公務機密
資訊安全維護

不要隨便點擊不明連結

並非所有網頁都是安全的

別忘記駭客們正潛伏在虛擬世界

等你露出破綻

資安時事案例

公部門內神通外鬼洩個資？ 確診者「精準」接到居隔書詐騙簡訊

收到支付運費電子郵件
請勿輕信填輸信用卡資料!

個人資料保護法

掌握個人資料安全守則！減少詐騙騷擾

生活中的資安

當網頁愛上人工智慧

數位學習

帳號被盜怎麼辦？後果比你想像的更嚴重！
https://www.youtube.com/watch?v=O2_ZyAw1ifQ

公部門內神通外鬼洩個資？確診者「精準」接到居隔書詐騙簡訊

出處／康健雜誌 文／康健編輯部 2022年5月10日

本土疫情海嘯般襲來，確診者逼近30萬人，接下來還會更多，奇異的是，就在收不到居隔書的民怨聲四起之際，不少確診者不約而同收到詐騙簡訊，以開立居隔書為名騙取確診者個資。由於收到簡訊的民眾都是確診者，代表名單「精準」，引發「公部門是不是有內神通外鬼？」的質疑。

一家企業的法務邱小姐5月3日確診，兩天後，她接到一封簡訊，簡訊上寫著「確診者居家照護方案，請回填基本資料，以便開立居隔通知書，若已回覆請您忽略。」簡訊並附上新北市政府關懷訊息的PDF檔連結。

（圖片來源 / 讀者提供）

「你看這簡訊，看起來是不是很可信？一般確診者是不是不太會有警覺？如果我不是法務，可能也不會懷疑，」邱小姐說，「我的個資應該已經被外洩了，它透過這個簡訊，蒐集到我完整的地址跟身份證字號，都可以去幫我辦信用卡了。」

警覺性很高的她打1922防疫專線，得知政府單位不會發這樣的簡訊，「我立刻向我的警察同學通報，請他追查這詐騙集團來源。」這位警察同學告訴她，「0987571673」這個號碼，已經被通報詐騙17次，但因這號碼是商用大量發放簡訊的號碼，不能封鎖。

邱小姐的警察同學替她通報專責偵查資訊、網路和科技犯罪的刑事警察局偵查第九大隊 ，偵九隊通知她，等她居家照護期滿出關，請她到偵九隊報案，才能分案偵辦。

除了邱小姐之外，家住苗栗的易先生也收到一樣的簡訊，他也是確診者，更神奇的是，簡訊下方所附的連結，是苗栗縣政府衛生局COVID-19專區的連結，他聽了邱小姐的個案，「這麼高度的客製化，太詭異了，你說公部門裡沒有內神通外鬼，我真的不相信，一定有很多確診民眾傻傻地回填了個資，尤其現在太多人居隔都期滿了還收不到居家隔離書。」

公部門一團亂的此刻，警方呼籲，如果你也收到這樣的簡訊，絕對不要用簡訊回報個資，各地衛生局已不會以簡訊進行疫調，從5月6日起，只有中央會以簡訊通知確診民眾，請民眾上衛福部疾病管制署的「COVID-19確診個案自主回報系統」回報個資及同住者資料。如果民眾懷疑收到類似的簡訊是詐騙簡訊，民眾可以打165，查該支門號是否有被通報詐騙，以及一共被通報幾次。

確診民眾收到簡訊填報「COVID-19確診個案自主回報系統」流程

（圖片來源 / 翻攝自疾管署官網）

詐騙跟病毒一樣猖獗

收到支付運費電子郵件 請勿輕信填輸信用卡資料!

近日詐騙集團假冒『台灣宅配通』發送電子郵件，內容為 某貨件(編號)仍在等待您的指示支付費用後將立即發貨 ，並提供點擊連結跳轉至網頁要求你輸入信用卡　　資料支付運費。

#內文很多簡體字

這是詐騙集團亂槍打鳥行騙

請民眾注意

收到不明郵件或釣魚簡訊請務必保持警覺 、先查證 ，勿輕信詐騙集團話術填輸信用卡資料，以免信用卡遭盜刷扣款。

資料來源：摘自內政部警政署 165 全民防騙網)

