**資安防護計畫與作為**  
 **人員編組如下**：

1. 資訊安全官：由資訊課長擔任，負責管理及資訊安全的統合作業。
2. 執行小組：由公司資訊部人員擔任，負責執行資訊安全的相關作業。
3. 稽核人員：由各部門主管職人員負責稽核及驗證資訊安全的作業。
4. 公司成員：配合跟遵守資訊安全的各項作業要求。

依照經濟部「中小企業資通安全最佳要求與實務」要求標準的六大構面，對本公司的資訊安全系統進行評估，這六大構面包括：網路安全、電腦安全、應用系統安全、人員安全、委外和資料安全等六大個層面，

| 名稱 | 要點 |
| --- | --- |
| 網路安全 | 網路資源管理、防火牆與特殊連線安全控制、以及無線上網等，主要以強化企業內部網路基礎建設及網路服務之保護措施，提升網路資料傳輸安全、降低弱點，減少系統受到網路攻擊之傷害。 |
| 電腦安全 | 各式電腦（含伺服器及個人電腦、筆記型電腦、行動裝置等）系統與設備的保護、防毒軟體、存取安全、以及帳號/密碼的管理等，主要針對電腦系統進行安全保護措施，提高系統運作穩定性與持續可用能力並減少被攻擊的機會。 |
| 應用系統管理 | 本部分包含電子郵件、即時通訊軟體、資料備份、以及異常事件處理程序等部分，其主要針對企業日常運作之應用系統使用安全，降低不當操作所造成的傷害，並且提升在事件發生時的應變與處理能力。 |
| 人員安全 | 本部分包含人員安全管理、認知教育與事件通報等，其主要目的為提升企業內部人員之安全意識，以及對於資安危機的瞭解，將有助於降低因安全意識不足所造成資安事件發生的機會。 |

| 委外 | 本部分主要說明委外之管理，主要為降低因委外所造成資安問題發生的機會。 |
| --- | --- |

葳錦網路資訊現況問題如下：

1. 加密管理、身分識別管理薄弱
2. 內網未做區段隔離
3. 郵件安全防護薄弱
4. 權限管理機制薄弱
5. 未完善資料存取、備援、備份管理機制
6. 系統可用性保護需加強
7. 未有完善定期資安教育訓練與社交演練

**(一)解析成因**

1. **對外資安防護薄弱**  
   * 現有防火牆，無啟動加密憑證(SSL)管理。
   * 無WAF功能，針對一些無法即時更新之操作系統，駭客容易透由這漏洞進行滲透、攻擊。
   * 沒有定期進行網路與主機弱點掃描，可能會有資安潛藏的風險。
   * 目前沒有對使用者身分做認證識別，且沒有相關記錄存檔，容易在資安事件發生時無歷史資料查證。
2. **內網未做區段隔離**  
   * 部門彼此之間是否做好不同區段的隔離，而且所有的流量傳遞是否都會經過檢查(例如：病毒、IPS、Sandstorm機制偵測)。
   * 為葳錦資訊內網提供多重的檢哨站與管制站，以便於在不影響既有的網路架構下，讓所有流量的封包檢測能更深入檢析。
   * 當遭受攻擊時如何緊急應變：當萬一真的讓駭客滲透、攻擊到企業內網時，如何有效主動隔離攻擊來源，確保網路運作安全。
   * 內網風險來源可能來自有線網路使用者，也可能來自無線用戶，彼此之間如果能利用威脅情報相互協防，可以在發現受感染的使用者前，先做好智能管理將受駭者先隔離。
3. **郵件安全防護薄弱**  
   * 提升偵測能力，可以對未知進階惡意程式附檔進行過濾。
   * 郵件內容驗證、SPF、DKIM、DMARC。
   * 導入DLP稽核過濾。
   * 提升密碼強度限制、帳號登入安全。
   * 定期舉行社交工程演練服務。
4. **權限管理機制薄弱**  
   * 主機無進行身分識別權限管理。
   * 管理者密碼無定期更新且密碼強度太弱(建議英文字母、大小寫、數字混搭)。
   * 建議雙重認證機制，降低被盜用機會。
5. **未完善資料存取、備援、備份管理機制**  
   * USB儲存媒體沒有使用控管，企業存在資料外洩及電腦中毒風險高。
   * 沒有電腦操作使用紀錄，無法有效追朔資安事件歷程。
   * 沒有人員存取內外部系統及資料傳輸之紀錄。
   * 缺乏災難復原演練機制，當意外狀況發生時，可能造成企業復原速度慢，甚至系統資料無法救援問題。
6. **系統可用性保護需加強**  
   * 系統更新為被動式，無法有效即時修補漏洞。
   * 尚無導入虛擬化，機器設備過多造成管理不便、維護不易、占空間、耗電、增加維護成本…等等眾多缺點。
   * 機器設備過多，管理維護不易，當設備發生異常狀況時，無法即時處理，增加管理者維護負擔。
   * 僅ERP DB系統有備援HA機制，應用程式AP系統等備份週期及還原速度需要加強。
   * WEB系統沒有制定弱點偵測掃描機制，應用系統存在備攻擊的風險。
7. **未有完善定期資安教育訓練與社交演練**  
   * 因為預算限制或人力資源不足，無法提供定期的資安教育訓練和社交演練，這可能會導致組織無法有效地提升員工的安全意識和溝通能 力。
   * 單位可能未能充分認識到資安教育訓練和社交演練的重要性，認為這些活動對於組織的安全性和運營並不至關重要，因此忽略了相關的培訓。
   * 很難安排定期的資安教育訓練和演練，因為這需要員工投入時間並可能影響日常業務運營。
   * 缺乏相關技術和基礎設施，可能難以實施有效的線上資安教育和社交演練。這可能涉及到教育平台的建立、遠程培訓的組織等問題。
   * 單位不了解如何設計和實施有效的資安教育訓練和社交演練計劃，缺乏相關知識和專業知識可能成為一個障礙。

