



# 總複習資料

2025/2/19



## Pearson Vue Taipei (聯合世紀大樓 12F)



ISC2 4/3/2025 2

## Floor Map

**考場 (一人一格、有隔板)**

- 如有人打字聲音大聲，可要求提供耳塞
- 需要上廁所、進食可舉手，但時間照算

**監控區**

**進出搜身**

**公用外套**

**報到桌**

**等候區 (座椅)**

如外套材質會有摩擦聲，會要求放寄物櫃，使用公用外套(或不穿)

**廁所**

**食物桌**

**置物櫃**

**逃生梯**

**電梯**

**進場流程**

- 詳細閱讀入口大門的考場須知，關閉SSCP
- 報到桌身分驗證(護照/(信用卡+身分證)核對、掌紋掃描)，取得考桌編號
- 取得置物櫃鑰匙並寄物，按照置物櫃編號在食物桌上放所需的食物和水
- 上廁所
- 回報報到桌確認準備完成
- 進入監控區搜身、掃掌紋
- 進入考場
- 試題做完，電腦畫面會突然黑掉，提示考試結束
- 監控區人員帶出場、掃掌紋
- 報到桌領成績單
- 考試結束(或下一場連續考試開始)

ISC2 4/3/2025

## 考前準備以題庫、考試大綱為基礎

**SSCP**

- <https://www.isc2.org/certifications/sscp/sscp-certification-exam-outline>
- [SSCP Systems Security Certified Practitioner Official Practice Tests 2nd Edition](#)

Domain 1: Security Concepts and Practices

- 1.1 Comply with codes of ethics
- 1.2 Understand security concepts
- 1.3 Identify and implement security controls

(ISC)² SSCP Systems Security Certified Practitioner OFFICIAL PRACTICE TESTS Second Edition

\* 考試大綱請務必看一遍，至少裡面每一個單字都要看得懂

ISC2

## SSCP Exam Introduction

**SSCP Examination Information**

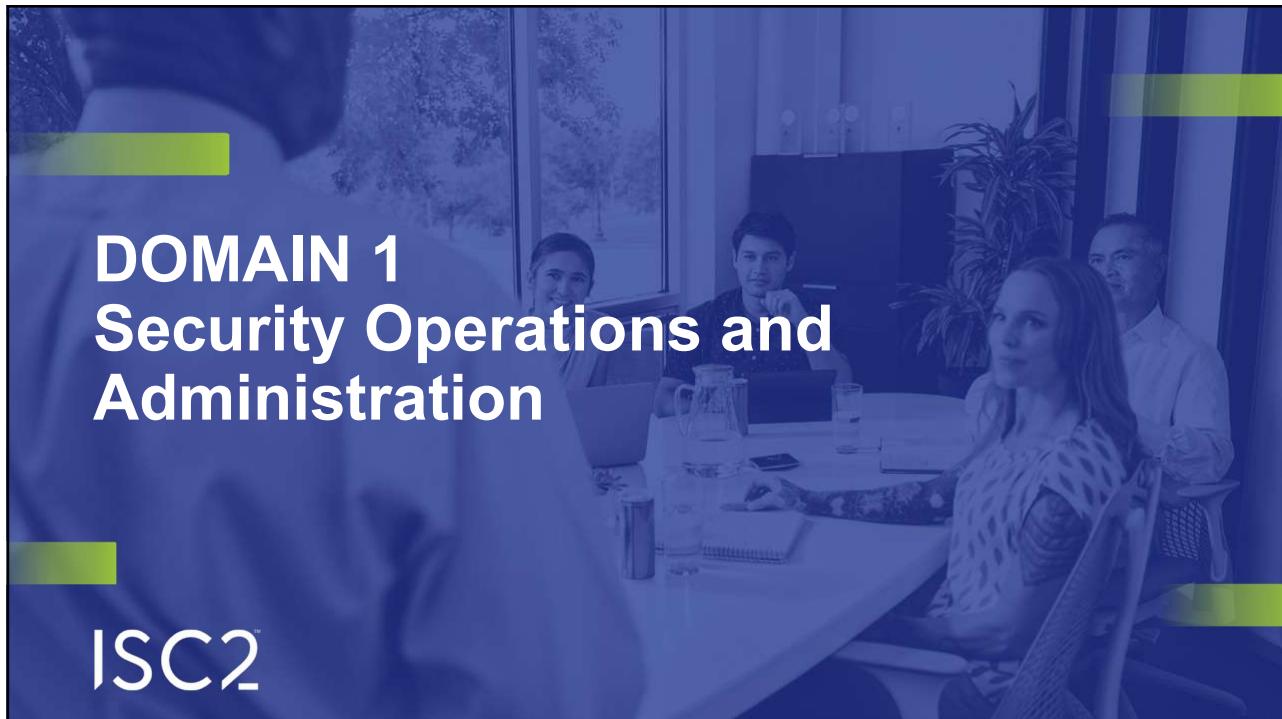
Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English, Japanese, Spanish
Testing center	Pearson VUE Testing Center



**SSCP Examination Weights**

Domains	Weight
1. Security Concepts and Practices	16%
2. Access Controls	15%
3. Risk Identification, Monitoring and Analysis	15%
4. Incident Response and Recovery	14%
5. Cryptography	9%
6. Network and Communications Security	16%
7. Systems and Application Security	15%
<b>Total:</b>	<b>100%</b>

ISC2



**DOMAIN 1**  
**Security Operations and Administration**

**ISC2™**

# 考試大綱 – Domain 1



## 1.1 Comply with codes of ethics

- » ISC2 Code of Ethics
- » Organizational code of ethics

## 1.2 Understand security concepts

- |                   |                               |
|-------------------|-------------------------------|
| » Confidentiality | » Non-repudiation             |
| » Integrity       | » Least privilege             |
| » Availability    | » Segregation of duties (SoD) |
| » Accountability  |                               |

## 1.3 Identify and implement security controls

- » Technical controls (e.g., firewalls, intrusion detection systems (IDS), access control list (ACL))
- » Physical controls (e.g., mantraps, cameras, locks)
- » Administrative controls (e.g., security policies, standards, procedures, baselines)
- » Assessing compliance requirements
- » Periodic audit and review

## 1.4 Document and maintain functional security controls

- » Deterrent controls
- » Preventative controls
- » Detective controls
- » Corrective controls
- » Compensating controls

## 1.5 Support and implement asset management lifecycle (i.e., hardware, software, and data)

- » Process, planning, design and initiation
- » Development /Acquisition (e.g., DevSecOps, testing)
- » Inventory and licensing (e.g., open source, closed-source)
- » Implementation/Assessment
- » Operation/Maintenance/End of Life (EOL)
- » Archival and retention requirements
- » Disposal and destruction

## 1.6 Support and/or implement change management lifecycle

- » Change management (e.g., roles, responsibilities, processes, communications, audit)
- » Security impact analysis
- » Configuration management (CM)

## 1.7 Support and/or implement security awareness and training (e.g., social engineering/phishing/tabletop exercises/awareness communications)

## 1.8 Collaborate with physical security operations (e.g., data center/facility assessment, badging and visitor management, personal device restrictions)

ISC2

# ISC2 Code of Ethics (必考)



1. 保護社會、共同利益、必要的公眾信任與信心，以及基礎設施。Protect society, the common good, necessary public trust and confidence, and the infrastructure.
2. 以光榮、誠實、公正、負責任和合法的方式行事。 Act honorably, honestly, justly, responsibly and legally.
3. 向委託人提供勤勉和稱職的服務。 Provide diligent and competent service to principals.
4. 促進並保護專業。 Advance and protect the profession.

ISC2

## Knowledge Check

- Which one of the following is not a canon of the ISC2 code of ethics?
- A. Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- B. Promptly report security vulnerabilities to relevant authorities.
- C. Act honorably, honestly, justly, responsibly, and legally.
- D. Provide diligent and competent service to principals.

ISC2 參考答案在下一頁的左上角...

B

## C I A + N A - P S

CIA 三要素



擴展安全屬性 ( CIANA+PS )

- 保密性 ( Confidentiality ) : 確保資訊僅對被授權者可及。
- 完整性 ( Integrity ) : 維護資訊的準確性和完整性。
- 可用性 ( Availability ) : 確保資訊在需要時可獲得。
- 不可否認性 ( Non-Repudiation ) : 保證某人無法否認其行為的有效性。
- 真實性 ( Authenticity ) : 驗證使用者和系統的身份。
- 隱私 ( Privacy ) : 保護個人資訊免受未授權存取。
- 安全性 ( Safety ) : 確保對個人和系統的防護，免受傷害。

ISC2

## Knowledge Check



- Bob is designing a messaging system for a bank and would like to include a feature that allows the recipient of a message to prove to a third party that the message did indeed come from the purported originator. What goal is Bob trying to achieve?
  - A. Authentication
  - B. Authorization
  - C. Integrity
  - D. Nonrepudiation

ISC2 參考答案在下一頁的左上角...

D

## 合規性專注重點



法規 / 指導原則	說明	主要適用於	主要特點
<b>OECD</b> 核心隱私指導原則	OECD於1980年提出的一套隱私保護原則，旨在促進國際間的資訊流通及個人資料保護。	各類型組織	包含七個基本原則：收集限制原則、數據質量原則、目的限制原則、使用限制原則、安全保障原則、透明度原則和個人參與原則。
<b>GDPR</b> (General Data Protection Regulation)	歐盟的通用數據保護條例，旨在保護歐盟公民的個人資料和隱私，並規範數據處理流程。	歐盟內組織及針對歐盟公民的全球組織	賦予個人更大的控制權，包括資料訪問權、刪除權，違反會有高額罰款，以及要求透明的數據處理。
<b>HIPAA</b> (Health Insurance Portability and Accountability Act)	美國的健康保險流通與問責法案，旨在保護個人健康資訊的隱私和安全。	醫療保健提供者和相關機構	規範醫療資訊的存取和保護，包括“隱私規則”和“安全規則”。
<b>PCI DSS</b> (Payment Card Industry Data Security Standard)	針對支付卡行業的數據安全標準，旨在確保支付卡持有者的信息及交易的安全性。	所有接受支付卡的商家及支付處理機構	包含一系列的安全標準和要求，以保護持卡人信息和防止數據洩露。

ISC2

## 其他重要觀念



- 縱深防禦
- 最小權限
- 阻止共謀 (Collusion) 的手段：職責分離、雙重控制、職位輪調、匿名舉報機制

ISC2

## 安全控制種類



- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• Technical / Logical 技術 / 邏輯控制           <ul style="list-style-type: none"> <li>• Configuration management 組態管理</li> <li>• FW / SW / IDS / IPS</li> </ul> </li> <li>• Physical 實體控制           <ul style="list-style-type: none"> <li>• 讀卡機、專門控制出入的通關機</li> <li>• CCTV</li> </ul> </li> <li>• Administrative 管理控制           <ul style="list-style-type: none"> <li>• 政策、標準、指引、程序、基線</li> <li>• 平衡計分卡 (Balancing scorecard)</li> </ul> </li> </ul> | <ol style="list-style-type: none"> <li>1. Directive 指引：影響行為</li> <li>2. Deterrent 嚇阻：打消念頭</li> <li>3. Preventive 預防：提高越線門檻</li> <li>4. Detective 偵測：持續監控</li> <li>5. Reactive 反應：事件後立即的動作</li> <li>6. Corrective 矯正：改正問題</li> <li>7. Recovery 復原：復原損失</li> <li>8. Compensating 補償：現行的某個方法有缺陷，其他控制措施補上</li> </ol> |
|--|--|

ISC2

## 資產生命週期 (順序和內容重要)



### 以 IT 資產管理的角度來看

1. Planning 規劃
2. Assigning Security Needs 分配安全需求
3. Acquiring 獲取
4. Deployment 部署
5. Managing 管理
6. Retiring 退役

### 以資料管理的角度來看

1. Create 建立
2. Store 儲存
3. Use 使用
4. Share 分享
5. Archive 封存
6. Destroy 銷毀

ISC2

## 資料角色



### 商務資料

- Data Owner: 分類、授權和問責
- Data Custodian: 實施和日常工作 (IT)
- Data Steward: 資料品質 (PM)
- Data User: 使用 (User)

### 隱私資料

- Data Controller: 決定資料處理目的和方式
- Data Processor: 代表控制者處理資料
- Data Subject / Principal: 被蒐集個資的人
- DPO (Data Protection Officer): 負責監督 GDPR 合規性

ISC2

## 資料分級分類



### 分級 (分高低)

- 高度受限 (Highly Restricted)
- 中度受限 (Moderately Restricted)
- 低敏感性 (僅限內部使用) (Low Sensitivity - Internal Use Only)
- 無限制公開資料 (Unrestricted Public Data)

### 分類 (依商務需求、合規...)

- 人身安全關鍵 (Human Safety Critical)
- 重要設備與財產安全 (Equipment and Property Safety Critical)
- 重要個人識別訊息 (Personally Identifiable Information Critical)
- 個人資料 (Private Data)
- 專有資料 (Proprietary Data)
- 合規資料 (Compliance Data)
- 時間關鍵資料 (Time-Critical Data)

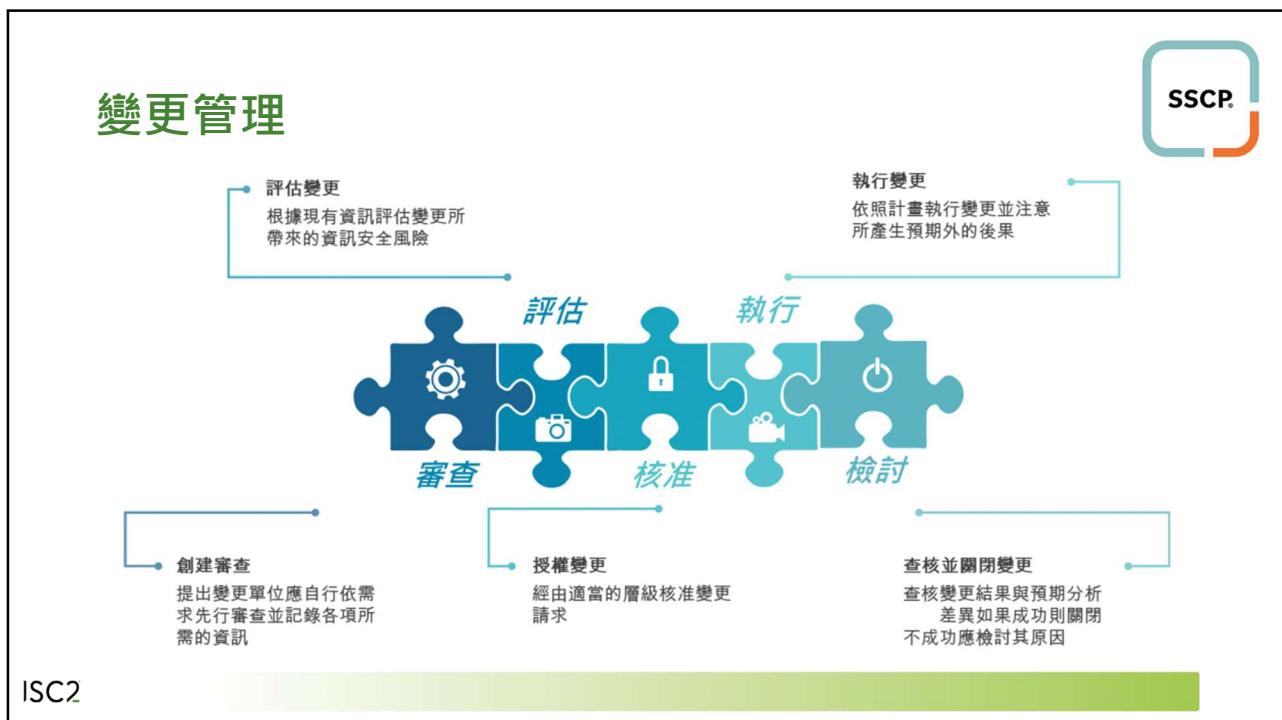
ISC2

## 資料銷毀技術



- 刪除 (Delete)**：從文件系統移除索引，但資料仍存在於儲存設備上，可能透過資料恢復工具找回。
- 重新格式化 (Reformat)**：在磁碟或儲存設備上執行格式化，但如果只是快速格式化，仍然可恢復資料。
- 擦除或覆蓋**：使用特定軟體來覆蓋舊資料，通常採用單次或多次寫入 0、1 或隨機數據的方式。
- 消磁**：透過強磁場（如工業級消磁機）破壞磁性儲存設備（如 HDD、磁帶），使其無法讀取資料。
- 加密刪除 (進階技術)**：先對數據進行完整加密，然後刪除加密金鑰，讓數據變得無法解密，等同於完全刪除。應使用全磁碟加密(FDE, Full Disk Encryption) 技術。
- SSD 的資料銷毀**：通過 Erase Unit 命令並非總是有效，需要物理銷毀。

