



近年受到Internet網路通訊的便捷多元影響，從傳統data base、data warehouse及data minding等走進大數據分析與應用，甚至於目前常討論到的區塊鏈經過篩選取得有用的數據做BI(business information)提供給決策者或經營者做為決策與分析的依據，同時讓高階主管等分析公司組織面及經營資源，進而透過SWOT分析等等，來判斷產品是否有市場競爭力及公司是否有組織應變力等等，所以不單單是一個分析表。

再加上物聯網（IoT）、雲計算(cloud computin)、大數據(big data)及區塊鏈（blocking chain）等新技術，都需要與資訊安全在系統整合及技術結合，作為智慧建築上系統建置努力的目標，將可創造更安全更有便利。

舉例如智慧宅的數據，預測未來頗據市場規模，呼應政府推廣政策。用資訊安全為基礎來保障智慧建築便利性、機密性、可用性及完整性，提升客戶信心及滿意度，進而提高產業升級。建立企業資訊安全標準作業程序易於管理、傳承，提升智慧建築資訊安全的保護等級，加強系統主動防護、即時監測、預防在前等，保護客戶及企業之機密資訊及智慧財產，並推動企業競爭優勢。

資訊安全為何重要：

無論是big data、IoT 到智慧節能都將成為未來趨勢，現在應該重視資訊安全，而非等到以後有嚴重的網路災情才亡羊補牢，智慧雲端社區將數據通訊都連絡至網路中，使用者可以方便操作，但駭客或有心人士，也方便進行攔截或攻擊，藉由這些數據讓住戶行蹤很容易被掌握。



目前導入通航智慧雲端社區，在internet進入社區時，第一道使用防火牆，第二道Server安裝防毒軟體及每日備份，第三道client端使用者除了安裝防毒軟體外，也需提高密碼複雜度及建議每3個月更改一次密碼，另外電信及電腦機房也要做好門禁管制、消防設備及監視錄影等。

讓住戶達到安全與幸福零距離空間，當訪客拜訪住戶時，同時透過家庭主機、手機、平板接聽影像通話，達到多螢幕且不限空間的聯繫。住戶在辦公室或國外透過手機可以了解家中重要門窗是否關閉，再遠端進入家庭主機設定保全，防止入侵。一旦有異常狀況時除了家庭主機發出警報嚇阻，同時也通知管理員，管理機上會出現該住戶及警報項目，並通知BA和物管，中控電視牆上同時跳出警報。住戶手機也同時收到推播通知達到即時通知即時處理。除了推播警報訊息外，當管理中心發出相關訊息時，住戶手機也可以進入家庭主機讀取訊息，如火災、地震……等。

電信公會如何做提升資訊安全從心臟地帶著手規劃：

資訊安全在於園區、社區、廠房核心都會談到實體機房資訊安全，而機房重鎮如何做好管理，除了管制人員進出管控，亦要定義縝密遊戲規則，也要有設備來輔助做加強，這對機房重地非常重要，例如資料備份、不斷電系統、溫濕度控制、結構安全、消防、影像監控、伺服器、網路線路及網路設備等等。



網域安全應定義各自區域：

網路作分割規劃就好像家庭成員一樣、各司其職，如企業中各種連結網路的設備有各自的角色一樣，Clinet網域、FTP Server、防火牆、WEB，應制定相對應的空間與網域給它們，不只要網路能通就好，也需要規畫VLAN將網段切開。故於社區也是相同，需要切開各子設備網段如監控網、對講網、門禁、KVM、社區 Wi-fi 使各設備僅達到有規

則的互通。通航採用WEB化的架構透過瀏覽器可以跨系統整合監控所有建築物裡的設備，如重要機房門被打開會發出警報，從電腦、平板、手機就可以同步收到訊號，也會推播到社區相關委員或警衛手機，達到即時通知、即時處理，警衛電視牆也會跳出，此外大樓的二線式燈光也可以在權限內人員從這些設備來做啟動或是排程。當系統收到地震或火災訊號時，會同時推播到全體住戶的室內機與住戶的手機能夠即時通知並自動開啟社區大門方便逃生。當資訊安全提升後，企業存活率也相對提升，故社區亦然，提高住戶對設備信賴感。

提升IT管理專業的益處：

近年無論話機、對講機、監視器逐漸往IP應用的功能提升，相對的管理的能力亦須提升，例如傳統設備時常要全案場查線，卻無法事先遠端分析原因、區塊，而浪費過多的時間成本，而網路型設備卻不只是線路對就好，需要注意的環節更多，這也是許多廠商的痛處，反之利用IT網路管理的技術在遠端了解無法通訊的狀況發生時，分析是線路問題，還是設備產生的問題，準確快速的處理排除故障點，更能提升營運效率。通航物管平台可以提供社區故障報修，做到及早通知，搭配現場回報照片即時處理。透過平台能夠簡單知道各個設備相關安裝維修紀錄及配合廠商資料。而公設預約、財務系統、設施管理、訪客及信件管理等相關社區所有的事項。透過電腦直接刷條碼方便將住戶信件登錄並即時發送到住戶掛號信件通知到該住戶手機，在住戶利用刷卡或是刷條碼方式收信電子簽名也可完整記錄。訪客透過平台登記



後對在訪客何時進出都有完整的紀錄，社區安全會更有保障。

落實資訊安全提升競爭力：

網際網路上每秒有著成千上萬的病毒碼在上面流串，當智慧建築強調IoT、APP服務、雲端服務管理平台此時已經是這些病毒的可能測試或攻擊目標，日前發生的勒索病毒大舉攻擊事件造成許多企業的損失，我們應正向面對資訊安全規劃已經不只是IT產業才需要注重的情况。為客戶規劃便捷服務時同時建置合適的資訊安全方案，使企業、一般

用戶能免於受到惡意入侵、監視影像、社區資料外洩等威脅，用資訊安全為基礎來保障智慧建築便利性、機密性、可用性及完整性，提升客戶信心及滿意度，進而提高產業升級。建立企業資訊安全標準作業程序易於管理、傳承，提升智慧建築資訊安全的保護等級，加強系統主動防護、即時監測、預防在前等，保護客戶及企業之機密資訊及智慧財產。絕對是提升廠商競爭力必須先進場佈局的方向，亦能為競爭激烈的電信、智慧建築電產業開啟新的一片藍海。

