(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-169147
(P2017-169147A)
(43)公開日　平成29年9月21日(2017.9.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
G06F 21/64	(2013.01)	G06F	21/64		

審査請求 未請求　請求項の数 19　ＯＬ　（全 25 頁）

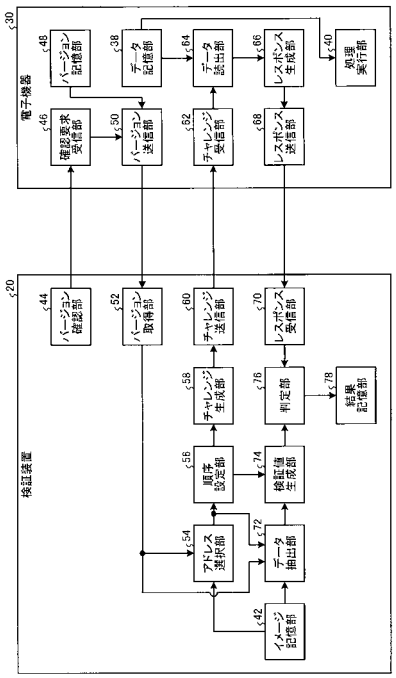
(21)出願番号　特願2016-54535(P2016-54535)
(22)出願日　平成28年3月17日(2016.3.17)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　趙　方明
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　春木　洋美
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　松下　達之
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】検証装置、電子機器、プログラムおよび検証システム

(57)【要約】
【課題】電子機器に記憶されている対象データを遠隔から検証する。
【解決手段】実施形態に係る検証装置は、イメージ記憶部と、アドレス選択部と、チャレンジ生成部と、チャレンジ送信部と、レスポンス受信部と、データ抽出部と、検証値生成部と、判定部とを備える。イメージ記憶部は、電子機器が備えるデータ記憶部のメモリイメージを記憶する。アドレス選択部は、アドレスを選択する。チャレンジ生成部は、選択されたアドレスを含むチャレンジ情報を生成する。チャレンジ送信部は、チャレンジ情報を電子機器に送信する。レスポンス受信部は、レスポンス値を電子機器から受信する。データ抽出部は、メモリイメージから選択されたアドレスに記憶されているべき対象データを抽出する。検証値生成部は、抽出した対象データから予め定められた演算アルゴリズムを用いて検証値を生成する。判定部は、レスポンス値と検証値とが一致する場合、正常であると判定する。
【選択図】図２



【特許請求の範囲】
【請求項１】
情報処理を実行する電子機器に記憶されている対象データをネットワークを介して検証する検証装置であって、
前記電子機器が備えるデータ記憶部のメモリイメージを記憶するイメージ記憶部と、
前記データ記憶部における少なくとも１つのアドレスを選択するアドレス選択部と、
選択された前記少なくとも１つのアドレスを含むチャレンジ情報を生成するチャレンジ生成部と、
前記チャレンジ情報を前記電子機器にネットワークを介して送信するチャレンジ送信部と、
前記チャレンジ情報を送信したことに応じて返信されたレスポンス値を前記電子機器からネットワークを介して受信するレスポンス受信部と、
前記メモリイメージから、選択された前記少なくとも１つのアドレスに記憶されているべき少なくとも１つの対象データを抽出するデータ抽出部と、
抽出した前記少なくとも１つの対象データから、予め定められた演算アルゴリズムを用いて検証値を生成する検証値生成部と、
前記レスポンス値と前記検証値とが一致する場合、前記データ記憶部に記憶されている対象データが正常であると判定する判定部と、
を備える検証装置。
【請求項２】
前記検証値生成部は、予め定められたハッシュ関数を用いて、抽出した前記少なくとも１つの対象データにより定まるハッシュ値を前記検証値として算出する
請求項１に記載の検証装置。
【請求項３】
前記アドレス選択部は、前記データ記憶部における複数のアドレスを選択し、
前記検証装置は、前記複数のアドレスをランダムに並べ替える順序設定部をさらに備え、
前記チャレンジ生成部は、選択された前記複数のアドレスを、並び順を識別可能に含む前記チャレンジ情報を生成し、
前記データ抽出部は、前記メモリイメージから、選択された前記複数のアドレスに記憶されているべき複数の対象データを抽出し、
前記検証値生成部は、設定された並び順で並べられた前記複数の対象データから、前記ハッシュ関数を用いて前記検証値を生成する
請求項２に記載の検証装置。
【請求項４】
前記検証値生成部は、抽出した前記複数の対象データを設定された並び順に従って連結し、連結されたデータを前記ハッシュ関数に与えて前記検証値を生成する
請求項３に記載の検証装置。
【請求項５】
乱数を発生する乱数発生部をさらに備え、
前記チャレンジ生成部は、前記少なくとも１つのアドレスおよび前記乱数を含む前記チャレンジ情報を生成し、
前記検証値生成部は、抽出した前記少なくとも１つの対象データおよび前記乱数を前記ハッシュ関数に与えて、前記検証値を生成する
請求項２に記載の検証装置。
【請求項６】
前記検証値生成部は、抽出した前記少なくとも１つの対象データと前記乱数とを連結し、連結されたデータを前記ハッシュ関数に与えて前記検証値を生成する
請求項５に記載の検証装置。
【請求項７】

前記データ記憶部に記憶されている対象データのバージョンを取得するバージョン取得部をさらに備え、
前記イメージ記憶部は、バージョン毎に前記メモリイメージを記憶し、
前記データ抽出部は、取得したバージョンに対応する前記メモリイメージから、前記少なくとも１つの対象データを取得する
請求項１から６の何れか１項に記載の検証装置。
【請求項８】
同一の前記メモリイメージを記憶する複数の電子機器を管理するグループ管理部をさらに備え、
前記チャレンジ送信部は、前記チャレンジ情報を前記複数の電子機器のそれぞれにネットワークを介して一斉送信する
請求項１から６の何れか１項に記載の検証装置。
【請求項９】
前記レスポンス受信部は、前記複数の電子機器のそれぞれから、前記レスポンス値と前記電子機器を識別する識別情報との組を受信し、
前記検証値生成部は、前記レスポンス値と前記識別情報との組を受信する毎に、抽出した前記少なくとも１つの対象データおよび前記識別情報を予め定められたハッシュ関数に与えて前記検証値を生成し、
前記判定部は、前記レスポンス値と前記識別情報との組を受信する毎に、前記レスポンス値と前記検証値とが一致する場合、前記データ記憶部に記憶されている対象データが正常であると判定する
請求項８に記載の検証装置。
【請求項１０】
前記検証値生成部は、抽出した前記少なくとも１つの対象データと前記識別情報とを連結し、連結されたデータを前記ハッシュ関数に与えて前記検証値を生成する
請求項９に記載の検証装置。
【請求項１１】
前記判定部は、前記識別情報が同一である複数の前記レスポンス値を受信した場合、受信した前記識別情報に対応する前記電子機器の前記データ記憶部に記憶されている対象データが正常ではないと判定する
請求項９または１０に記載の検証装置。
【請求項１２】
前記判定部が、前記データ記憶部における選択されたアドレスに記憶されている対象データが正常であると判定した場合、前記アドレス選択部にさらに他の少なくとも１つのアドレスを新たに選択させて、前記チャレンジ生成部、前記チャレンジ送信部、前記レスポンス受信部、前記データ抽出部、前記検証値生成部および前記判定部に、新たに選択された前記少なくとも１つのアドレスに基づき処理を再度実行させる繰返制御部
をさらに備える請求項１から１１の何れか１項に記載の検証装置。
【請求項１３】
情報処理装置を請求項１から１２の何れか１項に記載の検証装置として機能させるためのプログラム。
【請求項１４】
検証装置からネットワークを介して検証がされる電子機器であって、
対象データを記憶するデータ記憶部と、
前記データ記憶部に記憶されている前記対象データを読み出して情報処理を実行する処理実行部と、
前記検証装置からネットワークを介して、前記データ記憶部の少なくとも１つのアドレスを含むチャレンジ情報を受信するチャレンジ受信部と、
前記チャレンジ情報に含まれる前記少なくとも１つのアドレスの対象データを、前記データ記憶部から読み出すデータ読出部と、

読み出した前記少なくとも１つの対象データから、予め定められた演算アルゴリズムを用いてレスポンス値を生成するレスポンス生成部と、
前記レスポンス値を前記検証装置にネットワークを介して送信するレスポンス送信部と、
を備える電子機器。
【請求項１５】
前記レスポンス生成部は、予め定められたハッシュ関数を用いて、読み出した前記少なくとも１つの対象データからハッシュ値を、前記レスポンス値として算出する
請求項１４に記載の電子機器。
【請求項１６】
前記チャレンジ受信部は、前記少なくとも１つのアドレスおよび乱数を含む前記チャレンジ情報を受信し、
前記レスポンス生成部は、読み出した前記少なくとも１つの対象データおよび前記チャレンジ情報に含まれる前記乱数を前記ハッシュ関数に与えて、前記レスポンス値を生成する
請求項１５に記載の電子機器。
【請求項１７】
前記電子機器を識別する識別情報を記憶する識別情報記憶部をさらに備え、
前記レスポンス生成部は、読み出した前記少なくとも１つの対象データおよび前記識別情報を前記ハッシュ関数に与えて、前記レスポンス値を生成し、
前記レスポンス送信部は、前記レスポンス値と前記識別情報との組を前記検証装置に送信する
請求項１５または１６に記載の電子機器。
【請求項１８】
情報処理装置を請求項１４から１７の何れか１項に記載の電子機器として機能させるためのプログラム。
【請求項１９】
情報処理を実行する電子機器と、
前記電子機器に記憶されている対象データをネットワークを介して検証する検証装置と、
を備える検証システムであって、
前記電子機器は、
対象データを記憶するデータ記憶部と、
前記データ記憶部に記憶されている前記対象データを読み出して情報処理を実行する処理実行部と、
を備え、
前記検証装置は、
前記データ記憶部のメモリイメージを記憶するイメージ記憶部と、
前記データ記憶部における少なくとも１つのアドレスを選択するアドレス選択部と、
選択された前記少なくとも１つのアドレスを含むチャレンジ情報を生成するチャレンジ生成部と、
前記チャレンジ情報を前記電子機器にネットワークを介して送信するチャレンジ送信部と、
を備え、
前記電子機器は、
前記検証装置からネットワークを介して、前記チャレンジ情報を受信するチャレンジ受信部と、
前記チャレンジ情報に含まれる前記少なくとも１つのアドレスの対象データを、前記データ記憶部から読み出すデータ読出部と、
読み出した前記少なくとも１つの対象データから、予め定められた演算アルゴリズムを

