

財團法人電信技術中心

2019 年 PyCon Korea 出國報告

服務機關：財團法人電信技術中心資通安全組

出國人員：陳坤裕工程師、宋駿瑋副工程師

派赴國家：韓國

出國期間：108 年 8 月 14 日至 8 月 19 日

報告日期：2019 年 9 月 18 日

出國報告摘要

PyCon Korea 2019 於 2019 年 8 月 14 日至 2019 年 8 月 19 日於韓國首爾舉辦。此行主要目的為發表 Python 內建模組 zipfile 安全漏洞，並於簡報中分享取得 CVE 編號、協助 PSF (Python Software Foundation) 緩解、修補漏洞及充實 Python 官方文件之經驗。期望藉由技術分享展示本中心資安研發能量。

在參與 PyCon Korea 過程中，除了發表我們所研究的主題以外，我們也積極和與會人士如韓國講者、日本講者、PyCon Korea、PyCon Japan 工作人員交流各式與 Python 相關之經驗（如：Python 語言使用、Python 社群經營、協同合作經驗、不同國家 PyCon 差異性等）。

資訊科技產業是人才驅動的產業，一定要與外部產生關聯，不能閉門造車，如何與產業內頂尖人物交流並建立合作關係，是一項挑戰。為此，我們透過積極參與國際間重要研討會議，讓世界看見本中心優異研究能量，並建立強連結。藉此增進本中心未來發展各種可能性。另外，我們也將此經驗帶回給資通安全組成員，提升整體資訊安全知識能量。

目次

壹、會議參加目的	5
貳、會議時間、議程與地點.....	5
參、投稿內容摘要	10
肆、與會過程.....	12
伍、心得及建議.....	17

圖目錄

圖 1 Sprint 會場	12
圖 2 由左至右分別為陳坤裕、Carol Willing、宋駿瑋	13
圖 3 TTC 工程師陳坤裕	14
圖 4 TTC 工程師宋駿瑋	14
圖 5 Masataka Arai	15
圖 6 PSF Banner 陳坤裕	17
圖 7 PSF Banner 宋駿瑋	18

表目錄

表格 1 PyCon Korea 議程表	5
----------------------------	---

壹、會議參加目的

PyCon 最初於 2003 成立於北美，現在世界各地皆有以 PyCon 精神而成立的會議。是一年一度由 Python 愛好者舉辦、討論並提倡使用 Python 程式語言的會議，聚焦在 Python 技術與其多樣的可能應用的交流。

只要與 Python 程式語言有關的各式各樣的主題皆有機會投稿上 PyCon 這樣的研討會，並且各國對於審稿的主題接受度也不盡相同，因此我們希望除了投稿台灣 PyCon 以外，也積極嘗試投稿至國外各個 PyCon，讓世界肯定我們的成果。

貳、會議時間、議程與地點

本次會議時間、議程與地點如下所示。

- 舉辦日期：108 年 8 月 17 日至 108 年 8 月 18 日
- 舉辦地點：Coex Grand Ballroom, Seoul
- 會議議程：

表格 1 PyCon Korea 議程表

2019 年 8 月 14 日

時間	主題
09:30 ~ 09:40	Opening Pythonistas
09:40 ~ 10:20	Keynote 演講題目: 파이썬과 커뮤니티와 한국어 오픈데이터 演講者: Lucy Park
10:30 ~ 11:10	Keynote 演講題目: How did I get here? 演講者: Pradyun Gedam
11:20 ~ 12:00	Keynote 演講題目: 파이썬과 함께라면 못 할 것은 없다” 라는 마음가짐만 있다면 못 할 것은 없다 演講者: Byunghyun Ban
12:10 ~ 12:50	Keynote 演講題目: The State of Python 演講者: Carol Naslund Willing

