法官檢驗是否有理由得繼續監之），方能有效避免人民之基本權利遭受無邊際之鉅量侵擾。

肆、結論

我國近期對 GPS 監察於刑事實體法及程序法上之熱烈討論濫觴於數年前之海巡士官 GPS 監察案，美國聯邦最高法院在 2012 年 1 月底亦於 United States v. Jones 案[19]中否決美國政府主張「個人對於自己在公共場所移動而產生的虛擬資訊無隱私期待可言」的立場[20]，可見對於隱私權之期待以及隨之而來的侵害之理解皆已非同以往，重要性及關注度亦較往日高出許多。而 GPS 監察所產生之隱私權侵害，縱然在認為人力跟監合法的前提之下，相較人力跟監所產生之差距已然不僅止於以科技設備取代人力如此而已，當我們行走在公開的街道上時，可以預想得到此時與我們相對的任何人都能夠觀察到我們暴露在外的一切訊息，我們也接受這樣微量的隱私權侵害作為社會化的代價；然而我們卻應該不能預想得到當我們行走在公開的街道時，每一個位置座標都將被持續地、系統性地記錄、整理為資料檔案，並且可能再現、歸納以獲取解讀更多有關我們個人生活的資訊，這樣的侵害程度和前述路人照面的瞥見，事實上已然完全不同，縱然有學者提出並非一概侵害基本權利即屬強制處分並隨之產生法律保留及比例原則之適用，而係從層級化刑事訴訟之基本權干預出發，承認在一定門檻以下的微量干預措施，司法警察（官）得以一般調查權限之條款作為干預的授權基礎，在這樣的授權範圍下屬於任意偵查[21]，然而 GPS 所產生之侵害

18. 通保法第 12 條第 1 項：「第五條、第六條之通訊監察期間，每次不得逾三十日，第七條之通訊監察期間，每次不得逾一年；其有繼續監察之必要者，應釋明具體理由，至遲於期間屆滿之二日前，提出聲請。但第五條、第六條繼續之監察期間，不得逾一年，執行機關如有繼續監察之必要者，應依第五條、第六條重行聲請。」

19. 本案結論認為 GPS 偵查構成搜索，必須取得令狀方為合法。更多本案的相關討論，參見金孟華，GPS 跟監之程序適法性—從美國 United States v. Jones 案談起，月旦裁判時報，第 68 期，頁 24-35，2018 年 2 月；林利芝，從美國最高法院 United States v. Jones 案分析美國政府運用 GPS 定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，272 期，頁 177-188，2017 年 12 月。

20. 劉靜怡，政府長期追蹤與隱私保障，月旦法學教室，116 期，頁 9-10，2012 年 6 月。

21. 林鈺雄，干預保留與門檻理論—司法警察（官）一般調查權限之理論檢討，政大法學評論，96 卷，頁 33-34，2007 年 4 月。

已逾越微量干預之範疇，GPS 偵查已侵害憲法所保障人民之隱私權，屬於強制處分之範疇，基於憲法之誡命，應以法律規範明文其授權、救濟等制度，以落實正當法律程序。自然該當強制處分而有適用法律保留及比例原則之必要。

大法官解釋亦肯認憲法上保障人民隱私權，認為所謂的隱私權包含生活私密領域不受侵擾之自由及個人資料之自主權，其中所謂的個人資料之自主權，包含了是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權，此一權利不僅在私人生活領域中應受保障，縱於公共場域中，亦應享有依社會通念上，得不受他人持續注視、監看、監聽、接近等侵擾之私人活動領域及個人資料自主之權利。

從而，以 GPS 定位追蹤器作為偵查工具可取得人民無論在私生活領域或公共場域之個人位置資訊，經由大量蒐集此類資訊並分析後，得進一步窺知人民之日常作息及行為模式，此一偵查手段，實屬對於人民個人資訊自主權之侵害，且因人民無從得知遭 GPS 定位追蹤器跟監，自無法就國家取得關於自身資訊之事決定是否提供、更正或揭露，法律也無規定相關救濟管道。

在現行法皆未能作為 GPS 偵查之授權基礎條款時，此時即有迅速將 GPS 偵查法制化之必要，本文認為以刑事訴訟法專章或是立專法之方式，由二分模式決定強制處分之發動，並賦予第一線之司法警察、司法警察官急迫時無令狀之例外，同時可兼顧偵查之速效及對人民隱私權之保障，應屬適當。

伍、參考文獻

一、專書

1. 林鈺雄，刑事訴訟法，2013 年 9 月 7 版。
2. 陳宗廷，犯罪偵查實務，宏星公司，1992 年 9 月，四版。
3. 陳新民，中華民國憲法釋論，三民書局，2001 年 1 月，四版。
4. 陳樸生，刑事訴訟法實務，自版，1989 年 12 月，重訂初版。
5. 黃東熊，刑事訴訟法論，三民書局，1995 年 2 月，三版。
6. 黃昭元，無指紋則無身分證？換發國民身分證與強制全民捺指紋的憲法爭議分析，收於民主、人權、正義 - 蘇俊雄教授七秩華誕祝壽論文集，元照出版有限公司，2005 年 9 月，初版。
7. 黃清德，科技定位追蹤監視與基本人權保障，元照出版有限公司，2011 年 11 月，初版一刷。
8. 褚劍鴻，刑事訴訟法論，臺灣商務印書館，1996 年 2 月，二次修訂版。
9. 蔡墩銘，刑事訴訟法論，五南圖書出版股份有限公司，1997 年 11 月，重訂版。
10. 蔡震榮，警察職權行使法概論，元照出版有限公司，2004 年，初版。

蕭文生，一九八三年人口普查法，收於西德聯邦憲法法院裁判選輯（一），司法周刊雜誌社，2000 年 1 月。

二、期刊文獻

1. 蔡聖偉，私裝 GPS 跟監與刑法第三一五條之一—評臺灣高等法院一〇〇年度上

易字第二四〇七號判決，月旦裁判時報，32 期，2015 年 2 月。

2. 林裕順，GPS 偵查法治化研究，月旦裁判時報，68 期，2018 年 2 月。
3. 李榮耕，科技定位監控與犯罪偵查：兼論美國近年 GPS 追蹤法制及實務之發展，臺灣大學法學論叢，44 卷 3 期，2015 年 9 月。
4. 薛智仁，GPS 跟監、隱私權與刑事法 — 評最高法院 106 年度台上字第 3788 號刑事判決，月旦裁判時報，70 卷，2018 年 4 月。
5. 李錫棟，跟監對基本權利之干預，中央警察大學法學論集，第 9 期，2004 年 3 月。
6. 范里，跟監應屬刑事訴訟上之基本權干預 — 評最高法院 102 年度臺上字第 3522 號判決，刑事法雜誌，58 卷 2 期，2014 年 4 月。
7. 黃士軒，概觀日本糾纏騷擾行為罪的處罰現況，刑事法評論，第 5 期，2017 年 6 月。
8. 朱志平，GPS 定位追蹤於刑事偵查程序之運用及其授權基礎 — 從臺灣高等法院高雄分院 105 年度上易字第 604 號刑事判決出發，法令月刊，68 卷 9 期，2017 年 9 月。
9. 金孟華，GPS 跟監之程序適法性—從美國 United States v. Jones 案談起，月旦裁判時報，第 68 期，2018 年 2 月。
10. 林利芝，從美國最高法院 United States v. Jones 案分析美國政府運用 GPS 定位追蹤器探知個人位置資訊之適法性，月旦法學雜誌，272 期，2017 年 12 月。
11. 劉靜怡，政府長期追蹤與隱私保障，月旦法學教室，116 期，2012 年 6 月。
12. 林鈺雄，干預保留與門檻理論 — 司法警察（官）一般調查權限之理論檢討，政大法學評論，96 卷，2007 年 4 月。

