

明 細 書

発明の名称： 情報処理装置、及び情報処理システム

技術分野

[0001] 本発明の実施形態は、情報処理装置、及び情報処理システムに関する。

背景技術

[0002] 近年、ＩｏＴ（Internet of Things）の普及により様々な装置（例えば、ＩｏＴ機器）がインターネットに接続されるようになり、セキュリティの確保が重要になってきている。従来の情報処理システムでは、ＩｏＴ機器とネットワークとの間に情報処理装置を挿入して、情報処理装置がネットワーク上の通信経路の機密性を担保することで、様々な装置に対してセキュリティを付加する技術が知られている。しかしながら、このような従来の情報処理システムでは、例えば、情報処理装置が故障した場合に、システムの運用が継続できずに可用性が低下する場合があった。

先行技術文献

特許文献

[0003] 特許文献1：特開２００９－１１７８８７号公報

発明の概要

発明が解決しようとする課題

[0004] 本発明が解決しようとする課題は、セキュリティを確保しつつ、可用性を向上させることができる情報処理装置、及び情報処理システムを提供することである。

課題を解決するための手段

[0005] 実施形態の情報処理装置は、第１通信部と、第２通信部と、情報処理部と、切替部とを持つ。第１通信部は、ネットワークに接続される末端の装置である末端装置に接続し、前記末端装置との間で通信可能である。第２通信部は、ネットワークに接続し、前記ネットワークを介して前記ネットワークに接続された装置と通信可能である。情報処理部は、少なくとも前記第１通信

部が前記末端装置から情報を受信した場合に、受信した情報を暗号化して前記第2通信部を介して前記ネットワークに送信し、少なくとも前記第2通信部が前記ネットワークから暗号化された情報を受信した場合に、受信した情報を復号して前記第1通信部を介して前記末端装置に送信する。切替部は、前記情報処理部が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、前記第1通信部の前記末端装置との通信線と、前記第2通信部の前記ネットワークとの通信線とを直接接続し、前記末端装置と前記ネットワークとの間で、前記情報処理部を介さずに直接通信するパススルーモードに切り替える。

図面の簡単な説明

- [0006] [図1]第1の実施形態の情報処理システムの一例を示すブロック図。
[図2]第1の実施形態の情報処理装置の一例を示すブロック図。
[図3]第1の実施形態の通信リスク記憶部のデータ例を示す図。
[図4]第1の実施形態の通信情報記憶部のデータ例を示す図。
[図5]第1の実施形態の通信実績記憶部のデータ例を示す図。
[図6]第1の実施形態の許容期間記憶部のデータ例を示す図。
[図7]第1の実施形態のパススルー許容期間の決定例を示す図。
[図8]第1の実施形態の情報処理システムの機密通信動作の一例を示す図。
[図9]第1の実施形態の情報処理装置の縮退機能の動作の一例を示す図。
[図10]第1の実施形態の情報処理装置の動作の一例を示すフローチャート。
[図11]第2の実施形態の情報処理システムの一例を示すブロック図。
[図12]第2の実施形態の情報処理装置の一例を示すブロック図。
[図13]第2の実施形態の通信リスク記憶部のデータ例を示す図。
[図14]第2の実施形態の許容期間記憶部のデータ例を示す図。
[図15]第3の実施形態の情報処理システムの一例を示すブロック図。
[図16]第3の実施形態の情報処理装置の一例を示すブロック図。
[図17]第3の実施形態のICカード40のハードウェア構成例を示す図。
[図18]第3の実施形態のICカード40の機能構成例を示すブロック図。

[図19]第3の実施形態の情報処理システムの機密通信動作の一例を示す図。

発明を実施するための形態

[0007] 以下、実施形態の情報処理装置、及び情報処理システムを、図面を参照して説明する。

[0008] (第1の実施形態)

図1は、第1の実施形態の情報処理システム1の一例を示すブロック図である。

図1に示すように、情報処理システム1は、情報処理装置(10-1、10-2、10-3、...)と、IoT機器(21-1、21-2、...)と、上位装置22とを備える。

[0009] 本実施形態において、情報処理装置10-1と、情報処理装置10-2と、情報処理装置10-3とのそれぞれは、同一の構成であり、単に情報処理システム1が備える情報処理装置を示す場合、又は、区別しない場合には、情報処理装置10として説明する。

また、IoT機器21-1と、IoT機器21-2と、上位装置22とのそれぞれは、ネットワークNW1に接続される末端の装置であるエンドポイントであり、末端装置20の一例である。

[0010] ネットワークNW1は、例えば、インターネット通信網や、LAN(Local Area Network)などの情報通信網である。情報処理装置(10-1、10-2、10-3、...)は、ネットワークNW1に接続されており、ネットワークNW1を介して相互に通信可能である。

[0011] IoT機器21-1、IoT機器21-2、...は、例えば、パーソナルコンピュータ(PC)等のコンピュータ装置、電化製品、監視カメラ、自動車、工作機械、医療機器などのネットワークNW1に接続可能な各種機器である。IoT機器21-1は、情報処理装置10-1を介してネットワークNW1に接続され、IoT機器21-2は、情報処理装置10-2を介してネットワークNW1に接続される。

上位装置22は、例えば、サーバ装置やPCなどのコンピュータ装置であ

り、情報処理装置 10-2 を介してネットワーク NW1 に接続されている。

[0012] 情報処理装置 10 は、末端装置 20 とネットワーク NW1 との間に接続される通信制御装置である。情報処理装置 10 は、末端装置 20 とネットワーク NW1 との間の通信において、セキュリティを付加してデータ通信を中継する。情報処理装置 10 は、例えば、末端装置 20 から受信したデータを暗号化し、暗号化したデータをネットワーク NW1 に送信する。また、情報処理装置 10 は、例えば、ネットワーク NW1 から受信したデータを復号し、復号したデータを末端装置 20 に送信する。

[0013] なお、図 1 に示すように、情報処理装置 10-1 は、IoT 機器 21-1 とネットワーク NW1 との間に接続され、情報処理装置 10-3 は、IoT 機器 21-2 とネットワーク NW1 との間に接続されている。また、情報処理装置 10-2 は、上位装置 22 とネットワーク NW1 との間に接続されている。

[0014] 次に、図 2 を参照して、本実施形態の情報処理装置 10 の構成について説明する。

図 2 は、本実施形態の情報処理装置 10 の一例を示すブロック図である。

図 2 に示すように、情報処理装置 10 は、通信 I/F (Interface) 部 11 と、通信 I/F 部 12 と、フォトリレースイッチ 13 と、記憶部 14 と、情報処理部 15 とを備える。

[0015] 通信 I/F 部 11 (第 1 通信部の一例) は、末端装置 20 に接続し、末端装置 20 との間で通信可能なインタフェースである。また、通信 I/F 部 12 (第 2 通信部の一例) は、ネットワーク NW1 を介して同ネットワーク NW1 に接続されたサーバや他の装置と通信可能なインタフェースである。

[0016] フォトリレースイッチ 13 (切替部の一例) は、例えば、ノーマリクローズのスイッチであり、通信 I/F 部 11 の末端装置 20 との通信線と、通信 I/F 部 12 のネットワーク NW1 との通信線との間に接続されている。フォトリレースイッチ 13 は、内部にフォトダイオード (発光ダイオード) を有し、フォトダイオードを発光させることにより、通信 I/F 部 11 の末端

装置 20 との通信線と、通信 I / F 部 12 のネットワーク NW1 との通信線とを導通状態にする。

[0017] なお、フォトリレースイッチ 13 は、電源（電力）が供給されることで、フォトダイオードが発光して、オン状態（導通状態）になり、電源（電力）が供給されていない状態において、オフ状態（非導通状態）になる。フォトリレースイッチ 13 は、後述する情報処理部 15 が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、通信 I / F 部 11 の末端装置 20 との通信線と、通信 I / F 部 12 のネットワーク NW1 との通信線とを接続し、パススルーモードに切り替える。ここで、パススルーモードとは、例えば、末端装置 20 とネットワーク NW1 との間で、情報処理部 15 を介さずに直接通信するモードのことである。本実施形態では、当該パススルーモードを縮退モードということがあり、この縮退モード（パススルーモード）に切り替える機能を縮退機能という。

[0018] 記憶部 14 は、情報処理装置 10 の各種処理において利用される各種情報を記憶する。記憶部 14 は、通信リスク記憶部 141 と、通信情報記憶部 142 と、通信実績記憶部 143 と、許容期間記憶部 144 とを備える。

[0019] 通信リスク記憶部 141 は、相手先の情報処理装置 10 の通信状態に関するパラメータに対する通信リスクの一覧を記憶する。通信リスク記憶部 141 は、例えば、パラメータの値と、通信リスクとを対応付けて記憶する。ここで、図 3 を参照して、通信リスク記憶部 141 が記憶するデータ例について説明する。

[0020] 図 3 は、本実施形態の通信リスク記憶部 141 のデータ例を示す図である。

図 3 に示すように、通信リスク記憶部 141 は、「パラメータ名」と、「パラメータ値」と、「通信リスク」とを対応付けて記憶する。ここで、「パラメータ名」は、上述した相手先の情報処理装置 10 の通信状態に関するパラメータの項目を示す。なお、パラメータには、例えば、「通信実績」が含まれ、「通信実績」には、例えば、「認証回数」、「通信データ量」、及び

「連続通信期間」などが含まれる。

[0021] 「認証回数」は、自装置（情報処理装置 10）と、相手先の情報処理装置 10 との間において、例えば、相互認証などの認証処理が実行された回数を示し、「通信データ量」は、自装置と、相手先の情報処理装置 10 との間の通信データ量を示している。また、「連続通信期間」は、自装置と、相手先の情報処理装置 10 との間の連続して通信した期間（例えば、日にち）を示している。

[0022] また、パラメータには、例えば、「環境パラメータ」が含まれ、「環境パラメータ」には、例えば、「復旧見込み期間」、及び「ネットワーク環境」などが含まれる。

「復旧見込み期間」は、相手先の情報処理装置 10 が、故障してパススルーモードになった場合に、情報処理部 15 を用いた通常の通信を行う通常モードに復旧するまでに見込まれる期間を示している。また、「ネットワーク環境」は、例えば、ネットワーク NW1 の設置環境を示しており、例えば、インターネットなどの公衆通信網や、社内 LAN などのローカルなネットワークなどのネットワークの環境を示している。ここで、ネットワーク NW1 の設置環境は、ネットワーク NW1 における攻撃の容易性を示す攻撃容易性情報の一例である。

[0023] また、「通信リスク」は、相手先の情報処理装置 10 が、パススルーモードである場合に、セキュリティが担保されていない状態で通信を行う場合のリスクを示している。本実施形態では、「通信リスク」は、“高”（高リスク）、“中”（中程度のリスク）、及び“低”（低リスク）により示される。

[0024] 図 3 に示す例では、「認証回数」の「パラメータ値」が、“100 回未満”の場合に、「通信リスク」が“高”であり、“100 回以上 5000 回未満”の場合に、「通信リスク」が“中”であることを示している。また、「認証回数」の「パラメータ値」が、“5000 回以上”の場合に、「通信リスク」が“低”であることを示している。

[0025] なお、図3に示す例では、例えば、「認証回数」は、多い程、「通信リスク」が低く、少ない程、「通信リスク」が高く設定されている。また、「通信データ量」は、多い程、「通信リスク」が高く、少ない程、「通信リスク」が低く設定されている。また、「連続通信期間」は、長い程、「通信リスク」が低く、短い程、「通信リスク」が高く設定されている。また、「復旧見込み期間」は、長い程、「通信リスク」が高く、短い程、「通信リスク」が低く設定されている。また、「ネットワーク環境」は、範囲が狭い程、「通信リスク」が低く、範囲が広い程、「通信リスク」が高く設定されている。

