Email Technical Document

郵件 SPF、DKIM、DMARC 最佳化設定
防止電子報誤判成垃圾郵件

郵件技術白皮書

沛盛資訊有限公司
台北市內湖區新湖一路 83 號 3 樓
(02)7720-1866
contactus@itpison.com
https://www.itpison.com

TABLE OF CONTENTS

1. 郵件 SPF、DKIM、DMARC 最佳化設定 3
2. 郵件如何傳遞 4
3. 郵件身份驗證協定 5
   - A. SPF (Sender Policy Framework) 寄件者政策框架 5
   - B. DKIM (DomainKeys Identified Mail)，網域驗證郵件 5
   - C. DMARC (Domain-based Message Authentication,Reporting & Conformance) 5
   - D. SPF、DKIM、DMARC 協同運作機制 6
4. 沛盛資訊電子報郵件 DNS 設定 7
   - A. 選定發送電子報網域 7
5. SPF 設定 8
6. DKIM 設定 9
7. DMARC 設定 10
8. 追蹤連結網址設定 11
   - A. 追蹤連結設定原因 11
   - B. 追蹤連結設定做法 11
   - C. 追蹤連結設定說明 11
9. MX 設定 13
10. 郵件 DNS 設定總整理 14
11. 郵件 DNS 設定測試 15
    - A. 使用 nslookup 查詢 15
    - B. 驗證設定內容 15

1. 郵件 SPF、DKIM、DMARC 最佳化設定

台灣各領域規模最大的企業，電子報幾乎都是透過沛盛資訊所發送。客戶在透過正規獲取的客戶郵件名單並發送行銷電子報，最常遇到的問題就是行銷電子報被判定成垃圾郵件。以國際間對垃圾郵件有許多規範，但採用合法獲得的會員名單，並透過像沛盛資訊這樣正規電子報發送業者，發送行銷宣傳郵件是被國際認可的行銷行為。但若是客戶不了解國際間在對電子報防範濫發所設定的機制，沒有進行適當的設定，行銷宣傳電子報就容易被判定為垃圾郵件。

國際間相關組織制定了防治濫發垃圾郵件，制定了許多做法，除了在法律層面各國立法外，在國際間的郵件交換協定上，訂出了 SPF、DKIM 以及 DMARC 等規範。收信服務器如 Gmail、Yahoo、Hotmail 等，在收郵件時會去檢查這些規範有無被加入，如果沒有的話被判定成垃圾信的可能性大幅提高。對合法的電子報行銷郵件，沛盛資訊建議發信者都加入這些郵件安全性機制，以降低被判成垃圾信的可能。

