仁武區公所105年7月廉政電子報

仁武區公所政風室編輯

廉政天地-聯合國反貪腐公約

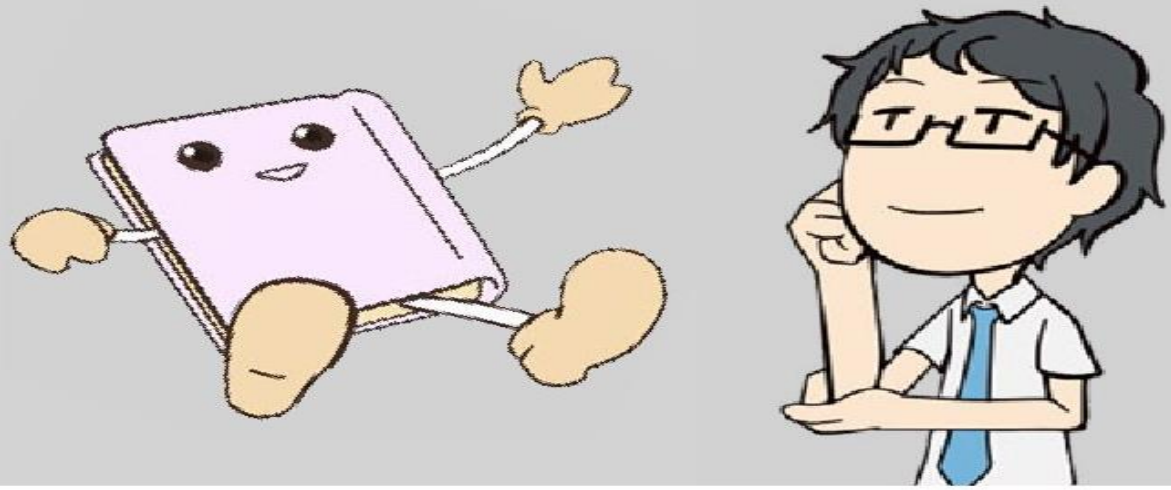
引自法務部廉政署網站

廉政小百科　法務部廉政署

聯合國反貪腐公約

「聯合國反貪腐公約」（United Nations Convention Against Corruption, UNCAC）於西元2003年10月31日聯合國大會通過，並於西元2005年12月14日生效，共計8章71條，目前共有177個締約方。為展現我國反貪腐之決心，並與現行全球反貪趨勢及國際法制接軌，更加有效地預防及打擊貪腐，總統已於104年5月20日公布本公約施行法，並於104年6月22日頒發本公約加入書，俟施行法正式施行後，本公約將正式國內法律之效力。

本公約主要在指導並提供各國政府反貪腐之法制及政策，內容包括貪腐行為的預防措施、定罪和執法、國際合作、不法資產之追回及技術援助和訊息交流等，建構出全球反貪腐法律架構，以促使世界各國共同致力於反貪腐議題。



例如國內知名企業員工集體收受回扣案及接連爆發之食安事件，引發外界關注私部門治理問題，本公約在「私部門之賄賂」（第 21 條）中強化私部門之行為規範，並在有關私部門之預防措施（第12條）內，對於不遵守規範之行為，得制定民事、刑事或行政處罰，均有助於私部門強化工作倫理，促使其誠實正直地從事商業活動。因此，本公約施行法對於我國抗制貪腐之刑事政策，有其積極正面的意義。

法務部廉政署將與各行政機關依本公約施行法規定，積極就國內法令與行政措施有不符本公約規定者，於 3 年內完成法令之制（訂）定、修正或廢止，以及行政措施之改進，共同落實本公約建立之反貪腐法律架構。

希望社會各界能給予最大的認同及支持，共同努力，期使我國及早邁入高度廉潔國家之林。

■ 廉政署結合「2016 年國際關務研討會」向各國海關人員展現我國「透明廉能」成效

法務部廉政署結合財政部關務署舉辦之「財政部 2016 國際關務研討會」(2016 International Customs Workshop)，於 2016 年 6 月 27 日上午 10 時至 12 時假財政部財政人員訓練所，規劃辦理「透明・廉能--促進海關通關便捷與課責(Transparency・Integrity -Promoting Customs Clearance Facilitation and Accountability)」專題研討。

由法務部廉政署、財政部關務署及臺灣透明組織協會，與 51 位來自薩爾瓦多、宏都拉斯、越南、泰國、印度、印尼、緬甸、聖克里斯多福及尼維斯邦聯、菲律賓、以色列等及我國海關官員，共同探討海關透明、廉能與課責的關係及我國海關落實推動透明廉能之效益。

會中廉政署副署長洪培根、財政部關務署簡任稽核趙台安及臺灣透明組織協會常務理事陳俊明，分別從「我國廉政現況」、「海關通關透明化成效」及「國際海關廉政政策」三個面向，就海關落實推動行政透明之廉能效益、世界關務組織(World Customs Organization, WCO)海關廉政策略、聯合國反貪腐公約施行法之要求及基隆關廉政評鑑結果，探討海關透明、廉能與課責的關係，並與現場來自不同國家的海關官員雙向交流。

