



# 長庚科技大學

## 113年度資通安全教育訓練

### ☑資通安全系列課程

★課程名稱：

資訊科技發展下對資訊安全應有之認知

★授課日期：113.11.21

★授課時數：3 小時

---



講師：鍾文魁 Mark

學歷：東吳大學法律學系科技法律組 碩士  
(關鍵資訊基礎設施保護法制面建構與分析)

華梵大學資訊管理學系資通安全組 碩士  
(惡意電子郵件攻擊之研究)

經歷：



# 大綱

一 資訊安全威脅趨勢

二 網路攻擊現況

三 資訊安全應有之認知

四 結論

# 大綱子題

## 一 資訊安全威脅趨勢

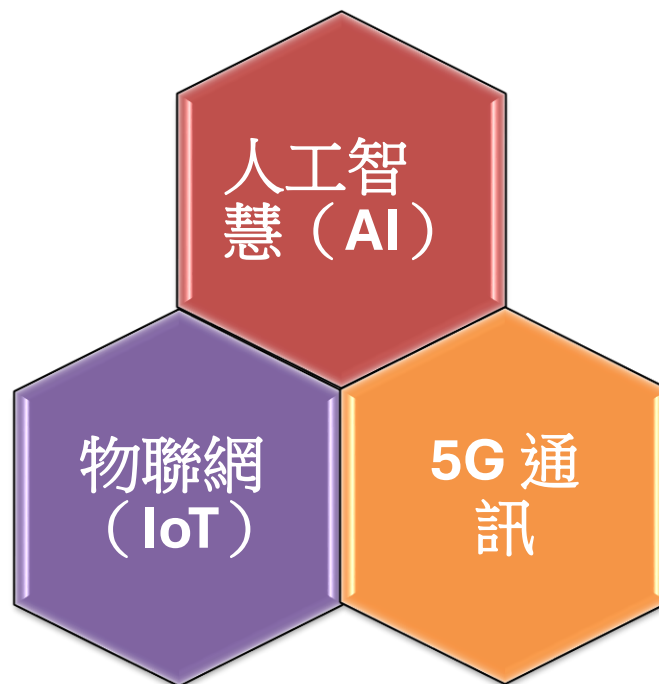
### 1 資訊科技發展與應用

### 2 資訊安全威脅趨勢

一

# 資訊安全威脅趨勢

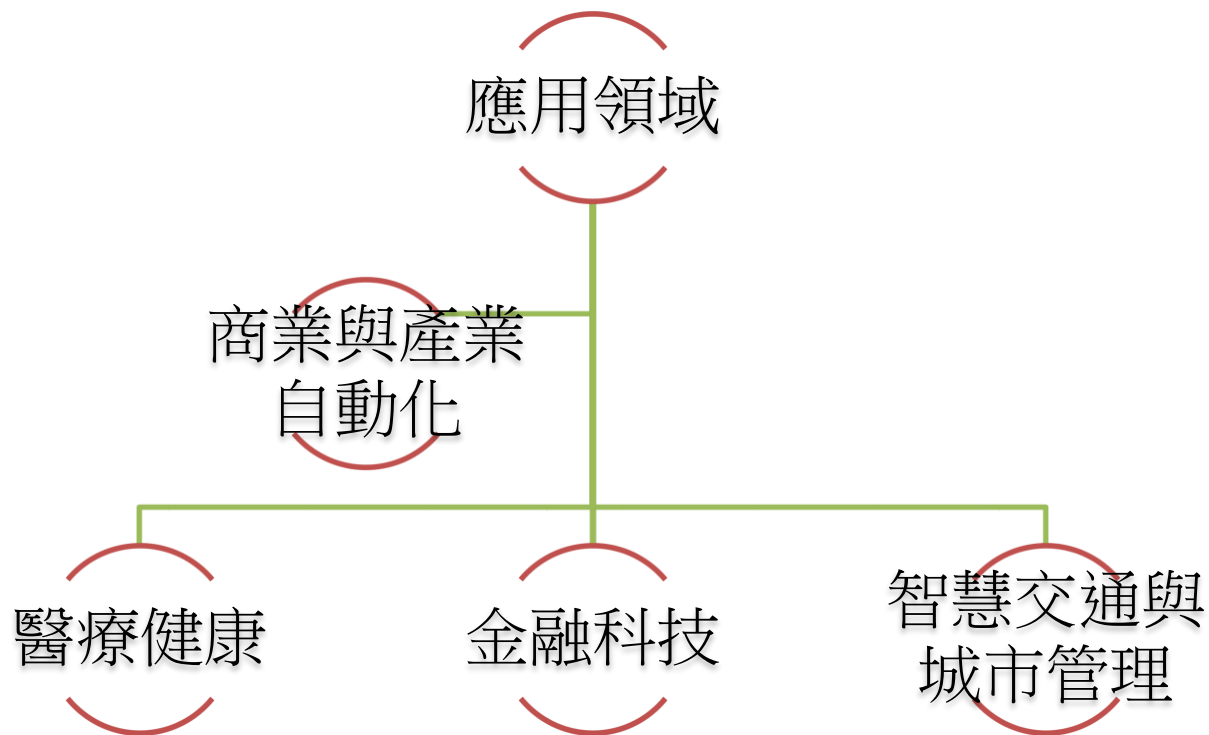
資訊科技  
發展與應用



# 一 資訊安全威脅趨勢

資訊科技  
發展與應用

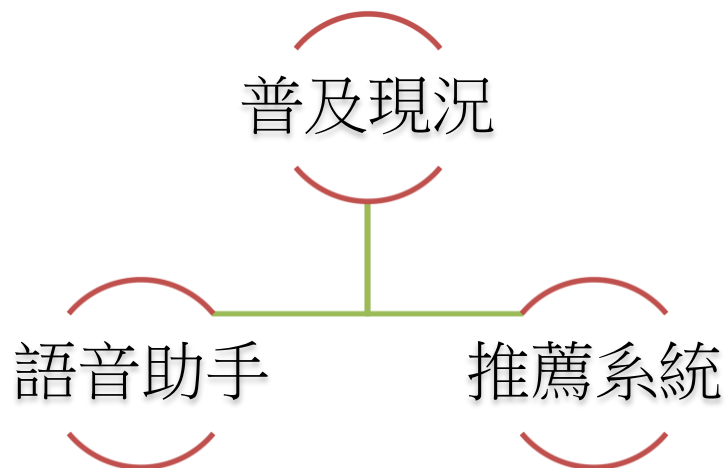
人工智  
慧 (AI)



