

## 貨櫃保全裝置運用於輸美貨櫃保全管理之個案探討

### Case Study on Container Security Device – Applying to the Security Management on Containers Destined to the United States

周和平 Ho-Ping Chou\*  
張啟隱 Ki-Yin Chang,\*\*  
袁智清 Chih-Ching Yuan\*\*\*  
薛安國 An-Kuo Shiue\*\*\*\*

#### 摘要

美國遭受「九一一恐怖攻擊事件」後，引起美國與全球的震驚與恐慌，為有效防止恐怖份子利用海運以進行類似大規模的攻擊與破壞，美國政府計劃推動科技產品－貨櫃保全裝置（CSD），將其安裝於輸美貨櫃，希望經由此裝置可以主動偵測貨櫃在運輸過程中任何之非法入侵，以達安全控管之目的。實務上貨櫃航商亦常遭遇所承載之貨櫃其封條在運送途中遺失或被更換，導致貨櫃內之貨物失竊或被放置毒品以進行走私。適值美國政府積極推動貨櫃保全裝置（CSD），此時機正是航商投入改善貨櫃封條管理的最好時機。因此航商宜及早與設備供應商合作進行先導測試，以了解貨櫃保全裝置（CSD）之實際功能與成效。

**關鍵字：**無線射頻識別（RFID）、貨櫃保全裝置（CSD）、電子封條（E-Seal）

#### ABSTRACT

On September 11<sup>th</sup>, 2001 America was under terrorist attack, the origin or the 911 attack has brought not only the U.S. but global shock, the U.S. Government actively adapts a feasibly technical product – Container Security Device (CSD) system on U.S.-bound shipping containers. Hopefully CSD system can monitor the

\*國立台灣海洋大學商船學系名譽教授。

\*\*國立台灣海洋大學商船學系教授。

\*\*\*開南大學物流與航運管理學系副教授。

\*\*\*\*長榮海運股份有限公司運航部協理。

door security status of cargo conveyances to prevent unauthorized access and then achieve an essential control to prescreen U.S. bound containers in advance. Sea carriers often suffer seal missing or changed stealthily en route, that also lead to cargo stolen or potential conveyors for illicit deliveries of drugs smuggling therein. The U.S. government get ongoing moving on global container security of transportation management. Sea carriers should be speedy in touch with suppliers to fix forerun test by real diagnosis of analysis the results of this technology to further understand the benefits in actual capability and effects.

**Keywords :** Radio Frequency Identification (RFID), Container Security Device (CSD), Electronic Seal (E-Seal) .

## 壹、前言

貨櫃在運送過程中經常發生貨櫃封條遺失、遭破壞或更換，導致貨櫃內部所承裝之貨物被偷竊或放置走私物品，主因在於貨櫃使用機械式封條（Mechanical Seal）加封，當貨櫃被非法入侵時，機械式封條不能傳送警訊至相關單位，以做出有效處理，導致在國際複合運送過程，如果其中幾個重要管制點沒有確實做好封條的查驗工作，一旦封條或貨櫃發生狀況，事後很難斷定事故發生的確實時間與真正地點，以追究與釐清責任的歸屬。如果責任無法確認，最終航商將概括承受賠償相關的損失。

在實際管理經驗中，雖“E”航商不斷加強貨櫃封條管理之監控，但從仍有不斷事件的發生看來，深感要確實做好貨櫃封條的管理工作仍有許多的困難，因此考慮使用以無線射頻識別（Radio Frequency Identification；RFID）技術所研發之貨櫃保全產品以輔助機械式封條其保全功能之不足。但此項計劃因涉及部份海運物流供應鏈業者的配合度不高，而無法全面落實。因此深感目前的封條管理制度仍存在一些缺陷，已非航商單方面所能掌控。

適值美國於2001年9月11日遭受恐怖份子有計劃性的攻擊，造成美國其本土及全球的震驚與恐慌，美國政府為防範於未然，因此立即展開防恐與反恐之行動；在海運尤其貨櫃運輸方面，除率先制定一系列以美國為中心之貨櫃保全規範，以補強國際相關保全規範在貨櫃運輸方面之不足外，並計劃要求輸美貨櫃皆需安裝貨櫃保全裝置（Container Security Device；CSD），以監控貨櫃運輸安全及協助人力查驗之不足。

因美國政府積極推動輸美貨櫃保全管理，其強大政治力的介入並要求所有海運相關物流供應鏈業者必需配合，此時正是“E”航商借力使力，投入改善貨櫃封條管理的最佳時機。有鑒於此，“E”航商隨即與生產貨櫃安全產品之國際知名廠商“Savi Networks”公司展開接觸並進行實際之測試，主要目的在於探討安裝貨櫃保全裝置（CSD）是否能夠確保貨櫃全程運送之安全；是否能夠防止貨物被偷竊或被利用走私以確保航商之權益與聲譽；是否能夠防止人為查驗貨櫃有可能之疏失並可精簡人力之配置。其特殊環境偵測功能是否有助於確認貨物之運送責任；貨櫃防水性能與貨櫃保全資料傳送是否夠快速；貨物是否可享有美國海關快速通關之優惠等功能與效益等。

### 貳、貨櫃保全管理相關規範

美國「九一一恐怖攻擊事件」，是2001年9月11日發生在美國本土的一次通過劫持民航飛機衝撞摩天高樓的自殺式恐怖攻擊，是繼美國墨西哥戰爭、珍珠港事件後，歷史上外國勢力對美國本土發動的第三次大規模性襲擊。在事件中，共有2,986人死亡，包括美國紐約地標性建築世界貿易中心雙塔在內的6座建築被完全摧毀。其他23座高層建築遭到破壞，美國國防部其總部所在地五角大廈也受到攻擊，美國經濟也因而遭到嚴重打擊。相較於珍珠港的軍事偷襲事件，這次事件可以說是針對美國最嚴重的恐怖攻擊事件<sup>[1]</sup>。

美國政府在「九一一恐怖攻擊事件」之後，對於交通運輸進行全面性的檢討，進而發現經由海運尤其貨櫃運輸的保全管理是其防恐最脆弱的一環。根據美國託運人主辦的航運數據庫「突堤（Pier）」全球情報數字顯示，美國2007年依船艙單計算，全年總共有1,896萬TEU的貨櫃進入美國，在如此大量的進口貨櫃中，海關查驗率僅有2%，因此貨櫃易為恐怖份子利用以進行大規模之恐怖攻擊與破壞。基於此，美國政府亦陸續推出一系列以美國為中心之貨櫃保全管理規範，以補強國際相關保全規範在貨櫃保全管理方面之不足。

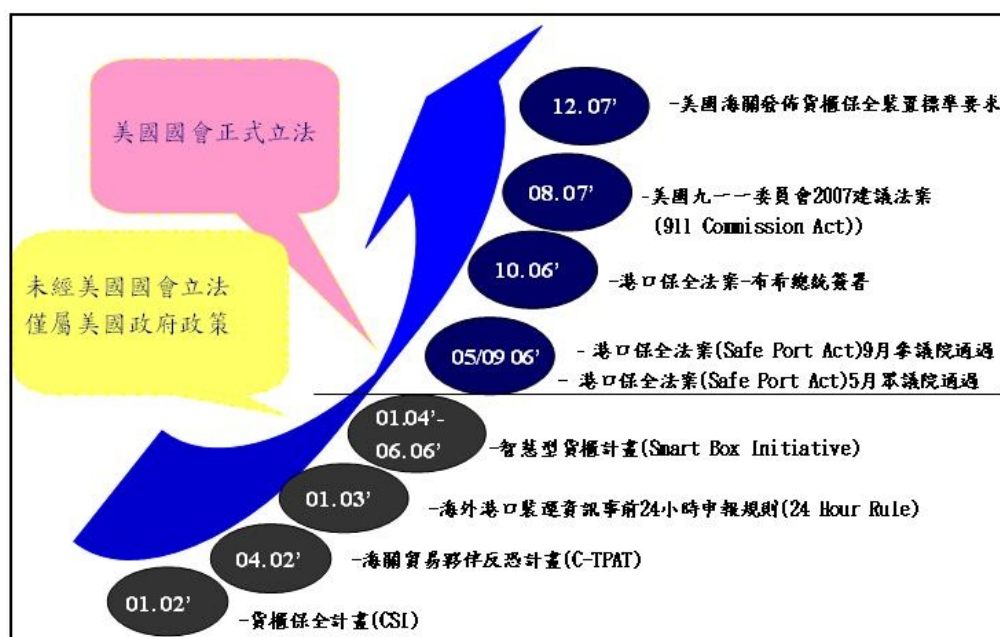


圖1 美國主要之貨櫃保全管理規範發展圖

資料來源：Henry Jen,「U.S. Conveyance Security Device Requirement (1.2 Version)」, April 26, 2008。

有關以美國為中心所制定之一系列主要之貨櫃保全管理規範，依序簡要說明如圖1所示。

### 一、美國貨櫃保全管理規範

以美國為中心所制定之一系列貨櫃保全管理規範，原屬北美洲地區含加拿大等國之要求規定，且號稱非強制性之保全管理規範，但因美國市場約佔全球商貿35%左右，受美國商業貿易及國勢強大之影響，全球各國輸往美國貨櫃的貨主、運輸業者以及國際物流供應鏈者等，為求輸美商貿順暢及貨運的快速通關，不得不加入其規範要求，進而成為貿易聯盟夥伴關係。

#### (一) 貨櫃保全計劃

美國政府於2002年1月宣佈執行「貨櫃保全計劃( Container Security Initiative ; CSI )」，主要目的是透過海關與海關間之跨國合作，在國際間查驗毀滅性武器，包括化學、核子及生化武器等，以防止恐怖份子利用輸美貨櫃，

將毀滅性或殺傷性武器暗藏於貨櫃內以海運方式進入美國境內犯罪。

「貨櫃保全計劃 (CSI)」主要內容包括下列四項:

