**專題說明**

近年來駭客猖獗、手法、身份又多，對於使用者來說防不勝防，尤其對於以發明為利益的科技公司與需要嚴格保密的銀行機關、保險公司、醫院等等的單位，如果資料被他人竊取，將會造成難以估計的後果。隨著監視器的普及使我們能用於各種方面，對於電腦的防衛上也有著比以往更有安全上的提升，而監視器對於犯罪和意外的記錄能提供顯著地幫助。

駭客入侵的手法主要分為：實體入侵、破解密碼、網站入侵、其它入侵，實體入侵是指企圖者會以到電腦前將電腦開啟或是直接取走硬碟藉以取得內部資料的方式，這種企圖者除了刻意事前偷取登錄密碼進入公司內部網路的駭客之外，也極有可能會趁使用者不注意在電腦上插入隨身碟來執行對自己有利的程式，一般預防情況是能在有人接近電腦時就記錄下來，對於使用者來說，就能在對方行動前就擁有紀錄和先發制人的警報。

過去警報系統往往需要出入口開啟，即使犯人經過也無法作為證據，同時也必須花費大量資源用在存放攝影機的影像上，但目前對於想直接竊取電腦的部分民眾則往往交由居家防盜或保全公司協助，使用者在第一時間無法得知情況；而破解密碼、網站入侵都需要使用者的電腦處於聯網的狀態下才能從外部取得使用者電腦的控制權。為了預防上述2種手段，各家軟體公司開發了許多保護程式，例如防毒軟體，能協助使用者遠離可疑的網站或是封鎖信件的連結和夾檔等等，但如果不購買全套的保護，就只能使用部分的防護，就像撐著一把有洞的傘去擋雨，有些病毒更是能偽裝成防毒軟體，假借更新或掃毒來清除正常檔案並擴散病毒，使用者付錢購買了升級保護，卻只是讓更多病毒入侵自己的電腦。

本專題將針對上述實體入侵的部分情況進行規劃與改善，畢竟這是使用者最難以掌握情況。系統將架設於電腦附近，以確保未經許可的接近者為竊盜的可能性，同時也節約監視器不斷儲存不必要的資源，提供使用者的電腦多一道強而有力的鎖。本系統設置的監控裝置能夠將走到電腦桌前使用的企圖者記錄下來，當使用者未使用電腦而被他人竊取資料時，能留下證據以便日後提供給警方，藉以達到防衛的目的。

本系統適用於開放空間的個人電腦或使用內部網路的商業機關電腦之監控，本專題具有下列特色：

* 手機遠端重啟監控系統。
* 兩組超音波感測，偵測角度達135°。
* 自動夜間感測照明裝置。
* 即時(real time)偵測及通知使用者手機。
* 排除網域的限制，能夠在不同網域的地方使用與控制。
* 警訊通知除了簡訊及電子郵件，還加設了Google Cloud Messaging(GCM)之技術，強調即時之功能。
* 拍攝之影像會存放於雲端(伺服器)，不浪費硬體空間。