14:10 ~ 14:35	演講題目: Detecting failure of air handling units at air circulation room at subway stations 演講者: Minjung Gim
	演講題目: 정적 타입 검사로 더 나은 Python 코드 작성하기 演講者: Changhui Lee
	演講題目: 이쁜의 변수 (강한 타입 Immutable vs Mutable, Class vs Instance) 演講者: Chris Cho
	演講題目: Optimization algorithm implementation in Python 演講者: Jiwon Cha
	演講題目: Code review tips for Pythonistas 演講者: Masataka Arai
15:05 ~ 15:30	演講題目: 하나의 Django 코드로 여러 사이트 운영하기 演講者: Jonghyun Park
	演講題目: Nowadays Pythonischool changing the future of the education 演講者: greatsong
	演講題目: Sponsor session (PRND) 演講者: Jihoon Lee
	演講題目: Efficient diet strategy for fat and slow Pandas 演講者: Sungwoo Oh
	演講題目: Click Click Boom! Bombs Over Our Minds 演講者: JunWei Song, KunYu Chen
15:45 ~ 16:25	演講題目: Network operation management in enterprise scale 演講者: Deoknyong Ko
	演講題目: 시간 복잡도로 살펴보는 파이썬 내장 자료형의 효율적인 활용 演講者: Daesung Kang
	演講題目: from banksalad import python 演講者: Sunghyun Hwang
	演講題目: 이쁜 3.7 어찌 그렇게 빨리졌나 演講者: JungWinter
	演講題目: Python 에서 DSL 제작하기 演講者: Las
16:40 ~ 17:20	演講題目: Real world Graphene: lessons learned from building a GraphQL API on top of a large Django project 演講者: Marcin Gębala
	演講題目: How to decrease 92% of your test runtime 演講者: Youngmin Koo

	演講題目: 신라닝 및 데이터 과학 연구자를 위한 python 기반 컨테이너 분산처리 플랫폼 설계 및 개발 演講者: Jeongkyu Shin
	演講題目: Only in Python - Image recognition speed run 演講者: Choi JeongHyeon
	演講題目: Build a Python Internet of Things (IoT) Image Classification solution and integrate with Azure Serverless Functions 演講者: Dave Glover
17:20 ~ 18:20	Lightning Talk Day 1 Pythonistas
2019 年 8 月 18 日	
10:00 ~ 10:40	演講題目: Extreme usage of server using Python: the bottom of Async I/O 演講者: SeomGi, Han
	演講題目: How to make a smart general conversation AI using 10 Billion chatting data 演講者: Junseong Kim
	演講題目: 추천시스템 이제는 돈이 되어야 한다 演講者: choi kyumin
	演講題目: Real-world asyncio 演講者: Joongi Kim
	演講題目: How to use Database Read Replicas 100% using Django DB Router and troubleshoot 演講者: Jongwon Han
10:55 ~ 11:20	演講題目: 잘못 직장인의 파이썬 아래한글 도전기 演講者: Myeongjin Shin
	演講題目: Let's become a little Mozart (Feat. Magenta) 演講者: Junu Kim
	演講題目: HYPERCONNECT Azar WebView Logging 演講者: Jun Young Lee
	演講題目: How to become a Pythonista from a MATLAB user 演講者: Cho Intae
	演講題目: Challenges on Korean spacing rule 演講者: Taekyoon Choi
11:55 ~ 12:35	演講題目: 파이썬 웹서버 REST API 문서 쉽고 빠르게 작성하기 演講者: Yongseon Lee

	演講題目: Characteristics of DB for multitasking environment and Django to handle them 演講者: Seokhwan Moon
	演講題目: 집에서 만든 머신러닝 기반 자동번역기 (NO 답러닝) 演講者: Hongjoo LEE
	演講題目: How to make twitter and discord event alarm bot for Splatoon2 演講者: Hyunsu Mun
	演講題目: Advanced Python testing techniques 演講者: Jaeman An
13:55 ~ 14:35	演講題目: Adapting from Spark to Dask: what to expect 演講者: Vaibhav Srivastav
	演講題目: Django Query Optimization for realtime medical artificial intelligence data preprocessing 演講者: Soyoung Yoon
	演講題目: Are the comments on online news real voice of people? - Part 2 演講者: Junbum Lee
	演講題目: Techniques and principles on py2exe implementation 演講者: Jeonghun Lee
	演講題目: gRPC 와 python 을 활용한 Microservice 개발기 演講者: Jihyung Song
14:55 ~ 15:35	演講題目: Quantum Physics in Python: 파이썬으로 양자컴퓨팅 즐기기 演講者: Samuel Choi
	演講題目: Debugging law 演講者: Jaeyoon Kim
	演講題目: 고등학생이 직접 개발한 파이썬 프로젝트 사례
	演講題目: Chemical experiment in Python - Boyle-Charles' law 演講者: 승우
	演講題目: Pickle & Custom Binary Serializer 演講者: Young Seok Kim
15:55 ~ 16:20	演講題目: Takeaways from my 5-year volunteering journey in the Python community (and why you should become one, too!) 演講者: Alysson Alvaran
	演講題目: Python Daemonize: Let's make a demon using Python

	演講者: Lee, Suho
	演講題目: Real world MetaClass
	演講者: Seonghyeon Kim
15:55 ~ 16:35	演講題目: The Right Frameworks for the Right Time 演講者: Sean Ahn
16:40 ~ 18:00	Lightning Talk Day 2 Pythonistas

