雲端安全

**NIST 雲端運算五大特性**

* 隨需應變自助服務：
  + 使用者可自行配置和使用雲端資源，無需人工介入。
  + 例如：自助式開通虛擬伺服器、儲存空間等。
* 隨時隨地用任何網路裝置存取：
  + 雲端服務透過網路可供多種裝置存取
  + 例如：如手機、電腦、平板。
* 多人共享資源池：
  + 資源以多租戶模式提供，共享計算、儲存等資源。
  + 例如：多家公司共用同一伺服器集群。
* 快速重新部署靈活度：
  + 可根據需求快速擴展或縮減資源。
  + 例如：流量高峰時動態增加伺服器數量。
* 可被監控與量測的服務：
  + 雲端資源使用量可以被量化並監控。
  + 例如：根據使用情況計費。

**雲端服務模式**

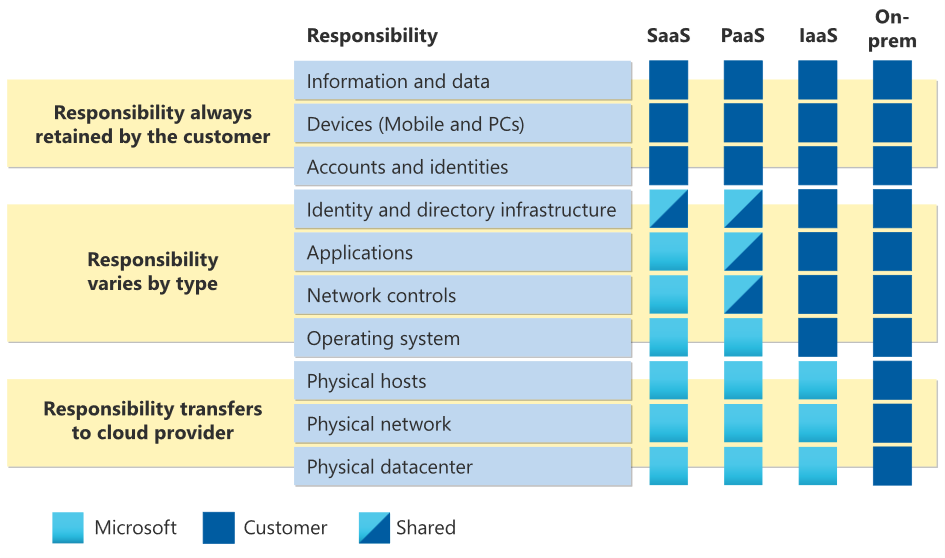
* 軟體即服務 (SaaS) ：
  + 定義：直接提供應用程式給用戶，無需管理基礎設施。
  + 例如：Gmail、Dropbox。
* 平台即服務 (PaaS) ：
  + 定義：提供開發與部署的環境，開發者專注於程式開發。
  + 例：AWS Elastic Beanstalk、Google App Engine。
* 基礎架構即服務 (IaaS) ：
  + 定義：提供虛擬機、儲存等基礎設施，由用戶自行管理。
  + 例：AWS EC2、Microsoft Azure。

**雲端部署模式**

* 私有雲 (Private Cloud) ：
  + 定義：雲端基礎設施專屬於單一組織，提供更高的安全性與控制。
  + 適用：金融機構、大型企業內部。
* 公有雲 (Public Cloud)：
  + 定義：由第三方提供服務，多租戶模式，成本較低。
  + 適用：一般商業應用、個人使用。
  + 例如：AWS、Azure、GCP三大雲端服務供應商(Cloud Service Provider, CSP)。
* 混合雲 (Hybrid Cloud)：
  + 定義：結合私有雲與公有雲，將敏感資料保留在私有雲，其餘部署於公有雲。
  + 適用：需要兼顧安全性與靈活性的企業。
* 社群雲 (Community Cloud)：
  + 定義：由多個組織共同使用，資源共享但需求一致。
  + 適用：教育機構聯盟、研究機構。
  + 例如：教育雲、醫療雲。

**共享責任模型**

* 定義：雲端安全責任由供應商和客戶共同承擔，具體責任分配因服務模式而異。
  + 用戶自建機房
    - 責任：所有責任由客戶承擔。
    - 適用場景：高度安全需求 (如金融機構)。
  + 基礎架構即服務 (IaaS)
    - 供應商負責：硬體、網路、資料中心安全。
    - 客戶負責：作業系統、應用程式、資料與帳號管理。
  + 平台即服務 (PaaS)
    - 供應商負責：硬體、網路、資料中心、作業系統和平台安全。
    - 客戶負責：應用程式邏輯、資料與帳號管理。
  + 軟體即服務 (SaaS)
    - 供應商負責：應用程式、伺服器和基礎架構的安全。
    - 客戶負責：資料與帳號管理 (如密碼、存取控制)。



