201741924

(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 201741924 A

(43)公開日： 中華民國 106 (2017) 年 12 月 01 日

(21)申請案號：105115962 (22)申請日： 中華民國 105 (2016) 年 05 月 23 日

(51)Int. Cl.： *G06F21/56 (2013.01)* *G06F21/57 (2013.01)*

(71)申請人：緯創資通股份有限公司 (中華民國) WISTRON CORPORATION (TW)
新北市汐止區新台五路一段 88 號 21 樓

(72)發明人：陳志明 CHEN, CHIH-MING (TW)

(74)代理人：葉璟宗；詹東穎；劉亞君

申請實體審查：有 申請專利範圍項數：17 項 圖式數：4 共 23 頁

(54)名稱

惡意碼的防護方法、系統及監控裝置

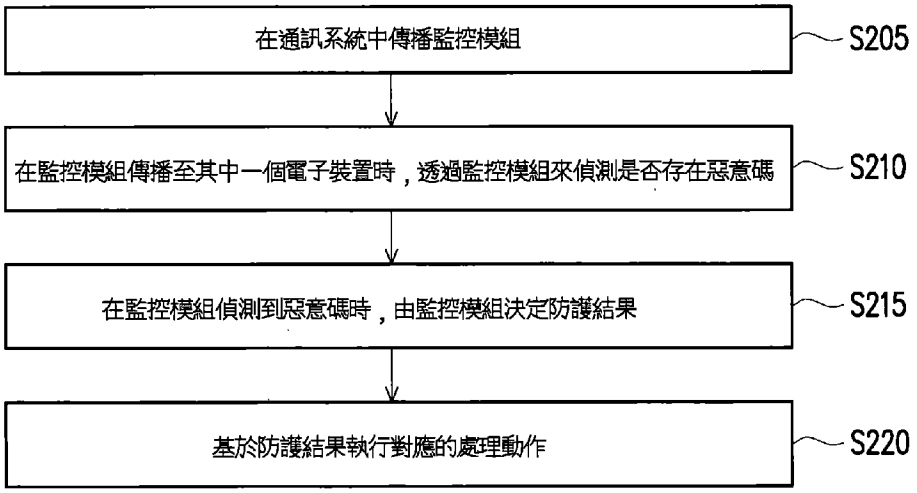
PROTECTING METHOD AND SYSTEM FOR MALICIOUS CODE, AND MONITOR APPARATUS

(57)摘要

一種惡意碼的防護方法、系統及監控裝置。由監控裝置在通訊系統中傳播由多個防毒系統組合而獲得的監控模組，藉以監控通訊系統的多個電子裝置。在監控模組傳播至其中一個電子裝置而偵測到惡意碼時，由監控模組來決定防護結果，並基於防護結果執行對應的處理動作。

A protecting method and system for malicious code, and a monitor apparatus are provided. The monitor apparatus circulates a monitor module including a plurality of antivirus systems to monitor a plurality of electronic apparatuses in a communication system. When the monitor module is circulated to one of the electronic apparatuses and the malicious code is detected, a protection result is decided and a corresponding process action is executed based on the protection result by the monitor module.

指定代表圖：



符號簡單說明：

S205~S220・・・惡意碼的防護方法各步驟

【圖2】

201741924
專利案號：105115962

申請日：105.5.23
IPC分類：G06F 21/56 (2013.01)
G06F 21/57 (2013.01)

201741924

【發明摘要】

【中文發明名稱】惡意碼的防護方法、系統及監控裝置

【英文發明名稱】PROTECTING METHOD AND SYSTEM FOR MALICIOUS CODE, AND MONITOR APPARATUS

【中文】一種惡意碼的防護方法、系統及監控裝置。由監控裝置在通訊系統中傳播由多個防毒系統組合而獲得的監控模組，藉以監控通訊系統的多個電子裝置。在監控模組傳播至其中一個電子裝置而偵測到惡意碼時，由監控模組來決定防護結果，並基於防護結果執行對應的處理動作。

【英文】A protecting method and system for malicious code, and a monitor apparatus are provided. The monitor apparatus circulates a monitor module including a plurality of antivirus systems to monitor a plurality of electronic apparatuses in a communication system. When the monitor module is circulated to one of the electronic apparatuses and the malicious code is detected, a protection result is decided and a corresponding process action is executed based on the protection result by the monitor module.

【指定代表圖】圖2。

【代表圖之符號簡單說明】

S205~S220：惡意碼的防護方法各步驟

【發明說明書】

【中文發明名稱】惡意碼的防護方法、系統及監控裝置

【英文發明名稱】PROTECTING METHOD AND SYSTEM FOR MALICIOUS CODE, AND MONITOR APPARATUS

【技術領域】

【0001】 本發明是有關於一種資料安全機制，且特別是有關於一種惡意碼的防護方法、系統及監控裝置。

【先前技術】

【0002】 隨著科技的演進與創新，網際網路除了促進全球的資訊交流外，愈來愈多人的生活形態從現實社會中逐漸融入虛擬世界。因此，不少有心人士會透過網際網路來進行惡意攻擊。而電腦病毒是其中一種惡意程式，會將程式自我複製、或感染電腦中其他正常的程式、或破壞電腦系統，進而導致電腦無法正常運作。

【0003】 而隨著物聯網（Internet Of Things，IoT）的流行，病毒數量及種類大增。傳統防毒系統需要取得病毒樣本，以人工研究其行為再造出病毒樣本（virus pattern）進行部署，如此費時費力成本高昂。在 IoT 時代，傳統防毒系統已經跟不上病毒演化的速度，需要有一種方式讓防毒系統伴隨著病毒演化才夠快。