[0026] 図2の説明に戻り、通信情報記憶部142は、相手先の情報処理装置10ごとの通信情報を記憶する。ここで、図4を参照して、通信情報記憶部142が記憶するデータ例について説明する。

[0027] 図4は、本実施形態の通信情報記憶部142のデータ例を示す図である。

図4に示すように、通信情報記憶部142は、「装置ID」と、「通信情報」とを対応付けて記憶する。ここで、「装置ID」は、相手先の情報処理装置10を識別する識別情報である。また、「通信情報」には、「通信方式」、「認証方式」、「デバイス情報」、「復旧見込み時間」、「ネットワーク環境」などが含まれる。また、「デバイス情報」は、例えば、MACアドレス値やIPアドレスなどであり、相手先の識別情報の一例である。

[0028] 図4に示す例では、「装置ID」が“M0001”である情報処理装置10と自装置との間の通信における「通信情報」は、「通信方式」が“SSL”（Secure Sockets Layer）であり、「認証方式」が“HTTP/FTP”であることを示している。また、相手先の情報処理装置10の「デバイス情報」は、“XX:XX:XX:XX:XX:XX”であることを示している。また、相手先の情報処理装置10の「復旧見込み時間」が、“20分”であり、「ネットワーク環境」が“社内LAN”であることを示している。

このように、通信情報記憶部142は、「通信情報」を相手先の情報処理装置10ごとに記憶する。

[0029] 再び、図2の説明に戻り、通信実績記憶部143は、相手先の情報処理装置10との通信実績情報を記憶する。ここで、図5を参照して、通信実績記憶部143のデータ例について説明する。

[0030] 図5は、本実施形態の通信実績記憶部143のデータ例を示す図である。

図5に示すように、通信実績記憶部143は、「装置ID」と、「通信実績情報」とを対応付けて記憶する。ここで、「通信実績情報」は、自装置と相手先の情報処理装置10との間の通信実績を示す情報であり、例えば、上述した「認証回数」、「通信データ量」、及び「連続通信期間」などである。

[0031] 図5に示す例では、「装置ID」が“M0001”である相手先の情報処理装置10との間の「通信実績情報」において、「認証回数」が“200回”であり、「通信データ量」が“500MB”（ここで、MBは、メガバイト）であり、「連続通信期間」が“30日”であることを示している。

このように、通信実績記憶部143は、通信実績情報を相手先の情報処理装置10ごとに記憶する。

[0032] 再び、図2の説明に戻り、許容期間記憶部144は、通信リスクと、パススルー許容期間（所定の期間の一例）とを対応付けて記憶する。ここで、図6を参照して、許容期間記憶部144のデータ例について説明する。

[0033] 図6は、本実施形態の許容期間記憶部144のデータ例を示す図である。

図6に示すように、許容期間記憶部144は、「通信リスク」と、「パススルー許容期間」とを対応付けて記憶する。ここで、「パススルー許容期間」は、自装置と相手先の情報処理装置10との間の通信において、パススルーモードの通信が許容される期間を示している。

[0034] 図6に示す例では、「通信リスク」が“高”（高リスク）である場合に、「パススルー許容期間」が“0分”であることを示している。また、「通信リスク」が“中”（中程度リスク）である場合に、「パススルー許容期間」が“20分”であることを示している。また、「通信リスク」が“低”（低リスク）である場合に、「パススルー許容期間」が“60分”であることを

示している。

このように、本実施形態では、「通信リスク」が高い程、「パススルー許容期間」が短くなるように設定されている。

[0035] 再び、図2の説明に戻り、情報処理部15は、例えば、CPU (Central Processing Unit) などを含むプロセッサであり、情報処理装置10を統括的に制御する。情報処理部15は、例えば、末端装置20とネットワークNW1を介した相手先の情報処理装置10との間の通信を制御する処理を実行する。情報処理部15は、例えば、通信I/F部11が末端装置20から情報(データ)を受信した場合に、受信した情報(データ)を暗号化して通信I/F部12を介してネットワークNW1に送信する。また、情報処理部15は、例えば、通信I/F部12がネットワークNW1から情報(データ)を受信した場合に、受信した情報(データ)を復号して通信I/F部11を介して末端装置20に送信する。

また、情報処理部15は、認証処理部151と、暗号処理部152と、通信制御部153とを備える。

[0036] 認証処理部151は、例えば、自装置と相手先の情報処理装置10との間で相互に正当性を確認する相互認証などの認証処理を実行する。

暗号処理部152は、例えば、RSA暗号などの公開鍵暗号や、共通鍵暗号による暗号化処理、及び復号処理を実行する。暗号処理部152は、認証処理や暗号データによる機密通信における暗号化処理、及び復号処理を実行する。

[0037] 通信制御部153は、末端装置20(例えば、IoT機器21-1、上位装置22など)及び相手先の情報処理装置10と、自装置との間の通信を制御する。通信制御部153は、例えば、自装置と相手先の情報処理装置10との間でセッションキーを生成する。通信制御部153は、例えば、通信I/F部11が末端装置20からデータ(平文データ)を受信した場合に、受信したデータをセッションキーで、暗号処理部152に暗号化させる。通信制御部153は、暗号化されたデータ(暗号データ)を、通信I/F部12

及びネットワークNW1を介して相手先の情報処理装置10に送信する。

[0038] また、通信制御部153は、例えば、ネットワークNW1及び通信I/F部12を介して、相手先の情報処理装置10からデータ（暗号データ）を受信した場合に、受信したデータをセッションキーで、暗号処理部152に復号させる。通信制御部153は、復号されたデータ（平文データ）を、通信I/F部11を介して末端装置20に送信する。

通信制御部153は、このような相手先の情報処理装置10との通信における通信情報を、例えば、図4に示すように、通信情報記憶部142に記憶させる。また、通信制御部153は、このような相手先の情報処理装置10との通信における通信実績を、図5に示すように、通信実績記憶部143に記憶させる。

[0039] また、通信制御部153は、相手先の情報処理装置10が、パススルーモードになった場合に、相手先の情報処理装置10との通信状態に関するパラメータに基づいて、所定の期間（例えば、パススルー許容期間）、相手先の末端装置20（例えば、上位装置22）との通信を許容（許可）する。また、通信制御部153は、所定の期間の経過後に、相手先の末端装置20との通信を制限（禁止）する。

[0040] ここで、相手先の末端装置20は、ネットワークNW1を介して末端装置20が通信する相手先末端装置であり、例えば、上位装置22である。また、相手先の情報処理装置10は、相手先末端装置（上位装置22）とネットワークNW1との間に接続され、自装置（情報処理装置10-1）と同一の構成である情報処理装置10-2である。すなわち、情報処理装置10-2は、情報処理装置10-1と同様に、通信I/F部11、通信I/F部12、情報処理部15、及びフォトリレースイッチ13備える。

[0041] なお、上述したパラメータには、相手先の情報処理装置10との通信実績（例えば、認証回数、通信データ量、及び連続通信期間など）が含まれ、通信制御部153は、通信実績に基づいて、パススルー許容期間を決定する。また、パラメータには、相手先の情報処理装置10におけるパススルーモー

ドが解除されるまでの復旧見込み時間が含まれ、通信制御部 153 は、復旧見込み時間に基づいて、パススルー許容期間を決定する。また、パラメータには、ネットワーク NW1 における攻撃の容易性を示す攻撃容易性情報が含まれ、通信制御部 153 は、攻撃容易性情報（例えば、ネットワーク環境）に基づいて、パススルー許容期間を決定する。

[0042] 通信制御部 153 は、例えば、通信リスク記憶部 141 から、相手先の情報処理装置 10 に対応するパラメータの値に基づいて取得した、相手先末端装置（上位装置 22）に対する通信リスクに基づいて、パススルー許容期間を決定する。具体的に、通信制御部 153 は、通信情報記憶部 142 が記憶する相手先の情報処理装置 10 に対応する環境パラメータ（例えば、復旧見込み時間及びネットワーク環境）を取得し、当該環境パラメータに対応する通信リスクを、通信リスク記憶部 141 から取得する。また、通信制御部 153 は、通信実績記憶部 143 が記憶する相手先の情報処理装置 10 に対応する通信実績（例えば、認証回数、通信データ量、及び連続通信期間）を取得し、当該通信実績に対応する通信リスクを、通信リスク記憶部 141 から取得する。

[0043] 図 7 は、本実施形態のパススルー許容期間の決定例を示す図である。

図 7 に示す例は、相手先末端装置が“機器 A”である場合の一例である。通信制御部 153 は、機器 A が接続されている相手先の情報処理装置 10 に対応する通信実績及び環境パラメータにより、通信リスク記憶部 141 から、図 7 に示すように通信リスクを取得する。図 7 に示す例では、通信リスクが全項目“中”であるため、通信制御部 153 は、全体リスク（全体の通信リスク）を“中”と判定し、許容期間記憶部 144 から通信リスクが“中”に対応するパススルー許容期間（“20分”）を取得し、パススルー許容期間を決定する。

[0044] なお、図 7 に示すように、複数のパラメータの項目に対応する通信リスクを用いて、パススルー許容期間を決定する場合には、通信制御部 153 は、例えば、当該複数の通信リスクの多数決で全体の通信リスクを決定してもよ

いし、最も高い通信リスクに決定してもよい。

[0045] また、通信制御部 153 は、相手先の情報処理装置 10 との通信における通信方式、認証方式、及び相手先の識別情報のうちの少なくとも 1 つに基づいて、相手先の情報処理装置 10 がパススルーモードになったか否かを検出する。通信制御部 153 は、例えば、通信情報記憶部 142 が記憶する通信情報に基づいて、相手先の情報処理装置 10 がパススルーモードになったか否かを検出する。すなわち、通信制御部 153 は、通信情報記憶部 142 が記憶する通信情報と、現在の通信における通信情報とを比較して、変化が生じた場合に、相手先の情報処理装置 10 がパススルーモードになったと判定する。

[0046] 次に、図面を参照して、本実施形態の情報処理システム 1 の動作について説明する。

図 8 は、本実施形態の情報処理システム 1 の機密通信動作の一例を示す図である。この図では、IoT 機器 21-1 と上位装置 22 との間の通信を、情報処理装置 10-1 及び情報処理装置 10-2 を用いて機密通信にする場合の一例について説明する。なお、情報処理装置 10-1 と情報処理装置 10-2 との間の認証処理、及びセッションキーの生成処理は、完了しているものとする。

[0047] 図 8 において、まず、IoT 機器 21-1 が、データ（平文）を情報処理装置 10-1 に送信する（ステップ S101）。情報処理装置 10-1 の通信制御部 153 は、通信 I/F 部 11 を介して、IoT 機器 21-1 からのデータを受信する。

[0048] 次に、情報処理装置 10-1 は、暗号化処理を実行する（ステップ S102）。情報処理装置 10-1 の通信制御部 153 は、IoT 機器 21-1 から受信したデータを、セッションキーにより暗号処理部 152 に暗号化させる。

[0049] 次に、情報処理装置 10-1 は、暗号データをネットワーク NW1 を介して情報処理装置 10-2 に送信する（ステップ S103）。情報処理装置 1

