(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6380479号
(P6380479)
(45)発行日　平成30年8月29日(2018.8.29)　(24)登録日　平成30年8月10日(2018.8.10)

(51)Int.Cl.　F I
*G06Q 10/06 (2012.01)*　G06Q 10/06 302
*G06Q 50/10 (2012.01)*　G06Q 50/10

請求項の数 20　(全 35 頁)

(21)出願番号　特願2016-145080(P2016-145080)
(22)出願日　平成28年7月25日(2016.7.25)
(65)公開番号　特開2017-33550(P2017-33550A)
(43)公開日　平成29年2月9日(2017.2.9)
審査請求日　平成28年12月21日(2016.12.21)
(31)優先権主張番号　特願2015-152746(P2015-152746)
(32)優先日　平成27年7月31日(2015.7.31)
(33)優先権主張国　日本国(JP)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100189751
弁理士　木村　友輔
(74)代理人　100208904
弁理士　伊藤　秀起
(72)発明者　深谷　大樹
東京都品川区東品川２丁目４番１１号　キヤノンＩＴソリューションズ株式会社内

審査官　後藤　昂彦

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム、制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置であって、
前記管理端末からログインしたユーザの数を取得するログインユーザ取得手段と、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得手段と、
前記ログインユーザ取得手段によって取得したユーザの数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、
を備えたことを特徴とする情報処理装置。
【請求項２】
前記不正判定手段は、前記ログインユーザ取得手段によって取得したユーザの数よりも前記人物取得手段によって取得した人物の数が多い場合、前記拠点において不正侵入がなされたとして判定を行うことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記不正判定手段は、前記人物取得手段によって取得した人物の数に変化があったときに、前記拠点における不正侵入がなされたか否かを判定することを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記不正判定手段は、前記ログインユーザ取得手段によって取得したユーザの数よりも

前記人物取得手段によって取得した人物の数が多いと判定した後、所定時間、前記ログインユーザ取得手段によって取得したユーザの数が増加せずに、前記人物取得手段によって取得した人物の数が減少した場合、前記拠点において不正侵入がなされたとして判定を行うことを特徴とする請求項１乃至３の何れか１項に記載の情報処理装置。

【請求項５】

前記不正判定手段は、前記ログインユーザ取得手段によって取得したユーザの数が減少したと判定した後、所定時間、前記人物取得手段によって取得した人物の数が減少しない場合、前記拠点において不正がなされたとして判定を行うことを特徴とする請求項１乃至４の何れか１項に記載の情報処理装置。

【請求項６】

前記不正判定手段は、前記ログインユーザ取得手段によって取得したユーザの数が減少したと判定した後、所定時間内に、前記人物取得手段によって取得した人物の数が減少した場合、前記拠点において不正がなされていないとして判定を行うことを特徴とする請求項１乃至５の何れか１項に記載の情報処理装置。

【請求項７】

前記不正判定手段は、前記ログインユーザ取得手段によって取得したユーザの数が減少したと判定した後、所定時間内に、前記人物取得手段によって取得した人物の数が減少せずに、前記ログインユーザ取得手段によって取得したユーザの数が増加した場合、前記拠点において不正がなされていないとして判定を行うことを特徴とする請求項１乃至６の何れか１項に記載の情報処理装置。

【請求項８】

前記ネットワークカメラによって撮影して得られた画像から検出された人物をログインしたユーザに対応付ける対応付手段を備え、

前記不正判定手段は、前記対応付手段によって人物がログインしたユーザに対応付けられない場合は、前記拠点において不正侵入がなされたとして判定することを特徴とする請求項１乃至７の何れか１項に記載の情報処理装置。

【請求項９】

前記対応付手段は、前記ネットワークカメラによって撮影して得られた画像から前記拠点において新たに検出された人物をログインしたユーザに対応付けることを特徴とする請求項８に記載の情報処理装置。

【請求項１０】

前記不正判定手段は、前記新たに人物が検出されてから所定時間、前記対応付手段によって人物をログインしたユーザに対応付けられない場合は、前記拠点において不正侵入がなされたとして判定することを特徴とする請求項９に記載の情報処理装置。

【請求項１１】

前記不正判定手段は、前記新たに人物が検出されてから所定時間以内に、当該新たに検出された人物が拠点を退室された場合、前記拠点において不正侵入がなされたとして判定することを特徴とする請求項９または１０に記載の情報処理装置。

【請求項１２】

前記対応付手段は、ログインしているユーザが在席している場合、前記拠点において新たに検出された人物をログインしたユーザに対応付けを行うことを特徴とする請求項８乃至１１の何れか１項に記載の情報処理装置。

【請求項１３】

前記不正判定手段は、ログインしたユーザの数と拠点内の人物の数とに基づいて、前記拠点において不正侵入がなされたと判定する場合であっても、前記ログインしているユーザが退室している場合は、不正侵入と見做さないことを特徴とする請求項８乃至１２の何れか１項に記載の情報処理装置。

【請求項１４】

前記ネットワークカメラによって撮影して得られた画像から検出された人物に対応付けられたログインしているユーザの情報の表示を制御する表示制御手段を備えたことを特徴

とする請求項８乃至１３の何れか１項に記載の情報処理装置。
【請求項１５】
前記表示制御手段は、前記対応付手段によってログインしているユーザに対応付けられた人物と、対応付けられない人物とを識別して表示することを制御することを特徴とする請求項１４に記載の情報処理装置。
【請求項１６】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムであって、
前記管理端末は、
ログインに係るユーザ情報を受付ける受付手段と、
前記受付手段によって受付けたユーザ情報を前記情報処理装置のユーザ情報受信手段へ送信する管理端末送信手段と、
を備え、
前記情報処理装置は、
前記管理端末送信手段によって送信されたユーザ情報を受信するユーザ情報受信手段と、
前記ユーザ情報受信手段によって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得手段と、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得手段と、
前記ログインユーザ取得手段によって取得したユーザの人数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、
を備えたことを特徴とする情報処理システム。
【請求項１７】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置の制御方法であって、
前記情報処理装置は、
前記管理端末からログインしたユーザの数を取得するログインユーザ取得ステップと、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得ステップと、
前記ログインユーザ取得ステップによって取得したユーザの数と前記人物取得ステップによって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定ステップと、
を実行することを特徴とする情報処理装置の制御方法。
【請求項１８】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置で読み取り実行可能なプログラムであって、
前記情報処理装置を、
前記管理端末からログインしたユーザの数を取得するログインユーザ取得手段と、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得手段と、
前記ログインユーザ取得手段によって取得したユーザの数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、
して機能させるためのプログラム。
【請求項１９】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムの制御方法であって、
前記管理端末は、

ログインに係るユーザ情報を受付ける受付ステップと、
前記受付ステップによって受付けたユーザ情報を前記情報処理装置のユーザ情報受信ステップへ送信する管理端末送信ステップと、
を実行し、
前記情報処理装置は、
前記管理端末送信ステップによって送信されたユーザ情報を受信するユーザ情報受信ステップと、
前記ユーザ情報受信ステップによって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得ステップと、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得ステップと、
前記ログインユーザ取得ステップによって取得したユーザの人数と前記人物取得ステップによって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定ステップと、
を実行することを特徴とする情報処理システムの制御方法。
【請求項２０】
拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムにおいて、
前記管理端末を、
ログインに係るユーザ情報を受付ける受付手段と、
前記受付手段によって受付けたユーザ情報を前記情報処理装置のユーザ情報受信手段へ送信する管理端末送信手段と、
して機能させ、
前記情報処理装置を、
前記管理端末送信手段によって送信されたユーザ情報を受信するユーザ情報受信手段と、
前記ユーザ情報受信手段によって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得手段と、
前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得手段と、
前記ログインユーザ取得手段によって取得したユーザの人数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、
して機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、テレワーク管理システムにおいて行う監視技術に関する発明であり、特に居室における人物の監視技術に関する。
【背景技術】
【０００２】
近年、ブロードバンドや情報セキュリティ技術の発達の他、災害時における事業継続性や節電対策への注目等がなされてきた時代背景の下、各企業でテレワークに対する関心が強まっている。
【０００３】
テレワークを導入する上では、管理者からテレワーカーの様子が見えにくいため、家族をはじめとする第三者による情報処理端末へのアクセスにより機密情報が漏えいするリスクや、労働管理がしにくい問題がある。
【０００４】
機密情報の漏えい予防手段としては、顔認識技術を用いて個人認証を行い、本人でない

場合は、情報処理端末をロックするといった技術が検討されている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００９－２１１３８１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
在宅勤務においては、作業空間を情報端末前に限定することができるため、Ｗｅｂカメラによってテレワーカーを高精度に識別することができ、また、機密情報の印刷物を持ち帰らせないなどのルールによって、その監視範囲を情報端末前の利用者に限定できる。
【０００７】
しかしながら、サテライトオフィス等の拠点においては、重要書類の保管庫などが存在する可能性もあり、拠点内の不正侵入者を検知できなくてはならず、監視範囲を情報端末前に限定することはできないこともあり、特許文献１に記載の発明では、このようなケースには十分な対応をとれないという問題が生じうる。
【０００８】
また、拠点内の監視を行う方法としては、拠点の入り口に認証システムを設置したり、拠点内の人物の顔を高精度に捉えられるネットワークカメラを設置して人物を識別・追跡したりすることが考えられるが、導入コストが多額になったり、後者においては各人物の顔を常に正面から捉えられるわけではないので、識別精度に疑問が残る。
【０００９】
また、労務管理としては、多くの会社では労務時間をタイムカードや入退室のログなどで管理すると思われるが、在宅では使いにくく、またサテライトオフィスにおいても複数名で残業する際に一人を残して退室したことにして残業記録を残さないようにするような労務時間を詐称する行為が行われる可能性がある。
【００１０】
本発明の目的は、拠点におけるセキュリティの管理を効率的に行うことが可能な情報処理装置、情報処理システム、制御方法、及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１１】
上記の課題を解決するための第１の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置であって、前記管理端末からログインしたユーザの数を取得するログインユーザ取得手段と、前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得手段と、前記ログインユーザ取得手段によって取得したユーザの数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、を備えたことを特徴とする情報処理装置である。
【００１２】
上記の課題を解決するための第２の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムであって、前記管理端末は、ログインに係るユーザ情報を受付ける受付手段と、前記受付手段によって受付けたユーザ情報を前記情報処理装置のユーザ情報受信手段へ送信する管理端末送信手段と、を備え、前記情報処理装置は、前記管理端末送信手段によって送信されたユーザ情報を受信するユーザ情報受信手段と、前記ユーザ情報受信手段によって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得手段と、前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得手段と、前記ログインユーザ取得手段によって取得したユーザの人数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数

が異なる状態であるか否かを判定する不正判定手段と、を備えたことを特徴とする情報処理システムである。

【００１３】

上記の課題を解決するための第３の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置の制御方法であって、前記情報処理装置は、前記管理端末からログインしたユーザの数を取得するログインユーザ取得ステップと、前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得ステップと、前記ログインユーザ取得ステップによって取得したユーザの数と前記人物取得ステップによって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定ステップと、を実行することを特徴とする情報処理装置の制御方法である。

【００１４】

上記の課題を解決するための第４の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置で読み取り実行可能なプログラムであって、前記情報処理装置を、前記管理端末からログインしたユーザの数を取得するログインユーザ取得手段と、前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から拠点内の人物の数を取得する人物取得手段と、前記ログインユーザ取得手段によって取得したユーザの数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、して機能させるためのプログラムである。

【００１５】

上記の課題を解決するための第５の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムの制御方法であって、前記管理端末は、ログインに係るユーザ情報を受付ける受付ステップと、前記受付ステップによって受付けたユーザ情報を前記情報処理装置のユーザ情報受信ステップへ送信する管理端末送信ステップと、を実行し、前記情報処理装置は、前記管理端末送信ステップによって送信されたユーザ情報を受信するユーザ情報受信ステップと、前記ユーザ情報受信ステップによって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得ステップと、前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得ステップと、前記ログインユーザ取得ステップによって取得したユーザの人数と前記人物取得ステップによって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定ステップと、を実行することを特徴とする情報処理システムの制御方法である。