1. 建立以安全檢查為目的之高危險群貨櫃篩選標準  
美國海關暨邊境保護局 (U.S. Customs and Border Protection ; CBP) 將加強其篩選高危險群貨櫃之機制，使用自動化系統鎖定高危險群貨櫃。為達到於出口港預先過濾高危險群貨櫃之目的，美國海關暨邊境保護局 (CBP) 已規定輸往美國之貨櫃，貨主、航商需於出口港裝船前 24 小時，向美國海關暨邊境保護局 (CBP) 傳送正確以及詳細之艙單資料，期使貨櫃裝載到美國之前可先行過濾檢查。
2. 事先檢查高危險群貨櫃方面  
美國海關暨邊境保護局 (CBP) 基於互惠合作之立場，派員進駐出口港其國家之港口，對篩選出之高危險群貨櫃，於裝船前先行檢查。
3. 使用高科技儀器作快速有效檢查高危險群貨櫃方面  
為避免在出口港檢查，而延誤出口通關與裝船作業，將使用大型貨櫃檢查儀器先行過濾檢查，以篩選出高危險群之貨櫃。
4. 使用貨櫃保全設備方面  
為確保輸美貨櫃運輸之安全，開發使用貨櫃保全裝置 (CSD) 之應用，在貨櫃上加裝可記載貨櫃保全資料之貨櫃保全裝置 (CSD) 等，俾能偵測讀取貨櫃在運送途中有無被非法入侵及遭受破壞等功能。

## (二) 海關貿易夥伴反恐計劃

「海關貿易夥伴反恐計劃 (Customs-Trade Partnership Against Terrorism ; C-TPAT)」是美國海關暨邊境保護局 (CBP)，因發生「九一一恐怖攻擊事件」後，所主張成立之自願性規範，其主要目的在於鼓勵進口業者及國際物流供應鏈者所推動之非強制性措施。該項措施係結合進口、運輸、報關、承攬、倉儲及製造廠商等，形成物流供應鏈之全面性安全網路，主要目的乃在確保整個物流供應鏈體系從起點至終點之運輸安全與資訊安全等能夠被美國海關暨邊境保護局 (CBP) 所完全掌握，以增進全球自由貿易國家間相互安全之提昇，並

防堵恐怖份子利用貨櫃做為大規模攻擊與破壞的工具<sup>[2]</sup>。

「海關貿易夥伴反恐計劃 (C-TPAT)」是美國政府與民間最大的反恐合作組織。該項新措施在2001年11月開始籌劃，於2002年4月16日正式實施。這項措施將是未來物流發展的趨勢，參與業者可享有美國海關暨邊境保護局(CBP)在安檢方面快速通關之優惠。參加「海關貿易夥伴反恐計劃 (C-TPAT)」的優點可以讓合格會員的貨櫃，運抵美國後享有快速通關的優惠，增進貨櫃流通的效率。其缺點主要在進入該組織時有申請的門檻，並非所有貨主或是物流業者皆可參加。既使參加該組織後，仍要歷經各種審核，才能成為最高等級的會員，享受免于查驗可以快速通關的優惠。

### (三) 海外港口裝運資訊事前 24 小時申報規則

美國海關暨邊境保護局(CBP)依據2002年所修正之貿易法(The Trade Act of 2002)，於2003年2月2日開始強制要求航商、貨主及承攬業者，開始實施「海外港口裝運資訊事前24小時申報規則 (24 Hour Rule)」，當貨櫃在國外出口港裝運24小時前，出口商須以自動化艙單向美國海關暨邊境保護局 (CBP) 申報艙單資料。主要以自動化篩選系統分析，先行過濾危險貨櫃以及貨物。

「海外港口裝運資訊事前24小時申報規則 (24 Hour Rule)」制度的優點，是可以增進貨櫃運送的效率；載貨證券可以以電子傳輸的方式製作或更改，整理檔的工作減少，運送人的營運效率增加；全球各國的港口當局可以直接與美國海關暨邊境保護局 (CBP) 連線，相互傳輸與查證資料。而其缺點主要在於查核貨櫃是否安全，僅以書面上的方式為之，恐怖份子有可能提供虛偽資料，因此無法完全防堵安全上的漏洞。

### (四) 港口保全法案

2006年10月美國總統布希 (George W. Bush) 簽署一項加強港口安全的法規，名為「港口保全法案 (The Security and Accountability For Every Port Act ; SAFE Port Act)」；該條款主要從三方面來保護美國港口安全，分述如下：

1. 「港口保全法案 (SAFE Port Act)」將利用科學方式加強港口實質之安全措施。海關人員能在不開櫃狀況下使用輻射偵測技術，檢測貨櫃內部之貨物狀況。
2. 該法案提供立法機關有關美國港口安全策略，將美國「貨櫃保全計劃 (CSI)」及「海關貿易夥伴反恐計劃 (C-TPAT)」納入，該二項規範分頭並行，可進一步提升貨物安全性。
3. 該法案並要求美國國土安全部 (U.S. Department of Homeland Security ; DHS) 提出計劃，當遭受恐怖份子進行攻擊後，能迅速恢復港口正常運作<sup>[3]</sup>。

#### (五) 國會九一一委員會 2007 年建議法案

2007年1月18日美國眾議院在國會第110會期第一次會議中，提出「國會九一一委員會2007年建議法案 (The 911 Commission Recommendations Act of 2007 ; 911 Commission Act)」，實質上就是港口安全法案 (SAFE Port Act) 的增修法案。美國總統布希 (George W. Bush) 在2007年8月3日已正式簽署這項法案。依據此項法案的規定，將強制要求各國出口港，必須使用大型X光 (X-Ray) 或伽瑪射線 (Gamma-Ray) 掃描機對輸美貨櫃做100%的查驗。並要求貨櫃要具備智慧型貨櫃 (Smart Container) 之功能，以便在遭逢非法入侵時能即時發出警訊。

在這項法案正式完成立法的3年內，凡是在2005年年輸出到美國的貨櫃總數量超過75,000 TEU的各國港口，都必須配合執行此項法案；而在5年之內，亦即2012年7月1日開始，要求所有港口都必須配合執行這項法案。該項法案明文要求，貨櫃要使用科技裝置以便能偵測貨櫃被非法入侵之行爲，並能夠記錄其時間，並要求國土安全部 (DHS) 需儘快制定該產品的標準要求<sup>[4]</sup>。

## 二、國際保全規範

國際海事組織 (International Maritime Organization ; IMO) 於2002年12月12日，會議通過海上人命安全國際公約 (International Convention on Safety of Life at Sea ; SOLAS) 的修正案，制定「國際船舶與港口設施保全章程

（International Ship and Port Facilities Security Code；ISPS Code）」並納入海上人命安全國際公約（SOLAS）第XI-2章「加強海上保全之特別措施」，主要在於規範船舶與港口在保全與防恐方面的管理。此章程已於2004年7月1日正式生效實施，強制要求各締約國政府均須確實遵行。

「國際船舶與港口設施保全章程（ISPS Code）」要求航商、船舶與港口之保全管理建制，至少需具備如下的功能：

1. 收集並評鑑有關保全威脅，而且與各締約國政府交換該等情報。
2. 要求船舶與港口之通訊方式的維持，以使雙方之情報及警報資訊之傳遞順暢。
3. 預防未經批准人員擅自登輪，進入港口設施與其管制區域。
4. 預防未經批准之武器、燃燒裝置或爆裂物攜入船舶或港口設施。
5. 提出發出警報之方法，以反應安全威脅及安全事故。
6. 以保全評鑑為基礎，要求船舶與港口設施之保全計劃。
7. 要求培訓、操練及演習，以確保相關人員熟悉保全計劃與程式。

「國際船舶與港口設施保全章程（ISPS Code）」實施的最終目的，是希望藉由各締約國政府、港口單位以及航運界所構建成的合作體制，共同維護保全並有效收集保全情報，來共同防阻災難、降低風險。為達保全功能，「國際船舶與港口設施保全章程（ISPS Code）」規定有嚴格的評估方法，要求船舶及港口主體均須備妥各項保全因應計劃及作業管制程式，平時做好保全措施，以因應有可能發生不同等級之保全威脅<sup>[5]</sup>。

### 三、美國貨櫃保全管理規範與國際保全規範相互關係

自從美國發生「九一一恐怖攻擊事件」之後，美國政府為防止恐怖份子使用貨櫃進行大規模之攻擊與破壞，因此率先制定與推動一系列以美國為中心之貨櫃保全管理規範，此規範主要針對輸美貨櫃之安全管理為目的而制定。而國際相關保全規範之「國際船舶與港口設施保全章程（ISPS Code）」主要針對港口設施與船舶安全管理為目的而制定。



二者保全之目標雖不盡相同，但輸美貨櫃經由國際複合運送必需經過港口、貨櫃場之存放、碼頭裝卸作業以及船舶之運送等過程，如港口設施與船舶安全管理，能依照「國際船舶與港口設施保全章程 (ISPS Code)」落實管理，則對輸美貨櫃在國際複合運送過程中之保全管理將有極大之貢獻。

以美國為中心所制定之一系列貨櫃保全管理規範與國際相關保全規範之「國際船舶與港口設施保全章程 (ISPS Code)」各自涵蓋區段、範圍與其貨櫃運送過程中各物流供應鏈間保全相互之關係，摘要如圖2所示<sup>[6]</sup>。

