109年第1季資通安全技術報告

Quarterly Technical Report

目　次

1. 資安威脅現況與防護重點 3
1.1 全球資安威脅現況 3
1.2 政府資安威脅現況 5
1.3 資安防護重點 8
2. 資安專題分享_零信任與 5G 資安防護 11
2.1 零信任簡介 11
2.2 5G 零信任資安防護 14
3.資安技術研析_ Dropbox Tunneling 攻擊手法簡介 17
3.1 Dropbox Tunneling 攻擊手法分析 17
3.2 偵測與因應機制 19
4. 結論 21

圖 目 次

圖 1　109 年第 1 季資安事件影響等級比率圖 6
圖 2　109 年第 1 季資安事件通報類型比率圖 7
圖 3　109 年第 1 季資安事件原因比率圖 8
圖 4　NIST 零信任架構 12
圖 5　5G 零信任資安防護示意圖 15
圖 6　車聯網之零信任應用 15
圖 7　Dropbox Tunneling 入侵流程 17
圖 8　Dropbox Tunneling 執行流程 18
圖 9　程式連線差異性 20

摘要

「第 1 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關於資安風險的關注重點。

「第 1 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為外匯交易公司遭勒索病毒攻擊；另一起案例為大學醫院因遭受網路攻擊而被迫關閉系統。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 58.2%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 14.93%)與「網頁攻擊」(占 7.46 %)為主要通報事件類型。

●2.資安專題分享

資安專題分享主題為零信任與 5G 資安防護。零信任的概念希望能突破傳統網路模型的資安困境，藉由重新定義網路安全防護方式，以保護資料或應用存取的邊界。資安專題分享零信任定義，並說明如何運用零信任於 5G 網路資安防護。

●3.資安技術研析

資安技術研析主題為 Dropbox Tunneling 攻擊手法簡介。近期駭客利用正常 Dropbox 雲端空間服務做為中繼站，下達控制命令與受害主機溝通。運用此新形態的手法控制遭駭主機，以正常運作模式掩飾惡意行為，成功導致現行偵測機制無法有效偵測。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享零信任與 5G 資安防護，說明如何運用零信任於 5G 網路資安防護。此外，資安技術研析，簡介 Dropbox Tunneling 攻擊手法，並說明偵測與因應機制。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因與可能之衝擊與影響。第 1 季(以下簡稱本季)探討因應遠端連線設備的廣泛使用，但資安防護概念卻未臻相應之成熟度，期藉由資安事件提醒遠端連線業者對其提供之設備應有完備之資安措施或驗證，而使用者在進行遠端連線時，亦應提高資安警覺，以防範更多資安弱點的暴露。另外，業務可用性一直是組織業務永續經營的目標，而駭客運用勒索病毒入侵手法，可以達到破壞組織業務持續運作，且能有利可圖，資安人員對此手法應全面提升資安防護整備度。

本章節之事件與議題皆配合整理相關之資安防護重點，提供組織就相關資安風險或議題進行評估，並依循資安防護重點進行強化。

1.1 全球資安威脅現況

隨著新冠肺炎(COVID-19)疫情持續，組織在面對無法預期的事件時，如何從容應對，確保業務持續運作及是否符合預設之最長可容忍中斷時間，並提供最低服務水準，以滿足利害相關者在事件發生時能接受基本維運功能。

許多網路攻擊者藉機利用疫情期間發動網路攻擊，台灣也出現許多以「Corona」為名的惡意軟體與惡意網域，如利用惡意網站銷售口罩，趁機竊取消費者個資。同時也出現利用新冠肺炎疫情為主題的社交工程郵件，攻擊者利用 COVID-19 所獲得的高度關注，誘使受害者打開惡意電子郵件的附件或點擊網路釣魚連結。

另一個必須提及議題則為資安準備與應對，包含遠端連線設備安全性、身分辨識、存取控制及容量負載等議題，均需在事前有充分準備與演練作業，方能順遂因應突如其來之衝擊。相關因應方式包含強化身分認證機

制，如設置不同帳號，區隔公務與個人帳號、使用多因子身分認證、安全連線設備及遭遇資安事件時之通報應變流程。

本季具指標性案例為外匯交易公司遭勒索病毒攻擊，為遠端連線設備造成資安風險；另一起案例為大學醫院因遭受網路攻擊而被迫關閉系統。

首先，探討案例為外匯交易公司 Travelex 遭勒索病毒攻擊。英國倫敦的外匯交易公司 Travelex，主要業務包含國際支付、貨幣兌換、全球匯款等，在全球擁有 1,500 個分公司，於 108 年 12 月 31 日傳出遭駭客攻擊，其網站與行動程式至 109 年 1 月 6 日仍未恢復正常。Travelex 表示，該公司遭病毒攻擊，危害部分服務，為避免病毒持續散布，決定關閉所有系統，調查後顯示並沒有個人或客戶資料外洩，而分公司則將繼續以人工方式提供各種外匯交易服務。