【００１６】

上記の課題を解決するための第６の発明は、拠点内に設置された少なくとも１以上の管理端末と通信可能な情報処理装置から構成される情報処理システムにおいて、前記管理端末を、ログインに係るユーザ情報を受付ける受付手段と、前記受付手段によって受付けたユーザ情報を前記情報処理装置のユーザ情報受信手段へ送信する管理端末送信手段と、して機能させ、前記情報処理装置を、前記管理端末送信手段によって送信されたユーザ情報を受信するユーザ情報受信手段と、前記ユーザ情報受信手段によって受信したユーザ情報から管理端末によってログインされたユーザの人数を取得するログインユーザ取得手段と、

前記拠点内を撮影するネットワークカメラによって撮影して得られた画像から前記拠点の人物の数を取得する人物取得手段と、前記ログインユーザ取得手段によって取得したユーザの人数と前記人物取得手段によって取得した人物の数とに基づいて、前記拠点において人数が異なる状態であるか否かを判定する不正判定手段と、して機能させるためのプログラムである。

【発明の効果】

【００１７】

本発明によれば、拠点におけるセキュリティの管理を効率的に行うことができる、という効果を奏する。

【図面の簡単な説明】

【００１８】

【図１】本発明の実施形態に係るテレワーク管理システムの構成の一例を示すシステム構成図である。

【図２】本発明の実施形態に係る監視端末、証跡監査端末、証跡管理サーバ、及びトリミングサーバに適用可能な情報処理装置のハードウェア構成を示すブロック図である。

【図３】本発明の実施形態に係る監視端末、証跡監査端末、証跡管理サーバ、及びトリミングサーバに必要な機能構成を示すブロック図である。

【図４】本発明の実施形態に係るテレワーク管理システムにおけるネットワークカメラによる拠点監視を行う一連の流れを示すフローチャートである。

【図５】本発明の実施形態に係るテレワーク管理システムにおける監視端末のカメラデバイスを使ってユーザを監視する一連の流れを示すフローチャートである。

【図６】本発明の実施形態に係るテレワーク管理システムにおける不正侵入者を検出する一連の流れを示すフローチャートである。

【図７】本発明の実施形態に係るテレワーク管理システムにおける労働時間の詐称にあたる行為を検出する一連の流れを示すフローチャートである。

【図８】本発明の実施形態に係るテレワーク管理システムにおけるテレワーク管理者が監査を行う一連の流れを示すフローチャートである。

【図９】本発明の実施形態に係るテレワーク管理システムにおける拠点監視画面の構成を示す構成図である。

【図１０】本発明の実施形態に係るテレワーク管理システムにおける拠点監視画面の構成を示す構成図である。

【図１１】本発明の実施形態に係るテレワーク管理システムにおける監査画面の構成を示す構成図である。

【図１２】本発明の実施形態に係るテレワーク管理システムにおけるユーザテーブルの構成を示す構成図である。

【図１３】本発明の実施形態に係るテレワーク管理システムにおける拠点テーブルの構成を示す構成図である。

【図１４】本発明の実施形態に係るテレワーク管理システムにおけるネットワークカメラテーブルの構成を示す構成図である。

【図１５】本発明の実施形態に係るテレワーク管理システムにおける拠点監視テーブルの構成を示す構成図である。

【図１６】本発明の実施形態に係るテレワーク管理システムにおける特徴量テーブルの構成を示す構成図である。

【図１７】本発明の実施形態に係るテレワーク管理システムにおける現在ユーザ情報テーブルの構成を示す構成図である。

【図１８】本発明の実施形態に係るテレワーク管理システムにおける現在拠点情報テーブルの構成を示す構成図である。

【図１９】本発明の実施形態に係るテレワーク管理システムにおける動静テーブルの構成を示す構成図である。

【図２０】本発明の実施形態に係るテレワーク管理システムにおけるユーザ異常テーブルの構成を示す構成図である。

【図２１】本発明の実施形態に係るテレワーク管理システムにおける監視端末証跡画像テーブルの構成を示す構成図である。

【図２２】本発明の実施形態に係るテレワーク管理システムにおける拠点異常テーブルの構成を示す構成図である。

【図２３】本発明の実施形態に係るテレワーク管理システムにおける証跡画像記憶テーブルの構成を示す構成図である。

【図２４】本発明の実施形態に係るテレワーク管理システムにおける人体検出情報記憶テーブルの構成を示す構成図である。
【図２５】本発明の実施形態に係るテレワーク管理システムにおけるネットワークカメラによる拠点監視を行う一連の流れを示すフローチャートである。
【図２６】本発明の実施形態に係るテレワーク管理システムにおけるネットワークカメラによる拠点監視を行う一連の流れを示すフローチャートである。
【図２７】本発明の実施形態に係るテレワーク管理システムにおける監視端末のカメラデバイスを使ってユーザを監視する一連の流れを示すフローチャートである。
【図２８】本発明の実施形態に係るテレワーク管理システムにおける人体情報テーブルの構成を示す構成図である。
【図２９】本発明の実施形態に係るテレワーク管理システムにおける拠点監視画面の構成を示す構成図である。
【発明を実施するための形態】
【００１９】
以下、図面を参照して、本発明の実施形態を詳細に説明する。
【００２０】
［第１の実施形態］
図１は、本発明のテレワーク管理システム（情報処理処理システム）の構成の一例を示すシステム構成図である。
【００２１】
テレワーク管理システム１００は、サテライトオフィスにおいては、１又は複数の監視端末１０２、及び１又は複数のネットワークカメラ１０４が設置されており、ローカルエリアネットワーク（ＬＡＮ）１０６及びルータ１０８を介してインターネット１１０と接続することで、サテライトオフィス以外の拠点に設置された各機器と接続される。
【００２２】
本社においては、１又は複数の証跡監査端末１１２が設置されており、ローカルエリアネットワーク（ＬＡＮ）１０６及びルータ１０８を介してインターネット１１０と接続することで、本社以外の拠点に設置された各機器と接続される。
【００２３】
データセンターにおいては、１又は複数のストリーミングサーバ１１６、及び１又は複数の証跡管理サーバ１１４が、ローカルエリアネットワーク（ＬＡＮ）１０６とルータ１０８、およびインターネット１１０を介して接続される構成となっている。
【００２４】
監視端末１０２は、使用するユーザ（テレワーカー）の動静およびユーザ本人以外の人物による使用等といったユーザ異常を検出し、それらの情報をユーザの証跡として証跡管理サーバ１１４に送信する。
【００２５】
また、動静およびユーザ異常の検出に使用するユーザの特徴を示す特徴量データを証跡管理サーバ１１４に送信する。
【００２６】
証跡監査端末１１２は、証跡管理サーバ１１４に記憶された特徴量データの承認操作と、証跡管理サーバ１１４に記憶された証跡の監査操作を行う。
【００２７】
証跡監査端末１１２は、テレワーク管理者の動静をテレワーカーに通知するまたは自身がテレワークを行う際に自身のテレワーク管理者に動静とユーザ異常を通知するために、監視端末１０２と同様の機能を備えることもある。
【００２８】
証跡管理サーバ１１４は、監視端末１０２から受信したテレワーカーの動静やユーザ異常等のユーザの証跡を記憶する。
【００２９】

また、証跡管理サーバ１１４は、ストリーミングサーバ１１６と連携し、各拠点での部外者の不正侵入やテレワーカーによる労働時間詐称などの異常を検出しその証跡を記録する。さらに、各証跡に対する証跡監査端末１１２の監査操作に対して処理を行う。

【００３０】

ネットワークカメラ１０４は、設置された拠点で撮影した画像をストリーミングサーバ１１６に送信する。

【００３１】

ストリーミングサーバ１１６は、ネットワークカメラ１０４から送られてきた画像を解析して人体を検出し、検出した人体検出情報を画像に合成し、その画像を証跡監査端末１１２に送信する。また、検出している人体の数の変化を証跡管理サーバ１１４に通知する。

【００３２】

テレワーカーの数だけ監視端末１０２を設置し、テレワーク管理者の数だけ証跡監査端末１１２を設置する。また、拠点の数だけネットワークカメラ１０４を設置し、場合によっては一つの拠点に複数台のネットワークカメラ１０４を設置することもある。

【００３３】

尚、サテライトオフィス、本社、及びデータセンターの各拠点をそれぞれ別の拠点としたが、このような拠点はあくまでも一例であり、全ての拠点を１つの拠点としても良いし、それぞれの拠点の組み合わせに応じて１つの拠点としても良い。

【００３４】

以下、図２を用いて、図１に示した監視端末１０２、証跡監査端末１１２、証跡管理サーバ１１４、及びストリーミングサーバ１１６に適用可能な情報処理装置のハードウェア構成について説明する。

【００３５】

図２は、図１に示した監視端末１０２、証跡監査端末１１２、証跡管理サーバ１１４、及びストリーミングサーバ１１６に適用可能な情報処理装置のハードウェア構成を示すブロック図である。それぞれの機器は、ほぼ同様な構成を備えるため、同一の符号を用いて以後説明する。

【００３６】

図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０３あるいは外部メモリ２１２には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　／　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各ＰＣの実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。

【００３７】

２０３はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０３あるいは外部メモリ２１２からＲＡＭ２０２にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。

【００３８】

また、２０５は入力コントローラで、キーボード（ＫＢ）２０９やカメラデバイス２１０、不図示のマウス等のポインティングデバイス等からの入力を制御する。

【００３９】

２０６はビデオコントローラで、ＣＲＴディスプレイ（ＣＲＴ）２１１等の表示器への表示を制御する。なお、図２では、ＣＲＴ２１１と記載しているが、表示器はＣＲＴだけでなく、液晶ディスプレイ等の他の表示器であってもよい。これらは必要に応じてテレワーク管理者が使用するものである。

【００４０】

２０７はメモリコントローラで、ブートプログラム、各種のアプリケーション、フォン

トデータ、ユーザファイル、編集ファイル、各種データ等を記憶する外部記憶装置（ハードディスク（ＨＤ））や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１２へのアクセスを制御する。

【００４１】

２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ１３０）を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いた通信等が可能である。

【００４２】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０２内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ＣＲＴ２１１上での表示を可能としている。また、ＣＰＵ２０１は、ＣＲＴ２１１上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【００４３】

本発明を実現するための後述する各種プログラムは、外部メモリ２１２に記録されており、必要に応じてＲＡＭ２０２にロードされることによりＣＰＵ２０１によって実行されるものである。

【００４４】

さらに、上記プログラムの実行時に用いられる定義ファイル及び各種情報テーブル等も、外部メモリ２１２に格納されており、これらについての詳細な説明も後述する。

【００４５】

以上で、監視端末１０２、証跡監査端末１１２、証跡管理サーバ１１４、ストリーミングサーバ１１６に適用可能な情報処理装置のハードウェア構成の説明を終了する。

【００４６】

次に、図３を用いて、本発明の監視端末１０２、ネットワークカメラ１０４、証跡監査端末１１２、証跡管理サーバ１１４、及びストリーミングサーバ１１６の機能ブロック図について説明する。

【００４７】

尚、各機能ブロックが処理する詳細な制御については、後述するフローチャートにて説明する。

【００４８】

まず、監視端末１０２の機能構成について説明する。

認証情報入力部３００は、ユーザによるアカウントＩＤやパスワード等を含む認証情報の入力を受け付け、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１１４の認証部３１２に送信し、テレワーク管理システム１００へのログインを行う。

【００４９】

また、認証部３１２から拠点リストを取得し、その中から現在の拠点の選択を受け付け、それを認証部３１２に送信する。

【００５０】

選択方法としては、拠点リストをＣＲＴ２１１に表示してユーザに選択させる方法や、近辺のＷｉｆｉ網から現在地の住所を推定し自動決定するなどの方法がある。

【００５１】

特徴量データ更新部３０２は、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１１４の特徴量データ制御部３１８から、ユーザの顔を識別するための特徴量データを取得する。

