

內政部國土測繪中心廉政專欄 (111.05)

本期目錄：

- 壹、 廉政檢舉管道：多元管道
- 貳、 法令園地：一般公務機密常見疑義解析
- 參、 廉政宣導小站：臺灣率先全球 公布聯合國反貪腐公約
第二次國家報告國際審查 8 月登場
- 肆、 反詐騙宣導小站：請注意近期詐騙集團假冒博客來書局
客服解除分期付款詐騙
- 伍、 資通安全視窗：2021 年具影響力的網路安全事件
- 陸、 機關安全維護宣導：行政院會通過「消防法」修正草案 翻
修 4 大重點提升安全
- 柒、 消費者服務專欄：預售屋建造期間較長 注意建商有無
履約擔保及內容
- 捌、 內政服務熱線： 1996



壹、廉政檢舉多元管道：

- 一、內政服務熱線：1996
 - 二、國土測繪中心 e-mail 檢舉信箱：k0@mail.nlsc.gov.tw
 - 三、國土測繪中心廉政檢舉信箱：臺中黎明郵局第 99 號信箱
 - 四、國土測繪中心廉政服務傳真：「 04-22592557」
 - 五、法務部廉政檢舉專線：「0800-286-586」（0800-你爆料-我爆料）。
 - 六、調查局反貪腐專線：舉報商品屯積免付費專線電話「0800-007-007」
- 「廉能是政府的核心價值，貪腐足以摧毀政府的形象，公務員應持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586 」

貳、法令園地：

一般公務機密常見疑義解析

李志強

重要概念

依據《文書處理手冊》可知，機密文書區分為國家機密文書（等級區分為絕對機密、極機密、機密）及一般公務機密文書（等級僅有密）。以下擇要說明兩者差異。

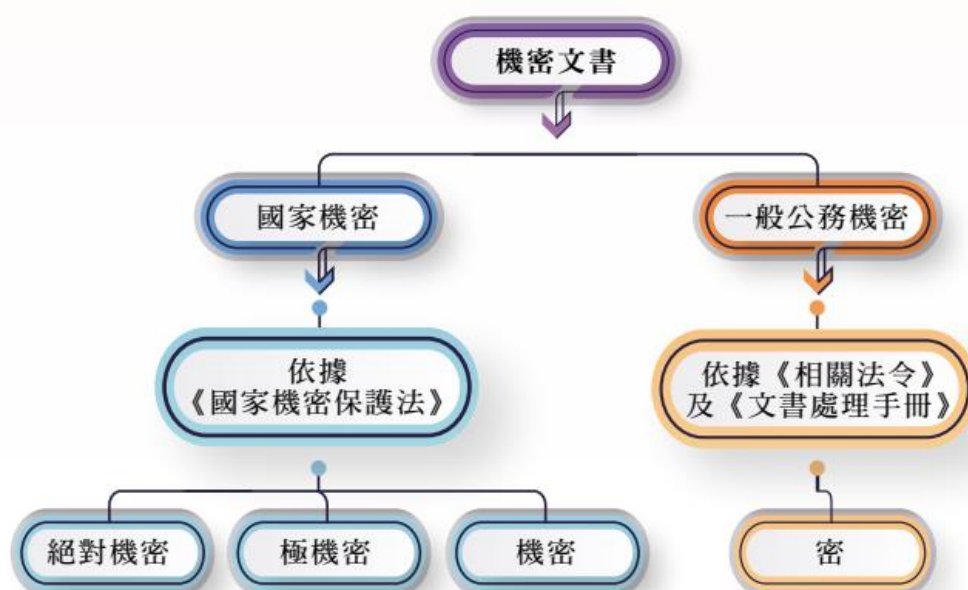
首先，在法源部分，國家機密主要是《國家機密保護法》，而一般公務機密並無專法，如《文書處理手冊》所示，各機關處理一般公務機密文書，除依法規外，依本手冊辦理，由於保密條款係散見在不同法令中，所以此自當依相關規定及《文書處理手冊》處理。

再者，就定義而言，依據《國家機密保護法》，指為確保國家安全或利益而有保密之必要，對機關持有或保管之資訊，經依本法核定機密等級者，而一般公務機密係機關持有或保管之資訊，除國家機密外，依法律或法律具體明確授權之法規命令有保密義務者。由此可知，一般公務機密即在不同法令中設予不同之定義，以營業秘密為例，依據《營業秘密法》乃指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合下列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。

