

投稿類別：商業類

篇名：

疫情下的救星：淺析視訊會議軟體 Zoom 的優勢與危機

作者：

張晉儀。私立曉明女中。高二甲班

陳怡嘉。私立曉明女中。高二甲班

廖晨芳。私立曉明女中。高二甲班

指導老師：

賴維真老師

壹、前言

一、研究動機

在新冠肺炎的肆虐下，世界各地皆災情慘重，必須實施封城和停課等政策以降低感染人數，人們被迫關在家中使用遠端視訊教學及工作。但同時，這樣的困境也帶來不少改變及成長，數位轉型速度飛速進展，令人驚豔的創意發想接二連三的出現，線上產業也隨之蓬勃發展。因此，本研究欲藉此機會研究在疫情期間成長最為迅速的線上視訊軟體，瞭解其成功的因素及爆紅後出現的爭議，並嘗試提出改善方法。

二、研究目的

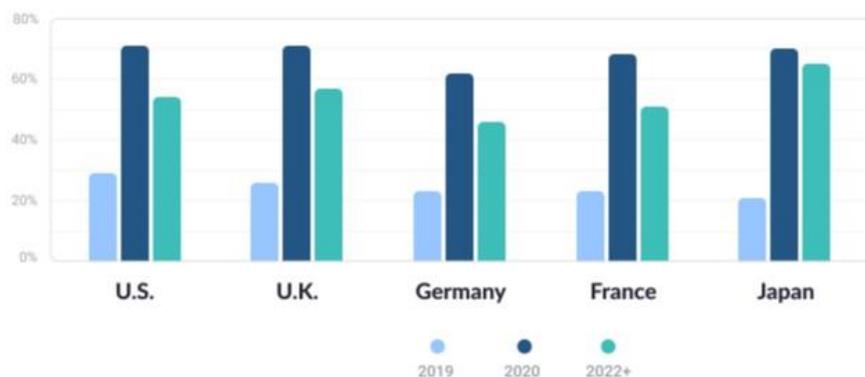
- (一) 以 Zoom 為主要研究對象，瞭解線上視訊軟體產業與新冠肺炎疫情的關係與發展。
- (二) 探究疫情以後 Zoom 對社會造成的影響，包括優缺點和爭議部分。
- (三) 比較 Zoom 和視訊會議軟體，探究其市佔率最高之成功因素。
- (四) 透過了解其爭議部分，學習如何保護自身的資訊安全。

貳、文獻探討

一、新冠肺炎疫情對線上視訊軟體帶來的影響

疫情的爆發迫使各地的機構尋找新的運作和聯繫方式以確保公眾安全。視訊會議成為了我們維持日常生活的唯一管道，使我們能夠在數字環境中繼續工作和學習，傳統的面對面操作也發生了轉變，教育和醫療保健等行業必須採用這些遠端會議的方法以繼續運營，各國被調查企業的視訊會議使用情況如圖一。

圖一：各國被調查企業的視訊會議使用情況



(圖一資料來源：Zoom 官網 (2021) 敏捷性和創新的故事：《COVID-19 疫情期間視訊通訊的

二、Zoom

(一) 簡介

Zoom 由曾為思科的首席工程師袁征於 2011 年成立，是一個被廣泛使用於在家工作、遠距教學與社交上的免費應用軟體，其主要業務為：以雲端運算為基礎的遠端會議軟體服務，並提供了用於視訊電話、即時通訊和商務電話系統的電腦軟體及行動應用程式。研究者選擇以 Zoom 為研究素材，乃因在新冠肺炎疫情惡化後，許多公司和學校開始採用遠端形式工作，使 Zoom 的使用量急劇增加，從年初到三月中旬成長了超過六成，銷售額增長 169%，為全部視訊會議軟體上市占率最大的公司，因此欲探討其市佔率最高之成功因素。

(二) 經濟發展

2019 年 4 月時 Zoom 上市，並向社會公開發售第一批股票，其估值為 159 億美元。Zoom 在截至於 2020 年 4 月 30 日的三個月中，銷售額增長 169%，至 3.282 億美元。自 2020 年 1 月份以來，該公司增加了超過 180,000 名擁有 10 名員工的客戶。同時也在此季度實現了 2700 萬美元的利潤，比上一財政年度的利潤高。

圖二：Zoom 股價圖（截至 2020 年 12 月）



(圖二資料來源：新浪財經(2021)行情中心。2021 年 5 月 1 日，取自 <https://reurl.cc/0jXQAA>)