【發明內容】

【0004】 本發明提供一種惡意碼的防護方法、系統及監控裝置，針對惡意碼的演化方向來組合多種防毒系統以形成監控模組，使得監控模組的朝向更佳的方向而自主演化。

【0005】 本發明的惡意碼的防護方法，包括：由監控裝置在通訊系統中傳播由多個防毒系統組合而獲得的監控模組，藉以監控通訊系統的至少一個電子裝置；在監控模組傳播至通訊系統的其中一個電子裝置時，透過監控模組來偵測是否存在惡意碼；在監控模組偵測到惡意碼時，由監控模組來決定防護結果；以及基於防護結果執行對應的處理動作。在此，在監控模組偵測到惡意碼時，由監控模組來獲得防護結果的步驟包括：在監控模組為混合式模型（admixture model）的情況下，自上述防毒系統中選擇至少其中一個作為選定模組，而透過選定模組來獲得對應於惡意碼的防護結果；以及在監控模組為結合式模型（association model）的情況下，透過結合這些防毒系統而獲得對應於惡意碼的防護結果。

【0006】 在本發明的一實施例中，上述在監控模組為混合式模型的情況下，包括：基於由監控裝置所決定的演化方向向量，自上述多個防毒系統中選擇其中一個作為選定模組；基於由選定模組所決定的機率向量，透過選定模組來識別惡意碼對應的代表叢集；以及依據演化方向向量以及機率向量，利用隨機分析演算法來識別與代表叢集對應的一組處理動作，而以該組處理動作來作為防護結果。

【0007】 在本發明的一實施例中，上述在監控模組為結合式模型

的情況下，包括：獲得由監控裝置所決定的演化方向向量，其中演化方向向量決定各防毒系統與惡意碼之間的相關性權重；在各防毒系統中，基於由各防毒系統所決定的機率向量，識別惡意碼在各防毒系統所對應的代表叢集；以及依據演化方向向量以及機率向量來識別與這些防毒系統的多個代表叢集相對應的一組處理動作，而以該組處理動作來作為防護結果。

【0008】 在本發明的一實施例中，上述在由監控模組決定防護結果之後，更包括：執行多目標最佳化演算法，以自防護結果所包括的多個目標解中獲得最佳目標解，以設定最佳目標解為最終的處理動作。

【0009】 在本發明的一實施例中，上述惡意碼的防護方法更包括：由監控裝置分析自電子裝置接收的惡意碼對應的多個攻擊行為而獲得行為特徵向量，並基於行為特徵向量來執行行為預測，進而獲得惡意碼與監控模組所包括的多個防毒系統對應的演化方向向量；以及在自其中一個電子裝置接收到異常訊息時，傳播監控模組至傳送異常訊息的電子裝置，而透過監控模組來偵測是否存在惡意碼。

【0010】 在本發明的一實施例中，上述監控模組所包括的多個防毒系統為樹狀階層結構，樹狀階層結構的多個層各自屬於混合式模型或結合式模型。

【0011】 本發明的惡意碼的防護系統，包括：電子裝置以及監控裝置。上述電子裝置及監控裝置位於一通訊系統中。監控裝置透

過通訊設備與各電子裝置進行溝通，並在通訊系統中傳播由多個防毒系統組合而獲得的監控模組，藉以監控通訊系統的各電子裝置。在監控模組傳播至電子裝置時，電子裝置透過監控模組來偵測是否存在一惡意碼，並且，在監控模組偵測到惡意碼時，電子裝置透過監控模組來決定防護結果，並基於防護結果執行對應的處理動作。在此，在監控模組偵測到惡意碼時，在監控模組為混合式模型的情況下，電子裝置自上述防毒系統中選擇至少一個作為選定模組，而透過選定模組來獲得對應於惡意碼的防護結果；在監控模組偵測到惡意碼時，在監控模組為結合式模型的情況下，電子裝置透過上述全部防毒系統而獲得對應於惡意碼的防護結果。

【0012】 本發明的監控裝置，包括通訊設備、儲存設備以及處理器。處理器耦接至通訊設備以及儲存設備。通訊設備與通訊系統的電子裝置建立連線。儲存設備包括行為分析模組及行為預測模組。處理器透過通訊設備在通訊系統中傳播由多個防毒系統組合而獲得的監控模組至電子裝置，藉以監控通訊系統的電子裝置。處理器驅動行為分析模組來分析自電子裝置所接收的至少一惡意碼對應的至少一個攻擊行為而獲得行為特徵向量，且處理器驅動行為預測模組基於行為特徵向量來執行行為預測，進而獲得監控模組所包括的防毒系統對應的演化方向向量，藉由演化方向向量決定監控模組為自多個防毒系統中選擇至少其中一個來決定防護結果或結合多個防毒系統來決定防護結果。

【0013】 基於上述，由監控裝置在通訊系統中傳播（circulate）由多個防毒系統組成的監控模組，藉以來監控通訊系統的各電子裝置。透過監控裝置的分析而可針對惡意碼的演化方向來組合多種防毒系統以形成監控模組，使得監控模組的朝向更佳的方向而自主演化。

