《資通安全防護技術》

一、請說明五個使用於電子郵件安全的相關技術，以及各技術的功能。（25分）

試題評析	1.依題意判斷，此題在測驗考生是否熟悉電子郵件相關的防護機制，所以答題重點在「防護技術」，可能會有部分考生往「社交工程防範」方面回答，就可能答非所問，因為社交工程防範大多為認知素養，與防護技術並無密切關係。 2.有考生可能會將Email DLP（Data Loss Prevention，資料防外洩）寫進去，雖然亦屬電子郵件安全，但因為DLP的重點在於「內對外」傳輸的資料保護，筆者認為，此題若往「外對內」收件有關的電子郵件安全來作答，相對會比較保險。 3.儘管題目只要求5個技術，但對此類「敘述過於簡短」的題目都要料敵從寬，因為題幹鋪陳太少，需花更多時間揣摩題意，很難確認寫出的答案是否符合出題者期望，只要時間夠，對此領域觀念有足夠把握，筆者認為多寫沒壞處。
考點命中	《高點・高上資通安全防護技術講義》第一回，金乃傑編撰，頁104~109密碼學的整合應用。

答：

(一)SPF（Sender Policy Framework，寄件者政策框架）

透過DNS驗證寄件者身分的技術。網域擁有者可在其DNS記錄中新增一筆SPF的TXT紀錄，用來列出哪些郵件伺服器（Mail Server）是被授權可以代表該網域寄送郵件的。當收件端郵件伺服器收到來自某個網域的郵件時，會查詢該網域的SPF紀錄並比對實際的發信伺服器IP是否被授權，若未通過驗證則可能拒收或標示為可疑，可有效防範發信者位址偽冒的行為。

(二)DKIM（DomainKeys Identified Mail，網域金鑰認證郵件）

用於驗證郵件在傳送過程中是否被竄改，並確認發信者的真實性。發信端的郵件伺服器會利用私鑰（Private Key）對郵件中的特定標頭（Header）與內容（Body）進行加密簽章，接著將簽章附加於郵件標頭中。收件端則透過DNS查詢該發信網域所公布的公鑰（Public Key），以驗證簽章是否正確無誤，若驗證失敗，表示郵件可能遭到竄改或偽冒。

(三)DMARC（Domain-based Message Authentication, Reporting & Conformance，基於網域的郵件驗證、回報與一致性政策）

建構於SPF與DKIM之上的驗證政策框架，目的是提供郵件擁有者控制未通過驗證郵件的處置方式。管理者可在DNS中設置DMARC記錄，明確規定收件端若發現郵件未通過SPF或DKIM驗證，應採取的行動（如拒收、隔離或觀察）。此外，DMARC支援回報機制，可將驗證結果報告寄送至指定的管理者信箱（透過mailto:格式），方便追蹤並分析濫用情形。

(四)惡意郵件掃描

現代的電子郵件閘道設備（Mail Gateway）或安全郵件系統通常具備惡意郵件掃描功能。系統會對進入的電子郵件進行深度檢查，包含掃描附件（Attachment）、標頭（Header）與內文（Body），藉由病毒特徵碼（Signature-based Detection）、URL過濾、規則比對等方式識別潛在的惡意檔案、勒索軟體或釣魚連結，並在郵件到達收件者之前予以阻擋或標示。

(五)郵件沙箱（Email Sandbox）

針對未知或零時差（Zero-day）威脅，部分安全郵件解決方案會使用沙箱（Sandbox）技術進行動態分析。系統會將可疑郵件的附件或內含的連結，在隔離的虛擬執行環境中進行開啟與模擬操作，觀察是否有異常行為（如存取系統資源、發起連線、下載可疑檔案等），以識別新型態或尚未被病毒碼收錄的惡意內容，有助於提前攔截針對性攻擊（如APT）或社交工程攻擊。

