200415458

申請日期： 93-3-26	IPC分類
申請案號： 93106239	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	利用郵件行為解析以管控電子郵件之方法
	英 文	
二、發明人(共1人)	姓 名(中文)	1. 鄭志文
	姓 名(英文)	1.
	國 籍(中英文)	1. 中華民國 TW
	住居所(中 文)	1. 新竹縣竹北市縣政六路58號4樓
	住居所(英 文)	1.
三、申請人(共1人)	名稱或姓 名(中文)	1. 碩琦科技股份有限公司
	名稱或姓 名(英文)	1.
	國 籍(中英文)	1. 中華民國 TW
	住居所(營業所)(中 文)	1. 新竹縣竹北市縣政六路58號4樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英 文)	1.
	代表人(中文)	1. 鄭志文
	代表人(英文)	1.

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構:

無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期:

無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明（1）

【發明所屬之技術領域】

本發明係有關一種管控電子郵件之方法，特別是關於一種利用郵件行為解析以管控電子郵件之方法。

【先前技術】

企業郵件資訊安全問題從病毒、駭客，乃至於垃圾郵件猖獗，絕大部分的郵件過濾稽核、病毒掃描加值與垃圾郵件防堵軟體公司，係奠基於龐大資料庫的運算與分析技術，以希冀藉由匯集大量垃圾的「郵件內容」，加以數值加權計算與智慧啟發方法，來達到「垃圾郵件防堵」功能。然而習知缺失為分類認定過於主觀，例如色情、發財、藥物、商業等，非決定性、可能誤判，以及郵件內容掃描過濾造成系統資源耗費和通訊效率降低。

為抵制垃圾郵件，各國相繼立法，經國際性共識，郵件大致區分為垃圾郵件及廣告郵件，故在談論「垃圾郵件防堵」前，我們必須先區別垃圾郵件與廣告郵件。以美國為例，Can-Spam立法下之垃圾郵件係指以匿名、偽造、濫發或非法(變動資訊或隱藏資訊等)等行逕傳送電子郵件者，其採用該等手法之可能原因如下：1. 無法追查來源；2. 變動聯繫方式；3. 讓收件者誤認為同事或友人；4. 讓收件者基於好奇而看信等，由於來路不明或無法成功拒絕，故需有特殊技術來辨識並拒絕接收。而廣告郵件係指寄件者經由特定管道取得收件者地址，以正常公開方式傳送電子郵件者，收件者可追溯來源地並有權利經正式管道取消訂閱。

五、發明說明（2）

習知垃圾郵件過濾阻隔技術大致可分為內容過濾、數值計算及啟發技術三種技術。內容過濾之做法係提供寄件者、收件者、郵件主旨、郵件內容、副檔名、檔案名稱和檔案內文等之過濾阻隔，其係透過黑名單收集方式，以防堵垃圾郵件；但具有名單收集不易、名單建立費時、阻擋率不高、黑名單誤判等缺點。數值計算之做法則係奠基於龐大資料庫的運算與分析技術，藉由匯集大量垃圾的「郵件內容」，加以數值加權計算方法，以達成垃圾郵件防堵之作用；然而具有分類認定過於主觀（例如色情、發財、藥物、商業等）、非決定性、可能誤判、郵件內容掃描過濾致使系統資源耗費和通訊效率降低等缺點。啟發技術則與前述數值計算方法類似，其亦係奠基於龐大資料庫的運算與分析以匯集大量垃圾的「郵件內容」，除了將郵件內容加以數值加權計算之外，同時亦加以智慧啟發方法，因此除了具有數值計算方法之缺失外，當資料庫越大時，則誤判率越高。

有鑑於此，本發明係針對上述之種種問題，提出一種利用郵件行為解析以管控電子郵件之方法，以有效克服習知之該等缺失。

【發明內容】

本發明之主要目的，係在提供一種利用郵件行為解析以管控電子郵件之方法，以達成郵件進出控管之目的。

本發明之另一目的，係在提供一種利用郵件行為解析以管控電子郵件之方法，以有效達成垃圾郵件防堵之功

五、發明說明 (3)

效。

本發明之再一目的，係在提供一種利用郵件行為解析以管控電子郵件之方法，不僅可精確地管控郵件，且具有節省網路頻寬、系統資源與硬碟空間之優點，藉以同時兼顧高網路安全性及高郵件通訊效率之雙重效益。

本發明之又一目的，係在提供一種利用郵件行為解析以管控電子郵件之方法，具有節省營運成本之優點。

根據本發明，一種利用郵件行為解析以管控電子郵件之方法係包括下列步驟：首先，利用郵件之信封資訊及標題資訊設定複數不同之郵件政策；當代理器(Agent)收到一電子郵件時，係以該等郵件政策逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符合該等郵件政策，並依據驗證結果採取一相對應之阻擋/傳送的行動。

底下藉由具體實施例配合所附的圖式詳加說明，當更容易瞭解本發明之目的、技術內容、特點及其所達成之功效。

【實施方式】

本發明係在郵件傳送代理器(Mail transfer agent，MTA)執行階段，利用預設之郵件政策來驗證一電子郵件之郵件傳輸資料的真假值，透過郵件信封與郵件標題等郵件傳輸資料的解析，以主動判斷該電子郵件之行為是否符合系統所允許之行為，進而達成郵件進出控管及垃圾郵件防堵之目的。