用いてレスポンス値を生成するレスポンス生成部と、
前記レスポンス値を前記検証装置にネットワークを介して送信するレスポンス送信部と、
をさらに備え、
前記検証装置は、
前記チャレンジ情報を送信したことに応じて返信された前記レスポンス値を前記電子機器からネットワークを介して受信するレスポンス受信部と、
前記メモリイメージから、選択された前記少なくとも１つのアドレスに記憶されているべき少なくとも１つの対象データを抽出するデータ抽出部と、
抽出した前記少なくとも１つの対象データから、前記レスポンス生成部と同一の前記演算アルゴリズムを用いて検証値を生成する検証値生成部と、
前記レスポンス値と前記検証値とが一致する場合、前記データ記憶部に記憶されている対象データが正常であると判定する判定部と、
をさらに備える
検証システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、検証装置、電子機器、プログラムおよび検証システムに関する。
【背景技術】
【０００２】
従来より、組込機器およびＩｏＴ（Internet of Things）機器等の電子機器が知られている。このような電子機器は、プログラムを実行するプロセッサ、および、プログラムおよびデータを格納したメモリを有し、プロセッサがメモリに記憶されているプログラムを実行する。また、このような電子機器は、通信機能を有し、ネットワークを介して新たなプログラムおよびデータを受信して、メモリに記憶されているプログラムおよびデータをアップデートすることができる。
【０００３】
ところで、このような電子機器は、プログラムのアップデート中にエラーが発生した場合、メモリに記憶されるプログラムまたはデータに欠陥が生じてしまう可能性がある。また、このような電子機器は、ネットワークに接続されているので、サイバー攻撃者から攻撃を受けて、メモリに記憶されたプログラムまたはデータが書き換えられる恐れもある。
【０００４】
このため、管理者は、電子機器のメモリに記憶されているプログラムおよびデータが正常であるか否かを定期的に確認しなければならない。また、管理者は、このような確認を、電子機器の動作を停止することなく遠隔からネットワークを介して実行することが望ましい。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１１－２３８２４６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明が解決しようとする課題は、情報処理を実行する電子機器に記憶されている対象データが正常であるか否かを、ネットワークを介して遠隔から検証することにある。
【課題を解決するための手段】
【０００７】
実施形態に係る検証装置は、情報処理を実行する電子機器に記憶されている対象データをネットワークを介して検証する。前記検証装置は、イメージ記憶部と、アドレス選択部

と、チャレンジ生成部と、チャレンジ送信部と、レスポンス受信部と、データ抽出部と、検証値生成部と、判定部とを備える。前記イメージ記憶部は、前記電子機器が備えるデータ記憶部のメモリイメージを記憶する。前記アドレス選択部は、前記データ記憶部における少なくとも１つのアドレスを選択する。前記チャレンジ生成部は、選択された前記少なくとも１つのアドレスを含むチャレンジ情報を生成する。前記チャレンジ送信部は、前記チャレンジ情報を前記電子機器にネットワークを介して送信する。前記レスポンス受信部は、前記チャレンジ情報を送信したことに応じて返信されたレスポンス値を前記電子機器からネットワークを介して受信する。前記データ抽出部は、前記メモリイメージから、選択された前記少なくとも１つのアドレスに記憶されているべき少なくとも１つの対象データを抽出する。前記検証値生成部は、抽出した前記少なくとも１つの対象データから、予め定められた演算アルゴリズムを用いて検証値を生成する。前記判定部は、前記レスポンス値と前記検証値とが一致する場合、前記データ記憶部に記憶されている対象データが正常であると判定する。

【図面の簡単な説明】

【０００８】

【図１】第１実施形態に係る検証システムの構成図。

【図２】第１実施形態に係る検証装置および電子機器の構成図。

【図３】第１実施形態に係る検証システムの処理の流れを示すフローチャート。

【図４】第２実施形態に係る検証装置および電子機器の構成図。

【図５】第２実施形態に係る検証システムの処理の流れを示すフローチャート。

【図６】第３実施形態に係る検証システムの構成図。

【図７】第３実施形態に係る検証装置および電子機器の構成図。

【図８】第３実施形態に係る検証システムの処理の流れを示すフローチャート。

【図９】第４実施形態に係る検証装置および電子機器の構成図。

【図１０】検証装置および電子機器のハードウェア構成図。

【発明を実施するための形態】

【０００９】

以下、図面を参照しながら実施形態に係る検証システム１０について詳細に説明する。検証システム１０は、情報処理を実行する機器に記憶されている対象データが正常であるか否かを、ネットワークを介して遠隔から検証することを目的とする。

【００１０】

（第１実施形態）

図１は、第１実施形態に係る検証システム１０を示す図である。検証システム１０は、検証装置２０と、電子機器３０とを備える。

【００１１】

検証装置２０は、サーバ等の情報処理装置である。検証装置２０は、ネットワークを介して電子機器３０との間で情報を送受信することが可能である。ネットワークは、どのようなものであってもよく、インターネット等の公衆ネットワークであっても、グループ内や建物内等においてクローズしている専用ネットワークであってもよい。

【００１２】

電子機器３０は、組込機器およびＩｏＴ機器等の機器である。電子機器３０は、プログラムを実行するプロセッサと、プログラムおよびデータを記憶するメモリを有する。電子機器３０は、メモリに記憶されたプログラムおよびデータをプロセッサが実行することにより処理を実行する機能を有する。また、電子機器３０は、ネットワークを介して他の装置と情報を送受信することが可能である。

【００１３】

例えば、電子機器３０は、家庭用の電化製品、または、工業用のロボット、飛行機および車両に設けられる電子制御装置（ＥＣＵ）等であってよい。電子機器３０は、ハードウェアとして、ＣＰＵ（Central Processing Unit）等の処理ユニット、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、不揮発性記憶装置等の記憶ユニッ

ト、検証装置２０と接続するための通信ユニット等を有する。このような電子機器３０は、プログラムとハードウェアとが協働して、情報処理および制御を実行する。

【００１４】

検証装置２０は、電子機器３０に記憶されている対象データを、ネットワークを介して遠隔から検証する。ここで、対象のデータは、プログラムおよびプログラムにより参照されるデータを含む。対象データは、電子機器３０の工場出荷時またはバージョン更新時において、メモリ上の特定のアドレスに書き込まれる。また、メモリに書き込まれた後には、次にバージョンの更新がされるまで書き換えがされない。

【００１５】

検証装置２０は、電子機器３０との間でネットワークを介して情報をやり取りして、電子機器３０のメモリに、本来書き込まれているべき対象データ（プログラムおよびデータ）が記憶されているか否かを確認する。これにより、検証装置２０は、電子機器３０のバージョン更新の処理が失敗してメモリに記憶されている対象データに異常が生じていたり、または、サイバー攻撃等によりメモリに記憶されている対象データに異常が生じていたりすることを検出できる。

【００１６】

図２は、第１実施形態に係る検証装置２０および電子機器３０の機能構成を示す図である。検証装置２０は、イメージ記憶部４２と、バージョン確認部４４と、バージョン取得部５２と、アドレス選択部５４と、順序設定部５６と、チャレンジ生成部５８と、チャレンジ送信部６０と、レスポンス受信部７０と、データ抽出部７２と、検証値生成部７４と、判定部７６と、結果記憶部７８とを有する。電子機器３０は、データ記憶部３８と、処理実行部４０と、確認要求受信部４６と、バージョン記憶部４８と、バージョン送信部５０と、チャレンジ受信部６２と、データ読出部６４と、レスポンス生成部６６と、レスポンス送信部６８とを有する。

【００１７】

電子機器３０におけるデータ記憶部３８は、検証対象となる対象データ（プログラムおよびデータ）を記憶する。データ記憶部３８は、例えば、不揮発性のメモリ等により実現される。不揮発性のメモリは、半導体メモリであってもよいし、ハードディスク等のディスク記録媒体であってもよい。データ記憶部３８に記憶されている対象データは、工場出荷時またはバージョン更新時等に書き換えられる。

【００１８】

電子機器３０における処理実行部４０は、データ記憶部３８に記憶された対象データ（プログラムおよびデータ）に基づき情報処理および制御処理等を実行する。

【００１９】

検証装置２０におけるイメージ記憶部４２は、電子機器３０が備えるデータ記憶部３８のメモリイメージを記憶する。ここで、メモリイメージは、データ記憶部３８に記憶された対象データと、そのデータが記憶されているアドレスとの関係が検出可能な情報である。従って、メモリイメージを参照することにより、データ記憶部３８上における特定のアドレスに記憶されている対象データを抽出することができる。イメージ記憶部４２は、メモリイメージをどのような形式で記憶していてもよい。

【００２０】

また、イメージ記憶部４２は、バージョン毎にメモリイメージを記憶する。例えば、イメージ記憶部４２は、データ記憶部３８に記憶されている対象データが更新される毎に、新たなバージョンのメモリイメージを記憶する。また、旧バージョンの対象データを記憶している電子機器３０と、新バージョンの対象データを記憶している電子機器３０とが混在する可能性がある場合、イメージ記憶部４２は、それぞれのバージョンのメモリイメージを記憶する。

