【書類名】明細書
【発明の名称】記憶装置及び方法
【技術分野】
【０００１】
本発明の実施形態は、記憶装置及び方法に関する。
【背景技術】
【０００２】
近年、端末装置に接続可能な記憶装置が提供されている。インターネット等の通信ネットワークを用いて、配信サーバと端末装置との間で例えばファームウェアのアップデート処理が行われる。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１０－１５２８７７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
本発明の実施形態は、記憶装置が実装された端末装置の信頼性を向上させる。
【課題を解決するための手段】
【０００５】
実施形態の記憶装置は、サーバから送られる、処理データ及び第一認証情報を、外部機器を介して受信する受信部と、前記処理データを記憶する記憶部と、予め記憶された第一鍵と前記受信した第一認証情報と基づいて第一署名を生成する生成部と、前記第一署名及び前記第一認証情報を含んだ応答データを、前記外部機器を介して前記サーバに送信する送信部と、を備える。
【図面の簡単な説明】
【０００６】
【図１】第１実施形態に係る記憶装置の構成を示したブロック図。
【図２】第１実施形態に係る記憶装置と端末装置と配信サーバによって構成されるシステムを示した図。
【図３】第１実施形態に係るファームウェアアップデート動作を示したシーケンス図
【図４】第２実施形態に係る記憶装置と端末装置と配信サーバによって構成されるシステムを示した図。
【図５】第２実施形態に係る配信サーバの動作の一例を示したフローチャート図である。
【図６】第３実施形態に係る記憶装置の構成を示したブロック図。
【図７】第３実施形態に係る記憶装置と端末装置と配信サーバによって構成されるシステムを示した図。
【図８】第３実施形態に係るファームウェアアップデート動作を示したシーケンス図。
【図９】第４実施形態に係る記憶装置の構成を示したブロック図。
【図１０】第４実施形態に係るパッチ適用動作を示したシーケンス図。
【発明を実施するための形態】
【０００７】
以下、実施の形態について、図面を参照して説明する。
【０００８】
本明細書では、いくつかの要素に複数の表現の例を付している。なおこれら表現の例はあくまで例示であり、上記要素が他の表現で表現されることを否定するものではない。また、複数の表現が付されていない要素についても、別の表現で表現されてもよい。
【０００９】

また、図面は模式的なものであり、厚みと平面寸法との関係や各層の厚みの比率などは現実のものと異なることがある。また、図面相互間において互いの寸法の関係や比率が異なる部分が含まれることもある。

【００１０】

（第１実施形態）

図１は、第１実施形態に係る記憶装置１の構成の一例を示したブロック図である。記憶装置１は例えばＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）であるが、これに限定されず、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）でも良いし、ＨＤＤとＳＳＤを組み合わせたものでも良い。

【００１１】

記憶装置１は、例えばデータ送信部１０、データ受信部２０、暗号処理部３０、ファームウェア格納領域４０、レスポンスデータ格納領域５０、デジタル署名生成部６０、及び秘密鍵格納領域７０を有する。また、暗号処理部３０は、暗号演算部３１、及び乱数生成部３２を含む。

【００１２】

図２は、記憶装置１を備える端末装置１００と、端末装置１００にデータを送る配信サーバ２００と、によって構成されるシステムを示す。端末装置１００と配信サーバ２００とは、ＩＰネットワーク３００（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　Ｎｅｔｗｏｒｋ）によって互いに接続される。尚、端末装置１００と配信サーバ２００とは、例えば、３Ｇ・４Ｇ網やＬＴＥ（Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ）、ＴＶの放送波等の他の方式によって接続されても良い。また、本実施形態において配信サーバ２００は、端末装置１００のファームウェアをアップデートする。

【００１３】

端末装置１００は、前述の通り記憶装置１が実装される。端末装置１００は、例えばＰＯＳ（Ｐｏｉｎｔ　Ｏｆ　Ｓａｌｅ）やＭＦＰ（Ｍｕｌｔｉｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）等の端末であるが、これらに限定されず、テレビ、レコーダ、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等でも良い。尚、端末装置１００は記憶装置１の外部機器とも称され得る。

【００１４】

配信サーバ２００は、例えば端末装置１００のファームウェアのアップデートを行う場合に、ファームウェアアップデート要求とともに、アップデートデータをＩＰネットワーク３００経由で端末装置１００に配信する。

【００１５】

また、後述するが、配信サーバ２００は端末装置１００のアップデートが完了した場合に、端末装置１００からレスポンスデータを受け取る。

【００１６】

図１に戻りデータ送信部１０は、記憶装置１の外部にデータを送信する。第１実施形態では例えば、データ送信部１０は、端末装置１００を介して配信サーバ２００からデータが送信されたことに応じて、端末装置１００を介して配信サーバ２００にレスポンスデータを送信する。

【００１７】

データ受信部２０は、記憶装置１の外部からのデータを受信する。本実施形態では例えば、データ受信部２０は、端末装置１００のアップデートの際に配信サーバ２００から受け取ったアップデートデータを、端末装置１００を介して受信する。

【００１８】

尚、データ送信部１０及びデータ受信部２０は説明の便宜上別のものとして例示したが、例えばデータ送信部１０及びデータ受信部２０を一体とするデータ送受信部、又はインタフェース部としても良い。

【００１９】

暗号処理部３０は、記憶装置１が取り扱うデータの暗号処理を行う。暗号演算部３１は

、例えば記憶装置１が受信したデータに認証情報として付加されるデジタル署名を、秘密鍵格納領域７０に格納された秘密鍵を用いて暗号化する。乱数生成部３２は、例えば予め設定された時間ごとに、データ受信部２０によって受信されたデータの有効性を判断するための乱数を生成する。

【００２０】

ファームウェア格納領域４０は、端末装置１００のファームウェアデータ、及び配信サーバ２００から配信されたアップデートデータを格納する。

【００２１】

レスポンスデータ格納領域５０は、配信サーバ２００に送られ、記憶装置１内で生成されたレスポンスデータを、一時的に格納する。

【００２２】

デジタル署名生成部６０は、配信サーバ２００から送られたチャレンジデータのデジタル署名を生成する。尚、当該デジタル署名はレスポンスデータとしてレスポンスデータ格納領域５０に格納される。

【００２３】

秘密鍵格納領域７０は、デジタル署名生成部６０がデジタル署名を生成する際に用いられる秘密鍵を格納する。

【００２４】

図３は、第１実施形態に係るファームウェアアップデート動作を示したシーケンス図である。以下、図３を参照して端末装置１００のファームウェアアップデート動作を説明する。

【００２５】

初めに配信サーバ２００は、端末装置１００のファームウェアをアップデートする必要が生じた場合、端末装置１００に対してファームウェアアップデート要求を発行する（Ｓ１．１）。このとき、配信サーバ２００は、ファームウェアアップデート要求と同時にアップデートデータを端末装置１００に送信する。

【００２６】

尚、配信サーバ２００は初めにファームウェアアップデート要求のみを端末装置１００に送り、端末装置１００がアップデート可能な状態であるかを確認してレスポンスを受け取った後で、アップデートデータを端末装置１００に送信するような構成としても良い。

【００２７】

以降、「ファームウェアアップデート要求」は、アップデートデータを含んでいるとして説明を行う。尚、本実施形態において「アップデートデータ」は、新ファームウェアのプログラムデータ並びにチャレンジデータを含んでいる。

