(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017 年 6 月 29 日(29.06.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/110363 A1

(51) 国際特許分類:
G06F 21/56 (2013.01) *G06F 21/60* (2013.01)

(21) 国際出願番号: PCT/JP2016/085003

(22) 国際出願日: 2016 年 11 月 25 日(25.11.2016)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2015-254597 2015 年 12 月 25 日(25.12.2015) JP

(71) 出願人: 株式会社日立ソリューションズ(HITACHI SOLUTIONS, LTD.) [JP/JP]; 〒1400002 東京都品川区東品川四丁目１２番７号 Tokyo (JP).

(72) 発明者: 井上　淳雄(INOUE Atsuo); 〒1400002 東京都品川区東品川四丁目１２番７号　株式会社日立ソリューションズ内 Tokyo (JP). 原田　建樹(HARADA Tateki); 〒1400002 東京都品川区東品川四丁目１２番７号　株式会社日立ソリューションズ内 Tokyo (JP). 押田　勇三(OSHIDA Yuzo); 〒1400002 東京都品川区東品川四丁目１２番７号　株式会社日立ソリューションズ内 Tokyo (JP).

(74) 代理人: 平木　祐輔, 外(HIRAKI Yusuke et al.); 〒1056232 東京都港区愛宕２丁目５番１号　愛宕グリーンヒルズＭＯＲＩタワー３２階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

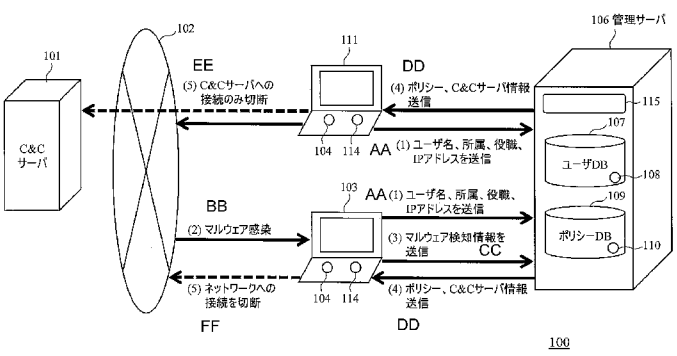
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: INFORMATION LEAKAGE PREVENTION SYSTEM AND METHOD

(54) 発明の名称 : 情報漏洩防止システム及び方法

図 1



101 C&C server
106 Administrative server
107 User database
109 Policy database
AA (1) Transmit user name, affiliation, title, IP address
BB (2) Malware infection
CC (3) Transmit malware detection information
DD (4) Transmit policy, C&C server information
EE (5) Only disconnect connection to C&C server
FF (5) Disconnect connection to network

(57) **Abstract**: Provided is an information leakage prevention technology which does not require any dedicated apparatus for administrating access on a network, and which has excellent flexibility in terms of security policy. The information leakage prevention system comprises a client terminal which has a client processing unit that performs network control in accordance with an acquired security policy, and an administrative server having: a user database which stores information about users using the client terminal; a security policy database which stores security policies for determining the network control content for each user attribute; and a server processing unit which selects a security policy on the basis of a user attribute and the time at which the security policy is distributed, and which transmits the selected security policy to a corresponding client terminal.

(57) 要約: ネットワーク上にアクセスを管理する専用装置を必要とせず、しかもセキュリティポリシーの柔軟性にも優れる情報漏洩防止技術を提供する。情報漏洩防止システムは、取得したセキュリティポリシーに応じてネットワーク制御を行うクライアント処理部を有するクライアント端末と、前記クライアント端末を利用するユーザに関する情報を格納するユーザデータベースと、ユーザの属性ごとにネットワーク制御内容を定めたセキュリティポリシーを格納するセキュリティポリシーデータベースと、ユーザの属性及び前記セキュリティポリシーを配布する時刻に基づいて前記セキュリティポリシーを選択し、選択された前記セキュリティポリシーを対応する前記クライアント端末に送信するサーバ処理部とを有する管理サーバとを有する。

WO 2017/110363 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： 情報漏洩防止システム及び方法

技術分野

[0001]　本開示は、例えばマルウェアによる情報漏洩を未然に防止する情報漏洩防止技術に関する。

背景技術

[0002]　マルウェア対策ソフトウェアによりマルウェア感染を検知した場合に、感染したクライアントマシンからＣ＆Ｃサーバへの接続をブロックし、又は、感染したクライアントマシンをネットワークから隔離することにより被害を防止するための技術として例えば特許文献１に記載の技術がある。特許文献１には、トラフィック異常を検出した場合、ファイアウォール（Firewall）装置と中継装置を使用して、特定のアドレスを宛先とするパケットを遮断する技術が記載されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１２－０１５６８４号公報

発明の概要

発明が解決しようとする課題

[0004]　しかし、特許文献１に記載の技術は、外部ネットワークとクライアントマシンの間にファイアウォール装置と中継装置が存在することを前提としており、クライアントマシンをファイアウォール装置と中継装置が存在する特定の内部ネットワークに設置する必要がある。このため、内部ネットワークの外に位置するクライアントマシンからの情報漏洩を防ぐことはできない。

[0005]　また、特許文献１に記載の技術は、ファイアウォール装置と中継装置を使用して、外部へのアクセスを一律に制限する。このため、内部ネットワークに存在する全てのクライアントマシンに対して同じレベルの対策しかできない。また、各クライアントマシンを使用するユーザによってセキュリティの

強度を変更し、安全と認められる範囲内でネットワーク接続を許可し、ユーザの利用制限を軽減するなどの柔軟な対応ができない。

課題を解決するための手段

[0006] 上記課題を解決するために、本開示は、例えば請求の範囲に記載の構成を採用する。本明細書は上記課題を解決する手段を複数含んでいるが、その一例を挙げるならば、「取得したセキュリティポリシーに応じてネットワーク制御を行うクライアント処理部を有するクライアント端末と、前記クライアント端末を利用するユーザに関する情報を格納するユーザデータベースと、ユーザの属性ごとにネットワーク制御内容を定めたセキュリティポリシーを格納するセキュリティポリシーデータベースと、ユーザの属性及び前記セキュリティポリシーを配布する時刻に基づいて前記セキュリティポリシーを選択し、選択された前記セキュリティポリシーを対応する前記クライアント端末に送信するサーバ処理部と、を有する管理サーバとを有する情報漏洩防止システム。」を特徴とする。

発明の効果

[0007] 本開示によれば、ファイアウォール装置や中継装置が存在しないネットワークでも、クライアント端末からＣ＆Ｃサーバへの情報送信をブロックし又はクライアント端末をネットワークから隔離することができる。また、本開示によれば、クライアント端末のユーザの属性に応じてセキュリティポリシーの強弱を変化させることができる。前述した以外の課題、構成及び効果は、以下の実施の形態の説明により明らかにされる。

図面の簡単な説明

[0008] [図1]実施例１に係るシステムの全体構成を示す図。

[図2]ユーザデータベースに格納されているデータの構造を説明する図（実施例１）。

[図3]セキュリティポリシーデータベースに格納されているデータの構造を説明する図（実施例１）。

[図4]クライアントマシン起動時の処理手順を説明するフローチャート（実施

例１）。

[図5]クライアントマシン起動時の管理サーバの処理手順を説明するフローチャート（実施例１）。

[図6]マルウェア感染時のクライアントマシンの処理手順を説明するフローチャート（実施例１）。

[図7]マルウェア感染時の管理サーバの処理手順を説明するフローチャート（実施例１）。

[図8]実施例２に係るシステムの全体構成を示す図。

[図9]ユーザデータベースに格納されているデータの構造を説明する図（実施例２）。

[図10]セキュリティポリシーデータベースに格納されているデータの構造を説明する図（実施例２）。

[図11]マルウェア感染時のクライアントマシンの処理手順を説明するフローチャート（実施例２）。

[図12]マルウェア感染時の管理サーバの処理手順を説明するフローチャート（実施例２）。

[図13]実施例３に係るシステムの全体構成を示す図。

[図14]ユーザデータベースに格納されているデータの構造を説明する図（実施例３）。

[図15]セキュリティポリシーデータベースに格納されているデータの構造を説明する図（実施例３）。

[図16]マルウェア感染時のクライアントマシンの処理手順を説明するフローチャート（実施例３）。

[図17]マルウェア感染時の管理サーバの処理手順を説明するフローチャート（実施例３）。

発明を実施するための形態

[0009] 以下、図面に基づいて、本開示の実施の形態を説明する。なお、本開示の実施の態様は、後述する形態例に限定されるものではなく、その技術思想の

範囲において、種々の変形が可能である。

[0010] （１）実施例１

（１－１）システム構成

図１は、本実施例に係る情報漏洩防止システム１００の全体構成を示す。情報漏洩防止システム１００は、クライアントマシンと管理サーバの協働により、クライアントマシンのネットワーク接続やＣ＆Ｃサーバへのアクセスを制御し、マルウェアの感染による情報漏洩を防止するシステムである。

[0011] 情報漏洩防止システム１００は、管理サーバ１０６とクライアントマシン１０３及び１１１を有している。管理サーバ１０６とクライアントマシン１０３及び１１１は、ネットワーク１０２を通じて接続されている。図１では、クライアントマシン１０３及び１１１のみを表しているが、クライアントマシンの台数は任意である。

[0012] クライアントマシン１０３及び１１１はそれぞれ、コンピュータを基本構成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース、ディスプレイ装置等で構成される。本実施例の場合、クライアントマシン１０３及び１１１には、ＣＰＵによるプログラムの実行を通じて機能が提供されるマルウェア対策ソフトウェア１０４とクライアント処理部１１４が実装されている。マルウェア対策ソフトウェア１０４は、マルウェアの感染を検知するプログラムである。

[0013] クライアント処理部１１４は、ユーザ情報送信機能、マルウェア検知情報送信機能、ネットワーク制御機能を含む。ユーザ情報送信機能はユーザ情報の送信に使用され、マルウェア検知情報送信機能はマルウェア検知情報の送信に使用され、ネットワーク制御機能はネットワーク等との接続又は切断を制御する。

[0014] 管理サーバ１０６は、コンピュータを基本構成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース等で構成される。管理サーバ１０６には必要に応じて表示装置も接続される。本実施例の管理サーバ１０６には、ユーザデータベース（データベース）１０７、セキュリ

ティポリシーデータベース（ＤＢ）１０９、サーバ処理部１１５が実装されている。

[0015] サーバ処理部１１５は、ＣＰＵによるプログラムの実行を通じ、ユーザ情報管理機能、セキュリティポリシー管理機能、セキュリティポリシー送信機能を提供する。ユーザ情報管理機能はユーザデータベース１０７を管理し、セキュリティポリシー管理機能はセキュリティポリシーデータベース１０９を管理し、セキュリティポリシー送信機能はセキュリティポリシーの送信に使用される。

[0016] ユーザデータベース１０７には、各ユーザのユーザ名（又は識別子）、所属、役職、クライアントマシンのＩＰアドレス等のデータ１０８が保存される。本明細書では、これら情報をまとめて「ユーザに関する情報」ともいう。また、各ユーザのユーザ名（又は識別子）、所属、役職をまとめて「ユーザ情報」ともいう。また、本実施例では、各ユーザの所属、役職、ポリシーを配布する時刻をまとめて「属性」ともいう。セキュリティポリシーデータベース１０９には、所属、役職、ポリシーを配布する時刻、ポリシー適用時の動作等を記述したデータ１１０が保存される。

[0017] 以下では、情報漏洩防止システム１００で実行される通信や動作の概略を説明する。なお、以下の動作１～５は、図中の（１）～（５）に対応している。

[0018] ・動作１

ユーザによって起動されたクライアントマシン１０３及び１１１は、予め登録されているユーザの情報（ユーザ名、所属、役職）と自機のＩＰアドレス（起動時）を管理サーバ１０６に送信する。クライアントマシン１０３及び１１１は、登録されているユーザ名、所属、役職、ＩＰアドレスのいずれかに変更があった場合、変更後のユーザ名、所属、役職、ＩＰアドレス（更新後）を管理サーバ１０６に送信する。管理サーバ１０６は、クライアントマシン１０３及び１１１から各ユーザのユーザ名、所属、役職、ＩＰアドレスの情報を受信すると、それらをユーザデータベース１０７に格納する。

[0019] ・動作２及び３

例えばクライアントマシン１０３がマルウェアに感染した場合、クライアントマシン１０３は、マルウェア対策ソフトウェア１０４が出力するマルウェア検知情報を管理サーバ１０６へ送信する。マルウェア検知情報には、検知日時とマルウェアの通信先であるＣ＆Ｃサーバ情報が含まれる。

