(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7586850号
(P7586850)

(45)発行日　令和6年11月19日(2024.11.19)

(24)登録日　令和6年11月11日(2024.11.11)

(51)国際特許分類
Ｇ０６Ｆ　21/60　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/60

請求項の数　15　（全26頁）

(21)出願番号　特願2022-57546(P2022-57546)
(22)出願日　令和4年3月30日(2022.3.30)
(65)公開番号　特開2023-149134(P2023-149134A)
(43)公開日　令和5年10月13日(2023.10.13)
審査請求日　令和6年2月16日(2024.2.16)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110001689
青稜弁理士法人
(72)発明者　礒川 弘実
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　菅原 健太
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
審査官　石坂 知樹

最終頁に続く

(54)【発明の名称】　データ消去装置、データ消去システム及びデータ消去方法

(57)【特許請求の範囲】

【請求項１】

所定の処理を行う処理装置と、所定のファイルが格納された記憶装置とを有するユーザ機器のデータ消去装置であって、

前記処理装置は、

データ消去部とアプリケーション起動部を有し、

前記記憶装置は、

残存許可ファイルが記載された残存許可一覧データと消去対象ファイルが記載された消去対象一覧データを格納し、

前記データ消去部は、

前記記憶装置に保存されている前記ファイルの一覧を残存ファイル一覧として取得し、

取得した前記残存ファイル一覧から前記残存許可一覧データと前記消去対象一覧データのどちらにも含まれないファイルを新たに追加する追加消去対象ファイルとして判定し、

前記追加消去対象ファイルを前記消去対象一覧データに追加して前記消去対象一覧データを更新し、

前記アプリケーション起動部は、

前記消去対象一覧データの更新が完了した後に、アプリケーションを起動し、

前記データ消去部は、

起動した前記アプリケーションの利用が終了した後に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とするデータ消去装置。

【請求項２】
前記データ消去部は、
起動した前記アプリケーションの利用が終了した後、前記ユーザ機器の電源ＯＦＦの前に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とする請求項１に記載のデータ消去装置。
【請求項３】
前記残存許可一覧データは、
残存許可識別子と前記残存許可識別子に対応した残存許可対象パスから構成され、
前記残存許可対象パスには、前記残存許可識別子に対応して残存許可対象とするファイルのパスが記載されていることを特徴とする請求項１に記載のデータ消去装置。
【請求項４】
前記消去対象一覧データは、
消去対象識別子と前記消去対象識別子に対応した消去対象パスから構成され、
前記消去対象パスには、前記消去対象識別子に対応して消去対象とするファイルのパスが記載されていることを特徴とする請求項１に記載のデータ消去装置。
【請求項５】
少なくとも一つのユーザ機器と管理機器とがネットワークを介して接続されたデータ消去システムであって、
前記ユーザ機器は、
所定の処理を行う第１の処理装置と、所定のファイルが格納された第１の記憶装置とを有し、
前記管理機器は、
所定の処理を行う第２の処理装置と、所定のファイルが格納された第２の記憶装置とを有し、
前記ユーザ機器の前記第１の処理装置は、
データ消去部とアプリケーション起動部を有し、
前記管理機器の前記第２の処理装置は、
管理部を有し、
前記ユーザ機器の前記第１の記憶装置は、
残存許可ファイルが記載された残存許可一覧データと消去対象ファイルが記載された消去対象一覧データを格納し、
前記管理機器の前記第２の記憶装置は、
前記残存許可一覧データと前記消去対象一覧データを格納し、
前記データ消去部は、
前記第１の記憶装置に保存されている前記ファイルの一覧を残存ファイル一覧として取得して、
取得した前記残存ファイル一覧から前記残存許可一覧データと前記消去対象一覧データのどちらにも含まれないファイルを新たに追加する追加消去対象ファイルとして判定し、
前記追加消去対象ファイルを前記管理部に送信し、
前記管理部は、
受信した前記追加消去対象ファイルを前記第２の記憶装置に格納されている前記消去対象一覧データに追加して前記消去対象一覧データを更新して、更新された前記消去対象一覧データを前記データ消去部に送り、
前記データ消去部は、
受信した前記消去対象一覧データに基づいて、前記第１の記憶装置に格納されている前記消去対象一覧データを更新し、
前記アプリケーション起動部は、
前記消去対象一覧データの更新が完了した後に、アプリケーションを起動し、
前記データ消去部は、
起動した前記アプリケーションの利用が終了した後に、更新された前記消去対象一覧デ

ータに記載された前記消去対象ファイルを消去することを特徴とするデータ消去システム。
【請求項６】
前記管理機器の前記第２の記憶装置は、
少なくとも一つの前記ユーザ機器の名称が記載されたユーザ機器一覧データを更に格納し、
前記管理部は、
少なくとも一つの前記ユーザ機器毎に受信した前記追加消去対象ファイルを集約して前記消去対象一覧データに追加して更新し、
前記データ消去部は、
前記ユーザ機器毎に受信した前記消去対象一覧データに基づいて、前記第１の記憶装置に格納されている前記消去対象一覧データを更新し、
前記アプリケーションの利用が終了した後に、前記ユーザ機器毎に更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とする請求項５に記載のデータ消去システム。
【請求項７】
前記管理部は、
前記追加消去対象ファイルを前記消去対象一覧データに追加する際に、前記追加消去対象ファイルを消去しても影響がないかを評価することを特徴とする請求項５に記載のデータ消去システム。
【請求項８】
前記管理部は、
前記追加消去対象ファイルを消去しても影響がないかを評価した結果、
前記追加消去対象ファイルを消去しても影響がないと判定された場合、前記追加消去対象ファイルを前記消去対象一覧データに追加して前記消去対象一覧データを更新し、
前記追加消去対象ファイルを消去すると影響があると判定された場合、前記追加消去対象ファイルを前記残存許可一覧データに追加して前記残存許可一覧データを更新することを特徴とする請求項７に記載のデータ消去システム。
【請求項９】
前記ユーザ機器は、
所定の評価用画面を表示する入出力装置を更に有し、
前記管理部は、
前記評価用画面を介してユーザにより入力された評価結果に基づいて、前記追加消去対象ファイルを消去しても影響がないかの前記評価を行うことを特徴とする請求項７に記載のデータ消去システム。
【請求項１０】
前記管理機器は、
所定の評価用画面を表示する入出力装置を更に有し、
前記管理部は、
前記評価用画面を介して管理者により入力された評価結果に基づいて、前記追加消去対象ファイルを消去しても影響がないかの前記評価を行うことを特徴とする請求項７に記載のデータ消去システム。
【請求項１１】
前記データ消去部は、少なくとも一つの前記ユーザ機器毎に、
起動した前記アプリケーションの利用が終了した後、前記ユーザ機器の電源ＯＦＦの前に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とする請求項５に記載のデータ消去システム。
【請求項１２】
前記残存許可一覧データは、
残存許可識別子と前記残存許可識別子に対応した残存許可対象パスから構成され、
前記残存許可対象パスには、前記残存許可識別子に対応して残存許可対象とするファイルのパスが記載されていることを特徴とする請求項５に記載のデータ消去システム。

【請求項１３】
前記消去対象一覧データは、
消去対象識別子と前記消去対象識別子に対応した消去対象パスから構成され、
前記消去対象パスには、前記消去対象識別子に対応して消去対象とするファイルのパスが記載されていることを特徴とする請求項５に記載のデータ消去システム。
【請求項１４】
所定の処理を行う処理装置と、所定のファイルが格納された記憶装置とを有するユーザ機器のデータ消去方法であって、
前記処理装置は、
記憶ステップと、データ消去ステップと、アプリケーション起動ステップを実行し、
前記記憶ステップは、
残存許可ファイルが記載された残存許可一覧データと消去対象ファイルが記載された消去対象一覧データを前記記憶装置に記憶し、
前記データ消去ステップは、
前記記憶装置に保存されている前記ファイルの一覧を残存ファイル一覧として取得し、取得した前記残存ファイル一覧から前記残存許可一覧データと前記消去対象一覧データのどちらにも含まれないファイルを新たに追加する追加消去対象ファイルとして判定し、前記追加消去対象ファイルを前記消去対象一覧データに追加して前記消去対象一覧データを更新し、
前記アプリケーション起動ステップは、
前記消去対象一覧データの更新が完了した後に、アプリケーションを起動し、
前記データ消去ステップは、
起動した前記アプリケーションの利用が終了した後に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とするデータ消去方法。
【請求項１５】
前記データ消去ステップは、
起動した前記アプリケーションの利用が終了した後、前記ユーザ機器の電源ＯＦＦの前に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とする請求項１４に記載のデータ消去方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ消去装置、データ消去システム及びデータ消去方法に関する。
【背景技術】
【０００２】
企業等の組織では、従業員が業務に使用する端末等の業務機器に、盗難や紛失時に業務機器内に保存した業務データを不正に利用されないようセキュリティリスクを低減する対策を施している。
【０００３】
セキュリティリスクを低減する方法の一つとして、業務機器内に保存した業務データを消去する方法がある。特許文献１では、情報処理端末から該情報処理端末が記憶しているファイルと、該情報処理端末における操作ログとを取得し、取得した操作ログに基づいて特定した、取得したファイルの記憶タイミングからの経過時間に応じてアラートを出力することで、情報処理端末に記憶されてから保存されたままとなっているデータの存在を認識することができるとしている。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０１８－９２５４４号公報
【発明の概要】