**(二)葳錦資訊資安建置規劃如下：**

1. 分部分段進行網路切割與控管，確保各區各層對外資訊流等安全防護。
2. 對外防火牆與內部網段防護，對ICS 實體存取、各區各層對外資訊流安全防護。
3. 強化內網零信任機制，提高使用者身分識別(結合多因子認證)，遠端存取管制、存取權限、應用程式使用服務限制及漏洞修補等安全防護。
4. 入侵偵測、惡意程式防護及系統監控等安全防護 。
5. 系統虛擬化，提供高可用備份備援機制及災難復原演練計畫。
6. 實施方法，資安能量登錄廠商進行建置之作法與服務驗證之規劃。
7. 進行系統建置之作法： 依據先期概念驗證(POC)之成果，展開系統建置細節、提出專案管理流程等。
8. 資訊安全組織：指派公司之專責人員負責資訊安全計畫、執行、查核及改善，並由管理階層指派高階人員負責協調專案資源。

針對「資訊安全系統建置」部分，將協助葳錦資訊建立設備端遠控連線的資訊安全防護及辨公室資通設備監診及安全防護，預計針對葳錦資訊的資安防護建構分為 5 大領域，分別建置規劃如下:  
  
**資通安全檢測項目**

* 網路架構檢視
* 網路惡意活動檢視
* 使用者端電腦惡意活動檢視
* 全伺服器主機惡意活動檢視
* 防火牆連線設定檢視

**D1.** 對外防火牆與內部網段防護，且對 **ICS** 實體存取、各區各層對外資訊流等安全防護：

1. **由外對內之資料流**

採用 2台資安設備進行雙機備援機制。主要防護有：IPS、NGFW、APT、SPI、DPI、防毒、垃圾郵件過濾、入侵偵測、SSL內容解析與阻擋、網頁應用程式防火牆等。 企業內部各區各層對外資訊流皆有防火牆防護，加強防護駭客、木馬及病毒入侵。