參、投稿內容摘要

目前組內正研發 APK 惡意程式自動化分析引擎，現階段以 Android 平台為主，目標為加入 VirusTotal，將惡意程式掃描平台推上國際舞台。於是我們寄信詢問了加入 VirusTotal 的標準，而 VirusTotal 也告訴我們了加入所需的要求項目，於是我們開始實作我們的分析引擎。

在一系列的標準中，我們對於其中一項規則，需要解決壓縮炸彈 (zip bomb)，無從解決。於是我們開始做了一系列研究，試著靠自己來解決這項問題。在一段時間的研究後，我們瞭解到，所謂的壓縮炸彈代表的是，透過高壓縮比例的方式壓縮檔案，使得一個非常巨大的檔案能夠被壓縮演算法壓縮完成後，能夠變成一個非常小的檔案。會有如此的技術出現，通常是惡意程式用來應對防毒軟體的掃描，因為防毒軟體要掃描病毒勢必要解開電腦中的壓縮檔案，因此如果所要解開的檔案非常巨大，則會讓解壓縮時間過久，甚至可能讓防毒軟體停止運作。

之後我們將所研究到的緩解方法整理，透過 Python 實作到我們的分析程式，在我們完成以後，確實可以解決壓縮炸彈的問題。但我們突然靈光一閃，會不會其實 Python PyPi 已經有類似的套件完成了我們所做的事情，於是我們開始搜尋 PyPi 中是否已有緩解 zip bomb 問題的套件。

在一番搜尋無果後，我們打算嘗試自製 PyPi 套件，做到一半發想，等等！。或許官方套件 zipfile 本身就有這個防禦機制了？，於是我們打算開始先去好好了解 zipfile 這個 Python 內建的模組。我們將 zipfile library 的原始碼仔細閱讀，梳理整個 zipfile 原始碼的思路，把精力聚焦在解壓縮這件事情上，最後得到的結論是，zipfile 確實沒有這個機制！

在得知這件事後，我們猜測或許可以將這個問題回報給 mitre.org，試圖申請 CVE 漏洞編號。一週後，我們得到了官方的回覆，他們指派這個問題為漏洞編號，CVE-2019-9674，並告知我們需要公開的連結，這個漏洞編號才能被對外公開。

緊接著，我們嘗試聯絡 Python 的安全維護團隊，打算將這個問題告知他們，並提供我們所撰寫的解決方案。在一來一往的對話中，與 Python Core Developers 建立的共識是，驗證壓縮檔案是使用者的責任，並不是 zipfile 的責任，但是我們可以將這個問題以及解壓縮可能潛在會有的問題一併整理至文件檔案中，讓使用者可以自行抉擇該如何處理。

自三月份申請並獲得 CVE 漏洞編號後，在今年四月中時，我們開始著手準備，將這一段經驗和過程，投稿至 Pycon Korea，並順利被錄取。在此次投稿主題中，我們是以開發惡意軟體掃描引擎作為投稿主題起始的方向，之後找到 Python 的內建模組漏洞，接著是我們如何去開始接觸 Python Community，與 Python Core Developers 互動，協助他們將漏洞修補。在這過程中我們也經歷不少失敗，原本以為會無疾而終，但我們仍秉持著永不放棄的精神，努力找出與 Python Core Developers 之間的共識，最後終於被他們所認可，接受我們的修補程式。

肆、與會過程

會前 Sprint

在研討會開始前，我們參與了 Python Korea Sprint，Sprint 是在一個團隊環境中對選擇的開源項目進行密集開發，並改進現有的程式或是文件檔案。我們選擇的開源項目是 RustPython。在與會的期間，帶領我們的講者是以韓文為主，所以我們不太理解整個過程，但我們還是試著自己摸索，並理解到什麼是 RustPython，以及 RustPython 的用途。並在過程中與坐在我們旁邊的 Carol Willing (CPython 首位女性核心開發人員) 進行討論，使得我們對 Python 的社群和開放原始碼的貢獻有更多地了解。



圖 1 Sprint 會場

與會過程

研討會開始後，我們參與了開場的 Keynote 議程，正是由 Carol Willing 進行演講，我們瞭解到了整個 CPython 貢獻的過程、守則，以及很多的經驗分享，以及 Carol Willing 在 Jupyter 上所做的貢獻。Carol 提及，一個好的程式碼，需要大量的與人溝通，在技術上並不會很困難，困難是在於每一個人都可以有意見，但是需要保持禮貌地與 Core Developers 討論，這也是 Python 社群能夠如此壯大的原因，每一個人都可以對 Python 做出貢獻，同時我們也要保持著互相尊敬、願意傾聽、分享、信任的態度，且擁有大膽的視野。在 Carol 的演講結束後，我們向 Carol Willing 討論我們的演講主題，以及有關 CPython 的貢獻和安全議題，並邀請她參與我們的演講，也在最後贈送她 TTC 的小禮物。