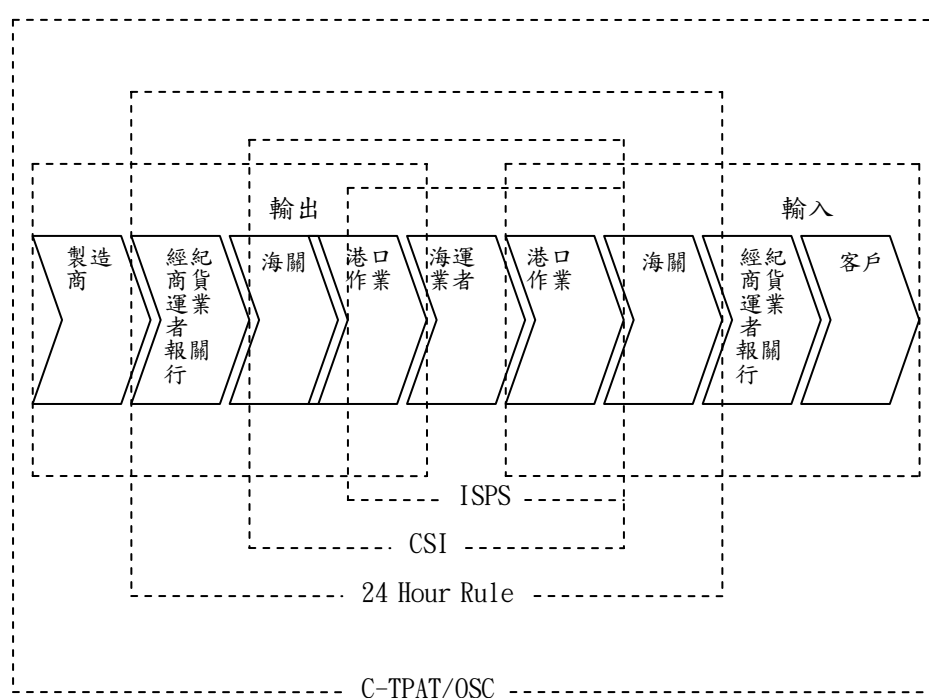


圖 2 全球供應鏈保全相關計劃範圍

資料來源：經濟部商業司 C-TPAT/SST 先導系統推動計劃執行報告。

「九一一恐怖攻擊事件」，已將戰爭帶入新的紀元，恐怖份子的攻擊隱匿性極高，且事先難以偵測其跡象而加以有效防範；而美國又為恐怖組織列為首要的攻擊目標，因而促使美國政府積極提升其國土安全管理，並徹底進行防恐、反恐政策的改革與推動。首先在體制上，成立國土安全部 (DHS) 以統籌

管理其所有國土安全事宜，其次在法規上，制定一系列以美國為中心之有關貨櫃保全管理規範，以補強國際保全規範「國際船舶與港口設施保全章程（ISPS Code）」其在貨櫃保全管理方面之功能；日後美國政府必將視國際防恐、反恐情勢之發展及其保全管理規範實施之情況，適當調整貨櫃保全管理策略。雖然目前這些一系列以美國為中心之貨櫃保全管理規範，大部份仍不具有強制性，但美國仍為國際最重要之貿易往來國家，每年輸入美國之貨櫃其數量龐大，因此航商、海運相關業者應該注意美國政府在輸美貨櫃保全管理策略方面的動向，以及早做好未雨綢繆與因應配套之措施。

### 參、貨櫃保全系統

依據「海關貿易夥伴反恐計劃（C-TPAT）」有關貨櫃保全之規範，航商必須保證其所保管的貨櫃之完整性，防止未經許可的物質或人員擅自進入。航商必須制訂適當的程序保證運輸途中其所保管的貨櫃之完整性。所有已裝船運往美國的貨櫃都必須施加一個高度安全的機械式封條（Mechanical Seal）；航商所使用的封條必須達到或超過目前國際標準組織ISO 17712有關於使用高度安全封條的規定。未來美國政府一旦公佈並實施有關封條查核和封條異常報告的規定，航商和港口、碼頭營運商都必須制訂適當的程序，以遵守相關規定的要求。

而在貨櫃檢查方面，依據「海關貿易夥伴反恐計劃（C-TPAT）」最低安全標準之規定，貨櫃裝貨前必須檢查包括檢查貨櫃櫃門的鎖閉設備其牢固之程度。航商必須在國外裝貨港以目視的方式檢查所有運往美國的空櫃，包括檢查貨櫃內部是否藏有非法物品等。在書面程序方面，航商必須確實管理其所使用的封條。未來美國政府一旦公佈並實施有關封條異常報告的規範，書面程序必需根據規範的要求，向海關暨邊境保護局（CBP）或外國相關單位報告有關已發現破損或遺失的封條和該貨櫃的實際情況。

經由「九一一恐怖攻擊事件」後，美國政府有感於使用高度安全的機械式封條仍有其保全管理不足之處，因此貨櫃保全系統已從傳統的機械式封條演進至藉由無線射頻識別（RFID）技術所研發之電子封條（E-Seal）到目前之貨櫃

保全裝置（CSD）的產品，其主要目的在輔助機械式封條不足之處，以確保貨櫃運送期間的安全無誤。

## 一、貨櫃封條之種類與應用

### （一）機械式封條

目前貨櫃運輸中使用的貨櫃封條大多是機械式封條（Mechanical Seal），它對貨櫃內的貨物安全可以作到相當的保護作用。機械式封條可區分為指示性封條、安全性封條和高度安全性封條等三種，三者的主要區別在於用封條的材料牢固程度不同。安全性封條和高度安全性封條很難被破壞，打開它需要專用的工具，而不像指示性封條只用普通的工具即可去除。貨櫃在放行或交接的時候，需要檢查封條的號碼及狀況，然後在交接的文件上進行紀錄，從而確認責任的劃分<sup>[7]</sup>。

貨櫃封條的標準為ISO 17712，主要針對貨櫃安全中關於機械式封條的分類方法、封條的認定與撤消方式建立統一的程序。在國際化的商業環境中，統一了有關貨櫃封條的相關規定。

#### 1. 機械式封條的主要特性

- （1）可追蹤性：可追蹤貨櫃封條的狀態，用來檢測貨櫃在整個運送過程中是否曾被打開。
- （2）單次使用性：機械式封條只允許一次使用，使用完後丟棄。
- （3）唯一識別性：含有辨識用標誌，如航商簡碼以及唯一的識別序號，並不得重覆。

#### 2. 機械式封條的型態

機械式封條的型態依效能測試、拉力測試、裁剪測試、彎曲測試、影響力測試可加以區分為：

- （1）指示性封條：指示性封條比起安全封條更加脆弱，只要用簡單的剪刀

等工具即可輕易的破壞，但仍可以用來檢測被破壞或曾遭受入侵。

- (2) 安全封條：安全封條對於外力的破壞較沒有抵抗能力，只能單純的用來樣樣檢測出貨櫃在運送過程中是否曾被打開。
- (3) 高度安全封條：高度安全封條是由金屬或是由金屬製纜線所構成，除非有特定的切割器具否則不容易遭外力破壞，相較於安全封條降低了被破壞的風險。

### 3. 機械式封條的種類及需求

機械式封條的種類：

- (1) 大致可分為鋼絲型封條 (Wire seal)，掛鎖型封條 (Padlock Seal)，帶狀封條 (Strap Seal)，鋼纜型封條 (Cable Seal)，螺栓型封條 (Bolt Seal)，拉緊型封條 (Cinch/Pull-up Seal)，旋轉型封條 (Twist Seal)，障礙型封條 (Barrier Seal) 等，如圖 3 所示。

#### (2) 基本需求

- 1. 堅固性及耐用性：針對安全封條及高度安全封條而言，不得出現意外毀損或提早失效等情況。
- 2. 安裝簡便性：封條安裝過程需簡單方便。
- 3. 防偽識別記號：每一個封條都需要一個唯一的永久識別標示，此識別碼不但需要能被快速的辨識，還需提供防偽偵測之功能。
- 4. 不可移除性：在非允許或封條尚未毀損的條件之下，無法移除或取下封條。
- 5. 限單次使用：除了障礙式封條之外，其他所有封條只允許單次使用。
- 6. 不可複製性：封條的設計需很難被複製及偽造。



圖 3 機械式封條樣式

資料來源：上海萬豪集裝箱封條製造有限公司。

#### 4. 識別記號

- (1) 爲了具有公證性，封條的識別記號必須由海關組織或較具權威之管理機構來認定。
- (2) 當封條一旦被購買或使用時，需馬上由其對應的海關組織給與一個唯一的序號作爲識別。
- (3) 若封條是被私有企業所使用，例如航商、製造商、貨運業者，仍需加上清晰且易辨識的唯一序號。除此之外，還需標明公司名稱或標識。

目前貨櫃運輸中使用的貨櫃封條大多是高度安全性的機械式封條，它對貨櫃內的貨物安全可以起到相當的保護作用。但在海運物流供應鏈運送期間常會發生封條遺失或遭破壞，因無主動偵測之功能，導致責任不清而航商最後需負賠償貨物損失之責<sup>[5]</sup>。

##### (二) 電子封條

電子封條 (Electronic-Seal ; E-seal) 是以機械式封條爲基礎建構，導入無線射頻識別 (RFID) 技術，經由無線射頻信號之間的傳遞，達成自動識別的特性。以無線射頻識別 (RFID) 技術研發之電子封條 (E-Seal)，其外觀如圖4所示；電子封條 (E-Seal) 主要安裝於貨櫃櫃門的把手處，如圖5所示。電子封條 (E-Seal) 主要特色在於封條插銷鎖上後一旦遭到外力裁剪或硬性破壞時，無線射頻信號即無法達成傳輸功能，在經過海運物流供應鏈所設定之管制點時將被攔截檢查。而其特殊單次使用特性，可落實貨櫃整體安全性，同時材質具有防水、防震及耐高溫之特性，強化了電子封條 (E-Seal) 整體堅固性，使貨櫃不僅達到自動識別、追蹤之功能，更提高防止貨櫃被破壞、盜竊的可能性。



圖 4 電子封條外觀圖

圖 5 電子封條安裝於櫃門之位置圖

資料來源：“Savi Networks”公司提供。資料來源：“Savi Networks”公司提供。

### 1. 電子封條的使用功能

目前的貨櫃運輸所使用之封條主要是機械式封條，在貨櫃交接時需要檢查封條號碼，封條號碼的任何變化都會在交接的文件中進行記錄，進而確定責任的歸屬。雖然機械式封條能夠起到一定的保護作用以及簡單的記錄，但因不具備無線射頻信號之裝置，因此並不能隨時隨地提供有關貨櫃具體狀態改變的時間、地點和被非法入侵的資料，而電子封條（E-Seal）卻可以提供更多類似這方面的訊息。

電子封條（E-Seal）的主要特點是使用距離短，成本低，一次性的。由於電子封條（E-Seal）之設備與功能較為簡單且不能提供持續的電力來檢測電子封條（E-Seal）的狀態，所以不能自行檢測和記錄非法入侵發生的時間，只能在通過裝有讀取器的管制點時，經由系統將訊息傳送到貨主、航商或有關的保全管理人員的電腦應用系統，提供電子封條（E-Seal）完整與否的資訊<sup>[7]</sup>。

### 2. 電子封條（E-Seal）之缺點

電子封條（E-Seal）安裝於櫃門外，除易遭受惡劣天候之影響其精確性外，也極易遭受人為之破壞。如圖 6 所示，貨櫃櫃門把手處容易被非法份子以螺絲起子將櫃門絞鏈（Door Hinge）與櫃門把手處所聯結之螺絲旋開，並不需破壞電子封條（E-Seal）或機械式封條，即可開啓櫃門進行非法入侵之行