接續有數家媒體報導，Travelex 其實是受到勒索軟體 Sodinokibi 攻擊，而且駭客要求高達 300 萬美元贖金。108 年才現身的 Sodinokibi 迄今已是全球第五大勒索軟體，市占率 4.5%。媒體 Bleeping Computer 更取得駭客本身證實，表示他們的確以 Sodinokibi 攻擊 Travelex，且在加密前備份 5GB 個人檔案，包含生日、社會安全碼及金融卡資訊等，並向 Travelex 勒索 300 萬美元。英國媒體 Computing 則報導，資安業者 Bad Packets 於 108 年 9 月就曾警告 Travelex，提醒該公司使用的 Pulse Secure VPN 有資安漏洞，將允許駭客滲透至企業網路，但未獲得 Travelex 任何回應，媒體推測這也許就是駭客入侵 Travelex 管道。

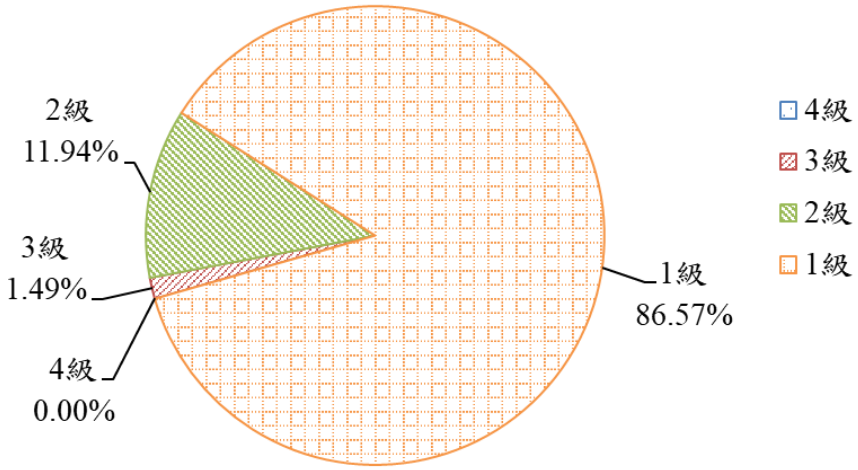
第 2 起案例為大學醫院因遭受網路攻擊而被迫關閉系統。位於捷克第二大城市布爾諾(Brno)的布爾諾大學醫院於 109 年 3 月 13 日遭到網路攻擊，該醫院不僅是當地大學醫院，也是捷克現今 18 個新冠肺炎(COVID-19)篩檢中心之一。目前歐洲因 COVID-19 疫情擴散造成醫療資源吃緊，此一攻擊行動無疑令當地之防疫雪上加霜。

布爾諾大學醫院目前正篩檢數十個可能罹患 COVID-19 案例，原本一天就能得到結果，但因遭受網路攻擊致系統癱瘓，相關篩檢作業可能要拉長到數天，讓需要緊急接受篩檢的病患無法取得結果，導致流失治療之黃金時間。醫院院長 Jaroslav Štěrba 表示，該院電腦系統遭到攻擊陸續當機，最後只能將電腦系統關閉，並要求員工不能開啟電腦，因此資安專家推測可能是遭到勒索軟體(Ransomware)攻擊。

綜覽本季重大資安事件，因應業務或事件應變的需求，開放員工居家上班時，隨著遠端連線需求的迫切，若干資安議題漸漸浮現。另外，勒索軟體的威脅已然成為駭客攻擊主要手法，面對勒索軟體之攻勢，除積極強化社交工程資安訓練、資通系統密碼設定及漏洞修補等風險外，更應依業務重要性訂定備份準則，以期能在預設時間恢復正常運作。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。彙整事件影響等級，本季以 1 級事件占 86.57%為大宗，2 級事件占 11.94%次之，3 級事件僅占 1.49%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

