資安推動策略及重點工作

數位發展部資通安全署

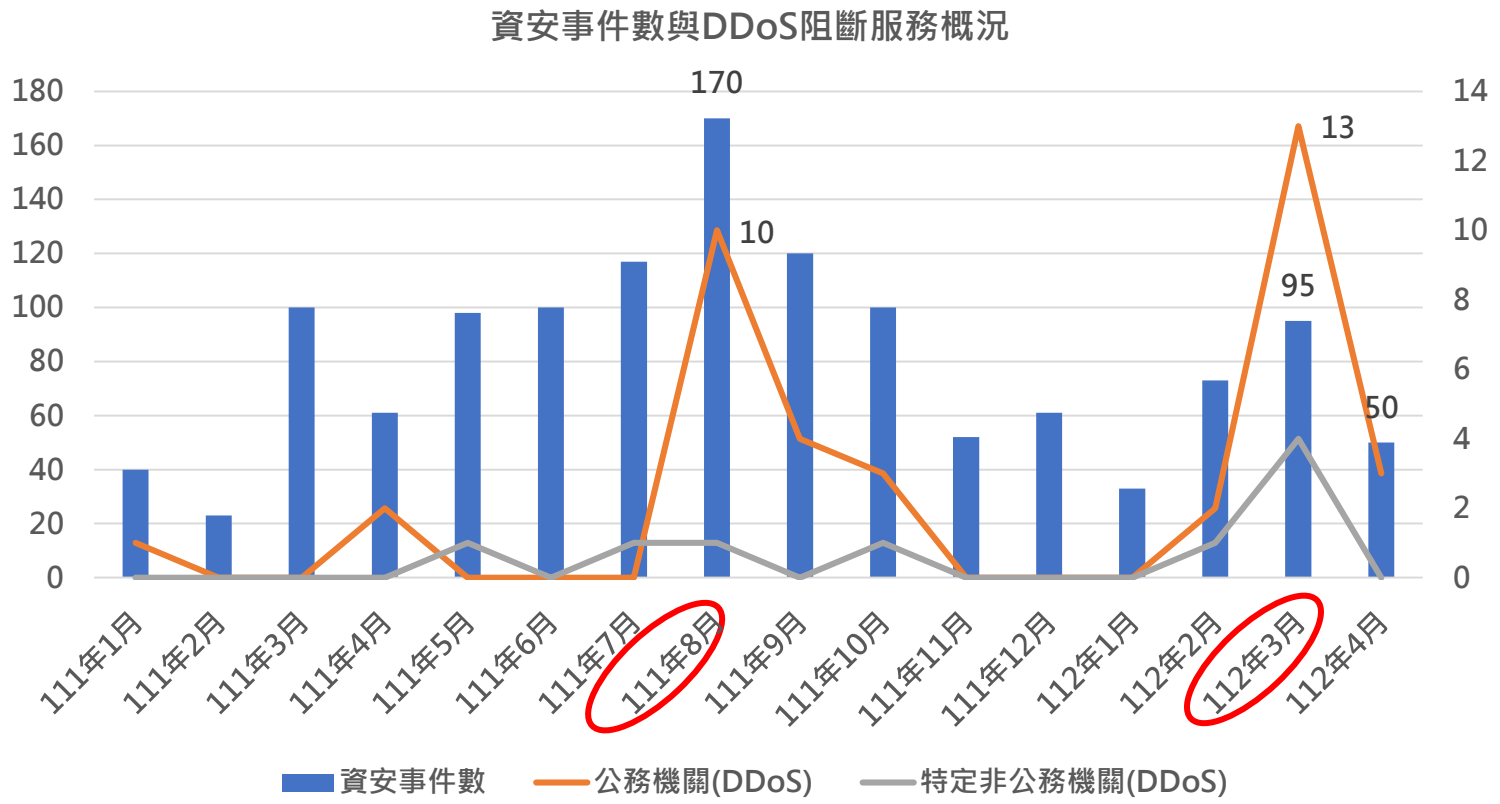
大綱

- 近期政府機關資安事件概況及防護建議
- 政府機關資安事件通報逾時概況及改善建議
- 重點工作宣導
  - 資安法調修重點
  - 資安稽核
  - 攻防演練
  - 政府零信任網路架構
  - 資安弱點通報機制(VANS)推動
- 綜合討論

近期政府機關資安事件概況及防護建議

近期網路攻擊情形

- 觀察111年起資安事件通報，整體而言在特定重大政治敏感議題熱議期間，通報事件量略有上升，且多為阻斷服務(DDoS)類型。



DDoS攻擊之應對建議

數位發展部資通安全署
Administration for Cyber Security, moda

DDoS攻擊特性：

- ➢技術門檻低且無法持續
- ➢短期干擾行為，無需過度關注
- ➢防護重要服務
- ➢影響形象，必要的媒體說明

事前

- ✓評估重要服務
- ✓預備靜態網頁及流量清洗方案
- ✓特定期間DNS代管規劃
- ✓規劃網站CDN

事中

- ✓服務如受影響應進行事件通報
- ✓啟動流量清洗及切換靜態網頁
- ✓適時媒體說明
- ✓切換DNS代管

事後

- 檢討閒置網站
- 落實DDoS防護演練

系統預設密碼風險

- 機關為民服務系統使用**相同預設密碼且帳號原則相同(如使用公司統編等公開資料)**登入，有心人士藉此嘗試取得機敏資料，致有資料外洩風險

建議防範措施

- 機關應落實普級防護基準設定(**預設密碼需於登入後強制變更密碼**)，若系統提供多種驗證方式，皆應依規定辦理
- 預設密碼不可相同，預設密碼建議採隨機亂數產生
- 顯示上次登入時間，供使用者確認是否有異常登入情形

