

政府人工智慧： 智慧治理、行政創新與風險管理

(AI in Government: Smart Governance, Administrative Innovation, and Risk Management)

時間：115年9月4日 9:00-12:00

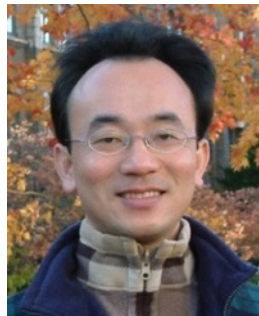
主辦單位：農業部農田水利署瑠公管理處

承辦單位：台灣水資源與農業研究院

 NVIDIA
University Ambassador
Certified Instructor

 aws
educate | Cloud
Ambassador
2020 Cohort

 aws
academy
Accredited
Educator
 aws
certified
Cloud
Practitioner
 aws
certified
Solutions
Architect
Associate



戴敏育 教授 (Prof. Min-Yuh Day)

國立臺北大學 資訊管理研究所 所長

跨域 AI 前瞻研究中心 (AI4X NTPU) 主任





戴敏育 教授

Prof. Min-Yuh Day



University Ambassador

Certified Instructor



Cloud Ambassador

2020 Cohort

aws academy

Accredited Educator

aws certified

Solutions Architect

Associate

aws certified

Cloud Practitioner

Director, Information Management, NTPU

Director, Intelligent Financial Innovation Technology, IFIT Lab, IM, NTPU

Director, Advanced Research Center for Cross-Disciplinary AI (AI4X), NTPU

Visiting Scholar, IIS, Academia Sinica

Ph.D., Information Management, NTU

Artificial Intelligence, Agentic AI, ESG and Green Financial Technology,
Big Data Analytics, Electronic Commerce



國立臺北大學
National Taipei University



Outline



1. 人工智慧最新發展趨勢

Latest AI Development Trends

2. 生成式AI於政府行政之應用案例 (含AI工具介紹)

Generative AI Use Cases in Government Administration
(with AI Tool Introductions)