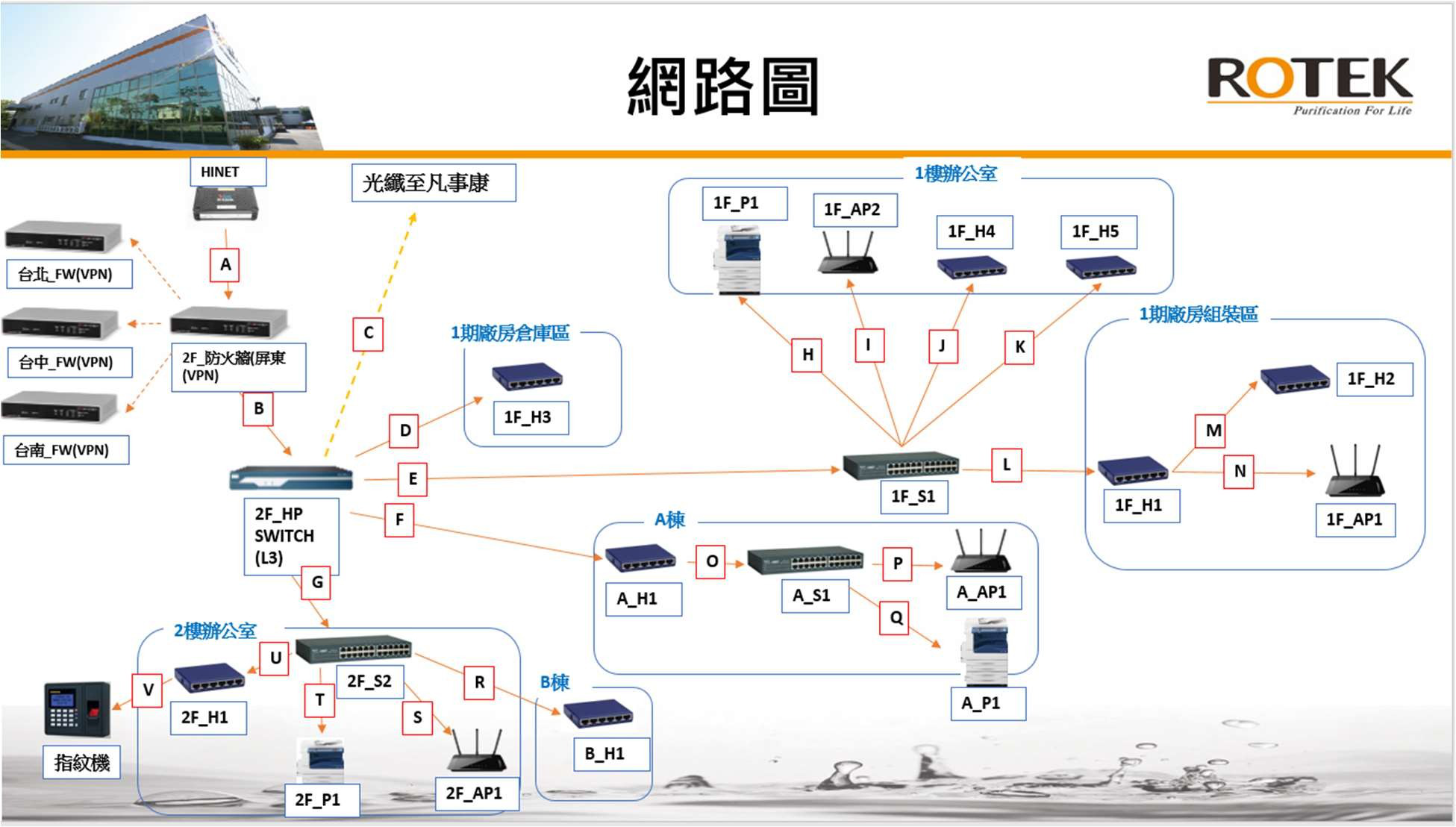


圖 1-2 葳錦資訊網路規劃架構圖

1. **將廠區(OT)網路安全區域獨立隔離**

透過對工業控制網路安全區域進行隔離防護。葳錦資訊應根據實際的情況，在不同網路邊界間或者各操作機台部署邊界安全閘道(圖 1-3)， 實現安全的訪問控制、阻隔非法的網路連線，嚴格禁止沒有防護的工業控制網路與網際網路相連接。此外，也可以利用虛擬區域隔離、埠禁用的安全配置強化內網的安全。

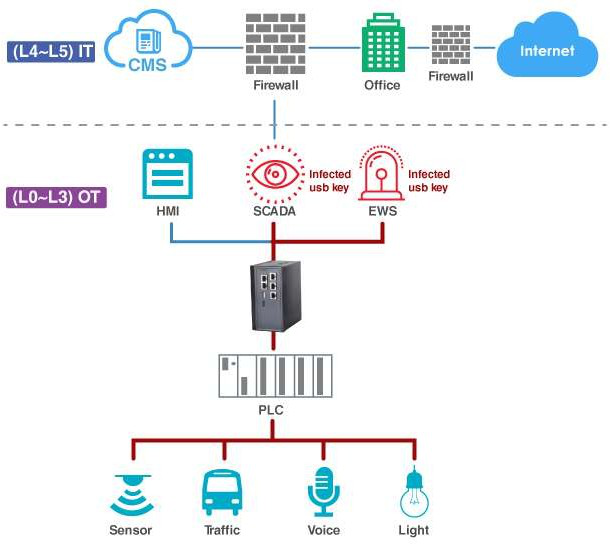


圖 1-3 OT 場域資安防護示意圖

1. **內網微區段隔離**  
   * 部門彼此之間是否做好不同區段的隔離，而且所有的流量傳遞是否都會經過檢查(例如：病毒、IPS、Sandstorm 機制偵測)。
   * 為葳錦資訊內網提供多重的檢哨站與管制站，以便於在不影響既有的網路架構下，讓所有流量的封包檢測能更深入檢析。
   * 當遭受攻擊時如何緊急應變：當萬一真的讓駭客滲透、攻擊到企業內網時，如何有效主動隔離攻擊來源，確保網路運作安全。
   * 內網風險來源可能來自有線網路使用者，也可能來自無線用戶，彼此之間如果能利用威脅情報相互協防，可以在發現受感染的使用者前，先做好智能管理將受駭者先隔離。
2. **權限管理機制薄弱**  
   * 主機無進行身分識別權限管理。