供應商遭駭致會員資料外洩

- 某政府機關委託單車租借業者辦理租借服務，使用**共用租借平台**，平台系統遭駭客攻擊，部分縣市亦有與該平台合作，部分會員資料(卡號及騎乘紀錄)恐遭外洩。

憑證填充攻擊:
自動化方式將某處偷來的同一組帳號密碼嘗試登入多個其他熱門網站的密碼填充攻擊

建議防範措施

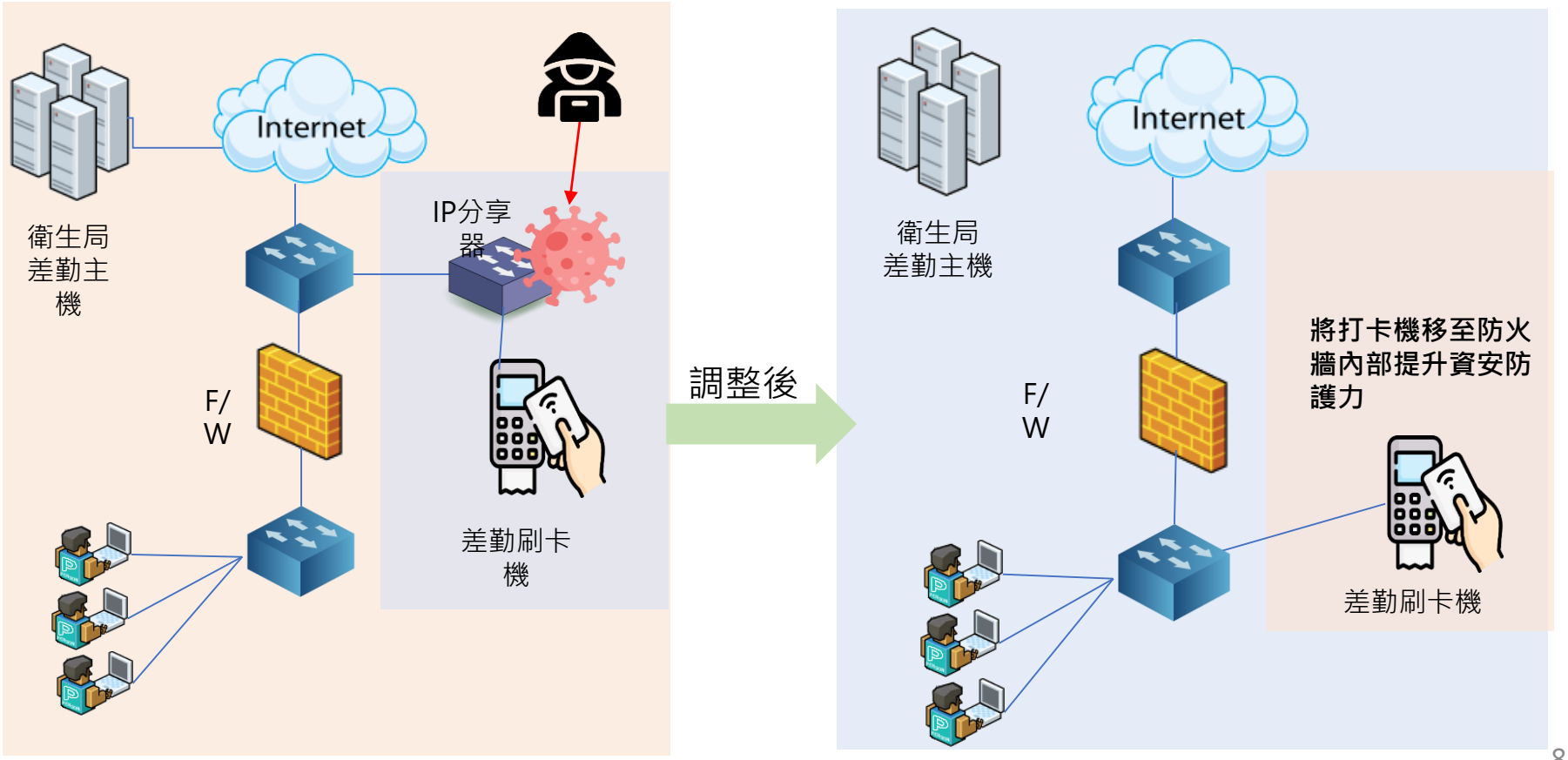
- 機關應減少使用容易取得之資訊**(如手機號碼及身分證字號)**當作帳號或密碼。
- 建議啟用雙重驗證並導入CAPTCHA，阻止惡意機器人
- 加強監控網路流量，是否有速度變慢、登入人數、網路查詢暴增情形。

物聯網設備未納入資安防護

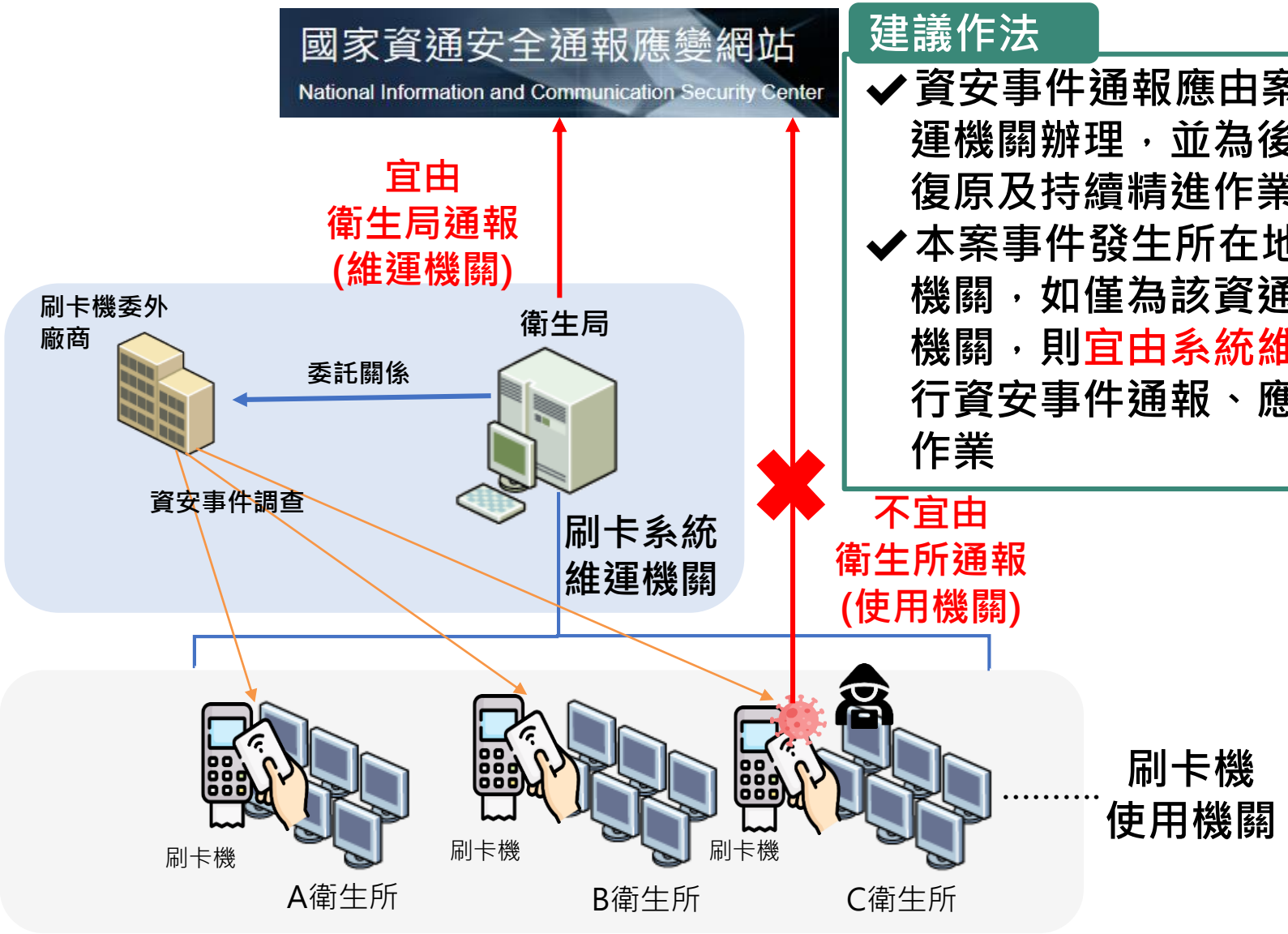
- 某縣市政府規劃各衛生所刷卡資料須回傳衛生局，並藉由IP分享器隱蔽其真實IP位置，惟該IP分享器曝露於外網，以致遭駭侵，並至惡意中繼站報到。

建議防範措施

- 落實物聯網設備盤點
- 妥適的網段區隔及防護



資安事件通報對象



建議作法

- ✔資安事件通報應由案關系統維運機關辦理，並為後續之應變復原及持續精進作業
- ✔本案事件發生所在地之IP使用機關，如僅為該資通系統使用機關，則宜由系統維運機關進行資安事件通報、應處及結案作業

