(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-84170
(P2017-84170A)
(43)公開日　平成29年5月18日(2017.5.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 13/00	(2006.01)	G06F	13/00	650A	5B084
H04M 11/00	(2006.01)	H04M	11/00	302	5K201

審査請求 未請求　請求項の数 13　ＯＬ　（全 21 頁）

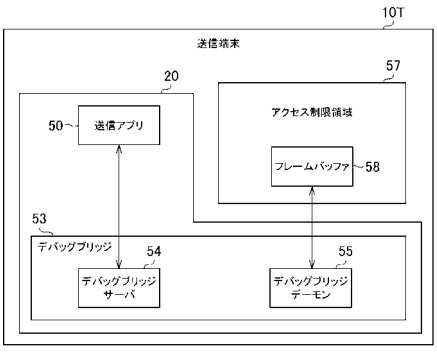
(21)出願番号　特願2015-213111 (P2015-213111)
(22)出願日　平成27年10月29日 (2015.10.29)

(71)出願人　504258527
国立大学法人　鹿児島大学
鹿児島県鹿児島市郡元一丁目２１番２４号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　大塚　作一
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　中山　翼
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内
(72)発明者　小野　智司
鹿児島県鹿児島市郡元一丁目２１番２４号
国立大学法人　鹿児島大学内

最終頁に続く

(54)【発明の名称】情報配信装置、情報配信方法、情報配信プログラム、情報共有認証装置、情報共有認証方法、情報共有認証プログラム、及び情報共有システム

(57)【要約】
【課題】複数端末間で画面共有を行う場合に、複数の各端末に専用デバイスを接続しておく必要がなく、端末操作権限の問題をも回避しつつ、各端末間の画面共有を可能にする。
【解決手段】アクセス制限領域５７のフレームバッファ５８と、そのバッファ５８へのアクセスが可能なデバッグブリッジデーモン機能５５と、受信端末に情報を配信する送信アプリ５０と、送信アプリ５０とデバッグブリッジデーモン機能５５の間を中継するデバッグブリッジサーバ機能５４とを有する。送信アプリ５０はバッファ５８の画面情報をサーバ機能５４に要求し、サーバ機能５４はデバッグブリッジデーモン機能５５にバッファ５８へのアクセスを要求し、デバッグブリッジデーモン機能５５はバッファ５８から画面情報を取得してサーバ機能５４へ転送し、サーバ機能５４は更に送信アプリ５０へ転送する。送信アプリ５０は画面情報を受信端末へ配信する。
【選択図】図１０



【特許請求の範囲】
【請求項１】
特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段と、
前記アクセス制限領域の記憶手段に対するアクセスが可能なアクセス手段と、
一以上の情報端末に対して情報を配信するための送信手段と、
前記送信手段と前記アクセス手段との間を中継する中継手段とを有し、
前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、
前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、
前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、
前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、
前記送信手段は、前記中継手段から転送されてきた情報を、前記一以上の情報端末に対して配信することを特徴とする情報配信装置。
【請求項２】
前記アクセス手段は、情報配信装置のオペレーティングシステムに付属して用意されているデバッグブリッジデーモン機能であり、
前記中継手段は、情報配信装置のオペレーティングシステムに付属して用意されているデバッグブリッジサーバ機能であり、
前記送信手段は、情報配信装置のオペレーティングシステムに対する外部アプリケーションであることを特徴とする請求項１に記載の情報配信装置。
【請求項３】
前記アクセス制限領域の前記記憶手段は、表示画面の情報を保持するフレームバッファであり、
前記送信手段は、前記フレームバッファに記憶されている表示画面の情報の取得を前記中継手段に要求し、
前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記フレームバッファへのアクセスを要求し、
前記アクセス手段は、前記中継手段からの要求に応じて、前記フレームバッファにアクセスして、前記フレームバッファに記憶されている表示画面の情報を取得して前記中継手段へ転送し、
前記送信手段は、前記中継手段から転送されてきた前記表示画面の情報を、前記一以上の情報端末に対して配信することを特徴とする請求項１又は２に記載の情報配信装置。
【請求項４】
所定の情報共有認証装置を接続可能な接続手段を有し、
前記送信手段は、
前記接続手段に前記情報共有認証装置が接続されたとき、前記一以上の情報端末との間で通信を行うための自己の識別情報を前記情報共有認証装置に対して送信し、
前記情報共有認証装置を通じて前記自己の識別情報が前記一以上の情報端末に送信された後に、前記一以上の情報端末から送られてくる各情報端末の識別情報を受信し、
前記情報を配信する際には、前記各情報端末の識別情報に対応した各情報端末へ前記情報を配信することを特徴とする請求項１～３のいずれか１項に記載の情報配信装置。
【請求項５】
前記中継手段と前記アクセス手段との間はデフォルトの状態では所定の通信方式による通信ができない状態に設定されており、
前記中継手段と前記アクセス手段は、前記接続手段に前記情報共有認証装置が接続されたとき、前記情報共有認証装置からの初期設定処理により前記所定の通信方式による通信が可能な状態に設定されることを特徴とする請求項４に記載の情報配信装置。
【請求項６】

一以上の情報端末に対して情報を配信するための送信手段が、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段に記憶されている情報の取得を中継手段に要求するステップと、
送信手段とアクセス手段との間を中継するための前記中継手段が、前記送信手段からの要求に応じて、アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求するステップと、
前記アクセス制限領域の記憶手段に対するアクセスが可能となされている前記アクセス手段が、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送するステップと、
前記中継手段が、前記アクセス手段から転送された前記情報を前記送信手段へ転送するステップと、
前記送信手段が、前記中継手段から転送されてきた情報を、前記一以上の情報端末に対して配信するステップと
を含むことを特徴とする情報配信方法。
【請求項７】
コンピュータを、
特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段に対するアクセスが可能なアクセス手段と、
一以上の情報端末に対して情報を配信するための送信手段と、
前記送信手段と前記アクセス手段との間を中継する中継手段として機能させ、
前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、
前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、
前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、
前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、
前記送信手段は、前記中継手段から転送されてきた情報を、前記一以上の情報端末に対して配信することを特徴とする情報配信プログラム。
【請求項８】
複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証装置であって、
前記情報端末と接続可能な接続手段と、
前記複数の情報端末のうち、情報を配信する側となる送信端末が前記接続手段に接続されたとき、当該送信端末に対して、情報配信のための所定の初期化設定を行う初期化設定手段と、
前記接続手段に接続されている前記送信端末から、当該送信端末の識別情報を取得する取得手段と、
前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段と
を有することを特徴とする情報共有認証装置。
【請求項９】
前記初期化設定手段は、前記送信端末に対する前記初期化設定として、前記配信する情報を前記送信端末の中で取得するための通信経路の通信方式を所定の通信方式に設定することを特徴とする請求項８に記載の情報共有認証装置。
【請求項１０】
前記初期化設定手段は、前記情報共有が行われるグループが形成される際に、前記複数の情報端末のうち、情報配信のためのアプリケーションが起動された情報端末が前記接続手段に接続されたとき、当該情報端末を前記送信端末として前記初期化設定を行い、

前記識別情報送信手段は、前記送信端末が前記接続手段から外された後に、前記情報配信のためのアプリケーションが起動されていない情報端末が前記接続手段に接続されたとき、当該情報端末を前記受信端末として、当該受信端末へ前記送信端末の識別情報を送信することを特徴とする請求項８又は９に記載の情報共有認証装置。

【請求項１１】

複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証方法であって、

前記複数の情報端末のうちで情報を配信する側となる送信端末が接続手段に接続されたとき、初期化設定手段が、当該送信端末に対して、情報配信のための所定の初期化設定を行うステップと、

取得手段が、前記接続手段に接続されている前記送信端末から、当該送信端末の識別情報を取得するステップと、

前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、識別情報送信手段が、前記送信端末の識別情報を前記受信端末へ送信するステップと

を含むことを特徴とする情報共有認証方法。

【請求項１２】

コンピュータを、

情報共有が行われるグループを形成する複数の情報端末のうち、情報を配信する側となる送信端末が接続手段に接続されたとき、当該送信端末に対して、情報配信のための所定の初期化設定を行う初期化設定手段と、

前記接続手段に接続されている前記送信端末から、当該送信端末の識別情報を取得する取得手段と、

前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段と

して機能させることを特徴とする情報共有認証プログラム。

【請求項１３】

複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証装置と、

前記複数の情報端末のうち情報を配信する側となる送信端末と、

前記複数の情報端末のうち前記送信端末から配信される情報を受信する側となる受信端末とを有する情報共有システムであって、

前記情報共有認証装置は、前記情報端末と接続可能な接続手段と、前記送信端末が前記接続手段に接続されたとき、当該送信端末に対して情報配信のための所定の初期化設定を行う初期化設定手段と、前記接続手段に接続されている前記送信端末から当該送信端末の識別情報を取得する取得手段と、前記受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段とを有し、

