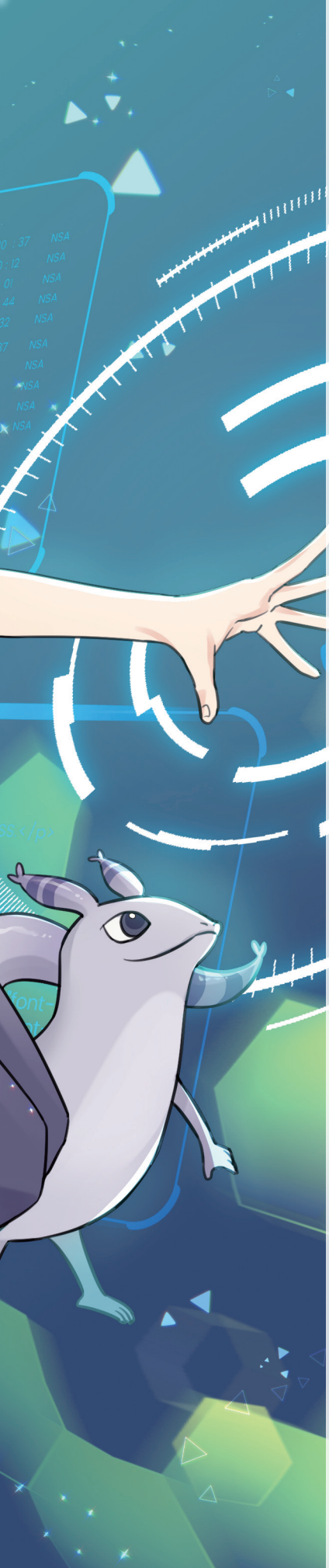

資訊
科技篇



一起來學習資訊科技

資訊科技教科書是依據科技領域的課程綱要，進行各章節內容的編寫與規劃。同時兼顧資訊科技潮流與未來發展趨勢，培養學生與時俱進的資訊科技基本能力，成為主動、積極且負責任的數位公民。課本的規劃以「終極任務」作為問題解決主軸，強調培養學生利用資訊科技與運算思維解決問題之能力。課本從國中一年級到三年級涵蓋資訊科技學習內容的六個主題：「演算法」、「程式設計」、「系統平臺」、「資料表示、處理及分析」、「資訊科技應用」以及「資訊科技與人類社會」。

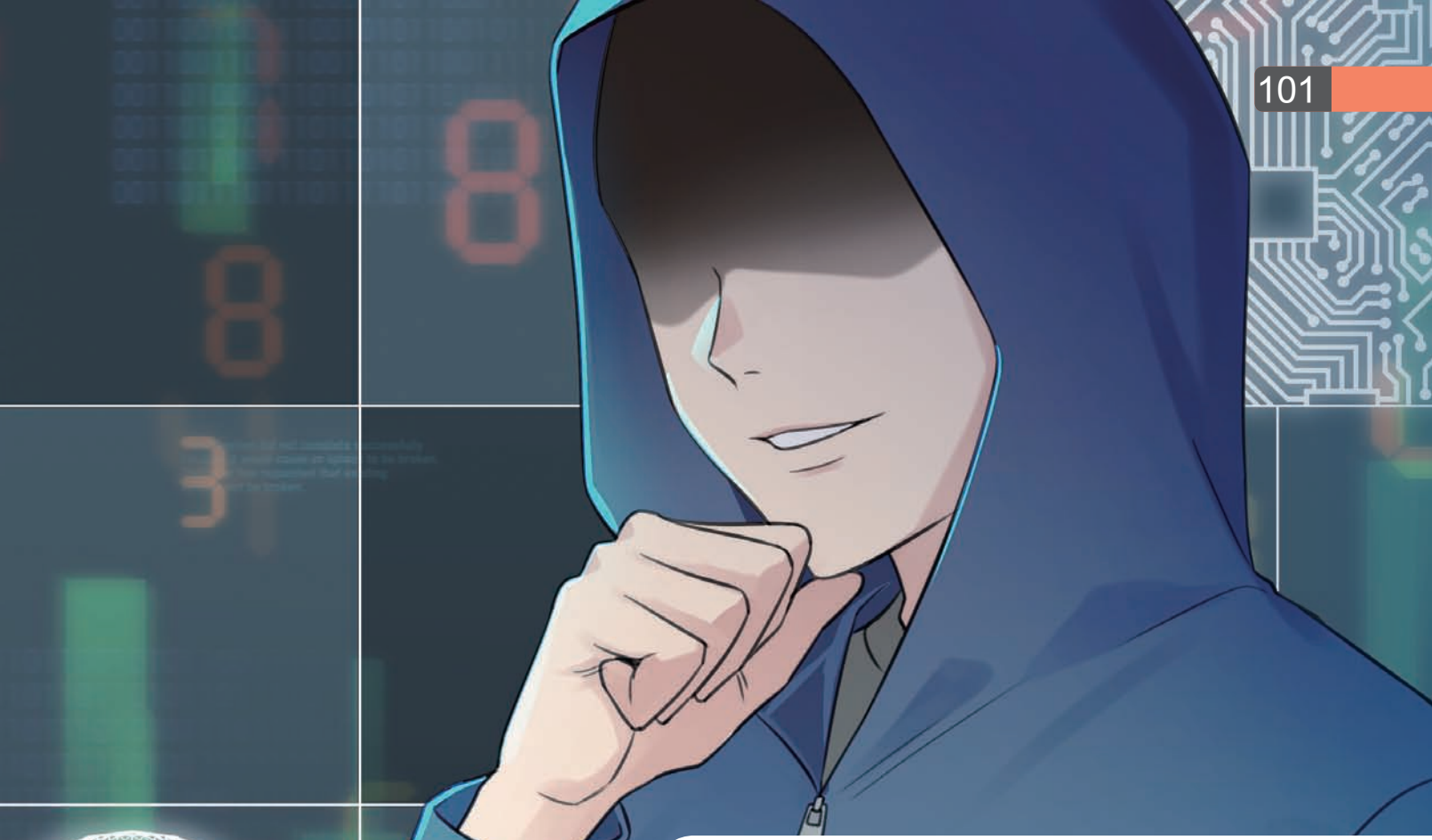
資訊科技之課程設計以運算思維為主軸，透過電腦科學相關知能的學習，培養學生邏輯思考、系統化思考等運算思維，並藉由資訊科技之設計與實作，增進運算思維的應用能力、問題解決能力、團隊合作以及創新思考。強調軟體的整合應用，輔以實作的概念與原則，解決問題或表達想法。

資訊科技之「演算法」與「程式設計」教學，運用「演算法」分析問題、設計問題解決方法，兼以「程式設計」實踐問題解決之程序，兩者環環相扣。學校可根據軟硬體設備或採用自由軟體進行教學。操作技能方面之評量在各章結束時規劃實作練習，可增加對該技能的熟練度。

CHAPTER 1

資訊科技對我們的影響

資訊科技發達的時代，因為資訊科技的輔助讓我們享受更便利的生活。然而，資訊科技帶來便利的同時，也伴隨著許多我們應該注意的資訊安全風險，面對這些風險我們應該如何預防與解決呢？本章將帶領你認識資訊安全風險與防護，並探討社會層面的相關議題。



概念內容

- 了解資訊科技發展對生活產生的影響。
- 了解資訊安全的意涵以及原則。
- 認識影響資訊安全的各種因素。

能力表現

- 能使用正確的工具，適時地讓生活更加便利。
- 能發現並思考隱藏在事物背後的另一層意涵。
- 能查詢辨別接受到的資訊真偽。

1 **資訊科技帶來的便利與資安防護** P.102

1-1 認識資訊安全
1-2 使用電腦與網路的資安防護
1-3 個人數位金融安全防護
1-4 智慧型裝置的資安防護

2 **資訊科技對社會的影響** P.116

2-1 數位資料與資安管理
2-2 社會秩序與隱私安全
2-3 人工智慧與未來挑戰

第 1 節

資訊科技帶來的便利與資安防護

隨著資訊科技發展，人們的許多生活方式也跟著改變。然而資訊科技對個人的影響除了帶來便利外，也產生許多個資安全防護議題。

1-1 認識資訊安全

資訊安全是指保護電腦系統、網路、軟體和資料不受未經授權的存取、損壞或洩漏的措施和方法。當我們享受著資訊科技發展所帶來的便利時，如果沒有良好的安全防護習慣，可能會導致個人資訊受到披露、盜用或是毀損，產生資訊安全風險。