資安事件之法遵意識

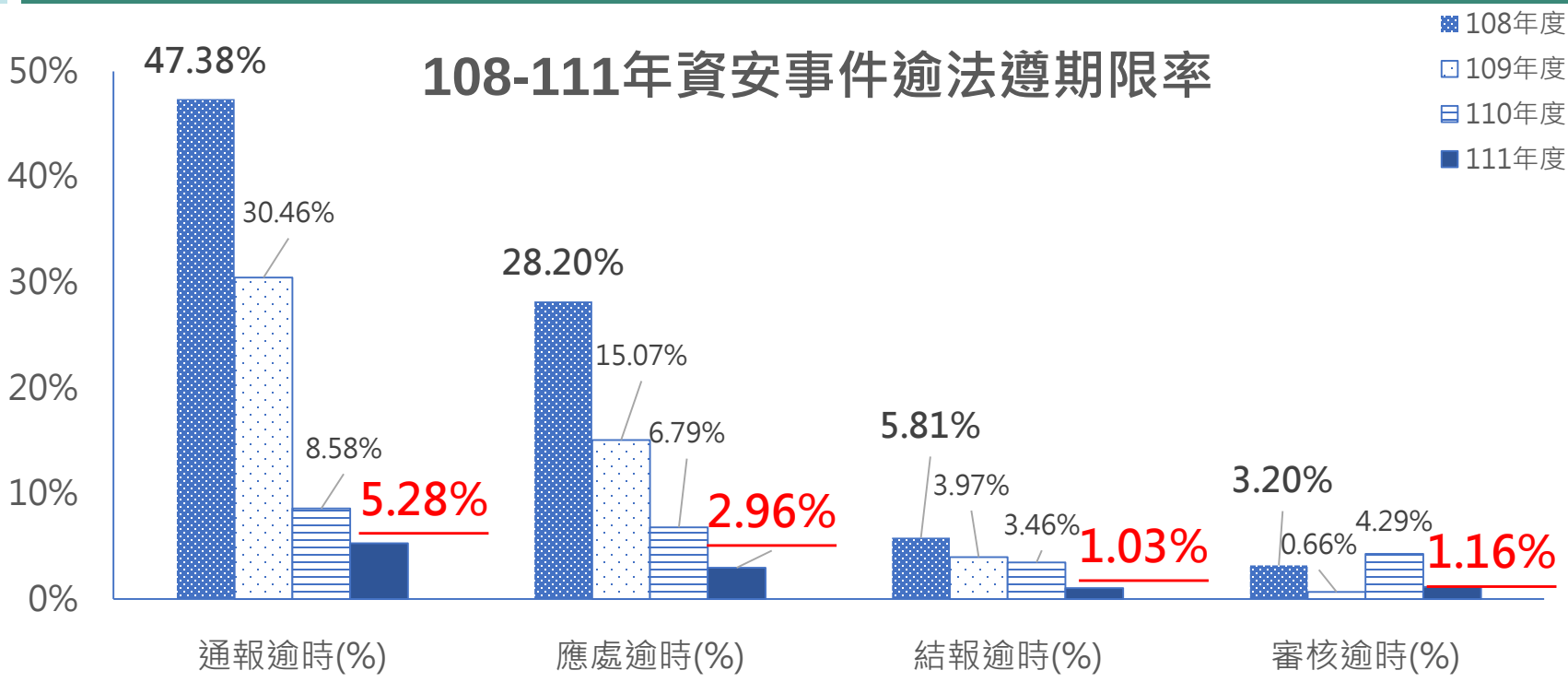
- 機關同仁進行大量圖資轉檔作業時，為求便利直接於對外伺服器端操作，遭外部有心人士讀取高階圖檔為其他利用，後經媒體揭露後始通報資安事件，致逾法遵期限

管理層面議題

- ✓ 資安事件不以駭侵為限、不以重大事件為限、不以核心業務為限，只要影響機密性(C)、完整性(I)或可用性(A)，不論造成原因為何，皆屬資通安全管理法規範之應通報資安事件
- ✓ 為利法遵時效，建議機關可先行通報，儘速完成調查後若確無CIA受影響，可申請撤單

政府機關資安事件通報
逾時概況及改善建議

資安事件通報應變逾時情形



	事件通報	應變處置	結報 (提交調查、處理及改善報告)	完成審核 (上級或監督機關)
起算時間點	知悉事件	知悉事件	完成應變處置	接獲通報
1、2級事件	1小時	72小時	1個月內	8小時
3、4級事件		36小時		2小時

範圍：所有納管機關

資安事件通報逾時原因及建議

收到警訊亦應通報

- ✔機關收到INT警訊時，表示機關已有駭侵事實
- ✔須循機關內部通報程序陳報外，並應依資通安全管理法執行資安通報作業

無法網站通報之處理

機關若因故無法連線至通報應變網站進行通報時，可改使用下列方式進行通報:

- ✔使用手機連線至網站通報
- ✔利用電話或傳真通報

不熟悉通報作業

- ✔無須等應處完成後才進行通報，知悉資安事件應同步通報，說明已知資訊。
- ✔落實人員資安教育訓練(包括網站操作熟悉度)

重點工作宣導
資安法調修重點

修法重點-主管機關調適

數位發展部資通安全署
Administration for Cyber Security, moda

目前

行政院公報　　第028卷　第160期　20220824　綜合行政篇

行政院公告　　中華民國111年8月24日
院臺規字第1110184307號

主　　旨：為配合數位發展部及其所屬機關（以下簡稱新機關）組織法規自中華民國一百十一年八月二十七日施行，相關法律、法規命令及職權命令條文涉及各該新機關掌理事項者，其管轄機關自中華民國一百十一年八月二十七日起變更為各該新機關，特此公告。

依　　據：依行政院功能業務與組織調整條例第三條第一項規定辦理。

公告事項：「配合行政院組織改造以111年8月27日作為新機關組織調整生效日者之變更管轄機關法律條文表」及「配合行政院組織改造以111年8月27日作為新機關組織調整生效日者之變更管轄機關法規命令及職權命令條文表」。

