

資料隔離架構

- 租戶隔離**：每間企業與每個協作區均為獨立授權邊界，僅經授權加入的成員可存取對應資料，無法跨企業或跨協作區查看
- 企業資產邊界明確**：企業管理後台僅能存取掛於企業名下的協作區；員工「個人」建立的協作區與個人名片庫，企業端完全不可見
- 個人資料雙軌**：員工的個人名片庫存於其手機本機與個人 iCloud，不經 CardNest 後端；上傳協作區採「複製快照」單向發佈，界線清楚

帳號與角色控管

- 認證委由 Apple / Google**：以 Sign in with Apple 或 Google 帳號登入，CardNest 不儲存任何密碼
- 角色權限**：協作區分 Owner / Admin / Member 三種角色，另有企業管理員層級，各角色可執行的操作明確區分
- 伺服器端強制驗證**：所有敏感操作（成員異動、角色變更、資料刪除等）均於伺服器端逐次驗證權限，並非僅介面上的限制；成員一經移除，存取權立即失效
- 預設拒絕**：資料庫存取規則採預設全部拒絕、逐項明確開放，並以自動化規則行為測試於每次變更前後驗證

辨識模式可依敏感度選擇

- 智慧辨識**：先於手機端辨識文字，再將辨識出的文字加密傳送至雲端 AI 整理欄位；手機端無法辨識時，才將名片影像加密傳送至雲端辨識服務
- 裝置端辨識**：名片 OCR 與欄位辨識全程於手機端完成，內容不傳送至外部 AI 服務，適合對資料外流敏感的企業
- 兩種模式可由使用者於 App 內自行切換

傳輸與儲存

- 傳輸加密**：所有連線均採 TLS 加密
- 基礎設施**：協作資料存於 Google Cloud（Firebase）台灣機房（asia-east1），由 Google 資料中心提供實體與平台層安全
- 憑證防護**：企業加入碼與授權碼均於伺服器端驗證，具暴力嘗試頻率限制；系統日誌與稽核紀錄一律不記錄碼本體

存取紀錄與供應商存取控管

企業看得到的紀錄

- 異動紀錄**：成員加入與移除、角色變更、席位與授權調整、加入碼重產、協作區建立等企業層級異動，均由伺服器端自動記錄
- 含供應商操作**：CardNest 維運端對企業帳戶的操作（如續約、席位調整）同樣寫入此紀錄，企業管理員可於後台直接查閱
- 唯讀且可匯出**：紀錄僅伺服器端可寫入，任何使用者端（含管理員）均無法修改或刪除，並支援 CSV 匯出供內部稽核留存

CardNest 端的存取控管

- 日常維運走專用系統**：所有日常維運操作均透過內部維運後台（Ops Console）執行，須具備專屬維運權限，所有操作（含讀取）全程留存稽核軌跡
- 維運後台不接觸名片內容**：Ops Console 僅能管理企業帳戶層資訊（席位、方案、成員名冊、協作區名稱與數量），在系統設計上即不具備讀取名片內容、影像與備註的功能
- 緊急存取分離**：緊急系統維運情境的存取屬例外程序（break-glass），與日常維運路徑分離管理

進一步資安需求

- 若企業內部有 IT / 資安相關規範、供應商資安檢核表，或對本文件所述機制有特定合規要求，歡迎提供，我們可依 CardNest 實際架構逐項確認與說明。

協作區成員權限（Owner / Admin / Member）

協作區內操作	Owner 擁有者	Admin 管理員	Member 一般成員
查看 / 新增名片	✓	✓	✓
編輯 / 刪除自己上傳的名片	✓	✓	✓
編輯 / 刪除其他成員上傳的名片	✓	✓	—
新增自己的團隊備註	✓	✓	✓
刪除其他成員的團隊備註	✓	✓	—
修改協作區名稱	✓	✓	—
重新產生邀請碼	✓	✓	—
移除一般成員	✓	✓	—
移除管理員	✓	—	—
指定 / 取消管理員	✓	—	—
解散協作區	✓	—	—

企業名下協作區的企業管理員（見下表）另享有比照 Owner 的資料存取與成員 / 管理員異動權限，但不可解散協作區、不可移除或取代 Owner。所有角色變更與異動均由伺服器端逐次驗證，非僅介面限制。

企業管理後台權限（企業管理員 / 企業一般成員）

企業層級操作	企業管理員	企業一般成員
以企業加入碼加入企業並取得席位	✓	✓
建立企業名下協作區	✓	✓
登入企業管理後台、查看總覽與統計	✓	—
查看企業成員名冊與席位使用狀況	✓	—
移除企業成員	✓	—
重新產生企業加入碼	✓	—
存取企業名下所有協作區的名片與備註（整理、匯出）	✓	—
升降 / 移除企業名下協作區的成員角色	✓	—
查看企業異動紀錄、匯出 CSV	✓	—

企業管理員僅能存取「掛於本企業名下」的協作區；員工個人建立、未掛企業的協作區與個人名片庫不在此範圍內。企業租戶本身的建立、續約、席位與到期日調整屬 CardNest 維運端權限（見第 1 頁「CardNest 端的存取控管」），企業管理員與一般成員均無法自行變更。

四種使用者介面共用同一組後端服務，皆以 Apple / Google 帳號驗證身分，各自對應不同的使用情境與存取範圍。

iOS App

原生開發

已上架 App Store

個人與協作區使用

Android App

原生開發（Kotlin / Jetpack Compose）

已上架 Google Play

涵蓋名片掃描與協作核心功能

Web App

瀏覽器端，免安裝

協作區查看 / 整理 / 匯出

桌面與行動裝置皆可

企業管理後台

企業管理員專用

席位 / 成員 / 協作區自助管理

即本文件第 1~2 頁所述範圍

↓ 皆以 Apple / Google 帳號登入驗證身分 ↓

CardNest 雲端服務（Google Firebase）

Firestore 資料庫 / Cloud Storage 影像 / Cloud Functions 商業邏輯，全數部署於 Google Cloud 基礎設施

各介面用途與使用族群

介面	使用族群	主要用途
iOS App	員工（個人與協作區）	名片掃描辨識、個人名片管理、協作區上傳與查看
Android App	員工（個人與協作區）	原生開發，涵蓋名片掃描與協作核心功能
Web App	員工（協作區成員）	瀏覽器端查看、整理、匯出協作區名片，免安裝
企業管理後台	企業管理員	自助管理席位、成員、協作區與異動紀錄

CardNest 內部另設有維運專用系統，僅供 RoughZone 內部人員於嚴格權限控管下執行帳戶層維運（席位、方案、到期日等），不具備讀取名片內容之功能，亦不對企業客戶開放，詳見第 1 頁「CardNest 端的存取控管」。