(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5192980号
(P5192980)
(45)発行日　平成25年5月8日(2013.5.8)　(24)登録日　平成25年2月8日(2013.2.8)

(51)Int.Cl.　　F I
G06F 21/50 (2013.01)　　G06F 21/00 150
G06F 13/00 (2006.01)　　G06F 13/00 358A
　　G06F 13/00 510A

請求項の数 8　(全 14 頁)

(21)出願番号　特願2008-269063(P2008-269063)
(22)出願日　平成20年10月17日(2008.10.17)
(65)公開番号　特開2010-97499(P2010-97499A)
(43)公開日　平成22年4月30日(2010.4.30)
審査請求日　平成23年5月19日(2011.5.19)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100087767
弁理士　西川　惠清
(72)発明者　河崎　利信
大阪府門真市大字門真１０４８番地　パナソニック電工株式会社内
(72)発明者　福田　尚弘
大阪府門真市大字門真１０４８番地　パナソニック電工株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】ネットワークシステム

(57)【特許請求の範囲】
【請求項１】
それぞれセキュリティレベルに関するサーバ属性情報を保持した複数台のセキュリティ管理サーバと、セキュリティ属性情報を保持したデバイスとをネットワーク上に備え、デバイスは、ネットワーク上に存在するセキュリティ管理サーバを検出するサーバ検出手段と、自己のセキュリティ属性情報とサーバ検出手段で検出された各セキュリティ管理サーバのサーバ属性情報とを比較することで、最も高いセキュリティレベルを実現できるセキュリティ管理サーバを選択して当該セキュリティ管理サーバが持つセキュリティ情報を取得するサーバ選択手段とを有することを特徴とするネットワークシステム。
【請求項２】
前記サーバ属性情報として、前記セキュリティ管理サーバに設定されている暗号鍵の種別を用いることを特徴とする請求項１記載のネットワークシステム。
【請求項３】
前記サーバ属性情報として、前記セキュリティ管理サーバにおける暗号鍵の生成過程の種別を用いることを特徴とする請求項１記載のネットワークシステム。
【請求項４】
前記サーバ選択手段は、前記ネットワーク上の前記セキュリティ管理サーバの増減を検知すると、セキュリティ管理サーバを再選択することを特徴とする請求項１ないし請求項３のいずれか１項に記載のネットワークシステム。
【請求項５】

前記ネットワーク上に追加された前記セキュリティ管理サーバは、自己の前記サーバ属性情報を前記デバイスに通知し、前記サーバ選択手段は、サーバ属性情報の通知を受けてネットワーク上のセキュリティ管理サーバの増加を検知することを特徴とする請求項４記載のネットワークシステム。

【請求項６】

前記サーバ選択手段は、前記ネットワーク上の前記セキュリティ管理サーバの持つ前記サーバ属性情報の変更を検知し、セキュリティ管理サーバを再選択することを特徴とする請求項１ないし請求項５のいずれか１項に記載のネットワークシステム。

【請求項７】

前記サーバ属性情報が変更された前記セキュリティ管理サーバは、自己の変更後のサーバ属性情報を前記デバイスに通知し、前記サーバ選択手段は、サーバ属性情報の通知を受けて前記ネットワーク上のセキュリティ管理サーバの持つサーバ属性情報の変更を検知することを特徴とする請求項６記載のネットワークシステム。

【請求項８】

前記デバイスは、前記セキュリティ管理サーバとの通信信頼性を評価するサーバ管理手段を有し、前記サーバ選択手段は、最も高いセキュリティレベルを実現できるセキュリティ管理サーバが前記ネットワーク上に複数台存在する場合に、当該複数台のセキュリティ管理サーバの中でサーバ管理手段での評価値が最も高いセキュリティ管理サーバを選択することを特徴とする請求項１ないし請求項７のいずれか１項に記載のネットワークシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク上のデバイスとセキュリティ管理サーバとを用いてセキュアな通信環境を実現するネットワークシステムに関するものである。

【背景技術】

【０００２】

従来、この種のネットワークシステムにおいて、図１０に示すようにデバイスＤ１が利用するセキュリティ管理サーバＳＡは固定的に決められており、デバイスの追加などシステム構成に変化が生じた場合には、セキュリティ管理サーバＳＡのメンテナンスを行うことでセキュリティレベルを維持する。つまり、セキュリティ管理サーバＳＡの設定データ（セキュリティポリシー）を動的に適用可能とすれば、高いセキュリティレベルを維持することができる（たとえば特許文献１参照）。