其次，有關保密範圍，依據《國家機密保護法施行細則》，國家機密包括：一、軍事計畫、武

器系統或軍事行動。二、外國政府之國防、政治或經濟資訊。三、情報組織及其活動。四、政府通信、資訊之保密技術、設備或設施。五、外交或大陸事務。六、科技或經濟事務。七、其他為確保國家安全或利益而有保密之必要者。而一般公務機密因在不同法令中有所規定，致使保密範圍不一。

最後，在核定權責人員部分，依據《國家機密保護法》，各機關之人員於其職掌或業務範圍內，有應屬國家機密之事項時，應按其機密程度擬訂等級，先行採取保密措施，並即報請核定，而有核定權責人員，應於接獲報請後30日內核定之，而該法另依絕對機密、極機密、機密不同等級明定核定權責人員。一般公務機密則依《文書處理手冊》規定，由原核定機關權責主管核定之，惟實務上多是由承辦人自行判定。



常見疑義解析

由於國家機密有制定專法，故在實際執行上爭議不大，而一般公務機密因無專法，且散見在不同法令，加上規範內容不一，尤其在保密期限或解密條件多缺乏明確性，致使公務員無所適從，僅能依個人判斷或慣例處理。以下就一般公務機密常見疑義提出說明：

- 一、在核列密等之判斷標準部分：由於公文書一經核列密等將影響人民知的權利，為提升政府施政之公開與透明，增進一般民眾對公共事務之瞭解、信賴及監督，依據《文書處理手冊》及法務部之函釋，各機關核列一般公務機密應以法律或法律具體明確授權之法規為依據，以符合法律保留原則。然依目前實務狀況，在缺乏前述法律位階規範之情形下，承辦人員雖可依行政規則核列一般公務機密，惟當無行政規則得以遵循時，多仰賴承辦人員經驗法則加以判斷，恐造成相同業務是否核列密等，甚至於設定保密年限長短，皆因人而異之現象。
- 二、在一般公務機密是否訂定最高保密期限部分：因各機關業管法規保護法益之不同而採取不同保護，難以齊一規定通案性保密年限，故依法務部函釋，各機關應秉持資訊公開原則，依各該秘密事項所適用之法規滾動檢討解密。以政治檔案為例，為建立符合轉型正義精神、兼顧檔案當

事人隱私之政治檔案開放應用制度，《政治檔案條例》特別明定政府機關（構）管有政治檔案於移轉為國家檔案前，應辦理機密檔案解降密檢討，而保密逾30年且無法律依據者，應予解密。

三、在一般公務機密核定保密期限或解密條件部分：此應依所據保密之法律或法規命令核定之，但考量在法規面通常並無明確規範，所以應衡量該法律或法規命令所定保密事項涉及之保護法益核定之。申言之，目前政府機關在核定一般公務機密時，尚無明確保密期限或解密條件之具體規範，即使應衡量保密事項涉及之保護法益加以核定之，但上述規定仍過於空泛抽象，實際上恐難認定，多由承辦人員自由判斷，是否妥適不無疑慮。法務部函釋以《性侵害犯罪防治法》為例，說明該法明定因職務或業務知悉或持有性侵害被害人姓名、出生年月日等資料，除法律另有規定外，應予保密，衡諸其保護之法益為被害人隱私權，被害人死亡前該等資料均應保密，難謂一定期間經過後可予解密。法務部另舉例說明，如《營業秘密法》係為維護產業倫理與競爭秩序，調和社會公共利益，而保護營業秘密。因營業秘密之構成要件之一即為秘密性，如果知悉或持有者擅予洩漏或使用，將造成營業秘密之侵害，並使營業秘密持有人遭受相當損害。含有營業秘密之機密文書係屬一般公務機密文書，其並無保密期限上限之規定，須俟該營業秘密已非營業秘密時（亦即已不符《營業秘密法》第2條之構成要件時），才能檢討解密。



四、一般公務機密核定保密期限後，應否就實際狀況適時解密部分：對此法務部認為，若有《政府資訊公開法》、《檔案法》規定豁免公開之情形（如保護檢舉人身分、防止妨害他人生命、身體、

自由、財產、保護公共安全及社會秩序等），實體上即未達「就實際狀況適時解密」之程度，亦即保護尚無完成期限，依法應持續保密。

五、在國家機密與一般公務機密競合部分：依《文書處理手冊》規定，機密文書與非機密文書或國家機密文書與一般公務機密文書合併處理時，應以其中最高之等級為機密。亦即等級越高之機密其核密期限越長，且依前揭規定如有適用多種情形時，僅得擇一適用，如於核密時即決定其最高核密期限，除法規另有規定得展延者外，不得再行認定為其他機密再次核密。