【００２１】

検証装置２０におけるバージョン確認部４４は、検証対象となる電子機器３０に対してネットワークを介してバージョンの確認要求を送信する。

【００２２】
電子機器３０における確認要求受信部４６は、検証装置２０からネットワークを介してバージョンの確認要求を受信する。電子機器３０におけるバージョン記憶部４８は、データ記憶部３８に記憶されている対象データのバージョンを表すバージョン情報を記憶する。電子機器３０におけるバージョン送信部５０は、確認要求受信部４６がバージョンの確認要求を受信した場合、バージョン記憶部４８に記憶されているバージョン情報を読み出す。そして、バージョン送信部５０は、読み出したバージョン情報を、ネットワークを介して検証装置２０に送信する。
【００２３】
検証装置２０におけるバージョン取得部５２は、電子機器３０からネットワークを介してバージョン情報を受信する。そして、バージョン取得部５２は、バージョン情報を解析して、データ記憶部３８に記憶されている対象データのバージョンを取得する。なお、バージョン取得部５２は、電子機器３０からではなく、それぞれの電子機器３０のバージョンを管理する管理装置等から、バージョン情報を取得してもよい。管理装置は、ネットワーク上に存在していてもよいし、検証装置２０が備えていてもよい。
【００２４】
検証装置２０におけるアドレス選択部５４は、データ記憶部３８の対象データが記憶されている領域における少なくとも１つのアドレスを選択する。本実施形態においては、アドレス選択部５４は、複数のアドレスを選択する。なお、アドレス選択部５４は、検証を実行する毎に、任意の複数のアドレスを選択する。アドレス選択部５４は、検証を実行する毎に異なるアドレスを選択する。アドレス選択部５４は、検証を実行する毎に、ランダムにアドレスを選択してもよいし、例えば予め登録されたリスト等を参照して異なるアドレスを選択してもよい。なお、アドレス選択部５４は、バージョン毎に対象データが記憶されている記録範囲が異なる場合には、バージョンに応じた記録範囲の中からアドレスを選択する。
【００２５】
検証装置２０における順序設定部５６は、アドレス選択部５４により選択された複数のアドレスをランダムに並べ替える。なお、アドレス選択部５４が１つのアドレスを選択する場合には、順序設定部５６は、何ら処理を実行しない。
【００２６】
検証装置２０におけるチャレンジ生成部５８は、選択された少なくとも１つのアドレスを含むチャレンジ情報を生成する。例えば、チャレンジ生成部５８は、選択された少なくとも１つのアドレスを含む配列データを、チャレンジ情報として生成する。本実施形態においては、チャレンジ生成部５８は、選択された複数のアドレスを、並べられた順序を識別可能に含むチャレンジ情報を生成する。例えば、チャレンジ生成部５８は、選択された複数のアドレスを、並び順に従った位置に格納した配列データを、チャレンジ情報として生成する。
【００２７】
検証装置２０におけるチャレンジ送信部６０は、チャレンジ生成部５８が生成したチャレンジ情報を電子機器３０にネットワークを介して送信する。
【００２８】
電子機器３０におけるチャレンジ受信部６２は、検証装置２０からネットワークを介してチャレンジ情報を受信する。電子機器３０におけるデータ読出部６４は、チャレンジ受信部６２がチャレンジ情報を受信した場合、チャレンジ情報に含まれる少なくとも１つのアドレスに記憶された対象データを、データ記憶部３８から読み出す。
【００２９】
電子機器３０におけるレスポンス生成部６６は、データ読出部６４が読み出した少なくとも１つの対象データから、予め定められた演算アルゴリズムを用いてレスポンス値を生成する。
【００３０】

ここで、予め定められた演算アルゴリズムは、例えば、予め定められたハッシュ関数である。ハッシュ関数は、不可逆な一方向関数である。ハッシュ関数は、同一の入力値（対象データ）を、同一の出力値（ハッシュ値）へと変換する。しかし、ハッシュ関数は、出力値を入力値へ変換する逆関数は存在せず、出力値から入力値を探索することは非常に困難である。

【００３１】

レスポンス生成部６６は、予め定められたハッシュ関数を用いて、読み出した少なくとも１つの対象データにより定まるハッシュ値を、レスポンス値として算出する。本実施形態においては、レスポンス生成部６６は、予め定められたハッシュ関数を用いて、読み出した複数の対象データおよび設定された並び順毎によって定まるハッシュ値を、レスポンス値として算出する。例えば、レスポンス生成部６６は、読み出した複数の対象データを、順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えてハッシュ値を算出する。

【００３２】

電子機器３０におけるレスポンス送信部６８は、レスポンス生成部６６が生成したレスポンス値を、検証装置２０にネットワークを介して送信する。この場合、レスポンス生成部は、検証装置２０から受信したチャレンジ情報の応答として、レスポンス値を返信する。

【００３３】

検証装置２０におけるレスポンス受信部７０は、チャレンジ情報を送信したことに応じて返信されたレスポンス値を電子機器３０からネットワークを介して受信する。

【００３４】

検証装置２０におけるデータ抽出部７２は、イメージ記憶部４２に記憶されているメモリイメージから、アドレス選択部５４により選択された少なくとも１つのアドレスに記憶されているべき少なくとも１つの対象データを抽出する。この場合、データ抽出部７２は、バージョン取得部５２が取得したバージョンに対応するメモリイメージから、少なくとも１つの対象データを取得する。本実施形態においては、データ抽出部７２は、アドレス選択部５４により選択された複数のアドレスに記憶されているべき複数の対象データを抽出する。

【００３５】

検証装置２０における検証値生成部７４は、データ抽出部７２が抽出した少なくとも１つの対象データから、予め定められた演算アルゴリズムを用いて検証値を生成する。例えば、検証値生成部７４は、予め定められたハッシュ関数を用いて、抽出した少なくとも１つの対象データにより定まるハッシュ値を、検証値として算出する。

【００３６】

本実施形態においては、検証値生成部７４は、予め定められたハッシュ関数を用いて、抽出した複数の対象データおよび順序設定部５６により設定された並び順によって定まるハッシュ値を、検証値として算出する。例えば、検証値生成部７４は、抽出した複数の対象データを、順序設定部５６が設定した順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えてハッシュ値を算出する。

【００３７】

ここで、検証値生成部７４が用いる演算アルゴリズムは、電子機器３０におけるレスポンス生成部６６が用いる演算アルゴリズムと同一である。レスポンス生成部６６においてハッシュ関数を用いる場合、検証値生成部７４は、同一のハッシュ関数および連結アルゴリズムを用いて検証値を生成する。

【００３８】

従って、電子機器３０におけるデータ読出部６４が読み出した少なくとも１つの対象データと、検証装置２０におけるデータ抽出部７２が読み出した少なくとも１つの対象データとが同一であれば、レスポンス値と検証値とは同一となる。つまり、レスポンス値と検証値とが同一であれば、データ記憶部３８における選択されたアドレスに記憶されている

対象データに異常はないと推定される。

【００３９】

検証装置２０における判定部７６は、レスポンス受信部７０が受信したレスポンス値と、検証値生成部７４が生成した検証値とを比較する。そして、判定部７６は、レスポンス値と検証値とが一致する場合、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常であると判定する。

【００４０】

また、判定部７６は、レスポンス値と検証値とが一致しない場合、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常ではないと判定する。すなわち、判定部７６は、レスポンス値と検証値とが一致しない場合、選択された少なくとも１つのアドレスに記憶されている対象データに、更新または攻撃等の何らかの原因により異常が生じていると判定する。

【００４１】

結果記憶部７８は、判定部７６による判定結果（正常または異常）を記憶する。結果記憶部７８は、検証対象となる電子機器３０毎に判定結果（正常または異常）を記憶してもよい。また、結果記憶部７８は、判定をしたアドレス（アドレス選択部５４により選択された少なくとも１つのアドレス）と対応付けて、判定結果を記憶してもよい。

【００４２】

図３は、第１実施形態に係る検証システム１０の処理の流れを示すフローチャートである。第１実施形態に係る検証システム１０では、検証装置２０および電子機器３０が図３に示す流れで検証を実行する。

【００４３】

まず、検証装置２０は、検証対象となる電子機器３０に対してネットワークを介してバージョンの確認要求を送信する（Ｓ１１）。

【００４４】

続いて、電子機器３０は、検証装置２０からネットワークを介してバージョンの確認要求を受信する（Ｓ１２）。続いて、電子機器３０は、バージョン記憶部４８に記憶されているバージョン情報を読み出す（Ｓ１３）。続いて、電子機器３０は、検証装置２０に対してネットワークを介してバージョン情報を送信する（Ｓ１４）。

【００４５】

続いて、検証装置２０は、電子機器３０からバージョン情報を受信し、バージョン情報を解析してバージョンを取得する（Ｓ１５）。続いて、検証装置２０は、バージョン毎に記憶している複数のメモリイメージのうち、取得したバージョンに対応するメモリイメージを特定する（Ｓ１６）。

【００４６】

続いて、検証装置２０は、任意の複数のアドレスを選択する（Ｓ１７）。例えば、検証装置２０は、ランダムに複数のアドレスを選択する。例えば、検証装置２０は、下記の式（１）に示すような３個のアドレスを選択する。

複数のアドレス＝（ａｄｄ＿１，ａｄｄ＿３，ａｄｄ＿８）…（１）

【００４７】

続いて、検証装置２０は、選択された複数のアドレスをランダムに並べ替える（Ｓ１８）。例えば、検証装置２０は、下記の式（２）に示すように３個のアドレスを並べ替える。

並べ替え後の複数のアドレス＝（ａｄｄ＿３，ａｄｄ＿８，ａｄｄ＿１）…（２）

【００４８】

続いて、検証装置２０は、選択された複数のアドレスを、ランダムに並べられた順序を識別可能に含むチャレンジ情報を生成する（Ｓ１９）。例えば、検証装置２０は、下記の式（３）に示すような、３個のアドレスを、並べた順序に従って先頭から格納した配列データをチャレンジ情報として生成する。