【０００３】

また、ユーザやデバイスごとにセキュリティレベルを変えることも考えられているが（たとえば特許文献２参照）、このような場合であっても、高いセキュリティレベルを維持するためには、セキュリティ管理サーバのメンテナンスが必要となる。

【０００４】

ここで、セキュリティレベルとセキュリティ管理サーバＳＡのメンテナンス工数とはトレードオフの関係にあり、たとえば図１０のようにセンターサーバ上にセキュリティ管理サーバＳＡが設けられている場合には、セキュリティ管理サーバＳＡのメンテナンスは容易に行えるものの、各デバイス固有の暗号鍵を用いるなどしてセキュリティレベルを高く設定する必要がある。

【０００５】

これに対して、図１１に示す住宅設備システムのように、ユーザ宅内に構築された閉鎖的なネットワーク（宅内ＬＡＮ）上にデバイスＤ１およびセキュリティ管理サーバＳＢが存在するネットワークシステムにおいては、セキュリティ管理サーバＳＢに対して外部（ユーザ宅外）から容易にアクセスすることができないため、セキュリティ管理サーバＳＢのメンテナンスを容易に行うことはできないが、複数台のデバイスに共通の暗号鍵を用い

るなどしてセキュリティレベルを低く設定することが可能である。
【特許文献１】特開２００５－２５２９４７号公報
【特許文献２】特開平８－２９７６３８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
ところで、たとえば宅内ＬＡＮ等の閉鎖的なネットワーク上に構築したネットワークシステムを拡張してインターネットに接続可能とする場合のように、システム構成に変化が生じた場合には、通信の安全性が変化することがある。たとえば、セキュリティレベルの低い宅内のセキュリティ管理サーバＳＢを利用していたデバイスがインターネットに接続されるようになると、当該デバイスに対してインターネット上の不特定の端末からアクセスを試みることが可能となるため、通信の安全性が低下することとなる。この場合、デバイスの設定を変更することにより、デバイスが利用するセキュリティ管理サーバを切り替えてセキュリティレベルの向上を図る必要がある。
【０００７】
しかし、このような場合に、デバイスが利用するセキュリティ管理サーバの選択をユーザが行う必要があるため、よりセキュリティレベルの高いセキュリティ管理サーバを見分ける知識のない一般的なユーザでは、最適なセキュリティレベルを実現することは困難である。
【０００８】
本発明は上記事由に鑑みてなされたものであって、ユーザに特別な知識がない場合でも、最適なセキュリティレベルを実現することができるネットワークシステムを提供することを目的とする。
【課題を解決するための手段】
【０００９】
請求項１の発明では、それぞれセキュリティレベルに関するサーバ属性情報を保持した複数台のセキュリティ管理サーバと、セキュリティ属性情報を保持したデバイスとをネットワーク上に備え、デバイスは、ネットワーク上に存在するセキュリティ管理サーバを検出するサーバ検出手段と、自己のセキュリティ属性情報とサーバ検出手段で検出された各セキュリティ管理サーバのサーバ属性情報とを比較することで、最も高いセキュリティレベルを実現できるセキュリティ管理サーバを選択して当該セキュリティ管理サーバが持つセキュリティ情報を取得するサーバ選択手段とを有することを特徴とする。
【００１０】
この構成によれば、デバイスは、サーバ検出手段でネットワーク上のセキュリティ管理サーバを検出し、サーバ選択手段にて自己のセキュリティ属性情報と各セキュリティ管理サーバのサーバ属性情報とを比較することで、最も高いセキュリティレベルを実現可能なセキュリティ管理サーバを選択して利用するから、ユーザがセキュリティ管理サーバの選択をすることなく、最適なセキュリティレベルを実現することができる。すなわち、デバイス自身が、最適なセキュリティレベルを実現可能なセキュリティ管理サーバを選択して利用するから、ユーザに特別な知識がない場合でも、最適なセキュリティレベルを実現できるという利点がある。なお、セキュリティ管理サーバが持つセキュリティ情報には、デバイス間でセキュアな通信を行うために必要なセッション鍵や、デバイス間での書き込みの可否等を示すアクセス制限情報などが含まれる。
【００１１】
請求項２の発明は、請求項１の発明において、前記サーバ属性情報として、前記セキュリティ管理サーバに設定されている暗号鍵の種別を用いることを特徴とする。
【００１２】
この構成によれば、デバイスのサーバ選択手段は、暗号鍵の種別に基づいてセキュリティ管理サーバを選択するから、暗号鍵の種別の違いによってセキュリティ管理サーバ間でセキュリティレベルに差がある場合に、セキュリティレベルの最も高いセキュリティ管理