【発明が解決しようとする課題】
【０００５】
特許文献１では、操作ログの取得を前提としており、操作ログの取得がなされていないまたは不十分な場合には保存されたままとなっているデータがあってもアラートされず存在の認識は難しいという課題がある。
【０００６】
また、残存ファイルの存在を認識した場合にアラートするのみで残存ファイルの漏洩リスクをどのように低減するかの言及が無く、セキュリティ確保には不十分である。
【０００７】
本発明の目的は、データ消去装置において、残存ファイルを把握して消去することにより消去漏れを防ぎ情報漏洩リスクを軽減することにある。
【課題を解決するための手段】
【０００８】
本発明の一態様のデータ消去装置は、所定の処理を行う処理装置と、所定のファイルが格納された記憶装置とを有するユーザ機器のデータ消去装置であって、前記処理装置は、データ消去部とアプリケーション起動部を有し、前記記憶装置は、残存許可ファイルが記載された残存許可一覧データと消去対象ファイルが記載された消去対象一覧データを格納し、前記データ消去部は、前記記憶装置に保存されている前記ファイルの一覧を残存ファイル一覧として取得し、
取得した前記残存ファイル一覧から前記残存許可一覧データと前記消去対象一覧データのどちらにも含まれないファイルを新たに追加する追加消去対象ファイルとして判定し、前記追加消去対象ファイルを前記消去対象一覧データに追加して前記消去対象一覧データを更新し、前記アプリケーション起動部は、前記消去対象一覧データの更新が完了した後に、前記アプリケーションを起動し、前記データ消去部は、起動した前記アプリケーションの利用が終了した後に、更新された前記消去対象一覧データに記載された前記消去対象ファイルを消去することを特徴とする。
【発明の効果】
【０００９】
本発明の一態様によれば、データ消去装置において、残存ファイルを把握して消去することにより消去漏れを防ぎ情報漏洩リスクを軽減することができる。
【図面の簡単な説明】
【００１０】
【図１】本発明の実施例１におけるデータ消去機器の全体の構成を説明する図の一例である。
【図２】本発明の実施例１における残存許可一覧データの構成を説明する図の一例である。
【図３】本発明の実施例１における消去対象一覧データの構成を説明する図の一例である。
【図４】本発明の実施例１におけるデータ消去機器の動作を説明するフローチャートの一例である。
【図５】本発明の実施例２におけるデータ消去システムの全体の構成を説明する図の一例である。
【図６】本発明の実施例２における管理機器の構成を説明する図の一例である。
【図７】本発明の実施例２におけるユーザ機器の構成を説明する図の一例である。
【図８】本発明の実施例２における残存許可一覧データの構成を説明する図の一例である。
【図９】本発明の実施例２における消去対象一覧データの構成を説明する図の一例である。
【図１０】本発明の実施例２におけるユーザ機器一覧データの構成を説明する図の一例である。
【図１１】本発明の実施例２におけるデータ消去システムの動作を説明するフローチャートの一例である。
【図１２】本発明の実施例３におけるデータ消去システムの全体の構成を説明する図の一例である。

【図１３】本発明の実施例３における管理機器の構成を説明する図の一例である。
【図１４】本発明の実施例３におけるユーザ機器の構成を説明する図の一例である。
【図１５】本発明の実施例３における残存許可一覧データの構成を説明する図の一例である。
【図１６】本発明の実施例３における消去対象一覧データの構成を説明する図の一例である。
【図１７】本発明の実施例３における消去可否判定一覧データの構成を説明する図の一例である。
【図１８】本発明の実施例３における残存ファイル一覧データの構成を説明する図の一例である。
【図１９】本発明の実施例３におけるユーザ機器一覧データの構成を説明する図の一例である。
【図２０】本発明の実施例３における評価依頼一覧データの構成を説明する図の一例である。
【図２１】本発明の実施例３におけるデータ消去システムの全体的な動作を説明するフローチャートの一例である。
【図２２】本発明の実施例３におけるデータ消去システムの一部の動作を説明するフローチャートの一例である。
【図２３】本発明の実施例３における評価開始依頼画面インターフェースを説明する図の一例である。
【図２４】本発明の実施例３における評価入力依頼画面インターフェースを説明する図の一例である。
【図２５】本発明の実施例３におけるデータ消去システムの一部の動作を説明するフローチャートの一例である。
【図２６】本発明の実施例３における消去判断依頼インターフェースを説明する図の一例である。
【発明を実施するための形態】
【００１１】
以下に本発明に係る実施例について、図１乃至図２６を用いて説明する。
【実施例１】
【００１２】
最初に、図１乃至図４を用いて本発明の実施例１に係るデータ消去機器を説明する。実施例１は、ユーザが利用するユーザ機器においてユーザ機器起動後に残存しているファイルの一覧を把握し、残存を許可するファイルの一覧と組み合わせて消去対象とするファイルの一覧を生成し、ユーザ機器の終了前に消去対象ファイルを消去することで、ユーザ機器の終了後に残存許可ファイル一覧に含まれないファイルが残存していない状態にするものである。
【００１３】
まず、図１乃至図３を用いて本発明の実施例１に係るデータ消去機器の構成を説明する。
【００１４】
図１は、実施例１の全体の構成を表す概略図である。ユーザ機器１０はユーザ１１が使用する装置である。ユーザ機器１０は、プロセッサ１２と、メモリ１３と、入出力装置１４と、記憶装置１５と、内部信号線１６と、モニタ１７と、キーボード１８と、マウス１９とで構成される。プロセッサ１２は、プログラムの処理をおこなう装置である。記憶装置１５は、ハードディスクや不揮発性メモリなどであり、プログラムやデータを格納する装置である。メモリ１３は、実行するプログラムの格納や、一時的なデータの格納をおこなうための記憶装置である。入出力装置１４は、モニタ１７への出力とキーボード１８とマウス１９からの入力を制御する装置である。記憶装置１５には、実施例１におけるデータ消去機器を実現するためのプログラムとデータが格納される。
【００１５】

プログラムとしては、ＯＳ（Operating System）プログラム１００、消去プログラム１０１、アプリケーションプログラム１０４が格納される。データとしては、残存許可一覧データ１０２、消去対象一覧データ１０３が格納される。メモリ１３には、記憶装置１５上のＯＳプログラム１００がロードされ、実行される。ＯＳプログラム１００は、入出力装置１４の制御、記憶装置１５からデータのメモリ１３へのロードなどを行う。また、ＯＳプログラム１００は、記憶装置１５から、消去プログラム１０１とアプリケーションプログラム１０４をメモリ１３にロードし、実行する。アプリケーションプログラム１０４は、アプリケーションのデータをアプリケーションデータ領域１０５に格納する。

【００１６】

処理装置であるプロセッサ１２は、ＯＳプログラム１００を介して記憶装置１５から消去プログラム１０１をメモリ１３にロードし実行することにより「データ消去部」として機能する。また、処理装置であるプロセッサ１２は、ＯＳプログラム１００を介して記憶装置１５からアプリケーションプログラム１０４をメモリ１３にロードし実行することにより「アプリケーション起動部」として機能する。

【００１７】

図２は、図１に示した残存許可一覧データ１０２の構成を説明する図である。残存許可一覧データ１０２は、残存許可ＩＤ２０１、残存許可対象パス２０２の各フィールドから構成される。残存許可ＩＤ２０１は、残存許可対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。残存許可対象パス２０２は、残存許可ＩＤ２０１に対応して残存許可対象とするファイルやフォルダのパスを記載するフィールドである。組織では、ユーザ１１がユーザ機器１０を使用開始する前に残存許可一覧データ１０２に残存許可するパスを登録しておく。

【００１８】

図３は、図１に示した消去対象一覧データ１０３の構成を説明する図である。消去対象一覧データ１０３は、消去対象ＩＤ３０１、消去対象パス３０２の各フィールドから構成される。消去対象ＩＤ３０１は、消去対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。

【００１９】

消去対象パス３０２は、消去対象ＩＤ３０１に対応して消去対象とするファイルやフォルダのパスを記載するフィールドである。ユーザ１１がユーザ機器１０を使用開始すると消去プログラム１０１により消去対象一覧データ１０３の内容は更新される。組織では、ユーザ１１がユーザ機器１０を使用開始する前に消去対象一覧データ１０３に消去対象とするパスの初期値を登録しておいても良い。

【００２０】

次に、図４を用いて本発明の実施例１に係るデータ消去機器の動作を説明する。

図４は、ユーザ１１がユーザ機器１０を起動して、アプリケーションを利用した作業を実施して、ユーザ機器１０を終了するまでの動作を説明するフローチャートである。この動作の中で残存ファイルを把握し、ユーザ機器１０の終了前に残存ファイルを消去している。まず、ユーザ１１はユーザ機器１０の電源を入れる（Ｓ４０１）。ユーザ機器１０では、ＯＳプログラム１００が起動する。ＯＳプログラム１００は消去プログラム１０１を起動する（Ｓ４０２）。

【００２１】

消去プログラム１０１はユーザ機器１０の記憶装置１５に保存されているファイルの一覧を残存ファイル一覧として取得する（Ｓ４０３）。そして、取得した残存ファイル一覧から残存許可一覧データ１０２と消去対象一覧データ１０３のどちらにも含まれないものを新たに追加する消去対象として判定し（Ｓ４０４）、追加する消去対象を消去対象一覧データ１０３に追加して（Ｓ４０５）、更新完了をＯＳプログラム１００に通知する（Ｓ４０６）。

【００２２】

ＯＳプログラム１００はユーザ機器１０の起動後に起動するプログラムの順番を制御し

、消去プログラム１０１が消去対象一覧データ１０３の更新を完了するまでアプリケーションプログラム１０４が起動しないように抑止する。その後、ユーザはアプリケーションを起動する操作を実施し（Ｓ４０７）、アプリケーションプログラム１０４を起動する（Ｓ４０８）。ユーザはアプリケーションプログラム１０４を利用して業務を行った（Ｓ４０９）後、ユーザ機器１０を終了する操作を実施する（Ｓ４１０）。

【００２３】

ユーザ機器１０の終了操作を受けたＯＳプログラム１００は、消去プログラム１０１に終了指示を出す（Ｓ４１１）。消去プログラム１０１は消去対象一覧データ１０３に記載の消去対象ファイルを全て消去し（Ｓ４１２）、消去完了をＯＳプログラム１００に応答する（Ｓ４１３）。その後ＯＳプログラム１００はユーザ機器１０の電源をＯＦＦにする（Ｓ４１４）。