ISC2



# 社交工程



## 常見手段

- 誘餌攻擊 (**Baiting**)：提供誘惑性的下載或 USB 隨身碟
- 電話釣魚 (**Phone Phishing, Vishing**)：假冒的互動語音回應系統
- 前置詐騙 (**Pretexting**)：冒充權威人物來獲取資訊
- 互惠交換 (**Quid Pro Quo**)：提供某些東西來換取登入憑證
- 尾隨 (**Tailgating**)：跟隨授權用戶進入受限區域
- 假旗操作 (**False-Flag Operations**)：假冒公司或身份來收集情報

## 防範方式

- Education, Training, Awareness
- 識別攻擊手段：了解常見的攻擊技巧
- 團隊合作：每個人都應該參與防禦攻擊的工作
- 保持警覺：一旦發現可疑活動，立即報告

ISC2

# 實體安全

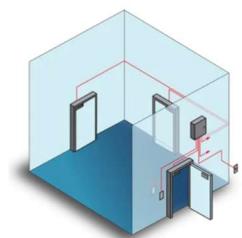


## 透過環境設計預防犯罪 (CPTED)

- 適當的照明
- 開放式設計
- 門禁與標示
- 景觀管理
- 關鍵區域隔離
- 門和窗戶
- 優先事項：在緊急情況下保護人命。

## 其他重要的管制設施

- 旋轉柵門 Turnstile
- 捕人陷阱 Mantrap



## 兩種不同尾隨的概念

- **Piggybacking (背小豬)**：當事人知情的情況下帶未經授權的人進入管制區
- **Tailgating (尾隨)**：當事人不知情的情況下，管制區被悄悄入侵

ISC2

## 資料中心分級



- Tier 1 基礎設施數據中心機房：可用性 99.671% (每年停機小於 28.8 小時)
- Tier 2 夾餘容量設施數據中心機房：可用性約 99.741% (每年停機小於 22 小時)
- Tier 3 運行可同時維護數據中心機房：可用性約 99.982% (每年停機小於 1.6 小時)
- Tier 4 容錯型數據中心機房：可用性約 99.995% (每年停機小於 26.3 分鐘)

ISC2

## 火災抑制與處理 - 1



### 概念

- 火災成因三要素：氧、燃料、溫度
- 火災抑制策略使用了縱深防禦概念

### 火災前

預防措施 (防火意識教育訓練、遵守建築物法規、定期消防安檢)

### 火災中 (偵測機制)

- 光電偵煙器 (Photoelectric Smoke Detector)
- 離子偵煙器 (Ionization Smoke Detector)
- 雙感應偵煙器 (Dual-Sensor Smoke Detector)
- 熱偵煙器 (Heat Detector)
- 吸氣式偵煙器 (Aspirating Smoke Detector) :  
ex. 極早期煙霧偵測系統 (Very Early Smoke Detection Apparatus, VESDA)

ISC2

## 火災抑制與處理 - 2

### 火災中 (手動滅火 - 滅火器)

- Class A (A for “Ash” 灰) : 一般可燃物
- Class B (B for “Barrel” 油桶) : 可燃液體
- Class C (C for “Current” 電流) : 電器類
- Class D (D for “Dynamite” 黃色炸藥) : 可燃金屬物質
- Class K (K for “Kitchen” 廚房)

### 火災中 (自動滅火)

- Water-based Suppression 用水滅火
- Gas-based Suppression 用氣體滅火
- CO2
- FM200
- Aerosol-based system (ex. Aero-K) 注入具有固體顆粒的惰性氣體，對資產和人員安全

ISC2

## 電力

### 常見問題

- Fault : 電力系統故障，短暫停電。
- Blackout : 長時停電。
- Spike : 瞬時高壓。
- Surge : 長時高壓。
- Sag : 瞬時低壓(電壓驟降)。
- Brownout : 長時低壓(限電)。

### 設備與注意事項

- 發電機、不斷電系統 (UPS)
- 防盜、防破壞、防事故的保護
- 燃料供應合約
- 定期故障切換測試

ISC2



## DOMAIN 2 Access Control

ISC2

### Identification - 1

SSCP

#### 身分證明 Identity Proofing

##### 身份保證等級 Identity Assurance Levels (IALs)

- **IAL1**：基本身份確認，ex. Gmail 帳號註冊。
- **IAL2**：中等程度的身份驗證，ex. 數位網銀帳戶開戶（視訊驗證）
- **IAL3**：高度嚴格的身份驗證，ex. 一般銀行開戶（本人到場）

#### 身份配置 Provisioning

- **Lifecycle**：身份建立 → 帳號設定 → 設定驗證 → 監控與審計 → 更新與維護 → 停用或刪除
- 配置類型：
  - 手動配置：人工操作
  - 自助服務配置：使用者可以根據需要在自助服務平台上完成
  - **JIT 即時配置**：使用者嘗試存取系統時，系統會根據預設的規則和流程自動建立使用者身份並配置相應的權限
  - 自動配置：利用自動化工具和流程來完成身份配置，用於高頻次身份更新的系統中

## Identification - 2



### 身份撤銷 Deprovisioning

撤銷啟動 (可能是聘僱終止、角色變更) → 存取審查和評估 (盤點需撤銷的權限) → 撤銷存取權限 → 資料清理和刪除 (確保隱私合規) → 通知與溝通 (通知相關部門該使用者權限撤銷)  
 → 確認與驗證 (透過自動化或手動檢查確認)  
 → 監控與審計 (檢查是否有不正當的存取嘗試)  
 → 撤銷後跟進 (確保所有相關的資料和存取權限都已完全撤銷及流程改善)

### 監控、報告與維護

- 角色變更 Role Change
- 新安全標準 New Security Standard 的實施

ISC2

## Identification - 3



### 身份即服務

#### Identity as a Service (IDaaS)

1. **Identity governance and administration (IGA)** 身分治理和管理：建立、修改屬性(或權限、密碼修改)、刪除等帳號管理功能
2. **Access 存取服務**：提供SSO的服務，你可以用 SAML、OAuth 等標準跟其他服務界接
3. **Intelligence 情報 (Accounting)**：Logging 紀錄、Monitoring 監控、Reporting 報告所有帳號的活動事件

### IAM 系統

- 幫助組織確保只有經授權的使用者能夠存取特定的資源和系統，並且在整個生命週期內有效地管理使用者身份和權限
- 實體
  - 使用者 (Users)
  - 角色 (Roles)
  - 資源 (Resources)
  - 政策 (Policies)

ISC2

# Authentication



## 三種 Type

- **Something you know (Type I)** : 知識型驗證，如 Password (密碼)、Passphrase (密碼短語)、PIN、answers to challenge questions
- **Something you have (Type II)** : 持有型驗證，如 Soft/Hard Token (令牌)、Smart Card (智慧卡)
- **Something you are (Type III)** : 生物特徵驗證

## Type III 常見技術 (背單字)

- Physiological (生理): Fingerprint (指紋), Hand Geometry (掌紋), Vascular Pattern(指靜脈), Facial (臉), Iris (虹膜, 偵測瞳孔週邊的虹膜), Retina (視網膜, 辨識視網膜(眼球內層)微血管分布, 光線侵入性)
- Behavioral(行為): Voice (聲音), Signature (簽名), Key stroke (鍵擊), Gait (步態)

ISC2

# 單因子 vs. 多因子驗證 (SFA vs. MFA)



## SFA

- 如果某個系統提供了密碼和 PIN 碼驗證，這仍是同一因子的兩種方法；因此，這仍視為 SFA
- 風險
  1. 易受到肩窺攻擊 (Shoulder-Surfing)、嗅探攻擊 (Sniffing) 及社交工程攻擊 (Social Engineering) 的威脅
  2. 易受暴力破解 (Brute Force)、字典攻擊 (Dictionary Attack) 及彩虹表攻擊 (Rainbow Table Attack) 影響

## MFA

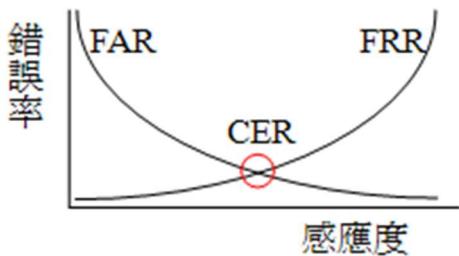
- 結合兩種或以上的身份驗證方式
- 特色
  1. 透過增加額外的驗證層級來提升安全性。
  2. 可能還會使用基於位置的因素 (Location-Based Factors)來加強身份驗證

ISC2

## 生物識別準確度指標

SSCP

- CER 代表了衡量生物識別系統有效性的最佳方法



ISC2

## Authorization - 1

SSCP

### 原則

- 最小權限原則 (Least Privilege)
- 僅知原則 (Need to Know)
- 職責分離 (Separation of Duties)

### 實作

- 雙重控制 (Dual Control)
- 分割知識 (Split knowledge)

### BLP vs. Biba (很重要)

- **BLP** : 著重機密性 · ex. 不窺探機密、不洩漏機密、只能讀寫同級，嚴格控制資訊流
- **Biba** : 著重完整性，用小數位精度的案例思考

ISC2

## Authorization - 2



- **自主存取控制 (Discretionary Access Control, DAC):** 資源擁有者可以決定誰可以存取資源。
- **強制存取控制 (Mandatory Access Control, MAC):** 基於安全標籤 (security labels) 和許可 (clearances) 來控制存取，通常用於高度安全環境。
- **基於角色的存取控制 (Role-Based Access Control, RBAC):** 基於使用者的角色分配存取權限，是最常見的模型。
- **基於屬性的存取控制 (Attribute-Based Access Control, ABAC):** 基於主體、客體、環境和操作的屬性來動態決定存取權限。
- **基於規則的存取控制 (Rule-Based Access Control):** 以if-then方式根據規則決定權限

ISC2

## Accountability



- 應防止日誌被刪除或篡改。
- 日誌通常儲存在安全與獨立系統內，甚至與管理員隔離，確保不被未授權存取或修改。
- 日誌是調查與法規遵循 (Compliance) 的重要依據
- SIEM (Security Information and Event Management, 安全資訊與事件管理)
  - 即時監控 (Real-time monitoring)
  - 事件關聯分析 (Event correlation)
  - 告警機制 (Alarm conditions) 以便緊急回應

ISC2

## 常見的 IAM 系統 - 1

SSCP

### Single Sign-On 單一登入

- 允許使用者只需進行一次身份驗證，就能夠存取多個系統，而無需再次進行身份驗證
- 風險**
  - 單點故障 (Single Point of Failure)**：依賴單一身份驗證伺服器，如果該伺服器發生故障，可能會導致大範圍的存取問題。
  - 安全漏洞 (Security Vulnerabilities)**：集中式存取點容易受到 DoS 或 DDoS 攻擊，這會影響多個系統。

### AD FS 同盟服務

- Active Directory 同盟服務 (ADFS) 是微軟提供的一個軟體組件，用於同盟身份管理，可促進跨組織邊界的安全部份與存取管理。
- 與 Active Directory (AD) 的整合 (Integration with Active Directory)
  - 無縫整合 (Seamless Integration)：利用現有的 AD 基礎架構，並使用使用者帳戶和群組。
  - 增強功能 (Enhanced Capabilities)：擴展 AD 的功能，包含聯邦身份管理 (FIM)。

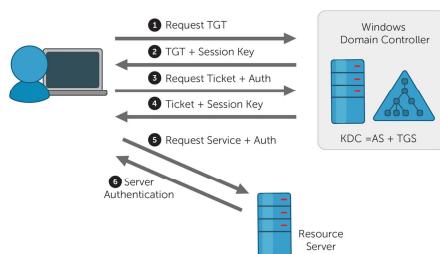
ISC2

## 常見的 IAM 系統 - 2

SSCP

### Kerberos

- 主要組件
  - Client (Principal)
  - KDC (Key Distribution Center) = AS (Authentication Service) + TGS (Ticket Granting Service)
  - Resource Server



### 考量

- 時鐘同步 (Clock Synchronization)
- 生命周期管理 (Lifetime Management)：限制 Ticket 的效期
- 實體安全 (Physical Security)：確保 KDC 安全並隔離 (密鑰明碼儲存、單點故障 SPoF)

### Kerberos 工具

Kerbtray.exe, Klist.exe, Ksetup.exe

ISC2

## 常見的 IAM 系統 - 3



特性	Security Assertion Markup Language (SAML)	OpenID Connect (OIDC)	Open Authorization (OAuth 2.0)
主要用途	企業單一登入 (SSO)	身分驗證 (Authentication)	授權 (Authorization)
基礎協議	XML	基於 OAuth 2.0	(本身就是一個協議)
資料格式	XML	JSON Web Tokens (JWT)	JSON
焦點	跨網域的單一登入，驗證後可存取多個服務	使用者身分驗證，確認「你是誰」	授權第三方應用程式存取資源，關注「你能做什麼」

ISC2

## 電腦安全系統的基礎 - TCB



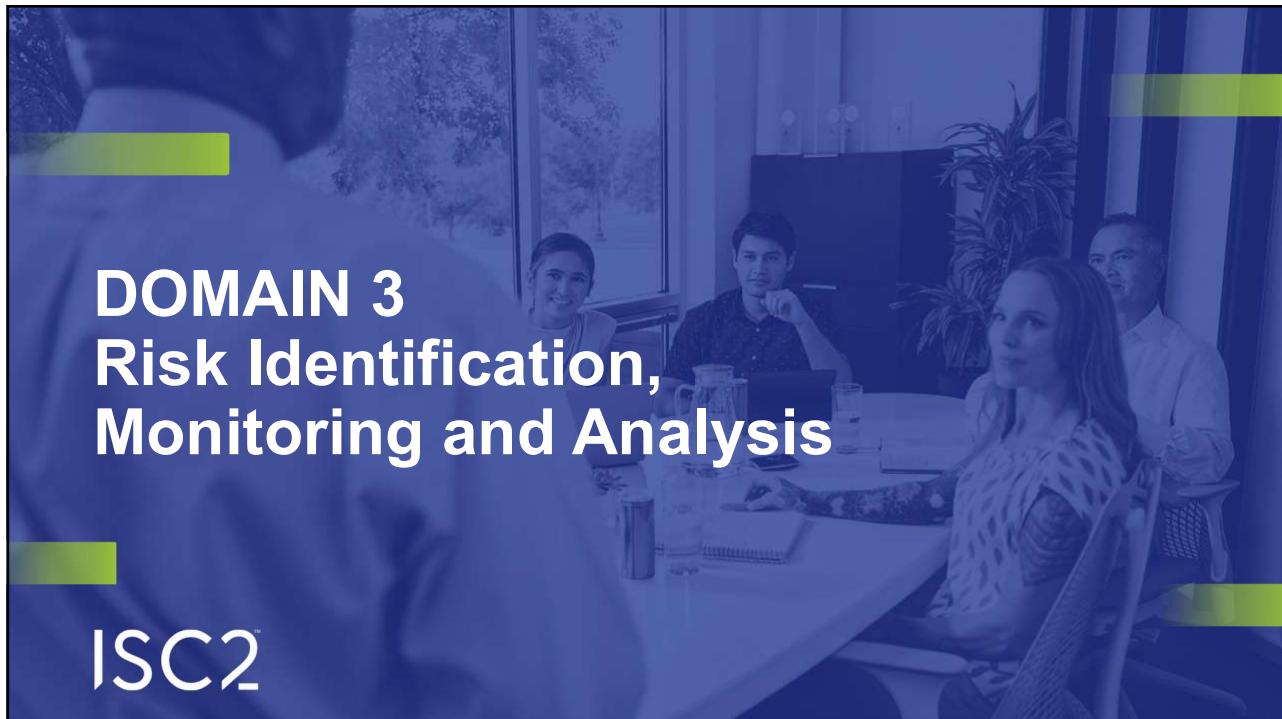
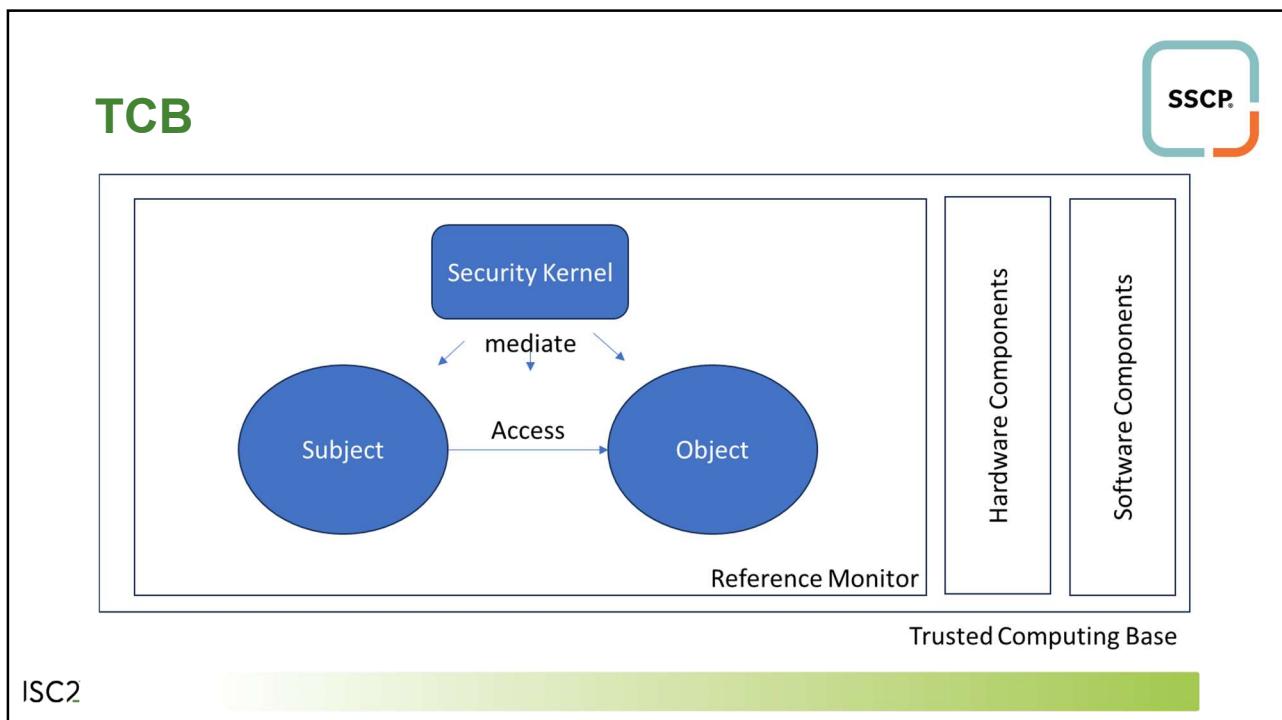
	與其他兩者的關係
TCB (可信計算基礎)	包含 Reference Monitor；Security Kernel 是 TCB 的一部分。
Reference Monitor (參考監控器)	被 TCB 包含；其概念由 Security Kernel 實作。
Security Kernel (安全核心)	屬於 TCB 的一部分；實作 Reference Monitor 的概念。