[0020] ・動作４

管理サーバ１０６は、マルウェア検知情報を受信した場合、当該検知情報からＣ＆Ｃサーバ情報を摘出する。次に、管理サーバ１０６は、ポリシーを配布する現在時刻を特定し、特定した現在時刻でセキュリティポリシーデータベース１０９に格納されているデータ１１０を検索する。ここで、管理サーバ１０６は、現在時刻に関連する所属と役職の組み合わせについて登録されているセキュリティポリシーを選定する。また、管理サーバ１０６は、ユーザデータベース１０７に格納されているデータ１０８の中から、現在時刻に関連する所属と役職の組み合わせに対応する各ＩＰアドレスを摘出し、当該ＩＰアドレスに宛てて、各ユーザに対応するセキュリティポリシーとＣ＆Ｃサーバ情報を送信する。ここでの送信先は、マルウェアに感染したクライアントマシン１０３に限定されない。図１の場合は、クライアントマシン１０３及び１１１のいずれもがセキュリティポリシーとＣ＆Ｃサーバ情報の送信先となる。

[0021] ・動作５

セキュリティポリシーとＣ＆Ｃサーバ情報を受信したクライアントマシン１０３及び１１１は、受信したセキュリティポリシーの内容に応じ、Ｃ＆Ｃサーバ１０１との接続を切断し、又は、ネットワーク１０２との接続を切断する。図１の場合、クライアントマシン１０３はネットワーク１０２との接続を切断し、クライアントマシン１１１はＣ＆Ｃサーバ１０１との接続のみ切断する（ネットワークとの接続は維持する）。

[0022] （１－２）ユーザデータベースの構成

図２に、ユーザデータベース１０７に格納されているデータ１０８の構造

例を示す。ユーザデータベース１０７は、データ項目として、各ユーザのユーザ名２０１、所属２０２、役職２０３、クライアントマシンのＩＰアドレス２０４を有している。これらの情報は、起動時に、クライアントマシン１０３及び１１１から管理サーバ１０６に送信され、管理サーバ１０６により対応する項目位置に格納される。

[0023] 受信したユーザ名２０１がユーザデータベース１０７に既に登録されている場合、管理サーバ１０６は、既存のユーザ名２０１に紐付けられている所属２０２、役職２０３及びＩＰアドレス２０４の情報を新たに受信した情報で上書きする。受信したユーザ名２０１がユーザデータベース１０７に登録されていない場合、管理サーバ１０６は、受信したユーザ名２０１、所属２０２、役職２０３、ＩＰアドレス２０４を新たな行に格納する。管理サーバ１０６の管理者は、不要となった行をユーザデータベース１０７から削除することもできる。

[0024] （１－３）セキュリティポリシーデータベースの構成

図３に、セキュリティポリシーデータベース１０９に格納されているデータ１１０の構造例を示す。セキュリティポリシーデータベース１０９は、データ項目として、所属３０１、役職３０２、ポリシーを配布する時刻３０３、ポリシー適用時の動作３０４を有している。

[0025] 管理サーバ１０６は、クライアントマシン１０３及び１１１のいずれかからマルウェア検知情報を受信した場合、ポリシーを配布する現在時刻でセキュリティポリシーデータベース１０９を検索し、前記現在時刻を含む時刻３０３に含むユーザ（所属３０１と役職３０２の各組み合わせで特定される）に適用するセキュリティポリシー（ポリシー適用時の動作３０４）を選定する。

[0026] ポリシーを配布する現在時刻を含む時刻３０３に紐付けられた所属３０１及び役職３０２の組み合わせがセキュリティポリシーデータベース１０９に登録されていない場合、管理サーバ１０６は、ポリシー適用時の動作３０４が「ネットワーク接続禁止」であるものとして扱い、管理下にある全てのク

ライアントマシンに当該ポリシーを配布する。「ネットワーク接続禁止」は、最も厳しい動作である。管理サーバ１０６の管理者は、所属３０１、役職３０２及び時刻３０３の組み合わせ毎に、ポリシー適用時の動作３０４を設定することができ、その設定後も、データを変更又は削除できる。

[0027] （１－４）処理動作

（１－４－１）クライアントマシン起動時の動作

図４に、クライアントマシン起動時にクライアントマシン１０３及び１１１で実行される処理手順を示す。ユーザによってクライアントマシン１０３及び１１１が起動されると（ステップ４０１）、クライアント処理部１１４はＯＳ（Operation System）にログインする（ステップ４０２）。次に、クライアント処理部１１４は、自身のＩＰアドレスを取得する（ステップ４０３）。続いて、クライアント処理部１１４は、ステップ４０３で取得した自身のＩＰアドレスと、予め登録されているユーザのユーザ情報（ユーザ名、所属、役職の情報）とを管理サーバ１０６に送信する（ステップ４０４）。

[0028] 図５に、クライアントマシン起動時に管理サーバ１０６で実行される処理手順を示す。管理サーバ１０６のサーバ処理部１１５は、クライアントマシン１０３及び１１１からＩＰアドレスとユーザ情報を受信する（ステップ５０１）。ここでのユーザ情報は、前記ステップ４０４で送信されたユーザ情報である。次に、サーバ処理部１１５は、受信したユーザ情報に含まれるユーザ名がユーザデータベース１０７に登録されているか否か確認する（ステップ５０２）。ユーザ名がユーザデータベース１０７に登録されている場合、サーバ処理部１１５は、前記ユーザ名に対応付けられている所属２０２、役職２０３及びＩＰアドレス２０４の各情報を、受信したユーザ情報の内容で上書き更新する（ステップ５０３）。一方、ユーザ名がユーザデータベース１０７に登録されていない場合、サーバ処理部１１５は、受信したユーザ情報の内容をユーザデータベース１０７に新規登録する（ステップ５０４）。

[0029] （１－４－２）マルウェア感染時の動作

図６に、マルウェアに感染したクライアントマシン１０３で実行される処理手順を示す。マルウェアへの感染は、クライアントマシン１０３で実行中のマルウェア対策ソフトウェア１０４によって検知される。マルウェアの感染を検知すると、マルウェア対策ソフトウェア１０４は、マルウェア検知情報を出力する（ステップ６０１）。続いて、クライアントマシン１０３のクライアント処理部１１４が、マルウェア検知情報を管理サーバ１０６に送信する（ステップ６０２）。

[0030] その後、クライアント処理部１１４は、管理サーバ１０６からセキュリティポリシーとＣ＆Ｃサーバ情報を受信する（ステップ６０３）。ここで、クライアント処理部１１４は、受信したセキュリティポリシーに含まれるポリシー適用時の動作が、「ネットワーク接続禁止」か「Ｃ＆Ｃサーバ接続禁止」かを確認する（ステップ６０４）。ポリシー適用時の動作が「ネットワーク接続禁止」であった場合、クライアント処理部１１４は、ネットワーク１０２への接続を切断し、自身をネットワークから隔離する（ステップ６０５）。一方、ポリシー適用時の動作が「Ｃ＆Ｃサーバ接続禁止」であった場合、クライアント処理部１１４は、受信したＣ＆Ｃサーバ情報に含まれるＣ＆Ｃサーバ１０１のアドレスに対してのみ接続を禁止する（ステップ６０６）。なお、マルウェアに感染していないクライアントマシン１１１では、ステップ６０３以降の動作が実行される。

[0031] 図７に、マルウェアへの感染が通知された管理サーバ１０６で実行される処理手順を示す。サーバ処理部１１５は、クライアントマシン１０３からマルウェア検知情報を受信する（ステップ７０１）。ここでのマルウェア検知情報は、前記ステップ６０２で送信されたマルウェア検知情報である。次に、サーバ処理部１１５は、ポリシーを配布する現在時刻に基づいてポリシーデータベース１０９を検索し、前記現在時刻を含む時刻３０３を有する所属と役職の組み合わせ毎に、配布するセキュリティポリシー（ポリシー適用時の動作３０４）を選定する（ステップ７０２）。ここでは、複数の組み合わせが選定され得る。

[0032] 次に、サーバ処理部１１５は、セキュリティポリシーが選定されたユーザを特定する所属及び役職の組み合わせと、ユーザデータベース１０７の所属と役職の組み合わせとを比較し、各ユーザに配布するセキュリティポリシーの送信先のＩＰアドレスを決定する（ステップ７０３）。この後、サーバ処理部１１５は、決定されたＩＰアドレスに宛てて、対応するセキュリティポリシーとＣ＆Ｃサーバ情報を送信する（ステップ７０４）。ここでのセキュリティポリシーとＣ＆Ｃサーバ情報は、前記ステップ６０３でクライアントマシンが受信したセキュリティポリシーとＣ＆Ｃサーバ情報である。

[0033] （１－５）まとめ

前述したように、本実施例の情報漏洩防止システム１００を構成するネットワーク１０２には、ファイアウォール装置も中継装置も存在しないが、クライアントマシン１０３及び１１１からＣ＆Ｃサーバ１０１への情報送信をブロックし又はクライアントマシン１０３及び１１１をネットワーク１０２から隔離することができる。また、クライアントマシン１０３及び１１１に適用されるセキュリティポリシー（ポリシー適用時の動作）は、ユーザの所属と役職の組み合わせに応じて決定することができる。すなわち、クライアントマシン１０３及び１１１を使用するユーザの属性に応じてセキュリティポリシーの強弱を変化させることができる。

[0034] （２）実施例２

（２－１）システム構成

本実施例では、クライアントマシンの位置情報を加味してセキュリティポリシーを決定し、クライアントマシンのネットワーク接続やＣ＆Ｃサーバへのアクセスを制御し、情報漏洩を防止するシステムついて説明する。図８に、本実施例に係る情報漏洩防止システム２００の全体構成を示す。図８には、図１との対応部分に同一又は類似の符号を付して示す。図８より分かるように、情報漏洩防止システム２００の基本構成は、実施例１の情報漏洩防止システム１００と同じである。

[0035] クライアントマシン８０３及び８１１はそれぞれ、コンピュータを基本構

成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース等で構成される。本実施例の場合、クライアントマシン８０３及び８１１には、ＣＰＵによるプログラムの実行を通じて機能が提供されるマルウェア対策ソフトウェア１０４とクライアント処理部８１４が実装されている。本実施例のクライアントマシン８０３及び８１１には、更にＧＰＳ端末８０５が実装されている。ＧＰＳ端末８０５はクライアントマシン８０３に対して外付けされてもよい。ＧＰＳ端末８０５は、各クライアントマシン８０３及び８１１の物理的な位置情報（緯度、経度、高度）を取得している。

[0036] クライアント処理部８１４は、ＣＰＵによるプログラムの実行を通じ、ユーザ情報送信機能、位置情報処理機能、マルウェア検知情報送信機能、ネットワーク制御機能を提供する。このうち、実施例１と異なる機能は、位置情報処理機能である。位置情報処理機能は、位置情報の要求に応じてＧＰＳ端末８０５から現在の位置情報を取得し、要求元（管理サーバ８０６）に送信する。クライアント処理部８１４が物理的な位置情報を管理上の位置情報（例えば社内、社外、顧客先、社員宅等）に変換するテーブルを有している場合、位置情報として管理上の位置情報を送信してもよい。変換に用いるテーブルは、クライアント処理部８１４内に事前に登録されていてもよいし、管理サーバ８０６から通知されてもよい。

[0037] 管理サーバ８０６は、コンピュータを基本構成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース等で構成される。管理サーバ１０６には必要に応じて表示装置も接続される。本実施例の管理サーバ８０６には、ユーザデータベース（データベース）８０７、セキュリティポリシーデータベース（ＤＢ）８０９、サーバ処理部８１５が実装されている。

[0038] サーバ処理部８１５は、ＣＰＵによるプログラムの実行を通じ、ユーザ情報管理機能、位置情報管理機能、セキュリティポリシー管理機能、セキュリティポリシー送信機能を提供する。このうち、実施例１と異なる機能は、位

置情報管理機能である。位置情報管理機能は、マルウェア検知情報を受信した場合に、クライアントマシン８０３及び８１１に対して現在の位置情報を要求する。位置情報管理機能は、クライアントマシン８０３及び８１１から位置情報を受信した場合、受信した位置情報をユーザデータベース８０７に登録する。位置情報管理機能は、ＧＰＳ端末８０５が出力するＧＰＳ情報をそのまま位置情報として受信する場合、物理的な位置情報であるＧＰＳ情報を管理上の位置情報に変換し、ユーザデータベース８０７に登録する。なお、位置情報管理機能にＧＰＳ情報を管理上の位置情報に変換するテーブルをクライアントマシン８０３及び８１１に送信する機能を実装してもよい。