前記送信端末は、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段と、前記アクセス制限領域の記憶手段に対するアクセスが可能なアクセス手段と、前記受信端末に対して情報を配信するための送信手段と、前記送信手段と前記アクセス手段との間を中継する中継手段とを有し、前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスして、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、前記送信手段は、前記中継手段から転送されてきた情報を、前記受信端末に対して配信し、

前記受信端末は、前記情報共有認証装置から受信した前記送信端末の識別情報に基づい

て、自己の識別情報を前記送信端末へ送信した後、前記送信端末から配信された情報を受信する
ことを特徴とする情報共有システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報端末間で画面情報等を共有する際の情報配信装置、情報配信方法、情報配信プログラム、情報共有認証装置、情報共有認証方法、情報共有認証プログラム、及び情報共有システムに関するものである。
【背景技術】
【０００２】
近年は、いわゆるスマートフォンやタブレット端末等の情報端末が広く普及しており、例えば複数人が同時に、端末内の資料を画面上で閲覧したり、端末のアプリケーションの紹介や発表等を行ったりするような状況も多くなりつつある。ただし、複数人が同時に一台の情報端末の画面を見ることは難しく、また操作性も損なわれる。
【０００３】
一方、複数の端末間で画面を共有する技術として、特許文献１には、画面共有を行う画面共有端末と通信端末との間で、通話網を介した通話の受発信を初めとする認証によって端末を相互に簡便に特定し、更に、受信した画面データを通信端末に転送させることで、通信端末と通信可能に接続された電子機器を利用した画面共有を可能とする技術が開示されている。
【０００４】
また、特許文献２には、画面上に書き込まれる描画オブジェクトを共有し合う１以上の画面共有端末を有し、それら画面共有端末は、共有される描画オブジェクトを記述する情報と、その作成主体を識別する主体識別情報とを保存する保存手段と、上記画面に対する入力操作に応答して、事前登録された操作イベントを検出するイベント検出手段と、上記操作イベントに対応する描画オブジェクトの主体識別情報に応じた他の画面共有端末に対し、操作内容を含むメッセージを発行する発行手段と、他の画面共有端末からメッセージを受信して、事前指定された表示条件にて、操作内容を表す画面表示を画面上に行う画像変換手段を有することにより、複数の端末間で表示画面を共有して手書きなどにより書き込みを行いながら、遠隔会議等を行う技術が開示されている。
【０００５】
また、特許文献３には、画面共有サーバが、表示元端末から配信された画面データをネットワーク経由で受信し、その画面データをネットワーク経由で１台以上のクライアント端末に配信する画面データ中継手段を備えるように構成し、これにより、表示元端末が、処理性能の低い組込み機器である場合でも、多くのクライアント端末と効率的に画面を共有することを可能にする技術が開示されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１４－２１５７７８号公報
【特許文献２】特開２０１３－６５１２５号公報
【特許文献３】特開２０１１－１００２７０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ところで、ＯＳ（Operating System）にＡＮＤＲＯＩＤ（登録商標）を使用したスマートフォンやタブレット端末等の情報端末において、例えばいわゆる画面ミラーリングのような画面共有を行う場合の専用デバイスとしてはＣＨＲＯＭＥＣＡＳＴ（国際登録商標）が知られている。この専用デバイスを接続している情報端末間では画面ミラーリングが可

能となるが、例えば複数の情報端末間で画面ミラーリングを行うような場合には、それら複数の情報端末に各々接続する複数の専用デバイスが必要になってしまう。

【０００８】

また、このＯＳを使用した情報端末において、例えば画面共有を行うためには端末のスクリーンショットを取得する必要があり、スクリーンショットを取得するためにはフレームバッファにアクセスしなければならないが、フレームバッファにアクセスするには、ｒｏｏｔ権限を取得する必要がある。しかしながら、ｒｏｏｔ権限つまり端末操作権限を端末ユーザ等に取得させることは、故障や安全上のリスクを考えると好ましくない。

【０００９】

本発明はこのような問題点に鑑みてなされたものであり、複数端末間で画面共有を行う場合に、複数の各端末にそれぞれ専用デバイスを接続しておく必要がなく、また、端末操作権限の問題をも回避しつつ、各端末間の画面共有を可能にする情報配信装置、情報配信方法、情報配信プログラム、情報共有認証装置、情報共有認証方法、情報共有認証プログラム、及び情報共有システ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】

【００１０】

本発明の情報配信装置は、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段と、前記アクセス制限領域の記憶手段に対するアクセスが可能なアクセス手段と、一以上の情報端末に対して情報を配信するための送信手段と、前記送信手段と前記アクセス手段との間を中継する中継手段とを有し、前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、前記送信手段は、前記中継手段から転送されてきた情報を、前記一以上の情報端末に対して配信することを特徴とする。

【００１１】

また、本発明の情報配信方法は、一以上の情報端末に対して情報を配信するための送信手段が、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段に記憶されている情報の取得を中継手段に要求するステップと、送信手段とアクセス手段との間を中継するための中継手段が、前記送信手段からの要求に応じて、アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求するステップと、前記アクセス制限領域の記憶手段に対するアクセスが可能となされているアクセス手段が、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送するステップと、前記中継手段が、前記アクセス手段から転送された前記情報を前記送信手段へ転送するステップと、前記送信手段が、前記中継手段から転送されてきた情報を、前記一以上の情報端末に対して配信するステップとを含むことを特徴とする。

【００１２】

また、本発明の情報配信プログラムは、コンピュータを、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段に対するアクセスが可能なアクセス手段と、一以上の情報端末に対して情報を配信するための送信手段と、前記送信手段と前記アクセス手段との間を中継する中継手段として機能させ、前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスし、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、前記送信手段は、前記中継手段から転送されてきた情報を、前記一以上の情報

端末に対して配信することを特徴とする。

【００１３】

また、本発明の情報共有認証装置は、複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証装置であって、前記情報端末と接続可能な接続手段と、前記複数の情報端末のうち、情報を配信する側となる送信端末が前記接続手段に接続されたとき、当該送信端末に対して、情報配信のための所定の初期化設定を行う初期化設定手段と、前記接続手段に接続されていて前記送信端末から、当該送信端末の識別情報を取得する取得手段と、前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段とを有することを特徴とする。

【００１４】

また、本発明の情報共有認証方法は、複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証方法であって、前記複数の情報端末のうちで情報を配信する側となる送信端末が接続手段に接続されたとき、初期化設定手段が、当該送信端末に対して、情報配信のための所定の初期化設定を行うステップと、取得手段が、前記接続手段に接続されていて前記送信端末から、当該送信端末の識別情報を取得するステップと、前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、識別情報送信手段が、前記送信端末の識別情報を前記受信端末へ送信するステップとを含むことを特徴とする。

【００１５】

また、本発明の情報共有認証プログラムは、コンピュータを、情報共有が行われるグループを形成する複数の情報端末のうち、情報を配信する側となる送信端末が接続手段に接続されたとき、当該送信端末に対して、情報配信のための所定の初期化設定を行う初期化設定手段と、前記接続手段に接続されていて前記送信端末から、当該送信端末の識別情報を取得する取得手段と、前記複数の情報端末のうち、前記送信端末から配信される情報を受信する側となる受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段として機能させることを特徴とする。

【００１６】

また、本発明の情報共有システムは、複数の情報端末の間で情報共有が行われる際に、前記情報共有が行われるグループを形成する各情報端末を認証する情報共有認証装置と、前記複数の情報端末のうち情報を配信する側となる送信端末と、前記複数の情報端末のうち前記送信端末から配信される情報を受信する側となる受信端末とを有する情報共有システムである。そして、前記情報共有認証装置は、前記情報端末と接続可能な接続手段と、前記送信端末が前記接続手段に接続されたとき、当該送信端末に対して情報配信のための所定の初期化設定を行う初期化設定手段と、前記接続手段に接続されていて前記送信端末から当該送信端末の識別情報を取得する取得手段と、前記受信端末が前記接続手段に接続されたとき、前記送信端末の識別情報を前記受信端末へ送信する識別情報送信手段とを有することを特徴とする。前記送信端末は、特別な権限の無いアクセスを制限するアクセス制限領域となっている記憶手段と、前記アクセス制限領域の記憶手段に対するアクセスが可能なアクセス手段と、前記受信端末に対して情報を配信するための送信手段と、前記送信手段と前記アクセス手段との間を中継する中継手段とを有し、前記送信手段は、前記記憶手段に記憶されている情報の取得を前記中継手段に要求し、前記中継手段は、前記送信手段からの要求に応じて、前記アクセス手段に対して前記アクセス制限領域の記憶手段へのアクセスを要求し、前記アクセス手段は、前記中継手段からの要求に応じて、前記アクセス制限領域の記憶手段にアクセスして、前記記憶手段に記憶されている情報を取得して前記中継手段へ転送し、前記中継手段は、前記アクセス手段から転送された前記情報を前記送信手段へ転送し、前記送信手段は、前記中継手段から転送されてきた情報を、前記受信端末に対して配信することを特徴とする。前記受信端末は、前記情報共有認証装置から