總結：

TCB、Reference Monitor 和 Security Kernel 是電腦系統安全的基石。  
TCB 是整體安全架構，Reference Monitor 是抽象的存取控制模型，Security Kernel 則是實際執行安全功能的程式碼。它們共同確保系統的安全性。

簡單來說：TCB 是「安全範圍」，Reference Monitor 是「安全規則」，Security Kernel 是「執行規則的程式」。三者合作，保護電腦安全。

ISC2



## 風險管理名詞解釋 - 1



SSCP

- **威脅 Threats**：對系統、資料或資源造成損害的潛在危險，ex. 資產遭竊、車禍、自然災害、內賊
- **弱點 (脆弱性) Vulnerabilities**：系統、應用程式或設備中的弱點，ex. 1F辦公室的落地窗、設計不良的自動駕駛、低窪的地形、無資料外洩防護解決方案的組織
- **影響 Impact**：攻擊成功後對系統或資料所造成的損害或損失，ex. 實體資產遭竊、車禍造成受傷或死亡、淹水造成資產減損、機密資料外洩
- **發生可能性 Likelihood of Occurrence**：發生的機率有多大，ex. 年化概率 = 一年發生 0.5 次
- **威脅建模 Threat Modeling**：分析系統中可能存在的威脅和弱點，並且評估攻擊者如何利用這些弱點。
- **威脅行為者 Threat Agents**：可能發動攻擊或造成威脅的人或團體。ex. 盜賊、駭客、內部員工

ISC2

## 風險管理名詞解釋 - 2



SSCP

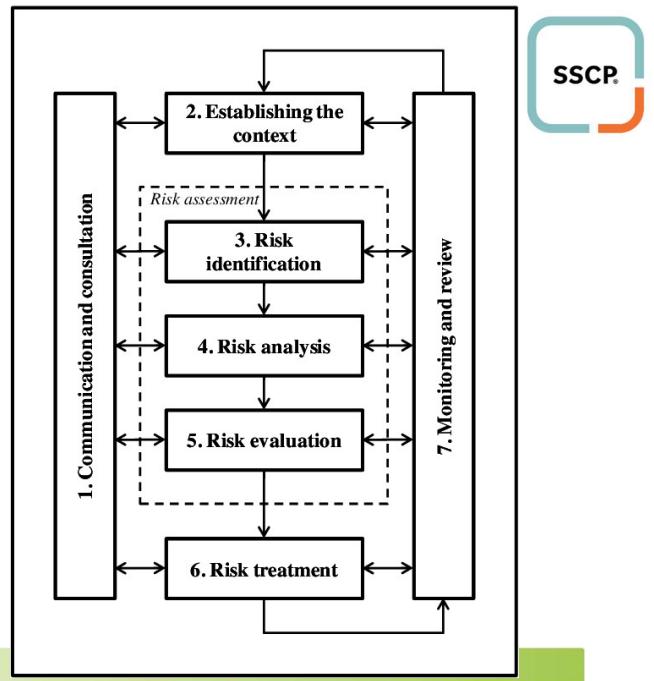
- **風險容忍度 (Risk Tolerance)**：能接受多少風險？通常比風險胃口更具體，會設定明確的數字或標準來衡量風險是否超出可接受範圍。ex. 組織最多能接受 10% 的年度收入損失。
- **風險胃口 (Risk Appetite)**：願意在特定領域承擔多少風險？想像成一個組織對風險的「口味」，決定願意冒多少風險來換取成長或收益。

ISC2

## 風險管理的實施流程

(請把右圖記下來)

SSCP



ISC2

## Establishing the context 建立全景

SSCP

### 分享威脅情報

#### Sharing Threat Intelligence

- 內部和與合作夥伴或可能遇到類似情況的其他組織共享資訊，使組織能夠更快地修復和減輕問題
- 關鍵內容**
  - 入侵指標 (Indicators of Compromise, IOCs)**：可用於識別和分析攻擊或威脅的跡象
  - 攻擊指標 (Indicators of attack, IOAs)**
  - 分析員的筆記：有關問題的詳細分析，幫助其他組織理解威脅背景
  - 修復步驟：針對已知問題的解決方案，協助其他組織更快地採取相應措施

### 其他情報來源

- 通用弱點評分系統 CVSS**
- MITRE ATT&CK 框架**
  - 對手的戰術、技術和常識的資料庫
- Cyber kill chain 網路攻擊鏈 (順序重要)**
  - 偵察 (reconnaissance) → 武器化 (weaponization)  
→ 傳遞 (delivery) → 利用 (exploitation) → 安裝 (installation) → 指揮與控制 (command and control) → 在目標行動 (actions on objectives)

ISC2

## Risk Identification 風險識別



### 風險登錄表

- 貫穿整個風險評鑑流程，記錄有關風險的資訊，包括相關的弱點、影響評估和可能的控制策略

Function/Activity		The Consequences of an Event Happening		Date of Risk Review _____	Compiled By _____	Date _____		
Ref	The Risk: What Can Happen and How It Can Happen	Consequences	Likelihood	Adequacy of Existing Controls	Consequence Rating	Likelihood Rating	Level of Risk	Risk Priority

### 威脅建模

- STRIDE**：偽冒 (Spoofing)、篡改 (Tampering)、否認 (Repudiation)、資料外洩 (Information Disclosure)、拒絕服務 (Denial of service)、提權 (Elevation of Privilege)
- DREAD
- PASTA
- Attack Trees
- Tailoring 量身訂製

ISC2

## 找出風險 - 執行安全評估與弱點分析



### 安全測試 Security Testing

- 計畫安全評估 Planning for Security Assessments

### 弱點管理的工具

- 一般弱點軟體 General Vulnerability Software
- 應用程式專用弱點工具 Application-Specific Vulnerability Tools
- 弱點評估軟體 Vulnerability Assessment (VA) Software

### 主機掃描 Host Scanning

- Host-based IDS** 入侵偵測系統 (HIDS)：主要用來監控主機上的活動，檢測異常行為或已知的攻擊跡象
- Host-based IPS** 入侵防禦系統 (HIPS)：除了檢測異常外，HIPS 還能夠主動防止攻擊

### 滲透測試 Penetration Testing

- 模擬威脅行為者的行動，找出真的可以被利用的漏洞
- 參與規則 (Rules of Engagement, RoE)**：明確定義進行滲透測試的條件

ISC2

## 找出風險 – 威脅狩獵



特性	IDS/IPS	威脅狩獵 EDR/XDR
主動性	被動 (依賴規則和簽名)	主動 (主動尋找潛在威脅)
目標	檢測和防止已知的威脅	發現未知的威脅或異常活動
回應方式	基於警報，管理員介入	基於發現的威脅進行干預和應對
技術需求	基於簽名、行為分析	需要深入的分析能力和靈活性

**假設突破原則 (Assume breach principle)**：防禦者應該在攻擊者達成目的之前，主動搜尋環境中隱藏的威脅行為者

### 其他威脅搜尋技術

1. **Passive (被動性)** : Vulnerability scanning (漏洞掃描)、Penetration testing (滲透測試)
2. **Active (主動性)** : Honey pot (蜜罐)、Threat Hunting (威脅狩獵)
3. **Offensive(進攻性)** : Botnet takedown、Hack-back attack

ISC2

## Risk Analysis & Evaluation 風險分析與評估



### 定量分析

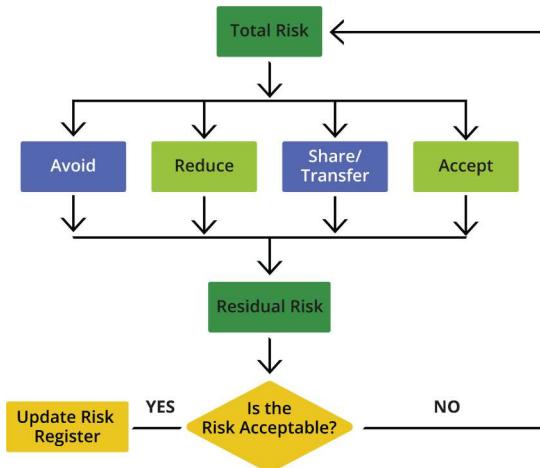
- 資產價值 **Asset value (AV)**
- 暴露因子 **Exposure factor (EF)**
- $AV \times EF =$  單次預期損失 Single Loss Expectancy (SLE)
- 年化發生率 **Annual Rate of Occurrence (ARO)**
- $SLE \times ARO =$  年化損失預期 Annualized Loss Expectancy (ALE)

### 定性分析

- 維度：可能性 (Likelihood)、衝擊 (Impact)
- 透過風險評估矩陣查表，得到曝顯程度 (Risk Exposure)

ISC2

## Risk Treatment 風險處置



- **迴避 Risk Avoidance**：通過修改決策或策略，完全避免風險
- **分享或轉移 Share or Transfer Risk**：風險轉嫁給外部實體或合作夥伴，以減少自身承擔風險的壓力
- **降低/減緩流程 Risk Reduction / Mitigation**：減少或消除風險的影響、減少風險發生的機會，把風險降低到可以接受的程度
- **接受 Risk Acceptance**

ISC2

## Risk Monitoring 風險監控



- 以終為始，風險管理的資料需求是什麼？
  - 風險評估：焦點在於了解持久且長期風險(以月為單位)、長期趨勢、歷史資安事故統計、與戰略目標一致。
  - 風險回應：焦點在於針對特定類型攻擊採取的控制措施是否有效(以分鐘到日為單位)、攻擊路徑、系統和技術的具體特徵資訊。
  - 風險監視：實時檢測並應對攻擊(以秒或毫秒為單位)、安全警報、事件監控系統。

### 事件關注點 Events of Interest (EOI)

- 安全事件：包括未經授權的存取、病毒攻擊、資料洩露等。
- 操作事件：可能影響業務流程的故障或異常，如伺服器當機、應用錯誤等。
- 合規事件：可能涉及違反法律法規或內部政策的事件。

### 監控機制

- 資料外洩防護 Data Loss Prevention (DLP)
- IP 流量：資料收集與分析 IP Flow: Data Collection and Analysis
- 主機入侵檢測系統 (HIDS)、網路入侵檢測系統 (NIDS)
- 安全信息與事件管理 (SIEM) 系統

ISC2

# Log Management 日誌管理



## 名詞解釋

- 裁剪閾值 **Clipping Levels**：設定事件紀錄的閾值，幫助減少日誌數據的數量
- 日誌過濾 **Log Filtering**：查看日誌時進行篩選的技術，用來縮小範圍、聚焦重要資訊，但不會影響實際儲存的日誌內容
- 日誌整合 **Log Consolidation** = Centralized Logging 集中式日誌管理
- 日誌保留 **Log Retention**：保存日誌的時間長短，以及何時刪除舊的日誌。
- 保護日誌 **Protection Logs**：對於法規遵循、事故調查追蹤非常重要，所以日誌規劃不僅只是規劃存放的空間，而要確保完整性與可用性
- 日誌審查 **Reviewing Logs**：定期檢視日誌是防範異常行為、偵測入侵的重要步驟
- 日誌異常 **Log Anomalies**：在日誌中發現的不尋常或異常的紀錄，這些紀錄可能是系統運行異常或安全問題的徵兆。

ISC2

# SIEM (Security Information and Event Management)



## 功能

- 聚合 **Aggregation**
- 正規化 **Normalization**
- 相關性 **Correlation**
- 安全儲存
- 自動化分析
- 報告產生

## 事件資料的聚合和相關性 **Aggregate and Correlate Event Data**

- **相關性的種類**：時間、空間 (地理、邏輯位置)、實體(軟體、硬體、資料、身份)
- **實例**
  - 時間相關性：在同一時間範圍內，來自多個伺服器的登入失敗次數急劇增加。→ 將時間戳進行關聯，以識別協調的暴力破解攻擊。
  - 空間相關性：不同的設備同時發出多次警報。→ 按地理位置將警報分組，以識別本地故障或惡意攻擊。
  - 實體相關性：特定使用者或設備相關的異常活動模式。→ 將所有使用者和設備分組，並考慮 VPN 的情況，判別內部帳號是否遭到攻擊。

ISC2

## SIEM vs. SOAR

SSCP

功能	SIEM (安全資訊與事件管理)	SOAR (安全協調、自動化與回應)
主要目標	收集、分析和關聯安全日誌，以識別和警報潛在的威脅	自動化安全操作任務，協調不同安全工具，加速事件應變流程
數據來源	多種來源，包括伺服器、網絡設備、安全設備和應用程式	SIEM、威脅情報平台、漏洞掃描器和其他安全工具
主要功能	日誌收集與管理、警報生成、事件關聯、合規性報告	警報分級與優先排序、自動化調查、事件應變協調、案例管理、威脅情報整合
自動化程度	有限的自動化，主要用於警報生成和規則觸發	高度自動化，可以自動執行許多安全操作任務
分析能力	基本的安全分析，例如規則匹配和異常檢測	更高級的分析能力，可以整合威脅情報和機器學習技術
應變能力	主要提供警報和資訊，供安全團隊進行手動應變	主動的應變能力，可以自動執行遏制和修復措施
優點	提供全面的安全可見性、簡化合規性報告、協助識別潛在威脅	提升應變速度和效率、減少人力成本、改進安全操作的準確性和一致性
缺點	可能產生大量的誤報警報、需要專業人員進行配置和管理、分析能力有限	需要整合不同的安全工具、初期部署和配置可能比較複雜

ISC2

## SOC Report (System and Organization Controls Reports) 系統與組織控制報告

SSCP

類型	描述	Type I	Type II
<b>SOC 1</b>	針對財務報告的內部控制，通常由會計師事務所進行審核。	評估控制設計是否適當，根據某一特定時間點的狀況	評估控制的運作效果，通常是過去一段時間的運作結果
<b>SOC 2</b>	針對組織的安全性、可用性處理完整性、保密性和隱私等方面控制。	評估控制設計是否適當，根據某一特定時間點的狀況	評估控制的運作效果，通常是過去一段時間的運作結果
<b>SOC 3</b>	與SOC 2相似，提供給公眾的概述性報告，不包含具體的敏感資訊。	N.A. (Single Type)	N.A. (Single Type)
<b>SOC for Cybersecurity</b>	針對企業在處理網路安全方面的控制措施進行審查。	N.A. (Single Type)	N.A. (Single Type)

ISC2

## Log、Event 與 Incident 的差異

SSCP

特性	Log (日誌)	Event (事件)	Incident (事件/事故)
定義	系統自動生成的記錄，包含事件的細節。	系統中可觀察到的變化或活動。	對業務造成負面影響或具有潛在負面影響的安全事件或一系列事件。
特性	客觀、詳細、大量、自動生成	可觀察、狀態變化、可能具有意義	負面影響/潛在負面影響、需調查處理、通常由多個 Event 組成
影響	無直接影響，提供資訊	可能觸發警報或自動化流程	對業務運作造成中斷或損失
處理方式	收集、儲存、分析	監控、觸發警報、可能需人工介入	啟動事件回應流程、調查、修復、改進
範例	使用者登入時間、IP 位址	三次登入失敗、CPU 使用率過高	勒索軟體攻擊、資料外洩、系統服務中斷
層級	基礎數據	中間層	最高層級

ISC2

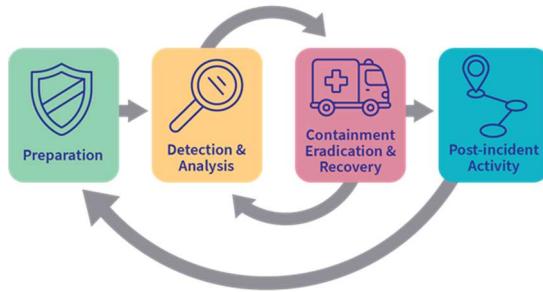
## DOMAIN 4 Incident Response and Recovery