【００５２】

また、カメラデバイス２１０で撮影して得られた画像から顔を検出し、その顔から取得した特徴量データを証跡管理サーバ１１４の特徴量データ制御部３１８に送信する。

【００５３】

ユーザ監視部３０４は、カメラデバイス２１０で撮影して得られた画像を取得し、その

画像から正規のログインユーザによる動静情報として「在席」・「離席」、ユーザ異常情報として第三者による「なりすまし」・「覗き見」の状態を検出する。

【００５４】

状態の検出には、顔検出、顔認証、場合によっては顔追跡の技術を利用するが、顔認証には、特徴量データ更新部３０２で取得した特徴量データを利用する。

【００５５】

既存の状態と異なる状態を検出した場合、その動静情報およびユーザ異常情報を、カメラデバイス２１０で撮影して得られた画像およびＣＲＴ２１１に出力していたもののスクリーンショットとともに証跡管理サーバ１１４のユーザ監視情報制御部３２１に送信する。

【００５６】

次に、証跡監査端末１１２の機能構成について説明する。

拠点情報表示部３０６は、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１１４の現在情報管理部３２６から取得した現在のユーザ情報と現在の拠点情報（詳細後述）と、ストリーミングサーバ１１６の拠点情報配信部３４０から取得したネットワークカメラ１０４で撮影して得られた画像をＣＲＴ２１１に表示する。

【００５７】

証跡管理サーバ１１４の更新通知部３２４から更新通知を受け取った際には、その表示の更新を行う。

【００５８】

監査操作部３１０は、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１１４の監査制御部３２８から取得したユーザ異常情報及び拠点異常情報（詳細後述）をＣＲＴ２１１に表示し、ユーザに未監査のユーザ異常及び拠点異常が問題かどうか監査させる。

【００５９】

問題ないかどうかの判断材料として、ユーザ異常発生期間および拠点異常発生期間の監視端末１０２のカメラデバイス２１０で撮影して得られた画像やスクリーンショットおよびネットワークカメラ１０４で撮影して得られた画像などを表示する。

【００６０】

次に、証跡管理サーバ１１４の機能構成について説明する。

認証部３１２は、監視端末１０２の認証情報入力部３００から受信した認証情報とマスタデータ記憶部３１４に記憶されたユーザ情報（詳細後述）を比較する。

【００６１】

一致するユーザ情報（詳細後述）があった場合に、現在情報記憶部３１６にユーザのログイン情報を記憶し（図１７参照）、監視端末１０２にマスタデータ記憶部３１４に記憶されているユーザが選択可能な拠点リストを返却する。

【００６２】

マスタデータ記憶部３１４は、ユーザ情報、拠点情報、ネットワークカメラ情報（各情報の詳細は後述）、特徴量データなどの情報を記憶する。

【００６３】

現在情報記憶部３１６は、各ユーザがテレワーク管理システム１００にログインしているか、在席しているか、ユーザ異常が発生しているか、どの拠点にいるかといった、ユーザの今現在の情報を記憶する。

【００６４】

また、各拠点にユーザが何人いるか、異常が発生しているかといった、拠点の今現在の情報をも記憶する。

【００６５】

特徴量データ制御部３１８は、監視端末１０２の特徴量データ更新部３０２からの要求を受けて、マスタデータ記憶部３１４に特徴量データを記憶したり、記憶されているユーザの特徴量データを返却したりする。

【００６６】

ユーザ監視情報制御部３２１は、監視端末１０２のユーザ監視部３０４から受信した動静情報およびユーザ異常情報を監査情報記憶部３２２に記憶する。また、現在情報記憶部３１６に記憶されているユーザがテレワーク管理システム１００にログインしているか否かを示すログイン情報を更新する。

【００６７】

監査情報記憶部３２２は、ユーザの動静情報とユーザ異常情報とを、ユーザ証跡画像（カメラデバイス２１０で撮影して得られた画像及びスクリーンショット）とともに記憶する。

【００６８】

また、拠点異常情報（詳細後述）を拠点証跡画像（ネットワークカメラ１０４で撮影して得られた画像）及び人体検出の結果とともに記憶する。

【００６９】

更新通知部３２４は、ユーザ監視情報制御部３２１や拠点異常検出部３２３からの依頼を受けて、証跡監査端末１１２の更新通知受信部３０８に動静やユーザ異常等に係る更新通知を送信する。

【００７０】

ネットワークカメラ情報管理部３２０は、マスタデータ記憶部３１４に記憶されたネットワークカメラ情報（詳細後述）を元に、ストリーミングサーバ１１６のネットワークカメラ制御部３３４にネットワークカメラ１０４の制御を依頼する。

【００７１】

拠点異常検出部３２３は、ストリーミングサーバ１１６の拠点情報配信部３４０から受信した拠点情報（詳細後述）を現在情報記憶部３１６に記憶し、現在情報記憶部３１６に記憶された現在のユーザ情報と現在の拠点情報（詳細後述）をもとに、拠点で発生している異常を検出する。検出した拠点異常情報（詳細後述）は、監査情報記憶部３２２に記憶する。

【００７２】

現在情報管理部３２６は、証跡監査端末１１２の拠点情報表示部３０６からの要求を受けて、拠点リストや各拠点の現在のユーザ情報（詳細後述）および現在の拠点情報（詳細後述）を返却する。

【００７３】

監査制御部３２８は、証跡監査端末１１２の監査操作部３１０からの要求を受けて、ユーザ異常情報および拠点異常情報（詳細後述）を返却し、監査処理結果を監査情報記憶部３２２に記憶する。

【００７４】

次に、ネットワークカメラ１０４の機能構成について説明する。

カメラ制御受信部３３０は、通信Ｉ／Ｆコントローラ２０８を介してネットワークカメラ制御部３３４から送られてきたカメラ制御命令を受け取り、ネットワークカメラ１０４の本体の向きを変更したり、画像の配信を開始・停止したりする。

【００７５】

画像送信部３３２は、通信Ｉ／Ｆコントローラ２０８を介してネットワークカメラ１０４で撮影して得られた画像を外部に送信する。

【００７６】

最後に、ストリーミングサーバ１１６の機能構成について説明する。

ネットワークカメラ制御部３３４は、通信Ｉ／Ｆコントローラ２０８を介した証跡管理サーバ１１４のネットワークカメラ情報管理部３２０からの命令を受けて、ネットワークカメラ１０４を制御する。

【００７７】

拠点監視部３３６は、通信Ｉ／Ｆコントローラ２０８を介してネットワークカメラ１０４の画像送信部３３２から送信されたネットワークカメラ１０４で撮影して得られた画像に対して人体検出を行い、その人体検出情報（詳細後述）を拠点監視情報記憶部３３８に

ネットワークカメラ１０４で撮影して得られた画像とともに記憶し、人の検出位置を埋め込んだ画像を通信Ｉ／Ｆコントローラ２０８を介して拠点情報配信部３４０に送信する。また、拠点内の人数が増減した場合に、通信Ｉ／Ｆコントローラ２０８を介して証跡管理サーバ１１４の拠点異常検出部３２３にその情報を送信する。

【００７８】

拠点監視情報記憶部３３８は、拠点証跡画像と人体検出情報（詳細後述）を記憶する。

【００７９】

拠点情報配信部３４０は、人体検出情報（詳細後述）を埋め込んだ画像を、通信Ｉ／Ｆコントローラ２０８を介して証跡監査端末１１２の拠点情報表示部３０６に送信する。

【００８０】

証跡管理部３４２は、通信Ｉ／Ｆコントローラ２０８を介した証跡管理サーバ１１４の拠点異常検出部３２３からの要求を受けて、拠点監視情報記憶部３３８に記憶されたネットワークカメラ１０４で撮影して得られた画像を返却する。

【００８１】

以上で、監視端末１０２、証跡監査端末１１２および証跡管理サーバ１１４の機能ブロック図に関する説明を終了する。

【００８２】

以下、図４を参照して、本実施形態のテレワーク管理システム１００において、ネットワークカメラ１０４による拠点監視を行う一連の流れを説明する。

【００８３】

証跡監査端末１１２、証跡管理サーバ１１４、及びストリーミングサーバ１１６の処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラム及びデータをＲＡＭ２０２に記憶することで実行される。

【００８４】

また、証跡管理サーバ１１４の処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムおよびデータをＲＡＭ２０２に記憶することで実行される。

【００８５】

ステップＳ１００では、証跡管理サーバ１１４が、マスタデータ記憶部３１４に記憶されたネットワークカメラ情報（図１４参照）をストリーミングサーバ１１６に送信し、ネットワークカメラ１０４の監視を開始するようカメラ制御命令を送信する。

【００８６】

図１４には、ネットワークカメラ情報を記憶するネットワークカメラテーブルが示されており、ネットワークカメラ１０４を一意に識別するためのカメラＩＤ、ネットワークカメラ１０４の設置場所等を示す名前、ネットワークカメラ１０４が設置された拠点を一意に示す拠点ＩＤを備えている。

【００８７】

また、ネットワークカメラテーブルは、ネットワークカメラ１０４と接続して通信を行うために必要となるＵＲＬや接続時に認証を行うためのパスワードを備えている。

【００８８】

ステップＳ１０２では、ストリーミングサーバ１１６が、ステップＳ１００で受信したネットワークカメラ情報を元に、ネットワークカメラ１０４をセットアップし、ネットワークカメラ１０４で撮影して得られた画像を受信できる状態にする。

【００８９】

ステップＳ１０４では、ストリーミングサーバ１１６が、ネットワークカメラ１０４から撮影して得られた画像を受信する。

【００９０】

ステップＳ１０６では、ストリーミングサーバ１１６が、ステップＳ１０４で受信したネットワークカメラ１０４で撮影して得られた画像に対して人の検出を行い、拠点証跡画像（図２３）とその人体検出情報（図２４）とを拠点監視情報記憶部３３８に記憶する。尚、記憶するネットワークカメラ１０４で撮影して得られた画像は、動画像形式であって

も複数の静止画像形式であってもよい。

【００９１】

図２３には、拠点証跡画像に関する情報を記憶するための証跡画像記憶テーブルの構成が示されており、証跡画像記憶テーブルは、拠点証跡画像を一意に識別するためのＩＤ、拠点証跡画像を撮影したネットワークカメラ１０４を一意に識別するためのカメラＩＤ、拠点証跡画像を示す画像データ、拠点証跡画像が撮影された日時等を含んで構成されている。

【００９２】

図２４には、人体検出情報を記憶するための人体検出情報記憶テーブルの構成が示されており、人体検出情報記憶テーブルは、人体検出情報を一意に識別するためのＩＤ、人体検出を行った画像を撮影したネットワークカメラ１０４を一意に識別するためのカメラＩＤ、当該画像から検出した人体数、画像に対しての検出した人体が位置する座標、当該画像がネットワークカメラ１０４で撮影された日時などを含んで構成されている。

【００９３】

ステップＳ１０８では、ストリーミングサーバ１１６が、現在、検出した人体の数と過去に検出した人体の数との比較を行う。

【００９４】

同一拠点に複数のネットワークカメラ１０４を設置している場合、複数のネットワークカメラ１０４で得られた結果を統合して人体の数を検出する。

【００９５】

最も単純な統合手段としては、最も検出した人体の数の多いネットワークカメラ１０４の結果を、その拠点内において検出した人体の数とするものである。

【００９６】

拠点内において検出した人体の数が増減しているのであれば、ステップＳ１１０では、証跡管理サーバ１１４に検出した人体の数の変化を通知し、変化がなければステップＳ１１８へ処理を進める。

【００９７】

ステップＳ１１０では、証跡管理サーバ１１４が、現在情報記憶部３１６に記憶された現在の拠点情報（図１８参照）の人体数を更新する。

【００９８】

図１８には、現在の拠点情報を記憶するための現在拠点情報テーブルの構成が示されており、現在拠点情報テーブルは、拠点を一意に識別するための拠点ＩＤ、当該拠点で撮影された画像から検出された人体数、当該拠点において不正侵入者がいるか否かを記憶するための異常フラグ、当該拠点に人が侵入した最終時刻、当該拠点に人が退室した最終時刻を含んで構成されている。