(資料來源：Azure官網)

**雲端運算聯盟(CSA) 2024 年雲端風險 Top 11**

* **錯誤配置與變更控制不足**：雲端儲存桶 （如 AWS S3） 權限設為「公開」，客戶資料外洩。
* **身分與存取管理不善**：員工離職後未撤銷雲端權限，前員工仍能刪除生產環境資料。
* **不安全的介面與API**：未啟用身分驗證的 REST API，攻擊者直接調用竊取資料。
* **雲端安全策略不當**：企業直接套用預設防火牆設定，未關閉不必要的通訊埠 (如 SSH 22) 。
* **不安全的第三方資源**：使用未審查的第三方容器映像 (Docker Image) ，內含挖礦惡意程式。
* **不安全的軟體開發**：未過濾用戶輸入值，駭客透過輸入欄位發動 SQL 注入攻擊。
* **意外資料暴露**：工程師誤將雲端金鑰上傳至 GitHub ，攻擊者取得後操控資源。
* **系統漏洞**：未修補雲端伺服器的 Log4j 漏洞，駭客遠端植入後門。
* **雲端可視性不足**：企業使用 AWS + Azure 多雲，卻無統一監控，異常流量未被偵測。
* **未經認證的資源共享**：雲端檔案分享連結未設密碼，任何人點擊即可下載敏感文件。
* **進階持續性威脅**：國家級駭客透過釣魚郵件入侵，長期潛伏竊取研發資料。

**考古題：**

3. 2023年發現某國際知名汽車大廠於將近10年期間，將超過200萬輛車子位置資訊公開在網路上，車上攝影機拍攝的影像也曝險了將近7年。經其內部分析，事件主要原因在於對員工的資料處理政策說明不夠徹底，導致雲端環境錯誤設定所致。請問下列何項措施，最「不」能防止類似事件再次發生？

(A) 強化員工教育訓練

(B) 定訂更明確之雲端資安政策

(C) 執行雲端弱點掃描

(D) 備份雲端環境設定

規劃 114-1 答案D

(備份雲端環境設定主要是用於在發生配置錯誤後進行恢復，而非防止錯誤發生。事件的根本原因在於員工對資料處理政策的說明不足，導致雲端環境設定錯誤。因此，透過加強員工教育、制定更明確的雲端資安政策以及執行弱點掃描，才是預防類似事件的有效措施。)

44. 企業若使用雲端服務作為企業資料的儲存，請問下列何項部屬模式更能確保機密性？

(A) 公有（Public）雲

(B) 自由（Free）雲

(C) 私有（Private）雲

(D) 混和（Hybrid）雲

技術 113-2 答案C

(私有雲技術可以將公司所有資料保留在公司內部，達到機密性)

45. 在雲端運算環境中，下列哪一項較「不」是常見的安全威脅？

(A) Distributed Denial of Service（DDoS）攻擊

(B) API（應用程式介面）的脆弱性

(C) 雲端實體主機的竊取

(D) 網路釣魚攻擊

技術 113-2 答案C

(雲端實體主機的竊取非屬常見的雲端威脅)

44. 依照雲端運算聯盟（Cloud Security Alliance CSA）於 2019年 8月發表雲端運算面臨十一大安全威脅報告中，請問沒有使用強密碼是下列何種安全威脅？

(A) 資料外洩（Data Breaches）

(B) 配置錯誤和變更控制不足（Misconfiguration and inadequate ）change control

(C) 缺乏雲端安全架構和策略（Lack of cloud security architecture and strategy）

(D) 驗證密碼控制機制不足（Insufficient identity, credential, access and key management）

技術 113-1 答案D

(此威脅明確指出身分驗證、憑證、存取權和金鑰管理的不足。沒有使用強密碼直接屬於此類別，因為它表示在身分驗證機制上存在弱點。弱密碼、缺乏多因素驗證、金鑰管理不善等都屬於此威脅)

44. 依照雲端運算聯盟（Cloud Security Alliance, CSA）於 2019年 8月發表雲端運算面臨十一大安全威脅報告中，請問賦予超過實際所需的權限是下列何種安全威脅？

(A) 資料外洩

(B) 設定錯誤

(C) 策略缺乏

(D) 認證不足

技術 112-2 答案B

45. 使用雲端資料庫與應用程式十分方便，但若設定稍有不慎將導致資料外洩或是服務遭到攻擊，下列何項是因設定不慎而導致問題，同時也列為 OWASP TOP 10 2021之一的漏洞？