# 一 資訊安全威脅趨勢

資訊科技  
發展與應用

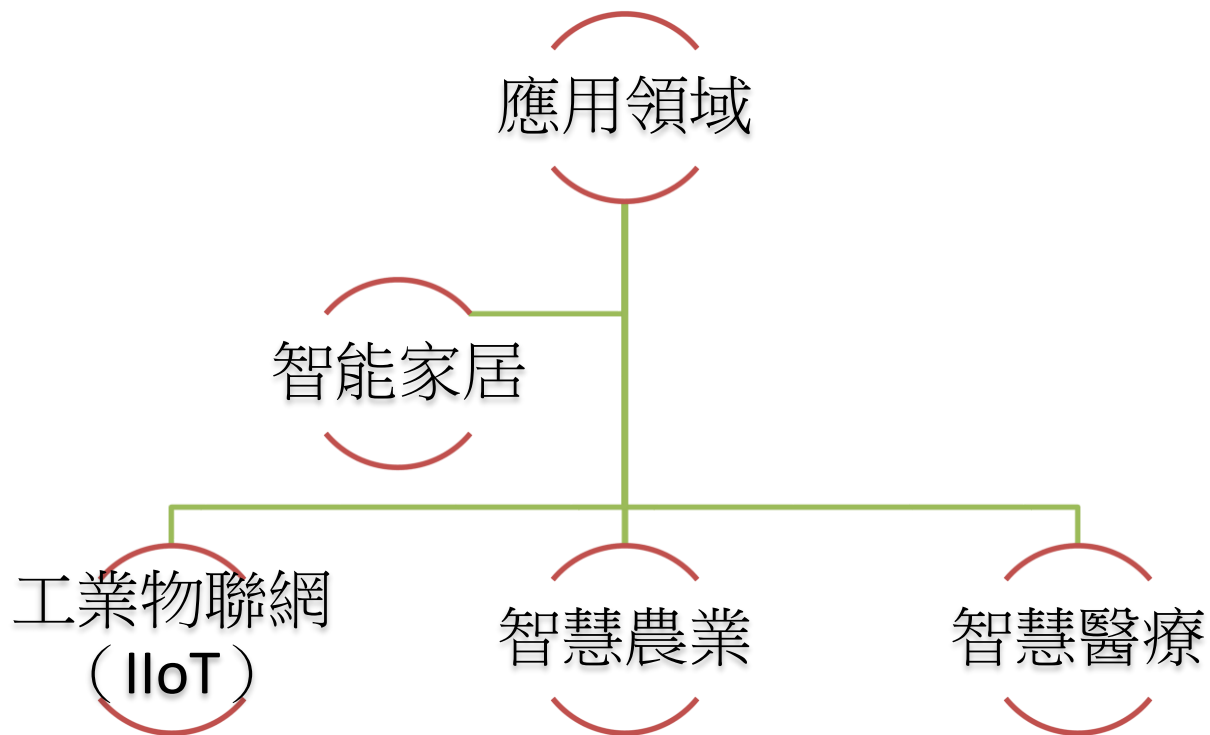
人工智  
慧 (AI)



# 一 資訊安全威脅趨勢

資訊科技  
發展與應用

物聯網  
(IoT)