サーバを選択して利用することができる。なお、暗号鍵の種別には、暗号鍵の鍵長や、暗号鍵の適用範囲などが含まれる。

【００１３】

請求項３の発明は、請求項１の発明において、前記サーバ属性情報として、前記セキュリティ管理サーバにおける暗号鍵の生成過程の種別を用いることを特徴とする。

【００１４】

この構成によれば、デバイスサーバ選択手段は、暗号鍵の生成過程の種別に基づいてセキュリティ管理サーバを選択するから、暗号鍵の生成過程の種別の違いによってセキュリティ管理サーバ間でセキュリティレベルに差がある場合に、セキュリティレベルの最も高いセキュリティ管理サーバを選択して利用することができる。なお、暗号鍵の生成過程の種別には、暗号鍵の生成に用いる乱数の精度などが含まれる。

【００１５】

請求項４の発明は、請求項１ないし請求項３のいずれかの発明において、前記サーバ選択手段が、前記ネットワーク上の前記セキュリティ管理サーバの増減を検知すると、セキュリティ管理サーバを再選択することを特徴とする。

【００１６】

この構成によれば、セキュリティ管理サーバがネットワーク上に追加されたりネットワーク上から離脱したりすることによって、ネットワーク上のセキュリティ管理が増減した場合でも、サーバ選択手段が自動的にセキュリティ管理サーバを再選択することにより最適なセキュリティレベルを実現することができる。

【００１７】

請求項５の発明は、請求項４の発明において、前記ネットワーク上に追加された前記セキュリティ管理サーバが、自己の前記サーバ属性情報を前記デバイスに通知し、前記サーバ選択手段が、サーバ属性情報の通知を受けてネットワーク上のセキュリティ管理サーバの増加を検知することを特徴とする。

【００１８】

この構成によれば、ネットワーク上に複数台のデバイスがある場合に、ネットワーク上にセキュリティ管理サーバが追加されたとしても、セキュリティ管理サーバから前記複数台のデバイスに対してサーバ属性情報が通知されることになるので、前記複数台のデバイスからセキュリティ管理サーバへのアクセスが集中することを回避でき、ネットワーク上の通信トラフィックを低減できるという利点がある。

【００１９】

請求項６の発明は、請求項１ないし請求項５のいずれかの発明において、前記サーバ選択手段が、前記ネットワーク上の前記セキュリティ管理サーバの持つ前記サーバ属性情報の変更を検知し、セキュリティ管理サーバを再選択することを特徴とする。

【００２０】

この構成によれば、サーバ検出手段にて既に検出されているセキュリティ管理サーバにおいてサーバ属性情報の変更があった場合に、サーバ選択手段は、変更後のサーバ属性情報に基づいて自動的にセキュリティ管理サーバを再選択することにより最適なセキュリティレベルを実現することができる。

【００２１】

請求項７の発明は、請求項６の発明において、前記サーバ属性情報が変更された前記セキュリティ管理サーバが、自己の変更後のサーバ属性情報を前記デバイスに通知し、前記サーバ選択手段が、サーバ属性情報の通知を受けて前記ネットワーク上のセキュリティ管理サーバの持つサーバ属性情報の変更を検知することを特徴とする。

【００２２】

この構成によれば、ネットワーク上に複数台のデバイスがある場合に、ネットワーク上のセキュリティ管理サーバの持つサーバ属性情報が変更されたとしても、セキュリティ管理サーバから前記複数台のデバイスに対して変更後のサーバ属性情報が通知されることになるので、前記複数台のデバイスからセキュリティ管理サーバへのアクセスが集中するこ