廣泛的資訊安全定義是指資訊的**機密性**（Confidentiality）、**完整性**（Integrity）與**可用性**（Availability），**簡稱 CIA** 。

機密性

只有通過認證的人才能夠訪問和查看資料，避免資料被隨意存取或使用。

舉例：使用電腦時，密碼貼在桌上讓其他人看到了，違反機密性。

完整性

只有獲得授權的人可以修改資料內容，避免資料被隨意竄改或破壞。

舉例：電腦中毒，檔案遭到駭客竄改，違反完整性。

可用性

在需要時能夠存取和使用資料，避免資料無法取得或失效。

舉例：隨身碟壞掉了無法存取資料，違反可用性。

圖 1-1 資訊安全三原則

CIA 三原則需要同時運作！

1-2 使用電腦與網路的資安防護

現代生活裡，電腦和網路已經成為我們生活中不可或缺的一部分，從協助學習到提供休閒娛樂，數位化的轉變已經深刻的改變了我們的生活方式。透過網路的無遠弗屆，我們可以輕鬆地獲取資料、與人聯繫，並進行許多日常活動。

圖 1-2 電腦與網路服務應用

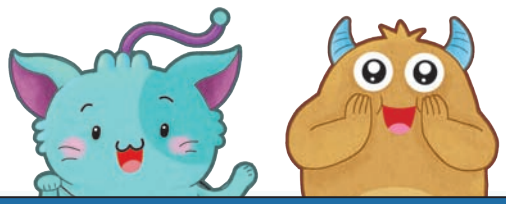
1. 資料搜尋：透過網路快速地搜尋到需要的資訊。
2. 完成作業：透過電腦軟體製作專題，可以提高效率及節省時間。
3. 檔案儲存：不受空間限制，備份、管理和尋找特定資料變得更加容易。
4. 調劑身心：線上遊戲、手機遊戲的蓬勃發展提供了更多元的娛樂方式。
5. 影音娛樂：串流媒體服務改變了人們觀看和聆聽多媒體內容的方式。
6. 豐富生活：多元的互動平臺提供了人們分享生活中的各種經驗，促進更多交流。
7. 網路購物：提供更多選擇及更簡便的購物體驗。
8. 線上學習：線上學習平臺帶來了新的學習方式和教育模式。

當我們透過電腦網路享受這些輔助學習與休閒娛樂便利時，許多個人資訊也以數位化形式，存放在方便攜帶的隨身儲存媒體（例如：隨身碟、外接硬碟）、電腦與網路平臺之中，因此衍生相關的資訊安全案例也時有所聞，例如：隨身儲存媒體保管不當遺失、各種網站平臺帳號遭到盜用或是電腦受到病毒感染等，都可能使個人隱私資料受到披露、盜用或毀損而造成損失。

1 運用公共電腦登入系統時，應避免「記憶密碼」，並在使用完畢後登出系統。

2 不隨意下載不明來源之檔案。

仰賴電腦與網路帶來的便利生活時，應該時刻提醒自己養成良好的資訊安全態度，以避免資訊安全風險。檢視自己是不是每次都有做到以下事項：



3 應定期檢查電腦更新，並安裝更新檔。

4 應安裝防毒軟體，並定時更新防毒版本。

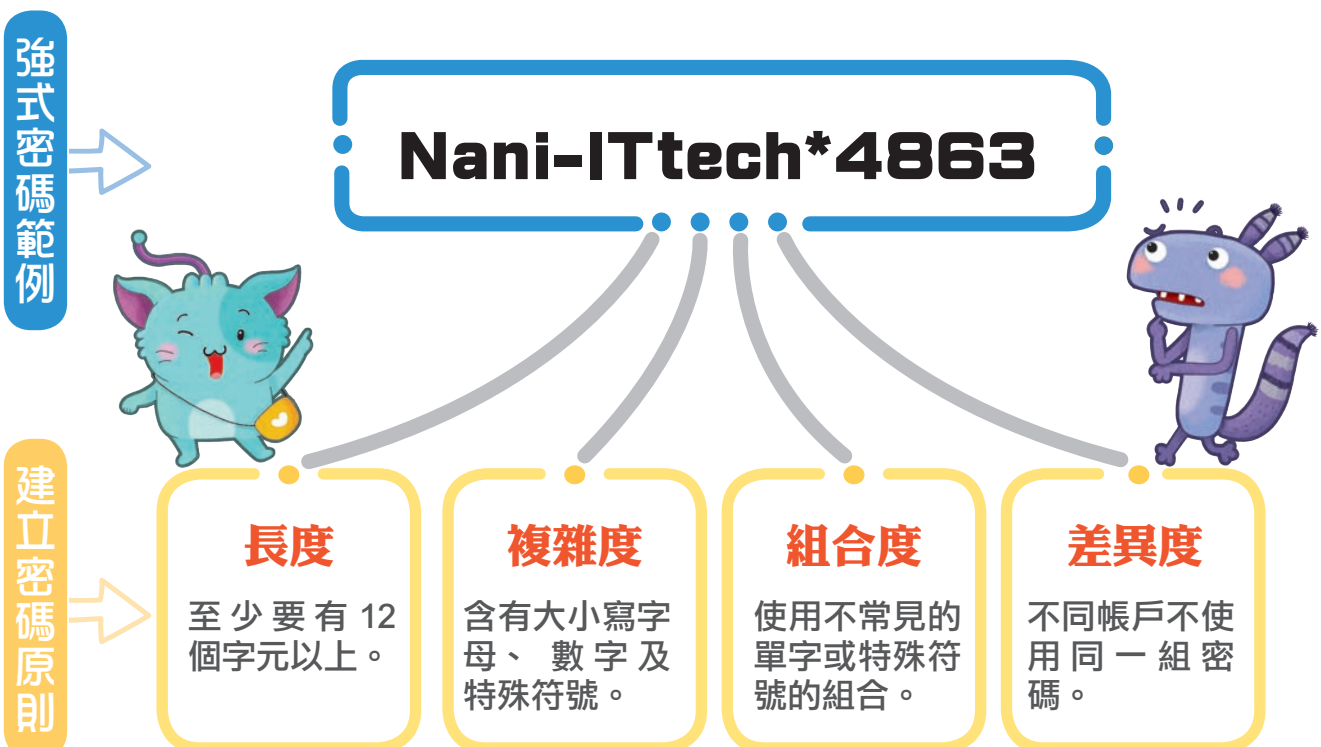
生活小劇場　不簡單的密碼設定

由於網路平台的興起，現代人往往有多個系統需要登入，有人因為常常忘記密碼造成無法登入或是帳號被鎖，便傾向將密碼設定得簡單好記就好，或是直接讓電腦「記住密碼」。但忽略了越簡單的密碼也越容易被破解，使用「記住密碼」也容易讓帳號被他人冒用登入喔！

延伸討論

1. 當帳號被盜用且無法再登入時，應該採取什麼行動呢？
2. 除了提升密碼的強度之外，還有什麼方法能降低帳號被盜用的風險呢？

密碼猶如保護個人資料的第一道關卡，防止**未經授權的資料存取**以及**個人資料**的外洩，大多數的網站在用戶建立帳號時，都會建議使用者設定一組比較不容易被破解或較難猜到的密碼，稱為「**強式密碼**」。