0-1の通信制御部153は、暗号処理部152に暗号化させたデータである暗号データを、通信I/F部12及びネットワークNW1を介して情報処理装置10-2に送信する。情報処理装置10-2の通信制御部153は、通信I/F部12を介して、情報処理装置10-1からの暗号データを受信する。

[0050] 次に、情報処理装置10-2は、復号処理を実行する（ステップS104）。情報処理装置10-2の通信制御部153は、受信した暗号データを、セッションキーにより暗号処理部152に復号させる。

[0051] 次に、情報処理装置10-2は、データ（平文）を上位装置22に送信する（ステップS105）。情報処理装置10-2の通信制御部153は、暗号処理部152に復号させたデータ（平文）を、通信I/F部11を介して上位装置22に送信する。

[0052] また、上位装置22が、データ（平文）を情報処理装置10-2に送信する（ステップS106）。情報処理装置10-2の通信制御部153は、通信I/F部11を介して、上位装置22からのデータを受信する。

[0053] 次に、情報処理装置10-2は、暗号化処理を実行する（ステップS107）。情報処理装置10-2の通信制御部153は、上位装置22から受信したデータを、セッションキーにより暗号処理部152に暗号化させる。

[0054] 次に、情報処理装置10-2は、暗号データをネットワークNW1を介して情報処理装置10-1に送信する（ステップS108）。情報処理装置10-2の通信制御部153は、暗号処理部152に暗号化させたデータである暗号データを、通信I/F部12及びネットワークNW1を介して情報処理装置10-1に送信する。情報処理装置10-1の通信制御部153は、通信I/F部11を介して、情報処理装置10-2からの暗号データを受信する。

[0055] 次に、情報処理装置10-1は、復号処理を実行する（ステップS109）。情報処理装置10-1の通信制御部153は、受信した暗号データを、セッションキーにより暗号処理部152に復号させる。

[0056] 次に、情報処理装置 10-1 は、データ（平文）を I o T 機器 21-1 に送信する（ステップ S 110）。情報処理装置 10-1 の通信制御部 153 は、暗号処理部 152 に復号させたデータ（平文）を、通信 I / F 部 11 を介して I o T 機器 21-1 に送信する。

このように、本実施形態の情報処理システム 1 は、I o T 機器 21-1 と上位装置 22 との間に、情報処理装置 10-1 及び情報処理装置 10-2 を接続することで、機密通信を可能にする。

[0057] 次に、図 9 を参照して、本実施形態の情報処理装置 10 の縮退機能の動作について説明する。

図 9 は、本実施形態の情報処理装置 10 の縮退機能の動作の一例を示す図である。

フォトリレースイッチ 13 は、情報処理部 15 が正常に動作している状態（通常モード）では、情報処理部 15 から電源（電力）が供給されて、オフ状態になっている。

[0058] この通常モードにおいて、例えば、電源の供給停止などのによって、情報処理部 15 からフォトリレースイッチ 13 に電源（電力）の供給が停止されると、フォトリレースイッチ 13 は、オン状態になり、通信 I / F 部 11 の末端装置 20 との通信線と、通信 I / F 部 12 のネットワーク NW1 との通信線とを接続する。これにより、情報処理装置 10 は、パススルーモードになる。

このように、本実施形態の情報処理装置 10 は、電源の供給停止などの情報処理部 15 が動作不能になった場合に、パススルーモードにする縮退機能を備える。

[0059] 次に、図 10 を参照して、本実施形態の情報処理装置 10 のパススルーモードの検出動作及びパススルー許容期間の決定動作について説明する。

図 10 は、本実施形態の情報処理装置 10 の動作の一例を示すフローチャートである。

[0060] 図 10 において、情報処理装置 10 の情報処理部 15 は、まず、相手先の

情報処理装置 10 がパススルーモードであるか否かを判定する（ステップ S 201）。情報処理部 15 の通信制御部 153 は、例えば、通信情報記憶部 142 が記憶する通信情報を参照し、通信情報記憶部 142 が記憶する通信情報と、現在の通信における通信情報とを比較して、2つの通信情報が一致するか否かによって、相手先の情報処理装置 10 がパススルーモードになったか否かを判定する。通信制御部 153 は、例えば、相手先の情報処理装置 10 がパススルーモードである場合（ステップ S 201：YES）に、処理をステップ S 202 に進める。また、通信制御部 153 は、例えば、相手先の情報処理装置 10 がパススルーモードでない場合（ステップ S 201：NO）に、処理をステップ S 201 に戻す。

[0061] ステップ S 202 において、通信制御部 153 は、パススルー許容期間を設定する。すなわち、通信制御部 153 は、通信情報記憶部 142 が記憶する相手先の情報処理装置 10 に対応する通信実績及び環境パラメータを、通信実績記憶部 143 及び通信情報記憶部 142 から取得し、通信実績及び環境パラメータに対応する通信リスクを、通信リスク記憶部 141 から取得する。通信制御部 153 は、例えば、図 7 に示すように、複数の通信リスクから全体の通信リスクを決定し、当該全体の通信リスクに対応するパススルー許容期間を許容期間記憶部 144 から取得する。

[0062] 次に、通信制御部 153 は、相手先の情報処理装置 10 の故障を管理装置（不図示）に通知する（ステップ S 203）。管理装置は、情報処理装置 10 が故障した旨を、例えば、電子メールなどで保守担当者に連絡して、故障した情報処理装置 10 の修理を手配する。

[0063] 次に、通信制御部 153 は、パススルーモードの通信を許可する（ステップ S 204）。通信制御部 153 は、自装置（情報処理装置 10）と、相手先の情報処理装置 10 に接続されている末端装置 20（例えば、上位装置 22 など）との間のパススルーモードによる通信を行う。

[0064] 次に、通信制御部 153 は、相手先の情報処理装置 10 がパススルーモードから復旧したか否かを判定する（ステップ S 205）。通信制御部 153

は、パススルーモードの判定と同様に、例えば、通信情報記憶部 142 が記憶する通信情報を参照し、現在の通信における通信情報とを比較して、パススルーモードから復旧したか否かを判定する。通信制御部 153 は、相手先の情報処理装置 10 がパススルーモードから復旧した場合（ステップ S205：YES）に、処理をステップ S209 に進める。また、通信制御部 153 は、相手先の情報処理装置 10 がパススルーモードから復旧していない場合（ステップ S205：NO）に、処理をステップ S206 に進める。

[0065] ステップ S206 において、通信制御部 153 は、パススルー許容期間が完了したか否かを判定する。通信制御部 153 は、パススルーモードの通信の許可後に、パススルー許容期間が経過したか否かを判定する。通信制御部 153 は、パススルー許容期間が完了した場合（ステップ S206：YES）に、処理をステップ S207 に進める。また、通信制御部 153 は、パススルー許容期間が完了していない場合（ステップ S206：NO）に、処理をステップ S205 に戻す。

[0066] ステップ S207 において、通信制御部 153 は、パススルーモードの通信を禁止する。

次に、通信制御部 153 は、再び相手先の情報処理装置 10 がパススルーモードから復旧したか否かを判定する（ステップ S208）。通信制御部 153 は、相手先の情報処理装置 10 がパススルーモードから復旧した場合（ステップ S208：YES）に、処理をステップ S209 に進める。また、通信制御部 153 は、相手先の情報処理装置 10 がパススルーモードから復旧していない場合（ステップ S208：NO）に、処理をステップ S208 に戻す。

[0067] ステップ S209 において、通信制御部 153 は、通常モードの通信を開始する。通信制御部 153 は、ステップ S209 の処理後に、処理をステップ S201 に戻す。

[0068] 以上説明したように、本実施形態による情報処理装置 10 は、通信 I/F 部 11（第 1 通信部）と、通信 I/F 部 12（第 2 通信部）と、情報処理部

15と、フォトリレースイッチ13（切替部）とを備える。通信I／F部11は、ネットワークNW1に接続される末端の装置である末端装置20に接続し、末端装置20との間で通信可能である。通信I／F部12は、ネットワークNW1に接続し、ネットワークNW1を介してネットワークNW1に接続された装置と通信可能である。情報処理部15は、少なくとも通信I／F部11が末端装置20から情報を受信した場合に、受信した情報を暗号化して通信I／F部12を介してネットワークNW1に送信する。情報処理部15は、少なくとも通信I／F部12がネットワークNW1から暗号化された情報を受信した場合に、受信した情報を復号して通信I／F部11を介して末端装置20に送信する。フォトリレースイッチ13は、情報処理部15が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、通信I／F部11の末端装置20との通信線と、通信I／F部12のネットワークNW1との通信線とを直接接続し、末端装置20とネットワークNW1との間で、情報処理部15を介さずに直接通信するパススルーモードに切り替える。

[0069] これにより、本実施形態による情報処理装置10は、例えば、情報処理部15が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、パススルーモードに切り替えるため、通信を継続することができる。また、本実施形態による情報処理装置10は、情報処理部15によって、ネットワークNW1上を暗号化された情報を送信するようにするため、セキュリティを確保することができる。よって、本実施形態による情報処理装置10は、セキュリティを確保しつつ、可用性を向上させることができる。

[0070] また、情報処理装置10は、末端装置20とネットワークNW1との間に挿入することで、末端装置20に手を加えずに、機密通信が可能になるため、既存のシステムに対して容易にセキュリティを付加及び向上させることができる。

[0071] また、本実施形態では、情報処理部15は、相手先の情報処理装置10が、パススルーモードになった場合に、相手先の情報処理装置10との通信状

態に関するパラメータに基づいて、所定の期間（例えば、パススルー許容期間）、相手先末端装置（例えば、上位装置２２）との通信を許容（例えば、許可）し、所定の期間の経過後に、上位装置２２との通信を制限（例えば、禁止）する。ここで、相手先の情報処理装置１０は、ネットワークNW１を介して末端装置２０が通信する相手先の末端装置２０である相手先末端装置（例えば、上位装置２２）とネットワークNW１との間に接続され、上述した通信Ｉ／Ｆ部１１、通信Ｉ／Ｆ部１２、情報処理部１５、及びフォトリレースイッチ１３を備える。

[0072] これにより、本実施形態による情報処理装置１０は、通信状態に関するパラメータに基づいて、例えば、パススルーモードの通信を許可する期間を制限するため、さらに、セキュリティを確保しつつ、可用性を向上させることができる。

[0073] また、本実施形態では、情報処理部１５は、通信状態に関するパラメータの値と、通信リスクとを対応付けて記憶する通信リスク記憶部１４１から、相手先の情報処理装置１０に対応するパラメータの値に基づいて取得した、相手先末端装置に対する通信リスクに基づいて、パススルー許容期間を決定する。

これにより、本実施形態による情報処理装置１０は、通信リスクに応じて、適切にパススルー許容期間を決定することができる。

[0074] また、本実施形態では、通信状態に関するパラメータには、相手先の情報処理装置１０との通信実績（例えば、認証回数、通信データ量、及び連続通信期間など）が含まれ、情報処理部１５は、通信実績に基づいて、パススルー許容期間を決定する。

これにより、本実施形態による情報処理装置１０は、相手先の情報処理装置１０との通信実績に応じて、適切にパススルー許容期間を決定することができる。

[0075] また、本実施形態では、通信状態に関するパラメータには、相手先の情報処理装置１０におけるパススルーモードが解除されるまでの復旧見込み時間

が含まれ、情報処理部 15 は、復旧見込み時間に基づいて、パススルー許容期間を決定する。

これにより、本実施形態による情報処理装置 10 は、相手先の情報処理装置 10 及び情報処理システム 1 の復旧するまでの期間を考慮して、適切にパススルー許容期間を決定することができる。

