(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201427366 A
(43)公開日： 中華民國 103 (2014) 年 07 月 01 日

(21)申請案號：101151161 (22)申請日： 中華民國 101 (2012) 年 12 月 28 日
(51)Int. Cl.： *H04L9/12 (2006.01)* *G06F21/45 (2013.01)*
(71)申請人：萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國
(72)發明人：余盈鋐 YU, YING HUNG (TW) ；蔡亞軒 TSAI, WESLEY YH (TW) ；哈里哈藍瑪哈德凡 HARIHARAN, MAHADEVAN (IN)
(74)代理人：蔡玉玲
申請實體審查：有 申請專利範圍項數：10 項 圖式數：4 共 22 頁

(54)名稱

企業網路中為了資料外洩保護而解密檔案的方法與資訊裝置

METHOD AND APPLIANCE OF DECRYPTING FILES FOR DATA LEAKAGE PROTECTION IN AN ENTERPRISE NETWORK

(57)摘要

揭示一種企業網路中解密加密檔案的電腦實施方法，包含：收集密碼模組辨識在終端進行一檔案加密程序所輸入之一密碼，並儲存該密碼；資料外洩保護模組接收一加密檔案；以及該資料外洩保護模組嘗試以該密碼對該加密檔案進行解密。

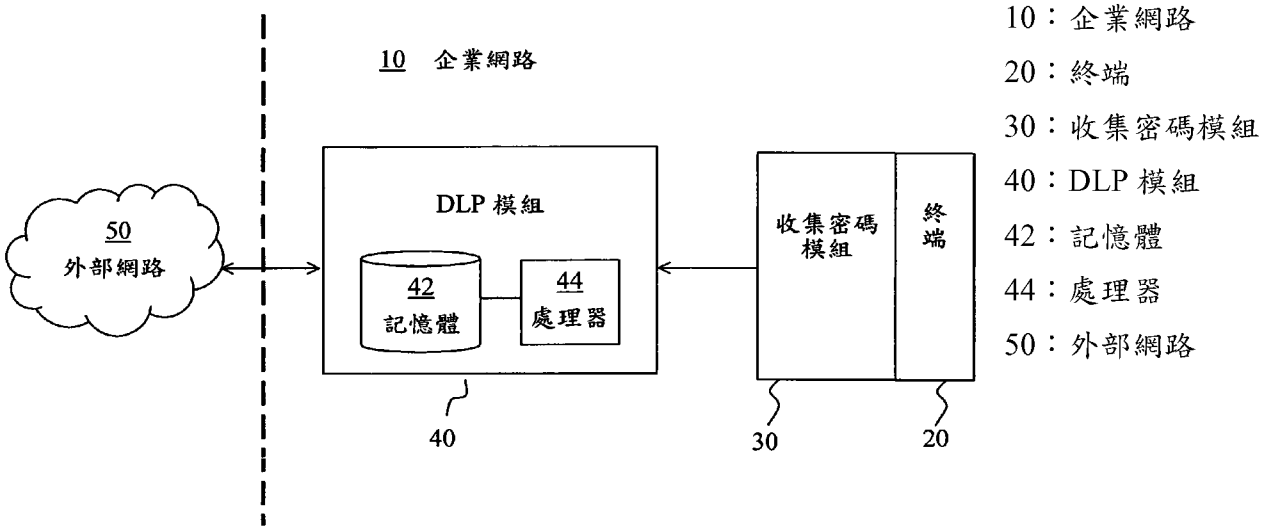

圖 1

201427366

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101151161

※申請日：101年12月28日　　※IPC分類：H04L 9/12 (2006.01)
G06F 21/45 (2013.01)

一、發明名稱：（中文/英文）

企業網路中為了資料外洩保護而解密檔案的方法與資訊裝置

METHOD AND APPLIANCE OF DECRYPTING FILES FOR DATA LEAKAGE PROTECTION IN AN ENTERPRISE NETWORK

二、中文發明摘要：

揭示一種企業網路中解密加密檔案的電腦實施方法，包含：

收集密碼模組辨識在終端進行一檔案加密程序所輸入之一密碼，並儲存該密碼；

資料外洩保護模組接收一加密檔案；以及該資料外洩保護模組嘗試以該密碼對該加密檔案進行解密。

三、英文發明摘要：

A method of decrypting an encrypted file within an enterprise network is provided. The method includes the following steps:

identifying by a password colleting module an password inputted in a file encryption procedure at a terminal and storing the password;

receiving an encrypted file by a data leakage protection (DLP) module; and

attempting to decrypt the encrypted file using the password by the DLP module.