とを回避でき、ネットワーク上の通信トラフィックを低減できるという利点がある。

【００２３】

請求項８の発明は、請求項１ないし請求項７のいずれかの発明において、前記デバイスが、前記セキュリティ管理サーバとの通信信頼性を評価するサーバ管理手段を有し、前記サーバ選択手段が、最も高いセキュリティレベルを実現できるセキュリティ管理サーバが前記ネットワーク上に複数台存在する場合に、当該複数台のセキュリティ管理サーバの中でサーバ管理手段での評価値が最も高いセキュリティ管理サーバを選択することを特徴とする。

【００２４】

この構成によれば、デバイスは、セキュリティ管理サーバとの通信信頼性の評価値をサーバ属性情報に加味してセキュリティ管理サーバを選択するので、セキュリティレベルが高くても通信状況が不安定なセキュリティ管理サーバは選択の対象から外されることとなり、結果的に、セキュリティレベルの運用が不安定になることを回避できるという利点がある。

【発明の効果】

【００２５】

本発明は、デバイス自身が、最適なセキュリティレベルを実現可能なセキュリティ管理サーバを選択して利用するから、ユーザに特別な知識がない場合でも、最適なセキュリティレベルを実現できるという利点がある。

【発明を実施するための最良の形態】

【００２６】

（実施形態１）

本実施形態のネットワークシステムは、図１に示すように、ユーザ宅内に設置された設備機器からなるデバイスＤ１と、それぞれセキュリティ管理サーバとして機能する宅内サーバＳ１およびバックアップ用宅内サーバＳ２とをネットワークとしての宅内ＬＡＮ上に備えた住宅設備システムからなる。このネットワークシステムでは、デバイスＤ１同士あるいは宅内サーバＳ１－デバイスＤ１間で通信を行うことにより、デバイスＤ１の制御や監視などデバイスＤ１を管理することが可能である。

【００２７】

デバイスＤ１は、図２に示すように、ネットワークに接続される通信手段１と、ネットワーク上のセキュリティ管理サーバを検出するサーバ検出手段２と、サーバ検出手段２を起動するためのトリガ信号を生成する検出トリガ手段３と、サーバ検出手段２で検出されたセキュリティ管理サーバの中から最適なセキュリティレベルを実現可能なセキュリティ管理サーバを選択するサーバ選択手段４と、セキュリティ管理サーバとの通信信頼性を評価するサーバ管理手段５と、セキュリティ属性情報を保持する情報保持手段６とを有している。

【００２８】

デバイスＤ１の情報保持手段６に保持されているセキュリティ属性情報は、デバイスＤ１自身が現在利用可能なセキュリティレベルに関する情報であって、ここでは「宅内共通の暗号鍵あり」と「機器固有の暗号鍵あり」との２つの情報を含んでいる。

【００２９】

宅内サーバＳ１およびバックアップ用宅内サーバＳ２は、それぞれ図３に示すように（図３では宅内サーバＳ１を例示する）、ネットワークに接続される通信手段７と、セキュリティ管理サーバとしての機能を実現するためのセキュリティ管理手段８と、セキュリティ管理サーバとしてのサーバ属性情報を保持する情報保持手段９と、情報保持手段９内のサーバ属性情報を管理するデータ管理手段１０と、サーバ属性情報の設定を変更する設定変更手段１１とを有している。

【００３０】

宅内サーバＳ１の情報保持手段９に保持されているサーバ属性情報は、ネットワーク上のデバイスＤ１に適用するセキュリティレベルに関する情報であって、ここでは「セキュ

リティレベル：中」、「宅内共通の暗号鍵を使用」、「暗号鍵の鍵長：２５６ｂｉｔ」、「乱数の精度は高い」の４つの情報を含んでいる。

【００３１】

同様に、バックアップ用宅内サーバＳ２の情報保持手段９に保持されているサーバ属性情報は、「セキュリティレベル：低」、「宅内共通の暗号鍵を使用」、「暗号鍵の鍵長：１２８ｂｉｔ」、「乱数の精度は低い」の４つの情報を含んでいる。

【００３２】

ここで、「暗号鍵の鍵長」は、ネットワークシステムで使用する暗号鍵の種別、具体的には暗号鍵のビット長を示すものであって、鍵長が長い（ビット数が多い）程セキュリティレベルが高いことを意味する。暗号鍵の種別としては、鍵長の他に、暗号鍵が機器（デバイス）固有の暗号鍵、あるいは宅内のデバイス間で予め決められたグループ内で共通の暗号鍵、若しくは宅内共通の暗号鍵のいずれであるかも規定され、通信の安全性は暗号鍵の適用範囲が広くなるほど、つまり機器固有、グループ内共通、宅内共通の順に低くなる。したがって、セキュリティレベルを高める場合には暗号鍵の適用範囲を狭めることが望ましい。なお、機器固有の暗号鍵とする場合には、たとえば暗号化に公開鍵を使用し、復号化に前記機器固有の暗号鍵を秘密鍵として使用する公開鍵暗号方式がデバイス間の通信に適用される。

