

【11】證書號數：I667589

【45】公告日：中華民國 108 (2019) 年 08 月 01 日

【51】Int. Cl. : G06F21/57 (2013.01)

發明

全 7 頁

【54】名稱：資安聯防方法、系統、電腦程式產品及電腦可讀取紀錄媒體

METHOD, SYSTEM, COMPUTER PROGRAM PRODUCT AND
COMPUTER-READABLE RECORDING MEDIUM OF INFORMATION
SECURITY JOINT DEFENSE MECHANISM

【21】申請案號：106130323 【22】申請日：中華民國 106 (2017) 年 09 月 05 日

【11】公開編號：201913440 【43】公開日期：中華民國 108 (2019) 年 04 月 01 日

【72】發明人：許建隆 (TW) HSU, CHIEN LUNG ; 史素珍 (TW) SHIH, SU JEN ; 彭威陽 (TW) PENG, WEI YANG

【71】申請人：關貿網路股份有限公司 TRADE-VAN INFORMATION SERVICES CO.

臺北市南港區三重路 19 之 13 號 6 樓
許建隆 HSU, CHIEN LUNG
臺北市中山區明水路 607 號 13 樓之 1

【74】代理人：林攸彥

【56】參考文獻：

TW I560569	TW M555500
TW 201122895A	TW 201141155A
US 2003/0046115A1	

資安人編輯部，"資安即國安與日常生活密不可分 關鍵資訊基礎設施保護"，
2017/06/19

審查人員：陳泰龍

【57】申請專利範圍

1. 一種資安聯防方法，包含下列步驟：一環境建置步驟：建置一資安管控伺服端；一聯防建置步驟：於一客戶伺服端安裝一資安訊息收集物件，且該資安訊息收集物件透過一網路連接該資安管控伺服端，並使該資安管控伺服端訊號連接至少一聯防伺服端及一保險伺服端，前述聯防伺服端包含一預警與監控伺服端及一通報與應變伺服端，該資安管控伺服端包含一資安訊息存證模組；一提供服務步驟：使該資安管控伺服端選擇性地與前述聯防伺服端及該保險伺服端交換該資安訊息收集物件取得之一資安訊息，以對前述客戶伺服端提供一聯防服務及一保險服務，該資安訊息存證模組用於同步儲存前述資安訊息，以藉此封存數位證據，以在資安事故發生時，供所述保險伺服端至該資安訊息存證模組調閱存證資料。
2. 如申請專利範圍第 1 項所述之資安聯防方法，其中，前述預警與監控伺服端包含一資訊分享與分析中心(ISAC)、一資安監控中心(SOC)、一資安工具提供單位、一電信服務中心、一資安風險評估單位、一資安檢測團隊之任一或組合。
3. 如申請專利範圍第 2 項所述之資安聯防方法，其中，前述通報與應變伺服端包含一政府資安資訊分享與分析中心(G-ISAC)、一金融資安中心(F-ISAC)、一資安調查鑑識單位、一資安應變團隊之任一或組合。