(三) 爭議事件

1. 科技網站 Motherboard 指出，Zoom 會將 IOS 版用戶數據發送到 Facebook，在隱私政策中，只說明會取用臉書資料，未指出會回傳資料。
解決方式：隔日 Zoom 查出是臉書 SDK 自行收集裝置資料，已經移除 SDK。

2. 網路安全公司 VMRay 的惡意程式研究人員 Felix Seele 指出 Zoom 會自動安裝於 macOS 版的 Zoom 程式，且使用預先安裝的腳本程式，以不清楚的內文警告使用者，容易使人被誤導。
解決方式：Zoom 的 CEO 袁征出面道歉，更新隱私政策，也緊急修補 Mac 和 Windows 的程式版 Zoom 軟體。
3. Zoom 允許會議主持人跟踪與會者，卻聲稱該應用程序已進行端到端加密，讓使用者錯誤的相信自己的資訊安全有受到系統保護。從加拿大多倫多大學市民實驗室（Citizen Lab）公佈的資料來看，Zoom 的資安白皮書與實際內容有落差，且會將訊息自動傳經中國的伺服器。
解決方式：他們表示已移除了不必要的追蹤功能。修正了將美國服務連向中國伺服器的失誤，現在是以用戶的所在地決定資料彙集處。

（四）Zoom bombing

1. 定義

Zoom bombing（Zoom-bombing 或 Zoom raiding）是在疫情下出現的新名詞，主要指在視訊通話中被病毒或駭客侵入的現象。2020 疫情中，全世界普遍在家工作，促使全世界大規模使用線上視訊後，駭客拆解網路密碼或漏洞進入 Discord、Reddit、Zoom 等對談，並散播種族主義、歧視、性暗示等偏激內容干擾會議。甚至有學生自願外洩密碼，請陌生人進行 zoom 轟炸，來增加上課的趣味性。

2. 事件

中國女權行動家尚美麗利用 Zoom 出席線上講座「後 MeToo 時代的女權運動」在會議開始前，有入侵者使用共享螢幕繪製男性生殖器官，還開啟麥克風罵髒話。會議途中，因應觀眾需求增加了參與者的數量，卻大量湧入重複留言「Sorry, I'm late, what I've missed?」（對不起我遲到了，我錯過了什麼？），還有聲音一直重複「Corona」（暗指「冠狀病毒」），更有參與者表示看到淫穢色情的畫面。最後只好暫停活動，使用人工審核。紐約時報舉例，美國匿名戒酒會（Alcoholics Anonymous）的 Zoom 會議近期也遭受駭客入侵，將喝酒的 GIF 圖像傳送給匿名戒酒會會議的參與者；有受訪者稱在最近三週內，受到將近十次的騷擾。此外，也有人在巴黎的美國猶太人委員會會議，播送種族主義信息。此行為逐漸蔓延全球，據《海峽時報》報導，新加坡一堂地理課被入侵，騷擾者將色情圖片畫面向 39 名學生展示，更留言要求一名 13 歲女同學「展示胸部」。

3. 發展

由於 Zoom 的使用量隨著疫情的升溫而逐漸增加，Zoom bombing 開始有組織性內容變本加厲，據紐約時報報導，有上千人的組織在 Instagram、Discord、Reddit、Twitter 和 4Chan 等社交媒體及討論平台發起入侵 Zoom 的活動，製造騷亂、散播種族仇恨言論等，形成因科技發展下的新形態網路暴力。

4. 外界反應

當資安問題爆發時，公司行號例如：Google Space X 和政府機構例如：美國參議員、德國外交部、中華民國政府及各國家教育機構紛紛禁止使用 Zoom。但自從資安問題被一一解決，現在全球只剩台灣教育機構禁止使用 Zoom，曾經告發 Zoom 的 Citizen Lab 也表示除了政府或敏感企業以外，普通用戶無需擔心改版後的 Zoom 會洩漏個資。BBC 中文指出，台灣會持續禁用 Zoom 是對於「逢中必反」的過度反應，將問題聚焦在開發者的中國背景上。台灣推廣新創教學的知名學者-葉炳成教授也指出，政治問題才是台灣禁用 Zoom 的主因。雖然有過非常多資安疑慮，但經過處理後，現在 Zoom 依舊是市佔率最高的視訊會議軟體。

