

中華開發金融控股有限公司

(113 年度)

版本號：v3.0

滲透測試

複測彙總報告

Penetration Testing Report



機密等級： ☐ 公開 ☐ 一般 ☐ 敏感 ☒ 機密

第二章 執行計畫

第一節 目的

滲透測試係利用系統化工具與流程，結合資訊安全專家（以下簡稱本團隊）之專業知識、資訊安全技術及駭客工具資料庫，對於雙方所約定之目標系統進行安全強度測試及模擬駭客入侵，並提供客戶專屬測試報告及系統補強建議。

本服務將由本團隊專業的資通安全專家，配合貴單位需求，從外部環境以攻擊者的角度對受測目標系統進行安全非破壞性的滲透測試，找出駭客可能之入侵管道，並利用各種滲透技術、攻擊手法、弱點攻擊程式、網站漏洞等技巧，來對受測目標進行滲透測試，並將於測試完成後提供專業之評估報告、改善建議及專業諮詢，協助貴單位做好各種資通安全防護措施。

第二節 作業規範

- (1) 貴公司同意、授權且委託本團隊因執行本服務所需，須對貴公司受測目標進行滲透測試安全檢測服務。
- (2) 於本服務中所獲得與蒐集之資訊，僅用來作為本服務執行之發現事項佐證資訊使用，不做其它用途之使用，且採取適當及必要之保護措施，不得在未經書面授權下洩露予第三者，或供非職務目的加以使用、拷貝、隱藏，並得經貴公司同意及簽訂保密切結書辦理。
- (3) 其它保密事項之規範，遵循雙方所簽訂之專案合約規範及保密合約。

凱基人壽保險股份有限公司

113 年滲透測試報告

(可由外部 Internet 直接連線之網路設備、伺服器及物聯網等設備安全檢測)

安永諮詢服務股份有限公司

2024 年 12 月 16 日



聲 明

本文件著作權屬安永諮詢服務股份有限公司所有，僅供凱基人壽保險股份有限公司（以下簡稱 貴公司）依約定的方式使用，未經本公司許可不得引用或翻印。除 貴公司以外之第三人不得以本報告所載之建議、評論分析或其他資訊作為任何決定之依據。除 貴公司以外之第三人亦不得曾閱覽本報告為由，向本事務所主張任何權利。

壹、簡介

凱基人壽保險股份有限公司（以下簡稱 貴公司）為因應中華民國人壽保險商業同業公會實施之「保險業辦理資訊安全防護自律規範」（113 年 7 月 18 日金管保綜字第 1130138369 號函，以下簡稱「保險業電腦系統資訊安全評估作業原則」），委託安永諮詢服務股份有限公司（以下簡稱安永團隊）以 貴公司所提供之對外網站與網路設備，進行外部網站安全性檢測，以模擬外部駭客之網路滲透技巧及入侵技術，找出潛在應用程式與作業系統之弱點，另針對 貴公司所提供之檢測清單進行弱點掃描或黑箱測試及網站目錄及網頁之存取權限等情況，以針對 貴公司的外部網站進行完整的檢測，進而發現可能潛在之資安威脅與弱點，藉以實施技術面與管理面相關控制措施，改善並提升網路與資訊系統安全防護能力。

貳、專案限制

本「可由外部 Internet 直接連線之網路設備、伺服器及物聯網等設備安全檢測報告」（以下簡稱「本報告」）因考量系統效能與可用性的影響，不採用暴力破解、字典檔破解與分散式阻斷攻擊等攻擊行為。安永團隊於所約定時間內盡可能找出所揭露之弱點，任何評估檢視的結果，僅表示於某一個時間點是有效的，未來可能因新型態攻擊手法與零時差攻擊而結果有所差異。因此，本報告僅針對檢測期間所檢出之結果提出改善建議，不代表現有安全性未來將持續有效。

參、執行摘要

一、評估目的

（一）符合中華民國人壽保險商業同業公會所訂之「保險業辦理資訊安全防護自律規範」相關要求。

（二）持續提昇資訊安全管理水準及防護能量。

凱基商業銀行股份有限公司
113 年度電腦系統資訊安全評估服務案
網路設備、伺服器及物聯網設備且連線至
Internet 者複測報告-01 滲透測試_113

文件編號：H07S11205014_4_113
V1.1

113 年 11 月 12 日

安基資訊股份有限公司

壹、關於本報告

一、報告說明

滲透測試 (Penetration Test) 是以駭客思維與手法進行的入侵演練測試。本報告為安碁資訊股份有限公司 (以下簡稱本公司) 承接凱基商業銀行股份有限公司 (以下簡稱貴公司) 「113 年度電腦系統資訊安全評估服務案」 (以下簡稱本案), 依貴我雙方約定之作業範圍, 在取得最少資訊的情況下, 嘗試突破網路或系統的防禦、尋找應用軟體及網路服務等系統設備之安全弱點與漏洞, 並設法取得控制權限或未授權之機敏資訊, 以評估企業之整體安全性後, 就本次作業所見之項目進行說明陳述, 提供相關優化、精進之資安防護機制之建議, 供貴公司做為後續防護規劃之依循參考。

二、盡責聲明

滲透測試為在一定的時間內, 使用不同手法盡可能確認測試標的的安全性, 並非以找出全部的系統漏洞為目標。當攻擊者的攻擊時程較長、或是測試標的更新、或是有了全新的攻擊手法出現, 都會使得系統或網站的安全性降低。唯有透過定期進行滲透測試, 才能確保系統與網站的安全性足夠抵禦外來的惡意攻擊。

本報告所使用之分析與檢測手法, 為當前資訊安全產業所通用之技術與工具, 本公司謹盡合理可能之最大努力, 就所見所聞如實提出本報告, 容或有不足之處, 仍請考量當前科技所能達成之極限, 予以諒解。

凱基證券股份有限公司

113 年度滲透測試報告(正式區)

民國 113 年 12 月



資誠

機密文件限閱

一、檢測依據

依據資誠智能風險管理諮詢有限公司（以下簡稱為“資誠”，“本公司”）與凱基證券股份有限公司（以下簡稱為“凱基證券”，“貴公司”）於 113 年度資通安全健診整合服務案製作完成。檢測範圍為提供網際網路服務與核心系統主機。