【0014】 為讓本發明的上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【圖式簡單說明】

【0015】

圖 1 是本發明一實施例的惡意碼的防護系統的示意圖。

圖 2 是依照本發明一實施例的惡意碼的防護方法流程圖。

圖 3 是依照本發明一實施例的混合式模型的架構示意圖。

圖 4 是依照本發明一實施例的結合式模型的架構示意圖。

【實施方式】

【0016】 圖 1 是本發明一實施例的惡意碼的防護系統的示意圖。防護系統包括監控裝置 110 以及多個電子裝置 120。在此，防護系統例如為建構在物聯網（Internet of Things，IoT）架構上。

【0017】 監控裝置 110 為具有智能且可進行惡意碼分析的裝置，例如為具有高運算能力的伺服器。電子裝置 120 例如為伺服器、個人電腦、筆記型電腦、平板電腦、智慧型手機、穿載式裝置、

智慧型家電等具有運算能力及連網功能的電子裝置。即，電子裝置 120 包括處理器與通訊設備（未繪示）。

【0018】 監控裝置 110 包括處理器 111、儲存設備 112 以及通訊設備 113。處理器 111 耦接至儲存設備 112 以及通訊設備 113。監控裝置 110 透過通訊設備 113 連接至網際網路來與各電子裝置 120 進行溝通。並且，監控裝置 110 透過通訊設備 113 在通訊系統中來傳播（circulate）多個防毒系統、或者由多個防毒系統組合而成的監控模組，藉以監控通訊系統底下的一個或多個電子裝置 120 是否存在惡意碼。

【0019】 所述惡意碼例如為電腦病毒（computer virus）、電腦蠕蟲（computer worm）、木馬程式（trojan horse）、勒索軟體（ransomware）、間諜軟體（spyware）、廣告軟體（adware）、恐嚇軟體（scareware）等。

【0020】 處理器 111 例如為中央處理單元（central processing unit，CPU）、可程式化之微處理器（microprocessor）、嵌入式控制晶片、數位訊號處理器（digital signal processor，DSP）、特殊應用積體電路（application specific integrated circuits，ASIC）或其他類似裝置。儲存設備 112 例如為非揮發性記憶體（non-volatile memory）、隨機存取記憶體（random access memory，RAM）或硬碟等。而通訊設備 113 例如為支援有線或無線通訊協定的晶片。

【0021】 儲存設備 112 包括資料庫 131、行為分析模組 132 以及行為預測模組 133。資料庫 131 中儲存多個防毒系統，使得處理器

111 經由通訊設備 113 而在通訊系統中來傳播至少一個防毒系統。

【0022】 行為分析模組 132 分別自位於各電子裝置 120 中的一個或多個防毒系統接收一惡意碼的多個攻擊行為，並分析這些攻擊行為以獲得一行為特徵向量。行為預測模組 133 基於行為特徵向量來執行行為預測，進而獲得惡意碼與多個防毒系統對應的演化方向（evolution bias）向量。例如，行為預測模組 133 利用馬可夫鏈蒙地卡羅（Markov chain Monte Carlo，MCMC）演算法，而自行為特徵向量來預測攻擊行為的演化方向，而獲得演化方向向量 π_i。並且，依據演化方向向量 π_i 中所包括的元素（element）內容來決定監控模組所包括的防毒系統。

【0023】 藉由演化方向向量決定監控模組為混合式模型或結合式模型。若處理器 111 決定監控模組為混合式模型，則在獲得的演化方向向量中的其中一個元素的數值遠大於其他元素的數值，例如(0.99, 0.01, 0.10, 0.06)。若處理器 111 決定監控模組為結合式模型，則在獲得的演化方向向量中常不存在一個元素的數值遠大於其他元素的數值，例如(0.81, 0.52, 0.63, 0.50)。

【0024】 由於監控裝置 110 會從傳播至其他電子裝置 120 的防毒系統獲得回饋，因而監控裝置 110 具有全局知識以動態調整機率向量（probability vector）或權重向量（weight vector）中的元素（element）。故，由監控裝置 110 所獲得的演化方向向量 π_i 可以將監控模組的演化引導至朝向更佳的方向。並且，監控裝置 110 可以決定監控模組所使用的演化方向向量 π_i 為機率向量或權重向量

（weight vector）。而當經由通訊設備 113 自其中一電子裝置 120 接收到異常訊息時，處理器 111 將對應於異常訊息的監控模組傳播至傳送異常訊息的電子裝置 120，以由監控模組來獲得對應的防護結果。例如，在偵測到其中一個電子裝置 120 停止傳送心跳封包時，判定其發生異常。

【0025】 底下搭配上述防護系統來說明惡意碼防護方法的各步驟。圖 2 是依照本發明一實施例的惡意碼的防護方法流程圖。請參照圖 1 及圖 2，在步驟 S205 中，由監控裝置 110 在通訊系統中傳播由多個防毒系統組合而獲得的監控模組，藉以監控通訊系統底下的多個電子裝置 120。在此，監控裝置 110 可以定時使一監控模組在通訊系統中進行傳播（circulate），也可以在接收到異常訊息時，將監控模組傳送至有異常的電子裝置 120。

【0026】 接著，在步驟 S210 中，在監控模組傳播至其中一個電子裝置 120 時，透過監控模組來偵測指定裝置中是否存在惡意碼。

【0027】 在步驟 S215 中，在監控模組偵測到電子裝置中存在惡意碼時，由監控模組決定防護結果。在此，監控模組可以是混合式模型（admixture model）與結合式模型（association model），其包括至少兩個防毒系統。在監控模組為混合式模型的情況下，選擇至少其中一個防毒系統作為一選定模組，而透過選定模組來獲得對應於惡意碼的防護結果。在監控模組為結合式模型的情況下，透過結合全部的防毒系統而獲得對應於惡意碼的防護結果。即，在監控模組為混合式模型的情況下，藉由惡意碼來訓練一個防毒