保護隱私　安全無慮

掌握個人資料安全守則！減少詐騙騷擾

資料來源：經濟部商業司

犯罪集團透過資料拼圖的手法，從A網站得知民眾的基本個資，從B總站得知近日消費內容，兩相組合，就可以編造天衣無縫的釣魚郵件，或精巧的詐騙話術，盡量不要讓個資被完整蒐集，就能減少被詐騙成功的機會。

公務機密維護宣導標語

依公務員服務法第4條：

公務員有絕對保守政府機關機密之義務，無論是否主管事務，均不得洩漏，退職亦同。

資料來源:清流雙月刊 39

◆社團法人台灣 E 化資安分析管理協會、嘉義大學資訊工程系教授－王智弘

要在多管齊下的誘騙中全身而退，最好的防範方式就是讓自己隔絕在威脅之外；而人工智慧是否能幫忙，一眼就看穿惡人的把戲？

原來是場騙局

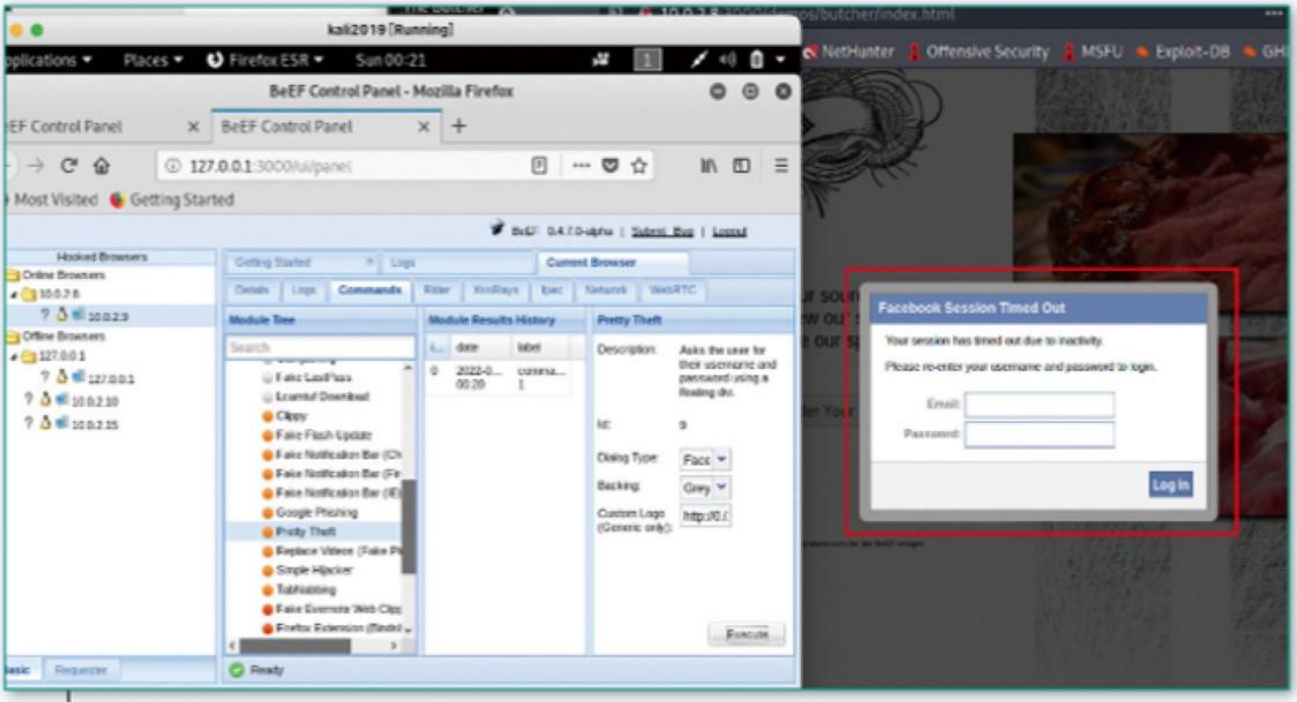
「盡信網路，不如無網路」，已成了現代人對於網路上充斥著太多假訊息，詐騙術無所不在的深沉無奈與抗議。以往享受於瀏覽網頁、沉浸在無論是文字知識的充實之樂，或是音樂影音的華麗饗宴，感受到無比的雀躍。現在卻得要處處防範、時時小心。深怕一個錯誤滑鼠的「click」，造成難以彌補的損失。在大量的影音互動所帶動的誘惑之下，詐騙的行為也因而開始升級。人們很難在多管齊下的誘騙之下能全身而退，最好的防範方式就是讓自己隔絕在這樣的威脅之外。然而，我們現今的科技足以支援這樣的服務嗎？哪些網站是有疑慮的？科技究竟能否幫我們忙，一眼就看穿惡人的把戲？

