

類 科：資訊處理

科 目：資訊管理與資通安全概要

考試時間：1 小時 30 分

座號：\_\_\_\_\_

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。。

一、機器學習（Machine Learning）是人工智慧（Artificial Intelligence）的一個分支；深度學習（Deep Learning）則是機器學習的一個分支。

(一)請說明深度學習與機器學習的差異性。(10 分)

(二)請說明深度學習模型之基本概念。(10 分)

(三)深度學習的辨識效能仰賴大量且有效的訓練資料集。請說明為何深度學習的辨識效能較佳。(10 分)

二、因應巨量資料的來臨，資料不僅在數量上變多，而且日益複雜，資料倉儲系統面臨許多挑戰與改變。

(一)請說明資料倉儲系統的主要功能。(10 分)

(二)面對巨量資料收集與分析，請說明巨量資料處理所需之主要技術與硬體架構。(10 分)

三、勒索軟體（Ransomware）是惡意軟體的一種，卻造成組織非常大的威脅。

(一)請說明勒索軟體之惡意行為，並舉例說明遭受勒索軟體攻擊之原因。(10 分)

(二)請說明勒索軟體運用的密碼學技術。(10 分)

(三)請說明如何預防此類攻擊。(10 分)

四、安全資訊與事件管理（Security Information and Event Management，簡稱 SIEM）乃結合安全資訊管理（Security Information Management，簡稱 SIM）與資安事件管理（Security Event Management，SEM）之整合系統，提供管理者整合組織企業之資訊安全管理所需資訊與管理功能。

(一)請說明安全資訊與事件管理系統（SIEM）之基本目標與功能。(10 分)

(二)請說明組織採用 SIEM 系統時，應考量那些成本？(10 分)