(六)PGP（Pretty Good Privacy，良好隱私保護機制）－加密與身分驗證技術

採非對稱加密（Asymmetric Encryption）機制，結合加密與數位簽章，可用於電子郵件的機密性與身分驗證。發信者可自行產生一對金鑰（公鑰與私鑰）並使用私鑰對郵件簽章，將公鑰夾帶於郵件中供收件者驗證簽章真偽。若收件者欲傳送加密郵件回覆，則可使用該公鑰加密內容，僅有原始發信者可利用其私鑰解密閱覽。

(七)S/MIME（Secure/ Multipurpose Internet Mail Extensions，安全多用途網際網路郵件延伸）

與PGP不同之處在於其透過公正第三方憑證機構（Certificate Authority, CA）所簽發的數位憑證來驗證身分，用戶需向CA申請憑證，系統自動於郵件簽章時附上憑證資訊，收件者可使用該憑證進行驗證。若收件者擁有對方的公鑰，也能進行加密回信。

【參考書目】
1.鳥哥，【mail server (MTA) 加上 SPF, DKIM, DMARC】，https://linux.vbird.org/events/email_spf_dkim_dmarc.php (2025.07.09)。
2.PAPAYA 電腦教室，【我的隱私將由我自己來守護！輕鬆加密你的檔案和訊息不讓外人窺探！】，https://www.youtube.com/watch?v=9kGw8CLwHPs (2025.07.09)。

3.粘添壽，【資訊與網路安全技術/ 9-4 Secure-MIME 安全郵件】，
https://www.tsnien.idv.tw/Security_WebBook/chap9/9-4%20Secure%20MIME%20%E5%AE%89%E5%85%A8%E9%83%B5%E4%BB%B6.html

二、請比較滲透測試、紅隊演練、BAS（Breach and Attack Simulation）三者的不同。（25分）

試題評析	1.題目舉了3種常見的攻擊型安全(Offensive Security)類型的資安評估方法，且題意已明確要求比較「不同」，「相同」之處一筆帶過即可。每個概念都要緊扣「不同」之處來敘述，如何在緊湊的時間下有脈絡地答出關鍵字，就顯得很重要。 2.筆者傾向在此提用敘述法，而非表格呈現，原因有二：其一，BAS跟另外兩者評估面向差異太大，較難找到可比較的屬性；其二，手寫考試畫表格非常花時間，若非比較屬性明確，比較能清晰描述觀念，否則會避免在有限的作答時間下，單一題投入太多作答時間（通常是在其他題目不寫的時候，才能分配出多餘的時間）。 3.因紅隊演練有部分概念會與滲透測試重疊，同質性較高，可先寫這兩者，並且把範圍較小的滲透測試放前面，再敘述更廣的紅隊演練，說明紅隊演練不同之處；BAS則獨立論述，並舉出其與前兩者屬於不同評估面向之處，此題難度會在於作答時間的掌握。
考點命中	《高點・高上資通安全防護技術講義》第二回，金乃傑編撰，頁108~113滲透測試。

答：

(一)滲透測試（Penetration Testing，PT）

1.目的：驗證已知（或潛在）弱點是否能被利用。

2.範圍：明確指定主機、系統或網段進行測試。

3.步驟概要：

(1)定義範圍與目標，雙方簽署授權與保密協議。

(2)情資收集（Reconnaissance）：針對選定之目標主機蒐集外部情報（如使用Nmap、Nessus、Metasploit、Shodan等工具），包括IP、服務Port、運行系統、版本、安裝軟體等，並依此資訊發現可利用（Exploitable）漏洞。