4. 如申請專利範圍第 1 項所述之資安聯防方法，更包含一資安風險評估步驟：以一風險評估模組依據該資安訊息運算一資安風險特徵模型，並依據該資安風險特徵模型計算一資安風險值。
5. 如申請專利範圍第 4 項所述之資安聯防方法，其中，該資安訊息包含一資安日誌(log)，該資安風險特徵模型包含一管理階層風險值、一基層資安風險值、一資訊管理安全值、一外部威脅值之任一或組合。
6. 如申請專利範圍第 1 項所述之資安聯防方法，將每一個資安訊息轉換為一區塊資料，該區塊資料分別儲存於一私有區塊鏈及一公有區塊鏈，該私有區塊鏈用以供一數位鑑識系統介接而讀取該區塊資料，該公有區塊鏈用以將前述區塊資料提供前述客戶伺服端及前述聯防伺服端讀取。
7. 一種資安聯防系統，用於連接至少一客戶伺服端，前述客戶伺服端安裝一資安訊息收集物件，該資安聯防系統包含：至少一聯防伺服端及一保險伺服端，前述聯防伺服端包含一預警與監控伺服端及一通報與應變伺服端；及一資安管控伺服端，訊號連接前述聯防伺服端及該保險伺服端，並訊號聯接該資安訊息收集物件，該資安管控伺服端包含一資安訊息存證模組，該資安管控伺服端用以選擇性地與前述聯防伺服端及該保險伺服端交換該資安訊息收集物件取得之一資安訊息，以對前述客戶伺服端提供下列服務：一資安預警與監控服務、一資安通報與應變服務、一資安損害保險服務，其中該資安訊息存證模組用於同步儲存前述資安訊息，以藉此封存數位證據，以在資安事故發生時，供所述保險伺服端至該資安訊息存證模組調閱存證資料。
8. 如申請專利範圍第 7 項所述之資安聯防系統，其中，前述預警與監控伺服端包含一資訊分享與分析中心(ISAC)、一資安監控中心(SOC)、一資安工具提供單位、一電信服務中心、一資安風險評估單位、一資安檢測團隊之任一或組合。
9. 如申請專利範圍第 8 項所述之資安聯防系統，其中，前述通報與應變伺服端包含一政府資安資訊分享與分析中心(G-ISAC)、一金融資安中心(F-ISAC)、一資安調查鑑識單位、一資安應變團隊之任一或組合。
10. 如申請專利範圍第 7 項所述之資安聯防系統，更包含一風險評估模組，訊號連接該資安管控伺服端，該風險評估模組用以依據該資安訊息運算一資安風險特徵模型，並依據該資安風險特徵模型計算一資安風險值。
11. 如申請專利範圍第 10 項所述之資安聯防系統，其中，該資安訊息包含一資安日誌(log)，該資安風險特徵模型包含一管理階層風險值、一基層資安風險值、一資訊管理安全值、一外部威脅值之任一或組合。
12. 如申請專利範圍第 7 項所述之資安聯防系統，更包含一存證模組，訊號連接該資安管控伺服端，該存證模組用以將每一個資安訊息轉換為一區塊資料，該區塊資料分別儲存於一私有區塊鏈及一公有區塊鏈，該私有區塊鏈用以供一數位鑑識系統介接而讀取該區塊資料，該公有區塊鏈用以將前述區塊資料提供前述客戶伺服端及前述聯防伺服端讀取。
13. 一種電腦程式產品，內儲一程式，當電腦載入該程式並執行後，可完成如請求項第 1 項至第 6 項中任一項所述之資安聯防方法。
14. 一種電腦可讀取紀錄媒體，內儲一程式，當電腦載入該程式並執行後，可完成如請求項第 1 項至第 6 項中任一項所述之資安聯防方法。

圖式簡單說明

[第一圖]係本發明實施例之主要系統架構示意圖。

[第二圖]係本發明實施例之系統方塊示意圖。

[第三圖]係本發明實施例之詳細系統方塊示意圖。

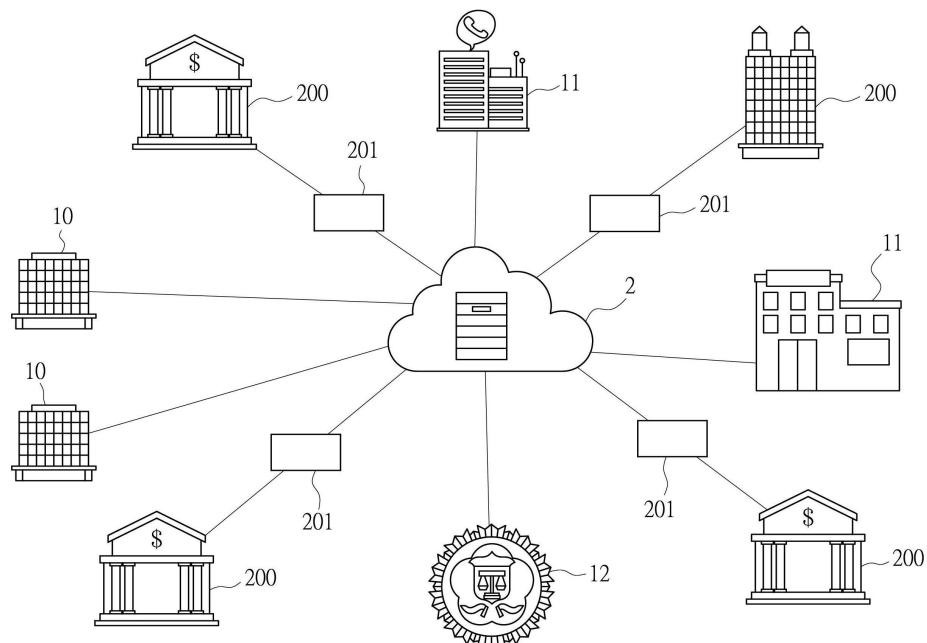
(3)

