(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4992378号
(P4992378)

(45)発行日　平成24年8月8日(2012.8.8)　(24)登録日　平成24年5月18日(2012.5.18)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 12/22	(2006.01)	H04L	12/22	
G06F 13/00	(2006.01)	H04L	9/00	601E
H04L 12/66	(2006.01)	G06F	13/00	357A
		G06F	13/00	351Z

請求項の数 9　(全 45 頁)　最終頁に続く

(21)出願番号　特願2006-285564 (P2006-285564)
(22)出願日　平成18年10月19日 (2006.10.19)
(65)公開番号　特開2008-104030 (P2008-104030A)
(43)公開日　平成20年5月1日 (2008.5.1)
審査請求日　平成20年11月17日 (2008.11.17)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100092152
弁理士　服部　毅巖
(72)発明者　長田　菜美
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　毛利　隆夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　光延　秀樹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】携帯端末装置、ゲートウェイ装置、プログラム、およびシステム

(57)【特許請求の範囲】

【請求項１】

第１のネットワークを介して接続された通信機器との通信接続の許可を要求する接続要求を、データを暗号化して通信を行う通信経路を介して受信すると、生成した第１の鍵情報を前記通信経路を介して送信し、前記通信機器で生成された第２の鍵情報を前記通信経路を介して受信すると、前記通信経路を介して登録完了通知を送信し、第２のネットワークを介して接続されたサーバ装置で提供される提供データの取得のための取得要求を、前記通信機器から受信した場合に、該取得要求に前記第１の鍵情報と前記第２の鍵情報との組が含まれていれば、該取得要求を前記サーバ装置に転送するゲートウェイ装置と、

前記通信機器との間でデータを暗号化して通信可能な他の携帯端末装置と、

のそれぞれと通信可能な携帯端末装置において、

前記第１のネットワークを介して接続された前記ゲートウェイ装置との間で、データを暗号化して通信を行う通信経路を確保する通信制御手段と、

無線接続された前記他の携帯端末装置から、前記提供データを識別するためのデータ識別情報を含む前記接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に、前記通信経路を介して前記ゲートウェイ装置に対して前記接続要求を転送する接続要求転送手段と、

前記通信経路を介して前記ゲートウェイ装置から前記第１の鍵情報を取得し、前記第１の鍵情報を、前記他の携帯端末装置を介して前記通信機器に転送する第１の鍵転送手段と、

前記他の携帯端末装置を介して前記通信機器から前記第２の鍵情報を取得し、前記通信経路を介して前記第２の鍵情報を前記ゲートウェイ装置に転送する第２の鍵転送手段と、
前記通信経路を介して前記ゲートウェイ装置から前記登録完了通知を取得し、前記記憶装置から前記データ識別情報を取得し、前記第１の鍵情報と前記第２の鍵情報との組を含めた、前記データ識別情報で示される前記提供データの取得要求の前記ゲートウェイ装置への送信を、前記通信機器に指示するデータ取得指示において、前記データ識別情報で前記提供データを指定し、該データ取得指示を前記他の携帯端末装置を介して前記通信機器に送信するデータ取得指示手段と、
を有することを特徴とする携帯端末装置。
【請求項２】
第１のネットワークを介して第１のサーバ装置が接続され、第２のネットワークを介して第２のサーバ装置が接続され、前記第２のサーバ装置で提供される提供データの第１のサーバ装置への転送を指示する、鍵情報を含むデータ転送要求を受信すると、前記第２のサーバ装置から前記提供データを取得し、前記提供データを該鍵情報で暗号化し、暗号化された提供データを前記第１のサーバ装置内に格納するゲートウェイ装置と、
前記第１のネットワークを介して前記第１のサーバ装置が接続された通信機器との間で、データを暗号化して通信可能な他の携帯端末装置と、
のそれぞれと通信可能な携帯端末装置において、
前記第１のネットワークを介して接続された前記ゲートウェイ装置との間で、データを暗号化して通信を行う通信経路を確保する通信制御手段と、
鍵情報を生成する鍵生成手段と、
無線接続された前記他の携帯端末装置から、前記提供データを識別するためのデータ識別情報を含む、前記通信機器による前記提供データの取得のための取得要求を受け取ると、前記鍵生成手段で生成された鍵情報を取得し、前記データ識別情報で示される前記提供データの前記第１のサーバ装置への転送を指示するデータ転送要求に該鍵情報を付加し、前記通信経路を介して該データ転送要求を前記ゲートウェイ装置に対して送信するデータ転送指示手段と、
前記第１のサーバからの前記暗号化された提供データの取得、および前記暗号化された提供データの前記鍵生成手段で生成された鍵情報による復号を前記通信機器に指示するデータ取得指示を、前記他の携帯端末装置を介して前記通信機器に送信するデータ取得指示手段と、
を有することを特徴とする携帯端末装置。
【請求項３】
第１のネットワークを介して接続された通信機器とゲートウェイ装置との通信接続の許可を要求する接続要求を、データを暗号化して通信を行う通信経路を介して前記ゲートウェイ装置に対して転送し、前記ゲートウェイ装置で生成された第１の鍵情報を取得すると、無線接続された他の携帯端末装置を経由して前記第１の鍵情報を前記通信機器に転送し、前記通信機器で生成された第２の鍵情報を前記他の携帯端末装置を経由して取得すると、前記第２の鍵情報を前記ゲートウェイ装置に転送し、前記ゲートウェイ装置から登録完了通知を取得すると、第２のネットワークを介して前記ゲートウェイ装置に接続されたサーバ装置が提供する提供データの取得を前記通信機器に指示するデータ取得指示を、前記他の携帯端末装置を介して前記通信機器に送信する携帯端末装置と、
前記他の携帯端末装置から前記第１の鍵情報を受信すると、前記第２の鍵情報を生成し、前記第２の鍵情報を前記他の携帯端末装置に送信し、前記データ取得指示を受信すると、前記第１の鍵情報と前記第２の鍵情報とを含めた前記提供データの取得要求を前記ゲートウェイ装置に対して送信する前記通信機器と、
のそれぞれと通信可能な前記ゲートウェイ装置において、
前記第１のネットワークを介して接続された前記携帯端末装置との間で、データを暗号化して通信を行う前記通信経路を確保する通信制御手段と、
前記通信経路を介して前記携帯端末装置から前記接続要求を受信すると、前記第１の鍵

情報を生成し、前記第１の鍵情報を鍵情報記憶手段に格納すると共に、前記通信経路を介して前記第１の鍵情報を前記携帯端末装置に送信する第１の鍵発行手段と、
前記通信経路を介して前記携帯端末装置から前記第２の鍵情報を受信すると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記通信経路を介して前記携帯端末装置に対して登録完了通知を送信する第２の鍵取得手段と、
前記通信機器から、前記第１の鍵情報と前記第２の鍵情報との組を含む、前記提供データの前記取得要求を受け取ると、前記取得要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、格納されている場合、前記取得要求を前記サーバ装置に転送する転送手段と、
を有することを特徴とするゲートウェイ装置。
【請求項４】
前記第１の鍵発行手段は、前記接続要求に、前記サーバ装置内のデータを取得する機器の機器ＩＤが含まれている場合、前記機器ＩＤと前記第１の鍵情報とを対応付けて前記鍵情報記憶手段に格納し、
前記転送手段は、前記取得要求から前記通信機器の機器ＩＤを取得し、前記取得要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組が、前記機器ＩＤに対応付けて前記鍵情報記憶手段に格納されているか否かを判断し、格納されていれば前記取得要求を前記サーバ装置に転送することを特徴とする請求項３記載のゲートウェイ装置。
【請求項５】
前記第１の鍵発行手段は、前記第１の鍵情報に有効期限を設定し、有効期限を付加した前記第１の鍵情報を前記鍵情報記憶手段に格納し、
前記第２の鍵取得手段は、有効期限付きの前記第２の鍵情報を取得すると、有効期限を付加した前記第２の鍵情報を前記鍵情報記憶手段に格納し、
前記転送手段は、前記取得要求に含まれる前記第１の鍵情報と前記第２の鍵情報の組と一致する前記第１の鍵情報の有効期限と前記第２の鍵情報の有効期限とが、両方とも過ぎていない場合に限り、前記取得要求を前記サーバ装置に転送する、
ことを特徴とする請求項３または４のいずれかに記載のゲートウェイ装置。
【請求項６】
第１のネットワークを介して接続された通信機器との通信接続の許可を要求する接続要求を、データを暗号化して通信を行う通信経路を介して受信すると、生成した第１の鍵情報を前記通信経路を介して送信し、前記通信機器で生成された第２の鍵情報を前記通信経路を介して受信すると、前記通信経路を介して登録完了通知を送信し、第２のネットワークを介して接続されたサーバ装置で提供される提供データの取得のための取得要求を、前記通信機器から受信した場合に、該取得要求に前記第１の鍵情報と前記第２の鍵情報との組が含まれていれば、該取得要求を前記サーバ装置に転送するゲートウェイ装置と、
前記通信機器との間でデータを暗号化して通信可能な他の携帯端末装置と、
のそれぞれと通信可能なコンピュータに、
前記第１のネットワークを介して接続された前記ゲートウェイ装置との間で、データを暗号化して通信を行う通信経路を確保し、
無線接続された前記他の携帯端末装置から、前記提供データを識別するためのデータ識別情報を含む前記接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に、前記通信経路を介して前記ゲートウェイ装置に対して前記接続要求を転送し、
前記通信経路を介して前記ゲートウェイ装置から前記第１の鍵情報を取得し、前記第１の鍵情報を、前記他の携帯端末装置を介して前記通信機器に転送し、
前記他の携帯端末装置を介して前記通信機器から前記第２の鍵情報を取得し、前記通信経路を介して前記第２の鍵情報を前記ゲートウェイ装置に転送し、
前記通信経路を介して前記ゲートウェイ装置から前記登録完了通知を取得し、前記記憶装置から前記データ識別情報を取得し、前記第１の鍵情報と前記第２の鍵情報との組を含めた、前記データ識別情報で示される前記提供データの取得要求の前記ゲートウェイ装置への送信を、前記通信機器に指示するデータ取得指示において、前記データ識別情報で前

記提供データを指定し、該データ取得指示を前記他の携帯端末装置を介して前記通信機器に送信する、
処理を実行させるプログラム。
【請求項７】
第１のネットワークを介して第１のサーバ装置が接続され、第２のネットワークを介して第２のサーバ装置が接続され、前記第２のサーバ装置で提供される提供データの第１のサーバ装置への転送を指示する、鍵情報を含むデータ転送要求を受信すると、前記第２のサーバ装置から前記提供データを取得し、前記提供データを該鍵情報で暗号化し、暗号化された提供データを前記第１のサーバ装置内に格納するゲートウェイ装置と、
前記第１のネットワークを介して前記第１のサーバ装置が接続された通信機器との間で、データを暗号化して通信可能な他の携帯端末装置と、
のそれぞれと通信可能なコンピュータに、
前記第１のネットワークを介して接続されたゲートウェイ装置との間で、データを暗号化して通信を行う通信経路を確保し、
鍵情報を生成し、
無線接続された前記他の携帯端末装置から、前記提供データを識別するためのデータ識別情報を含む、前記通信機器による前記提供データの取得のための取得要求を受け取ると、生成された前記鍵情報を取得し、前記データ識別情報で示される前記提供データの前記第１のサーバ装置への転送を指示するデータ転送要求に該鍵情報を付加し、前記通信経路を介して該データ転送要求を前記ゲートウェイ装置に対して送信し、
前記第１のサーバからの前記暗号化された提供データの取得、および前記暗号化された提供データの前記鍵生成手段で生成された鍵情報による復号を前記通信機器に指示するデータ取得指示を、前記他の携帯端末装置を介して前記通信機器に送信する、
処理を実行させるプログラム。
【請求項８】
第１のネットワークを介して接続された通信機器とゲートウェイ装置との通信接続の許可を要求する接続要求を、データを暗号化して通信を行う通信経路を介して前記ゲートウェイ装置に対して転送し、前記ゲートウェイ装置で生成された第１の鍵情報を取得すると、無線接続された他の携帯端末装置を経由して前記第１の鍵情報を前記通信機器に転送し、前記通信機器で生成された第２の鍵情報を前記他の携帯端末装置を経由して取得すると、前記第２の鍵情報を前記ゲートウェイ装置に転送し、前記ゲートウェイ装置から登録完了通知を取得すると、第２のネットワークを介して前記ゲートウェイ装置に接続されたサーバ装置が提供する提供データの取得を前記通信機器に指示するデータ取得指示を、前記他の携帯端末装置を介して前記通信機器に送信する携帯端末装置と、
前記他の携帯端末装置から前記第１の鍵情報を受信すると、前記第２の鍵情報を生成し、前記第２の鍵情報を前記他の携帯端末装置に送信し、前記データ取得指示を受信すると、前記第１の鍵情報と前記第２の鍵情報とを含めた前記提供データの取得要求を前記ゲートウェイ装置に対して送信する前記通信機器と、
のそれぞれと通信可能な前記ゲートウェイ装置に、
前記第１のネットワークを介して接続された前記携帯端末装置との間で、データを暗号化して通信を行う通信経路を確保し、
前記通信経路を介して前記携帯端末装置から前記接続要求を受け取ると、前記第１の鍵情報を生成し、前記第１の鍵情報を鍵情報記憶手段に格納すると共に、前記通信経路を介して前記第１の鍵情報を前記携帯端末装置に送信し、
前記通信経路を介して前記携帯端末装置から前記第２の鍵情報を受信すると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記通信経路を介して前記携帯端末装置に対して登録完了通知を送信し、
前記通信機器から、前記第１の鍵情報と前記第２の鍵情報との組を含む、前記提供データの取得要求を受け取ると、前記取得要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、格納されている場合、

前記取得要求を前記サーバ装置に転送する、
処理を実行させるプログラム。
【請求項９】
第１のネットワークを介して接続されたゲートウェイ装置との間で、データを暗号化して通信を行う第１の通信経路を確保し、無線接続された第２の携帯端末装置から、前記ゲートウェイ装置に第２のネットワークを介して接続されたサーバ装置で提供される提供データを識別するためのデータ識別情報を含む、前記ゲートウェイ装置に前記第１のネットワークを介して接続された通信機器との通信接続の許可を前記ゲートウェイ装置に要求する接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に、前記第１の通信経路を介して前記ゲートウェイ装置に対して前記接続要求を転送し、前記第１の通信経路を介して前記ゲートウェイ装置から、前記ゲートウェイ装置で生成された第１の鍵情報を取得し、前記第１の鍵情報を前記第２の携帯端末装置に転送し、前記第２の携帯端末装置から前記通信機器が生成した第２の鍵情報を取得し、前記第１の通信経路を介して前記第２の鍵情報を前記ゲートウェイ装置に転送し、前記第１の通信経路を介して前記ゲートウェイ装置から登録完了通知を取得し、前記記憶装置から前記データ識別情報を取得し、前記第２の携帯端末装置に対して、前記データ識別情報で前記提供データを指定したデータ取得指示を送信する第１の携帯端末装置と、
前記第１の携帯端末装置との間で前記第１の通信経路を確保し、前記第１の通信経路を介して前記第１の携帯端末装置から前記接続要求を受信すると、前記第１の鍵情報を生成し、前記第１の鍵情報を鍵情報記憶手段に格納すると共に、前記第１の通信経路を介して前記第１の鍵情報を前記第１の携帯端末装置に送信し、前記第１の通信経路を介して前記第１の携帯端末装置から前記第２の鍵情報を受信すると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記第１の通信経路を介して前記第１の携帯端末装置に対して登録完了通知を送信し、前記通信機器から、前記第１の鍵情報と前記第２の鍵情報との組を含む、前記提供データの取得要求を受信すると、前記取得要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、格納されている場合、前記取得要求を前記サーバ装置に転送する前記ゲートウェイ装置と、
前記第１のネットワークを介して接続された前記通信機器との間で、データを暗号化して通信を行う第２の通信経路を確保し、前記第１の携帯端末装置に対して前記接続要求を送信し、前記第２の通信経路を介して前記通信機器から前記第２の鍵情報を取得し、前記第２の鍵情報を前記第１の携帯端末装置に送信し、前記第１の携帯端末装置から受信した前記第１の鍵情報を前記第２の通信経路を介して前記通信機器に転送し、前記第２の通信経路を介して前記通信機器から送られた前記第２の鍵情報を、前記第１の携帯端末装置に転送し、前記第１の携帯端末装置から送られた前記データ取得指示を前記第２の通信経路を介して前記通信機器に転送する前記第２の携帯端末装置と、
前記第２の携帯端末装置との間で前記第２の通信経路を確保し、前記第２の携帯端末装置から前記第１の鍵情報を受け取ると、前記第１の鍵情報を記憶装置に格納し、前記第２の鍵情報を生成し、前記第２の通信経路を介して前記第２の鍵情報を前記第２の携帯端末装置に送信し、前記第２の通信経路を介して前記第２の携帯端末装置から前記データ取得指示を受け取ると、前記第１の鍵情報と前記第２の鍵情報とを含む、前記提供データの前記取得要求を、前記第１の携帯端末装置と前記第２の携帯端末装置とを介さずに前記ゲートウェイ装置に対して送信する前記通信機器と、
を有することを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は保護されたネットワークの管理に使用する携帯端末装置、ゲートウェイ装置、遠隔制御プログラム、アクセス制限プログラム、およびデータ転送システムに関し、特に保護されたネットワーク内のデータを外部からの操作で取得するための携帯端末装置、ゲ

ートウェイ装置、プログラム、およびシステムに関する。
【背景技術】
【０００２】
ＩＰ（Internet Protocol）携帯電話のようなＰＨＳ（Personal Handyphone System）と無線ＬＡＮ（Local Area Network）など複数の通信インタフェースを持つ携帯端末装置が発達している。このような携帯端末装置は、インターネットなどを通じて大容量のデータをダウンロードすることが可能である。そこで、ユーザは音楽や動画のような比較的容量の大きなデータを携帯端末装置に記憶させ、移動先で音楽や動画を視聴することが増えている。
【０００３】
ただし、依然として携帯端末装置は個人の扱う全てのデータを保存できるような容量の記憶装置は持っていない。そのため、自宅やオフィスにあるパーソナルコンピュータなどのファイルサーバでデータ全体を管理し、携帯端末装置で持ち歩くのはその一部のみというスタイルが一般的である。
【０００４】
ここで、自宅のファイルサーバに保管しているデータを、外出先で目の前にある装置に転送したい場合がある。このとき、出来るだけ少ない手間でデータ転送を出来ることが望まれている。そのための技術として、二次元バーコードの形式でデータ取得に必要な情報を、機器に入力する技術がある。たとえば、遠隔サーバがアクセス識別子を生成し、そのアクセス識別子を情報デバイスに転送する。情報デバイスはアクセス識別子を二次元バーコードで画面に表示する。表示された二次元バーコードをローカルデバイスに読み取らせると、ローカルデバイスがアクセス識別子に基づいて遠隔サーバに接続し、データ転送を行う。これにより、外出先の機器に自宅に保管しているデータを転送できる（たとえば、特許文献１参照）。
【特許文献１】特開２００５－１７４３１７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、自宅のファイルサーバに対して、外部の任意の装置からのアクセスを無制限に許可したのでは、ファイルサーバが危険にさらされてしまう。そこで、通常は、自宅のファイルサーバはゲートウェイ装置で保護されており、外部からのアクセスは制限される。そのため、特許文献１のように、単に遠隔サーバとのデータの受け渡し方法を規定しただけではデータを取得できない。すなわち、ファイルサーバがゲートウェイ装置で保護されている場合、遠隔操作によってゲートウェイ装置経由でのデータ転送を実行する手段が必要となる。
【０００６】
なお、転送すべきデータのデータ容量が小さければ、データを携帯端末装置に転送した後、そのデータを他の機器に転送することも可能である。例えば、互いに持っている携帯端末装置をゲートウェイとして利用し、それぞれのファイルサーバからのデータ通信を中継する方法が想定できる。この場合、携帯端末装置が、ＶＰＮ（Virtual Private Network）を使うなどして、自分が所属する自宅や会社のネットワークに安全に接続する手段を持っていれば、安全性を考慮したデータ交換が可能である。しかしながら、限られたＣＰＵ能力やバッテリ容量しか持たない携帯端末装置をゲートウェイとして利用すると、機能的、利用時間的に制限が大きかった（消費電力、転送速度の問題）。
【０００７】
代替手段として遠隔地にあるサーバ同士を接続してデータ交換を行う方法も考えられる。ただし、家庭内やオフィスなどのネットワーク（保護ネットワーク）は一般にファイアウォールやゲートウェイ（以下ゲートウェイ装置と表記する)などで通信が制限されており、他のネットワークから自由に接続することができない。
【０００８】