本場研討會促進各國海關業務交流，落實海關對廉能議題之實踐，同時對於我國廉政建設成就暨海關行政透明措施之具體成效，發揮正面宣導效益，有助提倡透明、廉正、誠信的海關組織文化。

■ **相關連結：國際反貪腐法令**

公務機密維護宣導
如何防範資料庫遭隱碼攻擊

摘錄自清流月刊

■ 前言

一個美國男子把自己的姓改為 Null，就可以免費租車、免費住旅館，這麼「好」的事情，是電腦誤判，還是人為疏失？

■ 國內外皆有遭受隱碼攻擊案例

最近有一則新聞曝光度很高，一直在 Facebook 上被人轉貼，話說一位美國男子，把自己的姓改成 Null，不但可以免費租了 2 次車，還免費住了 7 次旅館，甚至於去治療牙齒也不用付錢，因為他的姓會讓電腦誤判，而通過驗證。科技新貴小潘也看到了這則新聞，想到自己的公司最近正在投入跨境電商的業務，如果使用者能把自己的名字改成特定字，就可以進入資料庫，對於未來自己的電商系統的資料安全，豈不是一大風險。於是，小潘決定利用清明假期中的師生下午茶約會，把這個問題提出來，看看有沒有什麼方法解決。

司馬特老師喝口咖啡，先針對這個事件發生的可能性進行剖析。一般的管理資訊系統一定會有資料庫來儲存資料， 資料庫都有結構化的查詢語言(Structural Query Language, SQL)，提供程式開發人員運用它的指令做資料查詢之用，當資料庫設計有缺陷時，就可能會有安全漏洞發生在應用程式的資料庫內層，如果漏洞在系統做弱點偵側時沒有被發現，就有可能在未來系統上線後，遭到有心人士的入侵。

除了國外的這個案例之外，無獨有偶地， 國內近期也有相關的報導發生， 像 2015 年底就有傳出戶政事務所的系統有 4 處 SQLInjection 漏洞，2016 年 4 月日盛證券的網站系統也發現 SQL Injection 漏洞，導致數億筆資料可能洩漏。這些事件都是有心人士利用資料庫的安全漏洞，在輸入的字串中夾帶 SQL 指令，當系統的程式疏忽沒有檢查時，這些被夾帶的指令就會被資料庫伺服器誤認為

是正常的 SQL 指令而被執行，系統就遭到入侵或破壞，也就是大家所習稱的 SQL Injection，中文又稱為隱碼攻擊。

■ 系統受到隱碼攻擊會產生什麼影響

小潘趁著司馬特老師喝咖啡的空檔，抓到機會趕快問：一旦系統遭到隱碼攻擊，會有什麼後果？司馬特老師接著解釋，系統遭到隱碼攻擊，輕者可能會造成資料表中的資料外洩，像客戶資料、密碼…等。也可能會在攻擊中取得資料庫結構或管理員的帳號，足以日後再對資料庫做下一波的攻擊。嚴重者，駭客在取得較高的系統權限後，可以在網頁中加入惡意連結，也可以修改或控制作業系統，甚至於破壞硬碟、癱瘓整個系統。

■ 針對隱碼攻擊，我們應當如何防範

小潘聽到這裏，對隱碼攻擊已經有了個初步的概念，但是應該要怎麼防範呢？司馬特老師說一般人會以為隱碼攻擊只會針對微軟的 SQL Server 做攻擊，其實不然，只要是支援 SQL 指令的資料庫伺服器，都有可能會遭到隱碼攻擊。

因此，為防範系統遭到隱碼攻擊，首先在應用程式要存取資料庫時，就要設下第一道防線，把系統的使用者與管理者的權限分開，對於應用系統的使用者，不要賦予可以建立、修改、刪除資料庫的權限，以減少隱碼攻擊帶來的損害。

其次，要加強對使用者輸入資料的內容做檢核、驗證，可以利用現有的內容驗證工具或建立一些驗證規則，針對使用者輸入一些特殊的字元，先行過濾掉，讓那些惡意攻擊的 SQL 語法無法執行。

除了對使用者設限外，系統設計時也要配合隱碼攻擊做防護，以往程式設計都習慣使用動態字串結合的方式，來組成查詢語法，無形中提供了駭客一個舞台，如果使用者輸入的查詢變數，不要直接放到 SQL 查詢語法中，而是改成參數來傳遞，或者是使用 SQLServer 內建的安全參數，也可以避免駭客輸入攻擊語法。

■ 結語

目前很多網站的架設，都是採用 3-tier 或 N-tier 的架構，因此，在每一 tier 上的驗證就很重要，系統的設計不能只在最外層驗證成功，就讓使用者可以長驅直入，為了避免隱碼攻擊，每一 tier 都應該要做驗證，驗證不通過就要立刻採取行動，才不會讓駭客輕易的入侵。

最後，要運用弱點掃描工具來協助系統開發人員，有效的發掘可能造成隱碼攻擊的漏洞，適時的加以修復，如果系統開發人員、資料庫管理人員及資安人員能夠對資安漏洞事前防範，駭客就不易侵入。

