

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6524635号  
(P6524635)

(45) 発行日 令和1年6月5日(2019.6.5)

(24) 登録日 令和1年5月17日(2019.5.17)

(51) Int.Cl. F I  
**G06F 21/62 (2013.01)** G O 6 F 21/62 3 0 9  
**G06F 12/00 (2006.01)** G O 6 F 12/00 5 3 7 A

請求項の数 15 (全 28 頁)

(21) 出願番号	特願2014-212729 (P2014-212729)	(73) 特許権者	000006747 株式会社リコー
(22) 出願日	平成26年10月17日(2014.10.17)		東京都大田区中馬込1丁目3番6号
(65) 公開番号	特開2015-111405 (P2015-111405A)	(74) 代理人	100107766 弁理士 伊東 忠重
(43) 公開日	平成27年6月18日(2015.6.18)		
審査請求日	平成29年10月10日(2017.10.10)	(74) 代理人	100070150 弁理士 伊東 忠彦
(31) 優先権主張番号	特願2013-230547 (P2013-230547)	(72) 発明者	渡辺 太一 東京都大田区中馬込1丁目3番6号 株式 会社リコー内
(32) 優先日	平成25年11月6日(2013.11.6)	(72) 発明者	木村 純 東京都大田区中馬込1丁目3番6号 株式 会社リコー内
(33) 優先権主張国	日本国(JP)	審査官	上島 拓也

最終頁に続く

(54) 【発明の名称】 情報蓄積システム及び情報蓄積方法

(57) 【特許請求の範囲】

【請求項1】

2以上の情報処理装置と、情報蓄積装置とが接続された情報蓄積システムであって、  
 第1の情報処理装置からの要求に基づき、該第1の情報処理装置以外の他の情報処理装置からのアクセスが制限されている前記情報蓄積装置の所定の記憶領域にアクセスするためのアクセス情報を生成するアクセス情報生成手段と、

前記アクセス情報を前記第1の情報処理装置に表示させる表示手段と、

前記情報蓄積装置が、前記アクセス情報生成手段で生成したアクセス情報を、該アクセス情報の第1の有効期限に関する情報と関連付けて保存する保存手段と、

第2の情報処理装置が、前記第1の情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を前記情報蓄積装置に送信する送信手段と、

10

前記情報蓄積装置が、前記第2の情報処理装置から送信されたアクセス情報と、前記保存手段に保存されているアクセス情報とに基づき、前記第2の情報処理装置に対し前記所定の記憶領域へのアクセスを許可するアクセス手段と、

前記情報蓄積装置が、前記第1の情報処理装置から送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する更新手段と、

を有し、

前記アクセス手段は、

前記第1の有効期限が経過している場合、前記第2の情報処理装置に対し前記所定の記

20

憶領域へのアクセスを許可せず、

前記更新手段は、

前記第1の情報処理装置から定期的に送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する情報蓄積システム。

【請求項2】

前記アクセス手段は、

前記第2の情報処理装置から送信されたアクセス情報と、前記保存手段に保存されているアクセス情報とに基づき、前記第2の情報処理装置に対して前記所定の記憶領域へのアクセスを許可するか否かを判定し、前記第2の情報処理装置に対して前記所定の記憶領域へのアクセスを許可すると判定したとき、前記保存手段に保存されている前記アクセス情報を削除する、請求項1記載の情報蓄積システム。

10

【請求項3】

前記保存手段は、

前記アクセス情報と、該アクセス情報で前記所定の記憶領域にアクセス可能な回数を示すアクセス回数に関する情報を関連付けて保存し、

前記アクセス手段は、

前記アクセス回数が超過している場合、前記第2の情報処理装置に対し前記所定の記憶領域へのアクセスを許可しない、請求項1又は2に記載の情報蓄積システム。

20

【請求項4】

前記保存手段は、

前記アクセス情報と、該アクセス情報の第2の有効期限に関する情報を関連付けて保存し、

前記アクセス手段は、

前記第2の有効期限が経過している場合、前記第2の情報処理装置に対し前記所定の記憶領域へのアクセスを許可しない、請求項1ないし3のいずれか1項に記載の情報蓄積システム。

【請求項5】

前記更新要求は、前記第1の情報処理装置が非接触型の所定の記録媒体を読み取ることにより送信される、請求項1記載の情報蓄積システム。

30

【請求項6】

前記保存手段は、

前記アクセス情報と、前記第1の情報処理装置が非接触型の第1の記録媒体から取得した該第1の記録媒体の識別情報とを関連付けて保存し、

前記アクセス手段は、

前記第2の情報処理装置が非接触型の第2の記録媒体から取得した該第2の記録媒体の識別情報と、前記アクセス情報と、前記第1の記録媒体の識別情報とに基づき、前記第2の情報処理装置に対し前記所定の記憶領域へのアクセスを許可するか否かを判定する、請求項1ないし4のいずれか1項に記載の情報蓄積システム。

【請求項7】

前記記録媒体は、RFID又はNFCである、請求項5又は6に記載の情報蓄積システム。

40

【請求項8】

前記情報蓄積システムは、1以上の電子機器を含み、

前記保存手段は、

さらに、前記アクセス情報と、前記電子機器毎の該アクセス情報の第3の有効期限に関する情報を関連付けて保存し、

前記アクセス手段は、

前記第1の有効期限が経過している場合、前記所定の記憶領域に格納されている所定のファイルを前記第2の情報処理装置に対して送信するための前記所定の記憶領域へのアク

50

セスを許可せず、

前記第3の有効期限が経過している場合、前記所定の記憶領域に格納されている所定のファイルを前記電子機器に対して送信するための前記所定の記憶領域へのアクセスを許可しない、請求項1ないし7のいずれか1項に記載の情報蓄積システム。

【請求項9】

前記アクセス情報は、前記記憶領域に格納されているファイルの格納先に関する情報を含み、

前記アクセス手段は、

前記送信されたアクセス情報と該アクセス情報に含まれるファイルの格納先に関する情報に基づき、前記第2の情報処理装置に対し前記所定の記憶領域へのアクセスを許可した場合、前記所定の記憶領域に格納されている前記ファイルを送信する、請求項1ないし8のいずれか1項に記載の情報蓄積システム。

10

【請求項10】

前記表示手段は、

前記アクセス情報に基づきコード情報を生成し、該コード情報を前記第1の情報処理装置に表示させ

前記第2の情報処理装置は、前記第1の情報処理装置に表示されたコード情報から前記アクセス情報を取得する、請求項1ないし9のいずれか1項に記載の情報蓄積システム。

【請求項11】

前記コード情報は、QRコードである、請求項10記載の情報蓄積システム。

20

【請求項12】

2以上の情報処理装置に搭載されるアプリケーションと、情報蓄積装置とが接続された情報蓄積システムであって、

第1の情報処理装置に搭載されるアプリケーションからの要求に基づき、前記情報蓄積装置の前記第1の情報処理装置に搭載されるアプリケーション以外の他の情報処理装置に搭載されるアプリケーションからのアクセスが制限されている所定の記憶領域にアクセスするためのアクセス情報を生成するアクセス情報生成手段と、

前記アクセス情報を前記第1の情報処理装置に表示させる表示手段と、

前記情報蓄積装置が、前記アクセス情報生成手段で生成したアクセス情報を、該アクセス情報の第1の有効期限に関する情報と関連付けて保存する保存手段と、

30

第2の情報処理装置に搭載されるアプリケーションが、前記第1の情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を送信する送信手段と、

前記情報蓄積装置が、前記第2の情報処理装置に搭載されるアプリケーションから送信されたアクセス情報と、前記保存手段に保存されているアクセス情報とに基づき、前記第2の情報処理装置に搭載されるアプリケーションに対し前記所定の記憶領域へのアクセスを許可するアクセス手段と、

前記情報蓄積装置が、前記第1の情報処理装置から送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する更新手段と、

を有し、

40

前記アクセス手段は、

前記第1の有効期限が経過している場合、前記第2の情報処理装置に搭載されるアプリケーションに対し前記所定の記憶領域へのアクセスを許可せず、

前記更新手段は、

前記第1の情報処理装置から定期的に送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する、情報蓄積システム。

【請求項13】

情報処理装置と、1以上の他の情報処理装置とが接続された情報蓄積システムであって、

50

前記情報処理装置からの要求に基づき、前記他の情報処理装置からのアクセスが制限されている所定の記憶領域にアクセスするためのアクセス情報を生成するアクセス情報生成手段と、

前記アクセス情報を前記情報処理装置に表示させる表示手段と、

前記アクセス情報生成手段で生成したアクセス情報を、該アクセス情報の第1の有効期限に関する情報と関連付けて保存する保存手段と、

前記他の情報処理装置が、前記情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を送信する送信手段と、

前記送信されたアクセス情報と、前記保存手段に保存されているアクセス情報とに基づき、前記他の情報処理装置に対し前記所定の記憶領域へのアクセスを許可するアクセス手段と、

10

前記情報処理装置から送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する更新手段と、

を有し、

前記アクセス手段は、

前記第1の有効期限が経過している場合、前記他の情報処理装置に対し前記所定の記憶領域へのアクセスを許可せず、

前記更新手段は、

前記情報処理装置から定期的に送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する、情報蓄積システム。

20

#### 【請求項14】

情報処理装置に搭載されるアプリケーションと、1以上の他の情報処理装置に搭載されるアプリケーションとが接続された情報蓄積システムであって、

前記情報処理装置に搭載されるアプリケーションからの要求に基づき、前記他の情報処理装置に搭載されるアプリケーションからのアクセスが制限されている所定の記憶領域にアクセスするためのアクセス情報を生成するアクセス情報生成手段と、

前記アクセス情報を前記情報処理装置に表示させる表示手段と、

前記アクセス情報生成手段で生成したアクセス情報を、該アクセス情報の第1の有効期限に関する情報と関連付けて保存する保存手段と、

30

前記他の情報処理装置に搭載されるアプリケーションが、前記情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を送信する送信手段と、

前記送信されたアクセス情報と、前記保存手段に保存されているアクセス情報とに基づき、前記他の情報処理装置に搭載されるアプリケーションに対し前記所定の記憶領域へのアクセスを許可するアクセス手段と、

前記情報処理装置から送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する更新手段と、

を有し、

前記アクセス手段は、

前記第1の有効期限が経過している場合、前記他の情報処理装置に搭載されるアプリケーションに対し前記所定の記憶領域へのアクセスを許可せず、

40

前記更新手段は、

前記情報処理装置から定期的に送信される前記第1の有効期限に関する情報の更新要求に応じて、前記保存手段に保存された前記第1の有効期限に関する情報を更新する、情報蓄積システム。

#### 【請求項15】

2以上の情報処理装置と、情報蓄積装置とが接続された情報蓄積システムにおける情報蓄積方法であって、

第1の情報処理装置からの要求に基づき、該第1の情報処理装置以外の他の情報処理装置からのアクセスが制限されている前記情報蓄積装置の所定の記憶領域にアクセスするた

50

めのアクセス情報を生成するアクセス情報生成手順と、

前記アクセス情報を前記第 1 の情報処理装置に表示させる表示手順と、

前記情報蓄積装置が、前記アクセス情報生成手順で生成したアクセス情報を、該アクセス情報の第 1 の有効期限に関する情報と関連付けて保存する保存手順と、

第 2 の情報処理装置が、前記第 1 の情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を前記情報蓄積装置に送信する送信手順と、

前記情報蓄積装置が、前記第 2 の情報処理装置から送信されたアクセス情報と、前記保存手順で保存されたアクセス情報とに基づき、前記第 2 の情報処理装置に対し前記所定の記憶領域へのアクセスを許可するアクセス手順と、