擬調修

行政院

主管機關

moda 數位發展部 Ministry of Digital Affairs

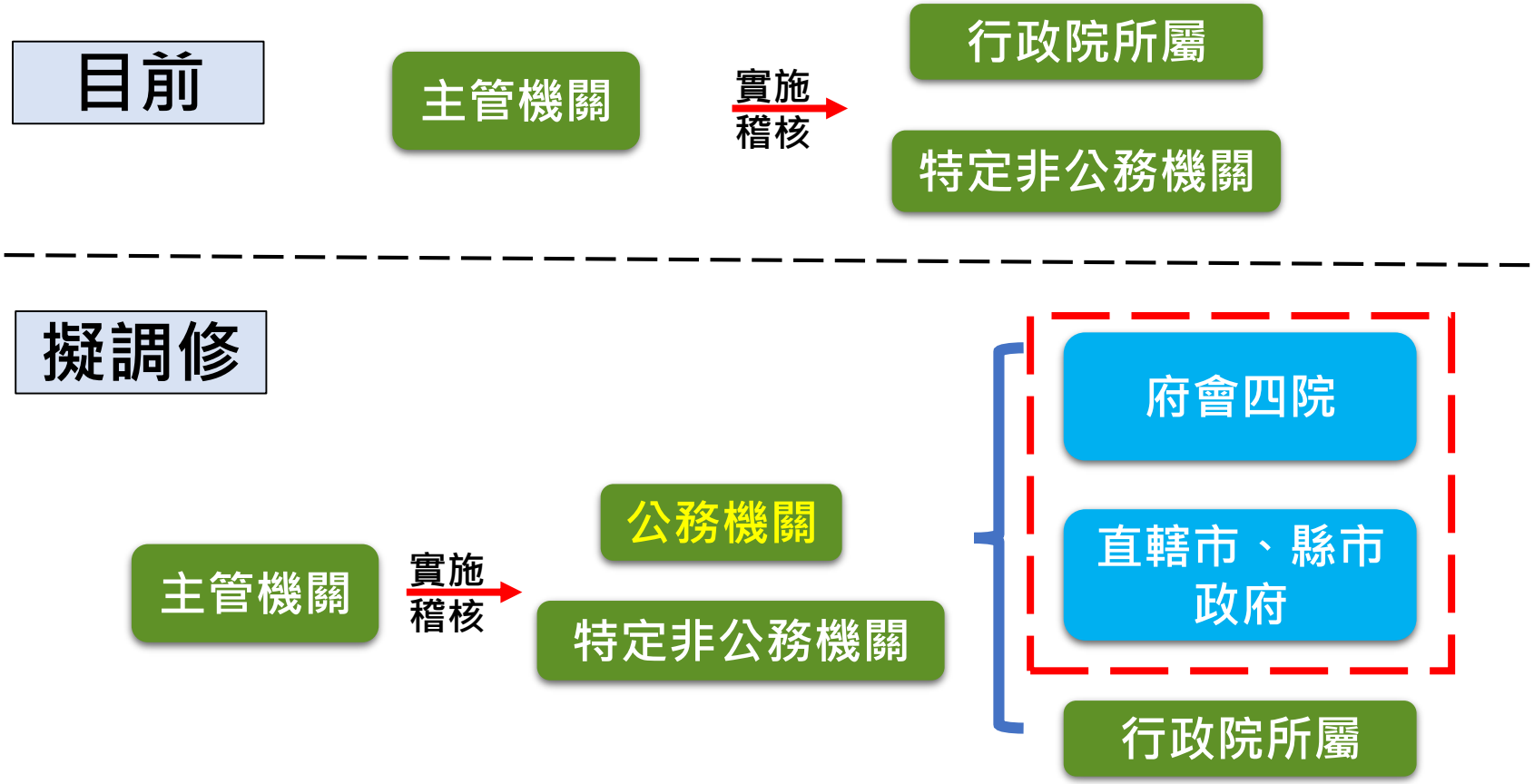
主管機關

資通安全署

規劃及執行機關

修法重點-擴大稽核範圍

- 為協助各機關檢視及強化資安防護作業，規劃增訂主管機關得依資安法稽核公務機關



修法重點-增訂專案查核

數位發展部資通安全署
Administration for Cyber Security, moda

現行作業

針對重大資安事件進行專案稽核，協助機關復原、鑑識、調查及改善

- 實兵演練
- 技術檢測
- 實地查核

精進作為

➢ **重點專案查核**：如資安重大矚目案件，聯合**上級機關或**中央目的事業主管機關執行查核

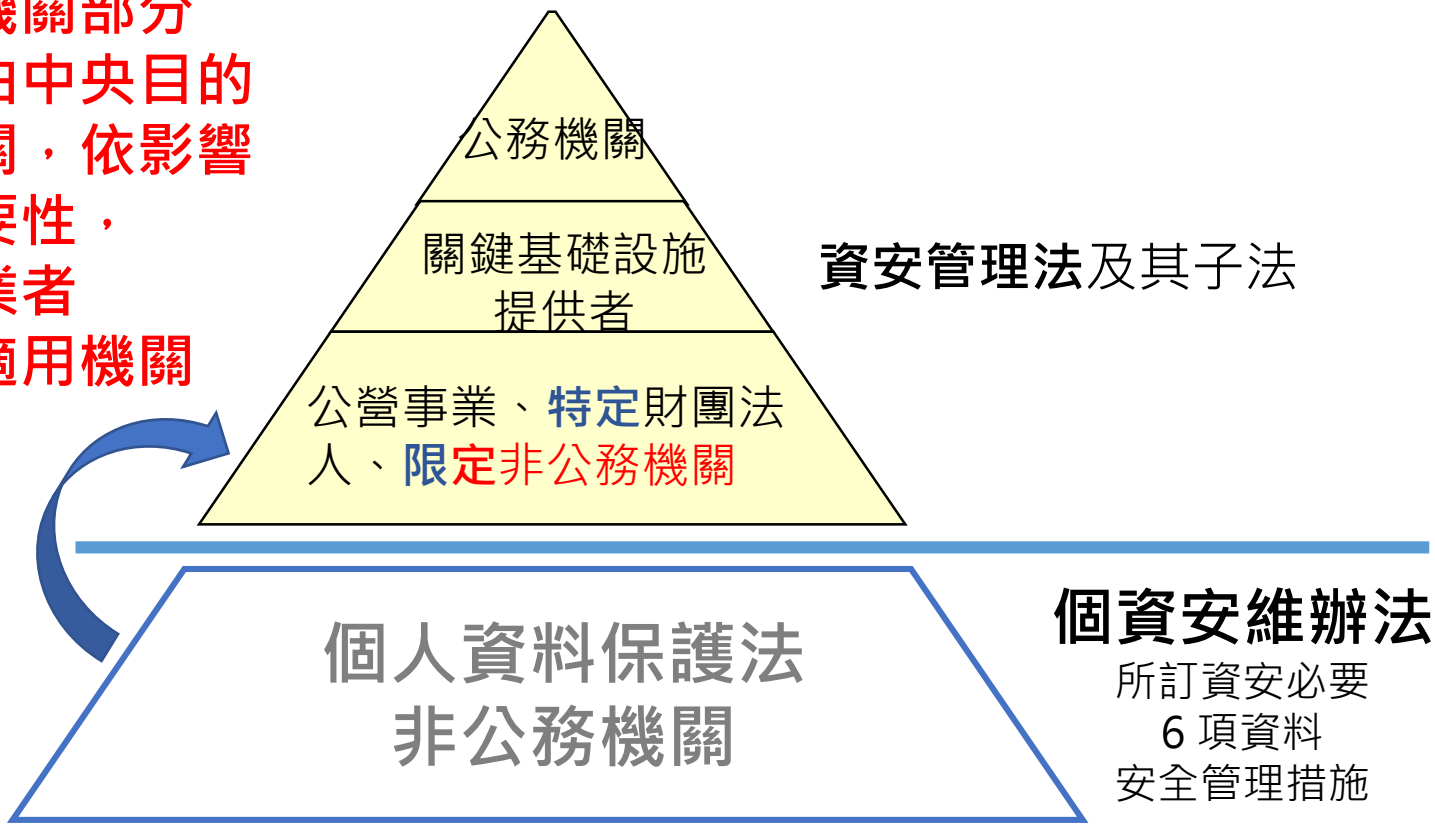
註：重大矚目案件：

✔行政院、立法院或監察院關注之資安事件

✔經媒體顯著披露之資安事件

修法重點-擴大納管範圍

特定非公務機關部分評估增加可由中央目的事業主管機關，依影響社會公益重要性，指定所管轄業者納入資安法適用機關



資安管理法及其子法

個資安維辦法
所訂資安必要
6 項資料
安全管理措施

重點工作宣導
資安稽核

資安法現行稽核機制

數位發展部資通安全署
Administration for Cyber Security, moda

- **公務機關** ← 中央、地方機關 (構) 或公法人。但**不包括軍事機關及情報機關**
  - **資安法 §13**
  - **行政院國家資通安全會報稽核**

總統府、**行政院**、四院、**直轄市縣市政府**、直轄市縣市議會、直轄市山地原住民區公所、區民代表會、鄉 (鎮) 市公所、市民代表會

無上級機關之公務機關

§13 應稽核

e.g. 司法院

所屬或所監督公務機關

§13 應稽核

e.g. 臺灣高等法院

所屬或所監督公務機關

e.g. 臺灣臺北地方法院

- **特定非公務機關**
  - **資安法 §7、§16、§17**

資安法主管機關 (數位部)