三、碩、博士學位論文（按作者姓名筆劃排列）

1. 王宏政，警察跟監活動與隱私權保護之研究，中央警察大學行政警察研究所碩士論文，2007 年 6 月。
2. 吳景欽，防制組織犯罪法律規範之研究，輔仁大學法律學研究所博士論文，2005 年 6 月。
3. 吳爾文，警察跟監制度之研究，台灣大學法律學研究所碩士論文，2007 年 6 月。
4. 李文章，數位資訊在犯罪偵查上之應用－以目標軌跡、全球衛星定位系統、電話通聯電腦分析系統為例，中央警察大學刑事警察研究所碩士論文，2007 年 1 月。
5. 李西河，警察蒐集刑事證據過程之研究，中央警察大學行政警察研究所碩士論文，2006 年 6 月。
6. 李翠玲，論偵查主體，中正大學法律研究所碩士論文，2004 年 6 月。
7. 周姵吟，刑法妨害秘密罪意涵之研究，東海大學法律學研究所碩士論文，2009 年 6 月。
8. 林昶瑁，論刑事程序之跟監行為，政治大學法學院碩士在職專班碩士論文，2009 年 5 月。
9. 林錦鴻，警察運用監視器之法律問題分析，台灣大學法律學研究所碩士論

文，2006 年 6 月。

10. 曹珮怡，論電信監察與談話監聽 - 以德國刑事訴訟法為中心，政治大學法律學研究所碩士論文，2008 年 6 月。

11. 莊武能，使用衛星定位追蹤器偵防犯罪之法律爭議探討，中國文化大學法律學研究所碩士論文，2008 年 6 月。

12. 黃壬聰，犯罪偵查勤務之研究，中央警察大學刑事警察研究所碩士論文，1999 年 6 月。

13. 黃政龍，科技偵查之研究—以公共空間行動資訊隱私權為範疇，中原大學財經法律研究所碩士論文，2009 年 1 月。

14. 黃鈺雯，個人資料蒐集於刑事偵查之爭議，政治大學法律學研究所碩士論文，2012 年 7 月。

15. 廖哲儀，司法警察為偵查主體之辯正，中正大學法律研究所碩士論文，2012 年 1 月。

16. 蔡達智，公權力利用衛星科技對隱私權的影響 - 以美國法為中心，政治大學法律學研究所博士論文，2006 年 3 月。

17. 戴東盛，偵查程序中資料蒐集與利用之研究 - 以跟監為中心，中央警察大學警察政策研究所碩士論文，2011 年 6 月。

18. 蘇逸修，行動蒐證之研究，臺灣大學法律學研究所碩士論文，2003 年 6 月。

物聯網需要更好的安全性

IoT Needs Better Security

作者：Hemant Patel
CISM，ITIL，PMP，TOGAF
譯者：謝家蘭
國立政治大學會計學系教授

物聯網（IoT）是一個連接事物（固定或移動設備）的生態系統。依據 2016 年商業內幕報告 (Business Insider report) 推估，2015 年將有 100 億台設備連接到互聯網，2020 年則將達到 340 億台，其中物聯網設備占 240 億台，而傳統的計算設備（如智能手機、平板電腦、智能手錶）占 100 億台。而且，未來五年，全球將投入 6 萬億美元於物聯網解決方案。[1]

為什麼我們需要安全的物聯網？

產業快速變化之際，新的物聯網應用也愈趨成熟。物聯網系統中增加了越來越多的功能，以實現產品率先上市和功能的優勢。然而，物聯網系統設備的安全性，往往在設計過程中被忽略。從最近的駭客事件中可以明顯看出：

- 美國食品及藥物管理局針對心臟設備，提出對駭客威脅問題的安全建議，而聖猶達兒童研究醫院也因此修補了易受攻擊的醫療物聯網設備。[2]
- 駭客對特斯拉 Model S 汽車展開無線攻擊。[3]
- 研究人員駭入 Vizio 智能電視，進入到家庭網絡。[4]

在物聯網安裝和配置過程中也容易遺漏安全的考量。ForeScout 物聯網安全調查[5]指出：「最初認為他們的網絡上沒有物聯網設備的受訪者，實際上卻擁有 8 種物聯網設備類型（當被要求從設備列表中選擇時），而其中只有 44％的受訪者知道有關物聯網的安全政策。」此外，只有 30％的人相信自己確實了解物聯網在網路上的運作概念。[6]

這些駭客攻擊和 ForeScout 調查結果的影響顯示，物聯網安全必須全面實施，因此需要了解物聯網架構。

物聯網架構

Zachman Framework [7]解答了關於物聯網安全 why, how, what, who, where 和 when 的問題。Why 的物聯網安全問題已經在這裡得到解決，在四個“建築層次”中解釋了 how 以及 what 問題。圖 1 描述了透過 Zachman 框架回答 IoT 安全體系結構問題。

圖1-Zachman Framework
物聯網安全體系

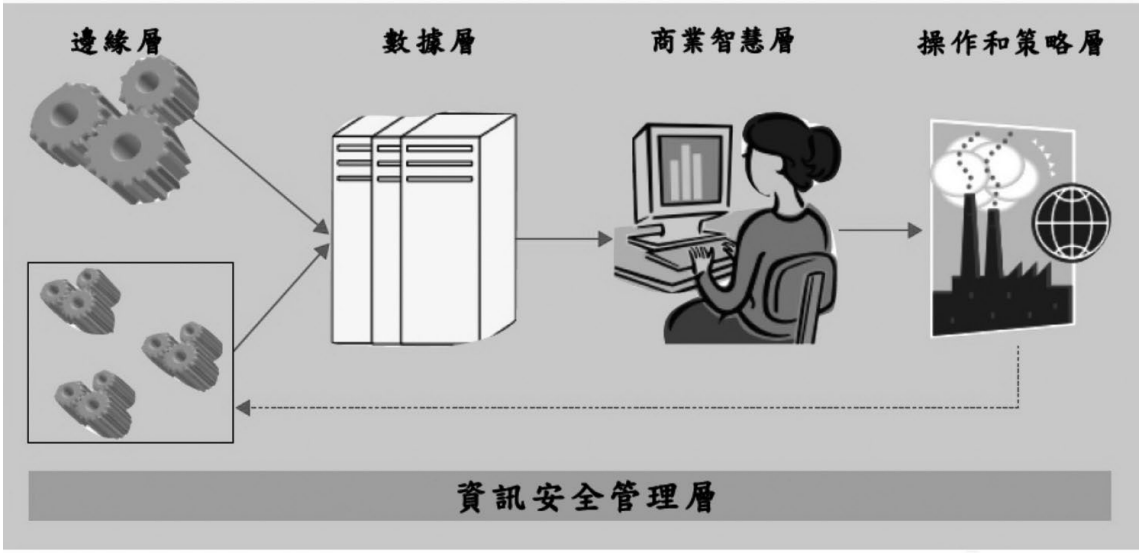
問題	物聯網安全
Why?	安全漏洞、建模的例子
How?	設備配置、整合、準則及流程
What?	其組成與關係列表
Who?	用戶、管理員、供應商、產業體系
Where?	架構中的每一層和組成
When?	設計,配置/實施和操作

Source: H. Patel. Reprinted with permission.