前記情報蓄積装置が、前記第 1 の情報処理装置から送信される前記第 1 の有効期限に関する情報の更新要求に応じて、前記保存手順で保存された前記第 1 の有効期限に関する情報を更新する更新手順と、

を有し、

前記アクセス手順は、

前記第 1 の有効期限が経過している場合、前記第 2 の情報処理装置に対し前記所定の記憶領域へのアクセスを許可せず、

前記更新手順は、

前記第 1 の情報処理装置から定期的に送信される前記第 1 の有効期限に関する情報の更新要求に応じて、前記保存手順で保存された前記第 1 の有効期限に関する情報を更新する  
情報蓄積方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報蓄積システム及び情報蓄積方法に関する。

【背景技術】

【0002】

ファイルやフォルダにアクセス権を予め付与し、複数のユーザ間でファイルの共有を行うことができるファイルサーバが従来より知られている（例えば特許文献 1 参照）。

【発明の概要】

【発明が解決しようとする課題】

【0003】

しかしながら、上記の従来技術においては、複数のユーザ間でファイルの共有を行うためには、ファイルやフォルダにアクセス権を予め付与する必要がある。したがって、例えば外出先などにおいてファイルの共有を行うことが必要になった場合、外出先からファイルやフォルダにアクセス権を付与する必要があり、セキュリティ上問題があった。

【0004】

本発明の一実施形態は、上記の点に鑑みてなされたもので、所定の情報処理装置以外はアクセスが許可されていない所定の記憶領域に対して、予めアクセスを許可することなく他の情報処理装置にアクセスさせることができる情報蓄積システム及び情報蓄積方法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】

【0005】

上記の目的を達成するため、本願請求項 1 は、2 以上の情報処理装置と、情報蓄積装置とが接続された情報蓄積システムであって、第 1 の情報処理装置からの要求に基づき、該第 1 の情報処理装置以外の情報処理装置からのアクセスが制限されている前記情報蓄積装置の所定の記憶領域にアクセスするためのアクセス情報を生成するアクセス情報生成手段と、前記アクセス情報を前記第 1 の情報処理装置に表示させる表示手段と、第 2 の情報処理装置が、前記第 1 の情報処理装置に表示された前記アクセス情報を取得し、該アクセス情報を前記情報蓄積装置に送信する送信手段と、前記情報蓄積装置が、前記第 2 の情報処理装置から送信されたアクセス情報に基づき、前記第 2 の情報処理装置に対し前記所定の

10

20

30

40

50

記憶領域へのアクセスを許可するアクセス手段と、を有することを特徴とする。

【発明の効果】

【0006】

本発明の一実施形態によれば、所定の情報処理装置以外はアクセスが許可されていない所定の記憶領域に対して、予めアクセスを許可することなく他の情報処理装置にアクセスさせることができる。

【図面の簡単な説明】

【0007】

【図1】第1の実施形態に係る情報蓄積システムの一例の構成図である。

【図2】第1の実施形態の利用シーンの一例を説明する図である。

10

【図3】第1の実施形態に係る情報蓄積装置の一例のハードウェア構成図である。

【図4】第1の実施形態に係る携帯端末装置の一例のハードウェア構成図である。

【図5】第1の実施形態に係る情報蓄積装置の一例の処理ブロック図である。

【図6】第1の実施形態に係る携帯端末装置の一例の処理ブロック図である。

【図7】第1の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【図8】アクセスキーの取得方法を示した一例の説明図である。

【図9】QRコードの一例のイメージ図である。

【図10】QRコードの情報の一例の説明図である。

【図11】アクセスキーの認証方法を示した一例の説明図である。

20

【図12】ファイル取得要求に含まれる情報を示した一例の説明図である。

【図13】第1の実施形態に係る情報蓄積装置におけるアクセスキー認証処理の一例のフローチャートである。

【図14】第2の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【図15】第3の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【図16】第4の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【図17】第5の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

30

【図18】第6の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【図19】第7の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【発明を実施するための形態】

【0008】

次に、本発明の実施の形態について、詳細に説明する。

【0009】

[第1の実施形態]

40

<システム構成>

図1は、第1の実施形態に係る情報蓄積システムの一例の構成図である。図1の情報蓄積システム1は、情報蓄積装置10、一台以上の携帯端末装置20、一台以上のMFP(Multi Function Peripheral)30、一台以上のプロジェクタ40がLAN(Local Area Network)などのネットワークN1に接続される構成を一例として示している。

【0010】

ネットワークN1は例えば企業内ネットワークなど、プライベート環境のネットワークを利用できる。

【0011】

情報蓄積装置10は、携帯端末装置20からアクセス可能なファイルなどを記憶するコ

50

ンピュータシステムである。情報蓄積装置 10 は、携帯端末装置 20 のユーザ毎にアクセス制限が設定可能なファイルシステム等を用いてファイルなどを記憶している。また、情報蓄積装置 10 は、携帯端末装置 20 からの要求に応じて、後述するアクセスキーの生成や受信したアクセスキーの認証などを行う。なお、情報蓄積装置 10 は複数のコンピュータに分散して構成するようにしてもよい。

#### 【0012】

携帯端末装置 20 はユーザが携帯して操作する情報処理装置の一例である。情報処理装置は、スマートフォンやタブレット端末、携帯電話、ノート PC など、ユーザが携帯して操作できる装置であればよい。携帯端末装置 20 は、情報蓄積装置 10 にアクセスして、情報蓄積装置 10 に記憶しているファイルなどを操作（読み取り、書き込み等）することができる。また、携帯端末装置 20 は、後述するように、情報蓄積装置 10 から取得したアクセスキーに基づいて QR コード（登録商標）を生成し、携帯端末装置 20 のディスプレイなどに表示させる。また、携帯端末装置 20 は、他の携帯端末装置 20 のディスプレイなどに表示された QR コードをカメラなどで読み取ることができる。なお、二台以上の携帯端末装置 20 を各々区別して記載するときは、携帯端末装置 20 a、携帯端末装置 20 b などと記載する。なお、QR コードは、マトリックス型二次元コードである。

10

#### 【0013】

MFP30 は、撮像機能、画像形成機能及び通信機能を備え、プリンタ、ファクシミリ、スキャナ、複写機として利用可能である。

#### 【0014】

プロジェクタ 40 は、投影機能及び通信機能を備える。

20

#### 【0015】

なお、上記情報蓄積システム 1 は、一例であって、上記以外の各種電子機器を含む構成でもよい。各種電子機器は、例えば、電子黒板（インタラクティブホワイトボード）やテレビ会議端末、カメラ、マイク、モニタ等である。

#### 【0016】

ここで、本実施形態に係る情報蓄積システム 1 の利用シーンについて説明する。図 2 は、本実施形態の利用シーンの一例を説明する図である。ユーザ A は携帯端末装置 20 a を用いて情報蓄積装置 10 にアクセスし、例えば個人フォルダに格納されたファイルを携帯端末装置 20 a に表示しているものとする。ユーザ A の個人フォルダにはアクセス制限が設定されており、ユーザ A の携帯端末装置 20 a 以外からはアクセスすることができない。

30

#### 【0017】

このとき、ユーザ A の携帯端末装置 20 a に表示されているファイルを、ユーザ B の携帯端末装置 20 b に表示させる（携帯端末装置 20 a と携帯端末装置 20 b でファイルの共有を行う）場合について説明する。

#### 【0018】

まず、ユーザ A の携帯端末装置 20 a は、表示しているファイルのアクセスキーの取得要求を情報蓄積装置 10 に行う。情報蓄積装置 10 は、アクセスキーを生成し、携帯端末装置 20 a に送信する。次に、携帯端末装置 20 a は、取得したアクセスキーをユーザ B の携帯端末装置 20 b に渡す。ユーザ B の携帯端末装置 20 b は、この取得したアクセスキーを情報蓄積装置 10 に送信することで、ユーザ A の携帯端末装置 20 a が表示しているファイルを取得することができる。すなわち、本実施形態に係る情報蓄積システム 1 は、情報蓄積装置 10 のアクセス制限が設定されている記憶領域に格納されているファイル等について、当該記憶領域にアクセス可能とするアクセスキーを取得することでファイルの共有等を行うことができる。なお、アクセスキーは、所定の記憶領域にアクセスするためのアクセス情報の一例である。

40

#### 【0019】

<ハードウェア構成>

情報蓄積装置 10

50

情報蓄積装置 10 は例えば図 3 に示すハードウェア構成の情報蓄積装置により実現される。図 3 は、第 1 の実施形態に係る情報蓄積装置の一例のハードウェア構成図である。

【 0 0 2 0 】

図 3 の情報蓄積装置 10 は、入力装置 101、表示装置 102、外部 I / F 103、RAM 104、ROM 105、CPU 106、通信 I / F 107、及び HDD 108などを備え、それぞれがバス B1 で相互に接続されている。

【 0 0 2 1 】

入力装置 101 はキーボードやマウスなどを含み、情報蓄積装置 10 に各操作信号を入力するのに用いられる。表示装置 102 はディスプレイなどを含み、情報蓄積装置 10 による処理結果を表示する。なお、入力装置 101 及び / 又は表示装置 102 は、情報蓄積装置 10 の必須の構成ではないため、なくてもよい。

10

【 0 0 2 2 】

通信 I / F 107 は情報蓄積装置 10 をネットワーク N1 に接続するインターフェースである。これにより、情報蓄積装置 10 は通信 I / F 107 を介して、他の装置、機器とデータ通信を行うことができる。

【 0 0 2 3 】

HDD 108 は、プログラムやデータを格納している不揮発性の記憶装置である。格納されるプログラムやデータには、情報蓄積装置 10 全体を制御する基本ソフトウェアである OS (Operating System)、及び、OS 上において各種機能を提供するアプリケーションソフトウェアなどがある。また、HDD 108 は、格納しているプログラムやデータを、所定のファイルシステム及び / 又は DB (Data Base) により管理している。

20

【 0 0 2 4 】

外部 I / F 103 は、外部装置とのインターフェースである。外部装置には、記録媒体 103a などがある。これにより、情報蓄積装置 10 は外部 I / F 103 を介して、記録媒体 103a の読み取り及び / 又は書き込みを行うことができる。なお、記録媒体 103a にはフレキシブルディスク、CD、DVD (Digital Versatile Disk)、SD メモリカード (SD Memory card)、USB メモリ (Universal Serial Bus memory) 等がある。

【 0 0 2 5 】

ROM 105 は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリ (記憶装置) である。ROM 105 には、情報蓄積装置 10 の起動時に実行される BIOS (Basic Input/Output System)、OS 設定、及びネットワーク設定などのプログラムやデータが格納されている。RAM 104 は、プログラムやデータを一時保持する揮発性の半導体メモリ (記憶装置) である。

30

【 0 0 2 6 】

CPU 106 は、ROM 105 や HDD 108 などの記憶装置からプログラムやデータを RAM 104 上に読み出し、処理を実行することで、情報蓄積装置 10 全体の制御や機能を実現する演算装置である。

【 0 0 2 7 】

本実施形態に係る情報蓄積装置 10 は、上記ハードウェア構成により、後述するような各種処理を実現できる。

40

【 0 0 2 8 】

携帯端末装置 20

携帯端末装置 20 は例えば図 4 に示すハードウェア構成の携帯端末装置により実現される。図 4 は、第 1 の実施形態に係る携帯端末装置の一例のハードウェア構成図である。

【 0 0 2 9 】

図 4 の携帯端末装置 20 は、入力装置 201、表示装置 202、外部 I / F 203、RAM 204、ROM 205、CPU 206、通信 I / F 207、HDD 208、及びカメラ装置 209などを備え、それぞれがバス B2 で相互に接続されている。なお、記録媒体 203a には、RFID (Radio Frequency Identifier) タグ若しくは NFC (Near field communication) タグ又はこれらを含むカード (RFID カード、NFC カード) 等が