系統；而在監控模組為結合式模型的情況下，藉由惡意碼來訓練全部的防毒系統。

【0028】 進一步來說，不管是混合式模型或結合式模型的監控模組，其都具有一個演化方向向量$\pi_i=(p_1, p_2, \ldots, p_m)$。在監控模組為混合式模型的情況下，演化方向向量$\pi_i$為機率向量，在此機率向量中具有一個機率趨近於100%的元素，進而基於機率選擇此一元素對應的防毒系統來作為選定模組。而在監控模組為結合式模型的情況下，演化方向向量π_i為權重向量，藉以來決定各防毒系統與惡意碼之間的相關性權重。

【0029】 圖 3 是依照本發明一實施例的混合式模型的架構示意圖。請參照圖3，混合式模型300在偵測到惡意碼時，基於由監控裝置110所決定的演化方向向量π_i（即，機率向量），自多個防毒系統310中選擇其中一個作為選定模組310_a。在圖3的多個防毒系統 310 中，以實線連接至被選擇的防毒系統，並且以虛線連接來表示未被選擇的防毒系統310。

【0030】 接著，以選定模組310_a針對惡意碼而基於機率向量π_i^A自多個代表叢集311中來獲得與惡意碼最相符的代表叢集311_1。上述機率向量π_i^A是由防毒系統 310_a 所遇過的惡意碼樣本來決定。機率向量π_i^A中具有一個機率趨近於 100%的元素，進而基於機率向量π_i^A選擇此一元素對應的代表叢集 311_1。在此，機率向量π_i^A例如是基於狄利克雷分布（Dirichlet distribution）使用匹配（match）的方式去識別對應的叢集。

【0031】 之後，混合式模型 300 依據演化方向向量π_i以及機率向量π_i^A，利用隨機分析（stochastic analytics）演算法（例如貝氏線性迴歸（Bayesian Linear Regression，BLR）演算法）來識別與代表叢集 311_1 對應的一組處理動作，而以此組處理動作來作為防護結果。例如，將演化方向向量π_i以及機率向量π_i^A做為一組特徵向量而輸入至基於 BLR 演算法的 BLR 模型，而 BLR 模型在經過運算後會回傳一組處理動作。

【0032】 圖 4 是依照本發明一實施例的結合式模型的架構示意圖。請參照圖 4，結合式模型 400 在偵測到惡意碼時，基於由監控裝置 110 所決定的演化方向向量π_i（即，權重向量），決定各防毒系統 410 與惡意碼之間的相關性權重。並且，每一個防毒系統 410 皆會針對惡意碼來獲得對應的一個代表叢集。以防毒系統 410_a 而言，其會基於機率向量π_i^A自多個代表叢集 411 中來獲得與惡意碼最相符的代表叢集 411_1。上述機率向量π_i^A是由防毒系統 410_a 所遇過的惡意碼樣本來決定。其他防毒系統 410 亦以此類推，而獲得對應的 n 個防毒系統 410 的 n 個代表叢集 411_1~411_n。

【0033】 之後，混合式模型 400 依據演化方向向量π_i以及機率向量π_i^A，利用隨機分析演算法來識別與 n 個代表叢集 411_1~411_n 對應的一組處理動作，而以此組處理動作來作為防護結果。例如，將演化方向向量π_i以及機率向量π_i^A做為一組特徵向量而輸入至基於 BLR 演算法的 BLR 模型，而 BLR 模型在經過運算後會回傳一組處理動作。在圖 4 中，以實線連接至全部的防毒系統 410 來

表示選擇全部的防毒系統 410 來執行後續動作。

【0034】 返回圖 2，在步驟 S220 中，監控模組基於防護結果執行對應的處理動作。例如，在防護結果中包括多個處理動作時，監控模組進一步執行多目標最佳化（multi objective optimization）演算法，以自防護結果所包括的多個目標解（處理動作）中獲得最佳目標解，以設定最佳目標解為最終的處理動作。例如，監控模組將每一個處理動作轉換成多目標向量$(O_1, O_2, ..., O_n)$，並且使用柏拉圖效率（Pareto efficiency）來獲得柏拉圖組合（Pareto set），該組合包括一個或多個最佳的處理動作。處理動作例如為，清除或刪除可疑檔案；若無法清除，則迅速地隔離受感染的網路區段或可疑檔案。上述多目標最佳化演算法可基於成本（cost）、效用（utility）等因素來選擇最佳目標解。

【0035】 在此，防毒系統採用的是貝氏非參數（Bayesian Nonparametric，BNP）模型。例如，BNP 模型為基於原型叢集（prototype clustering）以及子空間學習（subspace learning）的貝氏案例模型（Bayesian Case Model）。BCM 藉由原型（prototype）p_s以及子空間特徵指示符（subspace feature indicator）ω_s來描述（characterize）每一個叢集（cluster）。在此，叢集的數量可以動態增加或動態減少。

【0036】 在此，原型 p_s 被定義為 x 中 $p(p_s \mid \omega_s, z, x)$ 為最大化的一個觀察（observation）。原型是典型的觀察（quintessential observation），最能代表叢集。其中，x（$x=\{x_1, x_2, ..., x_N\}$）是自惡