為了理解物聯網安全需求，我們需要對物聯網有較高階的概念。如圖 2 所示，資訊從邊緣層（即物聯網設備、組件 / 機器）流向數據層，接著再流向商業智慧（BI）層，最後再流向操作和策略（OpS）層，而各個設備及層次是由區域網路或寬頻網路所連接。許多設備通常會被分組，用途為組件或機器的組裝。設備之間的通訊不一定會出現在組件或機器中，設備和組件連接到集線器或網路，以封裝獨特的設備功能並實現更好的標準化和管理。

全面性安全 (Holistic security) 包含對每個層級的安全與對層級間的通訊安全。除邊緣層以外的層可以駐留在場所或雲端中，理解每個層次的安全需求非常重要。

圖二－物聯網架構



Source: H. Patel. Reprinted with permission.

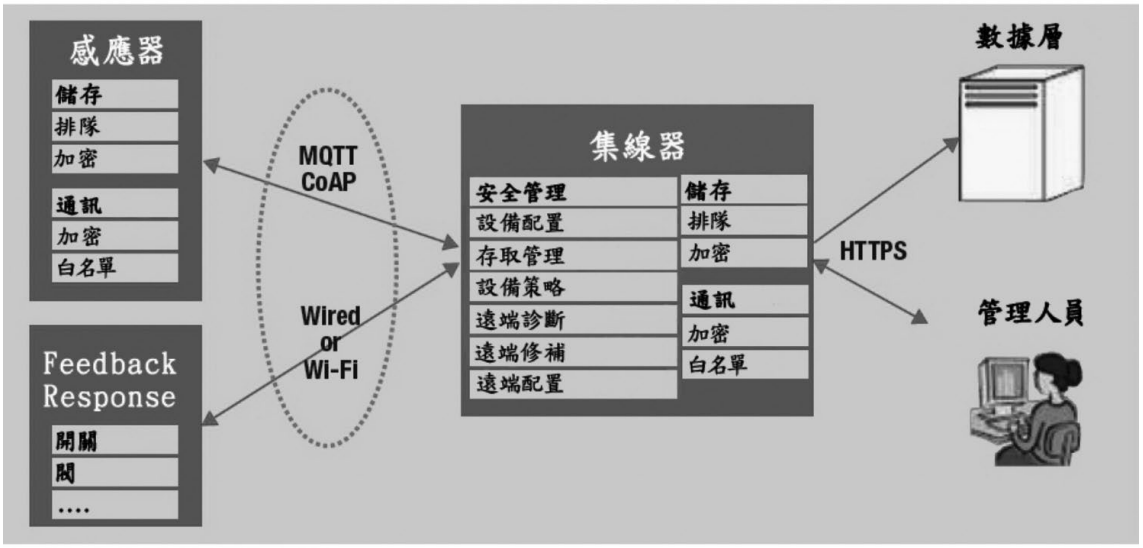
邊緣層安全性

物聯網安全應該成為資訊安全這個廣泛主題的一部分。邊緣層的設備 / 感應器產生的數據，是由物聯網體系結構的上游組件所處理，這些數據量遠遠超過互聯網用戶活動產生的數據量。

在設備的安全和物聯網集線器 / 網路管理軟件領域存在著巨大的競爭，並且存在大量的準則。Microsoft、IBM 和 Allegro 等公司對於高層次應用程式介面（API）及工具中，在設備為基礎封裝的安全性方面，表現突出。圖 3 描述了邊緣層安全架構的基本構建模塊：集線器或網路支持與物聯網安全相關的安全管理、存儲管理和通信組件。

> 全面性安全
> (Holistic security)
> 包含對每個層級的安全
> 與對層級間的通訊安全。

圖三-物聯網邊緣層安全架構



Source: H. Patel. Reprinted with permission.

設備可以與集線器互相連接或通訊，並且這種通訊軟體只需要較小的排隊能力。傳輸控制協議（ TCP）比較早被採用，緊接著有更好的協議，包括：

- 消息隊列遙測傳輸（MQTT）- 基於 TCP 的協議支持設備認證，安全套接字層（SSL）/ 傳輸層安全性（TLS）加密、排隊和訂閱功能。
- 約束應用協議（CoAP）- 基於用戶數據報協議（UDP）的傳輸，支援微型設備，且佔用空間小於 HTTP。它支援高級加密標準（AES）加密。[8]

無線區域網路 (WLAN) 被廣泛應用於許多使用 WPA 2 安全系統的領域中。而 Wi-Fi 系統由於缺乏安全性結構及時常使用安全性較弱之密碼，成為最常被駭客入侵之系統。一個通訊閘可以連接到多個集線器並提供較高層級的資料傳輸協議，例如：超文字傳輸安全協定 (HTTPS)，支援傳輸層安全性加密及表現層狀態轉換 (REST)- 簡單物件存取協定 (SOAP) 訊息。

裝置及集線器的賣家需要支援安全協定

及管理，正如文中所描述，賣家的支援可能因為多個不同的協議及不同的身分驗證方式而變得非常複雜。

另外一個需要被監督的事件是物聯網是否發生故障，故障發生的源頭可能是安全漏洞也有可能是其他原因。故障可能會引起裝置不停嘗試接觸資訊，結構並未限制重試的次數，可能有無數次的重試。由於每次的重試都會把一個錯誤訊息傳回集線器中，集線器可能會取得無數錯誤的訊息 (類似阻斷服務攻擊 [DDoS])，因此物聯網的集線器有可能會因為過大的負荷而無法正常運作，影響集線器的可用性。

故障有可能會使物聯網暫停產生資訊，使集線器無法接收任何資訊，並影響集線器之誠信。因此，裝置故障有可能會影響到物聯網安全性系統的可用性及誠信 (訊息的基本安全品質)。

資料層安全

資料層的活動包括數據接入、數據工程及使用結構化查詢語言 (SQL) 或傳統資料庫 NoSQL 科技數據轉換或大數據科技。SQL 資料庫提供資料列層級及單元性安全保護，較早之前的大數據科技提供資料夾及操作系統層級安全性保護，但是現時提供較低層級的安全性保護，例如 Apache Sentry[9]以角色為基礎的存取控制。

安全子層包括網路安全、授權與鑑定、資料倉儲與資料管理的產業標準加密。數據管理指示資料分開討論，包括企業數據建構、數據沿襲、審計與監管，低品質的數據建構及數據管理沿襲會犧牲掉資料的一致性與可用性。