(A) Cryptographic Failures

(B) Security Misconfiguration

(C) Vulnerable and Outdated Components

(D) Software and Data Integrity Failures

技術 112-2 答案B

44. 有一項雲端服務是由許多個組織來一起共享，以支援特定的服務，像是目前由相關單位所推動的醫療雲、教育雲等，以共同的訴求和具有相同使命的目的為號召，提供給特定對象使用。以上描述屬於哪一種雲端服務的部署模式？

(A) 公有雲（Public）

(B) 私有雲（Private）

(C) 混合雲（Hybrid）

(D) 社群雲（Community）

技術 112-1 答案D

45. 下列何者「不」是雲端服務（Cloud Service）的關鍵特徵？

(A) 隨需自助服務（On-demand Self-service）

(B) 多人共享資源池（Resource Pooling）

(C) 情境最佳化（Scenario Optimization）

(D) 快速重新部署靈活度（Rapid Elasticity）

技術 112-1 答案C

(一般認為的五大特性為：隨需應變自助服務、隨時隨地用任何網路裝置存取、多人共享資源池、快速重新部署靈活度、可被監控與量測的服務。)

45. 關於雲服務安全，下列敘述何者最為正確？

(A) 資料先加密再儲存於雲服務中，可降低外洩之危害

(資料加密後儲存，即使發生外洩，攻擊者仍需破解加密才能讀取內容，因此能有效降低危害。此為雲端資料保護的基礎實踐)

(B) 雲服務安全為供應商（CSP）之責任，非與使用者相關

(雲服務安全遵循「共同責任模型」，供應商（CSP）負責基礎設施安全，使用者需管理自身資料、存取控制等安全措施，責任並非僅在供應商)

(C) 服務皆具備高可用特性與災難復原功能，服務遷移其上即可有效避免中斷風險

(高可用性與災難復原功能需依賴使用者配置（如多區域部署、備份策略），並非所有服務「自動具備」，也無法完全避免中斷風險)

(D) 多因子驗證機制（Multi-factor Authentication）設置，可避免儲存於雲服務之資料受駭與外洩風險

(多因子驗證（MFA）可強化帳戶安全，但無法「避免」資料外洩風險（如配置錯誤、應用漏洞等仍可能導致外洩）)

技術 111-2 答案A

20. 下列何者「不」是常見的雲端運算的部署模式？

(A) 公有（Public）雲

(B) 私有（Private）雲

(C) 自由（Free）雲

(D) 混合（Hybrid）雲

技術 111-1 答案C

41. 「 消費者使用應用程式，但並不掌控作業系統、硬體或運作的網路基礎架構」，請問上述屬於下列何種服務之定義？

(A) PaaS（Platform as a Service）

(B) IaaS（Infrastructure as a Service）

(C) QaaS（Quality as a Service）

(D) SaaS（Software as a Service）

技術 111-1 答案D

零信任

<https://www.ithome.com.tw/tech/152241>，ithome NIST SP 800-207 簡介。

<https://dsp.twse.com.tw/brokerPromotionManual/list>，推動證券商導入金融零信任架構作業說明會。

<https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202407180002&dtable=News>，金融業導入零信任架構參考指引。

<https://moda.gov.tw/press/multimedia/blog/9773>，數位發展部零信任架構。

<https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/ZTA/>，資通安全院零信任架構(ZTA)。

<https://medium.com/chouhsiang/nist-sp-800-207-%E9%9B%B6%E4%BF%A1%E4%BB%BB%E6%9E%B6%E6%A7%8B-%E4%B8%AD%E6%96%87%E7%89%88-389c12e2e304>，NIST SP 800–207 零信任架構 中文版。

原由：

* 2004年Cisco國際論壇「Jericho」開始探討網路去邊界化議題；而在2010年，國際研究機構 Forrester 的首席分析師 John Kindervag 正式提出了「零信任」名詞及具體概念；2020年美國國家標準技術研究院(NIST)正式頒布標準文件《SP 800-207》，確立了零信任架構的基礎。
* 此外，美國網路安全暨基礎設施安全局（CISA）於2023年4月發布《Zero Trust Maturity Model Version 2.0》，依據白宮指令《OMB M-22-09》（2022年1月）調整，提出五大支柱與三個跨領域能力的成熟度模型，作為推動零信任架構的實作指南。