五、發明說明 (4)

一封完整的電子郵件稱為郵件文本(Mail text)。一般而言，郵件文本係含括郵件信封(Mail envelop)、郵件標題(Mail header)及郵件內容(Mail content)。一封完整的電子郵件在伺服器與用戶端將會有經過郵件傳送代理器(Mail transfer agent，MTA)和郵件用戶代理器(Mail user agent，MUA)處理的過程，此為電子郵件的基本傳輸模式。本發明即利用此電子郵件之郵件特性及傳輸原則，將一電子郵件的「郵件信封」與「郵件標題」等郵件傳輸資料的真假值加以解析，且經由反覆回溯驗證，以精確歸納與演繹出上百種郵件行為類型，進而達成管控電子郵件之進出以及垃圾郵件防堵之作用。

由於本發明會使用到一電子郵件的信封資訊來設定管理郵件之郵件政策，因此在說明本發明之方法之前，必須先說明信封資訊之內容。電子郵件之信封資訊通常為寄件者帳號、收件者帳號、收件者主機地址、寄件者主機地址、回覆地址、網域名稱伺服器(DNS)及電子郵戳等資訊；其中，電子郵件經由發信端伺服器、局端伺服器或聯網路服務提供者(ISP)伺服器等代理器傳送後，每一所經過之代理器係會在該電子郵件上加註一電子郵戳。

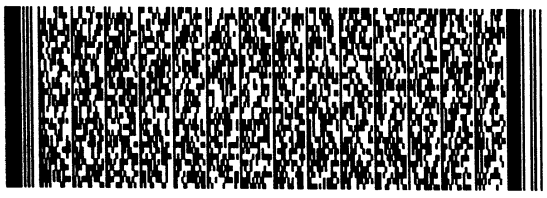
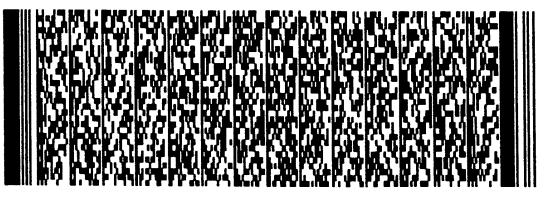
第一圖為本發明解析郵件行為以管控電子郵件的方法示意圖，係包括下列步驟：首先，利用郵件之信封資訊、標題資訊、內容及附加檔案等資訊來預先設定出複數不同之郵件政策10，且每一郵件政策10係包括有複數規則12。其中，第二圖所示，每一政策10之設定係包含有[信封寄

五、發明說明 (5)

件者]、[信封收件者]和[郵件標題]三規則12，上述三項規則12之設定必須同時符合，系統才會執行。關於規則12之設定，使用者可指定符合、不符合以及略過不比對其中之一者，亦即使用者可指定[信封寄件者]或[信封收件者]，不填寫則表示所有；亦可選擇比對或略過[郵件標題]，且所有規則12間之關聯性為[和]，必須全部符合該些設定才視為成立條件，系統才會執行以採取適當之行動。同樣地，在設定該等郵件政策10時，係可依需求指定符合、不符合以及略過不比對其中之一者。

在設定好郵件政策10及其規則12後，當代理器(Agent)收到一電子郵件時，係以該等郵件政策10逐一對該電子郵件之郵件傳輸資料進行比對，所比對之郵件傳輸資料係指包含有該電子郵件所屬之信封資訊及標題資訊，甚至是內容及附加檔案，端視所預先設定之郵件政策10及其規則12而定，藉以驗證該電子郵件之行為是否符合該等郵件政策10，並依據驗證結果採取一相對應之阻擋/傳送的行動。

其中，該等郵件政策10及其規則12係可由設定者定義成垃圾郵件之行為或免檢郵件之行為，以判斷一電子郵件是否為垃圾郵件，或判斷一電子郵件是否為免檢之禮遇郵件。當該等郵件政策10及其規則12係定義成垃圾郵件之行為，則此時代理器在收到電子郵件而驗證該電子郵件時，係包括下列步驟：以該等郵件政策10逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符

五、發明說明（6）

合該等郵件政策，若是，則代表該電子郵件為垃圾郵件，進而阻擋該電子郵件；若否，則傳送該電子郵件。

相反地，當該等郵件政策10及其規則12係定義成免檢郵件之行為時，則此時代理器在收到電子郵件而以該等郵件政策10逐一對其郵件傳輸資料進行比對後，若該電子郵件之行為符合該等郵件政策10，則代表該電子郵件為免檢郵件，故傳送該電子郵件；若不符合，則阻擋該電子郵件。藉由免檢郵件之設定，係可設定企業門禁政策之免檢禮遇對象，免檢郵件之發出者可為母公司、子公司、重要客戶、往來廠商、訂閱電子報的網域名稱或固定IP者，或者為企業允許內部成員於企業外部存取郵件(例如：員工家中、協力廠商、特殊駐外點等)，凡屬企業免檢禮遇對象則優先放行。