受信した前記送信端末の識別情報に基づいて、自己の識別情報を前記送信端末へ送信し、前記送信端末から配信された情報を受信することを特徴とする。

【発明の効果】

【００１７】

本発明によれば、複数端末間で画面共有を行う場合に、複数の各端末にそれぞれ専用デバイスを接続しておく必要がなく、また、端末操作権限の問題をも回避しつつ、各端末間の画面共有が可能となる。

【図面の簡単な説明】

【００１８】

【図１】実施形態の複数の情報端末と認証装置により画面共有のグループが形成される情報共有システムの概略構成例を示す図である。

【図２】情報端末の内部のハードウェア構成例を示す図である。

【図３】認証装置の内部のハードウェア構成例を示す図である。

【図４】認証装置のＣＰＵがプログラムを実行することにより実現される機能のブロック図である。

【図５】送信端末のＣＰＵがプログラムを実行することにより実現される機能のブロック図である。

【図６】受信端末のＣＰＵがプログラムを実行することにより実現される機能のブロック図である。

【図７】本実施形態の情報共有システムにおいて画面共有のためのグループが形成される際の認証装置と送信端末と受信端末のフローチャートである。

【図８】情報端末が送信端末に設定されて表示画面の情報を受信端末へ配信することになるまでの画面遷移例を示す図である。

【図９】情報端末が受信端末に設定されて送信端末から配信されてきた画面の情報を表示するまでの画面遷移例を示す図である。

【図１０】送信端末の送信アプリとデバッグブリッジ機能とアクセス制限領域の関係説明に用いる図である。

【図１１】デバッグブリッジサーバ機能の起動後、そのデバッグブリッジサーバ機能における、送信アプリからのキャプチャ画像要求受信に応じたキャプチャ画像の取得と転送の詳細なフローチャートである。

【図１２】送信端末におけるサーバプログラムの起動とキャプチャ画像の転送、送信端末から受信端末へのキャプチャ画像の配信の詳細なフローチャートである。

【発明を実施するための形態】

【００１９】

＜実施形態の情報共有システムによる情報共有の概要説明＞

図１には、本発明の一実施形態の情報共有システムの一概略構成例を示す。本実施形態の情報共有システムは、それぞれが送信側と受信側に成り得る複数の情報端末１０（１）～１０（ｎ）と、これらの各情報端末間で画面情報等を共有可能にするためのグループを生成する際に各情報端末１０（１）～１０（ｎ）に順に接続される情報共有認証装置１（以下、認証装置１とする。）とを有している。

【００２０】

図１の各情報端末１０（１）～１０（ｎ）は、一例として、いわゆるスマートフォンやタブレット端末等の携帯情報端末である。認証装置１は、例えば各情報端末１０（１）～１０（ｎ）が各々備えているレセプタクル側接続端子に対して接続可能なプラグ側接続端子を備えている。これら接続端子としては、一例として、いわゆるマイクロＵＳＢ端子を挙げることができる。なお、以下の説明では、各情報端末１０（１）～１０（ｎ）をそれぞれ個々に区別しない場合には情報端末１０と表記し、また、情報を配信する情報配信装置側となった情報端末１０については送信端末１０Ｔと表記し、情報を受信する側となった一以上の情報端末１０については受信端末１０Ｒと表記する。

【００２１】

図２には、本実施形態の情報端末１０の概略的な内部構成例を示す。この図２に示す情報端末１０は、主要な構成として、ＣＰＵ２０、ＲＡＭ２１、ＲＯＭ２２、ネットワークＩ／Ｆ２３、アンテナ２４、ディスプレイコントローラ２５、ディスプレイ２６、タッチパネルコントローラ２７、タッチパネルＩ／Ｆ２８、マイクロＵＳＢＩ／Ｆコントローラ２９、マイクロＵＳＢＩ／Ｆ３０等を有している。これら各構成は、内部バスを介して接続されており、この内部バスを介して互いにデータのやり取りを行うことができるようにされている。

【００２２】

情報端末１０のＲＡＭ２１は、ＣＰＵ２０の演算領域やディスプレイ２６への画面表示のためのフレームバッファ等のようなメモリ領域として利用される。ＣＰＵ２０は、ＲＯＭ２２に格納されたプログラムに従い、ＲＡＭ２１をワークメモリとして用いて、情報端末１０の各部を制御し、また各種情報処理と演算を行う。ＲＯＭ２２は、ＯＳ（オペレーティングシステム）と、ＯＳに対する外部アプリケーションの一つである本実施形態に係る情報配信プログラムである送信プログラム（以下、送信アプリとする。）と、受信プログラム（以下、受信アプリとする。）とを含む各種プログラム、この情報端末の識別情報、画像データや音声データ、その他の各種データなどを格納している。

【００２３】

ネットワークＩ／Ｆ２３は、携帯電話網等の無線通信ネットワーク、Ｗｉ－Ｆｉ通信やBluetooth（登録商標）通信等の近距離無線通信ネットワークのためのインターフェイス部であり、アンテナ２４が接続されている。アンテナ２４は、携帯電話網等の無線通信用と近距離無線通信用の両方のアンテナを有している。

【００２４】

ディスプレイ２６は、ＣＰＵ２０による制御の下で、ディスプレイコントローラ２５により生成されるＧＵＩ（Graphical User Interface）用の表示画像などを表示する。この場合、ＣＰＵ２０は、プログラムにしたがってＧＵＩ用の表示画像をディスプレイコントローラ２５に生成させ、そのＧＵＩ用の表示画像を一旦フレームバッファに記憶させる。その後、フレームバッファに記憶された表示画像が読み出されてディスプレイ２６に送られることにより、ディスプレイ２６にはＧＵＩの画面表示がなされる。

【００２５】

タッチパネルＩ／Ｆ２８は、いわゆるタッチパネルである。タッチパネルコントローラ２７は、ユーザによるタッチパネルＩ／Ｆ２８へのタッチ操作に応じた操作信号を生成してＣＰＵ２０へ送る。マイクロＵＳＢＩ／Ｆ３０は、前述したマイクロＵＳＢ接続端子である。マイクロＵＳＢＩ／Ｆコントローラ２９は、ＣＰＵ２０による制御の下で、マイクロＵＳＢＩ／Ｆ３０を介して信号の送受信を行う。

【００２６】

図３には、本実施形態の認証装置１の概略的な内部構成例を示す。この図３に示す認証装置は、主要な構成として、ＣＰＵ４０、ＲＡＭ４１、ＲＯＭ４２、ＵＳＢＩ／Ｆコントローラ４３、ＵＳＢＩ／Ｆ４４、マイクロＵＳＢＩ／Ｆコントローラ４５、マイクロＵＳＢＩ／Ｆ４６、ライトニング（Ｌｉｇｈｔｎｉｎｇ：登録商標）Ｉ／Ｆコントローラ４７、ライトニングＩ／Ｆ４８等を有している。これら各構成は、内部バスを介して接続されており、この内部バスを介して互いにデータのやり取りを行うことができるようにされている。

【００２７】

認証装置１のＲＡＭ４１は、ＣＰＵ４０の演算領域や情報端末の識別情報等を記憶するためのメモリ領域などに利用される。ＣＰＵ４０は、ＲＯＭ４２に格納された情報共有認証プログラムに従い、ＲＡＭ４１をワークメモリとして用いて、認証装置１の各部を制御し、また各種情報処理と演算を行う。ＲＯＭ４２は、情報端末との間の通信制御プログラムを含む各種プログラム、この認証装置１の識別情報、その他の各種データなどを格納している。

【００２８】

マイクロＵＳＢＩ／Ｆ４６は、前述したマイクロＵＳＢ接続端子である。マイクロＵＳＢＩ／Ｆコントローラ４５は、ＣＰＵ４０による制御の下で、マイクロＵＳＢＩ／Ｆ４６を介して信号の送受信を行う。また、認証装置１は、様々なタイプの情報端末との接続を考慮して、いわゆるＵＳＢ端子とライトニング端子も備えている。ＵＳＢＩ／Ｆ４４は、ＵＳＢ接続端子であり、ＵＳＢＩ／Ｆコントローラ４３は、ＣＰＵ４０による制御の下で、ＵＳＢＩ／Ｆ４４を介して信号の送受信を行う。ライトニングＩ／Ｆ４８は、ライトニング接続端子であり、ライトニングＩ／Ｆコントローラ４７は、ＣＰＵ４０による制御の下で、ライトニングＩ／Ｆ４８を介して信号の送受信を行う。

【００２９】

以下、図１に示した各情報端末１０（１）～１０（ｎ）のうち、例えば情報端末１０（１）が送信端末１０Ｔとなり、残りの情報端末１０（２）～１０（ｎ）が受信端末１０Ｒとなって、それら各情報端末１０（１）～１０（ｎ）の間で画面情報等の共有を可能にするグループが生成される例を挙げて説明する。