運作原則：

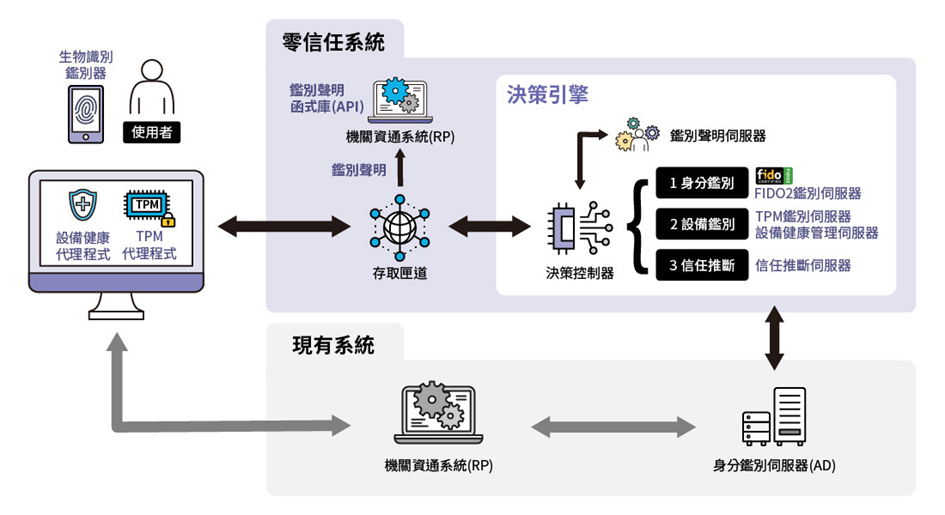
* 「永不信任，必須驗證」(Never trust, always verify)。

背景：

1. 以往企業會將防護重點建立在防火牆，外網信任度較低，內網信任度較高。
2. 攻擊者一旦突破分界線，便可能對內部相對薄弱的防護造成重大損害。
3. 隨著 BYOD、雲端服務、遠距/行動辦公等趨勢興起，傳統內外網分界日益模糊。

台灣推動情形

* 「國家資通安全發展方案(110年至113年)」內容包括評估及導入零信任，並逐步試行以驗證其可行性，推動規劃單位為數位發展部資通安全署；因應此趨勢，金融監督管理委員會在2022年12月27日發布的「金融資安行動方案」2.0中，也將「鼓勵零信任網路部署，強化連線驗證與授權管控」納入推動重點工作之一。

運作原理：

* 圖為我國政府機關推動零信任的架構。員工透過電腦想要存取機關資通系統(Relying Party, RP)時，所有的連線都會先經過存取閘道，接下來，員工需使用實體金鑰以鑑別其身分，電腦則需安裝代理程式，並使用公私鑰(可以是硬體或軟體)以鑑別其設備；等前面動作完成後，再由決策引擎根據使用者的身分鑑別及設備鑑別方式、來源IP、登入時間、設備健康(如安裝更新檔、導入安全性設定)等資料，決定是否允許存取。

存取閘道(Access Gateway)

* 不論來自內部或外部網路，均經由存取閘道進行存取。
* 透過反向代理(Reverse Proxy)技術，隱藏內部伺服器與機關資通系統之網路路徑。
* 實施負載平衡與防止阻斷服務攻擊之機制。

決策引擎(Decision Engine)為存取決策，包含決策控制器及身分鑑別、設備鑑別及信任推斷三大核心機制和鑑別聲明(Authentication Assertion)伺服器。

1. 決策控制器：負責控制存取決策之流程，包含設定存取允許條件、接收存取請求、驅動三大核心機制及授予鑑別聲明。
2. 三大核心機制：由身分鑑別、設備鑑別及信任推斷進行驗證與評估，並將結果回饋給決策控制器。
3. 鑑別聲明伺服器：針對獲得允許之存取，發行鑑別聲明，做為存取 RP 之憑據。

決策引擎組件之三大核心機制說明

1. 身分鑑別(Authentication)：以實體安全金鑰或手機 APP 進行無密碼雙因子身分鑑別，並可與現有AD共存與同步。

* 我國推動的零信任將身分鑑別區分為三個階段，各階段分別有不同的安全防護要求。
  1. 註冊(Enrollment)階段：使用者註冊時，需親自提供身分證明的證據，例如，申請自然人憑證需親自到戶政事務所提供身分證明文件。
  2. 鑑別(Authentication)階段：使用者登入系統時，不允許使用傳統的帳號密碼，而必須使用具備雙因子的硬體加密鑑別器，以鑑別用戶身分，如目前常見的FIDO2安全性金鑰。
  3. 聲明(Assertion)階段：在使用者登入成功之後，身分鑑別伺服器要將使用者的身分訊息傳送到使用者欲存取的RP，好讓RP知道誰要存取。在這個傳送過程中必須使用簽章與加密，以確保傳遞資訊的機密性、完整性及不可否認性。

