



# 數位轉型與智慧政府的課責

政治大學公共行政學系  
黃東益 教授

2020/07/30

# 大綱

一

**從電子化政府轉向智慧政府**

二

**數位轉型的內涵與障礙**

三

**課責作為克服數位轉型障礙的機制**

四

**課責與智慧政府的建構：以eID為例**

五

**討論與建議**



# 從電子化政府轉向智慧政府



# 臺灣電子化政府的推動歷程

國發會配合行政院「2017 – 2025 數位國家・創新經濟發展方案」，  
研議規劃「服務型智慧政府推動計畫」

## 我國電子化政府(e-Government)推動歷程



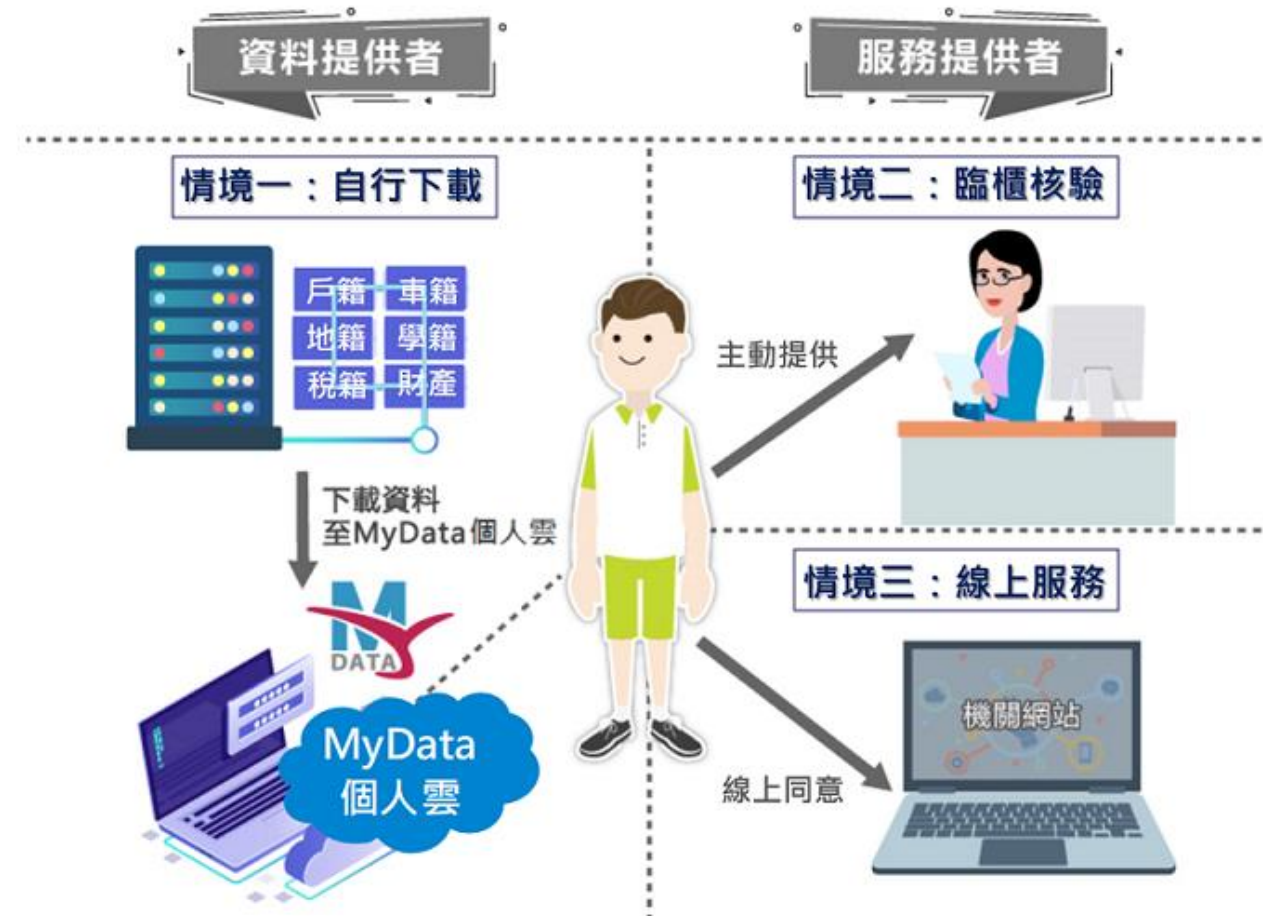
# 推動智慧政府方案的具體策略

- 「全面換發數位身分識別證」 ( New eID )