3. AI應用風險、資訊安全與倫理治理

AI Application Risks, Information Security, and
Ethical Governance

今天要帶走的三件事

Three Takeaways for Today



- 1 看懂AI正在改變政府工作的方式
- 2 學會把AI用在行政、庶務與協作流程
- 3 建立安全、合規、負責任的AI使用習慣

為什麼政府現在必須理解AI？

Why Government Must Understand AI Now



AI不只是科技工具，
而是行政流程、公共服務與治理模式的改變。

重點不是「AI會不會取代人」，
而是「人如何用AI提升判斷、效率與服務品質」。

AI的演進：從判斷走向生成與行動

The Evolution of AI: From Judgment to Generation and Action



4

物理AI

Physical AI

感測、控制實體設備、自主巡查（例：水閘自動控制）

3

代理式AI

Agentic AI

規劃、呼叫工具、採取行動（例：自動調度灌溉排程）

2

生成式AI

Generative AI

生成、摘要、轉寫（例：會勘紀錄摘要、巡檢報告初稿）

1

判別式AI

Discriminative AI

分類、預測、異常偵測（例：灌溉異常偵測、缺水風險評分）

Generative AI, Agentic AI, Physical AI

Physical AI

Self-driving cars
General robotics

Agentic AI

Coding assistants
Customer service
Patient care

Generative AI

Digital marketing
Content creation

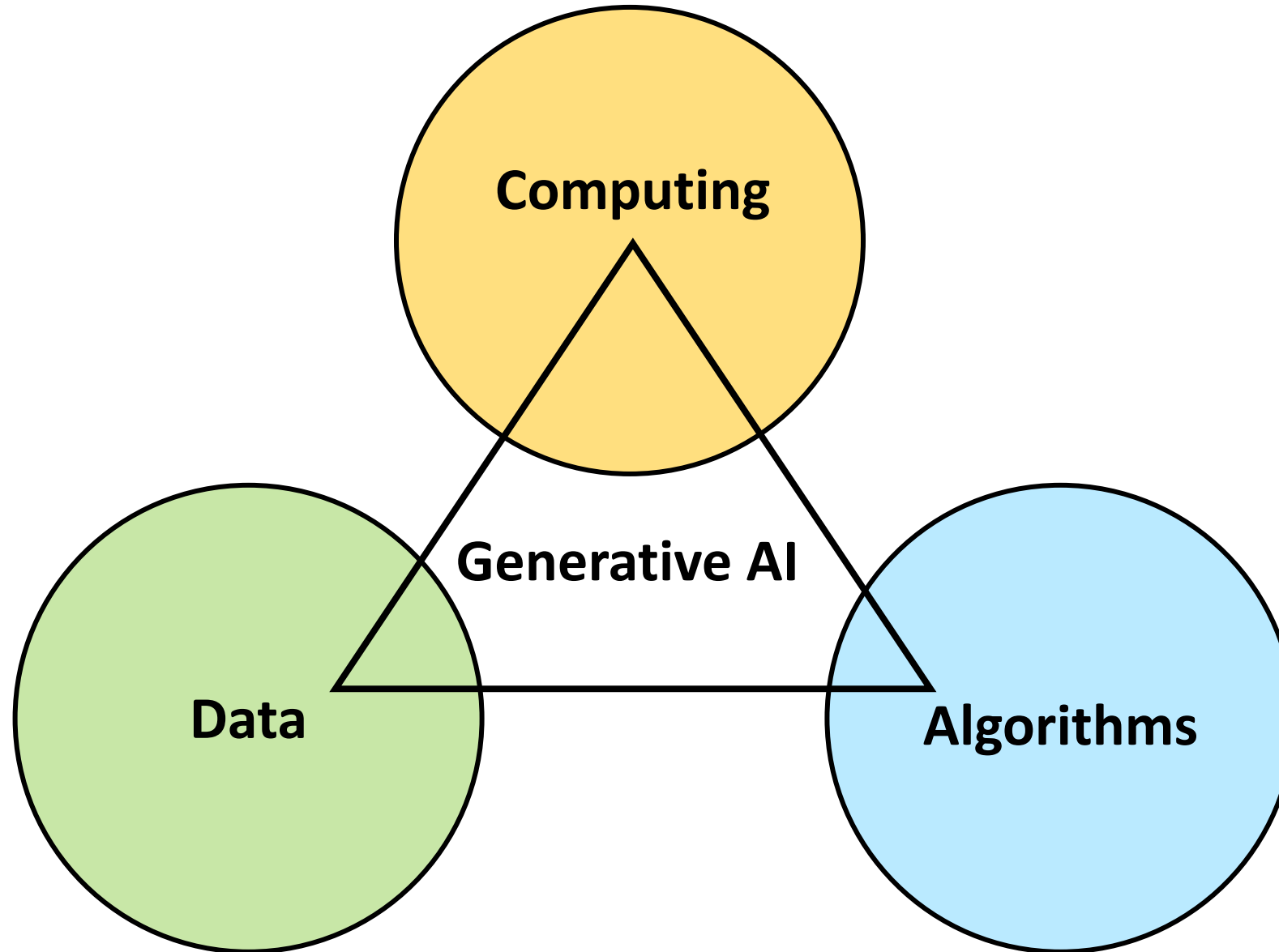