動，事畢後再關閉櫃門回復原狀，致使電子封條（E-Seal）與機械式封條無法發揮其應有之保全功能。

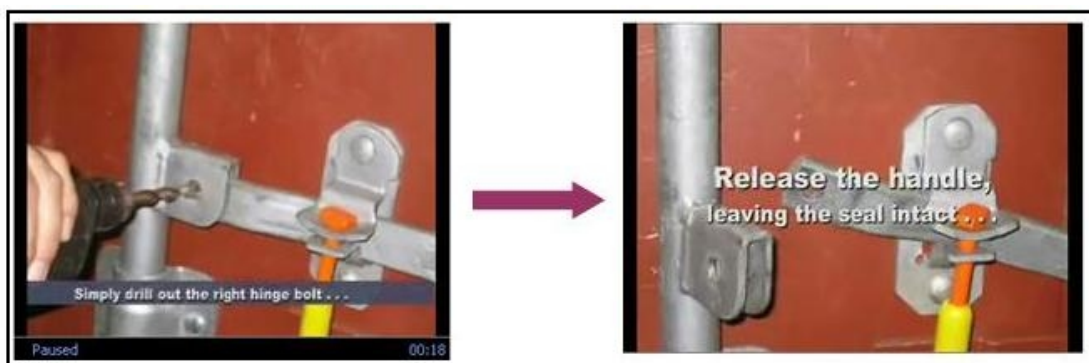


圖 6 破壞櫃門把手圖

資料來源：Henry Jen, 「U.S. Conveyance Security Device Requirement (1.2 Version)」, April 26, 2008

### （三）貨櫃保全裝置

由於電子封條（E-Seal）對於貨櫃保全防護仍有不足之處，故美國海關暨邊境保護局（CBP）另於2004年9月14日提出「智慧型貨櫃計劃（Smart Box Initiative）」。2005年5至9月間已有14家進口商參加「海關貿易夥伴反恐計劃（C-TPAT）」而成為會員，並參與1,500個貨櫃，行經19條貿易通道及6個參加「貨櫃保全計劃（CSI）」的港口，所進行的「智慧型貨櫃計劃（Smart Box Initiative）」先導測試。

「智慧型貨櫃計劃（Smart Box Initiative）」是透過無線射頻通信，配合無線射頻辨識（RFID）技術所研發出之貨櫃保全裝置（Container Security Device；CSD），而形成智慧型貨櫃（Smart Container）的計劃。依據美國海關對智慧型貨櫃（Smart Container）所下的定義：「貨櫃安裝高度安全性封條，並加裝貨櫃保全裝置（CSD）因而使其變得更聰明伶俐。」智慧型貨櫃可以經由貨櫃保全裝置（CSD）辨別合法或非法之入侵並與外界進行通訊，因此業界將廣泛地安裝無線射頻識別（RFID）技術所研發之貨櫃保全裝置（CSD）的貨櫃，稱為智慧型貨櫃（Smart Container）。



智慧型貨櫃 (Smart Container) 可對貨櫃執行預檢及保全控管，並可與全球貨物追蹤網路結合。貨櫃保全裝置 (CSD) 本身是一項具有磁性的裝置，可吸附在貨櫃的櫃門上，經手持式讀取器 (Handheld Reader) 輸入貨櫃保全資料，對於貨櫃的開啓與關閉有偵測的作用，可以在貨櫃運送途中經由裝有固定式讀取器的特定地點，如碼頭、貨櫃場等管制點，隨時回報貨櫃動態並且偵測貨櫃櫃門是否曾經被非法入侵。

因此貨主、貨櫃航商、海關皆可透過電腦應用系統了解貨櫃的即時動態以及貨櫃是否處於保全狀況。除此，貨櫃保全裝置 (CSD) 還可裝上環境感應器，以顯示記錄櫃內溫度、濕度、震動等實際狀況。在軍事方面美國國防部已引入了一批技術較簡單之貨櫃保全裝置 (CSD)，貨櫃並裝有連接電腦應用系統之無線電收發器，因而，無論在世界任何地方，貨櫃之行蹤可於瞬間透過電腦應用系統查詢。

本文特別介紹其中之一，由“Savi Networks”公司所生產的貨櫃保全裝置 (CSD) 其型號“Tag ST-676” (以下簡稱 “Tag ST-676”) 與手持式讀取器其型號“SMR-650” (以下簡稱 “SMR-650”)，如圖7所示。



圖7 貨櫃保全裝置型號-Tag ST676與手持式讀取器型號-SMR-650

資料來源：“Savi Networks”公司提供。

“Savi Networks”公司最新發明生產的“Tag ST-676”，由高性能之主動式無線射頻識別（RFID）電子標籤所組合，提供新一代貨櫃保全監測作業標準，具有主動偵測非法入侵和感應並記錄環境指數之功能。“Tag ST-676”運用於貨櫃運輸，可以使貨主、航商、海關等積極監督掌握貨櫃的動態。其主要構造：

- (1) 完整之 C 型鉗狀結構，可輕易夾在標準貨櫃之門柱上。
- (2) 感應器主體位於貨櫃櫃門之內。
- (3) 抽取式電池，密封在感應器內。
- (4) 隱蔽式天線，安裝在櫃門表面。
- (5) 蜂鳴式警報，當通過特定地點與遇有非法入侵時啟動。

“Tag ST-676”可以感應兩種不同方式的櫃門被開啓，第一種，為“Tag ST-676”之感應臂，可偵測另一扇櫃門之啓閉狀態，另一種，為入侵光線感應器，感應櫃門邊之入射光線強弱。同時“Tag ST-676”也可以偵測貨櫃內環境指數的變化，在運送階段之任何溫度、濕度、震動之狀況，使用者可以在“Tag ST-676”的感應器對環境參數做設定。若“Tag ST-676”所收集之環境參數超出設定範圍，“Tag ST-676”將超出設定範圍發生之日期、時間與警訊，在感應器之記憶體內做出事件之記錄。“Tag ST-676”的設計因具有磁性，可安裝在左邊櫃門門框之任何位置，如圖8所示。

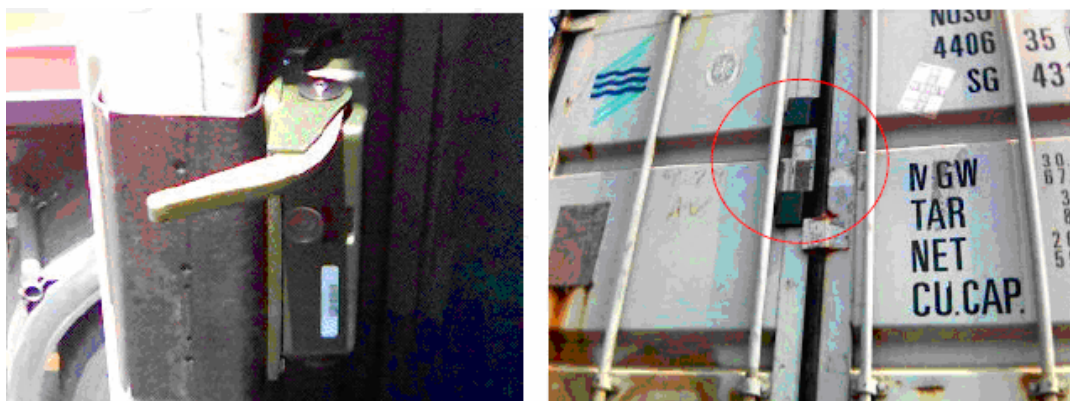


圖 8 貨櫃保全裝置裝設於貨櫃櫃門之位置

資料來源：“Savi Networks”公司提供。

“Tag ST-676” 主要功能為記錄貨櫃櫃門被開啓、關閉以及被非法入侵

的狀態與時間，設定的日期時間、設定人的帳號、解除設定的日期時間、解除設定人的帳號以達到安全控管的目的。“Tag ST-676” 並能將資訊狀態與記錄傳遞至手持式讀取器（Handheld Reader）或固定式讀取器（Fixed Reader），如圖9所示。

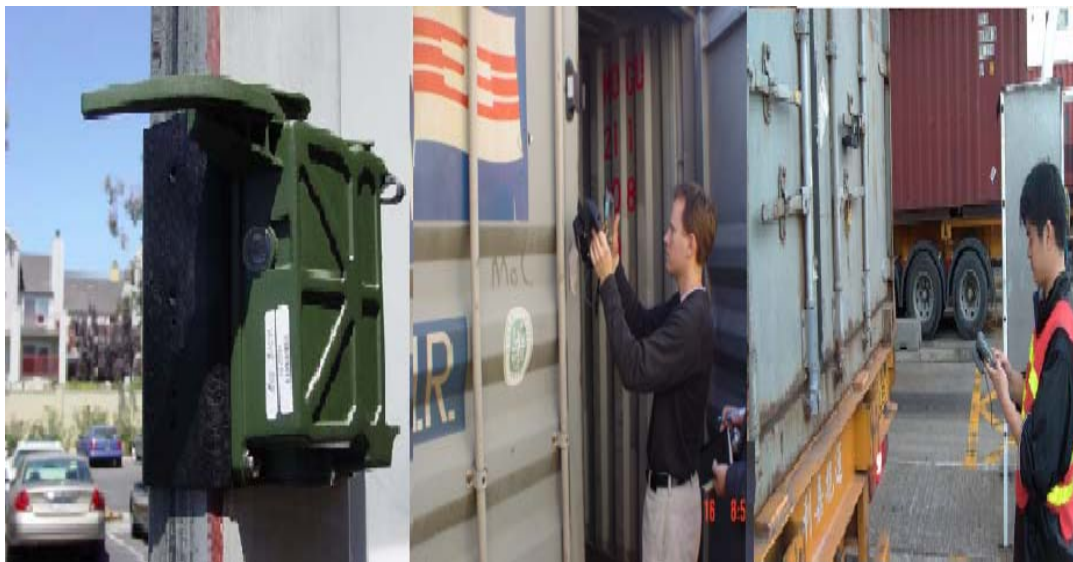


圖 9 讀取器資訊輸入與讀取圖

資料來源：“Savi Networks”公司提供。

貨櫃裝完貨物關閉櫃門後由手持式讀取器輸入貨櫃相關資訊，運送期間經由設置於各管制點，如貨櫃集散站、碼頭進出閘口與貨櫃起重機等處，經由固定式讀取器其型號為“SR-650”，可自動讀取貨櫃經過當時之資訊並記錄當時之狀態，其操作流程，如圖10所示。而手持式讀取器“SMR-650”可以直接對“Tag ST-676”做讀與寫之動作，並能對各種電子標籤做掃描與資料處理。該讀取器模組由“SMR-650”與手提電腦組成，能提供貨物即時的起始端至終點端間移動的訊息。