チャレンジ情報＝［ａｄｄ＿３，ａｄｄ＿８，ａｄｄ＿１］…（３）

【００４９】
続いて、検証装置２０は、生成したチャレンジ情報を電子機器３０にネットワークを介して送信する（Ｓ２０）。
【００５０】
続いて、電子機器３０は、検証装置２０からチャレンジ情報を受信する（Ｓ２１）。続いて、電子機器３０は、チャレンジ情報に含まれる複数のアドレスに記憶されている対象データを、データ記憶部３８から読み出す（Ｓ２２）。例えば、電子機器３０は、下記の式（４）に示すような、３個の対象データを読み出す。
複数の対象データ＝（ｄａｔａ＿１，ｄａｔａ＿３，ｄａｔａ＿８）…（４）
【００５１】
続いて、電子機器３０は、読み出した複数の対象データから、予め定められたハッシュ関数を用いてレスポンス値を生成する（Ｓ２３）。例えば、電子機器３０は、読み出した複数の対象データを、下記の式（５）に示すように、チャレンジ情報に含まれるアドレスの配置順に連結する。なお、式において、“｜｜”は、前後のデータを連結する関数を表す。
連結されたデータ＝（ｄａｔａ＿３｜｜ｄａｔａ＿８｜｜ｄａｔａ＿１）…（５）
【００５２】
そして、電子機器３０は、下記の式（６）に示すように、連結されたデータを予め定められたハッシュ関数に入力して、レスポンス値を算出する。なお、式において、ｈ（ｘ）は、ｘをハッシュ関数に入力して得られるハッシュ値を表す。
レスポンス値＝ｈ（ｄａｔａ＿３｜｜ｄａｔａ＿８｜｜ｄａｔａ＿１）…（６）
【００５３】
このような演算を実行することにより、電子機器３０は、レスポンス値を生成することができる。続いて、電子機器３０は、生成したレスポンス値を検証装置２０にネットワークを介して送信する（Ｓ２４）。
【００５４】
続いて、検証装置２０は、チャレンジ情報を送信したことに応じて返信されたレスポンス値を電子機器３０からネットワークを介して受信したか否かを判断する（Ｓ２５）。一定時間内にレスポンス値を受信できなかった場合（Ｓ２５のＮｏ）、検証装置２０は、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常でない（異常である）と判定する。そして、検証装置２０は、結果記憶部７８に異常の旨を登録し、本フローを終了する（Ｓ２６）。
【００５５】
一方、一定時間内にレスポンス値を受信できた場合には（Ｓ２５のＹｅｓ）、検証装置２０は、Ｓ１６で特定したメモリイメージから、Ｓ１７で選択した複数のアドレスに記憶されているべき対象データを抽出する（Ｓ２７）。例えば、検証装置２０は、下記の式（７）に示すような、３個の対象データを抽出する。
複数の対象データ＝（ｄａｔａ＿１′，ｄａｔａ＿３′，ｄａｔａ＿８′）…（７）
【００５６】
続いて、検証装置２０は、抽出した複数の対象データおよびＳ１８により設定されたアドレスの並び順に基づき、予め定められたハッシュ関数を用いて検証値を生成する（Ｓ２８）。具体的には、検証装置２０は、Ｓ２３において電子機器３０がレスポンス値を生成した演算と同一の演算により検証値を生成する。
【００５７】
例えば、検証装置２０は、抽出した複数の対象データを、下記の式（８）に示すように、Ｓ１８で並べ替えたアドレスの配置順に連結する。
連結されたデータ＝（ｄａｔａ＿３′｜｜ｄａｔａ＿８′｜｜ｄａｔａ＿１′）…（８）
【００５８】
続いて、検証装置２０は、下記の式（９）に示すように、連結されたデータを、Ｓ２３

のレスポンス値の生成で用いたハッシュ関数と同一のハッシュ関数に入力して、検証値を算出する。

検証値＝ｈ（ｄａｔａ＿３′｜｜ｄａｔａ＿８′｜｜ｄａｔａ＿１′）…（９）

【００５９】

続いて、検証装置２０は、レスポンス値と検証値とを比較する（Ｓ２９）。例えば、検証装置２０は、式（６）に示したレスポンス値と式（９）に示した検証値とが一致するか否かを判断する。

【００６０】

検証装置２０は、レスポンス値と検証値とが一致する場合（Ｓ２９のｔｒｕｅ）、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常であると判定する。そして、検証装置２０は、結果記憶部７８に正常の旨を登録し、本フローを終了する（Ｓ３０）。

【００６１】

検証装置２０は、レスポンス値と検証値とが一致しない場合（Ｓ２９のｆａｌｓｅ）、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常でないと判定する。そして、検証装置２０は、結果記憶部７８に異常の旨を登録し、本フローを終了する（Ｓ２６）。

【００６２】

以上のように、本実施形態に係る検証装置２０は、電子機器３０におけるデータ記憶部３８に記憶されている対象データが正常であるか否かを、ネットワークを介して遠隔から検証することができる。特に、検証装置２０が、検証を実行する毎に異なるアドレスを選択し、ランダムに並べ替えてチャレンジ情報を送信する。従って、検証装置２０は、検証を実行する毎に異なるチャレンジ情報を生成することができる。このため、攻撃者は、データ記憶部３８に記憶される対象データを改ざんする場合に、予めレスポンス値を準備することができない。従って、検証装置２０によれば、改ざんを高い確率で検知することができる。

【００６３】

（第２実施形態）

図４は、第２実施形態に係る検証装置２０および電子機器３０の構成を示す図である。

【００６４】

第２実施形態に係る検証システム１０は、第１実施形態に係る検証システム１０と略同一の機能および構成を有する。従って、第２実施形態を説明するにあたり、第１実施形態で説明したブロックと略同一の機能および構成を有するブロックについては、同一の符号を付けて相違点を除き説明を省略する。第３実施形態以降においても同様である。

【００６５】

第２実施形態に係る検証装置２０は、順序設定部５６に代えて、乱数発生部８２を有する。乱数発生部８２は、検証を実行する毎に異なる乱数を発生する。

【００６６】

検証装置２０におけるチャレンジ生成部５８は、選択された少なくとも１つのアドレスおよび乱数を含むチャレンジ情報を生成する。例えば、チャレンジ生成部５８は、選択された少なくとも１つのアドレスおよび乱数を含む配列データを、チャレンジ情報として生成する。

【００６７】

電子機器３０におけるレスポンス生成部６６は、データ読出部６４が読み出した少なくとも１つの対象データと、チャレンジ情報に含まれる乱数とから、予め定められた演算アルゴリズムを用いてレスポンス値を生成する。例えば、レスポンス生成部６６は、予め定められたハッシュ関数を用いて、読み出した少なくとも１つの対象データと乱数とにより定まるハッシュ値を、レスポンス値として算出する。例えば、レスポンス生成部６６は、読み出した少なくとも１つの対象データと乱数とを予め定められた順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えてハッシュ値を算出する

。
【００６８】
検証装置２０における検証値生成部７４は、データ抽出部７２が抽出した少なくとも１つの対象データと乱数発生部８２により発生された乱数とから、予め定められた演算アルゴリズムを用いて検証値を生成する。例えば、検証値生成部７４は、レスポンス生成部６６と同一の予め定められたハッシュ関数を用いて、抽出した少なくとも１つの対象データと乱数発生部８２により発生された乱数とにより定まるハッシュ値を、検証値として算出する。例えば、検証値生成部７４は、抽出した少なくとも１つの対象データと乱数発生部８２により発生された乱数とを予め定められた順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えてハッシュ値を算出する。
【００６９】
図５は、第２実施形態に係る検証システム１０の処理の流れを示すフローチャートである。第２実施形態に係る検証システム１０では、検証装置２０および電子機器３０が図５に示す流れで検証を実行する。
【００７０】
まず、検証装置２０および電子機器３０は、Ｓ１１からＳ１６までは、第１実施形態と同一の処理を実行する。
【００７１】
続いて、検証装置２０は、任意のアドレスを選択する（Ｓ４１）。例えば、アドレス選択部５４は、ランダムにアドレスを選択する。例えば、検証装置２０は、下記の式（１１）に示すような１個のアドレスを選択する。
アドレス＝ａｄｄ＿１…（１１）
【００７２】
続いて、検証装置２０は、乱数を発生する（Ｓ４２）。例えば、検証装置２０は、下記の式（１２）に示すような乱数を発生する。
乱数＝ＲＮＤ…（１２）
【００７３】
続いて、検証装置２０は、選択されたアドレスと乱数とを含むチャレンジ情報を生成する（Ｓ４３）。例えば、検証装置２０は、下記の式（１３）に示すような、アドレスと乱数とを格納した配列データをチャレンジ情報として生成する。
チャレンジ情報＝［ａｄｄ＿１，ＲＮＤ］…（１３）
【００７４】
続いて、検証装置２０は、生成したチャレンジ情報を電子機器３０にネットワークを介して送信する（Ｓ４４）。
【００７５】
続いて、電子機器３０は、検証装置２０からチャレンジ情報を受信する（Ｓ４５）。続いて、電子機器３０は、チャレンジ情報に含まれるアドレスに記憶されている対象データを、データ記憶部３８から読み出す（Ｓ４６）。例えば、電子機器３０は、下記の式（１４）に示すような、対象データを読み出す。
対象データ＝（ｄａｔａ＿１）…（１４）
【００７６】
続いて、電子機器３０は、読み出した対象データおよびチャレンジ情報に含まれる乱数から、予め定められたハッシュ関数を用いてレスポンス値を生成する（Ｓ４７）。例えば、電子機器３０は、読み出した対象データと乱数とを、下記の式（１５）に示すように予め定められた順序で連結する。
連結されたデータ＝（ｄａｔａ＿１｜｜ＲＮＤ）…（１５）
【００７７】
そして、電子機器３０は、下記の式（１６）に示すように、連結されたデータを予め定められたハッシュ関数に入力して、レスポンス値を算出する。
レスポンス値＝ｈ（ｄａｔａ＿１｜｜ＲＮＤ）…（１６）