現今網路上充斥著大量假訊息，詐騙術無所不在；然而，亦有許多網站可能本身沒有惡意，但卻因為具有漏洞而遭駭客利用犯罪。

我們常聽到有一種駭客攻擊方法稱作「跨站腳本程式碼攻擊」（Cross-site Scripting, XSS），讓你看似網站是正常的，但卻是潛藏危機。這些網站可能本身是沒有惡意的，但卻因為具有漏洞（Vulnerability）而遭受了駭客栽贓的禍害。網路上種種迷幻的效果，讓人目不暇給，也讓人覺得眼見的內容竟然也非事實。譬如社交工程裡的釣魚（Phishing）手法，甚至是復刻整個網站內容以達到欺騙的目的。近期新聞便有關犯罪者製作假的銀行網站並傳送簡訊給被害者，由於太過仿真，使得好幾十人以上受騙，損失竟逾千萬元。在數位包圍下生活，我們對於實與虛、真與假、正本與副本的界線判定已退化，尋求外力協助是可以理解的想法。**「以科技解決科技所製造的問題」，看來是當前可能的藥方**，否則當有一天你發現了所有背後隱藏的攻擊程序，才驚覺，原來之前看到的那些亮麗的網路資訊，都只是個騙局。

欺騙花樣層出不窮

當你連上了惡意或是有漏洞的網站，它所能搞欺騙的花樣可謂千奇百怪。大家可能會想到的是，假的網站可能會盜取使用者的密碼。因此現在防範的方式類似透過一次性密碼（One-time Password, OTP），傳送簡訊到手機或 email 信箱。然而，實際上，駭客透過腳本程式碼，如 Java Script，可以變出許多不同的花樣，令人防不勝防。例如透過跳出式視窗（Popup Window）的社交工程方式，於網頁瀏覽



利用在 Kali Linux 中的 BeEF 工具進行漏洞利用（Exploitation）測試，出現 Session 過期的通知，誆騙使用者鍵入正確的密碼。（圖片來源：作者提供）

的時期跳出類似 Session 過期的通知，誆騙使用者鍵入正確的密碼。此外，還有多種不同型的攻擊運作，例如，透過啟動自動重新導向（Redirection）的方式或是修改 HREFs 的連線網址，讓使用者不自覺中連線到具有 Hook 的惡意網站；也有其他的手法像是開啟相機（Webcam）、播放聲音、偽造虛假的通知欄（Notification Bar）等。每個人在長期地接受這些攻擊，不禁要問，如何能還我一個乾淨的瀏覽空間，告訴我哪些網站可連，而哪些網站有安全疑慮呢？

黑名單與白名單

網站的安全評分是一直以來許多專家建議的方式。安全評分的方式透過許多綜合的指標來評估一個網站的安全性，也透過一些回報機制來登錄部分問題網站。我們可以從網路上查到許多這類的服務，包括像是針對釣魚網站的檢查，如趨勢科技。[1] 此外，Google 的「安全瀏覽」（Google Safe Browsing）每天也都會進行數十億個網站檢查，以找到可能的威脅。而像是 ScamAdviser [2] 則能夠檢測可能的釣魚及詐騙網站，相當具有準確性。另外，也有針對網站聲譽（Reputation）