【００３０】

図４には、本実施形態の情報共有システムにおいて、画面情報等の共有を行う送信端末１０Ｔと受信端末１０Ｒのグループを生成する際に、認証装置１のＣＰＵ４０がＲＯＭ４２の情報共有認証プログラムを実行することにより実現される機能をブロックとして示している。また、図５には、画面情報等の共有において送信端末１０Ｔに設定された情報端末のＲＯＭ２２のＯＳと送信アプリ５０をＣＰＵ２０が実行することにより実現される機能ブロックを示し、図６には、画面情報等の共有において受信端末１０Ｒに設定される情報端末のＲＯＭ２２のＯＳと受信アプリ６０をＣＰＵ２０が実行することにより実現される機能ブロックを示している。なお、図５に示した送信端末１０Ｔの機能ブロックのうち、デバッグブリッジ機能５３の詳細については、これら図４～図５と以下の図７～図９の説明が終わった後に述べる。

【００３１】

また、図７には、本実施形態の情報共有システムにおいて、図１の情報端末１０（１）が送信端末１０Ｔに設定され、また、図１の情報端末１０（２）～１０（ｎ）が受信端末１０Ｒに設定される際の、認証装置１と送信端末１０Ｔ（情報端末１０（１））と受信端末１０Ｒ（情報端末１０（２）～１０（ｎ））のフローチャートを示す。なお、図７に示すフローチャートにおいて、認証装置１の処理は、図４に示したＣＰＵ４０において機能ブロックとして実現される認証部７１と端末初期化設定部７２が実行し、送信端末１０Ｔの処理は、図５に示したＣＰＵ２０において機能ブロックとして実現される認証部５１が実行し、受信端末１０Ｒの処理は、図６に示したＣＰＵ２０において機能ブロックとして実現される認証部６３が実行する。

【００３２】

また、図８には、図１の情報端末１０（１）が送信端末１０Ｔに設定される際の当該送信端末１０Ｔにおける画面遷移例と、送信端末１０Ｔが表示画面のデータを受信端末１０Ｒへ配信する際の画面遷移例を示している。図９には、図１の情報端末１０（２）～１０（ｎ）が受信端末１０Ｒに設定される際の当該受信端末１０Ｒにおける画面遷移例と、受信端末１０Ｒが送信端末１０Ｔから配信されてきた画面情報を受信して画面上に表示する際の画面遷移例を示している。

【００３３】

なお、前述した送信アプリ５０、受信アプリ６０、各認証部５１，６３，７１、端末初期化設定部７２、表示部６２、デバッグブリッジ機能５３の各部は、実際にはＣＰＵ２０がプログラムを実行することにより実現されるが、それら各部のうち何れがどの処理を行っているのかを明確にするため、以下、必要に応じて、それら各部を主体として説明を行う。

【００３４】

先ず、図１に示した各情報端末１０（１）～１０（ｎ）のうち情報端末１０（１）に対し、例えばタッチパネルを介したユーザ操作により、送信アプリの起動指示操作の入力が

なされたとする。このように送信アプリの起動指示操作が入力されると、情報端末１０（１）のＣＰＵ２０は、図７のステップＳ１の処理として、送信アプリ５０を起動させる。送信アプリ５０が起動すると、情報端末１０（１）のＣＰＵ２０は、例えば図８（ａ）に示すように、ディスプレイ２６の画面上に認証装置の接続をユーザに要求するメッセージを表示させる。なお、このときの情報端末１０（１）のＣＰＵ２０は、ディスプレイ２６の画面上に、認証装置の設定終了をユーザがタッチ操作で入力する際に使用される仮想ボタン（以下、認証装置設定終了ボタン１２とする。）も表示させる。この認証装置設定終了ボタン１２に対するタッチ入力がなされた場合、情報端末１０（１）のＣＰＵ２０は、送信アプリを終了させる。

【００３５】

そして、情報端末１０（１）のレセプタクル側接続端子に対して、認証装置１のプラグ側接続端子が挿入されると、認証装置１の認証部７１は、図７のステップＳ１０の処理として、情報端末１０（１）との間の接続処理を実行する。認証装置１との接続がなされると、情報端末１０（１）の送信アプリ５０は、図７のステップＳ２の処理として、自己の識別情報を認証装置１へ送信する。この識別情報を受け取った認証装置１は、その識別情報をＲＡＭ４１に記憶するとともに、端末初期化設定部７２により情報端末１０（１）を送信端末１０Ｔに設定する。なお、端末初期化設定部７２による送信端末１０Ｔの設定処理には、後述するデバッグブリッジ機能５３の設定処理が含まれている。デバッグブリッジ機能５３の設定処理の詳細については後に説明する。また、識別情報を認証装置１へ送信した後の送信端末１０ＴのＣＰＵ２０は、図８（ｂ）に示すように、ディスプレイ２６の画面上に、認証装置の準備が完了したこと、及び、認証装置の取り外しをユーザに要求するメッセージを表示する。

【００３６】

その後、送信端末１０Ｔから認証装置１が取り外されると、認証装置１は、認証部７１により、図７のステップＳ１１の処理として、接続解除処理を実行する。また、認証装置１が取り外されると、送信端末１０ＴのＣＰＵ２０は、図８（ｃ）に示すように、ディスプレイ２６の画面上に、別の新たな認証装置による接続、又は、認証装置設定終了ボタン１２による終了指示をユーザに要求するメッセージを表示する。なお、別の新たな認証装置による接続がなされた場合、送信端末１０Ｔの送信アプリ５０は、その新たな認証装置に対して、ステップＳ２における識別情報の送信処理を実行することになる。このように、本実施形態においては、送信端末１０Ｔに対して、複数の認証装置の接続を可能にすることにより、画面共有のためのグループを複数設定可能となされている。

【００３７】

また、このときの送信端末１０ＴのＣＰＵ２０は、ディスプレイ２６の画面上に、認証装置設定終了ボタン１２も表示させる。そして、送信端末１０ＴのＣＰＵ２０は、ユーザにより認証装置設定終了ボタン１２へのタッチ入力がなされると、別の認証装置による新たな接続がなされないと判断して、送信端末としての初期設定処理を完了させる。

【００３８】

初期設定処理が完了した送信端末１０ＴのＣＰＵ２０は、図８（ｄ）に示すように、ディスプレイ２６の画面上に、画面の共有を開始することをユーザがタッチ操作で入力する際に使用される仮想ボタン（以下、画面共有開始ボタン１３とする。）と、画面共有を一時的に停止することをユーザがタッチ操作で入力する際に使用される仮想ボタン（以下、共有一時停止ボタン１４とする。）と、送信アプリを終了することをユーザがタッチ操作で入力する際に使用される仮想ボタン（以下、アプリ終了ボタン１５とする。）とを表示させる。

【００３９】

次に、前述のようにして送信端末１０Ｔの初期設定処理が完了した後、図１の残りの情報端末１０（２）～１０（ｎ）のうち例えば情報端末１０（２）のレセプタクル側接続端子に対して、認証装置１のプラグ側接続端子が挿入されると、認証装置１の認証部７１は、図７のステップＳ１２の処理として、情報端末１０（２）との間の接続処理を実行する

。認証装置１との接続がなされると、情報端末１０（２）のＣＰＵ２０は、図７のステップＳ２０の処理として、受信アプリ６０を起動させる。

【００４０】

そして、情報端末１０（２）において受信アプリ６０が起動すると、認証装置１の端末初期化設定部７２は、図７のステップＳ１３の識別情報送信処理として、当該情報端末１０（２）に対して送信端末１０Ｔの識別情報を送信するとともに、この情報端末１０（２）を受信端末１０Ｒに設定する。送信端末１０Ｔの識別情報を受信した情報端末１０（２）のＣＰＵ２０は、図７のステップＳ２１の処理として、自己の識別情報をネットワークＩ／Ｆ２３を介した無線通信により送信端末１０Ｔへ送信させる。これにより、受信端末１０Ｒ（情報端末１０（２））は、後に送信端末１０Ｔから配信されてくる画面情報等を受信可能な受信端末としての初期設定処理が完了する。また、このときの送信端末１０Ｔでは、認証部５１において、その認証情報を送信してきた受信端末１０Ｒを、後に画面情報を配信する際の配信先の受信端末の一つとして認証する。その後、受信端末１０Ｒ（情報端末１０（２））から認証装置１が取り外されると、認証装置１の認証部７１は、図７のステップＳ１４の処理として、接続解除処理を実行する。

【００４１】

以下、情報端末１０（２）の場合と同様にして、図１の残りの各情報端末１０（３）以降の各情報端末に対して、順番に受信端末としての初期設定処理が行われ、最後の情報端末１０（ｎ）のレセプタクル側接続端子に対して、認証装置１のプラグ側接続端子が挿入されると、認証装置１の認証部７１は、図７のステップＳ１５の処理として、情報端末１０（ｎ）との間の接続処理を実行する。認証装置１との接続がなされると、情報端末１０（ｎ）のＣＰＵ２０は、図７のステップＳ３０の処理として、受信アプリ６０を起動させる。

