

# HERHSIANG

## MArchive 系列歸檔伺服器

### 2023

DKIM & DMARC 驗證機制設定方式



## 驗證機制說明:

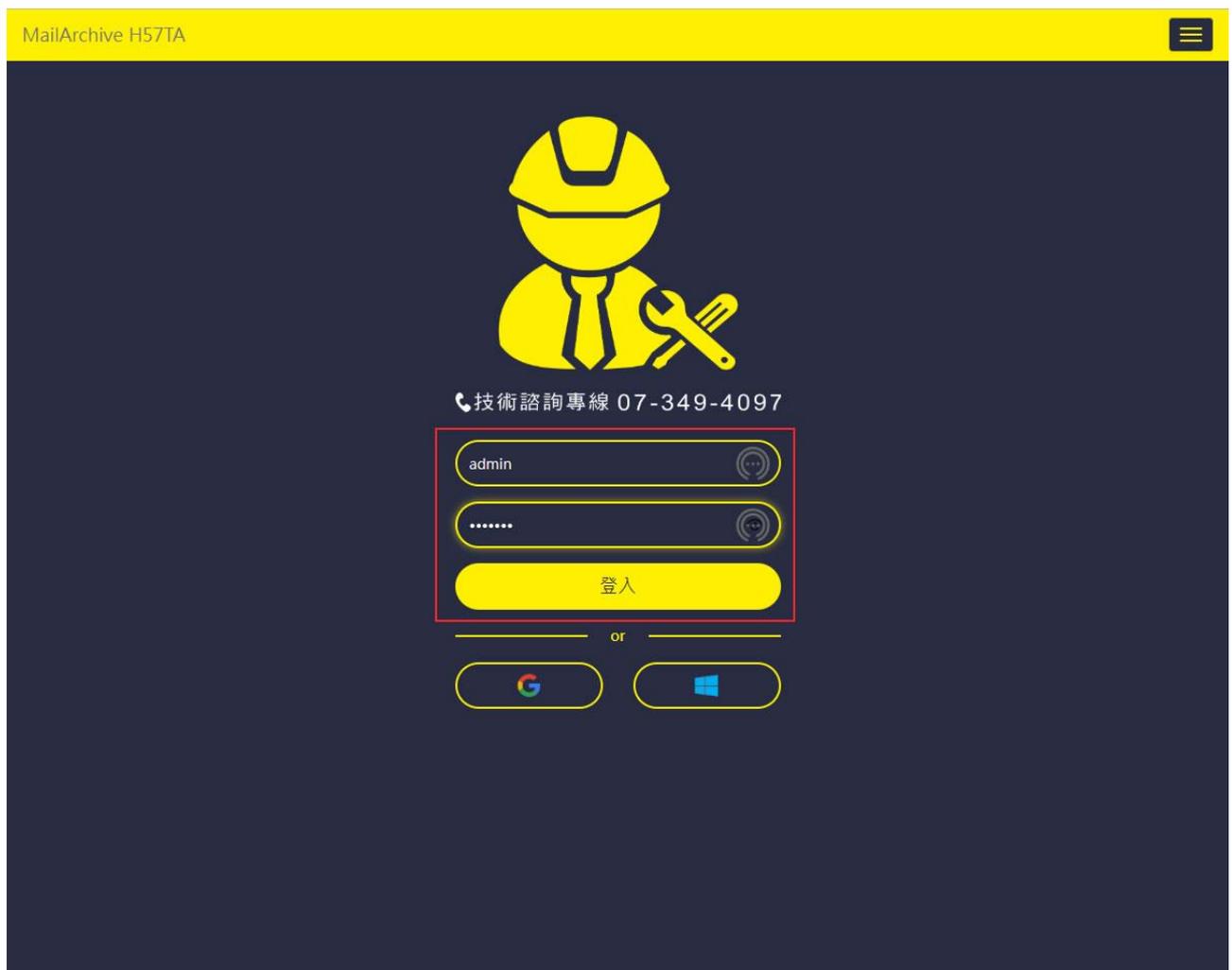
DKIM (DomainKeys Identified Mail) , 網域驗證郵件, 用來防止郵件內容遭到竄改  
跟隨 MArchive 郵件歸檔伺服器內建功能產生, 設定於管理網域 DNS SERVER.

DMARC 是用來輔助 SPF 與 DKIM 的不足跟隨 DKIM 功能內建於設備, DKIM 生效  
DMARC 自動生效.