1. 設備鑑別(Device Authentication)：可確認使用者設備為受機關管理之設備，且在可接受之資安狀態，可因應遠距與居家辦公之資安需求。

* 管理者可透過圖形化介面註冊、撤銷或鎖定使用者設備。此舉主要目的在於確保只有經過授權且處於安全狀態的設備才能存取系統資源。不同系統有不同的安全需求，例如公司內部重要系統通常只允許預先註冊的設備連線。使用者設備需安裝鑑別代理程式，並利用內建於硬體的信任平台模組(TPM)或軟體產生的金鑰等方式進行註冊與鑑別，以確保傳輸資訊的可信度。

1. 信任推斷(Trust Inference)：可隨時依使用者行為與設備狀態，偵測異常存取。

* 目的是決定最終是否允許使用者的連線或存取行為。例如，允許哪些特定的使用者群組及設備群組存取，並且設定「信任分數」的標準，分數達到幾分才能存取。以數位部官網為例：官網後臺系統只允許資訊單位同仁使用公發設備，且信任分數需達0.9(假設信任分數區間為0到1)以上才允許存取。
* 信任分數是參考各式各樣因素所計算得出的，如使用者所使用的身分鑑別方式、其設備鑑別方式、設備健康狀態(有無安裝防毒、更新作業系統等)、使用者來源IP位址、使用者登入的時間等。

| **比較項目** | **ZTA** | **傳統的資安控管** |
| --- | --- | --- |
| 信任 | 從不信任，始終驗證 | 信任內網，防禦外網 |
| 存取控制 | 動態且基於風險，根據即時情境評估授權 | 靜態且基於規則，預先定義的權限 |
| 防護範圍 | 全面的，涵蓋身分、設備、資料、服務和網路等 | 局部的，主要在邊界 |
| 防護方法 | 主動的，透過政策決策點和政策落實點來驗證和授權 | 被動的，依賴防火牆等設備過濾流量 |
| 防護效果 | 減少潛在的攻擊面，提高資安可見性和可追溯性，透過日誌記錄、監控和分析實現 | 難以防止內部橫向擴散，存在資安盲點，易受內部威脅影響 |
| 適用場景 | 適用於各種規模和類型組織，尤其適合複雜 IT 環境、大量遠端用戶或雲端應用 | 適用於簡單網路環境和有限資源的組織 |

11. 在零信任（Zero Trust）安全架構下，考慮到網路微分割（Network Micro-Segmentation）的實施，下列何項描述最準確地闡述了它與其他零信任安全控制措施（如身份和存取管理、加密和持續監控）的交互作用？

(A) 網路微分割獨立於其他零信任控制措施運作，不與身份和存取管理或加密策略互動

(B) 身份和存取管理策略在網路微分割實施之前是不必要的，因為微分割本身就足以防範網路入侵

(C) 網路微分割與身份和存取管理緊密結合，確保只有驗證和授權的用戶才能存取特定網路段，同時加密和持續監控提供額外的安全層

(D) 持續監控在網路微分割實施過程中不起作用，因為微分割旨在隔離和控制網路流量，而不是監控

114-1 防護 答案C

(在零信任架構下，網路微分割並非獨立運作，而是與身份和存取管理、加密及持續監控等控制措施緊密結合。這種結合確保只有通過身份驗證和授權的用戶能夠存取特定網路區段，而加密和持續監控則為網路提供了額外的安全保護層。因此，選項 (C) 最準確地描述了這些安全措施之間的互動關係。)

15. 在使用NIST SP 800-207 Zero Trust Architecture 架構中的進階身份治理（Enhanced Identity Governance）模式時，請問下列哪些要素會影響最終信任評等的結果計算？（複選）

(A) 資產狀態（Asset Status）

(B) 密碼長度（Password Length）

(C) 資源內容（Enterprise Resource）

(D) 環境因素（Environmental Factors）

114-1 防護 答案ACD

(在 NIST SP 800-207 中的進階身份治理模式，最終信任評等的計算會考慮與用戶、資產、資源及環境相關的各種因素：

資產狀態（Asset Status）：反映用戶所使用設備或資產的安全狀態，屬於評分的關鍵組成部分。

資源內容（Enterprise Resource）：不同的企業資源其敏感性和風險水平可能不同，因此會影響信任評等。

環境因素（Environmental Factors）：考慮包括地理位置、網路環境、使用時間等背景因素，這些也會影響最終的信任評等。

相對地，**密碼長度（Password Length）**屬於身份驗證機制中的一個具體參數，並不直接影響進階身份治理中最終信任評等的計算。)