【００４２】

そして、情報端末１０（ｎ）の受信アプリ６０が起動すると、認証装置１の端末初期化設定部７２は、図７のステップＳ１６の識別情報送信処理として、当該情報端末１０（ｎ）に対して送信端末１０Ｔの識別情報を送信するとともに、この情報端末１０（ｎ）を受信端末１０Ｒに設定する。送信端末１０Ｔの識別情報を受信した受信端末１０ＲのＣＰＵ２０は、図７のステップＳ３１の処理として、自己の識別情報をネットワークＩ／Ｆ２３を介した無線通信により送信端末１０Ｔへ送信させる。これにより、受信端末１０Ｒ（情報端末１０（ｎ））は、送信端末１０Ｔから配信されてくる画面情報等を受信可能な受信端末としての初期設定処理が完了する。また、このときの送信端末１０Ｔでは、認証部５１において、その認証情報を送信してきた受信端末１０Ｒ（情報端末１０（ｎ））を、後に画面情報を配信する際の配信先の受信端末の一つとして認証する。その後、受信端末１０Ｒ（情報端末１０（ｎ））から認証装置１が取り外されると、認証装置１の認証部７１は、図７のステップＳ１７の処理として、接続解除処理を実行する。

【００４３】

図９（ａ）は、前述のように情報端末１０（２）～１０（ｎ）がそれぞれ受信端末１０Ｒとして初期設定された場合に、各受信端末１０Ｒのディスプレイ２６の画面上に表示されるメッセージの一例を示している。具体的には、受信端末１０ＲのＣＰＵ２０は、ディスプレイ２６の画面上に、認証装置の準備が完了したこと、及び、認証装置の取り外しをユーザに要求するメッセージを表示させる。そして、受信端末１０ＲのＣＰＵ２０は、認証装置１が取り外されると、図８（ｂ）に示すように、ディスプレイ２６の画面上に、図８（ｄ）の例と同様な画面共有開始ボタン１３と、共有一時停止ボタン１４と、アプリ終了ボタン１５とを表示させる。

【００４４】

そして、送信端末１０Ｔにおいて図８（ｄ）の画面共有開始ボタン１３に対するタッチ入力がユーザ（例えば送信端末１０Ｔのユーザ）によりなされた場合、当該送信端末１０Ｔでは、送信アプリ５０が、後述するデバッグブリッジ機能５３を介してディスプレイ２６の表示画像のキャプチャ画像データを取得し、さらにサーバ部５２が、そのキャプチャ

画像データを、認証部５１において配信先として認証されている各受信端末１０Ｒに対して配信する。

【００４５】

ここで、サーバ部５２は、送信端末１０Ｔの送信アプリ５０と連動したサーバプログラムをＣＰＵ２０が実行することにより実現される。このサーバ部５２におけるサーバプログラムとしては、例えばいわゆるウェブソケットサーバと同様の機能を実現するプログラムを挙げることができる。そして、サーバ部５２は、後述するようにしてデバッグブリッジ機能５３が取得したキャプチャ画像データを、送信アプリ５０の認証部５１が保持している受信端末の識別情報のリストに対応した受信端末１０Ｒへ配信する。なお、サーバ部５２におけるキャプチャ画像データの配信処理の詳細については後述する。

【００４６】

一方、受信端末１０Ｒにおいても同様に図９（ｂ）の画面共有開始ボタン１３に対するタッチ入力がユーザ（各受信端末１０Ｒのユーザ）によりなされた場合、当該受信端末１０Ｒでは、受信アプリ６０が、送信端末１０Ｔから配信されてきたキャプチャ画像データを受信し、また認証部６３が、そのキャプチャ画像データが送信端末１０Ｔから配信されてきたものであるか認証し、そして送信端末１０Ｔからのキャプチャ画像データであると認証されると、表示部６２が、そのキャプチャ画像をディスプレイ２６に表示させる。具体例を挙げると、例えば図８（ｅ）及び図９（ｄ）のような表示画面のスクリーンショットの画像（画面のキャプチャ画像）が、送信端末１０Ｔのサーバ部５２を介して配信されてきた場合、各受信端末１０Ｒでは、図８（ｇ）及び図９（ｃ）に示すように、その配信されてきた画像を、表示部６２によりディスプレイ２６の画面上に表示することになる。

【００４７】

また、送信端末１０ＴのＣＰＵ２０は、画面共有の処理が実行されている際に、図８（ｆ）に示すようにディスプレイ２６の画面上部等に配置されている通知バー１６をユーザがタッチすると、ディスプレイ２６の画面を図８（ｄ）の画面に遷移させる。そして、送信端末１０ＴのＣＰＵ２０は、図８（ｄ）の画面において、ユーザが例えば共有一時停止ボタン１４をタッチすると送信アプリの実行を一時的に停止させ、また、ユーザが例えばアプリ終了ボタン１５をタッチすると送信アプリ５０を終了させる。

【００４８】

一方、受信端末１０ＲのＣＰＵ２０は、画面共有の処理が実行されている際、ディスプレイ２６の画面下部に、図９（ｃ）に示すように受信アプリ画面（図９（ｂ）の画面）へ戻ることをユーザが指示するための戻るボタン１７が表示させる。この戻るボタン１７がユーザによりタッチされると、受信端末１０ＲのＣＰＵ２０は、ディスプレイ２６の画面表示を、図９（ｂ）の画面に戻す。そして、受信端末１０ＲのＣＰＵ２０は、図９（ｂ）の画面において、ユーザが例えば共有一時停止ボタン１４をタッチすると受信アプリ６０の実行を一時的に停止させ、また、ユーザが例えばアプリ終了ボタン１５をタッチすると受信アプリ６０を終了させる。

【００４９】

前述したように本実施形態の情報共有システムにおいては、認証装置１は、送信アプリ５０が起動された状態の情報端末１０（１）を送信端末１０Ｔに設定すると共に当該送信端末１０Ｔの識別情報を取得し、その後に順番に接続された各情報端末１０（２）～１０（ｎ）に対して受信アプリ６０を起動させると共に送信端末１０Ｔの識別情報を送信してそれら各情報端末１０（２）～１０（ｎ）を受信端末１０Ｒに設定する。また、送信端末１０Ｔの識別情報を認証装置１から受け取った各受信端末１０Ｒは、それぞれ自己の識別情報を送信端末１０Ｔへ送信する。その後、それら送信端末１０Ｔと受信端末１０Ｒにおいて画面共有開始ボタン１３のタッチ操作がなされると、送信端末１０Ｔは、自己の表示画面のデータを各受信端末１０Ｒに配信し、各受信端末１０Ｒはその表示画面の画像をディスプレイ２６の画面上に表示する。本実施形態の情報共有システムは、このようにして画面共有を実現している。

【００５０】

＜デバッグブリッジ機能を用いた画面共有の説明＞
ところで、本実施形態の情報共有システムにおいて前述のような画面共有を実現するためには、送信端末１０Ｔは、表示画面のスクリーンショットつまり表示画面のキャプチャ画像を取得する必要がある。また、表示画面のキャプチャ画像を取得するためには、ＲＡＭ２１のフレームバッファに対するアクセスが必要になる。ただし、本実施形態の送信端末１０ＴのＯＳとして例えばＡＮＤＲＯＩＤ（登録商標）が用いられている場合、フレームバッファにアクセスするためには、ｒｏｏｔ権限を取得しなければならないが、ｒｏｏｔ権限をユーザ等に取得させることは故障や安全上のリスクを考えると好ましくない。
【００５１】
このようなことから、本実施形態において、送信端末１０ＴのＣＰＵ２０は、送信アプリ５０を介して、ＯＳに用意されている以下に説明するデバッグブリッジ機能５３を中継機能として用いることにより、ｒｏｏｔ権限を用いずにフレームバッファから表示画面のデータを取得し、その表示画面のデータを受信端末１０Ｒへ配信させるようにしている。本実施形態の場合、送信端末１０ＴのＣＰＵ２０は、画面共有を実現するための中継機能として、ＡＮＤＲＯＩＤのＯＳに用意されているデバッグブリッジ機能５３、具体的にはＡＤＢ（Android Debug Bridge）と称されている機能を、送信アプリ５０を介して利用する。
【００５２】
図１０には、本実施形態の送信端末１０Ｔが表示画面のキャプチャ画像を取得する場合における、デバッグブリッジ機能５３と、送信アプリ５０と、ｒｏｏｔ権限がなければアクセスが制限される領域（以下、アクセス制限領域５７とする。）との関係を示している。アクセス制限領域５７とフレームバッファ５８は、ＲＡＭ２１の一部のメモリ領域である。
【００５３】
この図１０の例において、デバッグブリッジ機能５３は、デバッグブリッジサーバ機能５４とデバッグブリッジデーモン機能５５を有している。デバッグブリッジデーモン機能５５は、ＯＳに付属してバックグラウンドプロセスとして動作するプログラムによる機能であり、アクセス制限領域５７のフレームバッファ５８に対するアクセスが可能となされている。同様に、デバッグブリッジサーバ機能５４は、ＯＳに付属してバックグラウンドプロセスとして動作するプログラムによる機能であり、デバッグブリッジデーモン機能５５に対する通信が可能となされている。また、デバッグブリッジサーバ機能５４は、ｒｏｏｔ権限を必要とせずに、送信アプリ５０を含む外部のアプリケーションからの通信を受け付け可能となされている。すなわち、デバッグブリッジサーバ機能５４は、送信アプリ５０とデバッグブリッジデーモン機能５５との間の中継手段として動作する。
【００５４】
このため、本実施形態の送信端末１０Ｔにおいて、アクセス制限領域５７のフレームバッファ５８内に保持されている画面キャプチャ画像のデータを取得する場合には、送信アプリ５０はデバッグブリッジサーバ機能５４に対してキャプチャ画像を要求し、デバッグブリッジサーバ機能５４はデバッグブリッジデーモン機能５５に対してキャプチャ画像を要求し、更にデバッグブリッジデーモン機能５５はアクセス制限領域５７のフレームバッファ５８に対するアクセスを実行して、当該フレームバッファ５８からキャプチャ画像データを取得する。そして、デバッグブリッジデーモン機能５５はフレームバッファ５８から取得したキャプチャ画像データをデバッグブリッジサーバ機能５４へ転送し、更に、デバッグブリッジサーバ機能５４は当該キャプチャ画像データを送信アプリ５０へ転送する。このように、本実施形態の送信端末１０Ｔにおいて、送信アプリ５０は、デバッグブリッジ機能５３内のデバッグブリッジサーバ機能５４とデバッグブリッジデーモン機能５５を中継することにより、アクセス制限領域５７のフレームバッファ５８内に保持されているキャプチャ画像データを取得している。
【００５５】
＜デバッグブリッジ機能を介したキャプチャ画像取得の流れ＞