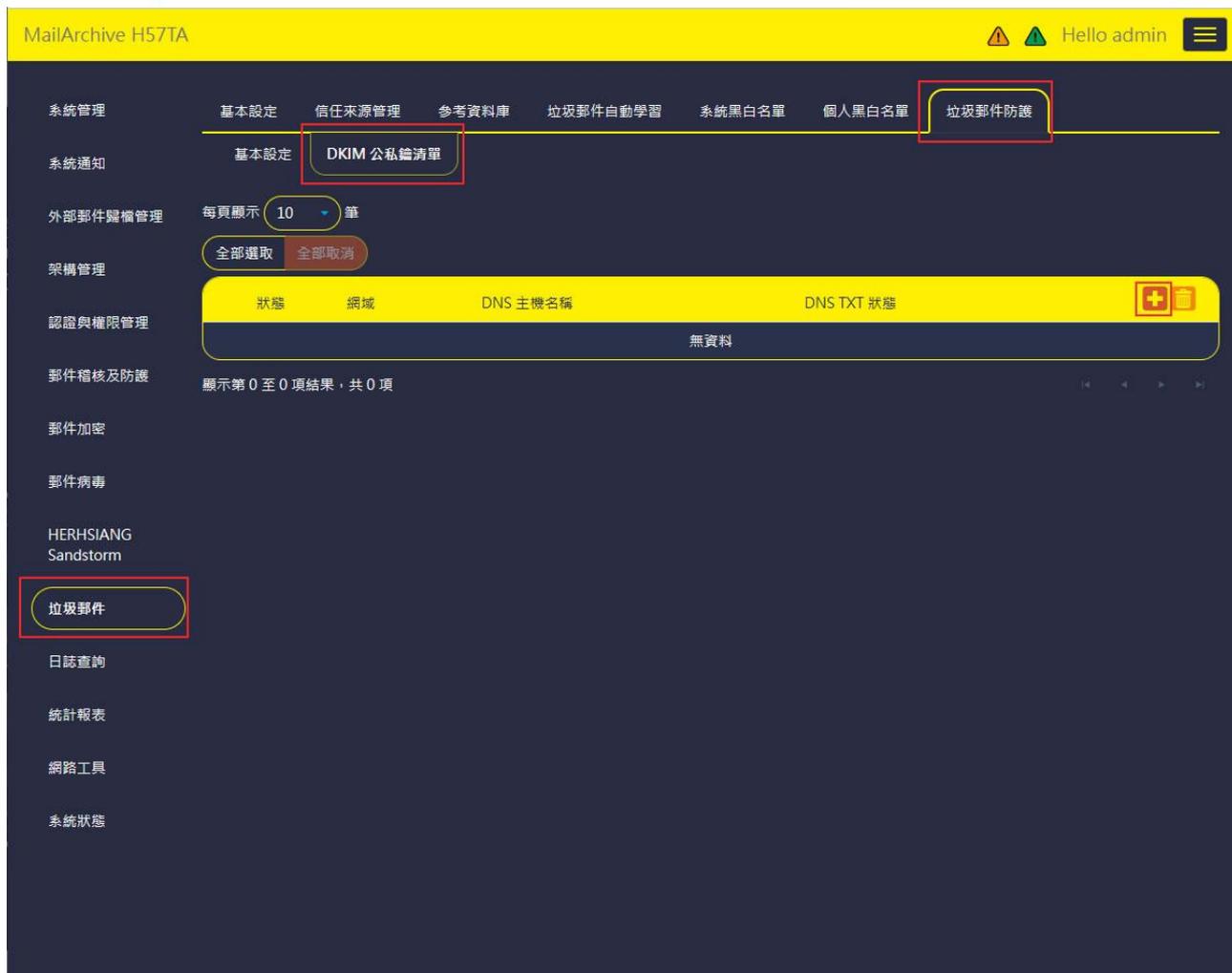
以下輸入 IP&帳號&密碼皆以出廠預設值及網域輸入以官網網域 herhsiang.com.tw 為  
範例, 如已修改 IP&帳號&密碼請換成已修改 IP&帳號&密碼輸入

