從資安長的角度來看零信任架構的佈局

主講人：查士朝
國立臺灣科技大學資訊管理系 教授
國立臺灣科技大學資通安全研究與教學中心主任

公開發行公司建立內部控制制度處理準則修訂 (110/12/28)

- 第 9-1 條
  - 公開發行公司應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。符合一定條件者，本會得命令指派綜理資訊安全政策推動及資源調度事務之人兼任資訊安全長，及設置資訊安全專責單位、主管及人員。
  - 前項一定條件，由本會定之。

分級標準	資安單位暨人力編制	實施時程
第一級： 符合下列條件之一者： • 資本額100億元以上 • 前一年底屬臺灣50指數成分公司 • 藉電子方式媒介商品所有權移轉或提供服務（如電子銷售平台、人力銀行等）收入占最近年度營業收入達80%以上，或占最近二年度營業收入達50%以上者	應設資安長及設置資安專責單位（包含資安專責主管及至少2名資安專責人員）	111年底設置完成
第二級： 第一級以外之上市（櫃）公司，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者。	資安專責主管及至少1名資安專責人員	112年底設置完成
第三級 第一級以外上市（櫃）公司，最近3年度稅前純益有連續虧損，或最近年度每股淨值低於面額。	至少1名資安專責人員	鼓勵設置

原本資通安全管理法就已經有對公務機關有要求，現在擴大到上市櫃公司

第 二 章 公務機關資通安全管理

第 10 條　公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

第 11 條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

第 12 條　公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。

第 13 條　1　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。

2　受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

第 14 條　1　公務機關為因應資通安全事件，應訂定通報及應變機制。

2　公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。

https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297

雖然我有聽過一些竅門，但是先假設有認真做好了

為什麼要有資訊安全長？

資訊安全長要做什麼？

過去企業對資訊安全長與資安部門的錯誤看法

研發

專案

業務

資訊部

資訊安全

錯誤觀念：
資訊安全是資訊部門的事，
那由資訊部門長出一塊來
負責資訊安全就好

錯誤觀念：
發生資訊安全事件就是
資訊安全部門的問題

在講資安長的或資安部門的責任前，最重要的是要在組織內建立以下概念

資訊安全是每個人的責任，而資訊安全專責單位是要協助每個人能盡到他的責任

最懂業務的資訊安全風險的還是各業務單位，資安專責單位是要協助釐清資安風險，並且進行控制

資安風險的因應有一定成本，要控制到什麼程度還是要靠各業務單位共同決定

資訊安全事件有時無法避免，事情發生後重點在如何妥善處理而非互相指責

資安長要做什麼？

- 公開發行公司建立內部控制制度處理準則第 9-1 條
  - 公開發行公司應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業

釐清法遵要求並要求符合	資訊安全制度之規劃	監控及執行資訊安全管理作業
與主管機關溝通和作為和主管機關溝通的負責人	規劃與調整資訊安全策略與藍圖	擬定預算執行藍圖
意外事件的處理與因應	向董事會或高層說明資訊安全策略或要推動的重要工作	推動或參與重大資訊安全設備或計劃的採購與執行

以我現在觀察，許多企業已經有設立資安長了，那就從資安長如何向董事會報告來看

- 其實很多董事會成員不見得對資訊安全很熟，但是對於重大資訊安全事件一定是有想要了解的
  - 過去發生的事件是否有解決？如果沒有，那對策是？
  - 其他公司或新聞上的事件是否會發生在本身的公司上
- 業務報告
  - 要讓人知道有一套制度在組織中有效運行
  - 這制度應該是基於一個被認可的框架
  - 過去常會說要有一個資安現況與績效表，但是要有感不容易
    - 例如和其他同類型公司比，資安事件與資安投資的比較
  - 過去規畫的執行狀況
- 接下來要進行的重要工作
  - 因應問題或是法規要求會比較容易鋪陳
  - 另外就是要有一個藍圖，表示不是臨時想到的結果

不是只拋出問題，要提供解決方案

時間有限，著重於大局，不是秀肌肉的時候

成本與效益是要思考的重點

零信任架構是現今資安長應該知道的法律規範，也可以是建立資訊骨幹的藍圖

- 2020 年：美國 NIST 發布 NIST SP 800-207
- 2021 年：美國國防部發布零信任參考架構
- 2021 年 5 月：美國總統拜登發布指令，要求美國聯邦政府將採用零信任架構，作為資通安全現代化的策略之一。
- 2022 年 1 月：美國預算與管理辦公室，據此制定備忘錄，要求美國聯邦政府單位在 2024 會計年度，一以下五大支柱，達成零信任架構的策略目標：

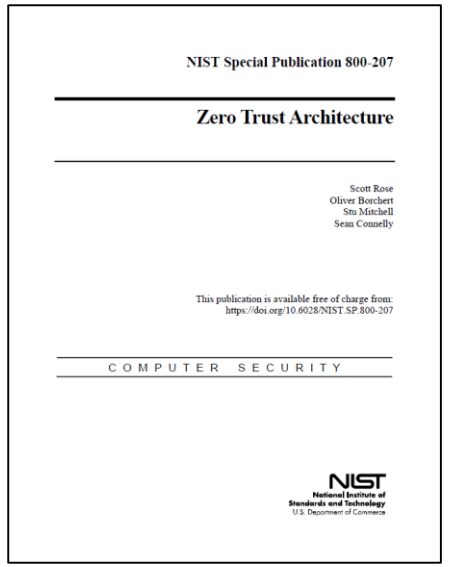
身分識別

裝置

網路

應用程式

資料


NIST Special Publication 800-207

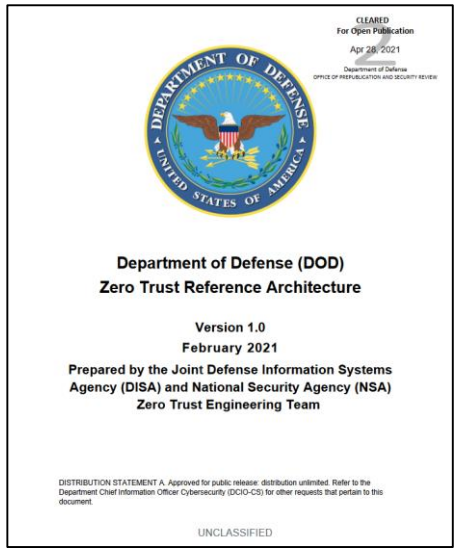
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


CLEARED
For Open Publication
Apr 28, 2021
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0
February 2021
Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Refer to the Department Chief Information Officer Cybersecurity (DCIO-CS) for other requests that pertain to this document.

UNCLASSIFIED


BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

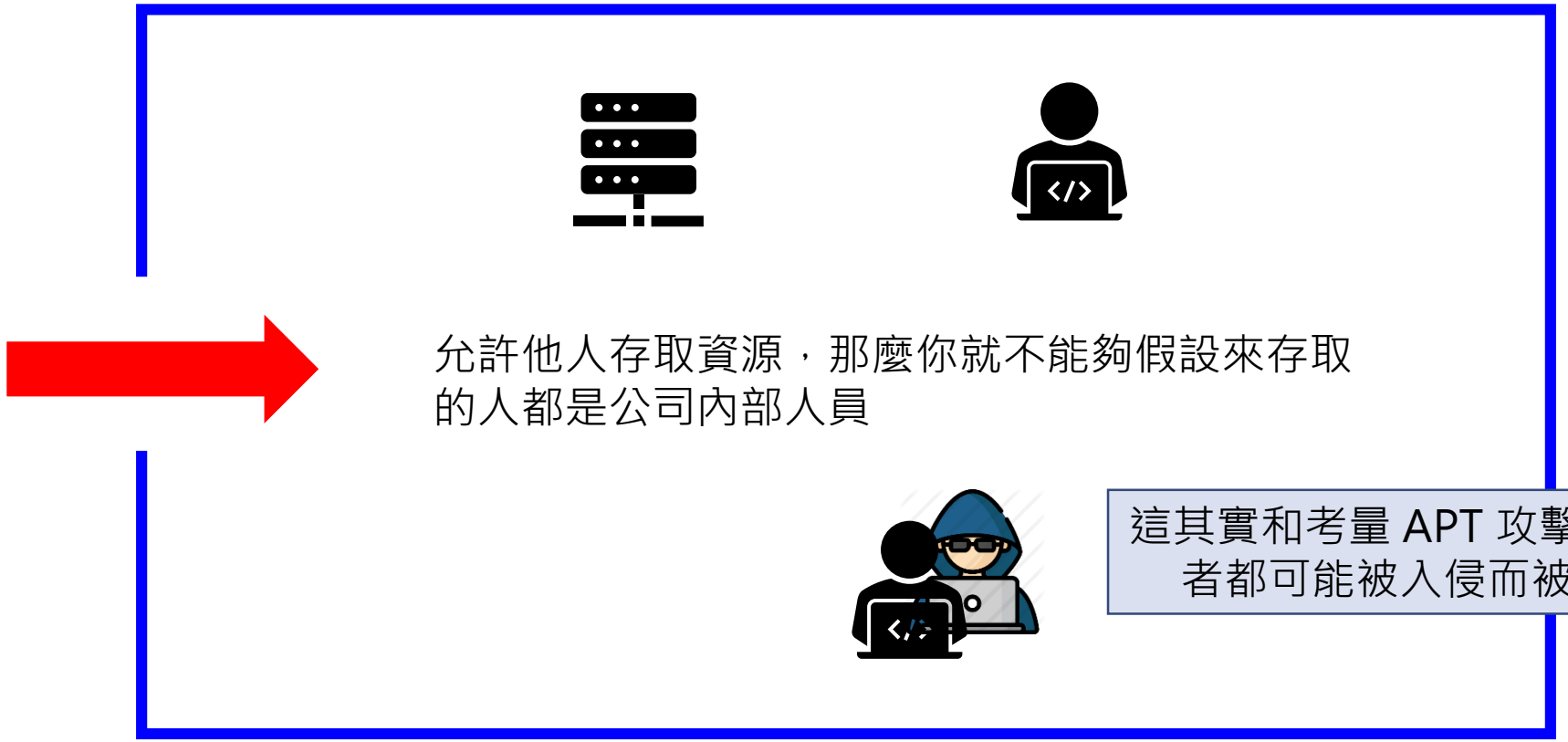
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