Perception AI

Speech recognition
Deep recommender systems
Medical imaging

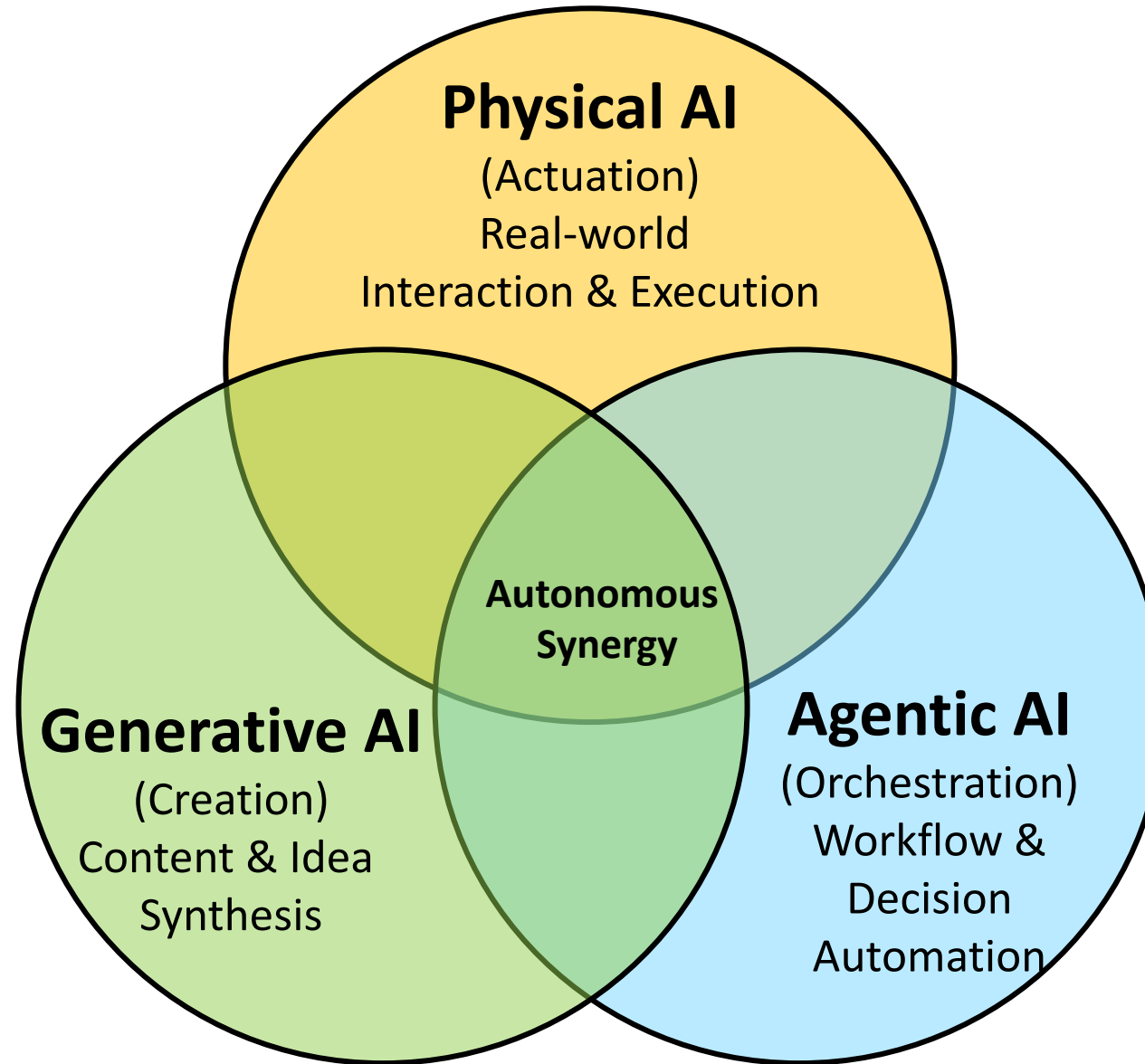
2012 AlexNet

Deep learning breakthrough

Generative AI



Generative AI, Agentic AI, Physical AI

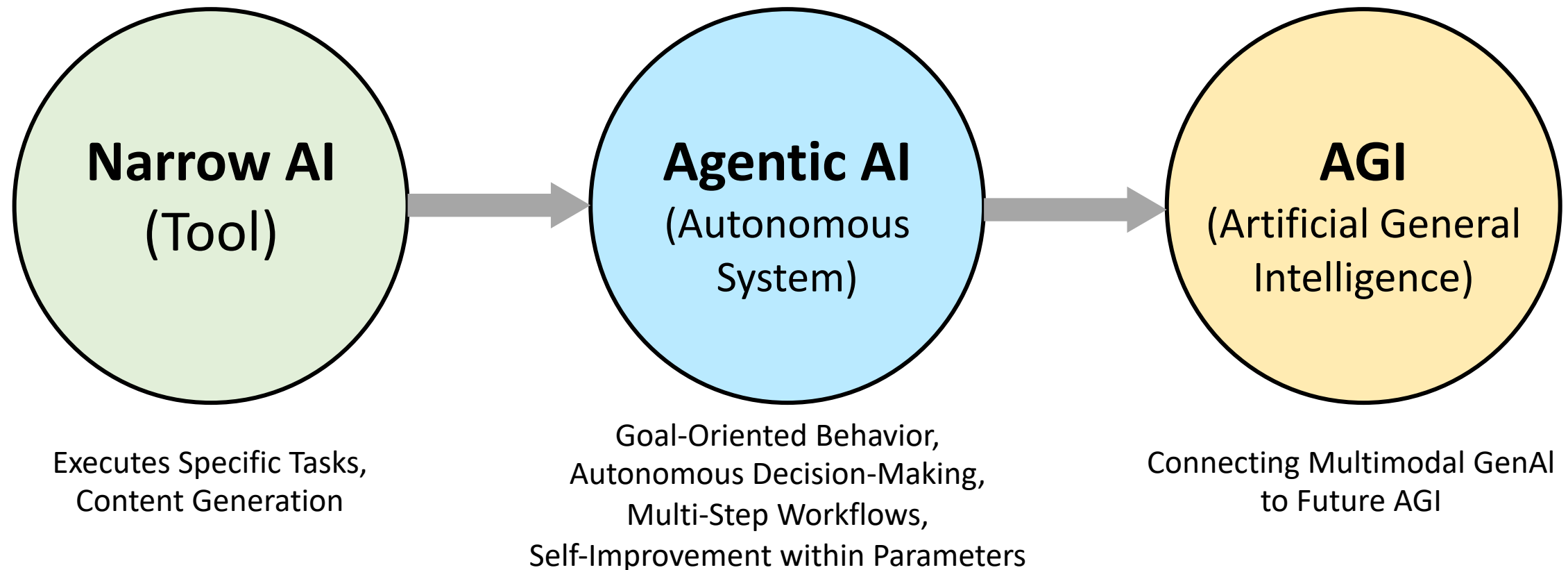


**New Economic
Paradigm Shift:
From Creation
to Execution**

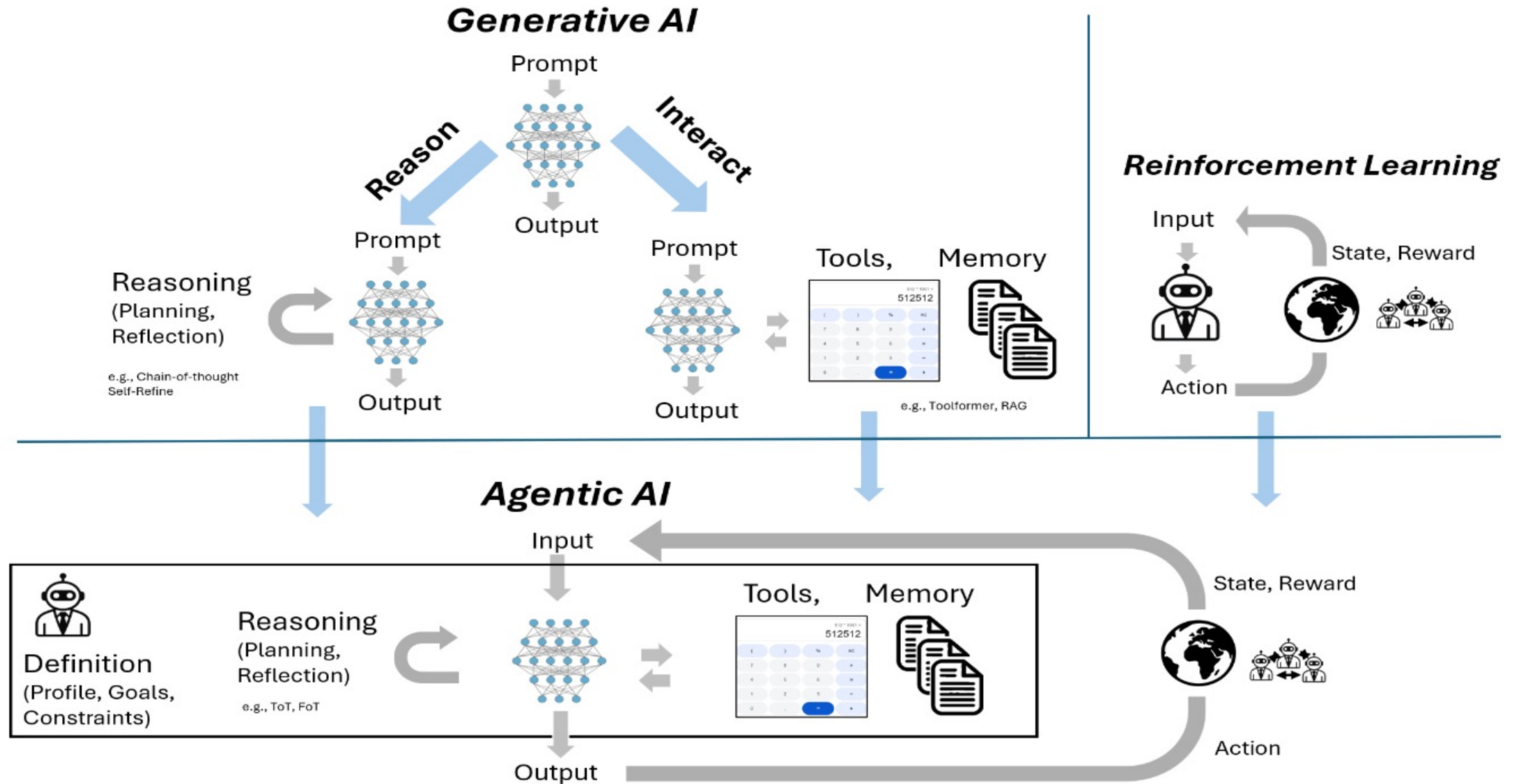
The Future of AI

From Tools to Agents:

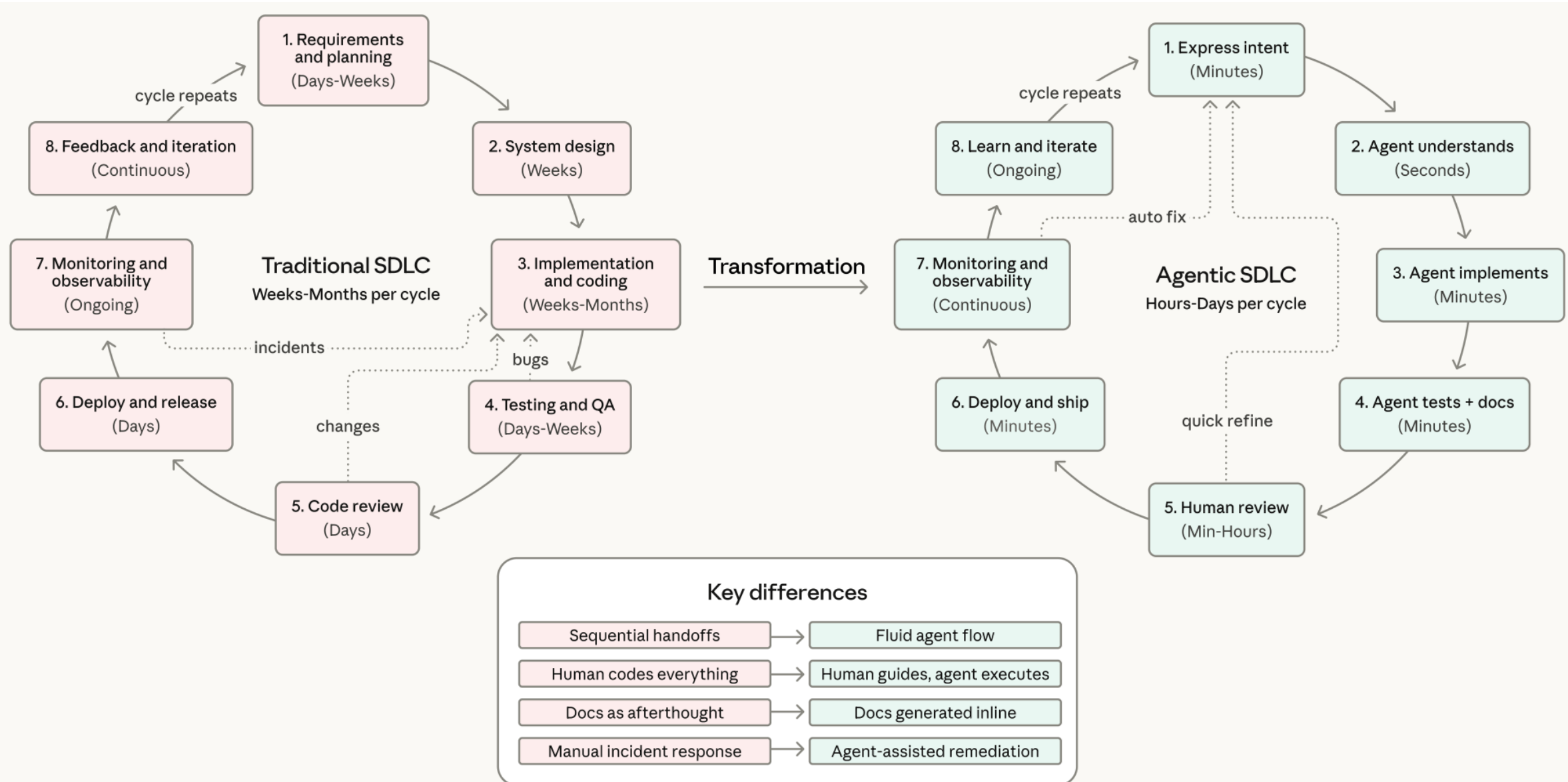
The Rise and Autonomy of Agentic AI



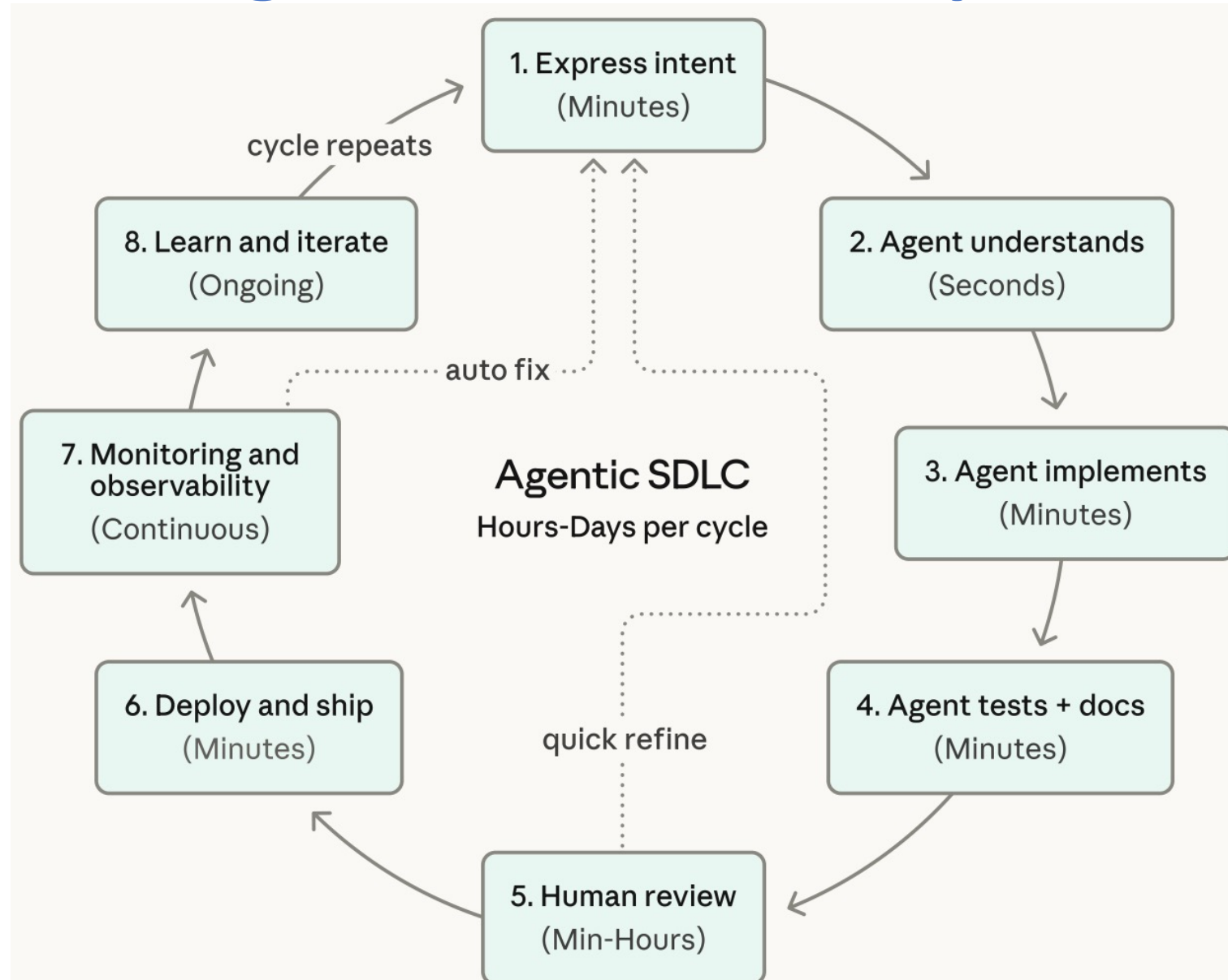
From Generative AI to Agentic AI



Agentic Coding Software Development Lifecycle



Agentic Coding Software Development Lifecycle



生成式AI助理與代理式AI的差別

Generative AI Assistants vs. Agentic AI



生成式AI助理

依提示產生內容，
通常由人逐次操作；
錯誤多停留在文字層。

代理式AI

保有目標與狀態，
可呼叫資料庫、API、工作流
；錯誤可能變成真實行動。

大型語言模型的運作原理

How Large Language Models (LMMs) Work



1

輸入

提示、文件、對話

2

表示

文字轉成 token

3

預測

計算下一個 token 的機率

4

生成

逐步形成回答

生成式AI的核心能力

Core Capabilities of Generative AI



生成

摘要

分類

改寫

翻譯

比對

推理

問答

模擬情境

政府常見應用：公文草稿、會議摘要、資料整理、民眾問答、教育訓練、知識查詢。

AI治理的國際趨勢

International Trends in AI Governance



OECD AI原則強調可信賴、人本、尊重人權與民主價值，並於2019年採納、2024年更新。

政府導入AI時，信任不是附加價值，而是使用前提。

AI風險管理趨勢

Trends in AI Risk Management



NIST AI風險管理框架主張在AI設計、開發、使用與評估過程中納入可信賴考量。

2024年另發布生成式AI風險管理相關文件。

政府AI的兩大方向

Two Directions for Government AI



對內

提升行政效率、
減少重複工作

對外

改善公共服務、
提升回應速度與品質

從「數位化」到「智慧化」