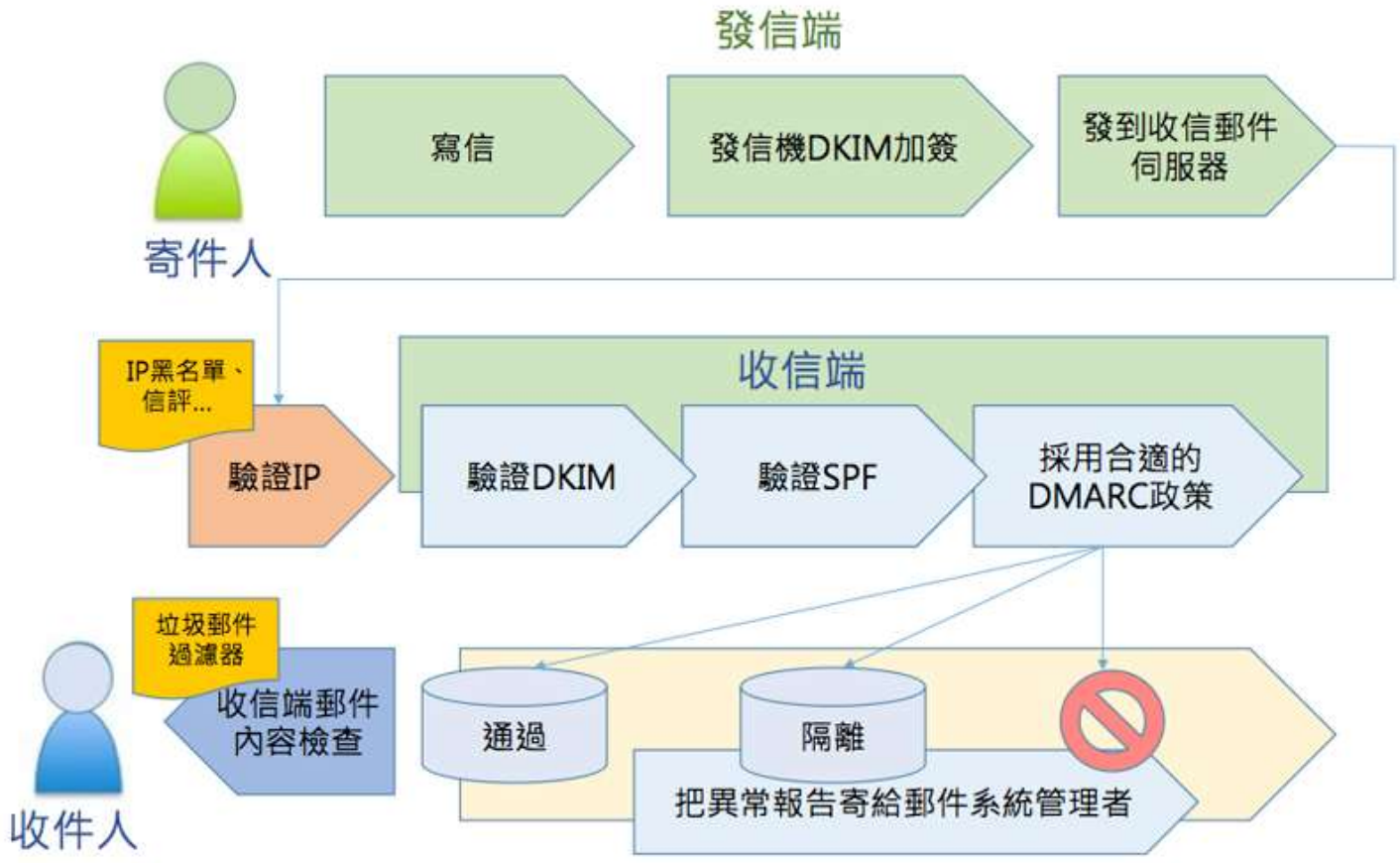
本郵件技術白皮書將以沛盛多年實務經驗，詳細說明企業如何進行電子報的 DNS 設定，主要是 SFP、DKIM 以及 DMARC，並額外介紹在設定電子報 DNS 的技巧。

2. 郵件如何傳遞

我們透過以下這張圖片，來解說 SPF/DKIM/DMARC，如何在一封郵件發信與收信中發生作用。

首先，寄信人寫完電子郵件按下發送後，這封郵件在發信服務器端進行 DKIM 加簽(加入私鑰)，確保過程不會遭到竄改。接下來傳送到收信端服務器，此時會先檢查發信機的 IP 是否可靠，有沒有在濫發郵件黑名單，在國際間有專門組織發佈濫發黑名單 IP 地址。通過之後收信服務器接著檢查 DKIM(公鑰)，看是否跟原本加簽的私鑰相符。之後驗證 SPF，這是檢查寄信者的網域，是否有同意這個發信 IP 去發信。

接著進行 DMARC，也就是說前面的 SPF/DKIM 檢查若有錯誤，這封郵件可以依舊發送、隔離(通常就是標注為垃圾郵件)，或是拒收。然後郵件才傳給收信程式(例如 Gmail 網頁介面，或 Outlook)，此時檢查內文看是否可能為垃圾信件(例如：大促銷、大降價等文字)。



原圖來自dmarc官網https://dmarc.org/，此為中譯方便理解。

3. 郵件身份驗證協定

A. SPF (Sender Policy Framework) 寄件者政策框架

SPF用來規範在選定的郵件發送服務器位址，可以用來發送寄件人的網域郵件。這樣機制可以避免垃圾信濫發業者，偽裝網域發送假冒郵件。SPF的設定裡面，列出明確許可的郵件發信機網域名稱，郵件收信服務器透過檢查發信人網域的SPF，就知道這封電子郵件是否來自被允許的發信機位址。

通常企業網域的SPF會列出自己的公司認可對外郵件服務器名稱，但以行銷電子報而言，則是透過像沛盛資訊這樣正規專業電子報發送廠商代發，因此電子報寄件人的網域，就需要加入沛盛資訊的發信機網域名稱。SPF幾乎已經是各大郵件信箱，如Gmail、Yahoo、Outlook等收信時必驗證欄位，若檢查不過會明顯提示這郵件來源有問題，建議所有企業發送的電子報都至少要加上SPF。