除了密碼保護外，在使用免費 Wi-Fi 服務時，盡量選用具有 **Wi-Fi 存取保護**（Wi-Fi Protected Access，簡稱 WPA）加密傳送的無線網路來使用，對個人的資訊安全可以再多增加一層防護，瀏覽網頁時，也應留意**不要隨意點選未知來源的連結**。

智慧王

Wi-Fi Protected Access

是一種保護無線網路（Wi-Fi）存取安全的技術標準，其中一項是在登入 Wi-Fi 前，需輸入正確的密碼才能使用網路。

想一想

生活中有哪些行為，可能導致自己的資訊安全存在隱憂？平時應該具備哪些良好的使用習慣呢？

生活小劇場　網路釣魚擅偽裝，個資外洩要提防

你是否經常看到這樣的訊息：「您的帳戶已被鎖定，請點擊連結恢復訪問權限！」、「恭喜！您贏得了一份大獎，請點擊領取！」，這些看似無害的訊息實際上是詐騙的常見手法，為了避免成為受害者，我們應該保持高度警惕。

延伸討論

1. 個資外洩真的沒關係嗎？
2. 個資外洩可能會造成什麼影響呢？

我們可能因為各種原因需要在網站上填寫個人資料，例如：參加線上心理測驗、參與抽獎活動、瀏覽看似無害的網頁等，即使內心有些許疑慮，仍輕率地將個人資料填寫提交，就會不自覺的陷入「**釣魚網站**」的陷阱或遭遇「**社交工程攻擊**」。這些填寫的個人資料可能帶來潛在的資安風險，不肖份子可能會利用我們所提供的資料，從而引發各種損害。

為了避免成為詐騙行為的受害者，應避免隨意在不信任的網站上填寫個人資料，也可利用**內政部警政署反詐騙諮詢專線 165** 諮詢、檢舉或報案。

網路釣魚

網路釣魚（Phishing）是一種詐騙手法，通常通過偽裝成合法機構、企業或個人來欺騙人們提供個人敏感資料，例如：帳戶密碼、信用卡號碼、電話號碼、地址等。不法意圖者會創建看似真實的電子郵件、網站或訊息，試圖引誘受害者點擊惡意連結、下載惡意附件，或在偽造的網站上輸入個人資訊。

社交工程攻擊

社交工程攻擊（Social Engineering Attack）是一種涉及心理學和人際關係的詐騙手法，利用人們的善意、好奇心、恐懼或對特定情境的信任，從而讓受害者在不知不覺中掉入陷阱，例如：提供個人資訊、點擊連結、下載檔案等，社交工程攻擊可以在不同的情境下發生，往往不依賴於技術上的漏洞，而是利用人類的行為和決策脆弱性來進行攻擊。

1-3 個人數位金融安全防護

資訊科技時代不斷發展出各種服務，同時也改變了人們的交易買賣方式，過去，人們主要使用現金進行交易，包括硬幣和紙鈔，人們需要攜帶足夠的現金來支付商品和服務，大多數交易是在實體商店進行的，需要親自前往購物地點。

圖 1-3 現金仍然是最廣為使用的支付方式。

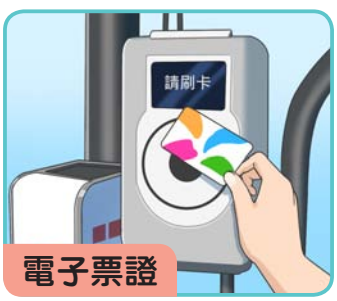


圖 1-4 只要使用相對應的讀卡裝置，就能夠靠卡感應進行支付扣款，省去攜帶零錢、找零的麻煩。

圖 1-5 信用卡是一種金融工具，允許持卡人在購買商品和服務時借款，而無需立即支付現金。

電子支付種類

電子化支付

- 電子票證
- 第三方支付
- 電子支付
- 行動支付
  - 感應式
  - 掃碼式

圖 1-6 悠遊卡

在資訊科技蓬勃發展的現代，**電子化支付技術**使人們能夠使用智能裝置或載具進行交易，而無需實際接觸交易，透過各種電子支付，我們不再被口袋裡大大小小的硬幣或卡片困擾，交易紀錄容易管理和追蹤，生活變得更加便利。

圖 1-7 Line Pay

特色及功能	常見支付
實體票卡，可預先儲值的多功能支付工具。	一卡通、悠遊卡
由第三方業者作為買賣家的交易中介，僅有代收付功能。	Paypal、綠界科技 ECPAY
市面上應用範圍最廣的支付種類，可轉帳、付款、儲值。	街口支付
無接觸式，付款過程更加方便。	Apple Pay、Google Pay
目前行動支付市場的主流付款形式。	Line Pay、臺灣 Pay

圖 1-8 感應式支付又稱為 NFC 支付，是行動支付當中最方便的，只要將卡片綁定在有 NFC 功能的裝置中，再靠近付款裝置就可以完成付款。

圖 1-9 行動掃碼支付只要由消費者手機安裝付款 APP，並綁定銀行帳戶、信用卡或簽帳金融卡，透過出示消費者的條碼或是掃描店家的 QR CODE 來做付款。

智慧王

NFC

近距離無線通訊 (Near-Field Communication, 簡稱 NFC) 是一套通訊協定，可以讓兩個電子裝置進行通訊，進而分享兩個裝置間的內容。

數位金融交易帶來了便利，使我們能夠快速、輕鬆的管理金錢、購物、支付費用，然而這種便利性也伴隨著一系列風險和隱憂，我們使用手機、平板電腦和電腦來交易，也使我們更容易成為駭客和詐騙者的目標，網路詐騙、身份盜竊、惡意軟體、虛假交易、小額詐騙等數位風險也顯著提升。

常見數位金融詐騙手法

中獎、補助詐騙信息，用來引誘人們點擊並洩露個資。

有心人士試圖竊取個人資料進行不當交易。

裝置被入侵或植入木馬後門程式引發異常交易。

社交軟體常見認證碼詐騙手法，誘使受害者提供特定訊息，以便盜刷錢財或帳號。

如何防範

1

不要安裝或下載來路不明的 App。

2

帳號使用完畢確實登出並且不依賴瀏覽器記憶帳號密碼。

3

智慧型手機的近距離無線通訊感應功能必要時才開啟。

4

安裝電腦防毒軟體或是手機專用的安全防護軟體。

1-4 智慧型裝置的資安防護

由於行動網路與智慧型裝置的普及，透過安裝各種行動應用程式（Mobile Application，簡稱 App）在日常生活中帶來許多便利。

攝影修圖 App：
留下美好的生活記憶。

Canva Snapseed 相片大師

社群通訊 App：
掌握時勢脈動及維持好友聯繫。

Facebook Instagram Line

觀光旅遊 App：
提供交通、住宿、購票等訊息。

Klook 台鐵 e 訂通 Agoda

網拍購物 App：
不用出門就可以買到需要的東西

蝦皮 MoMo SHEIN

休閒娛樂 App：
提供心情的放鬆和娛樂。

Youtube NETFLIX Disney+

APP 提供了許多便利，但有些免費 APP 可能會包含廣告或購買選項，在下載之前，應評估這些 APP 是否會在使用過程中帶來額外的費用，並謹記隨時留意帳戶資訊以避免不必要的支出。另一方面，付費 APP 通常提供更多功能和無廣告的使用體驗，在下載付費 APP 前，應評估是否真的需要這些附加功能，並確保了解價格和支付方式。

生活小劇場 不單純的權限開放

延伸討論

1. 你認為該授權哪些項目給相機 App 呢？
2. 個人資料及隱私比較可能經由哪些項目開放授權而洩漏出去呢？

智慧型裝置上的 App 可以為我們帶來許多便利，但背後也隱藏了許多資訊安全上的隱憂，當我們發現**不合理的權限要求**時，**應該提高警覺**多方查證，也可以尋找其他功能相似而要求權限在合理範圍內的 App 來替代。