一般人對零信任架構已經夠困擾了，又哪來五大支柱？

https://xtech.nikkei.com/atcl/nxt/column/18/00001/05816/?n_cid=nbpitp_fbed&fbclid=IwAR1ZzsvEypUKwYyFw1vwo7gHc--sE3lMtN0nCDUjs29mzEe8sMQ9FnxC8Jw

我建議回到零信任架構的源頭來思考

- 2004 的傑里科論壇 (Jericho Forum) 要求企業去周邊化 (de-perimeterization)，彼此能夠共享資源
- 如果企業間的資源可以共享，代表著甚麼？



美國聯邦零信任策略備忘錄的要求

身分識別

要決定可不可以存取前，要先判斷對方是誰

不可以不經過檢查就直接允許存取

網路

存取一般是經過網路，總不能是超能力吧

應用程式

應用程式通常是弱點所在，也是入口

系統

不信賴

政策決策與落實點 (Policy Decision/ Enforcement Point)

信賴

企業資源 Enterprise Resource

裝置

使用者的裝置可能被利用來當作跳板進行攻擊

用更能反映現行風險的規則去進行判斷

裝置

資料通常是核心需要保護的資源之一

美國聯邦零信任策略備忘錄的要求–身分識別

- 目標：員工使用全企業通用的身分識別去存取工作時所用的應用程式。使用避免釣魚的多因鑑別來避免個人收到複雜的線上攻擊
  - 減少使用者因為被釣魚而被當作跳板攻擊的機率與影響
- 動作：
  - 建立採用集中化的企業身分識別
    - Silo 與集中化的管理
  - 使用多因鑑別
    - 身分鑑別不是網路層級，而是要對各別使用者身分
    - 建議移除密碼中要使用特殊字元以及定期更新密碼的要求
  - 存取控制能夠更具有彈性
    - 至少要能針對存取裝置進行限制

對資安長的建議

- 盤點重要資訊資產，確保資訊資產的存取都需要經過身分鑑別與存取控制
  - 可參考工控安全領域的區域與管道概念
- 重新審視存取控制政策，審視身分鑑別機制的規則與設置方式
  - 重要資源存取的多因子身分鑑別
- 建立更具有粒度與彈性的存取控制方式

其實在該備忘錄當中有一段話蠻顛覆想像的

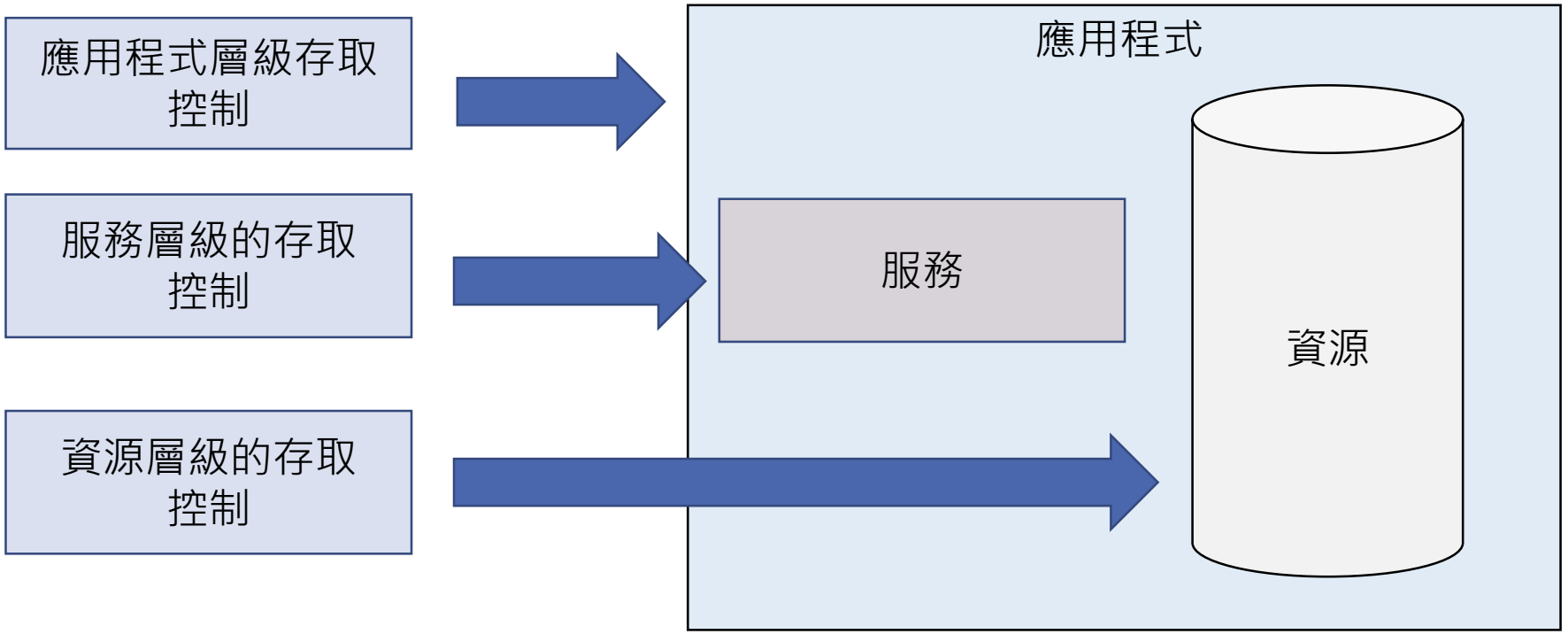
- *目前，許多聯邦政府單位的授權模型聚焦使用角色導向存取控制(RBAC)，而依賴先前定義的靜態角色，並且將使用者指派到這些角色，以決定他們的權限。零信任架構應該要整合更具粒度與動態的權限，像是屬性導向存取控制模型(ABAC)一般。*
- *Currently, many authorization models in the Federal Government focus on role-based access control (RBAC), which relies on static pre-defined roles that are assigned to users and determine their permissions within an organization. A zero trust architecture should incorporate more granularly and dynamically defined permissions, as attribute-based access control (ABAC) is designed to do*

重點是要能夠把動態的因子考慮進去

- 可以比對 NIST SP 800-207 當中的零信任架構其中一項教條：
  - *資源的存取應該要基於客戶端識別、應用服務，以及要求存取資產可觀察到的狀態，以及可能包括的行為或環境屬性去動態決定*
  - *Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes*

不能夠說一個裝置或使用者被信賴可存取就永遠可以存取

可以設定不同粒度的存取控制



美國聯邦零信任策略備忘錄的要求–裝置管理

- 目標：聯邦政府有其所使用與授權供政府作業用的裝置清單。並且能夠偵測對於這些裝置的意外事件並做出回應。
- 動作：
  - 建立資產清單
  - 參加美國網路與骨幹安全司(Cybersecurity and Infrastructure Security Agency, CISA)的 CDM (Continuous Diagnostics and Mitigation) 計畫
  - 確保每個使用者所操作的公發裝置都有安裝機構選擇的端點監控與回應工具(Endpoint Detection and Response, EDR)

對資安長的建議

- 選擇端點防護工具
- 確認所有的作業使用裝置都有至於端點防護保護之下 (或者有其他防禦機制)
- 能夠掌握作業裝置的安全狀態
- 安裝防火牆與確保更新
- 裝置組態安全強化
- 如果不能監控安全狀態，那就需要限制存取

美國聯邦零信任策略備忘錄的要求–網路

- 目標：機關對所有 DNS 與 HTTP 交通加密，並且按照應用切割網路。聯邦政府應該要找出傳輸電子郵件時有效的電子郵件加密方法。
- 動作：
  - 加密 DNS 流量 (DNS over HTTPS 或 DNS over TLS)
  - 強制使用 HTTPS
  - 加密電子郵件流量
  - 依應用切割網路

對資安長的建議

- 即便是內網，在零信任的架構下，都需要使用加密以避免資料被竊取
- 準備網路加密機制被入侵的對策
- 做到加密與監控的調和
- 停用經非安全通道傳輸的應用
- 做好網路分割

美國聯邦零信任策略備忘錄的要求–應用程式

- 目標：機關應該對於像是網路連線的應用程式進行嚴格的實務測試，並且安排好定期檢測的時程，並且歡迎外部的弱點報告
- 動作：
  - 應用程式安全測試
  - 善用第三方進行測試
  - 歡迎外部應用程式弱點報告
  - 確保可網際網路存取之應用程式的安全性
  - 發覺可被網際網路存取的應用程式
  - 建立 DevSecOps 的程序，而避免安全檢查工作被繞過

對資安長的建議

- 識別所有可由網際網路存取的應用程式
- 妥善安排弱點掃描與滲透測試
- 確保軟體開發生命週期安全程序的運作
  - 可以搭配自動化工具
- 歡迎外界的弱點通報並且建立處理程序