§7 得稽核

中央目的事業主管機關

§16 應稽核 CI 提供者
§17 得稽核其它

特定非公務機關

資安法中的各種稽核

第一方稽核

機關內部資安稽核

A：每年2次
B：每年1次
C：每2年1次

第二方稽核

- 上級機關對所屬機關
- 監督機關對行政法人
- 中央目的事業主管機關對特定非公務機關
- 資安法主管機關對特定非公務機關
- 機關對受託者

第三方稽核

資訊安全管理系統(ISMS)驗證

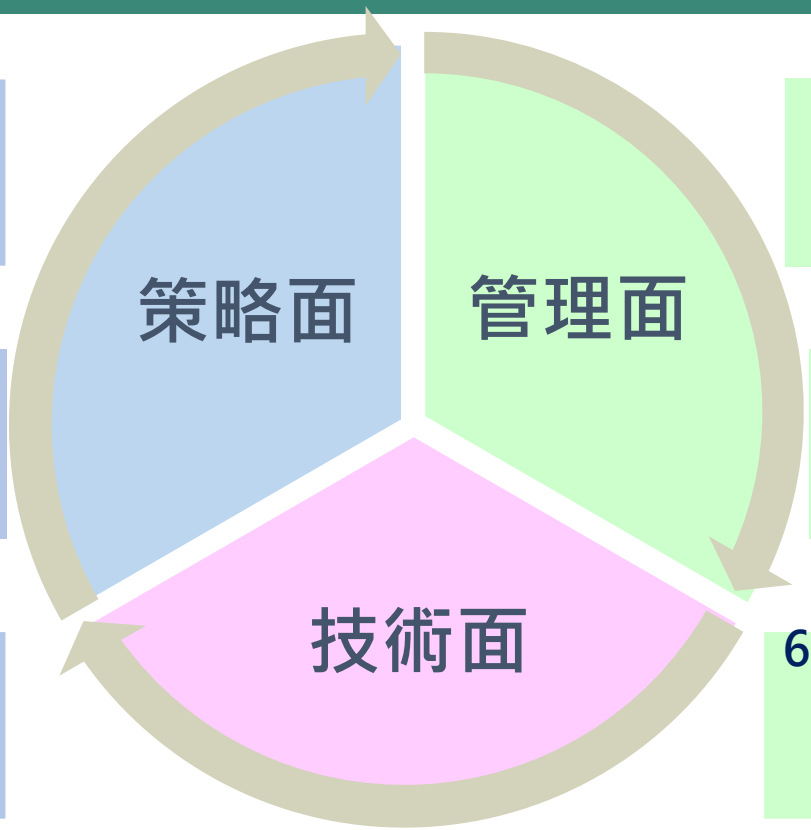
目的：檢視**全機關資通安全管理法及其子法**相關**法遵事項符合情形**

實地稽核項目作業說明

1.核心業務及其重要性

2.資通安全政策及推動組織

3.專責人力及經費配置



4.資通系統盤點及風險評估

5.資通系統或服務委外辦理之管理措施

6.資通安全維護計畫與實施情形之持續精進及績效管理機制

7.資通安全防護及控制措施

8.資通系統發展及維護安全

9.資通安全事件通報應變及情資評估因應

- 實地稽核項目檢核表，依「資通安全管理法」相關規定之不同，分為公務機關、特定非公務機關2式

https://moda.gov.tw/ACS/operations/drill-and-audit/652

112年度稽核重點

數位發展部資通安全署
Administration for Cyber Security, moda

資安法法遵事項及過去稽核發現 ✚ 重點推動之項目

大陸廠牌盤點及管控

禁用措施及實施作法，如使用
- ✓列冊管理、資安長簽署、報請核定
- ✓控管措施、汰換及報廢時程

第二方稽核執行情形

對所屬/管/監督機關之管理
- 訂定管理辦法
- 執行資安稽核
- 追蹤改善情形

因應網攻之網站韌性強化

核心或具代表性之網站，DNS
- ✓ 流量清洗服務方案
- ✓ 其他緩解機制(如阻擋IP、靜態頁)
- ✓ 評估特定期間DNS代管

電子防疫個資管制

- ✓ 涉資通系統(含APP)收集情形
- ✓ 依個資法規定，於特定目的消失後刪除，刪除佐證

建議各機關可評估納入資安稽核項目

重點工作宣導
攻防演練