SPF 官方網站 http://www.openspf.org/

B. DKIM (DomainKeys Identified Mail)，網域驗證郵件

DKIM是一種電腦數位簽章，採用公鑰與私鑰這種加密驗證法進行。在發送郵件時由發信服務器對郵件以私鑰進行簽章，而在郵件接收服務器上，會透過DNS到發信者的網域查詢 DKIM 紀錄，擷取上面記載的公鑰資料，然後對這封郵件做簽章解碼，如果公鑰與私鑰能配對成功，代表郵件確實為原始發信機所發出。

透過DKIM的導入，收信郵件服務器可以驗證郵件絕對是原本的郵件發信服務器所發出，而且在郵件複雜的傳送過程中，這封郵件內容也毫無被竄改過，這杜絕了濫發垃圾信業者，透過假冒的郵件發送機以及假冒的私鑰簽章寄送垃圾信。由於係採用公鑰與私鑰簽章架構，因此除了在網域做DKIM設定之外，在郵件發信服務器上也要進行對應的私鑰設定。

DKIM 官方網站 http://www.dkim.org/

C. DMARC (Domain-based Message Authentication,Reporting & Conformance)

DMARC是用來輔助SPF與DKIM的不足，用來讓發信端網域通知收件端郵件服務器，當遇到SPF與DKIM的設定檢查不過時，進行的處理方式。最知名的案例就是Yahoo在2014年，宣布DMARC設為「拒絕」，也就是說所有不是從Yahoo郵件服務器發出的郵件，寄信人都不能用Yahoo郵件地址。

由於企業的郵件架構可能極為複雜，以DKIM設定還要發信端服務器配合設定，某些企業郵件可能透過當地ISP做為郵件發信機，但這也是合法的郵件。由於真假不一，收信端很難知道遇到SPF/DKIM驗證不過該拒絕還是放行。但假若寄件者絕對知道所有的郵件都一定符合SPF/DKIM驗證，寄件方就可以透過DMARC通知收件方郵件服務器，遇到驗證不過時的處理方式(通過/隔離/拒絕)。

DMARC 官方網站 https://dmarc.org/

D. SPF、DKIM、DMARC 協同運作機制

透過SPF、DKIM、DMARC的郵件驗證機制，在收件端郵件服務器，首先由SPF可以檢查是否發信機的IP為認可發送該寄信者網域郵件。其次，以DKIM查看郵件發信時的私鑰與收信時的公鑰是否匹配，代表內容確實為該發信機發出。最後，由DMARC知道，假設SPF/DKIM驗證不過時，此封郵件該如何處理。以Gmail為例，必須做到SPF、DKIM、DMARC通通都設定且驗證通過，這封郵件才比較不可能被丟進垃圾信箱匣(另外還牽涉到郵件內文等)。

4. 沛盛資訊電子報郵件 DNS 設定

A. 選定發送電子報網域

透過沛盛資訊作爲電子報發送端，在設定郵件DNS之前，首先要決定要用來發電子報的域名。沛盛資訊建議分開公司原本域名跟電子報發送的域名，例如公司名稱為example.com，電子報寄件人則用example123.com。

將電子報發信網址與原本公司網址分開，這是因為電子報的發送量大，有可能發信域名的IP信評會受到不同層度的影響，為了避免發送電子報反而影響到公司原本正常使用的網域名稱信評，可能進而影響到員工郵件信箱(例如: name@example.com)發送，因此將電子報發送使用的域名與公司原本域名分開。

了解電子報寄件人網域要與原本公司網域分開的原理，在實務上以沛盛資訊的經驗，我們的企業客戶會採用兩種方法進行：

1 採用電子報專用域名
   - 1.1 做法：原本公司網域 example.com，電子報發信人的網域為 example123.com。
   - 1.2 原因：這樣的設定方法，收信的讀者足以辨認出這封電子報，是由原本 example.com 這間公司所發出。而電子報所使用的網域，又不會影響到原本公司網域的信評，此種作法為 90%的國內外大企業所採用

2 採用子網域
   - 2.1 做法：原本公司網域 example.com，電子報發信人的網域為 123.example.com。
   - 2.2 原因：有些類型的企業，希望保有公司對外統一形象，或者其它原因要求一定要使用公司原本網域名稱，這時候建議採用發送電子報專用的次網域名稱。由於設定電子報發送需要在 DNS 進行許多設定，這種作法對原本公司網域 example.com 的 DNS 不需做任何變動，只需要在子網域 123.example.com 進行相對應的 SPF、DKIM、DMARC 等 DNS 設定。跨國大型企業許多會採用這種作法。
   - 2.3 應用：沛盛資訊某客戶為跨國知名金融集團，透過電子報系統對它的全球客戶發送金融研究報告，屬於大量發送郵件但非行銷型電子報，因此要保留原有公司的網域名稱，便採用這種子網域的做法，針對子網域做所有 DNS 郵件最佳化設定。