為維持數據之保密性，系統監管、權限及轉置需要符合幾個產業的標準，例如美國健康保險便利和責任法案 (HIPAA) 及支付卡產業資料安全標準 (PCI DSS)。一篇 ISACA® 過去的文獻，「在裝置安全中回到未來：平衡 FIPPs 與積極管理物聯網保密和安全性風險」[10]，解釋物聯網各個部分處理數據過程中的保密性考量。

BI層級安全

資料遮罩、身分別授權與單一登入 (SSO) 提供此層級的安全性保護除了網路安全及防火牆。BI(預測的，規範的) 模型管理是資料監管的議題，此模型需要足夠的測試與認可。使用有缺陷的智能技術可能會因資料不足而影響企業的決定，並毀壞企業的名譽與信用。

資料外洩防護 (DLP) 與備用科技可提供額外的安全性保護。

OpS層級安全

反饋迴路可能會出現在裝置的運作系統中，傳統網路安全及防火牆、身分別授權，及 SSO 都在本層中提供安全性保護。

DevOps 工具可降低建構錯誤與疏失的風險，建構錯誤與疏失可能會影響到系統的可用性。

> 裝置故障會影響IoT(物聯網)安全的可用性與完整性(資訊安全的基本品質)。

策略會根據 BI 的結果決定一系列的動作。一個策略可能只是為了監察物聯網裝置中所接收的資訊，或包括處理物聯網裝置中所接收的資訊及根據有限度的資訊改變物聯網裝置，兩種策略 (需求與設計) 及反饋迴路 (執行) 均需被驗證 / 測試。

威脅管理與風險管理

圖 2 顯示反饋迴路的 OpS 層級至邊緣層級的架構。當缺少反饋迴路及裝置中的資料為非機密性時，在合理風險管理的情況下可降低接觸資料及資料加密的安全性保護。

風險緩和與反應策略可能會根據以下問題設計：

- 折衷性的裝置可使其他裝置與集線器共同協作嗎？
- 折衷性的裝置可以多快速的被察覺與被分離呢？
- 折衷性的裝置可帶來什麼影響？

> 物聯網安全並不只是裝置層級的安全性保護；它應該被應用到所有電子元件或物聯網的每個層級中。

這些問題並不是很全面，但應在設立風險管理指引時被考慮進去。

結論

在設計及執行物聯網系統時，對於物聯網的安全性往往缺乏優先考量。物聯網安全並不只是裝置層級的安全性保護；它應該被應用到所有電子元件或物聯網的每個層級中。安全性保護需要被應用在物聯網系統生命週期的每一個階段中，包含設計、安裝、結構及運作階段。

此外，增強密碼強度和金鑰認證、設計使人難以猜測的設備或主機名 / 身分標識、程式碼監管與分析、主動性的用戶及裝置管理，以及遵守產業指引或如美國國家標準暨技術研究院的安全建議，皆可補足物聯網的安全性。

原文出處：ISACA Journal 2017 volume 3 p. 27- 31

Endnotes

1. BI Intelligence, “Here’s How the Internet of Things Will Explode by 2020,” Business Insider, 31 August 2016, www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities- 2016- 2
2. Bacon, M.; “St. Jude Medical Finally Patches Vulnerable Medical IoT Devices,” TechTarget, 13 January 2017, http://searchsecurity.techtarget.com/news/ 450410935/St-Jude-Medical-finally-patches-vulnerable-medical-IoT-devices
3. Golson, J.; “Car Hackers Demonstrate Wireless Attack on Tesla Model S,” The Verge, 19 September 2016, www.theverge.

com/ 2016/ 9/ 19/ 12985120/tesla-model-s-hack-vulnerability-keen-labs

4. Zorz, Z.; "Researchers Hack Vizio Smart TVs to Access Home Network," Help Net Security, 12 November 2015, https://www.helpnetsecurity.com/ 2015/ 11/ 12/researcher-shack-vizio-smart-tvs-to-access-home-network/
5. ForeScout, IoT Security Survey Results, https://www.forescout.com/iot-security-survey-results/
6. Ibid.
7. Zachman, J.; "The Concise Definition of the Zachman Framework," Zachman International Enterprise Architecture, 2008, https://www.zachman.com/about-the-zachman-framework
8. Eclipse, MQTT and CoAP, IoT Protocols, www.eclipse.org/community/eclipse_newsletter/ 2014/february/article 2.php
9. Sentry, Apache Sentry, http://sentry.apache.org/
10. Rotman, D.; C. Kypreos; S. Pipes; "Back to the Future in Device Security: Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk," ISACA® Journal, vol. 6, 2015, https://www.isaca.org/Journal/archives

區塊鏈存證應用於司法數位證據之芻議

陳宏志
淡江大學產業經濟學系 兼任教師
hongzhi.mcu@gmail.com
鄒宗萱
資策會科技法律研究所創意智財中心 副主任
thtsou@iii.org.tw

前言

區塊鏈科技興起後，不限於加密貨幣，因其去中心化、可追蹤追溯、不易竄改等特性，應用在存證上，有助於提升農產品或相關生產履歷之信心。除了有形商品之存證，隨著科技的進步，因在司法訴訟中，越來越多的數位數據需要與紙本證據不同之作法。透過區塊鏈存證應用，不僅可協助檢核紙本轉數位之真偽，處理信任之議題，更可考量將日常業務或重要資訊直接存證於鏈上，節省成本及提升效率等。為解決此一需求，本文除簡介區塊鏈存證基本流程、以及應用於司法數位證據時可能遭遇之議題，如證據法則，更以美國、中國大陸法規及案例出發，希冀說明區塊鏈存證應用於司法數位證據將成為未來的趨勢，及企業可能因應與建議。

一、區塊鏈存證之基本流程

要達成區塊鏈存證應用，除分散式帳本、點對點傳輸、共識決等共通基礎技術一定必備外，相關系統至少還要能提供身分識別、資料加密、智能合約、資料查詢跟驗證等功能，以確保資料不被竄改、可供多方溝通或運用，甚至未來供對接司法機關等用途。基此，區塊鏈存證基本流程示意如下：

Step 1 檔案雜湊處理→	Step 2 存證上鏈→	Step 3 事後查證（取證）
（身分識別 / 資料加密）	（智能合約）	（資料查詢跟驗證）

在相關流程進行中，資料加密涉及演算法（Hash 值），可協助解決與原件相符之需求；而身分識別、資料查詢及驗證則係透過智能合約及公私鑰管理等，協助解決軟硬體與管理環境（用以生成、存儲、傳輸…）之可靠性，因上鏈後即可發揮區塊鏈不易竄改、可追蹤追溯之特色。具體說明如後[1]：

（一）檔案雜湊處理

1. 陳宏志（2020），〈企業營運資安難保萬一　區塊鏈存證有備無患〉，《網管人雜誌》，第 172 期，http://www.netadmin.com.tw/netadmin/zh-tw/magazine/-Viewpoint/78582583FE1744DDAA6034FFD1010359（最後瀏覽日：2020 年 7 月 22 日）。