この問題の解決方法の１つに、ゲートウェイ装置のポートマッピング機能を利用するなどして、必要なサービスに自由にアクセス可能にさせる方法がある。しかしこの場合は意図しない機器からのアクセスを区別できず、情報漏洩や悪意のある攻撃などに対して脆弱になってしまう。

【０００９】

本発明はこのような点に鑑みてなされたものであり、外部からの遠隔操作によってゲートウェイ装置で保護されているネットワーク上のデータを外部の機器に容易に転送させることができる携帯端末装置、ゲートウェイ装置、プログラム、および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】

本発明では上記課題を解決するために、図１に示すようなシステムが提供される。本発明に係る携帯端末装置１は、ネットワーク経由で接続された装置を遠隔制御するために、図１に示すような要素を有している。通信制御手段１ａは、ネットワークを介して接続されたゲートウェイ装置２との間で、安全な通信経路を確保する。接続要求転送手段１ｂは、ネットワークを介して接続された携帯端末装置４から、取得すべきデータを識別するためのデータ識別情報を含む接続要求を受け取ると、データ識別情報を記憶装置に格納すると共にゲートウェイ装置２に対して接続要求を転送する。第１の鍵転送手段１ｃは、ゲートウェイ装置２からデータ識別情報に対応するデータにアクセスするための第１の鍵情報を取得し、第１の鍵情報を他の携帯端末装置４に転送する。第２の鍵転送手段１ｄは、携帯端末装置４からデータ識別情報に対応するデータへのアクセス元が生成した第２の鍵情報を取得し、第２の鍵情報をゲートウェイ装置２に転送する。データ取得指示手段１ｅは、ゲートウェイ装置２から第２の鍵情報の登録完了通知を受け取ると、記憶装置からデータ識別情報を取得し、携帯端末装置４に対してデータ識別情報を指定したデータ取得指示を送信する。

【００１１】

また、本発明に係るゲートウェイ装置２は、保護ネットワークと他のネットワークとの間に配置されて、保護ネットワークＮ２への外部からのアクセスを制限するために、図１に示すような要素を有している。通信制御手段２ａは、他のネットワークを介して接続された携帯端末装置１との間で、安全な通信経路を確保する。鍵情報記憶手段２ｂは、保護ネットワークＮ２内のファイルサーバ装置３にアクセスするための鍵情報を記憶する。第１の鍵発行手段２ｃは、携帯端末装置１から接続要求を受け取ると、第１の鍵情報を生成し、第１の鍵情報を鍵情報記憶手段２ｂに格納すると共に、第１の鍵情報を携帯端末装置１に送信する。第２の鍵取得手段２ｄは、携帯端末装置１から、他のネットワークを介して接続された通信機器で発行された第２の鍵情報が送られると、鍵情報記憶手段２ｂに対して、第１の鍵情報に対応付けて第２の鍵情報を格納し、携帯端末装置１に対して登録完了通知を送信する。ファイル要求転送手段２ｅは、通信機器からファイル要求を受け取ると、ファイル要求に含まれる第１の鍵情報と第２の鍵情報との組と一致する第１の鍵情報と第２の鍵情報との組が鍵情報記憶手段２ｂに格納されているか否かを判断し、一致する鍵情報が格納されている場合、ファイル要求をファイルサーバ装置３に転送する。

【００１２】

このような携帯端末装置１とゲートウェイ装置２とによれば、まず、互いの通信制御手段１ａ，２ａにより、安全な通信経路が確保される。その後、携帯端末装置４から携帯端末装置１に接続要求が入力されると、接続要求転送手段１ｂによりゲートウェイ装置２に対して接続要求が転送される。ゲートウェイ装置２では、第１の鍵発行手段２ｃにより第１の鍵情報が生成され、第１の鍵情報が鍵情報記憶手段２ｂに格納されると共に、第１の鍵情報が携帯端末装置１に送信される。送信された第１の鍵情報は、携帯端末装置１の第１の鍵転送手段１ｃにより、携帯端末装置４に転送される。次に、第２の鍵転送手段１ｄにより、携帯端末装置４から第２の鍵情報が取得され、第２の鍵情報がゲートウェイ装置

２に転送される。転送された第２の鍵情報は、第２の鍵取得手段２ｄにより、鍵情報記憶手段２ｂに対して、第１の鍵情報に対応付けて格納される。そして、第２の鍵取得手段２ｄから携帯端末装置１に登録完了通知が送信される。すると、データ取得指示手段１ｅにより、携帯端末装置４に対してデータ識別情報を指定したデータ取得指示が転送される。そして、ゲートウェイ装置２に通信機器からファイル要求が入力されると、ファイル要求転送手段２ｅにより、ファイル要求に含まれる第１の鍵情報と第２の鍵情報との組と一致する第１の鍵情報と第２の鍵情報との組が鍵情報記憶手段２ｂに格納されているか否かが判断され、一致する鍵情報が格納されている場合、ファイル要求がファイルサーバ装置３に転送される。

【発明の効果】

【００１３】

本発明では、保護ネットワークとの他のネットワークとの間に配置されたゲートウェイ装置と携帯端末装置とを安全な通信経路で接続し、ゲートウェイ装置が発行した第１の鍵情報を携帯端末装置経由で他の通信機器に渡し、その通信機器が発行した第２の鍵情報を携帯端末装置経由でゲートウェイ装置に渡すようにした。これにより、ゲートウェイ装置が他の通信機器を認証するための第１の鍵情報と第２の鍵情報との組を安全な経路で受け渡し、実際のデータ転送に広帯域の経路を使うことが可能となる。その結果、携帯端末装置を用いた遠隔操作による大容量のデータ転送が容易となる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施の形態を図面を参照して説明する。

図１は、発明の概要を示す図である。ローカルネットワークＮ１には、携帯端末装置１、４が接続されている。保護ネットワークＮ２には、ゲートウェイ装置２とファイルサーバ装置３とが接続されている。保護ネットワークＮ３には、ゲートウェイ装置５とファイルサーバ装置６とが接続されている。ここで、携帯端末装置１とゲートウェイ装置２との間で安全な通信経路で通信が可能である。また、携帯端末装置４とゲートウェイ装置５との間で安全な通信経路で通信が可能である。

【００１５】

携帯端末装置１は、通信制御手段１ａ、接続要求転送手段１ｂ、第１の鍵転送手段１ｃ、第２の鍵転送手段１ｄ、およびデータ取得指示手段１ｅを有している。

通信制御手段１ａは、ネットワークを介して接続されたゲートウェイ装置２との間で、安全な通信経路を確保する。たとえば、ＶＰＮによって安全な通信経路を確保できる。

【００１６】

接続要求転送手段１ｂは、ネットワークを介して接続された他の携帯端末装置４から、取得すべきデータ（たとえば、ファイルサーバ装置３が提供しているデータ）を識別するためのデータ識別情報（たとえば、ＵＲＬ）を含む接続要求を受け取る。すると、接続要求転送手段１ｂは、データ識別情報を記憶装置に格納すると共にゲートウェイ装置２に対して接続要求を転送する。

【００１７】

第１の鍵転送手段１ｃは、ゲートウェイ装置２からデータ識別情報に対応するデータにアクセスするための第１の鍵情報を取得する。そして、第１の鍵転送手段１ｃは、第１の鍵情報を携帯端末装置４に転送する。

【００１８】

第２の鍵転送手段１ｄは、携帯端末装置４からデータ識別情報に対応するデータへのアクセス元（たとえば、ゲートウェイ装置５）が生成した第２の鍵情報を取得する。そして、第２の鍵転送手段１ｄは、第２の鍵情報をゲートウェイ装置２に転送する。

【００１９】

データ取得指示手段１ｅは、ゲートウェイ装置２から第２の鍵情報の登録完了通知を受け取ると、記憶装置からデータ識別情報を取得する。そして、データ取得指示手段１ｅは、携帯端末装置４に対してデータ識別情報を指定したデータ取得指示を送信する。

【００２０】
ゲートウェイ装置２は、通信制御手段２ａ、鍵情報記憶手段２ｂ、第１の鍵発行手段２ｃ、第２の鍵取得手段２ｄ、およびファイル要求転送手段２ｅを有している。
通信制御手段２ａは、ネットワークを介して接続された携帯端末装置１との間で、安全な通信経路を確保する。
【００２１】
鍵情報記憶手段２ｂは、保護ネットワークＮ２内のファイルサーバ装置３にアクセスするための鍵情報を記憶する。
第１の鍵発行手段２ｃは、携帯端末装置１から接続要求を受け取ると、第１の鍵情報を生成し、第１の鍵情報を鍵情報記憶手段２ｂに格納する。また、第１の鍵発行手段２ｃは、生成した第１の鍵情報を携帯端末装置１に送信する。
【００２２】
第２の鍵取得手段２ｄは、携帯端末装置１から、ネットワークを介して接続された通信機器（たとえば、ゲートウェイ装置５）で発行された第２の鍵情報が送られると、鍵情報記憶手段２ｂに対して、第１の鍵情報に対応付けて第２の鍵情報を格納する。その後、第２の鍵取得手段２ｄは、携帯端末装置１に対して登録完了通知を送信する。
【００２３】
ファイル要求転送手段２ｅは、通信機器（たとえば、ゲートウェイ装置５）からファイル要求を受け取ると、ファイル要求に含まれる第１の鍵情報と第２の鍵情報との組と一致する第１の鍵情報と第２の鍵情報との組が鍵情報記憶手段２ｂに格納されているか否かを判断する。鍵情報記憶手段２ｂに一致する鍵情報が格納されている場合、ファイル要求転送手段２ｅは、ファイル要求をファイルサーバ装置３に転送する。
【００２４】
ファイルサーバ装置３は、ゲートウェイ装置５からファイル要求を受け取ると、そのファイル要求で示されるデータを、ファイル要求の送信元宛に送信する。
携帯端末装置４は、携帯端末装置１に対して接続要求を送信することができる。また、携帯端末装置４は、携帯端末装置１から送られた第１の鍵情報をゲートウェイ装置５に転送し、ゲートウェイ装置５から送られた第２の鍵情報を携帯端末装置１に転送する。さらに、携帯端末装置４は、携帯端末装置１から送られたデータ取得指示をゲートウェイ装置５に転送する。
【００２５】
ゲートウェイ装置５は、携帯端末装置４から第１の鍵情報を受け取ると、その第１の鍵情報を記憶装置に格納する。その後、ゲートウェイ装置５は、第２の鍵情報を生成し、その第２の鍵情報を携帯端末装置４に送信する。また、ゲートウェイ装置５は、データ取得指示を受け取ると、そのデータ取得指示に示されるデータの取得を示すファイル要求をゲートウェイ装置２に対して送信する。なお、ファイル要求には、第１の鍵情報と第２の鍵情報とが含められる。そして、ゲートウェイ装置５は、ファイル要求に応じてデータを取得すると、そのデータをファイルサーバ装置６に転送する。
【００２６】
このような携帯端末装置１とゲートウェイ装置２とによれば、まず、互いの通信制御手段１ａ，２ａにより、安全な通信経路が確保される。その後、携帯端末装置４から携帯端末装置１に接続要求が入力されると、接続要求転送手段１ｂによりゲートウェイ装置２に対して接続要求が転送される。ゲートウェイ装置２では、第１の鍵発行手段２ｃにより第１の鍵情報が生成され、第１の鍵情報が鍵情報記憶手段２ｂに格納されると共に、第１の鍵情報が携帯端末装置１に送信される。送信された第１の鍵情報は、携帯端末装置１の第１の鍵転送手段１ｃにより、携帯端末装置４に転送される。さらに、第１の鍵情報は、携帯端末装置４からゲートウェイ装置５に転送され、ゲートウェイ装置５で保持される。
【００２７】
次に、ゲートウェイ装置５で第２の鍵情報が生成され、携帯端末装置４に送信される。すると、第２の鍵情報は、２つの携帯端末装置４，１で転送され、ゲートウェイ装置２に

送られる。そして、ゲートウェイ装置２において、先に生成された第１の鍵情報に対応付けて、第２の鍵情報が格納される。

【００２８】

第２の鍵情報が格納されると、ゲートウェイ装置２から登録完了通知が携帯端末装置１に対して出力される。すると、携帯端末装置１から携帯端末装置４にデータ取得指示が出される。そのデータ取得指示は、携帯端末装置４からゲートウェイ装置５に転送される。

【００２９】

ゲートウェイ装置５では、データ取得指示に応じて、第１の鍵情報と第２の鍵情報とを含むファイル要求をゲートウェイ装置２に対して広帯域の回線経由で送信する。すると、ゲートウェイ装置２において、ファイル要求に示される第１の鍵情報と第２の鍵情報との組が、鍵情報記憶手段２ｂに格納されているものと一致することを確認する。２つの鍵情報が一致すれば、ゲートウェイ装置２からファイルサーバ装置３へファイル要求が転送される。

【００３０】

ファイルサーバ装置３は、ファイル要求を受け取ると、ファイル要求で示されるデータを、ファイル要求の送信元宛に送信する。送信されたデータは、ゲートウェイ装置２で中継され、ゲートウェイ装置５に送られる。ゲートウェイ装置５は、取得したデータを、保護ネットワークＮ３内のファイルサーバ装置６に転送し、格納させる。

【００３１】

このように、鍵情報などの制御情報は、安全性の高い携帯端末装置経由の通信経路を用いてゲートウェイ装置２とゲートウェイ装置５との間で受け渡しを行い、実際のデータは他の経路で通信することで、携帯端末装置の通信時間を短縮し、同時に消費電力を抑制できる。しかも、重要な情報を安全に伝送することができる。

【００３２】

さらに、鍵情報を相互に交換し、２つの鍵情報を使用することで、２重の安全チェックが行われる。これにより、確実な安全性確認を行うことができる。

次に、本実施の形態の詳細を説明する。

【００３３】

［第１の実施の形態］

図２は、第１の実施の形態のシステム構成例を示す図である。第１の実施の形態では、インターネット１０に対して、Ａ氏宅の保護ネットワーク３０とＢ氏宅の保護ネットワーク４０とが接続されている。

【００３４】

保護ネットワーク３０は、ゲートウェイ装置３００を介してインターネット１０に接続されている。保護ネットワーク３０内には、ファイルサーバ装置５００が設けられている。同様に、保護ネットワーク４０は、ゲートウェイ装置４００を介してインターネット１０に接続されている。保護ネットワーク４０内には、ファイルサーバ装置６００が設けられている。

【００３５】

また、Ａ氏は、携帯端末装置１００を所有している。携帯端末装置１００は、無線ＬＡＮや公衆網接続（ＰＨＳ、３Ｇ（3rd Generation）携帯電話など）など複数の通信インタフェースを有している。携帯端末装置１００は、ＶＰＮによってゲートウェイ装置３００に接続し、保護ネットワーク３０内の機器として動作することができる。なお、携帯端末装置１００は、ゲートウェイ装置３００との間でＶＰＮ接続を行わなくても、接続の際にゲートウェイ装置３００において携帯端末装置１００の認証を行い、通信すべきデータの暗号化を行うことができればよい。

【００３６】

同様に、Ｂ氏は、携帯端末装置２００を所有している。携帯端末装置２００は、無線ＬＡＮや公衆網接続（ＰＨＳ、３Ｇ携帯電話など）など複数の通信インタフェースを有している。携帯端末装置２００は、ＶＰＮによってゲートウェイ装置４００に接続し、保護ネ

ットワーク４０内の機器として動作することができる。なお、携帯端末装置２００は、ゲートウェイ装置４００との間でＶＰＮ接続を行わなくても、接続の際にゲートウェイ装置４００において携帯端末装置２００の認証を行い、通信すべきデータの暗号化を行うことができればよい。

【００３７】

携帯端末装置１００，２００同士は、無線ＬＡＮのＡｄ－ｈｏｃ接続等を使って、ユーザ同士の認証によりローカルネットワーク２０を形成することもできる。Ａｄ－ｈｏｃ接続は、アクセスポイントを介さずに機器同士で直接通信を行う通信モードである。これにより、ファイルサーバ装置５００から携帯端末装置１００，２００を経由しファイルサーバ装置６００に至る信頼性の高い経路が形成できる。なお、ファイルサーバ装置５００からファイルサーバ装置６００への他の通信経路としては、携帯端末装置１００，２００を経由しない、インターネット１０経由の広帯域な経路も存在する。

【００３８】

本実施の形態では、Ａ氏とＢ氏とが外出先で互いの携帯端末装置１００，２００を無線ＬＡＮで接続することで、ローカルネットワーク２０を構成する。そして、Ａ氏とＢ氏とがそれぞれ携帯端末装置１００，２００を操作することで、携帯端末装置１００がアクセス可能なファイルサーバ装置５００上のデータを携帯端末装置２００がアクセス可能なファイルサーバ装置６００に転送する。

【００３９】

まず、携帯端末装置１００，２００を経由した信頼性の高い経路を使って、ゲートウェイ装置３００，４００が相互に、ＵＲＬ（Uniform Resource Locator）やＩＰアドレスなどの接続情報、認証や暗号化の情報などを交換する。次に、ファイルサーバ装置５００からファイルサーバ装置６００へインターネット１０を介した経路でデータ伝送を行う。このとき、ゲートウェイ装置３００，４００が接続情報、認証、暗号化情報を用いることで、安全性・信頼性を確保したデータ伝送が可能となる。

【００４０】

このように、信頼性は高いが、伝送能力の低い携帯端末装置１００，２００の経路では、安全性、信頼性に関わる少量のデータの伝送のみを行い、消費電力および伝送時間の削減を行う。更に、このとき得た情報を元に広帯域の経路で実際のファイル転送を行うことで、簡易性、信頼性を維持したデータ伝送を行う。

【００４１】

なお、第１の実施の形態では、ファイルサーバ装置５００からファイルサーバ装置６００にデータを転送する場合に、ゲートウェイ装置３００がファイルサーバ装置５００に接続するために必要な情報が含まれた第１のチケットを発行する。これを、携帯端末装置１００，２００を経由した、信頼性の高い経路で保護ネットワーク４０側に伝送する。

【００４２】

同様に、ゲートウェイ装置４００が、ファイルサーバ装置６００に接続するために必要な情報が含まれた第２のチケットを発行し、保護ネットワーク３０側に転送する。ファイルサーバ装置６００からファイルサーバ装置５００へ、ファイル要求を行う際には第１のチケットと第２のチケットとを添付する。ファイルサーバ装置５００側では第１のチケットがネットワーク３０内で発行されたものと一致すること、ファイル要求元が、第２のチケットの発行元と一致することを確認し、ファイル要求を受け付け、データ転送を開始する。

【００４３】

すなわち、相互にチケットを交換、チケットや接続元の同一性を確認することで、より安全性・信頼性の高いデータ伝送が可能となる。

図３は、第１の実施の形態におけるデータ転送手順の概略を示す図である。まず、携帯端末装置２００から携帯端末装置１００へ接続要求が出される（ステップＳ１１）。すると、携帯端末装置１００は、接続要求をゲートウェイ装置３００に転送する（ステップＳ１２）。ゲートウェイ装置３００は、接続要求に応答して、第１のチケットを発行する。

発行された第１のチケットは携帯端末装置１００に送られる（ステップＳ１３）。携帯端末装置１００は、第１のチケットを携帯端末装置２００に転送する（ステップＳ１４）。

【００４４】

すると、携帯端末装置２００は、第１のチケットを添付したチケット要求をゲートウェイ装置４００に送信する（ステップＳ１５）。ゲートウェイ装置４００は、チケット要求に応答して第２のチケットを発行する。第２のチケットは、携帯端末装置２００に送信される（ステップＳ１６）。