四、指定代表圖：

(一)本案指定代表圖為：圖 1。

(二)本代表圖之元件符號簡單說明：

10	企業網路
20	終端
30	收集密碼模組
40	DLP 模組
42	記憶體
44	處理器
50	外部網路

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無。

六、發明說明：

【發明所屬之技術領域】

本發明係關於企業的資料外洩保護，特別是為了資料外洩保護的需要而解密加密檔案以進行檢查。

【先前技術】

企業為了確保機密資料不會經由連外的網際網路等電子通訊方式而外洩，會設置有資料外洩保護(Data Leakage Protection、DLP)機制，以檢查對外的通訊內容中是否含有機密資料。對此可參考 Check Point Software Technologies Ltd. 的產品 Check Point DLP Software Blade。

另一方面，為了進行上述的 DLP 檢查，當通訊內容中含有加密檔案時，則必須對加密檔案進行解密才能檢查。現有利用暴力破解(Brute-force)的方式來嘗試解密加密檔案，但可想見地此方式相當耗時。另外也有藉由剖析(parse)電子郵件內容來建立暴力破解方式所需要的字典，對此可參考美國專利公開號 US 2012/0216046，在此以引用的方式併入本文。

【發明內容】

本發明一方面即在於：為了在企業網路中進行 DLP 檢查，預先收集企業網路內的終端進行加密程序所輸入的密碼，加以儲存收集為密碼候選名單，而當日後需要對加密檔案進行解密時，則可根據此密碼候選名單嘗試解密。

由於要送到企業網路之外的加密檔案，大部分都是在企

業網路內的終端完成加密程序，因此透過此方式，首先可大幅提高密碼的正確性，而不需要暴力破解方式盲目地嘗試解密。

另一方面，一般來說，企業網路中使用者所能設想到作為加密使用的密碼數量相對有限。因此相較於暴力破解方式所使用的字典，藉由本發明所收集的密碼候選名單短小的多。可想見地，在嘗試解密的過程中，使用本發明所產生的密碼候選名單會比使用字典的方式節省非常多的時間，因此也減少服務中斷(service interruption)的時間，而可達成即時的DLP檢查。

本發明另一方面即在於：藉由監控企業網路中終端所執行的特定應用程式(例如 7-Zip 或是 Microsoft Word)以及該應用程式所進行的檔案加密程序，可有效地辨識使用者所輸入的密碼。透過此方式，可不需要全程監控使用者在終端上的所有動作或輸入，除了可避免侵犯的隱私問題，亦可大幅降低所需的系統資源。

根據本發明一實施例，一種在企業網路中收集加密檔案的解密密碼的電腦實施方法，該方法包含：

- 監視在終端所執行的應用程式；
- 因應該終端執行一預定應用程式，開始監視該預定應用程式所進行的程序；以及
- 因應該預定應用程式進行該一檔案加密程序，開始辨識使用者為該檔案加密程序所輸入之一密碼。

5

根據本發明另一實施例，一種在企業網路中解密加密檔案的電腦實施方法，該方法包含：

- 從一終端接收一加密檔案；以及
- 嘗試以上述在企業網路中收集加密檔案的解密密碼的電腦實施方法所取得之該密碼對該加密檔案進行解密。

根據本發明另一實施例，一種在企業網路中解密加密檔案的電腦實施方法，該方法包含：

- 收集密碼模組辨識在終端進行一第一檔案加密程序所輸入之一第一密碼，並儲存該第一密碼；
- 資料外洩保護模組接收一加密檔案；以及
- 資料外洩保護模組嘗試以該第一密碼對該加密檔案進行解密。

在本發明其他實施例中，更提出可實行上述方法之資訊設備以及電腦可讀媒體或電腦程式產品。

本說明書中所提及的特色、優點、或類似表達方式並不表示，可以本發明實現的所有特色及優點應在本發明之任何單一的具體實施例內。而是應明白，有關特色及優點的表達方式是指結合具體實施例所述的特定特色、優點、或特性係包含在本發明的至少一具體實施例內。因此，本說明書中對於特色及優點、及類似表達方式的論述與相同具體實施例有關，但亦非必要。

此外，可以任何合適的方式，在一或多個具體實施例中結合本發明所述特色、優點、及特性。相關技術者應明白，在沒有特定具體實施例之一或多個特定特色或優點的情況下，亦可實施本發明。在其他例子中應明白，特定具體實施例中的其他特色及優點可能未在本發明的所有具體實施例中出現。

