

檔 號：

保存年限：

財團法人國家實驗研究院 函

機關地址：10636台北市大安區和平東路二段106號3樓

聯絡人：林懿燁

電話：06-5050940#665

傳真：

電子信箱：evalin@narlabs.org.tw

受文者：國立聯合大學

發文日期：中華民國109年11月26日

發文字號：國研授網資字第1090308189號

速別：普通件

密等及解密條件或保密期限：

附件：2020IoTSandBox研討會(attch1 73196449b06cb802fbb4ca849ef0502a_1090308189-0-0.pdf)

主旨：謹訂於109年12月11日(星期五)舉辦「IoT Sandbox 2020 智慧物聯網資安研討會」，敬請轉知及鼓勵相關人員參與，請查照。

說明：

- 一、隨著新興資訊科技的迅速發展，近年來全球智慧工廠遭受網路攻擊事件持續傳出，新興物聯網裝置應用平台與服務，因欠缺資安架構的設計，而衍生新的資安威脅。因應資安即國安的政策，沙崙智慧綠能科學城與產學研資源串聯，建立跨域應用「智慧資安」生態系，提升整體資安防護能量。本次研討期盼促進國內資安領域技術及資訊交流，並結合舉辦「IoT Sandbox 2020 智慧物聯網資安競賽-決賽」，歡迎親蒞觀摩了解資安技術的實際應用。
- 二、研討會地點：台南大飯店 2樓(台南市中西區成功路1號)
- 三、活動資訊請參閱 <https://most.nchc.org.tw/>

報名網址 [https://nchc-cdx.kktix.cc/
events/iotsandbox2020-conf](https://nchc-cdx.kktix.cc/events/iotsandbox2020-conf)

裝

訂

線



正本：教育部資訊及科技教育司、公私立大專校院

副本：14:39:52

院長 吳○○授權單位主管決行

裝

訂

線



2020 IOT SANDBOX

智慧物聯網資安研討會

隨著新興資訊科技的迅速發展，近年來全球智慧工廠遭受網路攻擊事件持續傳出，從雲端應用、大數據分析、物聯網的發展，到現在數位化與行動化的複合情境。對典型的資通訊技術早已建立起多層次的資安防禦機制，但工業4.0世代後所發展出來的智慧應用，以及新興的物聯網裝置應用平台與服務，卻因欠缺資安架構的設計，而衍生了新的資安威脅。

企業面臨新型態資安攻擊往往都無法有效的偵測及防禦，因而導致許多資安問題產生，嚴重造成企業營運中斷及財務上損失。因應資安即國安的政策，沙崙智慧綠能科學城與產學研資源串聯，建立跨域應用「智慧資安」生態系，透過沙崙園區導入強化資安，完備園區內的資安防護，進而擴散到南部相關產業，提升整體資安防護能量。

KKTIX線上報名 →

<https://nche-cdx.kktix.cc/events/iotsandbox2020-conf>

2020
12/11
FRIDAY

台南大飯店 2樓會議廳

(台南市中西區成功路1號)

本次研討會結合IoT Sandbox 2020 智慧物聯網資安競賽決賽，將安排實戰競賽展覽，歡迎蒞臨觀摩充滿挑戰的資安競賽活動。

指導單位
ADVISER



教育部

主辦單位
ORGANIZER



國家高速網路與計算中心
National Center for High-performance Computing

共同主辦
ORGANIZER



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER



中華資安國際
CHT Security

2020
IOT SANDBOX



Official Site



Register Now



CONTACT US

[cdx_support\[at\]nariabs.org.tw](mailto:cdx_support[at]nariabs.org.tw)

73196449b06cb802fbb4ca849ef0502a_1090308169-0-0.pdf