【００４５】

携帯端末装置２００は、第２のチケットを携帯端末装置１００に転送する（ステップＳ１７）。携帯端末装置１００は、第２のチケットをゲートウェイ装置３００に転送する（ステップＳ１８）。

【００４６】

ゲートウェイ装置３００は、第２のチケットを受け取るとチケット転送完了通知を携帯端末装置１００に対して発行する（ステップＳ１９）。携帯端末装置１００は、チケット転送完了通知を受けて、携帯端末装置２００に対してデータ取得指示を発行する（ステップＳ２０）。

【００４７】

携帯端末装置２００は、ゲートウェイ装置４００にデータ取得指示を発行する（ステップＳ２１）。ゲートウェイ装置４００は、ファイルサーバ装置５００宛のファイル要求を発行する（ステップＳ２２）。なお、ファイル要求には、第１のチケットと第２のチケットとが添付される。

【００４８】

ゲートウェイ装置３００は、ファイル要求に添付された第１のチケットと第２のチケットとを確認し、先に発行されたものと一致していれば、ファイル要求を通過させる。通過したファイル要求はファイルサーバ装置５００に渡される。ファイルサーバ装置５００は、ファイル要求に応じて、データをファイルサーバ装置６００に転送する（ステップＳ２３）。

【００４９】

以下、図３に示す処理を実現するための各装置の構成を具体的に説明する。

図４は、携帯端末装置のハードウェア構成を示す図である。携帯端末装置１００は、制御回路１０８によって全体が制御される。制御回路１０８には、無線ＬＡＮ通信回路１０１、無線電話通信回路１０２、マイクロホン１０３、スピーカ１０４、入力キー１０５、モニタ１０６及びメモリ１０７が接続されている。

【００５０】

無線ＬＡＮ通信回路１０１は、アンテナ１０１ａを介して、無線ＬＡＮアクセスポイントとの間で無線によるデータ通信を行う。無線電話通信回路１０２は、アンテナ１０１ｂを介して、携帯電話網の基地局との間で無線によるデータ通信を行う。

【００５１】

マイクロホン１０３は、ユーザから入力された音声を、制御回路１０８に渡す。スピーカ１０４は、制御回路１０８から出力された音声データに基づいて音声を出力する。

入力キー１０５は、テンキー等の複数のキーで構成されており、ユーザによって押下されたキーに応じた信号を制御回路１０８に渡す。モニタ１０６は、たとえば、液晶表示装置であり、制御回路１０８から送られた画像データを表示する。

【００５２】

メモリ１０７は、制御回路１０８で実行する処理内容を記述したプログラム、処理に必要なデータ等を記憶する。

なお、図４には、携帯端末装置１００のハードウェア構成例を示したが、携帯端末装置２００も同様のハードウェア構成で実現できる。

【００５３】

図５は、本実施の形態に用いるゲートウェイ装置のハードウェア構成例を示す図である

。ゲートウェイ装置３００は、ＣＰＵ（Central Processing Unit）３０１によって装置全体が制御されている。ＣＰＵ３０１には、バス３０８を介してＲＡＭ（Random Access Memory）３０２、ハードディスクドライブ（ＨＤＤ:Hard Disk Drive）３０３、グラフィック処理装置３０４、入力インタフェース３０５、および通信インタフェース３０６，３０７が接続されている。

【００５４】

ＲＡＭ３０２には、ＣＰＵ３０１に実行させるＯＳ（Operating System）のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、ＲＡＭ３０２には、ＣＰＵ３０１による処理に必要な各種データが格納される。ＨＤＤ３０３には、ＯＳやアプリケーションプログラムが格納される。

【００５５】

グラフィック処理装置３０４には、モニタ１１が接続されている。グラフィック処理装置３０４は、ＣＰＵ３０１からの命令に従って、画像をモニタ１１の画面に表示させる。入力インタフェース３０５には、キーボード１２とマウス１３とが接続されている。入力インタフェース３０５は、キーボード１２やマウス１３から送られてくる信号を、バス３０８を介してＣＰＵ３０１に送信する。

【００５６】

通信インタフェース３０６は、インターネット１０に接続されている。通信インタフェース３０６は、インターネット１０を介して、携帯端末装置１００やゲートウェイ装置４００との間でデータの送受信を行う。

【００５７】

通信インタフェース３０７は、保護ネットワーク３０に接続されている。通信インタフェース３０７は、保護ネットワーク３０を介して、ファイルサーバ装置５００との間でデータの送受信を行う。

【００５８】

以上のようなハードウェア構成によって、本実施の形態の処理機能を実現することができる。なお、図５には、ゲートウェイ装置３００のハードウェア構成を示したが、ゲートウェイ装置４００、およびファイルサーバ装置５００，６００も同様のハードウェア構成で実現することができる。ただし、ファイルサーバ装置５００，６００については、通信インタフェースは１つあればよい。

【００５９】

次に、本実施の形態に係る処理を実現するための機能を示す。

図６は、Ａ氏所有の各機器の機能を示すブロック図である。携帯端末装置１００は、ＶＰＮ制御部１１０、近傍機器検出部１２０、機器情報記憶部１３０、公開データリスト取得部１４０、データリスト記憶部１５０、データリスト提供部１６０、接続要求転送部１７０、アクセスチケット転送部１８０、およびデータ取得指示部１９０を有している。

【００６０】

ＶＰＮ制御部１１０は、ＶＰＮ機能により、保護ネットワーク３０のゲートウェイ装置３００に接続する。ＶＰＮ制御部１１０は、ゲートウェイ装置３００と通信する際には、通信するパケットを暗号化する。そして、ＶＰＮ制御部１１０は、暗号化されたデータ（暗号データ）に新たなヘッダ情報を付加し、インターネット１０経由でゲートウェイ装置３００宛に送信する。また、ＶＰＮ制御部１１０は、ゲートウェイ装置３００からパケットを受信すると、そのパケット内のデータを復号する。復号したデータには、暗号化前のパケットのヘッダ情報も含まれているため、ＶＰＮ制御部１１０はそのヘッダ情報に基づいて、復号したデータを所定の機能に渡す。

【００６１】

近傍機器検出部１２０は、ＶＰＮ制御部１１０によって携帯端末装置１００が保護ネットワーク３０に接続された後、保護ネットワーク３０に接続されている機器を検出する。たとえば、近傍機器検出部１２０は、所定のプロトコルに従って保護ネットワーク３０に対して、機器情報通知要求をブロードキャストで送信する。すると、その機器情報通知要

求に対応するプロトコルを搭載している機器から、機器情報が返信される。近傍機器検出部１２０は、返信された機器情報を、機器情報記憶部１３０に格納する。

【００６２】

機器情報記憶部１３０は、機器情報を記憶するための記憶装置である。たとえば、メモリ１０７の記憶領域の一部が機器情報記憶部１３０として使用される。

公開データリスト取得部１４０は、ＶＰＮ機能によって保護ネットワーク３０に接続された後、機器情報記憶部１３０に格納された機器情報に基づいて、ファイルサーバ装置５００の存在を認識する。そこで、公開データリスト取得部１４０は、ファイルサーバ装置５００にアクセスし、公開しているデータのリストを取得する。そして、公開データリスト取得部１４０は、取得したデータリストをデータリスト記憶部１５０に格納する。

【００６３】

データリスト記憶部１５０は、データリストを記憶する記憶装置である。たとえば、メモリ１０７の記憶領域の一部がデータリスト記憶部１５０として使用される。

データリスト提供部１６０は、データリスト記憶部１５０に記憶されたデータリストを、ローカルネットワーク２０を介して携帯端末装置２００に提供する。

【００６４】

接続要求転送部１７０は、携帯端末装置２００から送られた接続要求を、ゲートウェイ装置４００に転送する。その際、接続要求転送部１７０は、接続要求で示されているデータの識別情報（たとえばＵＲＬ）を、データ取得指示部１９０に渡す。

【００６５】

アクセスチケット転送部１８０は、ゲートウェイ装置４００から送られた第１のアクセスチケットを携帯端末装置２００に転送する。また、アクセスチケット転送部１８０は、携帯端末装置２００から送られた第２のアクセスチケットをゲートウェイ装置４００に転送する。

【００６６】

データ取得指示部１９０は、ゲートウェイ装置３００から第２のチケット転送完了通知を受け取ると、携帯端末装置２００に対してデータ取得指示を送信する。なお、データ取得指示部１９０は、接続要求転送部１７０から渡されたデータの識別情報をメモリ内に格納しておき、データ取得指示を送信する際にデータの識別情報をデータ取得指示に含める。

【００６７】

ゲートウェイ装置３００は、ＶＰＮ制御部３１０，通信機器申請受付部３２０、アクセスチケット発行部３３０、相手側アクセスチケット登録部３４０、発行チケット管理テーブル３５０、およびアクセス制御部３６０を有している。

【００６８】

ＶＰＮ制御部３１０は、インターネット１０経由で携帯端末装置１００とＶＰＮ接続を行う。その際、ＶＰＮ制御部３１０は、携帯端末装置１００の認証を行い、携帯端末装置１００がＡ氏の所有するものであることを確認する。携帯端末装置１００の認証は、たとえば、予め登録されている携帯端末装置１００のＩＤと、ＶＰＮ接続の際に携帯端末装置１００から送られてくるＩＤとが一致することを確認する。また、ＶＰＮ制御部３１０は、ＶＰＮで接続した携帯端末装置１００にデータを送信する際には、送信するパケットを暗号化して、インターネット１０送信用のヘッダ情報を付加して送信する。また、ＶＰＮ制御部３１０は、携帯端末装置１００からパケットを受け取ると、そのデータを復号する。そして、ＶＰＮ制御部３１０は、復号したデータに含まれるヘッダ情報に従ってデータ転送等の処理を行う。

【００６９】

通信機器申請受付部３２０は、携帯端末装置１００から送られた接続要求を受け取る。そして、通信機器申請受付部３２０は、受け取った接続要求に示される機器ＩＤを発行チケット管理テーブル３５０に登録する。また、通信機器申請受付部３２０は、接続要求を受け取ると、アクセスチケット発行部３３０に対してアクセスチケットの発行を依頼する

。
【００７０】
アクセスチケット発行部３３０は、通信機器申請受付部３２０からアクセスチケットの発行の依頼を受け取ると、第１のアクセスチケットを発行する。そして、アクセスチケット発行部３３０は、発行した第１のアクセスチケットを発行チケット管理テーブル３５０に登録すると共に、携帯端末装置１００に対して送信する。
【００７１】
発行チケット管理テーブル３５０は、機器ＩＤに対応付けて第１のアクセスチケットと第２のアクセスチケットとを格納するための記憶装置である。たとえば、ＲＡＭ３０２内の記憶領域の一部が発行チケット管理テーブル３５０として使用される。
【００７２】
アクセス制御部３６０は、ゲートウェイ装置４００からのファイル要求を受け取ると、そのファイル要求に含まれている第１のアクセスチケットと第２のアクセスチケットとの組と、発行チケット管理テーブル３５０に格納されている情報とを照合する。そして、アクセス制御部３６０は、ファイル要求に添付された第１のアクセスチケットと第２のアクセスチケットとの組に対応する情報が発行チケット管理テーブル３５０内に存在し、使用期限などの使用条件を満たしていれば、ファイル要求をファイルサーバ装置５００に転送する。
【００７３】
ファイルサーバ装置５００は、コンテンツ記憶部５１０、サービス情報通知部５２０、およびデータ公開部５３０を有している。
コンテンツ記憶部５１０は、公開するデータを記憶する記憶装置である。たとえば、ファイルサーバ装置５００に設けられたハードディスク装置内の一部の記憶領域が、コンテンツ記憶部５１０として使用される。
【００７４】
サービス情報通知部５２０は、機器情報通知要求に応答して、ファイルサーバ装置５００の機器情報を送信する。機器情報には、たとえば、ファイルサーバ装置５００を一意に識別するためのＩＤや、ファイルサーバ装置５００が有する機能に関する情報が含まれる。
【００７５】
データ公開部５３０は、ゲートウェイ装置３００から転送されたファイル要求に応答して、要求されたデータをコンテンツ記憶部５１０から取得する。そして、データ公開部５３０は、取得したデータをゲートウェイ装置３００経由で、ファイル要求の送信元に送信する。
【００７６】
図７は、Ｂ氏所有の各機器の機能を示すブロック図である。携帯端末装置２００は、ＶＰＮ制御部２１０、近傍機器検出部２２０、機器情報記憶部２３０、公開データリスト取得部２４０、データリスト記憶部２５０、接続要求部２６０、アクセスチケット要求部２７０、およびデータ取得指示転送部２８０を有している。
【００７７】
ＶＰＮ制御部２１０は、ＶＰＮ機能により、保護ネットワーク４０のゲートウェイ装置４００に接続する。ＶＰＮ制御部２１０は、ゲートウェイ装置４００と通信する際には、通信するパケットを暗号化する。そして、ＶＰＮ制御部２１０は、暗号化されたデータ（暗号データ）に新たなヘッダ情報を付加し、インターネット１０経由でゲートウェイ装置４００宛に送信する。また、ＶＰＮ制御部２１０は、ゲートウェイ装置４００からパケットを受信すると、そのパケット内のデータを復号する。復号したデータには、暗号化前のパケットのヘッダ情報も含まれているため、ＶＰＮ制御部２１０はそのヘッダ情報に基づいて、復号したデータを所定の機能に渡す。
【００７８】
近傍機器検出部２２０は、ＶＰＮ制御部２１０によって携帯端末装置２００が保護ネッ

トワーク４０に接続された後、保護ネットワーク４０に接続されている機器を検出する。たとえば、近傍機器検出部２２０は、所定のプロトコルに従って保護ネットワーク４０に対して、機器情報通知要求をブロードキャストで送信する。すると、その機器情報通知要求に対応するプロトコルを搭載している機器から、機器情報が返信される。近傍機器検出部２２０は、返信された機器情報を、機器情報記憶部２３０に格納する。

【００７９】

機器情報記憶部２３０は、機器情報を記憶するための記憶装置である。たとえば、メモリの記憶領域の一部が機器情報記憶部２３０として使用される。

公開データリスト取得部２４０は、携帯端末装置１００から、ファイルサーバ装置５００が公開しているデータのリストを取得する。そして、公開データリスト取得部２４０は、取得したデータリストをデータリスト記憶部２５０に格納する。

【００８０】

データリスト記憶部２５０は、データリストを記憶する記憶装置である。たとえば、メモリの記憶領域の一部がデータリスト記憶部２５０として使用される。

接続要求部２６０は、操作入力に応じて、データリスト記憶部２５０に登録されたデータの中から、取得するデータを選択する。また、接続要求部２６０は、操作入力に応じて、機器情報記憶部２３０に登録された機器情報の中から、データの転送先とすべき機器の機器情報を選択する。そして、接続要求部２６０は、選択されたデータを選択された機器（本実施の形態ではファイルサーバ装置６００）へ転送するための接続要求を、ローカルネットワーク２０を介して携帯端末装置１００に送信する。

【００８１】

アクセスチケット要求部２７０は、携帯端末装置１００から第１のチケットを受け取ると、第１のチケットを添付したチケット要求をゲートウェイ装置４００に対して送信する。また、アクセスチケット要求部２７０は、チケット要求に応答してゲートウェイ装置４００から第２のアクセスチケットが返されると、受け取った第２のアクセスチケットを携帯端末装置１００に対して送信する。

【００８２】

ゲートウェイ装置４００は、ＶＰＮ制御部４１０、アクセスチケット発行部４２０、発行チケット管理テーブル４３０、およびデータ要求部４４０を有している。

ＶＰＮ制御部４１０は、インターネット１０経由で携帯端末装置２００とＶＰＮの接続を行う。その際、ＶＰＮ制御部４１０は、携帯端末装置２００の認証を行い、携帯端末装置２００がＢ氏の所有するものであることを確認する。携帯端末装置２００の認証は、たとえば、予め登録されている携帯端末装置２００のＩＤと、ＶＰＮ接続の際に携帯端末装置２００から送られてくるＩＤとが一致することを確認する。また、ＶＰＮ制御部４１０は、ＶＰＮで接続した携帯端末装置２００にデータを送信する際には、送信するパケットを暗号化して、インターネット１０送信用のヘッダ情報を付加して送信する。また、ＶＰＮ制御部４１０は、携帯端末装置２００からパケットを受け取ると、そのデータを復号する。そして、ＶＰＮ制御部４１０は、復号したデータに含まれるヘッダ情報に従ってデータ転送等の処理を行う。

【００８３】

アクセスチケット発行部４２０は、携帯端末装置２００からチケット要求を受け取ると、チケット要求に添付されていた機器ＩＤと第１のアクセスチケットとを発行チケット管理テーブル４３０に格納する。さらに、アクセスチケット発行部４２０は、第２のアクセスチケットを発行する。そして、アクセスチケット発行部４２０は、発行した第２のアクセスチケットを発行チケット管理テーブル４３０に登録すると共に、携帯端末装置２００に対して送信する。

【００８４】

発行チケット管理テーブル４３０は、機器ＩＤに対応付けて、第１のアクセスチケットと第２のアクセスチケットとを格納するための記憶装置である。たとえば、ＲＡＭ内の記憶領域の一部が発行チケット管理テーブル４３０として使用される。

【００８５】
データ要求部４４０は、携帯端末装置２００からデータ取得指示を受け取ると、データ取得指示で示されているファイルを取得するためのファイル要求を、インターネット１０経由でゲートウェイ装置３００に対して送信する。なお、データ要求部４４０は、ファイル要求を送信する際には、発行チケット管理テーブル４３０を参照し、第１のアクセスチケットと第２のアクセスチケットとを取得する。そして、データ要求部４４０は、ファイル要求に、第１のアクセスチケット、第２のアクセスチケット、およびファイルサーバ装置６００の機器ＩＤを含める。
【００８６】
ファイルサーバ装置６００は、コンテンツ記憶部６１０、サービス情報通知部６２０、およびデータ取得部６３０を有している。
コンテンツ記憶部６１０は、取得したデータを記憶する記憶装置である。たとえば、ファイルサーバ装置６００に設けられたハードディスク装置内の一部の記憶領域が、コンテンツ記憶部６１０として使用される。
【００８７】
サービス情報通知部６２０は、機器情報通知要求に応答して、ファイルサーバ装置６００の機器情報を送信する。機器情報には、たとえば、ファイルサーバ装置６００を一意に識別するためのＩＤや、ファイルサーバ装置６００が有する機能に関する情報が含まれる。
【００８８】
データ取得部６３０は、ゲートウェイ装置４００から転送されたデータをコンテンツ記憶部６１０に格納する。
次に、Ａ氏が自宅のファイルサーバ装置５００に保管しているデータを、Ｂ氏宅のファイルサーバ装置６００に転送する手順を具体的に説明する。
【００８９】
図８は、第１の実施の形態におけるＡ氏側のデータ転送準備処理の手順を示すシーケンス図である。以下、図８に示す処理をステップ番号に沿って説明する。
［ステップＳ２１］Ａ氏がホットスポット（公衆無線ＬＡＮを利用できる場所）に移動し携帯端末装置１００が無線ＬＡＮでローカルネットワーク２０に接続された後、携帯端末装置１００のＶＰＮ制御部１１０は、ユーザ（Ａ氏）からの操作入力に応じて、保護ネットワーク３０のゲートウェイ装置３００にアクセスし、ゲートウェイ装置３００に対してＶＰＮの接続要求を送信する。なお、携帯端末装置１００からゲートウェイ装置３００へのアクセスはインターネット１０を介して行われる。
【００９０】
［ステップＳ２２］ゲートウェイ装置３００のＶＰＮ制御部３１０は、携帯端末装置１００からのＶＰＮ接続要求に応じてＶＰＮの通信環境を構築し、ＶＰＮ接続確認を行う。これにより、携帯端末装置１００は、保護ネットワーク３０の接続機器の１つとなる。すなわち、携帯端末装置１００は、ローカルネットワーク２０と保護ネットワーク３０との両方に接続された通信機器として機能する。
【００９１】
［ステップＳ２３］携帯端末装置１００は、保護ネットワーク３０に接続された機器から機器情報を取得する。具体的には、携帯端末装置１００の近傍機器検出部１２０は、保護ネットワーク３０に対して、機器情報通知要求を送信する。
【００９２】
［ステップＳ２４］ファイルサーバ装置５００のサービス情報通知部５２０は、携帯端末装置１００に対して機器情報４１を送信する。
図９は、機器情報のデータ構造例を示す図である。機器情報４１には、機器名、機器タイプ、製造元、ＩＤ、アクセスＵＲＬなどの項目に対応付けて、情報が設定されている。
【００９３】
機器名の項目には、機器情報４１を送信した装置の名称が設定される。機器タイプの項