ISC2™

## 事故回應 (IR) 生命週期



### Cyber Incident Response Cycle



- 準備：制定政策、計畫和程序。
- 偵測與分析：識別、調查並升級事件。
- 圍阻、根除與復原：控制並消除威脅，恢復系統。
- 事件後活動：審查並改進流程。
- 核心考量：確保及時處理事件。(效能 > 效用)

ISC2

## 準備 Preparation (政策、計畫、程序、人)



### IR 政策的關鍵組成

- 管理支持與認可：確保高階管理層支持。
- 與組織策略一致：將政策與使命、願景、目標對齊。(遵守法律法規)
- 目標與範圍：定義目的和界限。
- 角色與責任：分配明確的職責和問責制。(R&R、優先排序、溝通規劃)
- 指標與績效衡量

### 事故管理與 SOC 概念

- SOC 的角色與功能：管理和監督安全控制措施，在緊急情況下為高階管理層提供決策建議。(平時維運資安系統、戰時為戰情中心)
- SOC 會「升級緊急狀態」
- SOC 不會「做決策」，而是提供足夠的資訊供高階管理層做緊急決策

ISC2

# 偵測、分析、升級 Detection, Analysis, and Escalation



- **偵測**
  - 事件關聯 Event Correlation：把事件串成一個故事以描述事故的發展
  - 理解“正常行為” Understanding “Normal”
- **分析**
  - 系統分析 System Profiling: IRT 應該對每個系統進行分析，識別關鍵文件和敏感資訊，將已建立的分析檔案與預期行為進行比較
  - 完整性檢查軟體 Integrity Checking Software: 對於關鍵文件 (ex. 設定檔) 進行監視
- **升級**
  - 獲得適當的管理層對事件回應行動的認知和批准
- **通報**
  - 根據事件的嚴重程度決定
- **回應**
  - 圍阻：隔離損害 (ex. 阻止延燒)
  - 根除：消除原因 (ex. 滅火)
  - 恢復：恢復受影響的系統 (ex. 重建修復)

ISC2

# 圍阻(遏制) Containment



## 策略

- **鑑識證據保存**：對於法律行動和事後分析至關重要
- **服務可用性**：評估受圍阻組件提供的服務的重要性
- **潛在損害**：評估將受影響組件保留可能造成損害
- **有效時間區間**：考慮圍阻策略有效所需的時間
- **資源需求**：確定圍阻受影響組件所需的資源

## 常見的圍阻活動

- 斷開網路 Network Disconnection
- 密碼更改 Password Changes
- 流量分析 Traffic Analysis
- 防火牆修改 Firewall Modifications
- 日誌審查 Log Reviews
- 系統備份 System Backup
- **bit-by-bit copy**：將其所有的資料 (包括已刪除但未覆蓋的資料) 逐位元地完整複製，以利後續數位鑑識

ISC2

## 根除 Eradication



- 先識別根因 (Root cause) 然後予以移除
- **根除技術與活動**
  - 移除 Removal · ex. 檔案及備份資料清除 File / Backup Media Storage Cleaning
  - 歸零化 Zeroization : 確保被惡意實體佔據的空間進行歸零化 (寫 0)
  - 低階格式化 Low-Level Reformatting : 使硬碟恢復出廠的狀態，比一般的格式化更徹底，可有效清除硬碟上的所有資料
  - 記憶體清理 Memory Scrubbing : 將 CPU 的記憶體清除
- **根因分析的技術**
  - **Pareto analysis 帕累托分析 (80/20法則)**
  - Five whys
  - **Fishbone (Ishikawa) diagram 魚骨圖 (石川圖)**
  - Failure mode effect analysis 失效模式效應分析
  - **Fault trees 故障樹分析** : 使用**布林邏輯** (Boolean logic)的結果倒推分析方法。

ISC2

## 復原 Recovery



- 恢復流程 Recovery Process
- 系統檢查 System Checks : 驗證每一步恢復過程，確保其正確執行並完成。
- 工具與測試 Tools and Tests : 使用簡單的工具檢查狀態、狀況和健康資訊。
- 重新初始化順序 Order of Reinitialization : 複雜的系統可能需要特定的順序來重新初始化子系統和伺服器。ex. DB -> Web Server -> AP
- 事故文件 Incident Documentation
- 關鍵內容 5W
  - Who 誰 : 涉及和受影響的個體
  - What 什麼 : 事故的性質和已採取的行動
  - Why 為什麼 : 事故的原因
  - Where 哪裡 : 受影響的位置和系統
  - When 何時 : 事件的時間線
- 證據鍊 Chain of Custody
  - 為現場人員定義清晰的步驟，證據收集必須由專業人員處理
  - 記錄所有採證、經手流程並確保完整性

ISC2

## 事故後活動 Post-Incident Activities



- 經驗學習 Lessons Learned 會議
  - 目的：澄清事件發生順序，找出改進的地方
- 經驗學習的實施
  - 實現事故後的改進，必須有高階管理層的支持
  - 資安專業人員的角色應促進會議成員對技術安全問題和 End User 需求的理解（識別安全風險）
- 立即的應對措施
  - 即時偵測與回應改進 Immediate Detection and Response Improvement：防止重複攻擊
  - 弱點認知 Perception of Vulnerability
- 長期應對措施
  - 解決更深層的系統性問題，以實現更持久的安全改進。需要詳細分析、資源分配和策略性規劃。

ISC2

## 鑑識調查



- 數位鑑識 (Digital Forensics)
  - 證據收集 (Evidence Collection): 遵循標準程序，收集和保存數位證據。確保存據的有效性。
  - 證據分析 (Evidence Analysis): 使用鑑識工具和技術，分析數位證據，找出事件的根本原因和影響。
  - 證據呈現 (Evidence Presentation): 以清晰、簡潔的方式呈現鑑識結果，支持決策和法律程序。
  - 需要特別留意的是：\* 證據保全鏈 (Chain of Custody) \* 硬碟映像 (Disk Imaging) \* 記憶體分析 (Memory Analysis) \* 網路流量分析 (Network Traffic Analysis)
- 證據的五大原則 (Five Rules of Evidence)
  - 可接受性 (Admissible): 據必須符合法律規範，才能在法庭或調查中被接受（違法蒐集的證據不可作為證據）
  - 可靠性 (Authentic): 證據必須是真實的、未被篡改，才能確保可信度。
  - 完整性 (Complete / Integrity): 證據必須保持完整，不能缺少關鍵資訊。
  - 可信度 (Reliable): 證據的來源必須可靠，蒐集過程也要遵循標準程序。
  - 可證明性 (Believable / Repeatable): 證據必須可以被驗證或重現，讓其他專家也能得到相同的結果。

ISC2

## 鑑識調查類型



- **行政調查 (內部)**

- 在組織內部進行
- 遵循內部政策和程序
- 處理內部活動或政策違規問題

- **民事調查**

- 涉及沒有刑事起訴的訴訟
- 需要詳細的文件佐證和證據
- 主要關注賠償而非刑事處罰

- **刑事調查**

- 通知執法機關進行調查
- 受法律和程序的限制
- 遵循刑法

- **監管調查**

- 由監管機構進行
- 可能涉及監管機構和執法機關
- 聚焦於合規性和監管違規問題

ISC2

## BCP (管理面)



### 概念

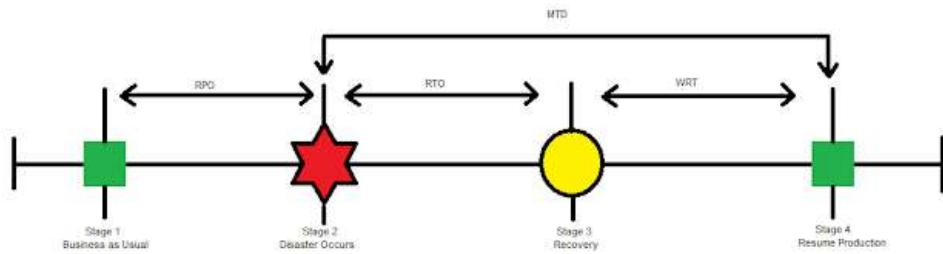
- 識別關鍵功能 (Critical Functions)：識別並優先考慮重要的業務功能
- 復原時間目標 (Recovery Time Objectives, RTOs)：確定關鍵功能可接受的停機時間
- 資源分配 (Resource Allocation)：確保為持續性工作提供必要的資源

### 參數

指標	主要用途	代表意義	案例
<b>MTTR</b> (平均修復時間)	影響修復速度	平均多久能修好？	技術人員修復故障問題平均要花多久時間？
<b>RTO</b> (復原時間目標)	業務恢復時間	當機後多久內要恢復？	購物網站故障，電商要花多久時間修好？
<b>RPO</b> (復原點目標)	影響資料遺失	最多能接受多少資料遺失？	資料庫上次備份是多前？
<b>MTD (最大容忍停機時間)</b>	影響業務存亡	系統最多能停多久？	超過這時間未恢復，企業可能倒閉

ISC2

## BCP - timeline



ISC2

## DRP (技術面) – 站點選擇



### 重要性

- 人員能迅速找到所需的資訊，專注於恢復活動
- 避免在需要立即行動時浪費寶貴時間搜尋文件
- 確保備用人員或第三方能遵循與主要人員相同的程序（考慮到主要人員傷亡的可能性）

### 文件類型

- 程序書
- 網路拓樸圖
- 第三方合約：與外部服務供應商的協議
- 供應商聯絡名單：列出供應商的聯絡訊息

ISC2

## DRP (技術面) – 站點選擇

SSCP

備份站點類型	描述	恢復時間	適用情境	其他考量
冷備站 (Cold Site)	具備網路、電力與空調，但無任何計算設備	需數週才能恢復運作	分階段恢復：先使用熱備站，再轉移到冷備站	
溫備站 (Warm Site)	部分設備齊全的資料中心，可在數日內啟用	需數日	作為中期恢復方案	具備部分資料、設備與網路能力，可透過供應商補充設備
商業熱備站 (Commercial Hot Site)	完整配備的資料中心，可快速使用	4 到 6 小時內可恢復運作	需要快速恢復的重要業務	成本較高，但低於多個運行中的資料中心；區域性災害時可能會供不應求
鏡像站點 (Mirrored Sites)	與主要站點同步更新的備援站點	幾分鐘內即可恢復運作	企業對停機時間容忍度極低	確保資料持續同步以避免資料遺失
多處處理中心 (Multiple Processing Centers)	平行運行的資料中心，確保業務不中斷	無需恢復，持續運作	企業需確保業務不間斷	成本極高，因需重複投資資源
行動備援站 (Mobile Sites)	伺服器機房整合至可移動的卡車，隨需部署	視部署時間而定	伺服器機房因火災或水災受損時使用	配備伺服器、網路能力、工作空間及電力
預先遷移至雲端 (Prior Migration to the Cloud)	業務功能遷移至雲端環境	取決於雲端可用性	降低實體災害影響	需確保資料與功能的冗餘及地理分散性

ISC2

## 備份類型

SSCP

備份類型	定義	優點	缺點	適用情境
完整備份 (Full Backup)	每次備份所有資料，無論資料是否改變	恢復速度快，因為所有資料都在同一份備份中	備份時間長，需要大量儲存空間	適用於每週或每月做一次全面備份，確保資料完整
增量備份 (Incremental Backup)	只備份自上次備份後有改變的資料	備份速度快，節省儲存空間	恢復時需要從完整備份開始，然後依序恢復增量備份，較慢	每日備份時，僅備份上次備份後改變的資料
差異備份 (Differential Backup)	只備份自上次完整備份後有改變的資料	恢復速度比增量備份快，較簡單	隨著時間推移，備份檔案會逐漸增大	每週做一次完整備份，每日做差異備份，平衡儲存與恢復速度
持續資料保護 (CDP, Continuous Data Protection)	即時備份每個變更的資料，隨時可回溯	可隨時恢復到任何時間點，資料遺失最少	需要大量儲存空間及較高的系統資源	高需求的關鍵資料保護，如金融機構和交易系統
雲端解決方案 (Cloud Solutions)	將資料備份到雲端伺服器，遠端儲存	可隨時隨地存取資料，減少硬體依賴	需穩定的網路連線，資料安全需加強保障	雲端儲存、資料共享，尤其適用於跨地區、跨設備存取的場景

ISC2

## 冗餘計畫

概念	定義與解釋	優點	注意事項
<b>Off-Site Storage</b>	將備份資料儲存於主要地點以外的地方，防止災難導致資料損壞。	<b>災難恢復力</b> ：保護資料不受主站災難影響。	<b>存取控制</b> ：僅授權人員可接觸備份媒介。
		<b>安全運輸</b> ：使用專業快遞運送備份資料。	<b>加密與金鑰管理</b> ：加密備份並單獨管理加密金鑰。
<b>Electronic Vaulting</b>	利用WAN或網路將資料備份傳送到遠端儲存點。	<b>機密性</b> ：加密資料保障傳輸過程中的安全性。	<b>快速恢復</b> ：可以直接從電子保險庫恢復資料。
		<b>高效性</b> ：可快速從保險庫恢復資料。	
<b>Remote Journaling</b>	傳輸日誌和資料庫交易日誌至遠端位置，確保資料持續性。	<b>快速恢復</b> ：中斷後可快速從遠端副本恢復。	<b>最小化資料遺失與停機時間</b> ：確保業務連續運行。
		<b>業務連續性</b> ：最小化資料遺失和停機時間。	

ISC2

## 系統和資料可靠性

### 叢集 (集群) Clustering

- 高可用性叢集 High-Availability
  - 主動/被動配置：主系統處於活動狀態，而次系統處於被動狀態，通過心跳信號進行監控
  - 故障轉移機制：如果主系統故障，次系統將接管
- 負載均衡叢集 Load-Balancing
  - 主動/主動配置：叢集中的所有節點都處於活動狀態，並共享負載
  - 冗餘性：如果某一系統故障，其他系統仍可繼續提供服務

### 獨立磁碟陣列 (RAID)

- RAID 0：提升性能但無冗餘
- RAID 1：其中 1 個硬碟損壞時資料可用
- RAID 5：其中 1 個硬碟損壞時資料可用
- RAID 6：其中 2 個硬碟損壞時資料可用

ISC2

## 測試與演練(重要)

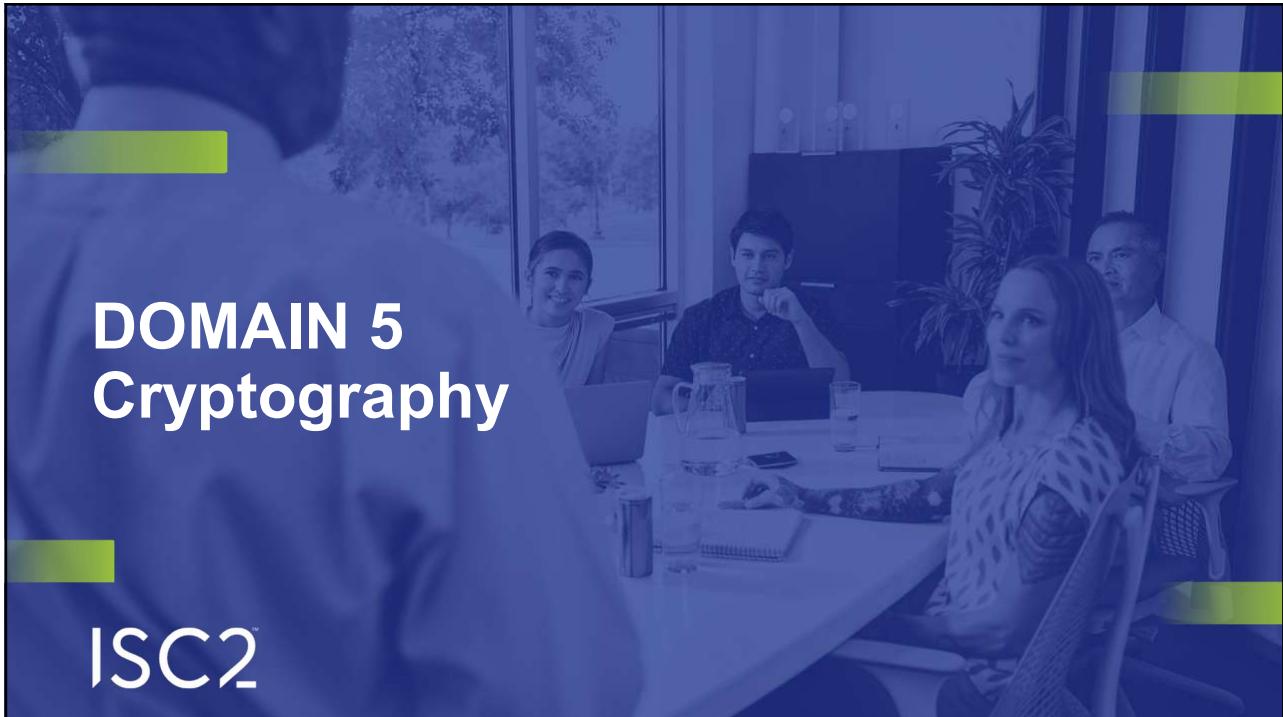


測試類型	文件檢查 (Desk-Check)	桌面演習 (Tabletop Exercise)	模擬測試 (Simulation)	平行測試 (Parallel Test)	完全中斷測試 (Full Interruption Test)
頻率	至少每年一次	定期進行，例如每年一次	視需要而定	定期進行	需要高階管理層批准，並且風險較高
負責人	各部門經理	恢復團隊成員	員工和管理層	使用商業熱站，並與生產系統平行運行	高階管理層層和 IT 部門
目的	確保計劃是最新的，符合當前的操作和人員需求	讓團隊成員了解自己在模擬危機情境中的角色和責任	測試員工的反應以及計劃的執行是否符合預期	確保備份數據完整，系統兼容，並且恢復時間符合預期	在危機情況下停用主要系統，並測試備份系統的有效性
活動	各部門經理檢視並更新其部門的計劃	團隊成員討論如何在模擬危機中互相協作，確保計劃覆蓋所有需要的步驟	模擬實際的危機情境，例如火災演習或伺服器重建	在熱站系統上運行數據，並與生產系統平行測試	停用主要系統，並啟用備份系統，檢查備份是否能在關鍵時間內恢復運行