- 「建立具安全且可信賴的資料交換機制」 ( T-road ) 二大基礎架構
- 以資料為骨幹，進行資料去識別化，擴大個人化資料的應用 ( 客製服務 )



# 數位服務個人化 ( MyData )

資料擁有者可透過平臺驗證身分並線上同意後，自資料提供機關（如內政部）下載個人資料，提供服務機構使用





# 數位轉型的內涵與障礙



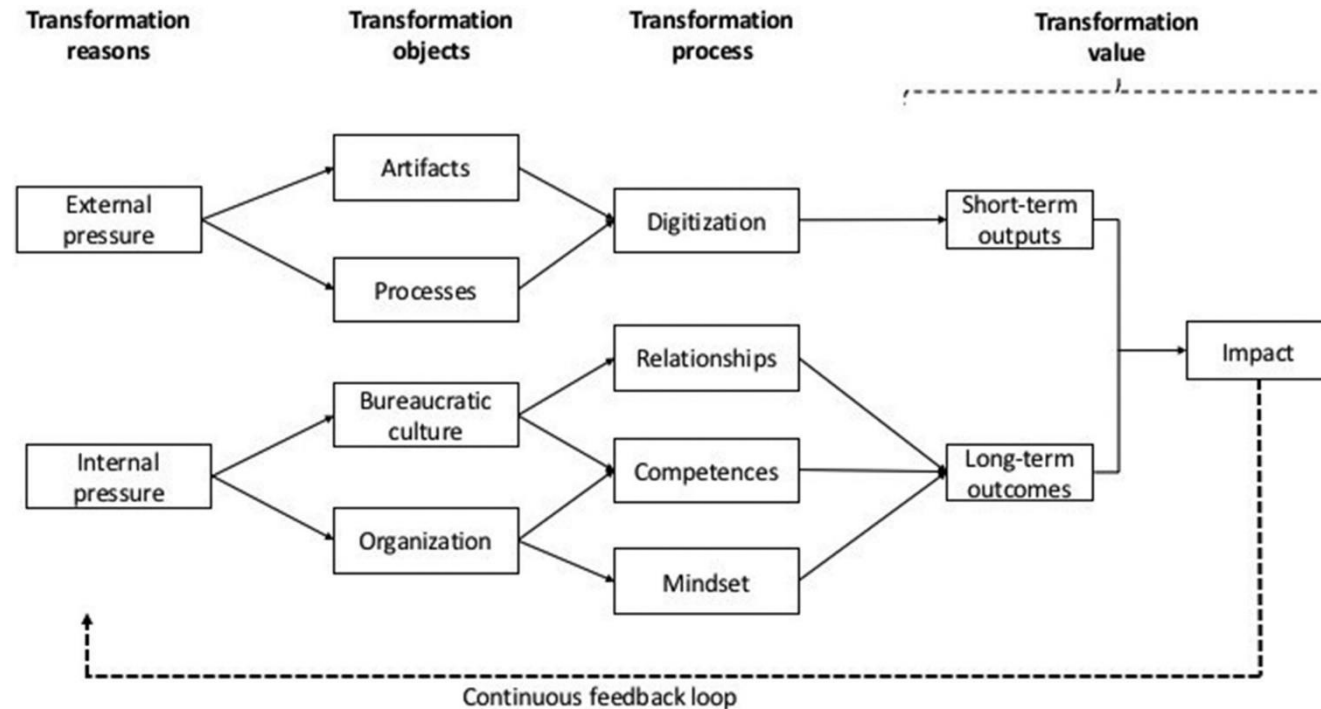
# 提高民眾辦理公務的效率，就是數位轉型的全部嗎？

- 大部分的數位政府計畫都只是改善現有服務，少涉及基礎的「**數位轉型**」
- 數位轉型能要驅動「**組織結構**」、「**組織文化**」的改革
- 改革不能只是引進IT，相反地，為了實現公部門數位轉型，公部門需要在**流程**、**員工關係**、**人力與思維**、**政策與領導效能**上進行根本性上的變革