[第四圖]係本發明實施例之主要步驟流程示意圖。

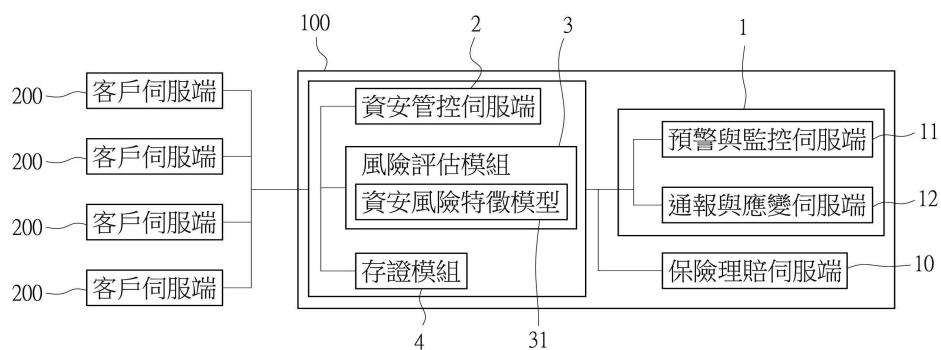
[第五圖]係本發明實施例風險評估之步驟流程示意圖。

[第六圖]係本發明實施例風險評估中資安日誌之解析狀態示意圖。