50



含まれる。したがって、携帯端末装置 20 は、外部 I / F 203 を介して、RFID タグや NFC タグ等に格納されている情報の読み取り及び / 又は書き込みを行うことができる。

#### 【0030】

入力装置 201、表示装置 202、外部 I / F 203、RAM 204、ROM 205、CPU 206、通信 I / F 207、及び HDD 208 は、それぞれ入力装置 101、表示装置 102、外部 I / F 103、RAM 104、ROM 105、CPU 106、通信 I / F 107、及び HDD 108 と同様の説明を省略する。

#### 【0031】

カメラ装置 209 は、撮像素子で撮影した被写体を画像データなどにするカメラなどである。なお、カメラ装置 209 は、静止画撮影及び / 又は動画撮影が可能であればよい。

10

#### 【0032】

本実施形態に係る携帯端末装置 20 は、上記ハードウェア構成により、後述するような各種処理を実現できる。

#### 【0033】

<ソフトウェア構成>

情報蓄積装置 10

本実施形態に係る情報蓄積装置 10 は例えば図 5 に示す処理ブロックで実現される。図 5 は、第 1 の実施形態に係る情報蓄積装置の一例の処理ブロック図である。情報蓄積装置 10 はプログラムを実行することで、OS 110、Web サーバ 111、共有フォルダ 112、ドキュメント管理 113、PC ブラウザ用 UI 114、MFP 用 UI 115、Web API 116、Web 制御 117、認証管理 118、設定情報管理 119 を実現している。

20

#### 【0034】

OS 110 は、情報蓄積装置 10 のオペレーティングシステムであり、システム全体を制御する。OS 110 は、例えば Windows (登録商標)、Linux (登録商標) などである。

#### 【0035】

Web サーバ 111 は、HTTP (Hyper Text Transfer Protocol) で情報を送受信するソフトウェアである。Web サーバ 111 は、例えば Apache Tomcat や IIS (登録商標) などである。

30

#### 【0036】

共有フォルダ 112 は、SMB (Server Message Block) プロトコルによってネットワーク N1 上で公開されたフォルダである。ユーザは携帯端末装置 20 などの情報処理装置を用いて、共有フォルダ 112 にアクセスできる。

#### 【0037】

ドキュメント管理 113 は、共有フォルダ 112 に置かれたファイルを管理し、Web 制御 117 からの要求に応じてデータ変換する処理を行う。

#### 【0038】

PC ブラウザ用 UI 114 は、HTTP のリクエストにより情報蓄積装置 10 の設定画面を表示させる。ユーザは例えば PC の Web ブラウザを使用して、情報蓄積装置 10 の各種設定の変更を行うことができる。

40

#### 【0039】

MFP 用 UI 115 は、HTTP のリクエストにより印刷画面、スキャン画面を表示させる。ユーザは例えば MFP のブラウザ機能を使用して、MFP の印刷やスキャン操作を行うことができる。

#### 【0040】

Web API 116 は、HTTP のリクエストを受け付け、このリクエストに応じた処理を行う。Web API 116 は、処理結果に対するレスポンスを行う。Web API 116 は、例えば関数やクラス等により構成される。

50

## 【 0 0 4 1 】

また、情報蓄積装置 1 0 の Web A P I 1 1 6 を S D K (ソフトウェア開発キット)として情報処理装置に搭載されるアプリケーションの開発者に提供できる。アプリケーションの開発者は S D K を使用してアプリケーションを開発できる。S D K は情報蓄積装置 1 0 の提供者以外のサードベンダにも提供できる。サードベンダは提供された S D K を使用してアプリケーションを開発できる。S D K を使用して開発されたアプリケーションは情報処理装置に搭載できる。

## 【 0 0 4 2 】

情報蓄積装置 1 0 の Web A P I 1 1 6 を S D K として提供することにより、情報処理装置は情報蓄積装置 1 0 の提供者が開発したアプリケーションだけでなく、サードベンダが開発したアプリケーションも搭載できるようになる。

10

## 【 0 0 4 3 】

認証管理 1 1 8 は、Web A P I 1 1 6 が受け付けた H T T P のリクエストが正当なユーザからのリクエストか否か判別を行う。すなわち、認証管理 1 1 8 は、H T T P のリクエストに含まれる認証情報に基づき、ユーザ認証を行う。また、認証管理 1 1 8 は、携帯端末装置 2 0 からの要求に応じて、携帯端末装置 2 0 が表示しているファイルにアクセスするためのアクセスキーの生成を行う。

## 【 0 0 4 4 】

設定情報管理 1 1 9 は、情報蓄積システム 1 に接続されている各種電子機器の機器情報やユーザ設定の管理を行う。

20

## 【 0 0 4 5 】

## 携帯端末装置 2 0

本実施形態に係る携帯端末装置 2 0 は例えば図 6 に示す処理ブロックで実現される。図 6 は、第 1 の実施形態に係る携帯端末装置の一例の処理ブロック図である。携帯端末装置 2 0 はプログラムを実行することで、OS 2 1 0、情報蓄積装置通信部 2 1 1、印刷管理部 2 1 2、プロジェクト管理部 2 1 3、ファイル一覧表示部 2 1 4、アップロード画面表示部 2 1 5、設定画面表示部 2 1 6、プレビュー画面表示部 2 1 7、認証情報管理部 2 1 8、コード情報処理部 2 1 9 を実現している。

## 【 0 0 4 6 】

OS 2 1 0 は、携帯端末装置 2 0 のオペレーティングシステムであり、システム全体を制御する。OS 2 1 0 は、例えば i O S、A n d r o i d (登録商標)、W i n d o w s P h o n e、B l a c k B e r r y などである。

30

## 【 0 0 4 7 】

情報蓄積装置通信部 2 1 1 は、情報蓄積装置 1 0 の Web A P I 1 1 6 と H T T P で情報を送受信する。情報蓄積装置通信部 2 1 1 は、情報蓄積装置 1 0 と情報を送受信する際に、認証情報管理部 2 1 8 で管理している認証情報を H T T P に付加する。なお、認証情報管理部 2 1 8 は、認証情報として例えばユーザ I D とパスワードの組を管理している。

## 【 0 0 4 8 】

なお、ファイル一覧表示部 2 1 4、アップロード画面表示部 2 1 5、設定画面表示部 2 1 6 は、情報蓄積装置通信部 2 1 1 を利用して情報蓄積装置 1 0 に記憶されている情報の取得や情報蓄積装置 1 0 に対する処理要求を行う。

40

## 【 0 0 4 9 】

印刷管理部 2 1 2 は、情報蓄積システム 1 に接続されている M F P の検索を行う。印刷管理部 2 1 2 は、情報蓄積装置 1 0 に M F P の登録を行う。また、印刷管理部 2 1 2 は、情報蓄積装置 1 0 に格納されているファイルについて、情報蓄積システム 1 に接続されている M F P に送信し、印刷処理を要求する。

## 【 0 0 5 0 】

プロジェクト管理部 2 1 3 は、情報蓄積システム 1 に接続されているプロジェクトの検索を行う。プロジェクト管理部 2 1 3 は、情報蓄積装置 1 0 にプロジェクトの登録を行う。また、プロジェクト管理部 2 1 3 は、情報蓄積装置 1 0 に格納されているファイルにつ

50

いて、情報蓄積システム 1 に接続されているプロジェクタに送信し、投影処理を要求する。

【 0 0 5 1 】

ファイル一覧表示部 2 1 4 は、情報蓄積装置 1 0 に格納されているファイルの一覧を携帯端末装置 2 0 の表示装置 2 0 2 に表示させる。ファイル一覧表示部 2 1 4 が表示させるファイルの一覧は、例えばユーザが携帯端末装置 2 0 を用いてアクセス可能なフォルダ（アクセス権限が付与されているフォルダ）に格納されているファイルの一覧などである。

【 0 0 5 2 】

アップロード画面表示部 2 1 5 は、情報蓄積装置 1 0 にファイルをアップロードする（情報蓄積装置 1 0 の記憶領域にファイルを格納させる）メニュー画面を携帯端末装置 2 0 の表示装置 2 0 2 に表示させる。また、アップロード画面表示部 2 1 5 は、情報蓄積装置通信部 2 1 1 を利用してファイルを情報蓄積装置 1 0 にアップロードする。

10

【 0 0 5 3 】

なお、情報蓄積装置 1 0 にファイルをアップロードする方法は、携帯端末装置 2 0 の HDD 2 0 8 などに格納されているファイルをアップロードする他、例えば携帯端末装置 2 0 のカメラ装置 2 0 9 で撮影した画像データをアップロードする方法がある。また、例えば情報蓄積システム 1 に接続されている MFP の表示画面等に表示されている QR コードなどを携帯端末装置 2 0 で読み取ることにより、この MFP でスキャンしたデータをアップロードすることもできる。

【 0 0 5 4 】

20

設定画面表示部 2 1 6 は、情報蓄積装置 1 0 に携帯端末装置 2 0 の登録を行う画面を携帯端末装置 2 0 の表示装置 2 0 2 に表示させる。また、設定画面表示部 2 1 6 は、携帯端末装置 2 0 の設定情報を携帯端末装置 2 0 の表示装置 2 0 2 に表示させる。

【 0 0 5 5 】

プレビュー画面表示部 2 1 7 は、ファイル一覧表示部 2 1 4 が携帯端末装置 2 0 の表示装置 2 0 2 に表示させたファイルの一覧において、ユーザが選択したファイルのプレビュー画面を携帯端末装置 2 0 の表示装置 2 0 2 に表示させる。

【 0 0 5 6 】

コード情報処理部 2 1 9 は、携帯端末装置 2 0 のカメラ装置 2 0 9 により読み取ったコード情報を解析する。コード情報には、例えば QR コードがある。また、コード情報処理部 2 1 9 は、情報蓄積装置 1 0 の認証管理 1 1 8 が生成したアクセスキーからコード情報（例えば QR コード）を生成する。

30

【 0 0 5 7 】

< 処理の詳細 >

以下では、本実施形態に係る情報蓄積システム 1 の処理の詳細について説明する。

【 0 0 5 8 】

図 7 は、第 1 の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。

【 0 0 5 9 】

ユーザ A は携帯端末装置 2 0 a を操作して、情報蓄積装置 1 0 に対して、情報蓄積装置 1 0 に記憶されているファイルの取得要求を行う（ステップ S 1 1 ）。例えば携帯端末装置 2 0 a のファイル一覧表示部 2 1 4 が表示したファイルの一覧から選択することで、選択したファイルの取得要求を行うことができる。なお、選択したファイルは、ユーザ A の個人フォルダ（ユーザ A に対してのみアクセス権限が付与されているフォルダ）に格納されているファイルであるとする。なお、個人フォルダは、例えば共有フォルダ 1 1 2 において所定のユーザにのみアクセス権限を付与したフォルダである。なお、ファイルの取得要求は、例えば携帯端末装置 2 0 a の Web API 1 1 6 を介して HTTP のリクエストにより行うことができる。

40

【 0 0 6 0 】

情報蓄積装置 1 0 は、携帯端末装置 2 0 a に要求されたファイルを送信する（ステップ

50

S 1 2 )。このとき、情報蓄積装置 1 0 の認証管理 1 1 8 は、ユーザ A の携帯端末装置 2 0 a のユーザ認証を行う。例えば情報蓄積装置 1 0 が受信した H T T P のリクエストに付加された認証情報に基づきユーザ認証を行い、認証成功の場合、要求されたファイルを携帯端末装置 2 0 a に送信する。なお、情報蓄積装置 1 0 は認証失敗の場合、携帯端末装置 2 0 a にエラー情報を送信してもよい。

