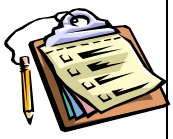
行政院原子能委員會
核能研究所
Institute of Nuclear Energy Research
Atomic Energy Council, Executive Yuan

廉政宣導雙月刊

112 年 1、2 月號

廉政倫理規範暨相關法令宣導



公務員申領或侵占小額款項個別案例分析

案情概述(一)

甲係○○部○○局○○中心組員，為受國家所屬機構依法委託，從事與委託內權限有關之公務員。

甲奉派前往外縣市觀摩會，因獲悉他中心同仁同日亦前往參加觀摩會，遂基於便利考量而搭乘他中心公務車，一同出差往返兩地。詎甲於申報該次差旅費時，明知中央政府各機關員工，因公奉派於國內出差，應按「國內出差旅費報支要點」第 5 點之規定申報差旅費，竟基於意圖為自己不法之所有及使公務員登載不實之犯意，於申報該次差旅費時，不實填載國內出差旅費報告表，申報「汽車及捷運」交通費新臺幣(下同)96 元、「火車」796 元，共計 892 元，致該中心人員審核時陷入錯誤，據以核發出差旅費，足以生損害於該中心管制出差費核發之正確性。

案情分析

本案公務員出差搭乘公務車，卻填寫不實國內出差旅費報告單，詐領差旅費，涉違反刑法第 339 條第 1 項、第 214 條、第 216 條，偵審情形為第一審有罪。(臺灣彰化地方法院 106 年易字第 482 號刑事宣示筆錄參照)

案情概述(二)

乙在○○部○○中心○○組擔任助理研究員，奉派出差外縣市參加會議。

乙明知其係搭乘友人所駕駛自小客車前往參與會議，於翌日再搭乘返回，而未搭乘高鐵往返出差地點，惟乙竟意圖為自己不

法所有而基於詐欺之犯意，不實報支出差日交通費，含高鐵費2,700元、汽車/捷運費40元及火車費50元，使該中心相關人員陷於錯誤，如數核給報支款項，乙因而詐得2,790元。

案情分析

本案公務員出差搭乘友人自小客車，卻填寫不實國內出差旅費報告單，詐領差旅費，涉違反刑法第339條第1項，偵審情形為緩起訴。(臺灣臺北地方檢察署110年度偵字第37212號檢察官緩起訴處分書參照)

案情概述(三)

丙為○○縣○○公所村幹事，係依據法令服務於地方自治團體所屬機關而具有法定職務權限之公務員。

丙於100年7月休假期間住宿於○○市旅館及刷卡加油消費2次，並用以申領強制休假補助，該鄉公所據此將補助款匯入丙之個人帳戶。詎丙竟持前揭休假加油刷卡之發票重複向村長申請村里辦公費之油料補助費，使不知情之村長陷於錯誤，同意丙請領費用，共詐得財物1,272元。

案情分析

本案公務員於休假期間刷卡加油並據以申領國旅卡休假補助後，復以同一消費事由請領村里辦公費之油料補助費，違反貪污治罪條例第5條第1項第2款；第一審判決有罪；第二、三審上訴駁回。(最高法院105年台上字第1034號刑事判決參照)

(上開案例摘自法務部廉政署111年7月15日函送「111年公務員申領或侵占小額款項宣導參考教材」)

機密視窗

您今天APP了嗎？

「小安，我最近常收到朋友傳來奇怪的訊息，裡面有些不知名的連結網址，有時候則是圖片。」在某次的下午茶聚會裡，小娜想到了最近的困擾，問她的好朋友小安有沒有遇過這種情況。聰明的小安一聽，馬上聯想到這些應該都是手機裡被安裝

惡意程式所造成的，於是問：「小娜，傳那些訊息給妳的朋友，是不是都用智慧型手機？」小娜想也不想地就回答說：「是呀，現在幾乎每個人都用智慧型手機，因為使用上很方便，以前出門如果臨時要查地圖或其他資訊，非得要帶筆記型電腦才行，現在只要一支小小的手機就可以走遍天下了！」

在現今幾乎是人手一支智慧型手機的年代，也應運而生出各式各樣的名詞，常聽見的「APP」，即是「Application」的縮寫，指應用程式或應用軟體。）

由於智慧型手機日漸普及，其功能也不再侷限於通話及簡訊的使用，增加了多媒體影音、錄影錄音、照相、遊戲、GPS定位等功能，甚至連電腦上的應用，像是瀏覽網頁、收發mail、office文書作業、網路電話、社交通訊等，都可透過智慧型手機輕鬆完成。此外，手機也可應用在電子付費、身分認證、網路銀行等。