【００２８】

端末装置１００は、配信サーバ２００から受け取ったファームウェアアップデート要求を、例えば専用のコマンドを使用して記憶装置１に送信する（Ｓ１．２）。記憶装置１のデータ受信部２０を介して受け取られたアップデートデータは、記憶装置１のファームウェア格納領域４０に書き込まれる。すなわち、ファームウェア格納領域４０内には、新ファームウェアのプログラムデータが格納される（Ｓ１．３）。

【００２９】

次に、記憶装置１において、デジタル署名生成部６０は、秘密鍵格納領域７０に予め格納された秘密鍵を用いて、アップデートデータ内に含まれるチャレンジデータのデジタル署名を生成する（Ｓ１．４）。生成されたデジタル署名は、チャレンジデータと併せてレスポンスデータとしてレスポンスデータ格納領域５０に格納される（Ｓ１．５）。記憶装置１は、ファームウェアアップデート要求に応じた処理を終了し、データ送信部１０を介してコマンドを端末装置１００に返す（Ｓ１．６）。

【００３０】

端末装置１００は、記憶装置１からコマンドを受けると、レスポンスデータ要求を記憶装置１に発行する（Ｓ１．７）。

【００３１】
記憶装置１は、データ受信部２０を介してレスポンスデータ要求を受けると、レスポンスデータ格納領域５０からレスポンスデータを取得し（Ｓ１．８）、データ送信部１０を介して端末装置１００に当該レスポンスデータ（コマンド）を送信する（Ｓ１．９）。
【００３２】
端末装置１００はコマンドを受け取ると、レスポンスデータとともにアップデート完了通知を配信サーバ２００に発行する（Ｓ１．１０）。配信サーバ２００は、受信したレスポンスデータのデジタル署名の認証を行うことで、端末装置１００のファームウェアアップデートが正しく完了したことを確認できる。
【００３３】
ここで、配信サーバ２００と端末装置１００との間で実行されるチャレンジ・レスポンス認証を説明する。配信サーバ２００が端末装置１００に対してファームウェアアップデート要求を発行する。端末装置１００は、ファームウェアアップデート要求とともにチャレンジデータを受け取る。その後、配信サーバ２００が、最終的に端末装置１００からレスポンスデータを受け取れば、チャレンジ・レスポンス認証完了となり、正しくファームウェアアップデートが行われたと判断される。
【００３４】
しかし、例えば端末装置１００が外部から不正アクセスされた場合、認証を偽ることでファームウェアアップデート完了が詐称される虞が有る。具体的には、端末装置１００はレスポンスデータを配信サーバ２００に返すが、新ファームウェアを記憶装置１に送らず、実際にはファームウェアの更新が行われない等の問題が生じ得る。
【００３５】
また、端末装置１００がウィルス等に感染している場合にも、前述と同様の問題が起こる虞が有る。さらには、ファームウェアの更新が端末装置１００によって妨げられる虞もある。
【００３６】
そこで本実施形態では、配信サーバ２００と記憶装置１との間でチャレンジ・レスポンス認証が行われる。
【００３７】
一般に記憶装置１は、端末装置１００から独立した専用のハードウェアで構成される。このため、端末装置１００と比較して外部からの不正なアクセスや改竄が困難である。このような記憶装置１と配信サーバ２００との間でチャレンジ・レスポンス認証を行うことで、ファームウェアアップデートが正しく完了したことを確認できる。
【００３８】
また、端末装置１００が不正なアクセスを受けて不正な操作をされた場合に、ファームウェアアップデートが正しく行われない状況を配信サーバ２００や記憶装置１が検出できる。このため、端末装置１００に対するＩＰネットワーク３００からの遮断や、保守員による初期化等の対策を迅速に行うことが可能になる。さらに、再起動をする際に、不正にアクセスすることが可能なファームウェアを起動しない等の対策を施すことも可能である。
【００３９】
（第２実施形態）
図４は、第２実施形態に係る記憶装置１が実装された端末装置１００及び配信サーバ２００によって構成されるシステムを示す。また図５は、第２実施形態における配信サーバ２００の動作の一例を示したフローチャート図である。尚、本実施形態の説明において、第１実施形態と同様の構成については、同様の符号を付して詳細な説明を省略する。
【００４０】
本実施形態において配信サーバ２００は、図４に示すようにタイマ２０１を有する。配信サーバ２００は、端末装置１００に対するファームウェアアップデート要求の発行に応じて、タイマ２０１を起動させる。この構成により、配信サーバ２００は、予め設定した

所定の時間内に端末装置１００からレスポンスデータ（アップデート完了通知）が送られてこない場合は、ファームウェアアップデートが正しく行われなかったと判断できる。
【００４１】
尚、「所定の時間」は、配信サーバの管理者が設定した値であっても良いし、ファームウェアアップデート要求とともに送られるアップデートデータ（特に新ファームウェア）の大きさや、ファームウェアアップデート処理の煩雑さ等に応じて適宜変更可能としても良い。
【００４２】
一般にタイマ２０１で設定する所定の時間は、アップデートデータが大きい場合は、アップデートデータが小さい場合よりも長く設定される方が望ましい。これは、アップデートデータの大きさが大きいほうが、ファームウェアアップデートに時間が掛かるからである。
【００４３】
また、タイマ２０１で計測する所定の時間は、ファームウェアアップデート処理の内容によって変更される構成としても良い。例えば、ファームウェアアップデートの内容が、アップデートデータを記憶装置１のファームウェア格納領域４０に追加（すなわち書き込み）する内容である場合を考える。この場合、ファームウェアアップデートの内容が、ファームウェア格納領域４０に既に格納されているファームウェアを変更（すなわち書き換え）する内容である場合より、ファームウェアアップデートに要する時間が短い。
【００４４】
例えば記憶装置１がＨＤＤである場合は、既存のデータに変更が生じると、既存のデータに対して新たなデータを上書きする。このため、空き領域にデータを書き込む場合と比較して、書き込みに要する時間はさほど変わらない。
【００４５】
一方で、記憶装置１がＳＳＤである場合、既存のデータを新たなデータに変更する場合、既存のデータのうち、不要となったものを消去する必要がある。一般にＳＳＤに用いられるフラッシュメモリは、書き込みよりも消去に時間が掛かるとされている。
【００４６】
ファームウェアアップデートにおいては、例えばファームウェア格納領域４０に格納されている更新前のファームウェアを消去して、新たなアップデートデータをファームウェア格納領域４０に格納する必要がある。このため、空き領域にデータを書き込む場合よりも時間が掛かる。
【００４７】
また、一般にＳＳＤはＨＤＤよりも書き込み速度が速い。よって、記憶装置１の種類に応じて、前述した「所定の時間」を変更できる構成としても良い。
【００４８】
図５に基づいて、本実施形態における配信サーバ２００の動作の一例を示す。配信サーバ２００は、端末装置１００のファームウェアをアップデートする必要が生じた場合、端末装置１００に対してファームウェアアップデート要求を発行する（Ｓ２．１）。
【００４９】
次に配信サーバ２００は、このファームウェアアップデート要求の発行に応じて、タイマ２０１を起動させ、経過時間ｔの計測を開始する（Ｓ２．２）。尚、ファームウェアアップデート要求とタイマ２０１の起動の順番は、逆でも良い。いずれの場合においても、Ｓ２．１とＳ２．２との間の時間が短いほうが望ましい。
【００５０】
その後、ファームウェアアップデート要求の発行から、所定の時間Ｔを経過したかが確認され（Ｓ２．３）、ｔ≧Ｔである場合、端末装置１００及び記憶装置１からのレスポンスが有るかが確認される（Ｓ２．４）。
【００５１】
Ｓ２．４で配信サーバ２００が、端末装置１００及び記憶装置１からのレスポンスを受

