關貿第 28 期電子報

哈燒話題：從需求整合到供給，打造網網相連的單一協同窗口

隨著時代變遷，企業經營全球化，國際競爭越來越激烈，供應鏈管理作業已成為各企業重要的課題。鴻海董事長郭台銘曾表示：「電子產業競爭不在技術，而是在供應鏈管理。」如何與供應商、物流業者，以及客戶緊密協同合作，便成為企業所面臨的最主要挑戰和競爭致勝的關鍵。

自 1985 年 Michael E. Porter 提出供應鏈管理（Supply Chain Management，SCM）的概念後，各企業大都發展出一套合適的商業經營模式，以各種方法提高供應鏈的效率並降低供應鏈的成本。但隨著新產品的開發與新技術發展日新月異，企業生產的商品生命週期愈來愈短，

使企業必須不斷開發新產品才得以在市場上維持競爭優勢。除了產品開發外，企業同時也必須維持售後服務的品質，這讓企業推出的產品與服務愈來愈多元。加上供應鏈與戰略夥伴橫向與垂直的產業整合趨勢，讓企業在運籌及物流管理的複雜性不斷提升。如何精準的做好需求預測與上下游協同整合，平衡生產計畫和庫存計畫，以及做好風險管理，成為企業目前最新的目標與挑戰。

今年 1 月 18 日在臺大醫院國際會議中心舉辦的運籌暨物流管理研討會中，關貿網路股份有限公司朱啟光顧問特別就史丹佛大學科學與工程管理、工程系李效良教授所倡導的 3A（Alignment、Adaptability、Agility）供應鏈的企業應用，進行了深入淺出的說明：

Alignment –協同運作

企業要與供應商建立更緊密的關係，才有可能為了達到供應鏈的共同利益而協同合作，組成牢靠的夥伴關係。藉由與供應商互信合作，提供及時的資訊交流，企業可以藉由及時的需求資訊，做為原料數量預測參考以及下訂單的依據，避免過多與不足的情況發生。藉由協調供應商提供準確的原物料交期資訊，確實溝通，以精確管理短期允交流程來提高實際訂單準確率。短期能滿足企業內部採購的如期交付，中期能以累積的資訊來進行成本分析並降低成本，最後能達到物流整合最佳化的終極目標。

Adaptability –適應性

企業藉由電子化系統與供應商、海關協同合作，資訊交換並整合各自的供應鏈流程，將庫

存與物流資料量化，簡化整體作業流程，減少庫存所佔成本，提高跨國供應鏈管理能力，以達到最適化、穩定化、效率化。

Agility –敏捷性

由於現代企業供應鏈越來越複雜，容易牽一髮而動全身，因此對於異常情況的發生，需要能快速的異常管控與因應措施。良好的供應鏈管理要能在異常發生的初期就要有警覺性，將影響控制在最小的範圍，更要具有良好的應變能力。

朱顧問表示：要善用 3A 供應鏈來提升企業價值，必須先以客戶價值為核心，整合上下游需求，改善供應商供貨流程並加強資訊溝通，將成本合理化，並落實績效管理，達成運籌物流最佳化。藉由促進供應鏈完整的運作，企業得以強化自家商品或服務的成本優勢，增加客戶滿意度，最終達到公司整體營收提升。

有鑑於此，關貿網路所提出之 Easy SRM 供應鏈解決方案，提供企業需求預測、協商與後續流程執行的整合模式，共包含以下幾種服務：

(一)預測管理服務

將企業訂單、物流公司在途庫存以及供應商原物料提供三方即時資訊整合，企業得以藉此預測需求、降低庫存，減少長鞭效應造成的風險。

(二)效能管理服務

以供應鏈管理系統將企業上下游資訊進行有效整合，更精確的掌握交期與數量，有效達到企業營運績效控管提升的目的。

(三)情報看板管理服務

由企業自行設定各類型異常情境模式，系統於異常情況發生時能迅速自動回報，讓企業能第一時間掌握進度與進行修改，提高風險管理的掌控與應對能力。

(四)運籌管理服務

由於全球化的趨勢影響，各企業供應鏈變得龐大而複雜。藉由運籌管理系統，企業營運總部得以將各地方供應鏈與運籌作業整合，提高決策效率以維持企業全球競爭力。

(五)安全營運管理服務

企業供應鏈要面對的上游廠商眾多，各式資訊瞬息萬變，唯有透過專業的供應鏈營運服務，才能維持供應鏈的穩定、資訊的安全與使用上的便捷，將可能的風險降至最低，落實企業規劃執行與管理。

