零信任網路導入陸軍行政網路防護作為之探討

作者：李勝宏

提要：

一、零信任網路的資安思維逐漸發展，陸軍行政網路現階段在實體隔離為原則下，實施防護作為，本文藉零信任網路的思維來探討陸軍行政網路可採取的安全性作為。

二、本文導入零信任網路的思維，採用網路分級方式對應司令部、作戰區、聯兵旅等，針對連線驗證、資料傳輸與權限管理等三方面，探討不區分層級與區分同層級間防護作為之差異。

三、零信任網路的導入，冀望能提供陸軍行政網路防護方法上更加安全且可靠的作法，藉此提供未來規劃網路管理作為時的參考方案。

關鍵詞：零信任、零信任網路、網路防護。

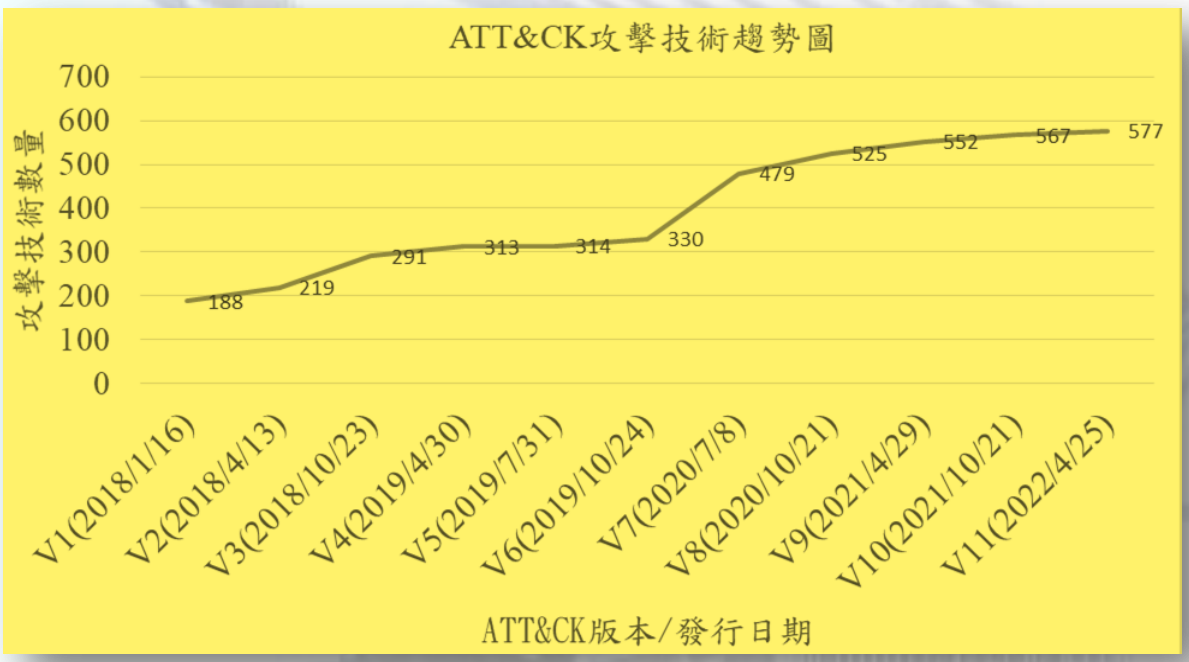
前言：

MITRE 是美國的一間非營利機構，進行多項資安相關研究，在 2015 年 5 月開始 ATT&CK 框架的研究計畫，以建立攻擊者所使用的策略與手法的知識庫，從 2018 年 1 月發行第一版本，其內容記載著攻擊技術為 188 種，到 2022 年 4 月已成長達到 577 種技術，由此可知，駭客攻擊手法愈來愈多(如圖 1)，另依據 2021 年 1 月世界經濟論壇（World Economic Forum，WEF）所發表「全球風險報告」（The Global Risks Report）中，前十大全球可能風險就有三項為科技面相關的風險，分別為集權控制數位資源、數位落差與資安防護失效(如圖 2)。而資安防護失效這項是指全球在現有的資安防護上將面臨到的風險與挑戰，資安防護失效在圖中的位置為發生率與發生後影響性都是屬於較高的區域，現今傳統被動式防禦已不足應付新興的資安攻擊手法，若是不加以轉變將會導致資安防護失效，要避免資安防護失效，從被動式防禦轉換為新型的資安防禦架構與概念-零信任(Zero Trust)網路，秉持著「所有連線都不可信任」、「持續不斷的驗證」來架構一個主動式的防禦資訊網。

本文是以零信任網路的概念來對陸軍行政網路的資安防禦架構實施探討，在零信任網路運用下，可消除原本網路架構的內網信任概念，避免遭進階持續性攻擊(Advanced Persistent Threat, APT)時可能的橫向移動及擴大損害，進一步可運用在不同層級機關(部隊

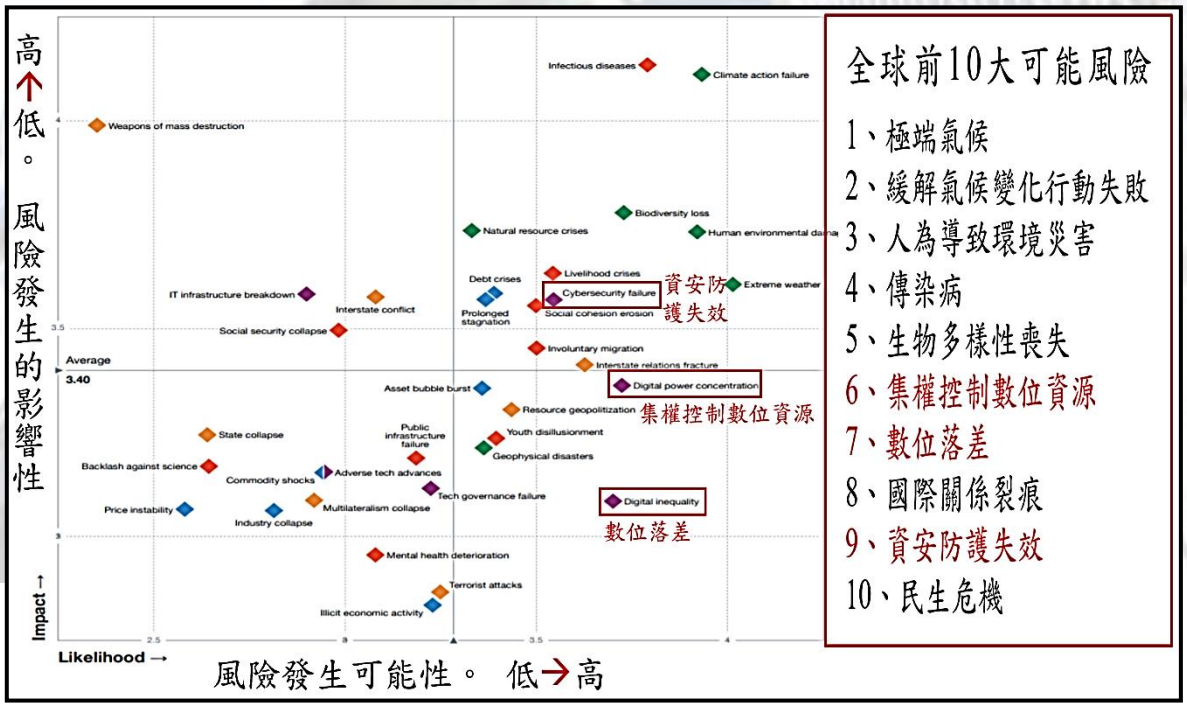
)間行政網路互連時的防護方法來架構一個更安全且可靠的網路環境，在時間與篇幅受限下，本文主要針對連線驗證、資料傳輸與權限管理等三方面進行研討。

圖 1 MITRE ATT&CK 歷年駭客攻擊技術統計圖



資料來源：作者繪製。

圖 2 世界經濟論壇 2021 年全球風險地圖



資料來源：Marsh McLennan, SK Group, Zurich Insurance Group, The Global Risks Report 2021 (World Economic Forum:Switzerland,2021),pp.11.