目には、機器情報４１を送信した装置が有している機能が示されている。図９の例では、ネットワークを介したファイル提供機能を示す情報「ファイルサーバ」が、機器タイプとして設定されている。製造元の項目には、機器情報４１を送信した装置を製造した企業の名称が設定される。ＩＤの項目には、機器情報４１を送信した装置を一意に識別するための識別情報が設定される。アクセスＵＲＬ（Uniform Resource Locator）の項目には、機器タイプで示される機能を実行するためのファイルのＵＲＬが設定される。

【００９４】

なお、ファイルサーバ装置５００から取得した機器情報４１は、機器情報記憶部１３０に格納される。

図８に戻り、機器情報４１取得後の処理を説明する。

【００９５】

［ステップＳ２５］携帯端末装置１００の公開データリスト取得部１４０は、ファイルサーバ装置５００に対して、データリストリクエスト４３を送信する。

図１０は、データリストリクエストのデータ構造例を示す図である。データリストリクエスト４３には、このリクエストがデータリスト閲覧要求であることを示す情報が設定されている。そして、データリストリクエスト４３には、コマンド実行時のパラメータとして、パスとリスト上限との項目に関する情報が含まれている。パスの項目には、閲覧対象のデータが格納されているフォルダを一意に識別するための情報（パス）が示される。なお、パスの値は、たとえば、公開データリスト取得部１４０が管理するメモリ領域に予め設定しておく。なお、データリストリクエスト４３を送信する際の操作入力によって、パスを指定することもできる。リスト上限の項目には、取得するリストに含まれるデータ名（データ名）の上限数が設定される。リスト上限の値は、たとえば、公開データリスト取得部１４０が管理するメモリ領域に予め設定しておく。なお、データリストリクエスト４３を送信する際の操作入力によって、リスト上限の値を指定することもできる。

【００９６】

なお、図１０に示したパスは、予めデータリストのファイルがファイルサーバ装置５００内に作成されているときの、そのファイルに対する基準のフォルダからの相対パスである。任意のフォルダ内のファイルリストを取得する場合には、該当するフォルダの絶対パス（たとえば、http://homegw.ddns.xyz/mediaserver/contents/）を指定することもできる。

【００９７】

図８に戻り、データリストリクエスト４３送信後の処理を説明する。

［ステップＳ２６］ゲートウェイ装置３００は、データリストリクエスト４３をファイルサーバ装置５００に転送する。

【００９８】

［ステップＳ２７］ファイルサーバ装置５００は、データリストリクエスト４３を受け取ると、パスで指定されたフォルダ内のデータリスト４４（リスト上限で指定された数以内のデータ名のリスト）をゲートウェイ装置３００へ送信する。

【００９９】

［ステップＳ２８］ゲートウェイ装置３００は、データリスト４４を携帯端末装置１００に転送する。

図１１は、データリストのデータ構造例を示す図である。データリスト４４には、この情報が、データリスト閲覧の要求に対する応答であることを示す情報が設定されている。また、データリスト４４には、リスト数の項目が設けられている。リスト数の項目には、データリスト４４に含まれるデータ名の数が設定される。そして、データリスト４４内に、リスト数に応じた数のデータ名が設定されている。データ名は、該当データにアクセスするためのＵＲＬが付与されている。なお、フォルダ名もリストに含まれている。

【０１００】

図８に戻り、データリスト４４応答後の処理を説明する。

［ステップＳ２９］携帯端末装置１００の公開データリスト取得部１４０は、取得した

データリスト４４をデータリスト記憶部１５０に格納する。

【０１０１】

以上の処理により、Ａ氏側の携帯端末装置１００においてデータ転送準備が整う。

図１２は、第１の実施の形態におけるＢ氏側のデータ転送準備処理の手順を示すシーケンス図である。以下、図１２に示す処理をステップ番号に沿って説明する。

【０１０２】

［ステップＳ３１］Ｂ氏がＡ氏と同じホットスポットに移動し携帯端末装置２００が無線ＬＡＮでローカルネットワーク２０に接続された後、携帯端末装置２００のＶＰＮ制御部２１０は、ユーザ（Ｂ氏）からの操作入力に応じて、保護ネットワーク４０のゲートウェイ装置４００にアクセスし、ゲートウェイ装置４００に対してＶＰＮの接続要求を送信する。なお、携帯端末装置２００からゲートウェイ装置４００へのアクセスはインターネット１０を介して行われる。

【０１０３】

［ステップＳ３２］ゲートウェイ装置４００のＶＰＮ制御部４１０は、携帯端末装置２００からのＶＰＮ接続要求に応じてＶＰＮの通信環境を構築し、ＶＰＮ接続確認を行う。これにより、携帯端末装置２００は、保護ネットワーク４０の接続機器の１つとなる。すなわち、携帯端末装置２００は、ローカルネットワーク２０と保護ネットワーク４０との両方に接続された通信機器として機能する。

【０１０４】

［ステップＳ３３］携帯端末装置２００は、保護ネットワーク４０に接続された機器から機器情報を取得する。具体的には、携帯端末装置２００の近傍機器検出部２２０は、保護ネットワーク４０に対して、機器情報通知要求を送信する。

【０１０５】

［ステップＳ３４］ファイルサーバ装置６００のサービス情報通知部６２０は、携帯端末装置２００に対して機器情報４２を送信する。

以上の処理により、Ｂ氏側の携帯端末装置２００においてデータ転送準備が整う。

【０１０６】

次に、携帯端末装置１００と携帯端末装置２００とをローカルネットワーク２０で接続し、互いに通信することで、転送するデータの選択、データ転送の指示を行う。

図１３は、データ取得指示を出力するまでの手順を示すシーケンス図である。以下、図１３に示す処理をステップ番号に沿って説明する。

【０１０７】

［ステップＳ４１］携帯端末装置１００のデータリスト提供部１６０は、データリスト記憶部１５０に格納されているデータリスト４４を携帯端末装置２００に送信する。

［ステップＳ４２］携帯端末装置２００の公開データリスト取得部２４０は、携帯端末装置１００から送られたデータリスト４４を取得し、データリスト記憶部２５０に格納する。

【０１０８】

［ステップＳ４３］接続要求部２６０は、データリスト記憶部２５０に格納されたデータリスト４４の中から取得するデータを選択する。具体的には、接続要求部２６０は、データリスト４４の内容を携帯端末装置２００のモニタに表示させ、取得するデータを指定する操作入力を受け付ける。ユーザ（Ｂ氏）によってデータが指定されると、接続要求部２６０は、指定されたデータを取得すべきデータとして選択する。

【０１０９】

図１４は、データ選択画面の例を示す図である。データ選択画面６０には、リスト表示部６１が設けられている。リスト表示部６１には、データリスト４４に示されるフォルダ名やデータ名が表示される。ユーザは、携帯端末装置２００の入力キーを操作して、任意のデータ名を指定することができる。

【０１１０】

リスト表示部６１の下には、戻るボタン６２と表示ボタン６３とが設けられている。戻

るボタン６２は、データ選択画面６０表示前の画面を表示させるためのボタンである。表示ボタン６３は、フォルダが選択された時に、そのフォルダの内容を表示させるためのボタンである。リスト表示部６１でフォルダが選択され、表示ボタン６３が押下された場合、選択されたフォルダ内のファイルが画面に表示される。

【０１１１】

図１３に戻り、データ選択後の処理を説明する。

［ステップＳ４４］接続要求部２６０は、機器情報記憶部２３０に格納された機器情報の中からデータ取得を実行させる機器を選択する。具体的には、接続要求部２６０は、機器情報の内容を携帯端末装置２００のモニタに表示させ、データの取得を実行させる機器を指定する操作入力を受け付ける。ユーザ（Ｂ氏）によって機器が指定されると、接続要求部２６０は、指定された機器を、データ取得を実行すべき機器として選択する。

【０１１２】

図１５は、機器選択メニューの表示例を示す図である。この例では、データ選択画面６０を表示中に所定のキーを操作することで、取得機器選択メニュー６４が表示される。取得機器選択メニュー６４には、機器情報記憶部２３０に格納された機器情報に示される機器名のリストが表示され、ユーザが、表示された機器名の１つを指定する操作入力を行うことで、接続要求部２６０によって指定された機器が取得機器として選択される。

【０１１３】

図１３に戻り、取得機器選択後の処理を説明する。

［ステップＳ４５］接続要求部２６０は、携帯端末装置１００に対して接続要求４５を送信する。

【０１１４】

図１６は、接続要求のデータ構造例を示す図である。接続要求４５には、アクション、コンテンツ、および機器ＩＤの項目が設けられている。アクションの項目には、当該要求が接続の許可処理を求めるメッセージであることが示されている。コンテンツの項目には、取得するデータを一意に識別するための情報が設定される。機器ＩＤの項目には、データの転送先となる機器の機器ＩＤが設定される。この例では、ファイルサーバ装置６００の機器ＩＤが設定される。

【０１１５】

図１３に戻り、接続要求送信後の処理を説明する。

［ステップＳ４６］携帯端末装置１００の接続要求転送部１７０は、携帯端末装置２００から送られた接続要求４５をゲートウェイ装置３００に転送する。

【０１１６】

［ステップＳ４７］ゲートウェイ装置３００の通信機器申請受付部３２０は、接続要求４５に含まれている機器ＩＤを、発行チケット管理テーブル３５０に登録する。そして、通信機器申請受付部３２０は、アクセスチケット発行部３３０に対してアクセスチケットの発行を依頼する。アクセスチケット発行部３３０は、接続要求４５に応じた第１のアクセスチケット４６を発行する。そして、アクセスチケット発行部３３０は、発行した第１のアクセスチケット４６を携帯端末装置１００に対して送信する。また、アクセスチケット発行部３３０は、発行した第１のアクセスチケット４６の内容を、発行チケット管理テーブル３５０に登録する。

【０１１７】

図１７は、第１のアクセスチケットのデータ構造例を示す図である。第１のアクセスチケット４６は、チケットデータと有効期限との項目が設けられている。チケットデータの項目には、第１のアクセスチケット４６を一意に識別するためのデータ（チケットデータ）が設定されている。チケットデータは、保護ネットワーク３０へアクセスするための鍵情報の１つである。チケットデータとして、例えば、アクセスチケット発行部３３０によってランダムに生成された値が使用される。なお、提供するコンテンツのパス、ファイル情報、取得機器のＩＤなどと、ゲートウェイ装置３００が有する秘密鍵を基にして、ハッシュ関数を用いてチケットデータを生成してもよい。有効期限の項目には、第１のアクセ

スチケット４６の有効期限が設定される。有効期限は、たとえば、アクセスチケット発行部３３０が、接続要求４５を取得した日時に所定時間を加算することで算出する。

【０１１８】

図１３に戻り、第１のアクセスチケット発行後の処理を説明する。

［ステップＳ４８］携帯端末装置１００のアクセスチケット転送部１８０は、ゲートウェイ装置３００から送られた第１のアクセスチケット４６を携帯端末装置２００に転送する。

【０１１９】

［ステップＳ４９］携帯端末装置２００のアクセスチケット要求部２７０は、携帯端末装置１００から送られた第１のアクセスチケット４６を受け取ると、ゲートウェイ装置４００に対してチケット要求４７を送信する。

【０１２０】

図１８は、チケット要求のデータ構造例を示す図である。チケット要求４７には、アクションと機器ＩＤとの項目が設けられている。アクションの項目には、チケットの発行を依頼するメッセージであることが示されている。機器ＩＤの項目には、データの転送先となる機器の機器ＩＤが設定される。この例では、ファイルサーバ装置６００の機器ＩＤが設定される。また、チケット要求４７には、第１のアクセスチケット４６が添付されている。

【０１２１】

図１３に戻り、チケット要求送信後の処理を説明する。

［ステップＳ５０］ゲートウェイ装置４００のアクセスチケット発行部４２０は、チケット要求４７に応じて第２のアクセスチケットを発行する。具体的には、アクセスチケット発行部４２０は、ランダムな値を生成し、チケットデータとする。さらに、アクセスチケット発行部４２０は、現在の時刻から所定の時間経過後の時刻を有効期限と決定し、チケットデータと有効期限との組を第２のアクセスチケット４８とする。次に、アクセスチケット発行部４２０は、チケット要求４７に含まれる機器ＩＤ、第１のアクセスチケット４６内のチケットデータ、および第２のアクセスチケットのチケットデータを組にして、発行チケット管理テーブル４３０に登録する。そして、アクセスチケット発行部４２０は、第２のアクセスチケット４８を携帯端末装置２００に送信する。

【０１２２】

図１９は、データ要求側の発行チケット管理テーブルのデータ構造例を示す図である。発行チケット管理テーブル４３０には、機器ＩＤ、第１のチケットデータ、および第２のチケットデータの欄が設けられている。機器ＩＤの欄には、データの転送先となる機器の機器ＩＤが設定される。第１のチケットデータの欄には、第１のアクセスチケット４６で示されたチケットデータが設定される。第２のチケットデータの欄には、第２のアクセスチケット４８のために生成されたチケットデータが設定される。

【０１２３】

図２０は、第２のアクセスチケットのデータ構造例を示す図である。第２のアクセスチケット４８は、チケットデータと有効期限との項目が設けられている。チケットデータの項目には、第２のアクセスチケット４８を一意に識別するためのデータ（チケットデータ）が設定されている。チケットデータは、保護ネットワーク３０へアクセスするための鍵情報の１つである。有効期限の項目には、第２のアクセスチケット４８の有効期限が設定される。有効期限は、たとえば、アクセスチケット発行部４２０が、チケット要求４７を取得した日時に所定時間を加算することで算出する。

【０１２４】

図１３に戻り、第２のアクセスチケット４８送信後の処理を説明する。

［ステップＳ５１］携帯端末装置２００のアクセスチケット要求部２７０は、チケット要求４７に応答して第２のアクセスチケット４８が返されると、その第２のアクセスチケット４８を携帯端末装置１００に転送する。

【０１２５】

［ステップＳ５２］携帯端末装置１００のアクセスチケット転送部１８０は、携帯端末装置２００から第２のアクセスチケット４８を受け取ると、その第２のアクセスチケット４８をゲートウェイ装置３００に転送する。

【０１２６】

［ステップＳ５３］ゲートウェイ装置３００の相手側アクセスチケット登録部３４０は、受信した第２のアクセスチケット４８の内容を発行チケット管理テーブル３５０に登録する。

【０１２７】

図２１は、データ送信側の発行チケット管理テーブルのデータ構造例を示す図である。発行チケット管理テーブル３５０には、機器ＩＤ、第１のアクセスチケットおよび第２のアクセスチケットの欄が設けられている。機器ＩＤの欄には、データの転送先となる機器の機器ＩＤが設定される。

【０１２８】

第１のアクセスチケットの欄には、第１のアクセスチケット４６の内容が登録される。具体的には、第１のアクセスチケットの欄は、データと有効期限との欄に細分化されている。データの欄には、第１のアクセスチケット４６のチケットデータが登録される。有効期限の欄には、第１のアクセスチケット４６の有効期限が設定される。

【０１２９】

第２のアクセスチケットの欄には、第２のアクセスチケット４８の内容が登録される。具体的には、第２のアクセスチケットの欄は、データと有効期限との欄に細分化されている。データの欄には、第２のアクセスチケット４８のチケットデータが登録される。有効期限の欄には、第２のアクセスチケット４８の有効期限が設定される。

【０１３０】

なお、図２１に示した発行チケット管理テーブル３５０は、アクセス可能なコンテンツの制限を設けない場合の例である。アクセス対象となるコンテンツ毎に個別のアクセスチケットを発行する場合、図２１に示した発行チケット管理テーブル３５０に対して、コンテンツＵＲＬの欄が追加される。コンテンツＵＲＬの欄には、接続要求４５のコンテンツの項目の値が設定される。

【０１３１】

図１３に戻り、第２のアクセスチケット４８登録後の処理を説明する。

［ステップＳ５４］相手側アクセスチケット登録部３４０は、第２のアクセスチケット４８の登録完了通知を携帯端末装置１００に送信する。

【０１３２】

［ステップＳ５５］携帯端末装置１００のデータ取得指示部１９０は、登録完了通知を受け取ると、携帯端末装置２００に対してデータ取得指示４９を送信する。なお、データ取得指示部１９０は、データ転送準備完了の画面表示を行い、ユーザ（Ａ氏）からデータ転送の実行を指示する操作入力が行われた場合に、データ取得指示４９を送信するようにしてもよい。

【０１３３】

また、データ取得指示部１９０は、接続要求転送部１７０から渡されたデータの識別情報をメモリに格納している。そして、データ取得指示部１９０は、登録完了通知を受け取った際には、メモリからデータの識別情報を読み出し、データ取得指示４９に含める。

【０１３４】

図２２は、データ取得指示のデータ構造例を示す図である。データ取得指示４９には、アクションとコンテンツとの項目が設けられている。アクションの項目には、データの取得を依頼することが示されている。コンテンツの項目には、取得すべきデータの識別情報（たとえばＵＲＬ）が設定される。

【０１３５】

図１３に戻り、データ取得指示４９送信後の処理を説明する。

［ステップＳ５６］携帯端末装置２００のデータ取得指示転送部２８０は、データ取得

指示４９を受け取ると、そのデータ取得指示４９をゲートウェイ装置４００に転送する。

【０１３６】

以上のようにして、携帯端末装置１００，２００を用いた操作入力によって、データ取得指示４９が出される。

図２３は、データ転送処理の手順を示すシーケンス図である。以下、図２３に示す処理をステップ番号に沿って説明する。

【０１３７】

［ステップＳ６１］ゲートウェイ装置４００のデータ要求部４４０は、データ取得指示４９に応じて、ゲートウェイ装置３００に対してファイル要求５０を送信する。

図２４は、ファイル要求のデータ構造例を示す図である。ファイル要求５０には、アクション、コンテンツ、第１のチケットデータ、第２のチケットデータ、および機器ＩＤの項目が設けられている。

【０１３８】

アクションの項目には、データの取得要求であることが示されている。コンテンツの項目には、要求するデータを一意に識別するための識別情報（たとえばＵＲＬ）が設定される。第１のチケットデータの項目には、第１のアクセスチケット４６によって送られたチケットデータが設定される。第２のチケットデータの項目には、第２のアクセスチケット４８によって送られたチケットデータが設定される。機器ＩＤの項目には、データの転送先となる機器の機器ＩＤが設定される。

【０１３９】

なお、データ取得指示４９には、取得すべきデータの識別情報（ＵＲＬ）のみが含まれているため、ファイル要求５０内の他の情報は、発行チケット管理テーブル４３０から取得される。ゲートウェイ装置４００と携帯端末装置２００との間はＶＰＮで接続されており、チケット要求４７とデータ取得指示４９とを同一コネクション内の通信で行うことができる。データ要求部４４０は、データ取得指示４９を受信した際には、同一コネクションのチケット要求４７に応じて登録された情報（機器ＩＤ、第１のチケットデータ、および第２のチケットデータ）を、発行チケット管理テーブル４３０から抽出する。そして、データ要求部４４０は、データ取得指示４９のコンテンツの項目の値と、発行チケット管理テーブル４３０から抽出した情報とから、ファイル要求５０を生成する。

【０１４０】

図２３に戻り、ファイル要求５０送信後の処理を説明する。

［ステップＳ６２］ゲートウェイ装置３００のアクセス制御部３６０は、ファイル要求５０に含まれるチケットの正否を確認する。この処理の詳細は後述する。

【０１４１】

［ステップＳ６３］アクセス制御部３６０は、ファイル要求のチケットが正しいことが確認できた場合、ファイル要求５１をファイルサーバ装置５００に転送する。

図２５は、転送されたファイル要求のデータ構造例を示す図である。ファイル要求５１は、ゲートウェイ装置４００から出力されたファイル要求５０からチケットデータと機器ＩＤとを削除したものである。