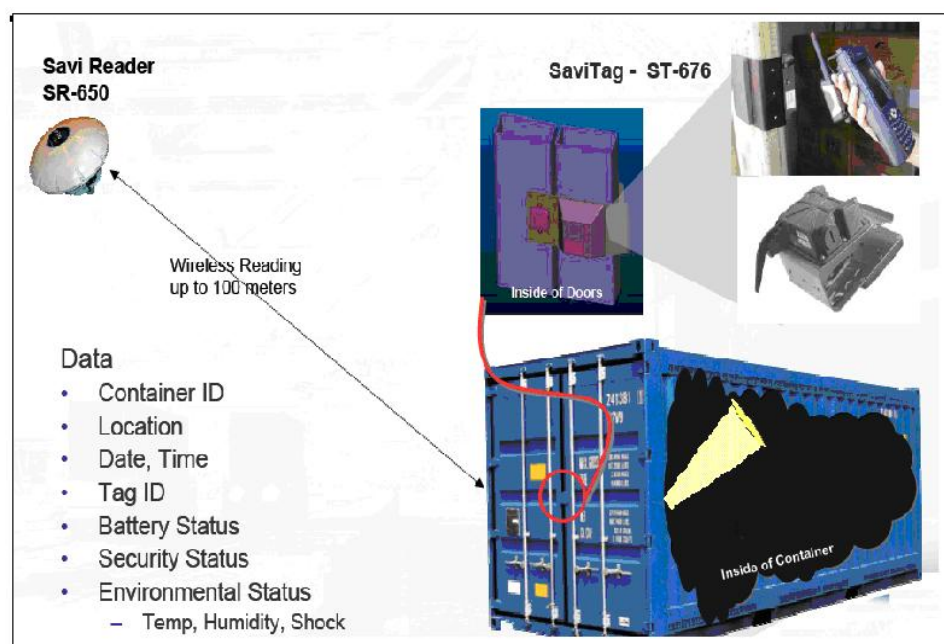


圖 10 貨櫃保全裝置與讀取器之操作流程圖

資料來源：“Savi Networks”公司提供。

## 二、無線射頻識別系統之發展

在國際物流的海、陸、空的聯運模式下，海運貨櫃需經船舶裝卸作業，貨櫃場的裝拆併櫃的處理，經過鐵、公路到科學園區、加工出口區、物流中心等組裝、分類之後再陸運至貨運倉儲中心，進行打盤作業。中間繁複的過程中，需要通過櫃場開口檢查貨櫃封條與櫃況，透過棧板容器等載運工具進行貨物的堆疊及運送等作業，如果具有辨識的資訊功能做為管理，將有助於運作過程中效率的提昇；而無線射頻識別（RFID）技術無疑具備這方面的優勢，主要在於無線射頻識別（RFID）技術使用射頻方式進行非接觸式雙向通信交換資訊，以達到識別之目的，因此完成識別工作不需人力介入，適合系統的自動化管理，且不易損壞，可以識別高速運動物體，並可同時識別多個射頻標籤，操作快速便捷，而且射頻標籤也不怕油漬、灰塵、污染等惡劣環境。因此無線射頻識別（RFID）技術已被引入日益複雜之交通做為有效率的管理，無線射頻識別（RFID）技術並已列為本世紀十大重要技術項目之一。

無線射頻識別（RFID）技術應用原理是整合簡單邏輯電路及記憶體的積

體電路晶片，搭配天線及讀取器而組成。電子標籤只要在10公分或1.5公尺左右的距離內通過讀取器，就可以透過無線通訊方式讀取資料，也因此一特性大大改善條碼直接接觸及一次僅能讀取一個的缺點。預計未來幾年無線射頻識別（RFID）系統將以其獨特的優勢，逐漸地被廣泛應用於生產、物流、交通、運輸、醫療、防偽、跟蹤設備、資產管理等需要收集和處理數據的應用領域。如全球第一大零售商美國“Wal-Mart”已要求旗下前一百大供應商於2005年1月起開始採用無線射頻識別(RFID)系統，而“IBM”；“Microsoft”；“Tesco”與日本三越百貨等公司也宣佈未來將以快速的腳步跟進。隨著大規模積體電路技術的進步及生產規模的不斷擴大，無線射頻識別（RFID）技術產品其成本將不斷降低，其應用將越來越廣泛。

而無線射頻識別（RFID）技術在海運運輸應用方面，自2001年美國紐約發生「九一一恐怖攻擊事件」以及2005年倫敦地鐵、馬德里火車爆炸案相繼發生之後，歐美國家對於進出口貿易通道安全稽核日趨嚴格，美國更將無線射頻識別（RFID）技術導入此一系列安全防護行動之中。希望藉由無線射頻識別（RFID）技術所研發之電子封條（E-Seal）與貨櫃保全裝置（CSD）做好貨櫃保全的管理。此一系列安全防護行動尚包括美國「貨櫃保全計劃（CSI）」及「海關貿易夥伴反恐方案（C-TPAT）」等相關之貨櫃保全管理規範。

全球相關港口，在以電子封條（E-Seal）的先導測試（Pilot Run）後，已驗證可提昇現階段機械式封條（Mechanical Seal）之自動化通關效率，國際標準組織（ISO）亦正訂定標準之中。但由於電子封條（E-Seal）對貨櫃保全防護方面仍有不足之處，故美國自2004年啟動「智慧型貨櫃計劃（Smart Box Initiative）」，明訂未來保全需求，希望使用保全層次更高標準的貨櫃保全裝置（CSD）能自動偵測非法入侵，經由系統通知相關單位處理，以防止恐怖份子利用貨櫃進行大規模之攻擊與破壞。對於遵守之進口商與其供應鏈成員即可享有美國海關綠色通道（Green Lane）之優惠。

### 三、無線射頻識別系統之基本工作原理

無線射頻識別（RFID）技術是一種非接觸式的自動識別技術，可以通過

無線射頻信號自動識別目標對象，獲取相關的資料，具有耐環境、可重複讀寫、非接觸式資料記錄豐富、可同時讀取範圍內多個電子標籤資料特性，而不需人工接觸、需經由光學即可完成訊息的輸入和處理，並且在操作上簡單快速。

#### (一) 無線射頻識別 (RFID) 系統之組成

無線射頻識別 (RFID) 系統通常由電子標籤 (Tag)、讀取器 (Reader)、應用系統 (Application System) 等三部份所組成。

#### (二) 基本工作流程

無線射頻識別 (RFID) 系統的基本工作流程。

1. 讀取器將無線電信號經由發射天線對外發射。
2. 當電子標籤進入發射天線的工作範圍時，電子標籤被啟動，再將電子標籤本的資訊代碼經由天線傳送出去。
3. 系統的接收天線接收到電子標籤發出的載波信號，經由天線的調節器傳送到讀寫器，讀寫器對接收到的訊息進行解調解碼，再傳送到後線的應用系統。
4. 應用系統根據邏輯推算、判斷該電子標籤的合法性，針對不同的設定做出對應的處理和控制，並發送指令信號執行機構的動作。
5. 執行機構依照應用系統的指令做出相應的動作。
6. 通過應用系統，將每個管制點聯接起來，築構成整體控制資訊平臺，依據不同項目所設計不同的軟體，完成需要實現的功能。

#### 四、無線射頻識別技術運用於貨櫃保全管理

隨著對貨物運送標準的更高要求，貨櫃運輸已快速的取代原有的傳統運輸方式，全球運輸貨櫃化的比例不斷的提高，尤其在國際運輸已經成爲最主要的運輸方式。在貨櫃運輸中每一個貨櫃都有其唯一的識別標誌，在整個運輸過程中，貨櫃的識別就是經由其櫃號來加以區別，貨櫃的交接也是依據櫃號來進

行。而在貨櫃運送過程中，人工的資料收集、處理難免會出現各式各樣的錯誤，同時人工的資料收集、處理也需要較長的時間。

而隨著貨櫃的普及化以及管理上的漏洞，貨櫃被偷竊的問題也越來越嚴重，據AXS-Alphaliner News統計，全球因貨櫃失竊所造成每年的損失高達300~500億美元，如包括間接損失每年損失高達2,000億美元左右，而即使港口操作人員十分用心，但因為工作時間的增長也會影響整個物流供應鏈的工作效率。又當海關對貨櫃進行抽驗的比率較高時，港口就會陷入癱瘓，如果降低抽查率又無法有效防止犯罪組織、恐怖份子利用貨櫃走私、運輸違禁物品或裝置毀滅性武器以進行大規模的恐怖攻擊與破壞。

這些種種事實都不符合現代化的管理，爲了增加市場競爭力，提升貨櫃的運輸效率和服務品質，以及防止恐怖份子利用貨櫃進行大規模的恐怖攻擊與破壞，貨櫃的保全管理需要一種更加自動化、智慧化與效率化的科技產品以取代目前的管理模式。無線射頻識別（RFID）技術無疑具備了這些特點，利用無線射頻識別（RFID）技術和現代化訊息技術的結合，將是貨櫃保全管理發展的一個契機，能夠對貨櫃運輸的物流和訊息流通進行跟蹤，進而消除貨櫃在運輸過程中可能產生的錯誤，因而可以加快通關的速度，提高了運輸安全性和可靠性，同時也可以嚇阻與防堵恐怖份子利用貨櫃進行大規模的恐怖攻擊與破壞的可能性，進而可以全面提升貨櫃運輸的服務與安全的品質<sup>[7]</sup>。

