張貼日期：2016/01/12

使用安全的通訊加密之郵件服務

主旨：為提高郵件服務的安全性，**本組信箱系統已提供網路加密的通訊協定，建議使用者多加利用**，以避免密碼遭網路側錄之可能性，詳說明。

說明：

1. 在開放的網路環境中，連線 POP3, IMAP, SMTP AUTH 等信箱服務時，有可能在用戶端與伺服器間的網路上遭人側錄密碼，**但若使用整合通訊加密的技術，如 TLS/SSL, STARTTLS，則可避免此問題，而提高信箱帳號的安全性**。
2. 本組信箱系統已提供網路加密的通訊協定，分別如下：
   - **POP3/IMAP 服務主機：同信箱網域名稱** (縮減名稱以節省購買憑證經費，例如，若信箱地址 user@mx.nthu.edu.tw 其服務主機為 mx.nthu.edu.tw，user@my.nthu.edu.tw 為 my.nthu.edu.tw，user@m104.nthu.edu.tw 為 m104.nthu.edu.tw，餘類推)
     - POP3 整合 TLS/SSL 之通訊埠為 995
     - IMAP 整合 TLS/SSL 之通訊埠為 993
   - **SMTP AUTH 服務主機：smtpauth.net.nthu.edu.tw**
     - SMTP AUTH 與 STARTTLS 之通訊埠為 25；**由於此服務為多網域共用，故帳號名稱須為完整信箱地址，方能識別**。
3. 已整理Thunderbird 設定說明為例，請多多參考利用。

計算機與通訊中心
網路系統組 敬啟