六、在調閱他機關機密文書部分：實務上常有民意代表、各級法院、司法警察機關等，因案需要調閱他機關之機密文書，或者提供機密文書予受委託辦理公務之團體、法人或個人。此依《機密檔案管理辦法》明文，調閱機關調用機密檔案時，應備函載明法律依據、調用目的、期間、承辦人員有關聯絡資料等，且於用畢後應即歸還，而機關借出機密檔案時，應注意其安全維護及防護措施，並應以書面告知該機密檔案之機密等級及保密之義務。

The infographic is divided into several sections. At the top left, a blue box with a megaphone icon asks '你知道嗎?' (Do you know?). Below it, it states '就在104年12月23日... 性侵害犯罪防治法已經修正通過' (On December 23, 2015... the Sexual Offense Prevention Act has been amended and passed). A central message reads '任何人都都不可以揭露被害人隱私!' (No one can reveal the victim's privacy!). To the right, an illustration shows a hand holding a pen over a scale of justice. Below the main text, a white box explains that the Act mandates the confidentiality of victim names and birth dates, unless otherwise specified. It lists examples of information that can be combined to identify a victim: name, nickname, school/class, residence, network accounts, and IP address. Social media icons for Facebook, WhatsApp, Line, YouTube, Instagram, and Twitter are shown. The bottom of the infographic states that any combination of this information can identify the victim and thus reveal their identity information.

你知道嗎?
就在104年12月23日...
**性侵害犯罪防治法
已經修正通過**
任何人
都不可以揭露被害人隱私!

《性侵害犯罪防治法》明定被害人姓名、出生年月日等資料，除法律另有規定外，應予保密，其保護之法益為被害人隱私權，被害人死亡前該等資料均應保密，難謂一定期間經過後可予解密。（資料來源：衛生福利部保護服務司，<https://dep.mohw.gov.tw/dops/cp-1143-63338-105.html>）

也就是說
一個性侵害被害人照片雖然打上馬賽克...但

姓名 暱稱
學校班級 居住地
網路帳號 IP位址

以上資訊任意組合，仍然可以讓身邊親友或一般人直接識別被害人是哪一位，就是揭露被害人身分資訊

結語

從本文可知，舉凡國家機密以外之其他公務機密，皆屬一般公務機密範疇，而我國現行中央及地方（含國營事業）涉及一般公務機密之法令高達2,300餘種，其中屬於法律或法律具體明確授權之法規命令者卻占少數，可見在法律保留之原則下，實應提高其法律位階，復因《文書處理手冊》

並未就一般公務機密文書之保密期限、展延次數等加以規範，可見現行依據顯有不足。

展望未來，若能制定以一般公務機密為中心之專法，並明確區分國家機密與一般公務機密之認定標準以及相關程序，不僅有助解決當前規範不一之情況，俾使公務員在處理相關案件時有所依循，同時也避免發生公務員甚至是民眾稍一不慎洩密觸法之憾事，此亦符合罪刑法定原則，可謂一舉數得。

機密檔案	範圍	核決權責	備註
複製作業	國家機密	屬機密、極機密者，應經原核定機關或其上級機關有核定權責人員書面授權或核准	絕對機密不得複製
	一般公務機密	除辦理該機密業務者外，應經單位主管以上人員核准	
機關內部借調檔案	國家機密	除辦理該機密事項業務者外，應經原核定機關或其上級機關有核定權責人員書面授權或核准	應由調案人填具調案單提出申請
	一般公務機密	經業務承辦單位主管核准	
機關間借調檔案	國家機密、一般公務機密	經該機密核定機關首長或其授權人員核准	應以書面提出請求，並註明借調期間、承辦單位名稱、承辦人員姓名及有關聯絡資料
依法有權調用檔案	國家機密、一般公務機密	應備函載明法律依據、調用目的、調用期間、承辦單位名稱、承辦人員姓名及有關聯絡資料	

【版權為國家發展委員會檔案管理局所有】

(摘自法務部調查局清流月刊)

參、廉政宣導小站

臺灣率先全球公布聯合國反貪腐公約 第二次國家報告國際審查 8 月登場

《聯合國反貪腐公約》(United Nations Convention against Corruption, 簡稱 UNCAC) 旨在指導並提供各國反貪腐法制及政策，締約國(方)自 2009 年起，就落實公約情況，實施國別審查機制，截至 2022 年 3 月止，189 個締約國(方)中，僅 19 個締約國(方)就整部公約執行情形，完整公布第 1 次的國家報告；我國雖然不是 UNCAC 締約國，為接軌國際，展現高度廉潔承諾，2015 年通過聯合國反貪腐公約施行法自主實踐公約，2018 年自主公布「聯合國反貪腐公約首次國家報告」，並邀請 5 名國際反貪專家來臺完成國際審查，可謂國際首創；歷經 4 年持續推動，由專家