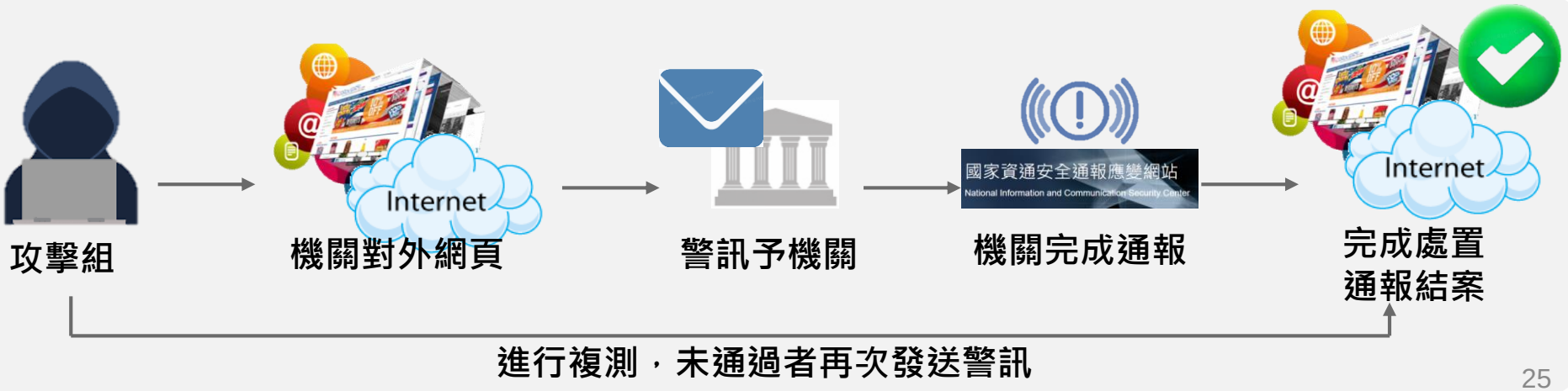
資通系統實兵演練

數位發展部資通安全署
Administration for Cyber Security, moda

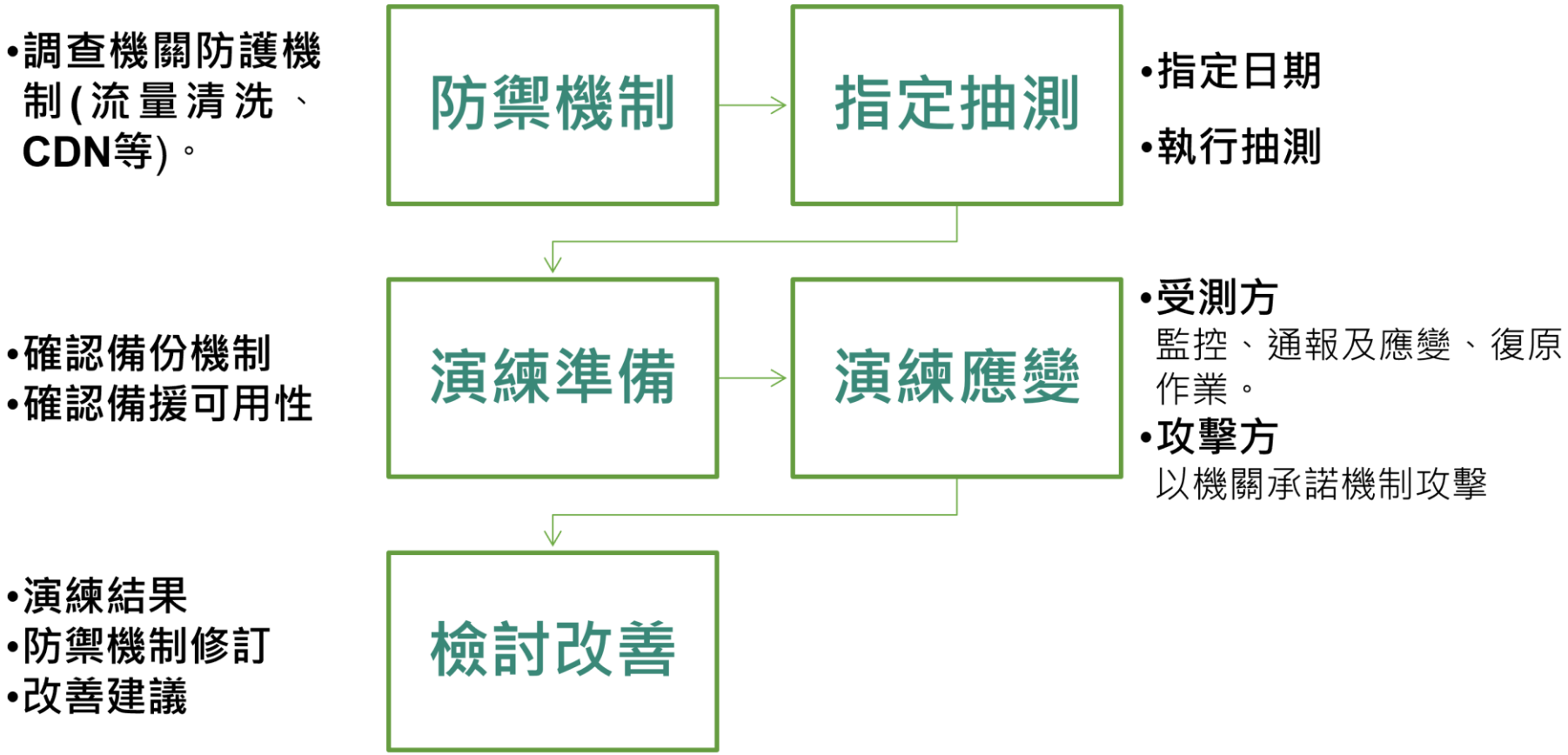
- **演練範圍**
  - **中央A級、地方政府**(含所屬資安責任等級B級機關)。
  - **重點機關：發生重大資安事件機關**

- **計分範圍：**系統**盤點**、系統**弱點**、通報**時效**、**修復**能力。

- **所屬加測：**攻擊組蒐集**弱點資訊**，於**GSN**搜尋攻擊目標，範圍外，攻擊手計分，機關不計分，結果納入政策推動之參考。



DDoS演練項目


•調查機關防護機制(流量清洗、CDN等)。
防禦機制
指定抽測
•指定日期
•執行抽測
•確認備份機制
•確認備援可用性
演練準備
演練應變
•受測方
監控、通報及應變、復原作業。
•攻擊方
以機關承諾機制攻擊
•演練結果
•防禦機制修訂
•改善建議
檢討改善

演練獎勵

數位發展部資通安全署
Administration for Cyber Security, moda

績優機關

- **各群排名**總成績**前3名者為表現績優機關**

良好機關

- **各群排名**總成績**4~5名者為表現良好機關**

進步卓越機關

- 112年攻防演練**新增獎項**
- 111年度表現為**後25%之機關**，於112年**進步至前25%之機關**

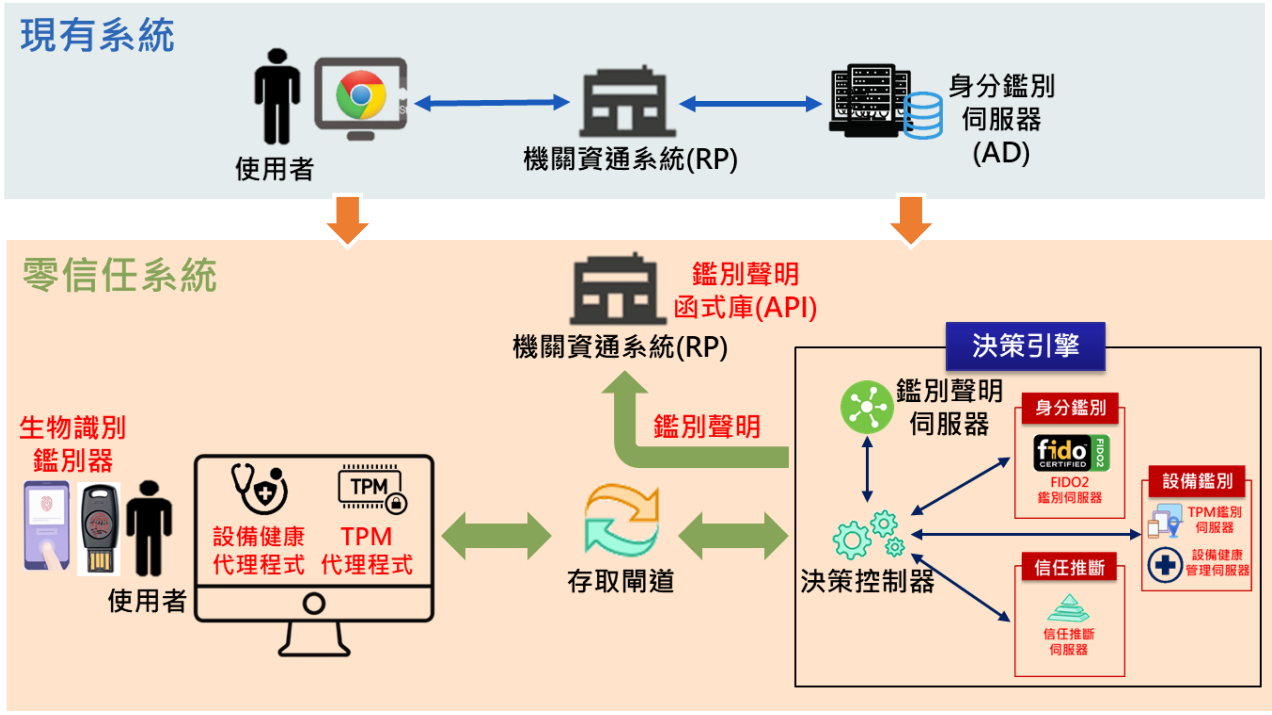
社交工程防護項意識提升良好機關

- **地方政府**分組**增設「意識提升良好機關」獎**
- 社交工程防護得分111年排序為**後25%之機關**，於112年**提升至前25%之機關**

重點工作宣導
政府零信任網路架構

零信任網路簡介

- **政府零信任網路架構：美國 NIST SP 800-207 標準**
  - **身分鑑別**：多因子身分鑑別與鑑別聲明
  - **設備鑑別**：設備鑑別與設備健康管理
  - **信任推斷**：使用者情境信任推斷機制