### 五、貨櫃保全裝置在貨櫃運輸保全管理之地位

#### （一）貨櫃運輸保全管理程式的建立

2004年9月14日美國海關暨邊境保護局（CBP）執行官 Robert C. Bonner 在第三屆美國海運安全年會上，明白表示美國海關暨邊境保護局（CBP）已成立「智慧型貨櫃計劃（Smart Box Initiative）」，並在2005年1月起開始進行相關之先導測試（Pilot Run），「智慧型貨櫃計劃（Smart Box Initiative）」除了將 ISO 17712 的機械式封條（Mechanical Seal）列爲基本要求外，並將藉由

貨櫃保全裝置 (CSD) 的裝設，在貨櫃運輸全程途中偵測貨櫃是否安全或已遭非法入侵。

依據「港口保全法案 (SAFE Port Act)」及「國會九一一委員會 2007 年建議法案 (911 Commission Act)」要求國土安全部 (DHS) 建立一套運用於貨櫃保全管理的標準，此一標準需註明作業、使用之技術以及成果的要求。所有輸美貨櫃如有安裝貨櫃保全裝置 (CSD) 都必須符合此一標準，並要建立完整的指導方針。

美國國土安全部 (DHS) 已於 2007 年 12 月 12 日，正式發佈有關運輸保全裝置 (Conveyance Security Device) 的標準要求。依據此標準要求：

1. 貨櫃保全裝置 (CSD) 必須裝置於貨櫃櫃門之內，當左邊櫃門被打開5公分時間持續超過 1 秒以上時，貨櫃保全裝置 (CSD) 之感應器需自動發出警訊。
2. 貨櫃保全裝置 (CSD) 其讀取成功率需高於 95%，誤失率需低於 4% 以下；
3. 固定式讀取器 (Fixed Reader) 讀取的距離，不得小於30.5公尺，手持式讀取器 (Handheld Reader) 讀取的距離不得小於3.05公尺。
4. 貨櫃保全裝置 (CSD) 可承受空櫃自3.05公尺重櫃自1.52公尺之高度掉落仍可使用。
5. 需可承受 -40°C 至 +70°C 之溫度變化。
6. 在車輛以每小時低於56公里的速度行進，貨櫃的資訊可被讀取器完全讀取。

依據美國國土安全部 (DHS) 所發佈運輸保全裝置 (Conveyance Security Device) 之標準要求，有關安裝貨櫃保全裝置 (CSD) 之貨櫃其運送過程、資訊傳遞、管制中心與攔截有高危險性的貨櫃之作業流程，簡要如圖 11 所示。



## 貨櫃保全裝置運用於輸美貨櫃保全管理之個案探討

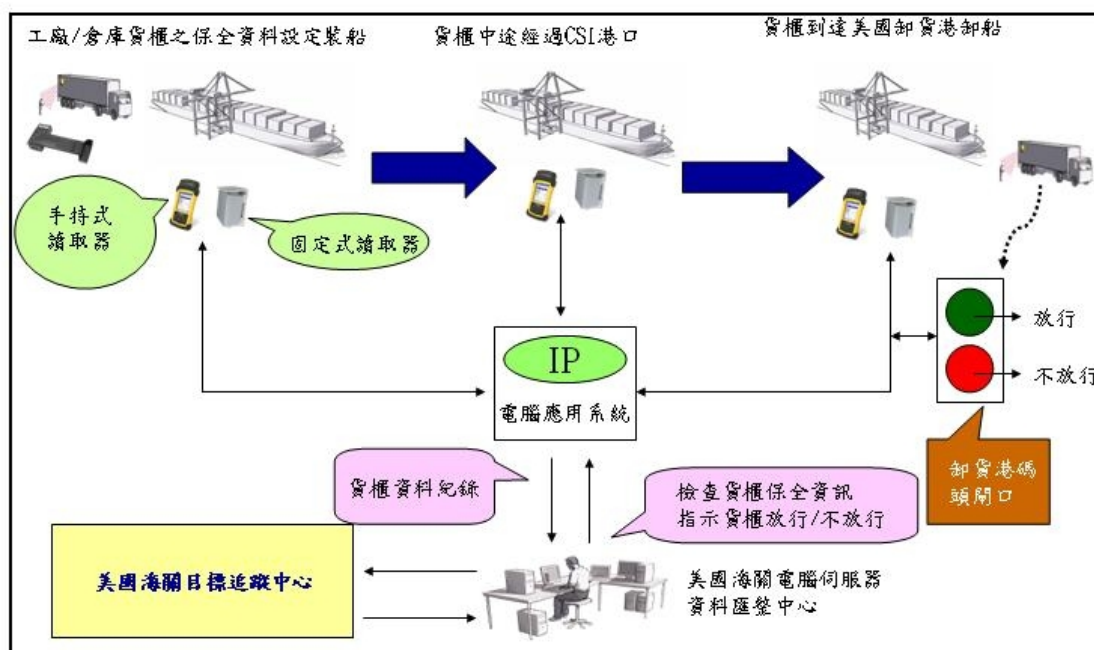


圖11 美國海關檢查輸美貨櫃流程圖

資料來源：Henry Jen, 「U.S. Conveyance Security Device Requirement (1.2 Version)」, April 26, 2008。

### (二) 航商對貨櫃保全裝置 (CSD) 導入之看法

貨櫃航商在貨櫃運輸保全管理方面，經常遭遇貨櫃運輸途中其貨櫃封條遺失、遭破壞或被更換的事件，導致貨櫃內部所承裝的貨物被偷竊或被放置走私物品，當事發後，造成其確實責任難以界定的困擾。經分析主因，在於出口貨櫃使用機械式封條加封後，若遭受任何非法入侵時，機械式封條不能傳送警訊至相關單位以做出及時與有效處理，導致在國際複合運送過程，歷經一系列複雜之作業，一旦貨櫃封條遺失、遭破壞或被更換時，很難確定事故發生的真正時間與地點，而釐清責任的歸屬。最終貨櫃航商將概括承受所有的責任。經研究分析航商要做好貨櫃運送的保安全管理，仍存在許多的困難，主要在於貨櫃進出海運相關物流供應鏈者之管制點時，仍需要藉助人力對進出之貨櫃查驗其外觀狀況及記錄封條號碼是否正確等，而每位從事此項工作的人員是否確實做好管理的工作，則不得而知。但從仍有不斷事件的發生看來，大部份的海運物流供應鏈者其配合度不高，因而無法全面落實貨櫃運輸的保全工作。

而輸美貨櫃雖依美國「海外港口裝運資訊事前 24 小時申報規則 (24 Hour Rule)」之規定，在國外裝貨港裝船前 24 小時向美國海關暨邊境保護局 (CBP) 申報艙單資料，並依美國「港口保全法案 (SAFE Port Act)」及「國會九一一委員會 2007 年建議法案 (911 Commission Act)」之規定，在裝貨港使用大型貨櫃掃描機器對輸美貨櫃進行掃描查驗，確認安全無誤後方可裝船。但輸美貨櫃裝船後並不能確保其在船舶運送期間的絕對安全，主要在於船員、碼頭工人、上船洽公人員中有可能被恐怖份子收買或偽裝潛伏，在船上利用工作之便對所承載之貨櫃進行非法之入侵，有可能進行偷竊、走私，放置毀滅性或生化武器等以進行大規模之攻擊與破壞。因此船舶在運送貨櫃期間之保全管理仍有其安全缺口而需加強防範。是以航商為防止貨櫃被利用以做為犯罪的工具，並進一步配合美國政府之有關貨櫃保全管理規範以確保本身之商業權益，唯有在貨櫃運送期間全程使用貨櫃保全裝置 (CSD) 以監控貨櫃之安全，才能徹底落實貨櫃運輸保全管理之工作。

## 肆、貨櫃保全裝置應用於貨櫃運輸之個案研究

### 一、貨櫃保全裝置導入需求與測試目的

#### (一) 導入需求

“E”航商有感於要落實貨櫃封條的管理，目前仍受一些外在因素的影響而致無法全面進行改善，因此亦希望能採用高標準的科技產品——貨櫃保全裝置 (CSD)，以確保貨櫃運送期間的安全。“E”航商經與生產貨櫃安全產品之設備供應商“Savi Networks”公司進行接觸與合作，積極研究如何配合美國政府對於海運有關貨櫃保全的管理規範及突破目前航商在貨櫃保全管理方面的受限，以提升航商之整體競爭力。

#### (二) 測試目的

##### 1. 確認貨櫃保全裝置 (CSD) 之安裝對於貨櫃保全管理之效益

經由測試從，分析貨櫃保全裝置 (CSD) 對於貨櫃保全所產生之實際效益。尤其貨櫃之保全資料其讀取成功率與誤失率是否符合美國政府相關規範之

要求。同時是否能夠保障貨櫃運送過程之安全，是否能確保貨物免於被偷竊或被利用走私，是否可以防止人為查驗之疏失並精簡人力等。

2. 貨櫃保全資料即時傳送性評估

確認“Savi Networks”公司之電腦主機是否能在雙方約定之15分鐘內傳送貨櫃保全資料至“E”航商之電腦主機。

3. 測試貨櫃保全裝置對環境偵測之功能

貨櫃保全裝置（CSD）之環境感應器可偵測並記錄貨櫃內之溫度、濕度與震動等資料，經由測試，分析其記錄是否與實際環境相符合。

4. 確認安裝貨櫃保全裝置對貨櫃防水性的影響

貨櫃保全裝置（CSD）安裝於櫃門門柱處是否會影響貨櫃原本之水密性？是否會導致貨損？有必要進行水密測試以確認內部貨物不致遭受影響。

5. 對現行之貨櫃運輸作業是否有影響

透過測試，以實際瞭解安裝貨櫃保全裝置（CSD）之貨櫃，在裝卸作業、運送過程、海關檢查、相關業者意見及是否會影響原貨櫃裝貨容積。

## 二、測試計劃與流程

### （一）測試計劃

“E”航商與“Savi Networks”公司歷經四個月的接觸、洽談與合作，主要以110個安裝貨櫃保全裝置（CSD）之輸美貨櫃的測試其所產生之效益為研究主體，分三個不同航次進行測試。