ISC2

## DOMAIN 5 Cryptography

ISC2™



## 考試大綱 – Domain 5



- 5.1 Understand reasons and requirements for cryptography
  - Confidentiality, Integrity and authenticity
  - Data sensitivity (e.g., personally identifiable information (PII), intellectual property (IP), protected health information (PHI))
  - Regulatory and industry best practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))
  - Cryptography entropy (e.g., quantum cryptography, quantum key distribution)
- 5.2 Apply cryptography concepts
  - Hashing, Salting
  - Symmetric/Asymmetric encryption/Elliptic curve cryptography (ECC)
  - Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails)

ISC2

## 考試大綱 – Domain 5



- Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA))
- Cryptographic attacks and cryptanalysis
- 5.3 Understand and implement secure protocols
  - Services and protocols (e.g., Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), DomainKeys Identified Mail (DKIM))
  - Common use cases (e.g., credit card processing, file transfer, web client, virtual private network (VPN), transmission of PII data)
  - Limitations and vulnerabilities

ISC2

## 考試大綱 – Domain 5



- 5.4 Understand and support public key infrastructure (PKI) systems
  - Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow)
  - Web of Trust (WOT) (e.g., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)

ISC2

## 密碼學核心觀念 - 1



- 定義: 密碼學是將資訊轉換為無法讀取的形式 (加密)，以及將其恢復為可讀形式 (解密) 的科學。
- 目標 (CIA + Non-repudiation):
  1. 機密性 (Confidentiality): 確保只有授權方可以訪問資訊。
  2. 完整性 (Integrity): 確保資訊未被竊改。
  3. 可用性 (Availability): 確保授權方在需要時可以訪問資訊。(雖然密碼學較少直接影響可用性, 但相關的金鑰管理會間接影響)
  4. 不可否認性 (Non-repudiation): 確保行為人無法否認其行為。

ISC2

## Knowledge Check



- Bob would like to enhance the security of his communication by adding a digital signature to the message. What goal of cryptography are digital signatures intended to enforce?
  - A. Secrecy
  - B. Availability
  - C. Confidentiality
  - D. Nonrepudiation

ISC2

D

## 密碼學核心觀念 - 2



- 熵 (Entropy) : 指的是密碼的隨機性或不可預測性 (密碼有多難被猜中)
  - 舉例 : 熵低 → 123456、熵高 → G7!x\$Pq9
  - 熵的來源 : 假隨機數生成器 (Pseudo Random Number Generator, PRNG)
- 量子加密 : 用量子的特性實作現代密碼學的技術
  - Quantum Key Distribution (QKD)
  - 任何人偷看都會留下痕跡 (量子測不準原理 Uncertainty Principle)。
  - 透過比對方式 · Alice 和 Bob 能夠偵測竊聽 (錯誤率監測 Error Rates)
  - 最終，他們能建立一組只有彼此知道的密碼來保護通訊

ISC2

目前在題庫沒找到類似的考題...

## 密碼學術語



- Plaintext 明文：未加密的資訊
- Ciphertext 密文：加密後的資訊
- Cipher 加密器
- Key material - Encryption Key 加密金鑰：用來加密的金鑰(一串密碼)
- Key material - Decryption Key 解密金鑰：用來解密的金鑰(一串密碼)
- Encryption 加密：把資料加密的過程 (明文→密文)
- Decryption 解密：把資料解密的過程 (密文→明文)
- Algorithm 演算法：用計算的數學算法
- Cryptovariables 加密參數：數學算法要求的參數 · ex. 區塊大小 (Block Size)、循環計數 (Cycle Count)、重複次數 (Repeat Count)

ISC2

## 密碼學演算法



### Symmetric Encryption 對稱式加密

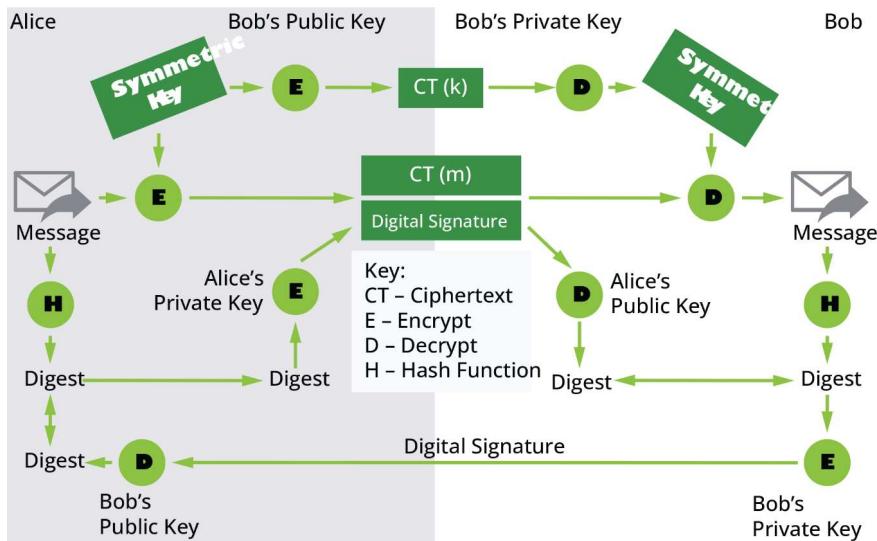
- Block cipher vs. Stream cipher
  - Block cipher 逐塊(ex. AES 128-bit block size)加密 · 重要的演算法 DES、3DES、AES
  - Stream cipher 逐 bit 加密 · 重要的演算法 RC4
- Block cipher 的運作模式
  - ECB 最快、但最不安全
  - Counter (CTR) 速度、安全平衡的最佳選擇 · 廣泛使用

### Asymmetric Encryption 非對稱式加密

- 分兩種演算法
  - Discrete logarithms 離散對數 · 重要的演算法 ECC
  - Prime factoring algorithms 質因數分解演算法 · 重要的演算法為 RSA
- ECC 是非對稱加密算法中效率最高的演算法 · 256-bit ECC = 3072-bit RSA · 加密效率高

ISC2

## 密鑰、公鑰、私鑰的混合運用



ISC2

## 密碼學分類 - 對稱 vs. 非對稱



### Symmetric Encryption 對稱式加密

- 加解密金鑰相同 (金鑰又稱 Pre-shared key、secret key)
- 網路環境不安全，金鑰的明文不能在網路傳輸
- 運算速度快，強度效率高 (用短的金鑰換到長的 Work factor)
- 拓展性差，若有 1,000 個人，每一個人都要跟其他 999 個人共享密鑰，所以需要  $1000 * 999 / 2 = 499,500$  支 key，數學公式是  $C(n, 2) = n(n - 1) / 2$
- 適用於檔案加密 (7-zip)

### Asymmetric Encryption 非對稱式加密

- 加解密金鑰不同 (有公鑰 Public key 和私鑰 Private key 之分)
- 公鑰可以在不安全網路傳輸，私鑰要收好
- 加密效率差 (不適合用在大檔案)
- 拓展性佳，若有 10 個人，每 1 個人都有一把公鑰和私鑰，所以需要  $10 * 2 = 20$  支鑰匙，數學公式是  $2n$

ISC2

## 對稱、非對稱、雜湊總複習表格



類別	對稱式加密 (Symmetric Encryption)	非對稱式加密 (Asymmetric Encryption)	雜湊 (Hashing)
主要用途	速度快的資料機密性保護	安全的金鑰交換、數位簽章、身份驗證	確保數據完整性、不可否認性
密鑰類型	單一密鑰 (Pre-shared Key)	公私鑰對 (Public & Private Key)	無密鑰 (使用演算法計算)
加解密方式	需要相同的密鑰進行加解密	依情境可能用公鑰或私鑰加密	單向轉換，不可逆
速度	快 (適合大檔加密)	極慢 (> 64 kb 不經濟)	快 (但輸出固定長度)
安全性	加密效率高，短金鑰長度達成強加密	公鑰可在不安全網路傳輸	防篡改，但易受碰撞攻擊
金鑰散布	$n*(n-1)/2$	$2n$	無
典型演算法	AES、DES (可用暴力破解)、3DES(被在中間相遇攻擊)	RSA、ECC(加密效率高)、Diffie-Hellman (用於金鑰交換)	SHA-256、SHA-3、MD5(不安全)
應用情境	VPN、磁碟加密、TLS session	數位簽章、PKI	資料完整性驗證、密碼儲存

ISC2

## Knowledge Check



- How many possible keys exist when using a cryptographic algorithm that has an 8-bit binary encryption key?
  - A. 16
  - B. 128
  - C. 256
  - D. 512

ISC2

C



## Knowledge Check

- Bob is designing a cryptographic system for use within his company. The company has 1,000 employees, and they plan to use an asymmetric encryption system. They would like the system to be set up so that any pair of arbitrary users may communicate privately. How many total keys will they need?
  - A. 500
  - B. 1,000
  - C. 2,000
  - D. 499,500

ISC2

C



## Knowledge Check

- Bob is choosing a cryptographic algorithm for his organization, and he would like to choose an algorithm that supports the creation of digital signature. Which one of the following algorithms would meet his requirement?
  - A. RSA
  - B. 3DES
  - C. AES
  - D. Blowfish

ISC2

A



## Knowledge Check

- Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificate signed by a mutually trusted certificate authority.
1. If Alice wants to send Bob a message that is encrypted for confidentiality, what key does she use to encrypt the message?  
**A. Alice's public key      C. Bob's public key**  
**B. Alice's private key      D. Bob's private key**

ISC2

C



## Knowledge Check

- Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificate signed by a mutually trusted certificate authority.
2. When Bob receives the encrypted message from Alice, what key does he use to decrypt the message's plaintext content?  
**A. Alice's public key      C. Bob's public key**  
**B. Alice's private key      D. Bob's private key**

ISC2

B

SSCP

## Knowledge Check

- Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificate signed by a mutually trusted certificate authority.
3. Which one of the following keys would Bob not possess in this scenario?
- A. Alice's public key      C. Bob's public key  
B. Alice's private key      D. Bob's private key

ISC2

B

SSCP

## Knowledge Check

- Alice and Bob would like to use an asymmetric cryptosystem to communicate with each other. They are located in different parts of the country but have exchanged encryption keys by using digital certificate signed by a mutually trusted certificate authority.
4. Alice would also like digitally sign the message that she sends to Bob. What key should she use to create the digital signature?
- A. Alice's public key      C. Bob's public key  
B. Alice's private key      D. Bob's private key

ISC2

# 雜湊 Hashing

## 雜湊 Hashing

- **MD5 不安全**
- **SHA-0 不安全** · 已發現碰撞
- **SHA-1 不安全** · 已發現碰撞
- **SHA-2** · ex. SHA-224、SHA-256、SHA-384、SHA-512 · 安全
- **SHA-3** · ex. SHA3-224、SHA3-256 · 安全

## 加鹽 Salting

在原文前增加一段固定的文字再雜湊

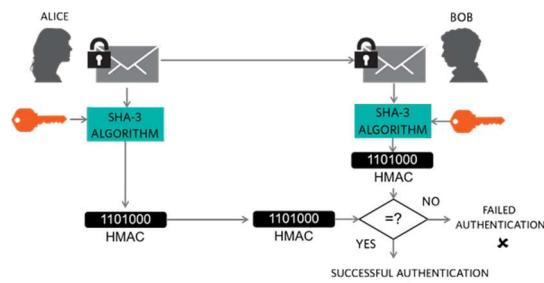
ISC2

## 雜湊攻擊

- 暴力破解攻擊：從 hash value 中找出原始消息或尋找碰撞
- 密碼分析：側信道攻擊、彩虹表攻擊 ·
- 生日悖論 **Birthday Paradox**
- 用於破解雜湊的工具 Cain and Abel

# HMAC雜湊訊息驗證碼

1. 選定雜湊函數 (SHA3)
2. 加入 Pre-shared key · 透過算法得出 HMAC (沒有加密、只做雜湊)
3. 對方也用一樣的算法驗證資料完整性



ISC2

## Crypt-analytic Attacks 密文分析攻擊

- **前提**：因為密文在不安全的網路環境下傳輸，密文是攻擊方一定會知道的資訊。
- **Ciphertext Only Attack** 僅知密文
- **Known Plaintext** 已知明文
- **Chosen Plaintext** 選定明文
- **Chosen Ciphertext** 選定密文：又稱午餐攻擊 (Lunchtime attack)
- **Linear Cryptanalysis** 線性破密：對大量已知明文/密文對進行統計分析。攻擊者試圖找到一個明文和密文之間的簡單線性關係，並利用這種關係來推導出密鑰。
- **Differential Cryptanalysis** 差分破密：大量比較分析已知明文與密文資訊輸入上的差別對輸出結果變化的影響，來識別密鑰的特徵和模式。

ISC2

## 針對密碼/雜湊的暴力攻擊

- **Brute Force Attacks** 暴力破解：攻擊者不斷地嘗試所有可能的密碼組合，直到找到正確的密碼。
- **Dictionary Attack** 字典攻擊：攻擊者使用包含常見密碼或詞彙的字典來試圖找到密碼。這比暴力破解更高效，因為許多人使用的都是常見、簡單的密碼。
- **Rainbow Table** 彩虹表：攻擊者使用預先算好的雜湊表(彩虹表)來查找密碼。
- **Birthday Attack** 生日攻擊：基於生日問題 (Birthday problem)，攻擊者不斷嘗試對消息進行雜湊處理，直到獲得產生相同雜湊值的消息為止，也是暴力攻擊的一種。

ISC2

## 針對加密設施的實體攻擊



- **Fault injection 故障注入攻擊**：攻擊者可以通過改變電壓、溫度或使用特殊的測試技術來引入錯誤，使設備產生異常回應。ex. 對加密晶片注入乾冰，使其超過工作溫度。
- **Fault Analysis Attack 故障分析攻擊**：通過故意引入錯誤來觀察系統的反應來獲取加密系統相關資訊。
- **Probing Attacks 探測攻擊**：觀察家密模組的電路分佈來獲取加密系統相關資訊。
- **Side Channel attacks 側通道攻擊**：利用加密系統中的物理特徵（如 Radiation emission 電磁泄漏、Power consumption 功耗和 Timing 計算時間）來獲取加密系統相關資訊。
- **Timing Attacks 計時攻擊**：利用系統對不同輸入的反應時間來推測密鑰。攻擊者可以通過測量解密過程中所需的時間來獲取加密系統相關資訊。

ISC2

## 重播攻擊



- **Man-in-the-Middle (MITM) Attacks 中間人攻擊**：攻擊者將自己放在對話之中，透過竊聽來回發送的通信，改變通信或破譯內容。
- **Replay Attacks 重放攻擊**：攻擊者重放之前有效的通信數據包來獲取未經授權的訪問。
- **Pass the Hash Attacks**：針對 NTLM (New Technology LAN Manager) 或 SMB (Samba Message Blocks) 的驗證封包進行重播。
- **Kerberos Exploitation**：攻擊者可以通過劫持或盜取 Kerberos 認證票證，進而獲取未經授權的訪問。

ISC2

## 針對密碼學演算法實作的攻擊

SSCP

- **Algebraic Attacks** 代數攻擊：通過分析加密算法中的特定方程式來推導出密鑰。
- **Factoring Attack** 因式分解攻擊：針對 RSA。
- **Frequency Attacks** 字頻攻擊：使用字母 (is, of, and, the ...) 或符號 (, .) 在特定語言中出現的頻率來破解加密。
- **Attacking the Random Number Generator** 攻擊隨機生成數：攻擊者能夠預測或劫持隨機數生成器的輸出，導致密鑰重用或碰撞。
  - 加密流程的簡要說明：隨機數產生器 (RNG) → 產生對稱式金鑰與初始化向量 (IV) → 進行加密 → 產生密文
- **Temporary Files** 暫存檔案：加密系統在計算過程中產生的暫存檔案未安全刪除或覆寫，導致攻擊者進行密碼分析攻擊。