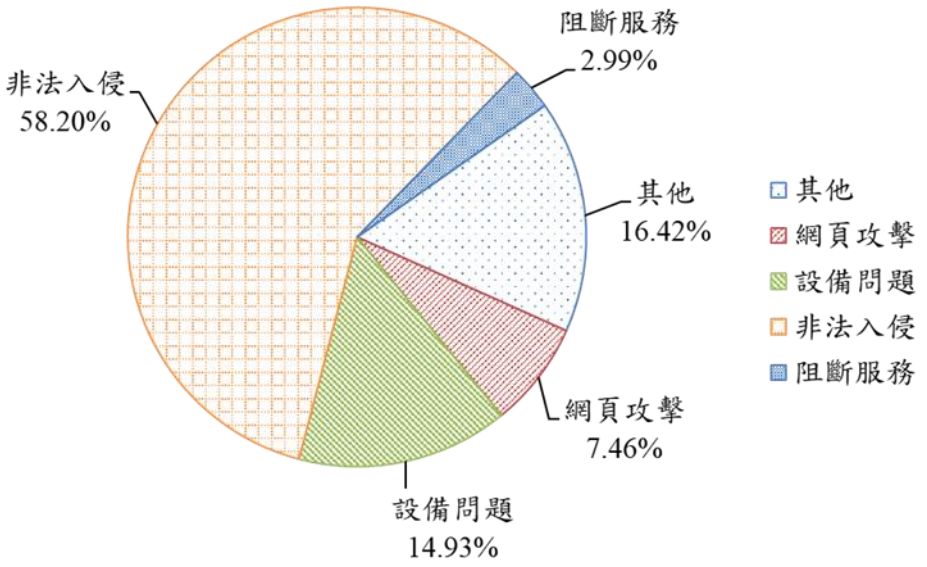


資料來源：本報告整理

圖1　109 年第 1 季資安事件影響等級比率圖

本季接獲之 3 級重要資安事件通報，為某機關數位學習平台遭外部使用者以不當存取方式，可經由平台取得系統權限進入後並竊取個人資料。所幸該平台之個人資訊欄位，係依資安政策規範以最小化進行蒐集，故未有過多個人資訊被揭露。

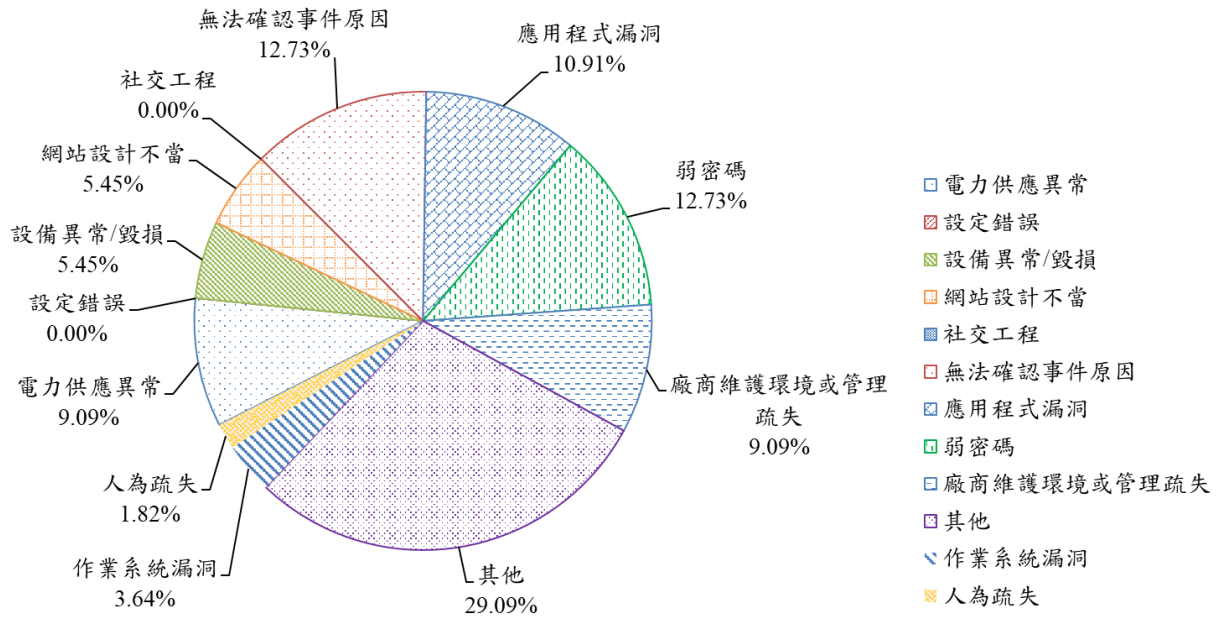
資安事件通報多以軟硬體設備異常或網路服務中斷，造成機關日常業務運作受到影響，此外，仍有部分機關因使用者信箱或系統管理者，如網站資料庫、差勤系統等資通系統存在弱密碼或預設密碼，再加上未限制外部存取權限而遭攻擊者植入惡意程式。其中，以「非法入侵」(占 58.2%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　109 年第 1 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以其他(29.09%)、弱密碼(12.73%)及無法確認事件原因(12.73%)位居前三名，其次分別為應用程式漏洞(10.91%)、廠商維護環境或管理疏失(9.09%)、電力供應異常(9.09%)、網站設計不當(5.45%)、設備異常/毀損(5.45%) 、作業系統漏洞(3.64%)及人為疏失(1.82%)，詳見圖 3。本季一般事件發生原因以其他為主，占 29.09%，皆無法以上述資安事件發生原因進行結報，其中包含電信公司線路異常、DNSSEC 同步鏈結錯誤等，機關通報符合資通安全管理法規範時程內通報，惟事件原因尚待調查鑑識且確認原因前，先行以「其他」進行結報，俟事件調查終結後，再進行事件原因調整。