學者、民間團體與政府機關的努力下，克服疫情之挑戰，終於在本月 20 日率先全球，公布「聯合國反貪腐公約第二次國家報告」。

本次報告提出 10 項執行亮點成果，包含洗錢防制相互評鑑、亞洲公司治理評鑑、國防廉潔指數皆獲得佳績，另接軌國際推動「開放政府國家行動方案」、拓展國際刑事司法互助，同時善用我國優勢，推動機關採購廉政平臺、透明品質獎試評獎、深化廉潔教育、跨域培訓反貪人才，並落實貪腐不法所得查扣與沒收，具體回應公約與國際趨勢之要求。

本次報告也提出 5 項策進作為，將持續健全法制，如整併貪污治罪條例及刑法瀆職罪章，擬定「影響力交易」規範、推動揭弊者保護等，並建立緊急採購透明化措施並進一步落實檢察機關追訴貪腐犯罪，以符合國際反貪腐趨勢及回應社會期待。

今年 8 月 30 日至 9 月 2 日，我國將舉辦第二次國家報告國際審查會議，邀請長期投入國際組織或非政府組織，在反貪腐領域深耕並具影響力之專家，來臺進行實地審查，並就報告內容再次提出結論性意見，5 名審查委員包含國際透明組織前主席 José Ugaz(秘魯籍)將再次受邀擔任本次審查會議委員會主席，另首次加入國際透明組織國際公約部部長 Gillian Dell(美國籍)、國際透明組織紐西蘭分會執行長 Julie Haggie(紐西蘭籍)等 2 位女性專家，期待以不同性別之觀點，拓展反貪腐議題之視野，同時曾參與首次國家報告之國際專家，國際透明組織韓國分會前主席 Geo-Sung Kim(韓國籍)及美國律師協會區域反貪腐法律倡議顧問 Peter Ritchie(澳洲籍)等 2 位，亦持續參與本次審查工作，屆時 5 位國際專家將齊聚一堂，針對我國落實公約的執行情形，與我國各機關進行深入對談，我國也將結合國內來自政府、企業與民間社會力量，讓國際更瞭解我國在捍衛反貪腐普世價值之具體作為與決心，相信將會是一場相當精采之盛會。

我國反貪腐與國際接軌的腳步及決心未曾停緩，推動廉政的努力有目共睹，今年國際透明組織公布的 2021 年清廉印象指數(Corruption Perceptions Index, CPI)，我國在排名與分數上皆為歷年來最佳成績，也是國際給予肯定的最佳印證，未來將持續關注國際趨勢與公約自主實踐，使臺灣各項表現更向上提升，讓世界看見更廉潔的臺灣。

(摘自法務部廉政署新聞稿)

肆、反詐騙宣導小站

請注意近期詐騙集團假冒博客來書局客服解除分期付款詐騙

請各位鄉親朋友注意：

近日如有接獲詐騙集團假冒「博客來書局」客服人員來電
該假冒的客服人員會先透露曾經所購買書籍等交易個資取得信任後再誣稱因客服人員操作錯誤
誤『升級高級會員、經銷商』、『分期付款』、『訂單錯誤』等理由需多次扣款而要求操作『ATM』、
『網路銀行APP』或『購買遊戲點數』來『解除』相關錯誤
請勿聽信，這一定是詐騙

如有接獲『+886』來電 並電話中透露上述內容
謹記1聽、2掛、3查證
請聯繫博客來書局客服人員或撥打165反詐騙諮詢專線查證

接到假冒「**博客來書店**」來電
要求操作**ATM**或**網路銀行**解除設定
這一定是詐騙!
謹記一聽、二掛、三查證
請聯繫**博客來書店**客服人員或
撥打**165**反詐騙諮詢專線查證!

(摘自內政部警政署)

伍、資通安全視窗： 2021年具影響力的網路安全事件

◎朱惠中

2021年，網路安全行業的多事之秋

對網路安全行業而言，剛剛結束的2021年是個非常多事的一年。從年初以關鍵基礎設施為攻擊目標之「前所未有」的勒索軟體浪潮，到2021年底以臭名昭彰的Log4j漏洞結束為止（威脅並未降低），勒索軟體已對世界各地政府機關及私有企業造成嚴重且持續的威脅。