【００７８】
続いて、電子機器３０は、生成したレスポンス値を検証装置２０にネットワークを介して送信する（Ｓ４８）。
【００７９】
続いて、検証装置２０は、チャレンジ情報を送信したことに応じて返信されたレスポンス値を電子機器３０からネットワークを介して受信したか否かを判断する（Ｓ４９）。一定時間内にレスポンス値を受信できなかった場合（Ｓ４９のＮｏ）、検証装置２０は、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常でない（異常である）と判定する。そして、検証装置２０は、結果記憶部７８に異常の旨を登録し、本フローを終了する（Ｓ５０）。
【００８０】
一方、一定時間内にレスポンス値を受信できた場合には（Ｓ４９のＹｅｓ）、検証装置２０は、Ｓ１６で特定したメモリイメージから、Ｓ４１で選択したアドレスに記憶されているべき対象データを抽出する（Ｓ５１）。例えば、検証装置２０は、下記の式（１７）に示すような対象データを抽出する。
対象データ＝（ｄａｔａ＿１′）…（１７）
【００８１】
続いて、検証装置２０は、抽出した対象データおよびＳ４２で発生した乱数から、予め定められたハッシュ関数を用いて検証値を生成する（Ｓ５２）。具体的には、検証装置２０は、Ｓ４７において電子機器３０がレスポンス値を生成した演算と同一の演算により検証値を生成する。
【００８２】
例えば、検証装置２０は、抽出した対象データおよび乱数を、下記の式（１８）に示すように、Ｓ４７のレスポンス値の生成で用いた順序で連結する。
連結されたデータ＝（ｄａｔａ＿１′｜｜ＲＮＤ）…（１８）
【００８３】
続いて、検証装置２０は、下記の式（１９）に示すように、連結されたデータを、Ｓ４７のレスポンス値の生成で用いたハッシュ関数と同一のハッシュ関数に入力して、検証値を算出する。
検証値＝ｈ（ｄａｔａ＿１′｜｜ＲＮＤ）…（１９）
【００８４】
続いて、検証装置２０は、レスポンス値と検証値とを比較する（Ｓ５３）。例えば、検証装置２０は、式（１６）に示したレスポンス値と式（１９）に示した検証値とが一致するか否かを判断する。
【００８５】
検証装置２０は、レスポンス値と検証値とが一致する場合（Ｓ５３のｔｒｕｅ）、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常であると判定する。そして、検証装置２０は、結果記憶部７８に正常の旨を登録し、本フローを終了する（Ｓ５４）。
【００８６】
検証装置２０は、レスポンス値と検証値とが一致しない場合（Ｓ５３のｆａｌｓｅ）、電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常でないと判定する。そして、検証装置２０は、結果記憶部７８に異常の旨を登録し、本フローを終了する（Ｓ５０）。
【００８７】
以上のように、本実施形態に係る検証装置２０は、電子機器３０におけるデータ記憶部３８に記憶されている対象データが正常であるか否かを、ネットワークを介して遠隔から検証することができる。特に、検証装置２０が、検証を実行する毎に異なるアドレスを選択し、さらに、検証を実行する毎に異なる乱数を発生してチャレンジ情報を送信する。従って、検証装置２０は、検証を実行する毎に異なるチャレンジ情報を生成することができ

る。このため、攻撃者は、データ記憶部３８に記憶される対象データを改ざんする場合に、予めレスポンス値を準備することができない。従って、検証装置２０によれば、改ざんを高い確率で検知することができる。

【００８８】

なお、本実施形態においては、アドレス選択部５４は、１個のアドレスを選択する構成であるが、第１実施形態と同様に複数のアドレスを選択してもよい。また、第１実施形態に係る検証装置２０および電子機器３０の構成に、第２実施形態の構成を追加してもよい。この場合、チャレンジ生成部５８は、複数のアドレスをランダムに並べ替えるとともに、乱数をチャレンジ情報に含める。このようにしても、検証装置２０は、改ざんを高い確率で検知することができる。

【００８９】

（第３実施形態）

図６は、第３実施形態に係る検証システム１０を示す図である。本実施形態に係る検証システム１０は、検証装置２０と、複数の電子機器３０とを備える。

【００９０】

本実施形態に係る検証装置２０は、複数の電子機器３０に対して一括して検証を実行する。複数の電子機器３０のそれぞれには、固有の識別情報が割り当てられている。本実施形態に係る検証装置２０は、複数の電子機器３０を効率良く検証することができる。

【００９１】

図７は、第３実施形態に係る検証装置２０および電子機器３０の構成を示す図である。

【００９２】

第３実施形態に係る検証装置２０は、グループ管理部８４をさらに有する。また、第３実施形態に係る検証装置２０は、第１実施形態と比較して、バージョン確認部４４、バージョン取得部５２および順序設定部５６を有さない。

【００９３】

第３実施形態に係る電子機器３０は、識別情報記憶部８８をさらに有する。また、第３実施形態に係る電子機器３０は、確認要求受信部４６、バージョン記憶部４８およびバージョン送信部５０を有さない。

【００９４】

検証装置２０におけるグループ管理部８４は、同一のメモリイメージを記憶する複数の電子機器３０のグループを管理する。具体的には、グループ管理部８４は、グループ毎に、そのグループに属する電子機器３０が記憶している対象データのバージョン、そのグループに属する複数の電子機器３０のそれぞれの識別情報、および、そのグループに属する複数の電子機器３０のそれぞれのネットワーク上のアドレスを記憶する。グループ管理部８４は、検証対象のグループに属する電子機器３０が記憶している対象データのバージョンを特定し、アドレス選択部５４およびデータ抽出部７２に与える。

【００９５】

検証装置２０におけるチャレンジ生成部５８は、選択された少なくとも１つのアドレスを含むチャレンジ情報を生成する。検証装置２０におけるチャレンジ送信部６０は、検証対象のグループに属する複数の電子機器３０のそれぞれのネットワーク上のアドレスを取得する。そして、チャレンジ送信部６０は、複数の電子機器３０のそれぞれにチャレンジ情報を一斉送信する。例えば、チャレンジ送信部６０は、チャレンジ情報をマルチキャスト送信またはブロードキャスト送信をする。

【００９６】

電子機器３０における識別情報記憶部８８は、自身に割り当てられた識別情報を記憶する。電子機器３０におけるレスポンス生成部６６は、識別情報記憶部８８から識別情報を取得する。

【００９７】

レスポンス生成部６６は、データ読出部６４が読み出した少なくとも１つの対象データと識別情報とから、予め定められた演算アルゴリズムを用いてレスポンス値を生成する。

例えば、レスポンス生成部６６は、予め定められたハッシュ関数を用いて、読み出した少なくとも１つの対象データと識別情報とにより定まるハッシュ値を、レスポンス値として算出する。例えば、レスポンス生成部６６は、読み出した少なくとも１つの対象データと識別情報とを予め定められた順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えてレスポンス値を生成する。

【００９８】

電子機器３０におけるレスポンス送信部６８は、レスポンス生成部６６が生成したレスポンス値と、識別情報記憶部８８に記憶された識別情報との組を、検証装置２０にネットワークを介して送信する。

【００９９】

検証装置２０におけるレスポンス受信部７０は、レスポンス値と識別情報との組を、検証対象のグループに属する複数の電子機器３０のそれぞれからネットワークを介して受信する。

【０１００】

検証装置２０における検証値生成部７４は、レスポンス値と識別情報との組を受信する毎に、検証値を生成する。検証値生成部７４は、データ抽出部７２が抽出した少なくとも１つの対象データと、電子機器３０から受信した識別情報とから、予め定められた演算アルゴリズムを用いて検証値を生成する。

【０１０１】

例えば、検証値生成部７４は、レスポンス生成部６６と同一の予め定められたハッシュ関数を用いて、抽出した少なくとも１つの対象データと受信した識別情報とにより定まるハッシュ値を、検証値として算出する。例えば、検証値生成部７４は、抽出した少なくとも１つの対象データと受信した識別情報とを、予め定められた順序に従って連結して１つのデータを生成し、連結されたデータをハッシュ関数に与えて検証値を算出する。

【０１０２】

検証装置２０における判定部７６は、レスポンス値と識別情報との組を受信する毎に、レスポンス受信部７０が受信したレスポンス値と、検証値生成部７４が生成した検証値とを比較する。そして、判定部７６は、レスポンス値と検証値とが一致する場合、受信した識別情報に対応する電子機器３０について、データ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常であると判定する。

【０１０３】

また、判定部７６は、レスポンス値と検証値とが一致しない場合、受信した識別情報に対応する電子機器３０について、データ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常ではないと判定する。また、判定部７６は、識別情報が同一である複数のレスポンス値を受信した場合、受信した識別情報に対応する電子機器３０のデータ記憶部３８に記憶されている対象データが正常ではないと判定する。

【０１０４】

結果記憶部７８は、複数の電子機器３０毎に判定結果（正常または異常）を記憶する。

【０１０５】

図８は、第３実施形態に係る検証システム１０の処理の流れを示すフローチャートである。第３実施形態に係る検証システム１０では、検証装置２０および電子機器３０が図８に示す流れで検証を実行する。

【０１０６】

まず、検証装置２０は、検証対象のグループを特定する（Ｓ６１）。続いて、検証装置２０は、グループに属する電子機器３０が有するデータ記憶部３８が記憶している対象データのバージョンから、対応するメモリイメージを特定する（Ｓ６２）。

【０１０７】

続いて、検証装置２０は、任意のアドレスを選択する（Ｓ６３）。例えば、アドレス選択部５４は、検証をする毎にランダムにアドレスを選択する。例えば、検証装置２０は、下記の式（２１）に示すような１個のアドレスを選択する。

アドレス＝（ａｄｄ＿１）…（２１）

【０１０８】

続いて、検証装置２０は、選択されたアドレスを含むチャレンジ情報を生成する（Ｓ６４）。例えば、検証装置２０は、下記の式（２２）に示すような、１個のアドレスを含む対象データをチャレンジ情報として生成する。

チャレンジ情報＝［ａｄｄ＿１］…（２２）

【０１０９】

続いて、検証装置２０は、生成したチャレンジ情報を、検証対象のグループに属する複数の電子機器３０のそれぞれに、ネットワークを介して一斉送信する（Ｓ６５）。例えば、検証装置２０は、チャレンジ情報をマルチキャスト送信またはブロードキャスト送信をする。

【０１１０】

続いて、それぞれの電子機器３０は、検証装置２０からチャレンジ情報を受信する（Ｓ６６）。続いて、それぞれの電子機器３０は、チャレンジ情報に含まれるアドレスに記憶されている対象データを、データ記憶部３８から読み出す（Ｓ６７）。例えば、それぞれの電子機器３０は、下記の式（２３）に示すような、対象データを読み出す。