經過多年來不斷研發改進，關貿網路提供客戶優質供應鏈管理服務，配合全球運籌服務與通關服務，無論是貨主、承攬業者、報關業者、倉棧、海關、航空公司，都能獲得更透明、更及時的貨物資訊；再透過供應鏈管理服務，將企業內部的生產計畫、物料需求計畫、現有庫存與庫存策略等，配合供應商之動態加以整合，有效運用各類型資訊，進而提升整體供應鏈效率。

本公司朱啟光顧問於運籌暨物流管理研討會中發表演說

研討會現場座無虛席

新聞播報：整合兩岸口岸間進出口貨物資料，提升貿易物流效率

在全球經貿合作的風潮中，我國政府與大陸於 2010 年簽署了「兩岸經濟合作架構協議」，讓兩岸商業交流更開放。為了強化經貿往來，加快兩岸港航資訊串接速度，建構互利互惠關係，由遼寧省長團隊所組成的貿易物流考察團於 2 月 17 日來台，假台北君悅飯店與我國企業界代表舉辦「大連-台灣航運合作懇談會」。會中由關貿網路股份有限公司何鴻榮董事長率同連鯤菁總經理與大連港集團有限公司代表孫宏總經理簽署合作協議，就通關、物流及金流資訊等部分，強化雙方原有資訊交換管道。

關貿網路在大陸口岸間連線發展策略上，已先後與福州口岸及上海口岸完成連線。大連口岸為大陸第二大集裝箱中轉港，其海運鐵路聯運量位居大陸內沿海港口之首。關貿網路於 2008 年起即與大連港集團就貨況追蹤方面進行合作，至 2010 年交換之貨況訊息已達十萬筆。此次雙方共同簽屬合作協議，藉由資訊串接，共同推動整合兩地口岸間提供的貨物資料，形成兩岸貨物動態查詢資料庫，以使貿易、物流業界即時掌握其貨物動態，滿足國際貿易（尤其三角貿易）之商流、物流及金流的迫切需求，創造兩岸企業互利互惠的雙贏局面。

關貿網路股份有限公司成立於 1996 年，初期以通關貿易為核心，近年來積極開拓雲端運算技術，並將業務擴展至電子商務以及全球運籌服務，目前提供超過 50 項 ASP(Application Service Provider)系統服務。服務範圍遍及進出口通關、電子商務、供應鏈管理平台等，提供企業全年無休、全方位、安全有保障的電子商務服務。關貿網路至今擁有超過 4 萬 9 千家客戶，包括各級政府機關、航運業、報關承攬業、物流業、房仲業、金融機構、產險業、流通業等。

(前排左 1：關貿網路連鯤菁總經理；前排左 2：大連港集團孫宏總經理)

創意關貿：關貿網路公司舉辦 2011 年創新競賽

因應市場上的激烈競爭，公司隨時都需要保持熱情與活力才能面對多變的挑戰。為了活化公司同仁的創意及活力，凝聚全體向心力，並培育同仁對於創新服務的規畫能力，本公司特舉辦「2011 年關貿網路創新競賽」。本次競賽項目包含：(一)流程創新、(二)技術創新、(三)商業模式創新及(四)電子發票加值服務創新。我們期盼從同仁的創意裡，找出能給予客戶更高的價值與更滿意的服務。

客戶感謝：新揚科技保稅系統導入之感謝函

在今年新揚科技第一次遭逢保稅廠年度重頭大戲 < 年度盤點作業 > 的時刻，因新揚先前所使用的保稅系統不符合其廠內生產作業流程，及 ERP 資料串接的種種問題，導入以來所有的保稅作業還是以人工方式進行。這些手工帳的資料導致其盤點作業的困難，進而嚴重影響到盤存與結算作業的盤盈及盤虧。

另外，有鑑於新揚年度盤點時間的緊迫性，當雙方合作一啟動，關貿技術團隊便進駐新揚，以便即時與新揚的工程師作有效的溝通，來進行其內部 ERP 系統串接、設計符合其廠內生產流程的保稅系統。同時也配合新揚實際需要，提供了年度盤點、按月彙報及系統操作的教育訓練。使得新揚年度盤點及按月彙報申請，能夠順利進行及如期完成，並產生出符合海關規定的年度盤點報表與帳冊。

因此當系統建置結束，新揚科技的洪庭筠經理及專責人員很感謝關貿從系統建置、實務輔導、教育訓練到海關審查，都給予新揚最大的支援與協助。因此洪庭筠經理特別發函來感謝：

「每當回憶起當初的慘狀，對關貿，我真的是滿懷的感謝。感謝所有參與這個案的關貿同仁；技術團隊令人讚嘆的功力，顧問犧牲假日來輔導，還有客服單位的大力協助，真的萬分感謝！」