ISC2

## 密碼學綜合運用

SSCP

- **S/MIME** 用於確保電子郵件機密性、身分驗證
- **Digital Signatures** 用於確保資料完整性、不可否認性
- **SSL/TLS** 確保資料傳輸階段的機密性、完整性、身分驗證
- **Steganography** 隱寫術：隱藏訊息，不像加密一樣明顯，即使第三方攔截，也看不出異常
- **NULL cipher** 如中文的藏頭詩，讓只有特定人能解讀 (需知道解密規則)

### IPSec

- 用於保護 IP 層的通訊。
- 了解 IPsec 的兩種模式 (傳輸模式和通道模式)、AH 和 ESP 協定、IKE (Internet Key Exchange)

### VPN

VPN 技術	特色
PPTP	透過 GRE 封裝建立隧道，設置簡單，已被認為不安全，容易被駭客攻擊
L2TP/IPsec	L2TP 本身不提供加密，需要靠 IPsec Tunnel mode 保證機密性
OpenVPN	開源軟體，使用 AES 256 bit 加密，安全性極高，可穿透大多數防火牆，需要額外安裝客戶端軟體，設定較為複雜
IPsec	提供強身份驗證與加密機制，設定較為困難，多用於企業內部網路
SSL VPN	透過瀏覽器連線，無需額外軟體(方便)

ISC2

## 金鑰生命週期的管理



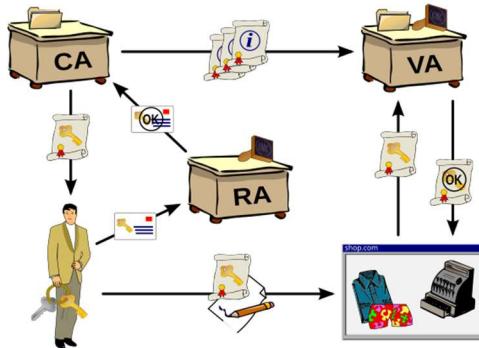
1. **Key Generation / Creation:** Key space 大且隨機、需有有效期限 (Cryptoperiod)、定期輪轉
2. **Key Storage / Key Wrapping, and Key Encrypting Keys (KEKs):**
  - 必須放在有完整性保護的儲存機制中
  - 在防竊改保護的硬體/晶片中: HSM, TPM
  - 用一組「保護金鑰」來加密其他金鑰 (Key Wrapping)
3. **Key Distribution**
  - Diffie-Hellman (DH)、Out-of-band、Hybrid
4. **Key Destruction**
  - 記錄金鑰的使用歷史，確保過期或被撤銷的金鑰不會被誤用
  - 避免被密碼蒐集與分析攻擊，所以需要安全地銷毀金鑰
5. **Key Recovery**
  - Dual Control 需要兩個或更多人執行某些操作才能恢復金鑰，ex. 兩人同時轉動自己的鑰匙才能發射導彈
  - Split Knowledge 將金鑰的支式分給兩個或多個人，為了恢復金鑰，這些人需聚在一起結合他們各自持有的知識來恢復完整金鑰
  - Key Escrow 加密金鑰的副本交由受信任的第三方託管

ISC2

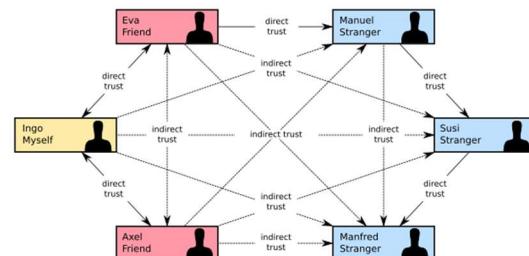
## 數位憑證信任網路



### CA 集中式信任 (PKI)



### WoT 分散式信任



ISC2

## 公鑰基礎措施(KPI) – 核心元件及功能描述

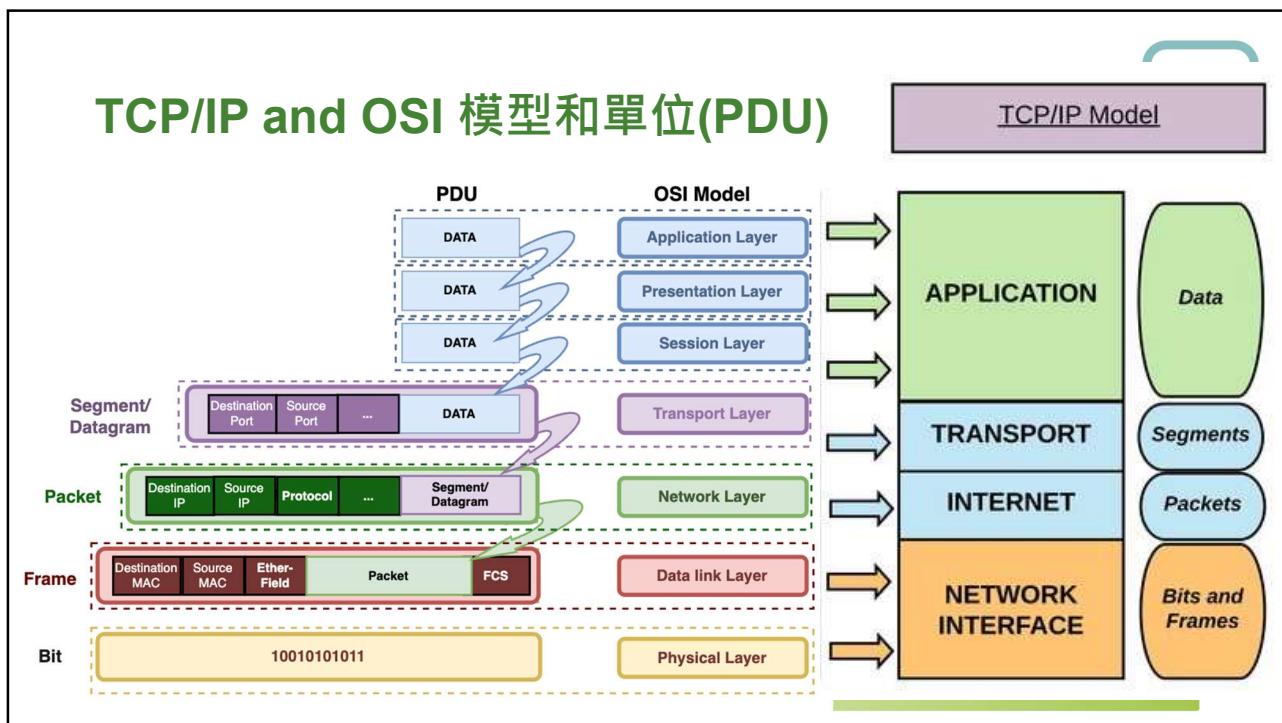
SSCP

核心元件	功能描述	比較
證書頒發機構 ( CA )	CA是PKI的核心，負責頒發和管理數字證書，驗證申請者的身份，確保所頒發證書的可信性。	CA的可信度直接影響PKI的安全性，選擇公認的CA能夠確保數字證書在廣泛環境中的有效性和信任度。例如：全球知名的CA，如Symantec、DigiCert等。
註冊機構 ( RA )	RA負責身份驗證和證書申請的處理，作為CA與用戶之間的中介。RA確認用戶的身份並將相關信息傳遞給CA。	RA並不頒發證書，但它的有效性和認證流程的完善性對整個PKI系統的安全性至關重要。RA與CA之間的合作關係密切。
數字證書	數字證書是一份電子文檔，包含公鑰及其持有者的身份信息，通常由CA簽名。證書用於身份驗證和加密通信。	數字證書的有效性和安全性取決於CA的聲譽和管理方式，數字證書的格式（如X.509）則確保了兼容性和標準化。
證書撤銷列表 ( CRL )	CRL是CA發布的，包含已吊銷數字證書的列表。通過檢查CRL，用戶可以確定某個證書是否仍然有效。	CRL的更新和管理對PKI的及時性和可用性至關重要。與CRL相對的是在線證書狀態協議（OCSP），後者提供了更即時的證書狀態查詢。
密鑰管理	密鑰管理涉及生成、分發、存儲、備份和註銷密鑰的過程，確保私鑰的安全性及其與相應公鑰的關聯。	良好的密鑰管理實踐對於預防密鑰洩露和保證數據安全至關重要，包括使用硬體安全模組（HSM）來存儲私鑰等安全措施。

ISC2

## DOMAIN 6 Network and Communications Security

ISC2™



## Layer 1 – 傳輸媒體



### 有線

- Twisted Pair Wiring 雙絞線
- Coaxial Cable (RG58) 同軸電纜
- Optical Fiber Cable 光纖
  - Single mode 單模
  - Multi mode 多模
  - Plastic optical fiber (POF) 塑膠光纖

### 無線

- Electromagnetic 電磁波：紅外線、衛星/微波、Wi-Fi 等
- Bluetooth
- WiMAX
- Zigbee
- Satellite Network
- Cellular Network

ISC2

## Layer 1 – 威脅與對策



### 威脅

- 實體入侵 (physical intrusions)
- 無線訊號干擾 (Injection of signals) 注入訊號、Radio Jamming 無線電蓋台(雪隧)、signal interference 訊號干擾)
- Wardriving 開車或行走在路上，使用無線設備搜尋並標記開放或不安全的無線網路
- 對藍芽的攻擊
  - Bluesnarfing：攻擊者藉由藍牙漏洞未經授權地存取並竊取目標設備的資料，像是聯絡人、日曆、訊息、電子郵件等
  - Bluebugging：攻擊者用藍牙漏洞遠端連接到目標設備，並控制其功能，如打電話、發送簡訊等，而目標使用者無法察覺

### 對策

- 實體保護 (鎖定設備機櫃、限制存取)
- 無線頻道監控 (RF 監測)，偵測與防止無線攻擊
- 選擇合適的傳輸媒介，減少干擾風險

ISC2

## Layer 2 – 簡介



### Media Access Control (MAC, 媒體存取控制)

- FF:FF:FF:FF:FF:FF (16進位，12個值)，前 6 個值是廠商的代碼，故做 nmap scan 可知道主機是哪個廠牌就是從這 6 個值判斷
- 可以透過軟體的方式修改 → MAC Spoofing

### 技術與應用

- Address Resolution Protocol (ARP, 地址解析協議) 與 Neighbor Discovery Protocol (NDP, 鄰居發現協議)：
  - ARP 用於 IPv4 網路，將 IP 地址轉換為 MAC 地址
  - NDP 用於 IPv6 網路，執行類似的地址解析功能
- PPP 與 PPPoE：
  - Point-to-Point Protocol (PPP, 點對點協議)：在兩個節點之間建立 L2 連接
  - PPP over Ethernet (PPPoE)：用於 ISP (Internet Service Provider) 提供家庭寬頻上網連接功能，需要發號連接
  - Fiber Channel / FC over Ethernet (FCoE)：用於 SAN (Storage Area Network)，常見於企業資料中心或大型儲存需求的機房

ISC2

## Layer 2 – 負載管理協議(解決碰撞問題)



### Polling Protocol 輪詢

- 主設備 (如主控器或伺服器) 定期向從設備 (如感測器或其他設備) 發送查詢命令。ex. 藍芽
- 優點：避免衝突
- 缺點：Polling Delay (即使設備沒有要傳資料，還是會被問輪詢)

### Contention-based Protocol 基於競爭的協議 (重要)

- CSMA/CD 用於乙太網路(有線)
- CAMA/CA 用於無線網路 (如Wi-Fi)

ISC2

## Layer 2 – 威脅與對策



### 威脅

- **MAC Address spoofing (偽冒) or cloning (複製)**
- **MAC flooding (氾濫)**：攻擊者試圖填滿交換機的 MAC Forwarding Table，使其無法記錄新的 MAC 地址，交換機將會回退到廣播模式，導致所有資料被廣播到所有 Port
- **VLAN hopping (跳躍)**：又稱 802.1Q attacks
- **Broadcast storms 廣播風暴**：
- **Reconnaissance probes (探測) using MAC sniffing**：攻擊者通過探測網路中的 MAC Address 來進行，了解網路結構和相關設備
- **ARP Poisoning (下毒)** 假造 ARP 回應，欺騙設備，改變資料轉發的流向，進而攔截(改到自己身上)或阻斷服務(全部的封包改到同一個對象)

ISC2

### 對策

- **MACsec (Media Access Control Security, 媒體存取控制安全) IEEE 802.1AE** 在 L2 加密有線網路流量，防止資料被竊聽、篡改
- 網卡 (NIC) 設定強化，限制未授權存取 → 從交換機端啟動 port-security、啟動 802.1X (NAC, Network Access Control)...
- **ARP 檢查 (ARP Inspection)** → DHCP Snooping 建立合法的 IP-MAC 綁定關係
- 服務監控 (Service Monitoring)，即時偵測異常行為
- VLAN 與交換機埠配置，確保 VLAN 的正確隔離與存取控制
- 入侵偵測與防禦系統 (IDS/IPS)，監測異常流量與攻擊行為

## Layer 3 – 簡介



### 傳輸型式

- **Unicast 單播**：1 對 1，ex. 網頁瀏覽
- **Broadcast 廣播**：1 對多個不特定對象，ex. 無線投影接收器
- **Multicast 多播**：1 對多個特定對象，ex. IPTV (MOD)
- **Anycast 任播**：1 對最近的 1 個對象 (由路由決策決定)，ex. CDN、DNS、Load balance
- **Geocast**：以地理位置為基礎，ex. 智慧城市的區域警報或天氣通知

ISC2

### NAT：解決 IPv4 地址不足的問題

- **Static NAT**：1 個內部 IP 映射到 1 個外部 IP，ex. Web Server
- **Dynamic NAT**：多個內部 IP 映射到 1 組外部 IP，ex. 內部電腦上網
- **PAT (Port Address Translation)**：又稱 NAT Overloading，多個內部 IP 映射到 1 個外部 IP 的不同 Port 號，ex. 節省外部 IP 的情境

## Layer 3 – 應用



### DDI (IP-Address-Based Asset Tracking)

- 基於 IP 地址的資產追蹤
- DDI 代表 DNS、DHCP 和 IP address management，它是一種統一管理網路設備 IP 地址、DNS 設定和 DHCP 分配的解決方案

### IPv4 → IPv6 過渡策略

- Native IPv6：直接在環境內部署和使用 IPv6 (適用於新的網路或有能力迅速過渡的環境)
- Dual Stack：同時支援 IPv4 和 IPv6，v4 和 v6 的設備各自溝通不干擾，逐步提高 v6 的流量比例，但需要所有設備兼容 v4 和 v6 協定
- Tunneling：將 IPv6 流量封裝在 IPv4 內，讓資料可以在不支援 v6 的環境中傳輸。

ISC2

## Layer 3 – 路由協議 (使路由器 (郵差) 有效率送信)



### 協議

- Distance-Vector Protocols 距離向量：採用廣播機制計算每條路的耗損 (hop counts 跳數)，不適合在大型網路內使用 ex. RIP (Routing Information Protocol)
- Path-Vector Protocols 路徑向量：**BGP** (**Border Gateway Protocol**)，透過網際網路不同自治系統 (AS) 之間的路由自行選擇，是網際網路的主要路由協定
- Link-State Protocols 鏈路狀態：路由器定期發鏈路狀態通告給全部的路由器，建立 Link-State 資料庫，根據資料的目的地最短路徑，廣泛用於企業內部網路，ex. **OSPF** (**Open Shortest Path First**)

### 協定

- **ICMP**：ex. Ping、Tracert 等，用來診斷遠端設備的連線問題
- **IGMP**：ex. MOD，用於管理多播 (multicast) 網路的群組，允許主機加入或離開群組並通報 Router，使流量只會發送到需要的設備上。

ISC2

## Layer 3 – 威脅



- **Routing attacks (RIP)** : 泛指針對路由協定 (ex. RIP, BGP...) 的攻擊
  - **Routing table poisoning** 路由表下毒
  - **ICMP attacks** : 一種 DoS , 又稱 **Ping of Death (PoD)** , 透過送出大型的封包 (長度大於 65535 bytes ) 瘫瘓目標 (無法處理正常請求)
  - **Ping flooding** : 一種 DoS , 向目標發送大量的 ICMP Echo Request (ping) 瘫瘓目標
  - **Smurf attacks** : 一種 DoS , 藍精靈攻擊 , 攻擊者偽冒一個封包 , 封包的來源位址是受害者的真實 IP 位址 , 然後將這個封包試圖透過廣播向多個系統向目標發送 , 收到封包的系統收到來自廣播裝置的要求後就會使用 ICMP 封包淹沒目標伺服器。  
(惡整朋友 , 廣發釣魚簡訊 , 請對方有興趣 call 我 , 但其實是朋友的手機號碼)
  - **IP address spoofing** : 攻擊者發送偽冒的 IP 封包 , 用於繞過安全措施管制
  - **Packet sniffing** : 攻擊者使用工具捕捉網路流量 , 可能提取敏感資料 (ex. 帳號密碼) 以進行未經授權的行為
- (以下補充 , 簡報/Textbook 沒有但題庫常見)
- **Teardrop Attack 淚滴攻擊** : 向目標機器發送損壞的 IP 封包 , 如重疊的封包或過大的封包載荷 , 使其難以被接收主機重新組合 , 可能導致 Win 7 或更舊的設備 OS 藍屏。
  - **Rogue Router 惡意路由器** : 在 BGP 中偽裝合法設備 , 廣播錯誤的路徑、影響封包流向 , 或實施中間人攻擊