【 0 0 6 1 】

携帯端末装置 2 0 a は、ステップ S 1 2 において情報蓄積装置 1 0 から送信されたファイルを受信すると、表示装置 2 0 2 に受信したファイルの内容を表示させる。

【 0 0 6 2 】

ユーザ A は携帯端末装置 2 0 a を操作して、表示装置 2 0 2 に表示されているファイルの共有開始操作を行う (ステップ S 1 3 )。共有開始操作とは、携帯端末装置 2 0 a が表示しているファイルを他の携帯端末装置 2 0 で表示させるためのアクセスキーを取得するための操作である。なお、共有開始操作は、例えば携帯端末装置 2 0 a の表示装置 2 0 2 に表示されている所定のボタンなどを押下することで行うことができる。

【 0 0 6 3 】

携帯端末装置 2 0 a は、情報蓄積装置 1 0 に対して、アクセスキーの取得要求を行う (ステップ S 1 4 )。なお、このアクセスキー取得要求には、携帯端末装置 2 0 a が表示しているファイルのファイルパス (情報蓄積装置 1 0 におけるファイルの格納場所などのアドレス情報) を含む。情報蓄積装置 1 0 の認証管理 1 1 8 は、携帯端末装置 2 0 a からのアクセスキー取得要求に応じてアクセスキーを生成し (ステップ S 1 5 )、生成したアクセスキーを携帯端末装置 2 0 a に送信する (ステップ S 1 6 )。なお、情報蓄積装置 1 0 は、ステップ S 1 5 で生成したアクセスキーを情報蓄積装置 1 0 の記憶領域に保存する。

【 0 0 6 4 】

図 8 は、アクセスキーの取得方法を示した一例の説明図である。携帯端末装置 2 0 a は、ファイルパスを含むアクセスキー取得要求を情報蓄積装置 1 0 に対して行う。情報蓄積装置 1 0 は、アクセスキー取得要求に応じてアクセスキーを生成し、記憶領域にアクセスキーとアクセスキー取得要求に含まれるファイルパスを関連付けて保存する。そして、情報蓄積装置 1 0 は、生成したアクセスキーを携帯端末装置 2 0 a に送信する。なお、情報蓄積装置 1 0 は、ファイルパスの他、例えば経過時間もアクセスキーと関連付けて記憶領域に保存する。経過時間は、アクセスキーを生成してから経過した時間であり、この経過時間が予め設定された所定の時間を経過した場合、このアクセスキーは無効となる (アクセスキーが情報蓄積装置 1 0 の記憶領域から削除される)。なお、所定の時間は、アクセス情報の第 1 の有効期限の一例である。

【 0 0 6 5 】

次に、携帯端末装置 2 0 a のコード情報処理部 2 1 9 は、取得したアクセスキーを含む情報をコード情報に変換する (ステップ S 1 7 )。本実施形態ではコード情報処理部 2 1 9 は、アクセスキーを Q R コードに変換する。なお、コード情報は、Q R コードの他、例えば S P コード、C P コードなどでもよい。携帯端末装置 2 0 a は、Q R コードを表示装置 2 0 2 に表示させる (ステップ S 1 8 )。

【 0 0 6 6 】

図 9 は、Q R コードの一例のイメージ図である。携帯端末装置 2 0 a は、情報蓄積装置 1 0 から取得したアクセスキーから Q R コードを生成し、携帯端末装置 2 0 a の表示装置 2 0 2 に表示させる。

【 0 0 6 7 】

図 1 0 は、Q R コードの情報の一例の説明図である。携帯端末装置 2 0 a の表示装置 2 0 2 に表示された Q R コードをカメラ装置 2 0 9 などでも読み取り、所定の解析を行うことで例えばアクセスキー ( o n e T i m e A c c e s s K e y )、ファイルパス ( f i l e P a t h )、情報蓄積装置 1 0 の I P アドレス ( s e r v e r A d d r e s s ) を取得することができる。

【 0 0 6 8 】

次に、ユーザBの携帯端末装置20bは、携帯端末装置20aの表示装置202に表示されているQRコードを携帯端末装置20bのカメラ装置209に読み取る(ステップS19)。携帯端末装置20bのコード情報処理部219は、読み取ったQRコードを解析し、例えば図10に示した所定の情報(アクセスキー、ファイルパス、IPアドレス)を取得する(ステップS20)。そして、携帯端末装置20bは、情報蓄積装置10に対して、ステップS20で取得したアクセスキーとファイルパスを含むファイル取得要求を行う(ステップS21)。なお、このとき、携帯端末装置20bは、ファイル取得要求に携帯端末装置20bの機器情報(例えば携帯端末装置20bの所有者ID、機器ID、機器名称など)を付加する。

#### 【0069】

情報蓄積装置10の認証管理118は、受信したファイル取得要求に含まれるアクセスキーの経過時間を参照し、アクセスキーの生成から予め設定した所定の時間が経過しているか否かを判定する(ステップS22)。情報蓄積装置10の認証管理118は、アクセスキーの生成から予め設定した所定の時間が経過している場合、携帯端末装置20bに対して、ファイル取得失敗であることを示す情報を送信する。これにより、アクセスキーの生成から所定の時間以内に限りファイルの共有を認めることでセキュリティを確保することができる。

#### 【0070】

情報蓄積装置10の認証管理118は、受信したファイル取得要求に含まれるアクセスキーとファイルパスの組み合わせが正しいか否かを判定する(ステップS23)。すなわち、情報蓄積装置10の認証管理118は、受信したファイル取得要求に含まれるアクセスキーとファイルパスの組み合わせと、情報蓄積装置10の記憶領域に関連付けて保存されているアクセスキーとファイルパスの組み合わせが一致するか否かを判定する。情報蓄積装置10の認証管理118は、アクセスキーとファイルパスの組み合わせが一致しない場合(又は一致する組み合わせのアクセスキーとファイルパスが情報蓄積装置10の記憶領域に存在しない場合)、携帯端末装置20bに対して、ファイル取得失敗であることを示す情報を送信する。

#### 【0071】

情報蓄積装置10は、受信したファイル取得要求に含まれるファイルパスに指定されているファイルを携帯端末装置20bに送信する(ステップS24)。そして、情報蓄積装置10は、情報蓄積装置10の記憶領域に保存されているアクセスキーを削除する(ステップS25)。これにより、一度アクセスキーを用いてファイルの共有を行うと、同じアクセスキーを用いてファイルの共有を行うことができないのでセキュリティを確保することができる(すなわち、本実施形態におけるアクセスキーはワンタイムキーである)。

#### 【0072】

携帯端末装置20bは、情報蓄積装置10から受信したファイルを表示装置202に表示させる(ステップS26)。これにより、ユーザBの携帯端末装置20bは、アクセスキーを用いて、アクセス制限がされているユーザAの個人フォルダ内のファイルを共有表示することができる。

#### 【0073】

図11は、アクセスキーの認証方法を示した一例の説明図である。携帯端末装置20bは、ファイル取得要求に図12に示す情報を付加して情報蓄積装置10に送信する。図12は、ファイル取得要求に含まれる情報を示した一例の説明図である。ファイル取得要求には、例えばアクセスキー(one Time Access Key)、ファイルパス(file Path)、端末名称(device Name)、端末種類(device Type)、端末ID(device ID)が含まれる。端末名称はユーザが設定する端末の任意の名称である。端末種類は端末の製品名などである。端末IDは例えば端末のMAC(Media Access Control)アドレスなどである。次に、情報蓄積装置10は、ファイル取得要求に含まれる情報からアクセスキーの認証などを行う。また、情報蓄積装置10は、ファイルの共有者に関する情報として、各種端末情報を保存する。そして、情報蓄積装置10

10

20

30

40

50

は、ファイル取得要求に含まれるファイルパスに指定されたファイルを携帯端末装置 20b に送信する。

【0074】

次に、図 11 で説明したアクセスキーの認証方法について、処理の詳細を説明する。図 13 は、本実施形態に係る情報蓄積装置におけるアクセスキー認証処理の一例のフローチャートである。

【0075】

情報蓄積装置 10 の認証管理 118 は、携帯端末装置 20b からのファイル取得要求に含まれるアクセスキーと同一のアクセスキーが情報蓄積装置 10 の記憶領域に存在するかどうかを判定する（ステップ S31）。同一のアクセスキーが情報蓄積装置 10 の記憶領域に存在する場合、ステップ S32 に進む。

10

【0076】

情報蓄積装置 10 の認証管理 118 は、携帯端末装置 20b からのファイル取得要求に含まれるアクセスキーと同一のアクセスキーが情報蓄積装置 10 の記憶領域に存在する場合、該当のアクセスキーを記憶領域から取得する（ステップ S32）。なお、このとき、該当のアクセスキーを取得したら当該アクセスキーを情報蓄積装置 10 の記憶領域から削除する。これにより、一度アクセスキーを用いた場合、当該アクセスキーを無効とすることができる。

【0077】

情報蓄積装置 10 の認証管理 118 は、ファイル取得要求に含まれるアクセスキーの経過時間が所定の時間以内か否かを判定する（ステップ S33）。これにより、アクセスキーの取得後、所定の時間経過している場合、当該アクセスキーを無効とすることができ、セキュリティを確保することができる。経過時間が所定の時間以内である場合、ステップ S34 に進む。

20

【0078】

情報蓄積装置 10 の認証管理 118 は、ファイル取得要求に含まれるアクセスキーとファイルパスの組み合わせが、情報蓄積装置 10 の記憶領域から取得したアクセスキーとファイルパスの組み合わせと一致するか否かを判定する（ステップ S34）。これにより、不正なファイル取得要求を防止することができる。一致する場合、ステップ S35 に進む。

30

【0079】

情報蓄積装置 10 の認証管理 118 は、ファイル取得要求に含まれるファイルパスに指定されたファイルを携帯端末装置 20b に送信する（ステップ S35）。

【0080】

情報蓄積装置 10 の認証管理 118 は、ファイル取得要求に含まれる携帯端末装置 20b の機器情報を情報蓄積装置 10 の記憶領域に保存する（ステップ S36）。これにより、ユーザ A の携帯端末装置 20a が表示しているファイルの共有者やファイルを共有している端末に関する情報を保存することができる。

【0081】

以上により、本実施形態に係る情報蓄積システム 1 では、ユーザ A の携帯端末装置 20a に表示しているファイルをユーザ B の携帯端末装置 20b に表示させることができる。この方法として、ユーザ A は携帯端末装置 20a を操作して、アクセスキーを取得し、このアクセスキーをコード情報に変換し、表示装置 202 に表示させることができる。そして、ユーザ B の携帯端末装置 20b は、このコード情報をカメラ装置 209 に読み取り、解析することで、情報蓄積装置 10 に保存されているファイルを取得することができる。

40

【0082】

また、本実施形態に係る情報蓄積システム 1 では、携帯端末装置 20a 及び携帯端末装置 20b 間でファイルを共有するためのアクセスキーを情報蓄積装置 10 の記憶領域にも保存しておき、携帯端末装置 20b からアクセスキーの認証要求を受け付けると、記憶領域に保存しているアクセスキーを削除する。これにより、一つのアクセスキーは一回のみ

50

使用することができるため、セキュリティを確保することができる。また、アクセスキーの生成（発行）から所定の時間経過した場合は、情報蓄積装置 10 の記憶領域から当該アクセスキーを削除することで、このアクセスキーを無効とすることができる。

【0083】

[第2の実施形態]

次に、第2の実施形態に係る情報蓄積システム1について説明する。第2の実施形態に係る情報蓄積システム1は、アクセスキーの生成を携帯端末装置20で行うものである。

【0084】

なお、第2の実施形態に係る情報蓄積システム1は、システム構成、ハードウェア構成、及びソフトウェア構成が、第1の実施形態に係る情報蓄積システム1と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。

