(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6888122号
(P6888122)
(45)発行日　令和3年6月16日(2021.6.16)　(24)登録日　令和3年5月21日(2021.5.21)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640D
G06F	21/57	(2013.01)	G06F	21/57	320

請求項の数 20　(全 35 頁)

(21)出願番号　特願2019-565643(P2019-565643)
(86)(22)出願日　平成30年1月19日(2018.1.19)
(86)国際出願番号　PCT/JP2018/001521
(87)国際公開番号　WO2019/142307
(87)国際公開日　令和1年7月25日(2019.7.25)
審査請求日　令和2年4月30日(2020.4.30)

(73)特許権者　302062931
ルネサスエレクトロニクス株式会社
東京都江東区豊洲三丁目２番２４号
(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100103894
弁理士　家入　健
(72)発明者　森山　大輔
東京都江東区豊洲三丁目２番２４号　ルネサスエレクトロニクス株式会社内
(72)発明者　鈴木　大輔
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】半導体装置、更新データ提供方法、更新データ受取方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
メモリと、乱数生成回路と、制御回路と、を有し、外部端末装置に更新データを提供する半導体装置であって、
前記メモリは、鍵情報を記憶し、
前記乱数生成回路は、第１乱数信号および第２乱数信号を生成し、
前記制御回路は、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、半導体装置。
【請求項２】
前記制御回路は、
前記第６乱数信号、前記第７乱数信号、および前記第８乱数信号を、

予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算する、
請求項１に記載の半導体装置。
【請求項３】
前記制御回路は、前記第２応答信号と前記第８乱数信号とが一致していない場合に、前記暗号化更新データに代えて、前記暗号化更新データと同じ桁数の乱数信号を前記外部端末装置に提供する、
請求項１に記載の半導体装置。
【請求項４】
前記制御回路は、前記外部端末装置から、提供した前記暗号化更新データに対する応答信号である第３応答信号を受け取った場合に、前記第３応答信号が、前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として生成された第１０乱数信号と一致するか否かを判定し、一致する場合にデータが更新されたことを登録し、一致しない場合には、データが更新されなかったことを登録する、
請求項１に記載の半導体装置。
【請求項５】
メモリと、制御回路と、を有し、外部サーバ装置から暗号化更新データを受け取る半導体装置であって、
前記メモリは、更新前データと、鍵情報を記憶し、
前記制御回路は、
前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、
半導体装置。
【請求項６】
前記制御回路は、
前記第６乱数信号、前記第７乱数信号、前記第９乱数信号、および前記第１０乱数信号を、
予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算する、
請求項５に記載の半導体装置。
【請求項７】
前記制御回路は、受け取った前記認証信号と、前記第１０乱数信号とが一致していない場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行わない、
請求項５に記載の半導体装置。
【請求項８】
前記制御回路は、予め設定された桁数の数値を順次インクリメントすることにより前記チャレンジコードを生成する、
請求項５に記載の半導体装置。
【請求項９】
前記制御回路は、前記第２乱数信号と前記第６乱数信号とを入力信号として、第１２乱数信号を生成することにより前記チャレンジコードを生成する、
請求項５に記載の半導体装置。

【請求項１０】
第３乱数信号を生成する乱数生成回路をさらに備え、
前記制御回路は、前記第９乱数信号および前記第１０乱数信号を生成する際に、前記第２乱数信号と前記第６乱数信号に加えて前記第３乱数信号も入力信号として入力し、
前記チャレンジコードとして第３乱数信号を前記外部サーバ装置へ出力する、
請求項５に記載の半導体装置。
【請求項１１】
前記制御回路は、少なくとも前記第２乱数信号と前記第６乱数信号とを入力信号として含む擬似ランダム関数の出力として第１３乱数信号を生成し、
前記暗号化更新データの復号処理が成功した場合に、前記第１３乱数信号を前記外部サーバ装置へ出力する、
請求項５に記載の半導体装置。
【請求項１２】
前記制御回路は、前記暗号化更新データの復号処理が成功しなかった場合に、前記第１３乱数信号に代えて、乱数信号を前記外部サーバ装置へ出力する、
請求項１１に記載の半導体装置。
【請求項１３】
真性乱数生成回路をさらに備え、
前記乱数信号は、真性乱数信号である、
請求項１２に記載の半導体装置。
【請求項１４】
外部端末装置に更新データを提供する方法であって、
鍵情報を記憶し、
第１乱数信号および第２乱数信号を生成し、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、
更新データ提供方法。
【請求項１５】
外部サーバ装置から暗号化更新データである暗号化更新データを受け取る方法であって、
更新前データと、鍵情報を記憶し、
前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、

更新データ受取方法。
【請求項１６】
コンピュータに以下の方法を実行させるプログラムであって、前記方法は、
外部端末装置に更新データを提供する方法であって、
鍵情報を記憶し、
第１乱数信号および第２乱数信号を生成し、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、
プログラム。
【請求項１７】
コンピュータに以下の方法を実行させるためのプログラムであって、前記方法は、
外部サーバ装置から暗号化更新データである暗号化更新データを受け取る方法であって、
更新前データと、鍵情報を記憶し、
前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、
プログラム。
【請求項１８】
メモリと、乱数生成回路と、制御回路と、を有し、外部サーバ装置から暗号化更新データを受け取り、受け取った暗号化更新データを外部端末装置に提供する半導体装置であって、
前記メモリは、前記外部サーバ装置との間で使用可能な共通鍵を記憶し、
前記制御回路は、
前記外部サーバ装置から、第１乱数信号、第２乱数信号、前記共通鍵により暗号化された第６乱数信号を含む暗号化鍵データ、および暗号化更新データを受け取り、
前記暗号化鍵データを前記共通鍵により復号して第６乱数信号を生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を出力し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データ

を前記外部端末装置に提供する、半導体装置。
【請求項１９】
前記第６乱数信号および前記第８乱数信号は、
予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算される、
請求項１８に記載の半導体装置。
【請求項２０】
前記制御回路は、
前記第２応答信号と前記第８乱数信号とが一致していない場合に、前記暗号化更新データに代えて、前記暗号化更新データと同じ桁数の乱数信号を前記外部端末装置に提供する、
請求項１８に記載の半導体装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、半導体装置、更新データ提供方法、更新データ受取方法およびプログラムに関する。
【背景技術】
【０００２】
ＩｏＴ（Internet of Things）機器が広く普及している。これらの機器に含まれるマイコン等の半導体装置に対して高いセキュリティを確保した状態でファームウェアアップデート等を行うことが期待されている。
【０００３】
特許文献１に記載の車外装置は、更新制御プログラム、当該プログラムに係るダイジェスト値の算出手段、更新後の動作が正常であるか否かを判定する手段、および判定結果を返答する手段を実現するプログラムを含む更新データを記憶している。そして、制御装置は、車外装置から送信される更新データを中継装置を介して受信する。さらに、制御装置は、受信した更新データに含まれる更新制御プログラムにより制御プログラムを更新すると共に、前記プログラムを実行して更新後の動作が正常であるか否かを判定して、その判定結果を中継装置に返答する。
【０００４】
特許文献２に記載の電子機器は、アプリケーションソフトウェアの動作に係るアプリケーションファイルを有し、ネットワークを介して前記アプリケーションファイルを更新する。かかる電子機器は、１つ以上のデータからなるアプリケーションファイルを記憶し、更新データと、前記アプリケーションファイルにおいて前記更新データによって更新する位置を示す位置情報とを、前記ネットワークを介して外部装置から受け取る。さらに、電子機器は、前記位置情報が示す位置に存在するデータを前記更新データに書き換えて、前記アプリケーションファイルの一部のみを更新し、更新された前記アプリケーションファイルが改竄されているか否かの確認を行う。
【０００５】
特許文献３に記載のプログラム書換えシステムは、マルチプロトコルに対応した車載中継装置において新プログラムと旧プログラムとの差分データを検索し、新プログラムにおける差分データをＥＣＵに送信して記憶する。
【０００６】
特許文献４に記載の組込機器は、ソフトウェアを更新する更新データが複数に分割された各セクションについて順に検証処理を行う。組込機器は、検証処理の途中で得られる中間値を記憶しておく。組込機器は、全てのセクションに対して検証処理が完了すると、検証処理で得られた値と、検証データとを比較して、改ざんがないことを確認する。改ざんがないことが確認できると、組込機器は、再び各セクションについて順に検証処理を行う。組込機器は、検証処理で得られた中間値と記憶しておいた中間値とを比較して、一致すると、そのセクションによってソフトウェアを更新する。

【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２０１５－１０３１６３号公報
【特許文献２】国際公開第２００６／１２９６５４号
【特許文献３】特開２０１４－１８２５７１号公報
【特許文献４】国際公開第２００６／１２９６５４号
【発明の概要】
【発明が解決しようとする課題】
【０００８】
特許文献１に記載の技術は、中継機が更新データに対して電子署名演算を行うことが可能でなければならない。また、特許文献１は、更新データの暗号化が行われないため、更新データの秘匿性を担保できていない。また、特許文献２に記載の技術は、部分的な検証を行う一方で、全体としての検証を行わない。そのため、ブロックごとに改ざん検出の管理を行うこととなり、保存データ量が多くなるおそれがある。また、特許文献３に記載の技術は、中継装置が更新データの電子署名や復号演算を行わなければならないため、中継装置に更新データの中身を開示する必要がある一方、中継装置とＥＣＵとの通信においてのセキュリティが担保されていない。また、特許文献４に記載の技術は、各セクションにかかる中間値を記憶しておく必要があり保存データ量が多くなるおそれがある。また、各セクションに対して各２回の検証処理が必要であるために計算に時間がかかるおそれがある。さらに、上記特許文献のいずれにおいても、正当な更新対象機器との通信が行われていることを確認する手段についての提案はなされていない。
【０００９】
その他の課題と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。
【課題を解決するための手段】
【００１０】
一実施の形態によれば、半導体装置は、メモリと、乱数生成回路と、制御回路と、を有し、外部端末装置に更新データを提供する。前記メモリは、鍵情報を記憶し、前記乱数生成回路は、第１乱数信号および第２乱数信号を生成する。前記制御回路は、前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、前記更新データに対して第７乱数信号を用いて暗号化更新データを生成する。前記制御回路は、前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取る。前記制御回路は、前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する。
【００１１】
一実施の形態によれば、半導体装置は、メモリと、制御回路と、を有し、外部サーバ装置から暗号化更新データを受け取る。前記メモリは、更新前データと、鍵情報を記憶している。前記制御回路は、前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成する。前記制御回路は、前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成する。また、前記制御回路は、予め設定された信号を含むチャレンジコードを生成し、前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力する。前記制御回路は、出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記暗号化更新データの復号処理を行う。
【発明の効果】

【００１２】
前記一実施の形態によれば、半導体装置は、効率的かつ安全に更新プログラムの授受を行い、プログラムの更新を実現することができる。
【図面の簡単な説明】
【００１３】
【図１】実施の形態１にかかる送受信システムの概略図である。
【図２】実施の形態１にかかる第１半導体装置のハードウェア構成図である。
【図３】実施の形態１にかかる第２半導体装置のハードウェア構成図である。
【図４】実施の形態１にかかる第３半導体装置のハードウェア構成図である。
【図５】実施の形態１にかかる送受信システムの送受信信号を示した図である。
【図６】実施の形態１にかかる第１半導体装置１１０の機能ブロック図である。
【図７】実施の形態１にかかる第３半導体装置の機能ブロック図である。
【図８】実施の形態１にかかる第１半導体装置の機能ブロック図である。
【図９】実施の形態１にかかる第３半導体装置の機能ブロック図である。
【図１０】実施の形態１の変形例にかかる第３半導体装置の機能ブロック図である。
【図１１】実施の形態２にかかる送受信システムのハードウェア構成図である。
【図１２】実施の形態２にかかる送受信システムの送受信信号を示した図である。
【図１３】実施の形態２にかかる第３半導体装置の機能ブロック図である。
【図１４】実施の形態２にかかる第１半導体装置の機能ブロック図である。
【図１５】実施の形態２にかかる第３半導体装置の機能ブロック図である。
【図１６】実施の形態２にかかる第１半導体装置の機能ブロック図である。
【図１７】実施の形態３にかかる第２半導体装置のハードウェア構成図である。
【図１８】実施の形態３にかかる送受信システムの送受信信号を示した図である。
【図１９】実施の形態３にかかる第１半導体装置の機能ブロック図である。
【図２０】実施の形態３にかかる第２半導体装置の機能ブロック図である。
【図２１】実施の形態３にかかる第２半導体装置の機能ブロック図である。
【発明を実施するための形態】
【００１４】
説明の明確化のため、以下の記載および図面は、適宜、省略、および簡略化がなされている。また、様々な処理を行う機能ブロックとして図面に記載される各要素は、ハードウェア的には、ＣＰＵ（Central Processing Unit）、メモリ、その他の回路で構成することができ、ソフトウェア的には、メモリにロードされたプログラムなどによって実現される。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは当業者には理解されるところであり、いずれかに限定されるものではない。よって、以下の説明に回路として例示した構成は、ハードウェアまたはソフトウェアのいずれかまたはその両方によって実現することが可能であり、ある機能を実現する回路として示された構成は、同様の機能を実現するソフトウェアの一部としても示され得る。例えば、制御回路と記載された構成は、制御部として記載され得る。なお、各図面において、同一の要素には同一の符号が付されており、必要に応じて重複説明は省略されている。
【００１５】
また、上述したプログラムは、様々なタイプの非一時的なコンピュータ可読媒体を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、ＣＤ－ＲＯＭ（Read Only Memory）ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリ（例えば、マスクＲＯＭ、ＰＲＯＭ（Programmable ROM）、ＥＰＲＯＭ（Erasable PROM）、フラッシュＲＯＭ、ＲＡＭ（Random Access Memory））を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光