## MArchive 歸檔伺服器如何設定產生 DKIM:

1. 瀏覽器輸入 <https://192.168.2.1:88> 登入郵件歸檔管理介面, 輸入管理帳號 /  
密碼:admin / adminpw



2. 進入畫面後選擇左邊欄位垃圾郵件選擇上面欄位垃圾郵件防護選擇 DKIM 公私鑰清單按+符號新增



3. 選擇自家網域，前置字串請自訂，金鑰大小請自選，1024 一般 DNS Server 及代管都能接受，2048 一般 DNS Server 及代管不一定能接受甚至需另外付費，1024 及 2048 有些代管需另外付費，2048 相對安全性高對方接受率也相對高，按新增及產生相對自家網域驗證數據。



4. 選擇啟用，先點說明，說明說將相對應參數複製下來，將該參數新增到自管 DNS Server 或代管 DNS 做 TXT，將 DNS 主機名稱及 TXT 資料等參數先複製至記事本備用，按確定，如要重新產生新金鑰請按重新產生金鑰。

編輯 DKIM 公私鑰 : hh2048\_domainkey

網域 herhsiang.com.tw

啟用  ON  OFF

DNS 主機名稱 hh2048\_domainkey

TXT 資料

```
"v=DKIM1; k=rsa; "  
"p=MIIBJjANBgkqhkiG9w0BAQEFAAOCAQ8  
AMIIBCgKCAQEAwxVuhDbA5G3mT8sdUd2  
1hB9hh03AFxgRJuY0PPzfTt7xRjd6hySXERA  
XM+9wP473CJGvKY+u9ccxfE/rkinTpC4jeN  
phWLQ0Prab4i5Qg22yS66Q9w11XsoF0D1  
nKT0cs8bP73ulu+E8vatG7kMoalP/idMAop
```