対象データ＝（ｄａｔａ＿１）…（２３）

【０１１１】

続いて、それぞれの電子機器３０は、自身に割り当てられている識別情報を取得する（Ｓ６８）。識別情報は、電子機器３０毎に異なる値である。例えば、それぞれの電子機器３０は、下記の式（２４）に示すような識別情報を取得する。

識別情報＝（ｉｄ＿ｉ）…（２４）

【０１１２】

続いて、それぞれの電子機器３０は、読み出した対象データおよび識別情報から、予め定められたハッシュ関数を用いてレスポンス値を生成する（Ｓ６９）。例えば、それぞれの電子機器３０は、読み出した対象データと識別情報とを、下記の式（２５）に示すように、予め定められた順序で連結する。

連結されたデータ＝（ｄａｔａ＿１｜｜ｉｄ＿ｉ）…（２５）

【０１１３】

そして、それぞれの電子機器３０は、下記の式（２６）に示すように、連結されたデータを予め定められたハッシュ関数に入力して、レスポンス値を算出する。

レスポンス値＝ｈ（ｄａｔａ＿１｜｜ｉｄ＿ｉ）…（２６）

【０１１４】

続いて、それぞれの電子機器３０は、生成したレスポンス値と、取得した識別情報との組を検証装置２０にネットワークを介して送信する（Ｓ７０）。例えば、それぞれの電子機器３０は、下記の式（２７）に示すような情報を検証装置２０に送信する。

送信情報＝（ｈ（ｄａｔａ＿１｜｜ｉｄ＿ｉ），ｉｄ＿ｉ）…（２７）

【０１１５】

続いて、検証装置２０は、何れかの電子機器３０から、レスポンス値と識別情報との組を受信したか否かを判断する（Ｓ７１）。検証装置２０は、レスポンス値と識別情報との組が受信できない場合（Ｓ７１のＮｏ）、処理をＳ７１で待機し、レスポンス値と識別情報との組が受信できた場合（Ｓ７１のＹｅｓ）、処理をＳ７２に進める。すなわち、検証装置２０は、レスポンス値と識別情報との組を受信する毎に、Ｓ７２以降の処理を実行する。

【０１１６】

レスポンス値と識別情報との組を受信した場合、検証装置２０は、受信した情報の中から識別情報を抽出する（Ｓ７２）。続いて、検証装置２０は、抽出した識別情報を既に受信しているか否かを判断する（Ｓ７３）。すなわち、検証装置２０は、識別情報が同一である複数のレスポンス値を受信したか否かを判断する。同一の識別情報を既に受信している場合（Ｓ７３のＹｅｓ）、悪意の第三者が何れかの電子機器３０から送信された情報を

コピーした可能性があるので、検証装置２０は、受信した識別情報に対応する電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが異常である旨を結果記憶部７８に登録する（Ｓ７４）。

【０１１７】

同一の識別情報を未だ受信していない場合（Ｓ７３のＮｏ）、検証装置２０は、Ｓ６２で特定したメモリイメージから、Ｓ６３で選択したアドレスに記憶されているべき対象データを抽出する（Ｓ７５）。例えば、検証装置２０は、下記の式（２８）に示すような対象データを抽出する。

対象データ＝（ｄａｔａ＿１′）…（２８）

【０１１８】

続いて、検証装置２０は、抽出した対象データおよびＳ７２で抽出した識別情報から、予め定められたハッシュ関数を用いて検証値を算出する（Ｓ７６）。ここでは、検証装置２０は、Ｓ６９において電子機器３０がレスポンス値を生成した演算と同一の演算により検証値を生成する。

【０１１９】

例えば、検証装置２０は、抽出した対象データおよび識別情報を、下記の式（２９）に示すように、Ｓ６９のレスポンス値の生成で用いた順序と同一の順序で連結する。

連結されたデータ＝（ｄａｔａ＿１′｜｜ｉｄ＿ｉ）…（２９）

【０１２０】

続いて、検証装置２０は、下記の式（３０）に示すように、連結されたデータを、Ｓ６９のレスポンス値の生成で用いたハッシュ関数と同一のハッシュ関数に入力して、検証値を算出する。

検証値＝ｈ（ｄａｔａ＿１′｜｜ｉｄ＿ｉ）…（３０）

【０１２１】

続いて、検証装置２０は、レスポンス値と検証値とを比較する（Ｓ７７）。例えば、検証装置２０は、式（２６）に示したレスポンス値と式（３０）に示した検証値とが一致するか否かを判断する。

【０１２２】

検証装置２０は、レスポンス値と検証値とが一致する場合（Ｓ７７のｔｒｕｅ）、受信した識別情報に対応する電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが正常である旨を結果記憶部７８に登録する（Ｓ７８）。検証装置２０は、レスポンス値と検証値とが一致しない場合（Ｓ７７のｆａｌｓｅ）、受信した識別情報に対応する電子機器３０におけるデータ記憶部３８の選択された少なくとも１つのアドレスに記憶されている対象データが異常である旨を結果記憶部７８に登録する（Ｓ７４）。

【０１２３】

Ｓ７４またはＳ７８の処理に続いて、検証装置２０は、グループに属する複数の電子機器３０の全てについて、レスポンス値と識別情報との組を受信したか否かを判断する（Ｓ７９）。全ての電子機器３０について、レスポンス値と識別情報との組を受信した場合には（Ｓ７９のＹｅｓ）、検証装置２０は、本フローを終了する。

【０１２４】

全ての電子機器３０について、レスポンス値と識別情報との組を受信していない場合には（Ｓ７９のＮｏ）、検証装置２０は、処理をＳ７１に戻し、処理を繰り返す。なお、Ｓ７１において、一定時間を経過してもレスポンス値と識別情報との組を受信できない場合（Ｓ７１のＮｏ）、検証装置２０は、強制的に本フローを終了してもよい。この場合、検証装置２０は、レスポンス値と識別情報との組を受信できない電子機器３０について、結果記憶部７８に異常の旨を登録してから本フローを終了してもよい。

【０１２５】

以上のように、本実施形態に係る検証装置２０は、複数の電子機器３０のそれぞれにおけるデータ記憶部３８に記憶されている対象データが正常であるか否かを、一括して、ネ

ットワークを介して遠隔から検証することができる。これにより、検証装置２０は、多数の電子機器３０を効率良く検証することができる。

【０１２６】

なお、本実施形態においては、アドレス選択部５４は、１個のアドレスを選択する構成であるが、第１実施形態と同様に複数のアドレスを選択してもよい。さらに、本実施形態に係る検証装置２０は、第１実施形態に示す順序設定部５６を備え、複数のアドレスをランダムに並べ替えたチャレンジ情報を生成してもよい。また、本実施形態に係る検証装置２０は、第２実施形態に示す乱数発生部８２をさらに有し、アドレスと乱数とを含むチャレンジ情報を生成してもよい。

【０１２７】

（第４実施形態）

図９は、第４実施形態に係る検証装置２０および電子機器３０の構成を示す図である。

【０１２８】

第４実施形態に係る検証装置２０は、第１実施形態に示す構成に加えて、繰返制御部９２をさらに有する。繰返制御部９２は、データ記憶部３８に記憶されている選択されたアドレスの対象データが正常であると判定した場合、アドレス選択部５４にさらに他の少なくとも１つのアドレスを選択させる。そして、繰返制御部９２は、順序設定部５６、チャレンジ生成部５８、チャレンジ送信部６０、レスポンス受信部７０、データ抽出部７２、検証値生成部７４および判定部７６に、新たに選択された少なくとも１つのアドレスに基づき処理を再度実行させる。

【０１２９】

これにより、本実施形態に係る検証装置２０は、データ記憶部３８における未検証の他のアドレスに記憶されている対象データをさらに検証することができる。また、本実施形態に係る検証装置２０は、データ記憶部３８に記憶されている対象データが正常でないと判定された場合には、繰り返して検証をさせないので、早期に検証処理を終了させることができる。

【０１３０】

なお、第２実施形態または第３実施形態に示す検証装置２０が、繰返制御部９２をさらに有してもよい。これにより、第２実施形態または第３実施形態に示す検証装置２０も第４実施形態と同様の効果を得ることができる。

【０１３１】

図１０は、実施形態に係る情報処理装置３００のハードウェア構成の一例を示す図である。上述した検証装置２０および電子機器３０は、例えば図１０に示すような情報処理装置３００により実現することができる。

【０１３２】

情報処理装置３００は、通常のコンピュータと同様の構成をしている。すなわち、情報処理装置３００は、ＣＰＵ３０２と、ＲＯＭ３０４と、ＲＡＭ３０６と、記憶装置３０８と、通信装置３１０とを有する。ＣＰＵ３０２、ＲＯＭ３０４、ＲＡＭ３０６、記憶装置３０８および通信装置３１０は、バスにより接続されている。

【０１３３】

ＣＰＵ３０２は、記憶装置３０８に記憶されたプログラムをＲＡＭ３０６に展開して実行し、各部を制御して入出力を行ったり、データの加工を行ったりする。ＲＯＭ３０４には、ＯＳの起動用プログラムを記憶装置３０８からＲＡＭ３０６に読み出すスタートプログラムが記憶されている。ＲＡＭ３０６は、ＣＰＵ３０２の作業領域としてデータを記憶する。

【０１３４】

記憶装置３０８は、例えば、ハードディスクドライブまたはフラッシュメモリ等である。記憶装置３０８は、オペレーティングシステム、アプリケーションプログラムおよびデータを記憶している。これらのプログラムは、インストール可能な形式または実行可能な形式のファイルで、コンピュータで読み取り可能な記録メディアに記録して配布される。

また、プログラムは、サーバからダウンロードすることにより配布されてもよい。通信装置３１０は、ネットワークに接続するためのインターフェイス装置である。

【０１３５】

本実施形態の情報処理装置３００で実行されるプログラムは、インストール可能な形式または実行可能な形式のファイルでＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録されて提供される。また、本実施形態の情報処理装置３００で実行されるプログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、本実施形態の情報処理装置３００で実行されるプログラムをインターネット等のネットワーク経由で提供または配布するように構成してもよい。また、本実施形態のプログラムを、ＲＯＭ３０４等に予め組み込んで提供するように構成してもよい。