美國聯邦零信任策略草案的要求 – 資料

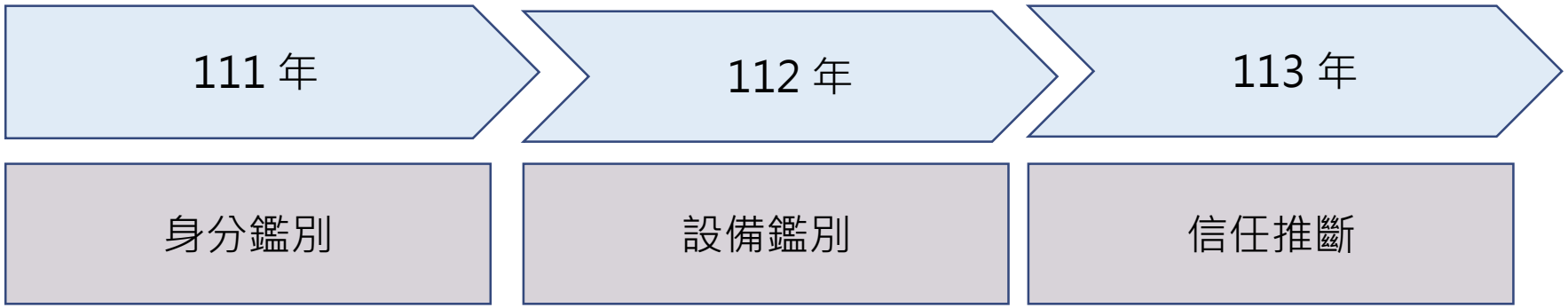
- 目標：
  - 機關依照資料分類，掌控資料流，並對資料進行保護。並且運用雲端安全服務與工具，去偵測、分類，與保護敏感資料，並且實作全企業的記錄與資訊分享控制機制。
- 動作：
  - 符合聯邦資料安全策略
  - 採用 SOAR 等自動化安全回應機制
  - 對於存取雲端服務上的敏感服務進行稽核
  - 及時對記錄進行評估

對資安長的建議

- 將資料按照敏感性分級並進行標記
- 掌握資安事件，並建立自動化安全回應機制
- 對於存取敏感資料的委外或雲端服務進行稽核。
- 收集紀錄並進行安全評估

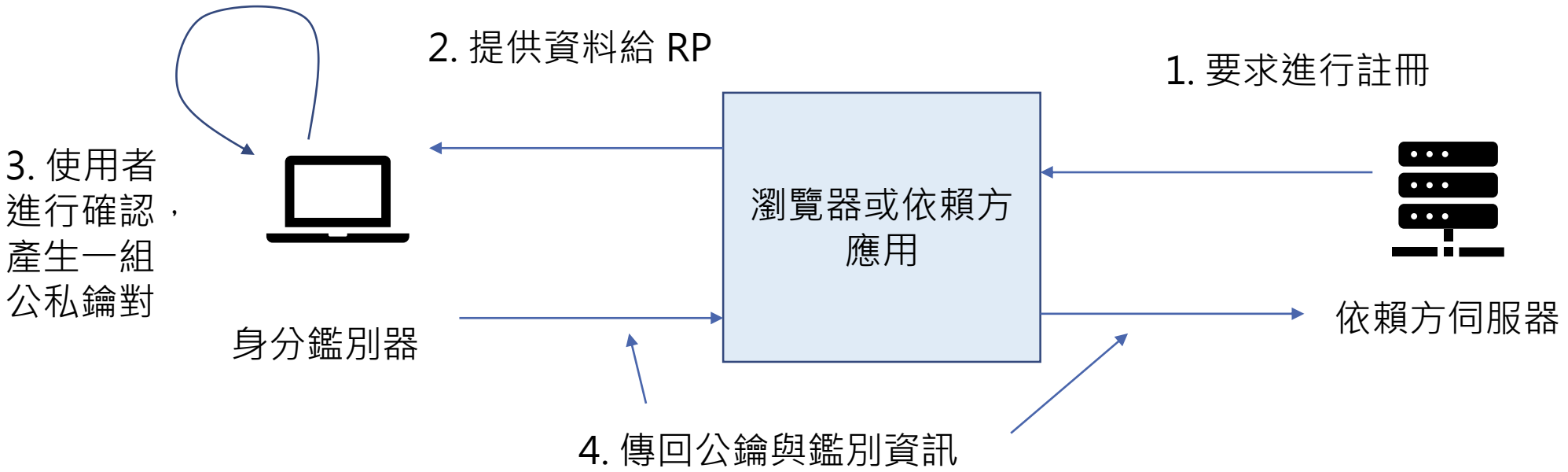
我國技服中心目前的規劃

- 行政院國家資通安全會報技術服務中心於 7 月 14 發布資料
  - *依據第六期「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，將發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深廣度*
  - *將由數位發展部資通安全署規劃投入經費，優先推動A級公務機關導入零信任網路*
  - *著眼於以下三項：*
    - *身分鑑別：FIDO2身分鑑別與鑑別聲明*
    - *設備鑑別：TPM設備鑑別與設備健康管理*
    - *信任推斷：基於分數與情境之信任推斷機制*



Fido 2 的註冊程序

其實註冊程序有個最重要的關鍵是在開始時，如何將鑑別器與使用者身分進行綁定

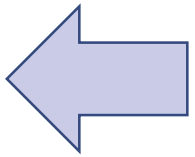


如果細分，Fido 2 可以分成 WebAuthn 與 CTAP 兩個協定，前者著重於瀏覽器或應用，後者針對與鑑別器間的通訊

在 Fido 1.0 的時候，分成 UAF (Universal Authentication Framework) 與 U2F，UAF 和上述程序類似，U2F 主要針對雙因子鑑別

這邊順便談一下 NIST SP 800-63-3 的三種身分鑑別等級

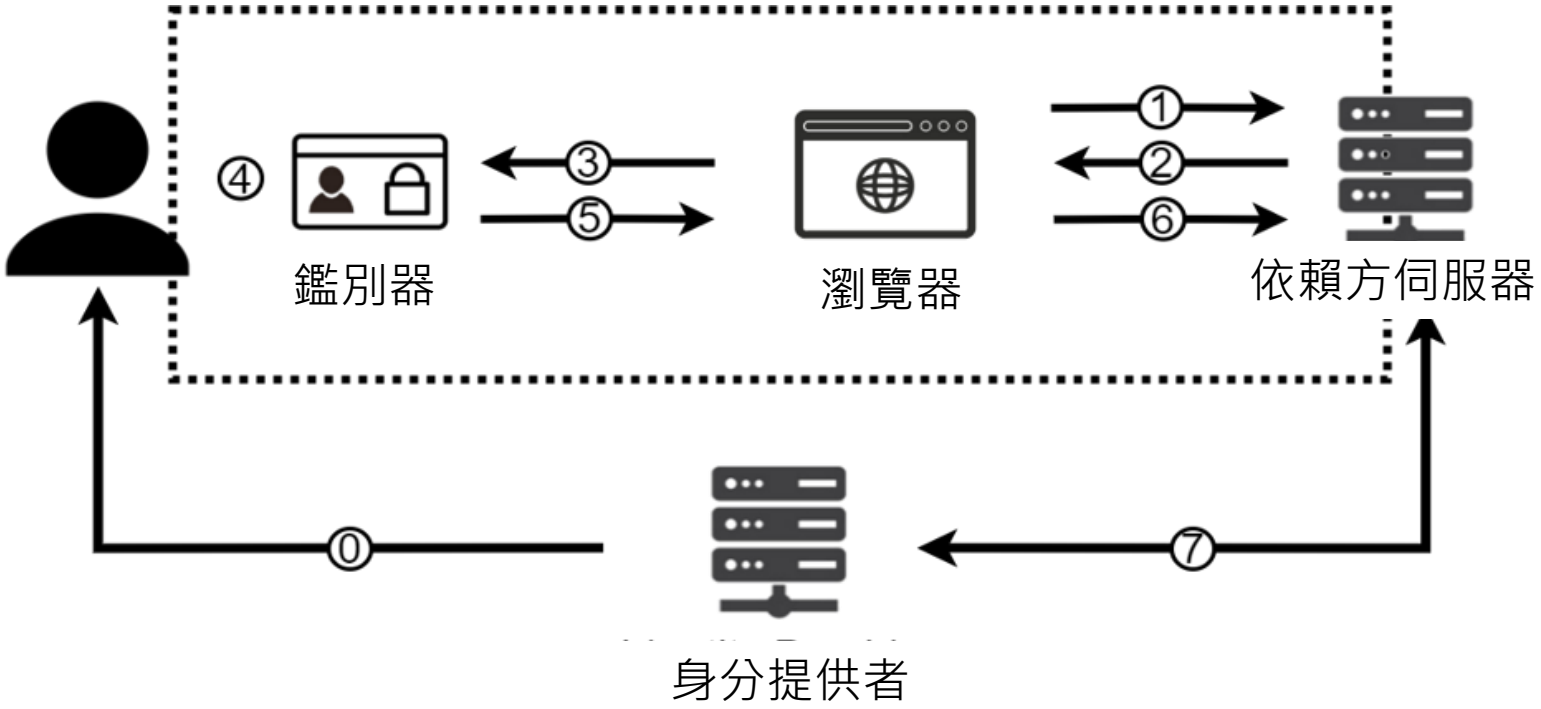
- 身分確認等級
  - IAL1: 屬性可以被自我宣告或是被視為是自我宣告
  - IAL2: 透過遠端或人面對面驗證身分
  - IAL3: 透過人面對面的驗證身分