   * 管理者密碼無定期更新且密碼強度太弱。
   * 建議雙重認證機制，降低被盜用機會。
3. **電子郵件過濾系統檢測**

* 透過異常寄送偵測、SMTP 流量異常偵測等機制，過濾傳統防火牆無法攔截的大宗郵件攻擊、木馬程式&駭客攻擊等，並依據來源 IP 和寄件者進行封鎖，針對 SMTP(S)、POP3(S)、IMAP(S)等驗證執行攔截，阻止大量試圖破解帳密的情形發生。
* 專屬郵件安全簽章，讓收件者以信件中的連結與寄件者的郵件主機確認原始郵件內容，降低信件被竄改的風險；SPF 能抵擋非法主機偽造合法網域寄出的信件，過濾寄件者網域或來源 IP；DKIM 網域驗證使用數位簽章防止郵件內容遭到竄改；DMARC 架構則必須搭配SPF 或DKIM 驗證使用，幫助使用者處理未經驗證的信件。
* 資料外洩防護可針對內外郵件的表頭、主旨、信件內容、附件名稱和大小進行設定，對符合稽核條例的郵件實施隔離、刪除、發送通知信、抄送副本等動作。因應個人可識別資訊保護意識興起，個資法過濾功能可針對具有敏感個資郵件進行過濾稽核設定。
* 為防止員工圖方便設置過於簡單的密碼，管理介面中可指定密碼強度限制如須包含大寫英文、符號或長度須超過多少字元；再者，可在個人信箱設定介面中可開啟兩步驟驗證，即使密碼被盜竊，不管是透過Google Authenticator、LINE 綁定的個人行動裝置，或備用EMAIL 信箱都能及時告知並驗證，依然可確保帳戶安全性。