資料來源：本報告整理

圖3　109 年第 1 季資安事件原因比率圖

分析第 1 季資安事件，資通系統存在著弱密碼或預設密碼的情況仍持續存在，從相關事件分析得知，資通系統未納入管理範圍或未依資通安全管理法規定之資通系統防護需求分級原則完成資通系統分級，致於日常維運管理上產生疏漏。

另一項待觀察事件則為資安事件通報之警訊通報事件，技服中心於 3 月偵測發現多個機關異常下載惡意程式腳本之連線紀錄，並發布入侵事件警訊，目前僅少數機關調查發現受害設備為 DVR 數位影像監視器外，其餘機關仍在進行事件調查。

1.3 資安防護重點

分析本季全球資安威脅現況，外匯交易公司遭勒索病毒攻擊，且在調查後聲稱沒有個人或客戶資料外洩，但隨之遭媒體揭露是受到勒索軟體 Sodinokibi 攻擊。據媒體報導，資安業者曾於 108 年 9 月就警告

Travelex，提醒該公司使用的 Pulse Secure VPN 有資安漏洞，將允許駭客滲透至企業網路，但未獲得 Travelex 任何回應。而另一起則為大學醫院因遭受網路攻擊而被迫關閉系統，該院電腦系統遭到攻擊陸續當機，最後只能將電腦系統關閉，並要求員工不能開啟電腦，推測可能遭到勒索軟體(Ransomware)攻擊。

分析政府機關通報的資安事件可看出，身分識別與資安管理一直是落實資通安全的首要防線，但資通系統使用弱密碼或預設密碼的情況仍時有所聞，且往往因此造成資安事件後，管理者才發現該資通系統並未納入日常存取控制檢視範圍。針對應用程式漏洞議題，除持續推動在系統發展生命週期中導入資安思維外，並應在每一階段檢視資安設計的可行性與落實度，於上線前確認程式未有後門與資安漏洞等風險。

綜整以上資安威脅現況，提供資安防護建議如下：

●遠端連線資安管理

– 選用具遠端連線功能等軟硬體資通設備前，應依業務需求進行風險評估，以及限制使用危害國家資通安全產品。

– 依風險考量，優先採購已獲得資安驗證之遠端連線產品，並檢視其所提供之資安措施與漏洞更新機制。

– 在不同區域網段部署資安控制措施，且設置多因子身分認證機制。

●應用程式資安管理

– 建立應用程式安全系統發展生命週期，不論是自行發展或委外開發之資通系統應有一致性之安全發展成熟度評量標準。

– 建立資安弱點通報機制，以及時辨識系統軟硬體之資安弱點。

– 應用程式上線前或功能變更時，須進行相關風險評估與源碼檢測。

●獨立系統或資料庫資安管理

– 建立資產盤點機制，定期檢視資安管理範圍內之軟硬體及周邊設備等清冊之完整性。

– 針對獨立性系統或資料庫，建立上線前修改預設密碼與定期變更密碼機制。

– 定期檢視相關軟硬體是否依資通系統防護需求分級原則完成資通系統分級，並確認防護措施之落實度。

2. 資安專題分享_零信任與 5G 資安防護

隨著資料或各項服務雲端化、使用者移動化及存取設備多元化，傳統網路模型正面臨一項資安挑戰極需突破。傳統網路建構是先建置階層式網路，再逐步增加資安控制，因此資安思維受限於階層式網路架構。此外，傳統網路建構基於信任邊界的網路威脅模型，邊界內存取受信任、邊界外存取不受信任。然而現今許多攻擊直接或間接來自於信任邊界內，且面對複雜的網路環境變化，邊界的形成越發困難。

現今零信任的概念正希望能突破傳統網路模型的資安困境，藉由重新定義網路安全防護方式，以保護資料或應用存取的邊界。在零信任中，任何資料存取應為永不信任且必須驗證，以最低且嚴格控管存取權限，創造無具體邊界，亦能讓使用者、設備、資料及應用能無所不在。