原本 WebAuthn 做法的等級

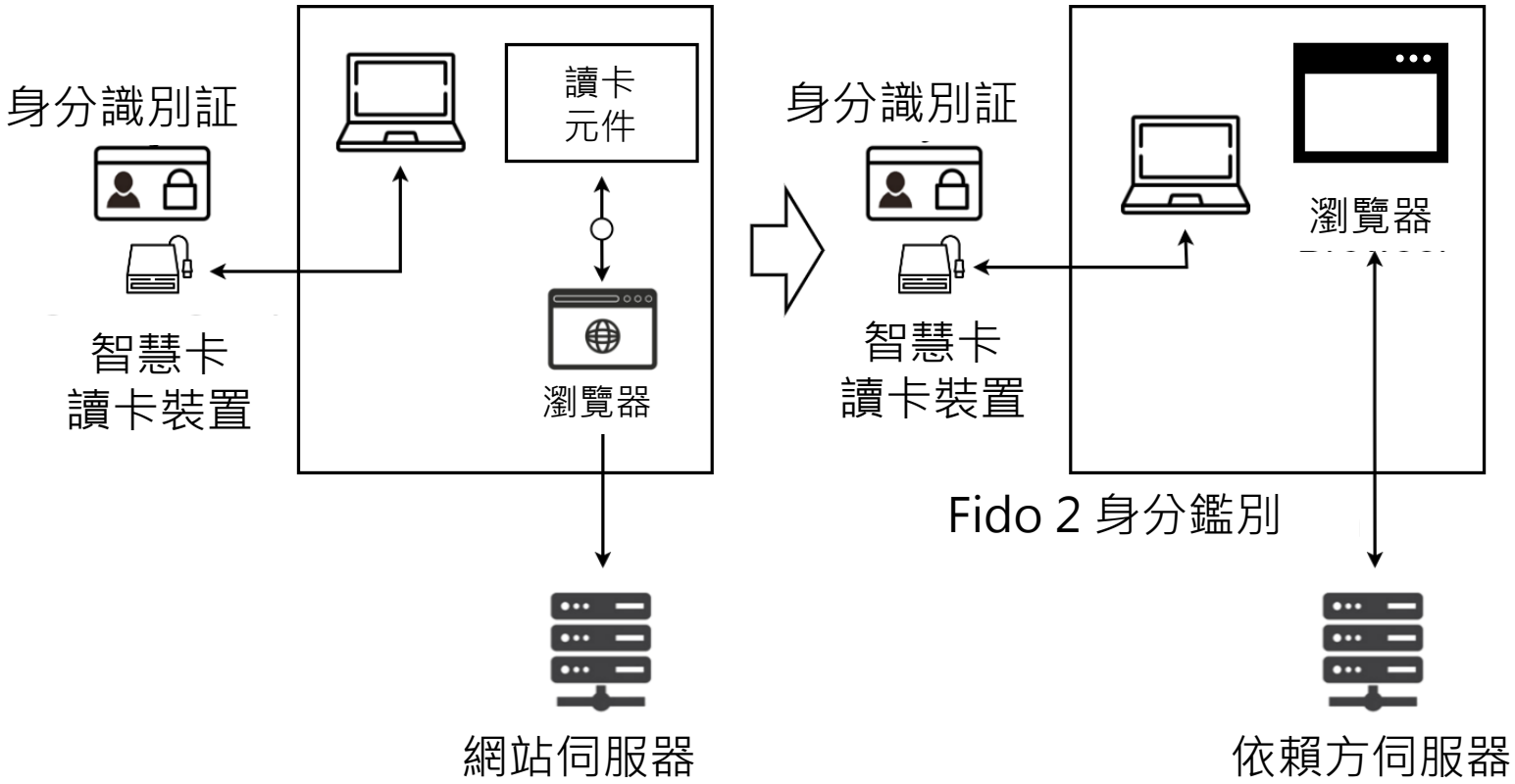
- 鑑別保證等級
  - AAL1: 提供最基本的單因子鑑別
  - AAL2: 透過雙因認證與安全鑑別協定，去確認鑑別器
  - AAL3: 除了滿足 AAL2，還要確認是使用硬體
- 聯合保證等級
  - FAL1: RP 允許身分提供者所發出的不記名聲明，而該聲明是由 IdP 所簽署
  - FAL2: 聲明有被加密，而 RP 可將之解密
  - FAL3: 註冊者能夠用自身的簽章去做證明
- 技術服務中心文件中提到：
  - *政府機關導入零信任網路應至少達到 IAL2/AAL3/FAL2 等級*

我們的研究成果 (1/2)



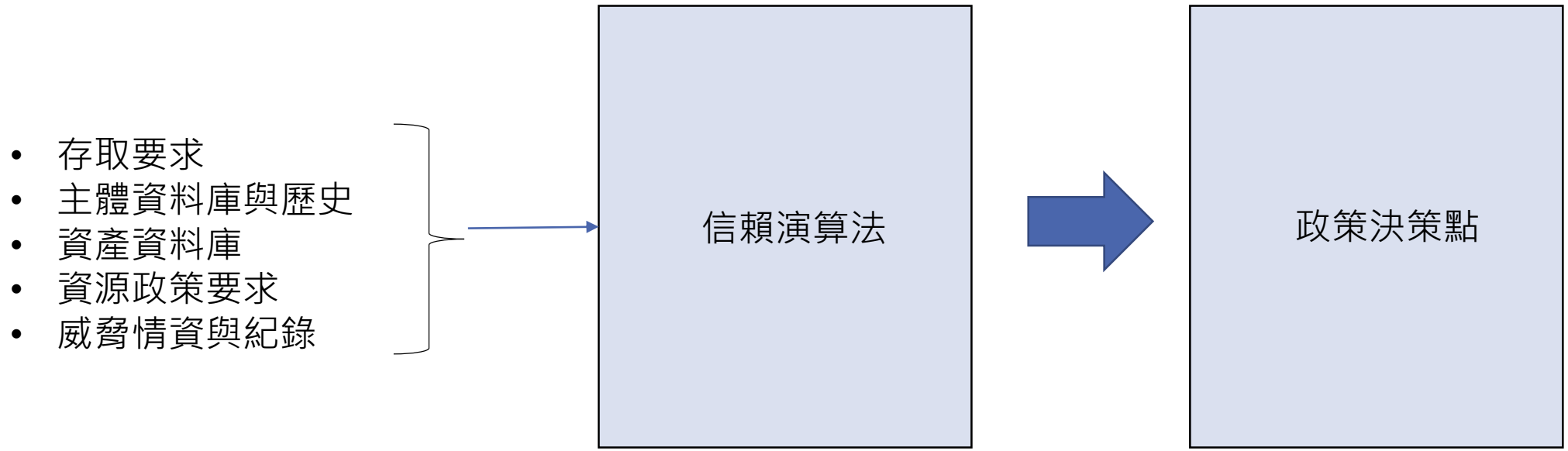
*曾在 IEEE RFID 2022 發表

我們的研究成果(2/2)