1. 若將原始檔案完整上傳至區塊鏈備份，不僅耗費作業時間，也會造成區塊鏈資料庫與區塊鏈節點擁有者的龐大負荷。因此，可先規劃將鏈上存證的文件進行雜湊處理，而常見雜湊演算法有MD 5、SHA 256 等。
2. 雜湊處理用意在於幫檔案生成一串獨有的雜湊值，雜湊值可作為檔案的指紋，若檔案內容更動，雜湊值也會更動，不僅能作為檔案正確性的證明，也大幅降低檔案存證的空間與時間成本。

（二）存證上鏈

1. 為了將存證所需資訊統整，並保存於區塊鏈之中，企業或組織會需設計一份存證用智能合約（Smart Contract，又稱智慧合約），智能合約中會儲存相關資訊，如：存證說明、檔案雜湊值及存證時間戳。
2. 透過智能合約將上述資料備齊後，連同資料呼叫存證上鏈API，系統後台會依照智能合約範本，將資料填入範本中，完成合約上鏈所需的基本設定，最後將合約原始資料（Raw Data）傳送回存證端的裝置上。
3. 每個裝置會存有一份僅此一把的私鑰，該私鑰可用來證明裝置或裝置使用者在區塊鏈上的身份。以此一私鑰做簽章並在區塊鏈上完成的交易，可利用該私鑰來證明交易者的身份。
4. 此一系統在接到合約原始資料後，裝置使用私鑰對合約原始資料做交易簽章，並透過交易上鏈API 將交易上傳至區塊鏈上，等待交易被寫入區塊鏈。
5. 前述交易完成後，持續監聽交易紀錄的後台將捕捉到存證交易完成的紀錄，該監聽模組會負責將交易紀錄寫入資料庫中，記錄下交易地址，至此即完成存證上鏈部分。

（三）事後查證

1. 若事後有查證需求，需要查驗檔案，即可至資料庫中查詢該檔案的存證交易地址，利用交易地址可存取該存證合約中的內容，並確認當初對存證合約簽章的私鑰是誰所有，是否符合權限。
2. 存證步驟可依序參考如後：（a）首先確認簽署存證合約之人的身份；（b）取出該合約中所儲存的檔案雜湊值、存證描述與存證時間戳；（c）使用以上資訊與被查驗檔案做比較，確認檔案雜湊值與修改時間是否符合以上資訊。
3. 被查驗的檔案是否遭受過竄改，即可利用存證合約來進行確認，藉此達成存證需求。

二、區塊鏈存證應用在司法數位證據之議題

除了透過區塊鏈應用協助存證，如欲推展至司法領域，需符合電子簽章法或相

關法令外，能否落實此一應用的關鍵在於司法機關的認可。以我國民事訴訟為例，因常是私權糾紛，法諺有云：「舉證之所在、敗訴之所在」，故證據是訴訟程序內非常重要的關鍵。如依民事訴訟法第 222 條第 1 項前段，法院為判決時，應斟酌全辯論意旨及調查證據之結果，依自由心證判斷事實之真偽。法官要形成心證，多以證據協助判斷事實真偽之關鍵。爰規劃以區塊鏈應用協助存證等，不僅需符合技術或規格需求，更先要符合司法實務對數位證據之相關見解。

在刑事訴訟領域，採用監視錄影器、錄音檔案等數位證據更是常見。以最高法院 107 年台上字第 3724 號刑事判決為例，判決書內提及：... 一般而言，數位證據具無限複製性、複製具無差異性、增刪修改具無痕跡性、製作人具不易確定性、內容非屬人類感官可直接理解（即須透過電腦設備呈現內容）。因有上開特性，數位證據之複製品與原件具真實性及同一性，有相同之效果，惟複製過程仍屬人為操作，且因複製之無差異性與無痕跡性，不能免於作偽、變造，原則上欲以之證明某待證事項，須提出原件供調查，或雖提出複製品，當事人不爭執或經與原件核對證明相符者，得作為證據。

然如原件滅失或提出困難，當事人對複製品之真實性有爭執時，非當然排除其證據能力。此時法院應審查證據取得之過程是否合法（即通過「證據使用禁止」之要求），及勘驗或鑑定複製品，苟未經過人為作偽、變造，該複製品即係原件內容之重現，並未摻雜任何人之作用，致影響內容所顯現之真實性，如經合法調查，自有證據能力。至於能否藉由該複製品，證明確有與其具備同一性之原件存在，並作為被告有無犯罪事實之判斷依據，則屬證據證明力之問題。

三、司法數位證據應符合訴訟之證據法則：中美案例分析

區塊鏈存證如欲運用於司法領域，關鍵在於應符合既有法令暨需求，如證據法則，再來才會討論技術實質內容，如時戳、簽章或憑證。因數位證據（泛指非紙本文件之內容）在存證之應用，其主要目的如同紙本文件希望透過公證取得一定之效力。除依我國司法實務之見解外，數位證據能否作為法院在訴訟案件內所採認之證據，及需要具備那些要件…（包含但不限於區塊鏈之應用），先以美國及中國大陸之實踐為例，說明如下：

（一）美國佛蒙特州

該州就區塊鏈科技應用作為法院程序（Title 12：Court Procedure）之證據訂有相關規範[2]。其在審判進行（Chapter 081：Conduct Of Trial）的規定內，認為區塊鏈之應用作為證據時，除有已宣誓之適格證人外，還需要有下列 4 要件，始能符合該州證據法則（Vermont Rule of Evidence 902）：

1. 存證時間（the date and time the record entered the blockchain），係指如於鏈上完成

2. 美國佛蒙特州法規查詢（The Vermont Statutes Online）https://legislature.vermont.gov/statutes/section/12/081/01913（最後瀏覽日：2020 年 7 月 22 日）。

交易之日期與時間。

2. 上鏈時間（the date and time the record was received from the blockchain），係指該交易紀錄達成共識後出塊之日期與時間。
3. 紀錄保存（the record was maintained in the blockchain as a regular conducted activity），係指該紀錄被保存在區塊鏈上，且因不斷出塊之設計，而具不易竄改、可追蹤追溯等特色。
4. 持續運作（the record was made by the regularly conducted activity as a regular practice），係指區塊鏈依原本設計之架構，持續於一定期間內達成共識並出塊的機制運作無礙。

而符合上開要件之證據，可用以推定以下事項：

1. 透過有效之區塊鏈應用，其驗證的事實或紀錄為真。
2. 透過區塊鏈應用建立事實或紀錄之日期和時間，即為該事實或紀錄上鏈之日期和時間。
3. 透過區塊鏈應用而取得紀錄者，即為本人。
4. 若法院或對照之當事人同意驗證區塊鏈紀錄之格式或方式等，則應以該特定格式或方式向法院證明符合本條規定之區塊鏈紀錄，且已獲得他方同意。

（二）中國大陸

中國大陸民間投入區塊鏈甚早，如ICO在2016至2017年間蔚為風潮，但也因此產生許多詐騙等不法情事。其主管機關意識到區塊鏈之重要性後，除2017年9月間由人民銀行等七單位聯名發布公告禁止不法ICO[3]外，也正視其影響力並透過官方的能量，投入區塊鏈應用等，如工信部於2018年5月發布「2018中國區塊鏈產業白皮書」[4]，內容除金融領域外，還包含徵信、大數據分析、資料市集、著作權存證等應用。