1. **強化資料安全傳輸與儲存**

**資料安全傳輸**

* + 使用加密協議：在資料傳輸過程中，使用安全的加密協議，如 TLS或SSL。
  + 數據加密：在傳輸前，對敏感數據進行加密處理。
  + 身份驗證和授權：在傳輸過程前，確保參與傳輸的雙方的身份驗證和授權。
  + 定期更新和修補：確保使用的傳輸協議、加密算法和安全措施始終是最新的版本，定期應用安全更新和修補程序。
  + 監控和日誌記錄：實施監控和日誌記錄機制，以追蹤數據傳輸的活動。
  + 備份和災難恢復：定期備份數據，以防止在傳輸過程中發生意外或故障。同時，建立恢復計劃，以便在發生數據傳輸中斷。

**資料安全儲存**

* 重要應用系統資料定期備份，包含系統設定及檔案資料。
* 定期進行備份資料復原之測試，以確保備份資料之有效性。
* 應用系統的重要資料維持兩套以上之備份。
* 重要機密資料，會將資料加密後進行備份，以降低備份資料遭盜用的可能

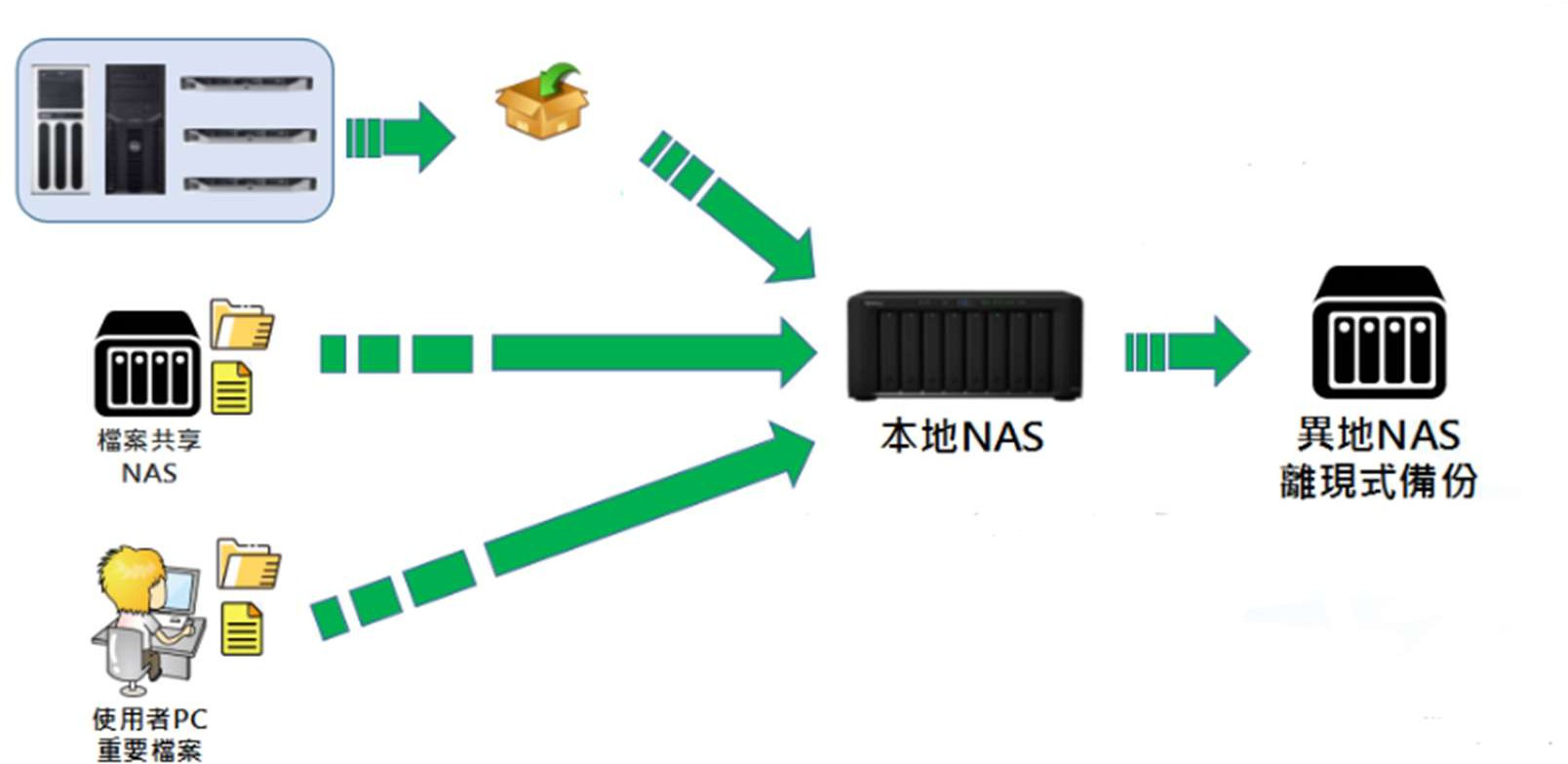


圖 1-5 資料備份儲存意境圖

**D3.對相關重要主機進行系統弱點掃描：**

1. **系統主機及網路弱點掃描**：

弱點掃描是抵擋駭客攻擊的基本功，盤點公司重要資產設備，並藉由弱點掃描查看是系統存在的弱點或是被植入木馬後才出現的弱點，並針對這一個弱點進行更新，對於具有高風險漏洞的電腦設備，有可以讓駭客透過這些弱點來進行攻擊或破壞設備的機會。

* **硬體弱點**

泛指網路設備在設計上的缺失或是韌體上的漏洞，可以讓駭客透過這些弱點來進行攻擊或破壞設備等。

* **軟體弱點**

泛指存在於作業系統或應用程式中的錯誤，可以讓駭客或蠕蟲對電腦進行入侵或取得資料。

* 1. 作業系統的弱點
  2. 應用程式的弱點
  3. TCP/IP 通訊協定的弱點
* **管理弱點**  
  1. 泛指管理上的疏失，導致被入侵或資料外洩。
  2. 系統設定錯誤
  3. 密碼過於簡單

1. **執行時機:**  
   * 建置時對全部連網環境做弱點掃描，並針對弱點掃描報告進行改善。
   * 設備加入時，需要提出弱點掃描的報告後才能進入網路。
   * 半年或一年執行一次弱點掃描的工作。
2. **弱點掃描:**  
   * 透過專業弱點掃描工具針對標的物進行檢測：  
     1. **主機弱掃工具：Nussus**為業界部署最廣泛的漏洞與系統設定評估產品。可進行高速探 索、系統設定稽核、資產剖析、敏感性資料探索、修補程式管理整合和漏洞分析。
     2. **網站弱掃工具：  
        OWASP Zed Attack Proxy**（簡稱 **ZAP**），於2010 年9 月從OWASP 開發，是一款測試網頁程式漏洞工具， 並設有簡單易用的介面。
   * 一次完整弱掃包含「初測+複測」

初測結束後會提供客戶弱點整理列表方便閱覽以及修復弱點建議。複測時間在初測結束後的三個月內執行，以確保弱點都已修補完成。

* 提供完整的弱掃相關建議與掃描報告用以記錄存檔

**D4.提高內網安全性**

內網威脅無所不在，像是我們常聽到的勒索軟體攻擊，可能就能讓企業造成巨大損害。其實最可怕的並不是已知的病毒，因為已知的病毒可以透過特徵碼的辨識過濾排除，未知的威脅才是最難預防的，因為它並無符合的特徵碼可以進行比對，讓駭客有機會滲入企業內網環境中，侵占重要的主機或伺服器。眾至內網防火牆，主要是提升內網偵測能力，除了具有傳統防火牆異常流量偵測功能外，更利用先進的內網防護技術-IPS、Sandstorm、WAF、Virus，四者共同運作強化內網安全防禦，可以有效降低駭客攻擊行為。