[0039] 本実施例の場合、管理サーバ８０６のサーバ処理部８１５は、マルウェア検知情報を受信すると、マルウェア検知情報からＣ＆Ｃサーバ情報を摘出する。また、サーバ処理部８１５は、ポリシーを配布する現在時刻に基づいてセキュリティポリシーデータベース８０９のデータ８１０を検索する。ここで、管理サーバ８０６は、現在時刻に関連する所属と役職の組み合わせについて登録されているセキュリティポリシーの候補と位置情報の組み合わせを選定する。また、管理サーバ８０６は、選定された組み合わせの位置情報と受信した位置情報を照合し、一致する位置情報を含む組み合わせに体操するセキュリティポリシーを該当するユーザに適用するセキュリティポリシーに決定する。また、管理サーバ８０６は、決定された組み合わせの所属と役職に対応するＩＰアドレスをユーザデータベース８０７から摘出し、当該ＩＰアドレスに宛てて、各ユーザに対応するセキュリティポリシーとＣ＆Ｃサーバ情報を送信する。

[0040] （２－２）ユーザデータベースの構成

図９に、ユーザデータベース８０７に格納されるデータ８０８の構造例を示す。ユーザデータベース８０７は、データ項目として、各ユーザのユーザ名９０１、所属９０２、役職９０３、クライアントマシンのＩＰアドレス９０４、位置情報９０５を有している。位置情報９０５以外の情報は、起動時に、クライアントマシン８０３及び８１１から管理サーバ８０６に送信され

、管理サーバ８０６によりユーザデータベース８０７に格納される。

[0041] 受信したユーザ名９０１がユーザデータベース８０７に既に登録されている場合、管理サーバ８０６は、既存のユーザ名９０１に紐付けられている所属９０２、役職９０３及びＩＰアドレス９０４の情報を新たに受信した情報で上書きする。受信したユーザ名９０１がユーザデータベース８０７に登録されていない場合、管理サーバ８０６は、受信したユーザ名９０１、所属９０２、役職９０３、ＩＰアドレス９０４を新たな行に格納する。

[0042] 管理サーバ８０６は、クライアントマシン８０３及び８１１から位置情報９０５を受信した場合、位置情報９０５の送信元であるＩＰアドレス９０４でユーザデータベース８０７内を検索し、ＩＰアドレス９０４が一致した行に受信した位置情報９０５を格納する。本実施例の場合、位置情報９０５には管理上の位置情報が記録される。

[0043] クライアントマシン８０３及び８１１は、起動時及びＩＰアドレスの変更時にユーザ情報を管理サーバ８０６に送信するため、位置情報９０５の送信元であるＩＰアドレス９０４は、必ずユーザデータベース８０７に格納されている。すなわち、位置情報９０５の送信元であるＩＰアドレス９０４がユーザデータベース８０７に格納されていない場合は考慮しない。

[0044] （２－３）セキュリティポリシーデータベースの構成

図１０に、セキュリティポリシーデータベース８０９に格納されているデータ８１０の構造例を示す。セキュリティポリシーデータベース８０９は、データ項目として、所属１００１、役職１００２、時刻１００３、位置情報１００４、ポリシー適用時の動作１００５を有している。本実施例の場合、位置情報１００４には管理上の位置情報が記録される。

[0045] 管理サーバ８０６は、クライアントマシン８０３及び８１１のいずれかからマルウェア検知情報を受信した場合、セキュリティポリシーデータベース８０９を参照し、ポリシーを配布する現在時刻を含むユーザの所属１００１、役職１００２、ポリシーを配布する時刻１００３及び位置情報１００４の組み合わせについて登録されているセキュリティポリシー（ポリシー適用時

の動作１００５）を候補に選定する。この時点では、位置情報による絞り込みが行われていないため、セキュリティポリシーを決定できない。

[0046] ポリシーを配布する現在時刻を含む時刻１００３、所属１００１、役職１００２及び位置情報１００４の組み合わせがセキュリティポリシーデータベース８０９に登録されていない場合、管理サーバ８０６は、ポリシー適用時の動作１００５が「ネットワーク接続禁止」であるものとして扱い、管理下にある全てのクライアントマシンに当該ポリシーを配布する。管理サーバ８０６の管理者は、所属１００１、役職１００２、時刻１００３及び位置情報１００４の組み合わせ毎に、ポリシー適用時の動作１００５を設定することができ、その設定後も、データを変更又は削除できる。

[0047] （２－４）処理動作

クライアントマシン起動時の動作は実施例１と基本的に同じであるため、以下では、マルウェア感染時の動作のみを説明する。図１１に、マルウェアに感染したクライアントマシン８０３で実行される処理手順を示す。マルウェアへの感染は、クライアントマシン８０３で実行中のマルウェア対策ソフトウェア１０４によって検知される。マルウェアの感染を検知すると、マルウェア対策ソフトウェア１０４は、マルウェア検知情報を出力する（ステップ１１０１）。続いて、クライアントマシン８０３のクライアント処理部８１４が、マルウェア検知情報を管理サーバ８０６に送信する（ステップ１１０２）。

[0048] その後、クライアント処理部８１４は、管理サーバ８０６から位置情報取得要求を受信する（ステップ１１０３）。クライアント処理部８１４は、ＧＰＳ端末８０５から位置情報を取得し、取得した位置情報を管理サーバ８０６に送信する（ステップ１１０４）。

[0049] その後、クライアント処理部８１４は、管理サーバ８０６からセキュリティポリシーとＣ＆Ｃサーバ情報を受信する（ステップ１１０５）。ここで、クライアント処理部８１４は、受信したセキュリティポリシーに含まれるポリシー適用時の動作が、「ネットワーク接続禁止」か「Ｃ＆Ｃサーバ接続禁

止」かを確認する（ステップ１１０６）。

[0050] ポリシー適用時の動作が「ネットワーク接続禁止」であった場合、クライアント処理部８１４は、ネットワーク１０２への接続を切断し、自身をネットワークから隔離する（ステップ１１０７）。一方、ポリシー適用時の動作が「Ｃ＆Ｃサーバ接続禁止」であった場合、クライアント処理部８１４は、受信したＣ＆Ｃサーバ情報に含まれるＣ＆Ｃサーバ１０１のアドレスに対してのみ接続を禁止する（ステップ１１０８）。なお、マルウェアに感染していないクライアントマシン８１１では、ステップ１１０３以降の動作が実行される。

[0051] 図１２に、マルウェアへの感染が通知された管理サーバ８０６で実行される処理手順を示す。サーバ処理部８１５は、クライアントマシン８０３からマルウェア検知情報を受信する（ステップ１２０１）。ここでのマルウェア検知情報は、前記ステップ１１０２で送信されたマルウェア検知情報である。

[0052] 次に、サーバ処理部８１５は、位置情報取得要求をクライアントマシン８０３及び８１１に送信する（ステップ１２０２）。すなわち、サーバ処理部８１５は、マルウェアの感染を検知したクライアントマシン８０３だけでなく、管理下にある全てのクライアントマシンに位置情報取得要求を送信する。その後、サーバ処理部８１５は、クライアントマシン８０３及び８１１から位置情報を受信する（ステップ１２０３）。ここでの位置情報は、前記ステップ１１０４で送信された位置情報である。次に、サーバ処理部８１５は、受信した位置情報をユーザデータベース８０７に格納する（ステップ１２０４）。

[0053] 次に、サーバ処理部８１５は、ポリシーを配布する現在時刻に基づいてポリシーデータベース８０９を検索し、前記現在時刻を含む時刻１００３を有するユーザについて登録されているセキュリティポリシー（ポリシー適用時の動作１００５）と位置情報１００４の組み合わせを選定する（ステップ１２０５）。

[0054] 次に、サーバ処理部８１５は、ステップ１２０５で選定したセキュリティポリシーに対応するユーザの位置情報１００４とユーザデータベース８０７に登録されている位置情報９０５とを比較して一致するユーザ（すなわち、時刻１００３と位置情報１００４の両方の条件を満たすユーザ）の属性とセキュリティポリシーを特定する。更に、サーバ処理部８１５は、ユーザデータベース８０７から、特定された属性と位置情報９０５に対応するユーザのＩＰアドレスを決定する（ステップ１２０６）。

[0055] この後、サーバ処理部８１５は、決定されたＩＰアドレスに宛てて、対応するセキュリティポリシーとＣ＆Ｃサーバ情報を送信する（ステップ１２０７）。ここでのセキュリティポリシーとＣ＆Ｃサーバ情報は、前記ステップ１１０５でクライアントマシンが受信したセキュリティポリシーとＣ＆Ｃサーバ情報である。

[0056] （２－５）まとめ

情報漏洩防止システム２００の場合も、ファイアウォール装置や中継装置が存在しないネットワークでも、クライアントマシン８０３及び８１１からＣ＆Ｃサーバ１０１への情報送信をブロックし又はクライアントマシン８０３及び８１１をネットワーク１０２から隔離することができる。また、クライアントマシン８０３及び８１１に適用されるセキュリティポリシー（ポリシー適用時の動作）は、ユーザの所属と役職とポリシーを配布する時刻に、位置情報の情報も組み合わせて決定することができる。すなわち、実施例１の場合によりも複雑な、換言すると柔軟なセキュリティポリシーの適用が可能になる。

[0057] （３）実施例３

（３－１）システム構成

本実施例では、ネットワーク管理者の在席人数を加味してセキュリティポリシーを決定し、クライアントマシンのネットワーク接続やＣ＆Ｃサーバへのアクセスを制御し、情報漏洩を防止するシステムついて説明する。本実施例の場合、ネットワーク管理者は、例えばシステム部門に属する全てのスタ

ッフ、各部門の管理職スタッフを想定する。

[0058] 図１３に、本実施例に係る情報漏洩防止システム３００の全体構成を示す。図１３には、図１との対応部分に同一又は類似の符号を付して示す。図１３より分かるように、情報漏洩防止システム３００の基本構成は、実施例１の情報漏洩防止システム１００と同じである。

[0059] クライアントマシン１３０３及び１３１１はそれぞれ、コンピュータを基本構成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース等で構成される。本実施例の場合、クライアントマシン１３０３及び１３１１には、ＣＰＵによるプログラムの実行を通じて機能が提供されるマルウェア対策ソフトウェア１０４とクライアント処理部１３１４が実装されている。

[0060] クライアント処理部１３１４は、ＣＰＵによるプログラムの実行を通じ、ユーザ情報送信機能、在席情報処理機能、マルウェア検知情報送信機能、ネットワーク制御機能を提供する。このうち、実施例１と異なる機能は、在席情報処理機能である。在席情報処理機能は、管理サーバ１３０６から在席情報送信要求（ping）を受信した場合に、ＰＣが起動中であれば応答（echo reply）を管理サーバ１３０６に送信する機能を提供する。

[0061] 管理サーバ１３０６は、コンピュータを基本構成とし、ＣＰＵ、ＲＡＭ、ＲＯＭ、ハードディスク装置、ネットワークインタフェース等で構成される。管理サーバ１３０６には必要に応じて表示装置も接続される。本実施例の管理サーバ１３０６には、ユーザデータベース（データベース）１３０７、セキュリティポリシーデータベース（データベース）１３０９、サーバ処理部１３１５が実装されている。

[0062] サーバ処理部１３１５は、ＣＰＵによるプログラムの実行を通じ、ユーザ情報管理機能、在席情報管理機能、セキュリティポリシー管理機能、セキュリティポリシー送信機能を提供する。このうち、実施例１と異なる機能は、在席情報管理機能である。在席情報管理機能は、マルウェア検知情報を受信した場合に、管理下にある全てのクライアントマシン１３０３及び１３１１

に対してpingを送信する機能を提供する。また、在席情報管理機能は、pingへの応答（echo reply）を受信した場合、その送信元のクライアントマシン１３０３及び１３１１のユーザがネットワーク管理者か否か判定し、ネットワーク管理者であれば在席情報をユーザデータベース１３０７に登録する機能を提供する。

[0063] 本実施例のセキュリティポリシー送信機能は、pingを送信した全てのクライアントマシン１３０３及び１３１１から応答（echo reply）を受信した場合、又は、タイムアウトとなった場合、受信したマルウェア検知情報からＣ＆Ｃサーバ情報を摘出し、ユーザデータベース１３０７に格納されているデータ１３０８から在席中のネットワーク管理者の人数をカウントする。また、本実施例のセキュリティポリシー送信機能は、ポリシーを配布する現在時刻と算出したネットワーク管理者の人数とに基づいて、当該条件に合致する所属と役職の組み合わせと、当該組み合わせについて適用するセキュリティポリシーをセキュリティポリシーデータベース１３０９から選定する。更に、本実施例のセキュリティポリシー送信機能は、選定されたセキュリティポリシーに対応する所属と役職の組み合わせに対応するＩＰアドレスをユーザデータベース１３０７から摘出し、当該ＩＰアドレスに先に選定したセキュリティポリシーとＣ＆Ｃサーバ情報を送信する。