【０１４２】

図２３に戻り、ファイル要求５１転送後の処理を説明する。

［ステップＳ６４］ファイルサーバ装置５００のデータ公開部５３０は、ファイル要求５１を受け取ると、そのファイル要求５１のコンテンツの項目で指定されたデータをコンテンツ記憶部５１０から取り出す。そして、データ公開部５３０は、ファイル要求５１に対する応答として、取り出したデータ５２を送信する。

【０１４３】

［ステップＳ６５］ゲートウェイ装置３００のアクセス制御部３６０は、ファイルサーバ装置５００から送られたデータ５２をゲートウェイ装置４００に転送する。

［ステップＳ６６］ゲートウェイ装置４００のデータ要求部４４０は、ファイル要求５０に対する応答として返されたデータ５２を取得し、ファイル要求５０の機器ＩＤで示さ

れるファイルサーバ装置６００に対して、データ５２を転送する。

【０１４４】

［ステップＳ６７］ファイルサーバ装置６００のデータ取得部６３０は、ゲートウェイ装置４００から送られたデータ５２を取得する。

［ステップＳ６８］データ取得部６３０は、取得したデータ５２をコンテンツ記憶部６１０に格納する。

【０１４５】

以上のようにして、携帯端末装置１００，２００からの操作によって、保護ネットワーク３０のファイルサーバ装置５００が提供するデータを別の保護ネットワーク４０のファイルサーバ装置６００に転送することができる。

【０１４６】

次に、チケット確認処理を詳細に説明する。

図２６は、チケット確認処理の手順を示すフローチャートである。以下、図２６に示す処理をステップ番号に沿って説明する。

【０１４７】

［ステップＳ７１］ゲートウェイ装置３００のアクセス制御部３６０は、ファイル要求５０を受信する。

［ステップＳ７２］アクセス制御部３６０は、ファイル要求５０から第１と第２のチケットデータと機器ＩＤとを抽出する。

【０１４８】

［ステップＳ７３］アクセス制御部３６０は、発行チケット管理テーブル４３０から、抽出した第１と第２のチケットデータと機器ＩＤとの組に対して、値が一致する発行チケット情報を検索する。

【０１４９】

［ステップＳ７４］アクセス制御部３６０は、ステップＳ７３における検索において、アクセスデータと機器ＩＤが一致する発行チケット情報が検出されたか否かを判断する。検出された場合、処理がステップＳ７５に進められる。検出されなかった場合、処理がステップＳ７７に進められる。

【０１５０】

［ステップＳ７５］アクセス制御部３６０は、現在の日時が、検出された発行チケット情報の第１と第２のアクセスチケットそれぞれに設定されている有効期限内か否かを判断する。第１と第２のアクセスチケット共に有効期限内であれば、処理がステップＳ７６に進められる。いずれか一方の有効期限を過ぎていれば、処理がステップＳ７７に進められる。

【０１５１】

［ステップＳ７６］アクセス制御部３６０は、受信したファイル要求５０からチケットデータと機器ＩＤとを除いたファイル要求５１を、ファイルサーバ装置５００に転送する。その後、処理が終了する。

【０１５２】

［ステップＳ７７］アクセス制御部３６０は、ファイル要求５０に応じたデータ送信を拒否することとし、エラーメッセージをゲートウェイ装置４００に送信する。その後、処理が終了する。

【０１５３】

以上のように、Ａ氏とＢ氏とが外出先で互いの携帯端末装置１００，２００を操作することで、Ａ氏宅のファイルサーバ装置５００からＢ氏宅のファイルサーバ装置６００へデータを転送することが出来る。この際、保護ネットワーク３０に対して外部からアクセスするために必要なチケットデータ（鍵情報）は、携帯端末装置１００，２００を利用した安全な通信経路で受け渡される。そして、転送されるデータは、携帯端末装置１００，２００を経由せずにデータ転送が行われる。その結果、携帯端末装置１００，２００の性能に依存せずに、高速なデータ転送が可能であると共に、保護ネットワーク３０の安全性を

損なわずに保護ネットワーク３０内のデータを他人に引き渡すことができる。

【０１５４】

［第２の実施の形態］

第２の実施の形態は、既存のゲートウェイ装置を利用して第１の実施の形態と同様の処理を実現するものである。

【０１５５】

図２７は、第２の実施の形態のシステム構成を示す図である。図２７において、第１の実施の形態と同じ機能を有する要素には、図２に示した要素と同じ符号を付して説明を省略する。

【０１５６】

第２の実施の形態では、第１の実施の形態におけるゲートウェイ装置３００の機能が、ゲートウェイ装置３００ａとデータ伝送装置７０１とに分かれている。すなわち、図６に示したゲートウェイ装置３００の要素のうち、ＶＰＮ制御部３１０と、アクセス制御部３６０におけるデータ転送機能はゲートウェイ装置３００ａに残され、他の要素とアクセス制御部３６０のチケット確認機能とはデータ伝送装置７０１に設けられる。

【０１５７】

また、第１の実施の形態におけるゲートウェイ装置４００の機能が、ゲートウェイ装置４００ａとデータ伝送装置７０２とに分かれている。すなわち、図７に示したゲートウェイ装置４００の要素のうち、ＶＰＮ制御部４１０はゲートウェイ装置４００ａに残され、他の要素はデータ伝送装置７０２に設けられる。

【０１５８】

このようにデータ伝送装置７０１，７０２を用いれば、既存のゲートウェイ装置３００ａ，４００ａをそのまま利用して、第１の実施の形態と同様の処理を実施することが可能である。

【０１５９】

なお、データ伝送装置７０１の機能をファイルサーバ装置５００内に実装し、データ伝送装置７０２の機能をファイルサーバ装置６００内に実装することも可能である。これにより、既存のハードウェア機器を用いて、第１の実施の形態と同様の処理を実施することが可能となる。

【０１６０】

［第３の実施の形態］

第３の実施の形態は、Ａ宅のファイルサーバ装置からＢ氏宅のファイルサーバ装置にデータを転送する場合に、共有ストレージサーバ装置を経由させるものである。共有ストレージサーバ装置は、Ａ氏が所有する携帯端末装置で指定する。

【０１６１】

共有ストレージサーバ装置としては、ネットワークサービス業者でサービスの一環として運用されている装置を利用することができる。このような業者の装置を利用する場合、データを暗号化して共有ストレージサーバ装置に格納することでデータの安全性を維持できる。

【０１６２】

図２８は、第３の実施の形態のシステム構成例を示す図である。本実施の形態では、携帯端末装置１００ａが暗号鍵を発行する。暗号鍵は、信頼性の高い経路（たとえばＶＰＮ）を介してゲートウェイ装置３００ｂに渡される。その暗号鍵を用いてゲートウェイ装置３００ｂがデータを暗号化して、共有ストレージサーバ装置８００に格納する。

【０１６３】

また、携帯端末装置１００ａで発行された暗号鍵は、携帯端末装置２００ａを経由してゲートウェイ装置４００ｂに渡される。このとき携帯端末装置２００ａとゲートウェイ装置４００ｂとの間も信頼性の高い経路（たとえばＶＰＮ）で接続しておくことで、暗号鍵を安全にゲートウェイ装置４００ｂに渡すことができる。

【０１６４】

ゲートウェイ装置４００ｂは、共有ストレージサーバ装置８００からデータを取得する。そして、ゲートウェイ装置４００ｂは、携帯端末装置１００ａから渡されている暗号鍵でデータを復号する。復号されたデータは、ファイルサーバ装置６００に転送されファイルサーバ装置６００内に格納される。

【０１６５】

これにより、ゲートウェイ装置３００，４００の設定の変更をせずに、既存のサービスを使って簡易かつ安全なデータ転送が可能となる。

図２９は、第３の実施の形態における動作の概略を示す図である。まず、携帯端末装置２００ａから携帯端末装置１００ａに対して、ローカルネットワーク２０を介してファイル要求が送信される（ステップＳ８１）。携帯端末装置１００ａは、ファイル要求を受け取ると暗号鍵を生成し、暗号鍵付きのデータ転送指示をゲートウェイ装置３００ｂに対して送信する（ステップＳ８２）。

【０１６６】

ゲートウェイ装置３００ｂは、データ転送指示をファイルサーバ装置５００に対して送信する（ステップＳ８３）。すると、ファイルサーバ装置５００からゲートウェイ装置３００ｂへデータが転送される（ステップＳ８４）。ゲートウェイ装置３００ｂは、携帯端末装置１００ａから渡された暗号鍵でデータを暗号化する。そして、暗号化された暗号データが、ゲートウェイ装置３００ｂから共有ストレージサーバ装置８００に転送される（ステップＳ８５）。共有ストレージサーバ装置８００では、暗号データをストレージデバイスに格納する。

【０１６７】

暗号データの転送が完了すると、ゲートウェイ装置３００ｂから携帯端末装置１００ａに対して、データ転送終了通知が送信される（ステップＳ８６）。携帯端末装置１００ａは、データ転送終了通知を受け取ると、携帯端末装置２００ａに対して、暗号鍵付きのデータ取得指示を送信する（ステップＳ８７）。携帯端末装置２００ａは、暗号鍵付きのデータ取得指示をゲートウェイ装置４００ｂに転送する（ステップＳ８８）。

【０１６８】

ゲートウェイ装置４００ｂは、データ取得指示を受け取ると暗号鍵を記憶した後、格納し、共有ストレージサーバ装置８００に対してファイル要求を送信する（ステップＳ８９）。共有ストレージサーバ装置８００は、ファイル要求に応答して暗号データをゲートウェイ装置４００ｂに転送する（ステップＳ９０）。ゲートウェイ装置４００ｂは、取得した暗号データを暗号鍵で復号し、平文となったデータをファイルサーバ装置６００に転送する（ステップＳ９１）。

【０１６９】

次に、本実施の形態に係る処理を実現するための機能を説明する。

図３０は、Ａ氏所有の各装置の機能を示すブロック図である。なお、図３０において、図６に示した第１の実施の形態の要素と同じ機能を有する要素については同じ符号を付し説明を省略する。

【０１７０】

携帯端末装置１００ａは、第１の実施の形態における接続要求転送部１７０とアクセスチケット転送部１８０とに代えて、データ転送指示部１７１、鍵生成部１７２、および鍵記憶部１７３を有している。また、データ取得指示部１９１の機能が、第１の実施の形態のデータ取得指示部１９０の機能と異なっている。

【０１７１】

データ転送指示部１７１は、携帯端末装置２００ａから渡されたファイル要求を受け取ると、鍵生成部１７２に暗号鍵の生成を依頼する。そして、データ転送指示部１７１は鍵生成部１７２から暗号鍵を受け取ると、暗号鍵付きのデータ転送指示をゲートウェイ装置３００ｂに対して送信する。

【０１７２】

鍵生成部１７２は、データ転送指示部１７１からの依頼に応じて、鍵情報を生成する。

鍵情報は、たとえば、ランダムに生成した値である。鍵生成部１７２は、生成した暗号鍵をデータ転送指示部１７１に渡すと共に、鍵記憶部１７３に格納する。

【０１７３】

鍵記憶部１７３は、暗号鍵を記憶するための記憶装置である。たとえば、携帯端末装置１００ａのメモリの記憶領域の一部が鍵記憶部１７３として使用される。

データ取得指示部１９１は、ゲートウェイ装置３００ｂからデータ転送終了通知を受け取ると、暗号鍵付きのデータ取得指示を携帯端末装置２００ａに対して送信する。

【０１７４】

ゲートウェイ装置３００ｂは、第１の実施の形態における通信機器申請受付部３２０、アクセスチケット発行部３３０、相手側アクセスチケット登録部３４０、および発行チケット管理テーブル３５０に代えて、データ転送指示制御部３２１、鍵記憶部３７０、および暗号化部３８０を有している。また、アクセス制御部３６１の機能が、第１の実施の形態におけるアクセス制御部３６０と異なる。

【０１７５】

データ転送指示制御部３２１は、携帯端末装置１００ａからデータ転送指示を受け取ると、そのデータ転送指示から鍵情報を抽出する。そして、データ転送指示制御部３２１は、抽出した鍵情報を鍵記憶部３７０に格納する。さらに、データ転送指示制御部３２１は、鍵情報を除いたデータ転送指示をファイルサーバ装置５００に転送する。

【０１７６】

鍵記憶部３７０は、暗号鍵を記憶するための記憶装置である。たとえば、ゲートウェイ装置３００ｂのＲＡＭの記憶領域の一部が鍵記憶部３７０として使用される。

暗号化部３８０は、ファイルサーバ装置５００からデータが転送されると、鍵記憶部３７０から暗号鍵を取得する。そして、暗号化部３８０は、ファイルサーバ装置５００から転送されたデータを、暗号鍵を用いて暗号化する。さらに、暗号化部３８０は、暗号化したデータ（暗号データ）をアクセス制御部３６１に渡す。

【０１７７】

アクセス制御部３６１は、暗号データを受け取ると、データ転送指示で示されていた共有ストレージ内の位置情報（ＵＲＬ）に対して、暗号データを転送する。

共有ストレージサーバ装置８００は、共有ストレージ８１０、データ受信部８２０、およびデータ送信部８３０を有している。

【０１７８】

共有ストレージ８１０は、データを記憶するための記憶装置である。たとえば、共有ストレージサーバ装置８００に設けられたハードディスク装置の記憶領域の一部が、共有ストレージ８１０として使用される。

【０１７９】

データ受信部８２０は、ゲートウェイ装置３００ｂから送られたデータを受信する。そして、データ受信部８２０は、受信したデータを共有ストレージ８１０に格納する。

データ送信部８３０は、ゲートウェイ装置４００ｂからのファイル要求に応じて共有ストレージ８１０からデータを取り出す。そして、データ送信部８３０は、ゲートウェイ装置４００ｂに対して取り出したデータを送信する。

【０１８０】

図３１は、Ｂ氏所有の各装置の機能を示すブロック図である。なお、図３１において、図７に示した第１の実施の形態の要素と同じ機能を有する要素については同じ符号を付し説明を省略する。

【０１８１】

携帯端末装置２００ａは、第１の実施の形態における接続要求部２６０とアクセスチケット要求部２７０とに代えて、ファイル要求部２６１が設けられている。ファイル要求部２６１は、ユーザ（Ｂ氏）からの操作入力により、データリスト記憶部２５０内のデータリストから取得するデータが選択され、機器情報記憶部２３０内の機器情報からデータの転送先とする機器の機器情報が選択されると、選択された情報を含むファイル要求を携帯

端末装置１００ａに対して送信する。

【０１８２】

ゲートウェイ装置４００ｂは、第１の実施の形態におけるアクセスチケット発行部４２０、および発行チケット管理テーブル４３０に代えて、鍵記憶部４５０、復号部４６０、およびデータ転送部４７０を有している。また、データ要求部４４１は、第１の実施の形態におけるデータ要求部４４０と異なる機能を有している。

【０１８３】

データ要求部４４１は、ゲートウェイ装置４００ｂからデータ取得指示を受け取ると、そのデータ取得指示から鍵情報を抽出する。そして、データ要求部４４１は、抽出した鍵情報を鍵記憶部４５０に格納する。さらに、データ要求部４４１は、データ取得指示に応答して、ファイル要求を共有ストレージサーバ装置８００に対して送信する。

【０１８４】

鍵記憶部４５０は、鍵情報を記憶するための記憶装置である。たとえば、ゲートウェイ装置４００ｂのＲＡＭ内の記憶領域の一部が鍵記憶部４５０といて使用される。

復号部４６０は、共有ストレージサーバ装置８００から暗号データが送られると、鍵記憶部４５０から鍵情報を取得する。そして、復号部４６０は、取得した鍵情報を用いて暗号データを復号する。復号された平文のデータは、データ転送部４７０に渡される。

【０１８５】

データ転送部４７０は、データをファイルサーバ装置６００に対して送信する。

次に、Ａ氏宅のファイルサーバ装置５００に保管されているデータを、Ｂ氏宅のファイルサーバ装置６００に転送する手順を具体的に説明する。なお、図８と図１２とに示した第１の実施の形態の処理は第３の実施の形態においても同様に実施されるため、説明を省略する。また、図１３に示した第１の実施の形態の処理のうち、ステップＳ４１～ステップＳ４４の処理は、第３の実施の形態においても同様に実施される。そこで、ステップＳ４４の処理以降に行われる第３の実施の形態の処理を以下に説明する。

【０１８６】

図３２は、データを共有ストレージサーバ装置に格納するまでの処理手順を示すシーケンス図である。以下、図３２に示す処理をステップ番号に沿って説明する。

［ステップＳ９１］携帯端末装置２００ａのファイル要求部２６１は、ユーザ（Ｂ氏）によって、取得するデータと転送先の機器とを選択する操作入力が行われると、携帯端末装置１００ａに対してファイル要求５０を送信する。

【０１８７】

図３３は、ファイル要求のデータ構造例を示す図である。ファイル要求５０には、アクション、コンテンツ、および機器ＩＤの項目が設けられている。アクションの項目には、データの取得要求であることが示されている。コンテンツの項目には、取得対象のデータを一意に識別するための識別情報（ＵＲＬ）が設定されている。機器ＩＤの欄には、データの転送先となる機器（この例では、ファイルサーバ装置６００）の機器ＩＤが設定されている。

【０１８８】

図３２に戻り、ファイル要求５０送信後の処理を説明する。

［ステップＳ９２］携帯端末装置１００ａの鍵生成部１７２は、ファイル要求５０に応じて暗号鍵を生成する。生成された暗号鍵は、データ転送指示部１７１に渡される。また、暗号鍵は鍵記憶部１７３に格納される。

【０１８９】

［ステップＳ９３］データ転送指示部１７１は、ファイル要求５０のコンテンツの項目で示されるデータのデータ転送指示５１をゲートウェイ装置３００ｂに対して送信する。この際、データ転送指示部１７１は、ユーザ（Ａ氏）からの操作入力により、共有ストレージサーバ装置８００内の記憶領域（フォルダ）を特定する情報（ＵＲＬ）を取得する。なお、共有ストレージサーバ装置８００のＵＲＬをデータ転送指示部１７１に予め設定しておくこともできる。

【０１９０】
なお、共有ストレージサーバ装置８００は、ファイルサーバ装置５００と携帯端末装置１００ａとの双方からアクセス可能であることが望ましい。そこで、携帯端末装置１００ａからアクセス可能な共有ストレージサーバのリストをファイルサーバ装置５００に送信し、その中で、ファイルサーバ装置５００からアクセス可能な共有ストレージサーバのリストをファイルサーバ装置５００から返信させるようにしてもよい。この場合、データ転送指示部１７１は、ファイルサーバ装置５００から返されたリストを表示し、ユーザ（Ａ氏）にデータの格納場所の選択を促す。そして、データ転送指示部１７１は、選択された共有ストレージサーバをデータの格納場所に決定する。なお、この例では、共有ストレージサーバ装置８００内のフォルダが選択されたものとする。

【０１９１】
図３４は、データ転送指示のデータ構造例を示す図である。データ転送指示５１には、アクション、コンテンツ、共有ストレージ、および暗号鍵の項目が設けられている。アクションの項目には、当該要求がデータの転送指示であることが示されている。コンテンツの項目には、転送対象となるデータを一意に識別するための情報（ＵＲＬ）が設定されている。共有ストレージの項目には、データの格納先となる共有ストレージサーバ装置のフォルダを一意に識別するための情報（ＵＲＬ）が設定されている。暗号鍵の項目には、鍵生成部１７２で生成された暗号鍵が設定されている。

【０１９２】
図３２に戻り、データ転送指示５１送信後の処理を説明する。
［ステップＳ９４］ゲートウェイ装置３００ｂのデータ転送指示制御部３２１は、データ転送指示５１から暗号鍵を抽出し、鍵記憶部３７０に格納する。