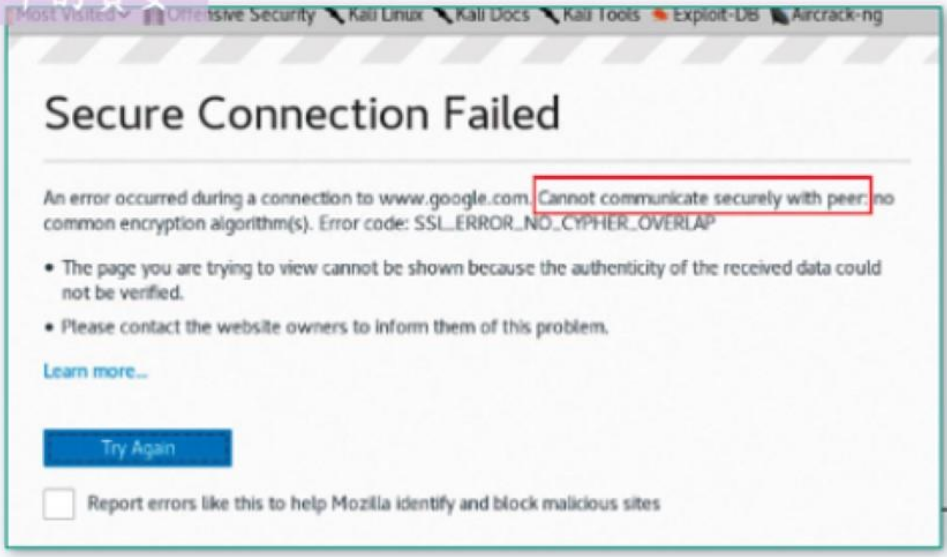
進行評分，如 URLVoid，[3] 能夠透過超過 40 個以上眾多不同的黑名單報告（Blacklist Report）資訊進行評估；亦有提供網域註冊（Domain Registration），從 whois 查詢網域資訊、Reverse DNS、ANS 以及位置資訊等。此外，著名病毒檢查網站 VirusTotal [4] 也可對於 URL 是否為惡意的情況進行檢查；而像是 Cisco Talos Intelligence [5] 也是一個相當知名的網站威脅分析工具。

上述的檢測服務，需要定期更新名單或是評估規則。因此雖基本上足夠使用，但難免也會有一些漏網之魚。此外，使用黑名單方法比較擔心的是因為檢測錯誤而導致用戶誤入有威脅的網站。另外一種方式則是建立白名單（Whitelist），只有被允許的網站或網域才能夠連上，其餘則進行攔阻。這樣做法安全性高，但對於用戶的限制也相對多，造成使用經驗與感受不佳。我們其實可以透過簡單的自救的方法，初步排除這些駭客的陷阱。

簡單自救方法

一、是否為安全加密連線？[6] 憑證（Certificate）是否有疑慮？

ScamAdviser 是一個免費的網站安全檢測服務，透過多種不同的指標來檢查網站是否安全可靠，使用者只要輸入網址就會顯示結果。（Source: https://www.scamadviser.com）



Google 網站有強制安全傳輸的機制，連線若受到攻擊，會出現連線失敗的回應。（圖片來源：作者提供）

我們鍵入網址時，可能不會加上 https:// 或是 http://，但安全網站會將其轉換成 https 的安全連線。然而有項駭客的技術稱為 SSLStrip，可透過中間人攻擊，將原來要連線至 https 的重導向而映射到 http 連線，駭客因此能夠擷取重要的傳輸機密。而目前最新技術加上強制安全傳輸的機制（HTTP Strict Transport Security, HSTS），不允許跟網站之間進行無安全加密的傳輸，如此應可避免這類攻擊。此外，若遇到安全連線時憑證有問題的情況，如類似「您的連線不是私人連線」，或者是「網站的安全性憑證不可靠」等警告頁面，也請勿按下「仍要繼續」，以免引來隱藏風險而不自知。

二、睜大眼睛注意網址

我們在連線網站之前，通常將游標放在連線處，會出現連線的 URL 資訊。[7] 建議要注意 URL 的內容，以下有幾個簡單的判斷方式：

（一）故意與某些知名網站類似，但卻有一些差異，如 go0g1e，或是 rnicro.soft.com 之類的，讓使用者產生錯亂。

（二）縮短網址（Short URLs），例如，bit.ly、TinyURL 所提供的縮短網址服務，能夠取代長網址而使得連結的交換較為便利。然而由於這類短網址掩蓋了真正網址的諸多資訊，譬如真正的域名以及隱含的參數或檔名等，因此判斷良善或惡意並不容易。[8]

（三）網址前放置令人信賴名稱，如 google 後面再加上擴增的網域名。例如 http://login.google.com.