由於代理器所採取之行動係依據郵件政策之設定內容之呈現相反結果，亦即當郵件政策係模擬垃圾郵件行為時，則在符合政策時係阻擋郵件，而當郵件政策係模擬免檢郵件行為時，則在符合政策時係放行郵件，其工作原理相同，故以下僅針對垃圾郵件之管控流程來詳細說明，關於免檢郵件之模擬則不再贅述。

其中，以垃圾郵件之管控為例，在驗證該電子郵件是否符合該等郵件政策10時，其詳細之步驟如第三圖所示，當該代理器收到該電子郵件時，係以第一郵件政策對電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第一郵件政策，若符合則進行步驟S12，即允許該電子郵

五、發明說明（7）

件可傳送出去，若不符合則進行步驟S14。

在步驟S14中，代理器係繼續以第二郵件政策追溯電子郵件之行徑，以判斷其是否符合該第二郵件政策，若符合則允許該電子郵件可傳送出去，即進行步驟S12；若不符合，則進行步驟S16，繼續以下一郵件政策追溯該電子郵件之行徑，直到最後一個郵件政策用完為止；當用到最後一郵件政策，如步驟S18所示，以最後一郵件政策驗證該電子郵件時，若該電子郵件符合此郵件政策，則進行步驟S12，若該電子郵件仍不符合此郵件政策之規則，則可確認該電子郵件確實係不被允許傳送者，此時則進行步驟S20，代理器係採取適當之行動使該電子郵件不被傳送。

其中，當不傳送電子郵件時，此時之處理方式係可拒絕接收電子郵件且回傳一錯誤代碼和錯誤訊息，或直接刪除該電子郵件，而此不傳送電子郵件之處理方式亦可在預設郵件政策時，即加以指定。

另外，在第三圖之之流程中，每當在利用其中一郵件政策對電子郵件之郵件傳輸資料進行驗證時，其詳細步驟可參第二圖所示，茲說明如下：

(a)首先，以第一規則對電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第一規則，若是則進行步驟(b)，若否則進行步驟(c)；

(b)以第二規則繼續對該電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第二規則，若否則進行步驟(c)，若是則繼續以下一規則追溯該電子郵件之行徑，

五、發明說明 (8)

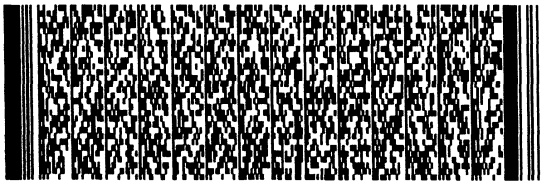
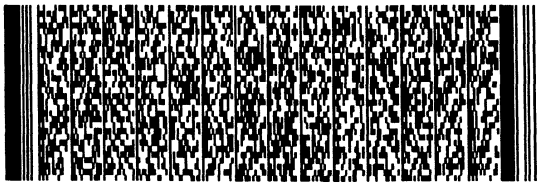
直到最後一規則用完為止，且依據所使用之最後一規則之驗證結果決定該電子郵件是否符合該郵件政策，若符合則允許該電子郵件可傳送出去，若不符合則進行步驟(c)；以及

(c)繼續以下一郵件政策中之規則來追溯該電子郵件之行徑，以判斷其是否符合此郵件政策，若符合，則允許該電子郵件可傳送出去，若不符合，則以又下一郵件政策繼續追溯該電子郵件之行徑，直到最後一郵件政策用完為止。

因此，本發明藉由掌握電子郵件的全面性重要資訊進行管制，只要正確設定郵件行為及其處理方式，俾能有效達成管制電子郵件之目的。

由於垃圾郵件係以匿名、偽造、濫發或非法(變動資訊或隱藏資訊等)等行逕傳送電子郵件者，不同於廣告郵件可追溯來源地並有權利經正式管道取消訂閱，如果能證實寄件者刻意以匿名、偽造、濫發或非法(變動資訊或隱藏資訊等)行逕傳送電子郵件，即可辨識其為可能的垃圾郵件濫發者。

上述郵件政策係可用以判斷該電子郵件是否為垃圾郵件，而判斷依據係藉由判斷該電子郵件是否有反常行為，該反常行為通常為匿名、偽造、濫發或非法等行為，若經驗證後，發現該電子郵件係有反常行為，則可判定其為垃圾郵件。舉例來說，匿名行為之態樣可能有標題資訊不明；寄件者主機與回覆信箱主機不同；或回覆信箱主機為

五、發明說明 (9)

網路服務供應商(ISP)主機等行為。偽造行為則係來源地主機為外部網域，但寄件者地址偽造成內部主機；或網域的網域名稱伺服器(DNS)不正確等行為者。濫發行為則係寄送方式異常且變動頻仍者。非法行為則係回覆地址為租賃主機者。

其中，關於匿名行為之解析，本發明之方法除了可判別上述列舉之匿名行為者，更可判別機器、駭客或人為發送之電子子件，例如判別郵政局長(Postmaster)、郵件核心(mailerdemon)或郵件列表伺服器(Listserver)等所發送之電子郵件。