智慧型手機是一種可以隨意安裝或移除應用軟體（APP）的手機，它擁有開放的系統環境，可讓第三方自行研發的APP，以付費或免費的方式提供給使用者自由運用；而透過這些APP軟體，使用者可以隨時隨地更新資訊，例如新聞媒體的APP點開後即可瀏覽最新的新聞訊息；社交應用類的APP可以發送免費的訊息或是撥打免費的網路電話等，因此，智慧型手機可說已完全融入現代人的生活。然而，對手機的依賴度越高，手機裡存放的私人或機密資料也就越多，而使用者對於手機的安全防護意識並未相對提高，所以對駭客來說，攻擊手機的容易度及成功率遠較電腦為高，智慧型手機自然就成了新一代駭客攻擊的目標。

儘管手機和電腦所使用的網路傳輸模式不太相同，但是駭客採取的攻擊模式卻極為類似，目前最主要的攻擊管道不外乎是SMS或MMS簡訊、作業系統或瀏覽器的安全性漏洞，亦或是仿造熱門下載的APP軟體，從中放置惡意程式等。像是之前出現過「假Skype」事件，就是針對這些高人氣軟體，在使用者不知情的情況下安裝APP後，也會自動安裝其他加值服務或是惡意程式，然後透過惡意程式自動發送

簡訊給通訊錄裡的名單，造成帳單金額暴增；而這些惡意程式也透過手機裡的通訊錄，不斷地四處發布有毒的手機簡訊或不明連結網址，一旦不小心誤點連結後，不只會讓手機遭受控制無法使用，更可能導致個人資料的外洩，造成難以想像的損失。因此，無論是電腦設備或是手機的使用，都應時時保持高度的警覺心。

為避免類此情況發生，每位使用者都應提高對安全性的敏感度，對於來路不明的手機程式不要亂安裝，若要下載應用程式，也應選擇合法的官方網站。另外，下載APP軟體前一定要先看過使用者評價，確認其安全性後再下載；如收到來路不明的簡訊，也不要打開，要立即將它直接刪除；而接受朋友傳送過來的檔案時，也必須再三確認是否為其本人，如非本人請不要隨意接受檔案。只有在使用上多一分警覺心，才能避免重要資料損毀，或造成其他方面難以估計的損失。

(本文摘錄自法務部清流月刊)

安全天地

新興威脅-無人機惡意運用之應處防護作為

邇來因滿足個人娛樂需求，運用無人機空拍風景之風氣盛行，也因此致生不少無人機之空拍意外。本文以維護國家安全及關鍵基礎設施防護為出發點，列舉出近年來因無人機使用所衍生出之安全問題，並輔以有心者可能惡意運用無人機之操作手法。

可能的隱憂與案例

無人機最大隱憂，首先在於有心人士或恐怖分子可能改造作為新式武器。試想，恐怖組織既能研製鞋底炸彈、內衣炸彈和暗藏人體的體內炸彈，改裝無人機攜帶炸彈或載具本身成為攻擊炸彈並不難。如果裝上威力強大的 C4 塑膠炸藥，或使用簡易爆炸裝置土製炸藥(Improvised Explosive Device,IED)，目標以人群聚集、政治領袖出現地點上空、機敏或關鍵基礎設施，再以遙控引爆，如此將成反恐的噩夢，後果不堪設想。

居高臨下，一覽無遺，無人機滿足了人類「想飛、想看」的慾望，隨著空拍照片、電影的盛行，無人機的蓬勃發展是新興高科技產業的發展趨勢，伴隨飛行軸、馬達、高倍數相機、無線遙控等技術的提升與整合，商業公司量產、價格低廉且獲得方式容易等因素下，無人機的普及化將成為新一代的科技產品。

在商業行為不可逆轉的潮流中，往往就產生了管理者與使用者之間的權與責，就使用者立場而言，未管制就是可「隨意」使用，此概念下所衍生之危安因素，成為管理者不得不立法、修法乃至於訂定罰則予以規範的主因，這也就是 FAA 正式推動無人機強制註冊制度，藉以確保無人機操作的「責任制」之始因。

因應未來無人機惡意操作所衍生之安全問題，相關管理單位或可依此思維，預擬對關鍵基礎設施防護中因無人機管理遭惡意運用之突發事件，尋求剋制解決之道，以確保國家安全。

(本文摘錄自法務部清流月刊)

法務部廉政署

檢舉服務專線:0800-286-586

傳真:(02)2381-1234

行政院原子能委員會核能研究所

政風室編印