From Digitalization to Intelligence



1

數位化

把紙本變成電子資料。

2

自動化

把固定流程交給系統。

3

智慧化

讓AI協助理解、判斷、摘要、預警與決策支援。

農田水利業務中的AI機會

AI Opportunities in Irrigation Authority Operations



水情資料整理

灌溉排程輔助

會勘紀錄摘要

工程文件檢核

民眾陳情分類

跨單位協作追蹤

庶務採購
資料整理

AI最適合協助的工作

Tasks Best Suited for AI Assistance



重複性高

文字量大

資料分散

需快速彙整

需要初稿

需要比對規定

需要建立清單

AI不適合直接取代的工作

Tasks AI Should Not Directly Replace



涉及裁量

機密事項

個資判斷

法定職權

權利義務判斷

敏感決策

最終核定

危機處理

政府使用AI的核心觀念

Core Principles for Government Use of AI



- 1 AI可以協助，但不能卸責
- 2 AI可以產生草稿，但不能自動代表機關立場
- 3 AI可以提供建議，但最後仍由承辦人與主管負責

行政院生成式AI指引重點

Key Points of the Executive Yuan's Generative AI Guidelines



- 1 不得提供公務應保密資訊、
個人資料或未經同意公開資訊
- 2 機密文書應由承辦人親自撰寫，
禁止使用生成式AI
- 3 使用AI應遵守資安、個資、著作權等規定

AI素養的五個能力

Five Core AI Literacy Skills



1

問對問題

2

判斷資料能不能輸入

3

驗證AI答案

4

保留人工審查

5

留下使用紀錄

Outline



1. 人工智慧最新發展趨勢

Latest AI Development Trends

2. 生成式AI於政府行政之應用案例 (含AI工具介紹)

Generative AI Use Cases in Government Administration
(with AI Tool Introductions)