【００９９】

また、マスタデータ記憶部３１４に記憶された拠点監視情報（図１５参照）から、当該拠点の監視者であるテレワーク管理者を特定し、その証跡監査端末１１２に現在の拠点情報の変化を通知する。

【０１００】

図１５には、拠点監視情報を記憶するための拠点監視テーブルの構成が示されており、拠点監視テーブルは、拠点監視情報を一意に識別するためのＩＤ、拠点を一意に識別するための拠点ＩＤ、テレワーク管理者を一意に識別するための監視者リストＩＤ（複数のテレワーク管理者を記憶可）等を含んで構成されている。

【０１０１】

ステップＳ１１２では、証跡監査端末１１２が、画面（図９参照）に表示している拠点内の人体の数を更新する。

【０１０２】

図９には、拠点監視画面４００の構成が示されており、拠点監視画面４００は、画面に監視結果を表示したい拠点を選択するための拠点選択欄４０１、当該拠点における監視結

果を表示する監視情報表示領域４０２、ネットワークカメラ１０４が設置された拠点を選択するためのカメラ拠点選択欄４０３、不正侵入の警告表示を行うための警告表示領域４０４、ネットワークカメラ１０４で撮影して得られた画像に係る拠点証跡画像として表示するための拠点証跡画像表示領域４０５等を含んで構成されている。

【０１０３】

つまり、本ステップにおいては、警告表示領域の人体検出の数を更新する。

【０１０４】

ステップＳ１１４では、証跡管理サーバ１１４が、過去の拠点内の人体の数と比べて人体の数が増えたか否かを確認する。

【０１０５】

さらに、当該拠点内のログインユーザ数よりもその人体の数が多いのであれば、拠点内に誰かが侵入したことになるので、ステップＳ１１６へ処理を進め、不正侵入者の検出を行い、それ以外の場合は、ステップＳ１１８へ処理を進める。

【０１０６】

ステップＳ１１６では、証跡管理サーバ１１４が、不正侵入者の検出を行う。詳細は図６を用いて後述する。

【０１０７】

ステップＳ１１８では、ストリーミングサーバ１１６が、ステップＳ１０６で検出した人体検出情報を埋め込んだネットワークカメラ１０４で撮影して得られた画像を証跡監査端末１１２に送信する。

【０１０８】

ステップＳ１２０では、証跡監査端末１１２が、ストリーミングサーバ１１６から取得した人体検出情報が埋め込まれたネットワークカメラ１０４で撮影して得られた画像を拠点監視画面４００の拠点証跡画像表示領域４０５に表示する。

【０１０９】

ステップＳ１２２では、ストリーミングサーバ１１６が、証跡管理サーバ１１４からネットワークカメラ１０４に対する監視停止命令がない限り、ステップＳ１０４において、ネットワークカメラ１０４で撮影して得られた画像の人体検出処理を繰り返し、停止命令があれば一連の処理を終了する。

【０１１０】

以上で、ネットワークカメラ１０４による拠点監視を行う一連の流れの説明を終了する。

【０１１１】

以下、図５を参照して、本実施形態のテレワーク管理システム１００において、監視端末１０２のカメラデバイス２１０を使ってユーザを監視する一連の流れを説明する。尚、備え付けのカメラに関わらず、監視端末１０２に接続されたＷｅｂカメラを使ってユーザを監視しても良い。

【０１１２】

監視端末１０２と証跡管理サーバ１１４の処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムおよびデータをＲＡＭ２０２に記憶することで実行される。

【０１１３】

ステップＳ２００では、ユーザが監視端末１０２を用いてテレワーク管理システム１００にログインすることにより、監視端末１０２が常駐アプリケーションを起動し、バックグラウンドで証跡管理サーバ１１４にアカウントＩＤとパスワードを送信する。

【０１１４】

ステップＳ２０２では、証跡管理サーバ１１４は、マスタデータ記憶部３１４に記憶されたユーザ情報（図１２参照）と比較し、一致すればログインを許可する。

【０１１５】

図１２には、ユーザ情報を記憶するためのユーザテーブルの構成が示されており、ユーザテーブルは、ユーザを一意に示すユーザＩＤ、ユーザのアカウント、パスワード、ユー

ザの名前、ユーザの名前に対するフリガナを備えている。
【０１１６】
また、ユーザテーブルは、ユーザがグループか個人等を識別するための種別、ユーザの住所、ユーザ本人の顔画像等の本人を特定するための画像を示すプロフィール画像、動静の監視対象とする居所を示す動静閲覧対象、監査を行う範囲（グループ）を示す監査対象を備える。
【０１１７】
さらに、ユーザテーブルは、ユーザに監視権限があるか否かを示す監視権限（ＴＲＵＥである場合、監視権限あり）、及びユーザが在宅勤務可能であるか否かを示す在宅権限（ＴＲＵＥである場合、可能）などを備えている。
【０１１８】
尚、アカウントとパスワードは、常駐アプリケーションの初回起動時にユーザが設定し、以降は設定された値を使用するものとする。
【０１１９】
認証に成功した場合、証跡管理サーバ１１４は、マスタデータ記憶部３１４に記憶された当該ユーザの利用可能な拠点に関する拠点情報を、監視端末１０２に送信する。
【０１２０】
ユーザの利用可能な拠点情報とは、マスタデータ記憶部３１４に記憶された拠点情報（図１３）の全てと、ユーザ情報の在宅権限がＴＲＵＥな場合は、ユーザの住所から生成した、名前が自宅である拠点情報である。
【０１２１】
図１３には、拠点情報を記憶するための拠点テーブルの構成が示されており、拠点テーブルは、拠点を一意に識別するための拠点ＩＤ、拠点の名称を示す名前、拠点の名称に対するフリガナ、拠点の住所などを備えている。
【０１２２】
現在情報記憶部３１６に当該ユーザの現在のユーザ情報（図１７参照）が存在する場合、最終利用拠点としてユーザの利用可能な拠点情報とともに監視端末１０２に送信する。
【０１２３】
図１７には、現在のユーザ情報を記憶するための現在ユーザ情報テーブルの構成が示されており、現在ユーザ情報テーブルは、ユーザを一意に識別するためのユーザＩＤ、ユーザが利用している監視端末１０２が接続された拠点を一意に識別するための拠点ＩＤを備えている。
【０１２４】
また、現在ユーザ情報テーブルは、在宅勤務か否かを示す在宅フラグ、テレワーク管理システム１００にログイン中であるか否かを示すためのオンラインフラグ、ユーザの動静情報、ユーザ異常情報、ユーザがテレワーク管理システム１００に最後にログインした日時、ユーザがテレワーク管理システム１００から最後にログアウトした日時を備えている。
【０１２５】
本ステップでは、ログインがなされたので、ログイン情報を現在ユーザ情報テーブルのオンラインフラグに記憶する。この場合、オンラインフラグにＴＲＵＥを記憶する。
【０１２６】
ステップＳ２０４では、監視端末１０２が接続している拠点を、証跡管理サーバ１１４から取得した拠点リストの中から選択を受付ける。
【０１２７】
監視端末１０２では、Ｗｉｆｉ網等から近辺住所を取得でき、取得した拠点リストから接続元拠点を特定できる場合、自動で接続元拠点を決定してユーザに確認し、近辺住所を取得できたが取得した拠点リストから接続元拠点の特定には至らない場合、拠点リストを近辺住所から近い順に表示し（最終利用拠点を先頭に表示する）、ユーザに選択させ、近辺住所を取得できない場合、最終利用拠点を先頭として、拠点リストを表示する。選択し

た拠点情報は証跡管理サーバ１１４に送信する。

【０１２８】

ステップＳ２０６では、証跡管理サーバ１１４が、監視端末１０２から受け取った拠点情報を、現在情報記憶部３１６の当該ユーザの現在のユーザ情報の拠点として登録し、当該ユーザがその拠点にログインしたことを、当該拠点の監視者の証跡監査端末１１２に通知する。

【０１２９】

通知を受けた証跡監査端末１１２は、当該ユーザが「オンライン」であることを画面に表示する。

【０１３０】

ステップＳ２０８では、証跡管理サーバ１１４が、ログインしたユーザの特徴量データがマスタデータ記憶部３１４に登録されているか否かを確認し、登録されていなければ、ステップＳ２１０において監視端末１０２に特徴量データを登録するよう命令し、登録されていれば、ステップＳ２１２において特徴量データを監視端末１０２に送信する。

【０１３１】

図１６には、特徴量データを記憶するための特徴量テーブルの構成が示されており、特徴量テーブルは、特徴量データを一意に識別するためのＩＤ、ユーザを特定するためのユーザ本人が居する画像データ、当該画像データから当該ユーザ本人を特定するための特徴量、当該画像が撮影された日時を含んで構成されている。

【０１３２】

ステップＳ２１０では、監視端末１０２が、カメラデバイス２１０で撮影して得られた画像中のユーザの顔を検出し、その顔画像から特徴量データを算出して証跡管理サーバ１１４へ送信する。

【０１３３】

尚、特徴量データは複数登録可能であり、登録する顔画像はユーザが選択できる。尚、カメラデバイス２１０で撮影して画像を得た後の処理は、証跡管理サーバ１１４で実施してもよい。

【０１３４】

ステップＳ２１２では、監視端末１０２が、証跡管理サーバ１１４から取得した特徴量データを使ってユーザの顔を認証できるようにする。

【０１３５】

ステップＳ２１４では、監視端末１０２が、ユーザが監視端末１０２の利用を終了しようとしているか否かを確認し、終了しようとしていなければ、ステップＳ２１６において動静を検出し、終了しようとしていれば、ステップＳ２２０においてログアウトする。

【０１３６】

ステップＳ２１６では、監視端末１０２が、カメラデバイス２１０で撮影して得られた画像に対して顔検出および顔認証を行うことでテレワーカーの動静（在席、離席）及びユーザ異常（なりすまし、覗き見）の発生を検出する。

【０１３７】

ユーザ自身の顔が一つだけ検出できれば「在席」、顔を検出できなければ「離席」、ユーザ自身の顔が検出できたが他にも顔を検出した場合は「覗き見」、ユーザ以外の顔だけ検出した場合は「なりすまし」とする。

【０１３８】

一度の検出結果で状態を決定せず、過去の検出結果を踏まえて総合的に状態遷移を判定する。

【０１３９】

状態が遷移して動静・ユーザ異常が発生したと判定した場合、その期間のユーザ証跡画像とともに検出結果を証跡管理サーバ１１４に送信する。

【０１４０】

同じ状態が継続した場合、定期的に動静およびユーザ異常の終了時刻の更新指示ととも

にユーザ証跡画像を証跡管理サーバ１１４に送信する。

【０１４１】

ステップＳ２２０では、証跡管理サーバ１１４が、監視端末１０２から送られてきた動静情報（図１９参照）、ユーザ異常情報（図２０参照）、及びユーザ証跡画像（図２１参照）を監査情報記憶部３２２に記憶する。

【０１４２】

図１９には、ユーザの動静情報を記憶するための動静テーブルの構成が示されており、動静テーブルは、動静情報を一意に識別するためのＩＤ、ユーザを一意に識別するためのユーザＩＤ、動静を検出した監視端末１０２を一意に識別するための端末ＩＤ、動静を示す状態、監視端末１０２で監視を開始した日時、終了した日時を含んで構成されている。

【０１４３】

図２０には、ユーザ異常情報を記憶するためのユーザ異常テーブルの構成が示されており、ユーザ異常テーブルは、ユーザ異常情報を一意に識別するためのＩＤ、監視端末１０２からログインしたユーザのユーザＩＤ、ユーザ異常を示す状態、拠点において不正侵入がなされた等の状態、監視端末１０２で監視を開始した日時、及び終了した日時を備えている。