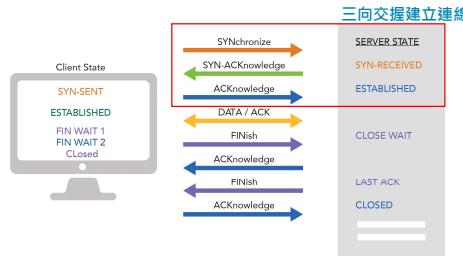
ISC2

## Layer 4 – 簡介



### TCP – 連接導向 (要建立連線)

- 優點：資料傳輸的可靠性與順序保證
- 缺點：資源占用大，延遲較高，效率較低
- 應用場景：HTTP/HTTPS、FTP



### UDP – 非連接導向

- 優點：簡單，成本低，效率高
- 缺點：無法確保完整性和順序 (靠應用程式實作)
- 應用場景：VoIP、視訊通話、線上遊戲

ISC2

## Layer 4 – 常見的協議及連接埠

SSCP

協定	連接埠	功能描述	關鍵攻擊/弱點	安全擴充
CIFS/SMB	137-139、445	文件共享協議，在 Windows 上流行。	透過嗅探或加密攻擊竊取憑證。	無法進行安全擴充，較為脆弱。
SMTP/ESMTP	25	用於路由電子郵件。	SMTP 中沒有身份驗證或加密。	ESMTP 增強功能：新增身份驗證機制。
FTP	20、21	用於檔案傳輸。	明文憑證和數據，容易受到多種攻擊。	帶有 TLS 的 FTP、SFTP (SSH 檔案傳輸協定)。
TFTP	69	FTP 的簡化版本，用於可信任網路。	沒有身份驗證，適合低延遲環境。	無法進行安全擴充，缺乏安全性。
SSH	22	安全的遠端登入、文件傳輸和命令執行。	防止會話劫持，透過連接埠轉發增強安全性。	無需其他擴充，原生安全性較高。
SNMP	161、162	用於網路管理。	容易受到針對社區字串的暴力攻擊，以明文形式發送資料（版本 3 之前的版本）。近期受關注的漏洞如 SUNBURST 攻擊。	SNMP 版本 3 增加了安全性功能。

ISC2

## Layer 4 – 威脅與對策

SSCP

### 威脅

- Network Time Protocol (NTP) de-synchronization attempts**：透過偽裝的 NTP 請求，攻擊者可能試圖將目標設備的時間回調或提前，導致時間同步失敗，影響依賴準確時間的應用。
- Fraggle (UDP broadcast flood)**：類似 Smurf，送出假造來源的 UDP broadcast 封包至目標網路，以產生放大的資料流。
- TCP sequence prediction**：猜測 TCP 中的序列號，以便建立有效的 TCP 資料包做於資料竊改。
- IP address spoofing, packet sniffing, and port scanning**：檢查目標主機上開放的 Port，以識別可能的攻擊入口。

### 對策

- TCP intercept and filtering**：防火牆
- DoS prevention services** 拒絕服務 (DoS) 的預防服務
- Allowed and blocked lists for IP addresses, URLs, and URIs** 允許和拒絕清單
- 使用安全版本的協定替代不安全的協定**
- Fingerprint scrubbing**：清除或隱藏設備或應用的指紋訊息，降低被端口掃描或識別攻擊的風險。

ISC2

## Layer 5 – 簡介

SSCP

### 身分驗證協定

#### Authentication protocol

- **PAP (Password Authentication Protocol)**：不安全，最基本的身份驗證協定，使用明文傳輸用戶名和密碼進行身份驗證。
- **CHAP (Challenge Handshake Authentication Protocol)**：基於挑戰-握手的身份驗證協定，伺服器發送一個隨機挑戰碼給客戶端，客戶端用密碼和挑戰碼計算結果並傳回給伺服器，伺服器驗證回應結果，不傳輸密碼本身，提高了安全性。
- **EAP (Extensible Authentication Protocol)**：一種框架，支持多種身份驗證方法
- **PEAP (Protected Extensible Authentication Protocol)**：PEAP 在 EAP 的基礎上增強了安全性，通常使用 TLS 在伺服器上掛憑證，常見用於企業無線網路。

### 通道協定 Tunneling protocol

- **PPTP (Point-to-Point Tunneling Protocol)**不安全
- **L2TP (Layer 2 Tunneling Protocol)**要結合使用 **IPSec**
- **IPsec**
- **OpenVPN**
- **SSL/TLS VPN**

ISC2

## Layer 5 – 其他協議

SSCP

- **Remote Procedure Call Protocol (RPC)**：允許程式在不同的主機上進行通信，像在本地執行程式一樣調用遠端服務。未使用 SSH 加以保護的話，是不安全的，若用 SSH 則名稱應為 SRPC。

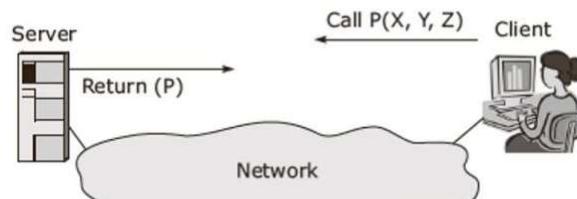


Figure 4-3 Basic RPC model

ISC2

## Layer 5 – 威脅與對策



### 威脅

- **Session hijack (劫持), MITM**
- **ARP, DNS, and poisoning of local hosts files** : 有 Cache 的地方就可以下毒。
- **Secure shell (SSH) downgrade attempt** : 攻擊者故意使系統放棄新、安全性高的協定，反而使用向下相容協定建立連線
- **Man-in-the-browser (MITB), Trojans in browser helpers, add-ons, or other software** : 攻擊者在受害者瀏覽器中的插件植入惡意程式。

### 對策

- 取代不安全的密碼身份驗證協定
- 遷移至強大的身份管理和訪問控制
- **Use PKI 公信單位簽發憑證**，確保憑證真實性
- Verify DNS is correctly configured 使用 **DNSSEC** (Domain Name System Security Extensions) 增強防護，防止假 DNS 招搖撞騙
- **主動監控**：部署更強大的入侵檢測和防禦系統 (IDS/IPS) 以及安全事件與事件管理 (SIEM) 系統

ISC2

## Layer 6 – 簡介



### 功能

- **資料格式化**：客戶端將交易請求轉換為標準格式
- **加密**：資料透過 SSL/TLS 進行加密，確保安全
- **壓縮**：減少資料大小，提高傳輸效率
- **傳輸**：往下層傳，透過網路層 (Layer 3) 與傳輸層 (Layer 4) 傳送至銀行伺服器
- **解密與解析**：伺服器解密資料，解析後送至應用層 (Layer 7) 處理

### 服務

- **翻譯服務 Translation Services**：字元集轉換
- **資料轉換與壓縮 Conversion and Compression Services**：JPEG、MP4
- **加密服務 Encryption Services**：SSL/TLS、S/MIME

ISC2

## Layer 6 – 威脅與對策



### 威脅

- NetBIOS attack**：攻擊者利用 NetBIOS 漏洞進行未授權存取。
- SMB attack**：利用 SMB 漏洞進行攻擊，ex. WannaCry 勒索病毒
- Downgrading session encryption**：攻擊者故意使系統放棄新加密演算法，反而使用向下相容的版本建立連線
- Path traversal (遍歷) attacks**：利用應用程式的漏洞進行的攻擊，通過修改 URL 中的路徑參數來達成，如 <http://link/../../>

### 對策

- 針對使用弱身份驗證或保護措施的應用程式進行替換或升級
- Migrate (遷移) to **more secure applications protection**
- Web application firewall (WAF)**
- Applications delivery platform (ADP)**：一個借助容器化實現的軟體交付與維運工具，可以實施統一的安全政策設定
- Migrate to **zero trust architecture**

ISC2

## Layer 7 – 簡介



### 關鍵協議

協議	功能
HTTP/HTTPS	網頁傳輸協議，提供網站存取 (HTTPS 提供加密保護)
DNS (網域名稱系統)	負責將網域名稱轉換為 IP 位址
DHCP (動態主機配置協議)	為裝置自動分配 IP 位址與網路參數
SNMP (簡單網路管理協議)	用於監控和管理網路設備
LDAP (輕量級目錄存取協議)	用於存取和管理用戶目錄 (例如 AD 服務)

### 關鍵資訊

- DNS**：分散式的系統，主要用於將域名轉換為 IP 地址。使用 Anycast 的方式
- SNMP**：使用Community string (社群字串) 起到類似密碼的作用，用於身分驗證
  - SNMP abuse attack**：public 和 private 通常是預設的社群字串，大多數人都不了解這是預設密碼，以致於長期下來，就會使用 public 作為 public community string，而把 private 當成是 private community string。

ISC2

## 網路架構類型



- 1. 網際網路 (Internet): 由骨幹路由器和通訊系統組成的全球網路，ISP 提供連接服務。
- 2. 內部網路 (Intranet): 組織控制範圍內的網路，透過路由器連接到網際網路。
- 3. 外部網路 (Extranet): 連接多個內部網路，用於組織間的資源共享。
- 4. 周邊網路 (Perimeter Networks): (又稱 DMZ) 不同安全等級網路間的安全連接。
- 5. 廣域網路 (WAN): 連接不同地理位置的區域網路 (LAN)。
- 6. 都會網路 (MAN): 連接不同建築物或城市的區域網路。
- 7. 區域網路 (LAN): 本地網路，通常在同一個建築物或園區內。
- 8. 個人區域網路 (PAN): 連接個人智慧裝置的網路。
- TOR 網路和暗網 (TOR Network and Dark Web):
  - 1. TOR (The Onion Router): 提供 匿名 網路瀏覽的 志願者網路。
  - 多層加密: 流量經過多個節點加密，隱藏來源和目的地。
  - 2. 暗網 (Dark Web): 只能透過 特殊軟體 (例如 TOR 瀏覽器) 訪問的 隱藏網站。
  - 可能包含 敏感 或 非法 內容。
- 區域範圍 : WAN >>> MAN >>> LAN >>> PAN

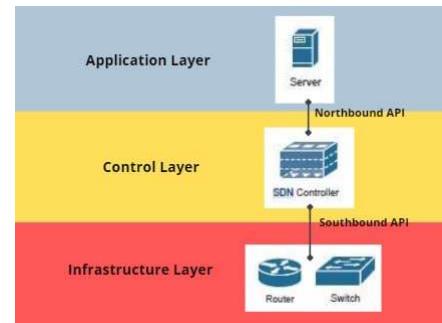
ISC2

## SDN 軟體定義網路



### 架構

- 應用層或管理層 – Application (Load Balance, Firewall...)
- (Northbound APIs 北向)
- 控制層 – SDN controller (East-West APIs 東西向 儲存空間、計算資源)
- (Southbound APIs 南向)
- 基礎設施層或資料層- Switch
- 使用 OpenFlow協議



ISC2

## Cyber Kill Chain 攻擊鏈



### 順序很重要



1. 偵察 (Reconnaissance): 收集目標資訊。
2. 武器化 (Weaponization): 準備攻擊工具。
3. 投遞 (Delivery): 將攻擊工具傳送到目標。
4. 漏洞利用 (Exploitation): 利用系統漏洞。
5. 安裝 (Installation): 安裝惡意軟體。
6. 指揮與控制 (Command and Control, C2): 建立與目標的通訊通道。
7. 目標達成 (Actions on Objectives): 執行攻擊目標 (例如：竊取資料、破壞系統)。

ISC2

## Network Access Control (NAC)

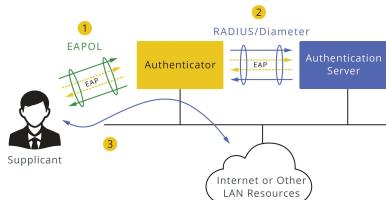


### 角色

- **Supplicant** 客戶端
- **Authenticator** 身份驗證者，網路設備，ex. Switch or Wi-Fi AP
- **Authentication Server** 身份驗證伺服器，儲存驗證資訊並執行驗證，ex. RADIUS Server
- 流程：客戶端 → 身份驗證者 → 身份驗證伺服器 → 驗證成功 → 身份驗證者允許客戶端加入網路

### 用來驗證身分的協議

- **RADIUS**：使用 UDP，只加密從用戶端傳至伺服器的存取要求封包中的密碼，封包的其餘部分並未加密，廣泛用於一般網路設備
- **TACACS+**：Cisco 專有的協議，改善 RADIUS 的所有問題，使用 TCP，加密封包的整個主體，只能用在 Cisco 網管設備
- **DIAMETER**：RADIUS 改善版本，適用於行動通訊 (3G/4G/5G) 或手機漫遊服務。
- **802.1X** 會透過上述驗證協議，使用 LDAP 向 AD 檢索資料



ISC2

## 不同層級防火牆比較



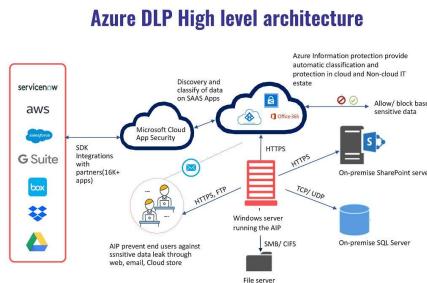
- **(L3 & L4) Static Packet Filtering 靜態封包過濾**：查看來源 IP、目的 IP、Port、Service，使用 ACL 管制，僅對每個數據包進行檢查，不保持任何連線狀態的記錄。
- **(L3 & L4) Stateful Packet Filtering 狀態封包過濾**：不僅檢查封包的 header，還跟蹤每個連線的狀態，根據連線的上下文進行決策。
- **(L4) Circuit-Level Gateway 電路級代理**：在客戶端和伺服器之間建立一個虛擬電路（伺服器 Proxy），只允許受信任的連結進行通信。檢查協定交握和 session 的正確性，但不會檢查傳輸的資料內容。
- **(L7) Web Application Firewall (WAF)**：查看進出網路的流量的內容，並基於應用層協定進行細粒度的規則設定，ex. SQL injection, XSS
- **(L7) Application-Level Proxy**：查並過濾 HTTP、FTP、SMTP 等應用層協議的流量
- **(L7) Web Proxy Servers**：主要用於 HTTP/HTTPS 流量，幫助使用者存取網站時隱藏 IP 或加速網頁載入（快取靜態內容）
- **DPI (Deep Packet Inspection, 深度封包檢測)** 是 WAF 的核心技術之一，ex. 阻擋 P2P 應用程式 (BitTorrent)，即使它使用 HTTP/HTTPS。DPI 也會用在其他安全技術上，ex. IDS、EDR...
- (綜合以上，重點在 L7) Next-Generation Firewall 下一代防火牆：整合 IDS/IPS、IAM 等功能，對流量進行深度檢查

ISC2

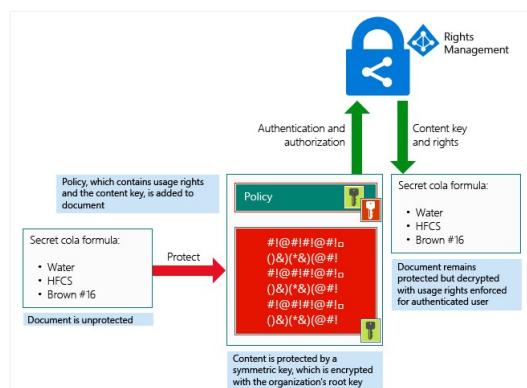
## DLP vs DRM



**DLP 防止資料離開企業可控環境，降低洩密風險**



**DRM 專注於 受保護資料的存取權限**

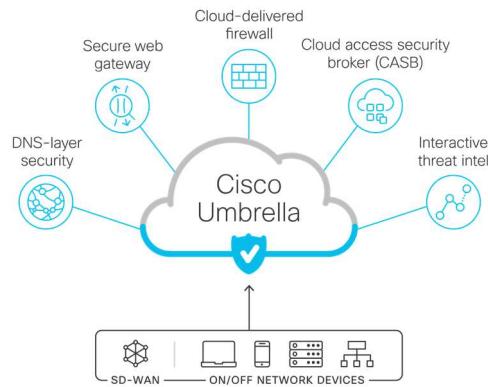


ISC2

## UTM 統一威脅管理

SSCP

- 一種一體化的安全解決方案，通過單一設備提供多種安全功能，通常直接放在 NGFW 中，也可能獨立放到雲端 (UTMaaS)



ISC2

## Wi-Fi 安全

SSCP

- Wireless Devices and Security 已被證明不足以保護系統的防護措施
  - MAC (Media Access Control) filtering
  - Disabling the service set identifier (SSID) broadcast
- 應採取的作法
  - WPA3 (Personal or Enterprise version)
  - Secure network architecture (isolation)
  - Radio-frequency (RF) management