(3)漏洞利用（Exploitation）：嘗試進入主機 (Initail Access)並取得系統權限。

(4)若成功進入主機，便會插旗；若進一步提權，就會在更高權限，如root或System32等目錄插旗

(5)報告撰寫：包含弱點描述、利用方式、操作歷程、建議修補措施。

4.依受測方提供的受測系統的訊息量，分為白箱(全知)、灰箱(部分資訊)、黑箱(無知)。

5.頻率與對象：通常上線前執行，後面每年一次，且針對特定應用系統或伺服器。

(二)紅隊演練（Red Team Exercise）

1.目的：模擬真實攻擊者的行為，全面測試組織的偵測、防禦與應變機制。

2.範圍：可能涵蓋整體網路、人員、裝置與物理安全。

3.特性：

(1)手段廣泛，可包含無線電波偵測、社交工程、掉落隨身碟、人員滲透、門禁尾隨等。

(2)目的是挑戰安全機制，測試組織員工或藍隊能否即時察覺並反應。

(3)常使用模糊範圍的目標進行多階段攻擊（Multi-Stage Attack），複雜度較高，專案時間往往長達數月。

4.步驟概要：

(1)簽署之合約範圍較PT廣泛。

(2)情報蒐集（Open-source intelligence, OSINT）：相較於PT，紅隊是先從外部攻擊面分析，尋找入侵突破點，管理制度漏洞也可能成為破口。

(3)以成功存取系統內部資料為最終目標，中間手法常會與PT步驟(2)~(4)相同，但攻擊路徑與手段會更多元。

(4)最後與藍隊交叉檢討後，撰寫檢測報告。

5.頻率與對象：通常每年或重大活動前辦理一次，範圍涵蓋整體資訊資產。

(三)BAS（Breach and Attack Simulation）

1.目的：透過自動化腳本模擬攻擊者行為，驗證資安設備或政策之防護能力。

2.特性：

(1)可常態執行，具低風險、可重複、可量化之優勢。

(2)原則不會產生破壞性攻擊，但能模擬惡意活動（如內部橫向移動、漏洞利用、釣魚郵件點擊）。

(3)驗證EDR、防火牆、SIEM、WAF等設備之事件回饋。

3.流程概要：

(1)部署模擬攻擊平台。

(2)定期執行攻擊模組，例如：

①PowerShell無檔案攻擊。

②社交工程郵件模擬。

③網路滲透腳本等。

(3)對照MITRE ATT&CK框架，比對哪些手法已被偵測。

(4)生成可視化報告，供藍隊優化偵測規則。

4.頻率與對象：可以長期持續地針對資安設備作有效性評估。

(四)結論

1.PT適合於開發或部署階段，專注於技術弱點利用驗證。

2.紅隊演練為全面實戰模擬，能檢視組織成員整體安全意識與藍隊應變能力。

3.BAS則為日常健康檢查工具，能快速反饋現有資安設備或偵測規則的效能。

【參考書目】

1. Gartner Peer Insights，【What are Breach and Attack Simulation (BAS) Tools?】，https://www.gartner.com/reviews/market/breach-and-attack-simulation-bas-tools (2025.07.09)

2.數位發展部數位產業署「113 年第五次電腦軟體共同供應契約採購－資通安全服務暨資訊服務」(招標案號：1130205)採購規範（投標須知附件五）【第 4 組滲透測試服務】、【第 7 組紅隊演練服務 (113 年新增)】。

三、請說明以下的經典資安攻擊的實行方法，並舉例攻擊成功後可達到的效果。（25分）

(一)路徑遍歷（Path Traversal）攻擊（5分）

(二)跨站腳本攻擊（XSS）（10分）

(三)越界讀取（Out-of-bounds Read）攻擊（10分）

試題評析	1.名詞解釋題純測記憶，對多數考生較陌生的名詞可能是「越界讀取」，因為現在普遍在用JAVA、Python、GO此類有防呆機制的程式語言。其餘兩者都是考試常客，若真忘記或不會寫，也不要留白，或許能有同情分。 2.此3個小題純考技術名詞，所以可像「程式語言」或「資料結構」考科一樣，簡要地把做法、發生原因跟效果寫出來即可，不必花太多時間著墨在文字敘述，把時間留給解釋名詞或概念更廣的題目，例如：第四題這種大哉問。 3.此題難度會在需具體描述技術實作。另外，題目雖然沒問，但如果時間充裕，可補充緩解方法。筆者個人認為，第二、四題若要寫出保險的答案，需分配較多作答時間（簡單來說，寫得少就不容易拿高分的題型），像第三題因為答案明確，給分較無彈性，縱使多寫，也未必吃香。
考點命中	《高點・高上資通安全防護技術講義》第二回，金乃傑編撰，頁7~9 OWASP。