除相機 App 之外，當我們在生活中越來越依賴智慧型裝置時，同時也可能帶來許多風險隱憂，例如：

- **語音通話在不知不覺中被監聽或錄音。**
- **訊息、郵件或瀏覽記錄被監控或披露。**
- **聯絡資料、影音檔案等被他人取得或複製。**
- **手機儲存的各種帳號密碼、虛擬金融資訊等遭受竊取。**
- **行動裝置定位資訊受到監控。**

所以，當我們在使用智慧型裝置時，除了確認 App 權限要求合理才下載安裝、安裝行動裝置安全防護軟體以外，透過 Android 與 iOS 系統本身的安全機制也可以為我們的資訊安全增加一道保護。

Android Google Play 安全防護

- 設定啟動密碼保護或圖形驗證。
- 啟用 Google 帳戶雙重驗證。
- 開啟〔掃描裝置中的安全性威脅〕。

iOS AppStore 安全防護

- 設定啟動密碼保護或圖形驗證。
- 啟用 Apple ID 雙重驗證。
- 非必要時不開啟 [App 內購買]。

想一想

使用智慧型裝置的時候，還有哪些行為可能造成資訊安全的威脅？

第 2 節 資訊科技對社會的影響

資訊科技的發展為生活帶來便利也伴隨著資訊安全隱憂，除了對個人層面的影響，也會對整體社會帶來新的生活形態與影響。

2-1 數位資料與資安管理

資訊科技的蓬勃發展使得資料更容易存取、管理和利用，從早期記錄在紙本文件的方式逐漸轉變為以數位形式記錄在電腦中，這樣的便利也伴隨著一系列的挑戰，特別是在個人資料的安全性和隱私權保護方面。

駭客盜取個資轉賣案例

駭客入侵系統

駭客攻擊網頁漏洞，破壞縣市機關及學校防火牆入侵系統後臺

學生個資外洩

駭客取得全國學生的個人資料共約 750 萬餘筆

駭客販售個人資料給中間人

中間人再轉售予補習班業者，不法獲利高達數百萬元

智慧王

個人資料保護法（以下簡稱個資法）中明確規定，保有個人資料之公務 / 非公務機關應積極履行監督、保護職責，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

《個資法第 41 條》條文節錄

意圖為自己或第三人不法之利益或損害他人之利益，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

臺灣近年個資外洩超過百萬筆，根據行政院資安處統計，全國政府部門每月平均遭到攻擊的次數約 2 千萬至 4 千萬次。在網路的環境中，駭客或病毒經常會**利用系統漏洞進行攻擊或入侵**，為了防止外部非法侵入，資訊系統通常包含**多重防護機制**，來保護系統安全。

防火牆 (Firewall)

防火牆是一種用於保護電腦網路安全的安全性裝置，主要功能是過濾、監視、控制網路流量以及管制資料流向，**防止未經授權的訪問和惡意攻擊**，目前多數作業系統均有提供防火牆的功能，建議應當要預設為「**啟用**」，不要輕易關閉。

當資訊科技深入到我們生活的各個層面時，安全隱患一旦出現，其影響將變得廣泛且深遠。近年臺灣政府數位發展部也將「**零信任 3A 資安溝通原則**」列入施政重點，打破「內部網路是安全的」的危險概念，這種框架轉變了傳統網路安全的信任模型，強調每個用戶和設備都應該在訪問資源時**經過身份驗證和授權**，而不是僅僅因為它們在組織網路內就被視為可信任，這種思維模式的轉變成為資訊安全領域的一個重要里程碑。

零信任 3A 資安溝通原則

Authentication
身分識別
在進行任何授權或紀錄的操作之前，首先需要確保使用者的身份以及是否有權利進入系統。

Authorization
授權存取
一旦使用者的身份經過驗證，根據使用者身份授予或拒絕不同的訪問權限。

Accounting
行為紀錄
為了追蹤、審查以及在發生安全事件時提供詳細的紀錄，系統會記錄每個使用者的活動用於事後的分析和調查。

2-2 社會秩序與隱私安全

不論是居家安全、公共環境監測或是產業的需求，都和資訊科技發展有密切關係。自從有了監視系統，人們不再需要親自到達現場，透過監視系統即可同時觀看不同地點的即時影像。透過無遠弗屆的網路，能突破空間限制建構遠端即時監控系統。例如：智慧校園或公寓大樓安全防護網的影像監視系統、高速公路即時路況資訊等。

圖 1-10 常見的監視器

圖 1-11 高速公路即時路況資訊

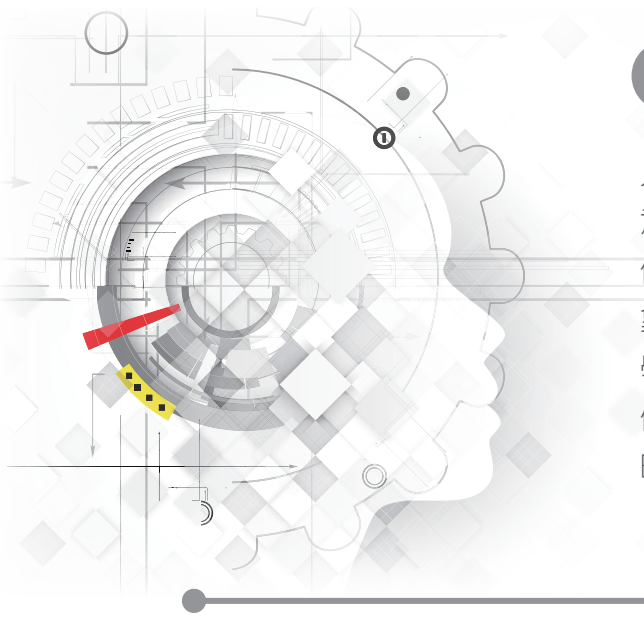
隨著科技發展與網路普及，加上社會秩序維護的需求，我們生活的周遭裡出現了越來越多的影像監視設備。當發生治安事件時，警察機關可以透過影像監視設備，快速掌握各種犯罪行為。然而如果影像監視設備遭到不當使用，就可能會發生個人隱私被監看的疑慮。

想一想

在維護社會秩序與保障個人隱私之間，影像監視設備應該怎樣規範才合理？

2-3 人工智慧與未來挑戰

人工智慧是一個正在迅速發展的領域，它讓機器可以**像人類一樣學習和做出決策**，這也帶來了一些重要的議題。



人工智慧

人工智慧（Artificial Intelligence，簡稱 AI）一詞的字面意思，是由「**人工**」所創造的「**智慧**」。而「智慧」這個詞指的是具備一系列特定能力，包括：邏輯思考、抽象思維、預測與規劃、理解複雜概念、現象和語言以及學習和解決問題等。目前我們已經能使機器展現出「類似擁有智慧」的行為，而這些機器只能在執行特定任務時表現出一定程度的智能，因此也稱為「**弱人工智慧**（Weak AI）」。

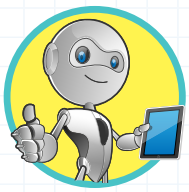
機器學習

最初的時候，電腦科學家為解決電腦面對的問題，創建了許多演算法，依據這些演算法撰寫程式，才能處理這些問題；後來問題變得更複雜了，就需要靠許多小程式彼此互相合作，才能完成最終目標，這就是 AI 最早的雛型。

經由演算法撰寫的程式，通常只能處理固定情境的問題，且採取的方法是固定的，無法隨著環境不同採用更適當的策略。當引進了人類學習的模式，加上大數據資料的出現，讓人工智慧的發展進入**機器也能模仿人類的學習能力**，現在一般大眾所說的人工智慧，常指的就是**機器學習** (Machine Learning)。