[0076] また、本実施形態では、通信状態に関するパラメータには、ネットワーク NW1 における攻撃の容易性を示す攻撃容易性情報が含まれ、情報処理部 15 は、攻撃容易性情報（例えば、ネットワーク環境）に基づいて、パススルー許容期間を決定する。

これにより、本実施形態による情報処理装置 10 は、情報処理システム 1 に対する攻撃容易性情報を考慮して、適切にパススルー許容期間を決定することができる。

[0077] また、本実施形態では、情報処理部 15 は、相手先の情報処理装置 10 との通信における通信方式、認証方式、及び相手先の識別情報（例えば、MAC アドレスなど）のうちの少なくとも 1 つに基づいて、相手先の情報処理装置 10 がパススルーモードになったか否かを検出する。

これにより、本実施形態による情報処理装置 10 は、パススルーモードになったか否かを高精度で検出することができる。

[0078] また、本実施形態による情報処理装置 10 は、相手先の情報処理装置 10 との通信における通信方式、認証方式、及び相手先の識別情報のうちの少なくとも 1 つを含む通信情報を記憶する通信情報記憶部 142 を備える。情報処理部 15 は、通信情報記憶部 142 が記憶する通信情報に基づいて、相手先の情報処理装置 10 がパススルーモードになったか否かを検出する。

これにより、本実施形態による情報処理装置 10 は、簡易な手法により、パススルーモードになったか否かを高精度で検出することができる。

[0079] また、本実施形態による情報処理システム 1 は、複数の末端装置 20 と、上述した情報処理装置 10 であって、複数の末端装置 20 のそれぞれとネットワーク NW1 との間にそれぞれが接続される複数の情報処理装置 10 とを

備える。

これにより、本実施形態による情報処理システム 1 は、上述した情報処理装置 10 と同様の効果を奏し、セキュリティを確保しつつ、可用性を向上させることができる。

[0080] (第 2 の実施形態)

次に、図面を参照して、第 2 の実施形態の情報処理装置 10a 及び情報処理システム 1a について説明する。

本実施形態では、情報処理システム 1a は、管理装置 30 を備え、第 1 の実施形態の情報処理装置 10 が備える記憶部 14 の一部を管理装置 30 が記憶する場合の一例について説明する。

[0081] 図 11 は、第 2 の実施形態の情報処理システム 1a の一例を示すブロック図である。

図 11 に示すように、情報処理システム 1a は、情報処理装置 (10a-1、10a-2、10a-3、...) と、IoT 機器 (21-1、21-2、...) と、上位装置 22 と、管理装置 30 とを備える。

なお、この図において、図 1 と同一の構成には、同一の符号を付与して、ここではその説明を省略する。

[0082] また、本実施形態において、情報処理装置 10a-1 と、情報処理装置 10a-2 と、情報処理装置 10a-3 とのそれぞれは、同一の構成であり、単に情報処理システム 1a が備える情報処理装置を示す場合、又は、区別しない場合には、情報処理装置 10a として説明する。

[0083] 情報処理装置 10a は、末端装置 20 とネットワーク NW1 との間に接続される通信制御装置である。情報処理装置 10a は、末端装置 20 とネットワーク NW1 との間の通信において、セキュリティを付加してデータ通信を中継する。

なお、図 11 に示すように、情報処理装置 10a-1 は、IoT 機器 21-1 とネットワーク NW1 との間に接続され、情報処理装置 10a-3 は、IoT 機器 21-2 とネットワーク NW1 との間に接続されている。また、

情報処理装置 10a-2 は、上位装置 22 とネットワーク NW1 との間に接続されている。

[0084] 図 12 は、本実施形態の情報処理装置 10a の一例を示すブロック図である。

図 12 に示すように、情報処理装置 10a は、通信 I/F 部 11 と、通信 I/F 部 12 と、フォトリレースイッチ 13 と、記憶部 14a と、情報処理部 15a とを備える。

なお、図 12 において、図 2 と同一の構成には、同一の符号を付与して、ここではその説明を省略する。

[0085] 記憶部 14a は、情報処理装置 10a の各種処理において利用される各種情報を記憶する。記憶部 14a は、通信情報記憶部 142 と、通信実績記憶部 143 とを備える。記憶部 14a は、通信リスク記憶部 141 と、許容期間記憶部 144 とを備えない点が第 1 の実施形態と異なる。

[0086] 情報処理部 15a は、例えば、CPU などを含むプロセッサであり、情報処理装置 10a を統括的に制御する。情報処理部 15a は、認証処理部 151 と、暗号処理部 152 と、通信制御部 153a とを備える。

なお、情報処理部 15a の基本的な機能は、第 1 の実施形態の情報処理部 15 と同様である。本実施形態では、記憶部 14a が、通信リスク記憶部 141 と、許容期間記憶部 144 とを備えないため、情報処理部 15a は、通信リスク記憶部 141 及び許容期間記憶部 144 が記憶する情報を、後述する管理装置 30 が備える通信リスク記憶部 321 及び許容期間記憶部 322 から取得する点が、第 1 の実施形態と異なる。

[0087] 図 11 の説明に戻り、管理装置 30 は、例えば、サーバ装置などのコンピュータ装置である。管理装置 30 は、情報処理システム 1a を管理する。管理装置 30 は、管理処理部 31 と、管理記憶部 32 とを備える。

[0088] 管理処理部 31 は、例えば、CPU などを含むプロセッサであり、管理装置 30 を統括的に制御する。管理処理部 31 は、例えば、情報処理装置 10a の要求に応じて、管理記憶部 32 が記憶する各種情報を読み出して、要求

元の情報処理装置 10a に送信する。また、管理処理部 31 は、例えば、情報処理装置 10a の更新情報や更新プログラムを、情報処理装置 10a に送信する。また、管理処理部 31 は、情報処理装置 10a が故障した場合に、例えば、電子メールなどで保守担当者に連絡して、故障した情報処理装置 10a の修理を手配する。

[0089] 管理記憶部 32 は、通信リスク記憶部 321 と、許容期間記憶部 322 とを備える。

通信リスク記憶部 321 は、相手先の情報処理装置 10 の通信状態に関するパラメータに対する通信リスクの一覧を記憶する。通信リスク記憶部 321 は、例えば、パラメータの値と、通信リスクとを対応付けて相手先の情報処理装置 10a ごとに記憶する。ここで、図 13 を参照して、通信リスク記憶部 321 が記憶するデータ例について説明する。

[0090] 図 13 は、本実施形態の通信リスク記憶部 321 のデータ例を示す図である。

図 13 に示すように、通信リスク記憶部 321 は、「装置 ID」と、「末端 ID」と、「パラメータ名」と、「パラメータ値」と、「通信リスク」とを対応付けて記憶する。ここで、「装置 ID」は、情報処理装置 10a を識別する識別情報であり、「末端 ID」は、情報処理装置 10a が接続されている末端装置 20 を識別する識別情報である。その他の情報は、上述した図 3 に示す通信リスク記憶部 141 と同様である。本実施形態の通信リスク記憶部 321 は、相手先の情報処理装置 10a ごとに通信リスク情報を記憶する点が、第 1 の実施形態の通信リスク記憶部 141 と異なる。

[0091] 再び、図 12 の説明に戻り、許容期間記憶部 322 は、通信リスクと、パスルー許容期間（所定の期間の一例）とを対応付けて、相手先の情報処理装置 10a ごとに記憶する。ここで、図 14 を参照して、許容期間記憶部 322 のデータ例について説明する。

[0092] 図 14 は、本実施形態の許容期間記憶部 322 のデータ例を示す図である。

図 1 4 に示すように、許容期間記憶部 3 2 2 は、「装置 I D」と、「通信リスク」と、「パススルー許容期間」とを対応付けて記憶する。本実施形態の許容期間記憶部 3 2 2 は、「装置 I D」（相手先の情報処理装置 1 0 a の識別情報）ごとに、「パススルー許容期間」が設定されている点以外は、上述した図 6 に示す第 1 の実施形態の許容期間記憶部 1 4 4 と同様である。本実施形態の許容期間記憶部 3 2 2 は、相手先の情報処理装置 1 0 a ごとにパススルー許容期間を記憶する点が、第 1 の実施形態の許容期間記憶部 1 4 4 と異なる。

[0093] 本実施形態における情報処理部 1 5 a の通信制御部 1 5 3 a は、例えば、管理記憶部 3 2 の通信リスク記憶部 3 2 1 から、相手先の情報処理装置 1 0 a に対応するパラメータの値に基づいて通信リスクを取得する。通信制御部 1 5 3 a は、取得した通信リスクに基づいて、管理装置 3 0 の許容期間記憶部 3 2 2 から相手先の情報処理装置 1 0 a に対応するパススルー許容期間を取得して、パススルー許容期間を決定する。また、情報処理部 1 5 a のその他の処理は、上述した第 1 の実施形態と同様であるため、ここではその説明を省略する。

[0094] 以上説明したように、本実施形態による情報処理装置 1 0 a では、情報処理部 1 5 a は、外部に備えられた管理装置 3 0 の通信リスク記憶部 3 2 1 から、相手先の情報処理装置 1 0 に対応するパラメータの値に基づいて取得した、相手先末端装置に対する通信リスクに基づいて、パススルー許容期間を決定する。

これにより、本実施形態による情報処理装置 1 0 a は、第 1 の実施形態と同様に、通信リスクに応じて、適切にパススルー許容期間を決定することができる。

[0095] また、本実施形態では、通信リスク記憶部 3 2 1 は、相手先の情報処理装置 1 0 a の識別情報と、通信状態に関するパラメータの値と、通信リスクとを対応付けて記憶する。

これにより、本実施形態による情報処理装置 1 0 a は、相手先の情報処理

装置 10a ごとに、通信リスクの設定を変更することができる。

[0096] また、本実施形態では、許容期間記憶部 322 は、相手先の情報処理装置 10a の識別情報と、通信リスクと、パススルー許容期間とを対応付けて記憶する。

これにより、本実施形態による情報処理装置 10a は、相手先の情報処理装置 10a ごとに、パススルー許容期間を変更することができる。

[0097] なお、上述した本実施形態では、情報処理装置 10a が、通信リスク記憶部 141 及び許容期間記憶部 144 を備えない例を説明したが、情報処理装置 10a が、通信リスク記憶部 141 及び許容期間記憶部 144 を備えるようにしてもよい。この場合、情報処理部 15a は、管理装置 30 の通信リスク記憶部 321 及び許容期間記憶部 322 が記憶する情報を、定期的に通信リスク記憶部 141 及び許容期間記憶部 144 に記憶させて使用するようにしてもよい。

[0098] これにより、本実施形態による情報処理装置 10a は、最新の情報に基づいて、適切に情報通信を行うことができる。また、情報処理システム 1a は、管理装置 30 により通信リスク及びパススルー許容期間を一元管理することができ、利便性を向上させることができる。

[0099] (第 3 の実施形態)

次に、図面を参照して、第 3 の実施形態の情報処理装置 10b 及び情報処理システム 1b について説明する。

本実施形態では、情報処理システム 1b は、管理装置 30a を備えるとともに、情報処理装置 10b が暗号処理部 152 の代わりに IC カード 40 を備える場合の変形例について説明する。

[0100] 図 15 は、第 3 の実施形態の情報処理システム 1b の一例を示すブロック図である。

図 15 に示すように、情報処理システム 1b は、情報処理装置 (10b-1、10b-2、10b-3、...) と、IoT 機器 (21-1、21-2、...) と、上位装置 22 と、管理装置 30a とを備える。