信号、および電磁波を含む。一時的なコンピュータ可読媒体は、電線および光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

【００１６】

＜実施の形態１＞

まず、図１を参照しながら、実施の形態１について概略を説明する。図１は、実施の形態１にかかる送受信システムの概略図である。送受信システム１は、端末装置１３が有する更新前データを、サーバ装置１１が有している更新データに更新するためのシステムである。送受信システム１は、サーバ装置１１において更新データを暗号化し、暗号化した更新データである暗号化更新データを端末装置１３に送信する。端末装置１３は、暗号化更新データを復号してデータを更新する。送受信システム１は、サーバ装置１１、中継装置１２、および端末装置１３を構成とする。サーバ装置１１と中継装置１２とは、通信可能に接続している。また、中継装置１２と端末装置１３とは、通信可能に接続している。図１の例示は、サーバ装置１１と中継装置１２とはネットワーク９００を介して通信可能に接続されている。なお、各構成を通信可能にする接続手段は有線、無線を問わず、インターネットを介しているか否かを問わない。

【００１７】

サーバ装置１１は、例えばパーソナルコンピュータやブレードサーバであって、情報処理を司る第１半導体装置１１０を有している。中継装置１２は、例えばスマートフォンやタブレット端末等であって、情報処理を司る第２半導体装置１２０を有している。また、端末装置１３は、ＩｏＴ機器と呼ばれるインターネット接続可能な機器や、その他通信機能を有する機器である。端末装置１３は、情報処理を司る第３半導体装置１３０を有している。

【００１８】

図２は、実施の形態１にかかる第１半導体装置１１０のハードウェア構成図である。情報処理を司る第１半導体装置１１０は、主な構成として、ＣＰＵ１１１、ＮＶＲＡＭ１１２（Non-Volatile Random Access Memory）、ＤＲＡＭ１１３（Dynamic Random Access Memory）、ＩＦ１１４（Interface）、およびＴＲＮＧ１１５（True Random Number Generator：真性乱数生成回路）を有しており、これらの構成は通信バスにより接続されている。

【００１９】

なお、以降の説明において、特別に説明を加えた場合を除き、名称が同一で符号が異なる構成は同様の機能を有するものとする。そのため、このような構成についての説明は省略する。

【００２０】

ＣＰＵ１１１は、第１半導体装置１１０において後述する演算処理等を行うための演算装置である。ＣＰＵ１１１は、ＰＲＦ演算回路１１１ａ、比較回路１１１ｂ、ＡＥ暗号化回路１１１ｃ、選択回路１１１ｄを主な構成として有している。なお、ＣＰＵ１１１は、ハードウェアとしてのこれらの構成を複数有していてもよいし、ソフトウェアとして並列処理可能に構成されていてもよい。また、本実施の形態において説明するＣＰＵは、ＣＰＵコア以外の周辺回路を含んでもよい。

【００２１】

ＰＲＦ演算回路１１１ａは、任意の入力信号を予め設定された擬似ランダム関数（ＰＲＦ=Pseudorandom function）により演算し、演算結果を出力する。擬似ランダム関数は、暗号学的には乱数として識別できない値であって、直感的には十分ランダムに見える出力を返す関数であり、真のランダム関数との間で両者を識別するような多項式時間のアルゴリズムが存在しないものを指す。また、ＰＲＦ演算回路１１１ａは、同じ入力に対しては同じ結果を出力する。ＰＲＦ演算回路１１１ａは、入力として出力変数の数を指定してもよい。なお、ＰＲＦ演算回路１１１ａは、上述のような出力がなされ、且つ安全性が担保できるのであれば、共通鍵暗号やハッシュ関数に基づいた関数など他の関数を用いたものであってもよい。

【００２２】
比較回路１１１ｂは、入力として２つの信号を受け取り、受け取った２つの信号を比較し、比較結果としてこれらの信号が一致するか否かを出力する。比較結果の出力信号の例としては、２つの信号が一致しない場合の出力信号は「０」であり、２つの信号が一致する場合の出力信号は「１」である。ただし、比較結果の出力信号はこれに限られない。
【００２３】
ＡＥ暗号化回路１１１ｃ（AE=Authenticated Encryption）は、任意の平文と鍵情報とを入力信号として、入力信号に対して認証付き暗号化処理を行う。鍵情報は、復号処理をする際にも使用される。認証付き暗号化処理を行うことにより、ＡＥ暗号化回路１１１ｃは、暗号文、認証タグ、およびヘッダ信号を出力する。
【００２４】
選択回路１１１ｄは、複数の入力信号の内いずれか選択した信号を出力する機能を有している。選択回路１１１ｄは、比較回路１１１ｂから供給される比較結果信号ＳＧ２０の値によって、複数の入力信号の内からどの信号を出力するかを選択する。つまり、比較結果信号ＳＧ２０は、選択回路１１１ｄの選択制御信号である。選択回路１１１ｄは、ハードウェア構成の例としてはマルチプレクサである。
【００２５】
ＮＶＲＡＭ１１２は、例えばフラッシュメモリのような読み書き可能な不揮発性の記憶装置である。ＮＶＲＡＭ１１２は、更新データや通信セキュリティを担保するための鍵情報等を記憶している。
【００２６】
ＤＲＡＭ１１３は、揮発性の記憶装置であって、種々のデータを一時的に記憶する。なお、本実施の形態におけるＤＲＡＭ１１３のハードウェア構成は一例であって、ＤＲＡＭ１１３は、ＳＲＡＭ(Static Random Access Memory)によって構成されてもよく、揮発性メモリに代えて、ＭＲＡＭ（Magnetoresistive Random Access Memory）、またはフラッシュメモリ等の不揮発性メモリによって構成されてもよい。
【００２７】
ＴＲＮＧ１１５は、真性乱数生成回路である。ＴＲＮＧ１１５は、例えば、ダイオードの生成するノイズや熱雑音、放射性物質の崩壊による放射線をセンサで検出する等、ランダムな物理現象を用い、その信号を元に乱数を生成する。ＣＰＵ１１１は、各構成の信号を処理し、処理に応じた信号を、ＩＦ１１４を介して中継装置１２に送信し、または、中継装置１２から受信した信号を、ＩＦ１１４を介して受け取り、受け取った信号を処理する。
【００２８】
図３は、実施の形態１にかかる第２半導体装置１２０のハードウェア構成図である。情報処理を司る第２半導体装置１２０は、主な構成として、ＣＰＵ１２１、ＮＶＲＡＭ１２２、ＤＲＡＭ１２３、およびＩＦ１２４を有しており、これらの構成は通信バスにより接続されている。第２半導体装置１２０は、これらの構成により、サーバ装置１１と通信し、サーバ装置１１から信号を受け取り、受け取った信号を必要に応じて処理し、端末装置１３に送信する。また、中継装置１２は、端末装置１３から信号を受け取り、受け取った信号を必要に応じて処理し、サーバ装置１１に送信する。
【００２９】
図４は、実施の形態１にかかる第３半導体装置１３０のハードウェア構成図である。情報処理を司る第３半導体装置１３０は、主な構成として、ＣＰＵ１３１、ＮＶＲＡＭ１３２、ＤＲＡＭ１３３、ＩＦ１３４、およびＴＲＮＧ１３５を有しており、これらの構成は通信バスにより接続されている。端末装置１３は、中継装置１２から信号を受け取り、受け取った信号を処理する。また、端末装置１３は、処理した信号を中継装置１２に送信する。
【００３０】
ＣＰＵ１３１は、第３半導体装置１３０において演算処理等を行うための演算装置であ

る。ＣＰＵ１３１は、ＰＲＦ演算回路１３１ａ、比較回路１３１ｂ、ＡＥ復号回路１３１ｃを主な構成として有している。

【００３１】

ＡＥ復号回路１３１ｃは、認証付き暗号化された信号に対して、復号処理および認証タグの検証を行う。すなわち、ＡＥ復号回路１３１ｃは、ＡＥ暗号化回路１１１ｃが出力した暗号文、認証タグ、およびヘッダ信号、ならびにＡＥ暗号化回路１１１ｃが使用した鍵情報を入力信号とする。ＡＥ復号回路１３１ｃは、暗号文を復号し、復号した結果生成された認証タグと、入力信号として受け取った認証タグが一致するか検証を行う。検証の結果、これらの認証タグが一致すると、ＡＥ復号回路１３１ｃは、復号した平文を出力する。一方、これらの認証タグが一致しないと、ＡＥ復号回路１３１ｃは、認証結果不一致を示す信号を出力する。

【００３２】

更新制御回路１３１ｄは、ファームウェアの更新を行うための信号制御を行う。更新制御回路１３１ｄは、入力信号として、フラグ信号と更新データ信号を受け取る。更新制御回路１３１ｄは、受け取ったフラグ信号がファームウェアの更新を実行するための値であれば、入力信号として受け取った更新データを更新前データと置き換える処理を実行する。また、更新制御回路１３１ｄは、ファームウェアの更新処理が成功したか否かを出力する機能を有していてもよい。

【００３３】

なお、実施の形態１の変形例として後述するように、端末装置１３は、ＴＲＮＧ１３５を有していない構成としてもよい。

【００３４】

次に、図５～図１０を参照しながら、送受信システム１の動作について詳細を説明する。まず、図５を参照しながら、送受信システム１にかかるそれぞれの装置が有する信号と、それぞれの装置が送受信する信号について説明する。図５は、実施の形態１にかかる送受信システム１の送受信信号を示した図である。

【００３５】

サーバ装置１１は、ＮＶＲＡＭ１１２に、更新データＳＧ０２、更新バージョンデータＳＧ０４、識別子ＳＧ０５、およびマスタ鍵ＳＧ０６を記憶している。更新データＳＧ０２は、例えば、端末装置１３のための新しいバージョンのファームウェアである。更新バージョンデータＳＧ０４は、更新データＳＧ０２のバージョン情報を含むデータである。識別子ＳＧ０５は、端末装置１３に固有に付与されている識別情報であって、例えば端末装置１３のＭａｃアドレス（Media Access Control address）や製品固有の識別番号等である。

【００３６】

端末装置１３は、ＮＶＲＡＭ１３２に、更新前データＳＧ０１、更新前バージョンデータＳＧ０３、識別子ＳＧ０５、およびマスタ鍵ＳＧ０６を記憶している。更新前データＳＧ０１は、例えば、端末装置１３が現在利用しているファームウェアである。更新前バージョンデータＳＧ０３は、更新前データＳＧ０１のバージョン情報を含むデータである。

【００３７】

以降は、送受信システム１にかかるそれぞれの装置が送受信する信号と、それぞれの装置が行う処理について信号の処理の流れに沿って説明する。ここに示す例では、送受信システム１は、端末装置１３のファームウェアのバージョンアップデート処理を行う。

【００３８】

まず、中継装置１２は、バージョンチェック要求信号ＳＧ０８を端末装置１３に送信する（ステップＳ１１）。バージョンチェック要求信号ＳＧ０８は、端末装置１３に対してファームウェアのバージョンを応答するように要求する信号である。

【００３９】

端末装置１３は、中継装置１２からバージョンチェック要求信号ＳＧ０８を受け取ると、受け取った要求信号に応じて、端末装置１３の現在のファームウェアのバージョンであ

る更新前バージョンデータＳＧ０３と、識別子ＳＧ０５とを中継装置１２に送信する（ステップＳ１２）。

【００４０】

中継装置１２は、端末装置１３から更新前バージョンデータＳＧ０３と、識別子ＳＧ０５とを受け取ると、これらのデータにバージョンアップ要求信号ＳＧ０９を加えて、サーバ装置１１に送信する（ステップＳ１３）。

【００４１】

図６を参照しながら、サーバ装置１１が中継装置１２から受け取った信号を処理して、要求信号を出力するまでの処理について説明する。図６において、サーバ装置１１が有する第１半導体装置１１０は、ファームウェアのバージョンアップデート処理を行うために、端末装置１３に対してかかる処理を行うか否かを判定する。かかる処理を行う場合、第１半導体装置１１０は、暗号化された更新データを復号する際に使用する鍵を生成するための信号と、端末装置１３を認証するためのチャレンジコードとを出力する。

【００４２】

図６は、実施の形態１にかかるサーバ装置１１における第１半導体装置１１０の機能ブロック図である。図６において、第１半導体装置１１０は中継装置１２からのバージョンアップ要求信号ＳＧ０９を受け付ける。次に、第１半導体装置１１０は、ＮＶＲＡＭ１１２のデータベース領域にアクセスして、ＮＶＲＡＭ１１２が記憶している識別子ＳＧ０５と、中継装置１２から受け取った識別子ＳＧ０５とが一致するか否かを照合する。

【００４３】

サーバ装置１１は、識別子に関するこれらの信号が一致した場合、中継装置１２から受け取った端末装置１３のファームウェアバージョンである更新前バージョンデータＳＧ０３と、ＮＶＲＡＭ１１２に記憶している更新バージョンデータＳＧ０４とを照合する。すなわち、第１半導体装置１１０は、ＮＶＲＡＭ１１２の更新データ領域にアクセスし、更新バージョンデータＳＧ０４をＣＰＵ１１１の比較回路１１１ｂに送信する。また、第１半導体装置１１０は、中継装置１２から受け取った更新前バージョンデータＳＧ０３を比較回路１１１ｂに供給する。そして、比較回路１１１ｂは、これらのデータを比較し、比較結果信号ＳＧ１０をＰＲＦ演算回路１１１ａに出力する。