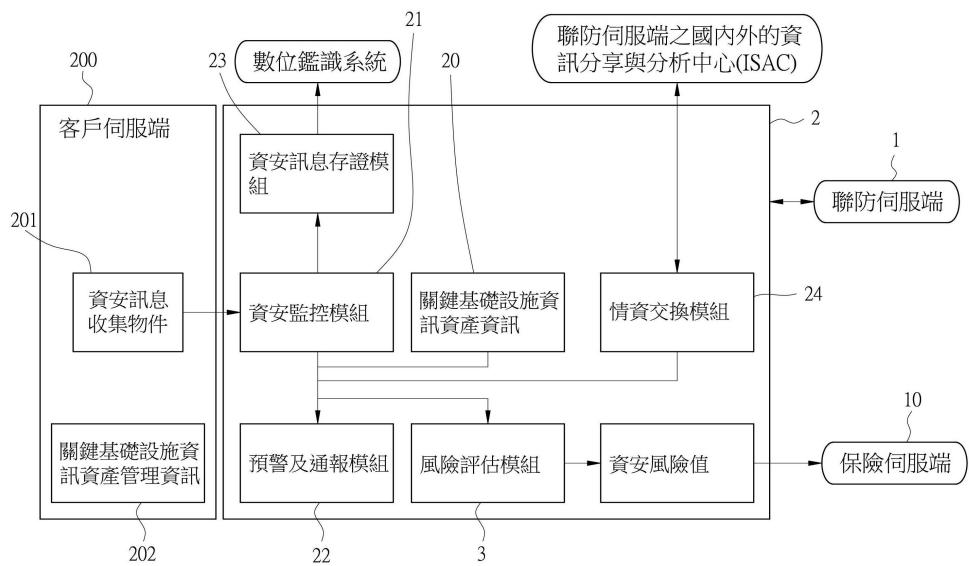
[第七圖]係本發明實施例存證之步驟流程示意圖。



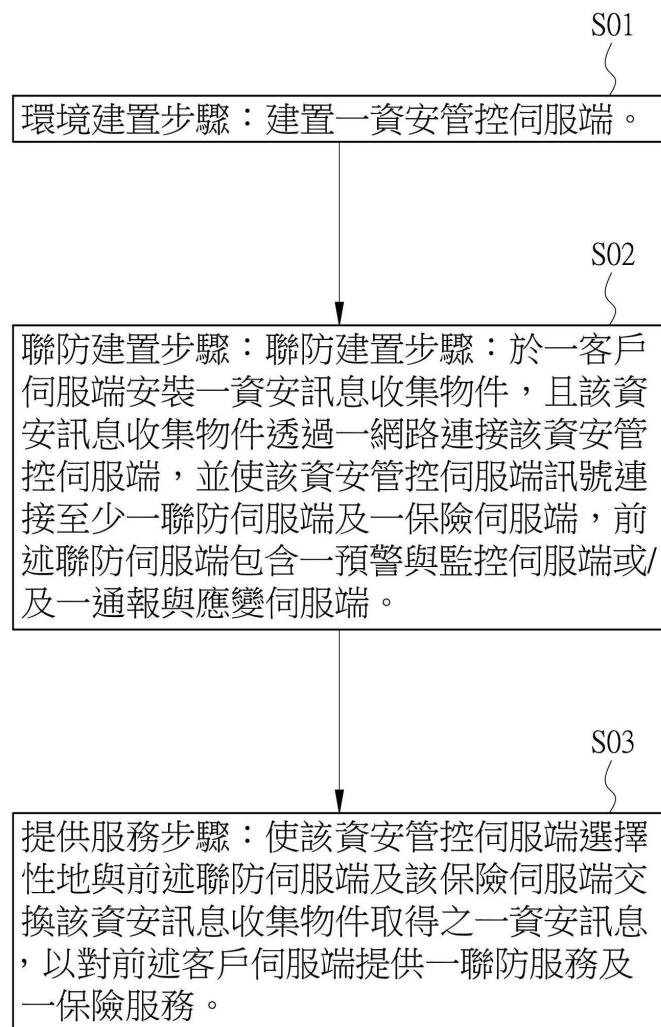
第一圖



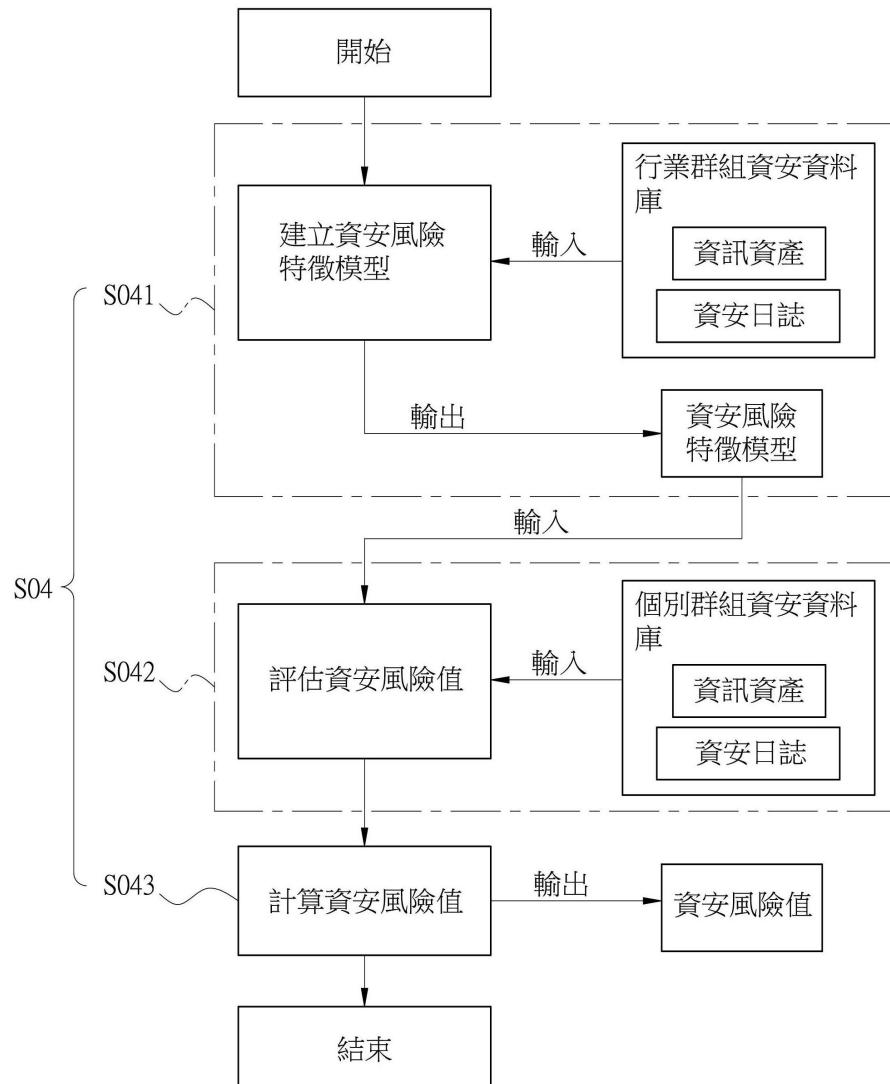