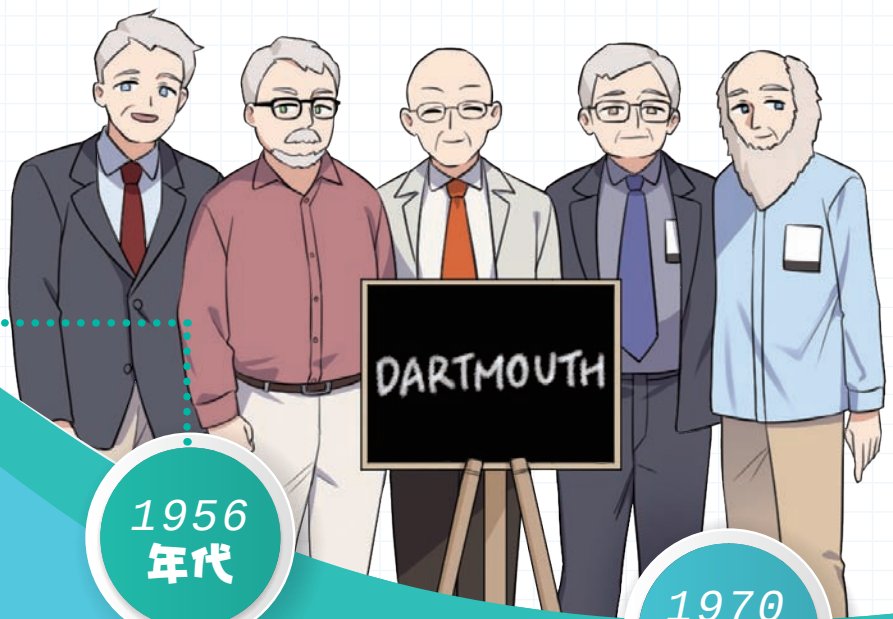
智慧王

演算法：可參考第三章 191 頁



人工智慧的發展歷史

達特茅斯會議被視為人工智慧領域的起源之一，會議的成果包括了一些早期的 AI 程式以及人工智慧的正式命名，藉由電腦與演算法的進步，從此揭開了 AI 研究的序幕。



1950 年代

圖靈測試 Turing Test

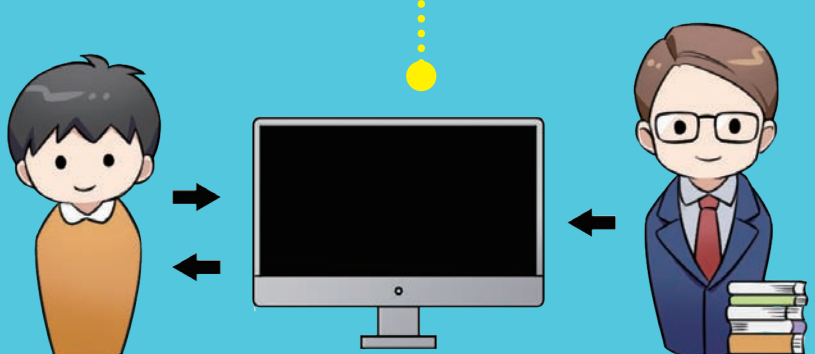
運用機器來測試是否具有宛如人類智慧的概念，是由艾倫．圖靈 (AlanTuring) 所提倡的，當時僅止於概念的闡述，並沒有正式命名。

1956 年代

達特茅斯會議 Dartmouth Workshop

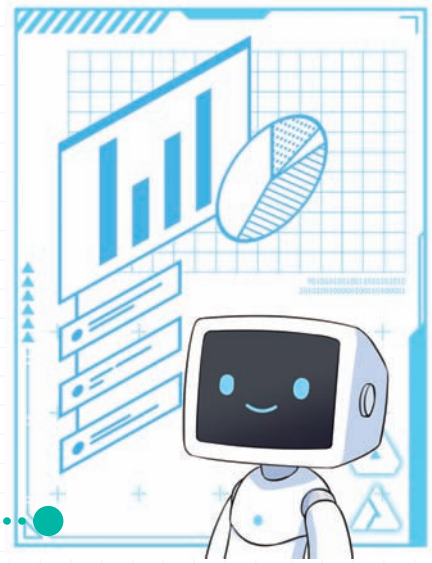
1970 年代

專家系統 Expert System



由於電腦硬體的加速發展，電腦處理資料的能力更加提升，催生了足以處理知識與資料的專家系統，其目標是在模擬人類專家在特定領域中的知識和決策能力。

隨著網際網路的普及，網路上充滿了可供人工智慧訓練和應用的大數據。這一發展推動了機器學習開始發揮其真正的潛力。



智慧王

大數據 (Big Data)：大數據是指規模龐大且多樣化的資料集合，包含了各種來源的資料，這些資料對於機器學習非常重要，因為機器學習演算法需要大量的資料來訓練模型，使得電腦能夠自動從數據中學習模式和規律。

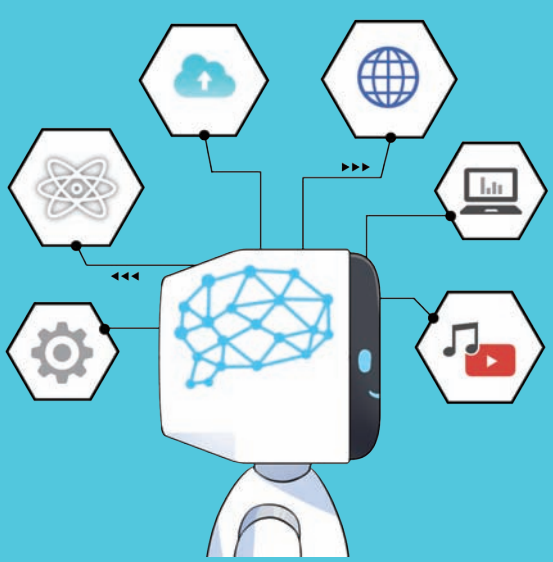
1990 年代

大數據時代機器學習

2010 年代

深度學習

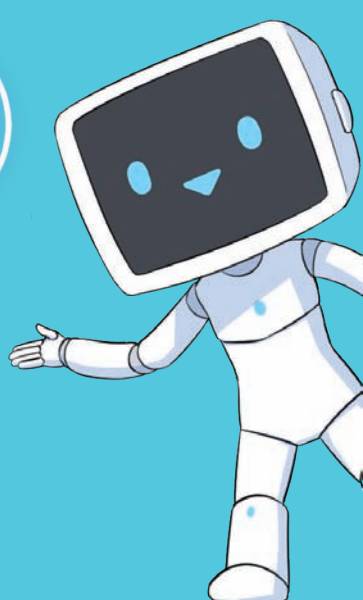
2010 年代，善於處理感知類型資料與學習的深度學習問世，電腦處理視覺與聽覺等相關資料的能力突飛猛進，因而取得了 A.I. 發展上的突破進展。



2023

生成式 AI

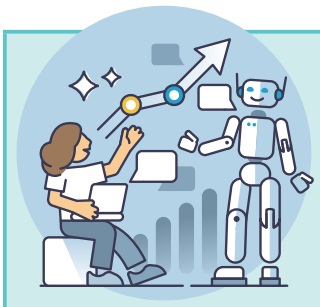
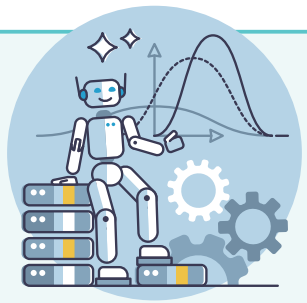
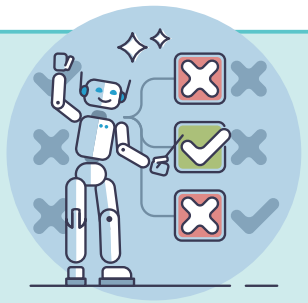
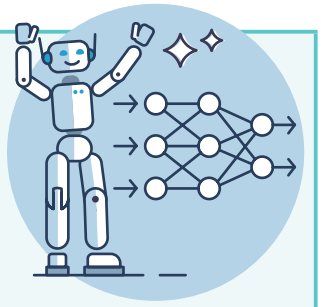
生成式人工智能（Generative AI）領域正在快速的發展，主要特點是可以產生文字、圖像、音樂等，而不僅僅是處理和分析資料。