なお、この図において、図1及び図11と同一の構成には、同一の符号を付与して、ここではその説明を省略する。

[0101] また、本実施形態において、情報処理装置10b-1と、情報処理装置10b-2と、情報処理装置10b-3とのそれぞれは、同一の構成であり、単に情報処理システム1bが備える情報処理装置を示す場合、又は、区別しない場合には、情報処理装置10bとして説明する。

[0102] 情報処理装置10bは、末端装置20とネットワークNW1との間に接続される通信制御装置である。情報処理装置10bは、末端装置20とネットワークNW1との間の通信において、セキュリティを付加してデータ通信を中継する。

なお、図15に示すように、情報処理装置10b-1は、IoT機器21-1とネットワークNW1との間に接続され、情報処理装置10b-3は、IoT機器21-2とネットワークNW1との間に接続されている。また、情報処理装置10b-2は、上位装置22とネットワークNW1との間に接続されている。

[0103] また、本実施形態では、IoT機器21-1をクライアント装置とし、上位装置22をサーバ装置として、クライアント装置から撮像データをサーバ装置に送付する一例について説明する。また、本実施形態では、情報処理装置10b-1をクライアント側通信制御装置とし、情報処理装置10b-2をサーバ側通信制御装置とする。本実施形態において、IoT機器21-1（クライアント装置）とネットワークNW1との間に接続された情報処理装置10b-1（クライアント側通信制御装置）が、IoT機器21-1（クライアント装置）が送信するデータを暗号化してネットワークNW1に出力する。また、上位装置22（サーバ装置）とネットワークNW1との間に接続された情報処理装置10b-2（サーバ側通信制御装置）が、上位装置22（サーバ装置）が送信する制御データを暗号化してネットワークNW1に出力する。これにより、IoT機器21-1（クライアント装置）、及び上位装置22（サーバ装置）を変更することなく、ネットワークNW1を流れ

る撮像データの安全性を向上させる。

- [0104] また、情報処理装置 10b-1（クライアント側通信制御装置）は、上位装置 22（サーバ装置）に対してデータを送信する際に、IoT機器 21-1（クライアント装置）から取得したデータを暗号化し、暗号化したデータを上位装置 22（サーバ装置）に対して送信する。

また、情報処理装置 10b-1（クライアント側通信制御装置）は、IoT機器 21-1（クライアント装置）にデータを出力する際に、上位装置 22（サーバ装置）から情報処理装置 10b-2（サーバ側通信制御装置）を介して取得したデータを復号し、復号したデータを情報処理装置 10b-1（クライアント側通信制御装置）に出力する。

- [0105] 情報処理装置 10b-2（サーバ側通信制御装置）は、IoT機器 21-1（クライアント装置）に対してデータを送信する際に、上位装置 22（サーバ装置）から取得したデータを暗号化し、暗号化したデータをIoT機器 21-1（クライアント装置）に対して送信する。

また、情報処理装置 10b-2（サーバ側通信制御装置）は、上位装置 22（サーバ装置）にデータを出力する際に、IoT機器 21-1（クライアント装置）から情報処理装置 10b-1（クライアント側通信制御装置）を介して取得したデータを復号し、復号したデータを上位装置 22（サーバ装置）に出力する。

- [0106] 本実施形態において、情報処理装置 10b-1 及び情報処理装置 10b-2 が行うデータの暗号化には、例えば、SSL/TLS (Transport Layer Security) のプロトコルによる暗号化が行われる。情報処理装置 10b-1 及び情報処理装置 10b-2 は、例えば、SSL/TLS プロトコルを、HTTP と組み合わせることで、HTTP に含まれるデータを暗号化し、安全性を向上させた HTTPS (HTTP Secure) に置き換える。

- [0107] また、情報処理装置 10b-1 及び情報処理装置 10b-2 は、SSL/TLS プロトコルを種々の通信プロトコルと組み合わせることにより、安全性を向上させたセキュアな通信プロトコルに置き換えてもよい。例えば、情

報処理装置 10b-1 及び情報処理装置 10b-2 は、FTP (File Transfer Protocol) を FTPS (FTP Secure) に置き換えてもよい。

[0108] 図 16 は、本実施形態の情報処理装置 10b の一例を示すブロック図である。

図 16 に示すように、情報処理装置 10b は、通信 I/F 部 11 と、通信 I/F 部 12 と、フォトリレースイッチ 13 と、記憶部 14 と、情報処理部 15b と、リーダライタ 35 と、IC カード 40 とを備える。

なお、図 16 において、図 2 と同一の構成には、同一の符号を付与して、ここではその説明を省略する。

[0109] 情報処理部 15b は、例えば、CPU などを含むプロセッサであり、情報処理装置 10b を統括的に制御する。情報処理部 15b は、認証処理部 151 と、通信制御部 153 とを備える。情報処理部 15b の基本的な機能は、第 1 の実施形態の情報処理部 15 と同様であるが、暗号処理部 152 を備えず、IC カード 40 がその機能を代用する。

[0110] 本実施形態における認証処理部 151 は、例えば、自装置と相手先の情報処理装置 10 との間で相互に正当性を確認する相互認証などの認証処理を実行する際に、リーダライタ 35 を介して IC カード 40 と通信して、認証処理を実行する。

また、本実施形態における通信制御部 153 は、例えば、通信 I/F 部 11 が末端装置 20 からデータ（平文データ）を受信した場合に、受信したデータをセッションキーで、IC カード 40 に暗号化させる。通信制御部 153 は、暗号化されたデータ（暗号データ）を、通信 I/F 部 12 及びネットワーク NW1 を介して相手先の情報処理装置 10 に送信する。

[0111] また、通信制御部 153 は、例えば、ネットワーク NW1 及び通信 I/F 部 12 を介して、相手先の情報処理装置 10 からデータ（暗号データ）を受信した場合に、受信したデータをセッションキーで、IC カード 40 に復号させる。通信制御部 153 は、復号されたデータ（平文データ）を、通信 I/F 部 11 を介して末端装置 20 に送信する。

[0112] リーダライタ 35 は、ＩＣカード 40 のコンタクト部 36 を介して、ＩＣカード 40 の間の通信を行う。

ＩＣカード 40（認証部の一例）は、例えば、プラスチックのカード基材に、ＩＣモジュール 41 を実装して形成されている。すなわち、ＩＣカード 40 は、ＩＣモジュール 41 と、ＩＣモジュール 41 が埋め込まれたカード基材とを備える。また、ＩＣカード 40 は、情報処理装置 10b に着脱可能に装着され、コンタクト部 36 及びリーダライタ 35 を介して情報処理装置 10b と通信可能である。

[0113] ＩＣカード 40 は、例えば、情報処理装置 10b がリーダライタ 35 を介して送信したコマンド（処理要求）を、コンタクト部 36 を介して受信し、受信したコマンドに応じた処理（コマンド処理）を実行する。そして、ＩＣカード 40 は、コマンド処理の実行結果であるレスポンス（処理応答）をコンタクト部 36 及びリーダライタ 35 を介して情報処理装置 10b に送信する。

[0114] ＩＣモジュール 41 は、コンタクト部 36 と、ＩＣチップ 42 とを備える。コンタクト部 36 は、ＩＣカード 40 が動作するために必要な各種信号の端子を有している。ここで、各種信号の端子は、電源電圧、クロック信号、リセット信号などをリーダライタ 35 から供給を受ける端子、及び、リーダライタ 35 と通信するためのシリアルデータ入出力端子（ＳＩＯ端子）を有する。ＩＣチップ 42 は、例えば、１チップのマイクロプロセッサなどのＬＳＩ（Large Scale Integration）である。

[0115] ここでは、ＩＣカード 40 のハードウェア構成について図 17 を用いて説明する。図 17 は、本実施形態のＩＣカード 40 のハードウェア構成例を示す図である。

[0116] ＩＣカード 40 は、コンタクト部 36 と、ＩＣチップ 42 とを備えたＩＣモジュール 41 を備えている。そして、ＩＣチップ 42 は、ＵＡＲＴ（Universal Asynchronous Receiver Transmitter）43 と、ＣＰＵ 44 と、ＲＯＭ（Read Only Memory）45 と、ＲＡＭ（Random Access Memory）46 と、Ｅ

EPROM (Electrically Erasable Programmable ROM) 47とを備える。

また、各構成(43から47)は、内部バスBSを介して接続されている。

[0117] UART43は、上述したSIO端子を介して、リーダライタ35とシリアルデータ通信を行う。UART43は、SIO端子を介して受信したシリアルデータ信号をパラレル変換したデータ(例えば、1バイトのデータ)を内部バスBSに出力する。また、UART43は、内部バスBSを介して取得したデータをシリアル変換して、SIO端子を介してリーダライタ35に出力する。UART43は、例えば、SIO端子を介してコマンドをリーダライタ35から受信する。また、UART43は、SIO端子を介してレスポンスをリーダライタ35に送信する。

[0118] CPU44は、ROM45又はEEPROM47に記憶されているプログラムを実行して、ICカード40の各種処理を行う。CPU44は、例えば、コンタクト部36を介して、UART43が受信したコマンドに応じたコマンド処理を実行する。

[0119] ROM45は、例えば、マスクROMなどの不揮発性メモリであり、ICカード40の各種処理を実行するためのプログラム、及びコマンドテーブルなどのデータを記憶する。RAM46は、例えば、SRAM (Static RAM)などの揮発性メモリであり、ICカード40の各種処理を行う際に利用されるデータを一時記憶する。EEPROM47は、例えば、電氣的に書き換え可能な不揮発性メモリである。EEPROM47は、ICカード40が利用する各種データを記憶する。EEPROM47は、例えば、ICカード40を利用した各種サービス(アプリケーション)に使用される情報を記憶する。

[0120] 次に、ICカード40の構成について、図18を用いて説明する。図18は、本実施形態のICカード40の機能構成例を示すブロック図である。ICカード40は、通信部400と、制御部401と、記憶部404とを備える。ここで、図18に示されるICカード40の各部は、図17に示されるICカード40のハードウェアを用いて実現される。

- [0121] 通信部400は、例えば、UART43と、CPU44と、ROM45に記憶されているプログラムとにより実現され、コンタクト部36を介して、例えば、リーダライタ35との間でコマンド及びレスポンスの送受信を行う。すなわち、通信部400は、所定の処理を要求するコマンド（処理要求）をリーダライタ35から受信するとともに、コマンドに対するレスポンス（処理応答）をリーダライタ35に送信する。通信部400は、UART43を介してリーダライタ35から受信した受信データをRAM46に記憶させる。また、通信部400は、RAM46に記憶されている送信データを、UART43を介してリーダライタ35に送信する。
- [0122] 制御部401は、例えば、CPU44と、RAM45と、ROM46又はEEPROM47とにより実現され、ICカード40を統括的に制御する。制御部401は、コマンド処理部402と、暗号化復号部403とを備える。
- [0123] ここで、コマンド処理部402が行う処理は、「認証処理」の一例である。また、暗号化復号部403が行う処理は、「暗号化復号処理」の一例である。
- [0124] コマンド処理部402は、各種コマンド処理を実行する。コマンド処理部402は、例えば、後述するHTTPスリクエストを要求するコマンド処理として、SSL/TLSハンドシェイクを行う。SSL/TLSハンドシェイクでは、暗号化された通信に必要な鍵情報等の交換、及び通信先の装置との相互認証を行う。ここで、相互認証とは、例えば、図15に示すIoT機器21-1（クライアント装置）に接続された情報処理装置10b-1（クライアント側通信制御装置）と、上位装置22（サーバ装置）に接続された情報処理装置10b-2（サーバ側通信制御装置）とが、通信を行う前に、互いに正当に認証された装置であることを相互に確認する認証処理である。
- [0125] 暗号化復号部403は、データを暗号化する処理、及び暗号化されたデータを復号する処理を実行する。暗号化復号部403は、通信部400を介して取得した装置（IoT機器21-1、又は上位装置22）により出力され