本發明利用郵件行為解析以管控電子郵件之方法通常係在一代理器內實施，較常使用者為郵件傳送代理器(MTA)，藉以在郵件傳送代理器(MTA)執行階段，利用預設垃圾郵件行為模擬，經由掌握「郵件信封」與「郵件標題」等資訊，以及回溯解析郵件傳輸資料的真假值，得以正確驗證出該行為是否符合「垃圾郵件行為」，其中，郵件傳送代理器(MTA)可為一路由器。

至此，本發明之利用郵件行為解析以管控電子郵件之方法的精神已說明完畢，以下特以三個具體範例來詳細驗證說明本發明之方法，以使熟習此項技術者將可參酌此範例之描述而獲得足夠的知識而據以實施。

範例一：郵件進出控管 — 特定內部使用者僅能傳送電子郵件給特定內部使用者。

五、發明說明（10）

啟用	信封資訊：規則間關聯性為[和]，全部符合才視為成立條件。			
☑	信封寄件者	比對項目 Host	含/非 +	選取名單 特定內部使用
☑	信封收件者	比對項目 Host	含/非 -	選取名單 特定內部使用
郵件標題	○ 比對 ◎ 略過			

啟用	郵件標題：規則間關聯性為[和]，全部符合才視為成立條件。				
☐	比對項目 Header	要件 Element	比對方式 Method	含/非 +/-	選取名單或自行輸寫
符合條件	◎ 符合 ○ 不符合 上述政策者，依照下述處理方式執行。				
處理方式	◎ 拒絕接收，回傳錯誤代碼和錯誤訊息 ○ 刪除郵件，不回傳錯誤代碼和錯誤訊息 ○ 直接傳送				

範例二：垃圾郵件防堵 — 匿名行為舉例說明，寄件者主機與回覆信箱主機不同。

啟用	信封資訊：規則間關聯性為 [和]，全部符合才視為成立條件。			
☐	信封寄件者	比對項目 EnvelopFrom	含/非 +/-	選取名單
☐	信封收件者	比對項目 EnvelopTo	含/非 +/-	選取名單
郵件標題	◎ 比對 ○ 略過			

啟用	郵件標題：規則間關聯性為 [和]，全部符合才視為成立條件。				
☑	比對項目 From	要件 Host	比對方式 Cache	含/非 +/-	選取名單或自行填寫
☑	比對項目 Return-Path	要件 Host	比對方式 Match Cache	含/非 +/-	選取名單或自行填寫
符合條件	○ 符合 ◎ 不符合 上述政策者，依照下述處理方式執行。				
處理方式	◎ 拒絕接收，回傳錯誤代碼和錯誤訊息 ○ 刪除郵件，不回傳錯誤代碼和錯誤訊息 ○ 直接傳送				

範例三：垃圾郵件防堵 — 偽造行為舉例說明，來源地主機為外部網域，寄件者地址偽造成內部主機

五、發明說明（11）

啟用	信封資訊：規則間關聯性為 [和]，全部符合才視為成立條件。			
☐	信封寄件者	比對項目	含/非	選取名單
		EnvelopFrom	+/-	
☐	信封收件者	比對項目	含/非	選取名單
		EnvelopTo	+/-	

郵件標題 ◎ 比對 ○ 略過				
啟用	郵件標題：規則間關聯性為 [和]，全部符合才視為成立條件。			
	比對項目	要件	比對方式	含/非	選取名單或自行填寫
☑	Sender	Sender Host	Domain	-	內部主機
	比對項目	要件	比對方式	含/非	選取名單或自行填寫
☑	From	Sender Host	Domain	+	內部主機
符合條件	◎ 符合 ○ 不符合 上述政策者，依照下述處理方式執行。				
處理方式	◎ 拒絕接收，回傳錯誤代碼和錯誤訊息 ○ 刪除郵件，不回傳錯誤代碼和錯誤訊息 ○ 直接傳送				

因此，本發明利用電子郵件之郵件特性及傳輸原則，將一電子郵件的「郵件信封」與「郵件標題」等郵件傳輸資料的真假值加以解析，且經由反覆回溯驗證，以精確歸納與演繹出郵件之行為是否為預設之郵件政策所允許者，進而達成管控電子郵件進出以及垃圾郵件防堵之作用。故本發明不僅可精確管控郵件，有效防堵垃圾郵件，以提高網路安全，且可節省網路頻寬、系統資源與硬碟空間，以達成增進郵件通訊效率及節省營運成本之功效。

以上所述係藉由實施例說明本發明之特點，其目的在使熟習該技術者能瞭解本發明之內容並據以實施，而非限定本發明之專利範圍，故，凡其他未脫離本發明所揭示之精神所完成之等效修飾或修改，仍應包含在以下所述之申請專利範圍中。