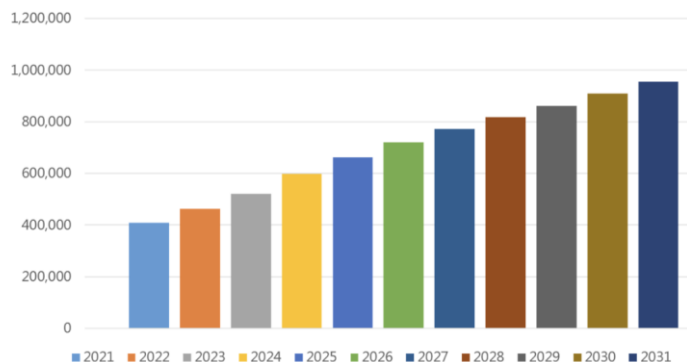
# 一 資訊安全威脅趨勢

## 資訊科技 發展與應用

### 物聯網 (IoT)

全球IoT終端電子市場成長趨勢

2021-2031年IoT終端電子市場規模



普及現況

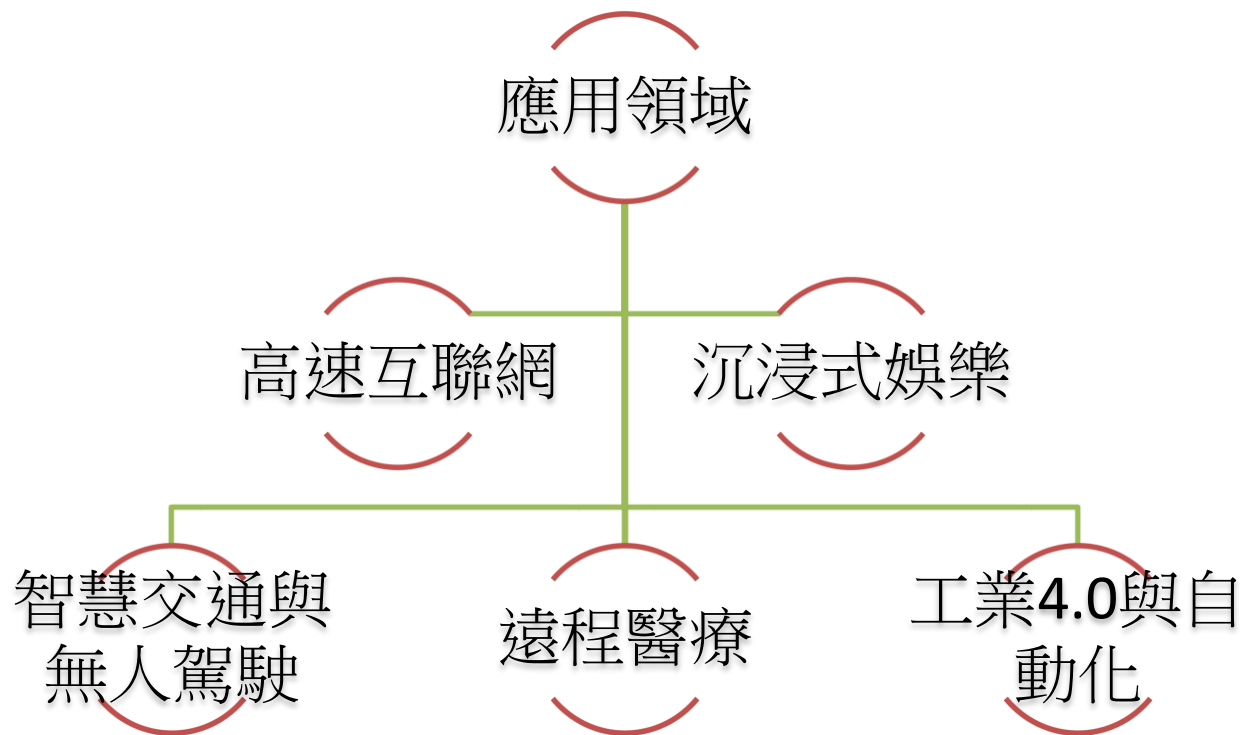
語音助手

推薦系統

# 一 資訊安全威脅趨勢

資訊科技  
發展與應用

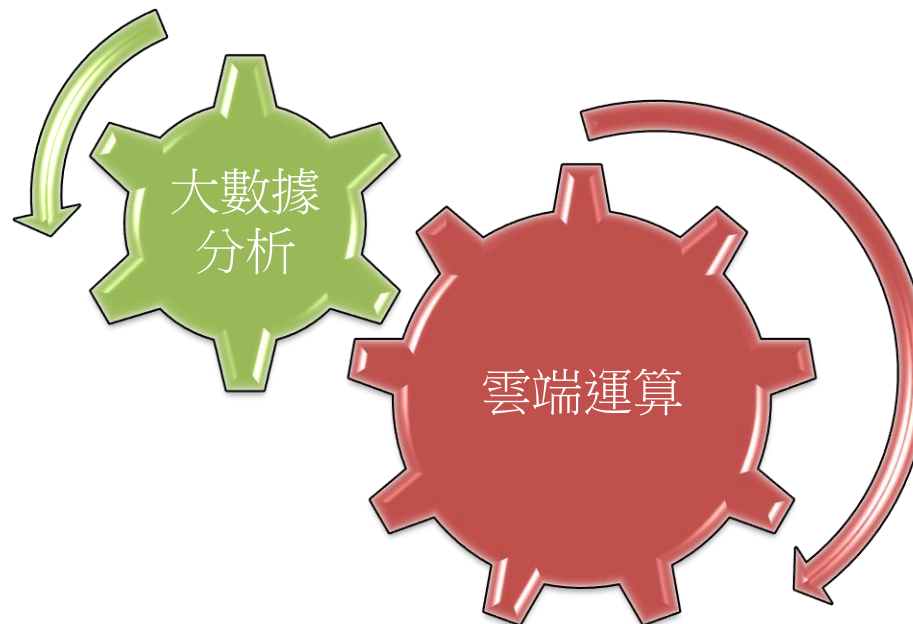
5G  
通訊



一

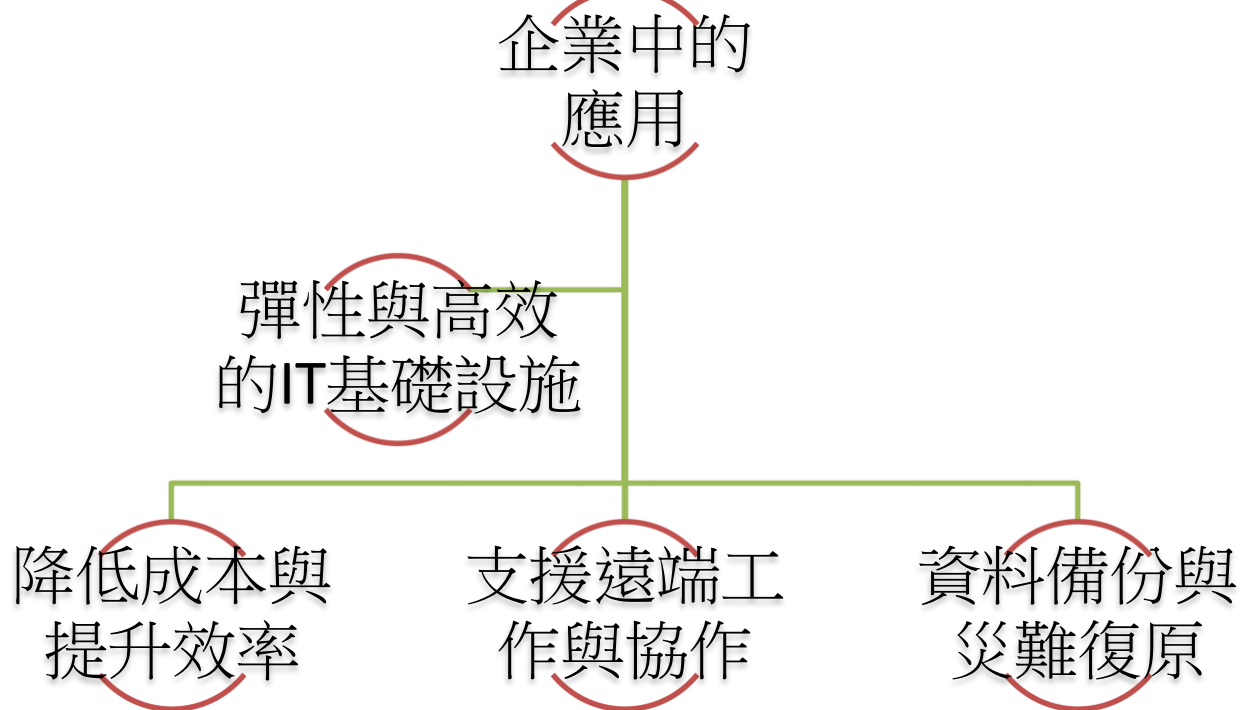
# 資訊安全威脅趨勢

資訊科技  
發展與應用



# 一 資訊安全威脅趨勢

資訊科技  
發展與應用



# 一 資訊安全威脅趨勢

資訊科技  
發展與應用



日常生活中的應用

串流媒體與  
娛樂

智能家居與  
IoT應用

行動應用與  
個人數據存儲

# 一 資訊安全威脅趨勢

資訊科技  
發展與應用



企業中的應  
用

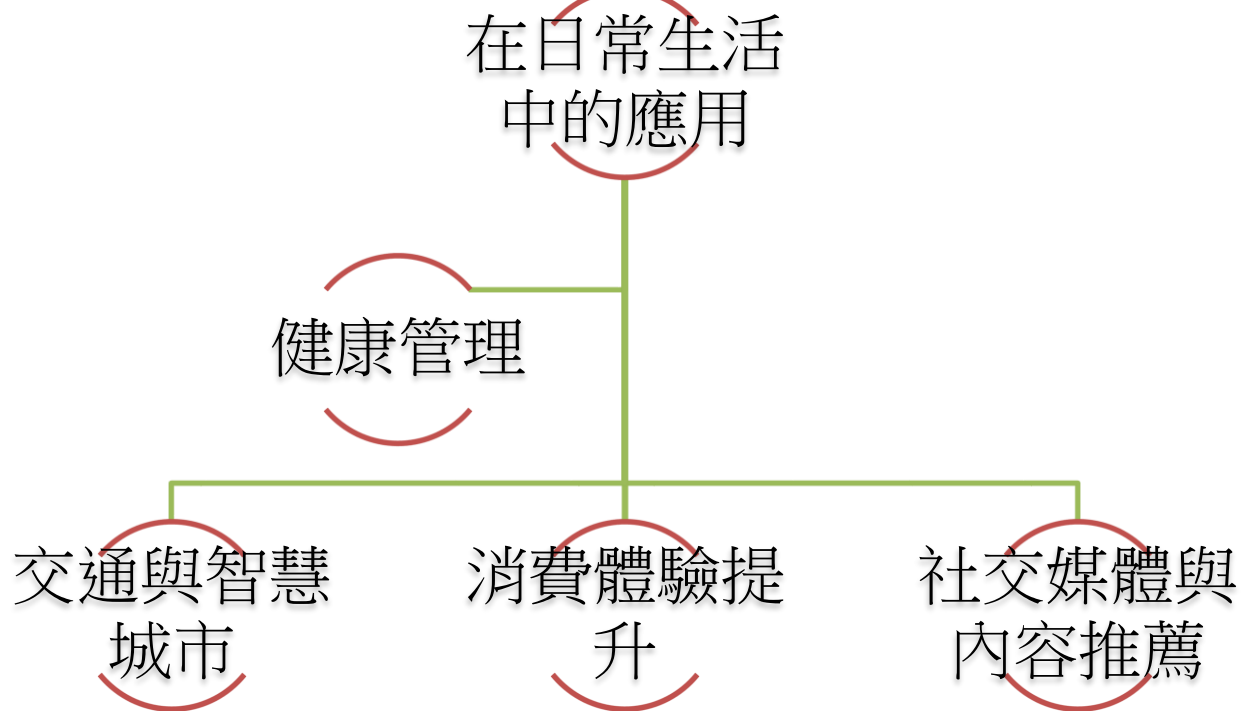
數據驅動決  
策

提升運營效  
率

風險管理與  
欺詐檢測

# 一 資訊安全威脅趨勢

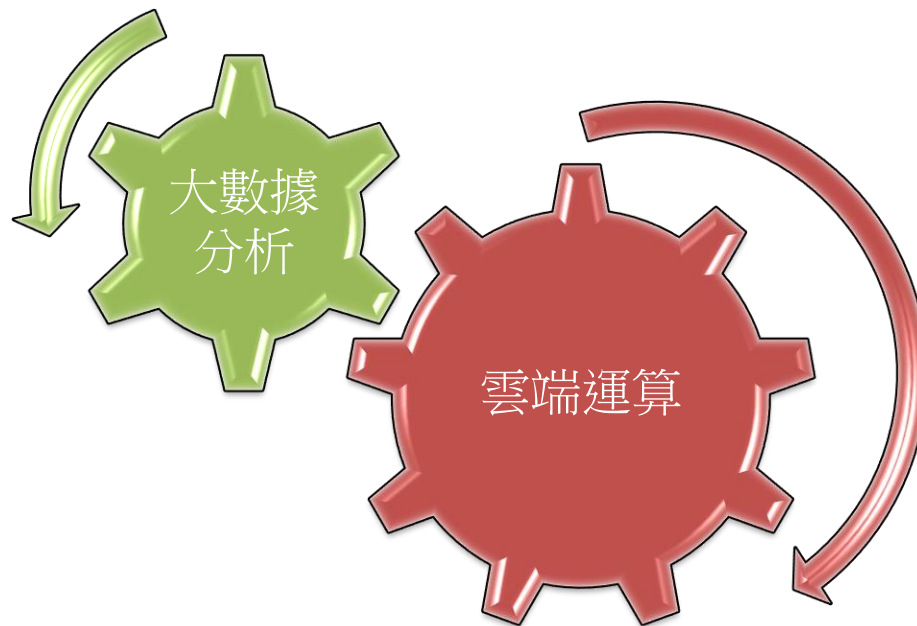
資訊科技  
發展與應用



一

# 資訊安全威脅趨勢

資訊科技  
發展與應用



數據處理  
效率提升

企業的數  
據化轉型

創新應用  
的推動



一

# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加

威脅的演變與  
複雜性增加

全球性資料  
安全挑戰

一

# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加

病毒攻擊

APT（進階  
持續性威脅）

# 一 資訊安全威脅趨勢

威脅的演變與  
複雜性增加

病毒攻擊

- ✓ Brain病毒（1986）：世界上第一個已知病毒，由巴基斯坦的兩名程式員創建，主要感染IBM PC的軟碟片。
- ✓ Morris蠕蟲（1988）：第一個網絡蠕蟲病毒，通過互聯網快速傳播，造成大量計算機癱瘓
- ✓ ILOVEYOU病毒（2000）：通過電子郵件傳播的病毒，以誘人的標題吸引用戶點擊附件，導致大量數據損毀。

一

# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加



病毒攻擊

- ✓ 零日漏洞（Zero-Day Exploits）
- ✓ 針對特定對象（如企業、政府機構）的攻擊
- ✓ 社交工程手段與技術攻擊結合，通過釣魚郵件、假網站等誘導用戶主動洩露信息或下載惡意軟體
- ✓ 多層次攻擊：攻擊者不僅鎖定單一系統，還試圖滲透整個網絡或供應鏈

# 一 資訊安全威脅趨勢

威脅的演變與  
複雜性增加

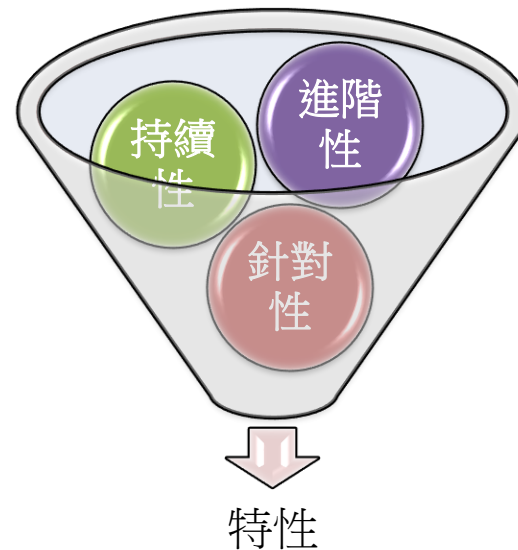


- ✓ Brain病毒（1986）：世界上第一個已知病毒，由巴基斯坦的兩名程式員創建，主要感染IBM PC的軟碟片。
- ✓ Morris蠕蟲（1988）：第一個網絡蠕蟲病毒，通過互聯網快速傳播，造成大量計算機癱瘓
- ✓ ILOVEYOU病毒（2000）：通過電子郵件傳播的病毒，以誘人的標題吸引用戶點擊附件，導致大量數據損毀。

一

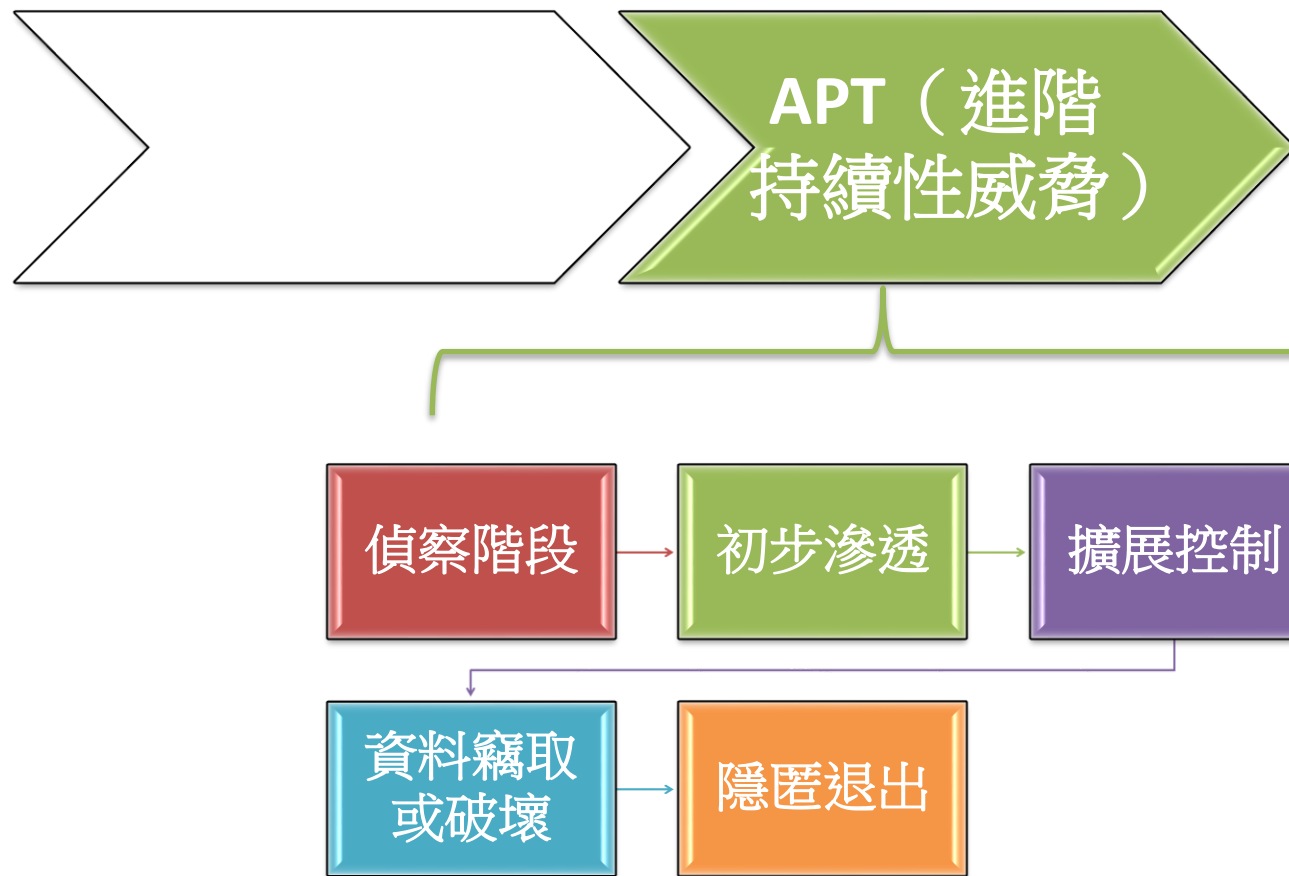
# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加