【０１３６】

情報処理装置３００を検証装置２０として機能させるためのプログラムは、バージョン確認モジュールと、バージョン取得モジュールと、アドレス選択モジュールと、順序設定モジュールと、チャレンジ生成モジュールと、チャレンジ送信モジュールと、レスポンス受信モジュールと、データ抽出モジュールと、検証値生成モジュールと、判定モジュールとを有する。情報処理装置３００は、プロセッサ（ＣＰＵ３０２）が記憶媒体（記憶装置３０８等）からプログラムを読み出して実行することにより各モジュールが主記憶装置（ＲＡＭ３０６）上にロードされ、プロセッサ（ＣＰＵ３０２）が、バージョン確認部４４、バージョン取得部５２、アドレス選択部５４、順序設定部５６、チャレンジ生成部５８、チャレンジ送信部６０、レスポンス受信部７０、データ抽出部７２、検証値生成部７４および判定部７６として機能する。また、ＲＡＭ３０６または記憶装置３０８は、イメージ記憶部４２および結果記憶部７８として機能する。なお、バージョン確認部４４、バージョン取得部５２、アドレス選択部５４、順序設定部５６、チャレンジ生成部５８、チャレンジ送信部６０、レスポンス受信部７０、データ抽出部７２、検証値生成部７４および判定部７６は、一部または全部がプロセッサ以外のハードウェアにより実現されてもよい。

【０１３７】

また、情報処理装置３００を電子機器３０として機能させるためのプログラムは、処理実行モジュールと、確認要求受信モジュールと、バージョン記憶モジュールと、バージョン送信モジュールと、チャレンジ受信モジュールと、データ読出モジュールと、レスポンス生成モジュールと、レスポンス送信モジュールとを有する。情報処理装置３００は、プロセッサ（ＣＰＵ３０２）が記憶媒体（記憶装置３０８等）からプログラムを読み出して実行することにより各モジュールが主記憶装置（ＲＡＭ３０６）上にロードされ、プロセッサ（ＣＰＵ３０２）が、処理実行部４０、確認要求受信部４６、バージョン送信部５０、チャレンジ受信部６２、データ読出部６４、レスポンス生成部６６およびレスポンス送信部６８として機能する。また、ＲＡＭ３０６または記憶装置３０８は、データ記憶部３８およびバージョン記憶部４８として機能する。なお、処理実行部４０、確認要求受信部４６、バージョン送信部５０、チャレンジ受信部６２、データ読出部６４、レスポンス生成部６６およびレスポンス送信部６８は、一部または全部がプロセッサ以外のハードウェアにより実現されてもよい。

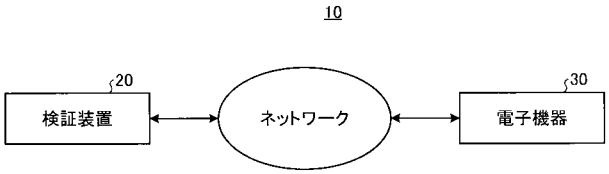
【０１３８】

本発明のいくつかの実施形態および変形例を説明したが、これらの実施形態および変形例は、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の範囲に含まれる。

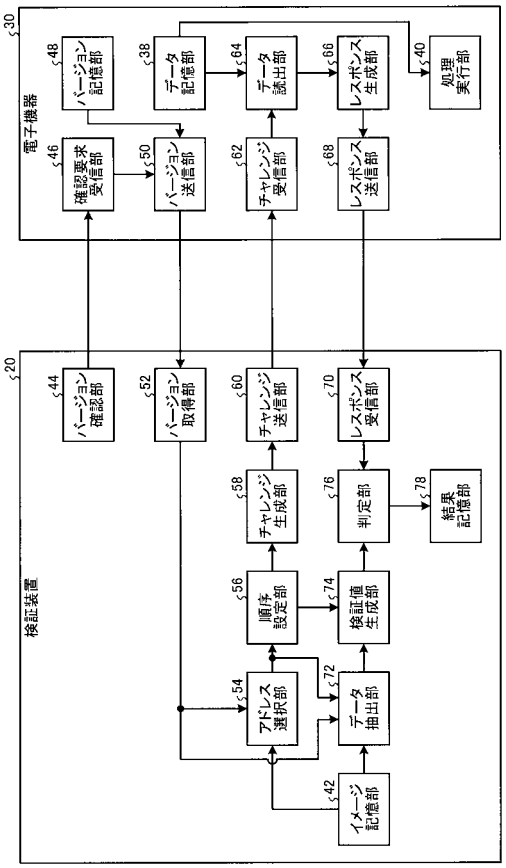
【符号の説明】

【０１３９】
１０　検証システム
２０　検証装置
３０　電子機器
３８　データ記憶部
４０　処理実行部
４２　イメージ記憶部
４４　バージョン確認部
４６　確認要求受信部
４８　バージョン記憶部
５０　バージョン送信部
５２　バージョン取得部
５４　アドレス選択部
５６　順序設定部
５８　チャレンジ生成部
６０　チャレンジ送信部
６２　チャレンジ受信部
６４　データ読出部
６６　レスポンス生成部
６８　レスポンス送信部
７０　レスポンス受信部
７２　データ抽出部
７４　検証値生成部
７６　判定部
７８　結果記憶部
８２　乱数発生部
８４　グループ管理部
８８　識別情報記憶部

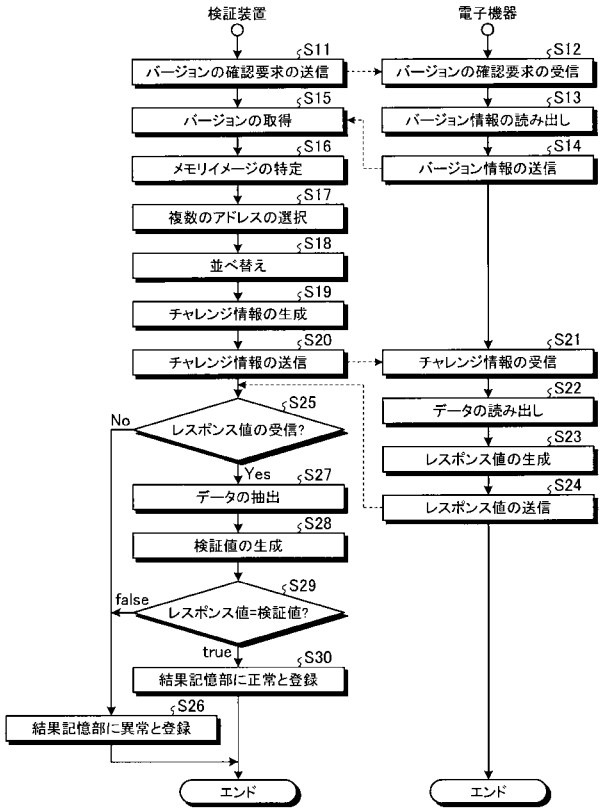
【図１】


10
20
検証装置
ネットワーク
30
電子機器

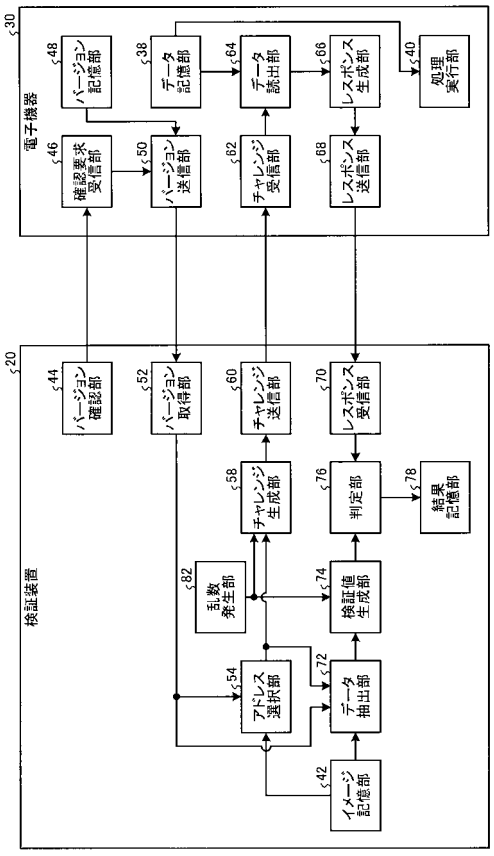
【図２】


30
電子機器
48 バージョン記憶部
38 データ記憶部
64 データ読出部
66 レスポンス生成部
40 処理実行部
46 確認要求受信部
50 バージョン送信部
62 チャレンジ受信部
68 レスポンス送信部
20
検証装置
44 バージョン確認部
52 バージョン取得部
60 チャレンジ送信部
70 レスポンス受信部
58 チャレンジ生成部
76 判定部
78 結果記憶部
56 順序設定部
74 検証値生成部
54 アドレス選択部
72 データ抽出部
42 イメージ記憶部