圖式簡單說明

圖式說明：

第一圖為本發明解析郵件行為以管控電子郵件的方法示意圖。

第二圖為本發明在利用一郵件政策中之數規則對電子郵件進行驗證時之詳細流程示意圖。

第三圖為本發明以預設之郵件政策驗證電子郵件之流程圖。

圖號說明：

10 郵件政策

12 規則

四、中文發明摘要　（發明名稱：利用郵件行為解析以管控電子郵件之方法）

本發明提供一種利用郵件行為解析以管控電子郵件之方法，其係先利用郵件之信封資訊及標題資訊預設複數不同之郵件政策，當代理器(Agent)收到一電子郵件時，係以該等郵件政策逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符合該等郵件政策，並依據驗證結果採取一相對應的行動；其中當郵件政策係設定垃圾郵件之行為時，若符合政策，則阻擋該電子郵件，當郵件政策係設定免檢郵件之行為時，若符合政策，則傳送該電子郵件。因此本發明可達成郵件進出控管及垃圾郵件防堵之目的，且有效增進郵件通訊效率、節省營運成本及提高網路安全。

（一）、本案代表圖為：第一圖

（二）、本案代表圖之元件代表符號簡單說明：

10　郵件政策

六、英文發明摘要　（發明名稱：）

四、中文發明摘要　（發明名稱：利用郵件行為解析以管控電子郵件之方法）

12　規 則

六、英文發明摘要　（發明名稱：）

六、申請專利範圍

1. 一種利用郵件行為解析以管控電子郵件之方法，包括下列步驟：

利用郵件之信封資訊及標題資訊設定複數不同之郵件政策；以及

當代理器(Agent)收到一電子郵件時，係以該等郵件政策逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符合該等郵件政策，並依據驗證結果採取一相對應之阻擋/傳送的行動。

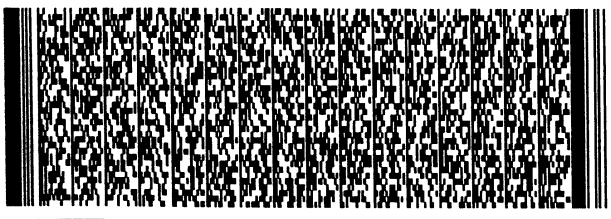
2. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該等郵件政策係用以判斷該電子郵件是否為垃圾郵件，則此時該代理器在收到該電子郵件而驗證該電子郵件之方法係包括下列步驟：

以該等郵件政策逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符合該等郵件政策，若是，則代表該電子郵件為垃圾郵件，進而阻擋該電子郵件；以及

若否，則傳送該電子郵件。

3. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該等郵件政策係屬於門禁政策，用以定義免檢郵件之行為，則此時該代理器在收到該電子郵件而驗證該電子郵件之方法係包括下列步驟：

以該等郵件政策逐一對該電子郵件之郵件傳輸資料進行比對，以驗證該電子郵件之行為是否符合該等郵件政策，若是，則代表該電子郵件為免檢郵件，進而傳送該電子郵



六、申請專利範圍

件；以及

若否，則阻擋該電子郵件。

4. 如申請專利範圍第3項所述之利用郵件行為解析以管控電子郵件之方法，其中，該免檢郵件之發出者係包括母公司、子公司、重要客戶、往來廠商、訂閱電子報的網域名稱以及固定IP者所組成之群組的至少其中之一者。

5. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，在設定該等郵件政策之步驟中，係包括有設定每一該郵件政策之驗證準則，該驗證準則係選自符合、不符合以及略過不比對其中之一者。

6. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該郵件傳輸資料係包含有該電子郵件所屬之信封資訊及標題資訊。

7. 如申請專利範圍第2項所述之利用郵件行為解析以管控電子郵件之方法，其中，驗證該電子郵件是否符合該等郵件政策之垃圾郵件行為的方法更包括下列步驟：

(a)當該代理器收到該電子郵件時，係以第一郵件政策對該電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第一郵件政策，若是則進行步驟(b)，若否則進行步驟(c)；

(b)允許該電子郵件可傳送出去；以及

(c)繼續以第二郵件政策追溯該電子郵件之行徑，以判斷其是否符合該第二郵件政策，若是則進行步驟(b)，若否則繼續藉由下一該郵件政策追溯該電子郵件之行徑，直

六、申請專利範圍

到最後一該郵件政策用完為止，且當該電子郵件仍不符合最後一該郵件政策時，則該代理器係阻擋該電子郵件。

8. 如申請專利範圍第2項所述之利用郵件行為解析以管控電子郵件之方法，其中，每一該郵件政策更包括有複數規則，在利用其中一該郵件政策對該電子郵件之郵件傳輸資料進行驗證時，更包括下列步驟：

(a)以第一規則對該電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第一規則，若是則進行步驟(b)，若否則進行步驟(c)；

(b)以第二規則繼續對該電子郵件之郵件傳輸資料進行真假驗證，以判斷其是否符合該第二規則，若否則進行步驟(c)，若是則繼續以下一該規則追溯該電子郵件之行徑，直到最後一該規則用完為止，且依據所使用之最後一該規則之驗證結果決定該電子郵件是否符合該郵件政策，若是則允許該電子郵件可傳送出去，若否則進行步驟(c)；以及

(c)繼續以下一該郵件政策追溯該電子郵件之行徑，以判斷其是否符合該下一郵件政策，且重複上述(a)、(b)步驟。

9. 如申請專利範圍第8項所述之利用郵件行為解析以管控電子郵件之方法，其中，以每一該規則驗證該電子郵件之驗證準則係選自符合、不符合以及略過不比對其中之一者，且該驗證準則係在設定該等郵件政策之步驟中所設定者。