# 一 資訊安全威脅趨勢

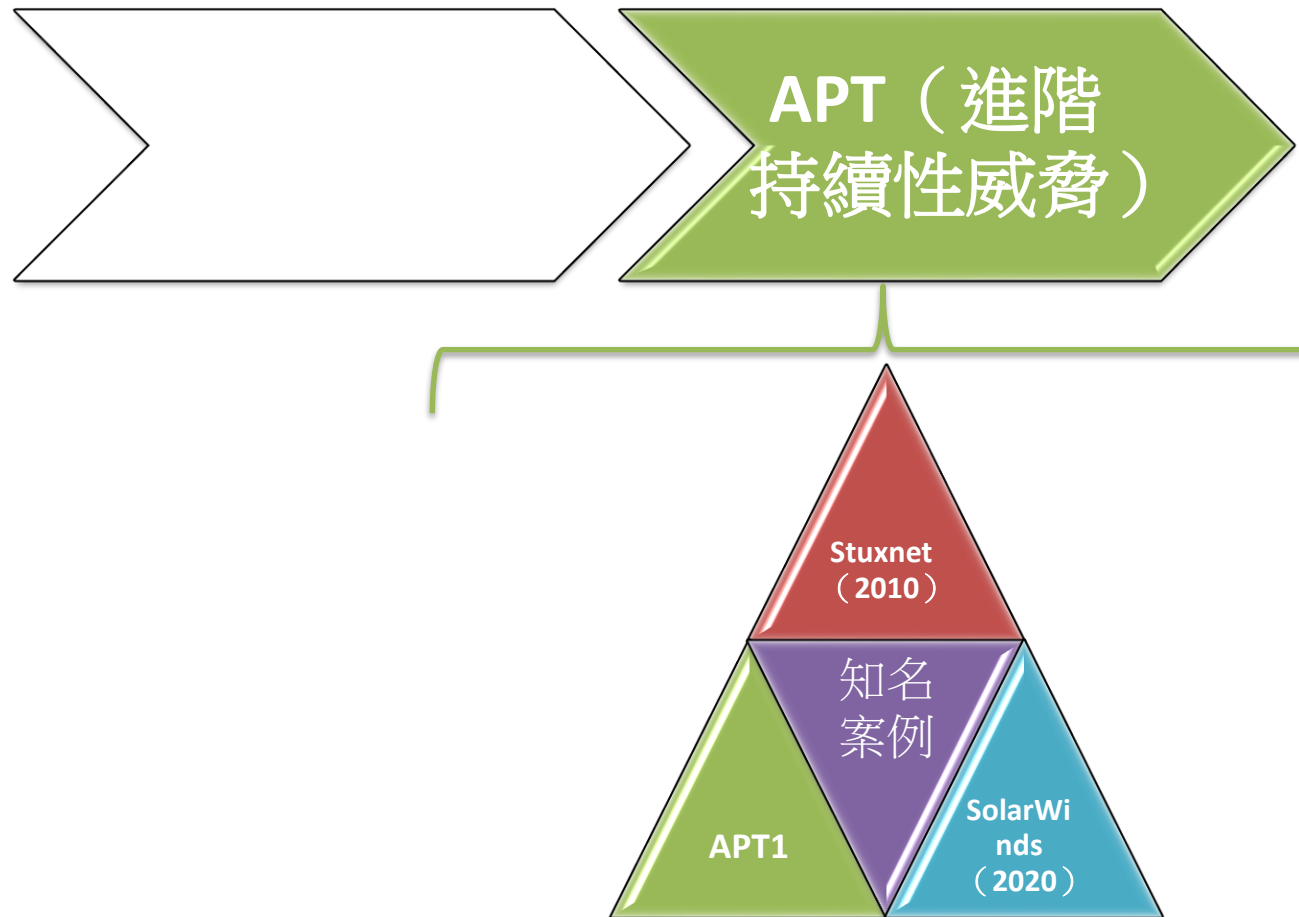
威脅的演變與  
複雜性增加



一

# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加





## 威脅的演變與 複雜性增加

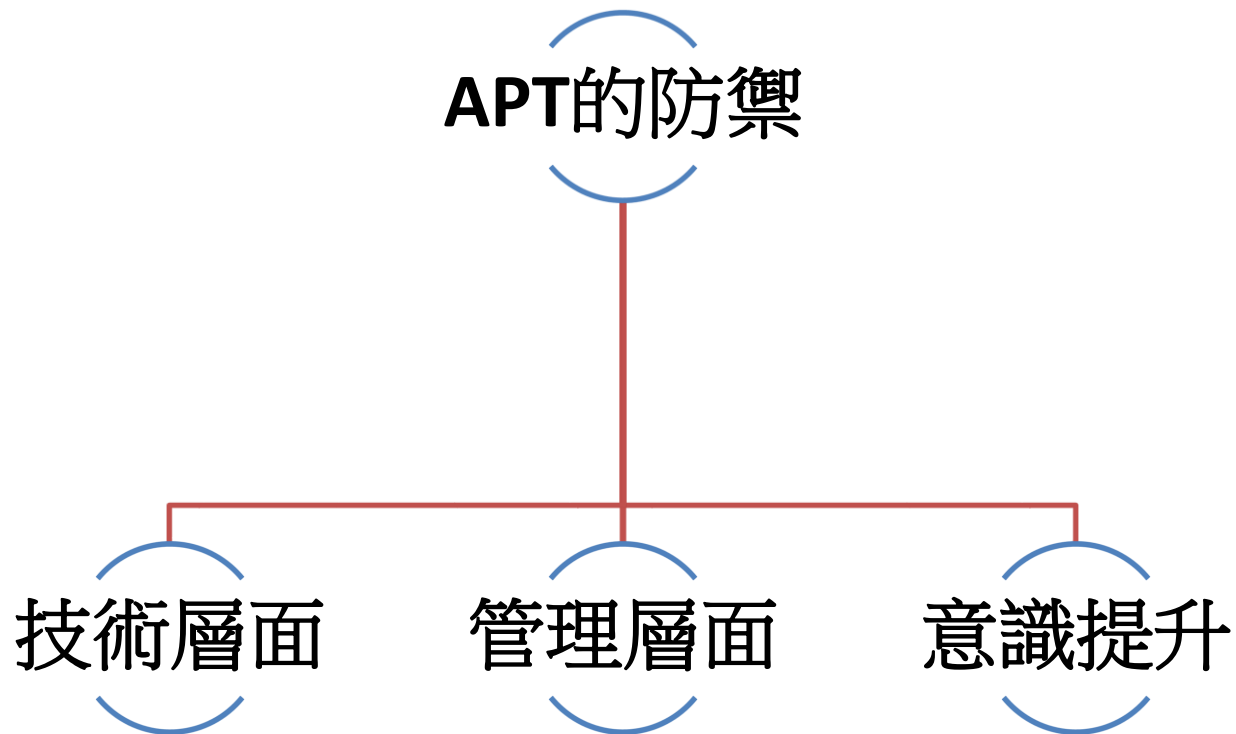
### 病毒與APT的對比

特徵	早期病毒攻擊	APT進階持續性威脅
攻擊目標	普遍性、大量用戶	高價值目標（政府、企業）
技術複雜度	相對簡單	高技術、多階段滲透
目的	惡作劇、炫技	竊取敏感數據、破壞基礎設施
偵測難度	容易偵測並清除	隱匿性高，難以察覺
持續時間	短期攻擊	長期、持續性滲透