參、研究方法

- 一、文獻分析法：蒐集書籍、網路與官方相關資料，進行歸納、比較與分析。
- 二、問卷調查法：藉由 Google 表單發放問卷，共收回 353 份問卷，依據調查結果進行分析與研究。
- 三、SWOT 分析法：透過相關資料的整理，分析線上視訊軟體在疫情底下蓬勃發展的優勢（Strength）、劣勢（Weakness）、機會（Opportunity）、威脅（Threat）。

肆、研究分析與結果

一、各家線上視訊會議軟體比較分析

表二：各家線上視訊會議軟體比較分析

	Zoom	Google Meet	Microsoft Teams	Cisco Webex
人數	100	250	250	100
時間	無限制	無限制	無限制	無限制
可共享內容	螢幕、軟體、文件、簡報	螢幕、軟體	螢幕、軟體、簡報	螢幕、軟體、文件、影片
遠端控制	有	無	無	有

疫情下的救星：淺析視訊會議軟體 Zoom 的優勢與危機

螢幕註解	有	無	有，付費版	有
白板	有	有	有	有
手機畫面 投影	有	有	有	有
舉手	有	有	有，付費版	有
錄影	有	有	有，付費版	有
分組討論	有	無	分頻道	進階版才有

(表二資料來源：研究者製)

二、問卷分析

(一) 填寫者基本資料

首先是填寫年齡分佈，41~50 歲佔最大比例，為 31.2%。其次是 13~22 歲，佔 28.9%。另外是 31~40 歲，佔 17.6%。50 歲以上則是 15.3%，最後是 23~30 歲，為 7.1%。而本次填寫中，以台灣人 72% 為最大宗，11% 為加拿大人，10% 為馬來西亞人，7% 為美國人。

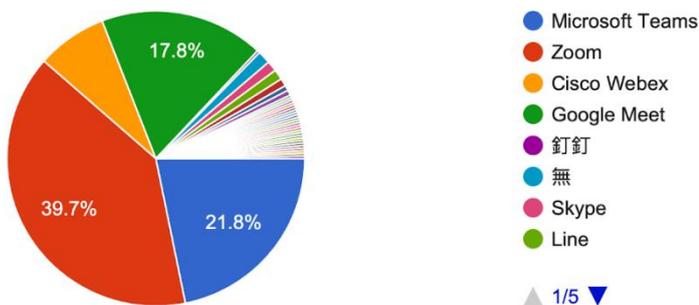
(二) 新冠肺炎對視訊會議軟體的影響

為了瞭解及佐證視訊會議軟體是因新冠肺炎而開始蓬勃發展，我們設計了問題，將受試者分為三塊。分別是「一直在使用視訊會議軟體」佔 32.9%，「新冠肺炎後才開始使用」，佔 58.1%，「從未使用」佔 9.1%。由此可知，有一半以上的人是在疫情爆發後才使用線上會議，和前面的文獻探討相呼應。

(三) 視訊會議軟體的用戶分佈

在 353 位受試者中，有 39.7% 的人使用 Zoom (請見表三)，與 Owl Lab 報告的 37.5% 相仿，是市占率最高的視訊會議軟體。再來是 Microsoft Teams 佔 21.8%，Google Meet 位居第三，為 17.8%，Cisco Webex 則為 7.1%，位居第四。