第二圖



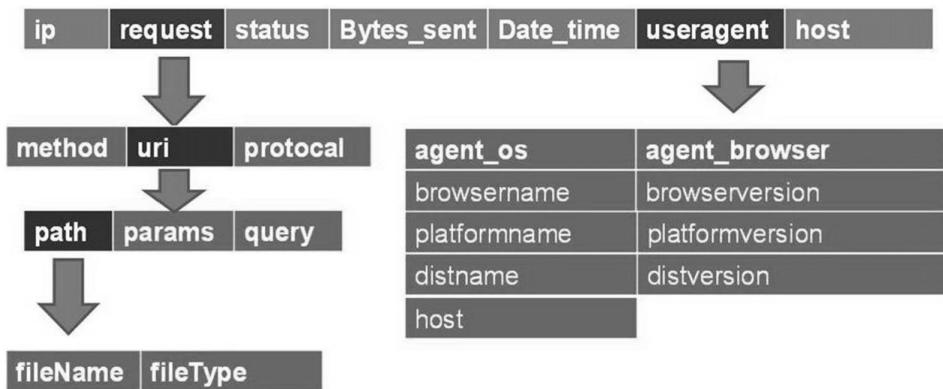
第三圖



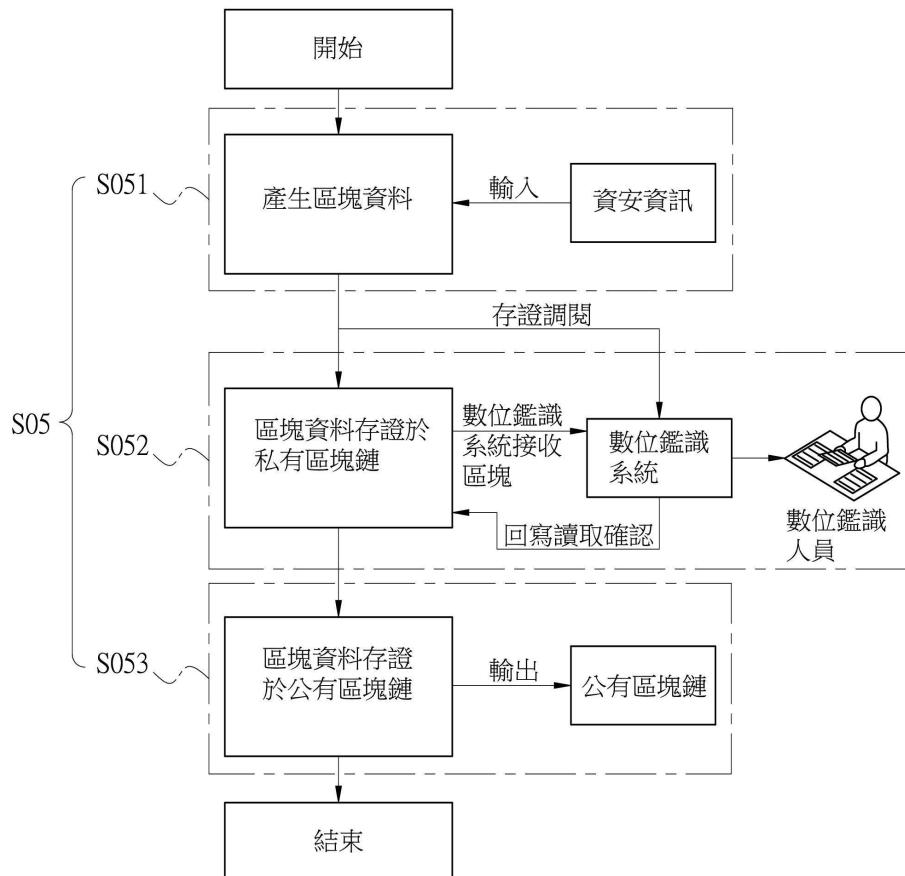
第四圖



第五圖



第六圖



第七圖