けていない場合（Ｓ２．４のＮｏ）、ファームウェアアップデートに失敗したと推定可能である。
【００５２】
また、Ｓ２．４で配信サーバ２００が、端末装置１００及び記憶装置１からのレスポンスを受けた場合（Ｓ２．４のＹｅｓ）、第１実施形態と同様に配信サーバ２００はレスポンス認証を行い（Ｓ２．５）、認証結果からアップデートが正しく行われたかを判断する。
【００５３】
レスポンス認証に成功した場合（Ｓ２．５のＹｅｓ）、端末装置１００のファームウェアアップデートに成功したことを、配信サーバ２００が認識する。一方で、レスポンス認証に失敗した場合（Ｓ２．５のＮｏ）、端末装置１００のファームウェアアップデートに失敗したことを、配信サーバ２００が認識する。
【００５４】
本実施形態で示した構成では配信サーバ２００は、第１実施形態で説明したようなチャレンジ・レスポンス認証の結果からだけでなく、端末装置１００及び記憶装置１からのレスポンスが所定の時間内に返ってこなかった場合に、ファームウェアアップデートが正しく実行されなかったと認識可能である。
【００５５】
このような構成により、例えば所定の時間が経過しても配信サーバにレスポンスデータが返ってこない場合、その要因が、端末装置１００がウィルス等に感染していることや、外部からの不正なアクセスや改竄等によるものであると推定される。その結果、ＩＰネットワーク３００からの遮断や、保守員による初期化等の対策を迅速に行うことが可能になる。
【００５６】
尚、本実施形態においてタイマ２０１は、必ずしも第１実施形態で示した配信サーバ２００に新たに設けられる必要は無く、配信サーバ２００の有するハードウェア構成又は機能の中に、計時機能が含まれている場合は、これを本実施形態におけるタイマ２０１として転用しても良い。
【００５７】
（第３実施形態）
図６は、第３実施形態に係る記憶装置１の構成の一例を示したブロック図である。また図７は、第３実施形態に係る記憶装置１が実装された端末装置１００及び配信サーバ２００によって構成されるシステムを示す。尚、第３実施形態の説明において、第１実施形態及び第２実施形態と同様の構成については、同様の符号を付して詳細な説明を省略する。
【００５８】
図６に示すように、記憶装置１は、公開鍵格納領域８０を有し、公開鍵格納領域８０には配信サーバ２００の公開鍵が格納される。
【００５９】
また、記憶装置１は認証部３５を有する。認証部３５は、公開鍵格納領域８０に格納された公開鍵を用いて、認証を行う。
【００６０】
さらに図７に示すように、配信サーバ２００は、秘密鍵格納領域２０２及びデジタル署名生成部２０３をさらに備える。秘密鍵格納領域２０２には、配信サーバ２００の秘密鍵が格納される。デジタル署名生成部２０３は、チャレンジデータに対するデジタル署名を生成する。
【００６１】
図８は、第３実施形態に係るファームウェアアップデート動作を示したシーケンス図である。以下、図８を参照して第３実施形態に係る端末装置１００のファームウェアアップデート動作を説明する。
【００６２】

配信サーバ２００は、端末装置１００のファームウェアをアップデートする必要が生じた場合、端末装置１００に対してファームウェアアップデート要求を発行する（Ｓ３．１）。このとき、配信サーバ２００は、ファームウェアアップデート要求と同時にアップデートデータを端末装置１００に送信する。尚、第３実施形態においてアップデートデータは、新ファームウェアのプログラムデータ並びに第一チャレンジデータを含んでいる。

【００６３】

端末装置１００は、配信サーバから受け取ったファームウェアアップデート要求を、例えば専用のコマンドを使用して記憶装置１に送信する（Ｓ３．２）。記憶装置１のデータ受信部２０を介して受け取られたアップデートデータは、記憶装置１のファームウェア格納領域４０に書き込まれ、ファームウェア格納領域４０内には、新ファームウェアのプログラムデータが格納される（Ｓ３．３）。

【００６４】

次に、記憶装置１において、デジタル署名生成部６０は、秘密鍵格納領域７０に予め格納された秘密鍵を用いて、アップデートデータ内に含まれる第一チャレンジデータの第一デジタル署名を生成する（Ｓ３．４）。生成された第一デジタル署名は、第一チャレンジデータと併せて第一レスポンスデータとしてレスポンスデータ格納領域５０に格納される（Ｓ３．５）。記憶装置１は、ファームウェアアップデート要求に応じた処理を終了し、データ送信部１０を介してコマンドを端末装置１００に発行する（Ｓ３．６）。

【００６５】

端末装置１００は、記憶装置１からのコマンドを受けると、第一レスポンスデータ要求を記憶装置１に発行する（Ｓ３．７）。

【００６６】

記憶装置１は、データ受信部２０を介して第一レスポンスデータ要求を受けると、レスポンスデータ格納領域５０から第一レスポンスデータを取得し（Ｓ３．８）、併せて、第二チャレンジデータを生成する（Ｓ３．９）。記憶装置１は、データ送信部１０を介して、第一レスポンスデータを端末装置１００に送信する（Ｓ３．１０）。

【００６７】

第３実施形態では、記憶装置１は、第一デジタル署名だけでなく第二チャレンジデータも端末装置１００に送信する。したがって端末装置１００が記憶装置１から受け取る第一レスポンスデータには、第一チャレンジデータの第一デジタル署名、及び第二チャレンジデータが含まれる。

【００６８】

端末装置１００は、記憶装置１からのコマンドを受けると、第二レスポンスデータ要求を配信サーバ２００に発行する（Ｓ３．１１）。このとき、第一レスポンスデータが端末装置１００から配信サーバ２００に送信される。

【００６９】

端末装置１００から第二レスポンスデータ要求を受け取ると、配信サーバ２００において、デジタル署名生成部２０３は、配信サーバ２００の秘密鍵格納領域２０２に予め格納された秘密鍵を用いて、第一レスポンスデータ内に含まれる第二チャレンジデータの第二デジタル署名を生成する（Ｓ３．１２）。生成された第二デジタル署名は、第二レスポンスデータとして端末装置１００に送信される（Ｓ３．１３）。

【００７０】

第二レスポンスデータを受け取った端末装置１００は、専用コマンドを記憶装置１に送信する（Ｓ３．１４）。

【００７１】

端末装置１００から第二デジタル署名を受け取った記憶装置１は、このコマンドで送られてきた第二レスポンスデータの認証を行う。具体的には、認証部３５が、配信サーバ２００の公開鍵を使用して第二レスポンスデータを検証することで、配信サーバ２００での認証が成功したかを記憶装置１が確認できる。

【００７２】

以上、上述したように第３実施形態では、配信サーバ２００と記憶装置１との間で、端末装置１００を介して、相互のチャレンジ・レスポンス認証が行われる。尚、本実施形態では記憶装置１は、配信サーバ２００から受け取った第一チャレンジデータに対するレスポンスを返す際に第二チャレンジデータを配信サーバ２００に送り、第二チャレンジデータに対するレスポンスを配信サーバ２００から受け取る構成となっている。