如何提昇工業控制系統 (Industrial Control System, ICS) 安全以避免關鍵基礎設施被攻擊，已成資訊安全的顯學。2021年上半年，在ICS中發現的漏洞有所增加，暴露出攻擊的高風險。同時，隨著企業持續將設備連接到互聯網並將IT系統與運營技術 (OT) 融合後，如何儘早應用美國國家標準與技術研究院 (National Institute of Standards and Technology, NIST) 所發布的資安框架 (CyberSecurity Framework, CSF) 指導範例，在新的平臺上執行辨識 (Identify)、保護 (Protect)、偵測 (Detect)、回應 (Respond) 和復原 (Recover)，將比過往任何時候都更加重要。

前事不忘後事之師，根據 darkreading 網站資料，整理2021年重大網路資安攻擊事件，指出潛在威脅並試著提出改善方案。



美國東海岸最大的油品供應商遭勒索事件

美國東海岸最大的油品供應商Colonial Pipeline 在2021年5月遭到勒索軟體攻擊，使得汽油、柴油、家用暖氣用油與軍用油品等供應均受到嚴重衝擊，影響到18州數百萬人的生活。美國聯邦機動運輸安全管理局 (Federal Motor Carrier Safety Administration, FMCSA) 在該等州發布緊急狀態，以緩解油品供應中斷問題。

美國聯邦調查局 (FBI) 確認此次攻擊的元凶是來自東歐的 DarkSide 駭客集團，其是銷售勒索軟體即服務 (RaaS) 的俄羅斯網路犯罪組織，此次攻擊除將該公司電腦系統鎖死外，DarkSide 還竊取了超過100GB的企業資料。

攻擊事件導致三成加油站都無油可賣，油品供應中斷影響車輛運輸。在 Colonial Pipeline 遭

駭客攻擊5天後，該公司依舊沒辦法完全恢復營運。為回歸正常生活，除政府發布囤積禁令外，該公司以支付440萬美元的比特幣贖金方式解決。

本事件不僅成為全球頭條新聞，而且還揭示勒索軟體攻擊能演變影響到實體世界。由於DarkSide 疑是通過利用未使用多因素身分驗證 (Multi-factor Authentication, MFA) 的帳戶，復以該公司系統建置於1960年代，資安防護效果薄弱，故駭客可輕易獲得對 Colonial Pipeline系統的存取權限。

英國資安公司Sophos專家深入研究後，對勒索軟體的防範，提供以下建議：

- 一、分析所有端點使用者的電腦，確保它們已經安裝修補程式，並要求任何遠距存取必須採用多因素驗證及限制能存取的網段。
- 二、確認系統的DMZ已經與區域網路隔離，並且鎖定伺服器不得執行PowerShell和未經授權的二進位檔案。
- 三、在所有電腦（尤其是伺服器）上執行進階端點保護。
- 四、監控所有日誌和感應器的異常活動，並追蹤警示和可疑活動，調查它們為什麼發生。
- 五、備妥備份和災難復原計畫，以防在調查過程中若發現部分系統遭駭需要離線重整，才能及時因應。

美國佛州水處理設施遭駭事件

2021年2月，駭客利用遠端桌面通訊協議 (Remote Desktop Protocol, RDP) 入侵佛州奧茲馬鎮 (Oldsmar) 內的一家水處理廠 (關鍵基礎設施) 的水質控制系統，試圖改變飲用水中氫氧化鈉 (NaOH) 的含量。值得慶幸的是，該公司值班人員適時



美國佛州一家水處理廠曾遭駭客入侵，其意圖改變飲用水中 NaOH 之添加量；皮膚若接觸未稀釋的 NaOH 會引發不適，嚴重時會造成灼傷。左圖為淨水系統示意圖，右圖為遭 NaOH 灼傷的皮膚。(Photo Credit: Blazius, https://commons.wikimedia.org/wiki/File:Sodium_hydroxide_burn.png)

發現，順利阻止受汙染的水流向公眾。這攻擊揭示了沒有安全遠端存取系統所面臨的風險，以及ICS保護措施的重要性。所幸駭客行為即時被發現，但此事已驚動白宮及聯邦調查局。

事後對該事件調查分析顯示，該廠水質控制系統密碼與該廠使用的TeamViewer軟體的預設密碼疑似相同，所以駭客利用其連上內部人員電腦，並取得該水廠操作員的存取權限，幸好，駭客作為即時被員工發現，進而取消此項作業。

這攻擊已將美國關鍵基礎設施的脆弱性暴露無遺，特別是證明了飲用水處理設施系統竟可被輕鬆地入侵。此一事件促使美國CISA向關鍵基礎設施運營商發出警告，提醒他們使用過時之桌面共享軟體或不再提供維護之軟體 (如 Windows 7) 的危險。

全球最大肉品供應商遭勒索事件

全球最大的肉類供應商JBS遭到俄國駭客RaaS集團REvil的攻擊，導致澳大利亞、加拿大和美國的工廠關閉，並摧毀了美國工廠近1/5的肉類加工能力，此次攻擊事件導致北美與澳洲地區之肉品處