【００３３】

また、「乱数の精度」は、暗号鍵の生成過程の種別、具体的には暗号鍵の生成過程において用いられる乱数の精度を示すものであって、精度が高い程セキュリティレベルが高いことを意味する。

【００３４】

以下では、本実施形態のネットワークシステムの動作例について図１および図４、図５を参照して説明する。

【００３５】

デバイスＤ１は、電源が投入されて起動したことを検出トリガ手段３で検知すると、検出トリガ手段３でトリガ信号を生成し、当該トリガ信号を受け取ったサーバ検出手段２によりネットワーク（宅内ＬＡＮ）上のセキュリティ管理サーバの検索を開始する。このとき、図１の例では宅内サーバＳ１とバックアップ用宅内サーバＳ２との２つのセキュリティ管理サーバが検出される。

【００３６】

それから、デバイスＤ１は検出した各セキュリティ管理サーバ（宅内サーバＳ１およびバックアップ用宅内サーバＳ２）の持つサーバ属性情報をそれぞれ取得して、各セキュリティ管理サーバが自己の利用可能なセキュリティ管理サーバか否かを判断する。ここで、デバイスＤ１は、セキュリティ情報として宅内共通の暗号鍵を有しているため、宅内サーバＳ１とバックアップ用宅内サーバＳ２との両方が利用可能と判断する。

【００３７】

そして、デバイスＤ１は利用可能と判断したセキュリティ管理サーバの中で最もセキュリティレベルの高いセキュリティ管理サーバを、対象サーバとしてサーバ選択手段４で選択する。ここでは、サーバ属性情報内の「セキュリティレベル」が「中」に設定されている宅内サーバＳ１が対象サーバとして選択される。

【００３８】

このように対象サーバとして選択されたセキュリティ管理サーバは、デバイス間でセキュアな通信を行うために必要なセッション鍵（暗号鍵）の生成や、デバイス間での書き込みの可否等を示すアクセス制限情報（パーミッション情報）の設定または生成を自己のサーバ属性情報に従って行う。要するに、サーバ属性情報では、当該セキュリティ管理サーバで生成されるセッション鍵やアクセス制限情報のセキュリティレベルを管理しているのであって、たとえば、「乱数の精度」が高くなるほどセキュリティレベルの高い（つまり、通信の安全性の高い）セッション鍵を生成することが可能となり、また、「セキュリティレベル」が高くなるほどアクセス制限情報を細かく設定することが可能となる。デバイ

スＤ１は、対象サーバとして選択したセキュリティ管理サーバから、上述のセッション鍵やアクセス制限情報などを含むセキュリティ情報を取得し、これらのセキュリティ情報を用いて通信を開始する。

【００３９】

ただし、対象サーバの判断基準は「セキュリティレベル」に限らずサーバ属性情報に含まれている情報であればよく、たとえばサーバ属性情報内の「暗号鍵の鍵長」を比較して、「暗号鍵の鍵長」が「２５６ｂｉｔ」である宅内サーバＳ１を対象サーバとして選択するようにしてもよい。また、セキュリティ管理サーバが暗号鍵を生成する過程において使用する「乱数の精度」を比較して、「乱数の精度」が「高い」に設定されているセキュリティ管理サーバ（ここでは宅内サーバＳ１）を対象サーバに選択することも考えられる。サーバ属性情報内のいずれの項目を対象サーバの選択時の判断基準に用いるかは、デバイスＤ１の情報保持手段６に保持されているセキュリティ属性情報にて規定することができる。すなわち、セキュリティ属性情報においては、たとえば「暗号鍵の鍵長」についてはビット長が長い程セキュリティレベルが高いものと判断し、ビット長が短い程セキュリティレベルが低いものと判断するように、セキュリティレベルの判断時の条件が規定される。