未來

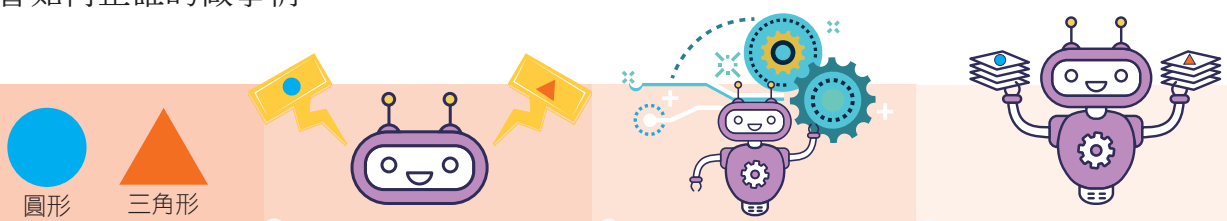
機器學習的方法

機器學習的方法主要可分為**監督式學習** (Supervised Learning)、**非監督式學習** (Unsupervised Learning)、**強化學習** (Reinforcement Learning) 及**深度學習** (Deep Learning)，這些機器學習的方法各有其適用的解決問題類型。

			
監督式學習 Supervised Learning	**非監督式學習** Unsupervised Learning	**強化學習** Reinforcement Learning	**深度學習** Deep Learning
用以解決分類、預測的問題；有標準答案。	用以解決分群的問題；沒有標準答案。	用以解決控制的問題或取得最優解。	用以解決複雜的問題，利用多層次的神經網絡處理和學習資料模仿人類大腦結構。

1 監督式學習

監督式學習的運作方式較直觀，就像是教電腦如何做事情的過程，我們告訴電腦要學習的東西，然後告訴它哪些是對的，哪些是錯的，通過這樣的訓練，電腦可以學會如何正確的做事情。



標註 (Label)

如果我們想讓電腦學習分類三角形及圓形，需要先正確標註它們的圖片。

特徵 (Feature)

將圖片輸入到電腦，讓電腦以演算法自行歸納這些輸入資料的特徵。

模型 (Model)

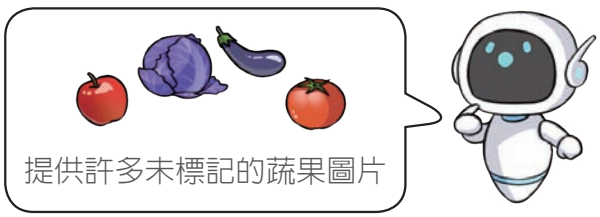
電腦完成設定的訓練回合後會建立模型。

測試 (Test)

若這個模型能通過其它辨識圖形的測試，電腦使用它時，就能擁有識別三角形和圓形圖片的能力。

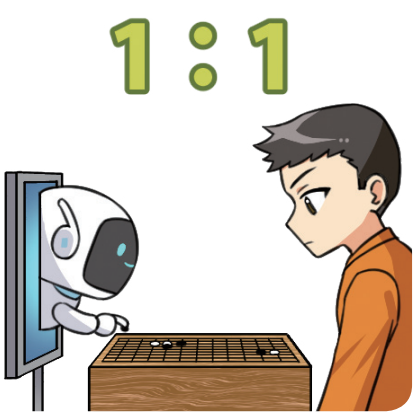
2 非監督式學習

非監督式學習是在**沒有標記過的訓練資料**中，電腦**能自動對資料進行分類或分群**。一般在處理問題時，並不容易取得具完整標記的資料，當不知如何分類資料，或是需要電腦從資料中自行尋找相同的模型時，非監督式學習將可以提供很大的幫助。



3 強化學習

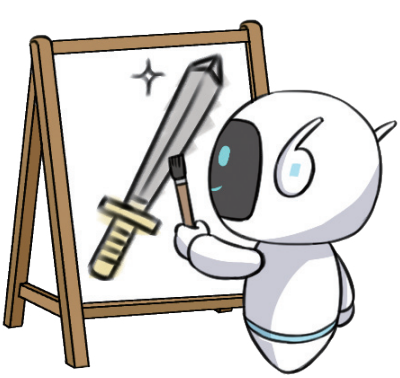
強化式學習是**電腦自動依據每次行為結果再重複學習的方法**。它可以訓練電腦做出決策，以實現最佳結果。強化式學習源自心理學行為學派的學習觀點，認為學習是刺激與環境互動的結果，完成目標的動作會得到增強，偏離目標的動作則被忽略。這種嘗試錯誤的學習方法，能使電腦在沒有人為干預、沒有明確指令下，就能夠做出一系列的決策。



強化式學習經常被應用在下棋或遊戲。

4 深度學習

深度學習是一種**以類神經網路為架構的演算法**，可指導電腦以類似人腦學習的方式來處理資料。深度學習中的形容詞「深度」是指使用多層類神經網路。在傳統的機器學習中，資料特徵通常是由人為標記產生出來的，需要經過專家對資料進行許多的分析及研究，才能產生出有用、效果良好的特徵。深度學習則具有自動抽取特徵的能力。



生成式 AI 就是深度學習的一種。

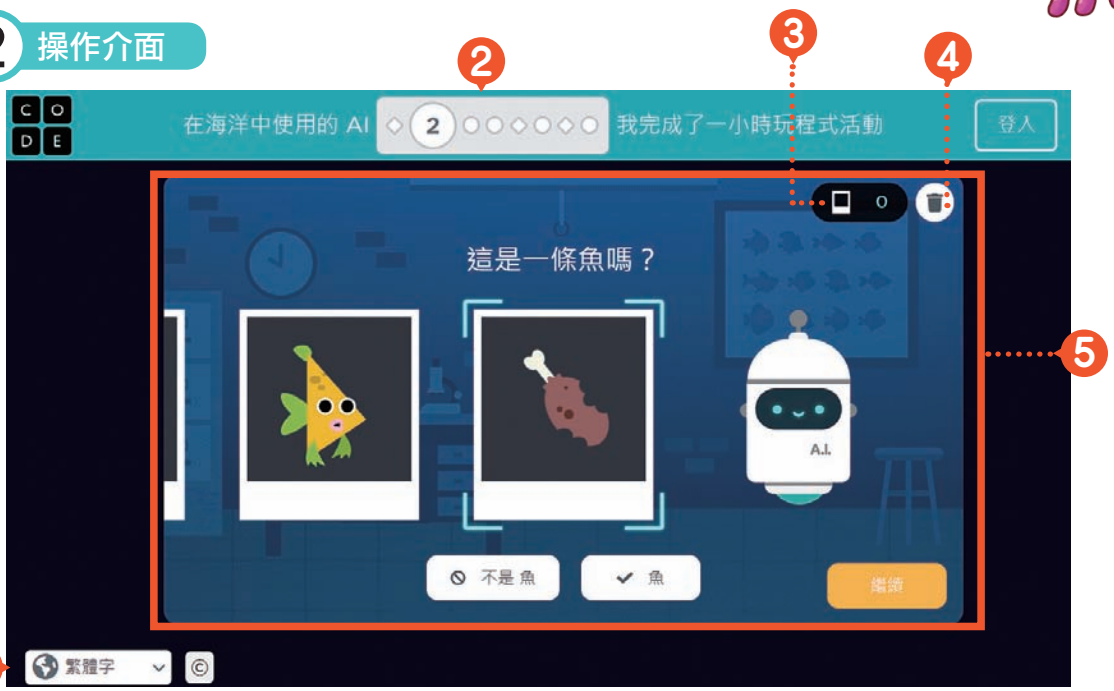
保護海洋的 AI

全球每年約有數億磅的垃圾流入海洋，隨著科技的發展，人類應用 AI 偵測辨別及清除海洋垃圾的技術越趨成熟，AI 藉由大量的資料學習辨識以及蒐集不同的海洋垃圾，以減輕塑膠垃圾對海洋造成的生態汙染，我們一起來了解機器是如何透過學習，解決海洋垃圾的問題。