【０１９３】
［ステップＳ９５］データ転送指示制御部３２１は、データ転送指示５１のコンテンツの項目によって、転送すべきデータがファイルサーバ装置５００によって管理されていることを認識する。そして、データ転送指示制御部３２１は、ファイルサーバ装置５００に対してデータ転送指示５２を送信する。

【０１９４】
図３５は、ゲートウェイ装置から送信されたデータ転送指示のデータ構造例を示す図である。データ転送指示５２には、アクション、コンテンツ、および共有ストレージの項目が設けられている。各項目の内容は、データ転送指示５１と同じである。すなわち、データ転送指示５２は、データ転送指示５１から暗号鍵を除去したものである。

【０１９５】
図３２に戻り、データ転送指示５２送信後の処理を説明する。
［ステップＳ９６］ファイルサーバ装置５００のデータ公開部５３０は、データ転送指示５２のコンテンツの項目で示されるデータ５３を、コンテンツ記憶部５１０から取得する。そして、データ公開部５３０は、取得したデータ５３をゲートウェイ装置３００ｂに送信する。なお、データ５３の送信パケットの宛先には、データ転送指示５２の共有ストレージの項目で示されていたＵＲＬが設定される。

【０１９６】
［ステップＳ９７］ゲートウェイ装置３００ｂの暗号化部３８０は、ファイルサーバ装置５００から送られたデータ５３を受信する。次に、暗号化部３８０は、鍵記憶部３７０から暗号鍵を取得する。さらに、暗号化部３８０は、取得した暗号鍵でデータ５３を暗号化し、暗号データ５４を生成する。そして、暗号化部３８０は、生成した暗号データ５４をアクセス制御部３６１に渡す。

【０１９７】
［ステップＳ９８］アクセス制御部３６１は、暗号データ５４を、データ５３の宛先として指定されている装置（この例では、共有ストレージサーバ装置８００）に転送する。
［ステップＳ９９］共有ストレージサーバ装置８００のデータ受信部８２０は、暗号データ５４を取得する。

【０１９８】
［ステップＳ１００］データ受信部８２０は、暗号データ５４を共有ストレージ８１０に格納する。
［ステップＳ１０１］ゲートウェイ装置３００ｂのデータ転送指示制御部３２１は、アクセス制御部３６１による暗号データ５４の送信が完了したことを確認すると、携帯端末装置１００ａに対してデータ転送終了通知５５を送信する。
【０１９９】
図３６は、共有ストレージサーバ装置からデータを取得する処理手順を示すシーケンス図である。以下、図３６に示す処理をステップ番号に沿って説明する。
［ステップＳ１０２］携帯端末装置１００ａのデータ取得指示部１９１は、データ転送終了通知を受け取ると、鍵記憶部１７３から鍵情報を取得する。そして、データ取得指示部１９１は、携帯端末装置２００ａに対して鍵情報を含むデータ取得指示５６を送信する。また、データ取得指示部１９１は、データ転送指示部１７１に対して指定された共有ストレージサーバ装置８００内のフォルダの識別情報を、データ取得指示５６に付加する。
【０２００】
図３７は、データ取得指示のデータ構造例を示す図である。データ取得指示５６には、アクション、データＵＲＬ、および暗号鍵の項目が設けられている。アクションの項目には、この指示がデータの取得指示であることが示されている。データＵＲＬの項目には、共有ストレージサーバ装置８００内の暗号データ５４が格納された場所を示すＵＲＬが設定されている。暗号鍵の項目には、データ５３の暗号化に使用された暗号鍵が設定されている。
【０２０１】
図３６に戻り、データ取得指示５６送信後の処理を説明する。
［ステップＳ１０３］携帯端末装置２００ａのデータ取得指示転送部２８０は、データ取得指示５７をゲートウェイ装置４００ｂに転送する。データ取得指示５７には、データの転送先となるファイルサーバ装置６００の機器ＩＤが含められる。
【０２０２】
図３８は、転送後のデータ取得指示のデータ構造例を示す図である。データ取得指示５７には、アクション、データＵＲＬ、暗号鍵、および機器ＩＤの項目が設けられている。アクション、データＵＲＬ、および暗号鍵の項目の設定内容は、データ取得指示５６と同じである。機器ＩＤの欄には、データの転送先となる機器（この例では、ファイルサーバ装置６００）の機器ＩＤが設定されている。
【０２０３】
図３６に戻り、データ取得指示５７送信後の処理を説明する。
［ステップＳ１０４］ゲートウェイ装置４００ｂのデータ要求部４４１は、データ取得指示５７から暗号鍵を抽出して、鍵記憶部４５０に格納する。また、データ要求部４４１は、データ取得指示５７で示される機器ＩＤをデータ転送部４７０に通知する。
【０２０４】
［ステップＳ１０５］データ要求部４４１は、データ取得指示５７のデータＵＲＬの項目で示されているＵＲＬに対するファイル要求５８を送信する。
［ステップＳ１０６］共有ストレージサーバ装置８００のデータ送信部８３０は、ファイル要求５８で示される暗号データ５４を共有ストレージ８１０から抽出し、ゲートウェイ装置４００ｂに対して送信する。
【０２０５】
［ステップＳ１０７］ゲートウェイ装置４００ｂの復号部４６０は、共有ストレージサーバ装置８００から送られた暗号データ５４を受け取る。次に、復号部４６０は、鍵記憶部４５０から暗号鍵を取得し、その暗号鍵を用いて暗号データ５４を復号する。そして、復号部４６０は、復号した平文のデータ５３をデータ転送部４７０に渡す。
【０２０６】
［ステップＳ１０８］データ転送部４７０は、データ要求部４４１から渡された機器Ｉ

Ｄに対応する機器（ファイルサーバ装置６００）に対して、データ５３を転送する。
［ステップＳ１０９］ファイルサーバ装置６００のデータ取得部６３０は、送られたデータ５３を取得する。
【０２０７】
［ステップＳ１１０］データ取得部６３０は、取得したデータ５３をコンテンツ記憶部６１０に格納する。
このようにして、共有ストレージを経由して、データを転送させることができる。その結果、保護ネットワーク３０，４０に対して外部の機器（ＶＰＮ経由を除く）からアクセスせずに済み、ゲートウェイ装置３００ｂ，４００ｂの保護機能を変更する必要がない。その結果、保護ネットワーク３０，４０を危険にさらさずに済む。
【０２０８】
なお、第２の実施の形態と同様に、第３の実施の形態におけるゲートウェイ装置３００ｂ，４００ｂの機能のうち、通常のゲートウェイ装置が有している機能を除き、他のデータ伝送装置に実装することもできる。また、ゲートウェイ装置３００ｂ，４００ｂの機能のうち、通常のゲートウェイ装置が有している機能以外の機能を、ファイルサーバ装置５００，６００に実装することもできる。
【０２０９】
また、上記第１～第３の実施の形態では、データ提供者（Ａ氏）の使用する携帯端末装置とデータ取得者（Ｂ氏）の使用する携帯端末装置との機能を個別に説明したが、それぞれの機能を１つの携帯端末装置に実装することもできる。同様に、Ａ氏宅のゲートウェイ装置の機能とＢ氏宅のゲートウェイ装置の機能とを、１つのゲートウェイ装置に実装することができる。このように双方の機能を併せ持った携帯端末装置およびゲートウェイ装置をＡ氏とＢ氏とがそれぞれ所有することで、相互にデータ伝送が可能となる。
【０２１０】
なお、上記の処理機能は、コンピュータによって実現することができる。その場合、携帯端末装置、ゲートウェイ装置、ファイルサーバ装置、共有ストレージサーバ装置が有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリなどがある。磁気記録装置には、ハードディスク装置（ＨＤＤ）、フレキシブルディスク（ＦＤ）、磁気テープなどがある。光ディスクには、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）などがある。光磁気記録媒体には、ＭＯ（Magneto-Optical disk）などがある。
【０２１１】
プログラムを流通させる場合には、例えば、そのプログラムが記録されたＤＶＤ、ＣＤ－ＲＯＭなどの可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。
【０２１２】
プログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。
【０２１３】
なお、本発明は、上述の実施の形態にのみ限定されるものではなく、本発明の要旨を逸

脱しない範囲内において種々の変更を加えることができる。
以上説明した実施の形態の主な技術的特徴は、以下の付記の通りである。
【０２１４】
（付記１）　ネットワーク経由で接続された装置を遠隔制御する携帯端末装置において、
前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保する通信制御手段と、
前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含む接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に前記ゲートウェイ装置に対して前記接続要求を転送する接続要求転送手段と、
前記ゲートウェイ装置から前記データ識別情報に対応するデータにアクセスするための第１の鍵情報を取得し、前記第１の鍵情報を前記他の携帯端末装置に転送する第１の鍵転送手段と、
前記他の携帯端末装置から前記データ識別情報に対応するデータへのアクセス元が生成した第２の鍵情報を取得し、前記第２の鍵情報を前記ゲートウェイ装置に転送する第２の鍵転送手段と、
前記ゲートウェイ装置から前記第２の鍵情報の登録完了通知を受け取ると、前記記憶装置から前記データ識別情報を取得し、前記他の携帯端末装置に対して前記データ識別情報を指定したデータ取得指示を送信するデータ取得指示手段と、
を有することを特徴とする携帯端末装置。
【０２１５】
（付記２）　ネットワーク経由で接続された装置を遠隔制御する携帯端末装置において、
前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保する通信制御手段と、
鍵情報を生成する鍵生成手段と、
前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含むファイル要求を受け取ると、前記鍵生成手段から前記鍵情報を取得し、前記鍵情報を付加した前記データ識別情報で示されるデータのストレージサーバ装置への転送を指示するデータ転送要求を前記ゲートウェイ装置に対して送信すると共に、取得した前記鍵情報を記憶装置に格納するデータ転送指示手段と、
前記ストレージサーバ装置に転送されたデータにアクセスするための前記データ識別情報と、前記鍵生成手段で生成された前記鍵情報とを含むデータ取得指示を前記他の携帯端末装置に送信するデータ取得指示手段と、
を有することを特徴とする携帯端末装置。
【０２１６】
（付記３）　保護ネットワークと他のネットワークとの間に配置されて、前記保護ネットワークへの外部からのアクセスを制限するゲートウェイ装置において、
前記他のネットワークを介して接続された携帯端末装置との間で、安全な通信経路を確保する通信制御手段と、
前記保護ネットワーク内のファイルサーバ装置にアクセスするための鍵情報を記憶する鍵情報記憶手段と、
前記携帯端末装置から接続要求を受け取ると、第１の鍵情報を生成し、前記第１の鍵情報を前記鍵情報記憶手段に格納すると共に、前記第１の鍵情報を前記携帯端末装置に送信する第１の鍵発行手段と、
前記携帯端末装置から、前記他のネットワークを介して接続された通信機器で発行された第２の鍵情報が送られると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記携帯端末装置に対して登録完了通知を送信する第２の鍵取得手段と、

前記通信機器からファイル要求を受け取ると、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組と一致する前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、一致する鍵情報が格納されている場合、前記ファイル要求を前記ファイルサーバ装置に転送するファイル要求転送手段と、

を有することを特徴とするゲートウェイ装置。

【０２１７】

（付記４） 前記接続要求に、前記ファイルサーバ装置にアクセスする機器の機器ＩＤが含まれている場合、前記機器ＩＤと前記第１の鍵情報とを対応付けて前記鍵情報記憶手段に格納し、

前記ファイル要求転送手段は、前記ファイル要求から前記通信機器の機器ＩＤを取得し、前記機器ＩＤに対応付けて前記鍵情報記憶手段に格納されている前記第１の鍵情報と第２の鍵情報との組が、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組と一致するか否かを判断し、一致すれば前記ファイル要求を前記ファイルサーバ装置に転送することを特徴とする付記３記載のゲートウェイ装置。

【０２１８】

（付記５） 前記第１の鍵発行手段は、前記第１の鍵情報に有効期限を設定し、有効期限を付加した前記第１の鍵情報を前記鍵情報記憶手段に格納し、

前記第２の鍵取得手段は、有効期限付きの前記第２の鍵情報を取得すると、有効期限を付加した前記第２の鍵情報を前記鍵情報記憶手段に格納し、

前記ファイル要求転送手段は、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報の組と一致する前記第１の鍵情報と前記第２の鍵情報との組の有効期限を過ぎていない場合に限り、前記ファイル要求を前記ファイルサーバ装置に転送する、

ことを特徴とする付記３記載のゲートウェイ装置。

【０２１９】

（付記６） ネットワーク経由で接続された装置を遠隔制御するコンピュータを、

前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保する通信制御手段、

前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含む接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に前記ゲートウェイ装置に対して前記接続要求を転送する接続要求転送手段、

前記ゲートウェイ装置から前記データ識別情報に対応するデータにアクセスするための第１の鍵情報を取得し、前記第１の鍵情報を前記他の携帯端末装置に転送する第１の鍵転送手段、

前記他の携帯端末装置から前記データ識別情報に対応するデータへのアクセス元が生成した第２の鍵情報を取得し、前記第２の鍵情報を前記ゲートウェイ装置に転送する第２の鍵転送手段、

前記ゲートウェイ装置から前記第２の鍵情報の登録完了通知を受け取ると、前記記憶装置から前記データ識別情報を取得し、前記他の携帯端末装置に対して前記データ識別情報を指定したデータ取得指示を送信するデータ取得指示手段、

として機能させる遠隔制御プログラム。

【０２２０】

（付記７） ネットワーク経由で接続された装置を遠隔制御するコンピュータを、

前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保する通信制御手段、

鍵情報を生成する鍵生成手段、

前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含むファイル要求を受け取ると、前記鍵生成手段から前記鍵情報を取得し、前記鍵情報を付加した前記データ識別情報で示されるデータのストレージ

サーバ装置への転送を指示するデータ転送要求を前記ゲートウェイ装置に対して送信すると共に、取得した前記鍵情報を記憶装置に格納するデータ転送指示手段、
前記ストレージサーバ装置に転送されたデータにアクセスするためのデータ識別情報と、前記鍵生成手段で生成された前記鍵情報とを含むデータ取得指示を前記他の携帯端末装置に送信するデータ取得指示手段、
として機能させる遠隔制御プログラム。

【０２２１】

（付記８） 保護ネットワークと他のネットワークとの間に配置されて、前記保護ネットワークへの外部からのアクセスを制限するゲートウェイ装置を、
前記他のネットワークを介して接続された携帯端末装置との間で、安全な通信経路を確保する通信制御手段と、
前記保護ネットワーク内のファイルサーバ装置にアクセスするための鍵情報を記憶する鍵情報記憶手段と、
前記携帯端末装置から接続要求を受け取ると、第１の鍵情報を生成し、前記第１の鍵情報を前記鍵情報記憶手段に格納すると共に、前記第１の鍵情報を前記携帯端末装置に送信する第１の鍵発行手段と、
前記携帯端末装置から、前記他のネットワークを介して接続された通信機器で発行された第２の鍵情報が送られると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記携帯端末装置に対して登録完了通知を送信する第２の鍵取得手段と、
前記通信機器からファイル要求を受け取ると、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組と一致する前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、一致する鍵情報が格納されている場合、前記ファイル要求を前記ファイルサーバ装置に転送するファイル要求転送手段と、
して機能させることを特徴とするアクセス制限プログラム。

【０２２２】

（付記９） ネットワーク経由で接続された装置を携帯端末装置により遠隔制御するための遠隔制御方法において、
通信制御手段が、前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保するステップと、
接続要求転送手段が、前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含む接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に前記ゲートウェイ装置に対して前記接続要求を転送するステップと、
第１の鍵転送手段が、前記ゲートウェイ装置から前記データ識別情報に対応するデータにアクセスするための第１の鍵情報を取得し、前記第１の鍵情報を前記他の携帯端末装置に転送するステップと、
第２の鍵転送手段が、前記他の携帯端末装置から前記データ識別情報に対応するデータへのアクセス元が生成した第２の鍵情報を取得し、前記第２の鍵情報を前記ゲートウェイ装置に転送するステップと、
データ取得指示手段が、前記ゲートウェイ装置から前記第２の鍵情報の登録完了通知を受け取ると、前記記憶装置から前記データ識別情報を取得し、前記他の携帯端末装置に対して前記データ識別情報を指定したデータ取得指示を送信するステップと、
を有することを特徴とする遠隔制御方法。

【０２２３】

（付記１０） ネットワーク経由で接続された装置を携帯端末装置により遠隔制御するための遠隔制御方法において、
通信制御手段が、前記ネットワークを介して接続されたゲートウェイ装置との間で、安全な通信経路を確保するステップと、

鍵生成手段が鍵情報を生成するステップと、
データ転送指示手段が、前記ネットワークを介して接続された他の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含むファイル要求を受け取ると、前記鍵生成手段から前記鍵情報を取得し、前記鍵情報を付加した前記データ識別情報で示されるデータのストレージサーバ装置への転送を指示するデータ転送要求を前記ゲートウェイ装置に対して送信すると共に、取得した前記鍵情報を記憶装置に格納するステップと、
データ取得指示手段が、前記ストレージサーバ装置に転送されたデータにアクセスするためのデータ識別情報と、前記鍵生成手段で生成された前記鍵情報とを含むデータ取得指示を前記他の携帯端末装置に送信するステップと、
を有することを特徴とする遠隔制御方法。

【０２２４】
（付記１１）　保護ネットワークと他のネットワークとの間に配置されて、前記保護ネットワークへの外部からのアクセスを制限するゲートウェイ装置によるアクセス制限方法において、
通信制御手段が、前記他のネットワークを介して接続された携帯端末装置との間で、安全な通信経路を確保するステップと、
第１の鍵発行手段が、前記携帯端末装置から接続要求を受け取ると、第１の鍵情報を生成し、前記第１の鍵情報を鍵情報記憶手段に格納すると共に、前記第１の鍵情報を前記携帯端末装置に送信するステップと、
第２の鍵取得手段が、前記携帯端末装置から、前記他のネットワークを介して接続された通信機器で発行された第２の鍵情報が送られると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記携帯端末装置に対して登録完了通知を送信するステップと、
ファイル要求転送手段が、前記通信機器からファイル要求を受け取ると、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組と一致する前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否かを判断し、一致する鍵情報が格納されている場合、前記ファイル要求を前記ファイルサーバ装置に転送するステップと、
を有することを特徴とするアクセス制限方法。

【０２２５】
（付記１２）　遠隔操作によるデータ転送を行うデータ転送システムにおいて、
前記ネットワークを介して接続された第１のゲートウェイ装置との間で、安全な通信経路を確保し、第２の携帯端末装置から、取得すべきデータを識別するためのデータ識別情報を含む接続要求を受け取ると、前記データ識別情報を記憶装置に格納すると共に前記第１のゲートウェイ装置に対して前記接続要求を転送し、前記第１のゲートウェイ装置から前記データ識別情報に対応するデータにアクセスするための第１の鍵情報を取得し、前記第１の鍵情報を前記第２の携帯端末装置に転送し、前記第２の携帯端末装置から第２のゲートウェイ装置が生成した第２の鍵情報を取得し、前記第２の鍵情報を前記第１のゲートウェイ装置に転送し、前記第１のゲートウェイ装置から前記第２の鍵情報の登録完了通知を受け取ると、前記記憶装置から前記データ識別情報を取得し、前記第２の携帯端末装置に対して前記データ識別情報を指定したデータ取得指示を送信することを特徴とする第１の携帯端末装置と、
前記第１の携帯端末装置との間で、安全な通信経路を確保し、前記第１の携帯端末装置から前記接続要求を受け取ると、前記第１の鍵情報を生成し、前記第１の鍵情報を鍵情報記憶手段に格納すると共に、前記第１の鍵情報を前記第１の携帯端末装置に送信し、前記第１の携帯端末装置から、前記第２の鍵情報が送られると、前記鍵情報記憶手段に対して、前記第１の鍵情報に対応付けて前記第２の鍵情報を格納し、前記第１の携帯端末装置に対して登録完了通知を送信し、前記第２のゲートウェイ装置からファイル要求を受け取ると、前記ファイル要求に含まれる前記第１の鍵情報と前記第２の鍵情報との組と一致する前記第１の鍵情報と前記第２の鍵情報との組が前記鍵情報記憶手段に格納されているか否