たデータを暗号化する。また、暗号化復号部403は、通信部400を介して取得したネットワークNW1からの暗号化されたデータを復号する。

[0126] 記憶部404は、例えば、EEPROM47により構成された記憶部であり、証明書情報記憶部405と、秘密情報記憶部406とを備える。証明書情報記憶部405は、管理装置30aが発行した装置（IoT機器21-1、又は上位装置22）に対する証明書を記憶する。具体的には、IoT機器21-1（クライアント装置）が接続されている情報処理装置10b-1に装着されるICカード40の証明書情報記憶部405には、クライアント証明書を示す情報が記憶される。また、上位装置22（サーバ装置）に接続された情報処理装置10b-2に装着されるICカード40の証明書情報記憶部405には、サーバ証明書を示す情報が記憶される。

[0127] 秘密情報記憶部406は、管理装置30が発行した装置（IoT機器21-1、又は上位装置22）に対する秘密鍵を記憶する。具体的には、IoT機器21-1（クライアント装置）が接続されている情報処理装置10b-1に装着されるICカード40の秘密情報記憶部406には、情報処理装置10b-1（クライアント側通信制御装置）に対して発行された秘密鍵を示す情報が記憶される。また、上位装置22（サーバ装置）に接続された情報処理装置10b-2に装着されるICカード40の秘密情報記憶部406には、情報処理装置10b-2（サーバ側通信制御装置）に対して発行された秘密鍵を示す情報が記憶される。

[0128] 図15の説明に戻り、管理装置30aは、例えば、サーバ装置などのコンピュータ装置であり、情報処理システム1bを管理する。管理装置30aは、情報処理装置10b-1に対し、クライアント証明書、及び秘密鍵を発行する。例えば、管理装置30aは、クライアント証明書、及び秘密鍵を記憶させたICカード40を発行する。また、管理装置30aは、ICカード40が装着された情報処理装置10b-1に対し、ICカード40に記憶させるクライアント証明書、及び秘密鍵を、ネットワークNW1を介して送信する。

[0129] また、管理装置30aは、情報処理装置10b-2に対し、サーバ証明書、及び秘密鍵を発行する。例えば、管理装置30aは、サーバ証明書、及び秘密鍵を記憶させたICカードを発行する。また、管理装置30aは、ICカード40が装着された情報処理装置10b-2に対し、ICカード40に記憶させるサーバ証明書、及び秘密鍵を、ネットワークNW1を介して送信する。クライアント証明書、サーバ証明書、及び秘密鍵のそれぞれは、情報処理装置10b-1と情報処理装置10b-2とが暗号化通信を行う場合に用いる共通鍵（セッションキー）を決定するために必要な情報である。

[0130] また、管理装置30aは、例えば、管理処理部31bと、管理記憶部32aとを備える。

管理処理部31bは、例えば、CPUなどを含むプロセッサであり、管理装置30aを統括的に制御する。管理処理部31bは、主に情報処理装置10b（10b-1、10b-2、・・・）の正当性を認めるプライベート認証局として機能する。管理処理部31bは、鍵作成部311と、証明書発行部312と、証明書更新部313と、証明書管理部314と、管理部315とを備える。

[0131] 鍵作成部311は、例えば、情報処理装置10b-1（10b-2）からの認証申請に基づいて、後述する証明書に含まれる公開鍵に対応する秘密鍵の発行を行う。

証明書発行部312は、例えば、情報処理装置10b-1（10b-2）からの認証申請に基づいて、情報処理装置10b-1（10b-2）の正当性を認める証明書の発行を行う。証明書には、公開鍵と、情報処理装置10b-1（10b-2）の所有者を示す情報が含まれる。

[0132] 証明書更新部313は、有効期限が経過した証明書に対して新たな有効期限を設定することにより、証明書の更新を行う。証明書更新部313は、例えば、情報処理装置10b-1（10b-2）からの更新申請に基づいて、当該情報処理装置10b-1（10b-2）に対して発行した証明書の有効期限を延長させた証明書を発行し、発行した証明書を情報処理装置10b-

1 (10b-2) に対して送信する。発行した証明書を示す情報が情報処理装置10b-1 (10b-2) により受信され、情報処理装置10b-1 (10b-2) のICカード40の証明書情報記憶部405に記憶されることで、情報処理装置10b-1 (10b-2) の証明書の有効期限が延長される。

[0133] 証明書管理部314は、既に発行済みの証明書に対する管理を行う。証明書管理部314は、例えば、情報処理装置10b-1 (10b-2) に装着されたICカード40の改ざん、又は盗難等により相互認証において互いの正当性が証明されない場合に、情報処理装置10b-1 (10b-2) に対して発行した証明書を無効化する処理を行う。また、証明書管理部314は、例えば、情報処理装置10b-1 (10b-2) からの問い合わせに基づいて、情報処理装置10b-1 (10b-2)、及び他の通信装置に対して発行した証明書が証明書管理部314により発行されたものか否か応答するようにしてもよい。また、証明書管理部314は、定期的に、発行済みの証明書が正当な情報処理装置10b-1 (10b-2) に使用されているかを確認するようにしてもよい。

[0134] 管理部315は、情報処理装置10b (10b-1、10b-2、・・・) を管理する。例えば、管理部509は、例えば、情報処理装置10b-1 (10b-2) が行う相互認証を、ネットワークNW1を介して遠隔制御する。

[0135] 管理記憶部32aは、例えば、鍵情報記憶部323と、証明書情報記憶部324とを備える。鍵情報記憶部323は、例えば、既に発行済みの公開鍵や、秘密鍵を示す情報を記憶する。証明書情報記憶部324は、例えば、既に発行済みの証明書を示す情報を記憶する。

鍵情報記憶部323と、証明書情報記憶部324とは、例えば、鍵作成部311が秘密鍵を発行する際、証明書発行部312が証明書を発行する際などに参照される。また、鍵情報記憶部323には、鍵作成部311が発行した秘密鍵を示す情報が記憶される。また、証明書情報記憶部324には、証

明書発行部 312 が発行した証明書を示す情報が記憶される。

[0136] 次に、図面を参照して、本実施形態の情報処理システム 1 の動作について説明する。

図 19 は、本実施形態の情報処理システム 1 b の機密通信動作の一例を示す図である。この図では、IoT 機器 21-1 (クライアント装置) と上位装置 22 (サーバ装置) との間の通信を、情報処理装置 10b-1 (クライアント側通信制御装置) 及び情報処理装置 10b-2 (サーバ側通信制御装置) を用いて機密通信にする場合の一例について説明する。

[0137] 図 19 において、IoT 機器 21-1 (クライアント装置) は、撮像データを上位装置 22 (サーバ装置) に送信する場合、まず、上位装置 22 に対する HTTP リクエストを送信する (ステップ S301)。IoT 機器 21-1 が送信した HTTP リクエストは、情報処理装置 10b-1 (クライアント側通信制御装置) により取得される (ステップ S302)。

[0138] 情報処理装置 10b-1 は、IoT 機器 21-1 により送信された HTTP リクエストを取得すると、情報処理装置 10b-2 (サーバ側通信制御装置) に対して、HTTPS のリクエスト (ClientHello) を送信する (ステップ S303)。これにより、情報処理装置 10b-1 と情報処理装置 10b-2 との間のハンドシェイクが開始される (ステップ S304)。

[0139] 具体的には、情報処理装置 10b-1 が送信する ClientHello には、例えば、TLS のバージョン、及び通信に用いる暗号方式やアルゴリズムのリストを示す情報が含まれる。情報処理装置 10b-2 は、ClientHello に対する応答として、情報処理装置 10b-1 に対し HTTPS のレスポンス (ServerHello) を送信する。情報処理装置 10b-2 が送信する ServerHello には、例えば、ClientHello で提示された選択肢の中で上位装置 22 が選択した情報が含まれる。換言すると、情報処理装置 10b-1 からの提示に対し、情報処理装置 10b-2 が選択を行うことで、通信における具体的な暗号化アルゴリズムが決定される。

[0140] そして、情報処理装置 10b-2 は、暗号化通信に用いる共通鍵に必要な

情報を送る。共通鍵に必要な情報には、例えば、上位装置22に対して発行された公開鍵とその証明書を示す情報、及びIoT機器21-1の公開鍵とその証明書を送ることを要求する情報が含まれる。情報処理装置10b-1は、情報処理装置10b-2に対して、自装置に対して発行された公開鍵とその証明書、及び暗号化通信に用いる共通鍵に必要な情報を送る。

[0141] 情報処理装置10b-1と情報処理装置10b-2との間の相互認証は、例えば次のように行われる。情報処理装置10b-1は、今までに受信したServerHello等から署名を生成し、情報処理装置10b-2に送信する。情報処理装置10b-2は、情報処理装置10b-1から受信した署名を、情報処理装置10b-1から受信した証明書に基づいて検証する。情報処理装置10b-2は、検証が成功すると、その証明書が間違いなく情報処理装置10b-1のものであると判定する。また、情報処理装置10b-2は、今までに受信したClientHello等から署名を生成し、情報処理装置10b-1に送信する。情報処理装置10b-1は、情報処理装置10b-2から受信した署名を、情報処理装置10b-2から受信した証明書に基づいて検証する。情報処理装置10b-1は、検証が成功すると、その証明書が間違いなく情報処理装置10b-2のものであると判定する。

情報処理装置10b-1と情報処理装置10b-2との間の相互認証が正しく行われると、情報処理装置10b-1と情報処理装置10b-2とは、それぞれ暗号化に用いる共通鍵を生成して交換する。

[0142] 情報処理装置10b-2から送付された上位装置22に対して発行された公開鍵とその証明書が、情報処理装置10b-1に許容される証明書であれば、

情報処理装置10b-2は、情報処理装置10b-1から送付された公開鍵とその証明書が、情報処理装置10b-2に許容される証明書であれば、ハンドシェイクを終了する。

[0143] 情報処理装置10b-2は、情報処理装置10b-1とのハンドシェイクが確立されると、上位装置22に対し、HTTPリクエストを送信する（ス

テップS305)。HTTPリクエストは、ステップS301においてIoT機器21-1から送信されるHTTPリクエストである。

[0144] 情報処理装置10b-2により送信されたHTTPリクエストは、上位装置22により受信される(ステップS306)。このとき、上位装置22は、IoT機器21-1からHTTPリクエストが要求されたと認識する。このため、上位装置22は、IoT機器21-1に対するHTTPレスポンスを応答する(ステップS307)。上位装置22が送信したHTTPレスポンスは、情報処理装置10b-2により取得される(ステップS308)。

[0145] 情報処理装置10b-2は、取得した上位装置22からのHTTPレスポンスを、ステップS304のハンドシェイクにおいて決定された共通鍵を用いて暗号化する(ステップS309)。情報処理装置10b-2により暗号化されたHTTPレスポンスは、ネットワークNW1を介して情報処理装置10b-1に受信される(ステップS310)。情報処理装置10b-1は、受信したHTTPレスポンスを、共通鍵を用いて復号する(ステップS311)。情報処理装置10b-1により復号されたHTTPレスポンスは、IoT機器21-1に取得される(ステップS312)。IoT機器21-1は、復号されたHTTPレスポンスを受信する(ステップS313)。このとき、IoT機器21-1は、上位装置22からHTTPレスポンスが応答されたと認識する。このため、IoT機器21-1は、上位装置22に対し、撮像データを送信する(ステップS314)。