*曾在 IEEE RFID 2022 發表

NIST SP 800-207 並沒有明確的信任判斷演算法定義



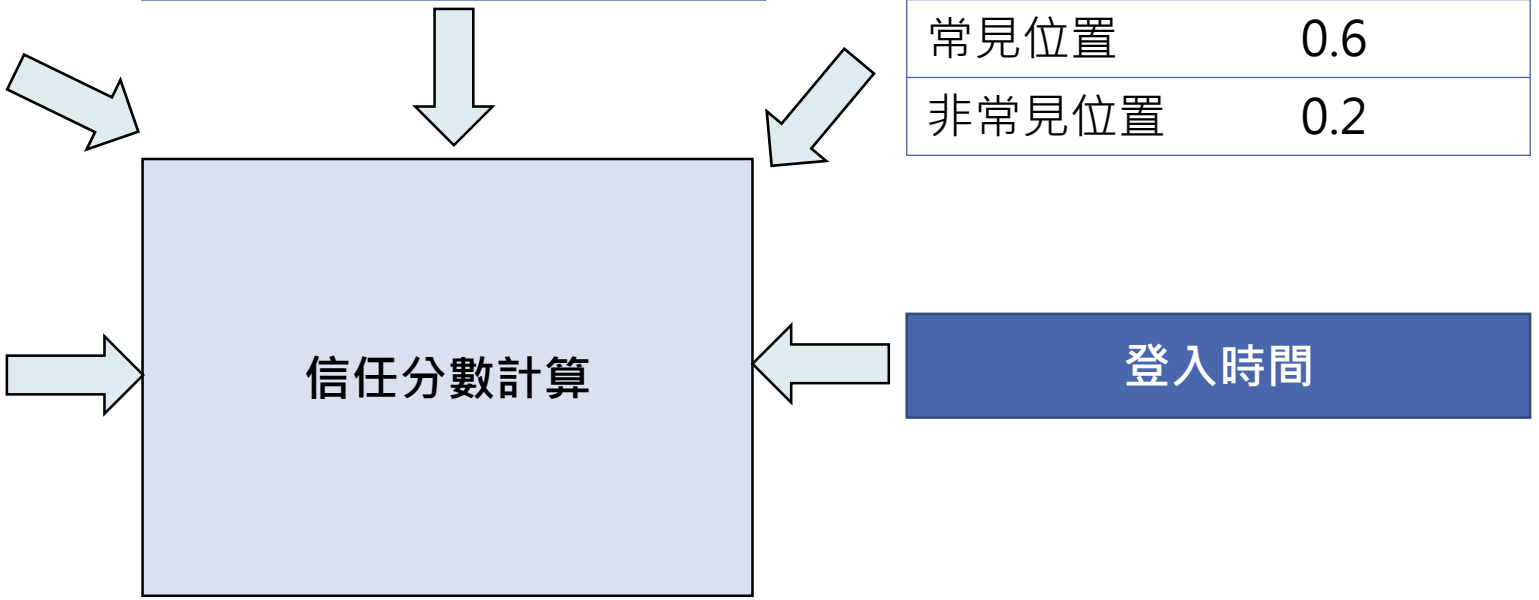
技術服務中心的信任推斷建議

身分鑑別方式	信任等級
AAL3	1.0
AAL2	0.8
AAL1	0.5

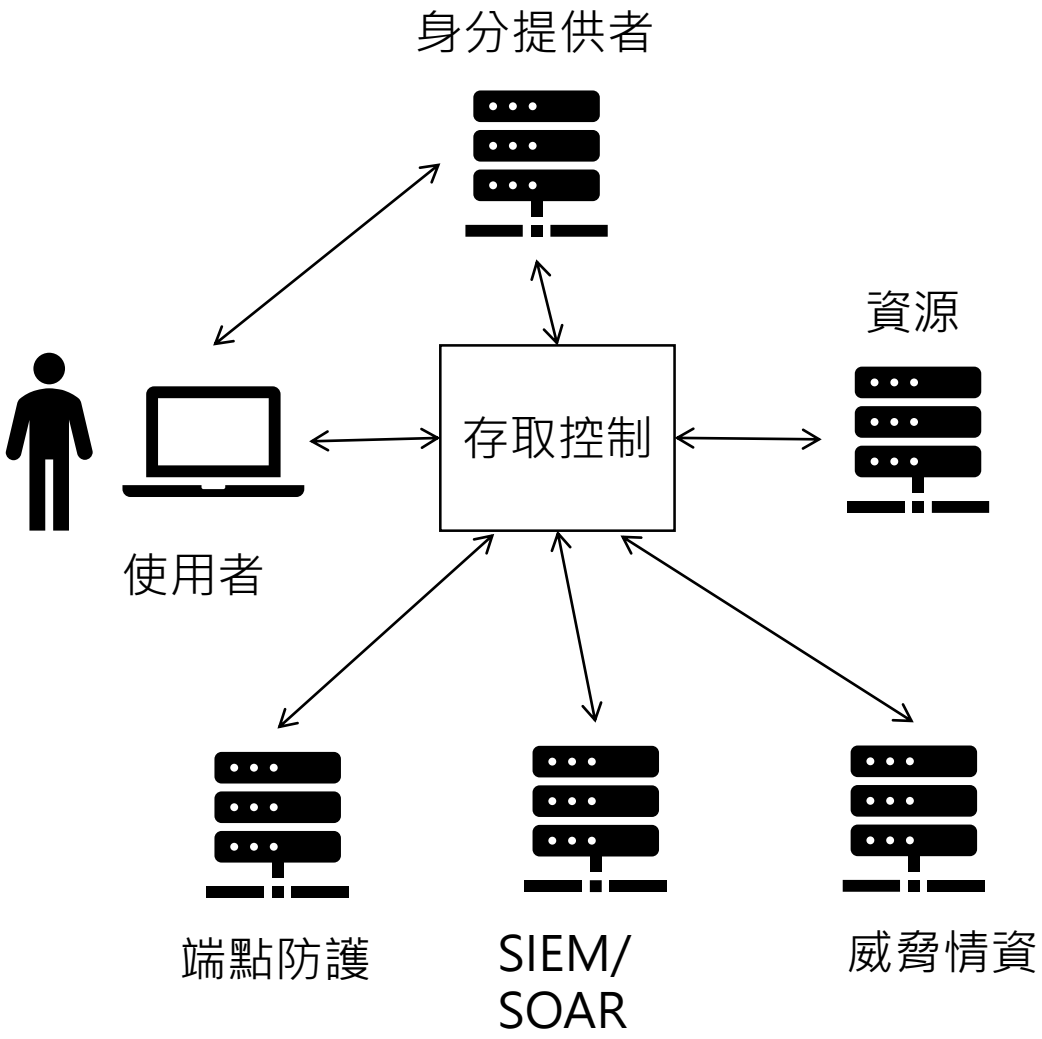
設備鑑別方式	信任等級
有 TPM	1.0
其他登錄設備	0.5

IP 位置	信任等級
內部位置	1.0
GSN 位置	0.8
常見位置	0.6
非常見位置	0.2

設備健康狀態	權重
作業系統更新	0.4
防毒更新	0.3
應用軟體更新	0.2
組態合規	0.1



但是

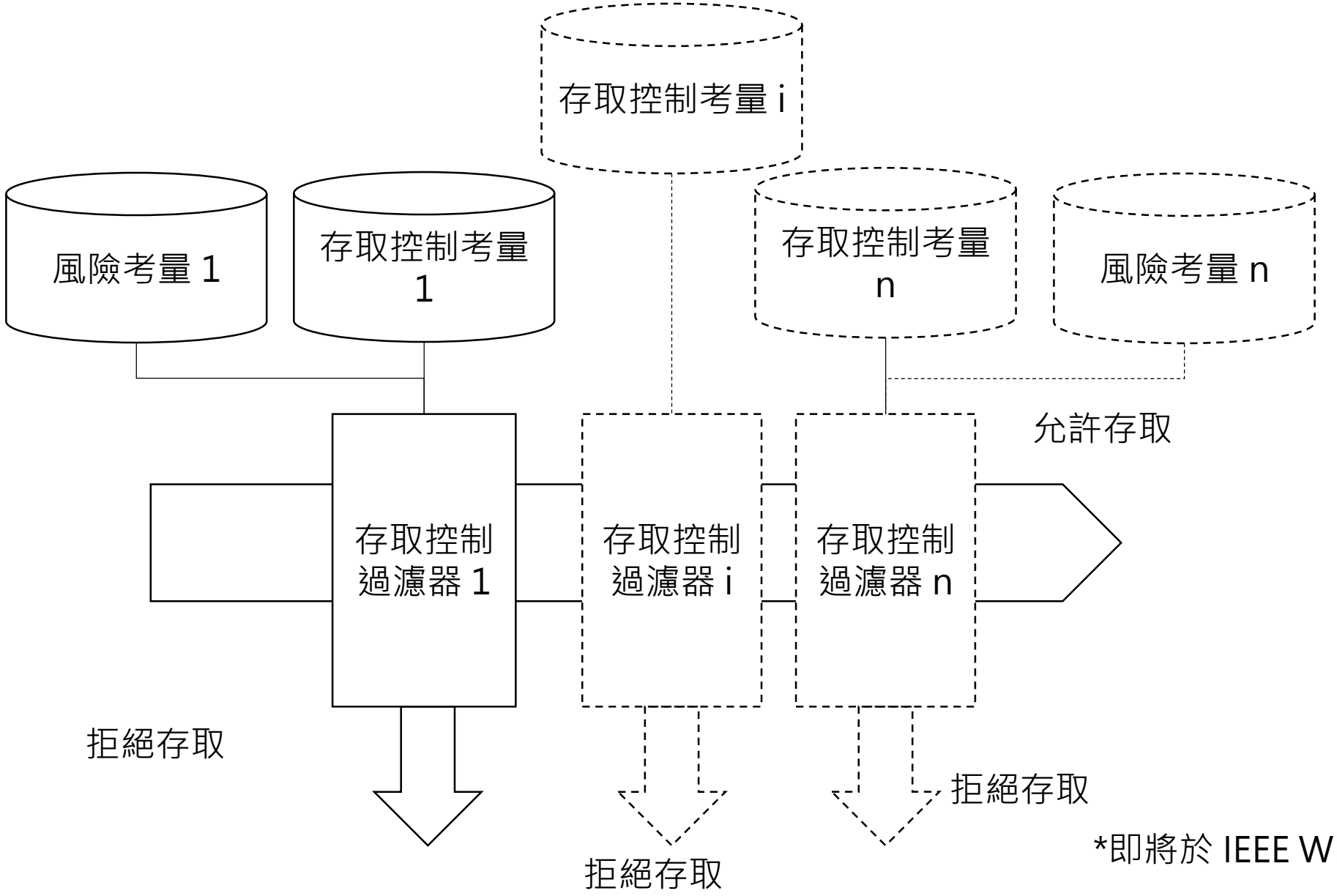


存取控制資料有很多不同來源

信任推定等級不見得所有人都會設

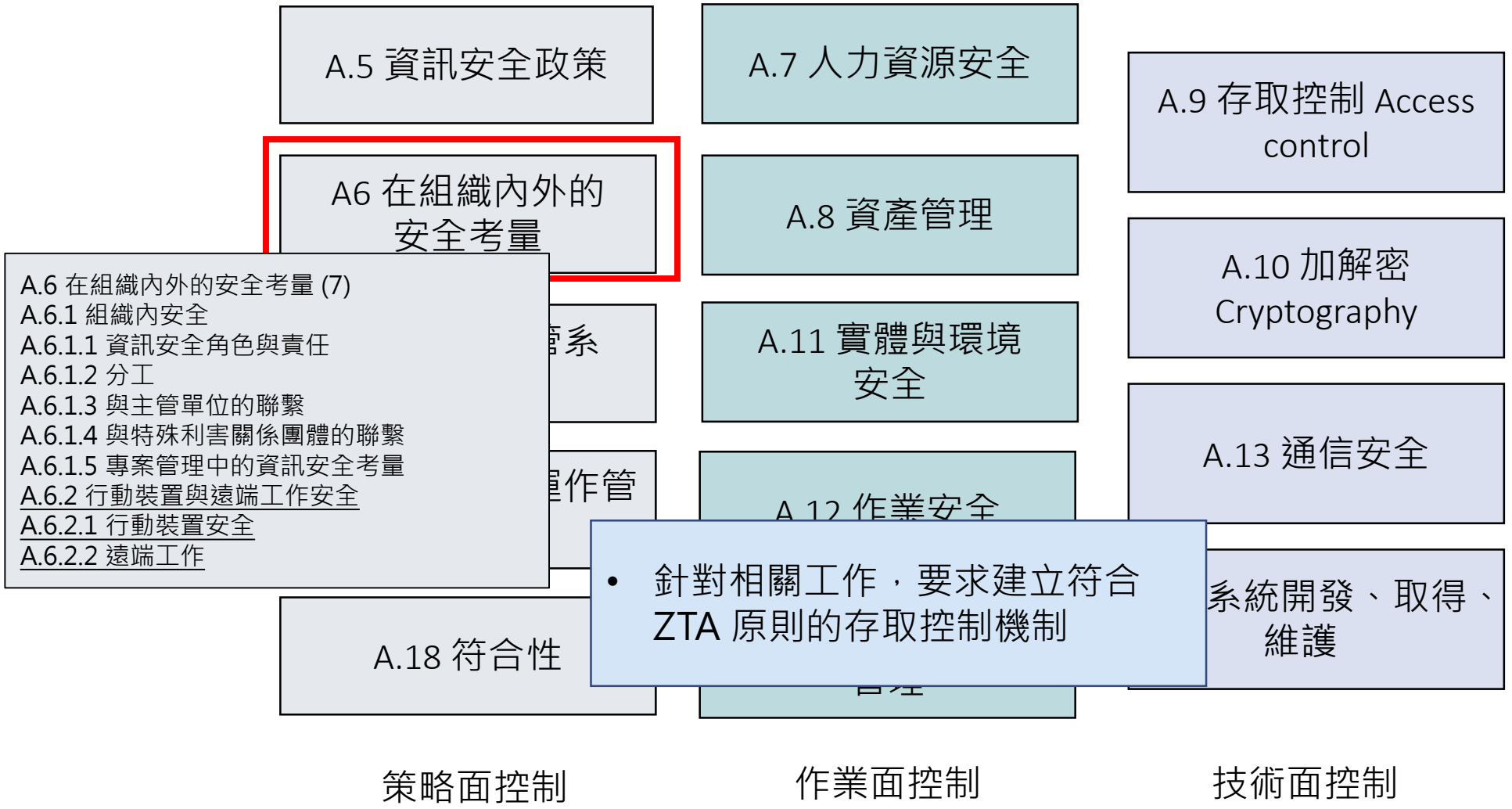
組織不見得一開始有足夠的資料

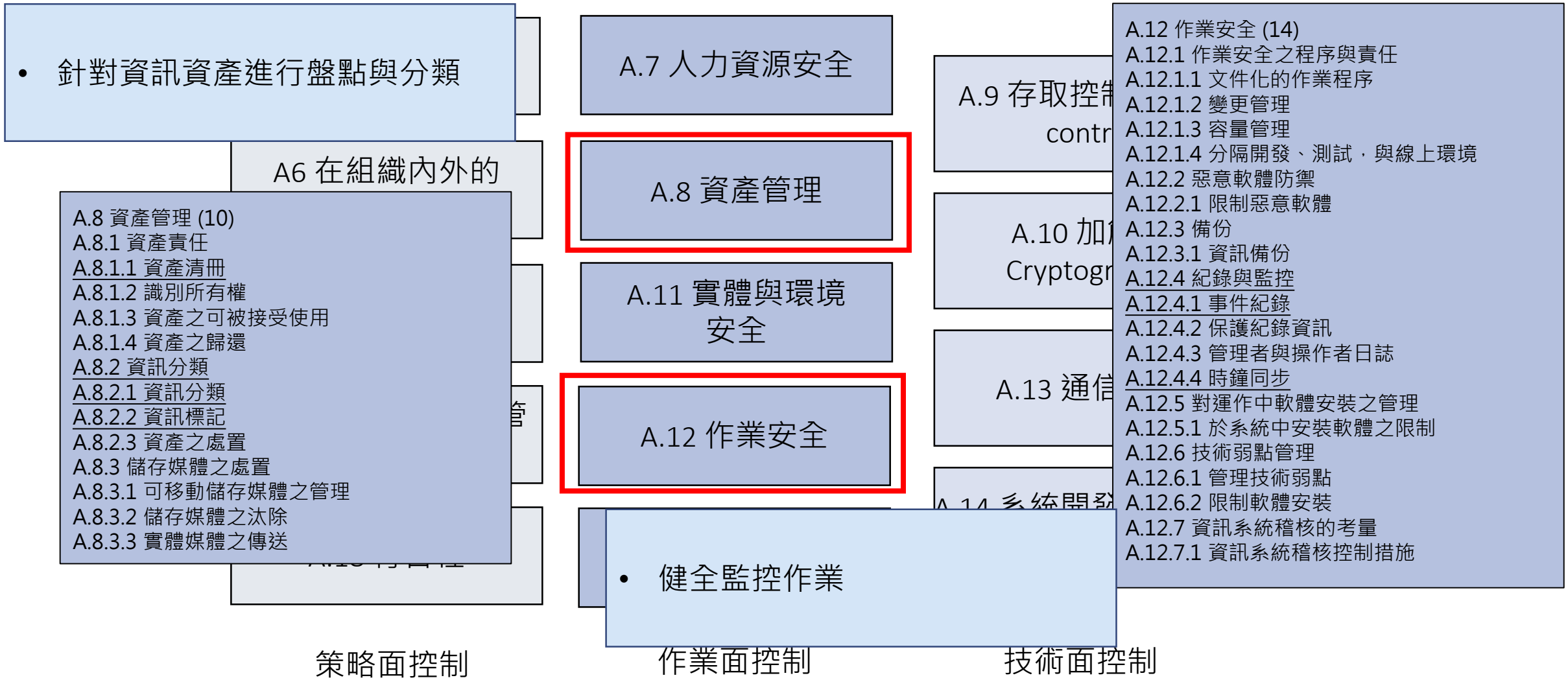
*即將於 IEEE WIoT 2022 發表

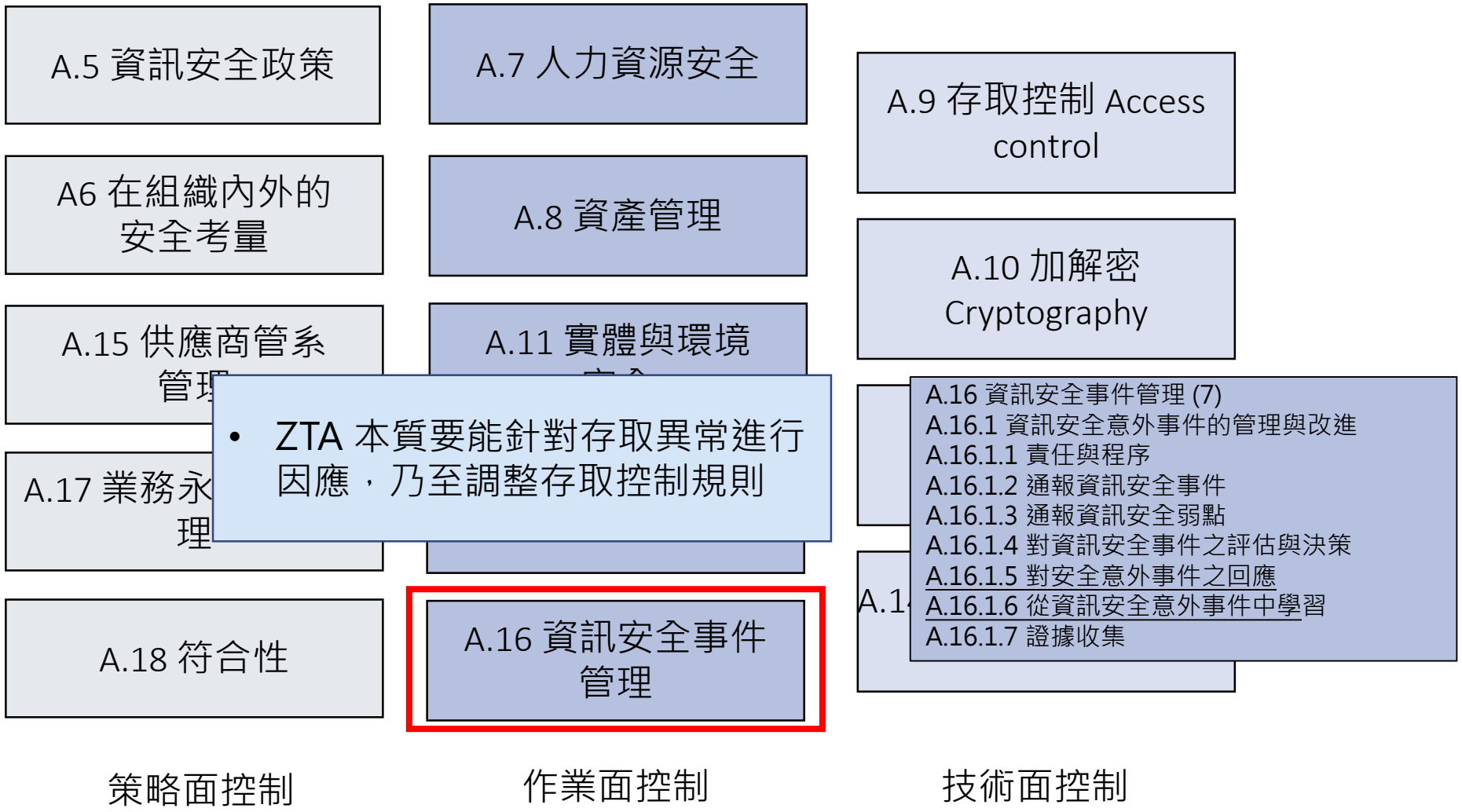


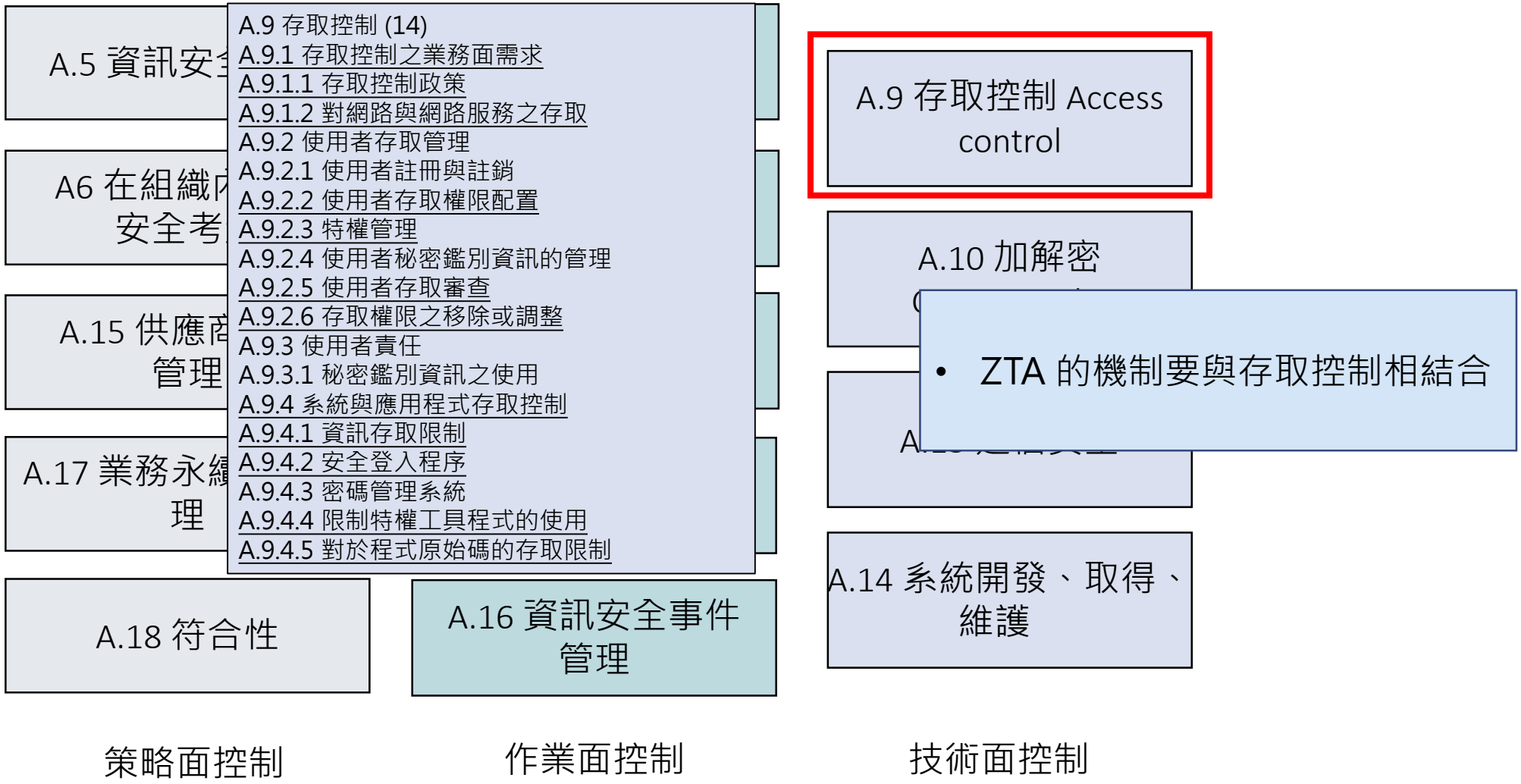
*即將於 IEEE WIoT 2022 發表

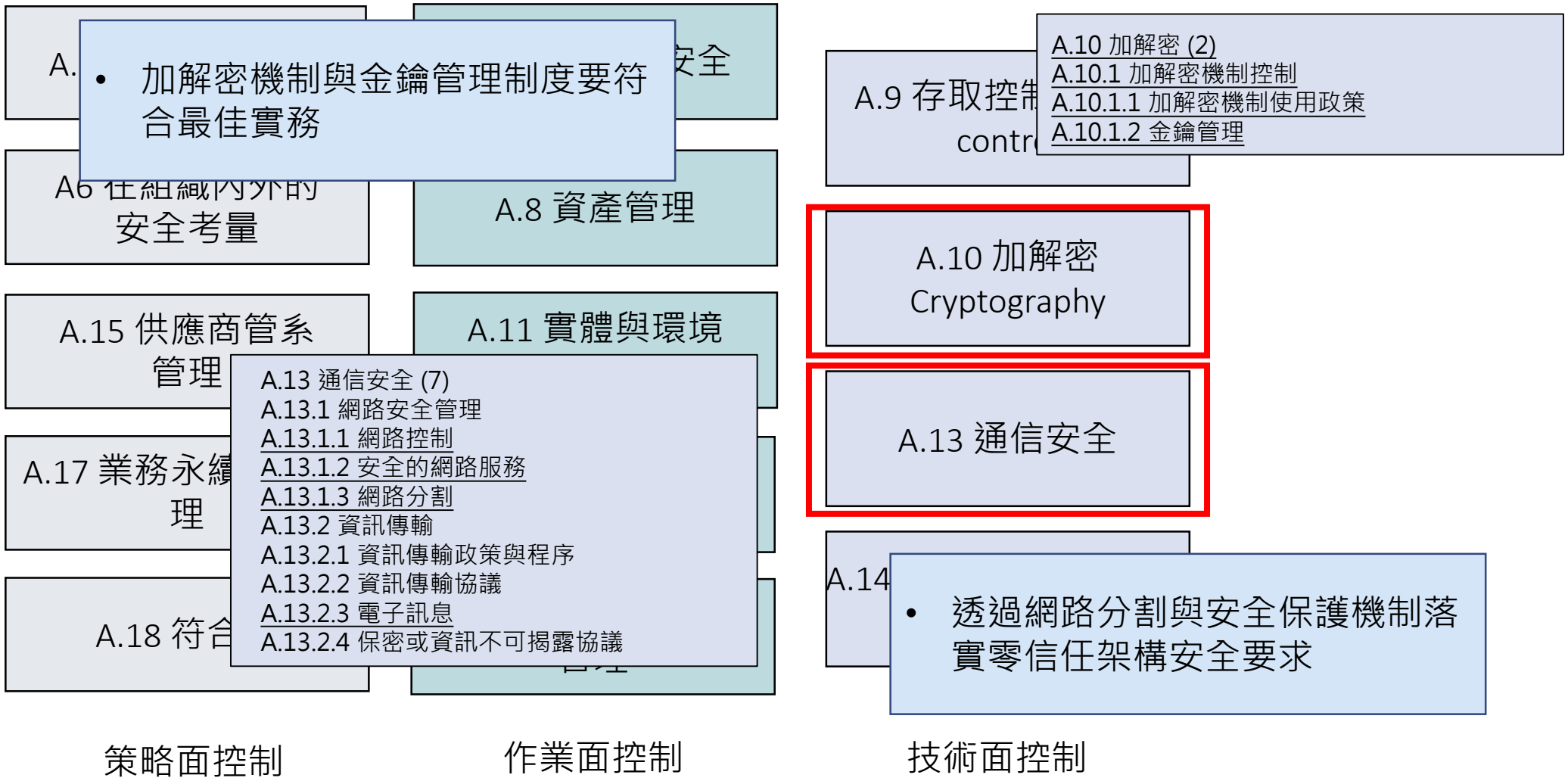
資安長應該要考慮到與將零信任架構與資訊安全管理制度整合

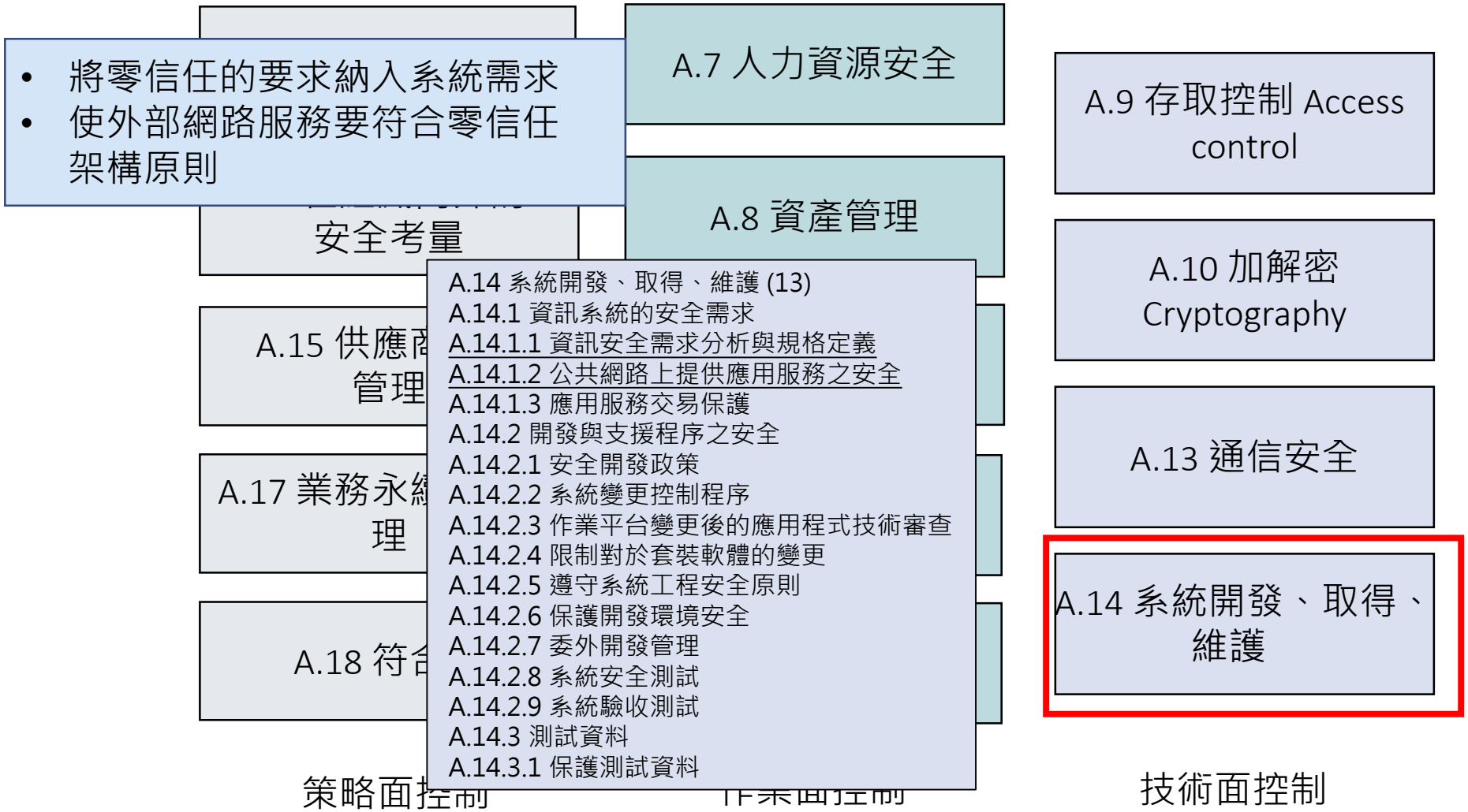

A.5 資訊安全政策
A.7 人力資源安全
A.9 存取控制 Access control
A6 在組織內外的安全考量
A.8 資產管理
A.10 加解密 Cryptography
A.6 在組織內外的安全考量 (7)
A.6.1 組織內安全
A.6.1.1 資訊安全角色與責任
A.6.1.2 分工
A.6.1.3 與主管單位的聯繫
A.6.1.4 與特殊利害關係團體的聯繫
A.6.1.5 專案管理中的資訊安全考量