答：

(一)路徑遍歷（Path Traversal）

1.實施方法

路徑遍歷是一種Web應用程式漏洞，當使用者提供的路徑參數未被妥善過濾或限制，攻擊者可以使用相對路徑（如 ../）來存取伺服器上原本無權限訪問的檔案。

2.範例

(1)原本正常請求：

```
https://abc.com/search
```

(2)攻擊者輸入：

```
https://abc.com/search?file=../../../log.txt
```

(3)若伺服器未過濾 ..等字符，就可能讀取到 /etc/passwd 等敏感檔案。

3.竊取伺服器上敏感檔案，如：記錄檔（log.txt）、憑證檔案（private.key）或配置檔（config.php），在部分情境下，可能進一步導致遠端程式碼執行（RCE）。

4.進階手法

(1)URL編碼繞過：%2e%2e

(2)雙重編碼繞過：%252e%252e

(二)跨站腳本攻擊（Cross-Site Scripting, XSS）

1.實施方法

XSS是當應用程式未妥善處理使用者輸入，使惡意腳本（通常為JavaScript）被注入並於其他使用者瀏覽器中執行。攻擊者可藉此竊取使用者資料、操控DOM、導致跳轉等。

2.三種類型

(1)反射式XSS（暫時型XSS）

■攻擊內容嵌入於URL或表單中，立即反映回瀏覽器執行。

■範例：

```
https://abc.com/login?username=<script>alert(1)</script>
```

(2)儲存式XSS（永久型XSS）

上述腳本若放在可長期儲存的網頁上，例如：留言板，便會使每個開啟頁面的使用者瀏覽器都會執行腳本，便可能將瀏覽器機敏資訊傳給攻擊者。

(3)DOM-based XSS

攻擊內容不經由伺服器處理，而是由客戶端瀏覽器JavaScript處理後插入網頁。將腳本植入含有JS腳本的DOM File可操控的輸入點中，如URL hash(#後的Payload)，例如：

```
https://abc.com/#<script>alert(1)</script>
```

(4)攻擊效果

■竊取使用者Cookie或Token。

■操控DOM介面。

■建立瀏覽器後門（如與攻擊者C2連線）。

(三)越界讀取（Out-of-bounds Read）

1.實施方法

此為記憶體處理錯誤所導致的漏洞，常發生在程式存取陣列、緩衝區（Buffer）等記憶體位址時未檢查邊界長度，導致可能會讀到非預期的敏感資料。

2.範例：預設不檢查邊界的C語言

```
int Arr[2];       //宣告Arr陣列長度為2，在Arr[0]、Arr[1]配記憶體位址。
int x = Arr[4];   //宣告x變數存放Arr[4]位址的值，超過原陣列地址，以致讀到非上述範圍的值。
```

3.攻擊效果：未經授權而能存取記憶體資料（如其他使用者憑證），提供了後續攻擊路徑。

【參考書目】
1.OWASP，【Path Traversal】，https://owasp.org/www-community/attacks/Path_Traversal (2025.07.09)
2.OWASP，【Cross Site Scripting (XSS)】，https://owasp.org/www-community/attacks/xss/ (2025.07.09)
3.DEVCORE，【OpenSSL CVE-2014-0160 Heartbleed 嚴重漏洞】，https://devco.re/blog/2014/04/09/openssl-heartbleed-CVE-2014-0160/ (2025.07.09)。