10

【0085】

<処理の詳細>

図14は、第2の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。なお、図14のシーケンス図におけるステップS41～S44及びS47～S56の処理は、それぞれ図7のシーケンス図におけるステップS11～S14及びS17～S26の処理と同様であるため、説明を省略する。

【0086】

ユーザAの携帯端末装置20aは、アクセスキーを生成し（ステップS45）、生成したアクセスキーを情報蓄積装置10に送信する（ステップS46）。なお、情報蓄積装置10は、携帯端末装置20aより取得したアクセスキーを記憶領域に保存する。

20

【0087】

以上により、第2の実施形態に係る情報蓄積システム1では、携帯端末装置20でアクセスキーを生成することができる。これにより、アクセスキーの生成に伴う情報蓄積装置10の処理負荷を分散することができる。従って、情報蓄積システム1に接続された複数の携帯端末装置20においてほぼ同時にアクセスキーを生成する場合においても情報蓄積装置10の処理が過大になることを防止することができる。

【0088】

[第3の実施形態]

次に、第3の実施形態に係る情報蓄積システム1について説明する。第3の実施形態に係る情報蓄積システム1は、アクセスキーに認証回数を含めたものである。つまり、一つのアクセスキーで所定回数の認証を行えるものである。

30

【0089】

なお、第3の実施形態に係る情報蓄積システム1は、システム構成、ハードウェア構成、及びソフトウェア構成が、第1の実施形態に係る情報蓄積システム1と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。

【0090】

<処理の詳細>

図15は、第3の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。なお、図15のシーケンス図におけるステップS61～S74及びS77の処理は、それぞれ図7のシーケンス図におけるステップS11～S24及びS26の処理と同様であるため、説明を省略する。

40

【0091】

情報蓄積装置10の認証管理118は、情報蓄積装置10の記憶領域に記憶されているアクセスキーに含まれる認証回数を更新する（ステップS75）。認証回数の更新は、例えば認証回数の値を1減じて更新する。

【0092】

情報蓄積装置10の認証管理118は、情報蓄積装置10の記憶領域に記憶されているアクセスキーに含まれる認証回数が0以下が否かを判断し、0以下である場合、記憶領域から当該アクセスキーを削除する（ステップS76）。

50

## 【 0 0 9 3 】

以上により、例えば複数台の携帯端末装置 2 0 間でファイルの共有を行う場合、当該台数に相当する認証回数を設定しておけば、これら複数台の携帯端末装置 2 0 間でファイルの共有を行うことができる。具体的には、例えば 3 台の携帯端末装置 2 0 間でファイルの共有を行う場合、認証回数を 2 に設定しておけばよい。

## 【 0 0 9 4 】

## 〔 第 4 の実施形態 〕

次に、第 4 の実施形態に係る情報蓄積システム 1 について説明する。第 4 の実施形態に係る情報蓄積システム 1 は、携帯端末装置 2 0 a が所定の画面を表示させている間に限り、携帯端末装置 2 0 b においてファイルの共有を行うものである。本実施形態に係る情報蓄積システム 1 の情報蓄積装置 1 0 は、アクセスキーと関連付けて、このアクセスキーの有効な時間を示す第 2 の有効期限が記憶領域に保存されている。本実施形態に係る情報蓄積システム 1 は、第 2 の有効期限を用いることで、携帯端末装置 2 0 a が所定の画面を表示させている間に限り、携帯端末装置 2 0 b においてファイルの共有を行う。

## 【 0 0 9 5 】

なお、第 4 の実施形態に係る情報蓄積システム 1 は、システム構成、ハードウェア構成、及びソフトウェア構成が、第 1 の実施形態に係る情報蓄積システム 1 と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。

## 【 0 0 9 6 】

## &lt; 処理の詳細 &gt;

図 1 6 は、第 4 の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。なお、図 1 6 のシーケンス図におけるステップ S 8 1 ~ S 9 5 の処理は図 7 のシーケンス図におけるステップ S 1 1 ~ S 2 6 の処理と同様であるため、説明を省略する。

## 【 0 0 9 7 】

ユーザ A の携帯端末装置 2 0 a は、携帯端末装置 2 0 b との間でファイルの共有を行うために所定の画面を表示させる。すると、携帯端末装置 2 0 a は、この所定の画面を表示している間、所定の間隔（例えば、1 秒ないし数秒程度の間隔）でアクセスキーの第 2 の有効期限の更新要求を情報蓄積装置 1 0 に送信する（ステップ S 9 6）。ここで、携帯端末装置 2 0 a が表示する所定の画面とは、この所定の画面を表示している間に限り携帯端末装置 2 0 b に対してファイルの共有を許可するための画面であり、例えば、ステップ S 8 8 で表示された Q R コードの表示画面や携帯端末装置 2 0 b と共有するファイルの表示画面等である。

## 【 0 0 9 8 】

情報蓄積装置 1 0 は、該当のアクセスキーの第 2 の有効期限の更新する（ステップ S 9 7）。すなわち、例えば、情報蓄積装置 1 0 は、該当のアクセスキーの第 2 の有効期限を延長（例えば、上記の所定の間隔と同じ秒数を延長）する更新を行う。

## 【 0 0 9 9 】

ユーザ B の携帯端末装置 2 0 b は、ステップ S 9 4 で取得したファイルを表示している間、所定の間隔毎に情報蓄積装置 1 0 に対して、該当のアクセスキーの第 2 の有効期限を経過しているか否かを確認する（ステップ S 9 8）。情報蓄積装置 1 0 は、該当のアクセスキーの第 2 の有効期限が経過していなければ、アクセスキーは有効であることを示す情報を応答し、携帯端末装置 2 0 b は、ファイルの表示を継続する（ステップ S 9 9）。

## 【 0 1 0 0 】

ここで、ユーザ A の携帯端末装置 2 0 a が所定の画面の表示を終了させた場合、該当のアクセスキーの第 2 の有効期限は更新されない。このため、情報蓄積装置 1 0 では、第 2 の有効期限が経過した場合、該当のアクセスキーを削除する（ステップ S 1 0 0）。したがって、上記のステップ S 9 8 で携帯端末装置 2 0 b が第 2 の有効期限が経過しているか否かを確認した際に、第 2 の有効期限が経過しており、該当のアクセスキーが削除されている場合、情報蓄積装置 1 0 は、携帯端末装置 2 0 b に対してアクセスキーは無効である

10

20

30

40

50



(存在しない)ことを示す情報を応答する(ステップS101)。すると、携帯端末装置20bは、ファイルの表示を終了させる(ステップS102)。

【0101】

以上により、第4の実施形態に係る情報蓄積システム1では、携帯端末装置20aが所定の画面を表示させている間、携帯端末装置20bでファイルを表示させるように制御することができる。これにより、携帯端末装置20bにおいてファイルを表示させる期間をより厳密に制御することができる。

【0102】

[第5の実施形態]

次に、第5の実施形態に係る情報蓄積システム1について説明する。第5の実施形態に係る情報蓄積システム1は、該当のアクセスキーの第2の有効期限を、情報端末機器20aが所定の記録媒体203a(例えば、RFIDタグやNFCタグ)から情報を読み取り可能な間、更新するものである。換言すれば、情報端末20aに対してRFIDタグやNFCタグ等を近付けている間に限り、該当のアクセスキーの第2の有効期限を更新するものである。

10

【0103】

なお、第5の実施形態に係る情報蓄積システム1は、システム構成、ハードウェア構成、及びソフトウェア構成が、第1の実施形態に係る情報蓄積システム1と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。

【0104】

<処理の詳細>

図17は、第5の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。なお、図17のシーケンス図におけるステップS111~S125の処理は、図16のシーケンス図におけるステップS81~S95の処理と同様であるため、説明を省略する。また、以降では、記録媒体203aは、RFIDタグ若しくはNFCタグを含むカード(RFIDカード、NFCカード)であるものとして説明する。

20

【0105】

ユーザAの携帯端末装置20aは、携帯端末装置20bとの間でファイルの共有を行うために所定の間隔で記録媒体203aの情報を読み取る(ステップS126)。換言すれば、ユーザAは、ユーザBとのファイルの共有を所望する間、記録媒体203aを携帯端末装置20aの所定の位置(外部I/F203が記録媒体203aを読み取り可能な位置)に近付けておく。すると、携帯端末装置20aは、記録媒体203aに記録されている情報を読み取る(ステップS127)。携帯端末装置20aは、記録媒体203aの読み取りに成功すると、アクセスキーの第2の有効期限の更新要求を情報蓄積装置10に送信する(ステップS128)。

30

【0106】

情報蓄積装置10は、該当のアクセスキーの第2の有効期限の更新する(ステップS129)。すなわち、例えば、情報蓄積装置10は、該当のアクセスキーの第2の有効期限を延長(例えば、上記の所定の間隔と同じ秒数を延長)する更新を行う。

【0107】

ユーザBの携帯端末装置20bは、ステップS124で取得したファイルを表示している間、所定の間隔毎に情報蓄積装置10に対して、該当のアクセスキーが存在するか否かを確認する(ステップS130)。情報蓄積装置10は、該当のアクセスキーが存在すれば、アクセスキーは有効であることを示す情報を応答し、携帯端末装置20bは、ファイルの表示を継続する(ステップS131)。

40

【0108】

ここで、例えばユーザAが記録媒体203aを携帯端末装置20aの所定の位置から離れた場合、携帯端末装置20aが記録媒体203aの読み取り動作を行っても(ステップS132)、携帯端末装置20aは記録媒体203aの読み取りに失敗する(ステップS133)。携帯端末装置20aは、記録媒体203aの読み取りに失敗すると、アクセス

50

キーの削除要求を情報蓄積装置 10 に送信する（ステップ S 1 3 4）。すると、情報蓄積装置 10 は、該当のアクセスキーを削除する（ステップ S 1 3 5）。

【 0 1 0 9 】

なお、携帯端末装置 20 a が記録媒体 20 3 a の読み取りに失敗した場合、アクセスキーの第 2 の有効期限の更新要求がされない。したがって、情報蓄積装置 10 は、第 4 の実施形態で説明した場合と同様に、第 2 の有効期限の経過に伴って該当のアクセスキーを削除してもよい。

【 0 1 1 0 】

上記のステップ S 1 3 0 で携帯端末装置 20 b が該当のアクセスキーが存在するか否かを確認した際に、該当のアクセスキーが削除されている場合、情報蓄積装置 10 は、携帯  
10  
端末装置 20 b に対してアクセスキーは無効である（存在しない）ことを示す情報を応答する（ステップ S 1 3 6）。すると、携帯端末装置 20 b は、ファイルの表示を終了させる（ステップ S 1 3 7）。

【 0 1 1 1 】

以上により、第 5 の実施形態に係る情報蓄積システム 1 では、携帯端末装置 20 a が記録媒体 20 3 a を読み取り可能な間に限り（例えば、RFID カードや NFC カードを携帯  
20  
端末装置 20 a の所定の位置に近付けている間に限り）、携帯端末装置 20 b でファイルを表示させるように制御することができる。これにより、第 4 の実施形態において携帯端末装置 20 a で所定の画面を表示させ続けることによる電力消費を抑えつつ、携帯端末装置 20 b においてファイルを表示させる期間を厳密に制御することができる。

【 0 1 1 2 】

[ 第 6 の実施形態 ]

次に、第 6 の実施形態に係る情報蓄積システム 1 について説明する。第 6 の実施形態に係る情報蓄積システム 1 は、情報端末装置 20 a で予め読み取った記録媒体 20 3 a の情報（例えば、記録媒体 20 3 a の固有の識別情報）と同一の情報が携帯端末装置 20 b で  
20  
読み取り可能な間に限り、携帯端末装置 20 b でファイルの共有を行うものである。