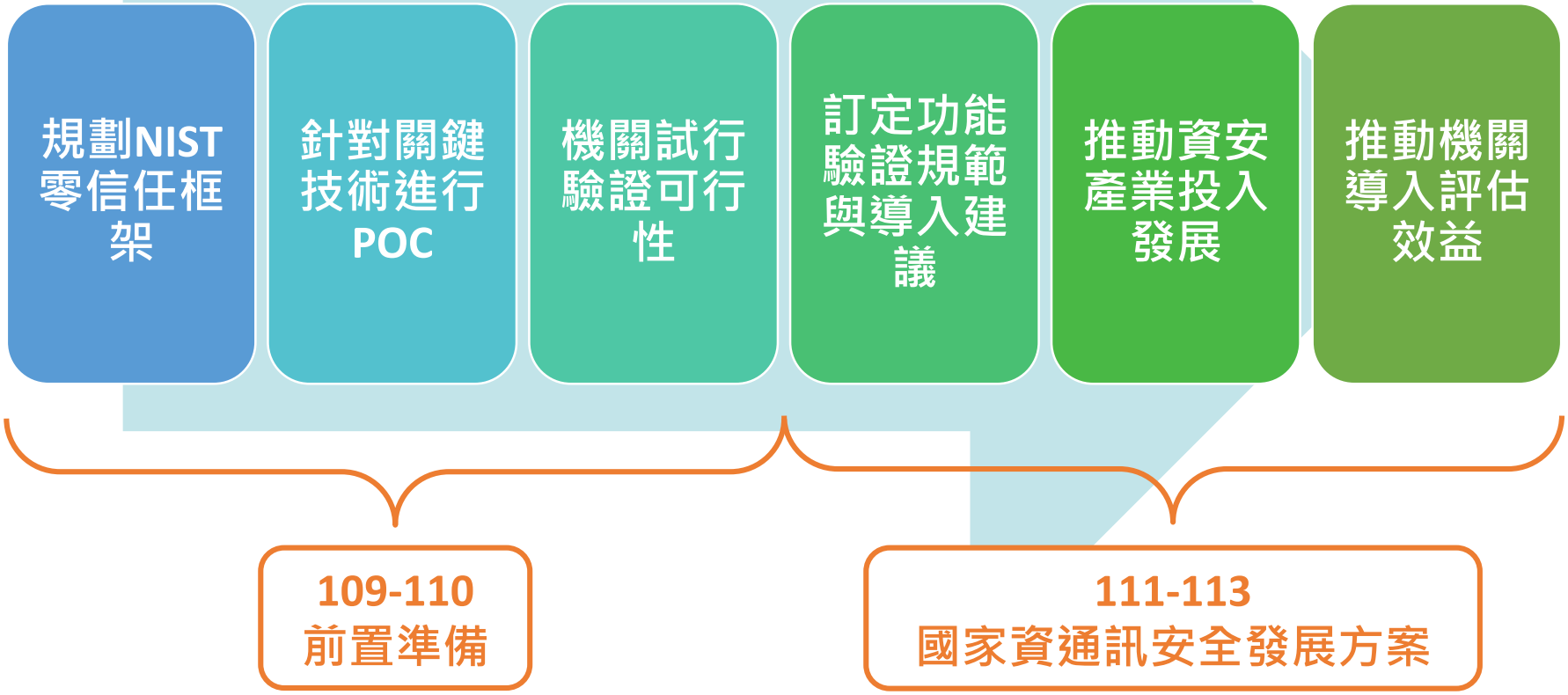


NIST SP 800-207

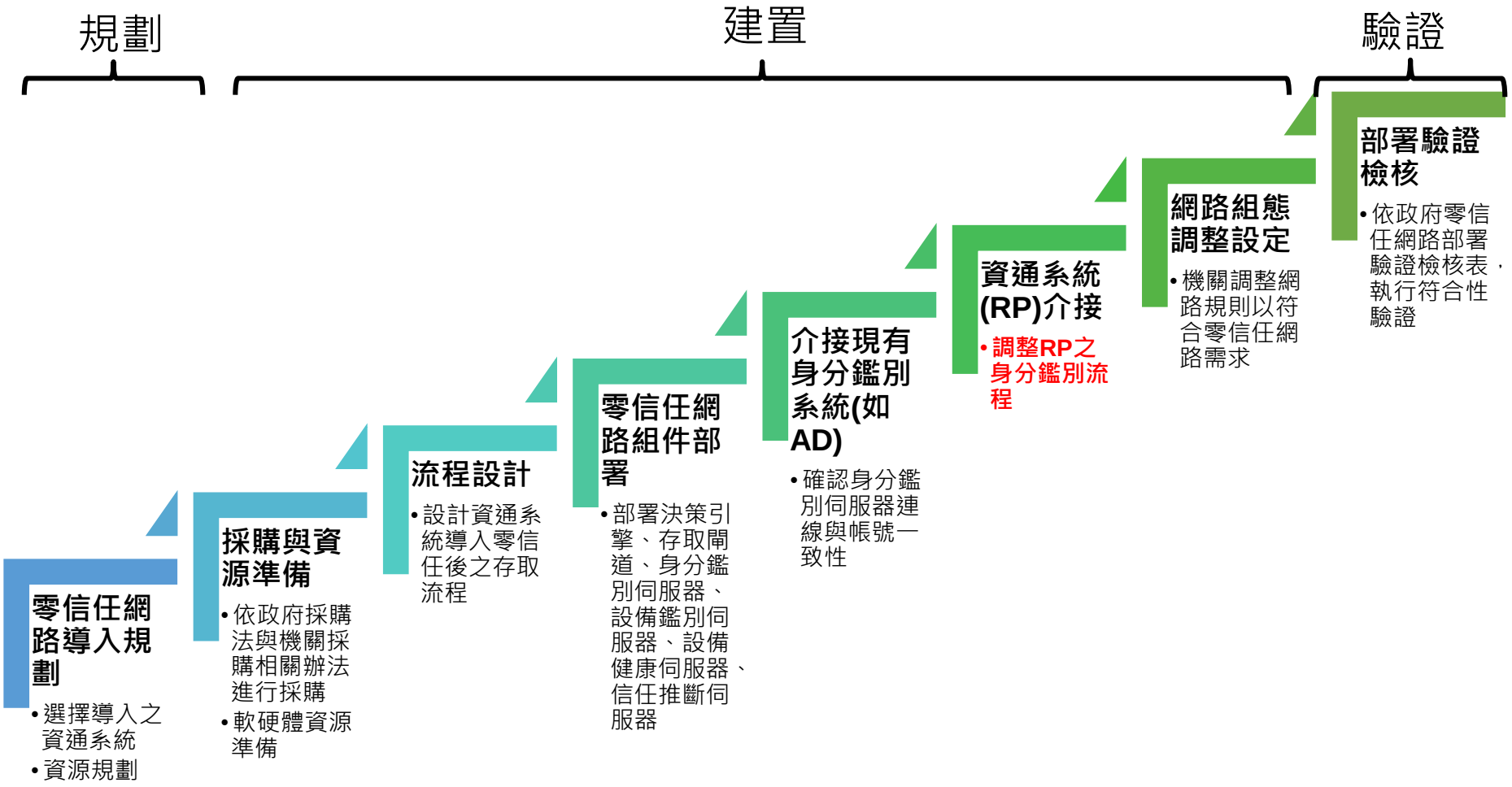
實施零信任會是一段過程，而不是一次大規模替換基礎架構，**且與傳統模式會同時混合運作**。