金鑰大小  1024  2048

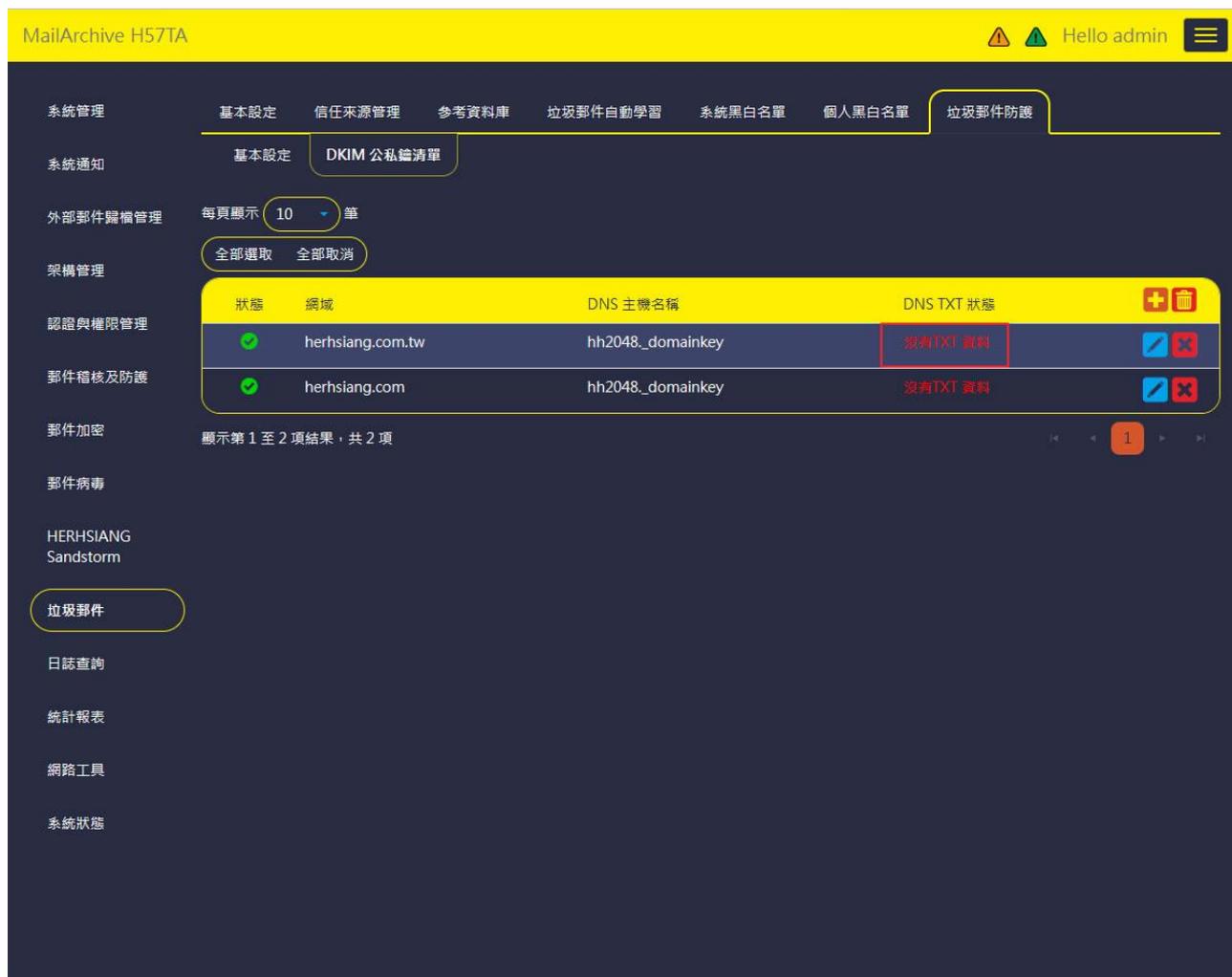
說明 **摺疊**

清單中的網域需再將 [DNS 主機名稱] 與 [TXT 資料] 增加至 DNS 相對應網域的 TXT 後，其他主機才可透過 DKIM(DomainKeys Identified Mail) 通訊協定驗證信件合法性。可從查看 [DKIM 公私鑰清單] 中相對應網域的 [DNS TXT 狀態] 資訊是否正確

確定 重新產生金鑰 關閉

5. 步驟 4 案確定後會產下圖片顯示已新增成功，但因 DKIM 金鑰參數還未加入 DNS Server 及代管 DNS，所以設備檢測顯示沒有 TXT 資料。

P.S. 有些 DNS Server 及代管不接受金鑰所產生特殊字元，但並不一定無效，請利用 Google gmail.com 郵件帳號檢測，檢測方式請 Google 搜尋相關測試方式，這裡不再說明。



MailArchive H57TA

系統管理 基本設定 信任來源管理 參考資料庫 垃圾郵件自動學習 系統黑白名單 個人黑白名單 垃圾郵件防護

系統通知 基本設定 DKIM 公私鑰清單

外部郵件歸檔管理 每頁顯示 10 筆 全部選取 全部取消

狀態	網域	DNS 主機名稱	DNS TXT 狀態	
✓	herhsiang.com.tw	hh2048_domainkey	沒有TXT 資料	✕
✓	herhsiang.com	hh2048_domainkey	沒有TXT 資料	✕