以下範例為電子報採用專有域名方式example123.com，並使用電子報寄件者edm@example123.com為例做介紹，DNS設定分別在主要網域與不同子網域設定，請仔細比對文件說明。

5. SPF 設定

請檢查寄件人信箱網域(example123.com)，在DNS裡是否有 SPF 的 TXT 紀錄，若原來沒有 SPF（TXT）記錄，請新增一筆紀錄如下，若原來已有紀錄請將以下紅色部分增加至原來 SPF 紀錄。例如電子報寄件人為edm@example123.com，則為檢查example123.com的DNS裡面TXT記錄。

Name	Type	Record
example123.com	TXT	v=spf1 include:spf.neweredm.com a mx ptr ?all

說明：
(1) v=spf1 表示 spf 所使用的版本。
(2) include 表示授權給該郵件伺服器。
(3) a 表示比對 DNS 紀錄中的"A"紀錄，允許在"A"紀錄裡面的IP為發送郵件來源IP。
(4) mx 表示比對 DNS 紀錄中的"MX"紀錄，允許在"MX"紀錄裡面的網域為發送郵件來源網域。
(5) ptr 表示比對 DNS 紀錄中的"PTR"，允許在"PTR"紀錄裡面的網域為發送郵件來源網域。
(6) ?all 表示還有其它可能傳送的郵件伺服器。

範例：以沛盛資訊itpison.com網域為例，使用 nslookup 解析出來成功的畫面

```
C:\CheckDNS>nslookup -q=txt itpison.com
伺服器:  google-public-dns-a.google.com
Address:  8.8.8.8

未經授權的回答:
itpison.com     text =

        "v=spf1 include:spf.neweredm.com a mx ptr ?all"
```

6. DKIM 設定

重要：DKIM設定完畢後，請務必通知沛盛資訊（沛盛系統也須對應設定私鑰）

同樣以電子報寄件人為edm@example123.com，請新增以下子網域：

s1024._domainkey.example123.com

之後在以上子網域增加一筆 TXT 紀錄：

k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFS
z/FSvVJywU1pBNF3rWkaaOjrzEIIb1vcIydgGi7xSXGbPqof9AnTHgVbX2cIASW09fTwTLokzj0dZ9gx9/Lsy
7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;

(不能有斷行)

說明:
(1) k 為加密演算法，預設為 rsa。
(2) p 為公鑰內容(public key)。

範例：以沛盛資訊itpison.com網域為例，使用 nslookup 解析出來成功的畫面

```
C:\CheckDNS>nslookup -q=txt s1024._domainkey.itpison.com
伺服器:  google-public-dns-a.google.com
Address:  8.8.8.8

未經授權的回答:
s1024._domainkey.itpison.com    text =

        "k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSvVJywU1pBNF3rWkaaOjrzEII
b1vcIydgGi7xSXGbPqof9AnTHgVbX2cIASW09fTwTLokzj0dZ9gx9/Lsy7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;"
```

7. DMARC 設定

同樣以電子報寄件人為edm@example123.com，請新增以下子網域：

_dmarc.example123.com

在以上子網域增加一筆 TXT 紀錄：

Name	Type	Record
_dmarc.example123.com	TXT	v=DMARC1; p=none; rua=mailto:dmarc-admin@example.com

說明：
(1) v 表示DMARC版本。
(2) p 表示採用的處理方式，none表示通過。
(3) rua 表示統計報表寄送信箱，此處改為電子報發件方系統管理者真實信箱(以公司原本網域example.com，而非電子報發件人網域example123.com)。
(4)務必設好SPF及DKIM 之後，才可設定此DMARC紀錄，否則請勿設定。