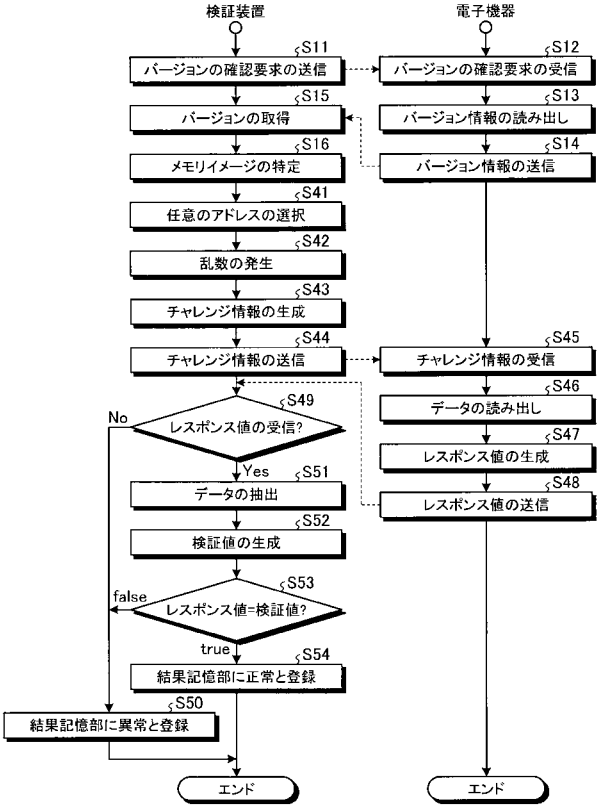
【図３】


検証装置
電子機器
S11 バージョンの確認要求の送信
S12 バージョンの確認要求の受信
S15 バージョンの取得
S13 バージョン情報の読み出し
S16 メモリイメージの特定
S14 バージョン情報の送信
S17 複数のアドレスの選択
S18 並べ替え
S19 チャレンジ情報の生成
S20 チャレンジ情報の送信
S21 チャレンジ情報の受信
S22 データの読み出し
S25 レスポンス値の受信?
No
Yes
S23 レスポンス値の生成
S27 データの抽出
S24 レスポンス値の送信
S28 検証値の生成
S29 レスポンス値=検証値?
false
true
S30 結果記憶部に正常と登録
S26 結果記憶部に異常と登録
エンド
エンド

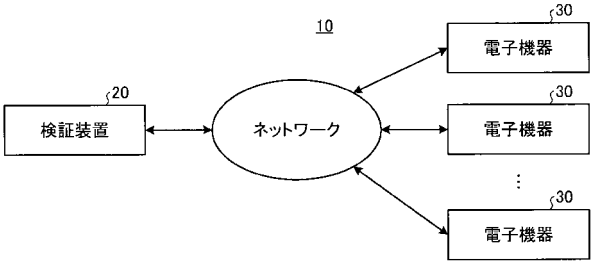
【図４】


30
電子機器
48 バージョン記憶部
38 データ記憶部
64 データ読出部
66 レスポンス生成部
40 処理実行部
46 確認要求受信部
50 バージョン送信部
62 チャレンジ受信部
68 レスポンス送信部
20
検証装置
44 バージョン確認部
52 バージョン取得部
60 チャレンジ送信部
70 レスポンス受信部
58 チャレンジ生成部
76 判定部
78 結果記憶部
82 乱数発生部
74 検証値生成部
54 アドレス選択部
72 データ抽出部
42 イメージ記憶部

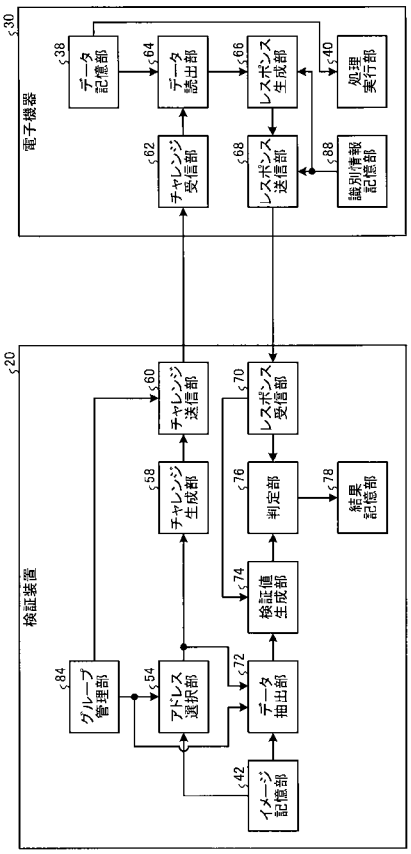
【図５】


検証装置
電子機器
S11
バージョンの確認要求の送信
S12
バージョンの確認要求の受信
S15
バージョンの取得
S13
バージョン情報の読み出し
S16
メモリイメージの特定
S14
バージョン情報の送信
S41
任意のアドレスの選択
S42
乱数の発生
S43
チャレンジ情報の生成
S44
チャレンジ情報の送信
S45
チャレンジ情報の受信
S46
データの読み出し
S47
レスポンス値の生成
S48
レスポンス値の送信
S49
レスポンス値の受信?
No
Yes
S51
データの抽出
S52
検証値の生成
S53
レスポンス値=検証値?
false
true
S54
結果記憶部に正常と登録
S50
結果記憶部に異常と登録
エンド
エンド

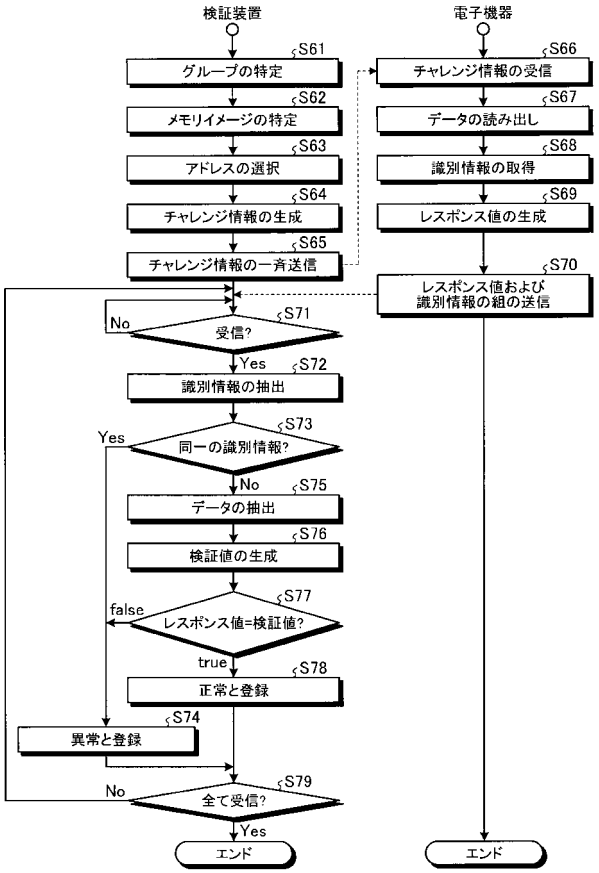
【図６】


10
20
検証装置
ネットワーク
30
電子機器
30
電子機器
30
電子機器

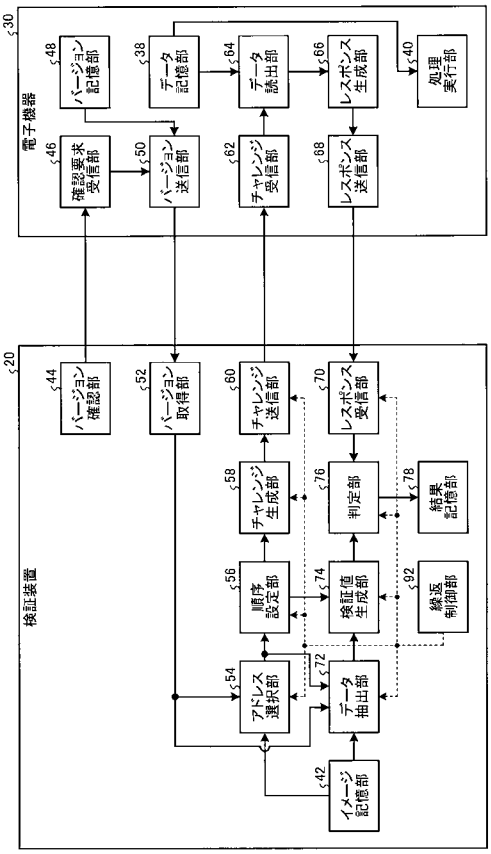
【図７】


30
電子機器
38
データ記憶部
64
データ読出部
66
レスポンス生成部
40
処理実行部
62
チャレンジ受信部
68
レスポンス送信部
88
識別情報記憶部
20
検証装置
60
チャレンジ送信部
70
レスポンス受信部
58
チャレンジ生成部
76
判定部
78
結果記憶部
74
検証値生成部
84
グループ管理部
54
アドレス選択部
72
データ抽出部
42
イメージ記憶部

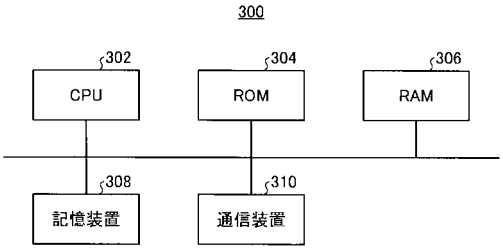
【図８】


検証装置
電子機器
S61
グループの特定
S66
チャレンジ情報の受信
S62
メモリイメージの特定
S67
データの読み出し
S63
アドレスの選択
S68
識別情報の取得
S64
チャレンジ情報の生成
S69
レスポンス値の生成
S65
チャレンジ情報の一斉送信
S70
レスポンス値および識別情報の組の送信
No
S71
受信?
Yes
S72
識別情報の抽出
Yes
S73
同一の識別情報?
No
S75
データの抽出
S76
検証値の生成
false
S77
レスポンス値=検証値?
true
S78
正常と登録
S74
異常と登録
No
S79
全て受信?
Yes
エンド
エンド

【図９】


30
電子機器
48
バージョン記憶部
38
データ記憶部
64
データ読出部
66
レスポンス生成部
40
処理実行部
46
確認要求受信部
50
バージョン送信部
62
チャレンジ受信部
68
レスポンス送信部
20
検証装置
44
バージョン確認部
52
バージョン取得部
60
チャレンジ送信部
70
レスポンス受信部
58
チャレンジ生成部
76
判定部
78
結果記憶部
56
順序設定部
74
検証値生成部
92
繰返制御部
54
アドレス選択部
72
データ抽出部
42
イメージ記憶部

【図１０】


300
302
CPU
304
ROM
306
RAM
308
記憶装置
310
通信装置

フロントページの続き

(72)発明者　中西　福友
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　青木　慧
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　高橋　俊成
東京都港区芝浦一丁目１番１号　株式会社東芝内
Ｆターム(参考) 5J104 AA07　AA16　AA32　DA03　EA08　JA01　LA01