【００２４】

上記のように、本発明の実施例１によれば、ユーザ機器１０が起動した際に残存ファイルを確認して、残存許可一覧データ１０２と消去対象一覧データ１０３のどちらにも含まれずに残存したファイルは消去対象一覧データ１０３に追加し、ユーザ機器１０の終了前に消去することが可能となり、ユーザ機器１０の残存データによるセキュリティリスクを低減できるようになる。

【実施例２】

【００２５】

次に、図５乃至図１１を用いて本発明の実施例２に係るデータ消去システムを説明する。実施例２は、ユーザが利用するユーザ機器においてユーザ機器起動後に残存しているファイルの一覧を把握し、残存を許可するファイルの一覧と組み合わせて消去対象とするファイルの一覧を生成し、消去対象とするファイルの一覧を１台以上のユーザ機器から管理機器に収集してマージし消去対象一覧データを生成し、１台以上のユーザ機器に適用してユーザ機器の終了前に残存していたファイルを消去することで、１台以上のユーザ機器から生成された消去対象一覧データを使用してユーザ機器の終了後にファイルが残存していない状態にするものである。

【００２６】

まず、図５乃至図１０を用いて本発明の実施例２に係るデータ消去システムの構成を説明する。

【００２７】

図５は、実施例２おけるデータ消去システムの全体の構成を説明する概略図である。管理機器５０はネットワーク５２に接続する。ユーザ機器５１は、ネットワーク５２に接続し、管理機器５０と通信する。管理者５３は管理機器５０にあるデータを閲覧、編集できる。ユーザ５４はユーザ機器５１の利用者である。

【００２８】

図６は、管理機器５０の構成を説明する構成図である。管理機器５０は、プロセッサ６１と、メモリ６２と、通信装置６３と、入出力装置６４と、記憶装置６５と、内部信号線６６と、モニタ６７と、キーボード６８と、マウス６９とで構成される。プロセッサ６１は、プログラムの処理をおこなう装置である。記憶装置６５は、ハードディスクや不揮発性メモリなどであり、プログラムやデータを格納する装置である。メモリ６２は、実行するプログラムの格納や、一時的なデータの格納をおこなうための記憶装置である。

【００２９】

入出力装置６４は、モニタ６７への出力とキーボード６８とマウス６９からの入力を制御する装置である。通信装置６３は、他の装置との間のネットワーク通信を行う装置である。記憶装置６５には、実施例２におけるデータ消去システムを実現するためのプログラムとデータが格納される。プログラムとしては、ＯＳプログラム６００、管理プログラム６０１が格納される。データとしては、残存許可一覧データ６０２、消去対象一覧データ６０３、ユーザ機器一覧データ６０４が格納される。メモリ６２には、記憶装置６５上のＯＳプログラム６００がロードされ、実行される。ＯＳプログラム６００は、入出力装置

６４の制御、記憶装置６５からデータのメモリ６２へのロードなどを行う。また、ＯＳプログラム６００は、記憶装置６５から、管理プログラム６０１をメモリ６２にロードし、実行する。

【００３０】

処理装置であるプロセッサ６１は、ＯＳプログラム６００を介して記憶装置６５から管理プログラム６０１をメモリ６２にロードし実行することにより「管理部」として機能する。

【００３１】

図７は、ユーザ機器５１の構成を説明する構成図である。ユーザ機器５１は、プロセッサ７１と、メモリ７２と、通信装置７３と、入出力装置７４と、記憶装置７５と、内部信号線７６と、モニタ７７と、キーボード７８と、マウス７９とで構成される。記憶装置７５には、実施例２におけるデータ消去システムを実現するためのプログラムとデータが格納される。プログラムとしては、ＯＳプログラム７００、消去プログラム７０１、アプリケーションプログラム４０２が格納される。

【００３２】

データとしては、残存許可一覧データ６０２、消去対象一覧データ６０３が格納される。メモリ７２には、記憶装置７５上のＯＳプログラム７００がロードされ、実行される。ＯＳプログラム７００は、記憶装置７５から、消去プログラム７０１とアプリケーションプログラム７０２をメモリ７２にロードし、実行する。アプリケーションプログラム７０２は、アプリケーションのデータをアプリケーションデータ領域７０３に格納する。

【００３３】

処理装置であるプロセッサ７１は、ＯＳプログラム７００を介して記憶装置７５から消去プログラム７０１をメモリ７２にロードし実行することにより「データ消去部」として機能する。また、処理装置であるプロセッサ７１は、ＯＳプログラム７００を介して記憶装置７５からアプリケーションプログラム７０２をメモリ７２にロードし実行することにより「アプリケーション起動部」として機能する。

【００３４】

図８は、図６に示した残存許可一覧データ６０２の構成を説明する図である。残存許可一覧データ６０２は、残存許可ＩＤ８０１、残存許可対象パス８０２の各フィールドから構成される。残存許可ＩＤ８０１は、残存許可対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。残存許可対象パス８０２は、残存許可ＩＤ８０１に対応して残存許可対象とするファイルやフォルダのパスを記載するフィールドである。

【００３５】

管理者５３は、データ消去システムが稼動開始前に管理機器５０を操作し、残存を許可するファイルの一覧を残存許可一覧データ６０２に登録する。また、データ消去システムが稼動開始後に残存を許可するファイルの一覧の追加や削除、変更があった際には、管理者５３は管理機器５０を操作し、残存許可一覧データ６０２の内容を変更する。管理プログラム６０１により残存許可一覧データ６０２の内容はユーザ機器５１に送信され適用される。

【００３６】

図９は、図６に示した消去対象一覧データ６０３の構成を説明する図である。消去対象一覧データ６０３は、消去対象ＩＤ６０１、消去対象パス６０２の各フィールドから構成される。消去対象ＩＤ６０１は、消去対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。消去対象パス６０２は、消去対象ＩＤ６０１に対応して消去対象とするファイルやフォルダのパスを記載するフィールドである。

【００３７】

管理者５３は、データ消去システムが稼動開始前に管理機器５０を操作し、消去の対象とするファイルの一覧の初期値を消去対象一覧データ６０３に登録しておいても良い。管理プログラム６０１により消去対象一覧データ６０３の内容は更新される。また、管理プ

ログラム６０１により消去対象一覧データ６０３の内容はユーザ機器５１に送信され適用される。

【００３８】

図１０は、図６に示したユーザ機器一覧データ６０４の構成を説明する図である。ユーザ機器一覧データ６０４は、ユーザ機器ＩＤ１００１、ユーザ機器名１００２の各フィールドから構成される。ユーザ機器ＩＤ１００１は、組織のユーザ機器に対して一意となる識別子を記載するフィールドである。ユーザ機器名１００２は、ユーザ機器ＩＤ１００１に対応するユーザ機器の名称を記載するフィールドである。管理者５３は、データ消去システムが稼動開始前に管理機器５０を操作し、ユーザ機器の一覧をユーザ機器一覧データ６０４に登録する。また、データ消去システムが稼動開始後にユーザ機器の追加や削除、変更があった際には、管理者５３は管理機器５０を操作し、ユーザ機器一覧データ６０４の内容を変更する。

【００３９】

次に、図１１を用いて本発明の実施例２に係るデータ消去システムの動作を説明する。

図１１は、ユーザ５４がユーザ機器５１を起動して、アプリケーションを利用した作業を実施して、ユーザ機器５１を終了するまでの動作を説明するフローチャートである。この動作の中で残存ファイルを把握し、管理プログラムに送信して、消去対象ファイルの一覧を更新し、ユーザ機器５１の終了前に残存ファイルを消去している。まず、ユーザ５４はユーザ機器５１の電源を入れる（Ｓ１１０１）。

【００４０】

ユーザ機器５１では、ＯＳプログラム７００が起動する。ＯＳプログラム７００は消去プログラム７０１を起動する（Ｓ１１０２）。消去プログラム７０１はユーザ機器５１の記憶装置７５に保存されているファイルの一覧を残存ファイル一覧として取得する（Ｓ１１０３）。そして、取得した残存ファイル一覧から残存許可一覧データ６０２と消去対象一覧データ６０３のどちらにも含まれないものを新たに追加する消去対象として判定し（Ｓ１１０４）、追加する消去対象を管理プログラム６０１に送信する（Ｓ１１０５）。

【００４１】

管理プログラム６０１は受信した追加する消去対象を消去対象一覧データ６０３に追加して更新する（Ｓ１１０６）。追加は既に登録済の消去対象パスに含まれているものは除外して追加することで重複追加を排除する。管理プログラム６０１は残存許可一覧データ６０２と更新した消去対象一覧データ６０３を消去プログラム７０１に送信する（Ｓ１１０７）。

【００４２】

消去プログラム７０１は受信した残存許可一覧データ６０２と消去対象一覧データ６０３を記憶装置７５に保存して（Ｓ１１０８）、更新完了をＯＳプログラム７００に通知する（Ｓ１１０９）。ＯＳプログラム７００はユーザ機器５１の起動後に起動するプログラムの順番を制御し、消去プログラム７０１が残存許可一覧データ６０２と消去対象一覧データ６０３の更新を完了するまでアプリケーションプログラム７０２が起動しないように抑止する。その後、ユーザ５４はアプリケーションを起動する操作を実施し（Ｓ１１１０）、アプリケーションプログラム７０２を起動する（Ｓ１１１１）。

【００４３】

ユーザ５４はアプリケーションプログラム７０２を利用して業務を行った（Ｓ１１１２）後、ユーザ機器５１を終了する操作を実施する（Ｓ１１１３）。ユーザ機器５１の終了操作を受けたＯＳプログラム７００は、消去プログラム７０１に終了指示を出す（Ｓ１１１４）。消去プログラム７０１は消去対象一覧データ６０３に記載の消去対象ファイルを全て消去し（Ｓ１１１５）、消去完了をＯＳプログラム７００に応答する（Ｓ１１１６）。その後ＯＳプログラム７００はユーザ機器５１の電源をＯＦＦにする（Ｓ１１１７）。