四、請就一般機構內的EDR（Endpoint Detection & Response）軟體、防毒軟體與WAF（Web Application Firewall）三者在核心功能、主動防禦、與SIEM（Security Information and Event Management）軟體的整合程度三個面向進行比較。（25分）

試題評析	1.此題在題幹敘述上過於簡短，不僅測驗考生較為陌生EDR和WAF功能，另外還要思考題意所謂「主動防禦」所指為何？MITRE Engage框架？顯然這3種資安系統與此概念毫無關係，因為都是攻擊者先有行為，才會觸發後續紀錄與反應，市面大多數資安防護系統均為被動防禦（Passive Defense），我們只能合理推測題目可能指「積極式防禦」（Proactive Defense），這時焦點就可能回到EDR跟WAF身上。 2.「與SIEM整合程度」也令人費解，究竟是指通訊串接？還是資料儲存？又或是事件查詢方式？當然，最保險的做法就是全都寫，但不同SIEM平台的原始資料保存、支援格式和欄位對應、資料結構到查詢語法差異不小，其整合程度也常跟EDR、WAF廠牌相關，恐難在30分鐘內作答完畢！ 3.筆者認為本題測驗這3種產品在業界定位與概念都已相當清晰，但難度會在於需要高度仰賴實務導入經驗，還有題意較難以摸透，考生只能盡力回答，寫越多越安全。 4.本題明確指出需比較的3個屬性，故答題方式用表格呈現就非常合適。
考點命中	《高點・高上資通安全防護技術講義》第二回，金乃傑編撰，頁60、79~80進階防火牆、監控防護體。

答：

	EDR	防毒軟體(AV)	WAF
核心功能	①詳細記載端點各種操作紀錄，並將其關聯後，能分析行為模式，針對異常行為發出告警，藉此察覺惡意程式活動。 ②能分析行為模式，回溯查詢與阻擋惡意行為（例如：勒索軟	①針對比對到惡意特徵（signature-based）之程式，例如：病毒、木馬，做出中斷、隔離或清除等行動，能快速自動阻斷高風險程式運行。 ②現代防毒也開始加入機器學習	①監控並攔阻網頁應用程式異常操作行為，例如：SQL Injection、XSS、CSRF 等，彌補 IPS/IDS 之不足。 ②網路防護（攔阻）

	體），並針對異常行為發出告警，藉此察覺惡意程式活動。 ③主機防護（偵測）	與啟發式分析。 ③主機防護（攔阻）	
主動防禦	①透過大量蒐集各種細碎的行為紀錄，可拼湊出長時間活動關聯事件，即威脅狩獵(Threat Hunting)或主動調查，可及早察覺 APT 事件。 ②可結合 MITRE ATT&CK 框架辨識攻擊手法與階段。 ③主動防禦能力強於防毒軟體，但需仰賴具備行為分析能力團隊，難以自動化。	①傳統 AV 只能針對已知之惡意特徵進行攔阻，仰賴定義檔更新，偏向被動式偵測與阻擋。 ②現代進階 AV 已能動態分析程式在記憶體活動，自動預先攔阻未知威脅，但效果有限，有一定誤判率。對未知攻擊與多階段攻擊應變效果不如 EDR。	透過原廠預設規則與管理員自定義特徵分析，可針對攻擊手法變化較大的應用層服務察覺異常操作，現在 WAF 產品也有引進 ML 分析高風險威脅。
與 SIEM 整合度	①EDR 行為紀錄非常繁瑣，雜訊量龐大，不宜將所有紀錄傳送到 SIEM(可能會占用授權)，而是應將觸發高風險或可疑行為這類經過過濾的行為送至 SIEM。 ②整合度高，但需做好事件分類與去雜訊，並將其複雜的欄位對應到平台。	AV 因為告警識別度與可信度高，欄位相對不多，大多 SIEM 現有欄位均能對應到告警事件欄位，故可直接傳送至 SIEM，整合度最高。	①不同廠牌的 WAF 事件欄位差異大，呈現方式也不同，若要整合進 SIEM，建議投入成本在 SIEM 客製欄位與剖析資料。 ②專注於應用層流量防禦，與端點不同層級，整合 SIEM 難度取決於部署方式與廠牌。