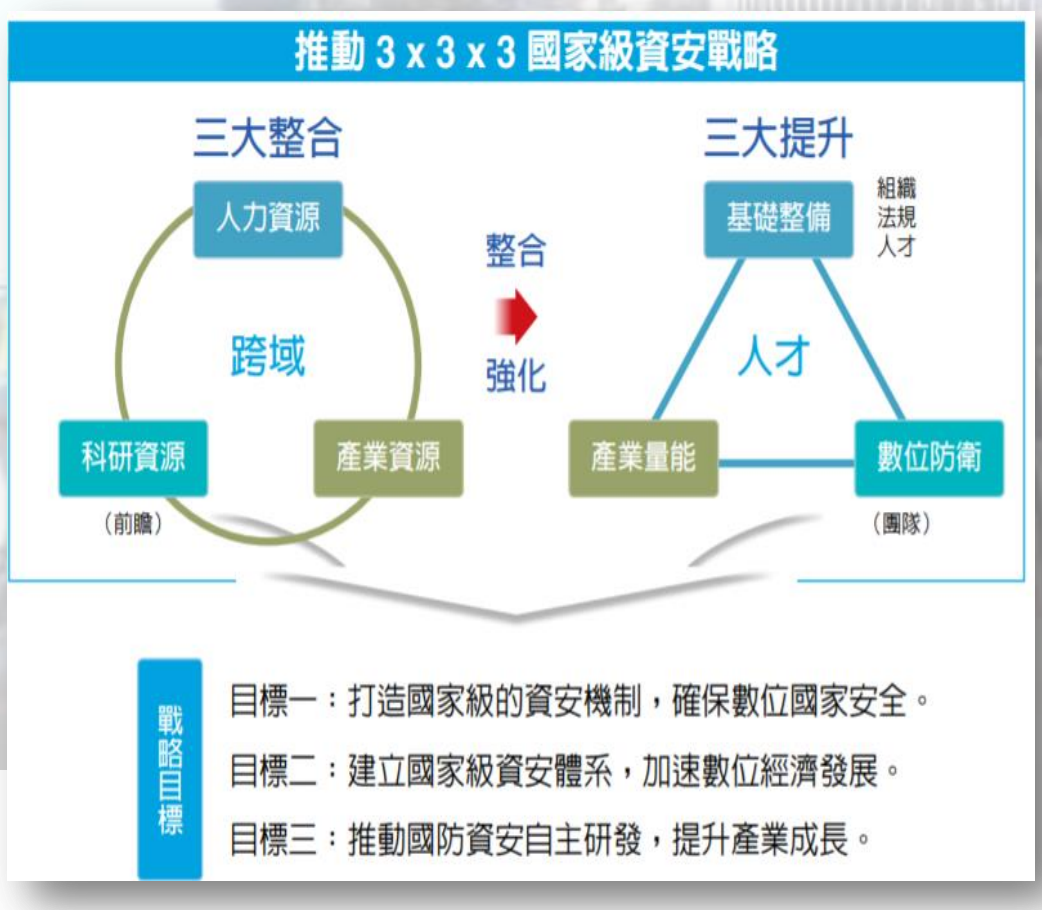
資安政策與防護作為

現今的資安威脅日益成長，為了打造安全可靠的數位國家，政府推動一連串的資安相關政策，並於民國 107 年已完成「資通安全管理法」立法，藉由網路責任分級進而規範相關防護作為，達到保護單位之目的，並且讓資安防護作為在政策面與管理面上都具有法源的支持；以現今技術面來說，在網路防護架構大多採用縱深防禦方式來防護複雜的網路攻擊環境，因此，後續將說明相關政策、防護作為與縱深防禦等。

一、資安政策

行政院自民國 90 年起，每四年制定一個重大資通安全計畫或方案，民國 109 年底已完成第五期發展方案，主要是藉「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」及「孕育優質資安菁英人才」等 4 大策略推動，逐步建構我國資安縱深防禦及聯防體系，以穩固我國數位國土的資安防線，並且訂出 3x3x3 的國家級資安戰略方針(如圖 3)，為了能推動資安法規立法，立法院於民國 107 年已完成「資通安全管理法」三讀通過，為後續推動資安作為、邁向安全可信賴的數位國家奠定良好的基石。

圖 3 國家資安戰略



資料來源：〈國家資通安全戰略報告〉，民國107年9月，頁15

(一)安全責任分級

「資通安全管理法」通過後，行政院資安處隨即公布「資通安全責任等級分級辦法」等6個子法，主要為了補足母法的不足，其中依照機關的業務及系統重要性，以及涉及範圍等差異，將公務機關與特定非公務機關之資通安全責任等級，區分為A級、B級、C級、D級、E級5個等級(如表1)。

(二)資安防護分級作法

網路責任分級後，在「資通安全管理法」中有規範各級公務機關應辦事項，其中對各級資安防護技術面有一定的規範，以維各單位資安防護之強度(如表2)

表 1 資通安全責任等級劃分一覽表

責任分級	涉及業務性質、範圍
A 級	1.業務涉及國家機密 2.業務涉及外交、國防或國土安全事項 3.業務涉及全國性民眾或跨公務機關共用性資通系統之維運 4.業務涉及全國性民眾或公務員個人資料檔案之持有 5.屬公務機關，且業務涉及全國性之關鍵基礎設施事項 6.屬關鍵基礎設施提供者，經事業主管機關認定其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響 7.屬公立醫學中心
B 級	1.業務涉及公務機關捐助、資助或研發之敏感科學技術資訊之安全維護及管理 2.業務涉及區域性、地區性民眾或跨公務機關共用性資通系統之維運 3.業務涉及區域性、地區性民眾個人資料檔案之持有 4.業務涉及中央二級機關及所述各級機關(構)共用性質資通系統之維運 5.屬公務機關，且業務涉及區域性、地區性之關鍵基礎設施事項 6.屬關鍵基礎設施提供者，經事業主管機關認定其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重之影響 7.屬公立區域醫院或地區醫院
C 級	各機關維運自行或委外開發之資通系統者
D 級	各機關自行辦理資通業務，未維運自行或委外開發之資通系統者
E 級	1.無資通系統且未提供資通服務 2.屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管 3.屬特定非公務機關，且全部資通業務由其中央業務主管、其所屬公務機關、所管特定非公務機關或出資之公務機關兼辦或代管

資料來源：〈資通安全責任等級分級辦法部分條文修正條文〉，民國110年8月23日，頁1-2

表 2 各資通安全責任等級機關之資通安全防護措施一覽表

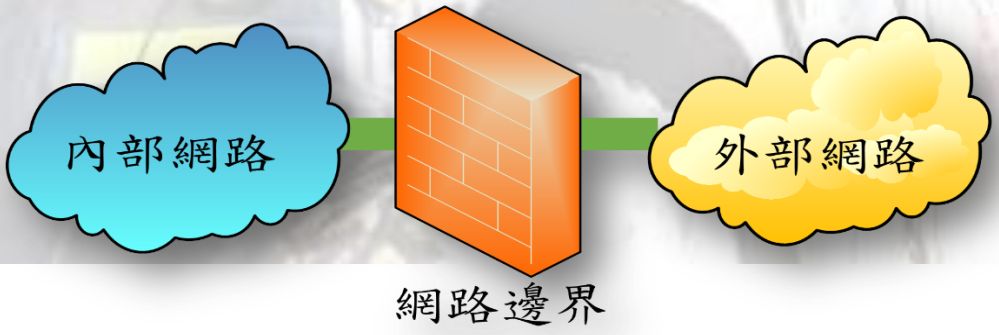
措施分級	網路防火牆	入侵偵測及防禦機制	防毒軟體	具有郵件伺服器者，應備電子郵件過濾機制	具有對外服務之核心資通系統者，應備應用程式防火牆	進階持續性威脅攻擊防禦措施
A 級	V	V	V	V	V	V
B 級	V	V	V	V	V	
C 級	V		V	V		
D 級	V		V			
E 級						
備註	V 為法規所規範應辦事項					

資料來源：〈資通安全責任等級分級辦法部分條文修正條文〉，民國110年8月23日，頁4-20

二、防護作為

目前的外部攻擊手法多數來自於網路，網路對於單位而言，區分外部網路與內部網路兩部分(如圖 4)，而大部分的網路防護作法都是從外部網路到內部網路的通道來實施防護，亦是在網路邊界實施相關的防護，網路邊界就是指內部網路與外部網路的分界線，因此，邊界安全防護儼然成為網路安全防護基礎架構的主要概念，而網路邊界常見的設備為防火牆、虛擬私人連線(Virtual Private Network, VPN)閘道器與入侵防禦系統(Intrusion Prevention System, IPS)，接著就是針對內部網路中的用戶與資料進行防護。網路邊界的防護設備，主要來防止及追蹤未經授權的存取、揭露與修改，或是阻絕網路服務，以維護機關重要資產的機密性、完整性與可用性，上述的相關作法詳述如後。

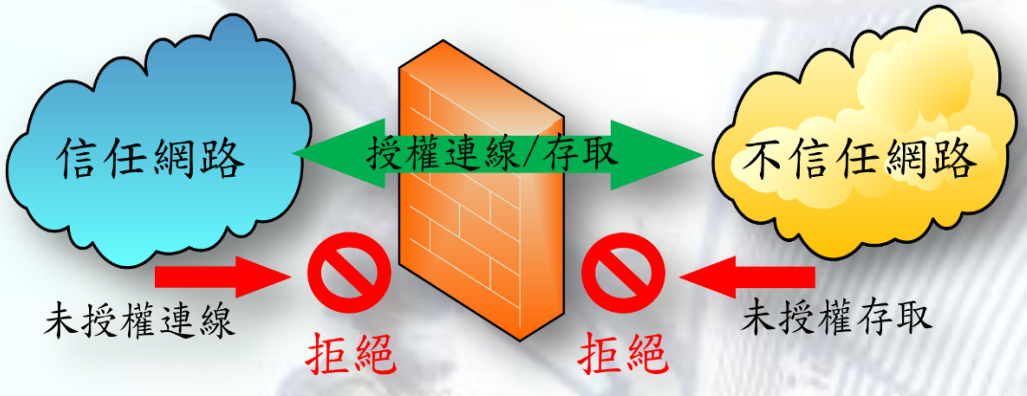
圖 4 網路邊界圖



資料來源：作者繪製

(一)防火牆：主要是監控輸入和輸出網路流量的網路設備，並依據已定義的存取規則來決定允許或封鎖特定流量，在安全受控制的信任內部網路和不信任的外部網路之間建立一道屏障，因此，防火牆一直是網路閘口的第一道防線(如圖 5)。