図１１には、デバッグブリッジサーバ機能５４が起動し、その後、送信アプリ５０からのキャプチャ画像要求に応じて、デバッグブリッジ機能５３がフレームバッファ５８からキャプチャ画像のデータを取得して、そのキャプチャ画像データを送信アプリ５０へ転送するまでの、当該デバッグブリッジ機能５３における処理のフローチャートを示す。

【００５６】

送信端末１０ＴのＣＰＵ２０は、図１１のフローチャートのステップＳ７０として、デバッグブリッジ機能５３のデバッグブリッジサーバ機能５４を起動させる。なお、デバッグブリッジ機能５３及びデバッグブリッジサーバ機能５４が既に起動しているような場合には、ステップＳ７０の起動処理は行わなくてもよい。

【００５７】

次に、図１１のステップＳ７１において、送信アプリ５０から接続要求を受信すると、ＣＰＵ２０は、デバッグブリッジサーバ機能５４とデバッグブリッジデーモン機能５５との間は所定の通信方式による通信が可能な状態になっているか否か、より具体的にはＴＣＰ（Transmission Control Protocol）による通信が可能な状態になっているか否かを判定する。そして、ＣＰＵ２０は、ステップＳ７１において、ＴＣＰによる通信が可能な状態になっていると判定した場合には、ステップＳ７４に処理を進める。

【００５８】

一方、ステップＳ７２においてＴＣＰによる通信が可能できない状態であると判定した場合、ＣＰＵ２０は、ステップＳ７３として、デバッグブリッジデーモン機能５５をＴＣＰ通信が可能な状態に設定した後、ステップＳ７４へ処理を進める。なお、デバッグブリッジサーバ機能５４とデバッグブリッジデーモン機能５５との間の通信経路においては、現状ではＴＣＰを用いた通信を行うようになされているが、デフォルトの設定状態ではＴＣＰによる通信ができない状態に設定されている。このため、ステップＳ７３の処理は、デフォルトの設定状態を変更して、ＴＣＰによる通信を可能にするために行われる。このデフォルトの設定状態（ＴＣＰ通信ができない設定状態）からＴＣＰ通信可能な状態への設定変更は、例えば認証装置１が送信端末１０Ｔに接続された際に、認証装置１内に用意されているデバッグブリッジサーバ機能から当該送信端末１０ＴのＣＰＵ２０を介したデバッグブリッジ機能５３への通信により行われる。すなわち、前述した認証装置１の端末初期化設定部７２による初期設定は、このステップＳ７３におけるデフォルトの設定状態からＴＣＰ通信可能な状態への設定変更が含まれている。

【００５９】

その後、送信アプリ５０からキャプチャ画像要求が送信されてくると、デバッグブリッジ機能５３のデバッグブリッジサーバ機能５４は、ステップＳ７４において、そのキャプチャ画像要求を受信する。

【００６０】

ステップＳ７４にて送信アプリ５０から送られてきたキャプチャ画像要求を受信すると、デバッグブリッジサーバ機能５４は、ステップＳ７５において、デバッグブリッジデーモン機能５５に対してキャプチャ画像要求を送信する。

【００６１】

ステップＳ７４にてデバッグブリッジサーバ機能５４から送られてきたキャプチャ画像要求を受信すると、デバッグブリッジデーモン機能５５は、ステップＳ７６において、フレームバッファ５８からキャプチャ画像データを取得する。

【００６２】

そして、デバッグブリッジデーモン機能５５は、ステップＳ７７において、キャプチャ画像データをデバッグブリッジサーバ機能５４へ転送し、次いで、デバッグブリッジサーバ機能５４は、ステップＳ７８において、そのキャプチャ画像データを送信アプリ５０へ転送する。

【００６３】

その後、送信端末１０ＴのＣＰＵ２０は、ステップＳ７９において、送信アプリ５０の終了等による画面共有の処理を終了させるか否か判定し、画面共有の処理を終了させない

場合にはステップＳ７４へ処理を戻し、一方、画面共有の処理を終了させる場合にはステップＳ８０へ処理を進める。

【００６４】

ステップＳ８０においては、送信端末１０ＴのＣＰＵ２０は、例えば端末シャットダウンとなるまで、デバッグブリッジ機能５３におけるＴＣＰ接続可能な状態を維持し、その後は待機状態となる。

【００６５】

＜画面共有時の送信アプリと受信アプリの処理及びサーバプログラムの説明＞

図１２には、例えば表示画面のキャプチャ画像の共有がなされている際の送信アプリ５０（送信端末１０Ｔ）と受信アプリ６０（受信端末１０Ｒ）の処理、及び、前述したサーバ部５２の処理の詳細なフローチャートを示す。

【００６６】

図１２において、送信端末１０ＴのＣＰＵ２０は、前述したように送信アプリ５０が起動されると、ステップＳ４１として、前述のサーバプログラム（サーバ部５２）を起動させる。サーバ部５２が起動すると、送信アプリ５０は、ステップＳ４２として、受信端末１０Ｒの識別情報のリストをサーバ部５２へ渡す。

【００６７】

その後、送信アプリ５０は、ステップＳ５１において、前述したようにしてデバッグブリッジ機能５３を介してキャプチャ画像のデータを取得すると、ステップＳ５２として、そのキャプチャ画像データを圧縮する。なお、デバッグブリッジ機能５３がフレームバッファ５８から取得したキャプチャ画像データは、圧縮されていないＲＡＷ（生）画像データであるため、ステップＳ５２において、送信アプリ５０は、そのＲＡＷ画像データを比較的データサイズの小さなＪＰＥＧ画像データに変換する。そして、送信アプリ５０は、ステップＳ５３において、そのＪＰＥＧ画像データに変換されたキャプチャ画像データを、サーバ部５２へ送信する。

【００６８】

一方、受信端末１０Ｒの受信アプリ６０は、ステップＳ６１としてキャプチャ画像の配信要求を送信端末１０Ｔへ送信する。この受信アプリ６０によるキャプチャ画像の配信要求はサーバ部５２により受け取られ、このときのサーバ部５２は、ステップＳ５４として、キャプチャ画像データを受信端末１０Ｒへ配信させる。

【００６９】

受信端末１０Ｒの受信アプリ６０は、送信端末１０Ｔから配信されてきたキャプチャ画像データを受け取ると、ステップＳ６２として、表示部６２によりＪＰＥＧのキャプチャ画像から表示用の画像を生成して、ディスプレイ２６の画面上に表示させる。

【００７０】

前述したような送信アプリ５０におけるステップＳ５１～Ｓ５３までの処理とサーバ部５２におけるステップＳ５４の処理、及び、受信アプリ６０におけるステップＳ６１，Ｓ６２の処理は、送信アプリ５０が画面共有処理を終了するまで、ループ処理Ｓ４３として繰り返される。

【００７１】

その後、送信アプリ５０は、ユーザからの終了指示等が入力された場合、画面共有処理を終了させるとともに、ステップＳ４４として、サーバ部５２には画面共有終了通知を送る。これにより、サーバ部５２の処理は終了する。また、サーバ部５２の処理が終了する際には、その終了通知が受信端末１０Ｒ側にも送られ、これにより受信アプリ６０も処理を終了する。

【００７２】

以上説明したように、本実施形態の情報共有システムによれば、一つの認証装置１を各情報端末１０（１）～１０（ｎ）に対して順に接続して情報共有のためのグループを形成し、また、共有する情報を配信する送信端末１０Ｔは、特別な端末操作権限を用いなければアクセスできない領域の情報を、中継機能を用いることで、特別な端末操作権限無しに