【００４４】

上記のように、本発明の実施例２によれば、ユーザ機器５１が起動した際に残存ファイルを確認して、残存許可一覧データ６０２と消去対象一覧データ６０３のどちらにも含ま

れずに残存したファイルの一覧は、管理サーバに送信されて他のユーザ機器の分も含め追加され更新される。そして、１台以上の残存ファイルの一覧を反映して更新された消去対象一覧データ６０３がユーザ機器５１に適用されユーザ機器５１の終了前に消去することが可能となり、ユーザ機器５１の残存データによるセキュリティリスクを更に低減できるようになる。

【実施例３】

【００４５】

次に、図１２乃至図２６を用いて本発明の実施例３に係るデータ消去システムを説明する。実施例３は、ユーザが利用するユーザ機器においてユーザ機器起動後に残存しているファイルの一覧を把握し、残存を許可するファイルの一覧と組み合わせて消去対象とするファイルの一覧を生成し、消去対象とするファイルの一覧を１台以上のユーザ機器から管理機器に収集してマージし消去対象一覧データを生成し、１台以上のユーザ機器に適用してユーザ機器の終了前に残存していたファイルを消去することで、１台以上のユーザ機器から生成された消去対象一覧データを使用してユーザ機器の終了後にファイルが残存していない状態にするものである。この中で、消去対象一覧データに消去対象を追加する前に一部のユーザ機器に消去を適用して影響がないかをユーザに問合せて確認し、影響確認の結果と管理者による判断に基づいて消去対象一覧データに消去対象を追加するかを決定するものである。

【００４６】

まず、図１２乃至図２０を用いて本発明の実施例３に係るデータ消去システムの構成を説明する。

【００４７】

図１２は、データ消去システムの全体の構成を説明する概略図である。管理機器１２０はネットワーク１２２に接続する。ユーザ機器１２１は、ネットワーク１２２に接続し、管理機器１２０と通信する。管理者１２３は管理機器１２０にあるデータを閲覧、編集できる。ユーザ１２４はユーザ機器１２１の利用者である。

【００４８】

図１３は、管理機器１２０の構成を説明する構成図である。管理機器１２０は、プロセッサ１３１と、メモリ１３２と、通信装置１３３と、入出力装置１３４と、記憶装置１３５と、内部信号線１３６と、モニタ１３７と、キーボード１３８と、マウス１３９とで構成される。プロセッサ１３１は、プログラムの処理をおこなう装置である。

【００４９】

記憶装置１３５は、ハードディスクや不揮発性メモリなどであり、プログラムやデータを格納する装置である。メモリ１３２は、実行するプログラムの格納や、一時的なデータの格納をおこなうための記憶装置である。入出力装置１３４は、モニタ１３７への出力とキーボード１３８とマウス１３９からの入力を制御する装置である。通信装置１３３は、他の装置との間のネットワーク通信を行う装置である。記憶装置１３５には、実施例３におけるデータ消去システムを実現するためのプログラムとデータが格納される。

【００５０】

プログラムとしては、ＯＳプログラム１３００、管理プログラム１３０１が格納される。データとしては、残存許可一覧データ１３０２、消去対象一覧データ１３０３、消去可否判定一覧データ１３０４、残存ファイル一覧データ１３０５、ユーザ機器一覧データ１３０６が格納される。メモリ１３２には、記憶装置１３５上のＯＳプログラム１３００がロードされ、実行される。ＯＳプログラム１３００は、入出力装置１３４の制御、記憶装置１３５からデータのメモリ１３２へのロードなどを行う。また、ＯＳプログラム１３００は、記憶装置１３５から、管理プログラム１３０１をメモリ１３２にロードし、実行する。

【００５１】

処理装置であるプロセッサ１３１は、ＯＳプログラム１３００を介して記憶装置１３５から管理プログラム１３０１をメモリ１３２にロードし実行することにより「管理部」と

して機能する。
【００５２】
図１４は、ユーザ機器１２１の構成を説明する構成図である。ユーザ機器１２１は、プロセッサ１４１と、メモリ１４２と、通信装置１４３と、入出力装置１４４と、記憶装置１４５と、内部信号線１４６と、モニタ１４７と、キーボード１４８と、マウス１４９とで構成される。記憶装置１４５には、実施例３におけるデータ消去システムを実現するためのプログラムとデータが格納される。プログラムとしては、ＯＳプログラム１４００、消去プログラム１４０１、アプリケーションプログラム１４０４が格納される。
【００５３】
データとしては、残存許可一覧データ１３０２、消去対象一覧データ１３０３、評価依頼一覧データ１４０２が格納される。メモリ１４２には、記憶装置１４５上のＯＳプログラム１４００がロードされ、実行される。ＯＳプログラム１４００は、記憶装置１４５から、消去プログラム１４０１とアプリケーションプログラム１４０２をメモリ１４２にロードし、実行する。アプリケーションプログラム１４０２は、アプリケーションのデータをアプリケーションデータ領域１４０３に格納する。また、ＯＳプログラム１４００は、記憶装置１４５へのファイルの作成を監視してファイル作成のログを生成し、ファイル作成ログデータ領域１４０５に格納する。
【００５４】
処理装置であるプロセッサ１４１は、ＯＳプログラム１４００を介して記憶装置１４５から消去プログラム１４０１をメモリ１４２にロードし実行することにより「データ消去部」として機能する。また、処理装置であるプロセッサ１４１は、ＯＳプログラム１４００を介して記憶装置１４５からアプリケーションプログラム１４０３をメモリ１４２にロードし実行することにより「アプリケーション起動部」として機能する。
【００５５】
図１５は、図１３に示した残存許可一覧データ１３０２の構成を説明する図である。残存許可一覧データ１３０２は、残存許可ＩＤ１５０１、残存許可対象パス１５０２の各フィールドから構成される。残存許可ＩＤ１５０１は、残存許可対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。残存許可対象パス１５０２は、残存許可ＩＤ１５０１に対応して残存許可対象とするファイルやフォルダのパスを記載するフィールドである。
【００５６】
管理者１２３は、データ消去システムが稼動開始前に管理機器１２０を操作し、残存を許可するファイルの一覧を残存許可一覧データ１３０２に登録する。また、データ消去システムが稼動開始後に残存を許可するファイルの一覧の追加や削除、変更があった際には、管理者１２３は管理機器１２０を操作し、残存許可一覧データ１３０２の内容を変更する。管理プログラム１３０１により残存許可一覧データ１３０２の内容は更新される。また、管理プログラム１３０１により残存許可一覧データ１３０２の内容はユーザ機器１２１に送信され適用される。
【００５７】
図１６は、図１３に示した消去対象一覧データ１３０３の構成を説明する図である。消去対象一覧データ１３０３は、消去対象ＩＤ１６０１、消去対象パス１６０２の各フィールドから構成される。消去対象ＩＤ１６０１は、消去対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。消去対象パス１６０２は、消去対象ＩＤ１６０１に対応して消去対象とするファイルやフォルダのパスを記載するフィールドである。
【００５８】
管理者１２３は、データ消去システムが稼動開始前に管理機器１２０を操作し、消去の対象とするファイルの一覧の初期値を消去対象一覧データ１３０３に登録しておいても良い。管理プログラム１３０１により消去対象一覧データ１３０３の内容は更新される。また、管理プログラム１３０１により消去対象一覧データ１３０３の内容はユーザ機器１２

１に送信され適用される。
【００５９】
図１７は、図１３に示した消去可否判定一覧データ１３０４の構成を説明する図である。消去対象一覧データ１３０４は、消去候補ＩＤ１７０１、消去候補パス１７０２、作成アプリケーション名１７０３、評価ユーザ機器（１）ＩＤ１７０４、評価結果（１）１７０５、評価ユーザ機器（２）ＩＤ１７０６、評価結果（２）１７０７の各フィールドから構成される。消去候補ＩＤ１７０１は、消去対象の候補とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。
【００６０】
消去候補パス１７０２は、消去候補ＩＤ１７０１に対応して消去対象の候補とするファイルやフォルダのパスを記載するフィールドである。作成アプリケーション名１７０３は、消去候補ＩＤ１７０１に対応して消去対象の候補とするファイルやフォルダを作成したアプリケーションの名称を記載するフィールドである。評価ユーザ機器（１）ＩＤ１７０４は、消去候補ＩＤ１７０１に対応して評価を依頼したまたは依頼中のユーザ機器のユーザ機器ＩＤを記載するフィールドである。
【００６１】
評価結果（１）１７０５は、消去候補ＩＤ１７０１に対応して評価ユーザ機器（１）ＩＤ１７０４記載のユーザ機器１２１に依頼した評価の結果を記載するフィールドである。実施例３では評価を２台のユーザ機器１２１に依頼することを可能とするため、評価ユーザ機器ＩＤと評価結果の組み合わせの２台目として、評価ユーザ機器（２）ＩＤ１７０６、評価結果（２）１７０７のフィールドを持つ。管理プログラム１３０１により消去可否判定一覧データ１３０４の内容は更新される。
【００６２】
図１８は、図１３に示した残存ファイル一覧データ１３０５の構成を説明する図である。残存ファイル一覧データ１３０５は、消去候補ＩＤ１８０１、管理機器内保存パス１８０２の各フィールドから構成される。消去候補ＩＤ１８０１は、消去対象とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。管理機器内保存パス１８０２は、消去候補ＩＤ１８０１に対応して消去対象の候補とするファイルやフォルダのコピーを保存した管理機器内のパスを記載するフィールドである。管理プログラム１３０１により残存ファイル一覧データ１３０５の内容は更新される。
【００６３】
図１９は、図１３に示したユーザ機器一覧データ１３０６の構成を説明する図である。ユーザ機器一覧データ１３０６は、ユーザ機器ＩＤ１９０１、ユーザ機器名１９０２の各フィールドから構成される。ユーザ機器ＩＤ１９０１は、組織のユーザ機器に対して一意となる識別子を記載するフィールドである。ユーザ機器名１９０２は、ユーザ機器ＩＤ１９０１に対応するユーザ機器の名称を記載するフィールドである。
【００６４】
管理者１２３は、データ消去システムが稼動開始前に管理機器１２０を操作し、ユーザ機器の一覧をユーザ機器一覧データ１３０６に登録する。また、データ消去システムが稼動開始後にユーザ機器の追加や削除、変更があった際には、管理者１２３は管理機器１２０を操作し、ユーザ機器一覧データ１３０６の内容を変更する。
【００６５】
図２０は、図１４に示した評価依頼一覧データ１４０２の構成を説明する図である。評価依頼一覧データ１４０２は、消去候補ＩＤ２００１、消去候補パス２００２、作成アプリケーション名２００３、評価終了日２００４、評価状態２００５の各フィールドから構成される。消去候補ＩＤ２００１は、消去対象の候補とするファイルやフォルダのパスに対して一意となる識別子を記載するフィールドである。
【００６６】
消去候補パス２００２は、消去候補ＩＤ２００１に対応して消去対象の候補とするファイルやフォルダのパスを記載するフィールドである。作成アプリケーション名２００３は

