【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成30年3月1日(2018.3.1)

【公開番号】特開2017-117354(P2017-117354A)
【公開日】平成29年6月29日(2017.6.29)
【年通号数】公開・登録公報2017-024
【出願番号】特願2015-254597(P2015-254597)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56

【手続補正書】
【提出日】平成30年1月17日(2018.1.17)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【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。