ISC2

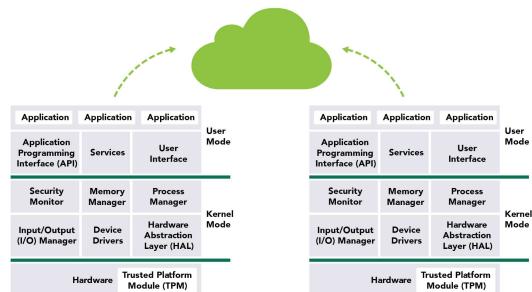
# DOMAIN 7 Systems and Application Security

ISC2

## 安全系統架構

SSCP

1. 最底層是 **硬體 (Hardware)**：包含了 Trusted Platform Module (TPM - 可信平台模組)、一個用來提供安全性的晶片。(如加密、身分驗證、確保系統完整性、儲存加密金鑰)
2. 中層是**作業系統核心 (Kernel Mode)**：承上啟下，監控系統安全 (存取權限、異常行為)、記憶體管理 (保護記憶體避免溢位錯誤或用盡)、程序管理(不同應用程式不互相干擾)、IO管理 (鍵盤滑鼠硬碟資料傳輸)、裝置驅動程式 (作業系統與硬體溝通)、硬體抽象層 (提供統一的硬體介面)
3. 上層是**應用程式層 (User Mode)**：放 API (應用程式介面)、服務、UI (使用者介面) 和各個應用程式
4. 最上層是存取這個軟體的其他系統、操作人員、商務流程等
5. 外層是法律、法規、合約或其他限制因素



## 從威脅的角度來看資料安全 - 1

SSCP

- **Aggregation and Inference 資料聚合與推理攻擊**：透過收集多個看似無害的資訊，推理出機密資訊。如在考試的時候用後面考題出現的題目內容，推斷前面考題的答案。從兩期人事總支出的差異，推斷新進人員的薪資範圍。
- **Bypass Attacks 繞過攻擊**：不直接破解系統，而是尋找繞過安全機制的方法。如網站需要登入才能查看內容，攻擊者發現透過特定的 URL 直接輸入，就可以不經驗證直接存取內部資訊。
- **Compromising Database Views 破壞資料庫視圖**：利用資料庫的查詢視圖 (Views) 來存取不該看到的資料。
- **Alternative Access Routes 替代存取路徑**：找到非正式的方式來進入系統。如測試後忘記關閉的管理者後門 (Backdoor)
- **Data Contamination 資料污染**：惡意修改、偽造、或插入錯誤的資料，影響系統決策。如在 AI 訓練資料集中，偷偷加入錯誤資訊，讓 AI 產生偏差判斷。
- **Deadlocking 死鎖**：多個程序同時等待對方釋放資源，導致系統無法運作。如 A 交易程式鎖住資源 X，B 交易程式鎖住資源 Y，然後 A 需要 Y、B 需要 X，結果兩者都卡住，導致系統無法回應。
- **Denial of Service (DoS) 拒絕服務攻擊**：駭客透過大量請求癱瘓系統，使其無法回應正常使用者。
- **Improper Modification of Information 資訊不當修改**：未經授權或不正當的方式更改資訊。如內部員工惡意修改公司的財務報表，欺騙投資人。

ISC2

## 從威脅的角度來看資料安全 - 2

SSCP

- **Interception of Data 資料攔截**：在傳輸過程中偷取或修改資料。如 MITM attack
- **Query Attacks 查詢攻擊**：透過巧妙的查詢請求，試圖獲取機密資訊。如 SQL injection，查詢使用者資料表的所有資訊。
- **Physical or Direct Logical Access 實體或直接邏輯存取**：攻擊者直接接觸到實體設備，或透過未加密的存取方式進入系統。如偷走伺服器的硬碟
- **Time of Check to Time of Use (TOCTOU) 檢查到使用的時間差攻擊**：在系統檢查某項條件後到執行動作的這段時間內，攻擊者修改環境，使檢查結果失效。如程式檢查使用者是否有權限存取，確認後打開文件。但駭客在這個瞬間換掉了文件，使他能存取不該存取的資訊
- **Web-Based Attacks 網頁攻擊**：利用網站的漏洞發動攻擊，如 XSS、SQL injection。如駭客在留言區輸入惡意 JavaScript 程式碼，當其他人瀏覽該頁面時，他們的 session 被偷走
- **Unauthorized Access 未授權存取**：未經允許進入系統或查看機密資訊。如員工猜對主管或者闖的密碼，偷偷登入 HR 系統偷看大家的薪資

ISC2

## 常見惡意程式碼類型



- **病毒 (Virus)**: 需要附著在檔案上才能傳播，當檔案被開啟時才會發作。
- **蠕蟲 (Worm)**: 不需要附著在檔案上，會自我複製並透過網路傳播，感染更多設備。
- **特洛伊木馬 (Trojan Horse)**: 偽裝成正常軟體，但實際上帶有惡意功能。
- **間諜軟體 (Spyware)**: 祕密收集使用者資訊，例如瀏覽習慣、鍵盤記錄或螢幕截圖。
- **廣告軟體 (Adware)**: 顯示不需要的廣告，可能追蹤使用者行為。
- **勒索軟體 (Ransomware)**: 加密使用者檔案，要求贖金才能解密。
- **Rootkit**: 隱藏惡意程式碼，獲得系統的最高權限。
- **後門 (Backdoor)**: 允許未經授權的遠端存取。
- **殭屍網路 (Botnet)**: 由受感染的電腦組成的網路，用於發動攻擊或執行其他惡意活動。
- **邏輯炸彈 (Logic Bomb)**: 在特定條件觸發時執行惡意功能。
- **鍵盤記錄器 (Keylogger)**: 記錄使用者的鍵盤輸入。
- **下載器(Dropper/Downloader)**：下載和安裝其它惡意軟體的程式。

ISC2

## 惡意軟體的對策 Malware Countermeasures



- **基本防護 Cybersecurity Hygiene Measures**：防火牆 (Firewall)、防毒與反惡意軟體系統 (Antimalware)、存取控制 (Access Control)、電子郵件過濾 (Email Filtering)
- **系統強化 System Hardening**：關閉不必要的功能與服務，減少攻擊表面
  - 關閉不必要的網路埠口 (避免駭客入侵)
  - 限制管理權限 (避免員工下載惡意軟體)
  - 定期更新系統與應用程式 (修補安全漏洞)
- **建立緊急應變團隊 (CERT - Computer Emergency Response Team / CSIRT - Computer Security Incident Response Team)**
- **反惡意軟體解決方案 Anti-Malware Products and Services**
  - 防毒軟體是資安的基本要求，只要有兩種偵測方式，都有各自的挑戰
  - **檔案簽名 (Signature) 資料庫**：必須即時更新，否則無法偵測新型病毒
  - **異常偵測 (Anomaly Detection)**：需了解「正常行為」才能發現異常，設定不當可能影響業務運作
- **進階惡意軟體分析技術**
  - **沙箱技術 Sandboxing**：隔離測試環境，可以讓企業安全執行不明程式，觀察其行為。
  - **互動行為測試 Interactive Behavioral Testing**：模擬駭客行為，讓安全人員與惡意軟體互動，觀察它的反應。

ISC2

## 社交工程



- 網路釣魚攻擊 **Phishing** 🎯
  - 簡訊釣魚 (**Smishing**)：透過 SMS 簡訊 進行詐騙，例如通知你「帳戶異常」，引導你點擊惡意連結。
  - 語音釣魚 (**Vishing**)：透過 電話詐騙，假裝是銀行客服或技術支援人員，要求提供個資或金融資料。
  - 標槍式釣魚 (**Spear Phishing**)：專門針對特定個人發動攻擊，郵件內容可能包含你的姓名、職位，讓它看起來更可信。
  - 捕鯨攻擊 (**Whaling**)：專門針對企業高層 (如 CEO、財務長) 進行詐騙，例如假裝成公司老闆要求財務部門匯款給「供應商」，導致企業損失巨額資金。
- 忽嚇軟體 **Scareware** 😱：製造假警報，讓受害者恐慌
  - 假冒防毒軟體：彈出警告視窗，告訴你「電腦中毒，請立即購買防毒軟體！」
  - 假冒政府機構：通知你「違反法律，必須立即繳交罰款」，否則將採取法律行動。
- 低技術蒐集資訊 **Low-Tech Reconnaissance**：攻擊者可能不直接入侵電腦，而是透過公開資訊蒐集資料，以便日後攻擊
  - 搜尋引擎 (**Google Hacking**)
  - 垃圾桶潛水 (**Dumpster Diving**)
  - 肩窺攻擊 (**Shoulder Surfing**)
  - 假裝技術支援 (**Phone Pretexting**)
- 刷卡盜刷攻擊 **Swiping Attacks**
  - 安裝隱藏攝影機：監視 ATM 使用者輸入密碼
  - RFID 盜刷：利用無線讀取器，在受害者不知情的情況下讀取感應式信用卡資訊
  - 假讀卡機：在 ATM 或 POS 機上安裝假的刷卡裝置，當受害者刷卡時，卡片資訊就會被記錄下來

ISC2

## 行為分析 Behavior Analytics



- 使用者與實體行為分析 (**User and Entity Behavior Analytics, UEBA**)：一種資安技術，可以監控使用者、設備或系統的行為，偵測異常活動。
- 行為封鎖軟體 **Behavior-Blocking Software** (或稱 **Behavior Blocker**)：透過即時監控應用程式行為，在其執行時判斷是否有惡意行為，並立即攔截。*(UEBA 的 IPS 版本)*
- 優點：
  - 能即時攔截可疑行為，即使病毒變形，也能偵測並封鎖其攻擊
- 缺點：
  - 惡意程式必須先執行，才能被偵測到，這代表它可能已經對系統造成部分影響
  - 有些惡意程式會先進行無害的行為 (如重新排列檔案)，再進行攻擊，這可能會導致部分檔案遺失

ISC2

## SCADA 監控與資料採集系統



- 控制伺服器 Control server**：裝有控制軟體，負責指揮網路中的設備，如開關或控制器。
- 遠端終端單元 (Remote terminal unit, RTU)**：支援遠端站點，通常有無線電功能，適合用在沒有地面通訊的地方。
- 人機介面 (Human-Machine Interface, HMI)**：讓操作員監控和控制系統的介面。
- 可程式邏輯控制器 (Programmable logic controller, PLC)**：一台小型電腦，用來控制開關、計數器等裝置。
- 智慧電子設備 (Intelligent electronic device, IED)**：負責感測資料並提供反饋，實現自動控制。(圖裡面的 Sensor)
- 輸入/輸出伺服器 (Input/Output (IO) server)**：收集各種設備的資訊，連接控制伺服器和其他組件。
- 歷史資料記錄器 (Data historian)**：像是一個資料庫，記錄所有設備的運作資訊

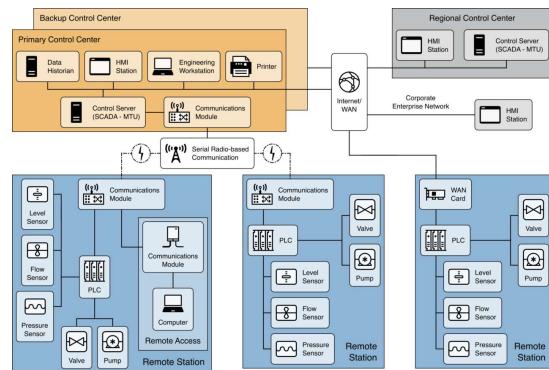


Figure 1: A comprehensive SCADA system implementation example (source: Draft NIST SP 800-82r3, Guide to Operational Technology (OT) Security)

ISC2

## Host-based vs. Cloud-based firewall



比較項目	主機型防火牆 (Host-Based Firewalls)	雲端安全群組 (Cloud-Based Security Groups)
運作位置	在主機的作業系統內運作，直接保護單台設備	在虛擬網路介面運作，像是一個雲端防火牆
功能	防止未經授權的進出連線，根據 IP 位址和端口設定規則	也是一種防火牆，但有「狀態記憶」 (stateful)，能記住連線狀態，規則不依賴作業系統
用途	保護單台主機(無論在地端或雲端)，適合用來實現「零信任」架構，減少惡意軟體擴散範圍	用來區隔(微分割)雲端的區域網路，保護整個虛擬網路環境
管理難度	管理比較麻煩，需要集中式管理系統來制定和執行規則	管理較簡單，規則統一設定，不用管主機的作業系統
與其他系統的整合	常與主機型入侵防禦系統 (HIPS)整合使用	獨立運作，專注於虛擬網路層的保護

ISC2

## 管理行動裝置



### • 行動裝置使用方法

- 本公司擁有、個人支援 (COPE)：本公司提供工作設備，但允許部分設備用於個人用途。
- 自帶裝置 (BYOD)：員工使用個人設備進行工作。
- 公司所有、僅限商業 (COBO)：本公司僅提供工作用的設備。
- 選擇您自己的設備 (CYOD)：員工從公司批准的設備中進行選擇。

### • 行動裝置管理 (MDM) 解決方案

- 有效地解決技術問題。
- 管理和分發應用程式。
- 執行安全政策。
- 設備加密。
- 密碼要求。
- 遠端擦除功能。
- 保護敏感資料並降低安全風險。

### • 行動應用程式管理 (MAM)：

- 控制載入哪些應用程式、資料存取以及端點上的功能。
- 標準化應用程式配置。
- 監控應用程式的使用情況和效能。
- 推送服務和應用程式級存取控制。
- 應用程式包裝：將應用程式容器化以供動態使用。

ISC2

## 雲端543



### 五個特徵

- Broad Network Access 廣泛的網路存取**：只要有網際網路，無論何種連線類型、設備型態都可以存取雲端服務。
- Rapid Elasticity 快速彈性**：根據需求獲取和釋放資源（如儲存空間、算力）的能力。
- Resource Pooling 資源池化**：根據工作負載需求，將資源集中並跨多個客戶共享。
- Measured Service 計量服務**：資源的使用情況可以被監控、控制、匯報，對供應商與使用者而言都如同使用水電服務一樣透明化。
- On-Demand Self-Service 按需自助服務**：使用者可隨時隨地按需獲取雲端資源。

### 四種佈署模式

- Public**: 公共雲是任何人（公眾）都可以使用的雲服務。雲服務供應商（CSP）擁有並運營可供公眾使用的雲基礎設施。
- Private**: 私有雲是為特定實體設置的專有網路或資料中心。
- Community**: 為具有共同利益或合規需求的群體共享基礎設施。（ex. Apple App Store）
- Hybrid**: 公共雲、私有雲和社群雲的組合。

ISC2

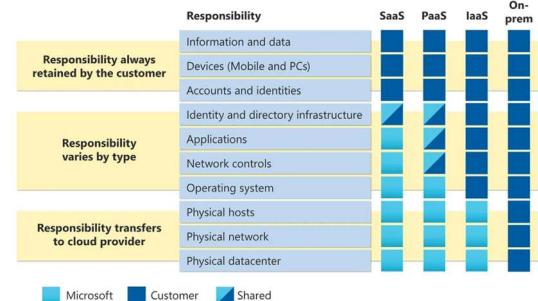
# 雲端543



## 三種服務模型

1. **SaaS 軟體即服務**：存取由供應商或 CSP 托管的軟體應用程式，如 Gmail、OneDrive
2. **PaaS 平台即服務**：租用硬體、作業系統、儲存和網路容量來構建和營運軟體，如 Azure SQL Database
3. **IaaS 基礎設施即服務**：租用如硬體、伺服器和網路元件等設備，如 VM

## Shared Responsibility



ISC2

## 資料分散與雲端資料外洩防護 Cloud Storage: Data Dispersion and Data Loss Prevention



### 資料分散技術 Data Dispersion Techniques

- 確保雲端資料的高可用性、性能，將資料分割成位元組寫到不同的實體儲存容器中
- 採用抹除碼 (Erasure Coding) 技術，將資料切碎再加一些備用碎片，即使有些碎片遺失了，還是可以用剩下的碎片把資料還原回來。每段碎片還會再經過加密，所以可以確保機密性、完整性和可用性。

### 雲端 DLP 技術 Cloud-Based Data Loss Prevention

- 資料在不同位置、資料中心和備份之間的移動和複製
- 只能使用雲端 DLP 進行資料移動管控

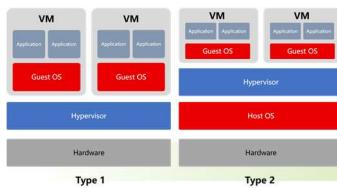
ISC2

# 虛擬平台的類型



## 虛擬機

- Type-1 Hypervisor (Bare-metal): (**攻擊面較少更安全**)
  - 直接運行在硬體上。
  - 高效能、低延遲。
  - 支援多個 VM 運行不同 OS。
- Type-2 Hypervisor (Hosted):
  - 運行在主機作業系統 (Host OS) 之上。
  - 較容易於安裝和管理。
  - 效能可能受主機 OS 影響。



## 虛擬化與容器化

特性	虛擬化	容器化
作業系統	每個虛擬機器有獨立的作業系統	所有容器共享主機作業系統核心
資源消耗	較高	較低
啟動時間	較慢	較快
隔離性	較強	較弱 (在作業系統層級隔離)
可攜性	良好	極佳
檔案大小	較大	較小
效能	接近原生系統，但仍有虛擬化開銷	更接近原生系統，效能開銷更小