【 0 1 1 3 】

なお、第 6 の実施形態に係る情報蓄積システム 1 は、システム構成、ハードウェア構成、及びソフトウェア構成が、第 1 の実施形態に係る情報蓄積システム 1 と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。  
30

【 0 1 1 4 】

< 処理の詳細 >

図 1 8 は、第 6 の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図である。なお、図 1 8 のシーケンス図におけるステップ S 1 4 1 ~ S 1 4 6 及びステップ S 1 5 3 ~ S 1 5 8 の処理は、それぞれ図 7 のシーケンス図におけるステップ S 1 1 ~ 1 6 及びステップ S 2 1 ~ S 2 6 の処理と同様であるため、説明を省略する。

【 0 1 1 5 】

ユーザ A の携帯端末装置 20 a は、記録媒体 20 3 a を読み取り（ステップ S 1 4 7）、この記録媒体 20 3 a に記録されている情報（例えば、記録媒体 20 3 a の固有の識別情報（カード ID 等））を取得する（ステップ S 1 4 8）。本実施形態では、携帯端末装置 20 a は、記録媒体 20 3 a を読み取り、この記録媒体 20 3 a の固有の識別情報を取得するものとする。  
40

【 0 1 1 6 】

次に、携帯端末装置 20 a は、アクセスキーと記録媒体 20 3 a の固有の識別情報とに基づき QR コード（コード情報）を生成し（ステップ S 1 4 9）、表示装置 20 2 に表示させる（ステップ S 1 5 0）。そして、携帯端末装置 20 b は、この QR コードをカメラ装置 20 9 で読み取ることで（ステップ S 1 5 1）、アクセスキーやファイルパス等に加えて、携帯端末装置 20 a が記録媒体 20 3 a から読み取った上記の固有の識別情報を取得することができる（ステップ S 1 5 2）。

【 0 1 1 7 】

ここで、ユーザBの携帯端末装置20bでファイルの共有(ファイルの表示)を開始する際には、上記のステップS147で用いた記録媒体203aを携帯端末装置20bの所定の位置に近付けておく。携帯端末装置20bは、ファイルを表示させている間、所定の間隔で記録媒体203aの情報を読み取り(ステップS159)、この記録媒体203aの固有の識別情報を取得する(ステップS160)。そして、携帯端末装置20bは、上記のステップS152で取得した固有の識別情報と、ステップS160で取得した固有の識別情報とが同一である場合、ファイルの表示を継続させる。一方、携帯端末装置20bは、上記のステップS152で取得した固有の識別情報と、ステップS160で取得した固有の識別情報とが同一でない場合、ファイルの表示を終了させる。

【0118】

他方、携帯端末装置20bは、上記のステップS159で記録媒体203aの読み取りに失敗した場合(ステップS161)、ファイルの表示を終了させる(ステップS162)。

【0119】

以上により、第6の実施形態に係る情報蓄積システム1では、情報端末装置20aで予め読み取った記録媒体203aの情報と同一の情報が携帯端末装置20bで読み取り可能な間に限り、携帯端末装置20bでファイルの共有を行うことができる。これにより、情報蓄積装置10と携帯端末装置20aとの間及び情報蓄積装置10と携帯端末装置20bとの間における通信負荷を抑えつつ、携帯端末装置20bにおいてファイルを表示させる期間を厳密に制御することができる。

【0120】

[第7の実施形態]

次に、第7の実施形態に係る情報蓄積システム1について説明する。第7の実施形態に係る情報蓄積システム1は、ファイルの表示(共有)と、ネットワークN1に接続されている他の機器の利用とを携帯端末装置20bが行う場合に、該当のアクセスキーに対して第2の有効期限に加えて、他の機器の利用に応じた有効期限(他の機器毎の有効期限)を有するものである。換言すれば、第7の実施形態に係る情報蓄積システム1は、携帯端末装置20bが利用する機能毎に、それぞれ有効期限が設定される。

【0121】

以降では一例として、情報端末装置20bが、ファイルの表示と、プロジェクタ40に対するファイルの投影要求とを行う場合について説明する。したがって、本実施形態に係る情報蓄積システム1の情報蓄積装置10は、アクセスキーと関連付けて、ファイルを携帯端末20bに表示させるために用いる第2の有効期限に加えて、ファイルをプロジェクタ40で投影させるために用いる第3の有効期限が記憶領域に保存されている。本実施形態に係る情報蓄積システム1は、第3の有効期限を用いることで、携帯端末装置20aが所定の画面を表示させている間に限り、プロジェクタ40でファイルの内容が投影される。なお、例えば、情報端末装置20bが、情報蓄積装置10に格納されているファイルを、ネットワークN1に接続されているデジタルサイネージに表示させる場合には、このために用いる第4の有効期限が該当のアクセスキーと関連付けて情報蓄積装置10の記憶領域に保存される。

【0122】

なお、第6の実施形態に係る情報蓄積システム1は、システム構成、ハードウェア構成、及びソフトウェア構成が、第1の実施形態に係る情報蓄積システム1と同様であるため、システム構成、ハードウェア構成、及びソフトウェア構成についての説明を省略する。

【0123】

<処理の詳細>

図19は、第7の実施形態に係る情報蓄積システム1の処理手順を表した一例のシーケンス図である。なお、図19のシーケンス図におけるステップS171~S185の処理は図16のシーケンス図におけるステップS81~S95の処理と同様であるため、説明を省略する。

10

20

30

40

50

## 【 0 1 2 4 】

ユーザ B は、携帯端末装置 2 0 b を用いて機器（プロジェクタ 4 0）の利用を開始するための操作を行う（ステップ S 1 8 6）。これは、例えば、ステップ S 1 8 5 で携帯端末装置 2 0 b に表示させたファイルを、プロジェクタ 4 0 を用いて投影させるための操作である。すると、携帯端末装置 2 0 b は、アクセスキーとファイルパスとを含む投影要求を情報蓄積装置 1 0 に対して送信し（ステップ S 1 8 7）、情報蓄積装置 1 0 は、ファイルパスで指定されたファイルを含む投影指示をプロジェクタ 4 0 に対して送信する（ステップ S 1 8 8）。これにより、プロジェクタ 4 0 は、投影指示に含まれるファイルの内容を投影する。

## 【 0 1 2 5 】

ユーザ A の携帯端末装置 2 0 a は、所定の画面を表示させる。すると、携帯端末装置 2 0 a は、この所定の画面を表示している間、所定の間隔でアクセスキーの第 2 の有効期限の又は / 及び第 3 の有効期限の更新要求を情報蓄積装置 1 0 に送信する（ステップ S 1 8 9）。ここで、本実施形態における所定の画面とは、例えば、以下のいずれかの画面である。

( 1 ) 携帯端末装置 2 0 b に対して、ファイルの表示（共有）のみを許可するための画面  
( 2 ) 携帯端末装置 2 0 b に対して、プロジェクタ 4 0 を用いてファイルの投影のみを許可するための画面

( 3 ) 携帯端末装置 2 0 b に対して、ファイルの表示及びプロジェクタを用いたファイルの投影の両方を許可するための画面

なお、上記の更新要求は、携帯端末装置 2 0 a が上記（ 1 ）の画面を表示させている場合は、第 2 の有効期限の更新要求であり、上記（ 2 ）の画面を表示させている場合は、第 3 の有効期限の更新要求であり、上記（ 3 ）の画面を表示させている場合は、第 2 の有効期限及び第 3 の有効期限の更新要求である。

## 【 0 1 2 6 】

次に、情報蓄積装置 1 0 は、該当のアクセスキーの第 2 の有効期限又は / 及び第 3 の有効期限の更新する（ステップ S 1 9 0）。

## 【 0 1 2 7 】

ユーザ B の携帯端末装置 2 0 b は、ステップ S 1 8 4 で取得したファイルを表示している間、又は、プロジェクタ 4 0 を用いてファイルを投影している間、所定の間隔毎に情報蓄積装置 1 0 に対して、該当のアクセスキーの第 2 の有効期限又は / 及び第 3 の有効期限を経過しているか否かを確認する（ステップ S 1 9 1）。本実施形態では、情報蓄積装置 2 0 b が該当のアクセスキーの第 3 の有効期限を経過しているか否かを確認する場合について説明する。なお、第 2 の有効期限を経過しているか否かを確認する処理については、第 4 の実施形態の図 1 6 のステップ S 9 9 ~ S 1 0 2 で説明した通りである。

## 【 0 1 2 8 】

情報蓄積装置 1 0 は、該当のアクセスキーの第 3 の有効期限が経過していなければ、アクセスキーは有効であることを示す情報を応答し（ステップ S 1 9 2）、携帯端末装置 2 0 b は、プロジェクタ 4 0 を用いたファイルの投影を継続する。

## 【 0 1 2 9 】

ここで、ユーザ A の携帯端末装置 2 0 a が、例えば、上記（ 3 ）の画面の表示を終了させて、上記（ 1 ）の画面を表示させた場合、該当のアクセスキーの第 3 の有効期限は更新されない（他方、第 2 の有効期限は更新される。）。このため、情報蓄積装置 1 0 では、第 3 の有効期限が経過した場合、アクセスキーは無効であることを示す情報を応答する（ステップ S 1 9 3）。すると、携帯端末装置 2 0 b は、アクセスキーとファイルパスとを含む投影終了要求を情報蓄積装置 1 0 に対して送信し（ステップ S 1 9 4）、情報蓄積装置 1 0 は、該当のファイルの投影終了指示をプロジェクタ 4 0 に対して送信する（ステップ S 1 9 5）。これにより、プロジェクタ 4 0 は、投影を終了させる。他方で、携帯端末装置 2 0 b でのファイルの共有（表示）は継続される。

## 【 0 1 3 0 】

以上により、第7の実施形態に係る情報蓄積システム1では、携帯端末装置20bでの他の機器の利用に関して、より厳密な制御が行える。換言すれば、第7の実施形態に係る情報蓄積システム1では、携帯端末装置20bでファイルの表示や他の機器の利用等の複数の機能を利用する場合に、それぞれの機能の利用に関して厳密な制御を行うことができる。

【0131】

なお、本実施形態では携帯端末装置20bが情報蓄積装置10に対して投影要求を送信したが、これに限らず、例えば、携帯端末装置20bから直接プロジェクタ40に対して投影要求を送信してもよい。また、本実施形態ではプロジェクタを例にして説明したが、これに限らず、各種電子機器（MFPや電子黒板、モニタ、カメラ等の電子データの入力又は出力が可能な機器）を用いてもよい。

10

【0132】

また、本実施形態では携帯端末装置20bが情報蓄積装置10に対して終了要求を送信したが、これに限らず、例えば、情報蓄積装置10がプロジェクタ40に対して「投影要求の受け付け禁止」を示す命令を送信してもよい。このような構成とすることにより、プロジェクタ40が携帯端末装置20bから投影要求を受信した場合でも、投影が行われなないようにすることができる。このような場合、上述した「投影要求の受け付け禁止」を示す命令には、対象となるファイルの識別情報や携帯端末装置20の識別情報等を含めるとよい。

【0133】

20

例えば、当該命令にファイルの識別情報を含めることで、携帯端末装置20bからファイルの投影要求を受信した場合に、プロジェクタ40が当該命令に含まれるファイルの識別情報と、受信した投影要求に含まれるファイルの識別情報とを比較することで、当該投影要求に含まれるファイルが投影を禁止されているか否かを判断することができる。また、例えば、当該命令に携帯端末装置20の識別情報を含めることで、プロジェクタ40は、受信した投影要求がアクセスキーが無効となった携帯端末装置20からの投影要求であるか否かを判断することができる。このような構成とすることにより、本実施形態に係る情報蓄積システム1は、ファイルの投影可否を適切に判断することができる。