郵件加密 顯示第 1 至 2 項結果，共 2 項

HERHSIANG Sandstorm

垃圾郵件

日誌查詢

統計報表

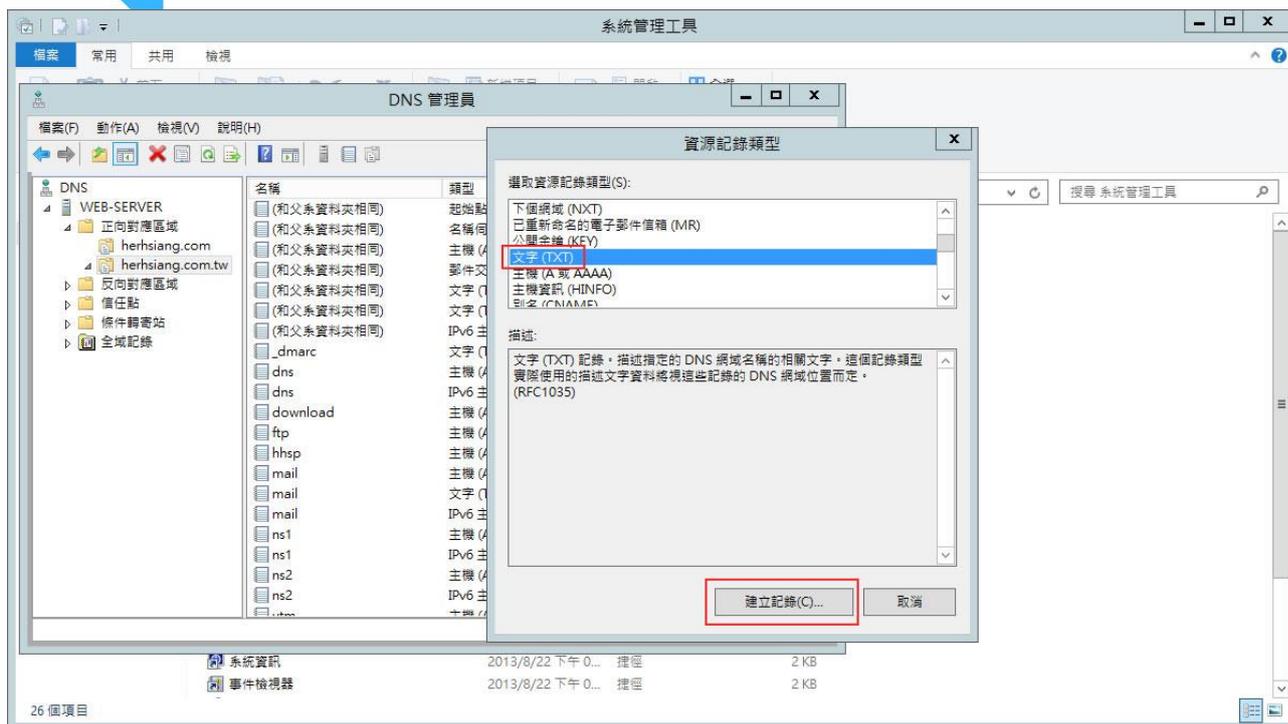
網路工具

系統狀態

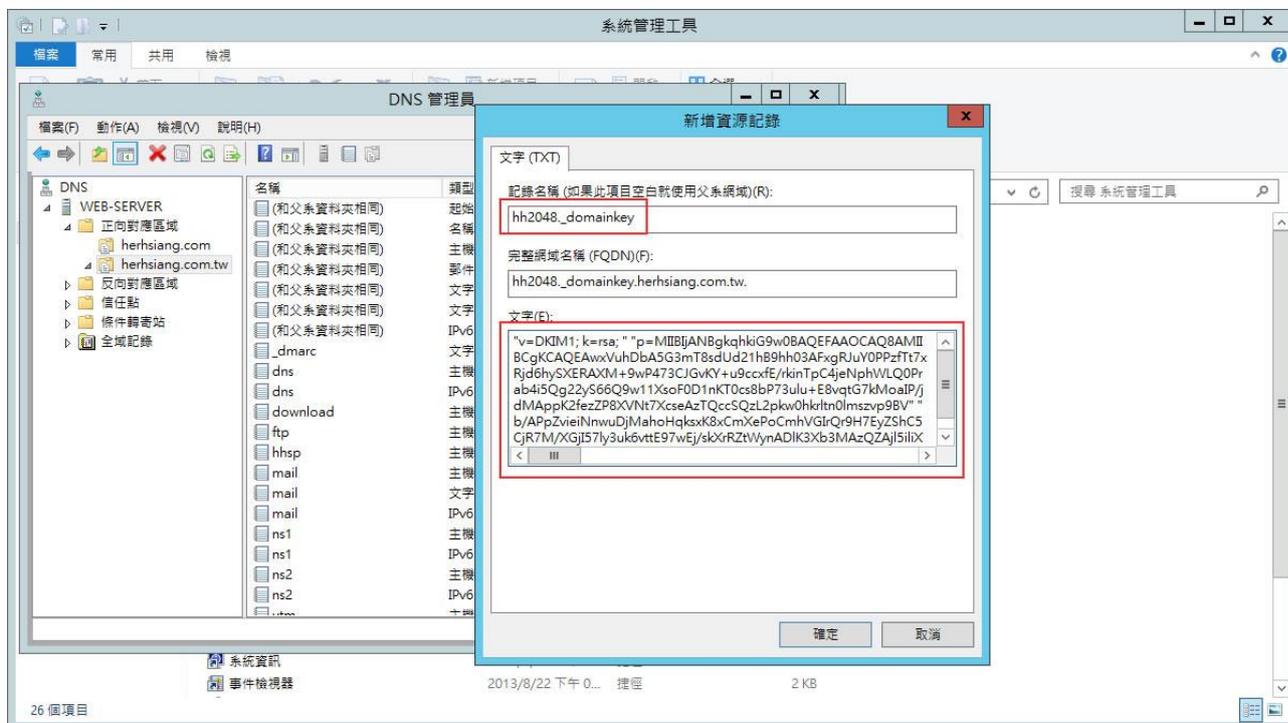
## 6. 參數格式說明

hh2048.\_domainkey.herhsiang.com.tw (前置字串+自家網域即為 DKIM 設定於 DNS Server 或代管 DNS TXT 說明網域，而非設定主網域 herhsiang.com.tw)