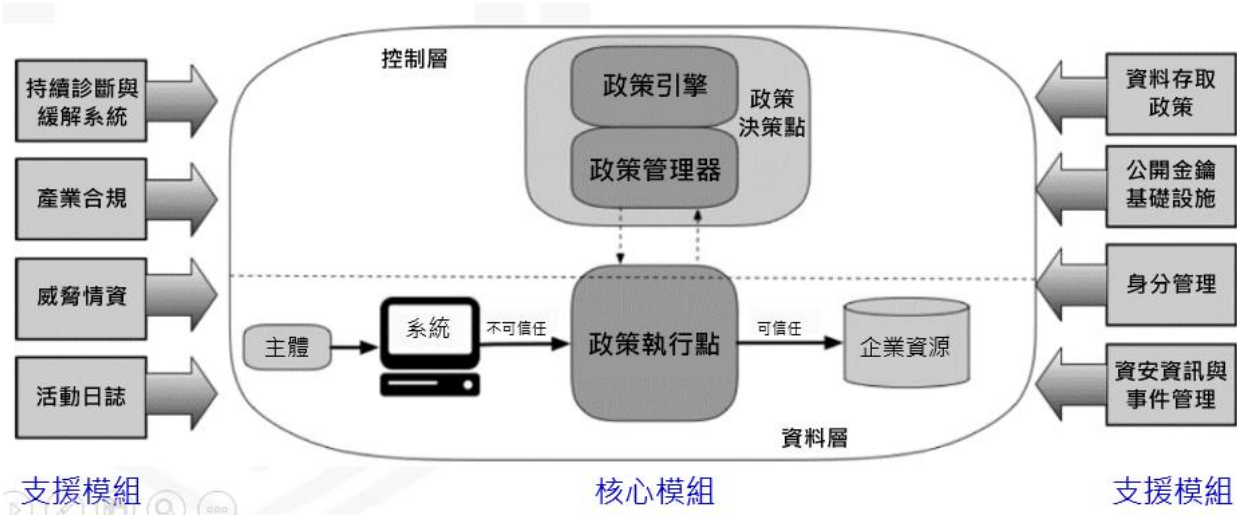
以下將概述零信任架構，並說明如何運用零信任於 5G 網路資安防護。

2.1 零信任簡介

NIST SP 800-207 指出零信任並非單一的網路架構，而是網路設計與運作的一套資安指導原則。針對每次資料或應用存取，零信任實施使用者認證、設備認證、最小授權及傳輸加密等措施，形成所謂軟體定義邊界(Software Defined Perimeter, SDP)。以下將進一步探討零信任架構、導入及實例等相關技術議題，並綜整零信任關鍵技術。

- 零信任架構(Zero Trust Architecture, ZTA)

  零信任架構分成核心模組與支援模組，核心模組主要執行認證、決定授權及管理連線，支援模組則支援存取決策的資訊與系統，詳見圖 4。



資料來源：本報告整理

圖4　NIST 零信任架構

●零信任導入

零信任導入並非一次大規模替換基礎架構，而是階段性實施。針對具備優先性資料，逐步實施零信任，因此零信任與傳統模式會同時混合運作。實施零信任是不斷反覆的週期，包含資產調查、風險評估、政策發展、技術部署及系統運作。

NIST 零信任導入步驟分幾個階段，首先，由識別與管理參與者開始，包含使用者與非使用者帳號，針對具有特殊權限之帳號(開發者或系統管理者)需特別辨識。第二階段為識別與管理資產，包含硬體設備與數位資產，如資料、應用服務及數位憑證等。第三階段則啟動識別關鍵業務並評估相關風險，依所有業務之價值與風險排定優先順序，理論上應由具備關鍵業務優先導入零信任，但實務上亦可先挑選擇低風險業務導入零信任以累積經驗。第四階段開始制定存取規則，針對擇定業務流程中使用資源，制定一套遵循資安政策的存取規則。第五階段為規劃解決方案，規劃部署架構，並尋求技術解決方案，不論是商用或客製開發產

品。第六階段為展開部署與監控，依所使用之解決方案，實施制定之存取規則，日常監控日誌並檢討待改善之處以進行必要之調整。最後階段則為逐步擴展零信任，將零信任導入其他業務，若業務內容有任何變動時，如資料、流程或設備變更時，則需重新檢視實施週期。

此外，Microsoft 亦針對零信任提出 4 階段方法，並定義每個階段之重要工作。第一階段為辨識身分(verify identity)，藉由無密碼、雙因子進行身分認證。第二階段則為辨識設備之運作狀態(verify device health)，將所有使用者設備註冊到設備管理系統，如 Microsoft Intune 等，以進行監控與管理。第三階段為確認存取(verify access)，針對來自網路與未納入管理之設備，提供最小授權。最後階段為確認服務(verify services)狀態，確保系統正常維運。

●零信任實例

Google BeyondCorp 為著名的零信任架構案例，其所設定之目標為讓每位 Google 員工都可以在不藉助 VPN 情況下，透過不受信任網路順利執行工作，實施至今 BeyondCorp 已經成功植入大部分 Google 員工之日常工作，雖僅在其內部實施，但深具指標性意義。