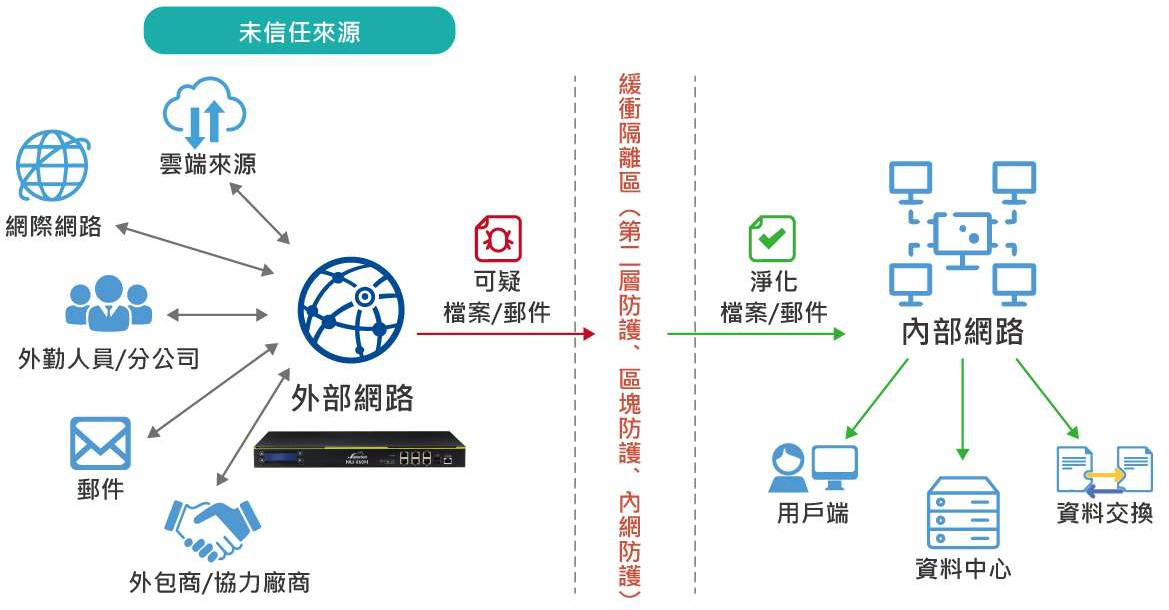


圖 1-6 內網非Zero Trust

* **多因子認證機制強化身分識別與存取限制**

疫情盛行時，多數企業為了維持穩定運作，大量開放使用者可透由SSL VPN 正常存取系統。因此，身分識別搭配多因子認證是現在SSL VPN 基本配備，透過第三方驗證碼增強保護性。除了身分驗證外，管理者並可依據使用者不同權限給予不同授權，例如來源IP、登入服務埠、時間管控、連線主機，在存取資源的規劃上，可透由眾至內網防火牆進行限制，讓用戶取得適當的權限。

* **同交換器、AP 協防，一起守護內網安全**

如果端點裝置被植入惡意程式或中毒，會透過內網滲透擷取未被授權的資源貨訊息，這些異常的行為會被眾至內網防火牆所偵測透過與交換器協防可發揮即時封阻效用，將未知的風險優先隔離並可封鎖該使用者的 IP、MAC。

此外，所有經由無線連線的封包亦會經過病毒特徵檢測、IPS 入侵偵測、SandStorm 偵測過濾，客戶不需要再另尋其他無線網安解決方案，即可落實有線與無線網路的整合控管與資安防禦。

* **特徵資料庫雙重更新機制(雲端或離線更新)**

欲確實防範已知型攻擊威脅，勢必得定期更新特徵碼資料庫，才能跟上惡意程式變種的風險。如果企業內網防護設備得以直接對外連線， 可與眾至雲端特徵值資料庫進行更新，倘若企業內網是封閉式內網環境，由於他們不能與外部連線，因此需要使用離線更新包方式(檔案包) 來進行資料庫更新。

當內部有多台主機要進行資料庫更新服務時，亦可在內部架設一台Update Server，透由 Update Server 派送更新包到每一台主機，可大大降低管理者維護負擔。

* **WAF 防護解決系統主機漏洞風險**

眾至內網防火牆具備針對各類 Web 應用攻擊的檢測和防禦能力，如蠕蟲威脅、駭客攻擊、SQL 注入、跨網站攻擊等，滿足對檢測、防禦能力在廣度和深度上的要求。很多 Web 應用安全問題，究其根本原因很多是在 Web 應用程式開發階段留下的安全隱患為攻擊者所利用。因應此問題，眾至 WAF 防護會在網站前先築起一道防護牆，並透過所有流量 WAF 資料庫進行流量分析比對，判斷每條流量的安全性，准許安全流量進入網站，並將可疑的、有害的、不信任的流量排除在外，避免惡意流量入侵網站影響安全。

**D5.資安備援機制與教育訓練：**

資通訊技術（Information and Communications Technology, ICT）災害復原能力是影響業務持續營運成敗的關鍵因素之一，而 ICT 災害復原是組織整體業務持續性管理（BCM）的一個過程。葳錦資訊災害復原計畫包含資源重置、異地備援、緊急應變處理及營運復原等規劃。當組

織因為發生天災、人為疏失或惡意破壞等突發事故，導致組織本地端的主機房或是資訊系統服務中斷時，即可透過電腦機房異地備援機 制，迅速回復。

**D5.系統虛擬化，提供高可用備份機制:**

將舊系統虛擬化，依實際需求狀況淘汰舊主機設備，新購新主機設備提高資安高可用性，解決機器設備過多造成管理不便、維護不易、占空間、耗電、增加維護成本之問題，降低管理成本並善用虛擬化特點提升應用系統備份備援高可用度。 (圖 1-7)