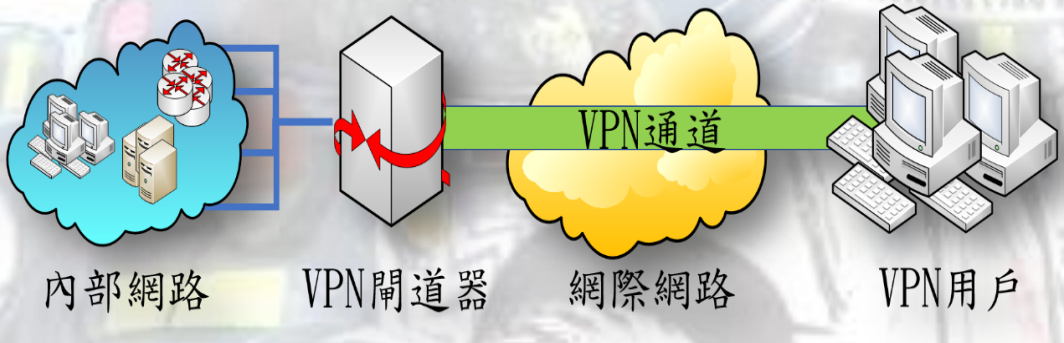
圖 5 防火牆架構圖



資料來源：作者繪製

(二)VPN 閘道器：VPN 即是指在網際網路架構上透過隧道協定(Tunneling Protocol)與加密方式與企業內部網路建立起一個私人且安全的連結通道，而 VPN 閘道器的功能主要就是建立起一個專屬通道把內部網路與網際網路鏈結起來(如圖 6)。

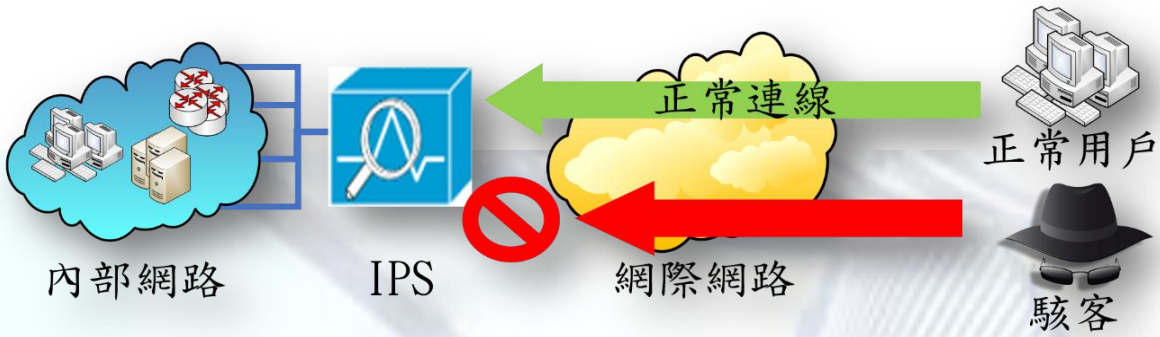
圖 6 VPN 閘道器架構圖



資料來源：作者繪製

(三)入侵防禦系統：IPS 具監測及防禦的雙重功能，可即時偵測到網路攻擊事件的發生，依照其設定針對網路攻擊或入侵行為來實施中止或阻絕，其處置作為包括自動攔截棄置攻擊封包，並將會留下攻擊紀錄並通知管理者等(如圖 7)。

圖 7 IPS 架構圖



資料來源：作者繪製

三、縱深防禦

面對多元的資安威脅(如圖 8)，已經無法就單一裝置或是單一管控就可以抵禦複合式的攻擊方式，尤其近來進階持續性滲透攻擊(Advanced Persistent Treat, APT)日益常見，故防護措施將大多採用縱深防禦機制來實施，縱深防禦是期望達到嚇阻、偵測、延遲、禁制等目的，若真的發生入侵事件，也能及時發現與阻擋，達到讓入侵行為更費時、費力進而放棄入侵之目標。

圖 8 多元資安威脅

資料來源：吳啟文，<資安威脅趨勢及防護策略>，《行政院國家資通安全會報技術服務中心》，ttps://secutechinfosecurity.tw.messefrankfurt.com/content/dam/messefrankfurt-redaktion/infosecurity/2021-march-seminar-agenda/資安威脅趨勢及防護策略_行政院國家資通安全會報中心-吳啟文-主任.pdf，2021/03/09，(檢視日期：2021/06/14)。

構建縱深防禦從外而內可概分：政策管理與資安意識、實體安全、邊界、內部網路、主機、應用程式與資料等 7 項(如圖 9)，本段篇幅僅針對邊界、內部網路、主機、應用程式與資料等 5 項防護作法實施說明(如表 3)，詳述如下：

圖 9 縱深防禦架構圖

資料來源：李宗翰，<治療資安憂鬱症的新配方：Security2.0>，《iThome》，https://www.ithome.com.tw/tech/39553，2006/09/25，(檢視日期：2021/12/24)。

表 3 縱深防禦防護措施

項次	項目	防護措施
1	邊界	1.網路防火牆 2.入侵偵測防禦系統
2	內部網路(周邊設備)	1.設備管控系統 2 端點防護系統
3	主機	1.防毒軟體 2.作業系統更新與修補
4	應用程式	1.應用程式版本管控 2.應用程式防火牆 3.郵件過濾系統
5	資料	1.加密 2.數位簽章 3.VPN

資料來源：作者整理

(一)邊界：網路入口處為第一道防護，在此防線設置了安裝防火牆、入侵偵測防禦系統來實施防護，以阻絕不合法、有入侵行為的連線。

(二)內部網路(含周邊設備)：藉由設備管控系統，針對內部相關設備實施控管，避免遭非法設備入侵，並防護周邊資訊產品內含惡意程式，使用端點防護系統針對各項輸出入周邊設備實施管控，以避免使用未授權或管制中的設備，進而遭惡意程式入侵，於內部網路形成破口。

(三)主機：防護主機基本的防護方式為安裝防毒軟體與作業系統持續完成更新與修補；防毒軟體主要是抵禦已知的電腦病毒入侵，作業系統更新與修補是不讓主機漏洞百出，成為駭客入侵的途徑。

(四)應用程式：在管理上應統一管控應用程式的版本，若該版本有公告漏洞時，應立即完成版本更新，以免遭駭客利用；另外對於本身所提供服務的應用程式，應安裝相關防護措施加強管控，如：Web 應用程式防火牆、電子郵件過濾系統等。

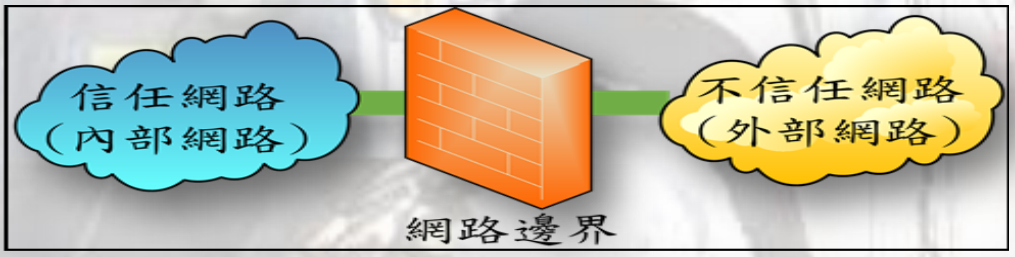
(五)資料：對資料存管的保護，從資料的存放，應先完成資料分級，針對機敏性資料完成加密，並且對資料存取、傳輸，必須完成權限設定，而在措施上可使用數位簽章完成身分驗證後方可存取資料，傳輸時資料應完成加密才可實施傳輸，必要時應於安全通道之建立後再進行傳輸，維護資料傳輸之安全性。[1]

零信任網路

一、信任與零信任網路

信任網路主要是透網路邊界的設備，將網路區分為內部網路與外部網路，將內部網路視為信任網路，而外部網路則視為不信任網路(如圖 10)。零信任網路則是不再依賴網路邊界的設備區隔網路，一律將網路視為不信任的網路，包含內部網路亦為不信任網路，因此，所有連線都需實施驗證，才可連線存取。