【００４４】

ここでは、比較回路１１１ｂがデータを比較した結果、バージョンデータが一致した場合、比較回路１１１ｂは、比較結果信号ＳＧ１０として「０」を出力する。この場合、端末装置１３のファームウェアは最新であり更新の必要はない。そのため、ＰＲＦ演算回路１１１ａは、ファームウェア更新のための処理を実行しない。一方、比較した結果、バージョンデータが一致しない場合、比較回路１１１ｂは、比較結果信号ＳＧ１０として「１」を出力する。この場合、サーバ装置１１は、後述する端末装置１３のファームウェアを更新するための処理を実行する。

【００４５】

比較回路１１１ｂから比較結果信号ＳＧ１０として「１」を受け取った場合、ＰＲＦ演算回路１１１ａは、ＮＶＲＡＭ１１２のデータベース領域にアクセスし、マスタ鍵ＳＧ０６を受け取る。また、ＰＲＦ演算回路１１１ａは、ＴＲＮＧ１１５から、第１乱数信号ＳＧ１１を受け取る。ＰＲＦ演算回路１１１ａは、マスタ鍵ＳＧ０６と、第１乱数信号ＳＧ１１とを入力として、第６乱数信号ＳＧ１３および第７乱数信号ＳＧ１４を生成し、生成したこれらの信号を、ＤＲＡＭ１１３に記憶させる。

【００４６】

ＴＲＮＧ１１５は、ＰＲＦ演算回路１１１ａに対して第１乱数信号ＳＧ１１を供給すると共に、第２乱数信号ＳＧ１２を生成し、生成した第２乱数信号ＳＧ１２をＤＲＡＭ１１３に記憶させる。ＴＲＮＧ１１５は、生成した第１乱数信号ＳＧ１１を、端末装置１３が更新データを復号するための鍵を生成するための情報として出力する。また、ＴＲＮＧ１１５は、生成した第２乱数信号ＳＧ１２を、端末装置１３に対する要求信号であるチャレンジコードとして出力する。

【００４７】
図５に戻る。サーバ装置１１は、ＴＲＮＧ１１５が出力した第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を、中継装置１２に送信する（ステップＳ１４）。
【００４８】
中継装置１２は、サーバ装置１１から受け取った第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を、端末装置１３に送信する（ステップＳ１５）。
【００４９】
図７を参照しながら、第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を受け取った端末装置１３が行う処理の概要について説明する。図７において、端末装置１３が有する第３半導体装置１３０は、サーバ装置１１から受け取った、鍵を生成するための信号（第１乱数信号ＳＧ１１）を使用して、暗号化された更新データを復号する際に使用する鍵（第７乱数信号ＳＧ１４）を生成する。また、第３半導体装置１３０は、サーバ装置１１から受け取った、チャレンジコード（第２乱数信号ＳＧ１２）に対する応答信号としてレスポンスコード（第９乱数信号ＳＧ１６）を出力する。さらに、第３半導体装置１３０は、応答する際にサーバ装置１１を認証するためのチャレンジコード（第３乱数信号ＳＧ１５）を出力する。
【００５０】
図７は、実施の形態１にかかる端末装置の機能ブロック図である。図７において、ＰＲＦ演算回路が２つ存在するため、ここでは説明の便宜上一方をＰＲＦ演算回路１３１ａ＿１、もう一方をＰＲＦ演算回路１３１ａ＿２と称する。当然ながら、ＰＲＦ演算回路１３１ａ＿１とＰＲＦ演算回路１３１ａ＿２とは、別の構成であっても構わないし、一個の構成であって、異なる演算を行うものであってよい。また、以降の説明においても１つのブロック図において同じ種類の構成が複数存在する場合には、同様の符号をつけることがある。
【００５１】
端末装置１３が有する第３半導体装置１３０は、受け取った第１乱数信号ＳＧ１１をＣＰＵ１３１が有するＰＲＦ演算回路１３１ａに入力する。また、ＰＲＦ演算回路１３１ａは、ＮＶＲＡＭ１３２が記憶しているマスタ鍵ＳＧ０６を入力信号として読み出す。
【００５２】
ＰＲＦ演算回路１３１ａ＿１は、マスタ鍵ＳＧ０６と、第１乱数信号ＳＧ１１とを入力として、第６乱数信号ＳＧ１３および第７乱数信号ＳＧ１４を生成する。ＰＲＦ演算回路１３１ａ＿１は、生成した信号のうち、第６乱数信号ＳＧ１３をＰＲＦ演算回路１３１ａ＿２に入力する。また、ＰＲＦ演算回路１３１ａ＿１は、生成した信号のうち、第７乱数信号ＳＧ１４をＤＲＡＭ１３３に記憶させる。
【００５３】
第６乱数信号ＳＧ１３が入力されたＰＲＦ演算回路１３１ａ＿２は、さらに中継装置１２から受け取った第２乱数信号ＳＧ１２を、入力信号として受け取る。また、ＰＲＦ演算回路１３１ａ＿２は、もう一つの入力信号として、ＴＲＮＧ１３５から第３乱数信号ＳＧ１５を受け取る。
【００５４】
ＰＲＦ演算回路１３１ａ＿２は、第６乱数信号ＳＧ１３、第２乱数信号ＳＧ１２、および第３乱数信号ＳＧ１５を入力信号として、第９乱数信号ＳＧ１６および第１０乱数信号ＳＧ１７を生成する。ＰＲＦ演算回路１３１ａ＿２は、生成したこれらの信号のうち、第９乱数信号ＳＧ１６を、サーバ装置１１から受け取った要求信号に対する応答信号として出力する。また、ＰＲＦ演算回路１３１ａ＿２は、生成したこれらの信号のうち、第１０乱数信号ＳＧ１７を、ＤＲＡＭ１３３に記憶させる。
【００５５】
ＴＲＮＧ１３５は、ＰＲＦ演算回路１３１ａ＿２の入力信号として生成した第３乱数信号ＳＧ１５を、サーバ装置１１から受け取った要求信号に対する応答信号として出力する。すなわち、第３半導体装置１３０は、第９乱数信号ＳＧ１６と、第３乱数信号ＳＧ１５

とを、サーバ装置１１から受け取った要求信号に対する応答信号として出力する。

【００５６】

図５に戻る。端末装置１３は、第３半導体装置１３０が出力した第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を、中継装置１２に送信する（ステップＳ１６）。

【００５７】

中継装置１２は、サーバ装置１１から受け取った第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を、サーバ装置１１に送信する（ステップＳ１７）。

【００５８】

図８を参照しながら、第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を受け取ったサーバ装置１１が行う処理について説明する。図８において、サーバ装置１１が有する第１半導体装置１１０は、端末装置１３から受け取った、チャレンジコード（第３乱数信号ＳＧ１５）に対する応答信号としてレスポンスコード（第１１乱数信号ＳＧ１９）を出力する。また、第１半導体装置１１０は、端末装置１３から受け取った、レスポンスコード（第９乱数信号ＳＧ１６）が期待値と一致するか否かを比較し、比較結果に応じた暗号文ＳＧ２３を出力する。

【００５９】

図８は、実施の形態１にかかる第１半導体装置の機能ブロック図である。第１半導体装置１１０は、受け取った第３乱数信号ＳＧ１５をＰＲＦ演算回路１１１ａに入力する。ＰＲＦ演算回路１１１ａは、さらに入力信号として、ＤＲＡＭ１１３から第６乱数信号ＳＧ１３および第２乱数信号ＳＧ１２を受け取る。

【００６０】

ＰＲＦ演算回路１１１ａは、第６乱数信号ＳＧ１３、第２乱数信号ＳＧ１２、および第３乱数信号ＳＧ１５を入力信号として、第８乱数信号ＳＧ１８と、第１１乱数信号ＳＧ１９とを生成する。ＰＲＦ演算回路１１１ａは、生成した第８乱数信号ＳＧ１８を比較回路１１１ｂに送信する。また、ＰＲＦ演算回路１１１ａは、生成した第１１乱数信号ＳＧ１９を端末装置１３から受け取ったチャレンジコードに応答するレスポンスコードとして出力する。

【００６１】

第１半導体装置１１０は、受け取った第９乱数信号ＳＧ１６を、比較回路１１１ｂに入力する。比較回路１１１ｂは、入力信号として、ＰＲＦ演算回路１１１ａが出力した第８乱数信号ＳＧ１８と、端末装置１３が出力した第９乱数信号ＳＧ１６とをそれぞれ受け取り、受け取ったこれらの信号を比較する。すなわち、サーバ装置１１は、サーバ装置１１が送信したチャレンジコードに対して端末装置１３が応答したレスポンスコードが期待値と一致するか否かを比較する。比較回路１１１ｂがデータを比較した結果、これらの信号が一致しない場合、比較回路１１１ｂは、比較結果信号ＳＧ２０として「０」を出力する。一方、比較した結果、これらの信号が一致する場合、比較回路１１１ｂは、比較結果信号ＳＧ２０として「１」を出力する。比較回路１１１ｂは出力した比較結果信号ＳＧ２０を、選択回路１１１ｄに供給する。

【００６２】

ＡＥ暗号化回路１１１ｃは、ＮＶＲＡＭ１１２から入力信号として更新データＳＧ０２と、更新バージョンデータＳＧ０４を受け取る。また、ＡＥ暗号化回路１１１ｃは、更新データＳＧ０２および更新バージョンデータＳＧ０４を暗号化するための鍵情報である第７乱数信号ＳＧ１４をＤＲＡＭ１１３から受け取る。ＡＥ暗号化回路１１１ｃは、これらの入力信号に基づいて、暗号化更新データＳＧ２１を出力し、出力した暗号化更新データＳＧ２１を選択回路１１１ｄに入力する。

【００６３】

ＴＲＮＧ１１５は、第４乱数信号ＳＧ２２を生成し、生成した信号を、選択回路１１１ｄに入力する。ＴＲＮＧ１１５が出力する第４乱数信号ＳＧ２２は、真性乱数であって、信号の桁数が暗号化更新データＳＧ２１と同じになるように設定されている。すなわち、復号できない場合、暗号化更新データＳＧ２１と第４乱数信号ＳＧ２２との区別は容易で

はない。

【００６４】

選択回路１１１ｄは、入力信号として、上述した暗号化更新データＳＧ２１と第４乱数信号ＳＧ２２とを受け取るとともに、選択制御信号として、比較結果信号ＳＧ２０を受け取る。選択回路１１１ｄは、比較結果信号ＳＧ２０の値が「１」の場合、出力信号である暗号文ＳＧ２３として暗号化更新データＳＧ２１を選択する。一方、選択回路１１１ｄは、比較結果信号ＳＧ２０の値が「０」の場合、出力信号である暗号文ＳＧ２３として暗号化更新データＳＧ２１に代えて第４乱数信号ＳＧ２２を選択する。選択回路１１１ｄは、このようにして信号を選択し、選択した信号を暗号文ＳＧ２３として出力する。

【００６５】

このように、第１半導体装置１１０は、端末装置１３の認証が正しく行われた場合には更新データを含む暗号化信号を出力し、端末装置１３の認証が正しく行われなかった場合には、正しく認証されない送信先にとって暗号化更新データＳＧ２１との区別が容易ではない乱数信号を送信する。このように、正しく認証されない相手に対して形式的に正しい信号と区別が容易ではない信号を送信することにより、第三者からの不要な攻撃を抑制することができる。

【００６６】

図８の構成により、第１半導体装置１１０は、チャレンジコードである第３乱数信号ＳＧ１５に対するレスポンスコードとして第１１乱数信号ＳＧ１９を出力し、端末装置１３から受け取ったレスポンスコードである第９乱数信号ＳＧ１６に応じて暗号文ＳＧ２３を出力する。

【００６７】

図５に戻る。サーバ装置１１は、第１半導体装置１１０が出力した第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を、中継装置１２に送信する（ステップＳ１８）。

【００６８】

中継装置１２は、サーバ装置１１から受け取った第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を、端末装置１３に送信する（ステップＳ１９）。

【００６９】

図９を参照しながら、第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を受け取った端末装置１３が行う処理について説明する。図９において、端末装置１３が有する第３半導体装置１３０は、サーバ装置１１から受け取った、レスポンスコード（第１１乱数信号ＳＧ１９）を使用して、サーバ装置１１に対する認証を行う。また、第３半導体装置１３０は、サーバ装置１１に対する認証結果に応じて、サーバ装置１１から受け取った暗号文ＳＧ２３を復号するか否かを判定し、判定結果に応じた処理を行う。

【００７０】

図９は、実施の形態１にかかる第３半導体装置の機能ブロック図である。図９において、端末装置１３の第３半導体装置１３０は、サーバ装置１１から受け取った第１１乱数信号ＳＧ１９と、ＤＲＡＭ１３３が記憶している第１０乱数信号ＳＧ１７とを比較回路１３１ｂ＿１に入力し、これらの信号を比較する。比較回路１３１ｂ＿１は、これらの信号が一致していない場合には比較結果信号ＳＧ２４として「０」を出力し、これらの信号が一致している場合には比較結果信号ＳＧ２４として「１」を出力し、出力した信号を、ＡＥ復号回路１３１ｃに供給する。

【００７１】

また、第３半導体装置１３０は、サーバ装置１１から受け取った、暗号文ＳＧ２３を、ＡＥ暗号化回路１１１ｃに入力する。ＡＥ暗号化回路１１１ｃは、さらに入力信号として、ＤＲＡＭ１３３が記憶している第７乱数信号ＳＧ１４を受け取る。

【００７２】

ここで、比較結果信号ＳＧ２４の値が「０」の場合は、サーバ装置１１の認証が正しく行われなかったことを意味している。この場合、ＡＥ復号回路１３１ｃは、暗号文ＳＧ２３を復号する処理を実行しない。一方、比較結果信号ＳＧ２４の値が「１」の場合は、サ