【００７３】

換言すれば、本実施形態において配信サーバ２００と記憶装置１とは、双方向に対してチャレンジ・レスポンス認証を行う。

【００７４】

したがって記憶装置１は、第二チャレンジデータに対するレスポンスを配信サーバ２００から受け取ることで、端末装置１００のファームウェアアップデートが正しく行われたかを確認することができる。

【００７５】

さらに、チャレンジ・レスポンス認証の結果に問題がある場合は、例えばファームウェアアップデートの失敗を示した情報を端末装置１００に出力することで、端末装置１００のユーザはファームウェアアップデートに失敗したことを知ることができる。尚この場合、例えば端末装置１００に備えられたディスプレイ等でユーザにファームウェアアップデートの失敗を通知することが可能である。

【００７６】

また、チャレンジ・レスポンス認証の結果に問題がある場合は、端末装置１００を次に起動する際に、記憶装置１が記憶しているファームウェアを端末装置１００が実行できないように（無効に）しても良い。

【００７７】

（第４実施形態）

第１実施形態乃至第３実施形態で示した配信サーバ２００と記憶装置１とのチャレンジ・レスポンス認証は、必ずしもファームウェアアップデートに用いられる必要は無い。

【００７８】

第４実施形態において配信サーバ２００は、例えば端末装置１００で実行されるＯＳへのパッチ適用が正しく行われたかどうかを、記憶装置１とのチャレンジ・レスポンス認証によって確認する構成としても良い。

【００７９】

図９は、第４実施形態に係る記憶装置１の構成の一例を示したブロック図である。また、図１０は、第４実施形態に係るパッチ適用動作を示したシーケンス図である。以下、図９及び図１０を参照して端末装置１００のパッチ適用動作を説明する。

【００８０】

配信サーバ２００は、必要に応じて端末装置１００に対してパッチ適用要求を発行する（Ｓ４．１）。尚「パッチ適用要求」は、パッチ適用に用いられるパッチデータと、チャレンジデータとを含んでいる。

【００８１】

端末装置１００は、配信サーバ２００から受け取ったパッチ適用要求を、例えば専用のコマンドを使用して記憶装置１に送信する（Ｓ４．２）。記憶装置１が受け取ったパッチデータは記憶装置１のパッチデータ格納領域９０に書き込まれる（Ｓ４．３）。

【００８２】

次に、記憶装置１において、デジタル署名生成部６０は、予め格納された秘密鍵を用いて、チャレンジデータのデジタル署名を生成する（Ｓ４．４）。生成されたデジタル署名は、チャレンジデータと併せてレスポンスデータとしてレスポンスデータ格納領域５０に格納される（Ｓ４．５）。記憶装置１は、パッチ適用要求に応じた処理を終了し、コマンドを端末装置１００に返す（Ｓ４．６）。

【００８３】

端末装置１００は、記憶装置１からのコマンドを受けると、レスポンスデータ要求を記

憶装置１に発行する（Ｓ４．７）。
【００８４】
記憶装置１はレスポンスデータ要求を受けると、レスポンスデータを取得して（Ｓ４．８）、端末装置１００に当該レスポンスデータ（コマンド）を送信する（Ｓ４．９）。
【００８５】
端末装置１００は記憶装置１からのコマンドを受け取ると、レスポンスデータとともにパッチ適用完了通知を配信サーバ２００に発行する（Ｓ４．１０）。配信サーバ２００は、受信したレスポンスデータのデジタル署名の認証を行うことで、端末装置１００のパッチ適用が正しく完了したことを確認できる。
【００８６】
尚、第２実施形態のように、配信サーバ２００がパッチ適用を開始する際にタイマを設定し、所定の時間内に記憶装置１からレスポンスデータが返ってこない場合に、パッチ適用が正しく実行されなかったと確認できる構成としても良い。
【００８７】
また、第３実施形態のように、記憶装置１がレスポンスデータを返す際に、記憶装置１が任意に生成した新たなチャレンジデータをレスポンスデータとともに配信サーバ２００に送り、この新たなチャレンジデータに対する新たなレスポンスデータを記憶装置１に送るような構成とすることで、配信サーバ２００と記憶装置１とが互いにチャレンジ・レスポンス認証を行っても良い。
【００８８】
以上の説明より、本実施形態において配信サーバ２００は、端末装置１００のパッチ適用が正しく行われたかを確認することができる。
【００８９】
また、端末装置１００が不正なアクセスを受けて不正な操作をされた場合に、パッチ適用が正しく行われない状況を配信サーバ２００や記憶装置１が検出できるため、ＩＰネットワーク３００からの遮断や、保守員による初期化等の対策を迅速に行うことが可能になる。
【００９０】
尚、第１実施形態乃至第４実施形態では、配信サーバ２００は、ファームウェアのプログラムデータやパッチデータを、端末装置１００を介して記憶装置１に送信したが、扱われるデータはこれらに限られず、例えばパラメータデータ等であっても良い。
【００９１】
また、第１実施形態乃至第４実施形態では、配信サーバ２００、端末装置１００、及び記憶装置１の間で様々なコマンド（命令・応答）がＩ／Ｆを介してやり取りされる。しかし、応答コマンドは、Ｉ／Ｆでなく、他の接続端子を利用したスタティック（静的な）信号でも良い。
【００９２】
さらに、記憶装置１は、ファームウェアのプログラムデータを受信後すぐにファームウェアを書き換えるのではなく、例えばＲＡＭ等の揮発メモリに一時的に格納し、チャレンジ・レスポンス認証が完了した後でファームウェアを更新する構成としても良い。
【００９３】
以上、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等に含まれる。
【符号の説明】
【００９４】
１：記憶装置、１０：データ送信部、２０：データ受信部、３０：暗号処理部、３５：認

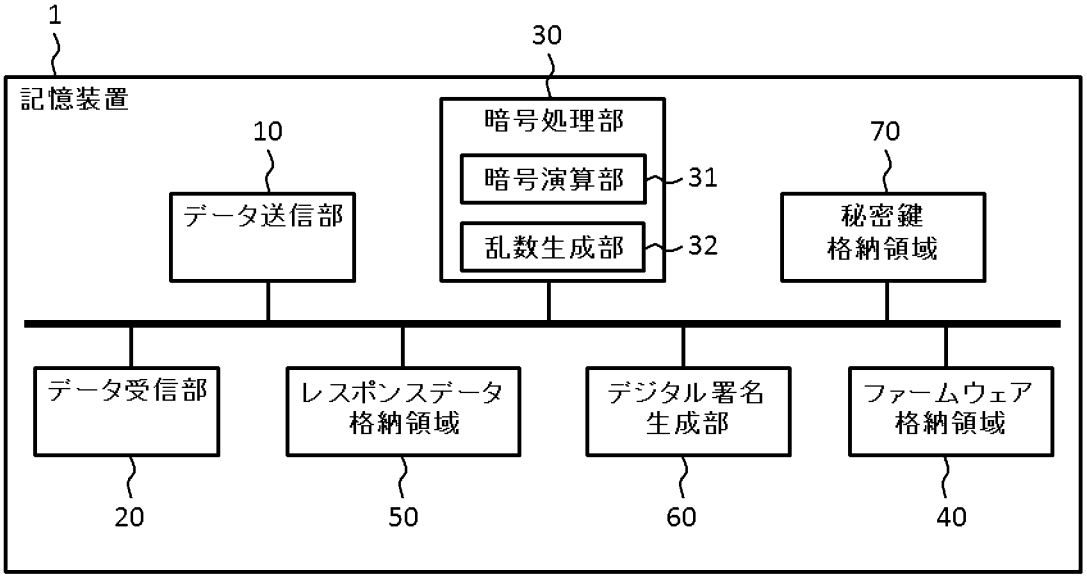
証部、４０：ファームウェア格納領域、５０：レスポンスデータ格納領域、６０：デジタル署名生成部、７０：秘密鍵格納領域、８０：公開鍵格納領域、９０：パッチデータ格納領域、１００：端末装置、２００：配信サーバ、３００：ＩＰネットワーク。