圖 10 信任網路圖



資料來源：作者繪製

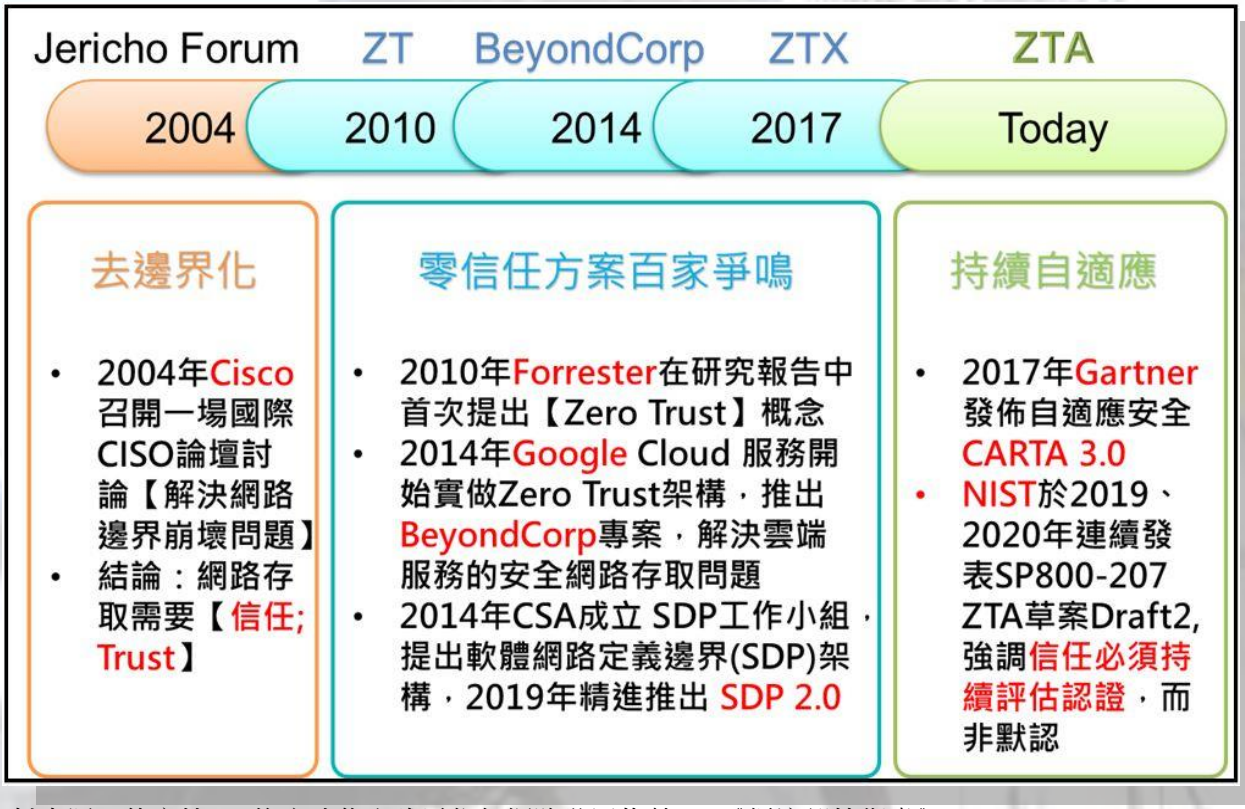
[1]李宗翰，<治療資安憂鬱症的新配方：Security2.0>，《iThome》，https://storage.ithome.com.tw/node/39553，2006/09/25，(檢視日期：2021/12/24)。

二、發展

零信任網路，源自 1994 年 Stephen Paul Marsh 的博士論文 Formalising Trust as a Computational Concept，這篇論文 Stephen Paul Marsh 所提出來的結論是信任不是一種簡單的對抗性(Confrontational)或純粹的人類現象，而是可以用數學結構來進行的有限描述，信任最終是超越了道德、醫學、合法、正義及判斷等的人為概念，並且在資訊網路上的認知是：在保障電腦系統、應用程式和資訊安全方面，零信任遠遠超過了不信任，才能夠更為安全的保障資料。[2]

而零信任在 1994 年因為其資料量沒有像現在這樣的龐大，因此這樣論點在當時沒有被廣泛應用，直到近幾年雲端服務及物聯網等科技的進步，隨著大量的資料處理需求、日趨複雜的網路攻擊技術與高度資料安全要求，因此，在 2004 年，思科在一場國際首席資安長論壇中，討論如何解決網路邊界崩壞的問題；到了 2010 年零信任的概念才開始受到產業界的關注並提出「絕不信任，必須驗證」的概念，零信任便開始蓬勃發展時期至今(如圖 11)。[3]

圖 11 零任信發展史



資料來源：徐富桂，<後疫時代全球零信任網路發展趨勢>，《經濟部技術處》，https://www.moea.gov.tw/MNS/doit/industrytech/IndustryTech.aspx?menu_id=13545&it_id=330，2020/10/21，(檢視日期：2021/06/14)。

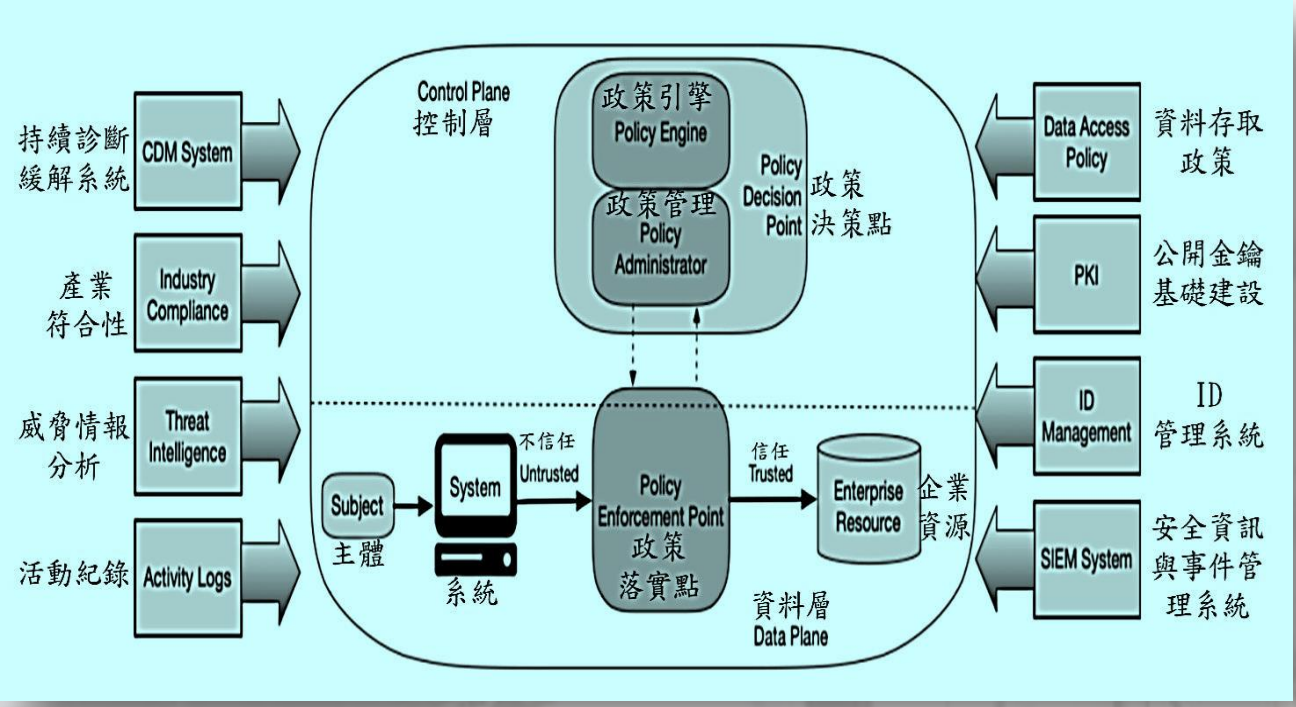
[2] 偉康科技，<新世代資安概念：零信任安全模型介紹(Zero Trust)>，《偉康科技洞察室》，https://www.webcomm.com.tw/blog/265/zero-trust-security-model/，2021/03/31，(檢索日期：2021/08/09)。

[3]徐富桂，<後疫時代全球零信任網路發展趨勢>，《經濟部技術處》，https://www.moea.gov.tw/MNS/doit/industrytech/IndustryTech.aspx?menu_id=13545&it_id=330，2020/10/21，(檢視日期：2021/06/14)。

三、零信任的標準

近年在資安防護的觀念上，零信任概念越來越熱門，在 2020 年 8 月美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）也發布了 SP 800-207 標準文件，探討並說明如何建立零信任架構（Zero Trust architecture，ZTA），在這份文件中提出 ZTA 的核心，就是對於任何關鍵資源，在存取前都要檢查使用者身分是否有所請求的權限。因此，任何需要經過存取控制的政策落實點(Policy Enforcement Point, PEP)，都需要實施權限檢查，如次世代防火牆可識別使用者的身分、裝置等資訊及控管不同的應用程式流量來達到政策控管的目的；另在檢查過程當中，政策規則是由政策決策點(Policy Decision Point, PDP)律定(如圖 12)，政策決策點也就是 ZTA 的大腦，透過演算法，藉由歷史的存取要求、主體資料庫及歷史、資產資料庫、資源政策要求、威脅情資與紀錄來做訓練後得到符合單位所需的政策規則後，再交由政策落實點執行管控，上述說明，也表示了零信任還是有信任關係存在，網路還是需要信任某些元件，如：政策決策點與政策執行點等，只是每次在執行存取前，都必須做到重新檢查其身分是否有所請求的權限。[4]