參考以下說明及隨附申請專利範圍或利用如下文所提之本發明的實施方式，即可更加明瞭本發明的這些特色及優點。

【實施方式】

本說明書中「一具體實施例」或類似表達方式的引用是指結合該具體實施例所述的特定特色、結構、或特性係包括在本發明的至少一具體實施例中。因此，在本說明書中，「在一具體實施例中」及類似表達方式之用語的出現未必指相同的具體實施例。

熟此技藝者當知，本發明可實施為資訊設備、方法或作為電腦程式產品之電腦可讀媒體。因此，本發明可以實施為各種形式，例如完全的硬體實施例、完全的軟體實施例（包含韌體、常駐軟體、微程式碼等），或者亦可實施為軟體與硬體的實施形式，在以下會被稱為「電路」、「模組」或「系統」。此外，本發明亦可以任何有形的媒體形式實施為電腦程式產品，其具有電腦可使用程式碼儲存於其上。

一個或更多個電腦可使用或可讀取媒體的組合都可以利用。舉例來說，電腦可使用或可讀取媒體可以是（但並不限於）電子的、磁的、光學的、電磁的、紅外線的或半導體的系統、裝置、

設備或傳播媒體。更具體的電腦可讀取媒體實施例可以包括下列所示（非限定的例示）：由一個或多個連接線所組成的電氣連接、可攜式的電腦磁片、硬碟機、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM 或快閃記憶體)、光纖、可攜式光碟片（CD-ROM）、光學儲存裝置、傳輸媒體（例如網際網路(Internet)或內部網路(intranet)之基礎連接）、或磁儲存裝置。需注意的是，電腦可使用或可讀取媒體更可以為紙張或任何可用於將程式列印於其上而使得該程式可以再度被電子化之適當媒體，例如藉由光學掃描該紙張或其他媒體，然後再編譯、解譯或其他合適的必要處理方式，然後可再度被儲存於電腦記憶體中。在本文中，電腦可使用或可讀取媒體可以是任何用於保持、儲存、傳送、傳播或傳輸程式碼的媒體，以供與其相連接的指令執行系統、裝置或設備來處理。電腦可使用媒體可包括其中儲存有電腦可使用程式碼的傳播資料訊號，不論是以基頻(baseband)或是部分載波的型態。電腦可使用程式碼之傳輸可以使用任何適體的媒體，包括（但並不限於）無線、有線、光纖纜線、射頻(RF)等。

用於執行本發明操作的電腦程式碼可以使用一種或多種程式語言的組合來撰寫，包括物件導向程式語言（例如 Java、Smalltalk、C++或其他類似者）以及傳統程序程式語言（例如 C 程式語言或其他類似的程式語言）。程式碼可以獨立軟體套件的形式完整的於使用者的電腦上執行或部分於使用者的電腦上執行，或部分於使用者電腦而部分於遠端電腦。

於以下本發明的相關敘述會參照依據本發明具體實施例之資

訊設備、方法及電腦程式產品之流程圖及／或方塊圖來進行說明。當可理解每一個流程圖及／或方塊圖中的每一個方塊，以及流程圖及／或方塊圖中方塊的任何組合，可以使用電腦程式指令來實施。這些電腦程式指令可供通用型電腦或特殊電腦的處理器或其他可程式化資料處理裝置所組成的機器來執行，而指令經由電腦或其他可程式化資料處理裝置處理以便實施流程圖及／或方塊圖中所說明之功能或操作。

這些電腦程式指令亦可被儲存在電腦可讀取媒體上，以便指示電腦或其他可程式化資料處理裝置來進行特定的功能，而這些儲存在電腦可讀取媒體上的指令構成一製成品，其內包括之指令可實施流程圖及／或方塊圖中所說明之功能或操作。

電腦程式指令亦可被載入到電腦上或其他可程式化資料處理裝置，以便於電腦或其他可程式化裝置上進行一系統操作步驟，而於該電腦或其他可程式化裝置上執行該指令時產生電腦實施程序以達成流程圖及／或方塊圖中所說明之功能或操作。