【書類名】特許請求の範囲
【請求項１】
　サーバから送られる、処理データ及び第一認証情報を、外部機器を介して受信する受信部と、
　前記処理データを記憶する記憶部と、
　予め記憶された第一鍵と前記受信した第一認証情報と基づいて第一署名を生成する生成部と、
　前記第一署名及び前記第一認証情報を含んだ応答データを、前記外部機器を介して前記サーバに送信する送信部と、
　を備えた記憶装置。
【請求項２】
　前記応答データは、前記記憶部に一時的に保存されるとともに、前記外部機器からの命令に応じて前記サーバに送信される請求項１に記載の記憶装置。
【請求項３】
　前記応答データは、前記サーバを認証するための第二認証情報をさらに含み、
　該第二認証情報と、該第二認証情報に対応し前記外部機器を介して前記サーバから受信した第二署名とに基づいて認証を行う認証部を更に備える請求項１または請求項２に記載の記憶装置。
【請求項４】
　前記認証に失敗した場合、前記外部機器に対して認証の失敗を示す情報を出力する請求項３に記載の記憶装置。
【請求項５】
　前記処理データは、前記外部機器のファームウェアのプログラムデータを含む請求項１乃至請求項４のいずれか一項に記載の記憶装置。
【請求項６】
　記憶部を備えた記憶装置において、
　サーバから送られる、処理データ及び第一認証情報を、外部機器を介して受信し、
　予め記憶された鍵と前記第一認証情報とに基づいて署名を生成し、
　前記署名及び前記第一認証情報を含んだ応答データを、前記外部機器を介して前記サーバに送信する
　ことを含んだ認証方法。
【請求項７】
　処理データを配信するサーバでの認証方法であって、
　記憶装置に前記処理データ及び第一認証情報を、外部機器を介して送信し、
　前記第一認証情報に基づいた第一署名及び前記第一認証情報を含んだ応答データを、前記外部機器を介して受信し、
　前記応答データを参照し、前記記憶装置との認証に成功したかを確認する
　ことを含んだ認証方法。
【請求項８】
　記憶装置と接続された端末装置での認証方法であって、
　サーバから送られる、処理データ及び第一認証情報を受信し、
　前記処理データ及び前記第一認証情報を、前記記憶装置に送信し、
　前記第一認証情報に基づいた第一署名及び前記第一認証情報を含んだ応答データを、前記記憶装置から受信し、
　前記応答データを、前記サーバに送信する
　ことを含んだ認証方法。

【書類名】要約書
【要約】
【課題】本発明の実施形態は、記憶装置が実装された端末装置の信頼性を向上させる。
【解決手段】実施形態の記憶装置は、サーバから送られる、処理データ及び第一認証情報を、外部機器を介して受信する受信部と、前記処理データを記憶する記憶部と、予め記憶された第一鍵と前記受信した第一認証情報と基づいて第一署名を生成する生成部と、前記第一署名及び前記第一認証情報を含んだ応答データを、前記外部機器を介して前記サーバに送信する送信部と、を備える。
【選択図】図１

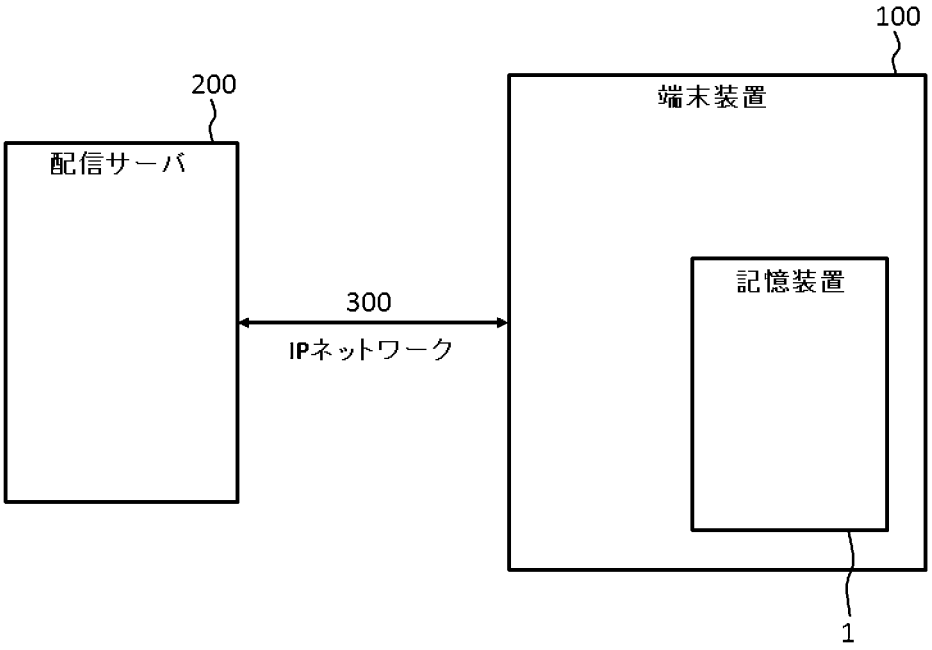
【書類名】図面
【図１】

図1


1
30
記憶装置
10
暗号処理部
暗号演算部
31
乱数生成部
32
70
データ送信部
秘密鍵
格納領域
データ受信部
レスポンスデータ
格納領域
デジタル署名
生成部
ファームウェア
格納領域
20
50
60
40