一

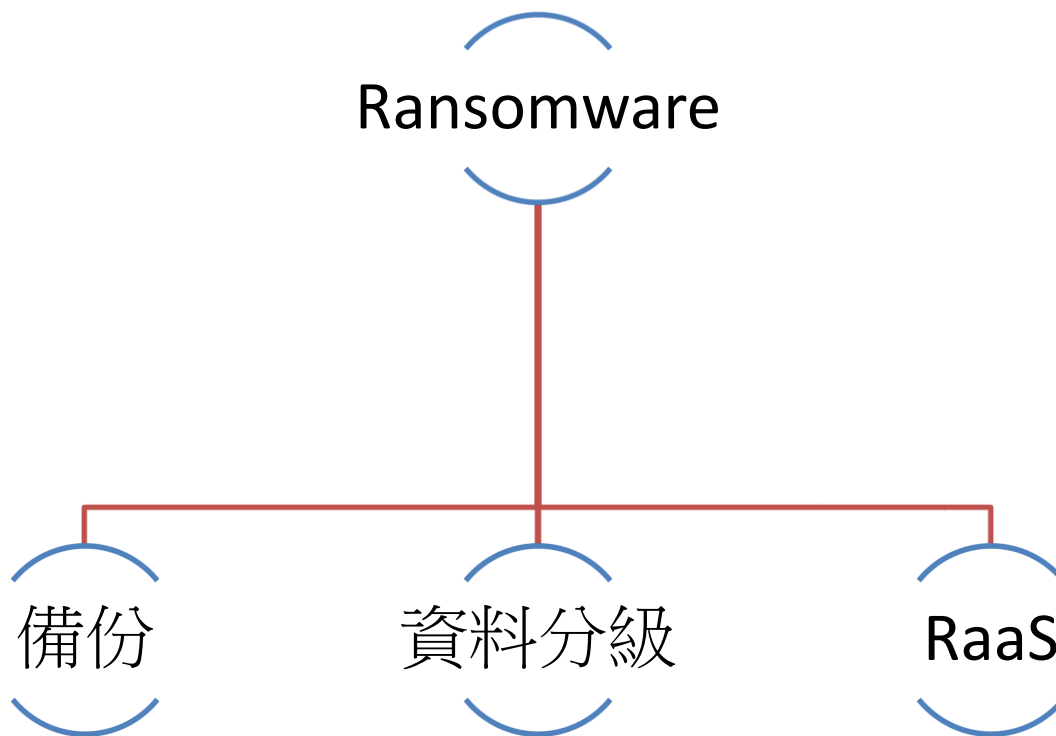
# 資訊安全威脅趨勢

威脅的演變與  
複雜性增加



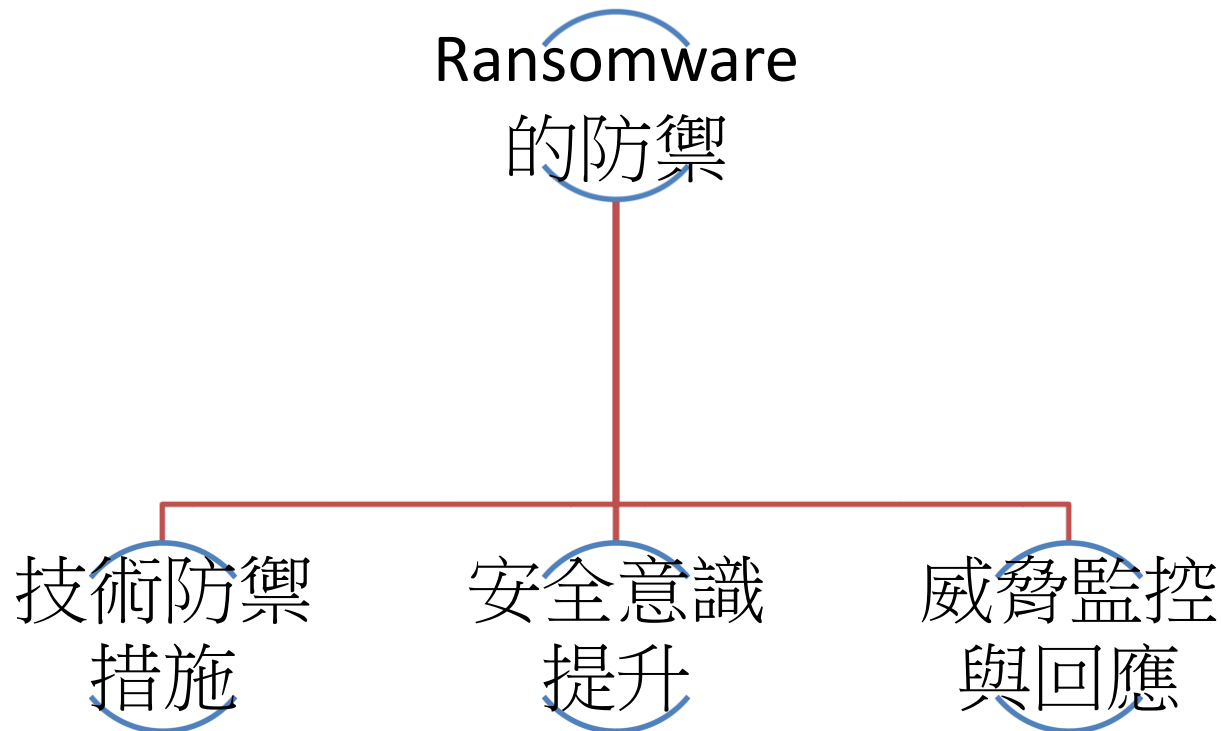
# 一 資訊安全威脅趨勢

威脅的演變與  
複雜性增加



# 一 資訊安全威脅趨勢

威脅的演變與  
複雜性增加



# 大綱子題

二

## 網路攻擊現況

1

### 駭客攻擊案例

2

### AI資安威脅與社交工程攻擊

## 二

# 網路攻擊現況

駭客攻擊案例

典型攻擊  
案例

攻擊手段  
的多樣性

### 駭客攻擊案例

#### 典型攻擊 案例



Image generated by DALL · E

2024 年，全球資料外洩事件頻傳，造成企業龐大經濟損失和聲譽影響。從電信巨擎 AT&T、醫療保健 Change Healthcare，到雲端資料產業 Snowflake，大型企業成為目標，大量敏感資料外洩。

### 駭客攻擊案例

#### 典型攻擊 案例

台積電晶圓廠之所以爆發大規模的病毒感染有兩個關鍵，其一是新機臺上線的SOP程序因為人為疏失出錯，導致早已藏匿病毒的機臺沒有被防毒軟體擋下。加上台積所有臺灣廠區的生產網路全部連結在一起，才會因為一臺機臺染上病毒，就造成北中南廠區大規模疫情的嚴重後果。



台積產線中毒大當機

主要衝擊是交貨延遲問題  
預估營收損失從78億元降低到52億元，  
但仍是破紀錄災損

看似無害的違反SOP小疏忽，最後竟導致52億元的預估營收損失



### 駭客攻擊案例

#### 典型攻擊 案例

### 2024 關鍵基礎設施調查報告： 能源與水利復原成本四倍暴增，漏洞利用攻擊占半數



Sophos今天發布最新行業調查報告《2024 年關鍵基礎設施的勒索軟體現況》。該報告顯示過去一年中，能源和水利兩個關鍵基礎設施行業的中位數復原成本暴增四倍，達到 300 萬美元。這是全球跨行業中位數的四倍。此外，針對這兩個關鍵基礎設施行業的勒索軟體攻擊，其中 49% 是源自於漏洞利用。