【０１４４】

図２１には、ユーザ証跡画像を記憶するための監視端末証跡画像テーブルの構成が示されており、監視端末証跡画像テーブルは、ユーザ証跡画像を一意に識別するためのＩＤ、ユーザ証跡画像が監視端末１０２のカメラデバイス２１０（あるいは、Ｗｅｂカメラ）で撮影して得られた画像かスクリーンショットかを識別するための種別、ユーザＩＤ、ユーザ証跡画像に係る画像データ、当該画像データが撮影あるいは取得された日時を含んで構成されている。

【０１４５】

また、ユーザ異常が発生していた場合、拠点証跡画像および人体検出情報をストリーミングサーバ１１６から取得し、監査情報記憶部３２２に記憶する。

【０１４６】

新たな動静情報およびユーザ異常情報を記憶した場合、現在情報記憶部３１６の現在ユーザ情報テーブルの当該ユーザの動静および異常を更新し、証跡監査端末１１２に動静情報及びユーザ異常情報を送信する。

【０１４７】

動静情報及びユーザ異常情報を受けた証跡監査端末１１２は、当該ユーザの動静情報を拠点監視画面４００に表示し、ユーザ異常であればユーザにアラートを出してユーザ異常を監査するように促す。

【０１４８】

ステップＳ２２０では、監視端末１０２が、ユーザが監視端末１０２の利用を終了することを受けて、テレワーク管理システム１００からログアウトする。

【０１４９】

ステップＳ２２２では、証跡管理サーバ１１４が、現在情報記憶部３１６の当該ユーザのログイン情報をログアウト、つまり現在ユーザ情報テーブルのオンラインフラグをＦＡＬＳＥに変更し、証跡監査端末１１２に当該ユーザのログアウトを通知する。

【０１５０】

通知を受けた証跡監査端末１１２は、当該ユーザが「オフライン」であることを画面に表示する。

【０１５１】

ステップＳ２２４では、証跡管理サーバ１１４が、ユーザがログアウトした後、一定時間内に拠点を退室したかどうかを確認する。

【０１５２】

監視端末１０２の利用を終了した後にも拠点内に居続ける行為は、労働時間の詐称にあたる可能性があるからである。尚、詳細は図７を用いて後述する。

【０１５３】
以上で、監視端末１０２のカメラデバイス２１０を使ってユーザを監視する一連の流れの説明を終了する。
【０１５４】
以下、図６を参照して、本実施形態のテレワーク管理システム１００において、ネットワークカメラ１０４で拠点内の人数が増えたこと、さらにその人数が拠点内のログインユーザ数よりも多くなったことを検出したところから、不正侵入者を検出する一連の流れを説明する。
【０１５５】
証跡監査端末１１２と証跡管理サーバ１１４の処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムおよびデータをＲＡＭ２０２に記憶することで実行される。
【０１５６】
ステップＳ３００では、証跡管理サーバ１１４が、拠点内の人数が増えたことを受けて拠点内の人数およびテレワーク管理システム１００にログインしているユーザ数（監視端末１０２の数）を監視する。
【０１５７】
本来、拠点内の人数がログインユーザ数よりも多くなったのであれば、新たに別の社員が拠点を訪れて監視端末１０２を利用するはずなので、その後拠点内のログインユーザ数が増えるはずである。
【０１５８】
一定時間何も変化がなければ、社員以外が拠点に進入して目的を達成して出て行くという不正侵入があったものとみなし、不正侵入情報（詳細後述）を登録する。
【０１５９】
ステップＳ３０２では、証跡管理サーバ１１４が、当該拠点のログインユーザ数を確認し、その数が増えたのであれば正規ユーザが勤務を開始したと推測できるので問題なしと判断して処理を終了し、そうでなければ、ステップＳ３０４へ処理を進めて、拠点内の人数を確認する。
【０１６０】
ステップＳ３０４では、証跡管理サーバ１１４が、拠点内の人数を確認し、その人数が減ったのであれば、不正侵入者が拠点から出たと判断して、ステップＳ３０６へ処理を進め、そうでなければ引き続き拠点内の人数およびログインユーザ数を監視する。
【０１６１】
ステップＳ３０６では、証跡管理サーバ１１４が、監査情報記憶部３２２に不正侵入情報（拠点異常情報、図２２参照）を記憶する。
【０１６２】
図２２には、拠点異常情報を記憶するための拠点異常テーブルを備えており、拠点異常テーブルは、拠点異常情報を一意に識別するためのＩＤ、ネットワークカメラ１０４を一意に識別するためのカメラＩＤ、拠点において不正侵入がなされた等の状態、監視端末１０２で監視を開始した日時、終了した日時を備えている。
【０１６３】
また、拠点異常テーブルは、テレワーク管理者が監査を行った結果を記憶するための監査結果、テレワーク管理者を一意に識別するためのユーザＩＤからなる監査者を含んで構成されている。
【０１６４】
同時に、ストリーミングサーバ１１６から拠点証跡画像及び人体検出情報を取得して監査情報記憶部３２２の証跡画像テーブル及び人体検出情報記憶テーブルに記憶する。
【０１６５】
また、現在情報記憶部３１６の当該ユーザの拠点異常情報も更新する。つまり、現在拠点情報テーブルの異常フラグを、例えば、不正侵入を示すフラグで更新する。

【０１６６】
ステップＳ３０８では、証跡管理サーバ１１４が、証跡監査端末１１２に拠点異常の発生を通知する。
【０１６７】
ステップＳ３１０では、証跡監査端末１１２が、証跡管理サーバ１１４から現在の拠点情報を取得して不正侵入の疑いがあることを拠点監視画面４００に表示する。
【０１６８】
テレワーク管理者が拠点監視画面４００を見ているとは限らないし、他の拠点を監視中かもしれないので、警告ダイアログなどを出して証跡を確認するよう促す。例えば、拠点監視画面４００の警告表示領域４０４にその旨を表示する。
【０１６９】
以上で、不正侵入者を検出する一連の流れの説明を終了する。
【０１７０】
以下、図７を参照して、本実施形態は、テレワーク管理システム１００において、テレワーカーが監視端末１０２の利用を終了してからも拠点内に居続ける労働時間の詐称にあたる行為を検出する一連の流れを説明する。
【０１７１】
証跡監査端末１１２と証跡管理サーバ１１４との処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムおよびデータをＲＡＭ２０２に記憶することで実行される。
【０１７２】
ステップＳ４００では、証跡管理サーバ１１４が、拠点内のログインユーザ数が増えたことを受けて拠点内の人数およびテレワーク管理システム１００にログインしているユーザ数（監視端末１０２の数）を監視する。
【０１７３】
本来ユーザが監視端末１０２の利用を終了してログアウトしたのであれば、その後拠点を退出する（つまり拠点内の人体数は減る）はずである。
【０１７４】
一定時間何も変化がなければ、監視端末１０２の利用を終了することで監視端末１０２による動静記録を逃れた上で継続して労働を行っている（すなわち労務時間の詐称）ものとみなして労務時間詐称情報（図２２参照）を登録する。
【０１７５】
労務時間詐称情報は、図２２に示す拠点異常テーブルに記憶され、基本的に拠点異常情報と変わりはないが、状態については、労務時間を詐称した旨を示す情報が記憶される。
【０１７６】
ステップＳ４０２では、証跡管理サーバ１１４が、当該拠点の人体数を確認し、その人体数が減ったのであれば正規ユーザが退社したと判断して処理を終了し、そうでなければ、ステップＳ４０４へ処理を進め、拠点内のログインユーザ数を確認する。
【０１７７】
ステップＳ４０４では、証跡管理サーバ１１４が、拠点内のログインユーザ数を確認し、その数が増えたのであればログインしていたユーザが監視端末１０２を再起動したり場所を移動するために一時的にオフラインになったりしていたと推測できるので問題なしと判断して処理を終了し、そうでなければ、引き続き拠点内の人体数およびログインユーザ数を監視する。
【０１７８】
ステップＳ４０６では、証跡管理サーバ１１４が、監査情報記憶部３２２の拠点異常テーブルに労務時間詐称情報（拠点異常情報）を記憶する。
【０１７９】
同時に、ストリーミングサーバ１１６から拠点証跡画像（静止画像または動画像）及び人体検出情報を取得して監査情報記憶部３２２の証跡画像テーブル及び人体検出テーブル

に記憶する。また、現在情報記憶部３１６の当該ユーザの拠点異常情報も更新、つまり現在拠点情報テーブルの異常フラグを更新する。

【０１８０】

ステップＳ４０８では、証跡管理サーバ１１４が、証跡監査端末１１２に拠点異常の発生を通知する。

【０１８１】

ステップＳ４１０では、証跡監査端末１１２が、証跡管理サーバ１１４から現在の拠点情報を取得して労務時間詐称の可能性があることを画面に表示する。

【０１８２】

テレワーク管理者が画面を見ているとは限らないし、他の拠点を監視中かもしれないので、警告ダイアログなどを出して証跡を確認するよう促す。表示する画面の例を図１０に示す。

【０１８３】

図１０には、拠点監視画面４００が示されており、拠点証跡画像表示領域４０５に労務時間詐称の可能性がある旨を示す情報が表示されている。

【０１８４】

以上で、労務時間の詐称にあたる行為を検出する一連の流れの説明を終了する。

【０１８５】

以下、図８を参照して、本実施形態のテレワーク管理システム１００において、テレワーク管理者がユーザの異常（なりすましや覗き見）と拠点の異常（不正侵入や労務時間詐称）を監査する一連の流れを説明する。

【０１８６】

証跡監査端末１１２と証跡管理サーバ１１４の処理は、そのＣＰＵ２０１により、ＲＯＭ２０３から取得したプログラムおよびデータをＲＡＭ２０２に記憶することで実行される。

【０１８７】

ステップＳ５００では、証跡監査端末１１２が、監視中の拠点で発生中の異常を監査するかどうかユーザに確認し、確認するのであれば、ステップＳ５０６へ処理を進め、その情報を即座に表示し、それ以外の過去の異常を監査するのであれば、ステップＳ５０４へ処理を進め、異常の一覧を表示する。

【０１８８】

ステップＳ５０２では、証跡管理サーバ１１４が、指定拠点内の異常の一覧を検索して証跡監査端末１１２に返却する。

【０１８９】

ステップＳ５０４では、証跡監査端末１１２が、ユーザからの監査対象の選択を受付ける。その際、一覧を異常の種類によってフィルタリングする機能や、並び順を変えるソート機能を提供してもよい。

【０１９０】

ステップＳ５０６では、証跡管理サーバ１１４が、指定の異常の発生期間内のネットワークカメラ１０４から取得した拠点異常情報（ネットワークカメラの動画像または静止画像および人体検出情報）及び、各ログインユーザの動静情報とユーザ異常情報及びその際のユーザ証跡画像を検索して証跡監査端末１１２に返却する。

【０１９１】

ステップＳ５０８では、証跡監査端末１１２が、拠点異常情報とユーザ異常情報を画面に表示し、テレワーク管理者に確認させて、最終的な異常（または異常なし）を決定させ、その監査結果を証跡管理サーバ１１４に送信する。

【０１９２】

情報の確認のさせ方としては、発生期間内の情報を自動で時系列順に流して確認させる方法や、確認したい時刻を指定させてその際の情報を確認させる方法などがある。異常を監査する画面の例を図１１に示す。

