尊敬的 ACS 客戶

我們有理由相信您的組織可能會遭受網路攻擊。

在過去的一個月，不當使用、超量下載、及非法使用情形顯著增加，世界各地超過 150 間圖書館網路都曾經歷大規模的不當使用與非法登入，ACS 過去一個月監測發現學術網路之下的非法侵入使用案件已達數千，且每一次的侵入都造成破百篇文章的下載量。

非法使用者根據所經歷過的"安全和統計監測工具"調整了攻擊方法，從我們與受害學術機構的互動得知，非法使用者會以各種方式透過第三方或欺詐手段取得經授權的使用者帳號和密碼，一旦非法使用者的身分獲得了學術網路的認證，他們即可在您的學術網域之下使用複雜的機械式下載引擎在幾分鐘內完成數百篇文章的下載。這類型的安全性漏洞將危及貴單位的網路資訊安全，同時也將使個人資料、研究和金融資料置於風險之中。

貴單位可以採取的行動：因為網路攻擊難以預測何時發生、如何發生，因此我們敦促您可以重設網路安全協定，並制定發生攻擊時的標準操作規程 (SOP)及調查策略

基於保護科學記錄的義務，ACS 嚴肅看待所有盜竊智慧財產權的行為，並正緊急修改監測協定以檢測和防止這些入侵(攻擊)再發生。我們正在採取的行動: 當 ACS 檢測到異常下載量時將自動停權可疑 IP，若單位 v 欲恢復該 IP 連線，將需配合提供調查報告以說明事件細節和可防止同樣事件再發生的修復計畫（歡迎參考調查報告範本）。直接停權可疑 IP 可能會使您感到不便，對此我們深感抱歉，但這是目前能夠預防其他網路攻擊繼續發生的最好預防措施。

經與美國執法機關就如何調查和防止網路攻擊的諮詢後，我們要求貴單位採取一切步驟來保留所有可能與非法下載事件相關的證據，其中，執法機關強調伺服器中的潛在網路證據尤為重要，因此，我們懇請貴機構保存所有下載活動 (log file)，尤需保留每組 IP 的位址、埠、時間戳記和時間格式（如 GMT、UTC 等）和 Proxy 伺服器的起始 IP 位址和所有活動 (log file)，請貴單位千萬要避免伺服器 log file 覆寫的狀況。此外，我們也要求您保存每個登入 (session)細節，如 user agent string 和 browser type 等詳細資訊。

任何問題，歡迎請聯繫 acs_pubs_assist@acs.org

誠摯的

Brandon A. Nordin
Senior Vice President
ACS Publications