意碼所獲得的特徵向量，z 為叢集索引（cluster index）。子空間特徵指示符 ω_s 代表自惡意碼中所擷取的特徵向量中最重要（感興趣）的特徵。即，子空間特徵指示符 ω_s 的取得是看哪個 ω_s 能最大化機率 $p(\omega_s \mid p_s, z, x)$。另外，監控裝置 110 也可以更新（增加、減少、或修改）監控模組裡面 BLR 模型的原型與對應的一組處理動作的映射，以便增強監控模組的病毒處理能力。例如，透過機器學習中的案例推論（Case Based Reasoning），來適當地調整對應的一組處理動作。

【0037】 另外，在一台電子裝置 120 中存在有多個監控模組的情況下，由這些監控模組自行協商（negotiate）決定由哪一個來對惡意碼進行處理。

【0038】 此外，不管是混合式模型的監控模組還是結合式模型的監控模組，其可以由多個混合式模型 300 組成，也可以由多個結合式模型 400 組成，更可以由混合式模型 300 及結合式模型 400 組成。

【0039】 例如，倘若監控模組的第一層為混合式模型，則僅會選擇底下其中一個支線來處理，再根據該支線為混合型或結合型來決定要選擇其中一個防毒系統而獲得一個代表叢集、或是選擇全部的防毒系統（假設 n 個）而獲得 n 個代表叢集。另一方面，倘若監控模組的第一層為結合式模型，則選擇底下全部支線，再根據每一個支線為混合型或結合型來決定要選擇其中一個防毒系統而獲得一個代表叢集、或是選擇全部的防毒系統（假設 n 個）而

獲得 n 個代表叢集。

【0040】 綜上所述，基於上述實施例，透過監控裝置的分析而可針對惡意碼的演化方向來組合多種防毒系統以形成監控模組，使得監控模組的朝向更佳的方向而自主演化。藉由防毒系統與防毒系統之間的基因重組（混合式或組合式）來產生新的防毒系統（即，監控模組），再由監控裝置在通訊系統中傳播（circulate）由多個防毒系統組成的監控模組，藉以來監控通訊系統底下各電子裝置。據此，透過監控裝置來收集多個攻擊行為並進行分析，使得監控模組得以因應惡意碼的演化而自主演化。

【0041】 雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明的精神和範圍內，當可作些許的更動與潤飾，故本發明的保護範圍當視後附的申請專利範圍所界定者為準。

【符號說明】

【0042】

110：監控裝置

111：處理器

112：儲存設備

113：通訊設備

120：電子裝置

131：資料庫

132：行為分析模組

133：行為預測模組

300：混合式模型

310、410、410_a：防毒系統

310_a：選定模組

311、311_1、411、411_1~411_n：代表叢集

400：結合式模型

π_i：演化方向向量

π_i^A：機率向量

S205~S220：惡意碼的防護方法各步驟

【發明申請專利範圍】

【第 1 項】一種惡意碼的防護方法，包括：

由一監控裝置在一通訊系統中傳播由多個防毒系統組合而獲得的一監控模組，藉以監控該通訊系統的至少一個電子裝置；

在該監控模組傳播至該通訊系統的一個所述電子裝置時，透過該監控模組來偵測是否存在一惡意碼；

在該監控模組偵測到該惡意碼時，由該監控模組決定一防護結果；以及

基於該防護結果來執行對應的處理動作；

其中，在該監控模組偵測到該惡意碼時，由該監控模組決定該防護結果的步驟包括：

在該監控模組為一混合式模型的情況下，自該些防毒系統中選擇至少其中一個作為一選定模組，而透過該選定模組來獲得對應於該惡意碼的該防護結果；以及

在該監控模組為一結合式模型的情況下，透過結合該些防毒系統而獲得對應於該惡意碼的該防護結果。

【第 2 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，其中在該監控模組為該混合式模型的情況下，包括：

基於由該監控裝置所決定的一演化方向向量，自該些防毒系統中選擇至少其中一個作為該選定模組；

基於由該選定模組所決定的一機率向量，透過該選定模組來識別該惡意碼對應的一代表叢集；以及

依據該演化方向向量以及該機率向量識別與該代表叢集對應的一組處理動作，而以該組處理動作來作為該防護結果。

【第 3 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，其中在該監控模組為該結合式模型的情況下，包括：

獲得由該監控裝置所決定的一演化方向向量，其中該演化方向向量決定每一該些防毒系統與該惡意碼之間的一相關性權重；

在每一該些防毒系統中，基於由每一該些防毒系統所決定的一機率向量，識別該惡意碼在每一該些防毒系統所對應的一代表叢集；以及

依據該演化方向向量以及該機率向量識別與該些防毒系統的多個所述代表叢集相對應的一組處理動作，而以該組處理動作來作為該防護結果。

【第 4 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，其中在由該監控模組決定該防護結果的步驟之後，更包括：

執行一多目標最佳化演算法，以自該防護結果所包括的多個目標解中獲得一最佳目標解，以設定該最佳目標解為最終的該處理動作。

【第 5 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，更包括：

由該監控裝置分析自該至少一電子裝置接收的該惡意碼對應的至少一個攻擊行為而獲得一行為特徵向量，並基於該行為特徵向量來執行一行為預測，進而獲得該惡意碼與該監控模組所包括

的該些防毒系統對應的一演化方向向量。

【第 6 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，更包括：

在該通訊系統的一個所述電子裝置發生異常時，由該監控裝置傳播該監控模組至發生異常的該電子裝置，而透過該監控模組來偵測是否存在該惡意碼。

【第 7 項】如申請專利範圍第 1 項所述的惡意碼的防護方法，其中該監控模組所包括的該些防毒系統為一樹狀階層結構，該樹狀階層結構的多個層各自屬於該混合式模型或該結合式模型。