依實際設備狀況擬定災難復原演練計畫並制定復原 SOP 文件，並每年至少一次以上定期做災難復原演練。

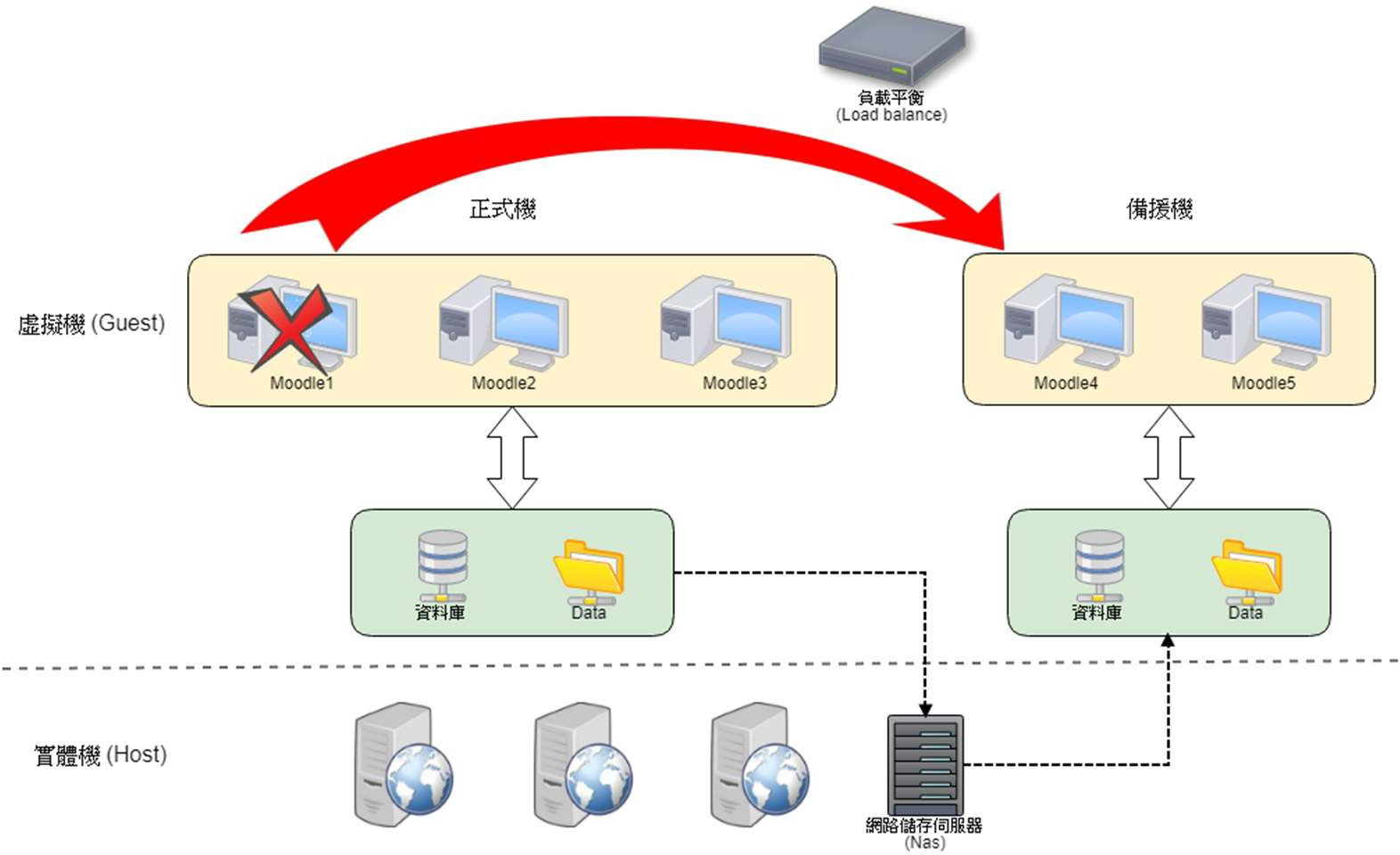


圖 1-7 建置備份、備援機制2.網路設備雙機備援機制

為了避免設備當機造所有內網線路全部不通或營運中斷，規劃像是防火牆、郵件伺服器相關設備須進行供HA(雙機備援機制)功能，允許兩台雙機備援的模式，來達到廣域網路連線環境最佳的容錯性。

在雙機備援模式下，採取主機(Master)和副機(Standby)相互備援，正常情況會以主機為優先的閘道設備，一旦Master 主機發生問題，Standby 備援主機將自動調整內部組態並取代主機的職務，來保持內/外部網路不斷線的運作，避免錯失商機。

網管人員亦可立即獲得新主機的訊息，來對原本故障的主機做修復保養的工作，使其能夠盡快恢復運作，來保障網路永續通暢。而設備也可以經由循環使用來延續雙機的壽命。

**D6.資安教育訓練：**

對 IT 人員與內部人員教育訓練，產出教育訓練文件，包含社交演練服務、資通安全法教育訓練。資安教育訓練分成2 個階段，事前與導入進行中，說明如下：

* **事前：**

最主要跟實際操作的人員初步溝通目前採用的系統架構、防護機制及被攻擊下如何因應，初期導入之後勢必會帶來某些不便，如何事先溝通這一些不便的操作並把他內化成正常工作的基本功，操作人員包含網路管理師、第一線操作人員、監控人員及程式設計師等。

* **導入進行中：**

最主要是對全公司所有人員的資訊安全意識的教育訓練，目的是如何避開釣魚網址或是郵件的引誘並且不任意安裝非必要或是沒被驗證的軟體。

* **社交演練：**

社交工程(Social Engineering)為一操控手法(圖1-8)，旨在利用人類心理上的弱點，以影響力或說服力來欺騙他人以獲得有用的資訊。駭客經由長期的觀察了解使用者習慣和企業的架構，再製作相對應釣魚郵件進行攻擊。現在的攻擊手法日新月異，一旦資安意識稍嫌不足，縱使郵件安全系統能夠做到99.9%的阻擋，那0.1%的漏網之魚仍可能誘使收件者開啟釣魚郵件，進而危害到企業的網路安全。