圖 12 ZTA 的核心



資料來源：National Institute of Standards and Technology, “Zero Trust Architecture,” NIST Special Publication 800-207, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, pp 6,2020/08/11

[4] 羅正漢，<台灣資安大會直擊：看懂零信任架構，先釐清對於ZTA常見的3大迷思>，《iThome》，https:// www.ithome.com.tw/news/144551，2021/05/21，(檢索日期：2021/08/11)

上述標準文件中提到了零信任架構的七大原則，分述如下，簡單來說就是識別可存取資源、連線安全、妥善存取控制、考量存取者狀態、了解資源狀態，以及監控裝置與資源風險，持續蒐集資訊與改善。[5]

(一)所有的資料來源與運算服務都要認為是資源。

(二)不管在何處的設備，連線都需要確保安全。

(三)對於個別的存取需求，應該要以每次連線實施驗證為基礎來核准其存取。

(四)資源的存取應該要基於用戶端識別、應用服務，以及要求存取應基於資安能監控之狀態，並可依據威脅狀況來動態決定是否准許存取資源。

(五)網路監控需衡量所有擁有與相關資訊資產的正確性與安全狀態。

(六)在允許存取之前，所有的資源的身分鑑別與授權機制，都要依監控結果動態決定，並且嚴格落實管控機制。

(七)單位應該要儘可能收集有關資訊資產、網路架構、骨幹，以及通訊網路的現況，並用這些資訊來增進安全狀態。

四、零信任優缺點

(一)優點

1.控制整個資訊資產：監控全部連線的資訊設備，不再區分網內、網外的方式，以維整體資訊網路安全。

2.以相同的方式管理和保護所有使用者：基於零信任網路之概念，不再區分內、外網連線，系統管理者可用相同的方式來管控所有使用者。這既可簡化資訊安全管理作業，又能確保所有設備與使用者受到平等對待。

3.大幅度減少惡意軟體或攻擊者的移動：藉由每次連線驗證機制，來增加攻擊者橫向移動之困難度，再透過各系統間身分的查驗，進一步限制其擴散能力，使攻擊者難以短時間完全掌握整個網路。

(二)缺點

建構零信任網路，其概念就是每次連線都是新的連線，均須實施驗證方可實施存取、連線，而驗證機制就針對身分、設備與權限三項實施驗證，與傳統架構上的驗證身分與權限的方式不同、次數也不同，所耗的網路成本也會增加，因此，零信任網路的困境主要是驗證頻繁所造成，其缺點如下:

1.效能下降。

2.便利性不足。

3.對即時性資料的無法快速處理[6]。

---

[5] 同註2

[6] Sophos白皮書，<揭秘零信任>，《Sophos》，https://www.fairline.com.tw/data/download/file/1598931730632791978.pdf

導入與研析

一、網路防護架構

陸軍網路區分行政網、指管網等網路架構，本文以行政網路實施探討，其探討區分兩種方式，第一種方式將國軍現階段不同機關、部隊層級行政網路視為整體網路架構，將陸軍行政網路視為同一層級的網路，對應到 A 級資通安全責任等級，並採取該等級律定的防護措施，來作為本研究對照組，第二種是以陸軍部隊型態來區分為司令部層級、軍團層級、聯兵旅階層的行政網路，分別對應到 A 級、B 級、C 級資通安全責任等級，也應對應採取的防護措施(如表 4)，因聯兵旅以下層級網路，維管仍由聯兵旅級維管，故聯兵旅以下層級網路視為聯兵旅層級網路，其探討分述如下：

(一)第一種方式的防護措施：將將國軍現階段不同機關、部隊層級行政網路視為整體網路架構，為一個大型的網路架構，採取資通安全責任等級中 A 級機關所需資通安全防護作為，包括網路防火牆、入侵偵測及防禦機制、防毒軟體、具有郵件伺服器之電子郵件過濾機制、對外服務的核心資通系統之應用程式防火牆與進階持續性威脅攻擊防禦措施等相關設施。

(二)第二種方式的防護措施：依陸軍部隊型態來區分為司令部層級、軍團層級、聯兵旅階層，分別對應採取資通安全責任等級中 A 級、B 級、C 級機關所需資通安全防護作為的防護作為。A 級機關所需的防護作為如前所述，B 級機關所需的防護作為包括網路防火牆、入侵偵測及防禦機制、防毒軟體、具有郵件伺服器之電子郵件過濾機制與對外服務的核心資通系統之應用程式防火牆，C 級機關所需的防護作為包括網路防火牆、防毒軟體與具有郵件伺服器之電子郵件過濾機制。A 級與 B 級機關資通安全防護作為差異，為 B 級未具有進階持續性威脅攻擊防禦措施等相關設施；B 級與 C 級機關資通安全防護作為差異，為 C 級未具有入侵偵測及防禦機制及對外服務的核心資通系統之應用程式防火牆與等措施。

二、零信任導入

導入零信任網路架構，根本精神為所有連線均不可信任，因此，對於每次連線都應重新驗證連線的來源，進而確認其相關權限，在權限管理應秉持最小權限來實施管理，以下就針對上述兩種架構導入零信任網路項目實施說明(如表 5)：

(一)所有網路連線均需通過身分驗證後才可連線：零信任網路中，針對所有的連線均須完成驗證後，方可實施連線，並且在網路上所收到的封包都需要進行檢查，以確認來源之合法性。

(二)加密傳輸：不能相信任何網路可以將資料做可靠的傳輸，因此，只要在網路上傳

，2020/01，(檢視日期：2021/12/24)

輸的資料都應該使用加密傳輸。

(三)身分授權應秉持最小權限之原則：定期的清理冗餘的帳號，並檢視相關的權限是否過大，以避免帳號遭盜用進而造成安全缺口。

三、研析比較

以下針對上述之兩種方式分別進行未導入零信任網路與導入後之分析說明，第一種方式採同一層級網路(如表 6)；第二種方式採不同一層級網路比較說明(如表 7)。

(一)第一種方式(同一層級網路)：未導入零信任網路的作法，在人員驗證方面，以往採用目錄伺服器實施人員身分驗證與人員權限管理，資料傳輸在傳送機密文件才實施加密，而在資料存取上採用存取過濾規則管理後均為加密後方可存取；導入零信任網路後，其差異在於人員身分結合憑證中心實施驗證、權限的管理由業務主管實施授權管理及資料傳輸須實施身分驗證與加密傳輸。

(二)第二種方式(不同一層級網路)：未導入零信任網路的作法與第一種方式相同，導入零信任網路後，主要差異在於人員身分結合憑證中心實施驗證及在跨不同層級網路時需網路防火牆來檢驗來源端的位址是否為合法位址、權限的管理應由業務主管實施授權管理；另在不同層級網路時應由單位資安長對外來人員的權限實施稽核，資料傳輸須實施身分驗證與加密傳輸。

綜合說明上述兩種方式在導入前後的比較，其中在網路連線驗證上，導入後不論人員、設備上線均須完成驗證後才可連線，其較未導入的方式來的安全，在權限授予部分，導入後由該業務主管負責對其所屬授予該部門相關權限，藉業務主管瞭解實需，進而達到最小權限之目的，讓權限不再有過多或過小之狀況。

上述所提之兩種方式導入零信任網路架構後，在身分驗證上都需要藉由目錄伺服器與憑證中心來實施人員身分驗證，兩者不同之處(如表 8)在於不同層級的網路在實施身分驗證時，則另外加上網路防火牆來針對來源 IP 位址及欲使用之服務進行管控，因此在不同層級的網路架構下較為安全；另零信任網路的架構對設備的驗證也是處在「每個設備的連線都是不可信任」的前提，因此對設備亦嚴格要求須完成設備驗證後，方可實施網路連線，設備須跨不同層級網路實施連線時，除上述驗證外，亦在網路防火牆實施稽核 IP 位址以確認為合法設備，以維護網路安全。

表 4 探討方式

區分	第一種方式	第二種方式
司令部層級	A 級資通安全責任等級	A 級資通安全責任等級
作戰區(防衛部)層級		B 級資通安全責任等級
聯兵旅階層		C 級資通安全責任等級

資料來源：作者調製

表 5 導入零信任項目一覽表

項目	內容
網路連線均需身分驗證	人員上線時須完成身分驗證
	設備上線時須完成確認
	資料傳輸前先完成身分驗證
加密傳輸	網頁傳輸
	資料傳輸
身分授權應為最小權限	定期檢核帳號擁有之權限
	清理冗餘帳號