其次，請參照圖 1 至圖 4，在圖式中顯示依據本發明各種實施例的資訊設備、方法及電腦程式產品可實施的架構、功能及操作之流程圖及方塊圖。因此，流程圖或方塊圖中的每個方塊可表示一模組、區段、或部分的程式碼，其包含一個或多個可執行指令，以實施指定的邏輯功能。另當注意者，某些其他的實施例中，方塊所述的功能可以不依圖中所示之順序進行。舉例來說，兩個圖示相連接的方塊事實上亦可以同時執行，或依所牽涉到的功能在某些情況下亦可以依圖示相反的順序執行。此外亦需注意者，每

個方塊圖及／或流程圖的方塊，以及方塊圖及／或流程圖中方塊之組合，可藉由基於特殊目的硬體的系統來實施，或者藉由特殊目的硬體與電腦指令的組合，來執行特定的功能或操作。

<系統架構>

圖 1 係簡要顯示應用本發明之企業網路 10 架構圖。企業網路 10 包含終端 20、收集密碼模組 30、以及 DLP 模組 40。終端 20 可實施為可為個人行動裝置(例如 Apple Inc.的產品 iPhone 或是 iPad)或是個人電腦，並可與企業網路 10 之外的外部網路 50 進行通訊，例如檔案傳輸或是發送電子郵件等。此外，圖 1 中雖僅繪示一台終端 20，但應可知本發明並不欲限制終端 20 的數量。

關於收集密碼模組 30 以及 DLP 模組 40 的細節將透過後續圖 2 至圖 4 進一步說明。而除了收集密碼模組 30 以及 DLP 模組 40 之外，企業網路 10 亦針對終端 20 與外部網路 50 的通訊提供現有的資料外洩或是其他資料安全的保護機制(未圖示)，對此可參考 Check Point Software Technologies Ltd.的產品 Check Point DLP Software Blade 或是 International Business Machines Corp. 的產品 Security Network Protection XGS 5000。換言之，本發明可與現有的保護機制，特別是下一代的防火牆產品(Next Generation Firewalls)加以整合。

<收集密碼模組>

收集密碼模組 30 較佳透過軟體的形式實施，例如可以常駐程式(Daemon)的形式在終端 20 上運作，但本發明不限於此，亦可實施為獨立的硬體，例如資訊設備。圖 2 顯示一實施例中，收集密

碼模組 30 以常駐程式的形式收集密碼的方法流程圖。

- 步驟 200：啟動設置於終端 20 上的收集密碼模組 30，以監視終端 20 是否執行一或多個預定應用程式，若判斷為是則進行到後續步驟 202，若否則回到自身。

  在此實施例中，收集密碼模組 30 可與終端 20 的作業系統(例如 WINDOWS 系統中的工作管理員)通訊，以知悉終端 20 上所要執行的應用程式。

  在此步驟前，選擇性地，可預先向收集密碼模組 30 登錄所關注的應用程式，特別是可進行加密程序的應用程式，例如 7-Zip、MICROSOFT WORD、WinRAR、MICROSOFT OUTLOOK 等，因此收集密碼模組 30 可不理會其他未登錄的應用程式，以節省系統資源。

- 步驟 202：收集密碼模組 30 監視該應用程式是否執行一檔案加密程序，若判斷為是則進行到後續步驟 204，若否則回到步驟 200。

  在此實施例中，收集密碼模組 30 可偵測應用程式的處理程序(process)或是圖形使用者介面(GUI)物件的動作(action)，以判斷應用程式當下正在要進行的程序(procedure)。對此可參考 Microsoft 的產品 Spy++。

  特別是一般應用程式在進行檔案加密程序時，都會提供特定的使用者介面訊息或是提示列，要求使用者輸入密

碼，因此收集密碼模組 30 可藉由偵測上述特定的使用者介面訊息或是提示列，來判斷該應用程式正在執行檔案加密程序。

- 步驟 204：收集密碼模組 30 辨識使用者因應應用程式加密程序之要求(例如透過特定使用者介面訊息或是提示列)而輸入的密碼。收集密碼模組 30 辨識密碼的作法可採用紀錄鍵盤(Keystroke tracking)，或是其他習知可偵測使用者輸入的作法。此部份本發明並不欲加以限制。在辨識出密碼後，收集密碼模組 30 可將密碼傳送給 DLP 模組 40 加以儲存為密碼候選表 PT。然後流程可結束或是回到步驟 200 或步驟 202，而可反覆執行多次，以獲得多組密碼並儲存至密碼候選表 PT。