17.關於NIST SP 800-207零信任架構（Zero Trust Architecture）中的網路敘述，下列何項錯誤？

(A) 企業內部網路不可視為隱式信任區（Implicit Trust Zone）

(B) 內部網路中的設備可能非企業所有或受企業管控

(C) 遠距企業人員可完全信任他們本地的網路連線

(D) 資產與流程於企業和非企業之基礎設施移動時，必須為一致的安全標準

114-1 規劃 答案C

(在零信任架構中，無論是內部或遠距連線，皆不應被視為自動可信。選項 (C) 主張遠距企業人員可完全信任他們本地的網路連線，這正是零信任理念所反對的做法，因為任何連線均應進行驗證和授權。)

20. 關於零信任架構（ZTA）的敘述，下列哪些正確？（複選）

(A) 對於資源的存取要求，以每次連線為基礎去許可

(B) 對於存取的要求，每次是以最小權限為原則去執行

(C) 允許存取之前，所有的資源的身分鑑別與授權機制，是依監控結果動態決定

(D) 是一種以邊界為基礎的資安架構，一旦連線通過了認證就值得信任 (零信任架構的核心理念是消除傳統網路邊界，不再假設內部網路是安全的。即使連線通過認證，仍需持續驗證與監控，而非直接信任。此選項描述的是傳統「邊界防禦」模型，與零信任完全矛盾。)

113-2 規劃 答案ABC

33. 政府零信任網路架構係參考NIST零信任架構，同時結合向上集中之防護需求，採取資源門戶部署（Resource Portal-Based Deployment）方式，下列何項「不」屬於該核心機制？

(A) 身分鑑別

(B) 系統識別 (這不屬於政府零信任網路架構的標準核心機制。根據NIST SP 800-207和採用資源門戶部署方式的政府零信任架構，核心機制包括身分鑑別、設備鑑別和信任推斷。「系統識別」雖然在零信任架構中很重要，但它通常被視為設備鑑別的一部分或子集，而非獨立的核心機制。)

(C) 設備鑑別

(D) 信任推斷

113-2 管理 答案B

10. 關於政府零信任（Zero Trust）網路之敘述，下列何項正確

(A) 政府推動零信任網路是由國家通訊傳播委員會推動主導 (不見得是單一機關，但通常包含數位發展部的資通安全署)

(B) 政府零信任網路包含身分鑑別、設備鑑別 及信任推斷等 3大

核心機制

(C) FIDO2無密碼雙因子驗證滿足零信任網路要求 (雖然FIDO2無密碼雙因子驗證是強化身分驗證的重要技術，但它只滿足零信任網路中「身分鑑別」這一部分的要求。零信任架構還需要設備鑑別和信任推斷等其他機制，單一的身分驗證解決方案不足以完全滿足零信任的全部要求。)

(D) 持續掌握設備健康管理即滿足設備鑑別要求 (設備健康管理是設備鑑別的一部分，但不是全部。完整的設備鑑別還包括設備身分識別、軟硬體合規性檢查、安全態勢評估、更新狀態等多方面因素。僅僅掌握設備健康管理不足以完全滿足零信任架構中的設備鑑別要求。)

113-1 規劃 答案B

33. 零信任架構（ZTA）的假設前提是：在確認可信之前，沒有任何連線、使用者或資產可以信任。主要目的是解決現今網路環境複雜造成信任邊界不明之資安窘境，期望透過對任何資料存取皆永不信任且必須驗證的原則，達成不論在何時何地存取資料皆保證一致安全性之相關技術。請問下列關於ZTA的描述何者較「不」正確？

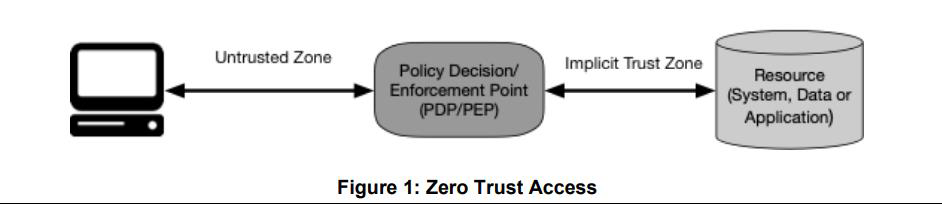
(A) 聚焦保護網路存取，非保護資料/應用存取 (零信任架構(ZTA)的核心理念恰恰相反 - 它聚焦於保護資料和應用程式存取，而非僅保護網路存取。ZTA摒棄了傳統依賴網路邊界的安全思維，轉而採用以身分和資源為中心的方法。在零信任模型中，資料和應用程式才是真正需要保護的資產，而網路只是連接媒介。)