ーバ装置１１の認証が正しく行われたことを意味している。この場合、ＡＥ復号回路１３１ｃは、暗号文ＳＧ２３を復号する以下の処理を実行する。

【００７３】

このように、認証が正しく行われなかった場合に受け取った暗号文の復号処理を実行しないことにより、悪意ある第三者等からのアップデート要求を防止することが出来る。

【００７４】

ＡＥ復号回路１３１ｃは、暗号文ＳＧ２３と、暗号文ＳＧ２３を復号するための鍵情報である第７乱数信号ＳＧ１４とを入力信号として、暗号文ＳＧ２３を復号する。暗号文ＳＧ２３が復号されると、ＡＥ復号回路１３１ｃは、出力信号に含まれている更新バージョンデータＳＧ０４を比較回路１３１ｂ＿２に供給する。比較回路１３１ｂ＿２は、ＮＶＲＡＭ１３２から第３半導体装置１３０が記憶する現在のファームウェアのバージョン情報である更新前バージョンデータＳＧ０３を受け取る。比較回路１３１ｂ＿２は、更新バージョンデータＳＧ０４が更新前バージョンデータＳＧ０３より大きいか否かを比較し、比較結果信号ＳＧ２５を更新制御回路１３１ｄに供給する。

【００７５】

更新制御回路１３１ｄは、比較回路１３１ｂ＿２から比較結果信号ＳＧ２５を受け取ると共に、ＡＥ復号回路１３１ｃから復号された更新データＳＧ０２を受け取る。更新制御回路１３１ｄは、ＮＶＲＡＭ１３２が記憶するファームウェアのバージョンよりも、復号されたファームウェアのバージョンが大きい場合には、ＮＶＲＡＭ１３２が記憶するファームウェアを更新する処理を行う。ファームウェアを更新する処理として、更新制御回路１３１ｄは、更新前データＳＧ０１に代えて、更新データＳＧ０２をＮＶＲＡＭ１３２に記憶させ、更新前バージョンデータＳＧ０３に代えて更新バージョンデータＳＧ０４をＮＶＲＡＭ１３２に記憶させる。

【００７６】

実施の形態１にかかる送受信システムは、以上のような構成となっている。上述した説明から、送受信システム１の処理をまとめると、以下のように説明することが出来る。すなわち、サーバ装置と、前記サーバ装置から更新データを受け取る端末装置とを含む送受信システム１は、以下のように処理を実行する。

【００７７】

まず、サーバ装置１１は、認証付き暗号を復号するための鍵を生成するための信号（１１１）および端末装置１３を認証するためのチャレンジコード（１１２）を端末装置１３へ送信する。

【００７８】

端末装置１３は、チャレンジコード（１１２）に対するレスポンスコードと、サーバ装置１１を認証するためのチャレンジコードをサーバ装置１１へ送信する。

【００７９】

サーバ装置は、レスポンスコードの検証を行い、検証結果に応じて、予め設定された暗号を送信するとともに、端末装置１３から受け取ったチャレンジコードに対するレスポンスコードを端末装置１３へ送信する。

【００８０】

端末装置１３は、サーバ装置１１から受け取ったレスポンスコードの検証を行い、検証結果に応じて、レスポンスコードと共に受け取った暗号に対する処理を決定する。

【００８１】

また、送受信システム１は、サーバ装置１１と端末装置１３との間に中継装置１２が介在し、サーバ装置１１と中継装置１２とが通信し、中継装置１２と端末装置１３とが通信する。

【００８２】

送受信システム１は、サーバ装置１１と端末装置１３とが有する共通鍵を用いて更新データを送受信する。また、送受信システム１は、サーバ装置１１と端末装置１３とが有する共通の擬似ランダム関数を用いて信号をそれぞれ演算する。そのため、送受信システム

１は、更新データの秘匿性を維持し、第三者への情報漏えいを防ぐことが出来る。
【００８３】
送受信システム１は、認証付き暗号化技術を利用して更新データの送受信をおこなう。そのため、仮に、端末装置１３に改ざんされた更新データが供給された場合、送受信システム１は、認証タグを検証することにより、正しくないデータによる更新を防止できる。
【００８４】
また、送受信システム１は、サーバ装置１１と端末装置１３との間に中継装置１２が介在する。これにより、送受信システム１は、サーバ装置１１の通信方式と、端末装置１３の通信方式が異なる場合にも、サーバ装置１１と端末装置１３との信号の送受信が可能となる。したがって、送受信システム１は、例えば、端末装置１３が直接インターネットに接続していない場合においても、ファームウェアの更新を行うことが出来、運用コストを低減することができる。
【００８５】
また、送受信システム１は、サーバ装置１１と端末装置１３とがそれぞれ共通の鍵を有している。このような構成により、送受信システム１は、高速に処理をおこなうことができる。例えば、一般的な公開鍵を利用したシステムと比較すると、本実施の形態にかかるシステムの処理速度は１００倍程度速い。
【００８６】
＜実施の形態１の変形例＞
以下に、図１０を参照しながら、実施の形態１の変形例について説明する。実施の形態１の変形例に係る送受信システム１は、端末装置１３がＴＲＮＧ１３５を有していない点において、上述した端末装置１３の構成と異なる。
【００８７】
図１０は、実施の形態１の変形例にかかる第３半導体装置の機能ブロック図である。図１０の機能ブロック図は、図５におけるステップＳ１５において第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を受け取った端末装置１３が行う処理について説明するものであって、実施の形態１の図７に対応する。
【００８８】
図１０は、実施の形態１にかかる端末装置の機能ブロック図である。図１０を参照しながら、第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を受け取った端末装置１３が行う処理について上述した実施の形態１と異なる点について概要を説明する。図１０において、端末装置１３が有する第３半導体装置１３０は、サーバ装置１１を認証するためのチャレンジコードとして、第３乱数信号ＳＧ１５に代えてＰＲＦ演算回路１３１ａ＿２が第１２乱数信号ＳＧ０７＿ｎを生成する。第３半導体装置１３０は、ＰＲＦ演算回路１３１ａ＿２が生成した第１２乱数信号ＳＧ０７＿ｎを、ＮＶＲＡＭ１３２に記憶させる。また、第３半導体装置１３０は、第９乱数信号ＳＧ１６をレスポンスコードとして出力すると共に、第１２乱数信号ＳＧ０７＿ｎをチャレンジコードとして出力する。
【００８９】
以下に、第１２乱数信号ＳＧ０７＿ｎについて詳細を説明する。図１０において、第３半導体装置１３０は、ＮＶＲＡＭ１３２に予め第１２乱数信号ＳＧ０７＿ｎの初期値として、乱数である第１２乱数信号ＳＧ０７＿０を記憶している。第３半導体装置１３０が最初に処理を行う場合、ＰＲＦ演算回路１３１ａは、ＮＶＲＡＭ１３２にアクセスし、第１２乱数信号ＳＧ０７＿０を受け取る。また、ＰＲＦ演算回路１３１ａ＿２は、第２乱数信号ＳＧ１２と、ＰＲＦ演算回路１３１ａ＿１が出力した第６乱数信号ＳＧ１３を同じく入力信号として受け取る。ＰＲＦ演算回路１３１ａ＿２は、これらを入力信号として演算を行い、出力信号として、第９乱数信号ＳＧ１６、第１０乱数信号ＳＧ１７、および第１２乱数信号ＳＧ０７＿１を生成する。ＰＲＦ演算回路１３１ａ＿２は、これらの出力信号のうち、第１２乱数信号ＳＧ０７＿１を、サーバ装置１１を認証するためのチャレンジコードとして外部に出力するとともに、第１２乱数信号ＳＧ０７＿１を、ＮＶＲＡＭ１３２に記憶させる。ＰＲＦ演算回路１３１ａ＿２は、演算の度に第１２乱数信号ＳＧ０７＿ｎを

新しい値に順次更新し、更新した信号をＮＶＲＡＭ１３２に記憶する。

【００９０】

これにより、端末装置１３は、ＴＲＮＧ１３５を有さず、サーバ装置１１の認証を行うことが出来る。したがって、送受信システム１は、端末装置１３を簡便な構成とすることができる。したがって、実施の形態１変形例において、送受信システム１は、簡便な構成により、効率的かつ安全に更新プログラムの授受を行い、プログラムの更新を実現することができる。

【００９１】

なお、実施の形態１の変形例としては、これに限らず、例えば、チャレンジコードとして、上述した第３乱数信号ＳＧ１５や第１２乱数信号ＳＧ０７＿ｎに代えて、外部に出力する度にインクリメントする数値を用いてもよい。このような構成にすることにより、実施の形態１変形例において、送受信システム１は、簡便な構成により、効率的かつ安全に更新プログラムの授受を行い、プログラムの更新を実現することができる。

【００９２】

＜実施の形態２＞

次に、図１１～図１６を参照して本発明の実施の形態について説明する。実施の形態２にかかる送受信システム２は、サーバ装置のＣＰＵの構成、および、端末装置のＣＰＵの構成が実施の形態１と異なる。また、実施の形態２にかかる送受信システム２は、サーバ装置において端末装置が有するファームウェアのバージョンを管理する点において、実施の形態１にかかる送受信システム１と異なる。

【００９３】

図１１は、実施の形態２にかかる送受信システムのハードウェア構成図である。送受信システム２は、サーバ装置２１、中継装置２２、および端末装置２３を有している。サーバ装置２１は、第１半導体装置２１０を有しており、第１半導体装置２１０は、ＣＰＵ２１１を含んでいる。ＣＰＵ２１１は、更新制御回路２１１ｅを含む点において、実施の形態１にかかるＣＰＵ１１１と異なる。端末装置２３は、第３半導体装置２３０を有しており、第３半導体装置２３０は、ＣＰＵ２３１を含んでいる。ＣＰＵ２３１は、選択回路２３１ｅを含む点において、実施の形態１にかかるＣＰＵ２３１と異なる。

【００９４】

次に、図１２を参照しながら、送受信システム２にかかるそれぞれの装置が有する信号と、それぞれの装置が送受信する信号について説明する。図１２は、実施の形態２にかかる送受信システムの送受信信号を示した図である。

【００９５】

サーバ装置２１は、ＮＶＲＡＭ１１２に、更新前バージョンデータＳＧ０３を記憶している点において、実施の形態１にかかるサーバ装置１１と異なる。すなわち、サーバ装置２１は、端末装置２３の現在のファームウェアのバージョンが何であるかを管理している。なお、端末装置２３は、実施の形態１にかかる端末装置１３と同様の信号を記憶している。

【００９６】

以降は、送受信システム２にかかるそれぞれの装置が送受信する信号と、それぞれの装置が行う処理について、実施の形態１と異なる点について説明する。図１２に示すように、送受信システム２は、ステップＳ１１からステップＳ１５までの処理は、実施の形態１と同様である。

【００９７】

次に、図１３を参照しながら、第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を受け取った端末装置２３が行う処理について、図７に示した実施の形態１と異なる点について説明する。図１３において、端末装置２３が有する第３半導体装置２３０は、ＰＲＦ演算回路２３１ａ＿２が出力する信号が、実施の形態１と異なる。すなわち、ＰＲＦ演算回路２３１ａ＿２は、第６乱数信号ＳＧ１３、第２乱数信号ＳＧ１２、および第３乱数信号ＳＧ１５を入力信号とした演算において、第９乱数信号ＳＧ１６と第１０乱数信号ＳＧ１

７に加え、第１３乱数信号ＳＧ２６も出力する。第１３乱数信号ＳＧ２６は、ファームウェアの更新が正しく行われたことを示すための信号として用いられる。ＰＲＦ演算回路２３１ａ＿２は、出力した第１３乱数信号ＳＧ２６をＤＲＡＭ１３３に記憶させる。図１３において、上述の処理を実行した第３半導体装置２３０は、実施の形態１と同様に、第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を出力する。

【００９８】

図１２に戻る。端末装置２３は、第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を中継装置２２に送信し（ステップＳ２６）、中継装置２２はこれらの信号をサーバ装置２１に送信する（ステップＳ２７）。

【００９９】

次に、図１４を参照しながら、第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を受け取ったサーバ装置２１が行う処理について、図８に示した実施の形態１と異なる点について説明する。図１４は、実施の形態２にかかるサーバ装置の機能ブロック図である。

【０１００】

図１４において、サーバ装置２１が有する第１半導体装置２１０は、ＰＲＦ演算回路２１１ａ出力する信号が、実施の形態１と異なる。すなわち、ＰＲＦ演算回路２１１ａは、第２乱数信号ＳＧ１２、第６乱数信号ＳＧ１３、および第３乱数信号ＳＧ１５を入力信号とした演算において、第８乱数信号ＳＧ１８と第１１乱数信号ＳＧ１９に加え、第１４乱数信号ＳＧ２７も出力する。第１４乱数信号ＳＧ２７は、端末装置２３から受け取るファームウェア更新結果信号を検証するための信号として用いられる。ＰＲＦ演算回路２１１ａは、出力した第１４乱数信号ＳＧ２７をＤＲＡＭ１１３に記憶させる。図１４において、上述の処理を実行した第１半導体装置２１０は、実施の形態１と同様に、第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を出力する。

【０１０１】

図１２に戻る。サーバ装置２１は、第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を中継装置２２に送信し（ステップＳ２８）、中継装置２２はこれらの信号を端末装置２３に送信する（ステップＳ２９）。

【０１０２】

次に、図１５を参照しながら、第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を受け取った端末装置２３が行う処理について、図９に示した実施の形態１と異なる点について説明する。図１５において、端末装置２３が有する第３半導体装置２３０は、更新制御回路２３１ｄが更新結果を出力し、更新制御回路２３１ｄが出力した更新結果に基づいて、第３半導体装置２３０が更新結果信号をサーバ装置２１に送信する点が、実施の形態１と異なる。