  在另一實施例中，收集密碼模組 30 除了辨識密碼外，更進一步辨識與此密碼相關的元資料(meta data)，例如，但不限於，檔案加密的時間、應用程式的名稱、加密檔案的類型(例如附檔名)、加密檔案的雜湊值、應用程式登入的使用者 ID 等。收集密碼模組 30 並將上述的元資料與密碼一同傳送給傳送給DLP模組40加以儲存至密碼候選表 PT，如圖 3 所示。更多的細節將於後續描述。

＜DLP 模組>

DLP 模組 40 係與終端 20 以及收集密碼模組 30 共同設置於企業網路 10 中，彼此可藉由企業網路 10 所提供的網路連線彼此通訊，包括固定連接之區域網路(LAN)或廣域網路(WAN)連線等，亦

不限於有線無線等各種連接方式。

DLP 模組 40 較佳透過資訊設備的形式實施，例如可與現有的無線網路橋接器(Access Point)、路由器(Router)、交換器(Switch)、閘道器(Gateway)、防火牆(firewall)裝置、代理伺服器(proxy)、或是侵偵測防禦(Intrusion Prevention System (IPS))裝置加以整合。

以資訊設備形式實現的 DLP 模組 40 具有記憶體 42 與處理器 44。記憶體 42 可為電腦磁片、硬碟機、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM 或快閃記憶體)、光碟片、光學儲存裝置、或磁儲存裝置。記憶體 42 用以存放程式碼以及例如圖 3 所示的密碼候選表 PT，而處理器 44 係存取記憶體 42 之程式碼與密碼候選表 PT，以執行預定的程式，如後續圖 4 之說明。熟此技藝者應可知，圖 1 中所述 DLP 模組 40 的硬體可以依照不同的實施例而有各種變化。亦有其它的內部硬體或週邊裝置，例如快閃唯讀記憶體(Flash ROM)、等效的非揮發記憶體、或光碟機等等，可以附加或取代圖 1 所示的硬體。

但在另一實施例中，亦可以應用程式的外掛(plugin)模組在終端 20 上運作，對此可參考現有網頁瀏覽器或是文書處理程式的外掛模組的運作方式，在此不予贅述。

以下圖 4 係顯示一實施例中，DLP 模組 40 嘗試解密的方法流程圖。需說明的是，以下實施例僅針對單一終端 20 的單一加密檔案的情況加以說明，但應可知，DLP 模組 40 可同時對不同的終端 20 或是同一終端 20 的不同檔案實施以下圖 4 的流程。

- 步驟 400:DLP 模組 40 從終端 20 接收或是攔截一加密檔案，攔截檔案的作法可參考習知的 DLP 或防火牆機制，在此不予贅述。選擇性地，此步驟亦包含辨識出加密檔案的元資料，例如檔案類型、雜湊值、與檔案發送來源的使用者 ID 等。對此可參考 International Business Machines Corp. 的產品 Security Network Protection XGS 5000 或其他下一代的防火牆產品。

- (選擇性)步驟 402：DLP 模組 40 係根據所辨識出加密檔案的元資料，可先初步判斷是否要使用收集密碼模組 30 所收集到的密碼來嘗試解密(例如可透過加密檔案的元資料與收集密碼模組 30 所收集到的密碼的元資料之間的比對)。若是，則進行到步驟 404 進行嘗試解密，若否，則進行到步驟 450 的執行既定規則(policy)，例如拒絕將此加密檔案傳送至外部網路 50，或是發送訊息要求加密檔案的發送者提供密碼。

- 步驟 404:DLP 模組 40 以收集密碼模組 30 所收集到的密碼(參見圖 2 的流程與圖 3 的密碼候選表 PT)嘗試對在步驟 400 所接收到的加密檔案進行解密。較佳地，步驟 404 係即時進行，也就是緊接在步驟 400 之後。

  在此步驟中，若密碼候選表 PT 包含複數組密碼，DLP 模組 40 可進一步對密碼候選表 PT 進行整理與排序(sorting)。圖 3 實施例中所示的密碼候選表 PT 係根據檔案加密的時間先後進行排序，DLP 模組 40 並可計算出各

密碼使用過的次數並加入至密碼候選表 PT 的欄位。在其他實施例中，DLP 模組 40 亦根據使用次數、應用程式名稱、檔案類型、雜湊值、或使用者 ID 進行排序。排序的結果即可作為嘗試解碼的優先順序。

在另一實施例中，DLP 模組 40 係根據加密檔案的元資料與收集密碼模組 30 所收集到的每一組密碼的元資料之間的比對，計算出每一組密碼與加密檔案的相符程度，進而來決定嘗試解碼的優先順序。而 DLP 模組 40 可視實際情況決定相符程度的計算方式，或是可調整元資料中各項目對於相符程度計算的權重，本發明並不欲加以限制。舉例來說，可設定為檔案類型比使用者 ID 貢獻較多的相符程度。