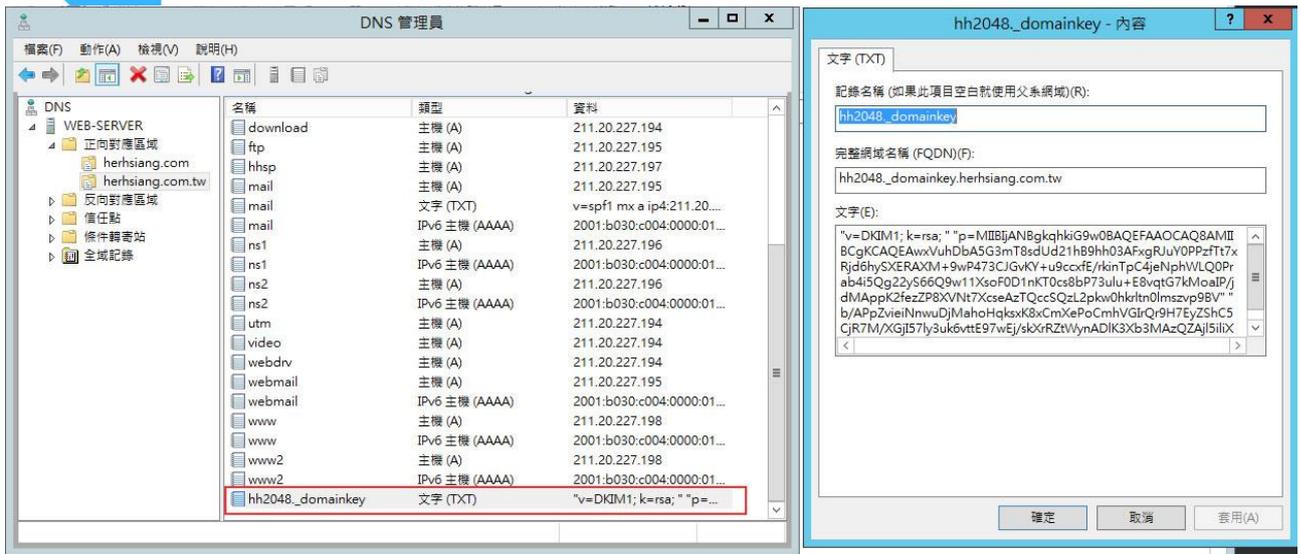
## 7. 範例為 WINDOWS SERVER DNS SERVER, 新增文字 TXT, 按建立記錄