六、申請專利範圍

10. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該等郵件政策係用以判斷該電子郵件是否有反常行為，該反常行為係包含有選自匿名、偽造、濫發及非法所組成之群組的至少其中之一行為者。

11. 如申請專利範圍第10項所述之利用郵件行為解析以管控電子郵件之方法，其中，該匿名行為係包含有選自標題資訊不明、寄件者主機與回覆信箱主機不同以及回覆信箱主機為網路服務供應商(ISP)主機所組成之群組的至少其中之一行為者。

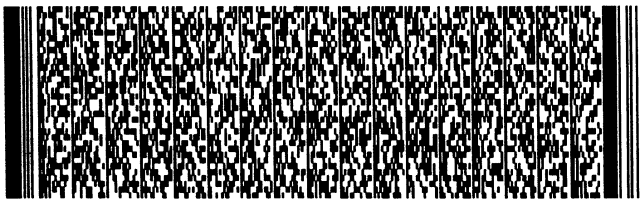
12. 如申請專利範圍第10項所述之利用郵件行為解析以管控電子郵件之方法，其中，該偽造行為係包含有來源地主機為外部網域但寄件者地址偽造成內部主機以及網域的網域名稱伺服器(DNS)不正確其中之一行為者。

13. 如申請專利範圍第10項所述之利用郵件行為解析以管控電子郵件之方法，其中，該濫發行為係包含有寄送方式異常且變動頻仍之行為者。

14. 如申請專利範圍第10項所述之利用郵件行為解析以管控電子郵件之方法，其中，該非法行為係包含有回覆地址為租賃主機之行為者。.

15. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，更可利用郵件之內容及附加檔案作為該等郵件政策之設定內容。

16. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該代理器為一郵件傳送代理器



六、申請專利範圍

(MTA)。

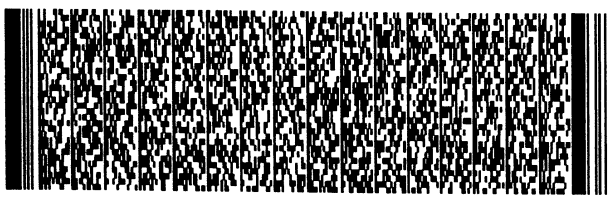
17. 如申請專利範圍第16項所述之利用郵件行為解析以管控電子郵件之方法，其中，該郵件傳送代理器(MTA)可為一路由器。

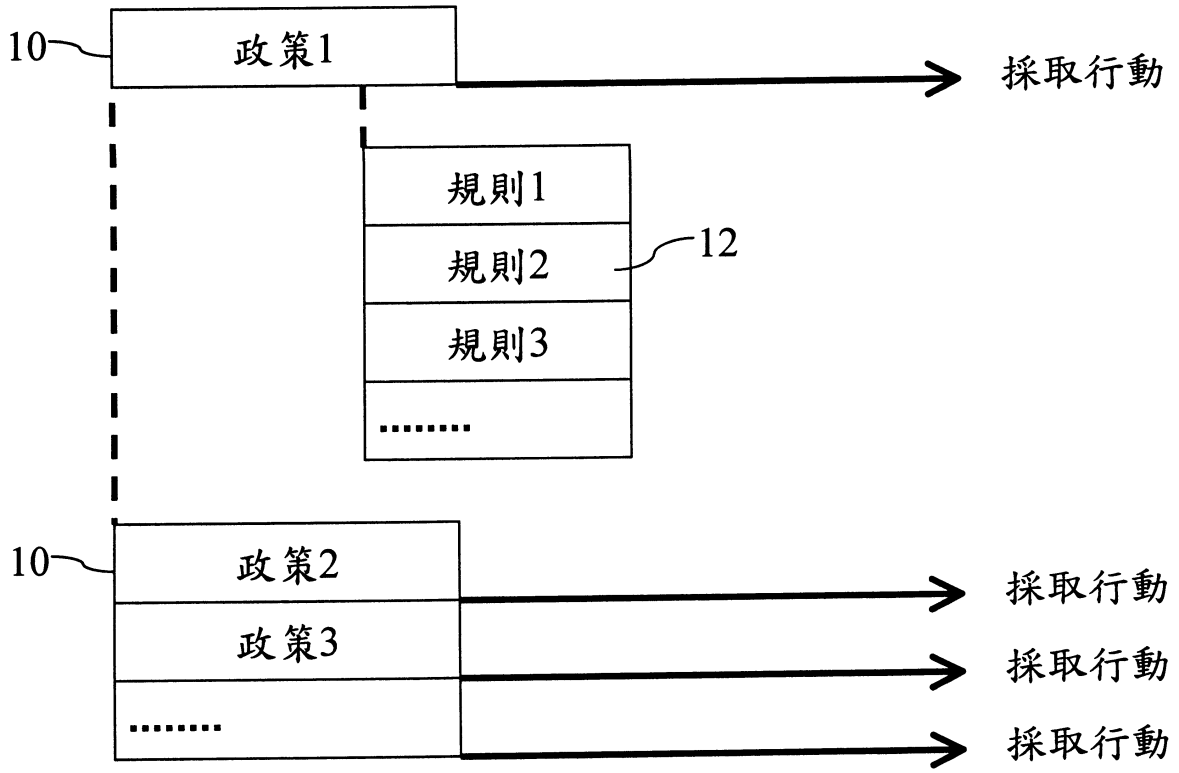
18. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，該信封資訊係選自寄件者帳號、收件者帳號、收件者主機地址、寄件者主機地址、回覆地址、網域名稱伺服器(DNS)及電子郵戳所組成之群組的至少其中之一者。