其中在司法領域部分，存證應用等也有初步成果，如民間在2019年4月發布「區塊鏈法規合規白皮書」[5]外，同年6月中國大陸最高人民法院資訊中心也發布「區塊鏈司法存證應用白皮書」[6]。因相關應用更涉及到電子證據相關，主要以最高人民法院於2019年10月14日公布修正之「最高人民法院關於民事訴訟證據的若干規定」為主，並自2020年5月

3. 陳宏志（2017），〈中國大陸、香港陸續發布對首次代幣發行（ICO）之相關規範〉，《科技法律透析》，29卷11期，頁9-10。
4. 中國大陸工業和信息化部（2018），《2018年中國區塊鏈產業白皮書》，http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf（最後瀏覽日：2020年7月22日）。
5. 深圳壹帳通智能科技有限公司（2019），《區塊鏈法律合規白皮書》，https://www.ocft.com/pdf/01.pdf（最後瀏覽日：2020年7月22日）。
6. 中國信息通信研究院（2019），《區塊鏈司法存證應用白皮書》，http://www.caict.ac.cn/kxyj/qwfb/bps/201906/P020190614499397999292.pdf（最後瀏覽日：2020年7月22日）。

1 日起施行[7]，調整許多涉及電子證據之規範，如第 14 條例示電子證據的規定、第 15 及 23 條提出及保全電子證據原件之要求、第 93 條採認電子證據考量因素等。

更重要的是，杭州互聯網法院已於 2018 年做出號稱是第一個區塊鏈存證的相關判決[8]：2018 浙 0192 民初 81 號民事判決（案件編號 055078），案由為杭州華泰一媒文化傳媒有限公司訴深圳市道同科技發展有限公司侵害作品資訊網路傳播權糾紛。

本案最後判決為被告賠償原告人民幣 4,000 元定讞，就杭州互聯網法院裁判觀之，關鍵在於華泰公司（原告）將網頁截圖、源碼資訊轉成 Hash 值後，並上傳至 Factom 區塊鏈，有助於確保真實性。綜合觀之，中國大陸因電子證據在科技應用上並不一定限於區塊鏈，參照「最高人民法院關於民事訴訟證據的若干規定」之精神，只要能證明該證據之生成、存儲、傳輸等所依據的軟硬體完整、可靠，可供監測、核查，以及能完整地被保存、傳輸等（該規定第 93 條參照），都可協助判斷其真實性。

四、結語

觀察美國或中國大陸之司法實務後，兩國對於數位或電子證據之認定，無論是否運用區塊鏈科技，核心均在於如何證明與原件相符（真實性），以及軟硬體與管理環境（用以生成、存儲、傳輸…）之可靠性等。除符合訴訟法之證據法則外，從技術面觀之，存證應用需至少提供身分識別、資料加密、智能合約、資料查詢跟驗證之功能。

以中國大陸系爭案件運用之 Factom 區塊鏈[9]為例，該公司在 2014 年成立於美國德州，以去中心化方式結合開源軟體，運用區塊鏈提供企業記錄與管理文件或資訊，並開發相關應用程式，如存證及取證、數位身分識別、公證、代幣化、監測、法令遵循及分散式資料存儲等功能。以存證為例，該公司係透過對應身分之憑證（API key），結合權限設計，以證明時間及狀態。至於公證則是發揮區塊鏈特色，越多人使用就越不容易竄改。

另在我國，如區塊科技之存證王 APP 亦提供存證相關服務。該 APP 可就數位證據（如照片、影音檔案），加上檔案產生時的時間戳與產生地點 GPS 訊息，檔案生成 Hash 值後，上傳至區塊鏈（先上傳至私鏈 Chromaway，累積 1, 000 筆交易後再上傳至以太鏈備份）中進行存證[10]。

惟需要進一步探討的是，由於區塊鏈應用的本質為去中心化之設計，利用分散式

7. 中國大陸最高人民法院（2019），《最高人民法院關於民事訴訟證據的若干規定》，http://www.court.gov.cn/fabu-xiangqing-212721.html（最後瀏覽日：2020 年 7 月 22 日）。
8. 杭州互聯網法院訴訟平台，案件查詢，https://www.netcourt.gov.cn/#lassen/search（最後瀏覽日：2020 年 7 月 22 日）。
9. Fatcom 公司網站，https://www.factom.com/（最後瀏覽日：2020 年 7 月 22 日）。
10. 區塊鏈存證王，https://app.chainsecurity.asia/blockchainwitness/web/index.html（最後瀏覽日：2020 年 7 月 22 日）。

帳本等作為提供服務的基礎。倘信任該應用所生的結果，如存證，在符合前述美國或中國大陸之證據法則下，理應符合證據能力及證明力之需求，用何種技術反而不是重點，如是否使用 Factom 或其他區塊鏈進行存證。此外，數位證據若涉及電子文件，在我國還可能有電子簽章法相關議題，如該存證屬電子簽章或數位簽章，或是否需要憑證機構、憑證實務作業基準等。基此，要落實區塊鏈之存證應用，對應之法制也會需要調整。

綜上所述，企業或組織透過區塊鏈應用如存證來保護內部資料，在技術上並非難事，系統設計只要符合前述規格，應可初步符合需求。但實務上常遭遇企業資料或營業祕密外洩的風險，對造或合作對象等會要求提供資料來源證明。更重要的是，當發生糾紛的時候，法院也會要求證明資料之真實性。在未修法或導入科技應用之情形下，目前大多只能透過提供大量書面資料等作為佐證，但常被質疑證明是否為真，花費攻防雙方極大心力。如採逐案公證，成本亦極高。

為促進信任、降低成本或提升效率，透過區塊鏈技術不易竄改、安全等特性幫助廠商存證，或許是解決方式之一，惟關鍵是讓法院認可新科技的解決方案。未來除推動研擬如美國、中國大陸之法令，在我國可能是民事或刑事訴訟法、電子簽章法等，並可提修配套法規，規範數位證據之證據法則外，區塊鏈存證系統或功能之規劃，可依法規需求與區塊鏈技術特性，將企業內部日常業務之機密或必要資訊，定期且自動存證於鏈上。發生爭議或需要訴訟時，更可讓法院等直接採認，確實發揮科技應用的效益。

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 月由張紹斌接任第十三屆理事長。副理事長由蒲樹盛擔任。秘書長由黃涼澤續任

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。

January-June 2020
Certification Exam Passers

ISACA Taiwan Chapter

	Exam Type	ID No.	Name	Top 3
1	CISA	796204	Shih-Fang Lee	No.3
2	CISA	994632	Kwan Kit Ben Teo	
3	CISA	1225290	Ya-Chih Huang	
4	CISA	1226215	Yu-Lin Lyu	No.2
5	CISA	1237310	Yung-Jan Yang	
6	CISA	1250457	Jung-Piao Wang	
7	CISA	1281848	Min-Hsuan Chiu	
8	CISA	1287180	Jiannjyh Shen	No.1
1	CISM	1062593	Chien-Yu Chen	
2	CISM	1187298	Johnson Liu	
3	CISM	1257661	Shu-Ying Lee	No.1
4	CISM	1262175	Yu-Hao Hsieh	No.3
5	CISM	1270558	Ching-Wei Chien	
6	CISM	1278041	Chih-Cheng Chen	No.2