資料來源：作者調製

表 6 同一層級網路導入零信任之比較表

項目	內容	同一層級網路 未導入零信任網路	同一層級網路 導入零信任網路
網路連線均需身分驗證	人員上線時須完成身分驗證	僅使用目錄伺服器實施身分查驗。	結合目錄伺服器與憑證中心實施身分查驗。
	設備上線時須完成確認	設備連上網時，使用資訊資產來確認為合法設備。	設備連上網時，結合資訊資產與憑證中心來確認為合法設備。
	資料傳輸前先完成身分驗證	以用目錄伺服器實施身分查驗，大多不再實施驗證。	結合目錄伺服器與憑證中心再次實施身分查驗。
加密傳輸	網頁傳輸	使用 https 協定。	使用 https 協定。
	資料傳輸	資料存取採加密方式。 資料傳輸未全使用加密。	資料存取採加密方式。 資料傳輸採加密方式。
身分授權應為最小權限	定期檢核帳號擁有之權限	1.帳號權限資訊(安)長核定後，再由資訊(安)部門實施設定。 2.資訊(安)長定期稽核部門權限授予是否適切。	1.帳號權限由業務主管勾稽。 2.資訊(安)長定期稽核部門權限授予是否適切。
	清理冗餘帳號	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，應對相關帳號實施清理。	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，對相關帳號實施清理。

資料來源：作者調製

表 7 不同層級網路導入零信任之比較表

項目	內容	不同層級網路 未導入零信任網路	不同層級網路 導入零信任網路
網路連線均需身分驗證	人員上線時須完成身分驗證	僅使用目錄伺服器實施身分查驗。	結合目錄伺服器與憑證中心實施身分查驗，然其網路架構區分等級，故應經由網路防火牆實施管控，方可確認為合法連線。
	設備上線時須完成確認	設備連上網時，使用資訊資產來確認為合法設備。	設備連上網時，結合資訊資產與憑證中心來確認為合法設備，然其網路架構區分等級，故應經由網路防火牆實施管控，方可確認為合法連線。
	資料傳輸前先完成身分驗證	以用目錄伺服器實施身分查驗，大多不再實施驗證。	結合目錄伺服器與憑證中心再次實施身分查驗，然其網路架構區分等級，應經由網路防火牆實施管控，方可確認為合法連線。
加密傳輸	網頁傳輸	使用 https 協定。	使用 https 協定。
	資料傳輸	資料存取採加密方式。 資料傳輸未全使用加密。	資料存取採加密方式。 資料傳輸採加密方式。
身分授權應為最小權限	定期檢核帳號擁有之權限	1.帳號權限資訊(安)長核定後，再由資訊(安)部門實施設定。 2.資訊(安)長定期稽核部門權限授予是否適切。	1.帳號權限由業務主管設定。 2.跨不同層級之權限由資訊(安)長核定後，再由資訊(安)部門實施設定 3.資訊(安)長定期稽核部門權限授予是否適切。
	清理冗餘帳號	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，應對相關帳號實施清理。	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，應對相關帳號實施清理。 3.跨不同層級之帳號，應任務結束後，由資訊(安)部門實施清理相關帳號與權限。

資料來源：作者調製

表 8 零信任導入後兩種方式比較表

項目	內容	第一種方式導入 (同一層級網路)	第二種方式導入 (不同層級網路)
網路連線均需身分驗證	人員上線時須完成身分驗證	結合目錄伺服器與憑證中心實施身分查驗。	結合目錄伺服器與憑證中心實施身分查驗，然其網路架構區分等級，故應經由網路防火牆實施管控，方可確認為合法連線。
	設備上線時須完成確認	設備連上網時，結合資訊資產與憑證中心來確認為合法設備。	設備連上網時，結合資訊資產與憑證中心來確認為合法設備，然其網路架構區分等級，故應經由網路防火牆實施管控，方可確認為合法連線。
	資料傳輸前先完成身分驗證	結合目錄伺服器與憑證中心再次實施身分查驗。	結合目錄伺服器與憑證中心再次實施身分查驗，然其網路架構區分等級，應經由網路防火牆實施管控，方可確認為合法連線。
加密傳輸	網頁傳輸	使用 https 協定。	使用 https 協定。
	資料傳輸	資料存取採加密方式。 資料傳輸採加密方式。	資料存取採加密方式。 資料傳輸採加密方式。
身分授權應為最小權限	定期檢核帳號擁有之權限	1.帳號權限由業務主管設定。 2.資訊(安)長定期稽核部門權限授予是否適切。	1.帳號權限由業務主管設定。 2.跨不同層級之權限由資訊(安)長核定後，再由資訊(安)部門實施設定 3.資訊(安)長定期稽核部門權限授予是否適切。
	清理冗餘帳號	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，應對相關帳號實施清理。	1.定期清理離(退)職人員帳號。 2.協力廠商結案後，應對相關帳號實施清理。 3.跨不同層級之帳號，應任務結束後，由資訊(安)部門實施清理相關帳號與權限。
備註	不同層級網路連線針對人員、設備的連線，除原本的驗證機制外，尚須加上網路防火牆實施管控，以維該網路之安全性。		

資料來源：作者調製

結論

綜述，本文所提以整合式網路概念及以部隊型態階層區分網路架構兩種方式，導入網路零信任概念，其最主要之目的在於有完整網路的可見性、能防止未經授權的存取、內網異常流量的分析等，而零信任網路架構後，以下就兩大方式摘述如后：

一、整合式網路概念

所謂整合式網路系將國軍現階段不同機關、部隊層級行政網路視為整體網路架構，即將實體骨幹視為一體，僅視為同網別之一個行政網，導入零信任概念分析其可行性，作為本研究對照組。

此整合性網路架構導入零信任概念，雖以單一閘道口實施驗證，惟此網路架構涵蓋面積較廣、收容戶較多，降低用戶使用效能及伺服器處理效能，驗證過程中缺乏分層負責，恐遭負荷過量。

二、部隊型態階層

此方式係以陸軍部隊型態來區分為司令部層級、軍團層級、聯兵旅階層的行政網路導入零信任概念，在網路閘道口新增網路防火牆、憑證中心、目錄服務等機制，來探討零信任可行性。研究結果發現，在不同層級網路的介接上，加入不一樣的資安管制機制，因網路防火牆針對來源實施管控、憑證中心驗證連線人員身分驗證、目錄服務管控人員對設備的使用權限，進而提升網路連線之安全性與可靠性。因此，藉由透過層層驗證可將不同層級網路間的連線將帶來更安全的三大軟硬體等管理效益：

(一)網路連線安全：在網路連線方面除了對人員實施身分驗證外，亦對設備實施驗證，以維護整體網路安全。

(二)帳號安全：帳號管理在任何系統上扮演第一關卡安全機制，透過定期的人員帳號稽查與離退清理，可以避免有冗餘的帳號存在，並可結合人事系統對離(退)職人之帳號實施管制後，由管理單位奉權責長官核定後再實施移除作業。

(三)權限的控管：透過業務主管授予因工作職掌所屬權限的方式，可符合該部門實際狀況與任務實需。若部屬業務涵蓋跨部門之屬性，則需要由上層單位資訊(安)長來針對該員權限實施稽核，以避免有權限失當之情事；另外在跨層級縱向網路的部分，網管人員可先行透過網路防火牆對 IP 與服務的管控，來稽核連線的來源端使用者、設備與所要使用的服務是否為核准使用，提供單位資安長判核憑據。

上述安全機制雖看似完善，惟在不同層級網路的介接上，因為零信任網路導入，加入管控、驗證機制，提升網路安全性與可靠性將會面臨頻繁的驗證，可能導致造網路連線與資料存取效能下降、便利性不足及即時性資料的無法快速處理等問題，故頻繁驗證的問題仍須克服。