### （二）測試流程

測試研究之目的，主要在於如何提升輸美貨櫃運輸之保全管理，在流程規劃中，依據貨櫃運輸管理的使用循環進行規劃。貨櫃運輸之使用循環主要分成九大項目，如圖12所示。

除流程圖所顯示之九大流程外，由於船期及貨主所在地等因素，貨櫃可能需透過拖運的方式由某一內陸櫃場拖至另一接近港口或港口之櫃場存放以便裝船，此種拖運情況在海運業相當頻繁，其安全性不可忽視<sup>[8]</sup>。

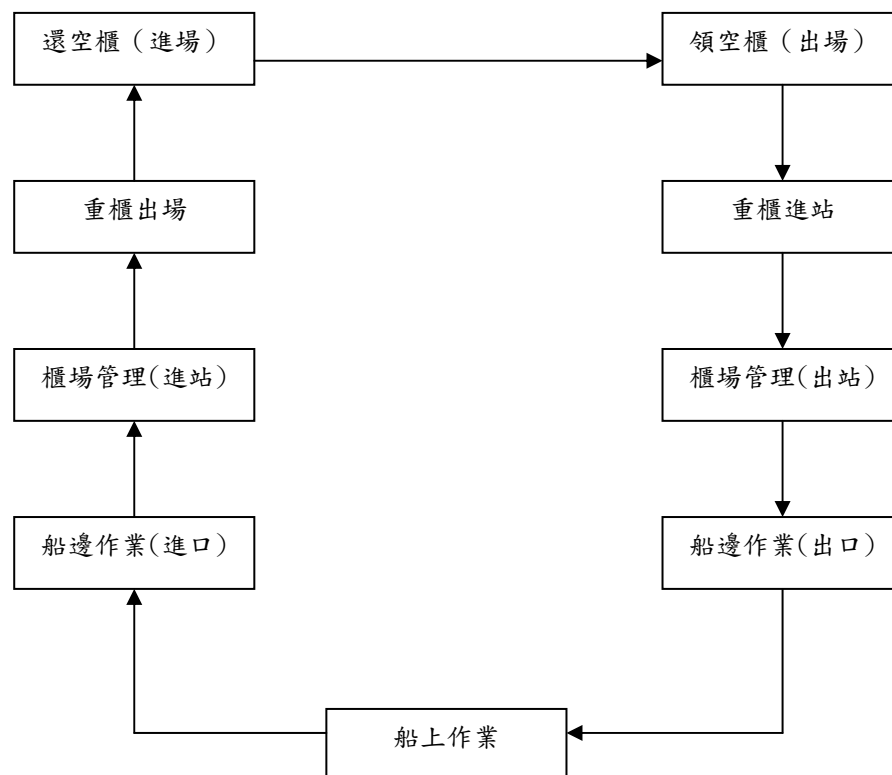


圖 12 貨櫃運輸作業之循環系統

### (三) 基本設備

在導入貨櫃保全裝置 (CSD) 前，須先在各重要管制點設置必要之基礎設備，以確保整個系統流程能夠順利進行。所需之地點與設備如下：

- 1.手持式讀取器 (Handheld Reader)：在貨主端，櫃場，碼頭等地裝設，由“Savi Networks”公司提供型號 “SMR-650” 之裝備。
- 2.固定式讀取器 (Fixed Reader)：架設在櫃場、碼頭閘門、貨櫃橋式起重機等地方。由“Savi Networks”公司提供裝備型號 “SR-650”。
- 3.電腦應用系統 (Application System)：在“Savi Networks”公司、“E”航商與貨主端等地方，安裝相關之電腦應用系統，以便相互聯繫之用。

### 三、 測試過程與結果

#### (一) 前置作業

“E”航商與“Savi Networks”公司使用約二個月的時間討論雙方合作的細節，包括貨主的選擇，固定式讀取器的安裝地點，裝、卸貨港碼頭櫃場的協調，設備供應商進行貨櫃保全裝置（CSD）的製造，向中國政府申請無線電發射設備的批准及測試安裝貨櫃保全裝置（CSD）的貨櫃其防水性能是否足夠等工作。

##### 1. 防水測試

測試“Savi Networks”公司所生產之貨櫃保全裝置（CSD）安裝在“E”航商的貨櫃其間的相容性。因櫃門門板有塑膠材質保護，以防止風浪、雨水等之滲入。而貨櫃保全裝置（CSD）需安裝在二個櫃門之間，恐壓迫櫃門之塑膠材質造成不緊密而進水，因此先安排在櫃場，經由高壓水射測試“E”航商自有之貨櫃在安裝貨櫃保全裝置（CSD）之後其水密性是否足夠，以避免運送期間受外力影響而導致貨損。經測試四個空櫃，在安裝貨櫃保全裝置（CSD）之位置及其櫃門邊並未發現有滲水現象。

##### 2. 申請中國政府核准使用無線電發射設備型號

根據中國政府之規定，為加強對進口和生產無線電發射設備的管理，凡向中國進口的無線電發射設備，或在中國境內生產的無線電發射設備，均須持有經中國訊息產業部核發的「無線電發射設備型號核准證」。出廠的無線電發射設備標示牌上須註明型號以及核准號碼等。因第一、二航次之測試起始點為中國鹽田港，因此“Savi Networks”公司必需依照規定向中國訊息產業部提出申請。經過兩個月的申請後於 2006 年 9 月取得中國訊息產業部的核准證明，可以正式合法使用。

#### (二) 測試過程

有關貨櫃保全裝置（CSD），經三航次測試之資料，如表1所示。

表1 測試船舶航次資料表

測試次數	船名/航次	鹽田/香港 開航日期	沙瓦那港 到達日期	測試櫃數	
				重櫃	空櫃
1	S.Round/077E	2006.10.15	2006.11.15	64	0
2	E.Repute/060E	2006.10.21	2006.11.22	44	0
3	E.Result/065E	2006.11.05	2006.12.05	0	12

資料來源：本研究整理。

#### 四、測試結果分析與展望

##### (一) 測試結果分析

##### 1. 貨櫃保全裝置 (CSD) 的水密性

經連續三航次的測試觀察，所有安裝貨櫃保全裝置 (CSD) 的貨櫃經過海上長程的運送，加上受冬季太平洋惡劣天氣的影響，確認於美國沙瓦那港 (Savanhan) 交貨時，所有參與測試的貨櫃與其貨物都安然無恙，證明其安裝並不影響貨櫃應有之水密性。

##### 2. 安裝貨櫃保全裝置 (CSD) 其貨櫃保全資料讀取成功率評估

表 2 貨櫃保全裝置各管制點讀取成功率

讀取地點	中國鹽田/香港開 口	中國鹽田/香港碼 頭	美國沙瓦那港開 口
第一次測試櫃量 64	31.25%*	100.00%	100.00%
第二次測試櫃量 44	86.36%*	97.72%**	97.72%**
第三次測試櫃量 2	100.00%	100.00%	100.00%
總測試櫃量 110	54.54%	99.09%	99.09%

資料來源：本研究整理。

註:

\* 表示第一、二航次，在中國鹽田港的櫃場開口讀取率不佳，主要原因在於測試期間，鹽田港的櫃場開口，因受閘門臨時性保養之影響，導致固定式讀取器無法正常運作，使得貨櫃保全資料之讀取不能有效達成而影響整體讀取

率。針對此問題，“Savi Networks”公司已進行改善並建立檢測機制，未來會自動掃描各個固定式讀取器的運作狀態是否正常。

\*\* 表示第二航次 44 個測試貨櫃中，有 1 個貨櫃的貨櫃保全裝置(CSD)之電池在裝貨工廠安裝時不慎掉落在貨櫃內，導致貨櫃保全裝置(CSD)的功能失效，故無法全程讀取貨櫃保全資料。因此該單一航次讀取成功率為 97.72% (43/44)。“Savi Networks”公司將評估與改善其電池裝備的堅固性。除此之外在第一航次與第三航次之貨櫃保全裝置(CSD)的讀取成功率皆為 100%。

經連續三航次，總共有 110 個安裝貨櫃保全裝置 (CSD) 之貨櫃參與測試，其中設定 2 個故意做入侵之開啓再關閉櫃門，1 個被美國海關臨時抽檢之貨櫃等，皆被正確讀取而無一失誤。但有一個裝有貨櫃保全裝置 (CSD) 之貨櫃，在鹽田運送途中，因受該貨櫃保全裝置 (CSD) 內電池掉落之影響，致整體讀取成功率為 99.09 % (109/110)，其讀取成效統計如表 2 所示。

- (1) 在第二航次的測試，一個裝有貨櫃保全裝置 (CSD) 的貨櫃，於沙瓦那港 (Savannah) 出櫃場開口時，被固定式讀取器偵測到此貨櫃有被入侵的狀態，並有紀錄其被入侵之時間。事後經查證，該貨櫃於出櫃場開口前七分鐘，曾被美國海關抽檢並開櫃查驗內部貨物。因此證明貨櫃保全裝置(CSD)確實能偵測貨櫃被非法入侵的狀況。
- (2) 在第三航次的測試中，有兩個裝有貨櫃保全裝置 (CSD) 的空櫃在香港裝貨港前經安排做故意入侵之動作，也在卸貨之沙瓦那港 (Savannah) 被固定式讀取器偵測到曾遭入侵之記錄。
- (3) 其餘 107 個沒有遭美國海關臨時抽檢以及做故意入侵之動作的貨櫃，在沙瓦那港 (Savanhan) 卸貨，其保全資料除讀取正常外皆顯示無入侵之紀錄。

### 3. 貨櫃保全資料即時資訊傳輸評估

“Savi Networks”公司收到參與測試之貨櫃保全資料，雙方約定必需在 15 分鐘內傳送到“E”航商的電腦主機。測試結果，貨櫃保全資料經由各地傳

送至“Savi Networks”公司其電腦主機的成功率為 100%，再傳送至“E”航商電腦主機，因部分資料被鎖住而無法如目標設定值 15 分鐘內傳送到“E”航商的電腦主機。事後“Savi Networks”公司已積極與“E”貨櫃航商研究改善方案。

#### 4. 對現行作業之影響

- (1) 本測試顯示貨櫃保全裝置 (CSD) 之安裝與卸除，對現行裝卸作業沒有任何不良之影響；同時也不影響貨櫃內原設定裝貨的容積。
- (2) 中國、香港與美國等相關碼頭工會、櫃場、海關、倉庫等相關作業單位，皆已事先知會並提出申請，因此並未發生任何抵制情形。