【０１０３】

図１５は、実施の形態２にかかる端末装置の機能ブロック図である。図１５において、更新制御回路２３１ｄは、比較回路２３１ｂから比較結果信号ＳＧ２５を受け取ると共に、ＡＥ復号回路２３１ｃから復号された更新データＳＧ０２を受け取る。更新制御回路２３１ｄは、ＮＶＲＡＭ１３２が記憶するファームウェアのバージョンよりも、復号されたファームウェアのバージョンが大きい場合には、ＮＶＲＡＭ１３２が記憶するファームウェアを更新する処理を行う。

【０１０４】

更新制御回路２３１ｄは、ファームウェアを更新する処理が完了すると、かかる処理が成功したか否かを示す第１更新結果信号ＳＧ２８を生成し、生成した第１更新結果信号ＳＧ２８を、選択回路２３１ｅに選択制御信号として供給する。ファームウェアを更新する処理が成功した場合、更新制御回路２３１ｄは、第１更新結果信号ＳＧ２８として「１」を出力する。一方、ファームウェアを更新する処理が成功しなかった場合、更新制御回路２３１ｄは、第１更新結果信号ＳＧ２８として「０」を出力する。

【０１０５】

選択回路２３１ｅは、入力信号として、ＤＲＡＭ１３３から第１３乱数信号ＳＧ２６を

受け取り、さらに、ＴＲＮＧ１３５から第５乱数信号ＳＧ２９を受け取る。第５乱数信号ＳＧ２９は、第１３乱数信号ＳＧ２６と同じ桁数の真性乱数である。選択回路２３１ｅは、更新制御回路２３１ｄから第１更新結果信号ＳＧ２８として「１」を受け取った場合、出力する信号として第１３乱数信号ＳＧ２６を選択する。一方、選択回路２３１ｅは、更新制御回路２３１ｄから第１更新結果信号ＳＧ２８として「０」を受け取った場合、出力する信号として第５乱数信号ＳＧ２９を選択する。選択回路２３１ｅは、選択した信号を、第２更新結果信号ＳＧ３０として出力する。第３半導体装置２３０は、選択回路２３１ｅが出力した第２更新結果信号ＳＧ３０を出力する。

【０１０６】

ファームウェアを更新する処理が成功したか否かを示すための信号をこのように出力することにより、かかる信号は秘匿性を維持し、第三者への情報漏えいを防ぐことが出来る。

【０１０７】

図１２に戻る。端末装置２３は、第２更新結果信号ＳＧ３０を中継装置２２に送信し（ステップＳ３０）、中継装置２２はこれをサーバ装置２１に送信する（ステップＳ３１）。

【０１０８】

次に、図１６を参照しながら、サーバ装置２１が行う処理について説明する。図１６は、実施の形態２にかかるサーバ装置の機能ブロック図である。図１６において、サーバ装置２１が有する第１半導体装置２１０は、第２更新結果信号ＳＧ３０を受け取ると、受け取った第２更新結果信号ＳＧ３０を比較回路２１１ｂに供給する。また、比較回路２１１ｂは、ＤＲＡＭ１１３から第１４乱数信号ＳＧ２７を受け取る。すなわち、比較回路２１１ｂは、第２更新結果信号ＳＧ３０と第１４乱数信号ＳＧ２７とを比較し、比較結果信号ＳＧ３１を更新制御回路２１１ｅに出力する。

【０１０９】

比較回路２１１ｂは、第２更新結果信号ＳＧ３０と第１４乱数信号ＳＧ２７とが一致していた場合は、比較結果信号ＳＧ３１として「１」を出力する。一方、比較回路２１１ｂは、第２更新結果信号ＳＧ３０と第１４乱数信号ＳＧ２７とが一致していない場合は、比較結果信号ＳＧ３１として「０」を出力する。

【０１１０】

更新制御回路２１１ｅは、比較結果信号ＳＧ３１として「０」を受け取った場合、ＮＶＲＡＭ１１２のデータを更新する処理を実行しない。この場合、端末装置２３が更新処理に失敗したと判断し比較結果信号ＳＧ３１をＮＶＲＡＭ１１２に保存してもよい。一方、更新制御回路２１１ｅは、比較結果信号ＳＧ３１として「１」を受け取った場合、ＮＶＲＡＭ１１２のデータを更新する処理を実行する。すなわち、更新制御回路２１１ｅは、ＮＶＲＡＭ１１２の更新データ領域にアクセスし、端末装置２３に送信した更新データにかかる更新バージョンデータＳＧ０４を受け取る。そして、更新制御回路２１１ｅは、ＮＶＲＡＭ１１２のデータベース領域に記憶されている更新前バージョンデータＳＧ０３に代えて、更新バージョンデータＳＧ０４を記憶させる処理を行う。

【０１１１】

以上に説明した構成を有することにより、実施の形態２にかかる送受信システムは、端末装置の更新データを容易に管理できる。したがって、例えばサーバ装置が複数の端末装置を管理する場合に、それぞれの有するデータの更新状況を管理することができ、ネットワーク脆弱性等を把握することが可能となる。

【０１１２】

＜実施の形態３＞

次に、図１７から図２１を参照して、実施の形態３について説明する。実施の形態３にかかる送受信システム３は、端末装置間の通信処理が実施の形態１と異なる。すなわち、実施の形態３にかかる送受信システム３は、まず、サーバ装置３１と中継装置３２との通信を行い、次に、サーバ装置３１と中継装置３２との通信を行うことがない状況において

、中継装置３２と端末装置３３との間の通信を行う。また、実施の形態３にかかる送受信システム３は、中継装置３２の構成が実施の形態１と異なる。

【０１１３】

図１７は、実施の形態３にかかる第２半導体装置のハードウェア構成図である。送受信システム３において、中継装置３２と端末装置が有する第２半導体装置３２０は、および、ＣＰＵ３２１の構成が、実施の形態１にかかるＣＰＵ１２１と異なる。ＣＰＵ３２１は、ＰＲＦ演算回路３２１ａ、比較回路３２１ｂ、ＡＥ復号回路３２１ｃ、および選択回路３２１ｄを主な構成として有している。また、第２半導体装置３２０は、ＴＲＮＧ３２５を有している点が実施の形態１と異なる。

【０１１４】

次に、図１８を参照しながら、送受信システム３にかかるそれぞれの装置が有する信号と、それぞれの装置が送受信する信号について説明する。図１８は、実施の形態３にかかる送受信システムの送受信信号を示した図である。

【０１１５】

図１８に示す送受信システム３は、サーバ装置３１のＮＶＲＡＭ１１２が共通鍵ＳＧ３２を記憶している点、および中継装置３２のＮＶＲＡＭ１２２が共通鍵ＳＧ３２を記憶している点において、実施の形態１と異なる。なお、端末装置３３のＮＶＲＡＭ１３２が記憶するデータは、実施の形態１と同様である。

【０１１６】

以降は、送受信システム３にかかるそれぞれの装置が送受信する信号と、それぞれの装置が行う処理について、実施の形態１と異なる点について説明する。図１８に示すように、送受信システム３は、ステップＳ１１からステップＳ１３までの処理は、実施の形態１と同様である。

【０１１７】

次に、図１９を参照しながら、サーバ装置１１が行う処理について実施の形態１と異なる点について説明する。図１９は、実施の形態３にかかるサーバ装置の機能ブロック図である。図１９において、サーバ装置１１の第１半導体装置１１０は、暗号化された更新データを復号する際に使用する鍵を生成するための信号（第１乱数信号ＳＧ１１）と、端末装置１３を認証するためのチャレンジコード（第２乱数信号ＳＧ１２）とを出力する。第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を出力するまでの処理については実施の形態１と同様であるため説明を省略する。

【０１１８】

第１半導体装置１１０は、共通鍵ＳＧ３２と、第６乱数信号ＳＧ１３とをＡＥ暗号化回路１１１ｃ＿１に入力する。ＡＥ暗号化回路１１１ｃ＿１は、これらの信号を受け取り、受け取った信号に対して認証付き暗号化処理を行い、暗号文ＳＧ３３を生成する。

【０１１９】

また、第１半導体装置１１０は、更新データＳＧ０２、更新バージョンデータＳＧ０４、および第７乱数信号ＳＧ１４をＡＥ暗号化回路１１１ｃ＿２に入力する。ＡＥ暗号化回路１１１ｃ＿２は、これらの信号を受け取り、受け取った信号に対して認証付き暗号化処理を行い、暗号化更新データＳＧ２１を生成する。

【０１２０】

以上の処理により、第１半導体装置１１０は、第１乱数信号ＳＧ１１、第２乱数信号ＳＧ１２、暗号文ＳＧ３３、および暗号化更新データＳＧ２１を外部へ出力する。そして、サーバ装置１１は、これらの信号を中継装置３２に送信する（図１８のステップＳ３１）。

【０１２１】

次に、図２０を参照しながら、上述の信号を受け取った中継装置が行う処理について説明する。図２０は、実施の形態３にかかる中継装置の機能ブロック図である。図２０において、中継装置３２の第２半導体装置３２０は、以下の処理を行う。

【０１２２】

まず、ＡＥ復号回路３２１ｃは、暗号文ＳＧ３３を入力信号として受け取り、さらにＮＶＲＡＭ１２２に記憶されている共通鍵ＳＧ３２を入力信号として受け取る。そして、ＡＥ復号回路３２１ｃは、これらを入力信号として、暗号文ＳＧ３３に含まれていた第６乱数信号ＳＧ１３を復号により生成する。ＡＥ復号回路３２１ｃは、生成した第６乱数信号ＳＧ１３をＮＶＲＡＭ１２２に記憶させる。

【０１２３】

次に、第２半導体装置３２０は、第１乱数信号ＳＧ１１、第２乱数信号ＳＧ１２、および暗号化更新データＳＧ２１をＮＶＲＡＭ１２２に記憶させるとともに、第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を端末装置３３へ出力する処理を行う。中継装置３２は、これらの信号を端末装置３３に送信する（図１８のステップＳ３２）。

【０１２４】

次に、端末装置３３は、中継装置３２から受け取った第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を処理し、中継装置３２に対して第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を送信する（図１８のステップＳ３３）。端末装置３３が第１乱数信号ＳＧ１１および第２乱数信号ＳＧ１２を処理し、中継装置３２に対して第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を送信する処理は、実施の形態１において図７を参照しながら説明したものと同様である。

【０１２５】

次に、図２１を参照しながら、第３乱数信号ＳＧ１５および第９乱数信号ＳＧ１６を受け取った中継装置３２が行う処理について説明する。図２１は、図１９は、実施の形態３にかかる中継装置の機能ブロック図である。

【０１２６】

第２半導体装置３２０において、ＰＲＦ演算回路３２１ａは、入力信号として、端末装置３３が送信した第３乱数信号ＳＧ１５を受け取る。また、ＰＲＦ演算回路３２１ａは、入力信号として、ＮＶＲＡＭ１２２に記憶している第６乱数信号ＳＧ１３、および第２乱数信号ＳＧ１２を受け取る。ＰＲＦ演算回路３２１ａは、これらの信号を入力信号として演算処理を行い、第８乱数信号ＳＧ１８、および第１１乱数信号ＳＧ１９を生成する。

【０１２７】

第２半導体装置３２０は、ＰＲＦ演算回路３２１ａが生成した第１１乱数信号ＳＧ１９を、端末装置３３のチャレンジコード（第３乱数信号ＳＧ１５）に対するレスポンスコードとして出力する。

【０１２８】

比較回路３２１ｂは、ＰＲＦ演算回路３２１ａが生成した第８乱数信号ＳＧ１８と、中継装置３２からレスポンスコードとして受け取った第９乱数信号ＳＧ１６とをそれぞれ受け取り、受け取ったこれらの信号を比較する。

【０１２９】

比較回路３２１ｂがデータを比較した結果、これらの信号が一致しない場合、比較回路３２１ｂは、比較結果信号ＳＧ２０として「０」を出力する。一方、比較した結果、これらの信号が一致する場合、比較回路３２１ｂは、比較結果信号ＳＧ２０として「１」を出力する。比較回路３２１ｂは出力した比較結果信号ＳＧ２０を、選択回路３２１ｄに供給する。

【０１３０】

ＴＲＮＧ１２５は、第４乱数信号ＳＧ２２を生成し、生成した信号を、選択回路３２１ｄに入力する。ＴＲＮＧ１２５が出力する第４乱数信号ＳＧ２２は、信号の桁数が暗号化更新データＳＧ２１と同じである真性乱数である。

【０１３１】

選択回路３２１ｄは、入力信号として、ＮＶＲＡＭ１２２に記憶されている暗号化更新データＳＧ２１と第４乱数信号ＳＧ２２とを受け取るとともに、選択制御信号として、比較結果信号ＳＧ２０を受け取る。選択回路３２１ｄは、比較結果信号ＳＧ２０の値が「１」の場合、出力信号である暗号文ＳＧ２３として暗号化更新データＳＧ２１を選択する。

一方、選択回路３２１ｄは、比較結果信号ＳＧ２０の値が「０」の場合、出力信号である暗号文ＳＧ２３として暗号化更新データＳＧ２１に代えて第４乱数信号ＳＧ２２を選択する。選択回路３２１ｄは、このようにして信号を選択し、選択した信号を暗号文ＳＧ２３として出力する。

【０１３２】

中継装置３２は、第２半導体装置３２０が出力した第１１乱数信号ＳＧ１９および暗号文ＳＧ２３を、端末装置３３に送信する（図１８のステップＳ３４）。以降の端末装置３３における処理は、実施の形態１において図９を参照しながら説明したものと同様である。