【0134】

<まとめ>

30

以上、本実施形態に係る情報蓄積システム1によれば、情報蓄積装置10に保存されているファイルを複数の携帯端末装置20で共有することができる。

【0135】

また、情報蓄積装置10は、携帯端末装置20の要求に応じて上記共有に用いるアクセスキーを発行する。そして、他の携帯端末装置20がこのアクセスキーを用いることで、情報蓄積装置10からファイルを取得することができる。これにより、当該ファイルにアクセスする権限を有しないユーザの携帯端末装置20であっても、ファイル共有を行うことができる。

【0136】

また、携帯端末装置20は、アクセスキーの発行を行うこともできる。これにより、情報蓄積装置10の処理の負荷を分散することができる。

40

【0137】

また、情報蓄積装置10は、アクセスキーの認証回数を保持することができる。これにより、所定の認証回数に達した場合にはアクセスキーを記憶領域から削除し、当該アクセスキーを無効とすることができる。したがって、例えば複数台の携帯端末装置20間でファイルの共有を行うことができる。なお、認証回数は、所定の記憶領域にアクセス可能な回数を示すアクセス回数の一例である。

【0138】

また、携帯端末装置20aが所定の画面を表示させている間、携帯端末装置20bでファイルを表示させるように制御することができる。これにより、携帯端末装置20bにお

50

いてファイルを表示させる期間をより厳密に制御することができる。

【0139】

また、携帯端末装置20aが記録媒体203aを読み取り可能な間に限り、携帯端末装置20bでファイルを表示させるように制御することができる。これにより、携帯端末装置20aで所定の画面を表示させ続けることによる電力消費を抑えつつ、携帯端末装置20bにおいてファイルを表示させる期間を厳密に制御することができる。

【0140】

また、情報端末装置20aで予め読み取った記録媒体203aの情報と同一の情報が携帯端末装置20bで読み取り可能な間に限り、携帯端末装置20bでファイルの共有を行うことができる。これにより、情報蓄積装置10と携帯端末装置20aとの間及び情報蓄積装置10と携帯端末装置20bとの間における通信負荷を抑えつつ、携帯端末装置20bにおいてファイルを表示させる期間を厳密に制御することができる。

10

【0141】

また、携帯端末装置20bでの他の機器の利用に関して、より厳密な制御が行える。

【0142】

本発明は、具体的に開示された上記の実施形態に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

【符号の説明】

【0143】

- 1 情報蓄積システム
- 10 情報蓄積装置
- 20 携帯端末装置
- 30 MFP
- 40 プロジェクタ
- 110 OS
- 111 Webサーバ
- 112 共有フォルダ
- 113 ドキュメント管理
- 114 PCブラウザ用UI
- 115 MFP用UI
- 116 WebAPI
- 117 Web制御
- 118 認証管理
- 119 設定情報管理
- 210 OS
- 211 情報蓄積装置通信部
- 212 印刷管理部
- 213 プロジェクタ管理部
- 214 ファイル一覧管理部
- 215 アップロード画面表示部
- 216 設定画面表示部
- 217 プレビュー画面表示部
- 218 認証情報管理部
- 219 コード情報処理部

20

30

40

【先行技術文献】

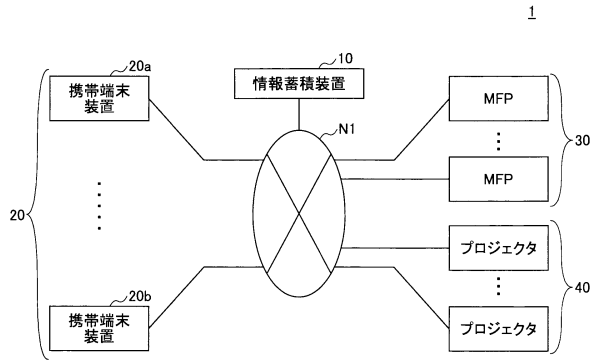
【特許文献】

【0144】

【特許文献1】特開2003-256260号公報

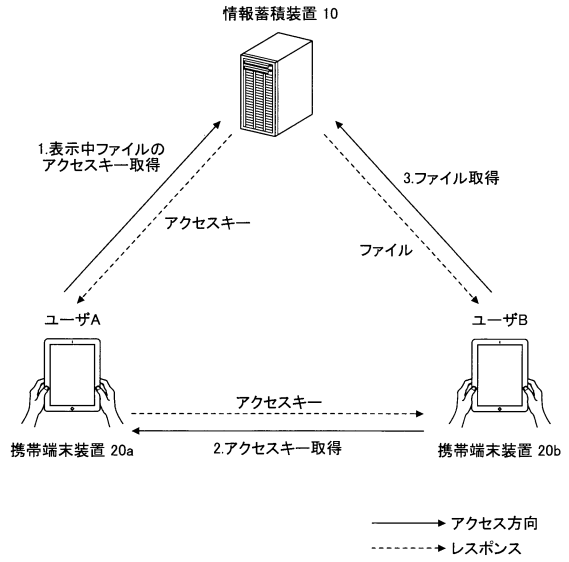
【図1】

第1の実施形態に係る情報蓄積システムの一例の構成図



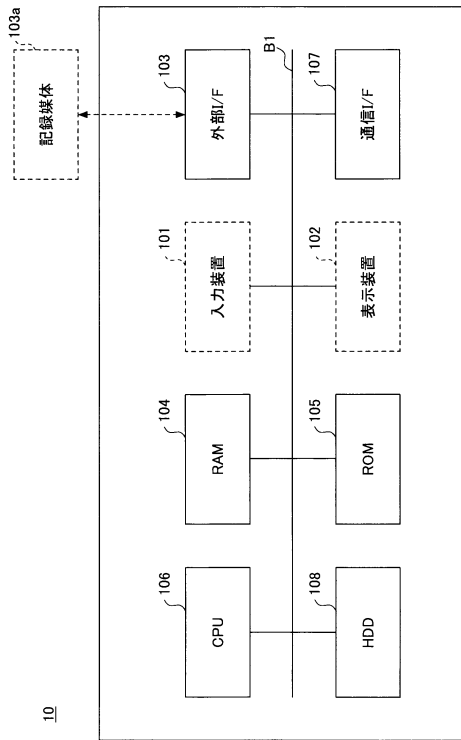
【図2】

第1の実施形態の利用シーンの一例を説明する図



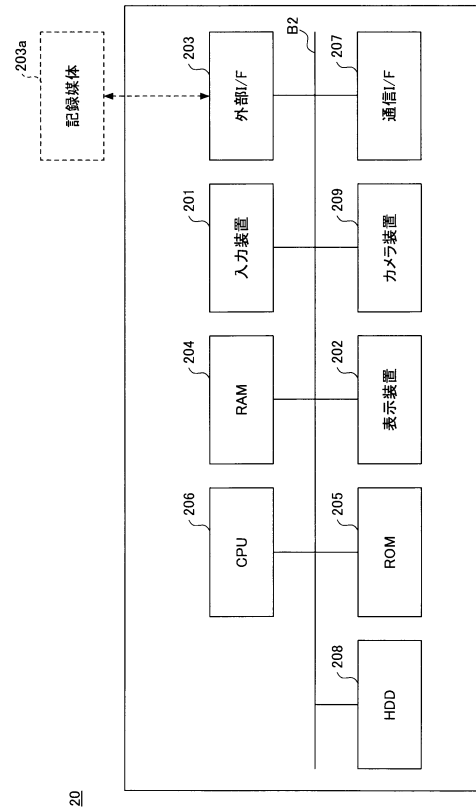
【図3】

第1の実施形態に係る情報蓄積装置の一例のハードウェア構成図



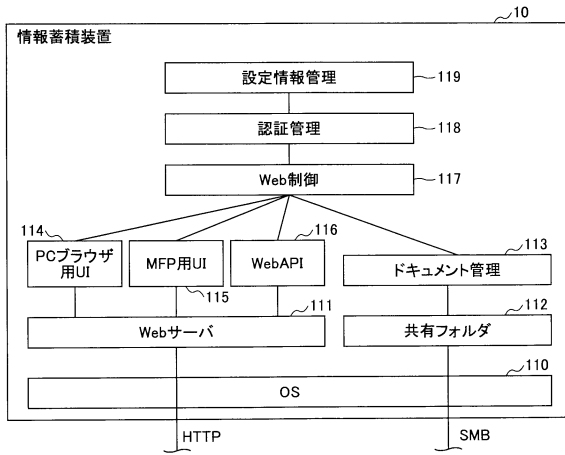
【図4】

第1の実施形態に係る携帯端末装置の一例のハードウェア構成図



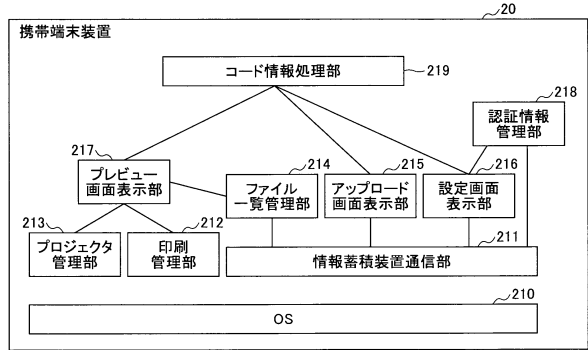
【図5】

第1の実施形態に係る情報蓄積装置の一例の処理ブロック図



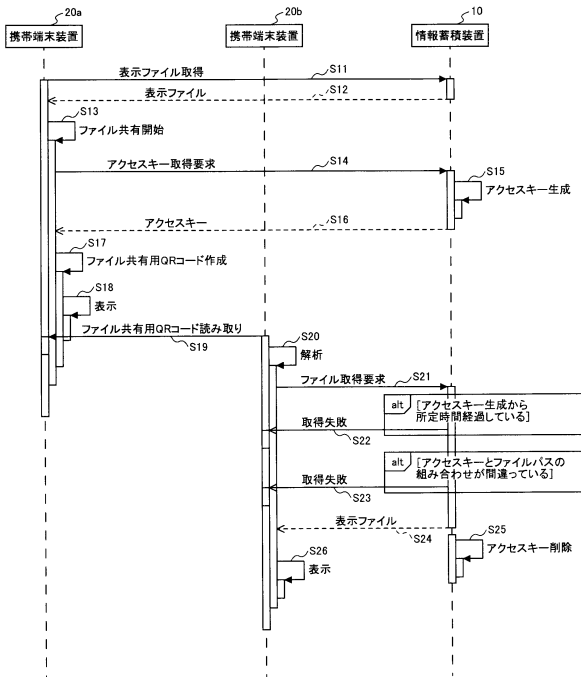
【図6】

第1の実施形態に係る携帯端末装置の一例の処理ブロック図



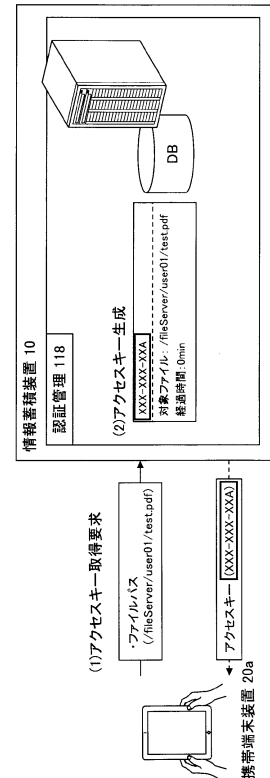
【図7】

第1の実施形態に係る情報蓄積システムの処理手順を表した一例のシーケンス図



【図8】

アクセスキーの取得方法を示した一例の説明図





【図9】

QRコードの一例のイメージ図



【図10】

QRコードの情報の一例の説明図

```
{
  "oneTimeAccessKey": "aaaaaaaa-bbbb-cccc-ddd-
  eeeeeeeeeee",
  "filePath": "/fileServer/user01/test.pdf",
  "serverAddress": "12.34.56.789"
}
```