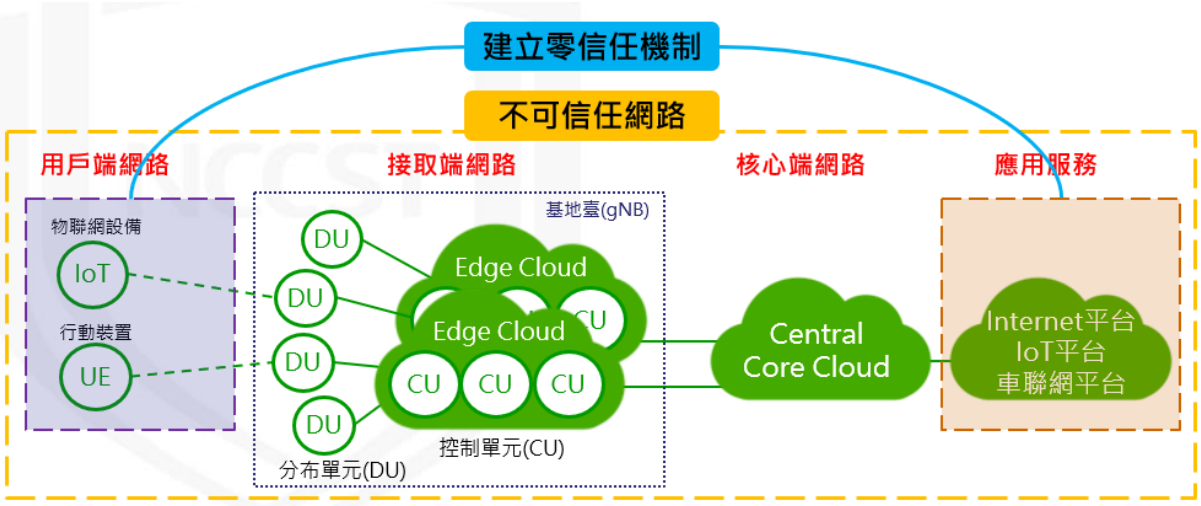
BeyondCorp 包含 5 個關鍵技術，第一為設備認證，建立設備清單資料庫並持續追蹤，發行設備憑證以進行設備認證。第二為移除信任網路，透過部署無特權網路環境，即使在 Google 辦公室也是直接連上外部網路，且所有應用皆透過公開的存取代理器(Access Proxy)存取。第三為使用者認證，建立使用者/群組資料庫，由單一登入(SSO)進行雙因子認證，並發行短期之認證令牌。第四為信任推斷，動態調整使用者與設備之信任等級，依據設備漏洞修補情形、設備種類及使用者位置等，進行適時異動。第五為部署存取控制，藉由存取控制引擎綜整設備認證、使用者認證及信任推斷資訊，以決定存取授權。

綜整上述對 NIST、Microsoft、Google 及其他相關文獻在架構、導入及實例之探討，歸納零信任主要關鍵技術包含「使用者認證」(無密碼且多因子身分認證)、「設備認證」(區別並追蹤組織擁有與非組織擁有、私有/公開設備，以進行設備健康檢查，包含組態設定、作業系統與漏洞更新狀態及攻擊情資等)及「存取授權」(支援決定最小存取授權之信任推斷或情境感知存取等)。

2.2 5G 零信任資安防護

美國國防創新委員會於 2019 年 4 月發布 5G 風險報告，指出 5G 之 3 大資安挑戰，包含供應鏈風險(Supply Chain Risks)、5G 基礎設施與服務(5G Infrastructure and Services)及 5G 設備(5G Devices)。此 3 大資安挑戰的核心，直指 5G 架構中從用戶端、接取端到核心端，無法避免使用中國或其他具惡意國家所生產設備衍生之設備後門、設備漏洞及入侵等資安風險。因此國防創新委員會建議美國國防部必須採用零信任架構，以因應 5G 資安挑戰。本章節以車聯網為例，說明如何運用零信任於 5G 網路資安防護。