【第 8 項】一種惡意碼的防護系統，包括：

一電子裝置，位於一通訊系統中；以及

一監控裝置，位於該通訊系統，並透過一通訊設備與該電子裝置進行溝通，在該通訊系統中傳播由多個防毒系統組合而獲得的一監控模組，藉以監控該通訊系統的該電子裝置；

其中，在該監控模組傳播至該電子裝置時，該電子裝置透過該監控模組偵測是否存在一惡意碼，並且，在該監控模組偵測到該惡意碼時，該電子裝置透過該監控模組來決定一防護結果，並基於該防護結果執行對應的處理動作，

其中，在該監控模組偵測到該惡意碼時，在該監控模組為一混合式模型的情況下，該電子裝置自該些防毒系統中選擇至少其中一個作為一選定模組，而透過該選定模組來獲得對應於該惡意碼的該防護結果；

在該監控模組偵測到該惡意碼時，在該監控模組為一結合式模型的情況下，該電子裝置結合該些防毒系統而獲得對應於該惡意碼的該防護結果。

【第 9 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其中在該監控模組為該混合式模型的情況下，在該電子裝置中，

基於由該監控裝置所決定的一演化方向向量，自該些防毒系統中選擇至少其中一個作為該選定模組；

基於由該選定模組所決定的一機率向量，透過該選定模組來識別該惡意碼對應的一代表叢集；

依據該演化方向向量以及該機率向量識別與該代表叢集對應的一組處理動作，而以該組處理動作來作為該防護結果。

【第 10 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其中在該監控模組為該結合式模型的情況下，在該電子裝置中，

基於由該監控裝置所決定的一演化方向向量，判定每一該些防毒系統與該惡意碼的一相關性權重；

在每一該些防毒系統中，基於由每一該些防毒系統所決定的一機率向量，識別該惡意碼在每一該些防毒系統所對應的一代表叢集；

依據該演化方向向量以及該機率向量識別與該些防毒系統的多個所述代表叢集相對應的一組處理動作，而以該組處理動作來作為該防護結果。

【第 11 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其

中在該電子裝置透過該監控模組來獲得該防護結果之後，執行一多目標最佳化演算法，以自該防護結果所包括的多個目標解中獲得一最佳目標解，以設定該最佳目標解為最終的該處理動作。

【第 12 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其中該監控裝置分析自該電子裝置及該通訊系統所包括的另一電子裝置至少其中一個接收的該惡意碼對應的至少一個攻擊行為，而獲得一行為特徵向量，並基於該行為特徵向量來執行一行為預測，進而獲得該惡意碼與該監控模組所包括的該些防毒系統對應的一演化方向向量。

【第 13 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其中在該電子裝置異常時，該監控裝置傳播該監控模組至該電子裝置，而透過該監控模組來偵測是否存在該惡意碼。

【第 14 項】如申請專利範圍第 8 項所述的惡意碼的防護系統，其中該監控模組所包括的該些防毒系統為一樹狀階層結構，該樹狀階層結構的多個層各自屬於該混合式模型或該結合式模型。

【第 15 項】一種監控裝置，包括：

一通訊設備，與一通訊系統的一電子裝置建立連線；

一儲存設備，包括一行為分析模組及一行為預測模組；以及

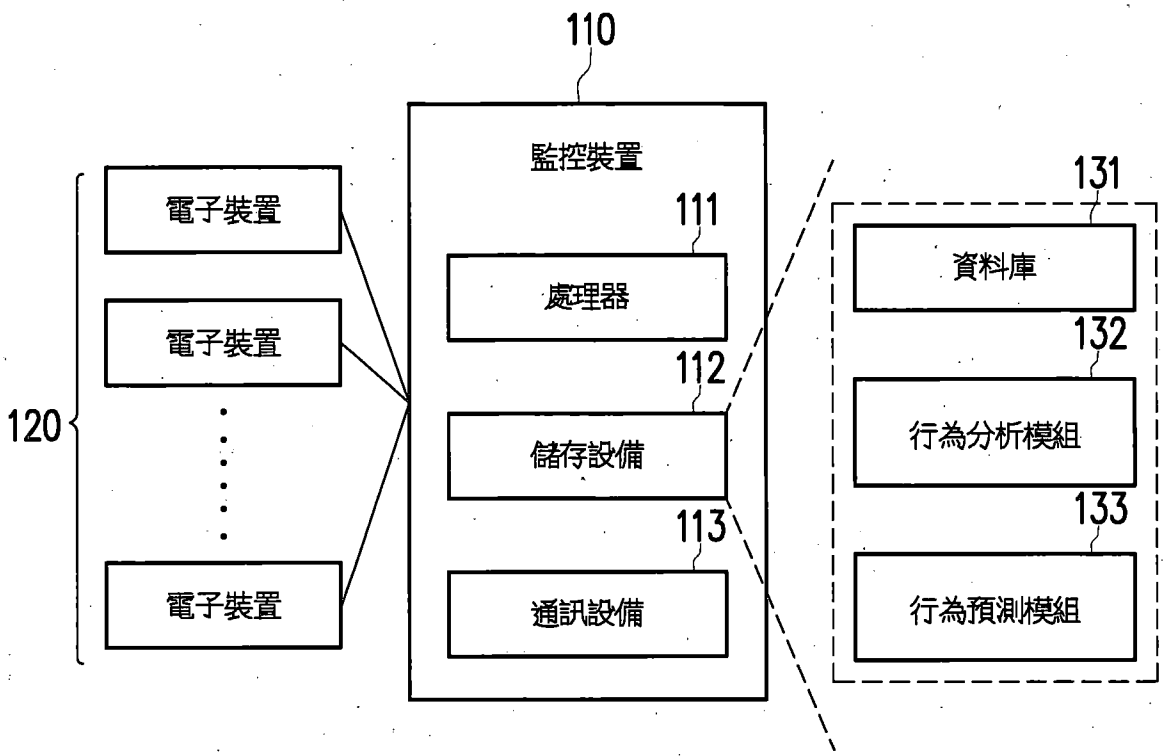
一處理器，耦接至該通訊設備以及該儲存設備，其中該處理器透過該通訊設備在該通訊系統中傳播由多個防毒系統組合而獲得的一監控模組至該電子裝置，藉以監控該通訊系統的該電子裝置，