- 步驟 406：若解密成功則流程結束，若所有密碼都無法解密，則進行到步驟 450 執行既定規則(policy)。

在不脫離本發明精神或必要特性的情況下，可以其他特定形式來體現本發明。應將所述具體實施例各方面僅視為解說性而非限制性。因此，本發明的範疇如隨附申請專利範圍所示而非如前述說明所示。所有落在申請專利範圍之等效意義及範圍內的變更應視為落在申請專利範圍的範疇內。

【圖式簡單說明】

為了立即瞭解本發明的優點，請參考如附圖所示的特定具體實施例，詳細說明上文簡短敘述的本發明。在瞭解這些

圖示僅描繪本發明的典型具體實施例並因此不將其視為限制本發明範疇的情況下，參考附圖以額外的明確性及細節來說明本發明，圖式中：

圖 1 為一種依據本發明具體實施例之企業網路示意圖；

圖 2 為依據本發明具體實施例之收集密碼的方法流程圖；

圖 3 為依據本發明具體實施例之密碼候選表 PT；

圖 4 為依據本發明具體實施例之嘗試解密的方法流程圖。

【主要元件符號說明】

10	企業網路
20	終端
30	收集密碼模組
40	DLP 模組
42	記憶體
44	處理器
50	外部網路
PT	密碼候選表

七、申請專利範圍：

1. 一種在企業網路中收集加密檔案的解密密碼的電腦實施方法，該方法包含：

監視在一終端所執行的應用程式；

因應該終端執行一預定應用程式，開始監視該預定應用程式所進行的程序；以及

因應該預定應用程式進行一檔案加密程序，開始辨識使用者為該檔案加密程序所輸入之一密碼。

2. 如請求項 1 所述之方法，其中該辨識步驟更包含：辨識該密碼的元資料。

3. 一種在企業網路中解密加密檔案的電腦實施方法，該方法包含：

從一終端接收一加密檔案；以及

嘗試以如請求項 1 或 2 所述之方法所取得之該密碼對該加密檔案進行解密。

4. 如請求項 3 所述之方法，其中該嘗試解密步驟係即時(real-time)進行。

5. 如請求項 3 所述之方法，其中該接收該加密檔案步驟更包含：辨識該加密檔案的元資料；

其中該嘗試解密步驟更包含：藉由判斷出該加密檔案的元資料與以如請求項 2 所述之方法所取得之密碼的元資料至少部份相符而選取該密碼。

6. 如請求項 3 所述之方法，其中該嘗試解密步驟係包含：以如請求項 1 或 2 所述之方法執行多次所取得之複數組密碼，嘗試對該加密檔案進行解密。

7. 如請求項 6 所述之方法，其中該接收該加密檔案步驟更包含辨識該加密檔案的元資料；
其中該嘗試解密步驟更包含：根據以如請求項 2 所述之方法執行多次所取得之該複數組密碼的元資料，決定嘗試各組密碼的順序。

8. 如請求項 6 所述之方法，其中該接收該加密檔案步驟更包含辨識該加密檔案的元資料；
其中該嘗試解密步驟更包含：分別判斷出該加密檔案的元資料與以如請求項 2 所述之方法執行多次所取得之該複數組密碼的元資料間的相符程度，以決定嘗試各組密碼的順序。