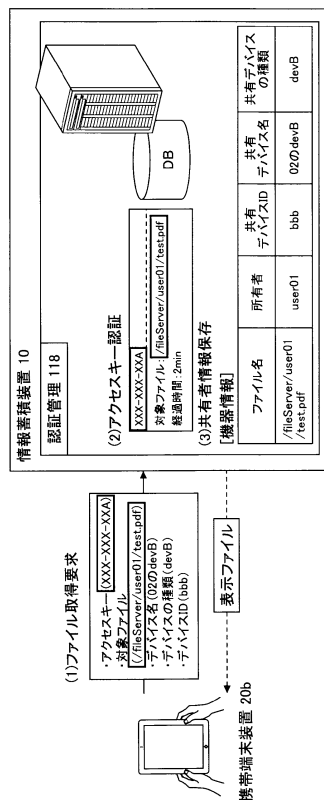
【図12】

ファイル取得要求に含まれる情報を示した一例の説明図

```
{
  oneTimeAccessKey: "XXX-XXX-XXX",
  filePath: "/fileServer/user01/test.pdf",
  deviceName: "02@devB",
  deviceType: "devB",
  deviceId: "bbb"
}
```

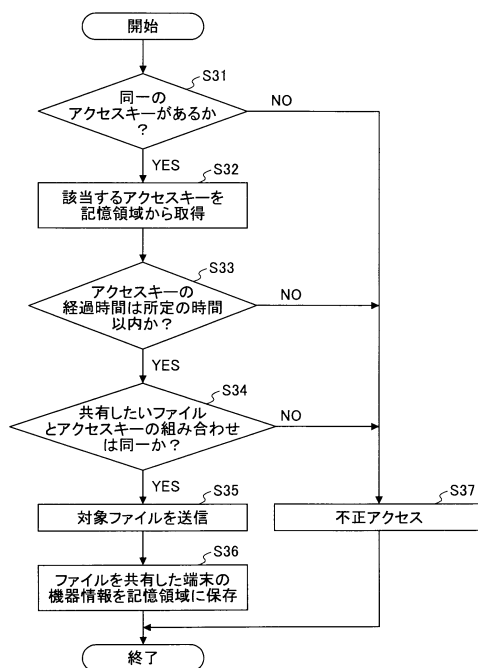
【図11】

アクセスキーの認証方法を示した一例の説明図



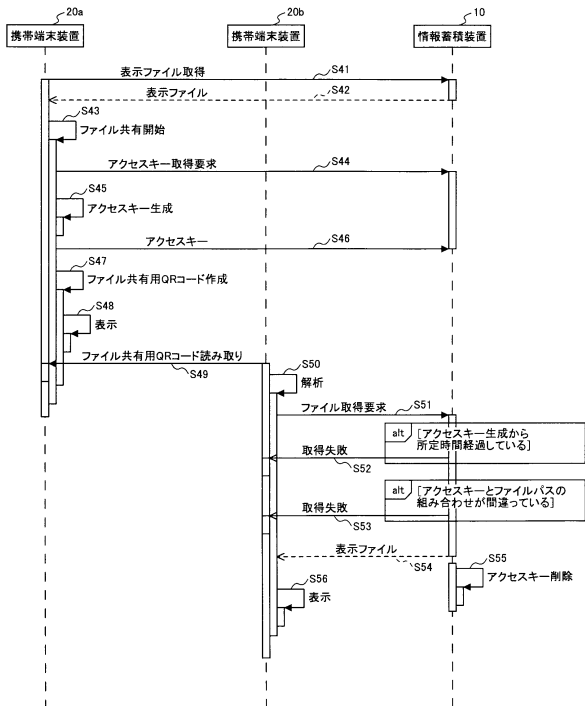
【図13】

第1の実施形態に係る情報蓄積装置におけるアクセスキー認証処理の一例のフローチャート



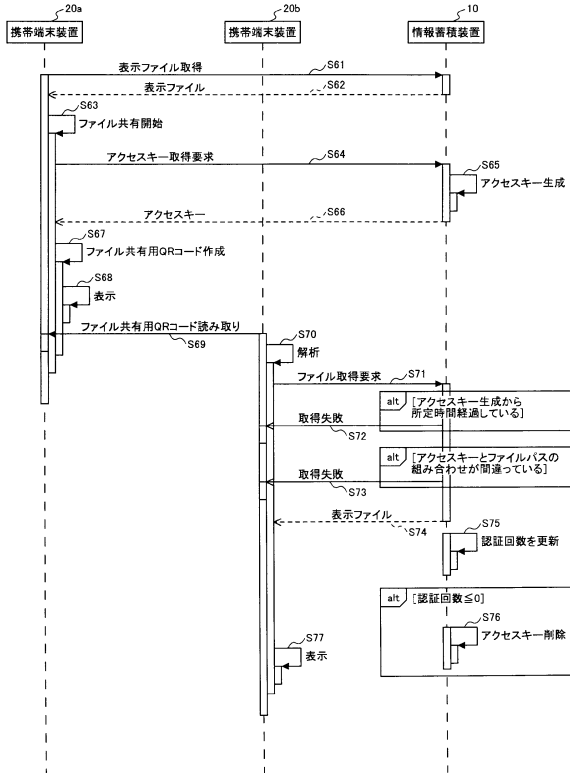
【図14】

第2の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



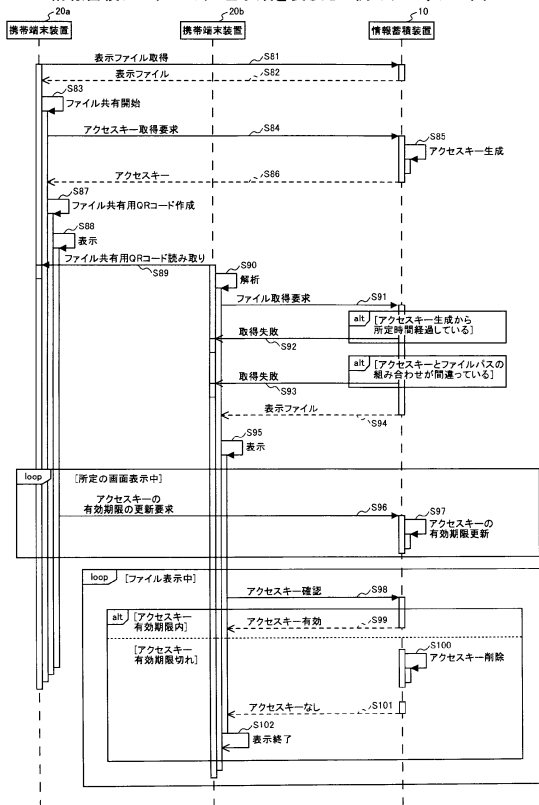
【図15】

第3の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



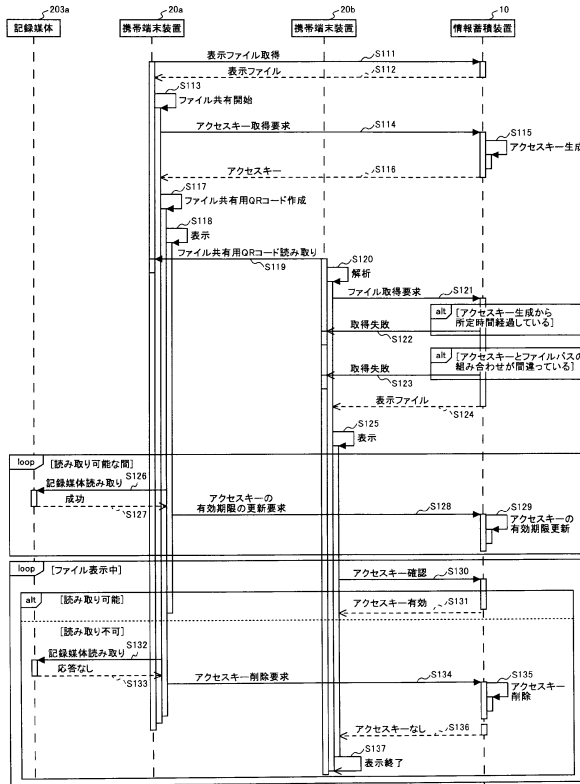
【図16】

第4の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



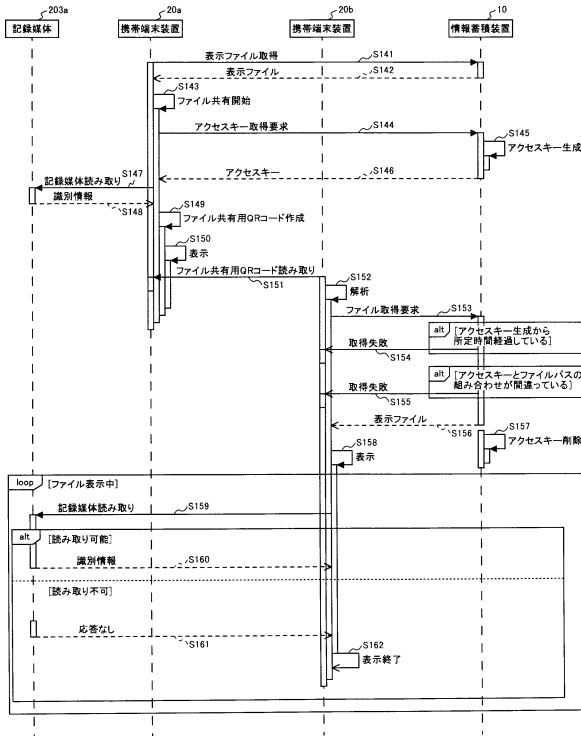
【図17】

第5の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



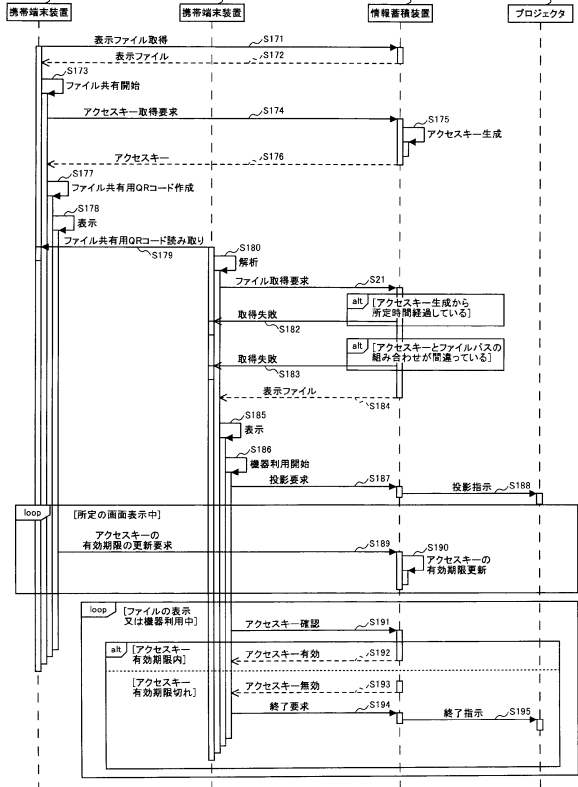
【図18】

第6の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



【図19】

第7の実施形態に係る  
情報蓄積システムの処理手順を表した一例のシーケンス図



---

フロントページの続き

- (56)参考文献 特開2013-065297(JP,A)  
特開2004-007589(JP,A)  
特表2011-525006(JP,A)  
特開2007-164449(JP,A)  
特開2002-358244(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/62

G06F 12/00