※ 以上資料來源： ISACA總會202007更新。

2020 年度下半年教育訓練課程列表

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	**9/17-18, 23-25**	NT$ 30,000
	CISA 國際電腦稽核師認證研習班_平日班 (與全智網合辦，上課地點：全智網)	30	**12/14-18**	NT$ 30,000
	CISA 國際電腦稽核師認證研習班_假日班 (與全智網合辦，上課地點：全智網)	30	**11/21, 22, 28, 29, 12/6**	NT$ 30,000
	CISM 國際資訊安全經理人認證研習班_平日班 (與全智網合辦，上課地點：全智網)	24	**11/24-27**	NT$ 24,000
	CISM 國際資訊安全經理人認證研習班_假日班 (與全智網合辦，上課地點：全智網)	24	**9/5, 12, 19, 26** **12/5, 12, 19, 26**	NT$ 24,000
	CISM 國際資訊安全經理人認證研習班_假日班 (與金融研訓院合辦，上課地點：研訓院)	24	**10/17, 24, 31, 11/7**	NT$ 24,000
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	40	**10/12-16、11/9-13、12/7-8, 14-16**	NT$ 53,000
	ISO 27001:2013 資訊安全管理系統 建置實務課程	24	**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	40	**11/30-12/4**	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	**10/6-7**	NT$ 22,000
	ISO 22301:2019 營運持續管理系統 CQI & IRCA 主導稽核員訓練課程	40	**12/7-11**	NT$ 55,000
	ISO 22301:2019 營運持續管理系統 轉版課程	8	**10/22**	NT$ 11,000
	ISO 22301:2019 營運持續管理系統 基礎課程	16	**12/2-3**	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	**12/14-18**	NT$ 55,000
	ISO/IEC 29100:2011+A1:2018(CNS 29100)隱私框架 國際標準基礎課程	8	**10/23**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準基礎課程	8	**11/23**	NT$ 8,000
	BS 10012:2009 個人資訊管理系統 國際標準建置課程	16	**12/14-15**	NT$ 15,000
內稽系列	內部稽核實作基礎班**(初任課程)**	12	**11/16-17**	NT$ 6,600
	NEW!查核人資假勤及薪資管理分析報表實作	7	**9/29**	NT$ 3,850
	NEW!利用資料庫(Database)以樞紐分析飆速編製損益表	7	**10/26**	NT$ 3,850
	NEW!範例設計五大組成要素之自行評估問卷	7	**12/9**	NT$ 3,850
	NEW!應用商業簡報視覺化技巧呈現經營分析與稽核報告	7	**12/16**	NT$ 3,850
	內部稽核有效應用財務報表實務**(初任課程)**★	6	**10/20**	NT$ 3,300
	內部稽核「工作達標」有效作法	6	**10/27**	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	**12/4**	NT$ 3,300
	內部稽核「協助組織達標」有效作法★	6	**12/8**	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	CISSP 認證研習課程－實體課程 (與全智網合辦，上課地點：全智網)	40	平日：**9/11, 17, 18, 24, 25** **11/5, 6, 12, 13, 20** 假日：**11/7, 14, 21, 28, 12/5**	NT$ 32,900
	CISSP 認證研習課程－線上課程 (與全智網合辦，上課地點：全智網)	40	平日：**9/11, 17, 18, 24, 25** **11/5, 6, 12, 13, 20** 假日：**11/7, 14, 21, 28, 12/5**	NT$ 29,900
	NEW!核決權限制定原則與執行稽核風險管控機制	7	**11/30**	NT$ 3,850
	有效成本管控設計與分析★	6	**9/11**	NT$ 3,300
	電腦稽核起手式(初任課程) ★	6	**9/15**	NT$ 3,300
	作業系統與通信傳輸查核★	6	**10/6**	NT$ 3,300
	應用系統導入 PKI 安全機制與檢查	6	**10/7**	NT$ 3,300
	數位時代電腦稽核實務(初任課程) ★	6	**10/13**	NT$ 3,300
	ERP 系統控管與查核實務★	6	**10/16**	NT$ 3,300
	稽核分析在銷售收款循環稽核個案演練 (Arbutus 操作)	6	**10/22**	NT$ 3,300
	談資安事件應變機制及稽核重點★	6	**10/23**	NT$ 3,300
	稽核分析在採購付款循環稽核個案演練 (Arbutus 操作)	6	**11/5**	NT$ 3,300
	網路與系統安全實務查核★	6	**11/12**	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★	6	**11/19**	NT$ 3,300
	資訊部門稽核與資訊系統控制查核★	6	**11/26**	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	**12/1**	NT$ 3,300
舞弊稽核與數位鑑識系列	NEW!企業舞弊最常使用在採購作業範例解析	7	**9/22**	NT$ 3,850
	NEW!企業舞弊最常使用在銷售作業範例解析	7	**10/19**	NT$ 3,850
	NEW!查核資料庫(Database)舞弊造假資料匯集案例實作班	7	**11/23**	NT$ 3,850
	利用數位鑑識分析人員不當行為	6	**9/30**	NT$ 3,300
	資安持續稽核與監控：組態安全管理之應用★	6	**10/15**	NT$ 3,300
	資料導向的舞弊偵測與查核實務	6	**10/21**	NT$ 3,300
	資安事件與資料外洩調查實務分享★	6	**10/30**	NT$ 3,300
	認識數位鑑識技術基礎與實務	6	**11/6**	NT$ 3,300
	結合系統資料與網路資源透析潛在舞弊事件	6	**11/20**	NT$ 3,300
	內部稽核舞弊偵查應用技巧實作(初任課程) ★	6	**11/25**	NT$ 3,300
	應用鑑識資料分析(FDA)技術查核財務舞弊★	6	**11/27**	NT$ 3,300
	數位證據與實例分享★	6	**12/2**	NT$ 3,300
個資外洩與保護系列	資料庫稽核與個資保護★	6	**10/29**	NT$ 3,300
	個人資料保護稽核★	6	**12/18**	NT$ 3,300
數位金融與電子支付系列	以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循 (與 BSI 合辦)	8	**12/15**	NT$ 8,000

※ 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。
※ 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

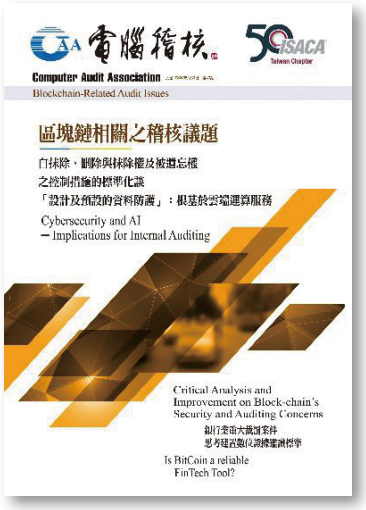
※ 歡迎企業包班，為您量身訂做所需課程。
※ 詳細課程規劃請上本會網站 www.caa.org.tw 查詢，或來電(02)2528-8875 洽詢。