19. 如申請專利範圍第18項所述之利用郵件行為解析以管控電子郵件之方法，其中，該電子郵戳之提供者係選自發信端伺服器、局端伺服器以及聯網路服務提供者(ISP)伺服器所組成之群組的至少其中之一者。

20. 如申請專利範圍第1項所述之利用郵件行為解析以管控電子郵件之方法，其中，阻擋該電子郵件之處理方式係選自拒絕接收該電子郵件、刪除該電子郵件其中之一方式者。

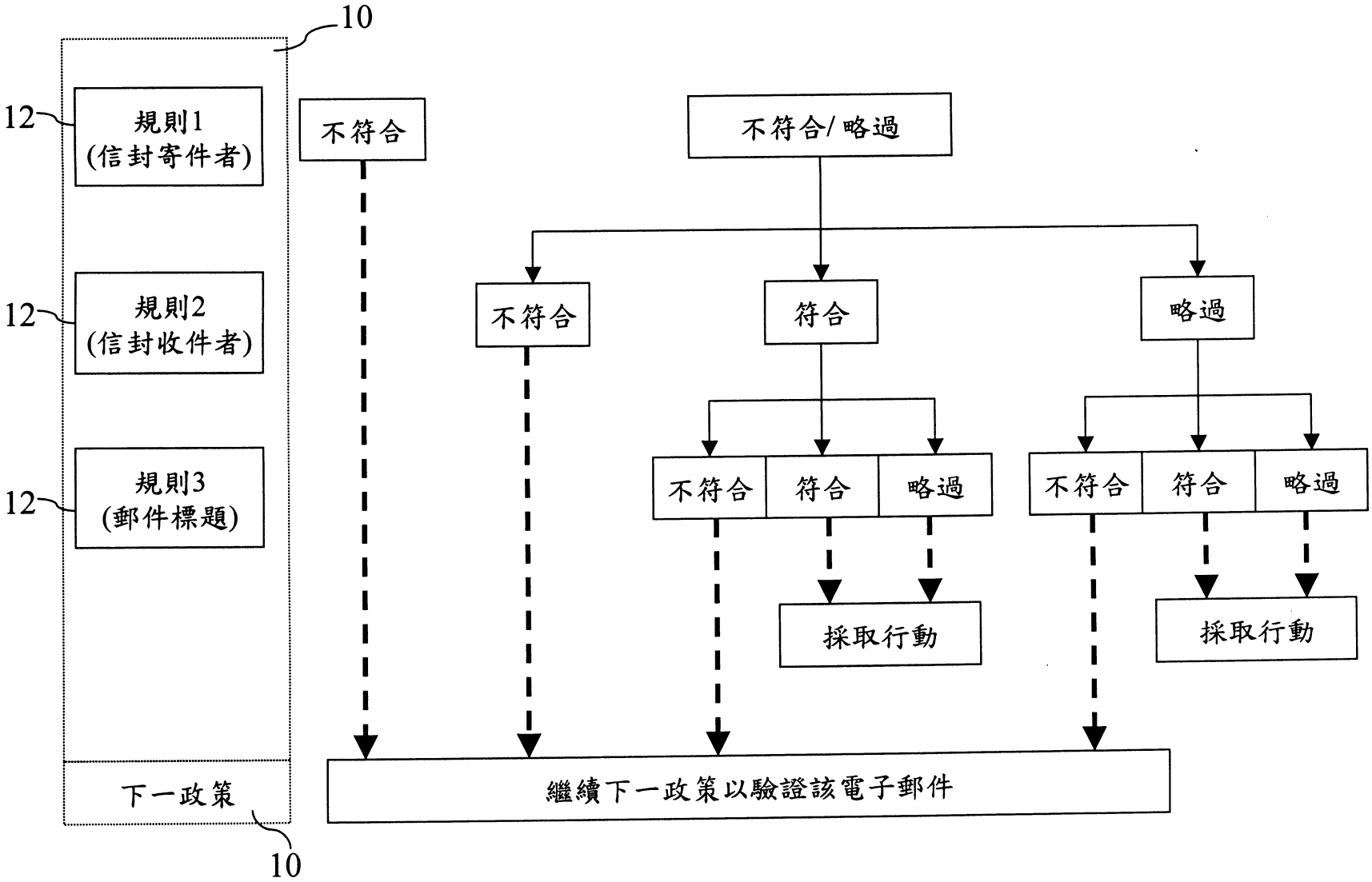
21. 如申請專利範圍第20項所述之利用郵件行為解析以管控電子郵件之方法，其中，當拒絕接收該電子郵件時，係同時回傳一錯誤代碼和錯誤訊息。