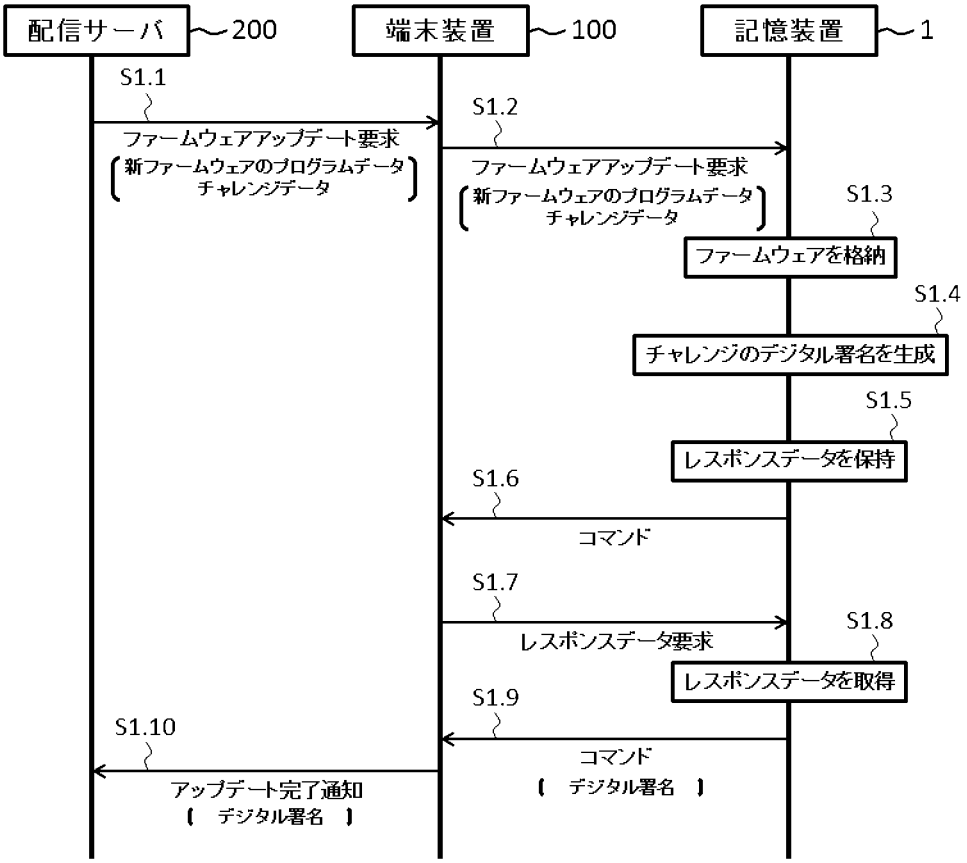
【図２】

図２


100
端末装置
200
配信サーバ
記憶装置
300
IPネットワーク
1

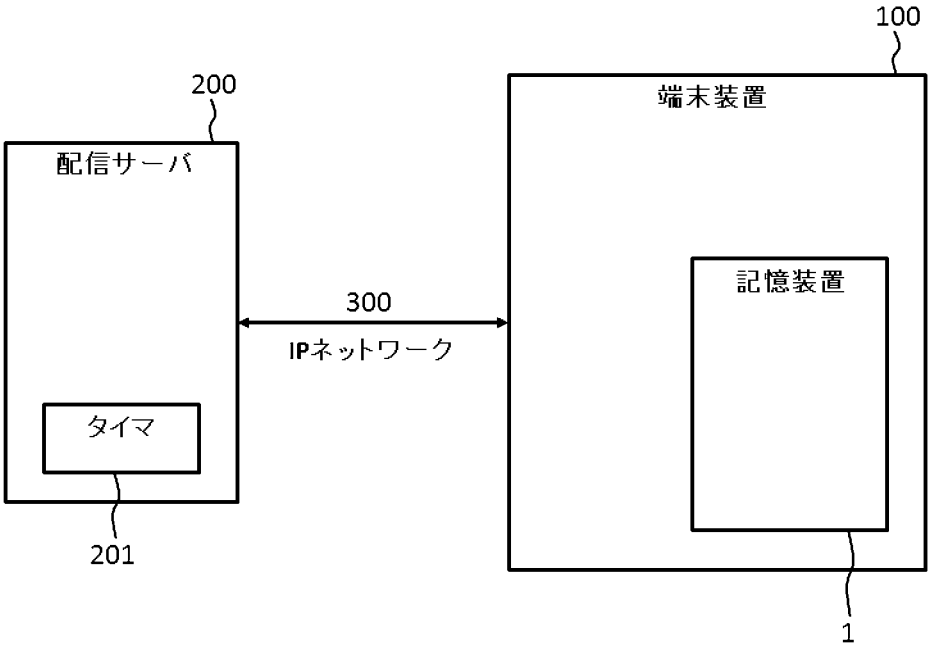
【図３】

図３


配信サーバ
200
端末装置
100
記憶装置
1
S1.1
ファームウェアアップデート要求
新ファームウェアのプログラムデータ
チャレンジデータ
S1.2
ファームウェアアップデート要求
新ファームウェアのプログラムデータ
チャレンジデータ
S1.3
ファームウェアを格納
S1.4
チャレンジのデジタル署名を生成
S1.5
レスポンスデータを保持
S1.6
コマンド
S1.7
レスポンスデータ要求
S1.8
レスポンスデータを取得
S1.9
コマンド
デジタル署名
S1.10
アップデート完了通知
デジタル署名