[0146] IoT機器21-1が送信した撮像データは、情報処理装置10b-1により取得される(ステップS315)。情報処理装置10b-1は、IoT機器21-1により送信された撮像データを、共通鍵を用いて暗号化する(ステップS316)。情報処理装置10b-1により暗号化された撮像データは、ネットワークNW1を介して情報処理装置10b-2に受信される(ステップS317)。

[0147] 情報処理装置10b-2は、受信した撮像データを、共通鍵を用いて復号

する（ステップS 3 1 8）。情報処理装置 1 0 b - 2 により復号された撮像データは、上位装置 2 2 にとり取得される（ステップS 3 1 9）。上位装置 2 2 は、復号された撮像データを受信する（ステップS 3 2 0）。このとき、上位装置 2 2 は、IoT機器 2 1 - 1 からの撮像データを受信したと認識する。

[0148] なお、上記フローチャートのステップS 3 0 4 において、情報処理装置 1 0 b - 1 と情報処理装置 1 0 b - 2 との間の相互認証が正しく行われなかった場合、情報処理装置 1 0 b - 1 は、通信先との通信を許可しない。具体的には、情報処理装置 1 0 b - 1 は、通信先から送信された情報をIoT機器 2 1 - 1 に出力しない。相互認証が正しく行われなかった場合、通信先が情報処理装置 1 0 b - 2 に見せかけた不正な通信装置である可能性があるためである。この場合、情報処理装置 1 0 b - 1 は、例えば、相互認証が正しく行われなかった場合の通信記録を管理装置 3 0 a に送信するようにしてもよい。これより、管理装置 3 0 a は、相互認証が正しく行われなかった場合の通信記録を取得することができ、管理下にある情報処理装置 1 0 b - 1 に対する不正な通信のパターンや頻度を把握することで、ネットワークNW 1 の異常を監視することができる。

[0149] また、情報処理装置 1 0 b - 1 は、上記図 1 9 に示すステップS 3 0 4 において行われるハンドシェイクにおいて相互認証の代わりにIoT機器 2 1 - 1 に対する通信を許可する通信機器の情報を示す送信先リストに基づいて、通信先との通信を許可するか否かを判定するようにしてもよい。送信先リストに示される通信機器の情報は、例えばURL（Uniform Resource Locator）である。情報処理装置 1 0 b - 1 の情報処理部 1 5 b は、通信先のURLが送信先リストに登録されているURLである場合に当該通信先との通信を許可し、送信先リストに登録されていない場合には通信を許可しない。

[0150] また、情報処理部 1 5 b は、送信先リストを更新するようにしてもよい。情報処理部 1 5 b は、例えば、一定期間にIoT機器 2 1 - 1 に対する通信を許可された通信先のURL、及び許可されなかった通信先URLを記憶さ

せる。そして、情報処理部15bは、例えば、送信先リストに登録されたURLのうち、一定期間に通信が行われた通信先のURLを再度登録する等することにより送信先リストを更新する。あるいは、情報処理装置10b-1は、一定期間に通信を許可された通信先URL、及び許可されなかった通信先URLを管理装置30aに送信するようにしてもよい。この場合、例えば、管理装置30aは、情報処理装置10b-1と通信を行った通信先URLに基づいて、送信先リストを更新するようにしてもよい。管理装置30aにより送信先リストが更新されることで、管理装置30aが管理下にある情報処理装置10b-1と通信する通信機器を一括して管理することができる。

[0151] また、情報処理装置10b-1は、上記図19に示すステップS304において行われるハンドシェイクが確立した後にIoT機器21-1に対して送信された情報（例えば、ファームウェアの更新プログラム）の内容が正しいか否かの検証を行うようにしてもよい。例えば、情報処理装置10b-1の情報処理部15bは、ネットワークNW1を介してIoT機器21-1のファームウェアの更新プログラムが送信された場合、検証用の鍵（検証鍵）を用いて検証する。この場合、管理装置30aは、例えば、情報処理装置10b-1及び情報処理装置10b-2それぞれに検証鍵を送信するようにしてもよい。

[0152] 例えば、情報処理装置10b-2は、IoT機器21-1へ送信する情報（平文）からハッシュ値を生成し、生成したハッシュ値を検証鍵で暗号化する。そして、情報処理装置10b-2は、平文と暗号化したハッシュ値をさらに秘密鍵で暗号してIoT機器21-1へ送信する。また、情報処理装置10b-1は共通鍵を用いて情報を復号化し、平文と暗号化されたハッシュ値とを取得する。

[0153] また、情報処理装置10b-1は、取得した平文からハッシュ値を生成するとともに、暗号化されたハッシュ値を検証鍵で復号する。情報処理装置10b-1は、平文から生成したハッシュ値と、復号化したハッシュ値とが等しい値である場合、IoT機器21-1に対して送信された情報は正しい内

容であると判定する。この場合、情報処理装置10b-1は、復号した情報（平文）をIoT機器21-1に出力する。一方、情報処理装置10b-1は、平文から生成したハッシュ値と復号化したハッシュ値が等しい値でない場合、IoT機器21-1に対して送信された情報は、上位装置22又は情報処理装置10b-2に見せかけた不正な通信装置から送信された不正な情報である可能性があるとして判定する。この場合、情報処理装置10b-1は、復号した情報（平文）をIoT機器21-1に出力しない。

[0154] これにより、IoT機器21-1は、検証済みである正しい内容であることが検証された情報のみを受け取ることができる。また、通常、IoT機器21-1がファームウェアを更新する際の更新プログラムの内容が正しいか否かの判定を行うと考えられるが、IoT機器21-1に代わり情報処理装置10b-2がIoT機器21-1に対して送信された情報の内容を検証することにより、IoT機器21-1の処理負担を軽減させることが可能となる。

なお、本実施形態における情報処理装置10bの縮退機能の動作については、上述した第1の実施形態と同様であるため、ここではその説明を省略する。

[0155] 以上説明したように、本実施形態による情報処理システム1bは、IoT機器21-1とネットワークNW1との間に接続される情報処理装置10b-1と、IoT機器21-1とネットワークNW1との間に接続される情報処理装置10b-2と、を備える。情報処理装置10b-1は、ICカード40と、情報処理部15bを有する。情報処理部15bは、ICカード40に、相互認証と暗号化復号処理とのうち少なくとも一方の処理を依頼し、暗号化された情報を情報処理装置10b-2に送信し、復号された情報をIoT機器21-1に送信する。情報処理装置10b-2は、ICカード40と、情報処理部15bを有する。情報処理部15bは、ICカード40に、相互認証と暗号化復号処理とのうち少なくとも一方の処理を依頼し、暗号化された情報を情報処理装置10b-2に送信し、復号された情報を上位装置2

2に送信する。この場合、情報処理装置10bの情報処理部15bは、ICカード40に相互認証の処理のみをさせてもよいし、暗号化復号処理のみをさせてもよいし、相互認証と暗号化復号処理との両方の処理をさせてもよい。

[0156] これにより、本実施形態による情報処理システム1bは、例えば、社会インフラシステムを変更することなく、社会インフラシステムの安全性を向上させることができる。情報処理装置10b-1から上位装置22に対して送信されたHTTPプロトコルの撮像データ（いわゆる平文）が、情報処理装置10b-1により、例えば、SSL/TLSプロトコルと組み合わせられて、安全性が向上されたHTTPSに置き換えられるためである。また、上位装置22からIoT機器21-1に対して送信された制御データは、暗号化されるが、情報処理装置10b-1により復号されて、IoT機器21-1に受信されるため、IoT機器21-1に復号させる処理を行わせる必要がなく、既存の装置を変更することなくそのまま利用することができる。

[0157] また、本実施形態による情報処理システム1bでは、情報処理装置10b-1と情報処理装置10b-2とが相互認証を行うため、いずれか一方方向のみの認証を行う場合よりも安全性を向上させることができる。一般的なクライアント端末とサーバ端末においては、サーバ端末に対して不特定多数のクライアント端末が通信を行うため、当該不特定多数のクライアント端末に対して正当なクライアント証明書を発行して管理し続けることは現実的ではない。しかしながら、社会インフラシステムにおいては、IoT機器21-1と上位装置22との関係は明確に特定されている。このため、情報処理装置10b-1と情報処理装置10b-2とが相互認証を行うことが可能であり、安全性を向上させることができる。

[0158] また、本実施形態において、SSL/TLSプロトコルを用いたセキュアな通信を常時行うようにしてもよいし、SSL/TLSプロトコルを用いた通信を行うか否かを選択可能にしてもよい。また、IoT機器21-1（クライアント装置）と上位装置22（サーバ装置）との間における双方向の通

信のうち一方の方向の通信のみをSSL/TLSプロトコルを用いた通信としてもよい。また、SSL/TLSプロトコルを用いたセキュアな通信を常時行うようにしてもよいし、SSL/TLSプロトコルを用いた通信を行うか否かを選択可能にしてもよい。

[0159] また、SSL／TLSプロトコルを用いた通信を常時行うようにすることで、情報処理装置10bにより認証された正当な情報処理装置10bとは異なる装置からの通信を遮断することができる。このため、IoT機器21-1（クライアント装置）や上位装置22（サーバ装置）に対する不正なアクセスや、IoT機器21-1（クライアント装置）や上位装置22（サーバ装置）がマルウェアに感染することを抑止することができる。

[0160] また、本実施形態の情報処理システム１ｂにおいて、情報処理装置１０ｂは、定期的に、自装置が接続されているＩＯＴ機器２１－１（クライアント装置）又は上位装置２２（サーバ装置）との接続が維持されているか否かを確認するようにしてもよい。この場合、管理装置３０ａに接続状態を示す情報が送信されるようにしてもよい。管理装置３０ａは、情報処理装置１０ｂから接続状態を示す情報が受信できない場合などには、情報処理装置１０ｂがＩＯＴ機器２１－１（クライアント装置）又は上位装置２２（サーバ装置）から切り離された判断し、当該切り離された情報処理装置１０ｂを無効とする。こうすることで管理装置３０ａは、切り離された情報処理装置１０ｂが不正な装置に接続されてなりすましに悪用されることを抑制する。

[0161] また、本実施形態の情報処理システム１ｂにおいて、上位装置２２（サーバ装置）や管理装置３０ａ等から、情報処理装置１０ｂを介して、ＩＯＴ機器２１－１（クライアント装置）のプログラムを更新させるようにしてもよい。情報処理装置１０ｂを介してプログラムの更新（ファームウェアのアップデート）が行われることにより、安全にＩＯＴ機器２１－１（クライアント装置）の機能を更新させることができる。このように上位装置２２（サーバ装置）からＩＯＴ機器２１－１（クライアント装置）に対してファームウェアが送信される場合、上位装置２２（サーバ装置）から送信されるファー

ムウェアには、例えば情報処理装置 10b-2（サーバ側通信制御装置）により暗号化された上位装置 22（サーバ装置）の署名が付与される。

[0162] この場合、IoT機器 21-1（クライアント装置）では、情報処理装置 10b-1（クライアント側通信制御装置）により署名が復号されることにより、送信されたファームウェアが間違いなく上位装置 22（サーバ装置）から送信されたファームウェアであると判定することができる。これにより、あたかも上位装置 22（サーバ装置）であるかのように装う不正な端末から、不正なファームウェアがIoT機器 21-1（クライアント装置）に送信されてしまった場合であっても、IoT機器 21-1（クライアント装置）に対し不正なファームウェアに基づく誤った更新がなされてしまうことを排除することができる。