9. 如請求項 3 所述之方法，更包含：
從另一終端接收另一加密檔案；以及
嘗試以如請求項 1 或 2 所述之方法所取得之該密碼對該另一加密檔案進行解密。

10. 一種資訊設備，設置在企業網路中且連結於一終端，該資訊設備包含：
一處理器，係根據一程式碼，執行如請求項 1 至 9 中任一項所述之方法。

八、圖式：

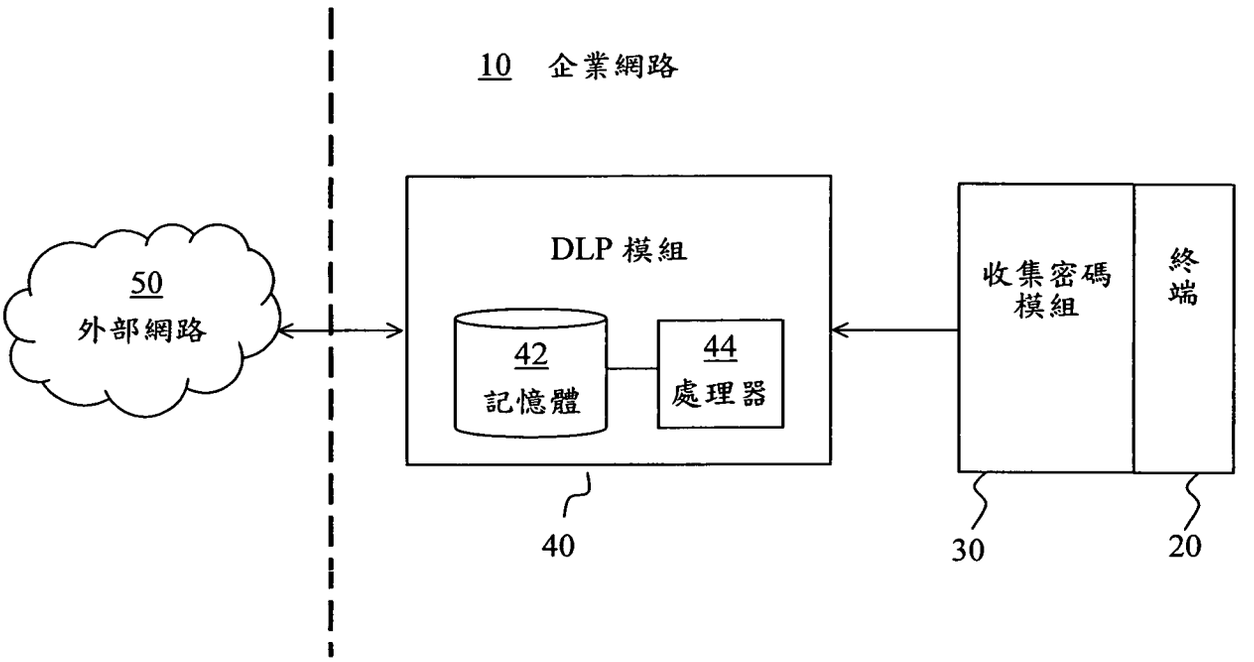

圖 1

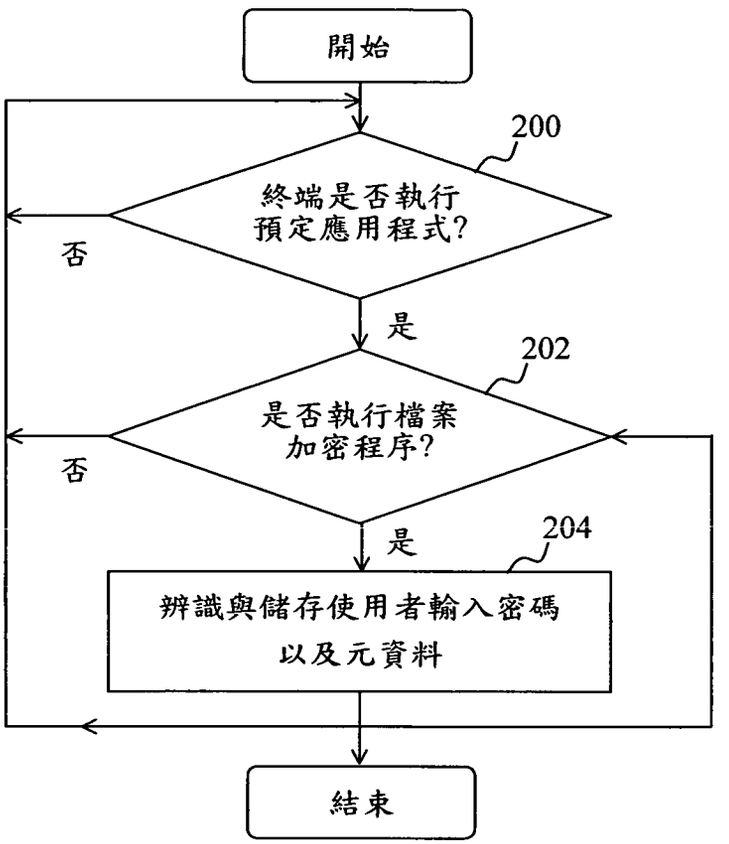
開始
200
終端是否執行
預定應用程式?
否
是
202
是否執行檔案
加密程序?
否
是
204
辨識與儲存使用者輸入密碼
以及元資料
結束