## 二

# 網路攻擊現況

駭客攻擊案例

攻擊手段  
的多樣性

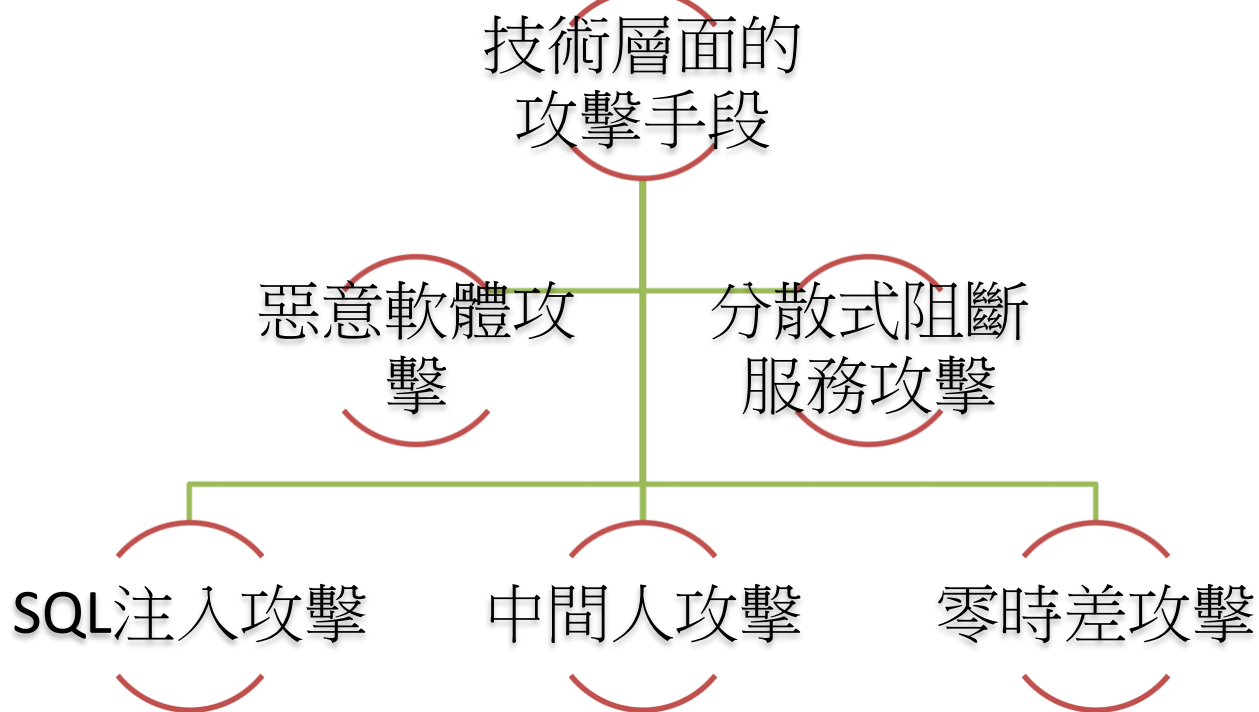


## 二 網路攻擊現況

駭客攻擊案例

攻擊手段  
的多樣性

技術  
層面



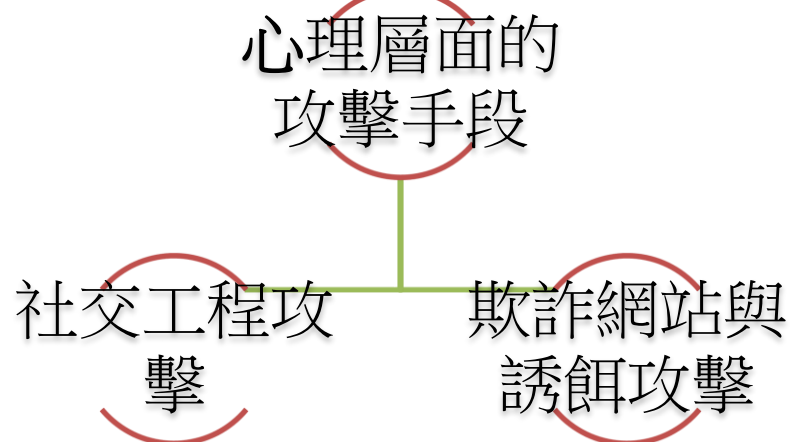
## 二

# 網路攻擊現況

駭客攻擊案例

攻擊手段  
的多樣性

心理  
層面



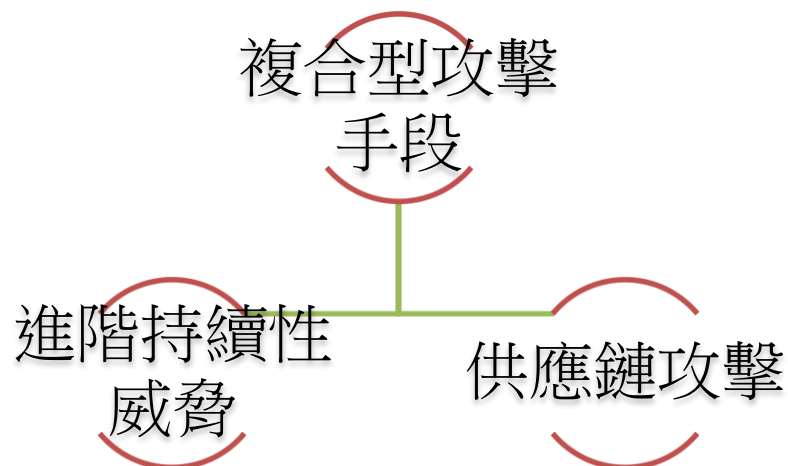
## 二

# 網路攻擊現況

駭客攻擊案例

攻擊手段  
的多樣性

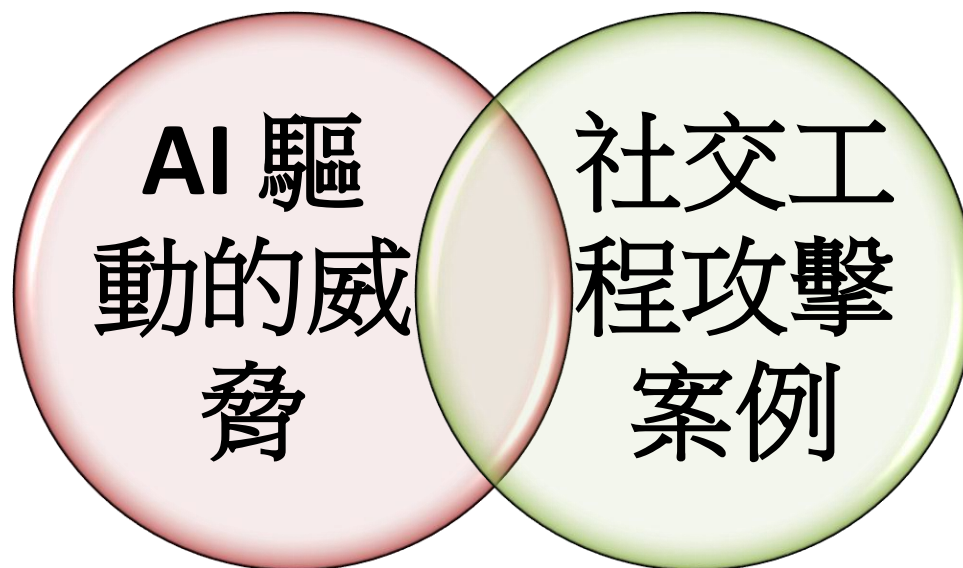
複合  
型



## 二

# 網路攻擊現況

AI資安威脅與  
社交工程攻擊



AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### AI如何用於生成惡意代碼與攻擊工具

基於生成式模型的惡意代碼  
開發

代碼混淆與加密技術的優化

多樣化變種建立

AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### AI輔助攻擊工具的開發

自動化漏洞  
探測

生成網釣攻  
擊

社交工程工  
具的增強

攻擊自動化



AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

優勢

### AI攻擊的優勢與挑戰

- ✓ **速度快**：AI工具能快速生成大量惡意代碼或變種，超越傳統手工編碼的效率。
- ✓ **高隱蔽性**：生成的代碼或攻擊策略能針對特定目標進行優化，降低被檢測的可能性。
- ✓ **降低技術門檻**：不需要攻擊者具備專業技能，AI可完成大部分技術細節。

AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

心理  
層面

### AI攻擊的優勢與挑戰

- ✓ 攻擊者的學習成本：雖然AI降低了技術門檻，但攻擊者仍需學習如何有效利用AI。
- ✓ 資源依賴：高效的AI模型需要大量計算資源，對資源有限的攻擊者構成限制

AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### AI攻擊的防範措施與應對策略

加強源碼審查與  
安全測試

人工智慧反制技  
術

教育與意識提升

AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### Deepfake與網路詐騙

假冒身份詐  
騙

網釣詐騙

商業詐騙

偽造名人或  
企業形象

勒索與聲譽  
威脅

AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### Deepfake詐騙特點與威脅



AI資安威脅與  
社交工程攻擊

AI 驅動的  
威脅

### 降低Deepfake詐騙風險

技術防護

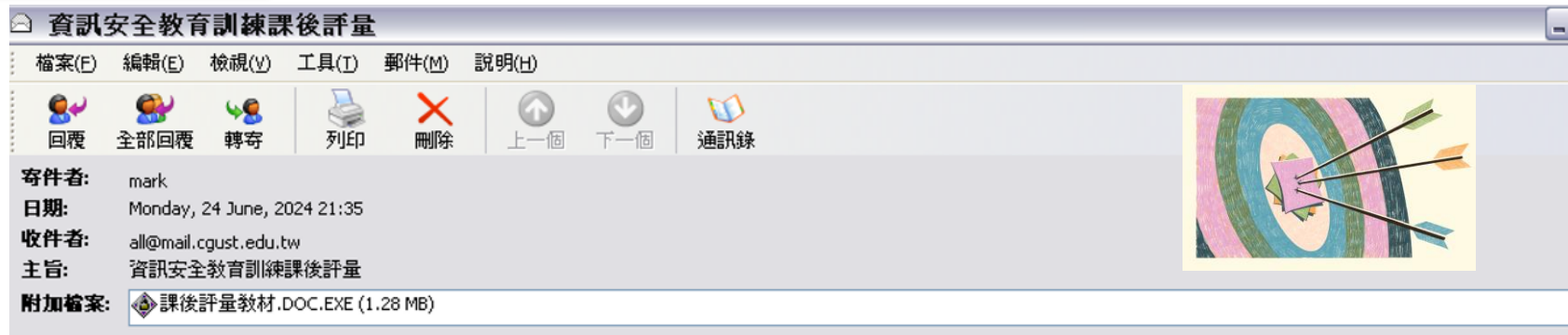
身份驗證  
機制

提高安全  
意識

## AI資安威脅與 社交工程攻擊

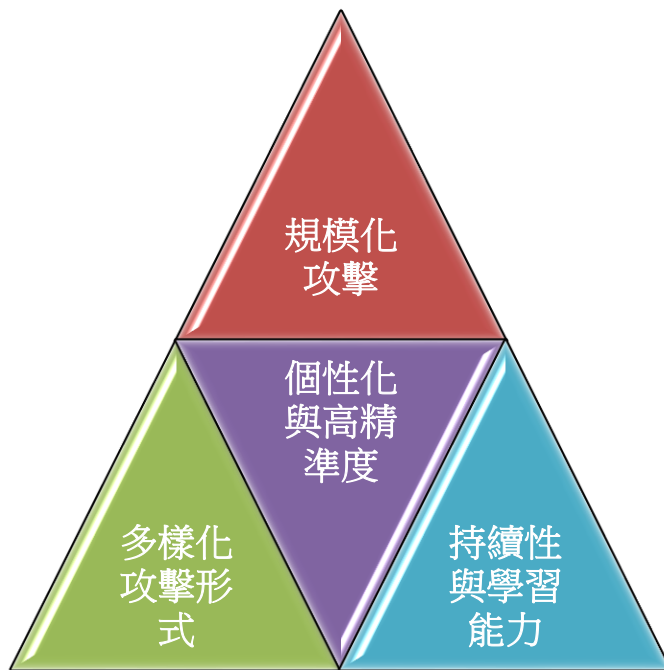
### 社交工程 攻擊案例

## AI驅動的社交工程攻擊



AI資安威脅與  
社交工程攻擊

### AI驅動的社交工程攻擊特性





### AI資安威脅與 社交工程攻擊

## AI驅動的社交工程攻擊風險



# 大綱子題

## 三 資訊安全應有之認知

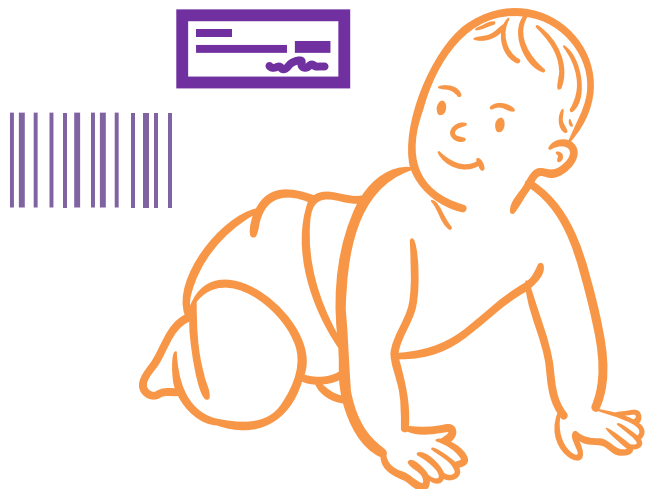
### 1 個人應有之認知

### 2 組織應有之作為

三

# 資訊安全應有之認知

個人應有  
之認知



網路好奇寶寶

數位  
足跡  
管理

日常  
習慣  
養成

三

## 資訊安全應有之認知

### 個人應有 之認知

### 惡意程式退散

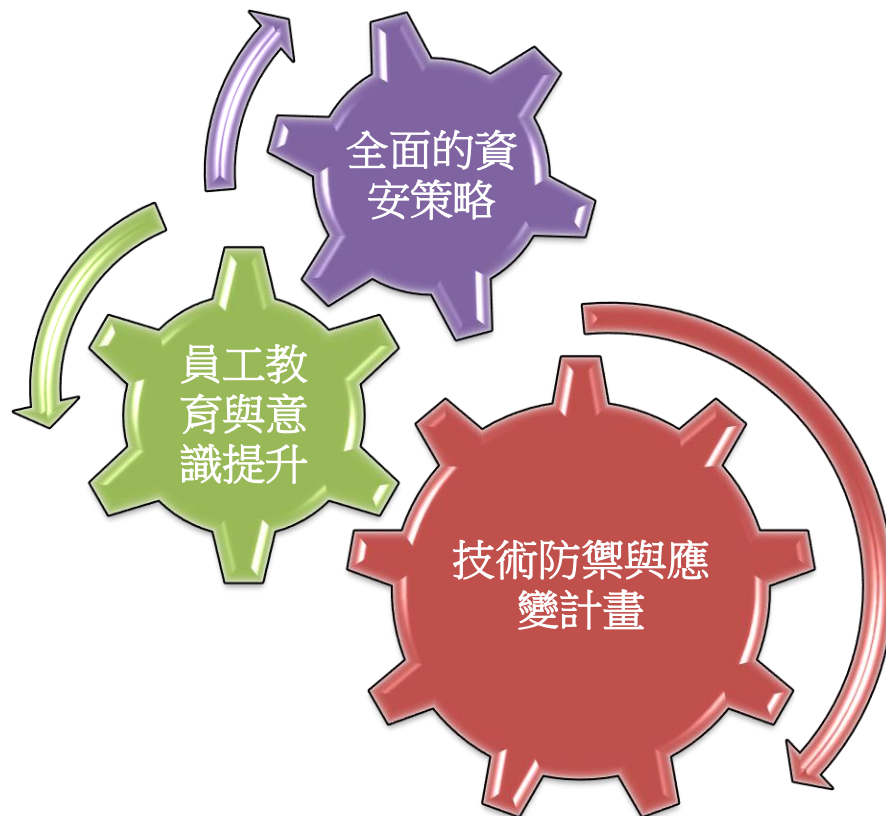
不隨意開啟來路不明之電子郵件  
不隨意點擊來路不明之連結或附件  
安裝防毒軟體並更新病毒碼  
定期執行病毒掃描  
定期執行弱點修補  
隨時注意電腦或網路使用狀態



三

## 資訊安全應有之認知

組織應有  
之作為



三

# 資訊安全應有之認知

組織應有  
之作為

## 風險管理機制

風險評鑑



風險處理



控制措施

資通  
安全  
維護  
計畫

資通安全管理政策  
資通安全組織架構管理作業程序  
資訊資產盤點管理作業程序  
風險管理作業程序  
資通管理作業程序  
資通安全事件通報及應變作業程序  
資通安全教育訓練管理作業程序  
內部稽核管理作業程序  
資通安全管理審查作業程序  
.....

## 四 討論