かを判断し、一致する鍵情報が格納されている場合、前記ファイル要求を前記ファイルサーバ装置に転送する第１のゲートウェイ装置と、

前記ネットワークを介して接続された前記第２のゲートウェイ装置との間で、安全な通信経路を確保し、前記第１の携帯端末装置に対して接続要求を送信し、前記第１の携帯端末装置から送られた前記第１の鍵情報を前記第２のゲートウェイ装置に転送し、前記第２のゲートウェイ装置から送られた前記第２の鍵情報を前記第１の携帯端末装置に転送し、前記第１の携帯端末装置から送られた前記データ取得指示を前記第２のゲートウェイ装置に転送する前記第２の携帯端末装置と、

前記第２の携帯端末装置から前記第１の鍵情報を受け取ると、前記第１の鍵情報を記憶装置に格納し、前記第２の鍵情報を生成し、前記第２の鍵情報を前記第２の携帯端末装置に送信し、前記データ取得指示を受け取ると、前記第１の鍵情報と前記第２の鍵情報とが含まれており、前記データ取得指示に示されるデータの取得を示す前記ファイル要求を前記第１のゲートウェイ装置に対して送信する第２のゲートウェイ装置と、

を有することを特徴とするデータ転送システム。

【図面の簡単な説明】

【０２２６】

【図１】発明の概要を示す図である。

【図２】第１の実施の形態のシステム構成例を示す図である。

【図３】第１の実施の形態におけるデータ転送手順の概略を示す図である。

【図４】携帯端末装置のハードウェア構成を示す図である。

【図５】本実施の形態に用いるゲートウェイ装置のハードウェア構成例を示す図である。

【図６】Ａ氏所有の各機器の機能を示すブロック図である。

【図７】Ｂ氏所有の各機器の機能を示すブロック図である。

【図８】第１の実施の形態におけるＡ氏側のデータ転送準備処理の手順を示すシーケンス図である。

【図９】機器情報のデータ構造例を示す図である。

【図１０】データリストリクエストのデータ構造例を示す図である。

【図１１】データリストのデータ構造例を示す図である。

【図１２】第１の実施の形態におけるＢ氏側のデータ転送準備処理の手順を示すシーケンス図である。

【図１３】データ取得指示を出力するまでの手順を示すシーケンス図である。

【図１４】データ選択画面の例を示す図である。

【図１５】機器選択メニューの表示例を示す図である。

【図１６】接続要求のデータ構造例を示す図である。

【図１７】第１のアクセスチケットのデータ構造例を示す図である。

【図１８】チケット要求のデータ構造例を示す図である。

【図１９】データ要求側の発行チケット管理テーブルのデータ構造例を示す図である。

【図２０】第２のアクセスチケットのデータ構造例を示す図である。

【図２１】データ送信側の発行チケット管理テーブルのデータ構造例を示す図である。

【図２２】データ取得指示のデータ構造例を示す図である。

【図２３】データ転送処理の手順を示すシーケンス図である。

【図２４】ファイル要求のデータ構造例を示す図である。

【図２５】転送されたファイル要求のデータ構造例を示す図である。

【図２６】チケット確認処理の手順を示すフローチャートである。

【図２７】第２の実施の形態のシステム構成を示す図である。

【図２８】第３の実施の形態のシステム構成例を示す図である。

【図２９】第３の実施の形態における動作の概略を示す図である。

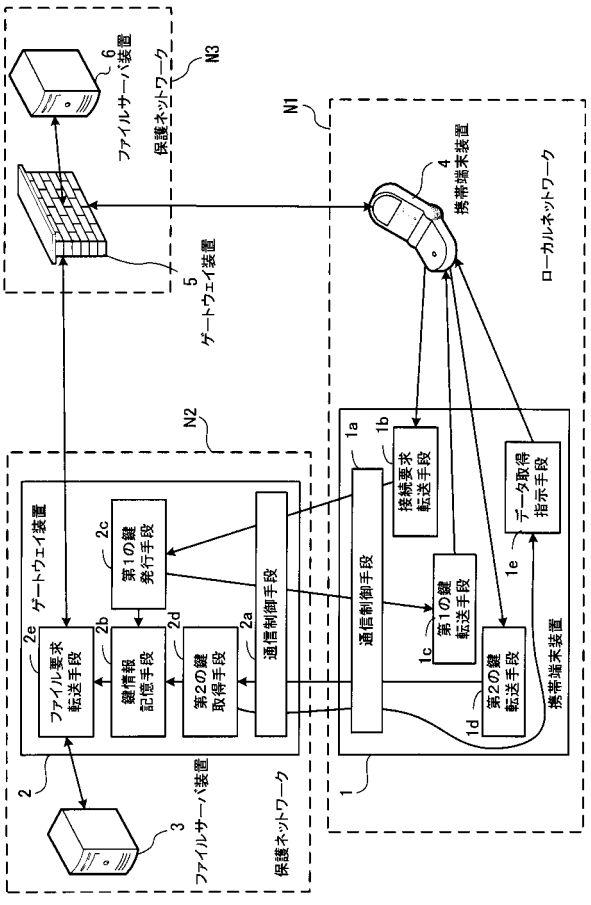
【図３０】Ａ氏所有の各装置の機能を示すブロック図である。

【図３１】Ｂ氏所有の各装置の機能を示すブロック図である。

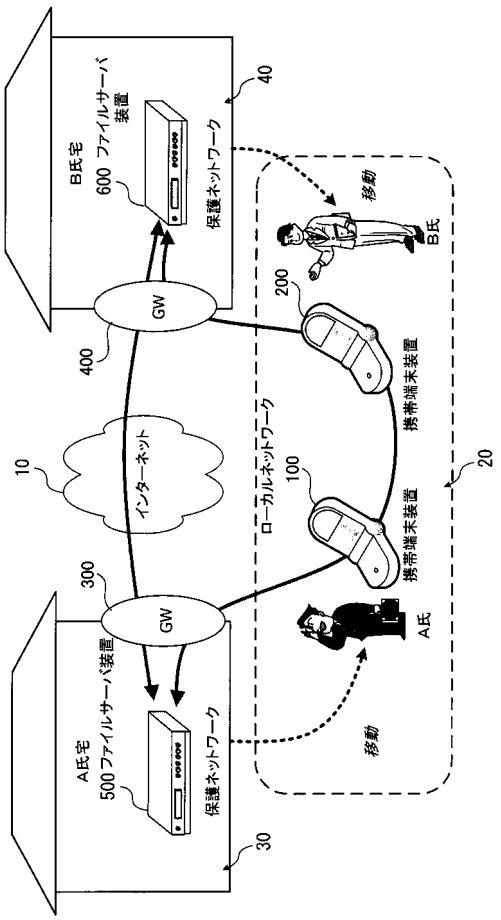
【図３２】データを共有ストレージサーバ装置に格納するまでの処理手順を示すシーケン

ス図である。
【図３３】ファイル要求のデータ構造例を示す図である。
【図３４】データ転送指示のデータ構造例を示す図である。
【図３５】ゲートウェイ装置から送信されたデータ転送指示のデータ構造例を示す図である。
【図３６】共有ストレージサーバ装置からデータを取得する処理手順を示すシーケンス図である。
【図３７】データ取得指示のデータ構造例を示す図である。
【図３８】転送後のデータ取得指示のデータ構造例を示す図である。
【符号の説明】
【０２２７】
１，４　携帯端末装置
１ａ，２ａ　通信制御手段
１ｂ　接続要求転送手段
１ｃ　第１の鍵転送手段
１ｄ　第２の鍵転送手段
１ｅ　データ取得指示手段
２，５　ゲートウェイ装置
２ｂ　鍵情報記憶手段
２ｃ　第１の鍵発行手段
２ｄ　第２の鍵取得手段
２ｅ　ファイル要求転送手段
３，６　ファイルサーバ装置
Ｎ１　ローカルネットワーク
Ｎ２，Ｎ３　保護ネットワーク

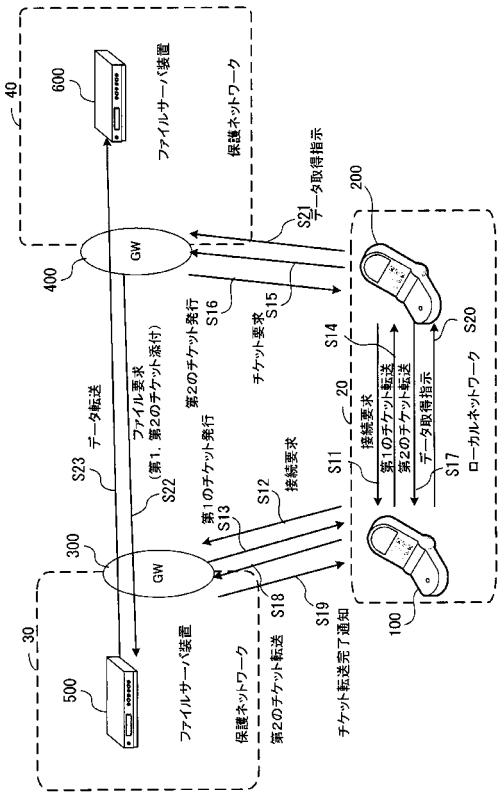
【図１】



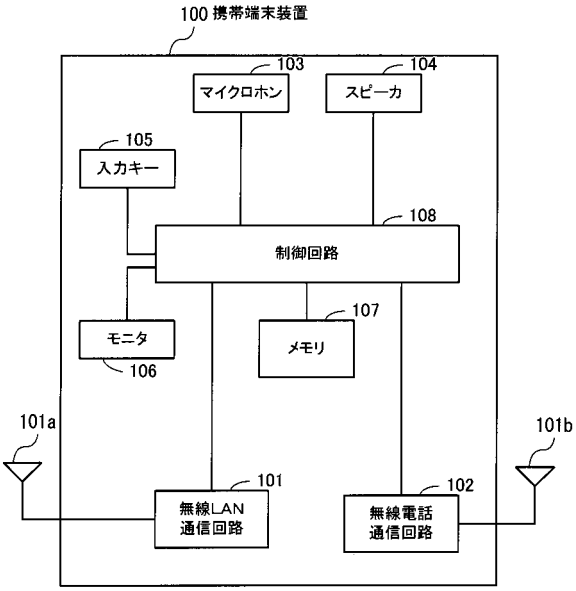
【図２】



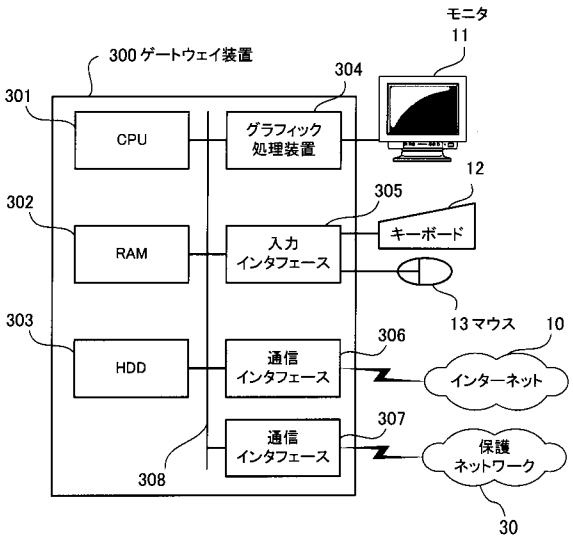
【図３】


40
600
ファイルサーバ装置
保護ネットワーク
400
GW
S21 データ取得指示
200
S16 第2のチケット発行
S15 チケット要求
S14
S20
S23 データ転送
S22 ファイル要求 (第1, 第2のチケット添付)
S13 第1のチケット発行
S12 接続要求
S11 接続要求
20
第1のチケット転送
第2のチケット転送
データ取得指示
S17
ローカルネットワーク
300
GW
S18 第2のチケット転送
S19 チケット転送完了通知
100
30
500
ファイルサーバ装置
保護ネットワーク

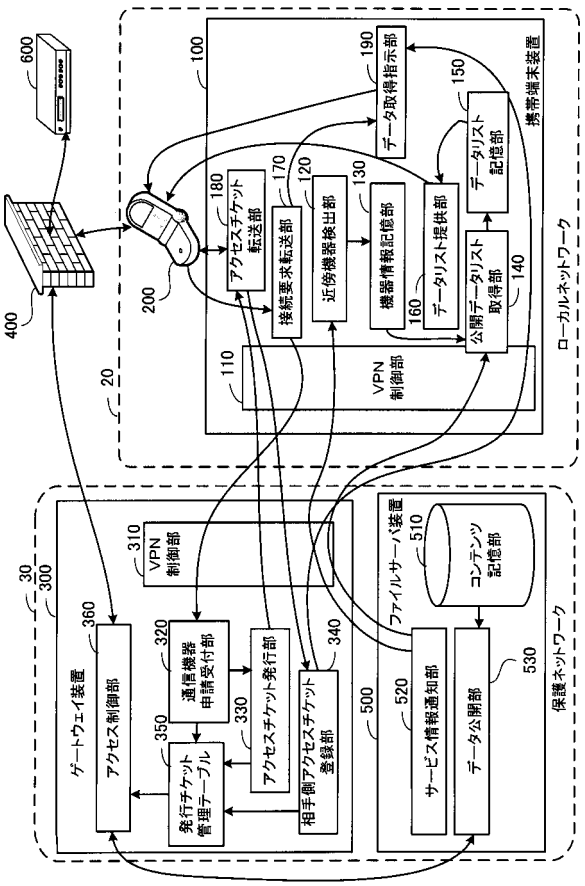
【図４】


100 携帯端末装置
103
マイクロホン
104
スピーカ
105
入力キー
108
制御回路
107
メモリ
モニタ
106
101a
101b
101
無線LAN 通信回路
102
無線電話 通信回路

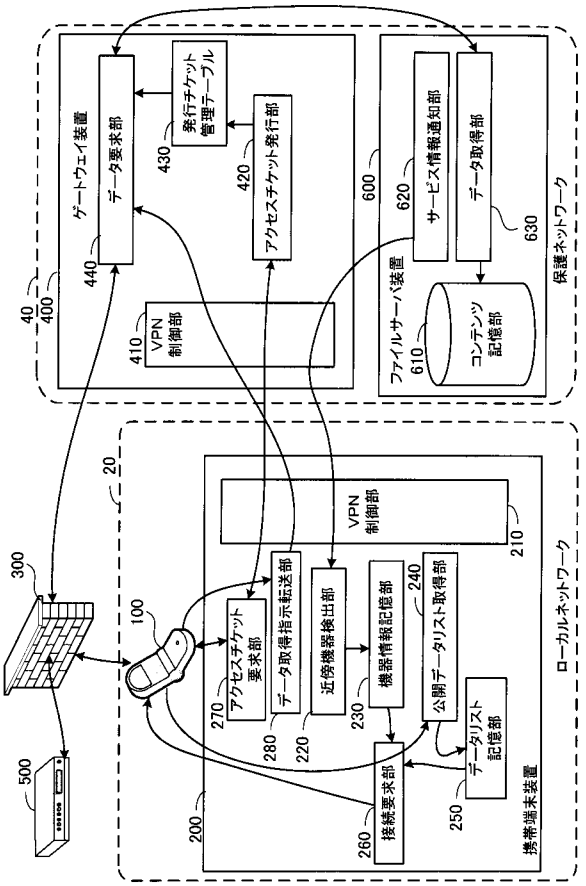
【図５】


モニタ
11
300 ゲートウェイ装置
304
301
CPU
グラフィック 処理装置
12
305
302
RAM
入力 インタフェース
キーボード
13 マウス
303
HDD
306
通信 インタフェース
10
インターネット
307
通信 インタフェース
保護 ネットワーク
308
30

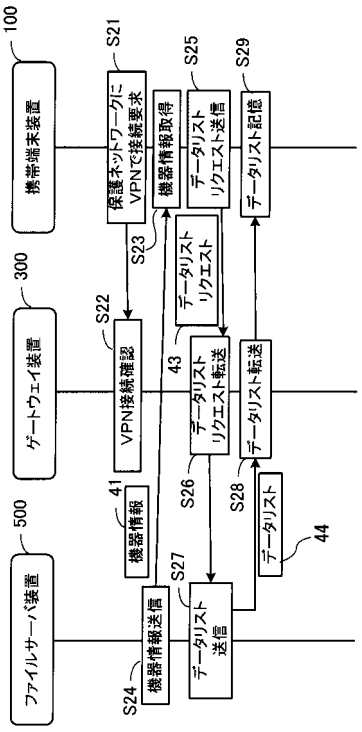
【図６】


600
100
携帯端末装置
190
データ取得指示部
150
データリスト 記憶部
180
アクセスチケット 転送部
170
120
130
接続要求転送部
近傍機器検出部
機器情報記憶部
データリスト提供部
160
公開データリスト 取得部
140
VPN 制御部
110
20
ローカルネットワーク
400
200
30
300
VPN 制御部
310
ファイルサーバ装置
510
コンテンツ 記憶部
ゲートウェイ装置
360
アクセス制御部
320
通信機器 申請受付部
330
アクセスチケット発行部
340
相手側アクセスチケット 登録部
350
発行チケット 管理テーブル
500
520
サービス情報通知部
データ公開部
530
保護ネットワーク

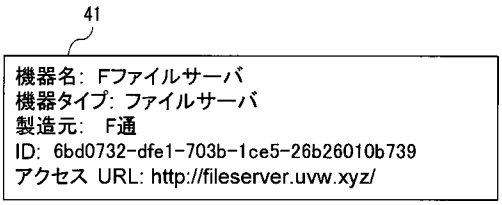
【図７】



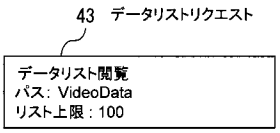
【図８】



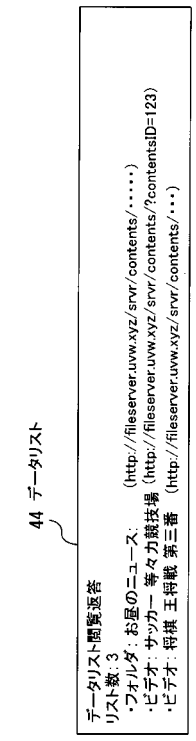
【図９】



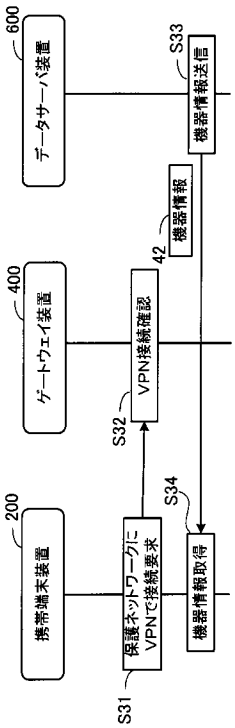
【図１０】



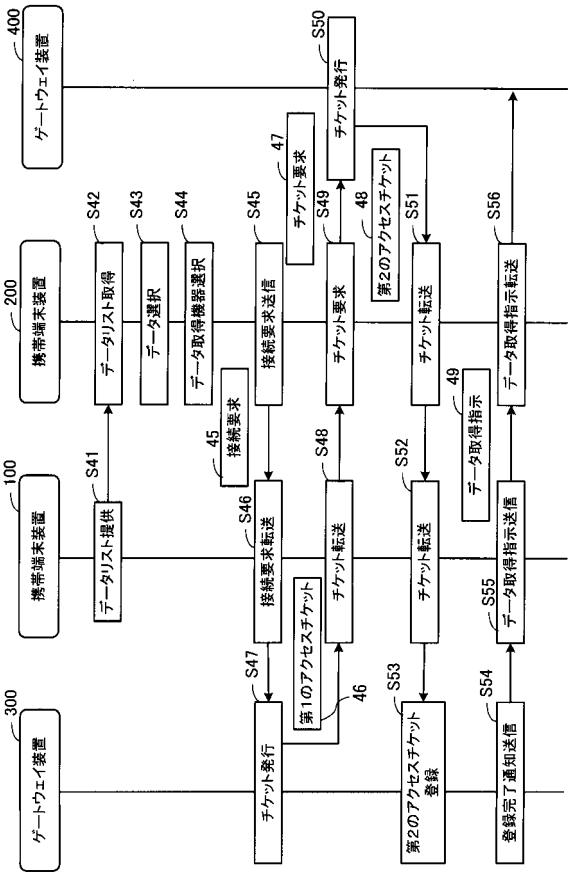
【図１１】



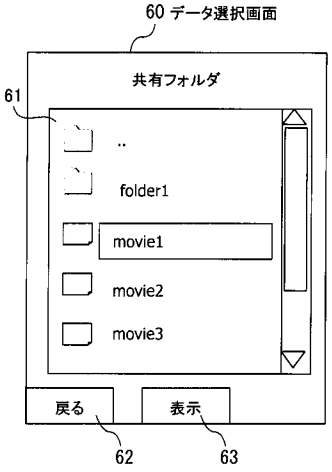
【図１２】



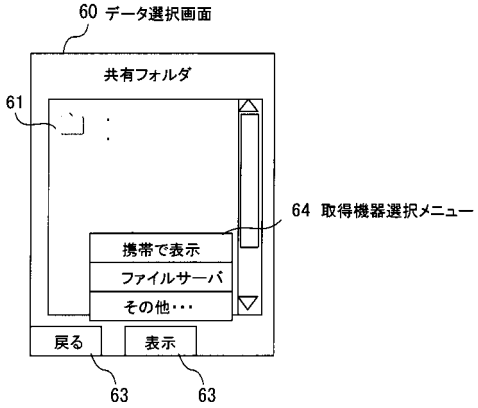
【図１３】



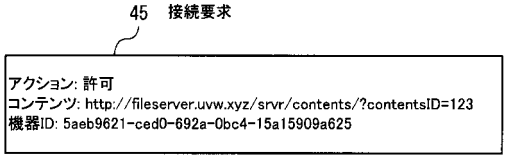
【図１４】



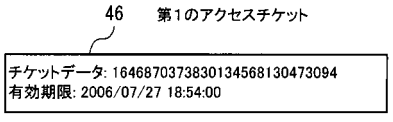
【図１５】



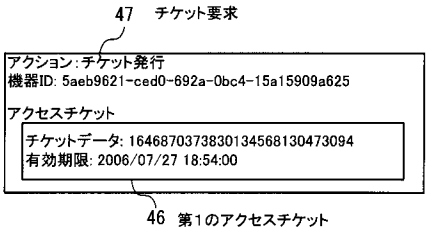
【図１６】



【図１７】



【図１８】

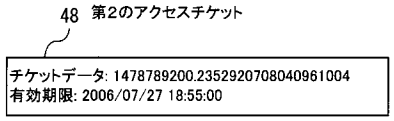


【図１９】

430 発行チケット管理テーブル

機器ID	第1のチケットデータ	第2のチケットデータ
5aeb9621-ced0-692a-0bc4-15a15909a625	16468703738301 34568130473094	1478789200.23529 20708040961004
・ ・ ・	・ ・ ・	・ ・ ・