# 政府數位轉型的不同過程


- 外部壓力→軟硬體、流程上的轉型(eID與T-Road) →短期輸出
- 內部壓力→官僚文化、組織結構上的轉型 →長期效果




# 政府數位轉型時，組織結構、組織文化上的障礙

組織結構	組織文化
<ul style="list-style-type: none"><li>• 不同部門同時執行不同轉型計畫，難以監管與評估計畫成效</li><li>• 數位轉型可能帶來的利益，分散在政府各個部門，因此缺少推動誘因</li></ul>	<ul style="list-style-type: none"><li>• 轉型計畫可能是由外部諮詢團隊推動，缺乏政府內部的實際營運團隊（operational team）的推動與決策</li><li>• 計畫初期推動成功，體制內的營運團隊缺乏持續運作的誘因與動力</li></ul>

- 數位轉型遇到的障礙，可以透過**課責**來處理嗎？



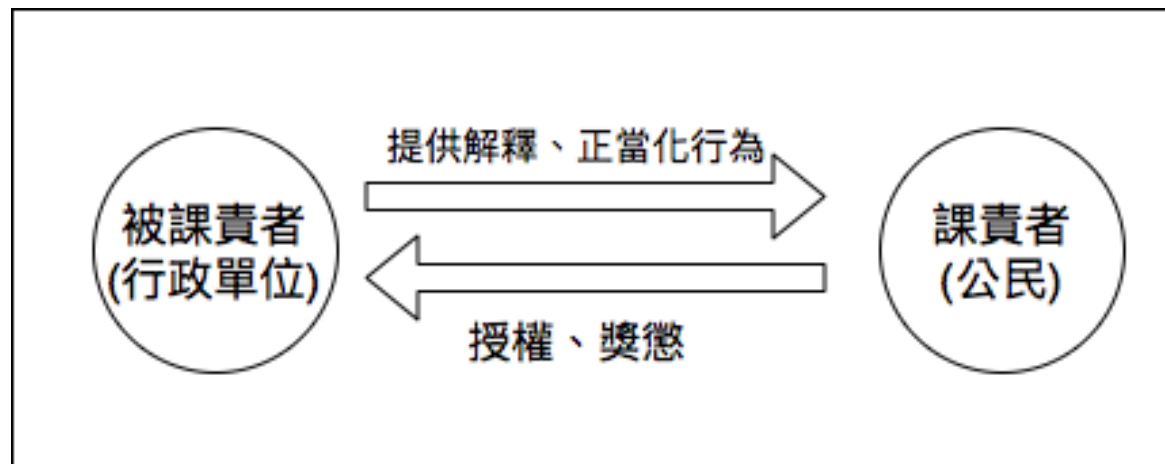
# 課責作為克服 數位轉型障礙的機制



# 課責的定義與流程

學者	定義
Romzek & Dubnick (1987); Boven (2014)	課責可以被視為一種社會關係，在這段社會關係當中，行為者有義務跟重要他人 <b>解釋與正當化</b> 其行為
Levine, Peters & Thompson (1990); Kim (2005); Pedersen & Nielsen (2016)	文官必須向民選官員 <b>答覆或報告</b> 相關事宜
Giddens (1984); Roberts, McNulty & Stiles (2005); Huse (2005)	行為者需要 <b>闡明原因，並提供規範依據</b> ，使公民認為該行為是有道理的
Przeworski, Stokes & Manin (1999); Ackerman (2004)	當公民可以應用 <b>懲罰機制</b> 來淘汰表現不良的政府，我們就說政府是有被課責的

## □ 課責的流程：委託-代理關係



# 課責的分類與策略

## □ 課責可以依照強制力的來源、程度分為四類

類型		控制來源(Source of Agency Control)	
		內部	外部
控制程度(Degree of Control Over Agency Actions)	高	官僚課責 - 層級節制的監督	法律課責 - 法規、契約簽訂的監督
	低	專業課責 - 專業同儕間的監督	政治課責 - 選民、民意代表的監督