[7] 注意有些惡意攻擊 XSS 攻擊，其連線實際上是 Submit 按鈕以及一大串的填入資料，此時要避免與其連線。

[8] 基於過去許多安全的事件也因縮短網址而起，建議連線時仍要特別留意。

myphishing.com/welcome.html，上述顯然不是 google 的網站，但前面的域名卻又與 google 登入的名稱相同，藉以混淆視聽。[9]

（四）注意特殊字元，例如是否有類似 email 的 @ 符號，或是很多的點（dot）或斜線（/, slash）。譬如一般的網址其 dot 的數量大概為 3 個，如果過多，那麼可能會是有問題的網站，如上述 google login 的例子。

（五）查詢網域名稱註冊時間是否最近才建立；若是最近註冊，應考慮駭客為釣魚而建立的新網域。

（六）要特別留意連線的 URL 是否為 IP 而非網域名稱。

三、透過評分網站檢查後再連線

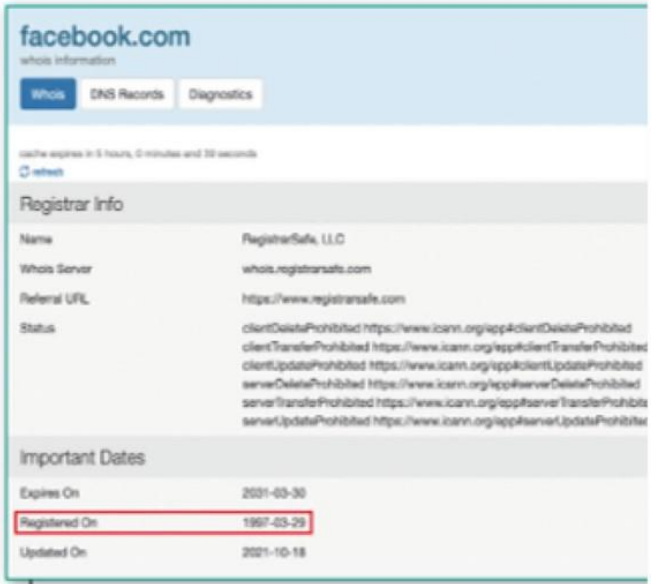
四、開網站後有問題，儘速離開

打開網站後要注意觀看內容，若有疑問，請儘速離開；然而有太多類型的攻擊是在一連線便進行，而且在極短時間內完成。

機器學習的可能與不可能

從上述的網址判別方法，可以思考透過更為自動的方式來進行。雖然目前已經有許多網站評分的服務，但若要找到潛藏的惡意網站，仍力有未逮。**透過機器學習（Machine Learning）的機制，以資料訓**

釣魚網站會故意採用與官方網站類似的網址，誘騙使用者登入，藉此竊取帳密資訊。（圖片來源：新北市政府警察局蘆洲分局，https://www.luzhou.police.ntpc.gov.tw/cp-1087-82938-23.html）



透過網域名稱註冊時間，可考慮是否為駭客為釣魚而建立的新網域；圖為 facebook.com 在 whois 所查詢的網域名稱註冊資訊。（圖片來源：作者提供）

[9] 注意 URL 長度，若網長，除了可能是上述的情況或是名稱解碼問題外，也可能是有一些惡意的參數輸入資料。

練方式替代人工制定規則，可能是對抗目前不斷激增且變異的惡意與釣魚網站的一個可選方案。

透過特徵（Feature）的篩選以及資料集的訓練，將會產生一個模型，[10] 該模型可儲存於雲端服務或是架設一臺代理伺服器（Proxy Server）以作為攔截檢查惡意連結，以及進一步深度檢測之用。圖 1 為可能的架構想法，表 1 則說明可能的特徵類型。

可以思考透過不同環境的訓練資料以強化情境分析。譬如有些惡意的連結來源是經由 Email，有一些是透過社群平臺，如 Facebook、Twitter 等，有些則是即時通訊如 Line、IG、Messenger 等，因此透過不同的訓練集或是模型參數，可以讓判斷更為精準，而若是對於網站有疑義，仍可經過一些深入的檢測模式（透過代理伺服器進行以避免用戶端身處險境）進行更為精準的判斷，提供用戶更好的安全監控及過濾服務。