【図２０】

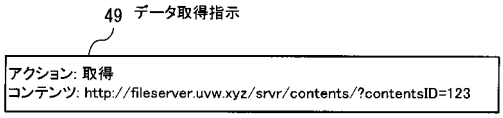


【図２１】

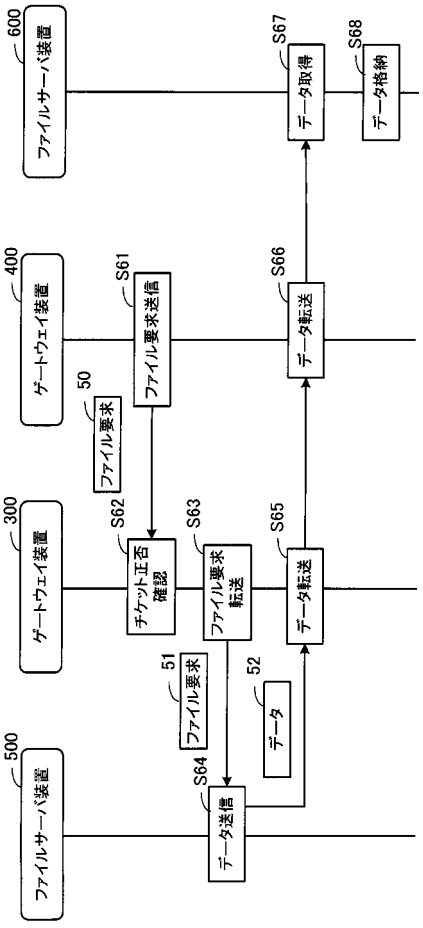
350 発行チケット管理テーブル

機器ID	第1のアクセスチケット		第2のアクセスチケット	
	データ	有効期限	データ	有効期限
5aeb9621-ced0-692a-0bc4-15a15909a625	16468703738301 34568130473094	2006/07/27 18:54:00	1478789200.23529 20708040961004	2006/07/27 18:55:00
69caa943d9c3-3210-7050-0024f2995c56	15867052229671274133720498753871	2006/07/27 19:37:00	・ ・ ・	・ ・ ・
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

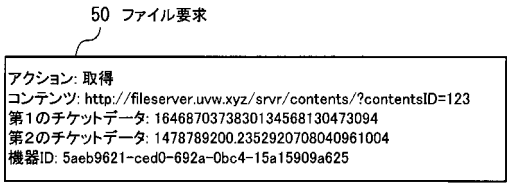
【図２２】



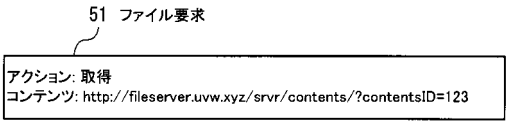
【図２３】



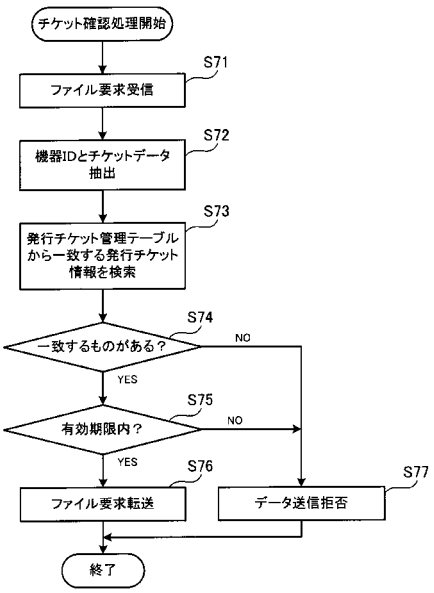
【図２４】



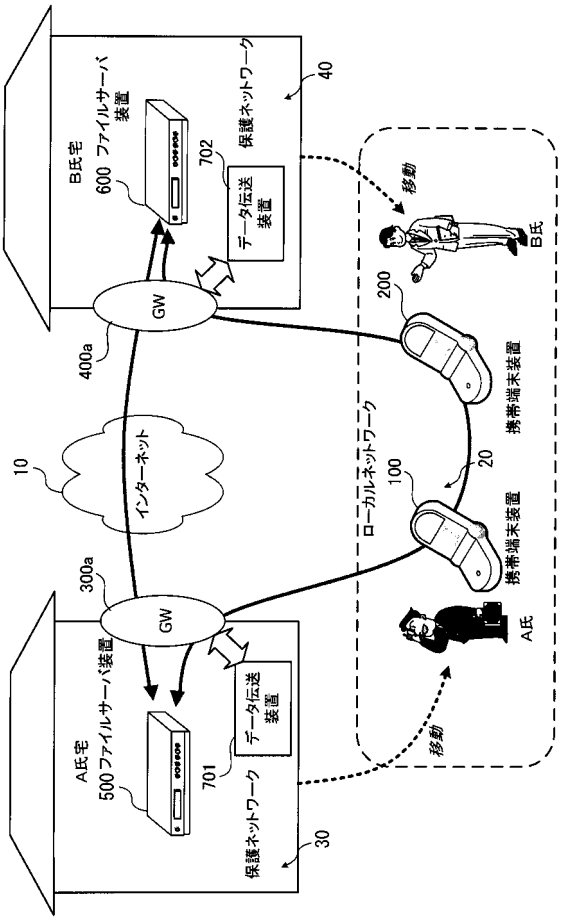
【図２５】



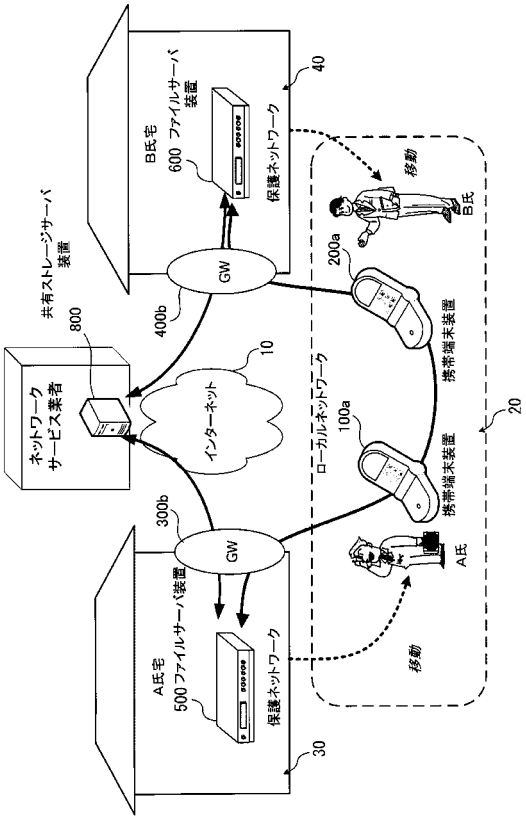
【図２６】



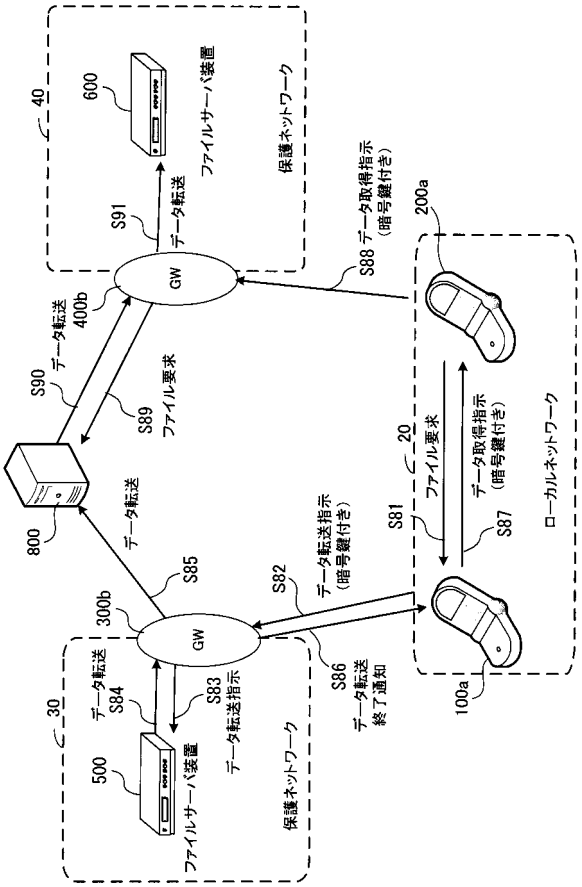
【図２７】



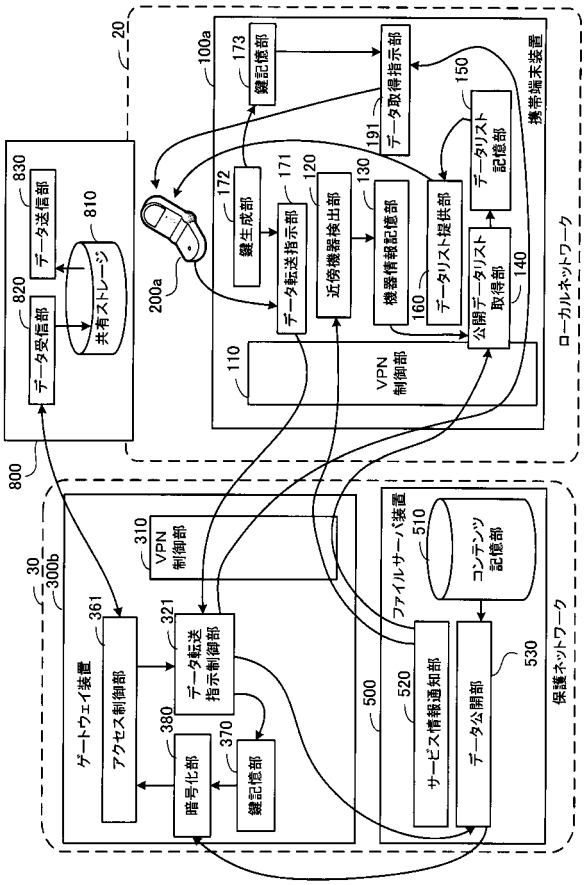
【図２８】



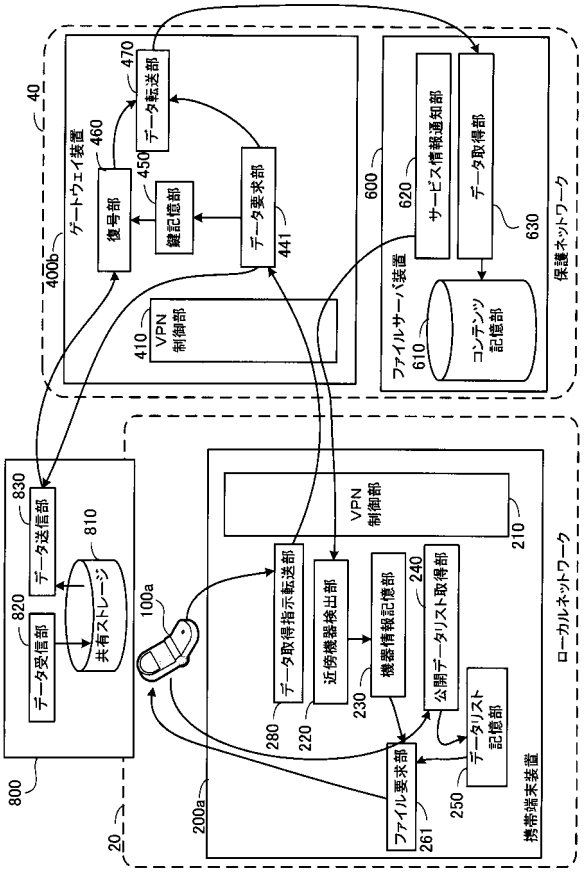
【図２９】



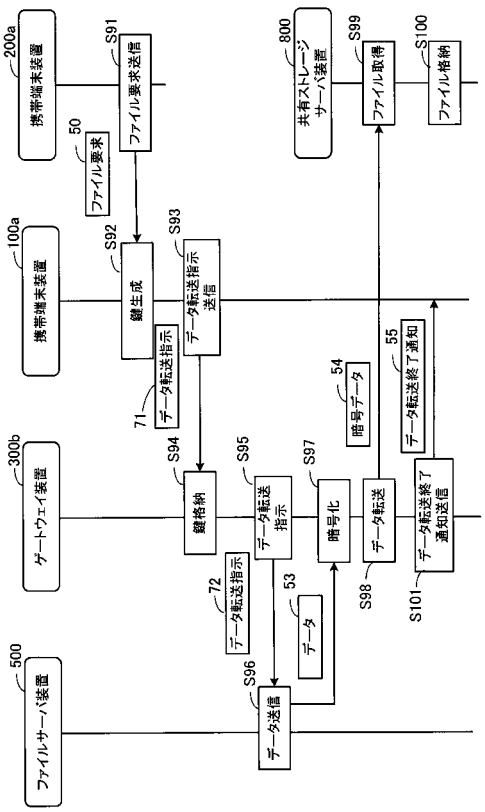
【図３０】



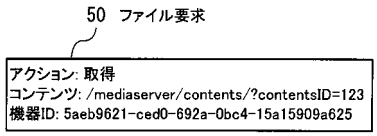
【図３１】



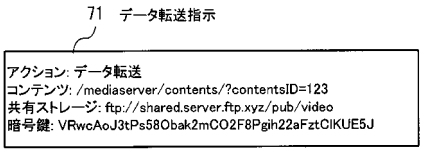
【図３２】



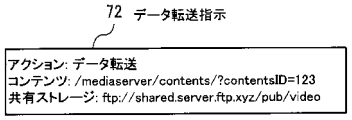
【図３３】



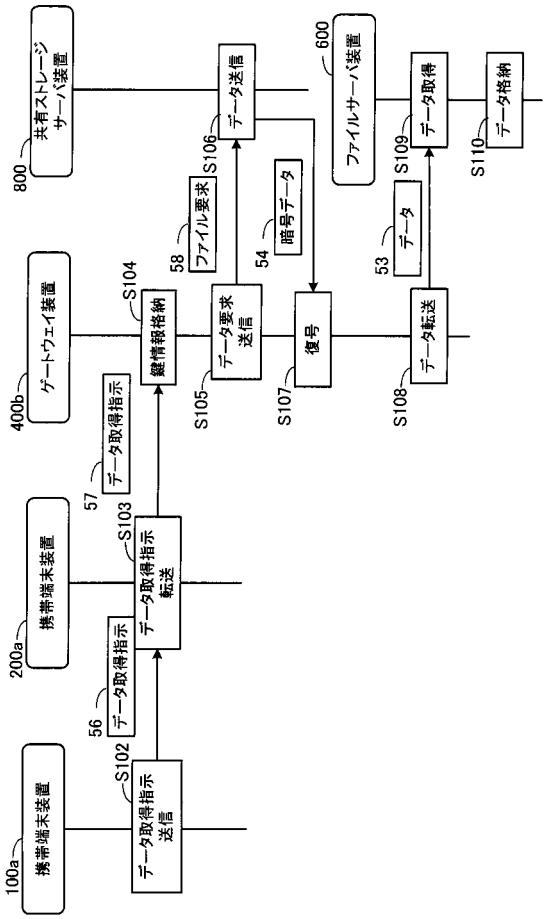
【図３４】



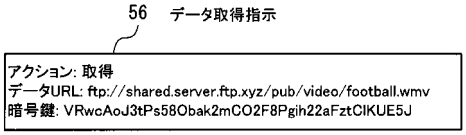
【図３５】



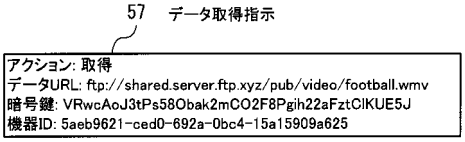
【図３６】


共有ストレージサーバ装置
800
データ送信
S106
ファイル要求
58
暗号データ
54
ファイルサーバ装置
600
データ取得
S109
データ
53
データ格納
S110
ゲートウェイ装置
400b
S104
鍵情報格納
データ要求送信
S105
復号
S107
データ転送
S108
データ取得指示
57
携帯端末装置
200a
S103
データ取得指示転送
データ取得指示
56
携帯端末装置
100a
S102
データ取得指示送信

【図３７】


56 データ取得指示
アクション: 取得
データURL: ftp://shared.server.ftp.xyz/pub/video/football.wmv
暗号鍵: VRwcAoJ3tPs58Obak2mCO2F8Pgih22aFztCIKUE5J

【図３８】


57 データ取得指示
アクション: 取得
データURL: ftp://shared.server.ftp.xyz/pub/video/football.wmv
暗号鍵: VRwcAoJ3tPs58Obak2mCO2F8Pgih22aFztCIKUE5J
機器ID: 5aeb9621-ced0-692a-0bc4-15a15909a625

フロントページの続き

(51)Int.Cl. FI
H04L 12/66 B

(72)発明者 福田 茂紀
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内

審査官 金沢 史明

(56)参考文献 特開平１１－２３７９６９（ＪＰ，Ａ）
特開２００１－１０３２３３（ＪＰ，Ａ）
特開２００５－３４８１６４（ＪＰ，Ａ）
特開２００６－２２１６０２（ＪＰ，Ａ）
国際公開第２００６／０２５２４１（WO，Ａ１）
米国特許出願公開第２００７／０２８８５５１（ＵＳ，Ａ１）
特開平０８－３３５２０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８