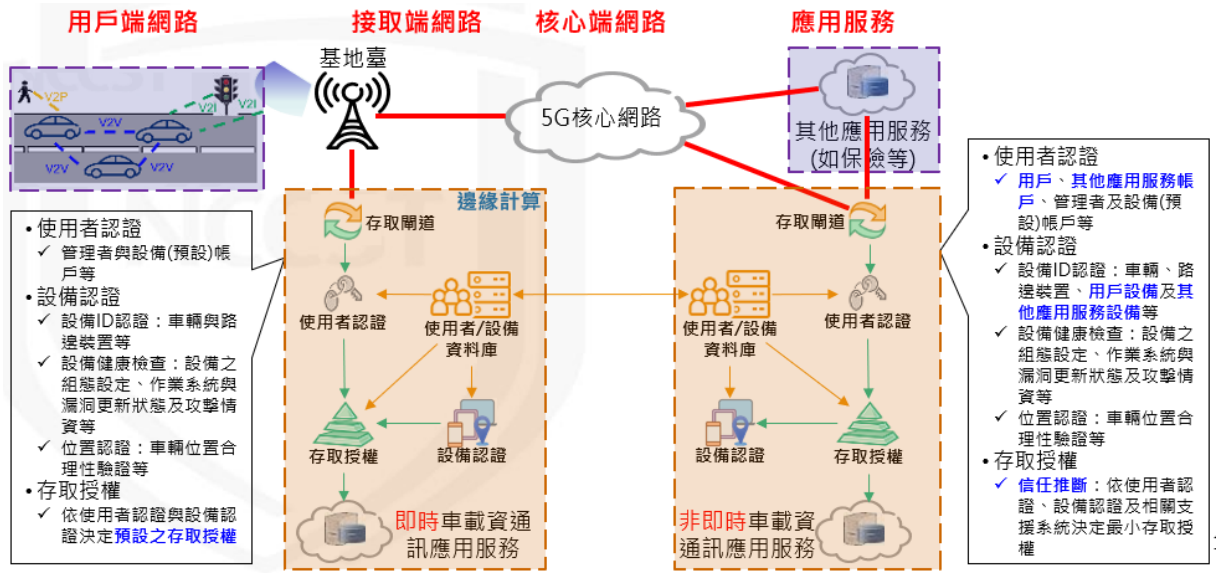
零信任概念套用到 5G 資安防護之原則，首先將 5G 網路視為不可信任網路，因此針對欲保護之應用服務，規劃建立用戶與應用服務之使用者認證、設備認證及存取授權等零信任機制，詳見圖 5。



資料來源：本報告整理

圖5　5G 零信任資安防護示意圖

依車聯網不同應用服務，分別實施零信任，包含接取端邊緣計算環境之即時車載資通訊應用服務與應用服務端之非即時車載資通訊應用服務。即時車載資通訊應用服務可建立低延遲之輕量零信任機制，而非即時車載資通訊應用服務，則建立多元存取之零信任機制，詳見圖 6。



資料來源：本報告整理

圖6　車聯網之零信任應用

透過使用者認證，管理使用者與設備預設帳號，藉由設備認證與管理，達到設備之組態安全性設定、作業系統與漏洞更新狀態及攻擊情資等資訊蒐集，並可進行車輛位置合理性驗證。在零信任架構下，最後依使用者認證與設備認證決定預設之最小存取權限。同時，亦能將零信任架構推展到其他車聯網相關應用服務，在同一框架下進行資安防護之應用。

以上概述零信任之概念、架構、導入程序、實例及關鍵技術，可做為未來政府機關導入零信任資安防護之參考。但在導入零信任架構時，仍需注意幾項議題，如設備多元化，零信任在小規模企業或複雜性較低之環境較易實施，但面對多元且數量龐大設備形成的公共互聯網，則存在一定挑戰性，設備多元可能衍生設備預設帳戶清單不完整，同時設備可能存在零時差(Zero-Day)等惡意程式風險。此外，需注意延遲問題，零信任針對每次存取皆需實施認證、授權甚至加密等相關措施，自然會增加處理時間，這對 5G 低延遲相關應用將是一大挑戰。5G 零信任架構之推動可強化與彈性運用存取控制機制，相關資安防護挑戰則需要持續關注。

3.資安技術研析_ Dropbox Tunneling 攻擊手法簡介

本季所探討的資安技術研析，是簡介 Dropbox Tunneling 攻擊手法。技服中心分析近期資安事件，發現駭客利用正常 Dropbox 雲端空間服務做為中繼站，下達控制命令與受害主機溝通。運用此新形態的手法控制遭駭主機，以正常運作模式掩飾惡意行為，成功導致現行偵測機制無法有效偵測。

透過分析與關聯過去情資，105 年曾發現有零星事件利用相同手法進行攻擊，惟因當時取得樣態稀少，時至今日始成功辨別其攻擊來源，同時可針對其手法做進一步解析。

3.1 Dropbox Tunneling 攻擊手法分析

Dropbox Tunneling 攻擊案例中，除接獲情資指出，某政府機關與所控管之中繼站有通聯情形外，技服中心偵測規則亦出現觸發現象，故進行現場實際調查作業。綜整分析近期相關案件手法，發現駭客均是在取得帳號密碼後，利用遠端桌面或網路登入進行控制，並於內部擴散，詳見圖 7。