A.6.2 行動裝置與遠端工作安全
A.6.2.1 行動裝置安全
A.6.2.2 遠端工作
A.11 實體與環境安全
A.13 通信安全
A.18 符合性
系統開發、取得、維護
• 針對相關工作，要求建立符合 ZTA 原則的存取控制機制
策略面控制
作業面控制
技術面控制


• 針對資訊資產進行盤點與分類
A6 在組織內外的
A.8 資產管理 (10)
A.8.1 資產責任
A.8.1.1 資產清冊
A.8.1.2 識別所有權
A.8.1.3 資產之可被接受使用
A.8.1.4 資產之歸還
A.8.2 資訊分類
A.8.2.1 資訊分類
A.8.2.2 資訊標記
A.8.2.3 資產之處置
A.8.3 儲存媒體之處置
A.8.3.1 可移動儲存媒體之管理
A.8.3.2 儲存媒體之汰除
A.8.3.3 實體媒體之傳送
A.7 人力資源安全
A.8 資產管理
A.11 實體與環境安全
A.12 作業安全
• 健全監控作業
A.9 存取控
contr
A.10 加
Cryptogr
A.13 通信
A.12 作業安全 (14)
A.12.1 作業安全之程序與責任
A.12.1.1 文件化的作業程序
A.12.1.2 變更管理
A.12.1.3 容量管理
A.12.1.4 分隔開發、測試，與線上環境
A.12.2 惡意軟體防禦
A.12.2.1 限制惡意軟體
A.12.3 備份
A.12.3.1 資訊備份
A.12.4 紀錄與監控
A.12.4.1 事件紀錄
A.12.4.2 保護紀錄資訊
A.12.4.3 管理者與操作者日誌
A.12.4.4 時鐘同步
A.12.5 對運作中軟體安裝之管理
A.12.5.1 於系統中安裝軟體之限制
A.12.6 技術弱點管理
A.12.6.1 管理技術弱點
A.12.6.2 限制軟體安裝
A.12.7 資訊系統稽核的考量
A.12.7.1 資訊系統稽核控制措施
策略面控制
作業面控制
技術面控制


A.5 資訊安全政策
A.7 人力資源安全
A.9 存取控制 Access control
A6 在組織內外的安全考量
A.8 資產管理
A.10 加解密 Cryptography
A.15 供應商管系
管理
A.11 實體與環境
A.17 業務永
理
A.18 符合性