理產線被迫中斷，食品價格高漲。

依iThome報導，因JBS有備份系統，故公司能即時恢復操作，JBS 也強調尚未有證據顯示客戶、供應鏈或員工的資料遭到危害或濫用。另據報導，該公司向攻擊者支付1,100萬美元的贖金，以恢復其營運能力。整起事件凸顯企業與政府機關資安系統的脆弱，駭客獅子大開口要求贖金，越來越肆無忌憚。



美國基礎設施軟體管理業者Solar Winds遭駭事件

2020年12月，傳出美國財政部與商務部遭到國家級駭客攻擊，且與這些機構所使用的IT監管平臺 SolarWinds Orion 有關；美國CISA發布緊急指令，要求所有的聯邦機構檢查網站，立即關閉或斷開所有該平臺產品。CISA指出，此事件為聯邦網路帶來了無法承受的安全風險。

SolarWinds 公司為美國專門研發系統／網路／基礎設施管理軟體的業者，全球客戶數為30萬家，包括眾多美國聯邦機構。SolarWinds 坦承安裝含漏洞版本的客戶接近1.8萬家。駭客藉由公司的安全漏洞滲透到客戶內部網路，並可藏匿於受害者系統長達數月之久。

勒索軟體的發展階段

RaaS 已成為新興的商業模式，因為它允許任何人利用漏洞並發起攻擊，它也被證明是一種有利可圖的商業模式；如同 Colonial Pipeline 與水廠事件，當營運中斷或遭惡意入侵時都可能危及生命。攻擊者瞭解到關鍵基礎設施組織是有利可圖的目標，他們不僅有足夠財力，且他們將不惜一切代價以恢復營運。

重要的是，許多民營食品飲料廠原始設計，從未考量到未來會連接到互聯網上，亦即沒有資安的設計；隨著數位化轉型，許多食品廠將實現製造流程自動化，這意味著與民眾切身相關的民生必需品供應將面臨到更大的安全威脅。

趨勢公司研究後得出以下結論：

- 一、勒索病毒是存在已久卻仍在持續演進的威脅：從 DarkSide 最近活動就能看出，今日勒索病毒在許多方面都已進化，包括更大的攻擊目標與更進階的勒索技巧。
- 二、勒索集團不再只滿足於將電腦鎖死，讓企業無法動彈來獲得贖金；現在，他們還會深入挖掘企業網路以找到更多獲利方法。例如，遭駭客入侵的雲端伺服器可能再經歷另外的攻擊流程，資料遭竊轉賣。已遭入侵的企業資產，在地下市場可說是暴利商品。