推動規劃

- 國家資通安全發展方案
  - 110年完成零信任網路與概念性驗證機制研究與部署機制
  - 111~113年遴選2個機關逐年導入身分鑑別等3大核心機制



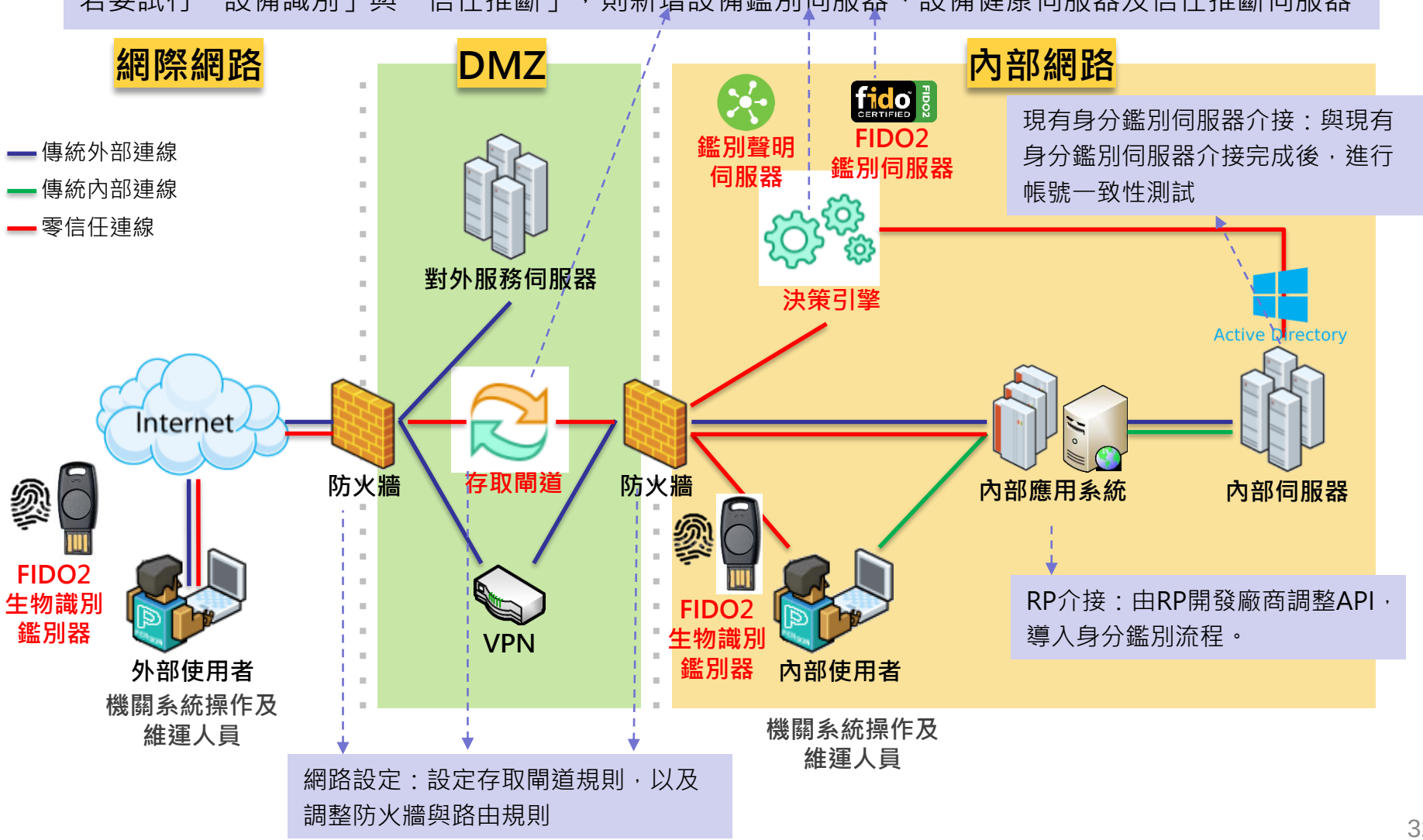
機關導入流程



政府零信任網路專區：
https://s.moda.gov.tw/qW6eU2dWc1sW

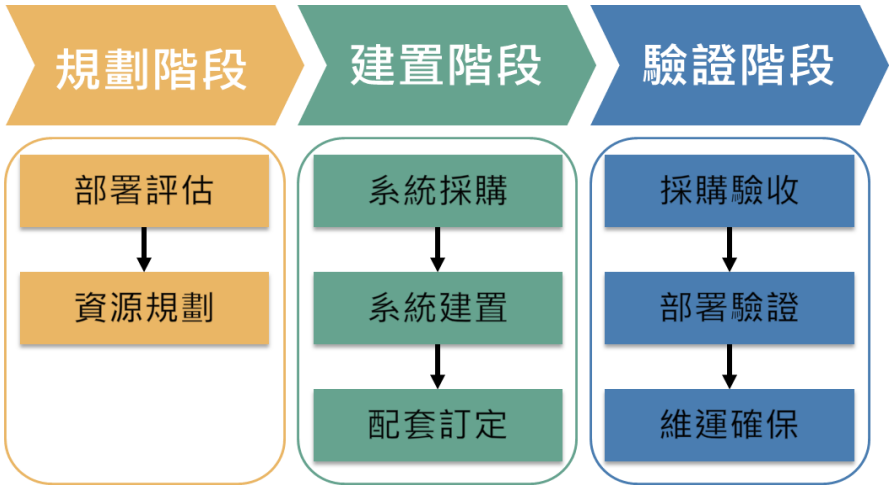
機關導入流程(至現有環境)

身分鑑別組件部署：提供3部主機(或虛擬機器)，用於部署決策引擎、存取閘道及FIDO2伺服器
若要試行「設備識別」與「信任推斷」，則新增設備鑑別伺服器、設備健康伺服器及信任推斷伺服器



機關試行與導入

- **機關遴選、試行與導入：110年 ~111年**
  - **遴選標準**
    - 機關資通系統之**帳號集中度高**
    - 所屬機關資通系統**向上集中度高**
    - 機關資通系統由**外網存取之需求高**
    - 機關之**配合意願高**
- **110年擇定身分驗證試行機關，111年正式導入完成**



重點工作宣導
資安弱點通報機制(VANS)推動

VANS推動情形

數位發展部資通安全署
Administration for Cyber Security, moda

應辦事項

- A、B級公務機關及關鍵基礎設施提供者初次受核定或等級變更後之1年內，完成VANS導入作業。
- C級公務機關及關鍵基礎設施提供者初次受核定、等級變更後之2年內或112年8月23日前（資通安全責任等級分級辦法110年8月23日修正施行前已受核定者），完成VANS導入作業。

法遵落實情形

- 截至112年4月底止，A、B級公務機關均已完成導入VANS。另查C級公務機關僅約20%完成導入。爰請協助督導所屬、所管或所監督資安責任等級C級公務機關，依限落實完成導入VANS。

VANS導入注意事項

數位發展部資通安全署
Administration for Cyber Security, moda

弱點修補及期限

注意弱點通知，高風險以上弱點(CVSS 7分以上)應即時完成修補，相關改善措施及弱點處置方式於1週內至系統填報。

資訊資產盤點

資料上傳VANS系統前應比對資訊資產(如作業系統數)與實際導入電腦數量是否相符，以確保系統上資訊資產盤點正確性。

帳號申請

於iAuth平台提出VANS機關管理者帳號權限申請，並填寫申請(異動)單(紙本)，完成後將表單Email予資安署審查。

結語

- 資安事件，不限駭侵與否、不限3級以上事件、不限核心系統，皆應於時效內通報。
- 持有全國性資料之彙整機關，建議強化以下行為：
  - ✓ 連結機關：盤點介接機關，要求資安作為、加強稽核、取消離線媒體交換等。
  - ✓ 資料保護：資料加密儲存、查詢過程遮蔽、最少揭露、大量資料查詢之審核預警機制、資料查詢日誌等。
  - ✓ 使用權限：個人資料蒐集應以最小且必要為原則、限縮申請項目及內容、職務異動即清除權限。
  - ✓ 核心系統納入資安威脅偵測管理（SOC）、導入端點偵測及應變機制（EDR）、定期存取日誌等。
- 辦理法遵規定事項，如EDR及VANS等，請注意法遵期限並落實辦理。

綜合討論

參考資訊-資通安全署

數位發展部資通安全署
Administration for Cyber Security, moda

- **https://www.acs.gov.tw/**

參考資訊-國家資通安全研究院

數位發展部資通安全署
Administration for Cyber Security, moda

- **https://www.nics.nat.gov.tw/**

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理