3. AI應用風險、資訊安全與倫理治理

AI Application Risks, Information Security, and
Ethical Governance

AI導入行政工作的基本流程

Basic Workflow for Adopting AI in Administration



1 盤點工作

2 選擇低風險場景

3 設計提示詞

4 產出初稿

5 人工檢核

6 修正定稿

7 建立SOP

案例一：會議紀錄摘要

Case 1: Meeting Minutes Summary



可協助整理：

會議重點

決議事項

待辦清單

負責單位

期限

風險提醒

會議紀錄提示詞範例

Sample Prompt: Meeting Minutes



提示詞範例

請將以下會議逐字稿整理為：

- 會議重點
- 決議事項
- 待辦事項表格
- 需主管確認事項
- 不確定資訊請標示「需人工確認」

案例二：公文與函稿初稿

Case 2: Official Document Drafting



AI可協助：

語氣調整

段落架構

法規
引用提醒

格式檢核

注意：不可輸入機密、個資、未公開案情；
正式內容仍須人工確認。

公文草稿提示詞範例

Sample Prompt: Official Document Draft



提示詞範例

請依政府機關正式語氣，協助草擬一份函稿架構。

目的：通知受文者辦理教育訓練報名。

請輸出：主旨、說明、辦法。

限制：不得自行創造法規或日期。

案例三：庶務協作

Case 3: Administrative Collaboration



AI可協助：

活動流程表

採購需求摘要

場地檢核表

物品清單

報到流程

講義整理

問卷摘要

庶務協作提示詞範例

Sample Prompt: Administrative Collaboration



提示詞範例

請協助製作教育訓練活動檢核表，分為：

會前準備、當日執行、會後結案。

每項請包含負責人、完成期限、注意事項。

案例四：民眾陳情分類

Case 4: Public Complaint Classification



AI可先協助分類：

水路維護

灌溉需求

設施損壞

用地問題

施工影響

其他

但不得讓AI直接做成行政處分或權利義務判斷。

案例五：資料彙整與決策支援

Case 5: Data Aggregation and Decision Support



可用於整理水情、災害通報、巡檢紀錄、工程進度、歷史案件。

重點：AI協助看趨勢，人負責做決策。

案例六：內部知識庫問答

Case 6: Internal Knowledge Base Q&A



將法規、SOP、常見問答、教育訓練資料整理成內部知識庫。

同仁可用自然語言查詢「這件事應該怎麼辦」。

RAG觀念：讓AI查自己的資料

The RAG Concept: Letting AI Search Its Own Data



1

定義

RAG = 檢索增強生成。

2

做法

先找出機關授權資料，再讓AI根據資料回答。

3

好處

降低AI亂編、提升可追溯性。

AI工具類型介紹

Types of AI Tools



通用型聊天AI

文件摘要與寫作工具

會議紀錄工具

試算表與資料分析工具

知識庫 / 內部問答系統

自動化流程工具

常見生成式AI工具介紹

Common Generative AI Tools



ChatGPT

OpenAI · 擅長文字生成與摘要

Claude

Anthropic · 擅長長文件分析與寫作

Gemini

Google · 整合文件與試算表工具

Microsoft Copilot

整合 Word、Excel、Outlook

NotebookLM

鎖定指定文件回答問題，附來源

會議逐字稿工具

自動轉錄會議錄音，產出重點摘要

行政工作與建議工具類型對照

Administrative Tasks vs. Recommended Tool Types



會議紀錄整理

→ 會議逐字稿與摘要工具

公文與函稿初稿

→ 通用型聊天式AI

資料彙整與分析

→ 試算表與資料分析工具

內部知識庫問答

→ 知識庫 / RAG 問答系統

庶務活動協作

→ 通用型聊天式AI / 文件摘要工具

流程提醒與追蹤

→ 自動化流程工具

選工具前先問五個問題

Five Questions Before Choosing a Tool



- 1 資料會送到哪裡？
- 2 是否會被拿去訓練？
- 3 能否關閉外部分享？
- 4 是否保留紀錄？
- 5 是否符合機關資安與採購規範？

好提示詞公式

A Formula for Good Prompts



提示詞範例

公式：角色 + 任務 + 資料 + 格式 + 限制 + 檢核

範例：你是政府行政幕僚，請根據以下資料整理會議摘要，輸出表格，不得新增未提供資訊，疑義請標示。

AI回覆要怎麼檢查？

How to Verify an AI Response



查來源

查日期

查法規

查數字

查語氣

查是否有個資

查是否涉及機密

查是否過度推論

小練習：把工作交給AI前

Quick Exercise: Before Handing a Task to AI



1

能不能用AI？

2

可輸入哪些資料？

3

哪些資料不能輸入？

4

AI產出後誰負責檢查？

第二單元小結

Unit 2 Summary



AI最先帶來價值的地方，是把「整理、摘要、初稿、分類、檢核」做好。

真正的行政專業，仍在承辦人的判斷與責任。

Outline



1. 人工智慧最新發展趨勢

Latest AI Development Trends

2. 生成式AI於政府行政之應用案例 (含AI工具介紹)

Generative AI Use Cases in Government Administration
(with AI Tool Introductions)