[0064] （３－２）ユーザデータベースの構成

図１４に、ユーザデータベース１３０７に格納されるデータ１３０８の構造例を示す。ユーザデータベース１３０７は、データ項目として、各ユーザのユーザ名１４０１、所属１４０２、役職１４０３、クライアントマシンのＩＰアドレス１４０４、在席情報１４０５を有している。在席情報１４０５以外の情報は、起動時に、クライアントマシン１３０３及び１３１１から管理サーバ１３０６に送信され、管理サーバ１３０６によりユーザデータベース１３０７に格納される。

[0065] 受信したユーザ名１４０１がユーザデータベース１３０７に既に登録されている場合、管理サーバ１３０６は、既存のユーザ名１４０１に紐付けられ

ている所属１４０２、役職１４０
３及びＩＰアドレス１４０４を新たに受信した情報で上書きする。受信したユーザ名１４０１がユーザデータベース１３０７に登録されていない場合、管理サーバ１３０６は、受信したユーザ名１４０１、所属１４０２、役職１４０３、ＩＰアドレス１４０４を新たな行に格納する。

[0066] 管理サーバ１３０６は、pingの送信に対してecho replyを受信した場合、pingの送信先であるＩＰアドレス１４０４を用いてユーザデータベース１３０７内を検索し、ＩＰアドレス１４０４が一致するユーザの役職１４０３が課長以上であれば在席情報１４０５に「在席」を格納する。この機能は、在席情報管理機能が実行する。

[0067] クライアントマシン１３０３及び１３１１は、起動時及びＩＰアドレスの変更時にユーザ情報を管理サーバ１３０６に送信するため、pingの送信先であるＩＰアドレス１４０４は、必ずユーザデータベース１３０７に格納されているものとし、pingの送信先であるＩＰアドレス１４０４がユーザデータベース１３０７内に格納されていない場合は考慮しない。

[0068] （３－３）セキュリティポリシーデータベースの構成

図１５に、セキュリティポリシーデータベース１３０９に格納されているデータ１３１０の構造例を示す。セキュリティポリシーデータベース１３０８は、データ項目として、所属１５０１、役職１５０２、ポリシーを配布する時刻１５０３、ポリシーの適用に必要なネットワーク管理者の在席人数１５０４、ポリシー適用時の動作１５０５を有している。

[0069] 管理サーバ１３０６は、クライアントマシン１３０３及び１３１０のいずれかからマルウェア検知情報を受信した後、pingの送信先の全てからecho replyを受信した場合、又は、タイムアウトとなった場合、ユーザデータベース１３０７から在席中のネットワーク管理者の人数をカウントする。更に、管理サーバ１３０６は、ユーザデータベース１３０７からカウントされたネットワーク管理者の人数とポリシーを配布する現在時刻とに基づいてセキュリティポリシーデータベース１３０９を参照し、条件に合致するユーザの所属

１５０１、役職１５０２、適用するセキュリティポリシー（ポリシー適用時の動作１５０５）を選定する。

[0070] ポリシーを配布する現在時刻を含む時刻１５０３及び管理者の在席人数１５０４を含む所属１５０１、役職１５０２、時刻１５０３、管理者の在席人数１５０４の組み合わせがセキュリティポリシーデータベース１３０９に登録されていない場合、管理サーバ１３０６は、ポリシー適用時の動作１５０５が「ネットワーク接続禁止」であるものとして扱い、管理下にある全てのクライアントマシンに当該ポリシーを配布する。管理サーバ１３０６の管理者は、所属１５０１、役職１５０２、時刻１５０３及び管理者の在席人数１５０４の組み合わせ毎に、ポリシー適用時の動作１５０５を設定することができ、その設定の後も、データを変更又は削除できる。

[0071] （３－４）処理動作

クライアントマシン起動時の動作は実施例１と基本的に同じであるため、以下では、マルウェア感染時の動作のみを説明する。図１６に、マルウェアに感染したクライアントマシン１３０３で実行される処理手順を示す。マルウェアへの感染は、クライアントマシン１３０３で実行中のマルウェア対策ソフトウェア１０４によって検知される。マルウェアの感染を検知すると、マルウェア対策ソフトウェア１０４は、マルウェア検知情報を出力する（ステップ１６０１）。続いて、クライアントマシン１３０３のクライアント処理部１３１４が、マルウェア検知情報を管理サーバ１３０６に送信する（ステップ１６０２）。

[0072] その後、クライアント処理部１３１４は、管理サーバ１３０６からpingを受信する（ステップ１６０３）。クライアント処理部１３１４は、echo replyを管理サーバ１３０６に送信する（ステップ１６０４）。

[0073] その後、クライアント処理部１３１４は、管理サーバ１３０６からセキュリティポリシーとＣ＆Ｃサーバ情報を受信する（ステップ１６０５）。ここで、クライアント処理部１３１４は、受信したセキュリティポリシーに含まれるポリシー適用時の動作が、「ネットワーク接続禁止」か「Ｃ＆Ｃサーバ

接続禁止」かを確認する（ステップ１６０６）。

[0074] ポリシー適用時の動作が「ネットワーク接続禁止」であった場合、クライアント処理部１３１４は、ネットワーク１０２への接続を切断し、自身をネットワークから隔離する（ステップ１６０７）。一方、ポリシー適用時の動作が「Ｃ＆Ｃサーバ接続禁止」であった場合、クライアント処理部１３１４は、受信したＣ＆Ｃサーバ情報に含まれるＣ＆Ｃサーバ１０１のアドレスに対してのみ接続を禁止する（ステップ１６０８）。なお、マルウェアに感染していないクライアントマシン１３１１では、ステップ１６０３以降の動作が実行される。

[0075] 図１７に、マルウェアへの感染が通知された管理サーバ１３０６で実行される処理手順を示す。サーバ処理部１３１５は、クライアントマシン１３０３からマルウェア検知情報を受信する（ステップ１７０１）。ここでのマルウェア検知情報は、前記ステップ１６０２で送信されたマルウェア検知情報である。

[0076] 次に、サーバ処理部１３１５は、pingをクライアントマシン１３０３及び１３１１に送信する（ステップ１７０２）。すなわち、サーバ処理部１３１５は、マルウェアの感染を検知したクライアントマシン１３０３だけでなく、管理下にある全てのクライアントマシンに位置情報取得要求を送信する。その後、サーバ処理部１３１５は、クライアントマシン１３０３及び１３１１からecho replyを受信する（ステップ１７０３）。ここでのecho replyは、前記ステップ１６０４で送信されたecho replyである。ただし、クライアントマシン１３０３及び１３１１の全てからecho replyが受信できるとは限らない。

[0077] 次に、サーバ処理部１３１５は、echo replyを送信したクライアントマシンを使用するユーザの在席情報をユーザデータベース１３０７に格納する（ステップ１７０４）。ただし、サーバ処理部１３１５は、ネットワーク管理者の在席情報のみをユーザデータベース１３０７に登録し、それ以外のユーザは在席情報を登録しない。

[0078] サーバ処理部１３１５は、ポリシーを配布する現在時刻と在席中のネットワーク管理者の人数の組み合わせを満たすユーザに基づいて、配布するセキュリティポリシーを選定する（ステップ１７０５）。サーバ処理部１３１５は、ステップ１７０５で選定したセキュリティポリシーに対応するユーザのユーザ情報（所属及び役職）と、ユーザデータベース１３０７のユーザ情報（所属及び役職）を比較し、各セキュリティポリシーの送信先となるＩＰアドレスを決定する（ステップ１７０６）。

[0079] この後、サーバ処理部１３１５は、決定されたＩＰアドレスに宛てて、対応するセキュリティポリシーとＣ＆Ｃサーバ情報を送信する（ステップ１７０７）。ここでのセキュリティポリシーとＣ＆Ｃサーバ情報は、前記ステップ１６０５でクライアントマシンが受信したセキュリティポリシーとＣ＆Ｃサーバ情報である。

[0080] （３－５）まとめ

情報漏洩防止システム３００の場合も、ファイアウォール装置も中継装置も存在しないネットワークでも、クライアントマシン１３０３及び１３１１からＣ＆Ｃサーバ１０１への情報送信をブロックし又はクライアントマシン１３０３及び１３１１をネットワーク１０２から隔離することができる。また、クライアントマシン１３０３及び１３１１に適用されるセキュリティポリシー（ポリシー適用時の動作）は、ユーザの所属と役職とポリシーを配布する時刻に、ネットワーク管理者の在席人数も組み合わせて決定することができる。すなわち、実施例１の場合によりも複雑な、換言すると柔軟なセキュリティポリシーの適用が可能になる。

[0081] （４）他の実施例

本開示は、上述した実施例に限定されるものでなく、様々な変形例を含んでいる。例えば、上述した実施例は、本開示を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備える必要はない。また、ある実施例の一部を他の実施例の構成に置き換えることができる。また、ある実施例の構成に他の実施例の構成を加えることもできる。また

、各実施例の構成の一部について、他の実施例の構成の一部を追加、削除又は置換することもできる。

[0082] また、上述した各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現しても良い。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することにより（すなわちソフトウェア的に）実現しても良い。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリ、ハードディスク、SSD（Solid State Drive）等の記憶装置、又は、ICカード、SDカード、DVD等の記憶媒体に格納することができる。また、制御線や情報線は、説明上必要と考えられるものを示すものであり、製品上必要な全ての制御線や情報線を表すものでない。実際にはほとんど全ての構成が相互に接続されていると考えて良い。

符号の説明

[0083] １００…情報漏洩防止システム、

１０１…Ｃ＆Ｃサーバ１０１

１０２…ネットワーク、

１０３、１１１…クライアントマシン、

１０４…マルウェア対策ソフトウェア、

１０６…管理サーバ、

１０７…ユーザデータベース、

１０９…セキュリティポリシーデータベース、

１１４…クライアント処理部、

１１５…サーバ処理部、

２００…情報漏洩防止システム、

８０３、２１１…クライアントマシン、

８０６…管理サーバ、

８０７…ユーザデータベース、

８０９…セキュリティポリシーデータベース、

８１４…クライアント処理部、

８１５…サーバ処理部、

３００…情報漏洩防止システム、

１３０３、１３１１…クライアントマシン、

１３０６…管理サーバ、

１３０７…ユーザデータベース、

１３０９…セキュリティポリシーデータベース、

１３１４…クライアント処理部、

１３１５…サーバ処理部。

請求の範囲

[請求項1] 取得したセキュリティポリシーに応じてネットワーク制御を行うクライアント処理部を有するクライアント端末と、

前記クライアント端末を利用するユーザに関する情報を格納するユーザデータベースと、ユーザの属性ごとにネットワーク制御内容を定めたセキュリティポリシーを格納するセキュリティポリシーデータベースと、ユーザの属性及び前記セキュリティポリシーを配布する時刻に基づいて前記セキュリティポリシーを選択し、選択された前記セキュリティポリシーを対応する前記クライアント端末に送信するサーバ処理部とを有する管理サーバと　を有する情報漏洩防止システム。

[請求項2] 請求項１に記載の情報漏洩防止システムにおいて、

前記サーバ処理部は、

前記クライアント端末から取得したユーザ情報を前記ユーザデータベースに格納するユーザ情報管理機能部と、

前記時刻に基づいて前記セキュリティポリシーデータベースを検索して前記ユーザの所属及び役職の組み合わせに対応付けられた前記セキュリティポリシーを選択するセキュリティポリシー管理機能部と、

選択した前記セキュリティポリシーに対応する所属及び役職に基づいて前記ユーザデータベースを検索して送信先となるクライアント端末のＩＰアドレスを取得し、前記ＩＰアドレスを有する前記クライアント端末に前記セキュリティポリシー及びＣ＆Ｃサーバ情報を送信するセキュリティポリシー送信機能部と

を更に有することを特徴とする情報漏洩防止システム。

[請求項3] 請求項１に記載の情報漏洩防止システムにおいて、

前記サーバ処理部は、

前記クライアント端末から取得したユーザ情報を前記ユーザデータベースに格納するユーザ情報管理機能部と、

前記クライアント端末からマルウェア検知情報を受信すると、前記

クライアント端末に対して位置情報の送信を要求して取得し、取得した前記位置情報を前記ユーザデータベースに格納する位置情報管理機能部と、

前記時刻に基づいて前記セキュリティポリシーデータベースを検索して前記ユーザの所属及び役職毎のセキュリティポリシーの候補を選択し、選択された前記セキュリティポリシーの候補のうち、前記ユーザデータベースに格納した位置情報と一致する位置情報に対応するセキュリティポリシーを選択し、選択した前記セキュリティポリシーに対応する所属及び役職に基づいて前記ユーザデータベースを検索して送信先となるクライアント端末のＩＰアドレスを取得し、前記ＩＰアドレスを有する前記クライアント端末に前記セキュリティポリシー及びＣ＆Ｃサーバ情報を送信するセキュリティポリシー管理機能部と