圖 2

No.	密碼	上次時間	使用次數	應用程式	檔案類型	雜湊值	使用者 ID
1	SH9M';Mk	2012.04.20 16:35:02	5	Winzip.exe 7z.exe	zip rar	<*value1*> <*value2*> <*value3*>	wesley@9.191.29.138
2	5hS+N>}1	2012.04.16 15:03:12	3	winword.exe symphony.exe	doc odt	<*value4*>	Hari@workpc.tw.ibm.com
3	J4Ls1q1S	2012.04.08 10:12:23	9	AcroRd32.exe	pdf	<value5>	Edward@9.191.7.5
4	p4wvwt2E	2012.03.28 22:41:05	22	WinZip.exe	zip	<value6> <value7>	Hari@9.191.52.102

圖 3

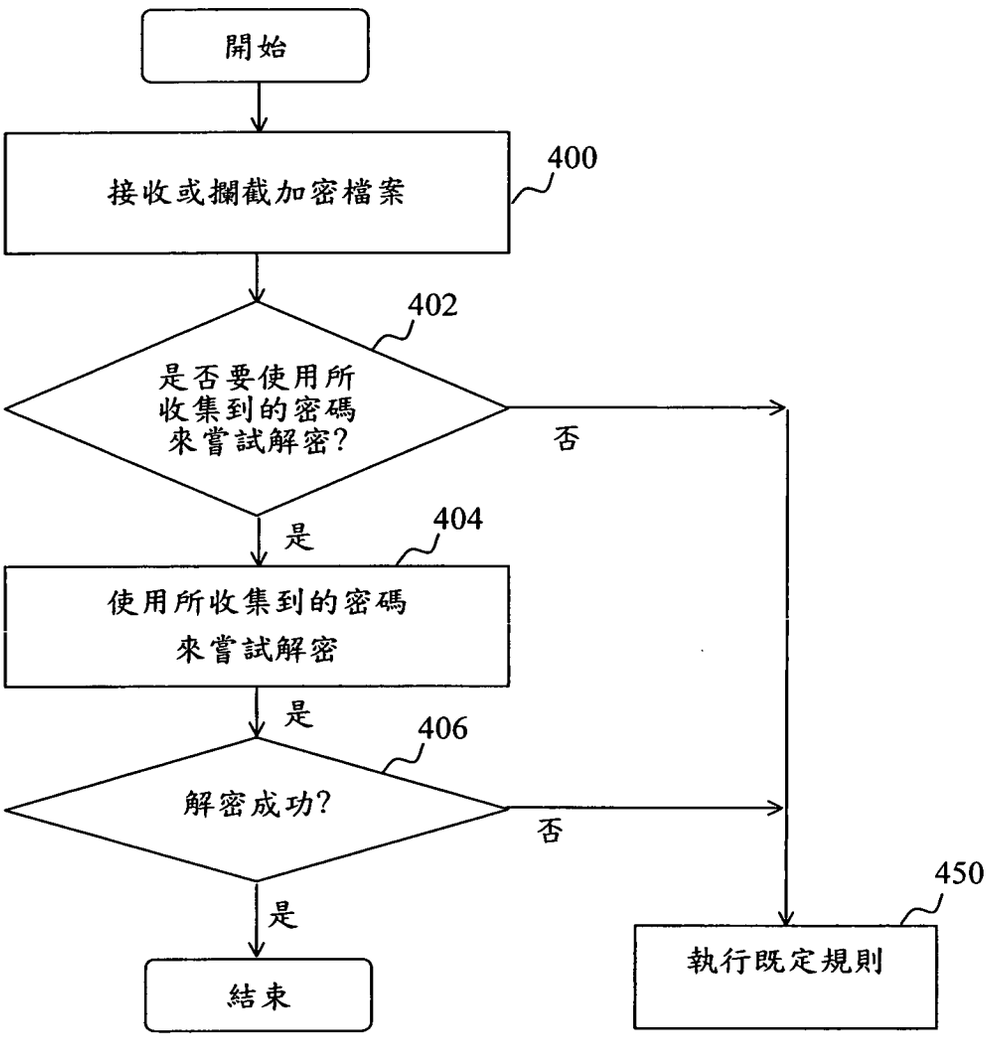
開始
接收或攔截加密檔案
400
402
是否要使用所收集到的密碼來嘗試解密?
否
是
404
使用所收集到的密碼來嘗試解密
是
406
解密成功?
否
是
結束
450
執行既定規則

圖 4