[0163] また、本実施形態の情報処理システム 1bにおいて、上位装置 22（サーバ装置）や管理装置 30a等から、情報処理装置 10bを介して、IoT機器 21-1（クライアント装置）の起動や停止を行ってもよい。情報処理装置 10bを介して起動や停止（リモートアクティベーション）が行われることにより、安全にIoT機器 21-1（クライアント装置）の機能を更新させることができ、セキュアな遠隔制御を実現させることができる。

[0164] また、本実施形態の情報処理システム 1bにおいては、IoT機器 21-1（クライアント装置）、及び上位装置 22（サーバ装置）が有線により通信する場合を例に説明したが、これに限定されることはない。IoT機器 21-1（クライアント装置）、及び上位装置 22（サーバ装置）のうち少なくともいずれかが無線LAN等により無線通信を行う装置であってもよい。例えば、IoT機器 21-1（クライアント装置）が無線通信により上位装置 22（サーバ装置）と通信を行う場合、情報処理装置 10b-1は、無線による通信機能を有し、IoT機器 21-1（クライアント装置）により送信されるデータを暗号化し、暗号化したデータを、無線通信により上位装置 22（サーバ装置）に送信する。

[0165] また、本実施形態の情報処理システム 1bにおいて、情報処理装置 10b

ー 1 が情報処理装置 10b-2 と通信を行う例を説明したが、情報処理装置 10b-1 の通信先はこれに限定されることはない。例えば、情報処理装置 10b-1 は、情報処理装置 10b-3 と通信を行ってもよい。情報処理装置 10b-1 は、情報処理装置 10b-3 から通信開始の合図を受信した場合、まず情報処理装置 10b-3 との間で相互認証を行い、情報処理装置 10b-3 が正当な通信端末であることを確認する。そして、相互認証が正しく行われた場合、情報処理装置 10b-1 は、情報処理装置 10b-3 から受信した情報を IoT 機器 21-1 に出力する。暗号を使用して送信データに認証子が付与されることにより、通信情報の改ざんの検出及び送信者の特定が可能となる。このため、本実施形態の情報処理システム 1b では、情報処理装置 10b 同士の通信において、「正しい相手から」、「改ざんされていないデータを受け取る」ことを確実にすることができる。

[0166] なお、上記の各実施形態において、暗号処理部 152 は、HSM (Hardware Security Module)、SAM (Secure Application Module)、上述した IC カード 40 などを使用するようにしてもよい。例えば、暗号処理部 152 は、IC カード 40 などを使用して着脱可能に構成されてもよい。

[0167] また、上記の各実施形態において、一例として、IoT 機器 21-1 と上位装置 22 との間の通信に、情報処理装置 10 (10a、10b) を適用する例を説明したが、これに限定されるものではない。情報処理装置 10 (10a、10b) は、例えば、IoT 機器 21-1 と IoT 機器 21-2 との間の通信に、情報処理装置 10 (10a、10b) に適用してもよいし、他の末端装置 20 間の通信に適用してもよい。

[0168] また、上記の各実施形態において、情報処理部 15 (15a、15b) は、通信情報記憶部 142 が記憶する相手先の情報処理装置 10 (10a、10b) との通信情報に基づいて、パススルーモードであるか否かを検出する例を説明したが、これに限定されるものではない。例えば、通信情報記憶部 142 が、相手先の情報処理装置 10 (10a、10b) が接続されている末端装置 20 との通信情報を記憶し、情報処理部 15 (15a、15b) は

、末端装置 20 との通信情報に基づいて、パススルーモードであるか否かを検出するようにしてもよい。すなわち、情報処理部 15 (15 a、15 b) は、現在の通信における通信情報が、末端装置 20 との通信情報に一致した場合に、相手先の情報処理装置 10 (10 a、10 b) がパススルーモードになったと判定するようにしてもよい。

[0169] また、情報処理部 15 (15 a、15 b) は、通信情報記憶部 142 が記憶する通信情報を利用して、例えば、第三者からのなりすましや改ざんなどの攻撃、マルウェアやウイルスの感染、等の異常を検出するようにしてもよい。

[0170] また、上記の各実施形態において、複数のパラメータに対応する通信リスクを用いる場合に、情報処理部 15 (15 a、15 b) が、多数決、又は最も高い通信リスクを全体リスクとして決定する例を説明したが、これに限定されるものではない。情報処理部 15 (15 a) は、例えば、通信リスクの平均値に基づいて全体リスクを決定してもよいし、重み付けを付加した合計値又は平均値から全体リスクを決定してもよい。

[0171] また、上記の各実施形態において、切替部の一例として、フォトリレースイッチ 13 を用いる例を説明したが、ノーマリクローズの接続であり、電源の供給が停止した場合に、オン状態を維持できるスイッチであれば、他のスイッチであってもよい。

また、上記の第 3 の実施形態は、第 1 の実施形態の情報処理システム 1 に適用する例を説明したが、第 2 の実施形態に適用するようにしてもよい。

[0172] 以上説明した少なくともひとつの実施形態によれば、少なくとも通信 I / F 部 11 が末端装置 20 から情報を受信した場合に、受信した情報を暗号化して通信 I / F 部 12 を介してネットワーク NW1 に送信し、少なくとも通信 I / F 部 12 がネットワーク NW1 から情報を受信した場合に、受信した情報を復号して通信 I / F 部 11 を介して末端装置 20 に送信する情報処理部 15 と、情報処理部 15 が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、通信 I / F 部 11 の末端装置 20 との通信線と、通信

I/F部12のネットワークNW1との通信線とを直接接続し、末端装置20とネットワークNW1との間で、情報処理部15を介さずに直接通信するパススルーモードに切り替えるフォトリレースイッチ13（切替部）とを持つことにより、セキュリティを確保しつつ、可用性を向上させることができる。

[0173] 上記実施形態は、以下のように表現することができる。

ネットワークに接続される末端の装置である末端装置に接続し、前記末端装置との間で通信可能な第1通信部と、

ネットワークに接続し、前記ネットワークを介して前記ネットワークに接続された装置と通信可能な第2通信部と、

少なくともコンピュータが実行可能なプログラムを記憶する記憶部と、

前記記憶部に記憶されたプログラムを実行するハードウェアプロセッサと

、

前記ハードウェアプロセッサが、少なくとも電源の供給停止を含む動作不能な状態になった場合に、前記第1通信部の前記末端装置との通信線と、前記第2通信部の前記ネットワークとの通信線とを直接接続し、前記末端装置と前記ネットワークとの間で、前記情報処理部を介さずに直接通信するパススルーモードに切り替えるスイッチと、を備え、

前記ハードウェアプロセッサは、前記プログラムを実行することにより、

少なくとも前記第1通信部が前記末端装置から情報を受信した場合に、受信した情報を暗号化して前記第2通信部を介して前記ネットワークに送信し、少なくとも前記第2通信部が前記ネットワークから暗号化された情報を受信した場合に、受信した情報を復号して前記第1通信部を介して前記末端装置に送信する処理を行う

ように構成されている、情報処理装置。

[0174] なお、実施形態における情報処理システム1（1a）及び情報処理装置10（10a）が備える各構成の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログ

ラムをコンピュータシステムに読み込ませ、実行することにより上述した情報処理システム 1 (1 a) 及び情報処理装置 10 (10 a) が備える各構成における処理を行ってもよい。ここで、「記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行する」とは、コンピュータシステムにプログラムをインストールすることを含む。ここでいう「コンピュータシステム」とは、OS や周辺機器等のハードウェアを含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM、CD-ROM 等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

[0175] 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同様に、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ものである。

請求の範囲

- [請求項1] ネットワークに接続される末端の装置である末端装置に接続し、前記末端装置との間で通信可能な第1通信部と、
- ネットワークに接続し、前記ネットワークを介して前記ネットワークに接続された装置と通信可能な第2通信部と、
- 少なくとも前記第1通信部が前記末端装置から情報を受信した場合に、受信した情報を暗号化して前記第2通信部を介して前記ネットワークに送信し、少なくとも前記第2通信部が前記ネットワークから暗号化された情報を受信した場合に、受信した情報を復号して前記第1通信部を介して前記末端装置に送信する情報処理部と、
- 前記情報処理部が、少なくとも電源の供給停止を含む動作不能な状態になった場合に、前記第1通信部の前記末端装置との通信線と、前記第2通信部の前記ネットワークとの通信線とを直接接続し、前記末端装置と前記ネットワークとの間で、前記情報処理部を介さずに直接通信するパススルーモードに切り替える切替部と
- 備える情報処理装置。
- [請求項2] 前記情報処理部は、
- 前記ネットワークを介して前記末端装置が通信する相手先の前記末端装置である相手先末端装置と前記ネットワークとの間に接続され、前記第1通信部、前記第2通信部、前記情報処理部、及び前記切替部を備える相手先の情報処理装置が、前記パススルーモードになった場合に、前記相手先の情報処理装置との通信状態に関するパラメータに基づいて、所定の期間、前記相手先末端装置との通信を許容し、前記所定の期間の経過後に、前記相手先末端装置との通信を制限する
- 請求項1に記載の情報処理装置。
- [請求項3] 前記情報処理部は、
- 前記パラメータの値と、通信リスクとを対応付けて記憶する通信リスク記憶部から、前記相手先の情報処理装置に対応する前記パラメータ

タの値に基づいて取得した、前記相手先末端装置に対する前記通信リス
クに基づいて、前記所定の期間を決定する

請求項 2 に記載の情報処理装置。

[請求項4] 前記パラメータには、前記相手先の情報処理装置との通信実績が含ま
れ、

前記情報処理部は、前記通信実績に基づいて、前記所定の期間を決
定する

請求項 2 又は請求項 3 に記載の情報処理装置。

[請求項5] 前記パラメータには、前記相手先の情報処理装置における前記パス
スルーモードが解除されるまでの復旧見込み時間が含まれ、

前記情報処理部は、前記復旧見込み時間に基づいて、前記所定の期
間を決定する

請求項 2 から請求項 4 のいずれか一項に記載の情報処理装置。

[請求項6] 前記パラメータには、前記ネットワークにおける攻撃の容易性を示
す攻撃容易性情報が含まれ、

前記情報処理部は、前記攻撃容易性情報に基づいて、前記所定の期
間を決定する

請求項 2 から請求項 5 のいずれか一項に記載の情報処理装置。

[請求項7] 前記情報処理部は、前記相手先の情報処理装置との通信における通
信方式、認証方式、及び前記相手先の識別情報のうちの少なくとも 1
つに基づいて、前記相手先の情報処理装置が前記パススルーモードに
なったか否かを検出する

請求項 2 から請求項 6 のいずれか一項に記載の情報処理装置。

[請求項8] 前記相手先の情報処理装置との通信における通信方式、認証方式、
及び前記相手先の識別情報のうちの少なくとも 1 つを含む通信情報を
記憶する通信情報記憶部を備え、

前記情報処理部は、前記通信情報記憶部が記憶する前記通信情報に
基づいて、前記相手先の情報処理装置が前記パススルーモードになっ

たか否かを検出する

請求項 7 に記載の情報処理装置。

[請求項9]

複数の末端装置と、

請求項 1 から請求項 8 のいずれか一項に記載の情報処理装置であって、前記複数の末端装置のそれぞれと前記ネットワークとの間にそれぞれが接続される複数の情報処理装置と

を備える情報処理システム。