(B) 參考美國國家標準技術研究院（NIST）零信任架構，採取資源門戶之部署方式（ Resource Portal-Based Deployment），包含 3大核心機制：身分鑑別、設備鑑別、信任推斷

(C) 根據美國國家標準技術研究院（NIST）頒布標準文件 NIST SP800-207將 ZTA分成核心組件與支援組件，「資料存取政策」歸類在支援組件中

(D) ZTA架構中的決策引擎組件是負責接收存取請求、決定允許與否與授予存取憑證

113-1 管理 答案A

17. 如附圖所示，關於 NIST SP 800-207零信任架構（ Zero Trust Architecture）的抽象模型敘述，下列何項錯誤？

(A) 政策決策點（ Policy Decision Point PDP））/政策落實點（ Policy Enforcement Point PEP）須適當判斷主體是否可存取資源

(B) 零信任（ Zero Trust）提供準則與概念，可使PDP/PEP移動並貼近資源

(C) PDP/PEP已提供一系列控制，因此通過 PEP的流量便能取得最高層級信任 (這個敘述違背了零信任的基本原則。零信任架構強調「永不信任，始終驗證」，即使流量通過了PEP，也不應被視為獲得了「最高層級信任」。在零信任模型中，信任是有限的、動態的，並持續需要重新評估。通過PEP的流量獲得的只是特定上下文和特定時間點的有限授權，而非永久或最高層級的信任。)

(D) 隱式信任區（Implicit Trust Zone）：區域中實體至少達到最後 PDP/PEP的信任等級

112-2 規劃 答案C

26. 關於零信任（ Zero Trust）的敘述，下列何者正確？

(A) 零信任是不用始終驗證 (零信任架構的核心原則正是「永不信任，始終驗證」(Never Trust, Always Verify)。這意味著無論使用者或設備位於何處，每次存取請求都必須經過完整的驗證和授權過程，即使是來自內部網路的請求。)

(B) 僅提供必要的權限

(C) 不需保持網路可見性 (零信任架構中，保持網路可見性是至關重要的。組織需要持續監控和記錄所有網路流量和活動，以便偵測異常行為和潛在威脅。沒有完整的可見性，就無法有效實施零信任策略。)

(D) 非所有流量都是不安全的前提下進行零信任設計 (零信任架構的基本前提是「所有流量都被視為不安全」，無論其來源。零信任模型不會根據流量的來源網路位置給予信任，而是將所有通訊視為可能存在風險，因此要求對所有流量進行驗證和檢查。)

112-2 管理 答案B

36. 利用零信任（Zero Trust）來保護資料完整性，下列敘述何者

錯誤？

(A) 在零信任設計上，存取決策不受加密控制 (在零信任架構中，加密是保護資料的關鍵控制措施之一，而且加密狀態通常是存取決策的重要考量因素。零信任模型要求所有通訊都應被加密保護，且系統會檢查資料的加密狀態作為授權存取的條件之一。存取決策實際上受到多種安全控制的影響，包括加密狀態、身分驗證、裝置狀態等。)

(B) 在零信任設計上，資料須能夠自動分類和標記

(C) 可以透過敏感度標籤和內容檢查的資料外洩防護（Data Loss Prevention, DLP）策略防止資料洩露

(D) 定期審核資料以瞭解用戶標籤、分類和保護活動

112-2 技術 答案A

11. 在存取控制上，零信任（ Zero Trust）是一個重要課題。關於

零信任的敘述，下列何者 較「不」適當？

(A) 零信任依循「永不信任，一律驗證」的原則

(B) 推動零信任，企業可能需要重新評估每項資產的保護方式

(C) 零信任倚重於最大特權原則等治理政策 (零信任架構實際上是基於最小特權原則(Principle of Least Privilege)，而非最大特權原則。最小特權原則要求只授予使用者完成其工作所需的最少權限，這與零信任「永不信任，一律驗證」的理念一致。最大特權原則與零信任的安全理念完全相反。)

(D) 是 Forrester的John Kindervag首次創造的一個名詞

112-1 規劃 答案C

19. 關於 NIST SP 800-207零信任架構（Zero Trust Architecture, ZTA）的基本規則敘述，下列何項錯誤？

(A) 所有的通訊都需被保護，無論其所在之網路位置

(B) 須觀察與量測所擁有資產與相關資產，其完整性與安全態勢

(C) 運算服務（Computing Service）和資料來源（Data Sources）皆可視為資源

(D) 應先蒐集資產、網路架構等現狀，建立資產清冊 (這是零信任架構實施過程中的一個步驟，但不屬於NIST SP 800-207定義的零信任基本規則或原則。雖然建立資產清冊是實施零信任架構的重要前置作業，但它是實施方法而非架構的基本規則。零信任的基本規則更關注於「永不信任，始終驗證」的安全思維，以及對所有資源的持續驗證和監控。)