三、趨勢科技總監Jon Clay列出勒索病毒發展階段：

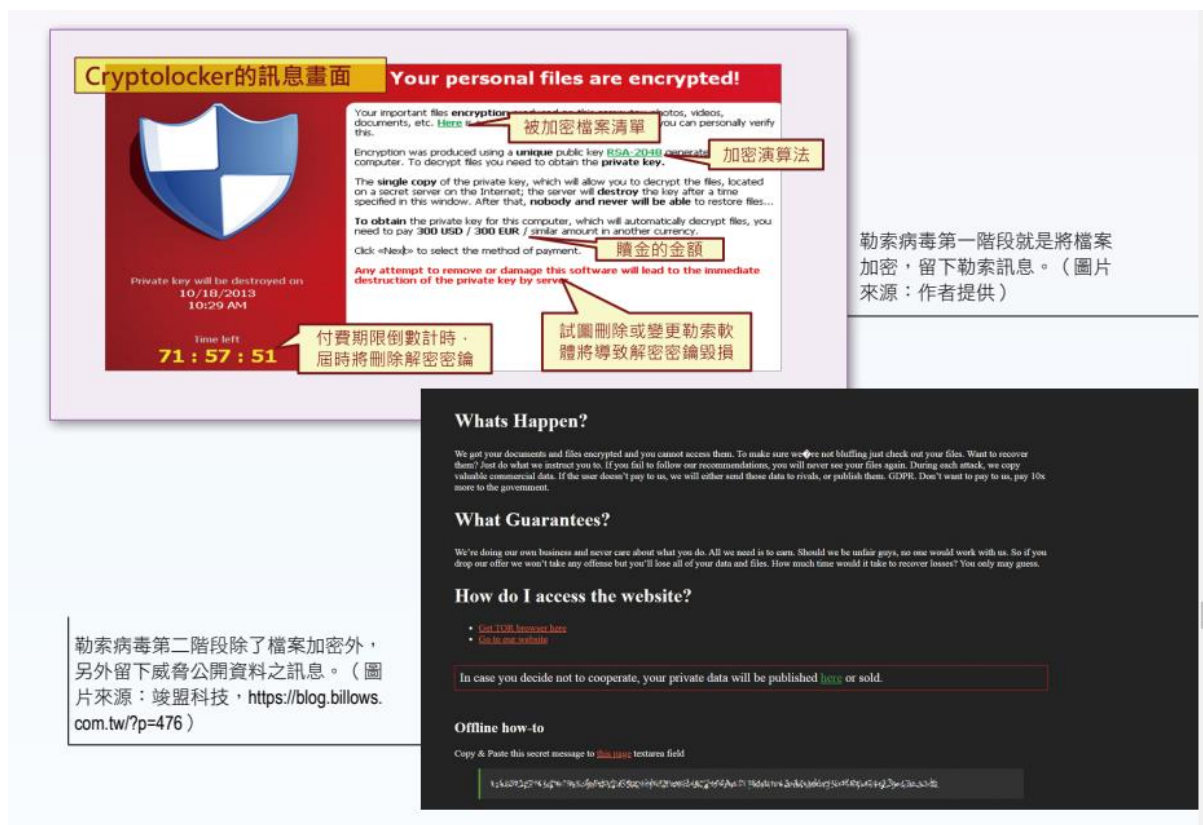
第1階段：單純只有勒索病毒。將檔案加密，留下一封勒索訊息，然後等著收錢。

第2階段：雙重勒索。第1階段+將資料外傳然後威脅公開資料。Maze是第一個採用此手法的已知案例。

第3階段：三重勒索。第1階段+第2階段+DDoS攻擊威脅。SunCrypt、RagnarLocker 和 Avaddon 是率先採用此手法的已知案例。

第4階段：四重勒索。第1階段+（可能搭配第2階段或第3階段）+直接發送郵件給受害者的客戶，或者雇用電訪中心跟客戶聯繫。

未來，勒索病毒仍會不斷演進，不幸的是，有些機構迄今仍未把網路資安列在第一順位，例如有資安專家就指出 Colonial Pipeline 仍在使用含有漏洞的舊版 Microsoft Exchange，而且還存在其他漏洞。未來，一旦民生必需服務業遭駭客攻擊，將對社會各層面帶來損害，因此，確保這類服務的安全，絕對是機關與企業的優先要務。



「供應鏈攻擊」為2022年新戰場

後疫情時代，預判有2種資安攻擊手法，除勒索軟體外，「供應鏈攻擊」亦將成為2022年的網路攻擊主流。

根據趨勢科技研究，「供應鏈攻擊」可歸納如下：

一、「供應鏈攻擊」是一種間接入侵單位的攻擊方式，網路犯罪分子會透過找尋與單位合作的第三方服務供應商，從中找到可以橫向至單位的攻擊路徑，這類攻擊存在於各種產業、生產製造、系統、軟體或委外服務架構中，目前常見的攻擊類型有：版本更新感染、派送脅持嫁接、程式庫感染、第三方元件感染、軟體漏洞及臭蟲等。

二、供應鏈資安有三大破口，分別發生在軟硬體供應鏈、產業垂直合作水平連結、外包維護廠商。

「供應鏈攻擊」將使得企業受害層面擴大至供應鏈上下游，造成企業面臨勒索事件發生時的危機處理更為艱困。

(摘自法務部調查局清流月刊)

陸、機關安全維護宣導

行政院會通過「消防法」修正草案 翻修 4 大重點提升安全

為強化公共安全，行政院會 111 年 3 月 24 日通過內政部擬具的「消防法部分條文修正草案」，將函請立法院審議。這次共修正 27 條，是消防法公布 36 年來最大幅度調整，未來修法通過後，營業場所違反消防安全將直接開罰，同時要求危險物品場所應增設安全技術人員，若發生石油煉製災害，課予業者主動通報責任，此外，也全面檢視提高違規罰責，以強化消防公權力行使，保障民眾生命財產安全。

內政部表示，為因應時空環境變遷、建築物使用形態越趨複雜及近期重大火災案例，針對消防法相關條文進行全盤檢視與檢討，其修正草案計有下列 4 大重點：

一、強化消防安全管理，營業場所違規可直接開罰 30 萬

以往營業場所消防安全設備等有故障或缺失，會先給予限期改善，未改善再予處罰，為強化營業場所負責人維護消防安全設備之責任，本次修法後不會再給予限期改善，只要檢查發現缺失就直接開罰，且罰鍰額度從原本 6 千至 5 萬元，提高到 2 萬至 30 萬元。這次修法也同步新增消防人員在第一線查核施工中消防防護計畫時，如有發生火災致生重大損害之虞，得勒令管理權人停工，防護計畫如未經所在地主管機關備查，不得擅自復工。