此外，與SIEM整合需依資安事件調查需求，綜合評估哪些Log要傳送、Log哪些欄位要紀錄，及如何標準化Log的資料供SIEM調查、標準化後又要如何關聯其他資安設備的Log。

【參考書目】
1.ATT&CK Matrix for Enterprise，https://attack.mitre.org/ (2025.07.09)
2.Paloalto Network，【What Is an Endpoint Protection Platform?】，https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint-protection-platform-epp (2025.07.09，筆者備註: 防毒會被歸類為 EPP 的一部分，本篇說明 EPP 與 EDR 的差異與關係)
3.Google Cloud，【收集 General Dynamics Fidelis XPS 記錄】，https://cloud.google.com/chronicle/docs/ingestion/default-parsers/F5-asm?hl=zh-tw (2025.07.09，筆者備註：本篇演示的 F5 WAF 如何整合 Google SIEM 平台，左側選單也有各種資安產品整合進 GSO 標準化的具體操作，進而瞭解實務上 SIEM 如何實作資安事件整合平台，又能做到何種程度。)

高點・高上公職

考取學長姊大推的優秀師資

資料結構

王致強(蕭立人)

- 獨創「程式碼記憶法」，大幅縮短記憶　和答題的時間！
- 教學採考題導向，範圍由淺入深，即使是底子不好，也能茅塞頓開！

廖○成(高大資管畢)

應屆考取　113高考資訊處理

資料結構要掌握這門科目對我來說非常不容易，**不過王致強老師教得非常好**，教學中有時候連比國考難的研究所考題都會提點，也讓大家能夠掌握國考所需再更以上的資料結構實力，我覺得非常不錯！

資通安全

金乃傑(魏取向)

- 以「學習地圖」概念展現資訊管理多構面的知識，並引入自創圖示標記知識所在位置及相連概念；輔以口訣背誦關鍵名詞、要點。

蔡○諺(中興應數畢)

跨域考取

113高考資訊處理【狀元】

題庫班專注於實戰演練，通過不斷作題，能更快適應考試題型，並且針對薄弱環節進行強化。**金乃傑老師在今年考試中預測的範圍非常準確**，特別是在加密演算法與資料保護法規的部分，考題幾乎全中。

資訊管理

蕭維文

- 具有產業與學術經驗，從不同角度提供最客觀的科技觀點。
- 時事與理論精準結合科技產業，透過精闢分析讓同學理解資訊界。

李○翌(北市大資科畢)

應屆考取

113高考資訊處理、普考資訊處理

資訊管理這科廣到沒有範圍，如果有寫考古題就會發現講義是由各種考古題的解答堆疊出來的，因此**蕭維文老師的魚骨解答法就顯得非常重要**，只需把改卷教授想要的關鍵字搭配以上的方法就可以把答案湊出來。

更多命中實證

更多上榜經驗分享

考點命中實證

《資料結構》

一、某一公司有下圖所示的8個優先順序分別為高或低的待執行工作，且將依順序自A至H每間隔一天的時間放入對應的高優先執行佇列（Qucue）或低優先執行佇列（Qucue），例如A（低）表示A工作排於第一天放入低優先執行佇列，而C（高）表示C工作排於第三天放入高優先執行佇列。此外，執行每個工作所需完成的時間均於工行名稱下顯示，例如執行A工作需要2天時間完成，而執行B工作需要1天時間完成。最後，各個工作的執行規則為，當高優先執行佇列內有工作待完成時，須優先執行該佇列內的工作（由第一個開始執行），直到高優先執行佇列內沒有任何待完成工作時，才可執行低優先執行佇列內的工作（由第一個開始執行）。