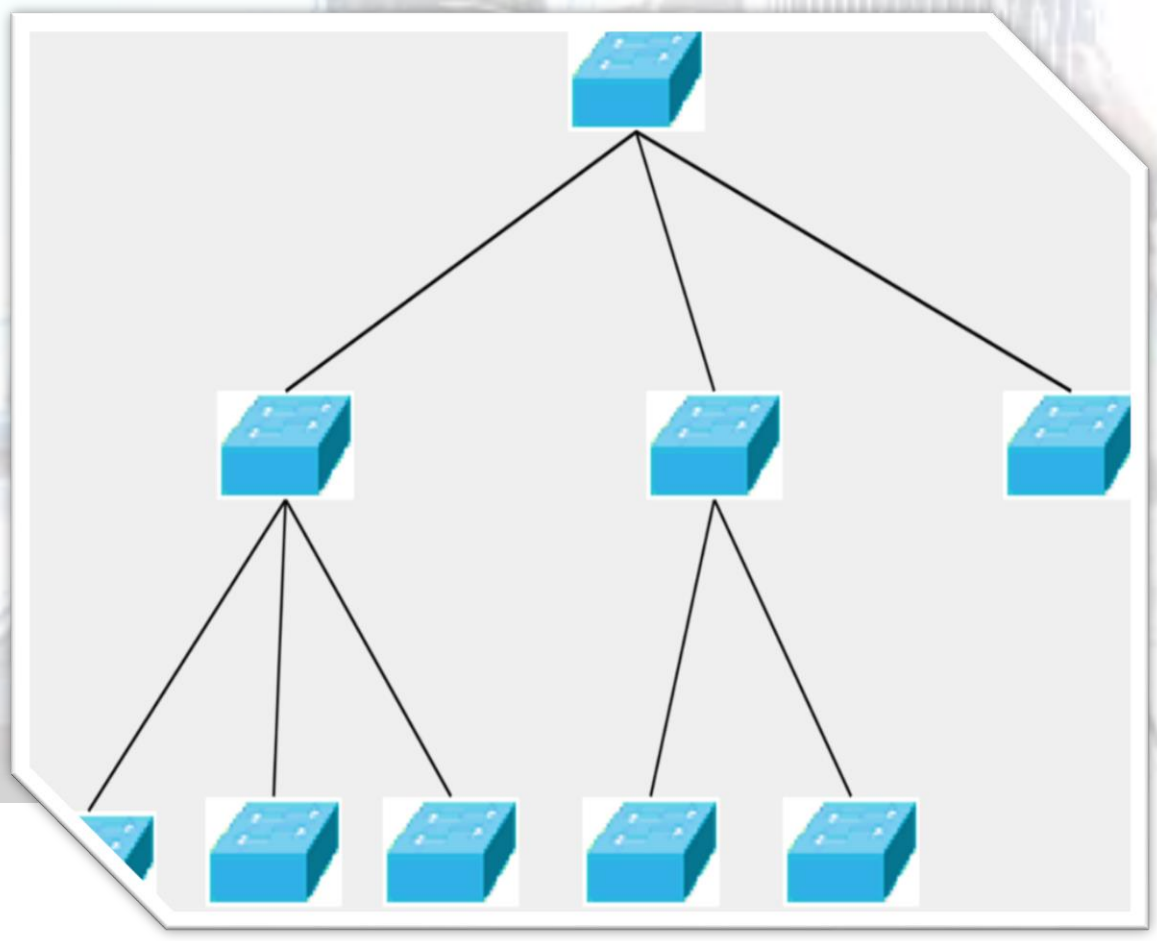
綜上結論，以國軍現行資安管理模式及網路建置模式，駭客入侵致橫向跨大危害及伺服器負載等後果，在資安防護失效所需承擔風險將遠遠超過以部隊階層網路架構區分，導入零信任概念的模式，複以驗證問題克服性，達到更為可靠之網路安全、資料安全之目的，相對效益高。

建議

一、本文針對部隊型態階導入零信任概念所遇限制，提出以下幾點建議，可供後續國軍網路嘗試零信任手段之參考：

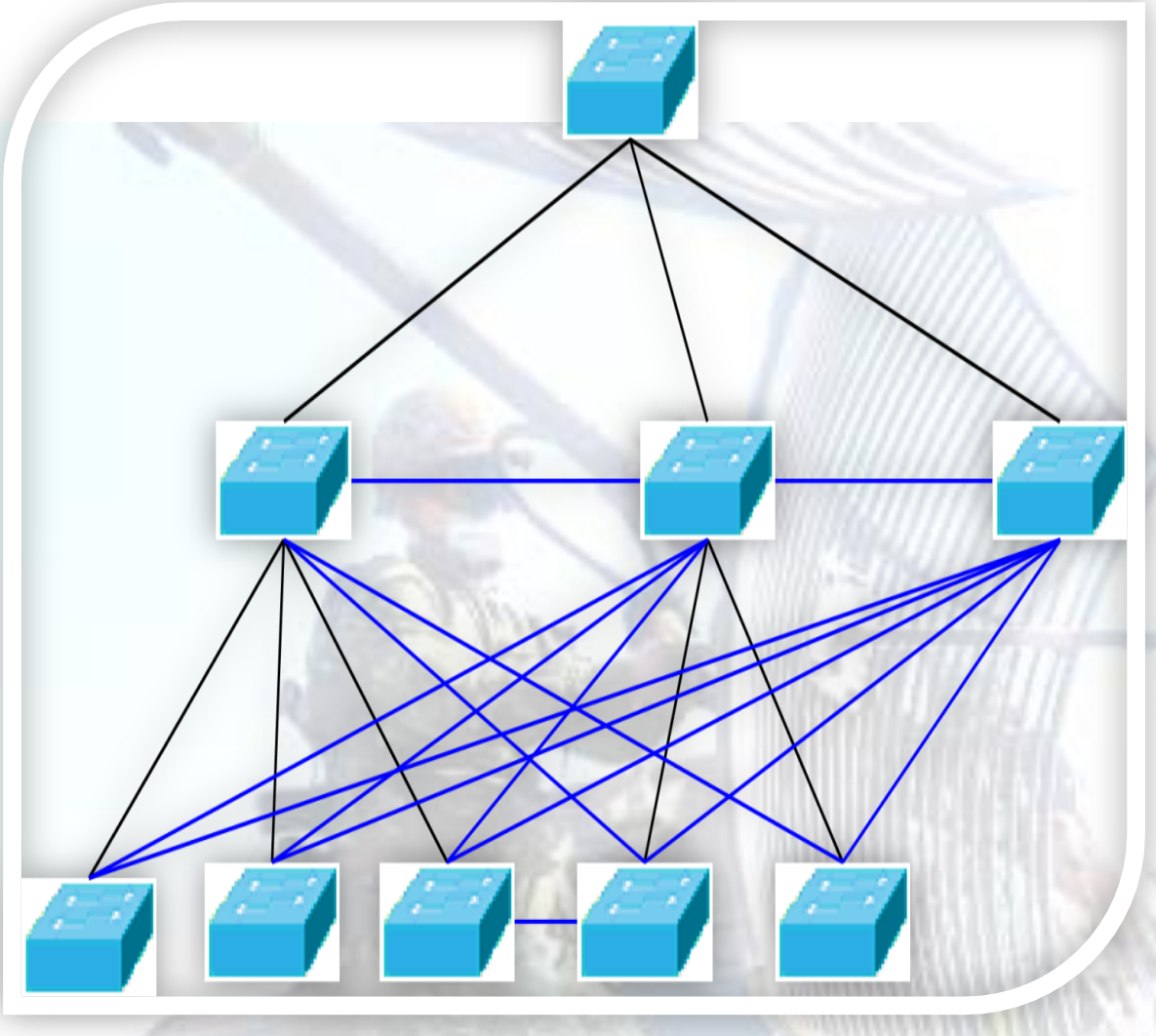
(一)由樹狀結構強化為網狀結構之基礎設施：現行國軍聯兵旅層級網路，網路連結採用的方式類似單一式連結的方式，如圖 13，建議採用複式配置來達到網路的強韌性與彈性，如圖 14，並且可以採用練錄聚合(Ether Channel)與服務品質(Quality of Service, QoS)等技術來強化區域網路內的效能與品質。

圖 13 單一架構



資料來源：作者繪製

圖 14 複式架構



資料來源：作者繪製

(二)擴充雲端服務架構：因頻繁驗證而導致效能下降，可透過結構的調整，採用雲端架構，藉由雲端高彈性、高速運算、快速處理資料等特性來改善效能下降之問題。

(三)結合多元辨識技術：頻繁的驗證可透過安全密碼、生物識別技術與單一登入(Single Sign-On, SSO)技術，簡化驗證的程序與密碼頻繁的輸入，藉此解決頻繁的驗證的問題。