【００４０】

ここにおいて、デバイスＤ１は、電源投入後、一定周期でネットワーク上のセキュリティ管理サーバの検索を繰り返し行う。つまり、検出トリガ手段３が一定の周期でトリガ信号を生成しサーバ検出手段２に与えることにより、サーバ検出手段２は前記一定周期でセキュリティ管理サーバの検索を行うこととなる。このとき、ネットワーク上のセキュリティ管理サーバの台数が増減することによりシステム構成自体が変化していると、サーバ選択手段４はシステム構成の変化後のセキュリティ管理サーバを対象として、対象サーバを再度選択する。なお、この構成に限らず、たとえばデバイスＤ１に備わるスイッチ（図示せず）等の操作により、ユーザが任意のタイミングでトリガ信号をサーバ検出手段２に与えてネットワーク上のセキュリティ管理サーバの検索を開始するようにしてもよい。

【００４１】

しかして、デバイスＤ１が対象サーバとして宅内サーバＳ１を選択している状態で、たとえば図４に示すように宅内サーバＳ１が動作を停止してネットワークから切り離された（離脱した）場合には、デバイスＤ１は、一定周期でネットワーク上のセキュリティ管理サーバを再検索した際に、宅内サーバＳ１が離脱していることを検知し、ネットワーク上に残ったセキュリティ管理サーバの中で最もセキュリティレベルの高いセキュリティ管理サーバ（ここではバックアップ用宅内サーバＳ２）を対象サーバとして選択し利用（対象サーバが持つセキュリティ情報を取得）する。

【００４２】

また、ネットワーク上のいずれかのセキュリティ管理サーバのメンテナンスが行われ、当該セキュリティ管理サーバの情報保持手段９に格納されているサーバ属性情報が設定変更された場合（つまりサーバ属性情報が書き換えられた場合）には、デバイスＤ１は、サーバ選択手段４にて変更後のサーバ属性情報を比較することで対象サーバを再選択する。要するに、デバイスＤ１は、サーバ検出手段２がネットワーク上のセキュリティ管理サーバを検出する度に、各セキュリティ管理サーバのサーバ属性情報を取得し、当該サーバ属性情報を前回のセキュリティ管理サーバ検出時に取得したサーバ属性情報と比較することで、サーバ属性情報の変更の有無を判断する。そして、サーバ属性情報が変更されていれば、変更後のサーバ属性情報を用いて再度対象サーバを選択する。

【００４３】

すなわち、デバイスＤ１が対象サーバとして宅内サーバＳ１を選択している状態で、たとえば図５に示すようにバックアップ用宅内サーバＳ２のサーバ属性情報が設定変更された場合には、デバイスＤ１は、ネットワーク上のセキュリティ管理サーバの検索時に、サーバ属性情報の変更を検知する。ここでは、バックアップ用宅内サーバＳ２のサーバ属性情報が「セキュリティレベル：低」から「セキュリティレベル：高」、「宅内共通の暗号

鍵を使用」から「機器固有の暗号鍵を使用」、「暗号鍵の鍵長：１２８ｂｉｔ」から「暗号鍵の鍵長：２５６ｂｉｔ」、「乱数の精度は低い」から「乱数の精度は高い」にそれぞれ変更されていたものとする。この場合、デバイスＤ１は、変更後のサーバ属性情報を比較対象とすることで、よりセキュリティレベルの高いセキュリティ管理サーバ（ここでは、バックアップ用宅内サーバＳ２）を対象サーバに選択する。

【００４４】

これにより、ネットワークシステムのシステム構成自体には変更がなく既存のセキュリティ管理サーバの設定変更があった場合でも、当該設定変更を考慮して最もセキュリティレベルの高いセキュリティ管理サーバを対象サーバとして利用することが可能になる。

【００４５】

ここで、セキュリティ管理サーバのサーバ属性情報の設定変更の検出は、前述のようにサーバ検出手段２がネットワーク上のセキュリティ管理サーバを検出する度に実施してもよいが、セキュリティ管理サーバの持つサーバ属性情報が設定変更された場合に、当該セキュリティ管理サーバがネットワーク上のデバイスＤ１に対して、自己の変更後のサーバ属性情報を含む起動通知を行う構成としてもよい。この場合、デバイスＤ１のサーバ選択手段２は、起動通知を受けてセキュリティ管理サーバのサーバ属性情報の変更を検知し、変更後のサーバ属性情報を用いて再度対象サーバを選択する。