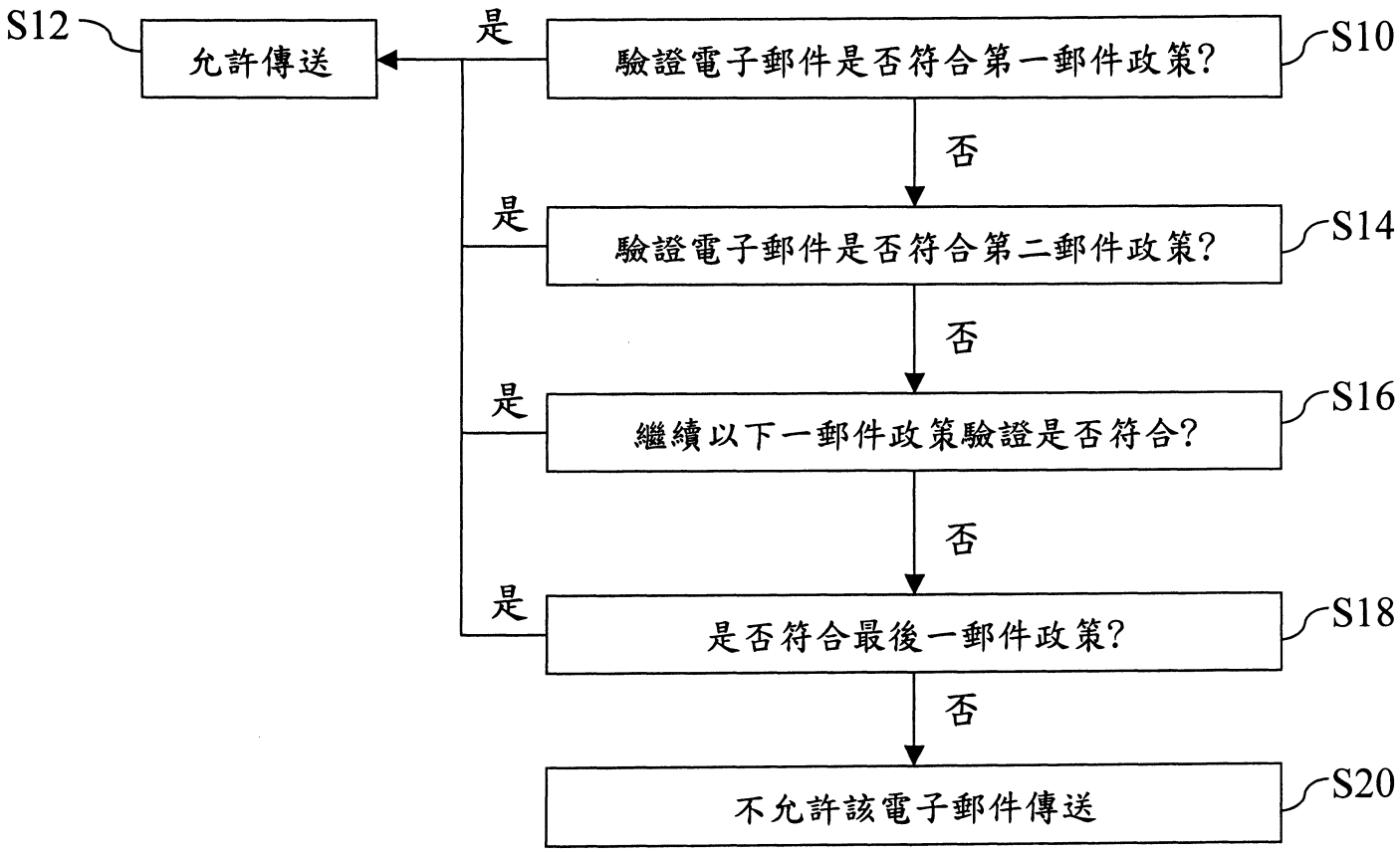
第一圖

200415458



第二圖

200415458



第三圖

200415458

P3 4 2

年　月　日　修正

申請日期： 93-3-26	IPC分類 G06F11/30
申請案號： 93108239	

(以上各欄由本局填註)

發明專利說明書 200415458

一、發明名稱	中 文	利用郵件行為解析以管控電子郵件之方法
	英 文	
二、發明人(共1人)	姓 名(中文)	1. 鄭志文
	姓 名(英文)	1.
	國 籍(中英文)	1. 中華民國 TW
	住居所(中 文)	1. 新竹縣竹北市縣政六路58號4樓
	住居所(英 文)	1.
三、申請人(共1人)	名稱或姓 名(中文)	1. 鄭志文
	名稱或姓 名(英文)	1.
	國 籍(中英文)	1. 中華民國 TW
	住居所(營業所)(中 文)	1. 新竹縣竹北市縣政六路58號4樓 (本地址與前向貴局申請者不同)
	住居所(營業所)(英 文)	1.
	代表人(中文)	1.
	代表人(英文)	1.