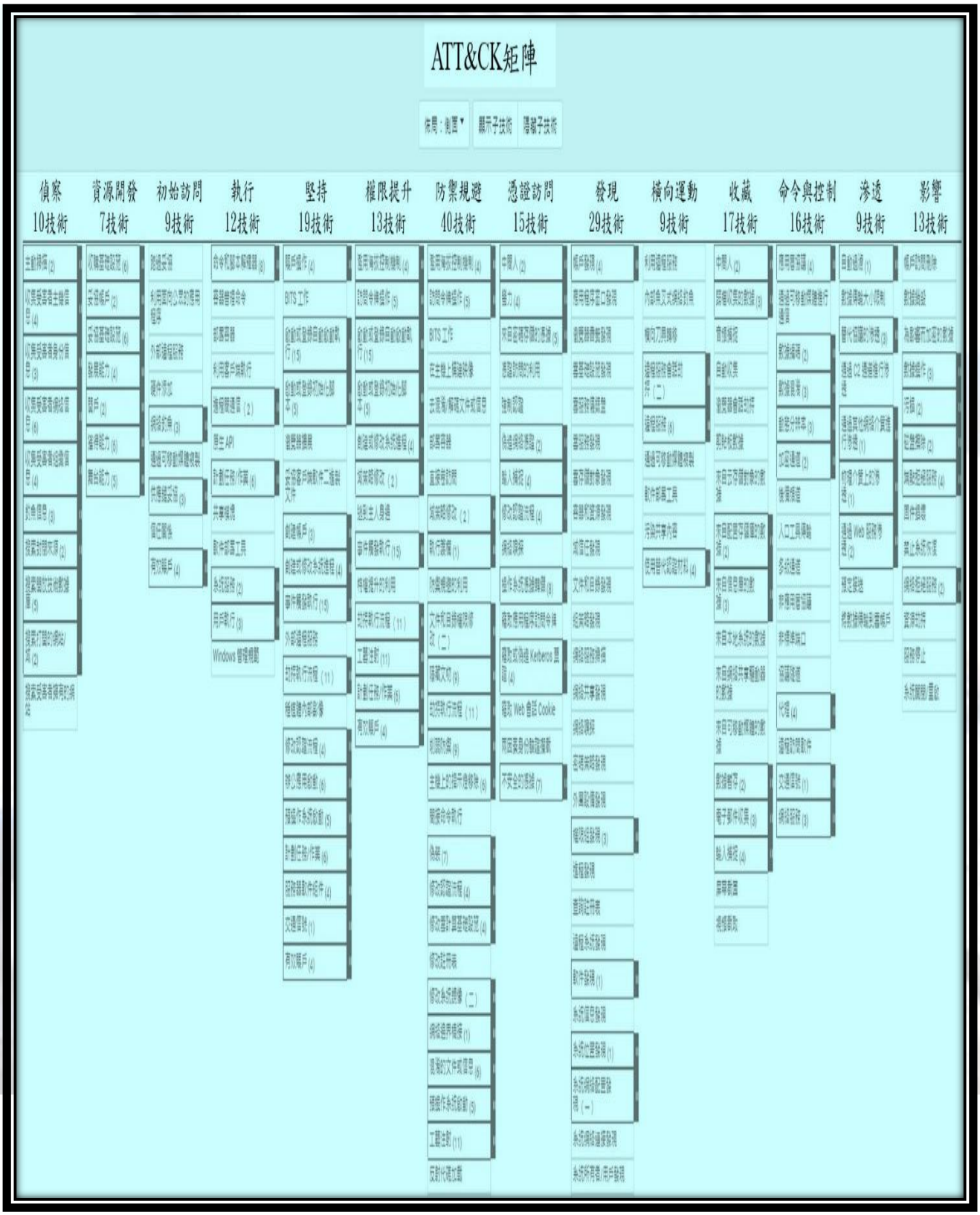
二、針對實際架構零信任時實施要領提出建議

(一)認清所面臨的威脅：可藉由 MITRE 所提出的資安攻擊矩陣圖(如圖 15)，針對本身所會面臨到的威脅實施列舉。

(二)評估現行之防護架構，妥善部署資源：導入零信任網路所需的前置作業，不外乎是先審視目前本身的網路防護架構，針對現有的防護設施，透過以下幾點來實施評估，冀以找出相關不足的地方，以便後續補強

(三)綜合評估：針對上述所列舉的威脅，透過防禦矩陣圖(如圖 16)實施評估，評估本身防禦架構是否有不足之處。

圖 15 攻擊矩陣圖



資料來源：MITRE,<Version of ATT&CK>《The MITRE Corporation》https://attack.mitre.org/resources/versions/，2021/04/29，(檢索日期2021/12/11)

圖 16 防禦矩陣圖

資料來源：羅正漢,<【用Cyber Defense Matrix搭配資安框架改善資安弱點】資安策略成效要靠真實威脅調整>《iThome》 https://www.ithome.com.tw/news/140095，2020/09/24，(檢索日期2022/7/13)

(四)盤點網路設備與資源，落實資訊資產管理：完成現有架構的審視與評估後，接續就是清查所有的設備與資料價值性鑑定，透過一系列的清查後，即可了解下列事項：

1.單位內所有資訊資產設備，其作用、位置、IP 等相關資料。

2.單位內所有資料的價值性與機敏性，並完成相關文件標示與註記。

(五)清查使用者帳號與權限，實踐最小權限：針對目前網路架構中所有的帳號與密碼還有其對應之權限實施清查，並針對系統內之權限管控實施稽核，將過大的權限實施修正，以達到權限最小化之目的，如此可以避免內部人員因權限過大而造成資安事件，及讓駭客不易實施橫向移動、提升權限。

(六)強化資訊教育，職能分工合作：在資訊教育可區分：針對所有人員的普及教育、業務主管的職能教育與資訊人員的專業教育等三項，針對上述三項實施說明：

1.普及教育：其對象為所有人，內容為資訊、資安的基本知識，方式可以參照每年學習時數護照方式實施。

2.職能教育：其對象為所有業務主管，內容為權限管理與設定及資安長所應具備之知識與技能，方式可採每年實施合格簽證。

3.專業教育：其對象為資訊人員，內容為資訊系統與資安技術，實施方式由國防大學師資結合部外師資並透過證照的方式實施簽證，並配合政府近期推動之「臺灣資安職務地圖」實施培育，以符合實需。

(七)推廣運用跨網別介接：在本文所探討在陸軍行政網內不同層級網路的介接上，可以知道藉由零信任網路導入，能提升網路連線之安全性與可靠性；因此，在不同網別的

介接上，導入零信任網路，依本文所述，亦可強化網路的安全性與可靠性，建議在未來陸軍行政網與指管網的介接時，可以導入零信任網路的架構，來提升網路安全性與可靠性。

參考文獻

一、江湖海，《零信任網路-在不受信任的網路中構信安全系統》(台北)，碁峯資訊股份有限公司，2020年11月。

二、MITRE,<Version of ATT&CK>《The MITRE Corporation》https://attack.mitre.org/resources/versions/，2021/04/29，(檢索日期2021/08/11) 。

三、Marsh McLennan, SK Group, Zurich Insurance Group, The Global Risks Report 2021 (World Economic Forum:Switzerland,2021),pp.11. 。

四、〈國家資通安全戰略報告〉，民國107年9月，頁15。

五、吳啟文，<資安威脅趨勢及防護策略>，《行政院國家資通安全會報技術服務中心》，https://secutechinfosecurity.tw.messefrankfurt.com/content/dam/messefrankfurt-redaktion/infosecurity/2021-march-seminar-agenda/資安威脅趨勢及防護策略_行政院國家資通安全會報中心-吳啟文-主任.pdf，2021/03/09，(檢視日期：2021/06/14)。

六、偉康科技，<新世代資安概念：零信任安全模型介紹(Zero Trust)>，《偉康科技洞察室》，https://www.webcomm.com.tw/blog/265/zero-trust-security-model/，2021/03/31，(檢索日期：2021/08/09)。

七、羅正漢，<台灣資安大會直擊：看懂零信任架構，先釐清對於ZTA常見的3大迷思>，《iThome》，https:// www.ithome.com.tw/news/144551，2021/05/21，(檢索日期：2021/08/11)。

八、NCSC，<Device Security Guidance>《NCSC》，https://www.ncsc.gov.uk/collection/mobile-device-guidance/infrastructure/network-architectures-for-remote-access，2021/06/21，(檢索日期：2021/08/11)。

九、徐富桂，<後疫時代全球零信任網路發展趨勢>，《經濟部技術處》，https://www.moea.gov.tw/MNS/doit/industrytech/IndustryTech.aspx?menu_id=13545&it_id=330，2020/10/21，(檢視日期：2021/06/14)。

十、National Institute of Standards and Technology, “Zero Trust Architecture,” NIST Special Publication 800-207,https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, pp 6,2020/08/11。

十一、Sophos白皮書，<揭秘零信任>，《Sophos》，https://www.fairline.com.tw/data/download/file/1598931730632791978.pdf，2020/01，(檢視日期：2021/12/24)。

十二、李宗翰，<治療資安憂鬱症的新配方：Security2.0>，《iThome》，https://storage.ithome.c

om.tw/node/39553，2006/09/25，(檢視日期：2021/12/24)。
十三、偉康科技洞察室，<新世代資安概念：零信任安全模型介紹>，《偉康科技》，https://www.webcomm.com.tw/blog/zero-trust-security-model/，2021/03/21，(檢視日期：2021/12/24)
十四、劉哲銘，<次世代防火牆需要具備的6項功能>，《iThome》，https://www.ithome.com.tw/news/95997，2010/01/08，(檢視日期：2022/7/17)
十五、簡如茵，<駭客終結者 2.0 登場！打破舊有資安概念，零信任架構 (ZTA) 引領資安新風潮——台科大教授兼資通安全研究與教學中心主任查士朝專訪>，《科技大觀園》，https://pansci.asia/archives/330016，2021/09/09，(檢視日期：2022/7/17)
十六、羅正漢，<【搞懂零信任，從理解NIST SP 800-207著手】打造以零信任原則的企業網路安全環境>，《iThome》，https://www.ithome.com.tw/news/145709，2021/07/21，(檢索日期：2022/07/17)。
十七、Mjcaparas，<什麼是零信任？>，《Microsoft》，https://docs.microsoft.com/zh-tw/security/zero-trust/zero-trust-overview，2022/06/10，(檢視日期：2022/7/17)

作者簡介

李勝宏少校，通資電正規班 190 期，國防大學理工學院資工所 101 年班，曾任排長、教官，現任陸軍通信電子資訊訓練中心網路作戰組教官。