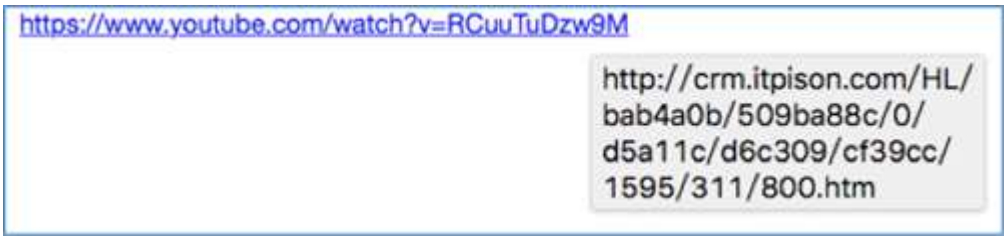
(note: 若不收錯誤狀況統計報表，也可不設rua=mailto:dmarc-admin@example.com)

範例：以沛盛資訊itpison.com網域為例，使用 nslookup 解析出來成功的畫面

8. 追蹤連結網址設定

A. 追蹤連結設定原因

沛盛資訊提供點選電子報連結紀錄，包含哪些客戶點了這些連結、點選的時間及次數、以及哪些產品連結最受客戶的青睞。追蹤點擊連結的做法如以下圖示:



以上圖而言，電子報的內文連結原本到youtube.com，但是為了進行點擊追蹤，點擊的連結會先到crm.itpison.com(沛盛資訊服務器)，進行點擊統計，之後再轉到原本的youtube.com。以電子報發信人edm@example123.com為例，電子報內追蹤連結網址會出現 http://crm.itpison.com/hl/…./xxx.htm。

對品牌大廠而言，整封電子報的連結應該都是要自己的網域名稱才合適，而且出現其它的域名，也會降低電子報信用等級，增加進入垃圾信匣的可能性。因此，可以進行DNS的設定，讓追蹤連結網址出現自己的網域，如http://click.example123.com/hl/…/xxx.htm

B. 追蹤連結設定做法

以電子報寄件人為edm@example123.com，請新增以下子網域(或其它合適子網域名稱)：

click.example123.com

接著可以透過DNS的A紀錄或CName記錄都可以達到同樣效果。以A紀錄做法而言，在以上子網域DNS增加一筆 A 紀錄，指定到沛盛服務器113.196.228.5：

Name	Type	Record
click.example123.com	A	113.196.228.5

或者是以CNAME做設定到hl.itpison.com (HL.ITPISON.COM)

Name	Type	Record
click.example123.com	CNAME	hl.itpison.com

(Note: hl.itpison.com的IP位址即為113.196.228.5)

C. 追蹤連結設定說明

(1) A Record（Address Record）位址紀錄，簡稱 A 紀錄：
DNS裡面的A紀錄，用來對應主機名稱和其 IP 位址，例：www.itpison.com (沛盛資訊公司網域)對應的主機位址 IP 為 113.196.228.10，當我們在瀏覽器網址列輸入 www.itpison.com，透過 DNS 解析便會找到 113.196.228.10 的主機。

因此，將 click.example123.com 設一個 A Record 到 113.196.228.5，再透過沛盛資訊後端程式的轉換，圖片中的追蹤連結網址就會變為 http://click.example123.com/hl/…/xxx.htm

(2) CName（Canonical Name Record）別名記錄：
例：在網址列輸入 www.itpison.com 或 itpison.com 都會找到同一個網站（113.196.228.10），其實 CName 記錄就好像是 A 記錄的分身，幫已存在的 A 紀錄設定其它的名字。

因此，將 click.example123.com 設一個 CName 到 hl.itpison.com，再透過沛盛資訊後端程式的轉換，圖片中的追蹤連結網址就會變為 http://click.example123.com/hl/…/xxx.htm

9. MX 設定

電子郵件在傳送時，收信端服務器會透過MX記錄，反查原本發信人郵件地址是否真實存在，不是虛假郵件地址。以電子報寄件人為edm@example123.com為例，這必須是有效且能收信，不可使用假的或是無效信箱。

以MX紀錄而言，若example123.com原本已經設立MX記錄，則不用做更動。但如果example123.com這是專門用來發電子報的網域名稱，完全沒有用在其它地方，且該網域本身也不想要收信，可將MX記錄設到沛盛資訊郵件服務器。

以電子報寄件人為edm@example123.com為例，請在example123.com網域的DNS，加入以下MX記錄。

Name	Type	Record	Priority
example123.com	MX	mx1.neweredm.com	10
example123.com	MX	mx1.neweredm.com	10

備註：
再強調一遍，把公司原本域名(example.com)跟電子報發送的域名(example123.com)分開，這是一個建議的好方法，可以讓電子報發送域名不影響原本公司使用的域名。將電子報專用域名example123.com加入MX記錄，會有助於減少收件服務器判定垃圾信的可能。