#### 5. 監控貨櫃環境能力評估

貨櫃保全裝置 (CSD) 對整個運送過程中之受測貨櫃所偵測及紀錄的環境數值資料，如溫度、溼度及震動等與實際狀況相吻合。此資料亦可提供日後評估貨損原因的重要參考數值<sup>[9]</sup>。

#### (二) 測試結果總結

此次測試經由二家公司的積極參與，有助於推展以無線射頻識別 (RFID) 技術所研發之貨櫃保全裝置 (CSD) 在貨櫃追蹤和保全方面的應用。經由連續三航次之實際測試結果顯示，貨櫃保全裝置 (CSD) 之讀取成功率與誤失率等成效，以及讀取器對貨櫃之偵測範圍皆能符合美國國土安全部 (DHS) 於 2007 年 12 月 12 日正式對外發佈有關運輸保全裝置 (Container Security Device) 的標準要求，從目前美國國土安全部 (DHS) 積極的行動的看來，貨櫃保全裝置 (CSD) 將是美國政府未來可能採用的重要貨櫃保全系統之一。

#### (三) 未來展望

美國「九一一恐怖攻擊事件」後，因國際政治利益的衝突仍未息止，種族、宗教間的糾紛也未曾中斷，恐怖份子仍會利用機會不斷製造矛盾與破壞，而恐



怖份子又大多藏身暗處其行蹤不易拿捏，尤其其作案時間、地點也難以事前掌握而加以有效控制。因此唯有依靠嚴謹之保全管理規範及高科技保全產品的配套使用，才能有效嚇阻與防止恐怖份子使用任何可能的手段，以進行大規模的攻擊與破壞。

海運尤其貨櫃運輸其運量龐大，通過海運各物流業者之運送關係更為複雜，如要依靠人力做好貨櫃的安全檢查工作甚為困難，是以易為恐怖份子所乘，利用貨櫃作為工具以進行大規模攻擊與破壞。因此未來如能使用經美國國土安全部（DHS）所認可之高科技產品－貨櫃保全裝置（CSD），經由其安裝可使每個輸美貨櫃如同雇用貼身保全警衛全程保護，經由其高度準確之保全監控性能與即時通報系統，對非法入侵的行為，立即進行確認，並即時傳送警訊至相關之保全單位以及早採取因應措施，可以有效防堵走私集團、恐怖份子有可能進行的偷竊、走私或進行大規模之攻擊與破壞。

貨櫃保全裝置（CSD）其未來之使用，將大幅度改變傳統貨櫃運輸的保全管理模式，不但能符合美國政府對於貨櫃運輸保全的管理規範，使美國海關暨邊境保護局（CBP）可以放心輸美貨櫃進入美國本土之安全；同時也可以讓使用者如航商、貨主、港口、櫃場經營商與相關海運物流業者等，對其貨櫃運輸過程中之保全機制確立信心；使用者如能符合美國政府之相關規定，其貨物進入美國國土並可享有美國海關快速通關之優惠，進而可加強其商業競爭能力。因此航商、貨主、港口、櫃場經營商、設備供應商與相關海運物流業者等都必需密切注意美國政府對貨櫃保全裝置（CSD）其未來正式標準的發佈與將實施之日期，以及早做好未雨綢繆的工作。

## 伍、結論與建議

### 一、 結論

本研究經以文獻分析法對貨櫃保全相關法規與文獻進行研究與分析，並以實證分析法針對輸美貨櫃使用貨櫃保全裝置（CSD）進行實際測試，以整體瞭解貨櫃保全裝置（CSD）其保全功能與成效，獲致之結論如下：

(一) 優異之保全功能，確保貨櫃運送之安全

貨櫃保全裝置(CSD)對於貨櫃運輸其保全資料的讀取成功率與誤失率等之實際成效與整體表現，皆能符合美國國土安全部(DHS)於2007年12月12日所發佈有關運輸保全裝置(Conveyance Security Device)的標準要求，可以確保貨櫃運送之安全。

(二) 確保貨櫃航商之權益與聲譽

安裝貨櫃保全裝置(CSD)的貨櫃，因其安裝可有效嚇阻或防止貨櫃被非法入侵，而導致貨物被偷竊、走私、放置毒品、毀滅性或生物性武器等不法情事之發生。如果遭受非法入侵，亦可經由偵測出之非法入侵時間點，確定國際複合運送途中各相關物流業者其責任之歸屬，進而確保貨櫃航商之合法權益與聲譽不致受損。

(三) 貨物享有美國海關快速通關之優惠

安裝貨櫃保全裝置(CSD)之輸美貨櫃，一旦遭受非法入侵，其警訊可經由電腦應用系統即時傳送至相關保全單位，以進行必要之安全控管及包括必要之攔截行動，可達事前防堵恐怖份子有可能進行之攻擊與破壞。同時安裝貨櫃保全裝置(CSD)可以符合美國海關暨邊境保護局(CBP)有關貨櫃保全管理規範之要求，貨櫃在美國港口卸岸後，可享有快速通關之優惠，強化航商、貨主全球貿易之競爭力。

(四) 防止人為疏失並可精簡人力配置

安裝貨櫃保全裝置(CSD)之貨櫃進出倉庫、櫃場、貨櫃碼頭、船邊裝卸貨作業與海關檢查站時，經由設置之固定式讀取器，可以對進出之貨櫃，讀取其貨櫃保全資料及記錄貨櫃之動態，不但可大幅度增加海關貨物檢查比率，同時亦可避免人工檢查貨櫃封條與櫃號可能產生之人為疏失與錯誤，進而可以精簡人力之配置。

(五) 特殊環境偵測功能有助於界定貨物運送責任

貨櫃保全裝置(CSD)對於溫度、濕度、震動等環境的偵測功能，其記錄有助於貨櫃運送過程，對於特殊或貴重貨物的損傷，可提供事故發生之時間與確定地點，釐清航商與海運相關物流供應鏈業者間之責任歸屬。

## 二、建議

貨櫃保全裝置（CSD）未來除可能全面使用於輸美貨櫃運輸外，其優異之保全功能並應擴及全球使用，除可防堵恐怖份子在國際間利用貨櫃進行大規模之攻擊與破壞外，並可確保使用該項裝置的航商、貨主、海運相關物流供應鏈業者之商業信譽與權益。因此國際間不論各國政府以及航商、貨主與海運相關物流業者，面對未來大環境可能的變動，應以更宏觀的角度與大方向的格局，以迎接未來的挑戰與需求。故本研究建議如下：

### （一）貨櫃保全裝置（CSD）之規格與標準需全球統一

目前貨櫃保全裝置（CSD）之各項科技規格、讀取頻率、讀取設備、作業模式、傳輸系統的規格與標準並未全球統一，造成使用業者的諸多顧慮與不便。主要因為貨櫃流動於全球各個港口和眾多的貨櫃櫃場，不同的地點採用不同之標準，影響使用業者的成本和運作的考量而降低其導入之意願。因此貨櫃保全裝置（CSD）的各項規格與標準需由國際標準組織（ISO）儘早制定並全球統一，以有所遵循。

### （二）貨櫃保全管理規範需全球一致

國際海事組織（IMO）及世界關務組織（World Customs Organization；WCO）應認真考慮以美國為中心所制定之一系列輸美貨櫃保全規範之優點，其適用範圍應納入國際相關保全規範之中，以加強目前國際保全規範在貨櫃保全管理方面之功能，並可避免國際間相互產生經濟、貿易往來不互惠之現象。

### （三）服務範圍與收費方式需明確化

貨櫃保全裝置（CSD）其設備與投資金額龐大，而全球有多達數千萬個貨櫃，使用業者必然有經濟性和負擔能力的考量，因此設備供應商需向使用業者明確說明未來長期使用或租用貨櫃保全裝置（CSD）之收費方式及其服務範圍，以便使用業者考慮如何反應在其成本之上，以進行同業間之競爭。

### （四）智慧型貨櫃（Smart Container）之推展

目前雖已有採取固定在貨櫃門柱，並可加上可感應溫度、濕度、震動、光線等之貨櫃保全裝置（CSD），但重要的是貨櫃保全裝置（CSD）不能有太高的讀取誤失率，否則無法可靠、有效的發揮保全之功能，而失去保護貨櫃安全的意義。未來國際間對於新造櫃應制定統一標準，在新造櫃櫃內即安裝必要之

內置式保全設備，可以偵測對於貨櫃任何位置之入侵，亦即貨櫃保全終極目標「智慧型貨櫃 (Smart Container)」之達成。

#### (五) 使用全球定位系統 (GPS) 傳送貨櫃保全資訊

目前以無線射頻識別 (RFID) 技術所研發之貨櫃保全裝置 (CSD) 其設立於海運各物流業者管制點所需之硬體設備，因投資金額龐大、需要定期維修及有可能被破壞之缺點，未來應考慮開發以全球定位系統 (Global Positioning system; GPS) 取代，其優點在於不需設置大量硬體設備可省卻龐大之投資金額並可避免人為破壞。一旦貨櫃遭受非法入侵，可立即傳送貨櫃保全資訊至相關保全單位處理，其涵蓋範圍可不受地理環境之限制，傳送距離可達無遠弗屆之境界。

### 參考文獻

1. 張中勇，“美國九一一事件後國土安全作為對臺灣安全之啓示”，中央警官大學，臺北市。
2. 郭淑敏，“台灣導入AEO認證機制之研究分析”，亞洲大學，2007年。
3. Koch, Christopher, “Safe Port Act Status of Implementation”, World Shipping Council, Oct. 31<sup>st</sup>, 2007.
4. “IV. International Container Security Initiatives”, Quarterly Issues Update, World Shipping Council, June 2007/September, 2007.
5. 游世青，“貨櫃定期航商營運供應鏈安全管理之研究”，碩士論文，臺灣海洋大學，基隆市，2007年。
6. 陳志誠、李明學，“RFID於貨運及港口運輸安全控管之應用”，大同大學，臺北市。
7. 周曉光、王曉華，“射頻識別(RFID)技術原理與應用實例”。
8. 連弘煉，“RFID技術應用於貨櫃運輸管理之個案研究-以陽明海運為例”，碩士論文，國立臺灣大學，臺北市，2005年。
9. “Evergreen Trial Observation and Results”, Savi Networks LLC, Jan. 5<sup>th</sup> 2007.