自A至H每間隔一天的時間放入對應的高優先佇列或低優先佇列

H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
1	2	1	1	2	2	1	2

（一）試計算執行此8個工作需要多少天方可完成。（10分）

（二）試計算此8個工作自放入佇列至開始執行的平均等待時間。（15分）

試題評析　佇列相關的基本應用問題，題目本身十分平易。在題意確實掌握的狀況下，正常操作佇列，計算正確時間，取分不難。

考點命中　《資料結構》，高點文化出版，王致強編著，頁4-16～4-17。

答：

（一）總共需要12天可以完成8個工作，如下圖：（灰底為執行中工作，括號為工作剩餘天數）

天數	12	11	10	9	8	7	6	5	4	3	2	1
到達工作					H（低）	G（高）	F（高）	E（低）	D（高）	C（高）	B（低）	A（低）
所需天數					1	2	1	1	2	2	1	2
高優先佇列				G(1)	G(2)	G(2)E(1)	F(1)D(1)	D(2)	D(2)C(1)	C(2)		-
低優先佇列	H(1)	H(1)E(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	H(1)E(1)B(1)	E(1)B(1)	E(1)B(1)	E(1)B(1)	B(1)	B(1)	B(1)A(1)	A(2)

（二）各項工作等待時間如下表：

工作	H	G	F	E	D	C	B	A
等待時間	4天	1天	1天	6天	1天	0天	8天	0天

《資通網路與安全》

五、防火牆（Firewall）是當今企業常見的安全防護設備，請問：

（一）企業常用防火牆隔離出一個網段，稱為DMZ（Demilitarized Zone），請詳細說明其用意為何。（5分）

（二）WAF（Web Applicatiou Firewall）和傳統的封包過濾式防火牆（Packet filtered Firewall）有何不同？請詳細說明。（10分）

（三）防火牆常根據從外部收到的IOC（Indicator of Compromise）來做規則調整，請問IOC的意義為何？（5分）

試題評析　本題為資訊安全之防火牆種類及安全網路架構之題型。

考點命中　《高點・高上資通安全講義》第二回，金乃傑編撰，頁14～28，第三章防護架構，二、防火牆（Firewall）與相關技術。

答：

（一）DMZ（Demilitarized zone）是介於內外路由器間的區域，用於放置組織對外重要的伺服器。DMZ 照字面直翻是指非軍事區域，而電腦網路中 DMZ 可以解析為一個既不屬於內部網域同時也不屬於外部網域的一個特殊區域，其目的就是了為防止外來人侵者直接存取內部機密資料，針對不同資源而提供不同安全級別的保護區域。一般企業將網路伺服器放在 DMZ 供網際網路使用者查詢使用，這些伺服器無法連接到內部資料，因此如果不幸被外來人侵者侵入，重要的資料仍不至於外洩。

（二）WAF（Web Application Firewall）提供應用層的訊息過濾與轉送處理，主要依據應用層的資訊來決定是否放行封包流量，與傳統的封包過濾式防火牆相較，WAF 可過濾傳送的資料內容與命令，確保應用層協定的安全；亦可過濾封包內容與命令，阻斷針對應用協定的攻擊。

（三）IOC 為電腦鑑識中的工具器物(Artifact)，其可從網路或作業系統中觀察，與電腦入侵高度相關。傳統的 IOC 包含病毒特徵、IP 位址、惡意檔案的 MD5 雜湊值，或是殭屍網路(Botnet)命令與控制伺服器的網址或網域名稱。通過事件回應與電腦鑑識的處理過程識別 IOC 後，其可用於入侵檢測系統(Intrusion Detection System, IDS)與防病毒軟體，對未來的攻擊嘗試進行早期檢測。