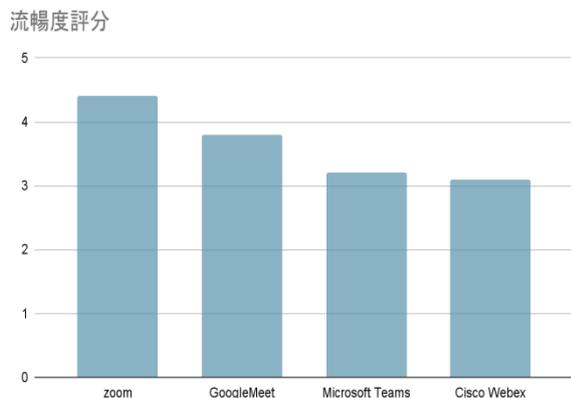
表三：視訊會議軟體的用戶分佈



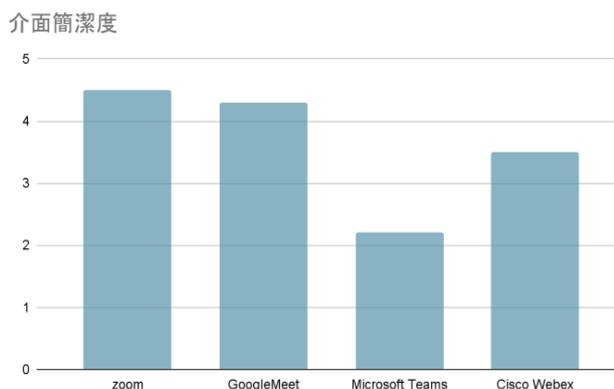
(四) 軟體流暢度和介面簡潔度評分

在事前查詢資料中，我們發現因疫情已持續蔓延長達一年，視訊會議軟體漸趨成熟，各視訊會議軟體功能大同小異（如：舉手、分享簡報、多人參與、更換背景等）。為了了解大眾對於各軟體的滿意度，我們使用流暢度和簡潔度這兩項顯示出各家特色及實力的指標來評分。在受試者對包含音質和畫面是否清晰的流暢度的評分中（請見表四），以 Zoom 的平均 4.4 分為冠，再來是 Google Meet 3.8 分，Microsoft Teams 3.2 分，Cisco Webex 3.1 分，而在介面簡潔度的評比上（請見表五），也是以 Zoom 的 4.5 分為冠，接著是 Google Meet 4.3 分，Cisco Webex 3.5 分，Microsoft Teams 2.2 分。

表四：軟體流暢度



表五：介面簡潔度



（表四、表五資料來源：研究者製）

三、SWOT 分析

從文獻探討、各家資料比較和問卷分析中我們得出以下 SWOT 表格。

表六：SWOT 分析

優勢 (Strength)	劣勢 (Weakness)

疫情下的救星：淺析視訊會議軟體 Zoom 的優勢與危機

1.首開多項視訊會議功能，如分享螢幕、錄製會議等等 2.不需帳號就可加入會議 3.較其他視訊會議軟體快，3G 網路也很流暢 4.友善的使用介面，清晰易懂，軟體會自動適應裝置使用語系，還提供了其他多語版本可供切換。 5.即時解決問題，受到用戶青睞	1.屢次爆出安全性不足 2.會關閉異議人士帳戶 3.個人資料有較大可能性會外洩
機會 (Opportunity)	威脅 (Threat)
1.日用戶數高達 3 億，居於首位	1.會議內容有流出或被入侵的疑慮 2.其他視訊軟體產業競爭

(表六資料來源：研究者製)

伍、研究結論與建議

一、結論

從以上文獻探討和問卷回答中，研究者可得出視訊會議軟體與疫情發展的連動性，和歸納出為何就算 Zoom 經歷許多資安危機，仍可以在眾多軟體中脫穎而出，以下是研究者之結論。

(一) 2020 疫情肆虐 Zoom 迅速發展

2013 年 1 月 Zoom 正式開始推出服務，直到 2013 年 5 月已經有約 100 萬的使用者，而到了 2020 年因為全球受到疫情肆虐，遠距商機逐漸崛起，也帶動 Zoom 迅速發展，不管是免費抑或是付費的每日會議參與者加總起來已從 2019 十二月的 1,000 萬人，至 2020 年四月成長到超越 3 億人，不到半年的時間成長了 30 倍。

(二) 成功因素—產品簡單容易上手使用

而經過筆者的探討後得知，Zoom 軟體大幅成長的原因不僅是疫情帶來的加成，其中很重要的一項是因素是產品簡單容易上手使用，有功能包括畫面可顯示最多至 49 位參與者、可使用虛擬背景、方便老師上課的分組討論、也可雲端錄影讓錯過的使用者重新補上工作或是學習進度等，且問卷得到的回覆中有受試者提到 Zoom 比其他視訊會議軟體更快，所以不論是教育、遠距辦公甚至是家庭聚會大部分的人都使用 Zoom 來完成。

(三) 成功因素—在視訊會議軟體中拔得頭籌

第二項重要的因素則是 Zoom 是第一個開啟多項視訊會議功能，如分享螢幕、錄製會議、書寫白板等的視訊會議軟體，在這方面的市場佔了優勢，進而使它成為全部視訊會議軟體中市占率最高的公司，在視訊會議軟體中拔得頭籌，獲得莫大的成功。

（四）資安疑慮

不過在成功的巔峰期，Zoom 卻迎來了各方質疑，而質疑的部分正是對視訊會議來說最為重要的資安問題，筆者在前文就提出了各種關於 Zoom 資安疑慮的舉例，如：Zoom bombing、將用戶數據擅自發送到其他程式、允許會議主持人跟踪與會者但謊稱已進行端到端加密等的問題使人心惶惶。