取得して、受信端末１０Ｒに配信可能となされている。したがって、本実施形態によれば、複数端末間で画面共有を行う場合に、複数の各情報端末にそれぞれ専用デバイスを接続しておく必要がなく、また、端末操作権限（ｒｏｏｔ権限）の問題をも回避しつつ、各端末間の画面共有が可能となる。

【００７３】

＜その他の実施形態＞

前述した図７のフローチャートの例では、情報端末１０（２）のステップＳ２１において、情報端末１０（２）は自己の識別情報を送信端末１０Ｔ（情報端末１０（１））に対してのみ送信したが、例えば接続されている認証装置１に対しても自己の識別情報を送信してもよい。この場合の認証装置１は、その後、別の情報端末（例えばステップＳ１６等で情報端末１０（ｎ））と接続された際に、送信端末１０Ｔ（情報端末１０（１））の識別情報と共に、それ以前の接続でそれぞれ取得した他の情報端末（図７の例では情報端末１０（２）等）の全ての識別情報を送信するようにしてもよい。このように、認証装置１が、それぞれ接続した各情報端末１０の識別情報を取得し、その後に接続された情報端末に対してそれら取得した識別情報を送信した場合、それらの識別情報を受け取った情報端末は、相互にネットワークＩ／Ｆ２３を介した無線通信等による接続が可能となる。これにより、前述の情報端末１０（１）以外の他の情報端末１０（２）～１０（ｎ）の何れかが新たに送信端末１０Ｔとなる場合でも、画面共有を行うグループ内における各情報端末の識別情報の再送信を行う必要がなくなる。

【００７４】

また、本実施形態では、認証装置１の接続を介することで、各情報端末１０（１）～１０（ｎ）の間で情報共有を行うグループが生成されたが、認証装置１の接続を介することなく情報共有のグループが生成される場合も本発明に含まれる。例えば、携帯電話網等のネットワークやインターネット等を介して、各端末の識別情報を暗号化等した上で相互に送受信することで、情報共有のグループを生成してもよい。

【００７５】

また、本実施形態では、情報端末１０は、認証装置１が接続された際に前述したような画面共有のための初期設定がなされるが、例えば電源投入時やユーザ操作による送信アプリ或いは受信アプリの起動時に自動的に画面共有に必要な初期設定がなされ、画面共有を行う相手端末の識別情報のみを、前述のようなネットワーク等を介して取得するようになされていてもよい。

【００７６】

その他、前述の実施形態では、情報端末としてスマートフォンやタブレット端末等の携帯情報端末を例に挙げたが、本発明は、前述した送信アプリ、中継機能、受信アプリ等を有するのであれば、例えば携帯型等のナビゲーション装置や、携帯型ゲーム機、腕時計型端末、ヘッドマウントディスプレイ、その他のウェアラブル端末、パーソナルコンピュータ等の各種情報端末にも適用可能である。

【００７７】

また、本発明は、以下の処理を実行することによっても実現される。すなわち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記録媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。このプログラム及び当該プログラムを記憶したコンピュータ読み取り可能な記録媒体は、本発明に含まれる。

【００７８】

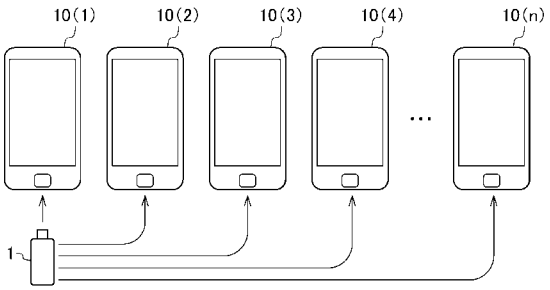
なお、上述した本発明の実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【符号の説明】

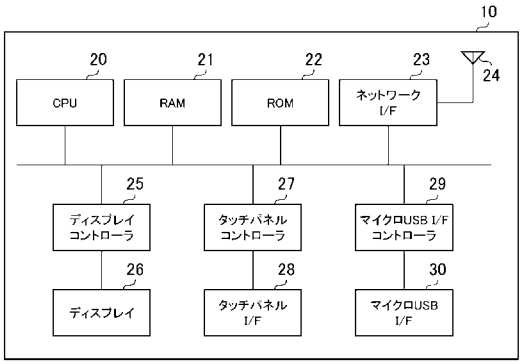
【００７９】

１：認証装置、１０（１）～１０（ｎ）：情報端末、１０Ｔ：送信端末、１０Ｒ：受信端末、２０，４０：ＣＰＵ、２１，４１：ＲＡＭ、２２，４２：ＲＯＭ、２３：ネットワークＩ／Ｆ、２５：ディスプレイコントローラ、２６：ディスプレイ、２７：タッチパネルコントローラ、２８：タッチパネルＩ／Ｆ、２９，４５：マイクロＵＳＢＩ／Ｆコントローラ、３０，４６：マイクロＵＳＢＩ／Ｆ、４３：ＵＳＢＩ／Ｆコントローラ、４４：ＵＳＢＩ／Ｆ、４７：ライトニングＩ／Ｆコントローラ、４８：ライトニングＩ／Ｆ、５０：送信アプリ、５１，６３，７１：認証部、５２：サーバ部、５３：デバッグブリッジ機能、６２：表示部、７２：端末初期化設定部