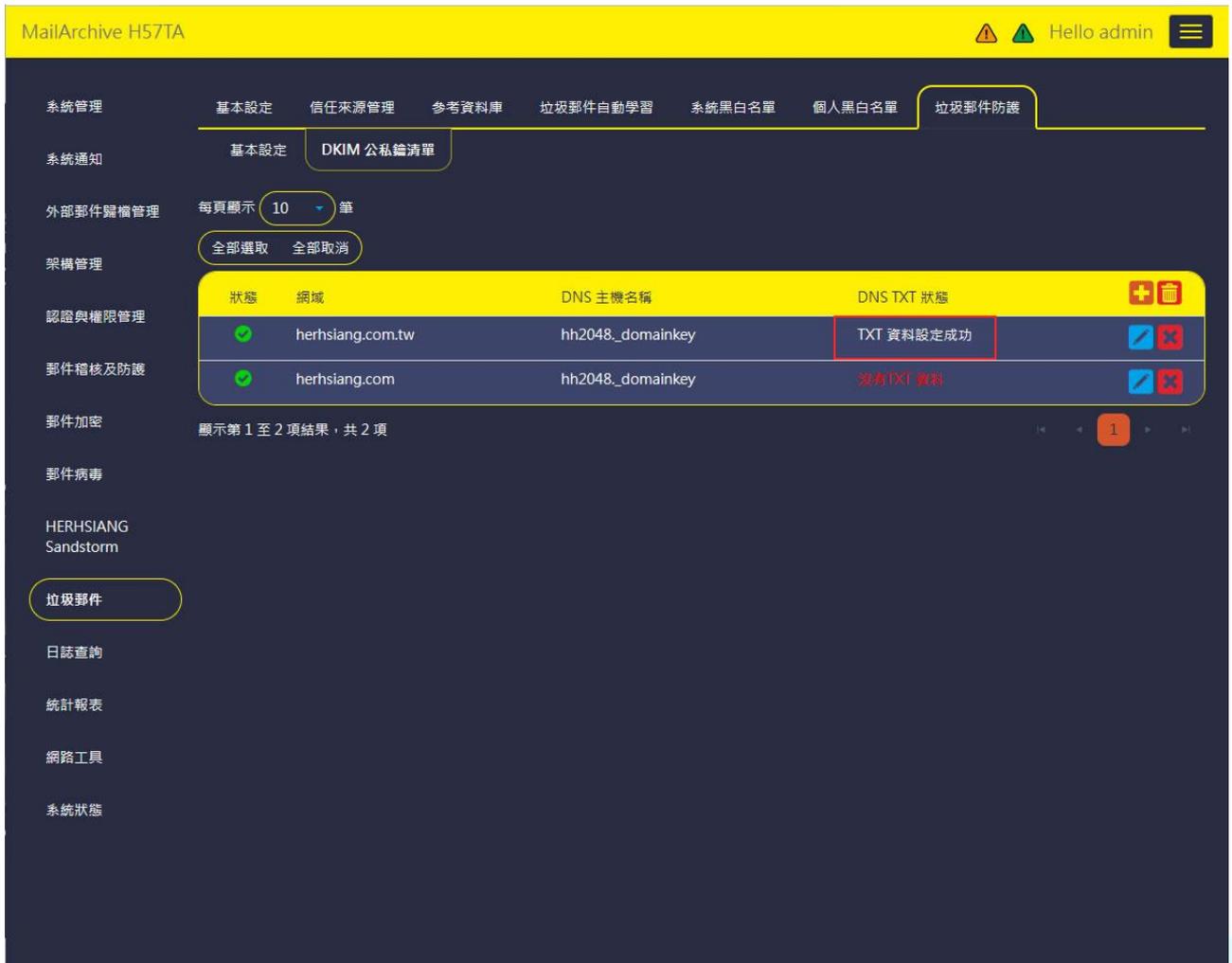
## 8. 將複製到記事本 DKIMR 金鑰參數複製到 TXT 設定欄位內, 按確定即新增 TXT 參數成功.



## 9. 再次核對設定資料



10. 待生效後，再次檢測顯示，TXT 資料設定成功，即完成 DKIM 驗證機制設定完成，請確定 SPF 驗證機制已生效，SPF+DKIM 兩者都生效 DMARC 驗證機制也會自動生效。



## 11. 啟動 DKIM 驗證功能, 即完成 DKIM 及 DMARC 我方網域驗證機制.

The screenshot shows the 'DKIM 驗證' (DKIM Verification) settings page in the MailArchive H57TA interface. The page is dark-themed with yellow accents. At the top, it says 'MailArchive H57TA' and 'Hello admin'. The main content is organized into sections:

- DKIM 驗證功能:** A toggle switch is set to 'ON'.
- 合法來源 (Legitimate Sources):**
  - Radio button selected: 不作處理 (Do nothing)
  - Radio button: 減少垃圾郵件分數 (Reduce spam score) with a value of 5.
- 來源可能有風險 (Sources may be risky):**
  - Radio button selected: 不作處理 (Do nothing)
  - Radio button: 直接刪除 (Delete directly)
  - Radio button: 轉到垃圾郵件隔離區 (Move to spam quarantine)
  - Radio button: 增加垃圾郵件分數 (Increase spam score) with a value of 5.
  - Checkbox checked: 附加主旨提示文字 (Add subject line text) with the value [DKIM - Sender may be risky].
- 非法來源 (Illegal Sources):**
  - Radio button selected: 不作處理 (Do nothing)
  - Radio button: 直接刪除 (Delete directly)
  - Radio button: 轉到垃圾郵件隔離區 (Move to spam quarantine)
  - Radio button: 增加垃圾郵件分數 (Increase spam score) with a value of 5.
  - Checkbox checked: 附加主旨提示文字 (Add subject line text) with the value [DKIM - Sender is illegal].
- 信任 寄件者 (Trust Senders):** An empty text input field.
- 信任 IP (Trust IPs):** An empty text input field.