機關安全維護宣導

「『竊』中要害 小心為上」

摘錄自法務部行政執行署網站

■ 前言

您身邊一定有不少同事，把存摺、印章或提款卡放在辦公室的抽屜內，因為公家機關附近多設有提款機或銀行，刷簿子、提錢、匯款都很方便；更有不少同事將自有現金、團購集資、旅遊基金置於抽屜內，因為公務機關 24 小時都有保全巡邏，各出入口都有監視器，比家裡還安全，為貪圖方便就不帶回家了。

若您也有以上的想法及行為，請仔細研讀下列案例，因為您認為最安全的地方，可能就是最危險的地方。

■ 案例摘要

「我一早來上班，就發現抽屜有被翻過的痕跡，裡面的現金都不見了，那是我跟同事們下個月要出國旅行的基金，收齊後就要交給旅行社，沒想到…」被害員工 A 驚慌失措的說著。

「這小偷真可惡，連我抽屜裡的幾十元零錢都要偷…」被害員工 B 義憤填膺的說著。

這是發生在某縣市政府的竊盜案，賊仔哥在數月內先後光顧高雄、臺南、臺中、新竹、桃園及彰化等 6 個縣市政府，作案手法如出一轍，趁上班時間洽公民眾進出頻繁之際混入大樓內，先躲在樓梯間等隱蔽角落，待員工下班後，伺機至各樓層，發現若沒有員工在內加班，就逕行闖入，隨機打開或撬開抽屜搜刮財物。

由於賊仔哥曾經從事公務機關事務機器業務，熟悉政府單位辦公環境及作息，於某次竊盜中，被返回取物的女員工撞見，賊仔哥運用過去當維修員經驗，竟然神色自若和女員工寒暄，等女員工走後，再好整以暇的竊取財物。

後因監視錄影畫面曝光，賊仔哥的友人向警方報案而落網，竊盜背後動機是因其向地下錢莊借款 80 餘萬元，連本帶利漲至 180 萬元，只好鋌而走險，連續犯下 6 件縣市政府竊盜案，不法所得竟高達 90 餘萬元，警方至其住處取出竊得剩餘的 19 餘萬元，其餘款項多拿去抵債或花用，蒙受損失的縣市政府員工大多求償無門，只能自認倒楣。

■ 問題分析

一、 為了洽公民眾方便，公務機關於上班時間難以門禁管制，此時如何在“機關安全”及“便民服務”間取得平衡點？

二、 辦公場所內雖設有保全巡邏及監視錄影設備，就能確保人員及財物安全無虞嗎？

三、 私人貴重物品放置辦公場所內是否妥當？機關同仁的安全維護觀念是否正確？

四、 若於辦公處所內發現可疑人士時該如何處置？機關同仁是否有保持高度警覺？

消費者保護專區

金管會提醒消費者應定期檢視已投保汽車保險之保險期間及保障範圍，以確保自身權益(金融監督管理委員會)

來源：行政院消費者保護會網站

金融監督管理委員會（以下簡稱金管會）表示，暑假馬上來臨，這段時間通常是結伴出遊、或者外出讀書子女回家的高峰期，也是開車出遊的高峰期，金管會提醒民眾應定期檢視已投保相關汽車保險之保險期間及保障範圍，如已到期，應儘速洽保險公司辦理續保手續，以確保自身權益。

金管會表示，目前市場上銷售之汽車保險，除強制汽車責任保險外，也包含以下所列之任意汽車保險商品，民眾除應定期檢視已投保項目之保險期間外，亦應定期檢視投保範圍是否符合自身需求：

一、 第三人責任保險（傷害責任保險、財損責任保險）：
傷害責任保險係對被保險人因所有、使用或管理被保險汽車發生意外事故，致第三人死亡或受有體傷，就超過強制汽車責任保險給付標準以上之部分，依法應負賠償責任而請求賠償時，對被保險人負賠償之責；而財損責任保險係對被保險人因所有、使用或管理被保險汽車發生意外事故，致第三人財物受有損害，依法應負賠償責任而請求賠償時，對被保險人負賠償之責。

二、 車體損失保險：
主要類型大致可分為甲式、乙式及丙式三種，甲式的承保範圍較大，除承保汽車因碰撞、傾覆、火災、閃電、雷擊、爆炸、拋擲物或墜落物所致之損失外，亦包含第三者之非善意行為(不明車損)、不屬保險契約特別載明為不保事項之任何其他原因(不明車損)等危險事故所致之毀損滅失；乙式，則排除不明車損，範圍較甲式小；至於丙式，則僅限於被保險汽車與車輛發生碰撞、擦撞所致之毀損滅失。

三、 竊盜損失保險：
因遭受竊盜、搶奪、強盜所致之毀損滅失，對被保險人負賠償之責。

另為方便民眾投保，金管會已開放保險業者可以提供民眾透過網路投保方式，投保強制汽車責任保險、任意汽車保險，此外，提醒駕駛人於投保時，可以附加駕駛人傷害保險、乘客體傷責任保險等，以增加相關保障。