112-1 規劃 答案D

20. 關於 NIST SP 800-207零信任架構（Zero Trust Architecture, ZTA）的邏輯元件敘述，下列哪些正確？（複選）

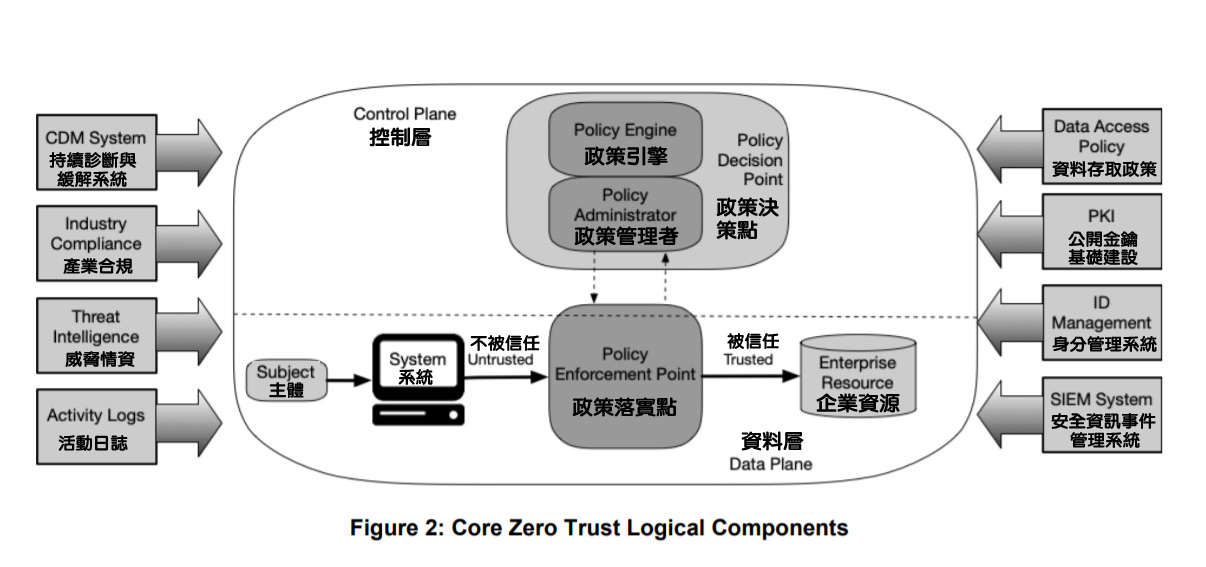
(A) 威脅情資（TI）來源：提供外部資訊給政策落實點（PEP），以進行存取決策 (根據NIST SP 800-207，威脅情資(Threat Intelligence)確實是零信任架構的一個元件，但它提供資訊給政策引擎(Policy Engine, PE)而非政策落實點(Policy Enforcement Point, PEP)。政策引擎負責決策，而政策落實點負責執行決策。)

(B) 持續診斷緩解（CDM）系統：收集資產目前狀態並套用更新至設定與軟體元件

(C) 公鑰基礎設施（PKI）：系統產生給資源、服務與應用程式之憑證，並進行紀錄

(D) 安全資訊事件管理（SIEM）系統 收集以安全為主的資訊，並用於日後分析

112-1 規劃 答案BCD



8. 關於零信任安全架構（Zero Trust Architecture），下列敘述何者「不」正確？

(A) 零信任基礎認知，也就是假設不信任任何人為前提的安全架構

(B) 從網路到裝置都是零信任控制點。換言之，不管是連接裝置、應

用程式或是組件，都視為威脅向量，必須經過認可及驗證

(C) 零信任包含：網路、設備、使用者、資料，不包含 Workloads (根據NIST SP 800-207等標準框架，零信任架構明確包含對 工作負載（Workloads） 的管控（如容器、虛擬機、微服務等），確保其通訊與操作的安全性。)

(D) 零信任安全架構四大支柱：身分可信、架構可信、存取可信、服

務可信 (此敘述可能因框架不同而有差異，但「身分可信」、「存取可信」是零信任的核心要素，而「架構可信」與「服務可信」亦可視為延伸原則（如確保系統架構與服務的安全設計）。儘管不同機構對支柱的分類可能不同，此選項並無明顯錯誤。)

110-1 防護 答案C

