# **資訊安全是什麼？**

首先要了解資訊是什麼？才能知道如何歸類資訊管理的方法，再進一步對資訊進行保護。

各種的資料彙集成資訊，對個人來說從姓名、生日、電話、地址到身份證字號、銀行帳號都是專屬於你的資訊。

對企業來說，則是公司、客戶資料、高層管理階層、金流紀錄、專利技術等，若上述資訊被有心人士掌握越多，影響及風險也就隨之擴大。因此，個人或企業都必須具備保護資訊的觀念，並執行對應的防護措施，以降低遭受惡意攻擊的風險。

### 資訊安全定義

透過剛剛舉例，我們發現部分資訊可以公開，但具有機密性的資訊，不適合公開，更不能被篡改，所以要刻意地進行保護及控管，避免重要資訊在未授權下的情況下，被無意或惡意地被讀取、使用甚至是變更等狀況，而對資訊進行保護、授權使用、維持資訊的機密性、確保其完整性和可用性等安全機制或技術，我們通常稱為「資訊安全」，通常簡稱為「資安」。

### 資訊安全管理3原則

這三個原則是資訊安全管理的基礎，無論是在企業內部還是個人層面，所有的安全策略都應圍繞這三大目標設計：

* 機密性：資料只能讓有權限的人看到，防止被偷看或外洩。  
  （像對資料增加密碼或設定只有自己能讀取的權限。）
* 完整性：確保資料不能被竄改，確保資料的真實性及唯一性。  
  （像檢查資料有沒有被動手腳，確保資料原封不動。）
* 可用性：確保能隨時取用資料，不會輕易因為系統當機或設備異常而受影響。  
  （像備份資料，防止設備損壞造成資料遺失。）

## **資訊安全具備要件有哪些？(軟體、硬體、資料)**

### 1.硬體安全

硬體設備故障的發生，往往會伴隨著資料遺失及毀損，而硬體故障的原因很多，除了溫度、濕度、老化外，也需要考量電力不穩或天災的因素。透過定期檢視的硬體設備狀態，隨時備份重要資料，以及設置備用電源或不斷電系統等等，可降低硬體故障機率。

硬體設備是非常明確的目標，當有心人士直接接觸到硬體設備時，就有機會竊取或破壞資料及資訊造成，如何適當地將硬體設備與外部做隔離，也是資訊安全防護規畫中必須具備的措施。

* 硬體資安防護重點如下：  
  – 防災(地震、水災、電力不足等)  
  – 防竊取

關於硬體安全的資訊安全防護，除了自行建置完善的機房環境外，尋找專業且可靠的機房代管業者，能有效節省許多支出，並降低維運與人力成本。

### 2.軟體安全

隨著資訊時代來臨，人們透過軟體技術將硬體的效益發揮的更加淋漓盡致。

軟體包括的範圍很廣泛，從電腦作業系統、資料庫系統、應用程式到網站系統等，現今在工作及生活中我們已經非常依賴各種軟體來完成工作，因此當軟體環境被駭客入侵或因感染病毒等異常狀況時，對我們的影響也會非常巨大。

* 軟體資安防護重點如下：  
  – 防駭客  
  – 防病毒

### 3.資料安全

不論哪個時代，資料保存都是個非常重要的課題，過去可能會透過圖書室，保險箱等措施來保護資料，只要特定地點進行保護就能達到防護的效果。

而現今許多的資訊及資料都以數據的方式存放在不同的媒介上，例如個人會將資料存放於電腦的硬碟中或USB隨身碟，而企業則會將資料放在檔案主機中或來儲存設備裡，這些資料一旦被竊取、損壞或者遺失，對於個人及企業來說都是莫大的損失，更是成為資訊安全的一大隱憂，因此我們對於各種的資料處理，應該抱著謹慎態度去面對。

* 資料資安防護重點如下：  
  – 防災 (地震、水災、電力不足等)  
  – 防病毒  
  – 防盜竊

我們還可以將資訊安全細分成如下資訊安全種類，進一步採取合適的應對措施。

### 1.網路安全

是指針對連接網路裝置、網路中傳輸的資訊、利用網路運作的軟體及透過的服務，這些項目的安全都包含在網路安全範圍內，有心人士會透過對網路的侵害，來達到竊取敏感資訊，癱瘓裝置、軟體或服務等，進而製造出個人的身份被盜用與詐騙，甚至是企業的重要資料被竊取或無法正常營運等問題。