資料來源：本報告整理

圖7　Dropbox Tunneling 入侵流程

駭客藉由植入惡意程式，利用 Dropbox 做為接收回報與控制機制，其執行流程說明如下，詳見圖 8。

資料來源：本報告整理

圖8　Dropbox Tunneling 執行流程

- 步驟 1，駭客會以 3 個參數進行認證，包含 appSecret、appKey、acessToken 連線認證協定，以符合 OAuth 1 認證流程。
- 步驟 2，為取得通訊用加密金鑰，下載雲端檔案/abc/10101，從程式中讀取解密字串，以 RC4 演算法解密 10101 取得金鑰。
- 步驟 3，成功建立特定資料夾，根目錄為/abc/[電腦名稱]，並建立子目錄，包含「001」用於放置執行過的指令與結果檔、「010」用於放置欲竊取之受害電腦檔案、「011」用於放置欲執行的後門或工具檔及「0111」用於放置駭客指令檔。
- 步驟 4，上傳加密報到資訊，包含取得電腦名稱、IP、網卡 MAC 及使用 RC4 加密存成 0001 檔案。

- 步驟 5，下載指令檔或惡意程式並執行，駭客從雲端下載指令檔至資料夾 0111，並以 RC4 解密。其中指令檔包含 3 種控制功能，分別為執行命令、上傳檔案及下載檔案或工具。執行後狀態碼加密為 0011 檔，亦會在執行後即刪除指令檔。

- 步驟 6，上傳執行指令執行結果或檔案，執行過的指令與結果檔會放在資料夾 001 中，首次上傳指令執行結果檔案為 0100，後續上傳指令執行結果之檔名則為特定時間編碼。相關指令執行結果會經加密後回傳。

- 步驟 7，程序休眠重啟。

3.2 偵測與因應機制

要主動發現類似案件並非易事，特別是朝向結合公開之社群服務或利用政府機關現行使用軟體漏洞而開發之後門程式，此類攻擊事件利用正常存取行為掩蓋異常駭侵活動，達到成功降低遭到偵測的可能性。

首先，可以先藉由偵測機制之運用，觀測程式執行過程之差異性找出異常連線，如比對駭客自行開發與官方程式執行過程差異性，可找出 content.dropboxapi.com/2/files/download 與 content.dropboxapi.com/2/files/upload 並非為官方程式之合法連線，詳見圖 9。

資料來源：本報告整理

圖9　程式連線差異性

再者，從相關案例分析得知駭客連線程式之邏輯設定，惡意程式每隔固定時間會休眠並重啟，故於正常執行下，報到資訊 001 檔的更新會有一定規律性，即 API [content.dropboxapi.com/2/files/upload]的呼叫亦會呈現一定規律性，同樣可嘗試藉此做為偵測依據。

上述做法雖可以運用做為早期入侵偵測判斷，但仍無法精準確認是否已被駭侵成功。尤其駭客是利用正常存取行為掩蓋其異常駭侵活動，因此能成功發現異常活動的可能性就減少許多。分析相關案件之啟始共通點多來自於帳號密碼遭竊，原因包含利用政府機關所使用之共通系統漏洞後，成功取得帳號密碼。因此，針對政府機關之共通系統首要之務應確保修改預設密碼並應定期變更密碼，方不致因共通系統委由同一建置廠商維運而產生資安漏洞。另外，使用公開之社群服務，亦應確實管理帳號密碼之安全性。

4. 結論

本季具指標性案例為透過研析外匯交易公司遭勒索病毒攻擊；另一起案例為大學醫院因遭受網路攻擊而被迫關閉系統。外匯交易公司遭勒索病毒攻擊，但據媒體報導肇因可能為該公司使用的 Pulse Secure VPN 有資安漏洞，而該公司雖有資安業者提出預警，但卻遭忽視其風險置之不理，終致資安事件的發生。管理者面對具遠端連線功能之裝置應視同為管理範圍內之資通系統，亦應評估其資通系統防護需求分級與相對應防護措施。國內部分，分析政府資安威脅現況，以非法入侵為主，排除綜合類型「其他」外，其次分別為設備問題與網頁攻擊事件為主要通報事件類型。針對本季全球與政府所面臨的主要資安威脅，本報告就「遠端連線資安管理」、「應用程式資安管理」及「獨立系統或資料庫資安管理」，提出資安防護建議。

資安專題分享零信任與 5G 資安防護。面對許多攻擊直接或間接來自於信任邊界內，且因應複雜的網路環境變化，邊界的形成越發困難。零信任的概念希望能突破傳統網路模型的資安困境，藉由重新定義網路安全防護方式，保護資料或應用存取的邊界。在零信任中，如何以最低且嚴格控管存取權限，創造無具體邊界，又能讓使用者、設備、資料及應用能無所不在，並說明如何運用零信任於 5G 網路資安防護。

此外，資安技術研析主題是簡介 Dropbox Tunneling 攻擊手法。技服中心透過分析與關聯過去情資，發現 105 年曾發現零星事件利用相同手法進行攻擊，惟當時取得樣態稀少，今始可進一步解析駭客如何利用 Dropbox 雲端空間服務做為中繼站，下達控制命令與受害主機溝通，藉以利用正常存取行為掩蓋其異常駭侵活動。