を更に有することを特徴とする情報漏洩防止システム。

[請求項4] 請求項１に記載の情報漏洩防止システムにおいて、

前記サーバ処理部は、

前記クライアント端末から取得したユーザ情報を前記ユーザデータベースに格納するユーザ情報管理機能部と、

前記クライアント端末へ送信した在席情報送信要求に対する応答の有無によりユーザの在席情報を取得し、前記ユーザデータベースに格納する在席情報管理機能部と、

前記ユーザデータベースを検索して管理者の在席人数を算出し、算出された前記在席人数及び前記時刻に基づいて前記セキュリティポリシーデータベースを検索して、前記ユーザの所属及び役職の組み合わせに対応する前記セキュリティポリシーを選択し、選択した前記セキュリティポリシーに対応する所属及び役職に基づいて前記ユーザデータベースを検索して送信先となるクライアント端末のＩＰアドレスを取得し、前記ＩＰアドレスを有する前記クライアント端末に前記セキュリティポリシー及びＣ＆Ｃサーバ情報を送信するセキュリティポリ

シー管理機能部と

を更に有することを特徴とする情報漏洩防止システム。

[請求項5] 請求項１に記載の情報漏洩防止システムにおいて、

前記クライアント処理部は、

前記クライアント端末を使用するユーザの情報を管理サーバに送信するユーザ情報送信機能部と、

Ｃ＆Ｃサーバ情報及びマルウェアに感染したクライアント端末を利用するユーザの情報を含むマルウェア検知情報を前記管理サーバに送信するマルウェア検知情報送信機能部と、

前記セキュリティポリシー及び前記Ｃ＆Ｃサーバ情報を前記管理サーバから取得するセキュリティポリシー受信機能部と、

取得した前記セキュリティポリシーがネットワークへの接続を禁止している場合、前記クライアント端末からのネットワークへの接続を禁止し、取得した前記セキュリティポリシーが前記Ｃ＆Ｃサーバへの接続を禁止している場合、前記クライアント端末から前記Ｃ＆Ｃサーバへの接続を禁止するネットワーク制御機能部と、

を更に有することを特徴とする情報漏洩防止システム。

[請求項6] 請求項５に記載の情報漏洩防止システムにおいて、

前記クライアント処理部は、

前記管理サーバからの位置情報の送信要求を受信すると、自端末の位置情報を取得して前記管理サーバに送信する位置情報処理機能部

を更に有することを特徴とする情報漏洩防止システム。

[請求項7] 請求項５に記載の情報漏洩防止システムにおいて、

前記クライアント処理部は、

前記管理サーバから受信した在席情報送信要求への応答を前記管理サーバに送信する在席情報処理機能部

を更に有することを特徴とする情報漏洩防止システム。

[請求項8] クライアント端末と管理サーバとを有する情報漏洩防止システムに

おいて実行される情報漏洩防止方法において、

マルウェアへの感染を検知した前記クライアント端末が、Ｃ＆Ｃサーバ情報及び自端末を利用するユーザの情報を含むマルウェア検知情報を前記管理サーバに送信する処理と、　前記マルウェア検知情報を受信した前記管理サーバが、セキュリティポリシーを配布する時刻に基づいてユーザの属性ごとにネットワーク制御内容を定めたセキュリティポリシーを格納するセキュリティポリシーデータベースを検索して前記セキュリティポリシーを選択する処理と、

前記管理サーバが、選択された前記セキュリティポリシーと前記Ｃ＆Ｃサーバ情報を対応する前記クライアント端末に送信する処理と、

前記クライアント端末が、前記セキュリティポリシー及び前記Ｃ＆Ｃサーバ情報を前記管理サーバから受信する処理と、

前記クライアント端末が、取得した前記セキュリティポリシーがネットワークへの接続を禁止している場合、自端末からのネットワークへの接続を禁止し、取得した前記セキュリティポリシーが前記Ｃ＆Ｃサーバへの接続を禁止している場合、自端末から前記Ｃ＆Ｃサーバへの接続を禁止する処理と

を有することを特徴とする情報漏洩防止方法。

[請求項9]　請求項８に記載の情報漏洩防止方法において、

前記マルウェア検知情報を受信した前記管理サーバが、前記クライアント端末に対して位置情報の送信を要求する処理と、

前記位置情報の送信の要求を受信した前記クライアント端末が、自端末の位置情報を取得して前記管理サーバに送信する処理と、

前記管理サーバが、前記クライアント端末から受信した前記位置情報を、前記クライアント端末を利用するユーザに関する情報を格納するユーザデータベースに格納する処理と　を更に有し、

前記管理サーバによる前記セキュリティポリシーを選択する処理において、前記管理サーバが、前記時刻に基づいて選択したユーザの属

性毎のセキュリティポリシーの候補の中から、前記ユーザデータベースに格納した位置情報と一致する位置情報に対応するセキュリティポリシーを選択する

ことを特徴とする情報漏洩防止方法。

[請求項10] 請求項８に記載の情報漏洩防止方法において、

前記マルウェア検知情報を受信した前記管理サーバが、前記クライアント端末に対して在席情報送信要求を送信する処理と、

前記クライアント端末が、受信した前記在席情報送信要求に対して応答する処理と、

前記管理サーバが、前記応答の有無によりユーザの在席情報を取得し、前記クライアント端末を利用するユーザに関する情報を格納するユーザデータベースに格納する処理と

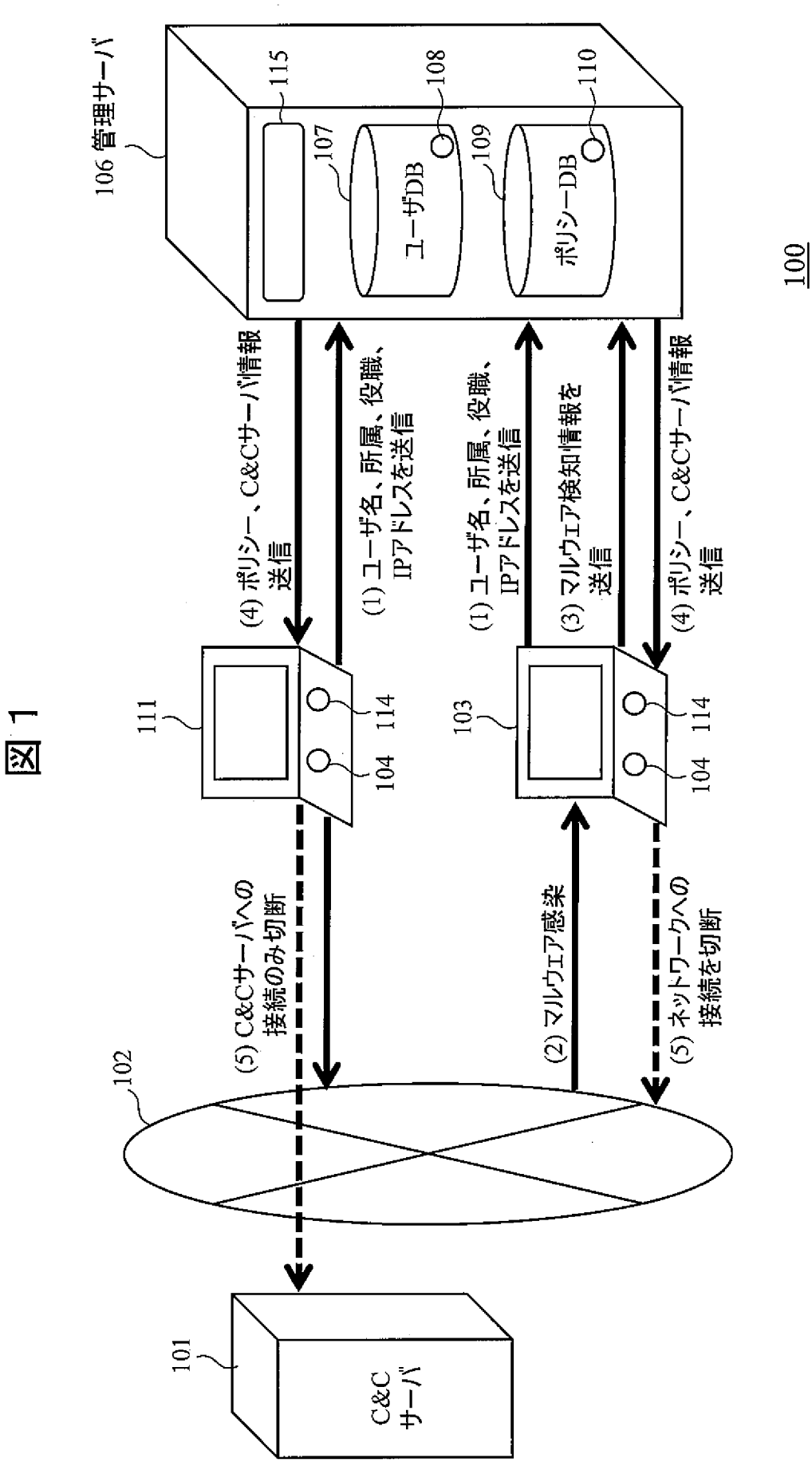
を更に有し、

前記管理サーバによる前記セキュリティポリシーを選択する処理において、前記管理サーバが、前記ユーザデータベースを検索して管理者の在席人数を算出し、算出された前記在席人数及び前記時刻に基づいて前記セキュリティポリシーデータベースを検索して、前記ユーザの属性の組み合わせに対応する前記セキュリティポリシーを選択する

ことを特徴とする情報漏洩防止方法。

[図1]

図 1


106 管理サーバ
115
107
108
ユーザDB
109
110
ポリシーDB
100
(4) ポリシー、C&Cサーバ情報 送信
(1) ユーザ名、所属、役職、IPアドレスを送信
(1) ユーザ名、所属、役職、IPアドレスを送信
(3) マルウェア検知情報を送信
(4) ポリシー、C&Cサーバ情報 送信
111
114
104
103
114
104
(5) C&Cサーバへの接続のみ切断
(2) マルウェア感染
(5) ネットワークへの接続を切断
102
101
C&C サーバ

[図2]

図２

108

ユーザ名 - 201	所属 - 202	役職 - 203	IPアドレス - 204
User1	営業部	課長	192.168.1.101
User2	設計部	主任	192.168.2.101
User3	設計部	一般	192.168.2.102
・ ・ ・			

[図3]

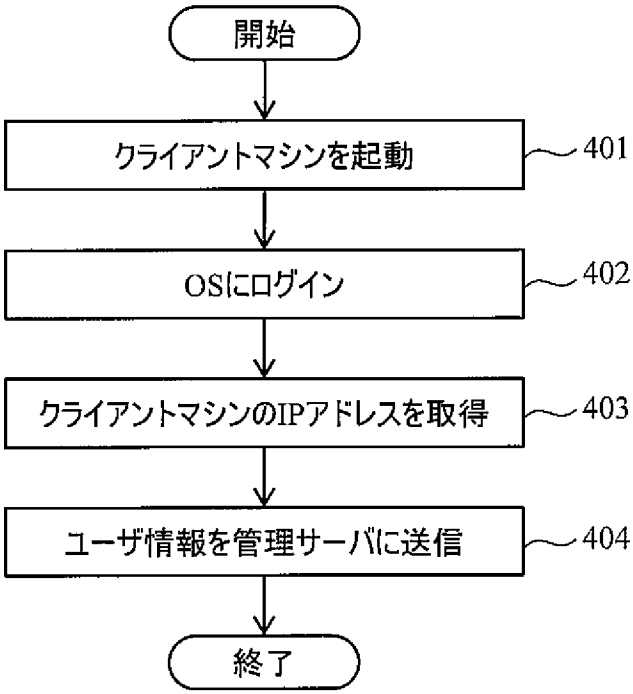
図３

110

所属 - 301	役職 - 302	時刻 - 303	ポリシー適用時の動作 - 304
営業部	課長	00:00～24:00	C&Cサーバ接続禁止
設計部	主任	00:00～09:00	ネットワーク接続禁止
設計部	主任	09:00～18:00	C&Cサーバ接続禁止
設計部	主任	18:00～24:00	ネットワーク接続禁止
設計部	一般	00:00～24:00	ネットワーク接続禁止
・ ・ ・			