其中，該處理器驅動該行為分析模組來分析自該電子裝置所接收的至少一惡意碼對應的至少一個攻擊行為而獲得一行為特徵向量，且該處理器驅動該行為預測模組基於該行為特徵向量來執行一行為預測，進而獲得該監控模組所包括的該些防毒系統對應的一演化方向向量，藉由該演化方向向量決定該監控模組為自該些防毒系統中選擇至少其中一個來決定一防護結果或結合該些防毒系統來決定該防護結果。

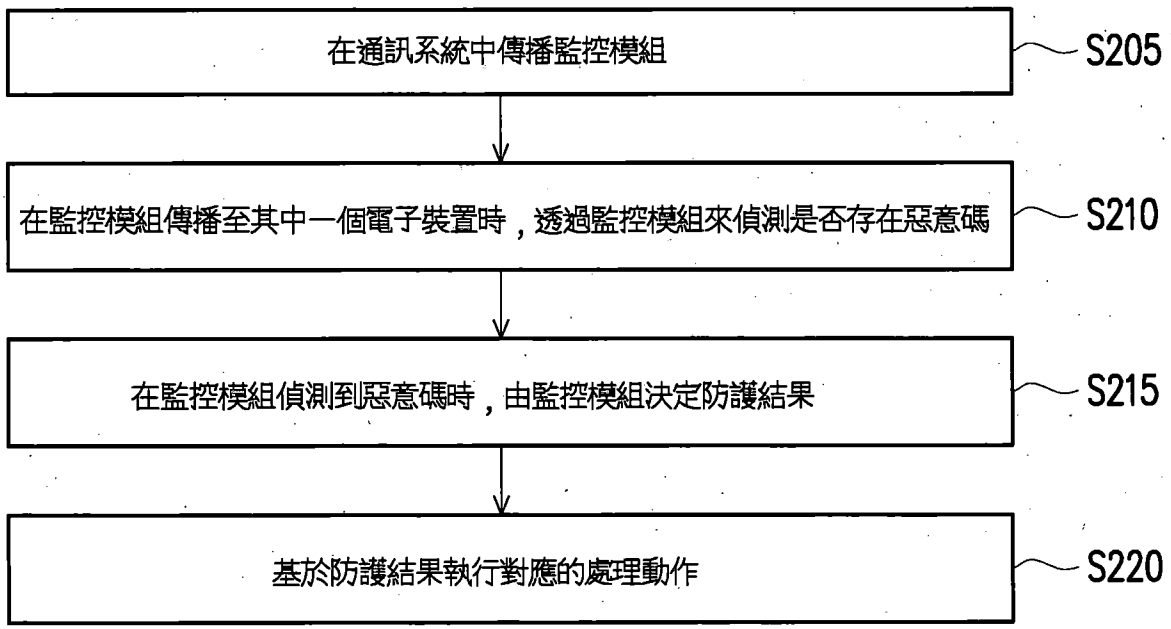
【第 16 項】如申請專利範圍第 15 項所述的監控裝置，其中當該電子裝置發生異常時，該處理器將該監控模組傳播至該電子裝置，以由該監控模組來決定該防護結果。

【第 17 項】如申請專利範圍第 15 項所述的監控裝置，其中該處理器藉由該演化方向向量決定該監控模組為一混合式模型或一結合式模型，其中該混合式模型的該監控模組是透過自該些防毒系統中選擇至少其中一個來決定該防護結果，而該結合式模型的該監控模組是基於該演化方向向量來決定每一該些防毒系統與該惡意碼之間的一相關性權重，進而透過結合該些防毒系統來決定該防護結果。