A.16 資訊安全事件管理
A.16 資訊安全事件管理 (7)
A.16.1 資訊安全意外事件的管理與改進
A.16.1.1 責任與程序
A.16.1.2 通報資訊安全事件
A.16.1.3 通報資訊安全弱點
A.16.1.4 對資訊安全事件之評估與決策
A.16.1.5 對安全意外事件之回應
A.16.1.6 從資訊安全意外事件中學習
A.16.1.7 證據收集
• ZTA 本質要能針對存取異常進行因應，乃至調整存取控制規則
策略面控制
作業面控制
技術面控制


A.5 資訊安全
A6 在組織內 安全考
A.15 供應商 管理
A.17 業務永續 理
A.18 符合性
A.9 存取控制 (14)
A.9.1 存取控制之業務面需求
A.9.1.1 存取控制政策
A.9.1.2 對網路與網路服務之存取
A.9.2 使用者存取管理
A.9.2.1 使用者註冊與註銷
A.9.2.2 使用者存取權限配置
A.9.2.3 特權管理
A.9.2.4 使用者秘密鑑別資訊的管理
A.9.2.5 使用者存取審查
A.9.2.6 存取權限之移除或調整
A.9.3 使用者責任
A.9.3.1 秘密鑑別資訊之使用
A.9.4 系統與應用程式存取控制
A.9.4.1 資訊存取限制
A.9.4.2 安全登入程序
A.9.4.3 密碼管理系統
A.9.4.4 限制特權工具程式的使用
A.9.4.5 對於程式原始碼的存取限制
A.16 資訊安全事件管理
A.9 存取控制 Access control
A.10 加解密
A.14 系統開發、取得、維護
• ZTA 的機制要與存取控制相結合
策略面控制
作業面控制
技術面控制


A.
安全
A6 在組織內外的
安全考量
A.8 資產管理
A.15 供應商管系
管理
A.11 實體與環境
A.17 業務永續
理
A.18 符合
A.9 存取控制
contr
A.10 加解密
Cryptography
A.13 通信安全
A.14
• 加解密機制與金鑰管理制度要符合最佳實務
A.10 加解密 (2)
A.10.1 加解密機制控制
A.10.1.1 加解密機制使用政策
A.10.1.2 金鑰管理
A.13 通信安全 (7)
A.13.1 網路安全管理
A.13.1.1 網路控制
A.13.1.2 安全的網路服務
