

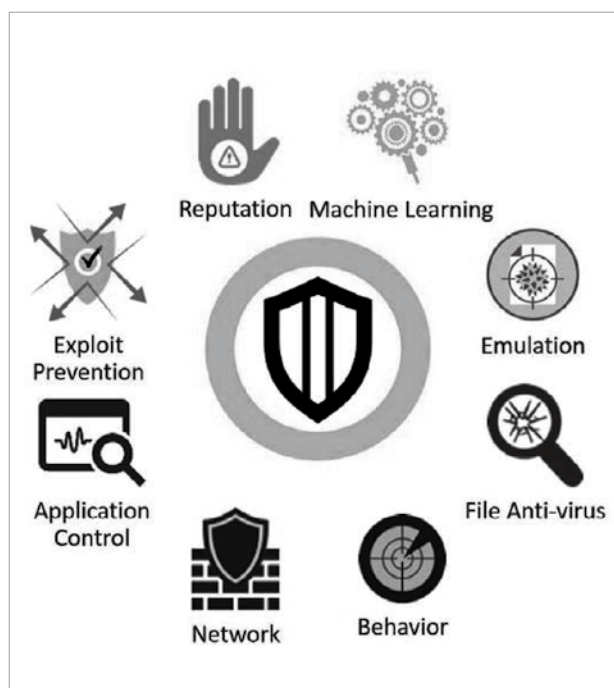
抵禦網路安全防護措施

編譯 蔡明朗
參考 趨勢科技

關注重點隱私保護

在新型高速網路通訊主機設備問市，將帶給人們無限方便，但也帶來致命的危機。無論是商業或軍事應用，全都須靠電子設備運作，資通訊保全顯得特別重要，要如何處以安全不會受到攻擊入侵，應是一門重要課題。

先前，發生了轟動國際的一銀盜領案，用戶的所有資料與存款，全都在歹徒的掌控中。只要稍有不慎，所有機構都很有可能發生個資外洩的事故，若是政府機關或企業公司的重要資料流落於有心人士的手中，未來會發生什麼重大損失，誰也不可預知。



回首 2016 過往的結束，迎向 2017 嶄新的開始，隱私保護議題仍不斷被提起，小從蔚為風潮，從 8 歲到 80 歲都人手一抓的寶可夢，是否藉由存取過多的個人資料，而有隱私、甚至是機密的外洩疑慮，大至轟動國際的一銀盜領案，用戶資料及銀行內的現金，如電影情節般，僅透過駭客於彈指之間，便竊取大量用戶資料，進而對銀行獲消費者重大損害；同時，亦不論你是政府機關或企業公司，只有稍有不慎，便有可能發生個資外洩事故，或發生員工監守自盜的情況，而使組織蒙受損失，而違法者更有被判刑的可能。因此，個人資料與資訊安全維護的需求，在新的一年仍應是持續關注的重點。

網路安全威脅無遠弗屆

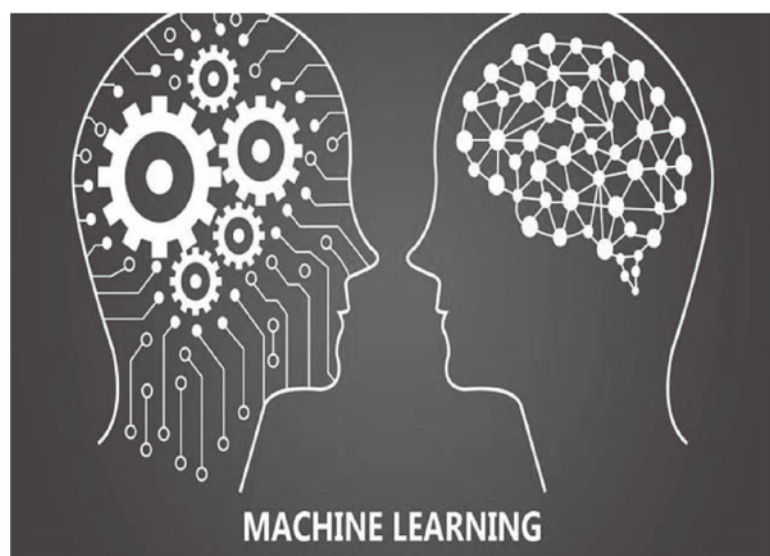
相較於過往僅對於個人資料保護法條文內容的理解，展望 2017，無論是組織或是個人，更應加強對以下內容的瞭解與認識，以期加強對隱私保護之能力。