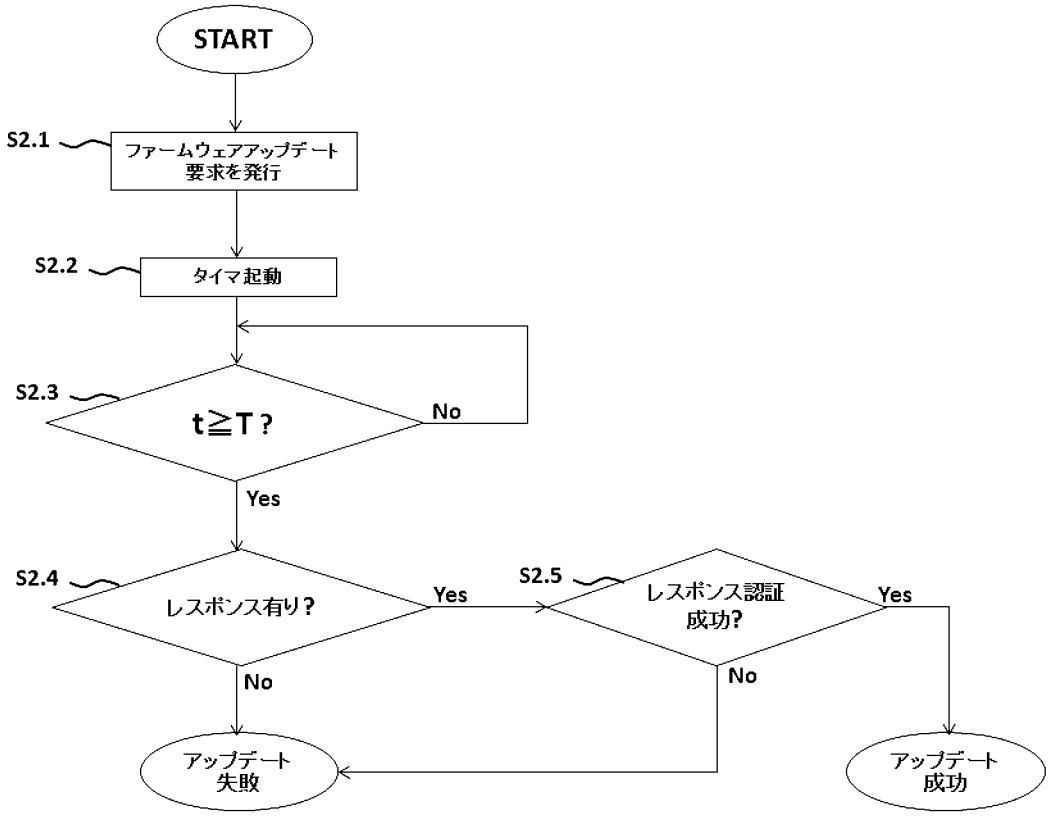
【図４】

図4


100
端末装置
200
配信サーバ
記憶装置
300
IPネットワーク
タイマ
201
1

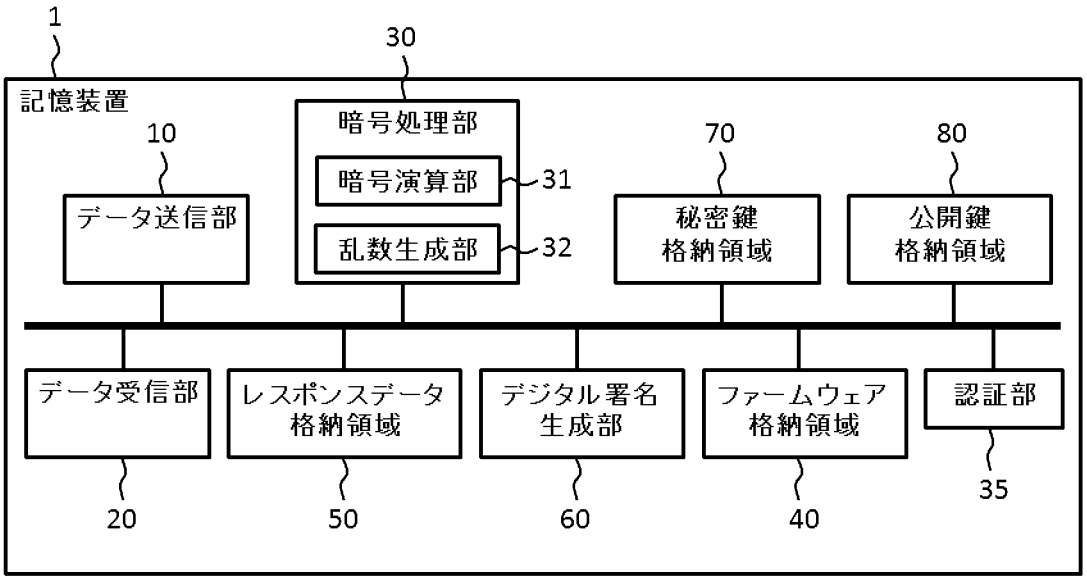
【図５】

図5


START
S2.1
ファームウェアアップデート
要求を発行
S2.2
タイマ起動
S2.3
t≧T?
No
Yes
S2.4
レスポンス有り?
Yes
S2.5
レスポンス認証
成功?
Yes
No
No
アップデート
失敗
アップデート
成功

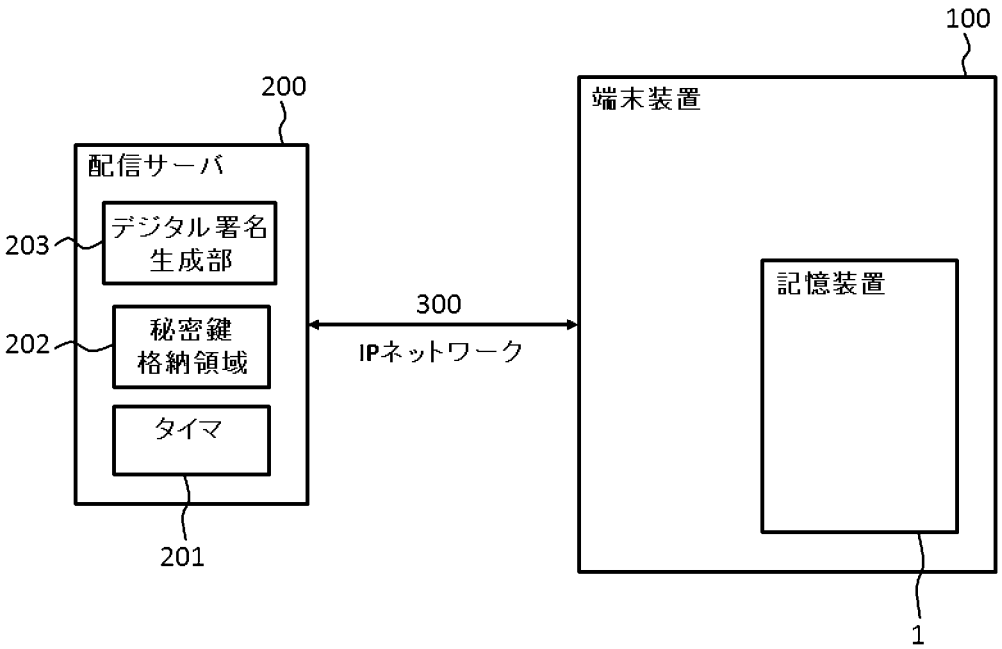
【図６】

図6


1
30
記憶装置
10
暗号処理部
暗号演算部
31
乱数生成部
32
70
80
データ送信部
秘密鍵
格納領域
公開鍵
格納領域
データ受信部
レスポンスデータ
格納領域
デジタル署名
生成部
ファームウェア
格納領域
認証部
20
50
60
40
35