【０１９３】
図１１には、監査画面５００の構成が示されており、監査画面５００は、監査対象とする拠点を示す拠点表示領域５０１、拠点の異常の種類によって監査すべき対象を絞り込むための状態選択欄５０２、当該拠点における監視結果を表示する監視情報表示領域５０３を備えている。
【０１９４】
また、監査画面５００は、ネットワークカメラ１０４が設置された拠点を選択するためのカメラ拠点選択欄５０４、不正侵入の警告表示を行うための警告表示領域５０５、ネットワークカメラ１０４で撮影して得られた画像に係る拠点証跡画像として表示するための拠点証跡画像表示領域５０６を備えている。
【０１９５】
ステップＳ５１０では、証跡管理サーバ１１４が、監査結果を拠点異常テーブルへ記憶し、当該拠点を監視しているすべての証跡監査端末１１２に監査が行われたことを通知する。
【０１９６】
通知を受けた証跡監査端末１１２は、証跡管理サーバ１１４から現在の拠点情報を取得して画面の表示を更新する。
【０１９７】
ステップＳ５１２では、証跡監査端末１１２が、他の異常を監査するかどうかユーザに確認し、継続するのであれば、ステップＳ５０２へ処理を進めて、異常の一覧を表示し、継続しないのであれば処理を終了する。
【０１９８】
以上で、テレワーク管理者がユーザの異常と拠点の異常を監査する一連の流れの説明を終了する。
［第２の実施形態］
【０１９９】
次に、第２の実施形態について説明を行うが、基本的な構成及び処理については、ほぼ同様な構成及び処理を備えるため、第１の実施形態と同一の構成及び処理については、詳細な説明を省略して、同一符号を用いて説明を行う。
【０２００】
図２５及び図２６には、ネットワークカメラ１０４による拠点監視を行う一連の流れを説明する。
【０２０１】
ステップＳ６００では、ストリーミングサーバ１１６において、拠点監視部３３６は、撮影して得られた画像に対して人の検出を行い、拠点証跡画像と人体検出情報とを拠点監視情報記憶部３３８に記憶する。そして、証跡管理サーバ１１４に対して拠点証跡画像と人体検出情報とを送信する。
【０２０２】
ステップＳ６０２では、証跡管理サーバ１１４において、拠点異常検出部３２３は、ストリーミングサーバ１１６から送信される拠点証跡画像に対して、新たに入室した者（不明者）がいるかいないかの判定を行い、不明者がいると判定した場合は、ステップＳ６０４へ処理を進め、不明者がいると判定しない場合は、処理を終了する。
【０２０３】
本判定方法の１例として、ネットワークカメラ１０４の追尾機能を用いて、既に追跡している人体以外の人体が検知できたときに、新たに入室した者（不明者）がいるとして判定を行う。
【０２０４】
ステップＳ６０４では、証跡管理サーバ１１４において、不明者の入室した時間（撮影日時）を人体情報テーブル（図２８）へ記憶する。
【０２０５】

図２８には、ネットワークカメラ１０４で追尾対象となる人体とログインしているユーザとの対応を示す人体情報を記憶するための人体情報テーブルが図示されており、ネットワークカメラ１０４の追跡対象となる人体を一意に識別するためのＮＯ、追跡対象となる人体に関わる特徴量等の人体情報、人体に紐付けられたユーザＩＤ、人体が入室した時間等を含んで構成されている。

【０２０６】

ステップＳ６０６では、証跡管理サーバ１１４において、拠点証跡画像から特定される人体のうち、ログインユーザと紐付いていない人体が存在するか否かを判定し、存在すると判定した場合は、ステップＳ６０８へ処理を進め、存在すると判定しない場合は、ステップＳ６１０へ処理を進める。

【０２０７】

本ステップでは、人体情報テーブルにおいて、ユーザＩＤが登録されていない人体情報が存在する場合、ステップＳ６０８へ処理を進め、存在すると判定しない場合、ステップＳ６１０へ処理を進める。

【０２０８】

ステップＳ６０８では、証跡管理サーバ１１４において、人体とログインユーザとの紐付けを行う。紐付けの方法としては、例えば、人体の顔画像と、ログインしているユーザのユーザ情報に含まれるプロフィール画像（顔画像）との類似度が高いものを紐付ける方法や、人体の顔画像と、カメラデバイス２１０で撮影して得られた人の画像の上半身との色ヒストグラムによる類似度が高いものを紐付ける方法がある。

【０２０９】

また、人体と、ネットワークカメラ１０４で撮影して得られた監視端末１０２との距離が近い場合、当該監視端末１０２にログインしているものとして扱って、紐付ける方法などがあげられる。

【０２１０】

そして、紐付けられた人体に関する人体情報に対応して、ログインしているユーザのユーザＩＤを人体情報テーブルへ記憶する。

【０２１１】

ステップＳ６１０では、証跡管理サーバ１１４において、不明者の数が減ったか否かを判定し、減ったと判定した場合は、ステップＳ６１４へ処理を進め、減ったと判定しない場合は、ステップＳ６１２へ処理を進める。

【０２１２】

本ステップにおける判定方法の１例としては、前述したように、ネットワークカメラ１０４において、追尾対象となる人体の数の増減によって判定することが可能である。

【０２１３】

これにより、入室した不明者が、すぐに退室したことが想定され、悪意のある者か、悪意の無い者かに関わらず監視者へ通知を行う。

【０２１４】

ステップＳ６１２では、証跡管理サーバ１１４において、不明者が入室してから一定時間経過したか否かを判定し、一定時間経過したと判定した場合は、ステップＳ６１４へ処理を進め、一定時間経過したと判定しない場合は、ステップＳ６１６へ処理を進める。

【０２１５】

これによって、不明者が入室した後、一定時間以内に、監視端末１０２の前に座って、ログインを行ったか否かによって、不正侵入がなされていることを監視者へ通知することが可能となる。

【０２１６】

ステップＳ６１４では、不正侵入であることを証跡監査端末１１２へ通知する。

【０２１７】

ステップＳ６１６では、証跡管理サーバ１１４において、人体と紐付けられたユーザの人数が減ったか否かを判定し、減ったと判定した場合は、ステップＳ６１８へ処理を進め

、減ったと判定しない場合は、ステップＳ６００へ処理を進める。
【０２１８】
ステップＳ６１８では、監視端末１０２において、ログインしているユーザの在席状況を判定し、離席、あるいはログアウトしていると判定した場合は、ステップＳ６２０へ処理を進め、在席していると判定した場合は、ステップＳ６２２へ処理を進める。
【０２１９】
ステップＳ６２０では、ユーザの動静を退室したものとして、動静情報を監査情報記憶部３２２へ記憶し、ステップＳ６２２では、ログインしているユーザと、まだ紐付いていない人体との紐付けを見直すが、見直しの方法は、ステップＳ６０８と同様な処理を行う。
【０２２０】
ステップＳ６２４では、人体に紐付けられたユーザのログアウトから一定時間経過したか否かを判定し、経過したと判定した場合は、ステップＳ６２６へ処理を進め、経過したと判定しない場合は、ステップＳ６００へ処理を進める。
【０２２１】
以下、図２７を参照して、本実施形態のテレワーク管理システム１００において、監視端末１０２のカメラデバイス２１０を使ってユーザを監視する一連の流れを説明する。
【０２２２】
ステップＳ７００では、監視端末１０２が、カメラデバイス２１０で撮影して得られた画像に対して顔検出および顔認証を行うことでテレワーカーの動静（在席、離席）及びユーザ異常（なりすまし、覗き見）を証跡管理サーバ１１４に送信する。
【０２２３】
ステップＳ７０１では、証跡管理サーバ１１４において、監視端末１０２から送信される動静を受付け、ステップＳ７０２では、証跡管理サーバ１１４において、ステップＳ７０２で受付けた動静が、在席であるか否かを判定し、在席であると判定した場合は、ステップＳ７０４へ処理を進め、在席であると判定しない場合は、ステップＳ２１６へ処理を進める。
【０２２４】
ステップＳ７０４では、証跡管理サーバ１１４において、在席であると判定したユーザに紐付いた人体がいるか否かを判定し、いると判定した場合は、ステップＳ２１６へ処理を進め、いると判定しない場合は、ステップＳ７０６へ処理を進める。
【０２２５】
本ステップにおける判定の１例として、人体情報テーブルのユーザＩＤが存在しない人体情報が存在する場合は、ステップＳ７０６へ処理を進める。
【０２２６】
ステップＳ７０６では、証跡管理サーバ１１４において、不明者の人数を判定し、１人であると判定した場合は、ステップＳ７０８へ処理を進め、２人以上であると判定した場合は、ステップＳ７１０へ処理を進める。
【０２２７】
ステップＳ７１０では、証跡管理サーバ１１４において、人体とログインユーザとの紐付けを行う。紐付けの方法としては、前述した方法があげられる。
【０２２８】
ステップＳ７１２では、ユーザの動静を在室したものとして、動静情報を監査情報記憶部３２２へ記憶する。
【０２２９】
尚、本処理では、ログアウトされて、そのユーザが、ネットワークカメラ１０４において追尾できなくなったときに、人体情報テーブルの人体情報を削除する。
【０２３０】
また、本処理において、監視者へ通知を行う際に、図２９に示すような拠点監視画面４００において通知され、拠点証跡画像表示領域４０５には、不審者となる人体を識別して

表示を行うとともに、人体に紐付けられたログインユーザが識別可能なようにユーザ名や顔画像等を人体の近辺に表示する。

【０２３１】

さらに、ログインしているユーザの人数と拠点人数とが一致しない場合であっても、ログインしているユーザが退室した場合であれば、不正侵入がなされたと見做さないような運用を取ることが可能となる。

【０２３２】

以上、本発明によれば、拠点における人物の数と情報処理システムにログインしている人数とを比較することで、拠点における人物の監視を精度良く行うことができる。

【０２３３】

以上、実施形態例を詳述したが、本発明は、例えば、方法、プログラムもしくは記憶媒体等としての実施態様をとることが可能であり、具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

【０２３４】

また、本発明におけるプログラムは、各処理方法をコンピュータが実行可能（読み取り可能）なプログラムであり、本発明の記憶媒体は、各処理方法をコンピュータが実行可能なプログラムが記憶されている。

【０２３５】

なお、本発明におけるプログラムは、各装置の処理方法ごとのプログラムであってもよい。

【０２３６】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読取り実行することによっても、本発明の目的が達成されることは言うまでもない。

【０２３７】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記憶した記録媒体は本発明を構成することになる。

【０２３８】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク等を用いることができる。

【０２３９】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータで稼働しているＯＳ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２４０】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２４１】

また、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。

【０２４２】

また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログ

ラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０２４３】

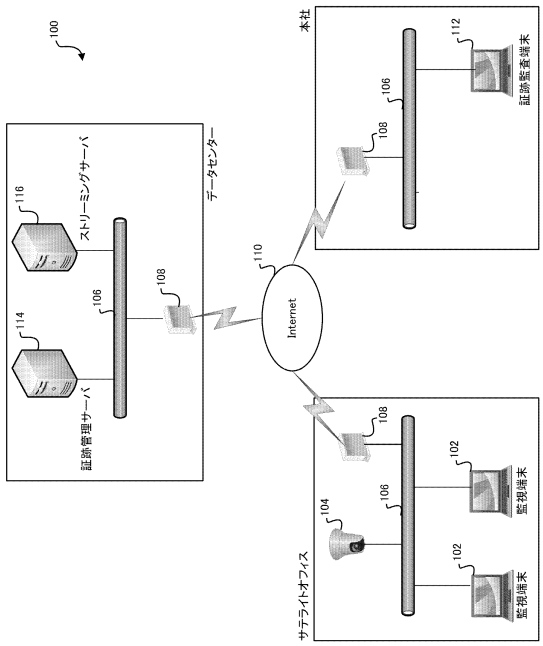
さらに、本発明を達成するためのプログラムをネットワーク上のサーバ，データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステム、あるいは装置が、本発明の効果を享受することが可能となる。なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

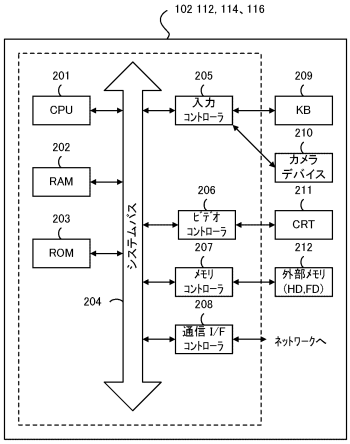
【０２４４】

１００　テレワーク管理システム
１０２　監視端末
１０４　ネットワークカメラ
１０６　ローカルエリアネットワーク（ＬＡＮ）
１０８　ルータ
１１０　インターネット
１１２　証跡監査端末
１１４　証跡管理サーバ
１１６　ストリーミングサーバ
２０１　ＣＰＵ
２０２　ＲＯＭ
２０３　ＲＡＭ
２０４　システムバス
２０５　入力コントローラ
２０６　ビデオコントローラ
２０７　メモリコントローラ
２０８　通信Ｉ／Ｆコントローラ
２０９　ＫＢ
２１０　カメラデバイス
２１１　ＣＲＴ
２１２　外部メモリ