、消去候補ＩＤ２００１に対応して消去対象の候補とするファイルやフォルダを作成したアプリケーションの名称を記載するフィールドである。評価終了日２００４は、消去候補ＩＤ２００１に対応して評価を終了する日付を記載するフィールドである。評価状態２００５は、消去候補ＩＤ２００１に対応して消去候補のユーザ機器における評価状態を記載するフィールドである。消去プログラム１４０１により評価依頼一覧データ１４０２の内容は更新される。

【００６７】

次に、図２１乃至図２６を用いて本発明の実施例３に係るデータ消去システムの動作を説明する。

【００６８】

図２１は、ユーザ１２４がユーザ機器１２１を起動して、アプリケーションを利用した作業を実施して、ユーザ機器１２１を終了するまでの動作を説明するフローチャートである。この動作の中で残存ファイルを把握し、管理プログラムに送信して、消去対象ファイルの一覧を更新し、ユーザ機器１２１の終了前に残存ファイルを消去している。まず、ユーザ１２４はユーザ機器１２１の電源を入れる（Ｓ２１０１）。

【００６９】

ユーザ機器１２１では、ＯＳプログラム１４００が起動する。ＯＳプログラム１４００は消去プログラム１４０１を起動する（Ｓ２１０２）。消去プログラム１４０１はユーザ機器１２１の記憶装置１４５に保存されているファイルの一覧を残存ファイル一覧として取得する（Ｓ２１０３）。そして、取得した残存ファイル一覧から残存許可一覧データ１３０２と消去対象一覧データ１３０３のどちらにも含まれないものを新たに追加する消去対象ファイルとして判定し（Ｓ２１０４）、追加する消去対象ファイルのパスとファイル、また消去対象ファイルを作成したアプリケーション名をファイル作成ログデータ領域１４０５に格納されているログから取得して管理プログラム１３０１に送信する（Ｓ２１０５）。

【００７０】

管理プログラム１３０１は受信した追加する消去対象のパスが消去可否判定一覧データ１３０４に既に含まれているかどうかを確認する。パスが含まれている場合は、さらに消去可否判定一覧データ１３０４の評価ユーザ機器（２）ＩＤ１７０６の内容を確認して未登録の場合は、消去可否判定一覧データ１３０４の評価ユーザ機器（２）ＩＤ１７０６に送信してきたユーザ機器１２１のユーザ機器ＩＤを登録し、評価結果（２）１７０７に未開始を登録する。パスが含まれていない場合は、消去可否判定一覧データ１３０４に新たな行を追加し、新たな消去候補ＩＤを付与して消去候補ＩＤ１７０１に記載、送信されてきたパスを消去候補パス１７０２に記載、送信されてきたアプリケーション名を作成アプリケーション名１７０３に記載、送信してきたユーザ機器１２１のユーザ機器ＩＤを評価ユーザ機器（１）ＩＤ１７０４に記載、評価結果（１）１７０５に未開始を記載して登録する（Ｓ２１０６）。

【００７１】

管理プログラム１３０１は残存許可一覧データ１３０２と消去対象一覧データ１３０３を消去プログラム７０１に送信する。また、Ｓ２１０６で評価ユーザ機器（１）または（２）に追加した場合は、追加した消去候補について消去候補ＩＤ１７０１に記載の消去候補ＩＤと消去候補パス１７０２に記載の消去候補パスと作成アプリケーション名１７０３に記載の作成アプリケーション名を評価依頼として消去プログラム７０１に併せて返信する（Ｓ２１０７）。

【００７２】

消去プログラム１４０１は受信した残存許可一覧データ１３０２と消去対象一覧データ１３０３を記憶装置１４５に保存し（Ｓ２１０８）、評価依頼を受信した場合は、評価依頼一覧データ１４０２に新たな行を追加し、受信した消去候補ＩＤ、消去候補パス、作成アプリケーション名を記載し、評価状態を未開始として更新する。その後、消去プログラム１４０１は評価処理を行う（Ｓ２１０９）。評価処理Ｓ２１０９のフローチャートを図

２２に示す。

【００７３】

図２２は、消去プログラム１４０１が管理プログラム１３０１と連携し、未開始の消去候補の評価開始と、期限満了の消去候補の評価を実施するまでの動作を説明するフローチャートである。この動作の中で、未開始の消去候補の評価をユーザに問合せて確認した上で開始する動作と、評価期限満了した消去候補についてユーザに消去影響を問い合わせて評価回答を受け取り管理プログラムに登録する動作を行っている。まず、消去プログラム１４０１は評価依頼一覧データ１４０２の内容を確認し（Ｓ２２０１）、評価状態２００５が未開始となっている消去候補があるかを確認する（Ｓ２２０２）。もし未開始となっている消去候補があれば、該当する消去候補についてユーザ１２４に図２３で示す評価依頼画面インターフェースで提示する（Ｓ２２０３）。

【００７４】

図２３は、消去候補の消去影響の評価開始の依頼をユーザに提示する評価開始依頼画面インターフェースを示す図である。評価開始依頼画面インターフェースは、タイトル表示エリア２３０１、操作内容表示エリア２３０２から構成される。操作内容表示エリア２３０２には、消去候補のパス、作成アプリケーション名、評価満了日と、協力するか協力しないかをユーザ１２４が回答するボタンが表示される。評価終了日は一週間後などデータ消去システムや管理者で規定した期間を経過した日付とする。ユーザ１２４は、ボタンを押すことで回答する（Ｓ２２０４）。

【００７５】

評価開始依頼の回答が協力ありの場合、消去プログラム１４０１は評価依頼一覧データ１４０２の該当する消去候補について評価状態２００５を評価中に変更した上で、評価開始通知として該当する消去候補ＩＤを管理プログラム１３０１に送信する（Ｓ２２０６）。管理プログラム１３０１は、受信した消去候補ＩＤについて、消去可否判定一覧データ１３０４の該当するユーザ機器ＩＤの評価結果を評価中に更新し（Ｓ２２０７）、更新完了を消去プログラム１４０１に返信する（Ｓ２２０８）。

【００７６】

次に、消去プログラム１４０１は評価依頼一覧データ１４０２を見て評価満了日２００４に記載の日付が過ぎているかを調べることで期限満了の消去候補があるかを確認し（Ｓ２２０９）、もし期限満了の消去候補があれば、該当する消去候補についてユーザ１２４に図２４で示す評価入力画面インターフェースで提示する（Ｓ２２１０）。

【００７７】

図２４は、消去候補の消去影響の評価入力の依頼をユーザに提示する評価入力依頼画面インターフェースを示す図である。評価入力依頼画面インターフェースは、タイトル表示エリア２４０１、操作内容表示エリア２４０２から構成される。操作内容表示エリア２４０２には、消去候補のパス、作成アプリケーション名、評価満了日と、消去による影響をユーザ１２４が評価して入力するための影響有無入力のラジオボタンやテキスト入力エリアが表示される。ユーザ１２４は、ボタンを押したりテキスト入力したりすることで回答する（Ｓ２２１１）。

【００７８】

ユーザ１２４が評価入力を行った後、消去プログラム１４０１は評価依頼一覧データ１４０２の該当する消去候補を削除した上で、評価結果として該当する消去候補ＩＤと評価入力内容を管理プログラム１３０１に送信する（Ｓ２２１２）。管理プログラム１３０１は、受信した消去候補ＩＤが該当する消去可否判定一覧データ１３０４の内容を更新する。送信してきたユーザ機器１２１が評価ユーザ機器（１）ＩＤ１７０４記載のものであれば評価結果（１）１７０５に受信した評価入力内容を登録し、評価ユーザ機器（２）ＩＤ１７０６記載のものであれば評価結果（２）１７０７に受信した評価入力内容を登録する（Ｓ２２１３）。

【００７９】

さらに、評価結果（１）１７０５と評価結果（２）１７０７がどちらも未開始や評価中

ではなく登録された状態になった場合、該当の消去候補について残存許可一覧データ１３０２と消去対象一覧データ１３０３の一覧更新処理を実施する（Ｓ２２１４）。一覧更新処理Ｓ２２１４のフローチャートを図２５に示す。