【０１３３】

なお、図１８のステップＳ１１およびステップＳ１２において中継装置３２と端末装置３３とが送受信するデータは、秘匿性があるものではない。そのため、端末装置３３にかかる更新前バージョンデータＳＧ０３および識別子ＳＧ０５を、中継装置３２が予め記憶しておいてもよい。

【０１３４】

このような構成により、実施の形態３にかかる送受信システム３は、サーバ装置３１と中継装置３２との通信と、中継装置３２と端末装置３３との通信と、を分離してデータの更新処理を行うことが出来る。例えば、送受信システム３は、端末装置３３が遠隔の地にある場合や、近距離通信のみを備えている場合であって、サーバ装置３１と中継装置３２との通信を行うことが出来ない環境であっても、端末装置３３に対して更新データを提供することができる。

【０１３５】

なお、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。

【０１３６】

例えば、上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

【０１３７】

（付記１）

メモリと、乱数生成回路と、制御回路と、を有し、外部端末装置に更新データを提供する半導体装置であって、

前記メモリは、鍵情報を記憶し、

前記乱数生成回路は、第１乱数信号および第２乱数信号を生成し、

前記制御回路は、

前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、

前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、

前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、

前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、

前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、

前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、半導体装置。

【０１３８】

（付記２）

前記制御回路は、

前記第６乱数信号、前記第７乱数信号、および前記第８乱数信号を、

予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算する、

付記１に記載の半導体装置。

【０１３９】
（付記３）
前記制御回路は、前記第２応答信号と前記第８乱数信号とが一致していない場合に、前記暗号化更新データに代えて、前記暗号化更新データと同じ桁数の乱数信号を前記外部端末装置に提供する、
付記１に記載の半導体装置。
【０１４０】
（付記４）
前記制御回路は、前記外部端末装置から、提供した前記暗号化更新データに対する応答信号である第３応答信号を受け取った場合に、前記第３応答信号が、前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として生成された第１０乱数信号と一致するか否かを判定し、一致する場合には、データが更新されたことを登録し、一致しない場合には、データが更新されなかったことを登録する、
付記１に記載の半導体装置。
【０１４１】
（付記５）
メモリと、制御回路と、を有し、外部サーバ装置から暗号化更新データを受け取る半導体装置であって、
前記メモリは、更新前データと、鍵情報を記憶し、
前記制御回路は、
前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、
半導体装置。
【０１４２】
（付記６）
前記制御回路は、
前記第６乱数信号、前記第７乱数信号、前記第９乱数信号、および前記第１０乱数信号を、
予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算する、
付記５に記載の半導体装置。
【０１４３】
（付記７）
前記制御回路は、受け取った前記認証信号と、前記第１０乱数信号とが一致していない場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行わない、
付記５に記載の半導体装置。
【０１４４】
（付記８）
前記制御回路は、予め設定された桁数の数値を順次インクリメントすることにより前記チャレンジコードを生成する、
付記５に記載の半導体装置。

【０１４５】
（付記９）
前記制御回路は、前記第２乱数信号と前記第６乱数信号とを入力信号として、第１２乱数信号を生成することにより前記チャレンジコードを生成する、
付記５に記載の半導体装置。
【０１４６】
（付記１０）
第３乱数信号を生成する乱数生成回路をさらに備え、
前記制御回路は、前記第９乱数信号および前記第１０乱数信号を生成する際に、前記第２乱数信号と前記第６乱数信号に加えて前記第３乱数信号も入力信号として入力し、
前記チャレンジコードとして第３乱数信号を前記外部サーバ装置へ出力する、
付記５に記載の半導体装置。
【０１４７】
（付記１１）
前記制御回路は、少なくとも前記第２乱数信号と前記第６乱数信号とを入力信号として含む擬似ランダム関数の出力として第１３乱数信号を生成し、
前記暗号化更新データの復号処理が成功した場合に、前記第１３乱数信号を前記外部サーバ装置へ出力する、
付記５に記載の半導体装置。
【０１４８】
（付記１２）
前記制御回路は、前記暗号化更新データの復号処理が成功しなかった場合に、前記第１３乱数信号に代えて、乱数信号を前記外部サーバ装置へ出力する、
付記１１に記載の半導体装置。
【０１４９】
（付記１３）
真性乱数生成回路をさらに備え、
前記乱数信号は、真性乱数信号である、
付記１２に記載の半導体装置。
【０１５０】
（付記１４）
外部端末装置に更新データを提供する方法であって、
鍵情報を記憶し、
第１乱数信号および第２乱数信号を生成し、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、
更新データ提供方法。
【０１５１】
（付記１５）
外部サーバ装置から暗号化更新データである暗号化更新データを受け取る方法であって、
更新前データと、鍵情報を記憶し、

前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、
更新データ受取方法。
【０１５２】
（付記１６）
コンピュータに以下の方法を実行させるプログラムであって、前記方法は、
外部端末装置に更新データを提供する方法であって、
鍵情報を記憶し、
第１乱数信号および第２乱数信号を生成し、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記更新データに対して第７乱数信号を用いて暗号化更新データを生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を生成し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、
プログラム。
【０１５３】
（付記１７）
コンピュータに以下の方法を実行させるためのプログラムであって、前記方法は、
外部サーバ装置から暗号化更新データである暗号化更新データを受け取る方法であって、
更新前データと、鍵情報を記憶し、
前記外部サーバ装置から第１乱数信号および第２乱数信号を要求信号として受け取り、
前記第１乱数信号および前記鍵情報から第６乱数信号および第７乱数信号を生成し、
前記第２乱数信号と前記第６乱数信号とを入力信号として、第９乱数信号および第１０乱数信号を生成し、
予め設定された信号を含むチャレンジコードを生成し、
前記要求信号に対する応答信号として前記第９乱数信号および前記チャレンジコードを前記外部サーバ装置へ出力し、
出力した前記応答信号に基づいて前記外部サーバ装置から認証信号と前記暗号化更新データとを受け取り、
受け取った前記認証信号と、前記第１０乱数信号とが一致している場合に、前記外部サーバ装置から受け取った前記暗号化更新データの復号処理を行う、
プログラム。
【０１５４】
（付記１８）
メモリと、乱数生成回路と、制御回路と、を有し、外部サーバ装置から暗号化更新デー

タを受け取り、受け取った暗号化更新データを外部端末装置に提供する半導体装置であって、
前記メモリは、前記外部サーバ装置との間で使用可能な共通鍵を記憶し、
前記制御回路は、
前記外部サーバ装置から、第１乱数信号、第２乱数信号、前記共通鍵により暗号化された第６乱数信号を含む暗号化鍵データ、および暗号化更新データを受け取り、
前記暗号化鍵データを前記共通鍵により復号して第６乱数信号を生成し、
前記外部端末装置に送信する要求信号として前記第１乱数信号および前記第２乱数信号を出力し、
前記要求信号に対する応答信号として前記外部端末装置から第１応答信号および第２応答信号を受け取り、
前記第１応答信号と前記第２乱数信号と前記第６乱数信号とを入力信号として、第８乱数信号を生成し、
前記第２応答信号と前記第８乱数信号とが一致している場合に、前記暗号化更新データを前記外部端末装置に提供する、半導体装置。
【０１５５】
（付記１９）
前記第６乱数信号および前記第８乱数信号は、
予め設定された同一の擬似ランダム関数に入力することよりそれぞれ演算される、
付記１８に記載の半導体装置。
【０１５６】
（付記２０）
前記制御回路は、
前記第２応答信号と前記第８乱数信号とが一致していない場合に、前記暗号化更新データに代えて、前記暗号化更新データと同じ桁数の乱数信号を前記外部端末装置に提供する、
付記１８に記載の半導体装置。
【０１５７】
（付記２１）
サーバ装置と、前記サーバ装置から更新データを受け取る端末装置とを含む送受信システムであって、
前記サーバ装置と、前記端末装置とは、マスタ鍵情報をそれぞれ予め記憶し、
前記サーバ装置は、前記端末装置に対して、第１乱数信号と、前記端末装置を認証するための第１チャレンジコードと、を前記端末装置へ送信し、
前記端末装置は、サーバ装置に対して、
前記第１乱数信号および前記第１チャレンジコードに基づいて生成した第１レスポンスコードと、前記サーバ装置を認証するための第２チャレンジコードと、を送信し、
前記サーバ装置は、前記端末装置に対して、
前記第１レスポンスコードが期待値と一致する場合に、前記マスタ鍵により暗号化された暗号化更新データと、前記第２チャレンジコードに対する第２レスポンスコードを送信し、
前記端末装置は、
前記第２レスポンスコードが期待値と一致する場合に、前記マスタ鍵を用いて受け取った前記暗号化更新データを復号する、
送受信システム。
【０１５８】
（付記２２）
前記サーバ装置と、前記端末装置とは、それぞれ共通の擬似ランダム関数を記憶し、
前記端末装置は、前記擬似ランダム関数に前記第１チャレンジコードを入力して前記第１レスポンスコードを生成し、

前記サーバ装置は、前記擬似ランダム関数に前記第２チャレンジコードを入力して前記第２レスポンスコードを生成する、
付記２１に記載の送受信システム。
【０１５９】
（付記２３）
前記サーバ装置は、真性乱数生成回路を有しており、
前記第１乱数信号と前記第１チャレンジコードとはそれぞれ真性乱数信号である、
付記２１に記載の送受信システム。
【０１６０】
（付記２４）
前記端末装置は、真性乱数生成回路を有しており、
前記第２チャレンジコードは真性乱数信号である、
付記２３に記載の送受信システム。
【０１６１】
（付記２５）
前記端末装置は、受け取った前記暗号化更新データに基づいて更新データの登録が完了した場合に、前記第１乱数信号および第１チャレンジコードに基づいて生成した更新結果信号を前記サーバ装置に送信し、
前記サーバ装置は、
前記端末装置から受け取った前記更新結果信号が、期待値と一致する場合には、前記端末装置のデータが前記更新データであることを登録するか、期待値と一致しない場合には、前記端末装置のデータが前記更新データでないことを登録する、
付記２１に記載の送受信システム。
【０１６２】
（付記２６）
前記サーバ装置は、前記第１チャレンジコードが期待値と一致しない場合に、前記暗号化更新データに代えて、前記暗号化更新データと同じ桁数の乱数信号を送信する、
付記２１に記載の送受信システム。
【０１６３】
（付記２７）
前記端末装置は、前記レスポンスコードが期待値と一致しない場合に、受け取った前記暗号化更新データを復号しない、
付記２１に記載の送受信システム。
【０１６４】
（付記２８）
前記サーバ装置と前記端末装置との通信を中継する中継装置を更に有し、
前記中継装置は、前記端末装置に対して更新前データのバージョン情報を要求する信号を送信し、前記端末装置から受け取った前記バージョン情報と、前記更新前データを更新する処理を要求する信号と、を前記サーバ装置に送信する、
付記２１に記載の送受信システム。
【０１６５】
（付記２９）
前記サーバ装置と前記端末装置との通信を中継する中継装置を更に有し、
前記サーバ装置と、前記中継装置とは、共通鍵をそれぞれ予め記憶し、
前記サーバ装置は、前記中継装置に対して、
第１乱数信号、前記第１チャレンジコード、前記共通鍵により暗号化された第６乱数信号を含む暗号化鍵データ、および前記暗号化更新データ、を送信し、
前記中継装置は、前記端末装置に対して、
前記第１乱数信号と、第１チャレンジコードと、を送信し、
前記端末装置は、前記中継装置に対して、

前記第１乱数信号と、前記第１レスポンスコードと、前記第２チャレンジコードと、を送信し、
　前記中継装置は、前記端末装置に対して、
前記第１レスポンスコードが期待値と一致する場合に、
前記暗号化更新データと、前記第２レスポンスコードと、を送信し、
　前記端末装置は、前記第２レスポンスコードが期待値と一致する場合に、受け取った前記暗号化更新データを復号する、
付記２１に記載の送受信システム。
【産業上の利用可能性】
【０１６６】
　一実施の形態は、更新プログラムの授受を行うサーバ装置、端末装置等に適用可能である。
【符号の説明】
【０１６７】
１、２、３　送受信システム
１１、２１、３１　サーバ装置
１２、２２、３２　中継装置
１３、２３、３３　端末装置
１１０、２１０　第１半導体装置
１２０、３２０　第２半導体装置
１３０、２３０　第３半導体装置
９００　ネットワーク
ＳＧ０１　更新前データ
ＳＧ０２　更新データ
ＳＧ０３　更新前バージョンデータ
ＳＧ０４　更新バージョンデータ
ＳＧ０５　識別子
ＳＧ０６　マスタ鍵
ＳＧ０７　第１２乱数信号
ＳＧ０８　バージョンチェック要求信号
ＳＧ０９　バージョンアップ要求信号
ＳＧ１０　比較結果信号
ＳＧ１１　第１乱数信号
ＳＧ１２　第２乱数信号
ＳＧ１３　第６乱数信号
ＳＧ１４　第７乱数信号
ＳＧ１５　第３乱数信号
ＳＧ１６　第９乱数信号
ＳＧ１７　第１０乱数信号
ＳＧ１８　第８乱数信号
ＳＧ１９　第１１乱数信号
ＳＧ２０　比較結果信号
ＳＧ２１　暗号化更新データ
ＳＧ２２　第４乱数信号
ＳＧ２３　暗号文
ＳＧ２４　比較結果信号
ＳＧ２５　比較結果信号
ＳＧ２６　第１３乱数信号
ＳＧ２７　第１４乱数信号
ＳＧ２８　第1更新結果信号