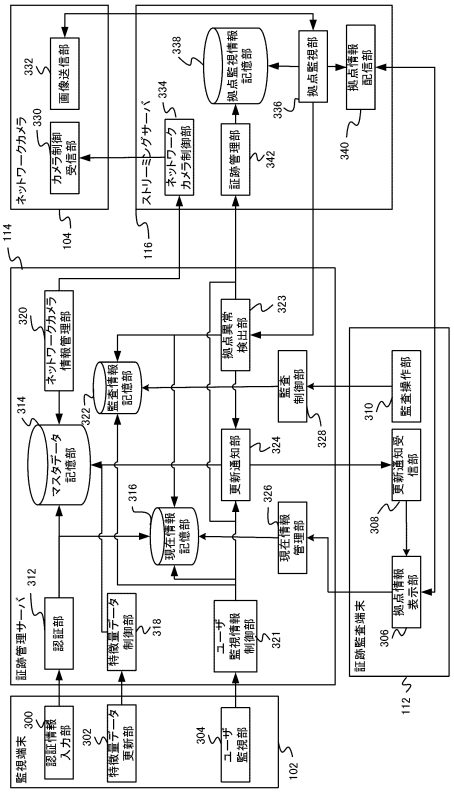
【図１】


100
本社
データセンター
ストリーミングサーバ
証跡管理サーバ
Internet
証跡監査端末
監視端末
サテライトオフィス
監視端末
116
114
106
108
110
112
102
104

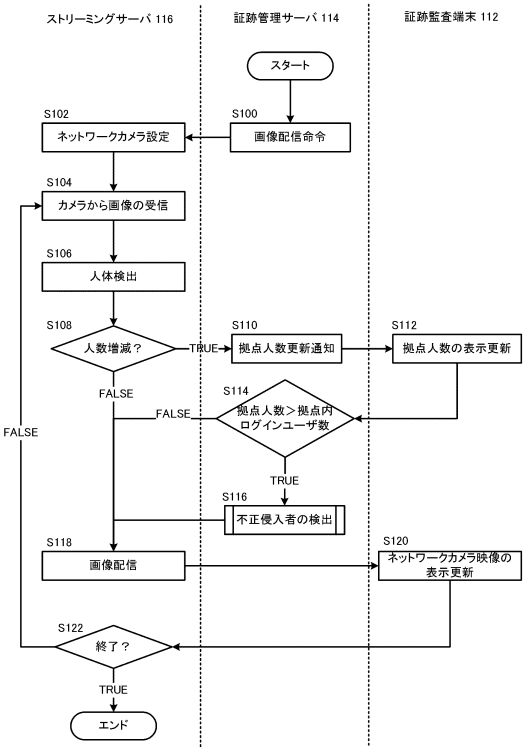
【図２】


102 112, 114、116
CPU
RAM
ROM
システムバス
204
入力コントローラ
ビデオコントローラ
メモリコントローラ
通信 I/F コントローラ
KB
カメラデバイス
CRT
外部メモリ (HD,FD)
ネットワークへ
201
202
203
205
206
207
208
209
210
211
212

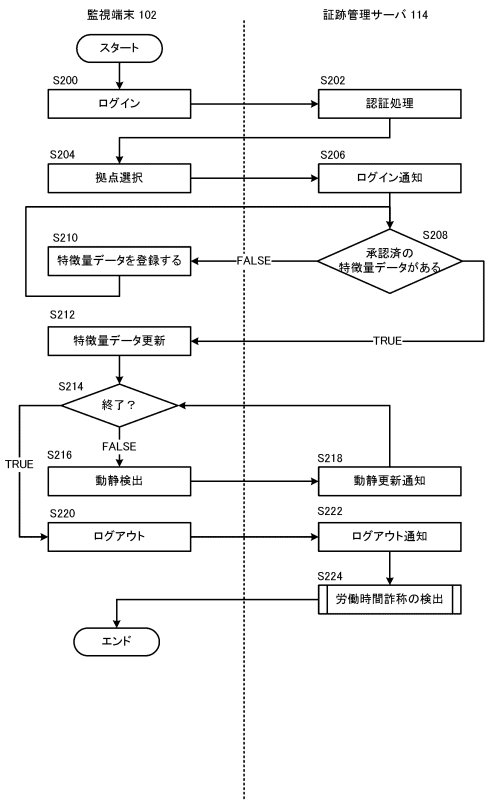
【図３】


監視端末
認証情報入力部
特徴量データ更新部
ユーザ監視部
証跡管理サーバ
認証部
特徴量データ制御部
ユーザ監視情報制御部
現在情報記憶部
マスタデータ記憶部
ネットワークカメラ情報管理部
監査情報記憶部
更新通知部
現在情報管理部
拠点異常検出部
監査制御部
証跡監査端末
監査操作部
更新通知受信部
拠点情報表示部
ネットワークカメラ
画像送信部
カメラ制御受信部
ストリーミングサーバ
ネットワークカメラ制御部
拠点監視情報記憶部
拠点監視部
拠点情報配信部
証跡管理部
102
104
112
114
116
300
302
304
306
308
310
312
314
316
318
320
321
322
323
324
326
328
330
332
334
336
338
340
342

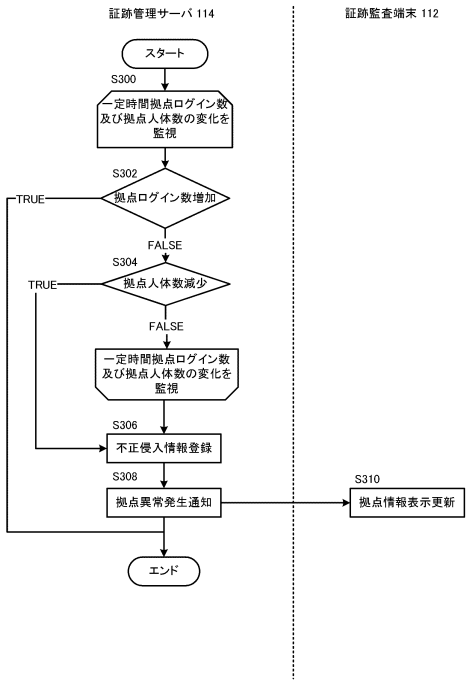
【図４】


ストリーミングサーバ 116
証跡管理サーバ 114
証跡監査端末 112
スタート
S100
画像配信命令
S102
ネットワークカメラ設定
S104
カメラから画像の受信
S106
人体検出
S108
人数増減？
TRUE
FALSE
S110
拠点人数更新通知
S112
拠点人数の表示更新
S114
拠点人数＞拠点内ログインユーザ数
FALSE
TRUE
S116
不正侵入者の検出
S118
画像配信
S120
ネットワークカメラ映像の表示更新
S122
終了？
TRUE
エンド
FALSE

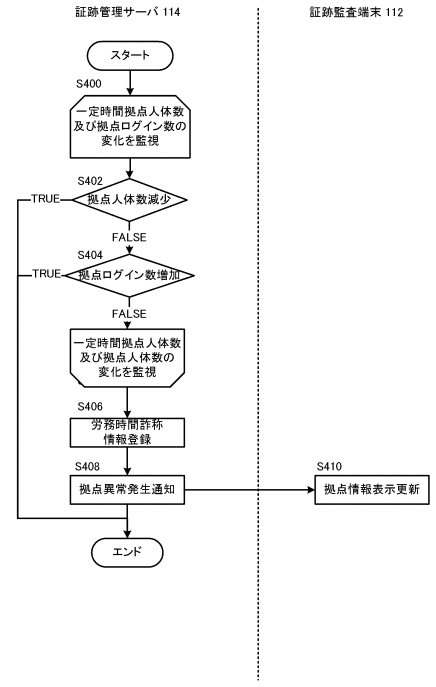
【図５】


監視端末 102
証跡管理サーバ 114
スタート
S200
ログイン
S202
認証処理
S204
拠点選択
S206
ログイン通知
S208
承認済の特徴量データがある
FALSE
S210
特徴量データを登録する
TRUE
S212
特徴量データ更新
S214
終了？
FALSE
TRUE
S216
動静検出
S218
動静更新通知
S220
ログアウト
S222
ログアウト通知
S224
労働時間詐称の検出
エンド

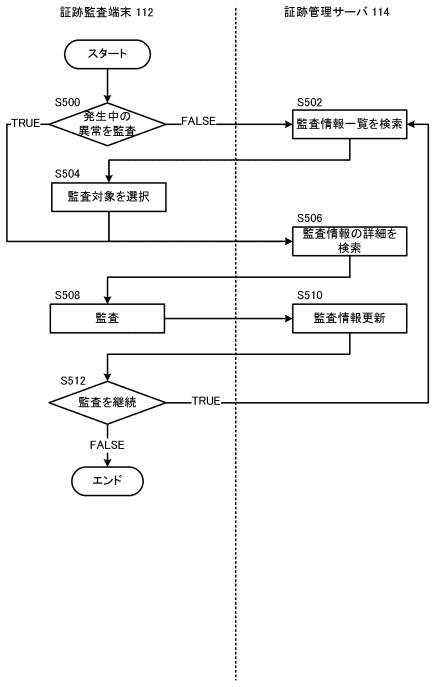
【図６】


証跡管理サーバ 114
証跡監査端末 112
スタート
S300
一定時間拠点ログイン数及び拠点人体数の変化を監視
S302
拠点ログイン数増加
TRUE
FALSE
S304
拠点人体数減少
TRUE
FALSE
一定時間拠点ログイン数及び拠点人体数の変化を監視
S306
不正侵入情報登録
S308
拠点異常発生通知
S310
拠点情報表示更新
エンド

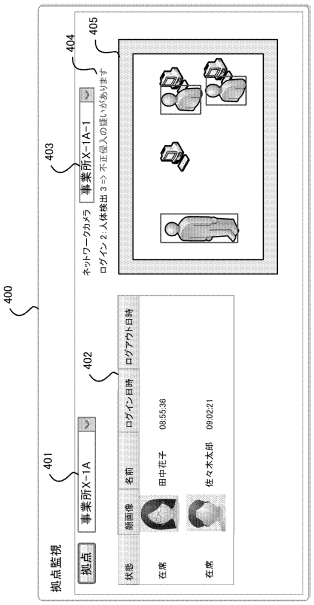
【図７】


証跡管理サーバ 114
証跡監査端末 112
スタート
S400
一定時間拠点人体数及び拠点ログイン数の変化を監視
S402
拠点人体数減少
TRUE
FALSE
S404
拠点ログイン数増加
TRUE
FALSE
一定時間拠点人体数及び拠点人体数の変化を監視
S406
労務時間詐称情報登録
S408
拠点異常発生通知
S410
拠点情報表示更新
エンド

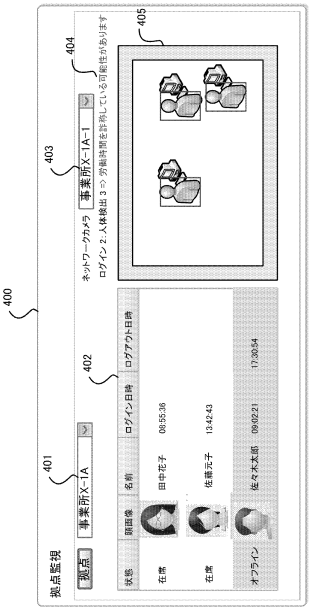
【図８】


証跡監査端末 112
証跡管理サーバ 114
スタート
S500
発生中の異常を監査
TRUE
FALSE
S502
監査情報一覧を検索
S504
監査対象を選択
S506
監査情報の詳細を検索
S508
監査
S510
監査情報更新
S512
監査を継続
TRUE
FALSE
エンド