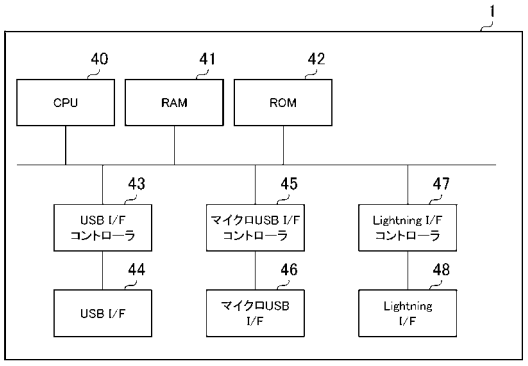
【図１】



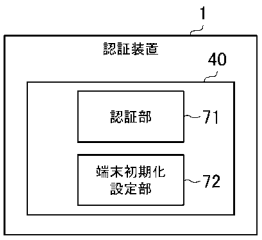
【図２】



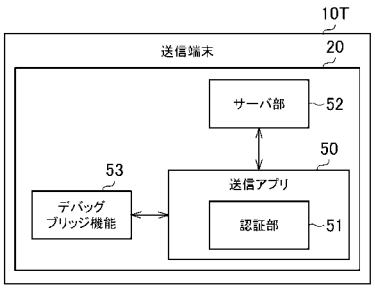
【図３】



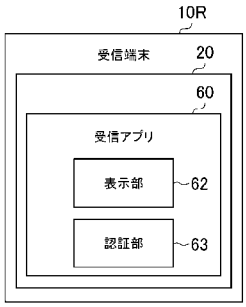
【図４】



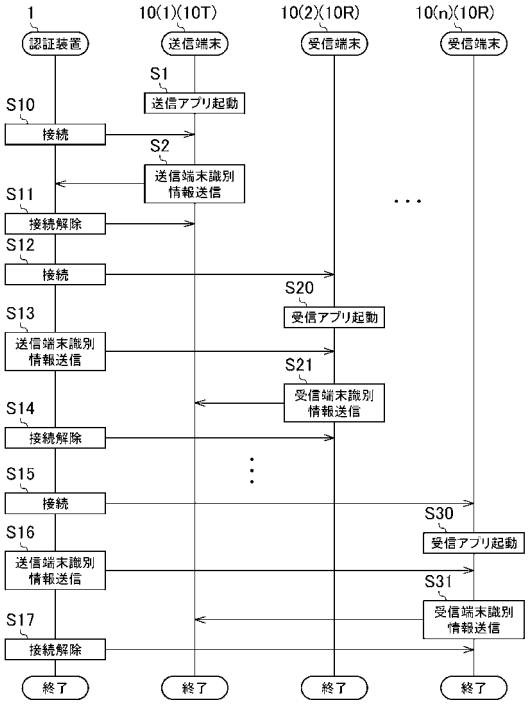
【図５】


10T
送信端末
20
サーバ部
52
50
53
送信アプリ
デバッグ
ブリッジ機能
認証部
51

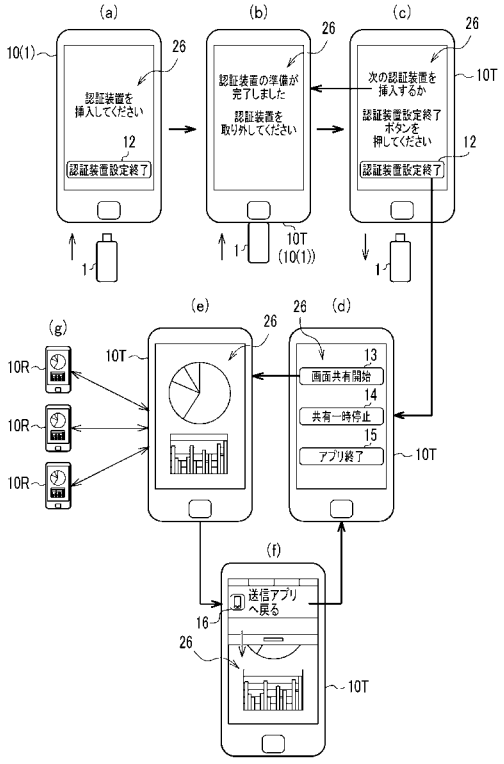
【図６】


10R
受信端末
20
60
受信アプリ
表示部
62
認証部
63

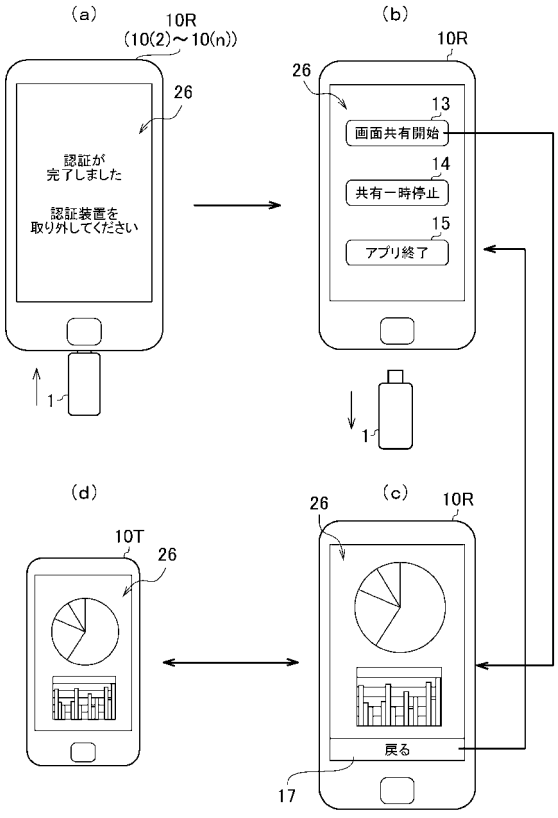
【図７】


1
認証装置
10(1)(10T)
送信端末
10(2)(10R)
受信端末
10(n)(10R)
受信端末
S1
送信アプリ起動
S10
接続
S2
送信端末識別
情報送信
S11
接続解除
S12
接続
S20
受信アプリ起動
S13
送信端末識別
情報送信
S21
受信端末識別
情報送信
S14
接続解除
S15
接続
S30
受信アプリ起動
S16
送信端末識別
情報送信
S31
受信端末識別
情報送信
S17
接続解除
終了
終了
終了
終了

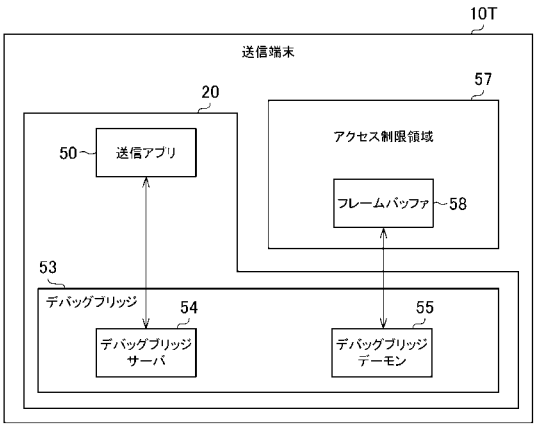
【図８】


(a)
(b)
(c)
10(1)
26
認証装置を
挿入してください
12
認証装置設定終了
認証装置の準備が
完了しました
認証装置を
取り外してください
次の認証装置を
挿入するか
認証装置設定終了
ボタンを
押してください
10T
10T
(10(1))
1
(e)
(d)
(g)
10R
13
画面共有開始
14
共有一時停止
15
アプリ終了
(f)
送信アプリ
へ戻る
16
17

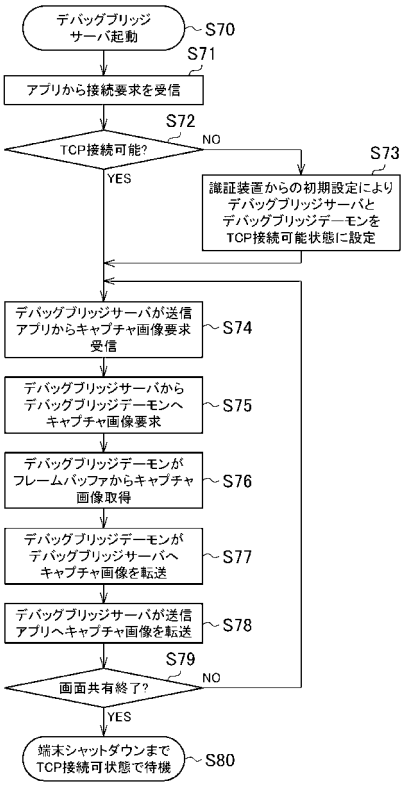
【図９】


(a)
10R
(10(2)～10(n))
26
認証が
完了しました
認証装置を
取り外してください
1
(b)
10R
26
13
画面共有開始
14
共有一時停止
15
アプリ終了
(d)
10T
26
(c)
10R
戻る
17

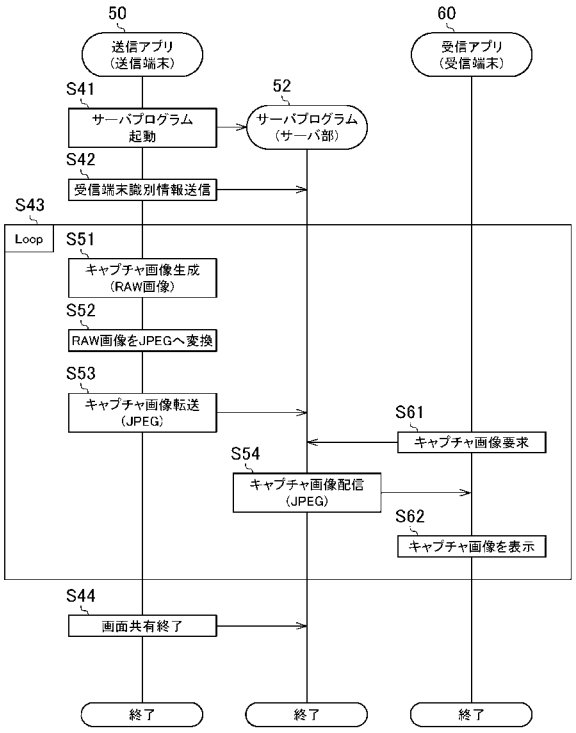
【図１０】


10T
送信端末
20
57
50
送信アプリ
アクセス制限領域
フレームバッファ
58
53
デバッグブリッジ
54
55
デバッグブリッジ
サーバ
デバッグブリッジ
デーモン

【図１１】


デバッグブリッジ
サーバ起動
S70
S71
アプリから接続要求を受信
S72
TCP接続可能?
NO
YES
S73
識証装置からの初期設定により
デバッグブリッジサーバと
デバッグブリッジデーモンを
TCP接続可能状態に設定
デバッグブリッジサーバが送信
アプリからキャプチャ画像要求
受信
S74
デバッグブリッジサーバから
デバッグブリッジデーモンへ
キャプチャ画像要求
S75
デバッグブリッジデーモンが
フレームバッファからキャプチャ
画像取得
S76
デバッグブリッジデーモンが
デバッグブリッジサーバへ
キャプチャ画像を転送
S77
デバッグブリッジサーバが送信
アプリへキャプチャ画像を転送
S78
S79
画面共有終了?
NO
YES
端末シャットダウンまで
TCP接続可状態で待機
S80

【図１２】


50
送信アプリ
(送信端末)
60
受信アプリ
(受信端末)
S41
サーバプログラム
起動
52
サーバプログラム
(サーバ部)
S42
受信端末識別情報送信
S43
Loop
S51
キャプチャ画像生成
(RAW画像)
S52
RAW画像をJPEGへ変換
S53
キャプチャ画像転送
(JPEG)
S61
キャプチャ画像要求
S54
キャプチャ画像配信
(JPEG)
S62
キャプチャ画像を表示
S44
画面共有終了
終了
終了
終了

フロントページの続き

(72)発明者　山之上　卓
鹿児島県鹿児島市郡元一丁目２１番２４号　国立大学法人　鹿児島大学内
(72)発明者　小田　謙太郎
鹿児島県鹿児島市郡元一丁目２１番２４号　国立大学法人　鹿児島大学内
(72)発明者　下園　幸一
鹿児島県鹿児島市郡元一丁目２１番２４号　国立大学法人　鹿児島大学内

Ｆターム(参考) 5B084 AA02 AA16 AA29 AA30 AB06 AB36 BB16 BB17 CA07 DA04
DB08 DC05 DC06 EA47 FA04
5K201 AA09 BA05 BC23 CA04 DB02 EB06 EC06 ED04 EE03 EE04
EF01 EF09