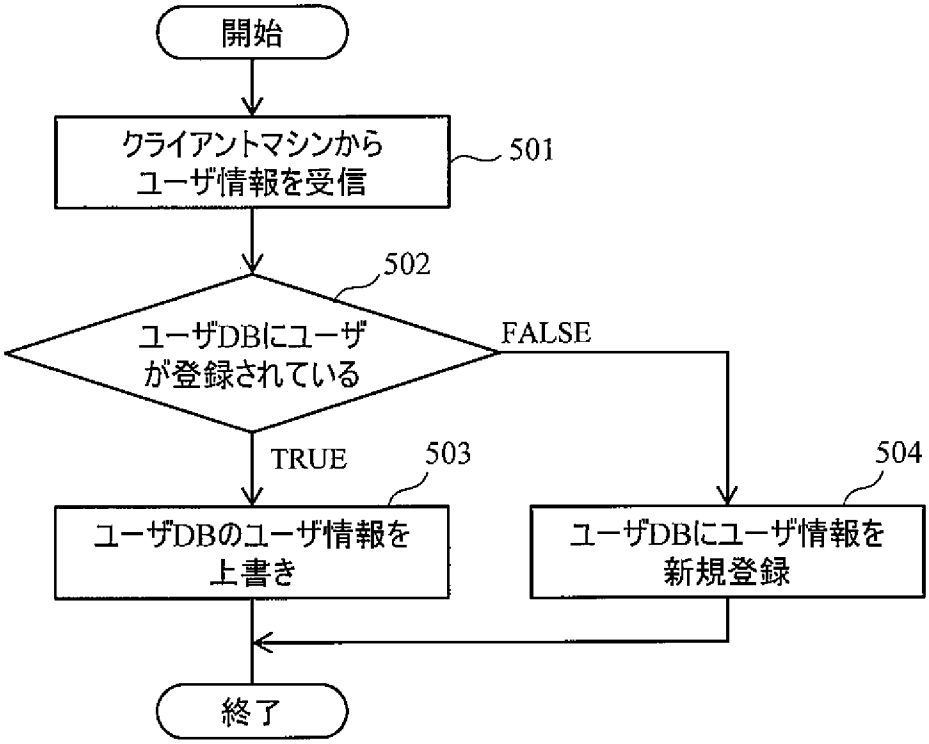
[図4]

図４


開始
クライアントマシンを起動
401
OSにログイン
402
クライアントマシンのIPアドレスを取得
403
ユーザ情報を管理サーバに送信
404
終了

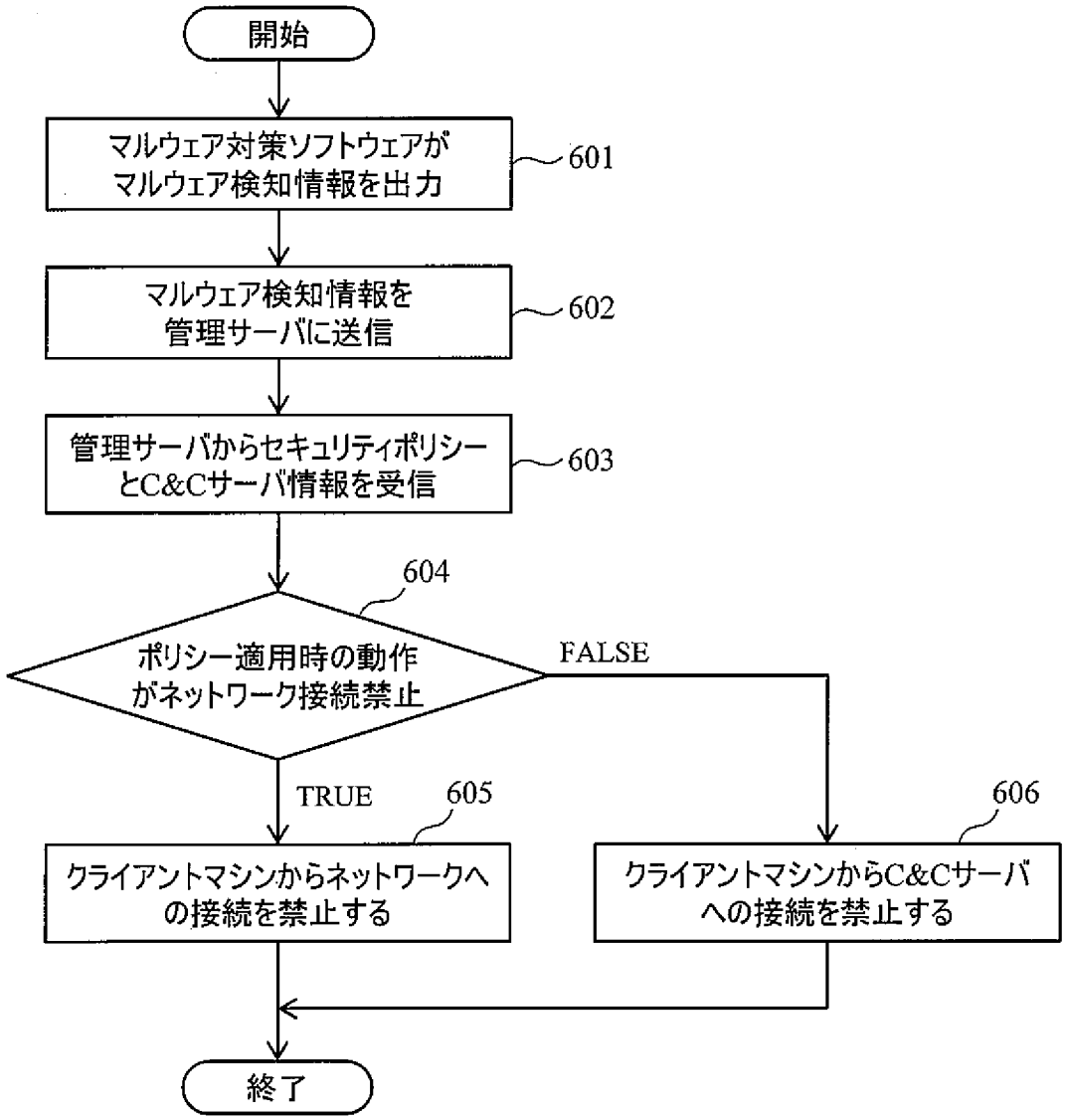
[図5]

図５


開始
クライアントマシンから
ユーザ情報を受信
501
502
ユーザDBにユーザ
が登録されている
FALSE
TRUE
503
504
ユーザDBのユーザ情報を
上書き
ユーザDBにユーザ情報を
新規登録
終了

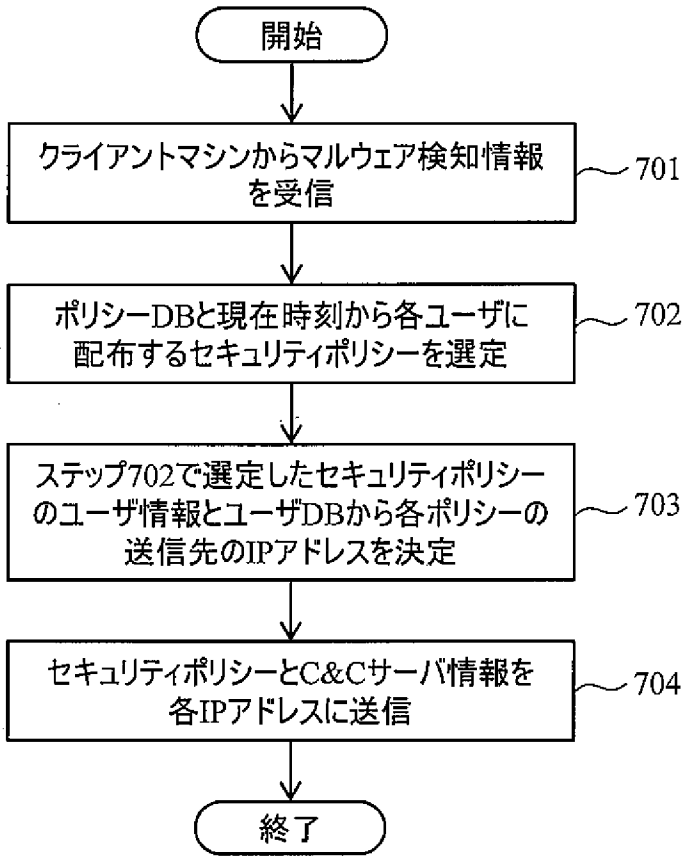
[図6]

図６


開始
マルウェア対策ソフトウェアが
マルウェア検知情報を出力
601
マルウェア検知情報を
管理サーバに送信
602
管理サーバからセキュリティポリシー
とC&Cサーバ情報を受信
603
604
ポリシー適用時の動作
がネットワーク接続禁止
FALSE
TRUE
605
606
クライアントマシンからネットワークへ
の接続を禁止する
クライアントマシンからC&Cサーバ
への接続を禁止する
終了

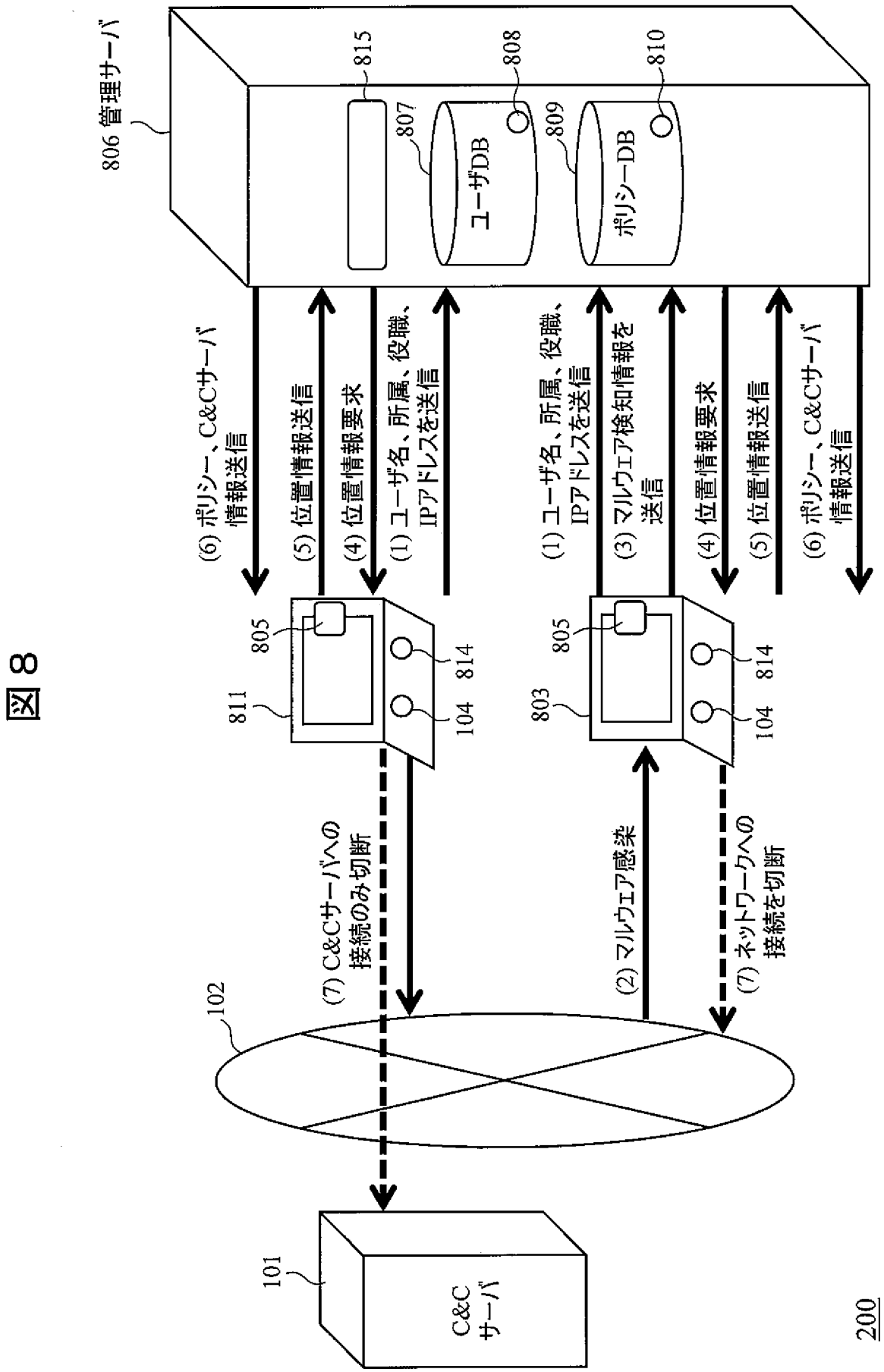
[図7]

図 7


開始
クライアントマシンからマルウェア検知情報を受信
701
ポリシーDBと現在時刻から各ユーザに配布するセキュリティポリシーを選定
702
ステップ702で選定したセキュリティポリシーのユーザ情報とユーザDBから各ポリシーの送信先のIPアドレスを決定
703
セキュリティポリシーとC&Cサーバ情報を各IPアドレスに送信
704
終了

[図8]