圖 2 由左至右分別為工程師陳坤裕、Carol Willing、副工程師宋駿瑋

在我們演講時，Carol Willing 也真的來參與我們的演講，並在我們演講結束後，和我們分享一些經驗以及該如何更好的貢獻 Python，她也期許我們可以為 Python 的安全性能有更多貢獻。



圖 3 TTC 工程師陳坤裕



圖 4 TTC 工程師宋駿瑋

參與議程 - Code review tips for Pythonistas, Masataka Arai

我們參與了由日本講者所分享的議程，與我們分享在開發軟體時，常見的 Code Review 方式，同時此位講者也是 PyCon JP 的工作人員，講者提到 Code Review 是一件非常重要的事情，但通常我們在開發軟體時常常忽略其重要性。第一，程式碼的風格可以透過一些現有工具統一風格如 Black、autopep8 等等來保證大家的程式碼具有同等的風格，提升程式碼可讀性。第二，在每一次的程式碼提交，盡可能保持單一功能的修改，以及程式碼變動幅度要小，如此一來審閱程式碼的人才可以更快進入狀況，給予程式碼提交者意見。第三，作為審閱者，在給予意見或是詢問問題時，確保自身的說詞能夠讓對方清楚明白，且讓對方精準地知道自己下一步該做什麼。

圖 5 Masataka Arai



講者晚宴

第一天研討會傍晚，大會舉辦講者晚宴。與會者皆是 PyCon Korea 的重要人仕，因此我們把握機會，積極與各講者進行交流。

在這之中，我們也和 PyCon JP 和 PyCon Korea 的工作人員交流，透過交流，我們談論各種 Python 技術相關議題，例如：Python 語言使用、Python 社群經營、協同合作經驗、不同國家 PyCon 差異性等。從中吸取優點，並反思自我改進處。

此外，透過此交流，我們也得知前 PSF director，Younggun Kim 與 PyCon Japan Staff，Masataka Arai 今年九月也會來台參與 PyCon Taiwan。我們彼此相約屆時再見。透過晚宴交流，彼此建立連結，並交換了社交網路帳號。透過社交網路，彼此討論各種技術議題。也期望未來能替本中心建立各種合作機會。

伍、心得及建議

本次參與完 PyCon Korea 2019 後，除了對於 Python 以及漏洞挖掘、開放原始碼相關技術獲益良多外，我們反思目前工作內容與資安組業務，有四點心得與建議陳述如下：

一、鼓勵同仁投稿至國際重要會議

透過投稿至國際重要會議，優點如下：1. 研究成果能接受國際專家檢驗，避免閉門造車。2. 研究成果能透過國際舞台發表，提升本中心對外能見度，增加對外影響力。

二、鼓勵同仁做基礎研究

此次研發經驗，我們大部份精力都花在解決最基礎的問題上。令我們感到吃驚的是很多基礎技術，其實尚不少問題待解決。因此，若能將心力花在基礎上，一方面可扎實自身基本功，另一方面也有機會解決基本、但重要的問題。一魚兩吃，樂趣無窮。

三、鼓勵同仁挑戰艱難議題

挑戰艱難議題，優點如下：1. 因為是艱難議題，所以多數人畏懼。因此，我們競爭者少。2. 因為是艱難議題，因此一旦被我們攻破，則成果之價值必定不低。3. 我們設定目標是前往火星，但其實我們飛到月球時，已經超乎我們想像了。

四、積極參與開源社群

透過參與開源社群，可讓自己直接與世界一流技術者交流，並讓自己的各種能力接受檢驗。過程必定痛苦，但收穫肯定扎實。舉凡我們日常所使用的作業系統、程式開發、應用軟體，都有著開源社群的身影。參與開源社群需要非常多的熱情，才能夠不斷貢獻著開源社群，而這也是一個很好的指標，未來招聘新人時，能夠透過是否有參與大型開源社群，來篩選出具熱情之人。

此行坤裕與駿瑋皆深受啟發，對自主研發資安技術之決心更加堅定。雖人物力等研發資源匱乏，但這正是大展身手的好時機。我們定戮力繼續突破各種困難，為中心貢獻己力。

圖 6 PSF Banner 陳坤裕



圖 7 PSF Banner 宋駿瑋