網路安全與人工智慧之競合

面對科技，我們常會悠遊於它所帶來的便利，但也始終擔心它的負面效應。網

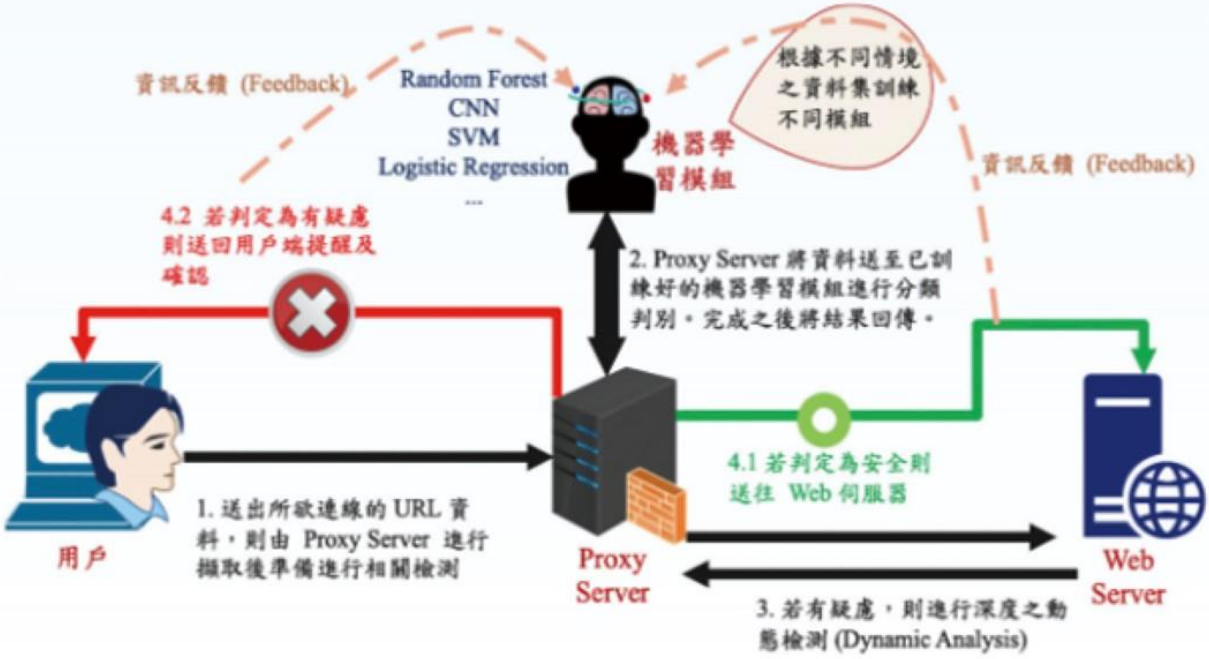


圖 1　整合機器學習的網頁安全性判別模式

[10] 如採用隨機森林（Random Forest）、卷積神經網路（Convolutional Neural Network, CNN）或其他機器學習模式。

表 1　網頁連結之安全性特徵例舉

安全性特徵	舉　例
從 URL 字面上所取得的特徵	URL 的長度、是否使用 IP 位址、是否使用縮短網址、是否有 @ 的符號、URL 中出現 '.'（dot）及 '/'（slash）次數、是否有前綴（Prefix）及後綴（Suffix）、是否使用 https 開頭、是否使用特殊的埠號（Port）等
URL 連接之網頁內容或行為	回傳網頁具有內部或外部連結的數量、是否使用跳出式視窗（Popup Window）、服務表單處理程序 Server Form Handler（SFH）是否為空白或是指向不同網域、是否啟動電子郵件服務傳遞資訊、是否載入大量外部網域之圖片、是否重導向等
網域及網站排名之相關特徵	網域名稱註冊距離現在時間、網站的名聲或排名、網站的流量大小等

路成癮、健康損害以及安全隱私的破壞都是我們所熟知的問題。然而，作為新一代科技人，我們要能夠掌握科技的脈動，要能駕馭科技而不是被科技所支配。當安全問題能夠假人工智慧之手而獲得更好的保障，這將是對抗惡意、詐欺等行為最佳的良藥解方。然而人工智慧也面臨自身系統被攻擊的問題，如最近非常熱門的研究議題—深偽技術（Deepfake），把深度學習（Deep Learning）與偽造（Fake）結合在一起，這讓依賴人工智慧為安全判斷依據的防衛方法面臨不小的威脅。「道高一尺，魔高一丈」，看來這場網路安全與人工智慧之間的競合勢必還有一大段長路要走。

社團法人台灣 E 化資安分析管理協會（ESAM）