3. AI應用風險、資訊安全與倫理治理

AI Application Risks, Information Security, and
Ethical Governance

AI風險不是不用，而是要會管

AI Risk Isn't About Avoidance, But Management



不用AI可能失去效率；

亂用AI可能造成外洩、錯誤、偏見與責任不清。

目標：安全使用、可控導入、可追溯管理。

政府AI風險地圖

Government AI Risk Map



資安風險

個資風險

機密外洩

錯誤資訊

偏見歧視

著作權風險

責任歸屬不清

供應商與
採購風險

風險一：機密與未公開資訊

Risk 1: Confidential and Undisclosed Information



不可輸入：

尚未公告政策

內部簽呈

採購底價

個案資料

人事資料

爭議案件資料

內部帳號密碼

風險二：個人資料

Risk 2: Personal Data



姓名

身分證字號

電話

地址

病歷

財務

申訴內容

員工資料

原則：不必要就不蒐集、不輸入、不複製。

風險三：AI幻覺

Risk 3: AI Hallucination



AI可能把不存在的法規、數字、案例講得很像真的。

處理方式：

凡涉及法規、金額、日期、決策依據，一律回查正式來源

風險四：偏見與不公平

Risk 4: Bias and Unfairness



AI可能受到訓練資料影響，產生刻板印象或不公平建議。

政府使用AI時，須特別注意公平性、透明性與救濟機制。

風險五：著作權與人格權

Risk 5: Copyright and Personality Rights



AI產出不一定完全可自由使用。

對外發布前應確認圖片、文字、資料來源與引用方式，
避免侵害著作權或人格權。

風險六：提示注入攻擊

Risk 6: Prompt Injection Attacks



惡意文件可能指示AI忽略規則、洩漏資料或產生錯誤答案。

內部知識庫與文件摘要系統尤其需要防護。

風險七：影子AI

Risk 7: Shadow AI

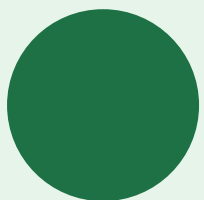


同仁自行使用未核准工具，可能導致資料外洩、紀錄不可查、責任難追。

解方：建立可用工具清單、禁止事項、申請流程。

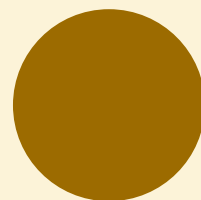
AI使用紅黃綠燈

AI Use Traffic Light System



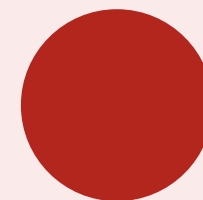
綠燈

公開資料、
教育訓練、
一般文字潤飾。



黃燈

內部資料、草案
、會議資料，
須去識別化與
主管確認。



紅燈

機密、個資、
採購敏感資料、
未公開決策，
不得輸入。

政府AI治理架構

Government AI Governance Framework



政策原則：

能用

會用

敢用

慎用

管理機制：

資料分級

工具分級

使用紀錄

人工覆核

教育訓練

稽核改善

AI導入前檢核表

Pre-Adoption Checklist for AI



1 業務目的清楚嗎？

4 有人負責審查嗎？

2 資料可以使用嗎？

5 產出可追溯嗎？

3 風險等級判斷了嗎？

6 錯誤時如何補救？

AI使用SOP建議

Recommended SOP for AI Use



1 先判斷資料等級

2 選擇核准工具

3 撰寫提示詞

4 產出初稿

5 人工驗證

6 主管審核

7 留存紀錄

8 定期檢討

溜公管理處可優先試行場景

Priority Pilot Scenarios for Liugong Management Office



會議紀錄摘要

教育訓練教材

庶務活動檢核表

公開資料問答

巡檢紀錄格式化

內部SOP查詢

行動承諾

Action Commitment



每位同仁回到工作崗位後，選一項低風險工作試用AI：

不輸入敏感資料

不直接採信答案

不省略人工審查

原則：安全使用、如實核對、保留人工把關。

結語

Closing Remarks



AI不是替政府做決定，
而是協助政府更快整理資訊、
更好服務民眾、
更穩健管理風險。

智慧治理的核心，仍是人的專業、責任與信任。

Summary



1. 人工智慧最新發展趨勢

Latest AI Development Trends

2. 生成式AI於政府行政之應用案例 (含AI工具介紹)

Generative AI Use Cases in Government Administration
(with AI Tool Introductions)

3. AI應用風險、資訊安全與倫理治理

AI Application Risks, Information Security, and
Ethical Governance

農業部農田水利署瑠公管理處
115-116年度員工知能培訓及庶務協作計畫



Q & A

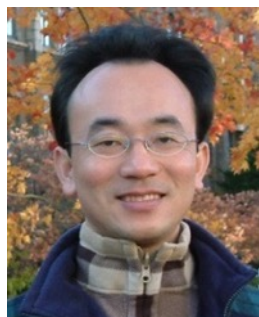
政府人工智慧： 智慧治理、行政創新與風險管理

(AI in Government: Smart Governance, Administrative Innovation, and Risk Management)

時間：115年9月4日 9:00-12:00

主辦單位：農業部農田水利署瑠公管理處

承辦單位：台灣水資源與農業研究院



戴敏育 教授 (Prof. Min-Yuh Day)

國立臺北大學 資訊管理研究所 所長

跨域 AI 前瞻研究中心 (AI4X NTPU) 主任