【００８０】

図２５は、管理プログラム１３０１が管理者１２３と連携し、消去による影響の評価結果および管理者による判定結果により、残存許可一覧データ１３０２と消去対象一覧データ１３０３を更新する動作を説明するフローチャートである。まず、管理プログラム１３０１は該当の消去候補について、消去可否判定一覧データ１３０４の評価結果（１）１７０５と評価結果（２）１７０７の内容を確認し、どちらも影響無しの場合は、消去対象一覧データ１３０３に該当の消去候補を追加する（Ｓ２５０６）。どちらか一方でも影響有りの場合は、該当する消去候補について管理者１２３に図２６で示す消去判断依頼画面インターフェースで提示する（Ｓ２５０２）。

【００８１】

図２６は、消去候補の消去影響の評価結果を提示し消去するかどうかの判定を管理者１２３に依頼する消去判断依頼インターフェースを示す図である。消去判断依頼インターフェースは、タイトル表示エリア２６０１、操作内容表示エリア２６０２から構成される。操作内容表示エリア２６０２には、消去候補のパス、作成アプリケーション名、評価結果、消去候補のファイルの管理機器内保存パスと、消去するかしないかを管理者１２３が回答するボタンが表示される。

【００８２】

管理者１２３は、管理機器内保存パスに示されたファイルを開いて内容を確認した上で判定を実施して回答する（Ｓ２５０３）。

【００８３】

Ｓ２５０３の回答の結果が消去しないの場合は、残存許可一覧データ１３０２に該当の消去候補を追加し（Ｓ２５０５）、消去可否判定一覧から該当の消去候補の行を削除する（Ｓ２５０７）。Ｓ２５０３の回答の結果が消去するの場合は、消去対象一覧データ１３０３に該当の消去候補を追加し（Ｓ２５０６）、消去可否判定一覧から該当の消去候補の行を削除する（Ｓ２５０７）。

【００８４】

上記の一覧更新処理（Ｓ２２１４）が終了したら、管理プログラム１３０１は、登録完了を消去プログラム１４０１に返信する（Ｓ２２１５）。以上が図２２で示した、未開始の消去候補の評価開始と、期限満了の消去候補の評価を実施するまでの動作である。更新された残存許可一覧データ１３０２と消去対象一覧データ１３０３は全てのユーザ機器に送付され適用される。

【００８５】

上記のように、本発明の実施例３によれば、ユーザ機器１２１が起動した際に残存ファイルを確認して、残存許可一覧データ１３０２と消去対象一覧データ１３０３のどちらにも含まれずに残存したファイルの一覧は、管理サーバに送信されて他のユーザ機器の分も含め追加され更新される。追加の際には、消去の影響を１台以上のユーザ機器で評価し、その評価結果と管理者による判断に従って追加するかどうかが判定される。

【００８６】

すなわち、消去の影響がないと評価された場合は消去対象に追加され、消去の影響がある場合は管理者が判断した結果で消去対象もしくは残存許可対象に追加される。そして、１台以上の残存ファイルの一覧を反映し消去の影響も加味して更新された消去対象一覧データ１３０３がユーザ機器１２１に適用されユーザ機器１２１の終了前に消去することが可能となり、ユーザ機器１２１の残存データによるセキュリティリスクを更に低減できるようになる。

【００８７】

上記実施例は、装置に保存されたデータを消去するデータ消去機器であって、装置の起動後に装置内に残存したデータの一覧を残存データ一覧として取得する手段と、残存デー

ター一覧を用いて装置の終了前にデータを消去する手段を持つ。そして、装置の起動後に装置内に残存したデータの一覧を取得が完了するまではアプリケーションの起動を抑止する手段を持つ。

【００８８】

また、装置に保存されたデータを消去するデータ消去システムであって、装置の起動後に装置内に残存したデータの一覧を残存データ一覧として取得する手段と、１台以上の装置で取得した残存データ一覧を管理機器に収集する手段と、収集した残存データ一覧を集約した集約残存データ一覧を作成して装置に配布する手段と、集約残存データ一覧を用いて装置の終了前にデータを消去する手段を持つ。そして、装置の起動後に装置内に残存したデータの一覧を取得が完了するまではアプリケーションの起動を抑止する手段を持つ。

【００８９】

また、上記データ消去システムにおいて、残存データを消去した場合の影響を評価した上で集約残存データに追加するかどうかを判断する手段を持つ。また、上記データ消去システムであって、残存データを消去した場合の影響を装置のユーザが評価する手段を持つことを特徴とする。また、上記データ消去システムであって、残存データを消去するかどうかを管理者が判定する手段を持つ。

【００９０】

上記実施例によれば、データ消去装置において、残存ファイルを把握して消去することにより消去漏れを防ぎ情報漏洩リスクを軽減することができる。

【００９１】

なお、本発明は、上記の実施例に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。例えば、実施例３では２台のユーザ機器で影響を評価したが１台または３台以上に拡張しても良い。また、実施例３では管理者が消去対象とするかを判断しているが、残存ファイルにキーワードが入っているかどうかなどにより機械的に判断しても良い。さらに、実施例３ではユーザへの評価の終了の判断は日にちによって行っているが、評価開始からのユーザ装置の起動回数やアプリケーションの起動回数、アプリケーションの利用時間などその他の方法により判断しても良い。

【００９２】

また、組織のセキュリティ方針を反映した消去対象決定ポリシを定義可能として、例えばデータ消去の影響が無かったと回答した人が２人以上だと消去対象に追加する、影響がある場合でもすべて消去対象に追加する、消去対象とするパスを限定するなどとしても良い。

【００９３】

消去の評価を行う際に、バックアップを取って置き、データ消去の影響があったらすぐに元に戻せるようにしても良い。さらに、ユーザ機器上の残存したファイル名やフォルダ名には、ユーザ名やユーザ機器名、ファイル生成時刻など、ユーザ機器ごとに異なる文字列が含まれる場合があるため、同じ用途のファイルであっても複数のユーザ機器間で異なるファイル名やフォルダ名となっている場合を想定し、ファイル名やフォルダ名の正規化やマッチング処理を実施した上で残存ファイルの確認や消去を行うようにしても良い。

また、図１、図６、図１３、図１４のシステム構成図において、プログラムやデータの一部又は全ては、予め記憶装置１５、記憶装置６５、記憶装置１３５及び記憶装置１４５に格納されていても良いし、非一時的記憶媒体から又は外部の非一時的記憶装置を備えた情報処理装置からネットワーク経由で導入されても良い。

【符号の説明】

【００９４】

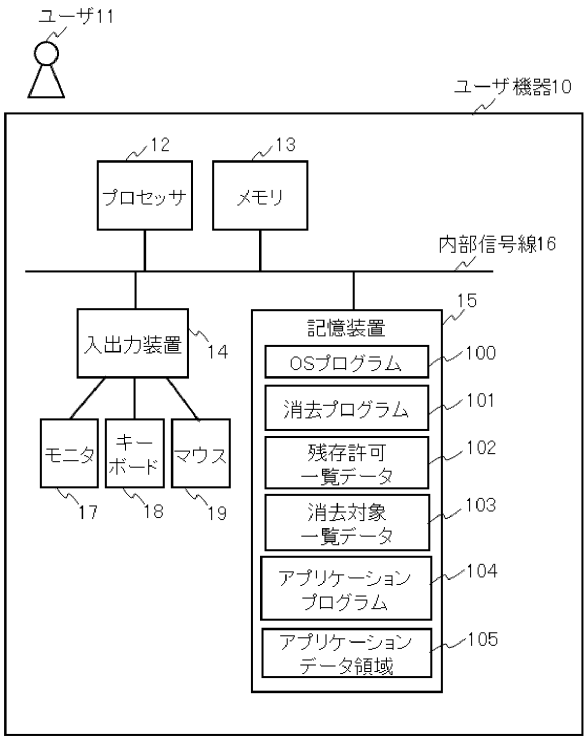
１０　ユーザ機器
１２　プロセッサ
１５　記憶装置
１００　ＯＳプログラム
１０１　消去プログラム

１０２　残存許可一覧データ
１０３　消去対象一覧データ
１０４　アプリケーションプログラム
１０５　アプリケーションデータ領域
５０　管理機器
５１　ユーザ機器
６１　プロセッサ
６５　記憶装置
６００　ＯＳプログラム
６０１　管理プログラム
６０２　残存許可一覧データ
６０３　消去対象一覧データ
６０４　ユーザ機器一覧データ
７１　プロセッサ
７５　記憶装置
７００　ＯＳプログラム
７０１　消去プログラム
７０２　アプリケーションプログラム
７０３　アプリケーションデータ領域
１２０　管理機器
１２１　ユーザ機器
１３１　プロセッサ
１３５　記憶装置
１３００　ＯＳプログラム
１３０１　管理プログラム
１３０２　残存許可一覧データ
１３０３　消去対象一覧データ
１３０４　消去可否判定一覧データ
１３０５　残存ファイル一覧データ
１３０６　ユーザ機器一覧データ
１３０７　残存ファイルデータ領域
１４１　プロセッサ
１４５　記憶装置
１４００　ＯＳプログラム
１４０１　消去プログラム
１４０２　評価依頼一覧データ
１４０３　アプリケーションプログラム
１４０４　アプリケーションデータ領域
１４０５　ファイル作成ログデータ領域

【図面】

【図１】

図1



【図２】

図2

201 残存許可ID	202 残存許可対象パス
A001	C:¥Windows¥*
A002	C:¥Program Files¥*
A003	C:¥Users¥*¥App1¥config.ini
A004	C:¥Program Data¥App3¥app.ini
:	:

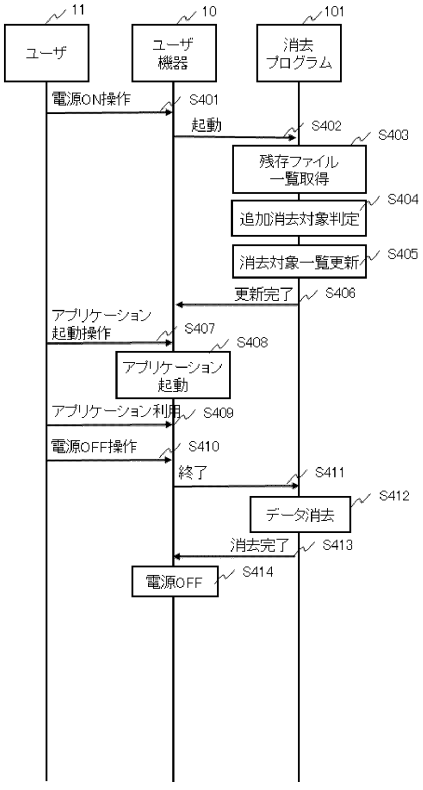
【図３】

図3

301 消去対象ID	302 消去対象パス
F001	C:¥Users¥*¥appdata¥App1¥appdata.dat
F002	C:¥Users¥*¥appdata¥App2¥data.txt
F003	C:¥Program Data¥App3¥data.dat
F004	C:¥Program Data¥App3¥data_dir¥
:	:

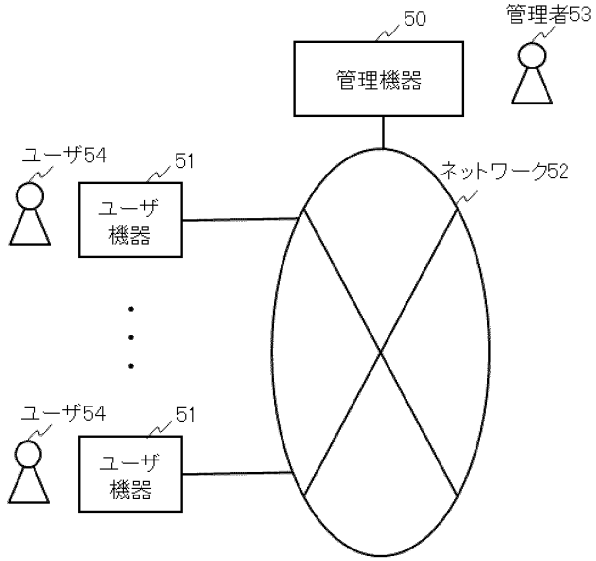
【図４】

図4



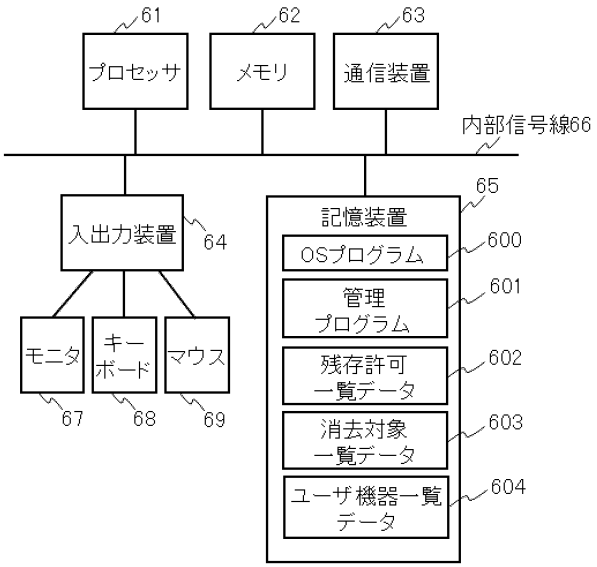
【図５】

図5



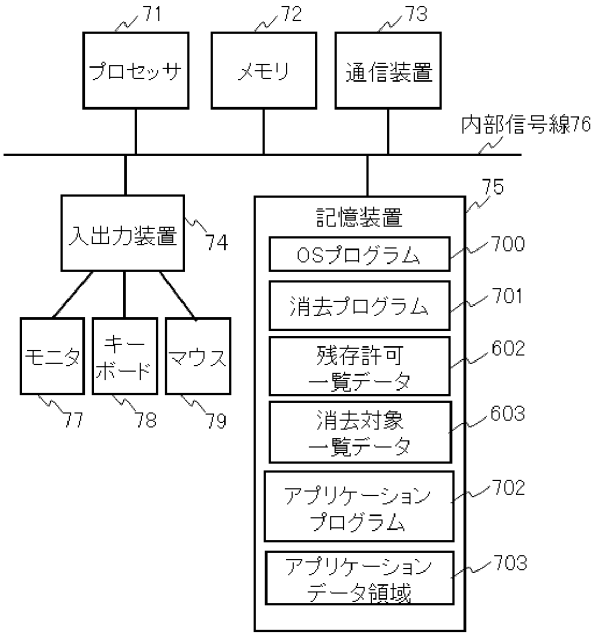
【図６】

図6



【図７】

図7



【図８】

図8

801 残存許可ID	802 残存許可対象パス
A001	C:¥Windows¥*
A002	C:¥Program Files¥*
A003	C:¥Users¥*¥App1¥config.ini
A004	C:¥Program Data¥App3¥app.ini
:	:

【図９】

図9

901 消去対象ID	902 消去対象パス
F001	C:¥Users¥*¥appdata¥App1¥appdata.dat
F002	C:¥Users¥*¥appdata¥App2¥data.txt
F003	C:¥Program Data¥App3¥data.dat
F004	C:¥Program Data¥App3¥data_dir¥
:	:

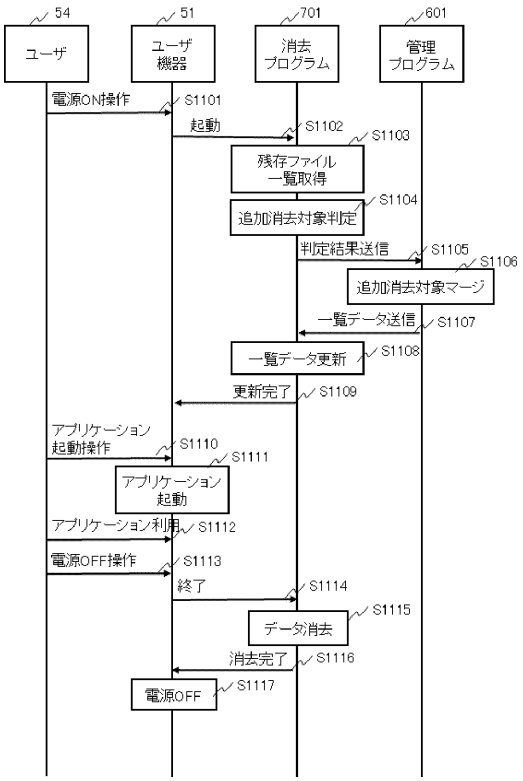
【図１０】

図10

1001 ユーザ機器ID	1002 ユーザ機器名
D001	Terminal1
D002	Terminal2
D003	Terminal3
D004	Terminal4
:	:

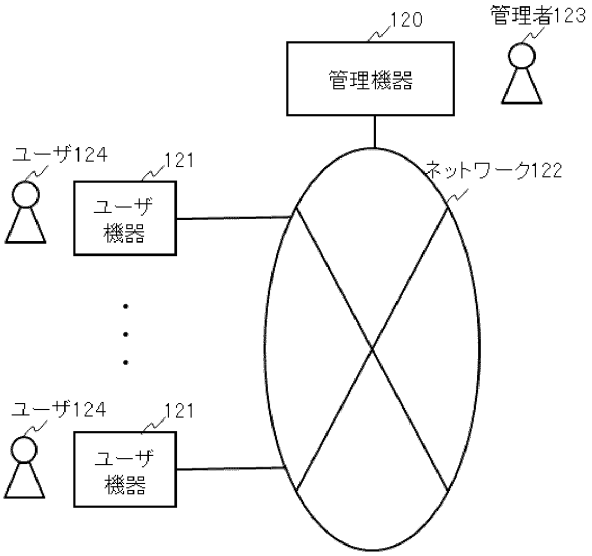
【図１１】

図11



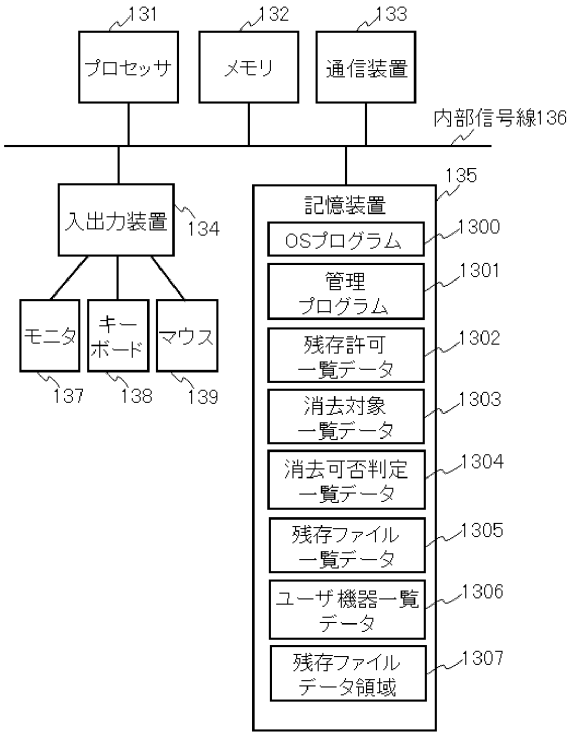
【図１２】

図12



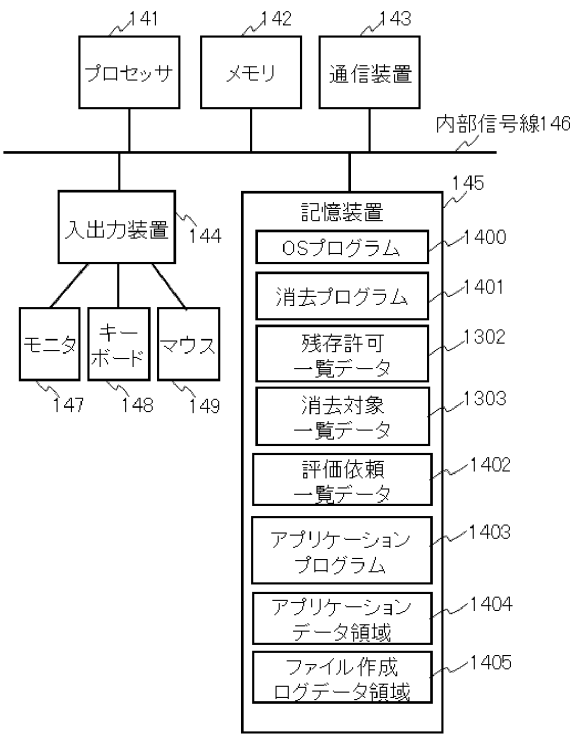
【図１３】

図13



【図１４】

図14



【図１５】

図15

1501 残存許可ID	1502 残存許可対象パス
A001	C:¥Windows¥*
A002	C:¥Program Files¥*
A003	C:¥Users¥*¥App1¥config.ini
A004	C:¥Program Data¥App3¥app.ini
:	:

【図１６】

図16

1601 消去対象ID	1602 消去対象パス
F001	C:¥Users¥*¥appdata¥App1¥appdata.dat
F002	C:¥Users¥*¥appdata¥App2¥data.txt
F003	C:¥Program Data¥App3¥data.dat
F004	C:¥Program Data¥App3¥data_dir¥
:	:

【図１７】

図17

1701 消去候補ID	1702 消去候補パス	1703 作成アプリケーション名	1704 評価ユーザ機器(1)ID	1705 評価結果(1)	1706 評価ユーザ機器(2)ID	1707 評価結果(2)
E001	C:¥Users¥**¥appdata¥App4¥data.dat	App4.exe	D001	影響無し	D003	評価中
E002	C:¥Users¥**¥appdata¥App5¥data.ini	App5.exe	D002	影響有り（警告画面表示された）	未登録	未開始
E003	C:¥ProgramData¥App6¥appdata.dat	App6.exe	D004	影響無し	D002	未開始
:	:	:	:	:	:	:

【図１８】

図18

1801 消去候補ID	1802 管理機器内保存パス
E001	C:¥manager¥filedata¥E001¥data.dat
E002	C:¥manager¥filedata¥E002¥data.ini
E003	C:¥manager¥filedata¥E003¥appdata.dat
:	:

【図１９】

図19

1901 ユーザ機器ID	1902 ユーザ機器名
D001	Terminal1
D002	Terminal2
D003	Terminal3
D004	Terminal4
:	:

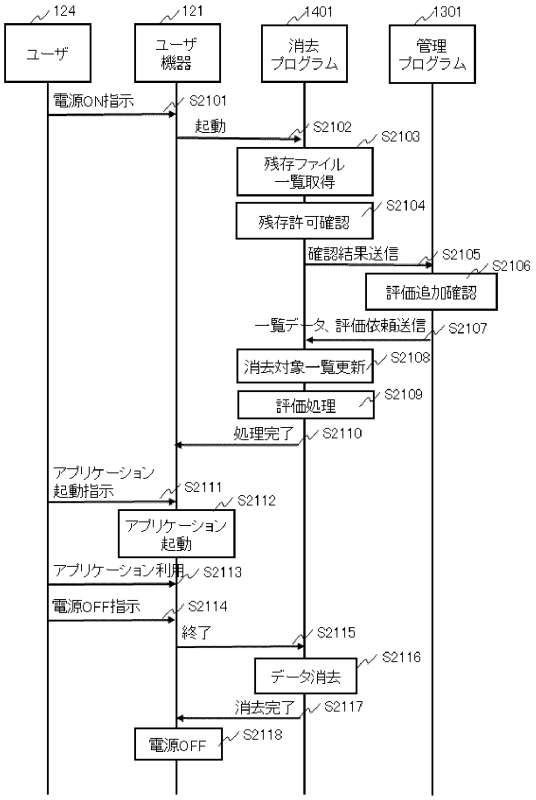
【図２０】

図20

2001 消去候補ID	2002 消去候補パス	2003 作成アプリケーション名	2004 評価満了日	2005 評価状態
E001	C:¥Users¥**¥appdata¥App4¥data.dat	App4.exe	2021/12/03	評価中
:	:	:	:	:

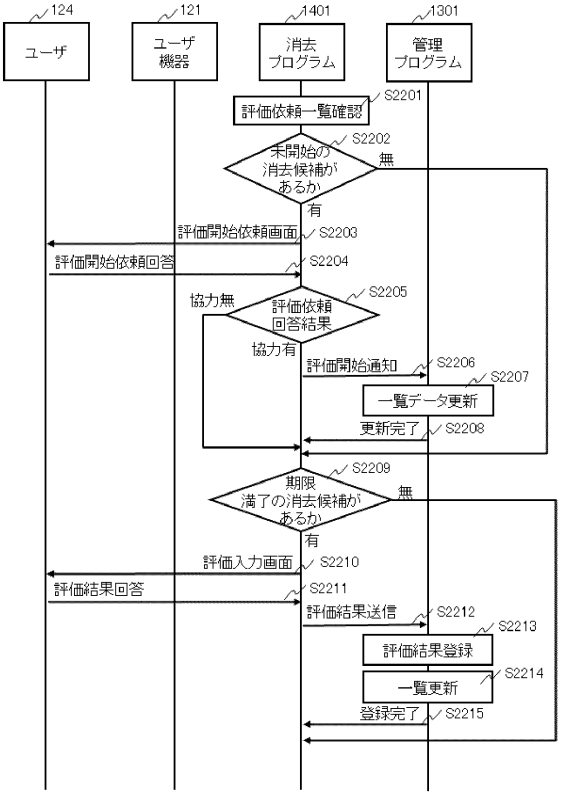
【図２１】

図21



【図２２】

図22

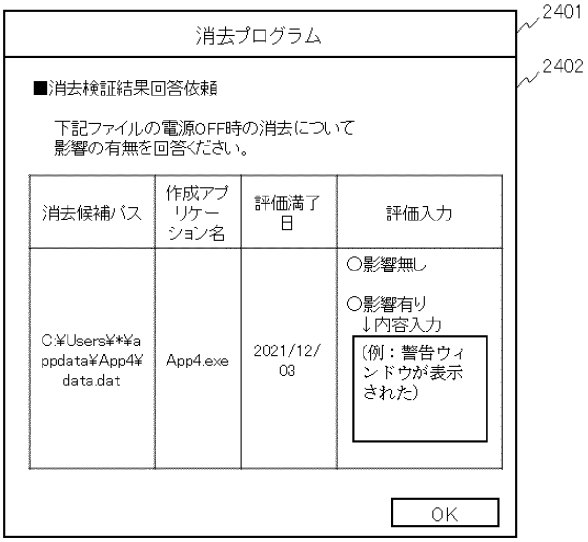


【図２３】

図23

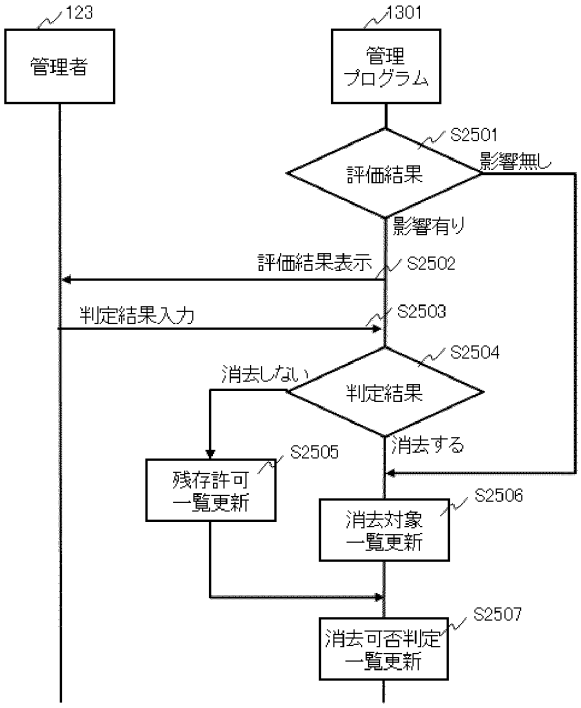
【図２４】

図24



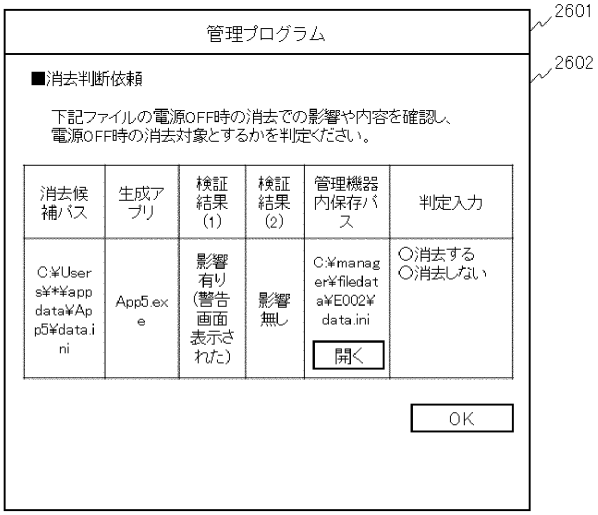
【図２５】

図25



【図２６】

図26



フロントページの続き

(56)参考文献　特開２００７－２５７６４８（ＪＰ，Ａ）
特開２０１４－００２６２３（ＪＰ，Ａ）
特開２００７－２９３６１９（ＪＰ，Ａ）
特開２００８－２５０５７４（ＪＰ，Ａ）
特開２０１９－１８５５３８（ＪＰ，Ａ）
特開２００３－３２６７７７（ＪＰ，Ａ）
特開２００９－１０４７０９（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０