（五）各界對策

由於這些資安問題的浮現，各界也祭出了對策，像是某些政府機構完全禁止使用 Zoom 來進行線上會議、公司行號禁止使用 Zoom 來談公事、教育機構因 Zoom bombing 而停止使用 Zoom。

（六）Zoom 的對策

不過除了下文會提到的普遍解決辦法外，Zoom 也在 2020 年 4 月開始，推出 90 天資安強化計畫，將資源投入至增強產品安全和隱私性的方面，並且推出 Zoom 5.0 的更新，其中增加了許多安全性層面的功能，已用於滿足全球使用者的要求，也已於 2020 年 7 月取得進展。未來 Zoom 也會持續努力精進產品的安全性與保護隱私的功能，保證將打造一個容易安裝且具大規模的端到端加密通訊平台。

二、建議

現今視訊會議軟體已成為不可缺少的日常工具之一，除了去關心可能會產生的安全漏洞，我們應當從自己做起，執行基本的防護措施，以下是對於一般民眾使用 Zoom 的建議事項。

（一）購置產品解決問題

如防火牆、IDS、內容安全、弱點管理等安全裝置就是有效的防禦設備，但是也只能解決部分問題，再加上管理者在設定上如果有失誤或是時常更改設定的話，即會不夠安全，所以最好的辦法依然是制定安全政策，規定誰可以更改設定、如何去更改設定等。

（二）公司只能盡量控制資安風險

只要系統需要人力來操作的話就一定會有問題產生，也就代表不可能完全的安全，若企業在建立資訊安全管理制度上能做到準確的管理人員、控制流程與增加技術能力，就可將資安風險控制在合理範圍內。

(三) 利用傳播媒體宣導資安觀念

資訊安全最大的問題在於教育，大部分民眾都知道電腦中毒要如何解決但其實這只是其中的一小部分，在其他部分可能就比较缺少警覺性，例如電腦運作速度變緩或是出現某些異常行為，很可能就是遭到駭客攻擊。若媒體能增加報導駭客攻擊網站或政府網站被駭等消息，企業就會開始注意自己的網站狀況是否安全。媒體報導的越多，民眾、企業，政府就會越有警覺，進而開始思考怎麼做防護。

陸、參考文獻

- 林宏文（2020年11月16日）。不要再強調台灣防疫很成功了！遠距視訊、醫療、保險、運動崛起 我們有抓到這些新商機嗎？。 <https://reurl.cc/NrR21Q>
- BBC 中文新聞（2020年9月1日）。Zoom 營收暴增 受益於疫情的會議軟件如何掙錢。 <https://reurl.cc/zeNQ8a>
- 陳嘉建（2020年8月7日）。視訊會議三優勢。 <https://reurl.cc/GmEady>
- 鍾張涵（2020年4月8日）。Zoom 備受質疑 在家工作如何顧資安？台積電有祕技.....。 <https://reurl.cc/AkO9R3>
- CT、Jennifer（2015年09月21日）。視訊通話是近代科技？早在20世紀初就有了。 <https://reurl.cc/YOXDvn>
- BXB 卡訊電子（2020年8月24日）。商務視訊會議該用誰？4款線上視訊會議軟體比較、硬體搭配推薦。 <https://reurl.cc/VE128b>
- 林嘉怡（2020年4月11日）。視訊會議軟體哪種最好用？Zoom、WebEx 等9種超完整比較測試報告。 <https://reurl.cc/AkO94p>
- 陳映璇（2020年10月19日）。疫情下當紅炸子雞！Zoom 亞太業務成長573%，走出資安泥淖後，下一步要做到比擬真人會議。 <https://reurl.cc/qgNpvD>
- iThome（2004年9月7日）。行家告訴你資安問題如何解。 <https://reurl.cc/O046YR>
- 羅正漢（2021）。生活資安五四三！：從生活周遭看風險與資訊安全。博碩文化
- Brendan Ittelson（2021年3月25日）。敏捷性和創新的故事：《COVID-19 疫情期間視訊通訊的影響力》報告調查結果。 <https://reurl.cc/R0X8ye>
- TechCola（2020年10月2日）。「Zoom」為何創業者必備？Zoom 團隊會議，超詳盡教學！ <https://reurl.cc/mL3X5G>
- 劉季清（2020年8月3日）。遠距視訊需求暴增 Zoom 使用者半年翻30倍。 <https://reurl.cc/MANDnv>
- Jill Duffy（2020年4月16日）。How to Prevent Zoom-Bombing。 <https://reurl.cc/KAQVDn>