1 登入 AI for Oceans

輸入網址：http://video.nani.com.tw/oceangame

2 操作介面



❶顯示語言：預設為英文，可改為「繁體中文」顯示。

❷當前學習進度。

❸顯示目前已訓練的圖片張數。

❹刪除訓練資料：會歸零當前進度已訓練的資料。

❺互動學習主要操作介面。

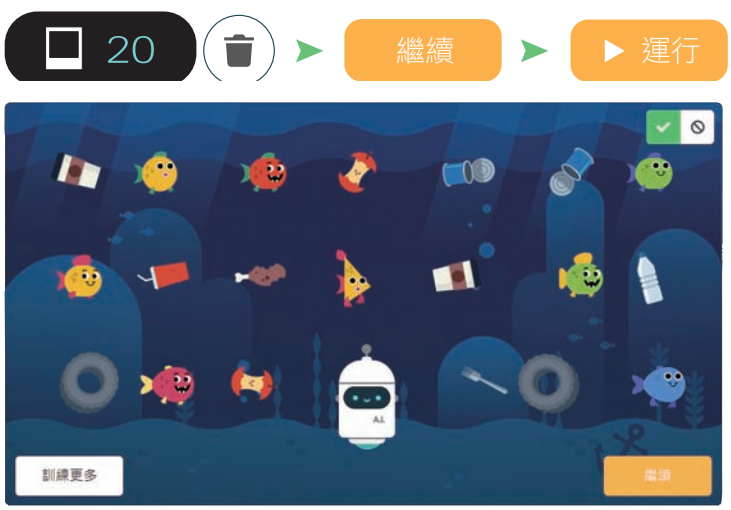
3 訓練 AI

以滑鼠點選【魚】或【不是魚】按鈕，告訴 AI 機器人這張圖片的正確答案，這個動作稱之為標註 (label)，是監督式學習的關鍵動作，目的是讓機器人知道答案，並能從中提取具有辨識度的重要特徵。

AI 會從你的錯誤中學習，如果你做了「錯誤」的選擇，AI 機器人就會跟你犯一樣的錯誤喔！

4 測試 AI

當測試的圖片到達「20」張時，請點選右下角「繼續」，並點選「運行」，運行過程可以看到機器辨識每張圖片的結果，請在機器辨識 20 張測試圖片後，點選【繼續】，可得到整體辨識結果，看看 AI 機器人辨識的結果如何呢？



想一想

當訓練的圖片很少時，會發生什麼事呢？

牛刀小試 2-3.1

依據「保護海洋的 AI」活動測試結果，回答下面的問題。

表示 AI 辨識為「魚」的圖片。 ✓ ⊘ 表示 AI 辨識為「不是魚」的圖片。

(1) 利用 5 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張； ⊘ AI 辨識為垃圾的魚有 ___ 張。

(2) 利用 10 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張； ⊘ AI 辨識為垃圾的魚有 ___ 張。

(3) 利用 25 張圖片訓練 AI，完成訓練後，使用 20 張圖片測試 AI。

✓ AI 辨識為魚的垃圾有 ___ 張； ⊘ AI 辨識為垃圾的魚有 ___ 張。

(4) 以上 AI 辨識垃圾和魚，發生錯誤次數最低的訓練是第 ____ 次。

(5) 若要提高電腦正確辨識垃圾和魚的成功率，我可以怎麼做？

牛刀小試 2-3.2

在頁面上方可以看到活動的進度，請點選「◇◇◇ 4 ◇◇◇◇ (進度 4) 訓練 AI 來清潔海洋」，依據提示完成活動並回答問題。

(1) 分別利用 5 張以及 25 張圖片訓練 AI，並使用 20 張圖片測試 AI。

請問哪一個訓練出現辨識海洋生物錯誤的次數最低，為什麼？

(2) 如果「不小心」將其中幾張是海洋生物的圖片點錯了，變成「垃圾」，會發生什麼事？要怎麼做才能更正呢？

人工智慧的應用

人工智慧 (AI) 已經成為現代潮流發展的一個關鍵詞， 2023 年生成式 AI 蓬勃發展，不僅在科技界引起廣泛討論，也深刻影響了我們與世界互動的方式。生成式 AI 是基於深度學習的架構，機器透過大量資料的學習，模仿人類感知的能力，關於**影像辨識**、**語音辨識**、**自然語言處理**、**圖像生成**等應用也跟著不斷推陳出新。

1 影像辨識— Quick, Draw

網址：http://video.nani.com.tw/qdraw

「Quick, Draw!」 是由 Google 開發的遊戲，這款遊戲挑戰你在 20 秒內繪畫特定物體，而 AI 將竭盡全力猜測你所畫的是什麼，在這個遊戲中，影像辨識技術扮演了關鍵角色，當你開始畫一個物體時，你的筆劃將即時被傳送到 Google 的伺服器，而 AI 通過比對你的筆劃與已知物體的筆劃模式，並參考龐大的數據庫，試圖猜測出你所畫的是什麼物體。

圖 1-12 Quick Draw 畫面

2 語音辨識—雅婷逐字稿

網址：http://video.nani.com.tw/yating

「雅婷逐字稿」 是一個嶄新的語音辨識應用，系統通過分析聲音波形、音調和音頻特徵，將語音準確轉錄成文字。這一過程需要使用大量的資料，用以訓練語音辨識模型，從而提高辨識準確性，除了可以使用麥克風語音輸入辨識，也可以上傳影音檔或 Youtube 連結辨識。

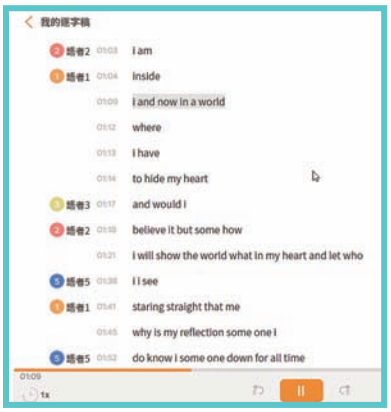
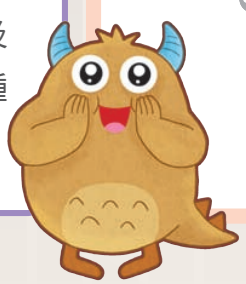
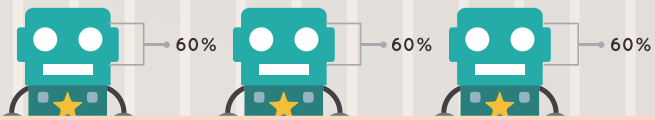