A.13.1.3 網路分割
A.13.2 資訊傳輸
A.13.2.1 資訊傳輸政策與程序
A.13.2.2 資訊傳輸協議
A.13.2.3 電子訊息
A.13.2.4 保密或資訊不可揭露協議
• 透過網路分割與安全保護機制落實零信任架構安全要求
策略面控制
作業面控制
技術面控制


將零信任的要求納入系統需求
使外部網路服務要符合零信任架構原則
A.7 人力資源安全
A.8 資產管理
安全考量
A.15 供應商管理
A.17 業務永續管理
A.18 符合
A.14 系統開發、取得、維護 (13)
A.14.1 資訊系統的安全需求
A.14.1.1 資訊安全需求分析與規格定義
A.14.1.2 公共網路上提供應用服務之安全
A.14.1.3 應用服務交易保護
A.14.2 開發與支援程序之安全
A.14.2.1 安全開發政策
A.14.2.2 系統變更控制程序
A.14.2.3 作業平台變更後的應用程式技術審查
A.14.2.4 限制對於套裝軟體的變更
A.14.2.5 遵守系統工程安全原則
A.14.2.6 保護開發環境安全
A.14.2.7 委外開發管理
A.14.2.8 系統安全測試
A.14.2.9 系統驗收測試
A.14.3 測試資料
A.14.3.1 保護測試資料
A.9 存取控制 Access control
A.10 加解密 Cryptography
A.13 通信安全
A.14 系統開發、取得、維護
策略面控制
技術面控制

結論

- 先不論名詞，零信任架構的確能夠解決現今的存取控制需求
  - APT 攻擊猖獗
  - BYOD 與遠端存取需求旺盛
- 但零信任架構要達到的目的很廣
  - 重點是要思考要解決的問題
- 可以從技術和制度上去進行規範
  - 技術上
    - 要求盤點使用者與資源
    - 要求做好網路分割與資源配置
    - 檢視權限並落實存取控制
    - 具備掌握資源與使用者狀態的能力
    - 對既有系統的要求
  - 制度上
    - 能夠針對遠端存取管理程序進行強化
    - 落實資產盤點與標記
    - 於存取控制管理程序中納入相關概念
    - 要求妥善進行記錄並檢視
    - 能夠按照風險設計存取控制政策

感謝各位的聆聽