## □ 達成課責的策略

□ 政府內部組織結構與法規的調整

□ 外部公民社會與民意代表監督



# DPAs面臨的問題

- 缺乏民主合法性（誰來擔任資料保護專員？）
- 因預算、人員數量不足而導致監督效率不佳
- 難以處理現代資訊科技與法律規範外的新興議題
- 該如何解決？
  - 納入新的參與者：公民、CSOs、跨國網絡
  - 投入更多的預算與人力資源
  - 定義更具體的工作內容（e.g. 保護什麼隱私？）

# 從外部公民社會來實現課責

□ 資訊科技發展下，一些課責方案特別強調由**外部公民**進行課責

## 互動課責(interactive accountability)

- 將政府資料整理為統計報告，再由機關**邀請公眾來參加座談會、聽證會**等形式的互動式會議
- 例：犯罪地圖



## 動態課責(dynamic accountability)

- 以開放政府資料系統為基礎，建立動態的施政資料庫，讓**公民自主針對政策績效進行詢問、課責**。
- 例：社會住宅戰情中心



## 公民提案課責(citizen-initiated accountability)

- 由**公民自主提出問題、建議與解決方法**。公民不僅要求政府負責，自己也在處理社會問題上扮演主要角色
- 例：JOIN平台



提點子



眾開講



來監督



# 課責與智慧政府 的建構：以eID為例

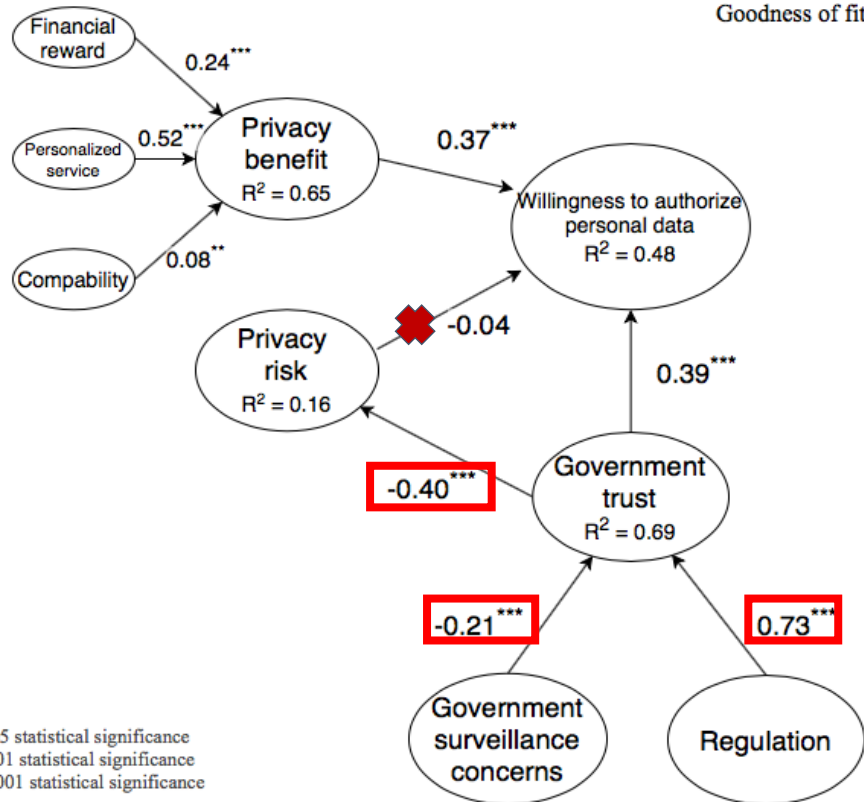


# 課責可作為一種隱私風險管理機制

- 在課責關係中，民眾可以要求被課責者提供**解釋**
  - 事前如何蒐集：我需要提供哪些資料？
  - 事中如何運用：資料是怎麼被使用的？
  - 事後如何救濟：出事要找誰？
- 當民眾感受不到管理機制時，會有三種**不合作行為**（Lwin et al., 2007）
  - 保留（withhold）：拒絕提供個人資料或拒絕使用服務
  - 保護（protect）：使用某些工具保護自身的線上隱私
  - 偽造（fabricate）：提供錯誤的個人資料
- 假如使用者都**不願意**透過New eID提供個人資料...？
  - 內部：政府管制（法規）的修正
  - 外部：公民個人資料自主管理機制