ＳＧ２９　第５乱数信号
ＳＧ３０　第２更新結果信号
ＳＧ３１　比較結果信号
ＳＧ３２　共通鍵
ＳＧ３３　暗号文

【図１】

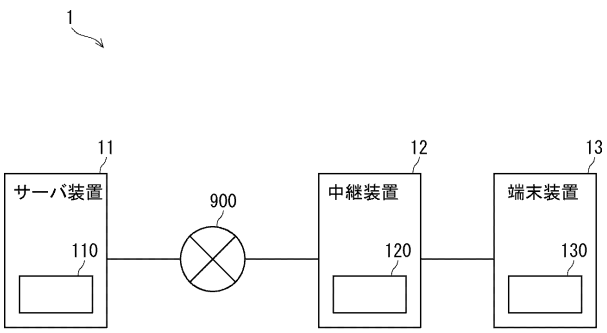

Fig. 1

【図２】

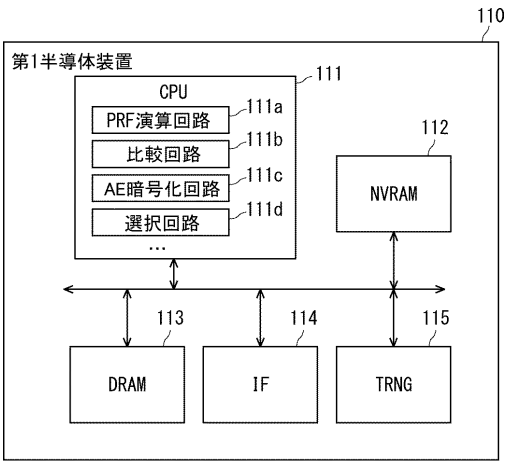

Fig. 2

【図３】

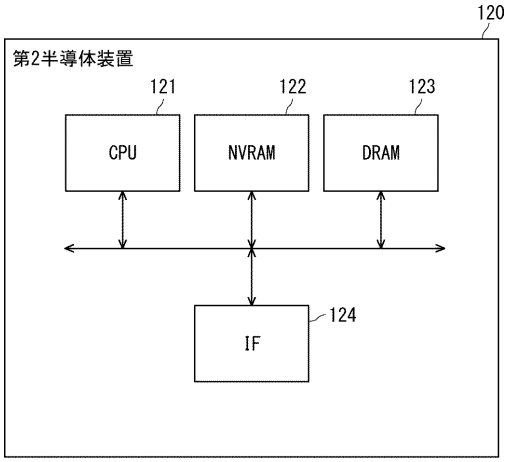

Fig. 3

【図４】

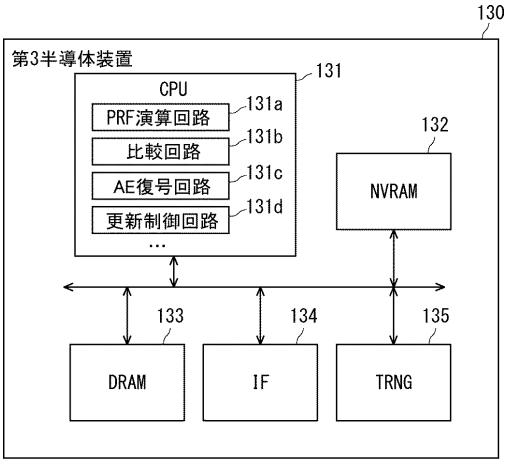

Fig. 4

【図５】

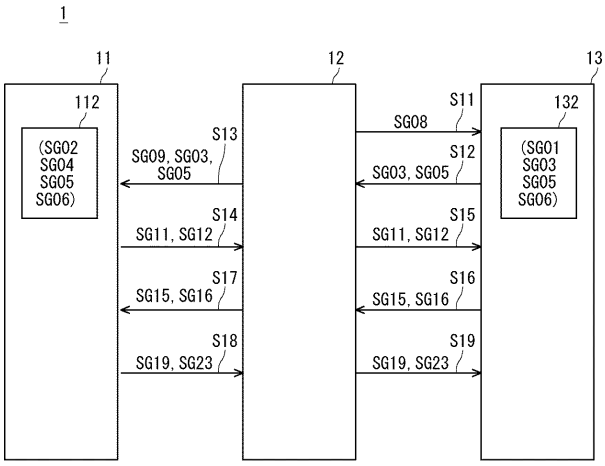

Fig. 5

【図６】

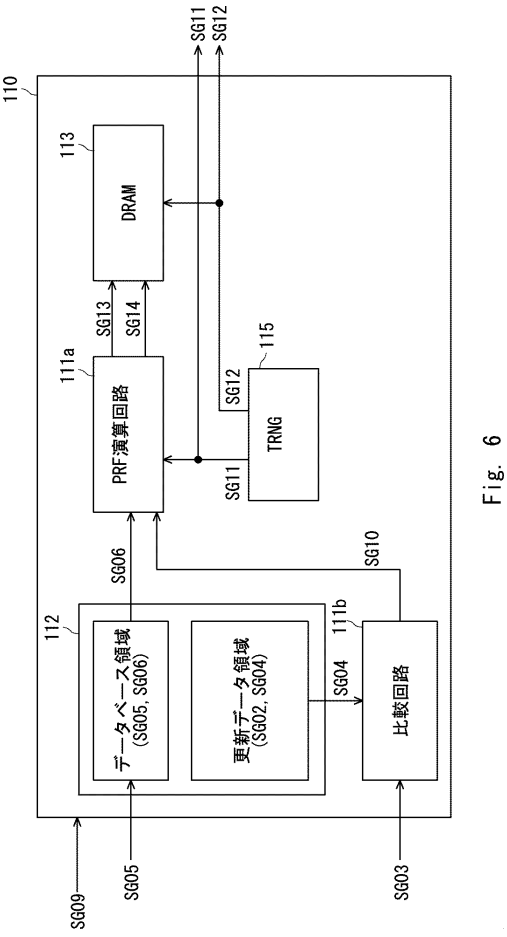

Fig. 6

【図７】

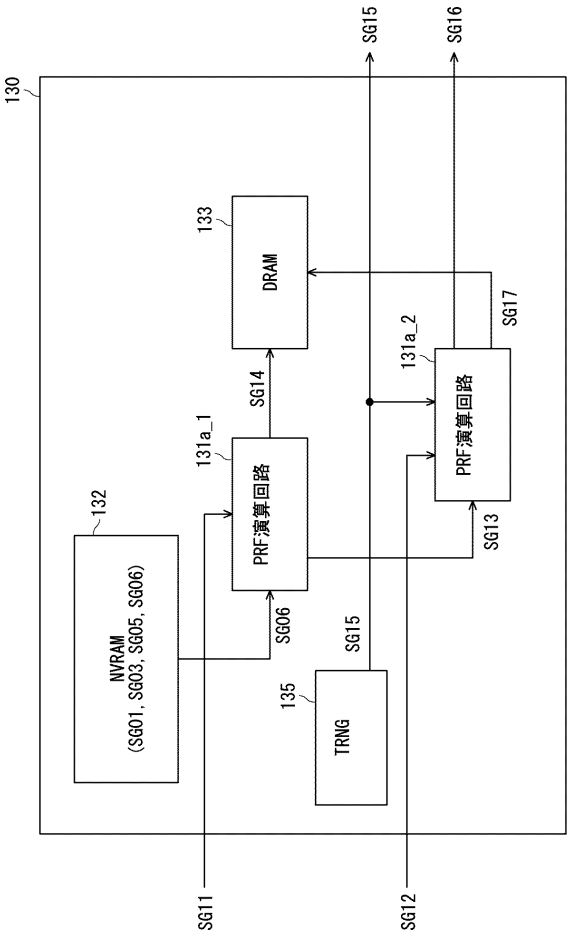

Fig. 7

【図８】

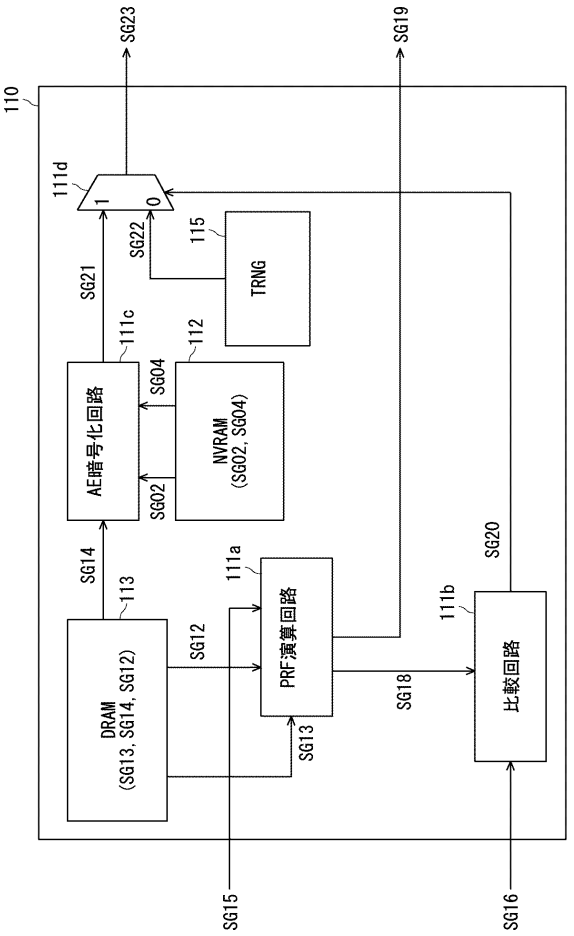

Fig. 8

【図９】

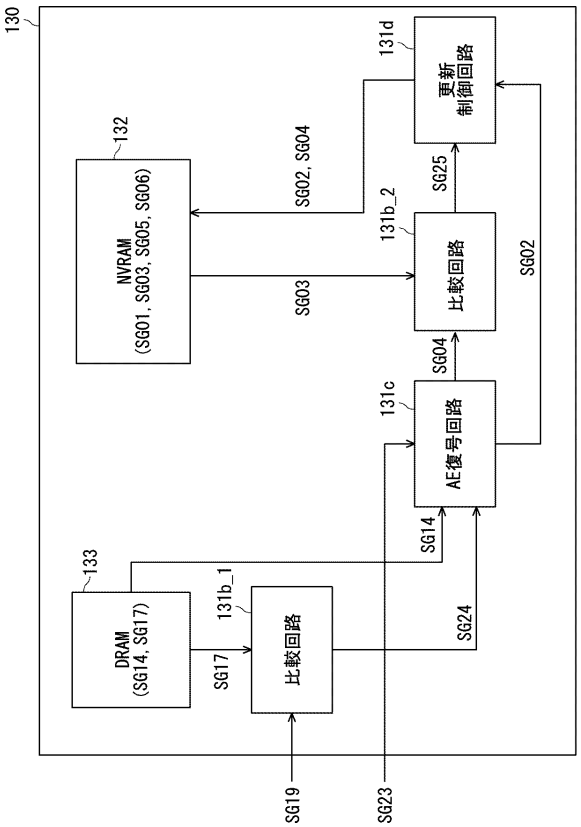

Fig. 9

【図１０】

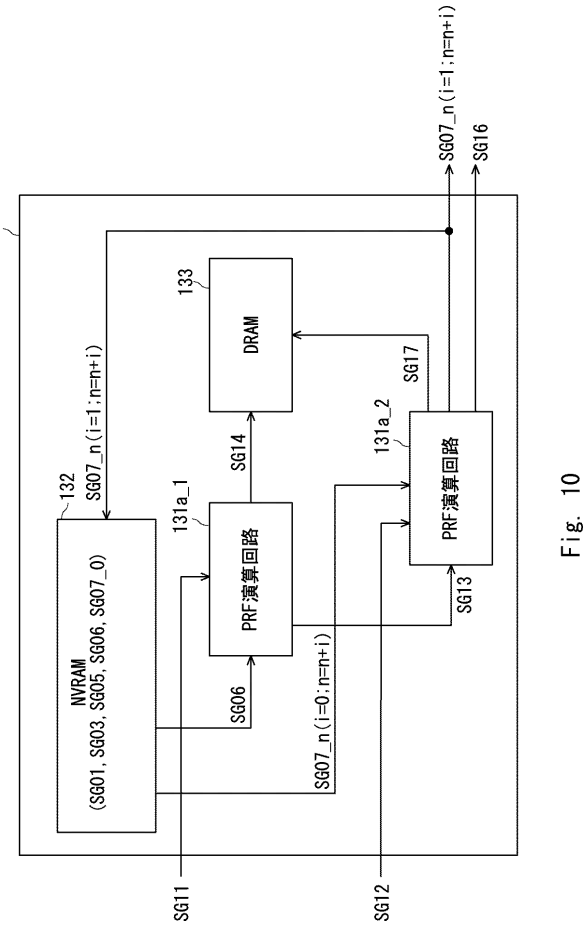

Fig. 10

【図１１】

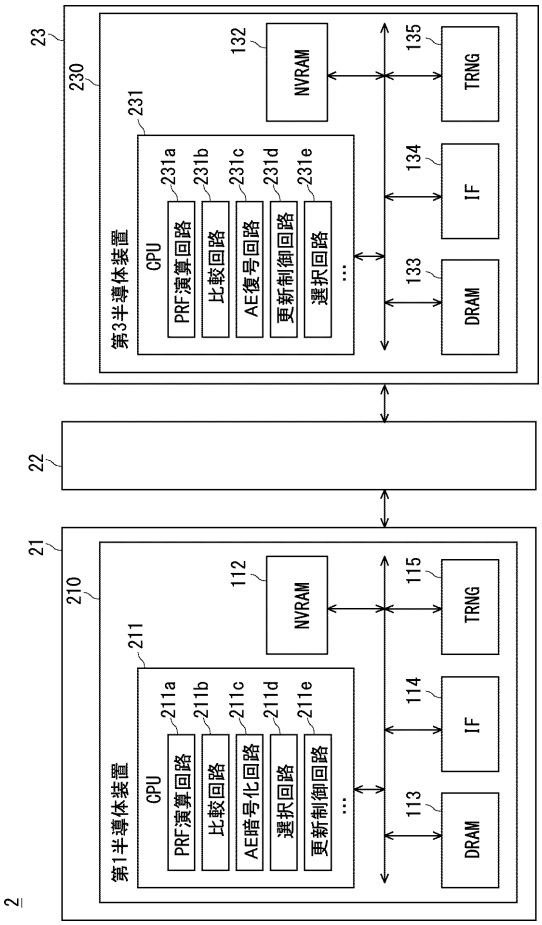

Fig. 11

【図１２】

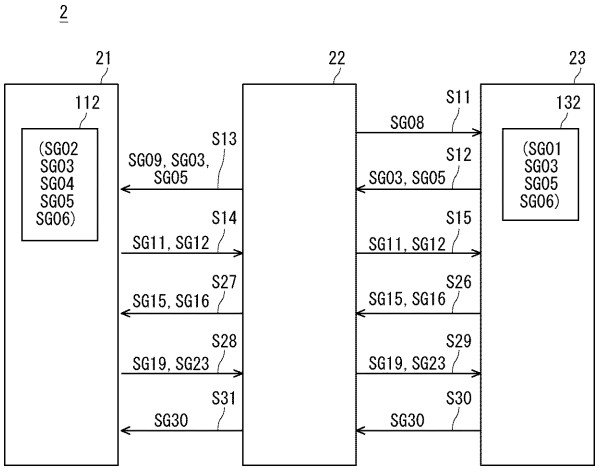