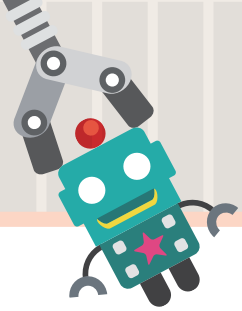
圖 1-13 雅婷逐字稿畫面

牛刀小試 2-3.3

請動手玩玩看「Quick, Draw ！」以及「雅婷逐字稿」，並說說看你對這兩種技術的印象如何？它們的準確性如何？







3 自然語言處理— ChatGPT

網址：http://video.nani.com.tw/cgpt

ChatGPT 是一個以自然語言為基礎的對話模型，它可以理解和生成文字，並被設計用於進行與人類自然而流暢的對話，以回答問題、提供信息，或參與對話交流。

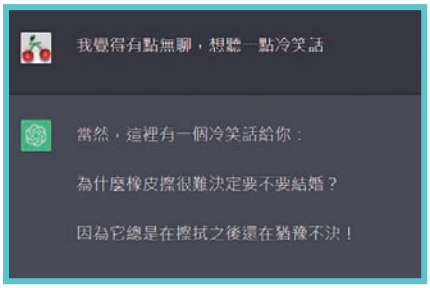


圖 1-14 ChatGpt 畫面

自然語言 (Natural Language) 是人類日常生活中使用的語言，通常指的是人們用來溝通、表達思想和交流信息的語言。例如：中文、英文。

4 圖像生成— Dream by WOMBO

網址： http://video.nani.com.tw/dai

Dream by WOMBO 是一個利用 AI 生成圖像的工具，可以通過文字描述或概念，選擇圖片風格後，讓 AI 生成符合描述的藝術圖像。

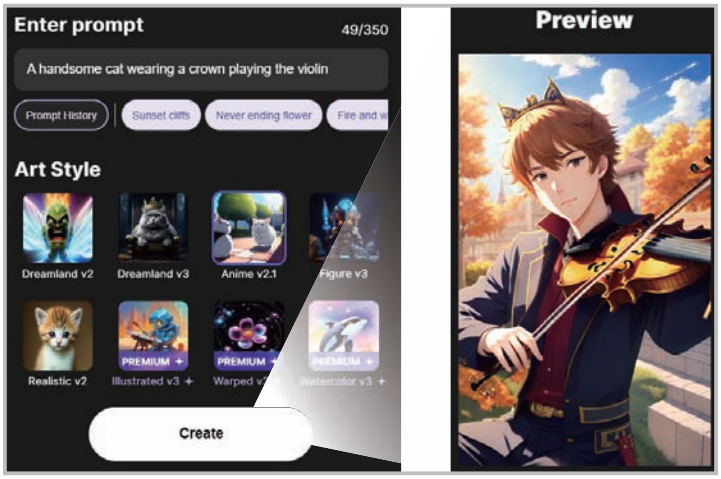


圖 1-15 Dream by WOMBO 畫面

牛刀小試 2-3.4

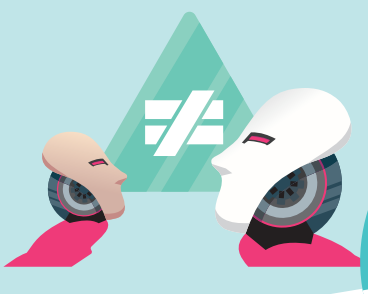
請動手玩玩看「ChatGPT」以及「Dream by WOMBO」，並說說看你對這兩種技術的印象如何？它們有什麼優缺點？

人工智慧與挑戰

人工智慧可以提高我們工作上的效率，其技術將被廣泛應用於各個領域，例如：家居、交通、醫療、金融、教育等，並推動這些領域的轉型升級。然而 AI 提供更多的創新機會和可能性的同時，也引發許多挑戰。

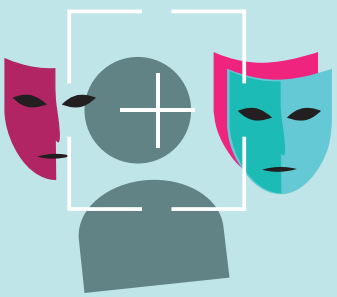
偏見 1

機器學習常會伴隨人類的價值觀，例如：監督式學習中，電腦的訓練受到人類提供的資訊影響，如果標註本身帶有偏見 (Bias)，那麼模型也可能學到這些偏見，進而在預測時產生偏見。



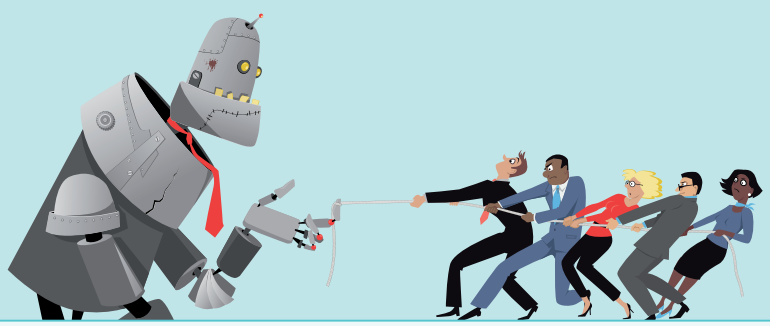
濫用 2

透過人工智慧技術，可以輕鬆地製造虛假的影片或影像，使其看起來極為真實，例如：深偽技術（Deepfake），這可能導致誤導、欺騙和詐騙，並對個人隱私構成潛在威脅。



3 誤判

AI 在做出決策或預測時，可能因為訓練資料不足、訓練過程不完善或演算法的限制等出現判斷錯誤的情況，對個人、組織甚至社會造成影響。



想一想

在自動化和智能化的環境下，如果人工智慧系統被駭客攻擊，可能會對社會造成嚴重的影響。你能想像有哪些潛在的攻擊手法？應該如何加強防禦措施，以降低這些風險？

綜合應用

任 務　**請你試著回答，下面文章中，樂樂的行為可能造成哪些資訊安全的風險呢？**

1 當樂樂開始使用文書處理軟體製作報告的時候，作業系統與軟體不斷跳出更新的提示，樂樂覺得非常干擾：更新好浪費時間喔，不管它啦！於是每次遇到更新提示總是毫不思索的關閉它。

2 上網搜尋參考資料時，發現有些網址非常奇怪。樂樂也不以為意：不漏掉可能的線索，任何網址都點開來看一看，有異狀再關掉囉！

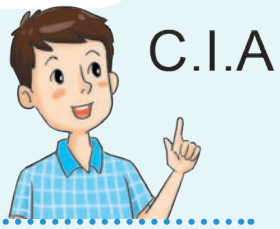
3 USB 隨身碟接上電腦就自動執行瀏覽，樂樂心想：怕調皮的弟弟亂動自己的作業，可不要存放在電腦上，存到隨身碟就好。

4 呼！總算告一段落，可以來休閒一下慰勞自己囉！上網搜尋一下好玩的益智小遊戲。看起來越是吸引人的遊戲，越需要許多的權限允許或安裝外掛，當下載到遊戲安裝檔案時，電腦跳出提示：要關閉病毒掃描，避免誤判才能安裝，而安裝過程也出現「要填寫信箱接收認證信」，樂樂心想：沒辦法，就是想玩，就都同意了再說。

此時，突然收到朋友傳來組隊打球缺人的訊息，太棒了！徵得了家人的同意之後，手邊進行的事情都先擱著就好，趕快換裝穿鞋出門去運動囉！

課後檢測站

學完本章節後，你了解多少呢？請回答下面的題目並選出正確的答案。



1. 廣泛的資訊安全定義是指資訊的 _____、_____、與 _____, 簡稱 C.I.A 。

2. 以下有關資訊安全的使用行為，正確請打 O，錯誤請打 X。

( ) 使用公用電腦登入系統，避免麻煩最好把密碼存起來。

( ) 收到免費遊戲的邀請郵件，一定要下載來玩。

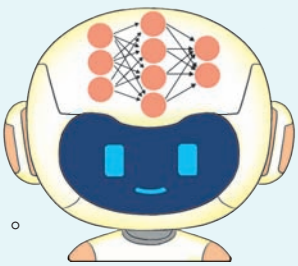
( ) 設定密碼很麻煩，用我自己的生日比較好記。

( ) 通知我中獎的郵件，我要趕快來填資料領獎品。

( ) 同學說，他的媽媽是業務需要業績，跟我索取身分字號跟出生年月日，不用我付錢，他媽媽會幫我保險，想想我也沒有甚麼損失，就把資料給他。

( ) 這款 APP 不用錢，很好用可以幫我修圖，我要下載，但不必要的權限我會想一下要不要開放。

3. 下列關於人工智慧的敘述，何者正確？



☐ 人工智慧意味著由「機器」所創造的「智慧」。

☐ 目前的人工智慧多為強人工智慧。

☐ 監督式學習的其中一個重點是標註。

☐ 機器學習的方法主要可分為複製法、深度法、猜測法、隨機法。