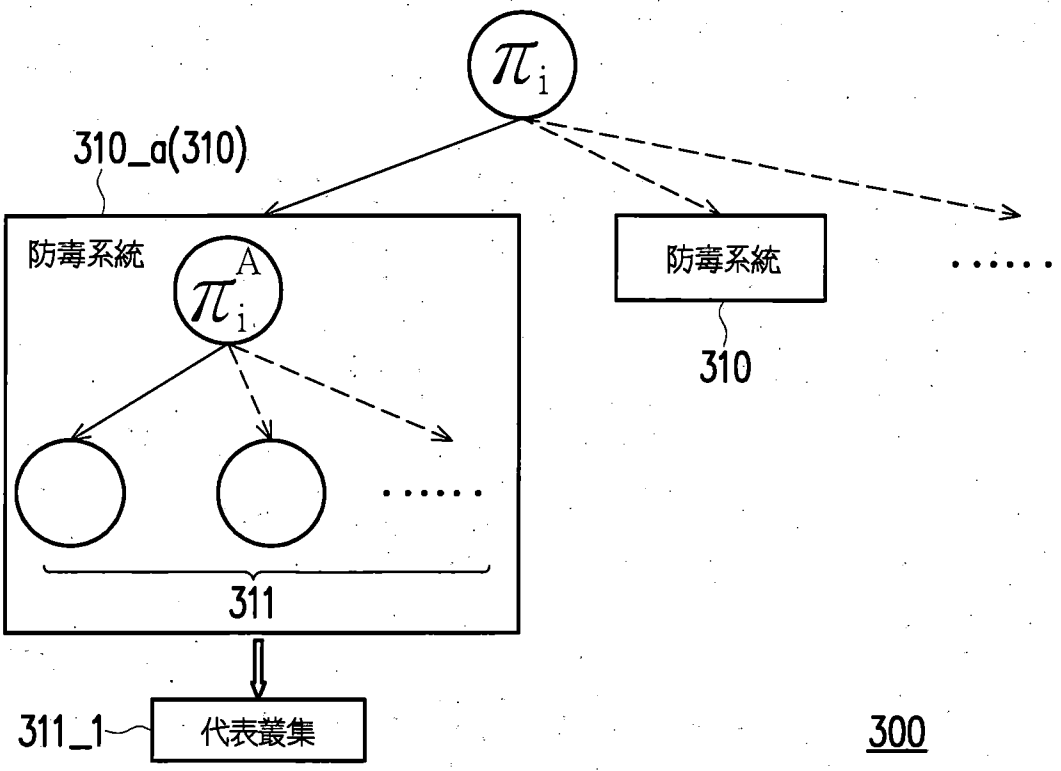
【發明圖式】


110
監控裝置
111
處理器
112
儲存設備
113
通訊設備
120
電子裝置
電子裝置
電子裝置
131
資料庫
132
行為分析模組
133
行為預測模組

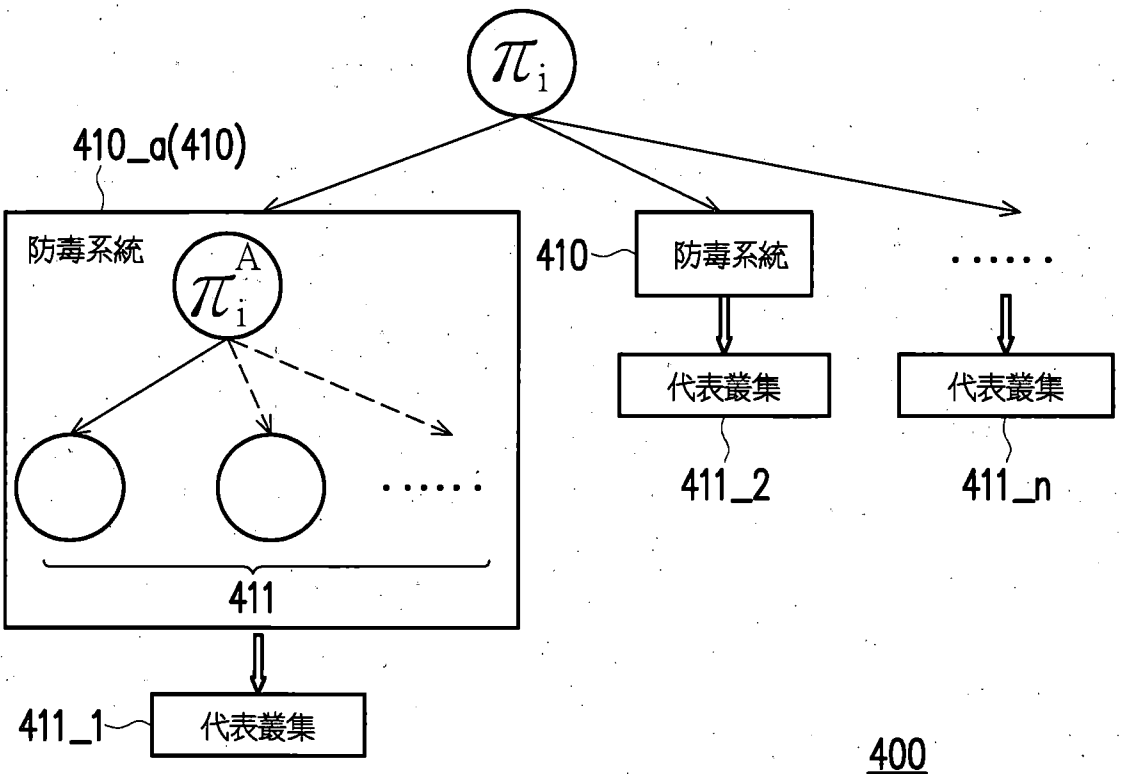
【圖1】


在通訊系統中傳播監控模組
S205
在監控模組傳播至其中一個電子裝置時，透過監控模組來偵測是否存在惡意碼
S210
在監控模組偵測到惡意碼時，由監控模組決定防護結果
S215
基於防護結果執行對應的處理動作
S220

【圖2】


π_i
310_a(310)
防毒系統
π_i^A
311
311_1
代表叢集
防毒系統
310
300

【圖3】


π_i
410_a(410)
防毒系統
π_i^A
411
411_1
代表叢集
410
防毒系統
代表叢集
411_2
代表叢集
411_n
400

【圖4】