# 政府管制與法規的功能

Sample size = 743  
Weighting Scheme: PathWeighting  
Bootstrapping nboots = 5000  
Average Commuality = 0.84  
Average R<sup>2</sup> = 0.50  
Goodness of fit = 0.64



- 2020年2月份透過政治大學選舉研究中心PollcracyLab，採網路調查形式，完成743份有效樣本
- 內部課責（政府管制）的效果
  - 民眾對政府管制認知會提高對政府的信任
  - 間接降低隱私風險認知
  - 間接提高資料授權意願
  - 政府監控疑慮會產生與管制相反的效果
- 隱私風險考量對民眾資料授權意願影響不顯著<sup>19</sup>

# 外部引入公民監督：愛沙尼亞「Data-tracker」

## Security and defense

### Safety and Security

Protection of personal data and privacy

Usage of personal data

Computer Security

Weapons and weapons permits

National defence hazards

Emergency preparedness of state

National internal security

- 提昇資料使用的透明度，讓公民自主管理隱私
- 公民可以登錄到自己的eID帳戶，查看哪些政府網站曾經要求存取過自己的個人資料（追蹤政府機構的數位足跡）
- The tool gives citizens the possibility to always keep an eye on who is accessing their data

# 外部引入公民監督：愛沙尼亞「Data-tracker」

- Data-Tracker 追蹤範圍涵蓋愛沙尼亞四個主要的政府資料庫
  - 就業登記資料庫 ( 每月11,767,330 次存取要求 )
  - 健康資訊系統 ( 每月8,828,045 次存取要求 )
  - 人口登記資料庫 ( 每月 7,298,599 次存取要求 )
  - 健保基金資料庫 ( 每月 7,182,244 次存取要求 )
- e-Estonia的核心精神
  - 透明可以提昇公民對於機構的信任
  - 專責機構與專責法規



# 討論與建議



# 提高公民的隱私風險意識與自主管理能力

## □ 增強隱私風險意識

- 辦理身分證換發時，公民風險意識的培力
- 公部門舉辦個人**資安演練**，**模擬隱私外洩**情境

## □ 強化公民隱私的自主管理能力

- 針對不同族群制定**客製化的隱私管理機制**（例如資訊代理人）
- 當政府機關透過 New eID 存取個人資料時，應**立即主動通知**
- 當其他服務商存取你的Google帳號時？



「academia.edu」已取得您的 Google 帳戶存取權

如果您並未授予存取權，建議您檢查這個活動以保護帳戶。

[查看活動](#)

# 重視外部與內部的課責機制

- 內部：針對New eID的授權制定專門法規與機構
  - 明定公民在面臨New eID上隱私問題的救濟、課責程序
  - 專責機構可以由政府機關、國內CSOs、跨國機構等共同組成
  - 行使獨立審查權、法定行政預算、設立具體績效指標
- 外部：系統程式碼的開源
  - 愛沙尼亞將eID系統的程式碼都公布於開源軟體程式碼平臺上
  - 白帽駭客（ethical hacker）：協助測試系統安全性

# 常任文官正向課責的可能

- 多數研究跟機制都忽略了課責的正向功能
  - Romzek 在2014年APSA ( American Political Science Association ) 的演講
  - 『我們對於敘獎審查、獎金與獎勵發放或選舉勝利等**正向課責**的討論不多，大多數都聚焦在制裁跟懲罰等**負向課責**之上。』
  - 如何建立一個兼顧**懲罰**與**誘因**的課責機制？
- 強化常任文官的**內控**機制：讓課責成為行政機構的正向回饋
  - 針對資料保護優良的部會酌加敘獎：「有功有賞、打破要賠」
  - 推動優良機關作業流程上的**標竿學習**



**簡報結束  
謝謝聆聽**