図8


806 管理サーバ
815
807
808
ユーザDB
809
ポリシーDB
810
(6) ポリシー、C&Cサーバ 情報送信
(5) 位置情報送信
(4) 位置情報要求
(1) ユーザ名、所属、役職、IPアドレスを送信
(1) ユーザ名、所属、役職、IPアドレスを送信
(3) マルウェア検知情報を送信
(4) 位置情報要求
(5) 位置情報送信
(6) ポリシー、C&Cサーバ 情報送信
805
811
814
104
803
805
814
104
(7) C&Cサーバへの接続のみ切断
(2) マルウェア感染
(7) ネットワークへの接続を切断
102
101
C&C サーバ
200

[図9]

図９

808

ユーザ名 - 901	所属 - 902	役職 - 903	IPアドレス – 904	位置情報 - 905
User1	営業部	課長	192.168.1.101	社内
User2	設計部	主任	192.168.2.101	顧客先
User3	設計部	一般	192.168.2.102	社内
・ ・ ・				

[図10]

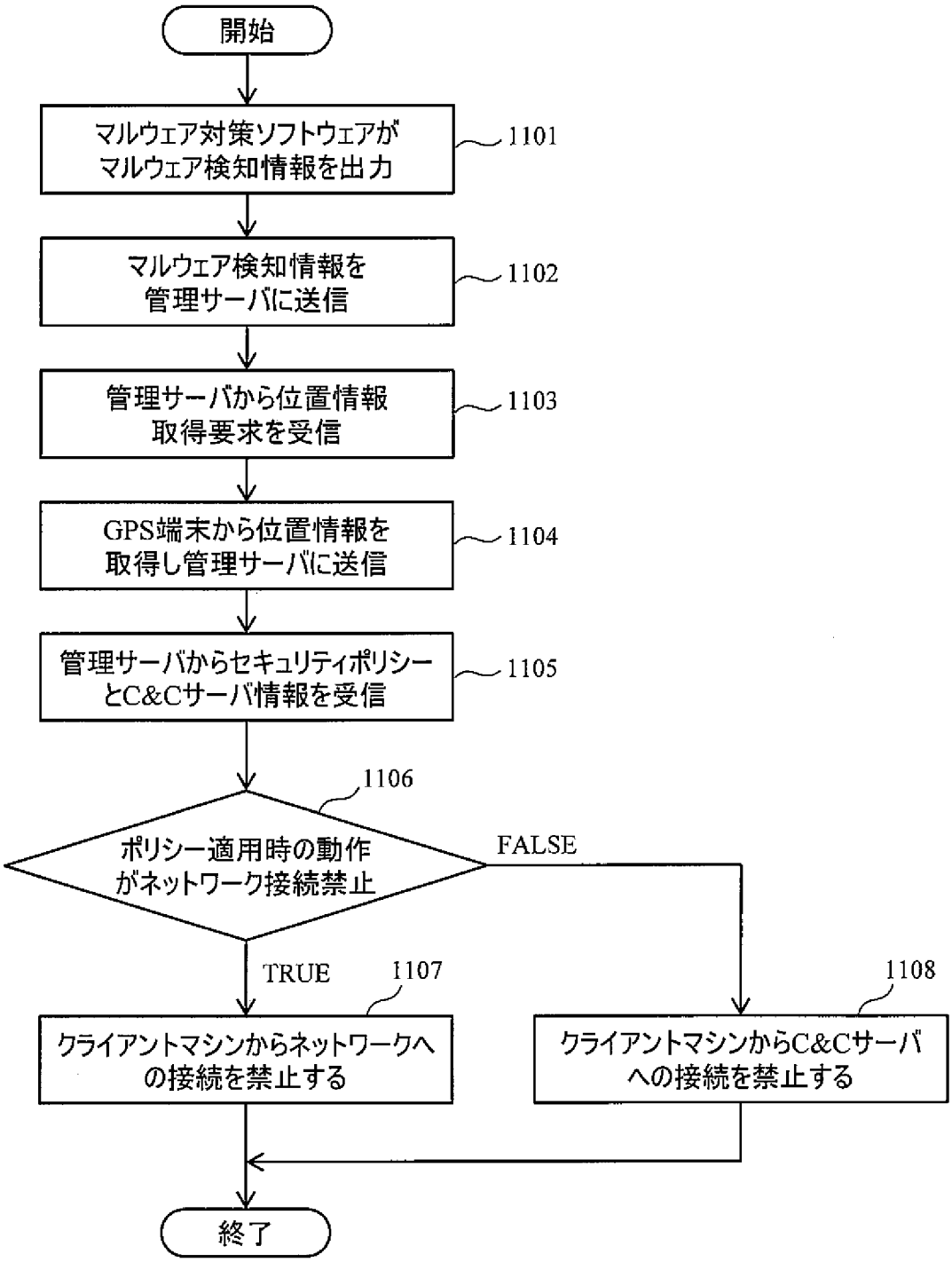
図１０

810

所属 - 1001	役職 - 1002	時刻 - 1003	位置情報 - 1004	ポリシー適用時の動作 - 1005
営業部	課長	00:00～24:00	社内	C&Cサーバ接続禁止
営業部	課長	00:00～24:00	顧客先	C&Cサーバ接続禁止
設計部	主任	09:00～18:00	社内	C&Cサーバ接続禁止
設計部	主任	09:00～18:00	顧客先	ネットワーク接続禁止
・ ・ ・				

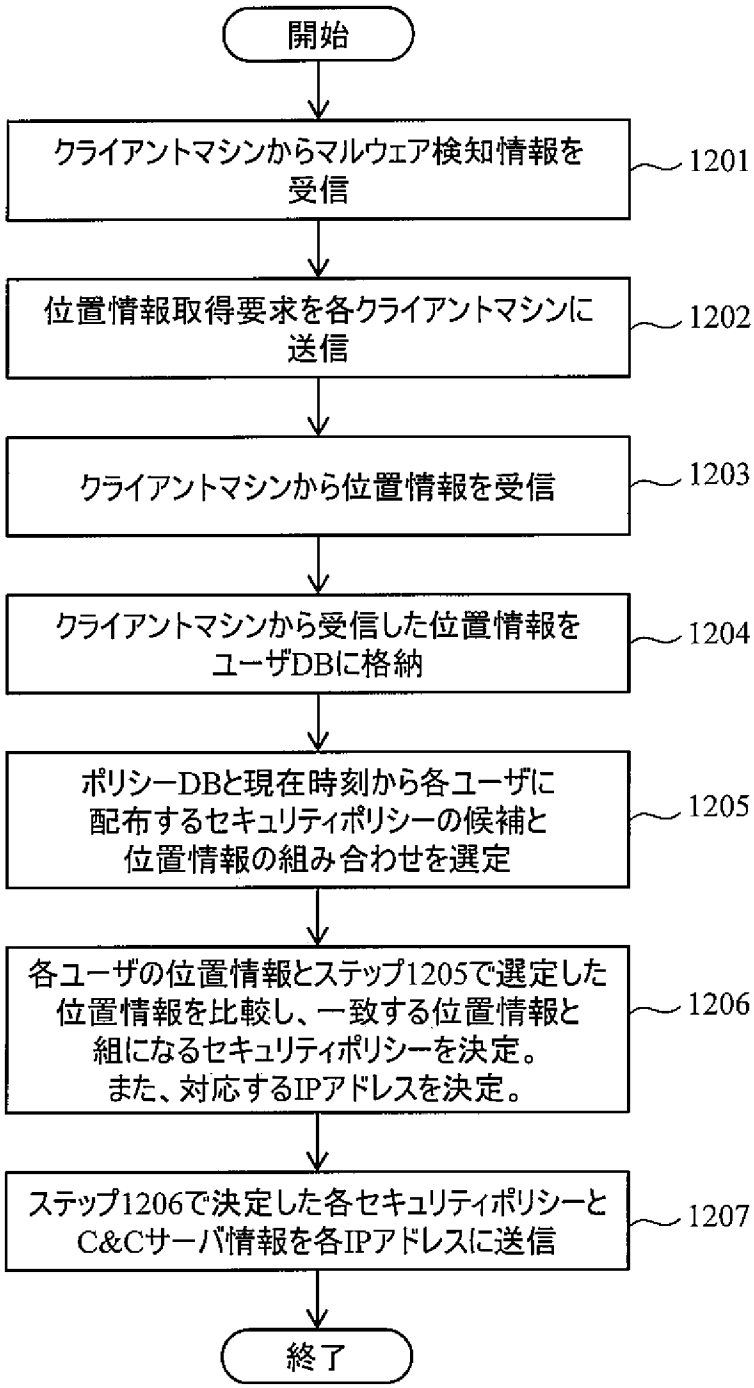
[図11]

図１１


開始
マルウェア対策ソフトウェアが
マルウェア検知情報を出力
1101
マルウェア検知情報を
管理サーバに送信
1102
管理サーバから位置情報
取得要求を受信
1103
GPS端末から位置情報を
取得し管理サーバに送信
1104
管理サーバからセキュリティポリシー
とC&Cサーバ情報を受信
1105
1106
ポリシー適用時の動作
がネットワーク接続禁止
FALSE
TRUE
1107
1108
クライアントマシンからネットワークへ
の接続を禁止する
クライアントマシンからC&Cサーバ
への接続を禁止する
終了

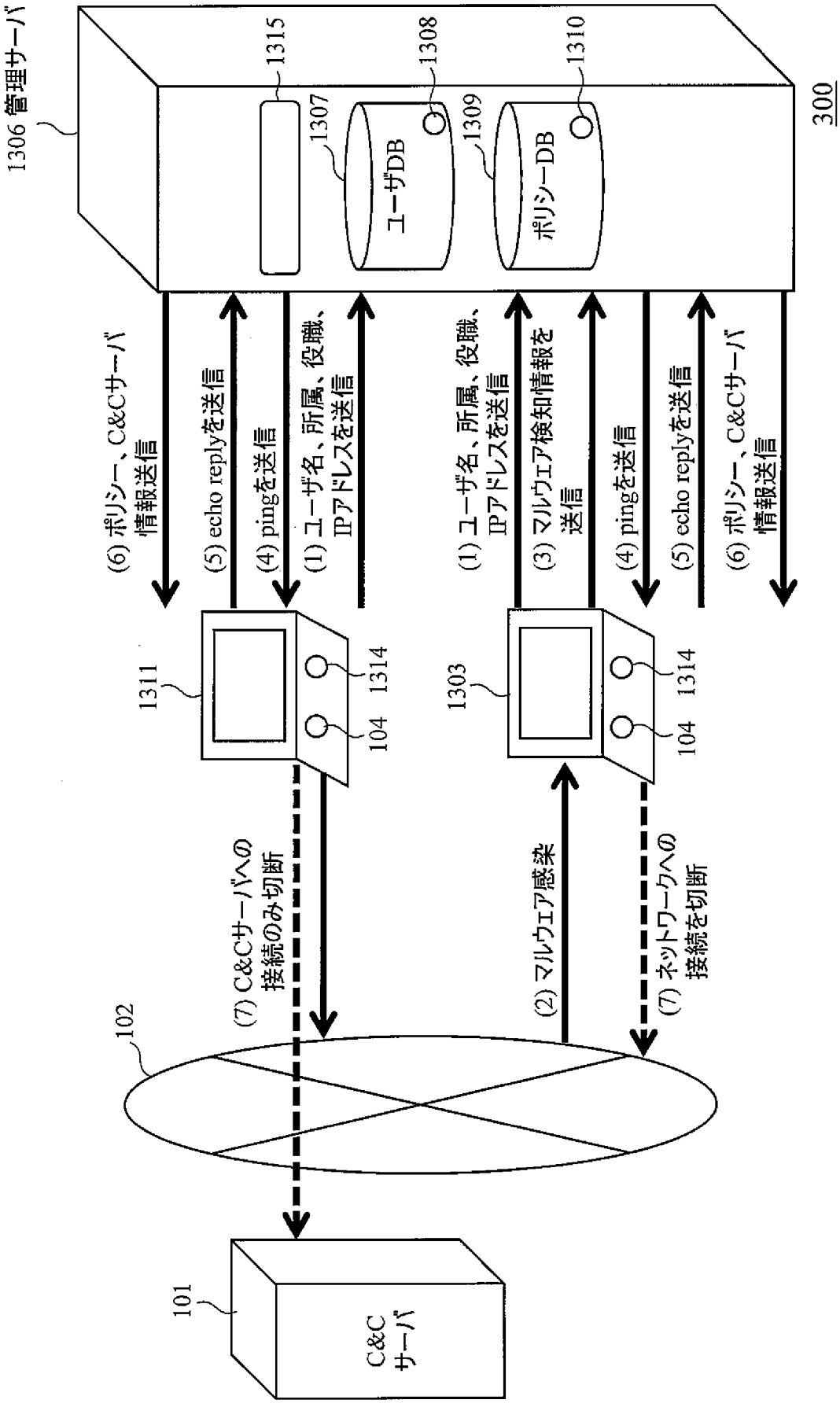
[図12]