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

第四十期_區塊鏈相關之稽核議題



- 區塊鏈如何影響會計與審計
- 自抹除、刪除與抹除權及被遺忘權之控制措施的標準化談「設計及預設的資料防護」：根基於雲端運算服務
- Cybersecurity and AI — Implications for Internal Auditing
- Critical Analysis and Improvement on Block-chain’s Security and Auditing Concerns
- 銀行業重大裁罰案件思考建置數位證據鑑識標準
- Is BitCoin a reliable FinTech Tool ？

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

ISACA摘譯期刊近期篇名整理

第22期

- ◆ 企業大數據之審計
  Auditing Big Data in Enterprises
- ◆ 運用人工智慧於應用程序安全
  Applying AI in Application Security
- ◆ 機器學習稽核 —CRISP-DM 架構
  The Machine Learning Audit— CRISP-DM Framework
- ◆ 信息與通信審計之革新
  Innovation in the IT Audit Process
- ◆ 資料隱私稽核
  Auditing Data Privacy
- ◆ 區塊鏈技術的諾言和危險
  The Promises and Jeopardies of Blockchain Technology

第23期

- ◆ 從精算師及風險管理觀點探討數據治理
  Data Governance From the Actuary and Risk Management Perspectives
- ◆ 我們為何失敗了
  Why We Failed
- ◆ 如何查核物聯網
  Auditing the IoT
- ◆ 區塊鏈在審計行業的影響
  Impacts of Blockchain on the Auditing Profession
- ◆ 比特幣對企業的推波助瀾
  Bitcoin Boosting Businesses

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

2020.05.08

【2020 全國大專院校電腦稽核個案線上競賽暨專題研討會 】

◆全國電腦稽核個案線上競賽 -(左起) 勤業眾信聯合會計師事務所侯玉燁副總、中華民國電腦稽核協會黃淙澤秘書長、兆益數位股份有限公司莊盛祺總經理、台北商業大學會計資訊系林維衍主任、安侯建業聯合會計師事務所陳怡如副總、安永聯合會計師事務所蕭嘉慧資深經理、財團法人國家實驗研究院稽核室陳政龍正工程師、台北商業大學會計資訊系李興漢教授

「全國大專院校電腦稽核個案線上競賽暨專題研討會 」為國立台北商業大學所主辦的活動，期望透過個案競賽與專題研討的激盪交流，提升學生電腦稽核分析、獨立思考、團隊合作之能力，並為數位時代培育數位會計人才。

本屆競賽由台灣證券交易所、四大會計師事務所（安永聯合會計師事務所、安侯建業聯合會計師事務所、資誠聯合會計師事務所、勤業眾信聯合會計師事務所 ）及兆益數位股份有限公司贊助經費。四大會計師事務所及審計部派出督導員蒞各校督導。協辦單位包括會計師公會全國聯合會、中華民國內部稽核協會、中華民國電腦稽核協會。

2020.05.27

【 第三方風險管理白皮書研討會暨第 11 屆北區會員代表選舉 】

今年這場突如其來的疫情，對企業在第三方廠商高度關聯的供應斷鏈議題造成全球性的影響，也讓企業重新審思產業佈局與風險評估方法。而 ISACA 在去年所發佈的「第三方風險管理 」白皮書，正好對這方面進行了全面的分析。該白皮書提供關於治理問題的最佳實踐方法、並將第三方風險評估的形式，整合至風險分析流程中；除此之外，也包含了必要的控制措施，對企業應該如何進行提供了更深入的見解。藉此白皮書的內容，可協助企業改進第三方風險管理計劃，並採取適當作為以避免潛在的第三方違約或企業持續營運風險。本協會為讓各界先進瞭解此白皮書內容，特地將白皮書翻譯成中文版、與此同時也邀請業界專家於研討會上為大家進行精采的導讀與介紹。目前會上的白皮書中文版及導讀資料都已在官網下載區開放給會員進行下載。

◆第三方風險白皮書研討會 -(左起) 安永聯合會計事務所黃誌緯資深經理、勤業眾信聯合會計師事務所陳鴻棋協理、財團法人國家實驗研究院稽核室陳政龍正工程師、中華民國電腦稽核協會張紹斌理事長、兆益數位股份有限公司莊盛祺總經理、安侯建業聯合會計師事務所副總經理

2020.05.28

【「 SAP ERP 稽核實務 」例會專題演講暨第 11 屆南區會員代表選舉 】

SAP 系統身為當前最具影響力的企業管理系統，被廣泛地應用在各行各業。為了讓大家能夠對這個系統更加了解，此次例會邀請勤業眾信聯合會計事務所 - 風險諮詢服務部沈政鴻經理，以「 SAP ERP 稽核實務 」為主題，對 SAP 系統進行詳盡的介紹、內容包含：權限架構、特權帳號管理、程式安全管理、資料表管理、變更管理。期望能給予學員更多幫助與指引，讓與會學員將來也能學以致用。

◆ SAP ERP 稽核實務專題演講 - 勤業眾信聯合會計師事務所沈政鴻經理

2020.06.16

6 月新竹例會

【 連網設備的資安風險與信任管理策略 】

在科技日新月異的發展下，非傳統裝置、作業系統數量及多樣性也呈現爆炸性的成長，過往的安全防護已不適用於目前現況，且在資安的世界裡，所有的狀態不是靜止的，唯有持續性監控才能掌握風險。

◆連網設備的資安風險與信任管理策略專題演講 - 美商 Forescout Technology 張恩綾總經理

本次新竹例會邀請到美商 Forescout Technology 張恩綾總經理，以「 連網設備的資安風險與信任管理策略 」為主題，針對如何持續性監控風險範例進行講解。根據新加坡網路安全局的建議，重要資安單位、監督單位以及歐美資安規範與資安框架的基本要求為「 可視可控 」，因此對 IoT 設備從設備用途、本身安全性到使用者，都應有更深更廣的了解，唯有全面了解網路中所有的設備裝置，才能更有效的掌控並降低網路和操作風險。

2020.06.30

6 月台北例會

【 一場無聲的網路戰爭 】

「 星星之火，可以燎原 」，一個小小的資安漏洞，就有可能導致整個企業運作面臨停擺甚至造成巨大的損失。近年商業詐騙事件層出不窮，手法也更加多變，例如：駭客透過假冒的名稱，佯裝成廠商向企業進行匯款帳戶更改、追討貨款，或者是聲稱自己已滲透企業網路，掌握大量客戶資料，威脅要求支付鉅額款項，更甚者直接佯裝成企業老闆，發送夾帶病毒的郵件給員工。在這樣的情況下，事前做好預防是非常重要的一環。

◆一場無聲的網路戰爭專題演講 - 安侯企業管理股份有限公司林大馗副總經理

本次例會邀請到安侯企業管理股份有限公司林大馗副總經理進行專題演講，以「 勒索軟體 」及「 BEC 商務電子郵件入侵 (變臉詐騙) 」為主題，提出案例並由手法分析開始講解，讓學員了解平時應注意的事項及如何預防破壞性攻擊，達到更好的自我保護效果。

ISACA®

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

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
www.caa.org.tw Web : www.isaca.org.tw