網路安全威脅的影響隨著聯網時代來臨更加無遠弗屆。據趨勢科技2019年資安預測報告顯示，網路威脅者開始利用AI人工智慧發動目標式攻擊，透過AI預測判定企業管理階層和特定對象的相關動向，進而取信周圍相關人士進行入侵威脅；但與此同時，資安廠商也已運用人工智慧模擬以偵測任何潛在的網路威脅，提供企業與消費者多層式的防護。

多重認證的帳密保護措施

抵禦駭客變化莫測的攻擊手法，趨勢科技資深技術顧問簡勝財分享資安教戰守則：「

面對未來連網技術進步與跨平台連網趨勢，企業不能只依靠單一的資安工具，應採取跨世代的威脅偵測技術，在正確的時刻採取有效的防護策略；而民眾更應培養資安意識，對於電子郵件或是通訊軟體上的訊息提高警覺，降低遭受網路釣魚詐騙的風險，或可透過安裝防毒軟體協助保護個人資料與交易安全，此外，除了定期更新密碼，使用多重認證的帳密保護措施，以及密碼管理工具以保護相關憑證資訊，也可幫助個人機密資料的保護。」



趨勢科技2019 年資安預測報告各大重點摘要如下：

- 透過社交工程信的網路釣魚將取代漏洞攻擊套件成為主要攻擊模式。
- 憑證外洩盜用事件的數量與嚴重度將大幅提高。
- 員工在家工作及使用家用裝置連網的趨勢，使企業面臨類似BYOD自帶設備的資安風險。

- 歐盟將針對違反GDPR的大型企業開處全球營業額4%或是2千萬歐元高額罰鍰。
- 除了企業管理階層，變臉詐騙將更深入企業其他管理層級或是相關員工。
- 自動化將提高商業流程入侵的風險。
- 工控系統的目標攻擊持續成為隱憂，HMI人機界面也將持續成為SCADA監控與資料擷取系統的主要漏洞。

網路釣魚取代過去漏洞套件攻擊

在現今多元裝置以及操作系統趨勢下，駭客將不再透過以往單一軟體系統層面的漏洞攻擊套件模式，轉而利用社交工程廣布式地進行網路釣魚攻擊。截至今年第三季，趨勢科技Smart Protection Network已阻擋超過2億多筆網路釣魚相關的URL，相較於2017年成長接近三倍；預期2019年會再創高點。而有別於以往偽造企業往來信件格式的手法，駭客將透過竊取員工社群網路上的資訊，提高網路釣魚詐騙信件的可信度，達到入侵企業的目的；消費者方面，除了抓住大眾對重大活動的好奇心，透過如2020東京奧運的時事議題來進行社交工程詐騙之外，利用網路紅人的傳散能力，駭客將鎖定網紅的社群帳號並嘗試入侵取得控制權，成為駭客進行水坑式攻擊（Watering Hole）的工具，植入惡意程式的連結或是訊息，騙取追蹤粉絲點閱，使得粉絲遭牽連受駭，造成個人資料與財物損失。

報告另外指出，除了傳統信件，網路釣魚手法開始出現在手機簡訊以及通訊帳戶上，結合社交工程手法的新興網路攻擊開始出現

，如SIM卡劫持手法（SIM-jacking）：犯罪者取得個人電話號碼和資訊，假冒手機用戶，向電信廠商技術服務人員申辦新的SIM卡，爾後透過簡訊存取用戶的帳號資料甚至盜用電子錢包。



企業與個人資安意識內化，採取跨世代防護技術多層式保護連網安全

「回顧今年全球資安政策推動，可觀察到各組織及企業對於資料安全的重視；重大資訊安全事件的發生亦凸顯連網裝置普及所面臨的資安問題。預期在2019年企業和組織將導入更多連網設備，而連網速度也將大幅提升，資訊安全將面臨更廣泛與多元的挑戰，不僅企業對於資訊安全團隊的需求將提高，多層式智能防護的資安政策將在企業經營中扮演關鍵的角色，企業領導人對於網路安全的重視及培養經營團隊資安意識，更是建構自身企業網路安全防護架構的重要基石。」