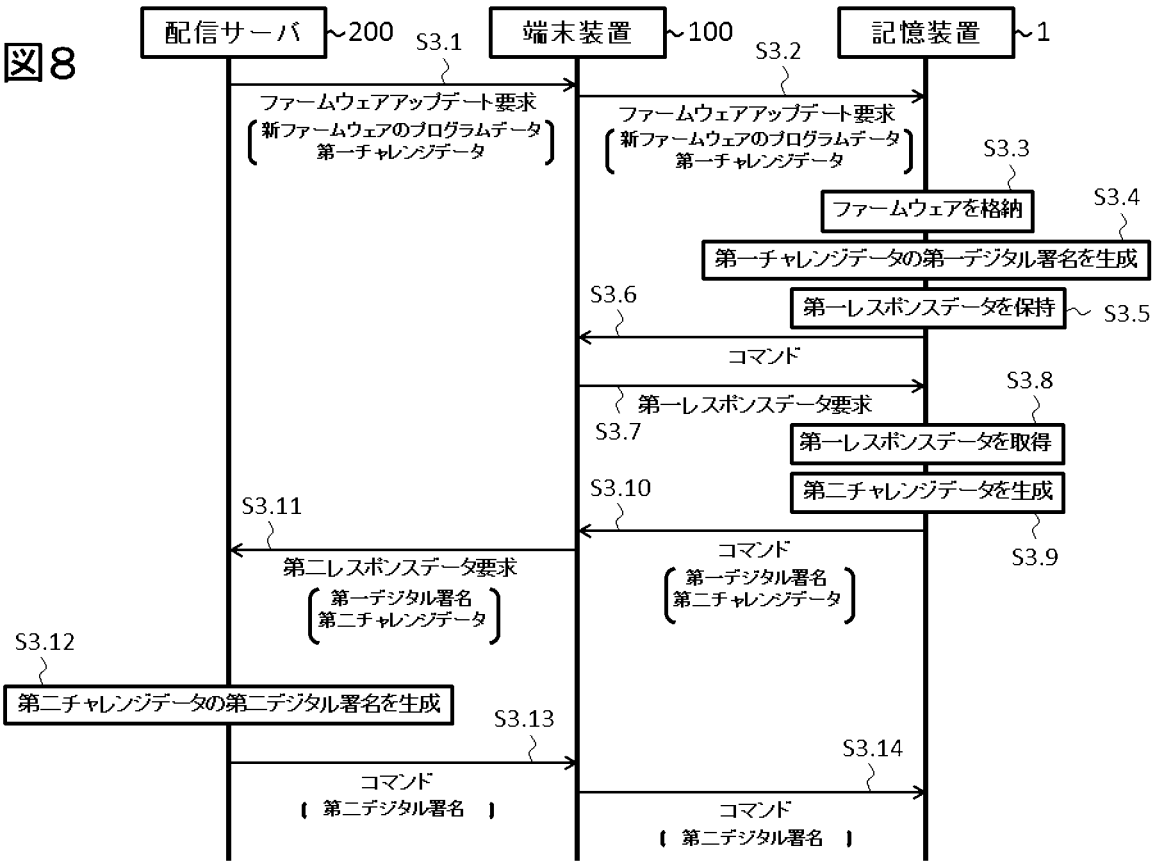
【図７】

図7


100
200
端末装置
配信サーバ
203
デジタル署名
生成部
202
秘密鍵
格納領域
タイマ
300
IPネットワーク
記憶装置
201
1

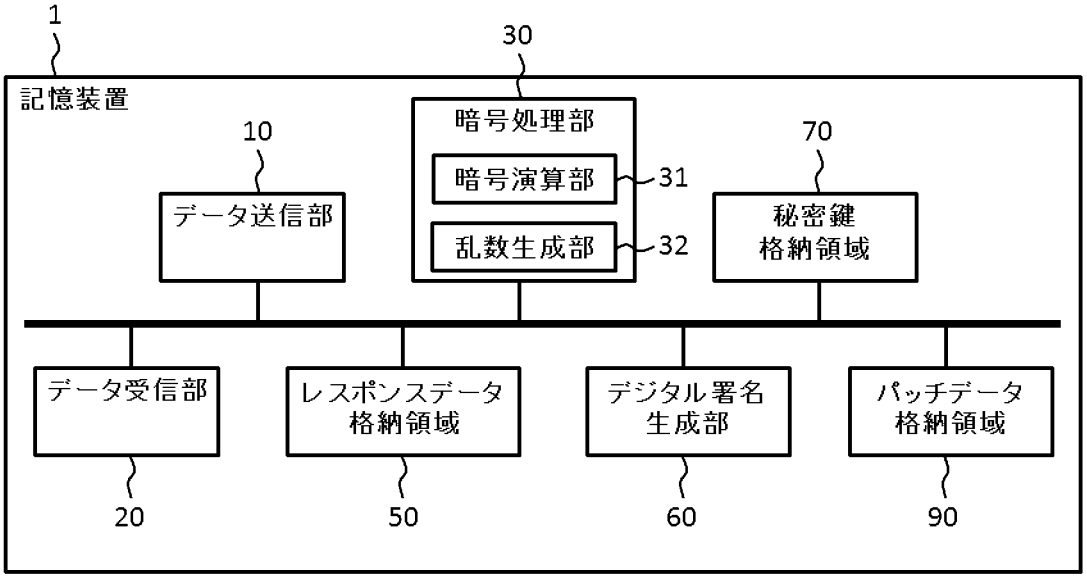
【図８】

図8


配信サーバ
200
端末装置
100
記憶装置
1
S3.1
ファームウェアアップデート要求
新ファームウェアのプログラムデータ
第一チャレンジデータ
S3.2
ファームウェアアップデート要求
新ファームウェアのプログラムデータ
第一チャレンジデータ
S3.3
ファームウェアを格納
S3.4
第一チャレンジデータの第一デジタル署名を生成
S3.6
第一レスポンスデータを保持
S3.5
コマンド
S3.8
第一レスポンスデータ要求
S3.7
第一レスポンスデータを取得
S3.10
第二チャレンジデータを生成
S3.9
S3.11
コマンド
第一デジタル署名
第二チャレンジデータ
第二レスポンスデータ要求
第一デジタル署名
第二チャレンジデータ
S3.12
第二チャレンジデータの第二デジタル署名を生成
S3.13
S3.14
コマンド
第二デジタル署名
コマンド
第二デジタル署名

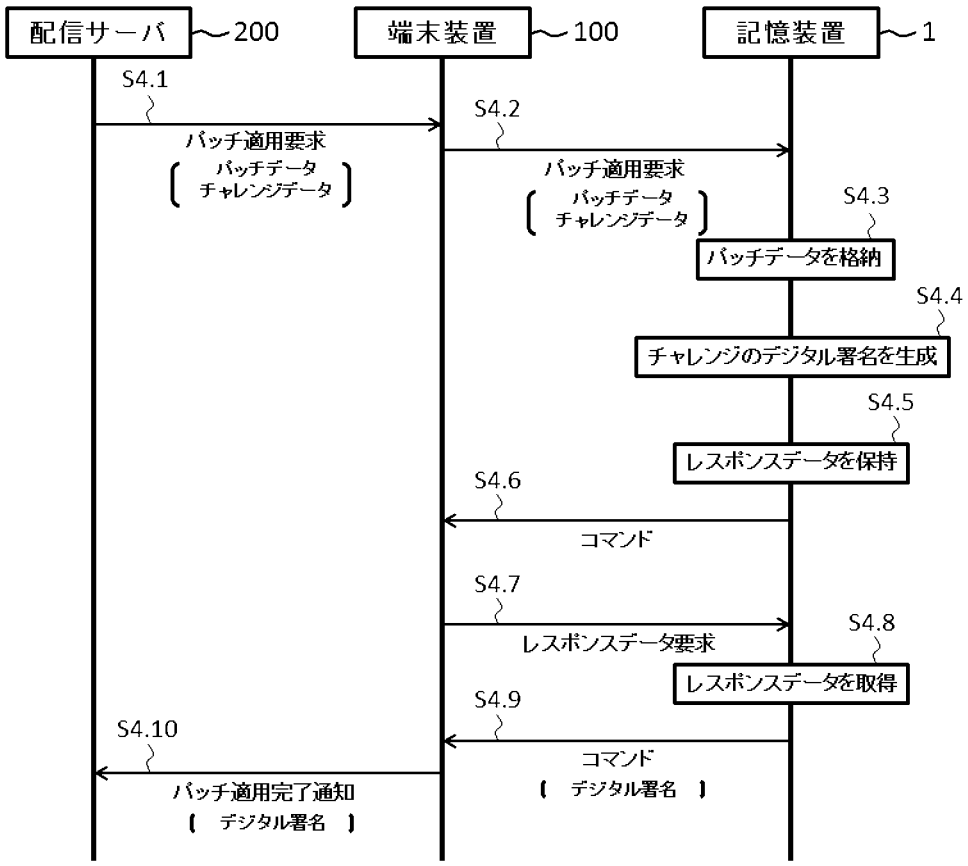
【図９】

図9


1
記憶装置
30
暗号処理部
暗号演算部
31
乱数生成部
32
10
データ送信部
70
秘密鍵
格納領域
データ受信部
20
レスポンスデータ
格納領域
50
デジタル署名
生成部
60
パッチデータ
格納領域
90

【図１０】

図10


配信サーバ
200
端末装置
100
記憶装置
1
S4.1
バッチ適用要求
（バッチデータ
チャレンジデータ）
S4.2
バッチ適用要求
（バッチデータ
チャレンジデータ）
S4.3
バッチデータを格納
S4.4
チャレンジのデジタル署名を生成
S4.5
レスポンスデータを保持
S4.6
コマンド
S4.7
レスポンスデータ要求
S4.8
レスポンスデータを取得
S4.9
コマンド
（デジタル署名）
S4.10
バッチ適用完了通知
（デジタル署名）