

# Proton Mail 安全性與隱私性分析

---

## 1. 端對端加密 (End-to-End Encryption)

發送者與接收者之間的郵件內容，皆使用 PGP 標準加密。  
伺服器無法解密用戶信件內容，Proton Mail 官方亦無法存取。

## 2. 零存取架構 (Zero Access Architecture)

使用者密碼永不傳送到伺服器，所有信件的解密過程皆於本地端進行。

## 3. 瑞士法律保護

資料存儲於瑞士，受到比歐盟或美國更嚴格的隱私法規保護。  
當局需具備瑞士法院授權才可要求資料。

## 4. 支援匿名註冊與 Tor 存取

可不提供電話號碼或真實身份註冊。  
提供 onion 網址：<https://protonmail.com/tor>，供深層匿名訪問。

## 5. 開源加密技術與安全審查

前端使用 OpenPGP.js，且 Proton Mail 開源部分元件供社群審查。

## 6. 潛在限制與風險

若收件方非 Proton 用戶，需經雙方配合手動密碼傳遞，無法達成完整自動加密。  
信件主旨 (Subject line) 未加密 (PGP 限制)。  
使用 JavaScript 加密可能暴露於瀏覽器供應鏈風險。

## 7. 總結

Proton Mail 是極具信賴性的隱私電郵服務，適合重視通訊保密的使用者。  
搭配良好操作習慣（不暴露身分、不登入追蹤平台、使用 Tor 等），可大幅提升電子郵件的匿名性與資訊安全性。