另考量高層建築物或地下建築物消防安全風險程度較高，規範要求此類建築應置防災中心服勤人員，其服勤人員應先經過專業機構訓練合格，並定期複訓，以確保災害發生初期，能有足夠自主應變能力。

二、健全危險物品場所管理，增設安全技術人員

為加強危險物品場所管理，這次修法增訂液化石油氣容器零售業者，需設置安全技術人員，執行供氣安全檢查，並明定其須經專業訓練合格，及定期複訓。此外，也將現行公共危險物品場所的保安監督人規定，提升至法律位階，並增訂管理權人應遴用保安檢查員，執行場所構造、設備維護及自主檢查等事項，以強化場所自主防災。

三、掌握救災資訊，提升救災效能

為掌握救災資訊，這次修法也規定消防機關得向電信事業查詢或調取待救者通信紀錄，及其個人相關資訊的權限，以利執行人命救助或緊急救護任務。此外，也規範石油煉製業等業者，若發生災變，管理權人應立即依規定通報，克盡災害通報責任，以提升救災效能。

四、全面檢視提高罰責，以強化消防公權力行使

內政部指出，因應時代變遷，全面審視並提高消防法罰責額度，包括謊報火警、營業場所消防設備或防火管理不符規定、危險物品場所違反規定或規避妨礙消防檢查及火災調查等，其最高罰鍰額度，至少提升 3 倍，最高提升至 10 倍，以強化消防公權力行使，維護公共安全。

內政部強調，這次修法幅度較大，將積極與立法院朝野各黨團溝通協調，希望能儘速完成修法，確保公共安全及民眾生命財產權益。

(摘自內政部消防署)

柒、消費者服務專欄：

預售屋建造期間較長 注意建商有無履約擔保及內容

清明連假係預售屋之熱銷期，行政院消費者保護處（下稱行政院消保處）與金融監督管理委員會檢查局（下稱金管會檢查局）就日前預售屋履約擔保機制的「不動產開發信託」、「價金信託」及「價金返還保證」辦理專案查核，發現 11 個建案 5 件有缺失，已要求建商全部改善完畢。

依照內政部公告「預售屋買賣定型化契約應記載不得記載事項」規定，預售屋的履約擔保機制有「價金返還保證」等 5 種類型。行政院消保處於去（110）年 11、12 月間，查核 24 個預售屋建案，均有辦理履約擔保，其中 11 個建案使用「不動產開發信託」、「價金信託」及「價金返還保證」，故請金管會檢查局就實質信託及保證事宜進行後續查核。查核結果發現部分建商有下列缺失：

收訖價金延遲交付信託：共計 4 件。編號 2 及 11 未於收到消費者所繳價金的次一營業日交付信託，而拖延數日。編號 4 及 6 將數月所收到的多筆價金一次交付信託。

未如期提供價金明細予信託機構：計 1 件。編號 7 拖延 1 個月才提供價金明細。

未經第三人或會計師查核：計 1 件。編號 4，依規定應定期或至少每年提供第三人或會計師之查核報告，惟迄去年 12 月間尚未經查核。

預售屋履約擔保有 5 種不同類型之多，行政院消保處在此提醒消費者，應特別注意以下事項：

一、「價金返還保證」對消費者最有利：

如採取「價金返還保證」，建商未能如期完工，將由擔保的金融機構如數返還消費者已繳價金。

二、「不動產開發信託」及「價金信託」可上網查詢信託情形：

依規定金融機構應建置網頁，提供消費者查詢所繳價金的交付信託資訊，而建商亦應於簽約時，告知網頁的查詢方式，故消費者可隨時上網查詢。

但消費者應注意，「不動產開發信託」及「價金信託」目的，係在分別確保興建資金或買方所繳價金「專款專用」，並不具有「完工保證」或「價金返還保證」的功能。且信託契約之受益人為建商，

當建商無法依約完工或交屋時，信託帳戶如有剩餘款項才會歸屬於消費者。

三、「同業連帶擔保」應注意同業間之關聯：

許多建案採用「同業連帶擔保」方式，但實務上擔保者與被擔保者如屬關係企業或同一集團，彼此間有一定關聯性，如被擔保者發生問題，擔保者的保證能力可能連帶受到影響。故消費者在購買預售屋時，應多詢問或打聽兩者間的關係，作為購屋時參考。

(摘自行政院消費者保護處)

捌、內政服務熱線：1996

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

內政部國土測繪中心政風室