図１２


開始
クライアントマシンからマルウェア検知情報を受信
1201
位置情報取得要求を各クライアントマシンに送信
1202
クライアントマシンから位置情報を受信
1203
クライアントマシンから受信した位置情報をユーザDBに格納
1204
ポリシーDBと現在時刻から各ユーザに配布するセキュリティポリシーの候補と位置情報の組み合わせを選定
1205
各ユーザの位置情報とステップ1205で選定した位置情報を比較し、一致する位置情報と組になるセキュリティポリシーを決定。また、対応するIPアドレスを決定。
1206
ステップ1206で決定した各セキュリティポリシーとC&Cサーバ情報を各IPアドレスに送信
1207
終了

[図13]

図１３


1306 管理サーバ
1315
1307
1308
ユーザDB
1309
1310
ポリシーDB
300
(6) ポリシー、C&Cサーバ情報送信
(5) echo replyを送信
(4) pingを送信
(1) ユーザ名、所属、役職、IPアドレスを送信
(1) ユーザ名、所属、役職、IPアドレスを送信
(3) マルウェア検知情報を送信
(4) pingを送信
(5) echo replyを送信
(6) ポリシー、C&Cサーバ情報送信
1311
1314
104
1303
1314
104
(7) C&Cサーバへの接続のみ切断
(2) マルウェア感染
(7) ネットワークへの接続を切断
102
101
C&C サーバ

[図14]

図１４

1308

ユーザ名 - 1401	所属 - 1402	役職 - 1403	IPアドレス - 1404	在席情報 - 1405
User1	営業部	課長	192.168.1.101	在席
User2	設計部	主任	192.168.2.101	―
User3	設計部	一般	192.168.2.102	―
⋮				

[図15]

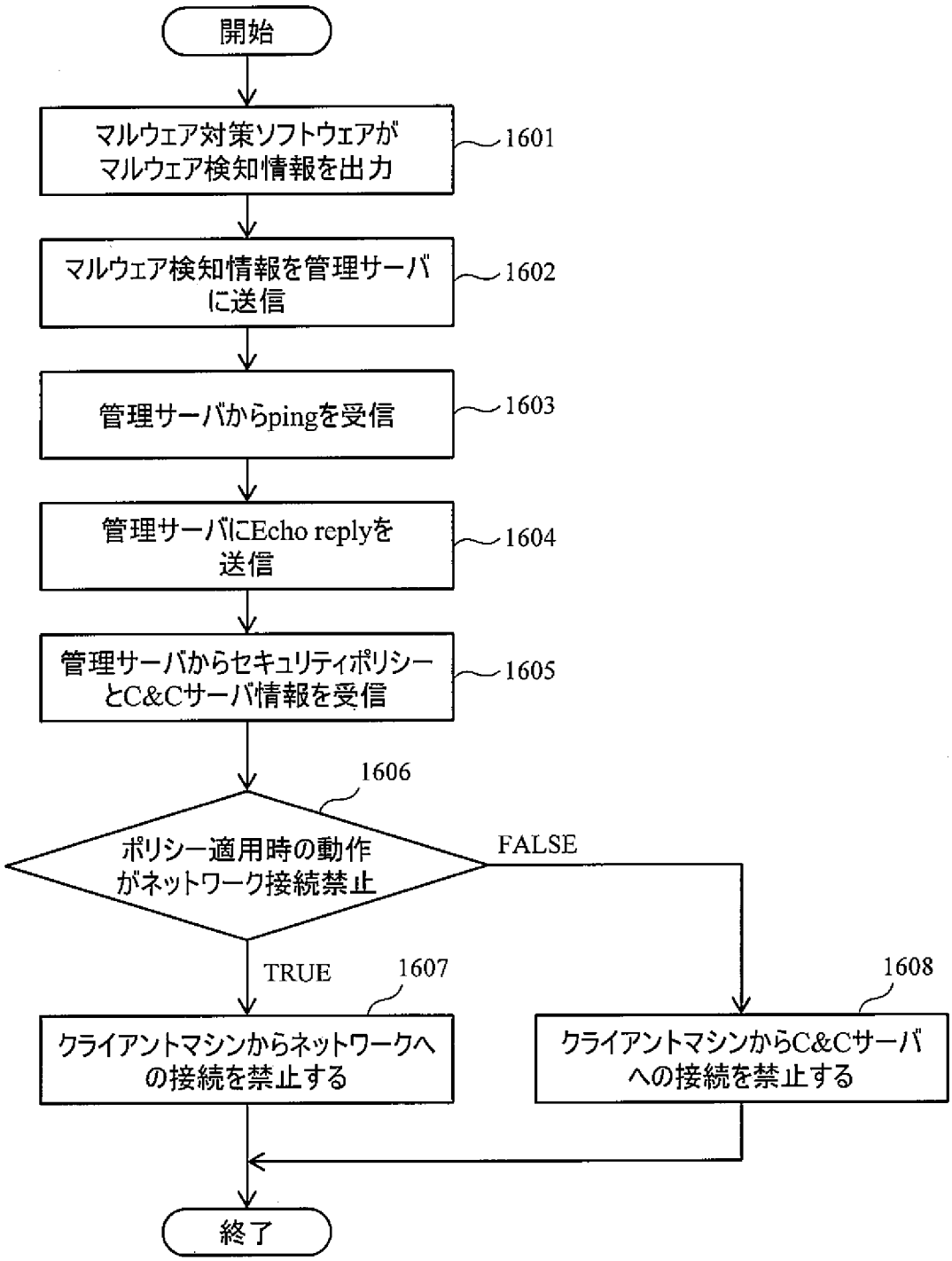
図１５

1310

所属 - 1501	役職 - 1502	時刻 - 1503	管理者の在席人数 - 1504	ポリシー適用時の動作 - 1505
営業部	課長	00:00～24:00	１人以上	C&Cサーバ接続禁止
設計部	主任	09:00～18:00	２人以上	C&Cサーバ接続禁止
設計部	主任	09:00～18:00	１人以下	ネットワーク接続禁止
⋮				

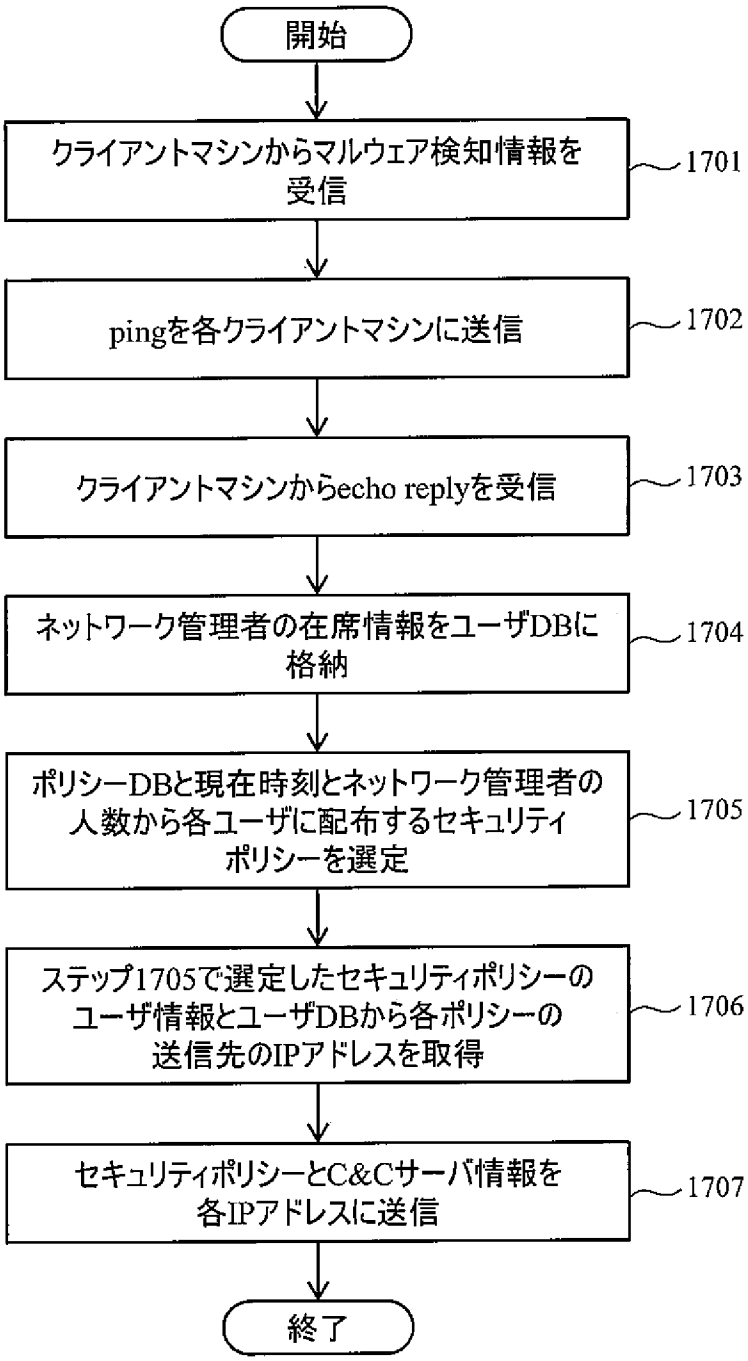
[図16]

図１６


開始
マルウェア対策ソフトウェアが
マルウェア検知情報を出力
1601
マルウェア検知情報を管理サーバ
に送信
1602
管理サーバからpingを受信
1603
管理サーバにEcho replyを
送信
1604
管理サーバからセキュリティポリシー
とC&Cサーバ情報を受信
1605
1606
ポリシー適用時の動作
がネットワーク接続禁止
FALSE
TRUE
1607
1608
クライアントマシンからネットワークへ
の接続を禁止する
クライアントマシンからC&Cサーバ
への接続を禁止する
終了

[図17]

図１７


開始
クライアントマシンからマルウェア検知情報を受信
1701
pingを各クライアントマシンに送信
1702
クライアントマシンからecho replyを受信
1703
ネットワーク管理者の在席情報をユーザDBに格納
1704
ポリシーDBと現在時刻とネットワーク管理者の人数から各ユーザに配布するセキュリティポリシーを選定
1705
ステップ1705で選定したセキュリティポリシーのユーザ情報とユーザDBから各ポリシーの送信先のIPアドレスを取得
1706
セキュリティポリシーとC&Cサーバ情報を各IPアドレスに送信
1707
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/085003

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/56(2013.01)i, *G06F21/60*(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/56, G06F21/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-70073 A (Sumitomo Electric Industries, Ltd.), 02 April 2009 (02.04.2009), paragraphs [0030] to [0047]; fig. 1, 4 to 6 (Family: none)	1-10
A	JP 2008-288686 A (Fuji Xerox Co., Ltd.), 27 November 2008 (27.11.2008), paragraphs [0074] to [0081]; fig. 1 to 2, 4 to 5 (Family: none)	1-10
A	JP 2009-169719 A (Fuji Xerox Co., Ltd.), 30 July 2009 (30.07.2009), fig. 8 (Family: none)	1-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 2017 (17.02.17)	28 February 2017 (28.02.17)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/085003

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2011-100362 A (Nippon Telegraph and Telephone Corp.), 19 May 2011 (19.05.2011), paragraph [0078]; fig. 7 (Family: none)	1-10
A	JP 2008-165601 A (Secureware Inc.), 17 July 2008 (17.07.2008), entire text; all drawings & US 2008/0215721 A1	1-10
A	JP 2010-68427 A (Oki Electric Industry Co., Ltd.), 25 March 2010 (25.03.2010), entire text; all drawings (Family: none)	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０８５００３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56(2013.01)i, G06F21/60(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56, G06F21/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2009-70073 A（住友電気工業株式会社）2009.04.02, [0030]-[0047], 図1, 4-6（ファミリーなし）	1-10
A	JP 2008-288686 A（富士ゼロックス株式会社）2008.11.27, [0074]-[0081], 図1-2, 4-5（ファミリーなし）	1-10
A	JP 2009-169719 A（富士ゼロックス株式会社）2009.07.30, 図8（ファミリーなし）	1-10

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１７．０２．２０１７	２８．０２．２０１７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３９８３
岸野　徹
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2011-100362 A (日本電信電話株式会社) 2011.05.19, [0078], 図7 (ファミリーなし)	1-10
A	JP 2008-165601 A (株式会社セキュアウェア) 2008.07.17, 全文、全図 & US 2008/0215721 A1	1-10
A	JP 2010-68427 A (沖電気工業株式会社) 2010.03.25, 全文、全図 (ファミリーなし)	1-10