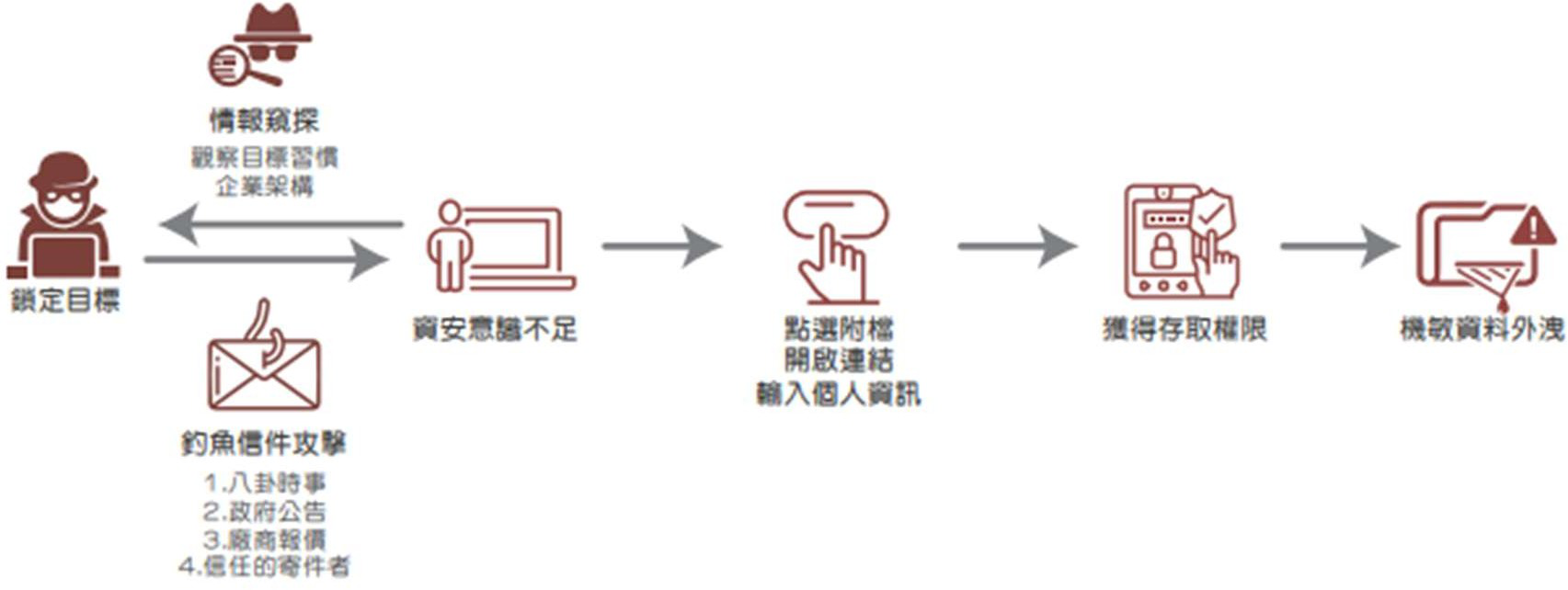


圖1-8 社交演練情境圖

* + - **模擬真實攻擊情況**

提供時事新聞、業界動態、熱門八卦、政府公告等不同主題的擬真釣魚郵件。演練時會由多種的測試帳號依據受測組織的部門結構做出調整，完整模擬釣魚攻擊的實際情況。

* + - **完整統計報告**

每一封信件會記錄受測者的動作，包括開啟信件、點擊連結、輸入個資/帳密和下載附檔。這些記錄下來的動作經過測試 團隊的分析、整理後彙整成一份詳細的報告提供給客戶，報告會依照客戶的組織結 構、測試表現提供圖表分析，讓企業能夠完整了解內部資安的弱點。

* **資安教育訓練**

藉由演練結果的統計報告，可以分析企業內部高風險人員是誰，以及這些人員個別的點閱習慣。企業可透過後續定期、 針對個別人員弱點的教育訓練進行資安意識的強化，幫助員工在面對日新月異的攻擊手法時，能保持最佳的判斷力。

**計畫內資安經費及其算式**

| 資安輔導工作項目服務 | 資安輔導顧問 | 預計金額 |
| --- | --- | --- |

| 網路環境架構檢視 |  | 30,000 |
| --- | --- | --- |
| 資安檢測服務(惡意活動檢視、使用者端電腦檢視、伺服器主機惡意活動檢視、防火牆連線設定檢視) |  | 170,000 |
| 新世代UTM |  | 920,000 |
| 郵件伺服器 |  | 400,000 |
| 系統主機弱掃 |  | 108,000 |
| 源碼檢測 |  | 250,000 |
| 備援機制 |  | 80,000 |
| 資安教育訓練課程 |  | 35.000 |
| 總計 |  | 1,993,000 |

**資安軟硬體來源**

| 資安軟硬體系統產品 | 生產國別 | 製造商名稱 | 金額 |
| --- | --- | --- | --- |
|  |  |  |  |
| 總計 | | |  |