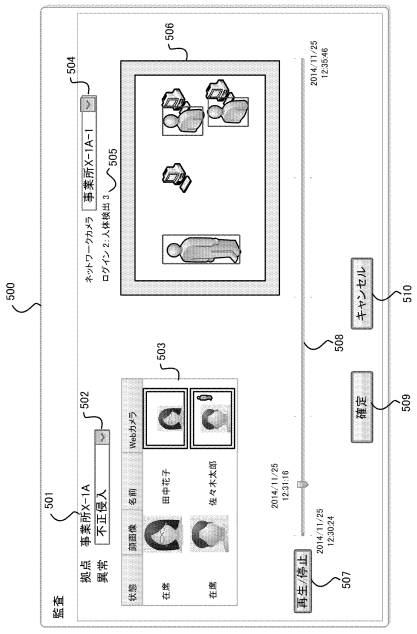
【図９】




【図１０】




【図１１】




【図１２】

| ユーザID | アカウント | パスワード | 名前 | フリガナ | 種別 | 住所 | プロフィール画像 | 勤務開始対象 | 監査対象 | 監視権限 | 在宅権限 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| user01 | kanshijuco | p20k17178 | 監視重郎 | カンシジュウロウ | 個人 | 東京都豊島区 | 1111.jpg | office01 | observe01 | TRUE | |
| user02 | tanakahanako | ppyy89 | 田中花子 | タナカハナコ | 個人 | 富山県小山町 | 2222.jpg | office03 | | | TRUE |
| user03 | suzukichiro | sat325kk | 鈴木一郎 | スズキイチロウ | 個人 | 富山県富山市 | 3333.jpg | office04 | | | TRUE |
| user04 | satomotoko | bwc89894 | 佐藤元子 | サトウモトコ | 個人 | 富山県富山市 | 4444.jpg | office04 | | | |
| user05 | asashitaro | kkk2455 | 佐々木太郎 | ササキタロウ | 個人 | 神奈川県横浜市 | 5555.jpg | office01 | | | TRUE |
| user06 | darekajuco | kkk4467 | だれか重二 | ダレカジュウジ | 個人 | 神奈川県横浜市 | 6666.jpg | office01 | observe01 | | |
| ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ |
| ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ |

【図１３】

| 拠点ID | 名前 | フリガナ | 住所 |
|---|---|---|---|
| office01 | 本社4A | ホンシャ4A | 東京都港区 |
| office02 | 本社4B | ホンシャ4B | 東京都港区 |
| office03 | 事業所X-1A | ジギョウショX-1A | 富山県富山市 |
| office04 | 事業所X-1B | ジギョウショX-1B | 富山県富山市 |
| ・ | ・ | ・ | ・ |

【図１４】

| カメラID | 名前 | 拠点ID | URL | パスワード |
|---|---|---|---|---|
| camera01 | 事業所X-1A-1 | office03 | https://hogehoge.office03.co.jp:8001 | ******** |
| camera02 | 事業所X-1A-2 | office03 | https://hogehoge.office03.co.jp:8002 | ******** |
| camera03 | 事業所X-1B-1 | office04 | https://hogehoge.office04.co.jp:8001 | ******** |
| ・ | ・ | ・ | ・ | ・ |

【図１５】

| ID | 拠点ID | 監視者IDリスト |
|---|---|---|
| oo01 | office03 | [user01,user06] |
| oo02 | office04 | [user01] |
| ・ | ・ | ・ |

【図１６】

| ID | ユーザID | 画像データ | 特徴量 | 撮影日時 |
|---|---|---|---|---|
| ft01 | user02 | ・・・・ | ・・・・ | 2014/11/19 9:55 |
| ft02 | user02 | ・・・・ | ・・・・ | 2014/11/19 9:57 |
| ・ | ・ | ・ | ・ | ・ |

【図１７】

| ユーザID | 拠点ID | 在宅 | オンライン | 動静 | 異常 | 最終ログイン日時 | 最終ログアウト日時 |
|---|---|---|---|---|---|---|---|
| user02 | office04 | | TRUE | 在席 | | 2014/11/19 8:55 | 2014/11/18 18:31 |
| user05 | office04 | | TRUE | 在席 | | 2014/11/19 9:02 | 2014/11/18 17:30 |
| user04 | office04 | | FALSE | 離席 | | 2014/11/18 13:42 | 2014/11/18 18:12 |
| user03 | office04 | TRUE | TRUE | 離席 | なりすまし | 2014/11/19 8:41 | 2014/11/18 19:12 |
| ・ | ・ | ・ | ・ | ・ | ・ | ・ | ・ |

【図１８】

| 拠点ID | 人体数 | 異常 | 最終入室 | 最終退室 |
|---|---|---|---|---|
| office01 | 5 | | 2014/11/19 14:55 | 2014/11/19 14:31 |
| office02 | 1 | | 2014/11/19 13:02 | 2014/11/19 14:30 |
| office04 | 3 | 不正侵入 | 2014/11/19 14:42 | 2014/11/19 15:12 |
| ・ | ・ | ・ | ・ | ・ |

【図１９】

| ID | ユーザID | 端末ID | 状態 | 開始日時 | 終了日時 |
|---|---|---|---|---|---|
| movement01 | user02 | terminal02 | 在席 | 2014/11/19 8:55 | 2014/11/19 12:00 |
| movement02 | user02 | terminal02 | 離席 | 2014/11/19 12:00 | 2014/11/19 12:58 |
| movement03 | user02 | terminal02 | 在席 | 2014/11/19 12:58 | 2014/11/19 18:31 |
| ・ | ・ | ・ | ・ | ・ | ・ |

【図２０】

| ID | ユーザID | 状態 | 開始日時 | 終了日時 | 監査結果 | 監査者 |
|---|---|---|---|---|---|---|
| unauthorized04 | user02 | なりすまし | 2014/11/19 12:30 | 2014/11/19 12:38 | なりすまし | user01 |
| unauthorized05 | user02 | 覗き見 | 2014/11/19 17:30 | 2014/11/19 19:43 | 異常なし | user01 |
| ・ | ・ | ・ | ・ | ・ | ・ | ・ |

【図２１】

| ID | 種別 | ユーザID | 画像データ | 撮影日時 |
|---|---|---|---|---|
| image01 | Webカメラ | user02 | ・・・・ | 2014/11/19 8:52 |
| image02 | Webカメラ | user02 | ・・・・ | 2014/11/19 9:00 |
| image03 | Webカメラ | user02 | ・・・・ | 2014/11/19 12:30 |
| image04 | スクリーンショット | user02 | ・・・・ | 2014/11/19 12:30 |
| image05 | Webカメラ | user02 | ・・・・ | 2014/11/19 12:35 |
| image06 | Webカメラ | user02 | ・・・・ | 2014/11/19 12:38 |

【図２２】

| ID | カメラID | 状態 | 開始日時 | 終了日時 | 監査結果 | 監査者 |
|---|---|---|---|---|---|---|
| unauthorized04 | camera01 | 不正侵入 | 2014/11/19 12:30 | 2014/11/19 12:38 | 不正侵入 | user01 |
| unauthorized05 | camera01 | 労働時間詐称 | 2014/11/19 17:30 | 2014/11/19 19:43 | 異常なし | user01 |
| ・ | ・ | ・ | ・ | ・ | ・ | ・ |

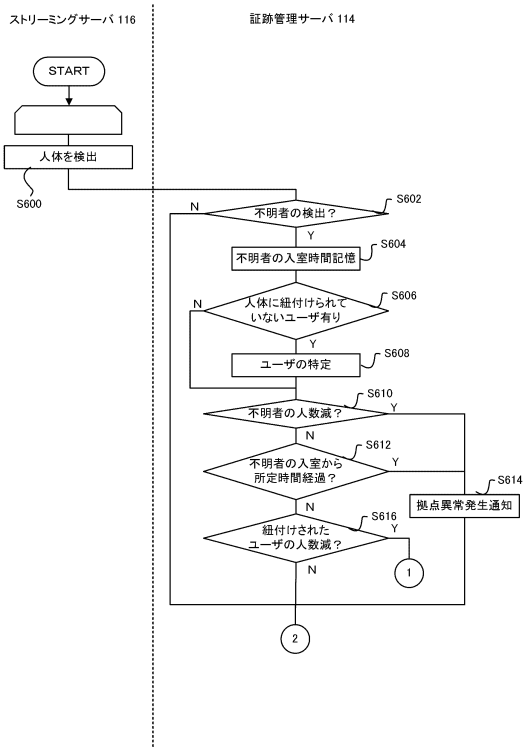
【図２３】

| ID | カメラID | 画像データ | 撮影日時 |
|---|---|---|---|
| image01 | camera01 | ・・・・ | 2014/11/19 8:52 |
| image02 | camera01 | ・・・・ | 2014/11/19 9:00 |
| image03 | camera01 | ・・・・ | 2014/11/19 12:30 |

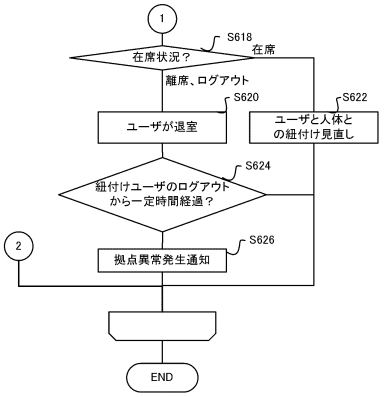
【図２４】

| ID | カメラID | 人体数 | 座標 | 撮影日時 |
|---|---|---|---|---|
| body01 | camera01 | 1 | ・・・・ | 2014/11/19 8:52 |
| body02 | camera01 | 2 | ・・・・ | 2014/11/19 8:53 |
| body03 | camera01 | 3 | ・・・・ | 2014/11/19 8:54 |
| body04 | camera01 | 3 | ・・・・ | 2014/11/19 8:55 |
| body05 | camera01 | 3 | ・・・・ | 2014/11/19 8:56 |
| ・ | ・ | ・ | ・ | ・ |

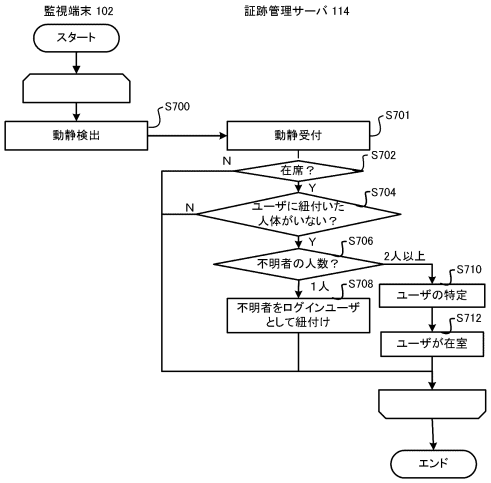
【図２５】




【図２６】



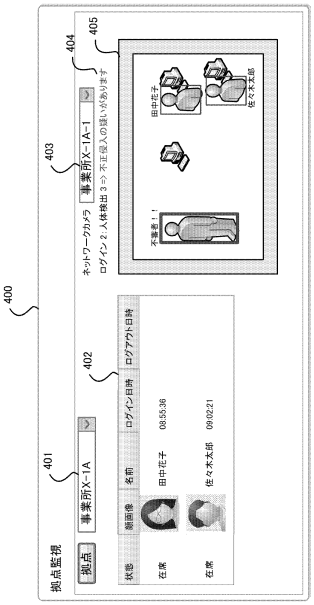

【図２７】




【図２８】

| NO | 人体情報 | ユーザID | 入室時間 |
|---|---|---|---|

【図２９】


400
401
402
403
404
405
拠点監視
拠点
事業所X-1A
ネットワークカメラ
事業所X-1A-1
ログイン 2：人体検出 3 => 不正侵入の疑いがあります
状態
顔画像
名前
ログイン日時
ログアウト日時
在席
田中花子
08:55:38
在席
佐々木太郎
09:02:21
不審者＃1
田中花子
佐々木太郎

フロントページの続き

(56)参考文献 特開２００８－０４０９３７（ＪＰ，Ａ）
特開２００９－０８０６４１（ＪＰ，Ａ）
特開２００６－０７２４４６（ＪＰ，Ａ）
特開２００７－２８６９１２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００