10. 郵件 DNS 設定總整理

	設定原因	域名	型態	內容
1	SPF	example123.com	TXT	v=spf1 include:spf.neweredm.com a mx ptr ?all
2	DKIM	s1024._domainkey.example123.com	TXT	
3	DMARC	_dmarc.example123.com	TXT	v=DMARC1; p=none;rua=mailto:dmarc-admin@example.com
以下第4項與第5項兩者取其一即可				
4	點擊追蹤	click.example123.com	A	113.196.228.5
5	點擊追蹤	click.example123.com	CNAME	hl.itpison.com
若原本example123.com沒有MX才設以下6、7項				
6	驗證發件人	example123.com	MX	mx1.newermail.com
7	驗證發件人	example123.com	MX	mx2.newermail.com

11. 郵件 DNS 設定測試

A. 使用 nslookup 查詢

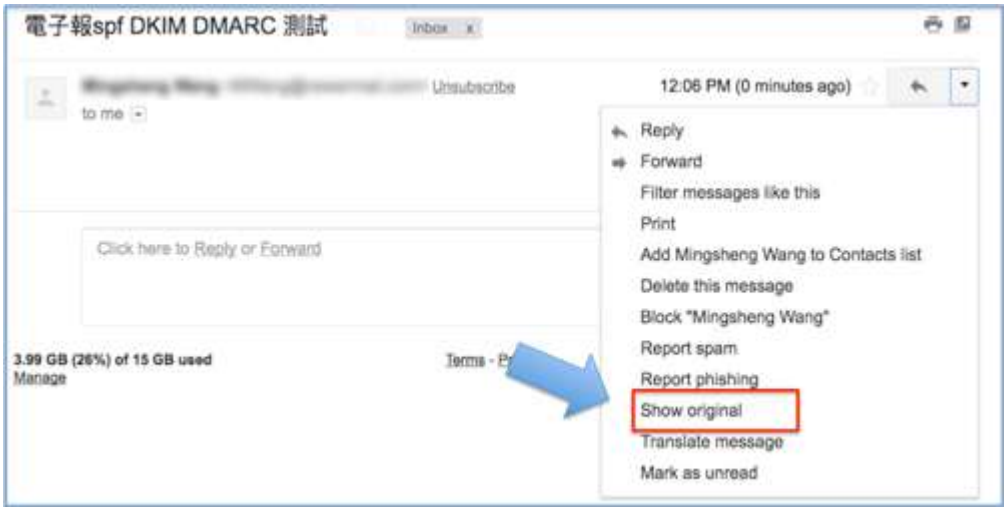
郵件DNS設定完畢後，可以透過 nslookup 程式下參數指令來進行 DNS 內容查詢，或者利用網路版(註1)查詢。自有DNS設定完，須等待數小時對外做正式公佈，以下的查詢係透過中華電信 dns.hinet.net來查看是否已經正式生效。

註1：http://www.kloth.net/services/nslookup.php

	設定原因	域名	型態	nslookup 指令
1	SPF	example123.com	TXT	nslookup -q=txt example123.com dns.hinet.net
2	DKIM	s1024._domainkey.example123.com	TXT	nslookup -q=txt s1024._domainkey.example123.com dns.hinet.net
3	DMARC	_dmarc.example123.com	TXT	nslookup -q=txt _dmarc.example123.com dns.hinet.net
以下第4項與第5項兩者取其一即可				
4	點擊追蹤	click.example123.com	A	nslookup -q=a click.example123.com dns.hinet.net
5	點擊追蹤	click.example123.com	CNAME	nslookup -q=cname click.example123.com dns.hinet.net
若原本example123.com沒有MX才設以下6、7項				
6,7	驗證發件人	example123.com	MX	nslookup -q=mx example123.com dns.hinet.net

B. 驗證設定內容

最準確的測試SPF、DKIM、DMARC有沒有設定成功，就是利用沛盛資訊電子報發信系統，實際以電子報寄件人edm@example123.com，發送測試郵件到Gmail帳號，之後登入Gmail，如下圖指示來查看Gmail郵件原始檔。



在郵件的原始檔內，就可以看到SPF、DKIM、DMARC是否通過的訊息，務必做到這三項設定全部都通過，整個設定才算大功告成。

沛盛資訊有限公司 | 台北市內湖區新湖一路 83 號 3 樓 | (02)7720-1866

contactus@itpison.com | https://www.itpison.com