* 合適的資訊安全措施：  
  面對[DDoS攻擊](https://www.easpnet.com/blog/ddos-service/)的主動式DDoS緩解服務、MDR威脅偵測應變服務、網管監控服務、資安顧問諮詢、資安防護架構規劃。

### 2.系統安全

電腦系统或者網站系統的安全，會隨著技術的日新月異，隱藏於其中的缺陷也隨之浮現或被發掘，這些缺陷我們通常稱之為漏洞，而漏洞的存在將使得系统和資料的保密性、完整性、可用性、授權機制都面臨有心人士的威脅。針對系統安全，通常會透過對漏洞進行管理作為應對措施。

漏洞管理的第一步就是定期進行資安檢測，如系統弱點掃描，並以風險為依據排定補救措施優先順序。此外最好隨時檢測資訊環境中是否存在異常的網路行為，以提前發現漏洞。

* 合適的資訊安全措施：  
  定期[資安檢測](https://www.easpnet.com/security-inspection/)(網站弱掃、系統弱掃)、[MDR](https://www.easpnet.com/blog/mdr-edr-services/)威脅偵測應變服務、網管監控服務、資安顧問諮詢、資安防護架構規劃。

### 3.應用程式安全

上述說明中有提到軟體安全中包含了應用程式安全，而應用程式玲瑯滿目，更與生活也息息相關，從文書作業、訊息的傳遞到商業的交易都有應用程式的存在。我們需要了解如何避免有心人士從應用程式的運作中，找出潛藏的漏洞，進而用以侵害個人隱私，財產甚至是人身安全。

因此使用者必須留意且重視正在使用的應用程式之來源、發佈應用程式的單位或組織是否主動地檢視程式的安全性，並在整個應用程式生命週期內保護程式避免威脅迫害。降低網路犯罪者找出並利用應用程式中的漏洞來竊取資料、智慧財產以及機密資訊等行為。

* 合適的資訊安全措施：  
  定期資安檢測(網站弱掃、原始碼檢測、App認證)、資安顧問諮詢、資安防護架構規劃。

### 4.資料加密及身份認證授權

在資料安全上除了確保資料的保存外，也要考慮到資料被竊取的可能性，目前有許多的機制及技術能對資料進行加密，讓非經授權的有心人士無法識別及解讀，萬一發生被竊取時，可以藉此增加對資料的保護能力，降低損害。

近期頻傳的勒索病毒也是對資料保護的嚴重考驗，過去單純保護資料不被竊取的方式，已經無法滿足這種惡意行為，必須採取新的資安思維及防護技術來保障資料。

現今的生活中，已不再需要到特定地點辦理，使用網路就可以執行，大大地增加便利性，但隨之而來的問題是如何確保身份認證的授權身份、資料的管理及使用。近年來國際間提出許多相應的規範與認證，政府單位、金融機構服務及企業網站，可以參考或遵循國際標準或國家規範，來保護及使用民眾的資料。

* 合適的資訊安全措施：  
  [防勒索雲端儲存服務](https://www.easpnet.com/secure-drive/)、資安憑證(SSL憑證)、資安顧問諮詢。

### 5.雲端安全(雲端運算安全)

所謂的「雲端運算」與傳統電腦系統及架構不同之處，[雲端運算](https://www.easpnet.com/blog/cloud-services-101/)是一定要透過網際網路來使用可共享的軟、硬體資源之運算技術。

由於雲端運算是依靠著網路來實現，並且能將架構中的軟、硬體及應用程式，以共享的方式提供給不同用戶使用，因此在討論雲端運算安全時，必須將網路安全、系統安全、應用程式安全及資料加密安全及身份認證授權等條件一起考量，所以一個可靠且值得信賴的雲端運算環境必須同時具備多個面向的安全能力。

* 合適的資訊安全措施：  
  專業可靠的公有雲服務、自建雲服務、[混合雲服務](https://www.easpnet.com/gwshybridcloud/)