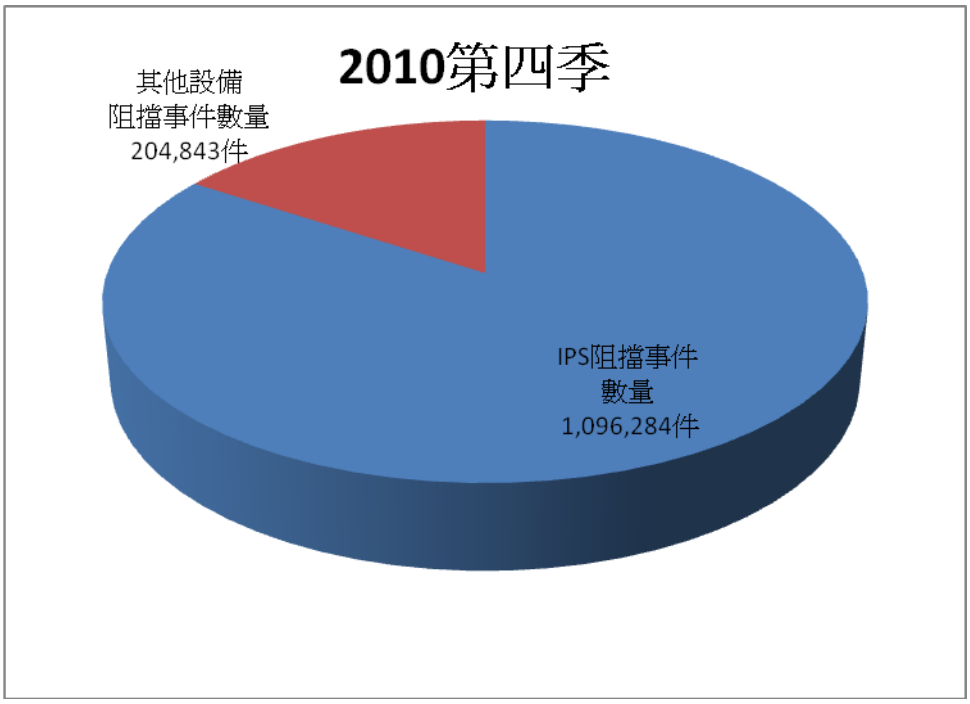
資安小常識：入侵防護系統(Intrusion Prevention System)

近年來企業為了抵檔網頁竄改、阻斷式攻擊、個人資料外洩等駭客攻擊行為，資安人員部署各項資安設備於企業網路中；如入侵偵測系統、入侵防護系統、網頁應用防火牆等。隨著網路設備的多樣化，強化端點防禦更是目前重點防禦趨勢，而部署於各網路設備上的入侵防護系統尤其重要。

傳統的入侵偵測系統(Intrusion Detection System)分為(1)網路型-監控網路環境內封包，如SNORT[1]、(2)主機型-監控主機內部註冊表、行程、系統紀錄檔等資訊，如 OSSEC[2]。管理者制定規則來偵測惡意入侵行為，當入侵者違反規則時觸發警報，藉由警報來提供管理者關鍵資訊。入侵偵測系統在網路環境中扮演監視器的腳色，對於入侵行為只單純做好紀錄及通知的工作，但當入侵者對伺服器發動攻擊時，入侵偵測系統無法主動防護。

入侵防護系統主要分為(1)網路型、(2)網路行為型、(3)無線網路型及(4)主機型-如WinPooch[3] ，依偵測類型可分為(1)誤用偵測 - 利用特徵碼來偵測惡意行為、(2)異常行為偵測-使用行為偵測來偵測惡意行為，例如管理者定義正常行為，當使用者違反正常行為時觸發警報進行阻擋，入侵偵測系統與入侵防護系統相輔相成，當入侵偵測系統有警報產生時，管理者可利用此警報資訊撰寫入侵防護系統政策來進行防護。相較於入侵偵測系統，入侵防護系統主要設計來阻擋真正的攻擊行為，如零時差攻擊。當防毒軟體及軟體廠商並未及時提供病毒碼或修補程式前，入侵防護系統可提供主動防護。當使用者違反管理者所制定的政策時判定為惡意行為進行阻擋，入侵防護系統在網路環境中扮演警衛的腳色。

入侵防護系統補強了入侵偵測系統的不足之處，在即時監控的狀態下提供了主動防禦的功能。如在一個戒備深嚴的商業大樓，不只需要在各進入口部署監視器並且要警衛站哨才能有效阻擋入侵者。在 2010 年第四季關貿網路所阻擋的攻擊事件總數量 1,301,127 件，其中由入侵防護系統所阻擋的事件共 1,096,284 件，佔總事件量的 84%，可見入侵防護系統是目前縱深防禦的重要環節。



參考資料

[1]Snort: **http://www.snort.org/**
[2]OSSEC **http://*www.ossec.net***
[3]WinPooch **http://sourceforge.net/projects/winpooch/**