Fig. 12

【図１３】

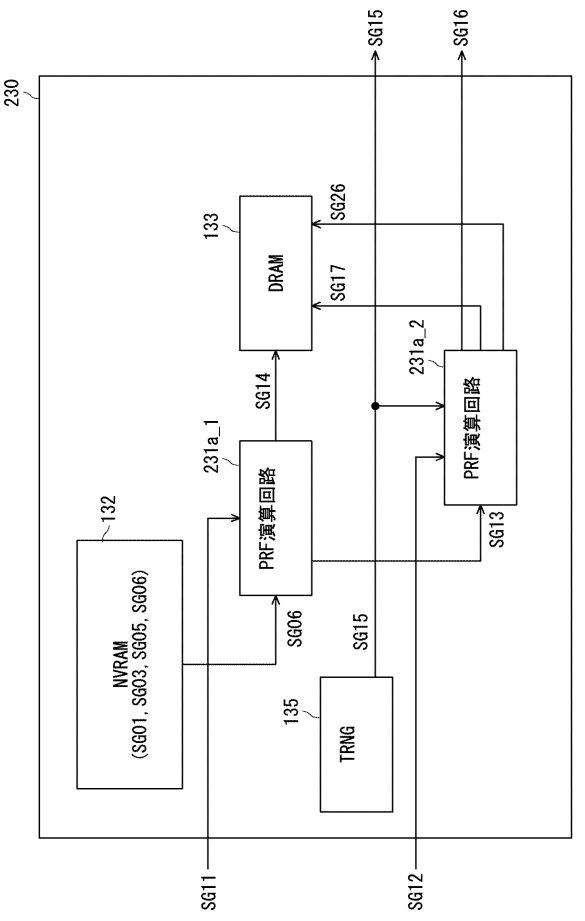

Fig. 13

【図１４】

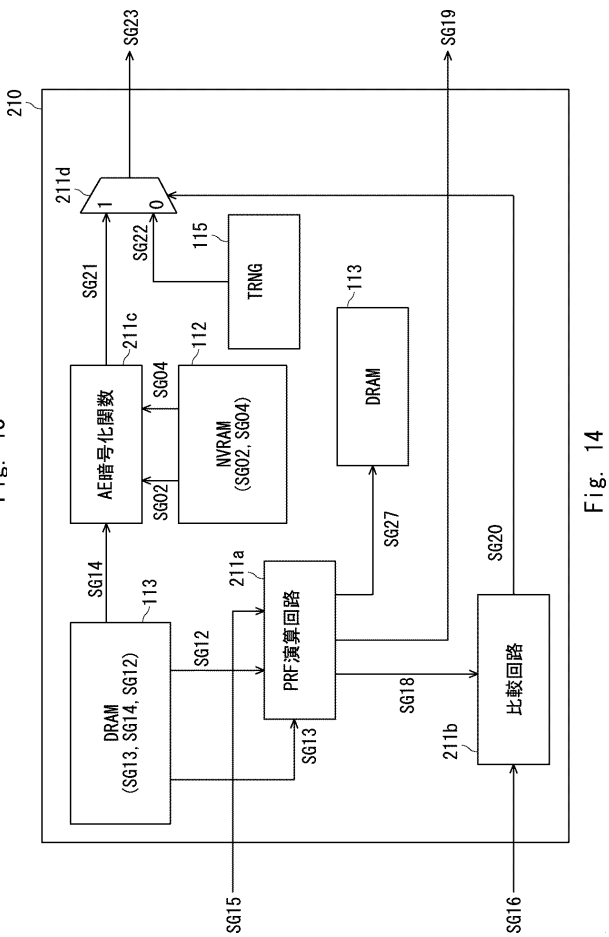

Fig. 14

【図１５】

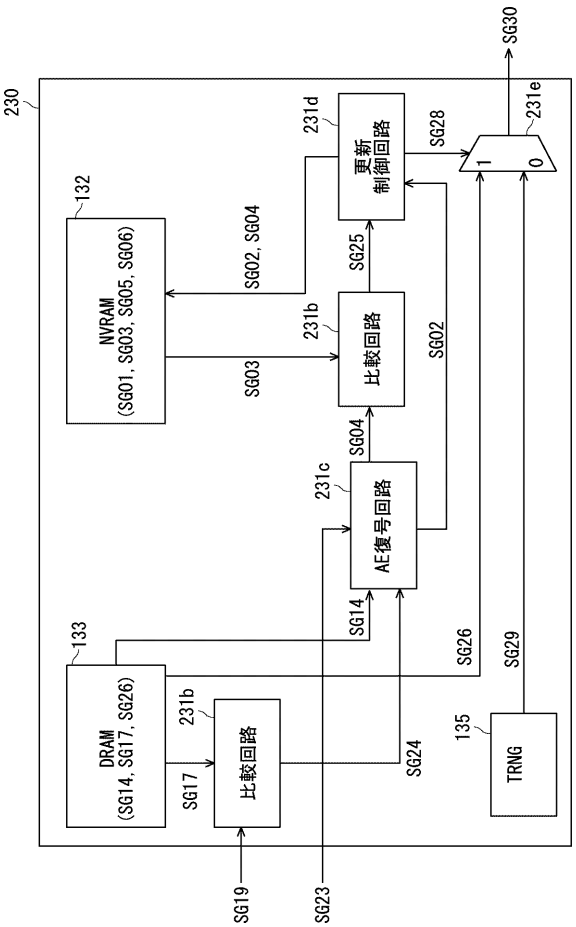

Fig. 15

【図１６】

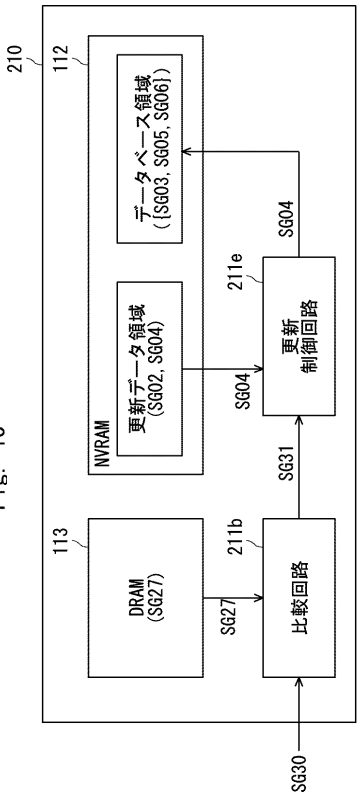

Fig. 16

【図１７】

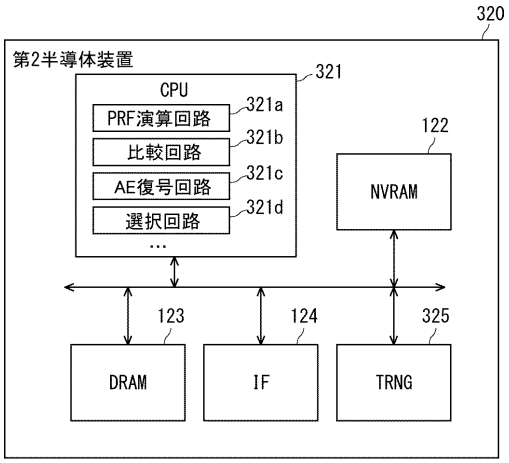

Fig. 17

【図１８】

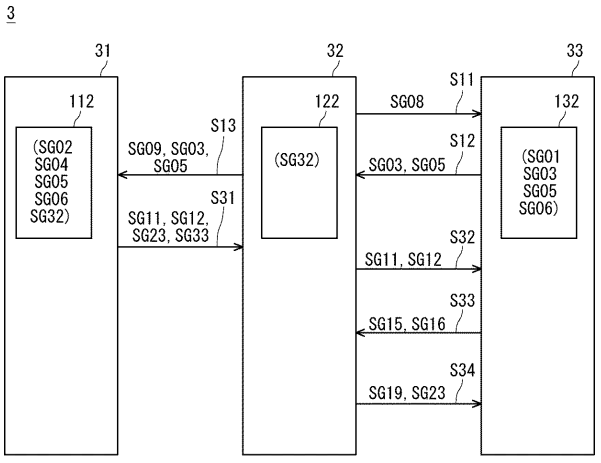

Fig. 18

【図１９】

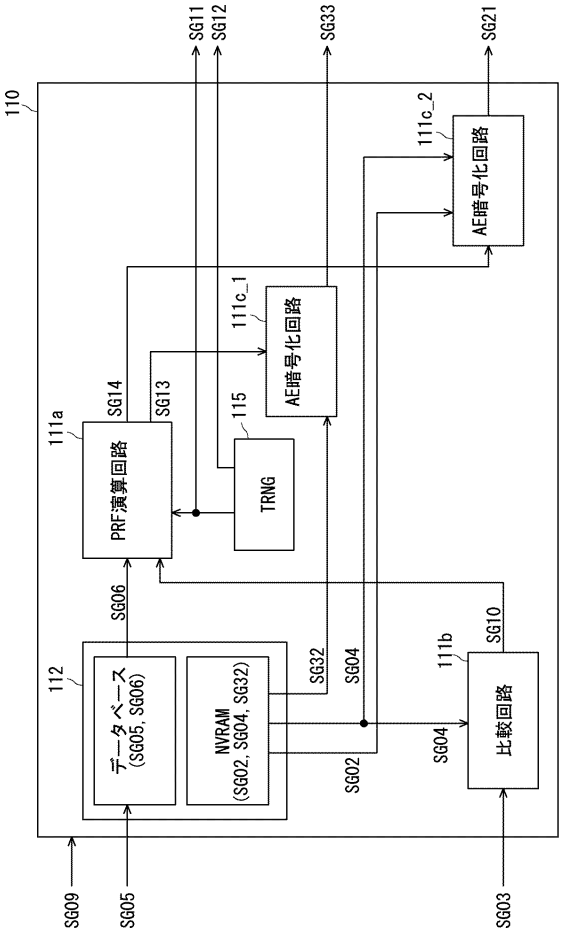

Fig. 19

【図２０】

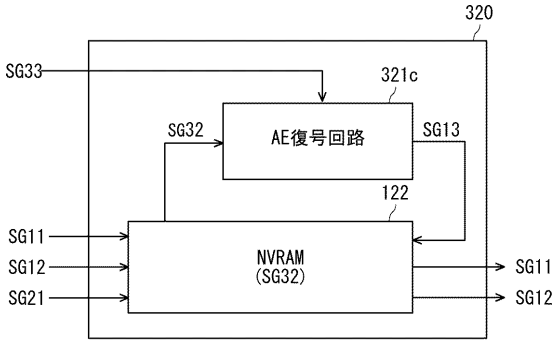

Fig. 20

【図２１】

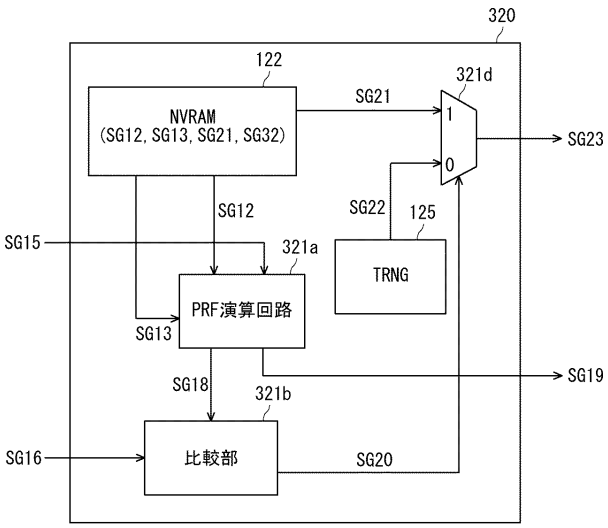

Fig. 21

フロントページの続き

審査官　寺谷　大亮

(56)参考文献　国際公開第２０１６／０２０６４０（WO，Ａ１）
特開２０１７－２２６５４（ＪＰ，Ａ）
特開２００３－１５０４５３（ＪＰ，Ａ）
特開２０１２－９３９２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／５７
Ｇ０９Ｃ　　１／００