【００４６】

（実施形態２）

本実施形態のネットワークシステムは、図６に示すように宅内ＬＡＮとインターネットを介して接続されるセンターサーバＳ３が追加され、当該センターサーバＳ３にもセキュリティ管理サーバとしての機能が備わっている点が実施形態１のネットワークシステムと相違する。

【００４７】

本実施形態では、閉鎖的なネットワーク（宅内ＬＡＮ）上に構築したネットワークシステムを拡張してインターネットと接続することにより、拡張前には宅内ＬＡＮ上のセキュリティ管理サーバＳ１，Ｓ２しか利用できなかったデバイスＤ１が、インターネット上のセキュリティ管理サーバ（センターサーバＳ３）を利用可能となった場合を想定している。このような場合、デバイスＤ１に対してインターネット上の不特定の端末からアクセスを試みることが可能となり、通信の安全性が低下することとなるので、デバイスＤ１が対象サーバとして利用するセキュリティ管理サーバを切り替えてセキュリティレベルの向上を図る必要がある。

【００４８】

以下では、宅内ＬＡＮとインターネットとを合わせて１つのネットワークとする。また、図６の例では、「セキュリティレベル：低」のサーバ属性情報を持つバックアップ用宅内サーバＳ２とデバイスＤ１とが宅内ＬＡＮ側のネットワークに接続されているものとする。

【００４９】

ここで、センターサーバＳ３の情報保持手段に格納されているサーバ属性情報は、「セキュリティレベル：高」、「機器固有の暗号鍵を使用」、「暗号鍵の鍵長：２５６ｂｉｔ」、「乱数の精度は高い」の４つの情報を含んでいる。

【００５０】

したがって、宅内ＬＡＮ上に存在するデバイスＤ１がインターネットを介してセンターサーバＳ３に接続されると、デバイスＤ１は、サーバ検出手段２によりネットワーク上のセキュリティ管理サーバとしてバックアップ用宅内サーバＳ２とセンターサーバＳ３とを検出する。そして、バックアップ用宅内サーバＳ２とセンターサーバＳ３とのサーバ属性情報を比較して、よりセキュリティレベルの高いセキュリティ管理サーバ（ここではセンターサーバＳ３）を対象サーバとして選択して利用する。

【００５１】

ところで、新たに追加されたセキュリティ管理サーバの検出は、前述のようにデバイス

Ｄ１が一定周期で実施してもよいが、デバイスの台数が多くなると通信トラフィックが増加するという問題がある。すなわち、図７に示すようにネットワーク（ここでは宅内ＬＡＮ）上に複数台のデバイスＤ１～Ｄ３が存在する場合、これら複数台のデバイスＤ１～Ｄ３が一斉にセンターサーバＳ３にアクセスしてサーバ属性情報を取得することにより、ネットワーク上のトラフィックが増大する可能性がある。

【００５２】

そこで、セキュリティ管理サーバ（ここではセンターサーバＳ３）がネットワーク上に追加された場合には、当該セキュリティ管理サーバがネットワーク上のデバイスＤ１～Ｄ３に対して、自己のサーバ属性情報を含む起動通知を行う構成とすることが望ましい。起動通知は、セキュリティ管理サーバからネットワーク上の全デバイスＤ１～Ｄ３に対してブロードキャスト方式で行われるものとし、これによりネットワーク上のトラフィックの増大を抑制することができる。

【００５３】

要するに、図７の例では、センターサーバＳ３がネットワーク（宅内ＬＡＮ）に接続されると、センターサーバＳ３からの起動通知が宅内ＬＡＮ上のデバイスＤ１～Ｄ３に一斉送信され、これらのデバイスＤ１～Ｄ３は、サーバ検出手段２にてセンターサーバＳ３からの起動通知を受けることによりセンターサーバＳ３の存在を検出する。その後、各デバイスＤ１～Ｄ３はセンターサーバＳ３をネットワーク上の他のセキュリティ管理サーバと比較することで、利用可能なセキュリティ管理サーバの中で最もセキュリティレベルの高いセキュリティ管理サーバ（ここでは、センターサーバＳ３）を対象サーバとして選択し利用する。このようにセキュリティレベルの高いセキュリティ管理サーバが新たに利用可能になると、デバイスＤ１～Ｄ３は、よりセキュリティレベルの高いセキュリティ管理サーバを対象サーバとするように自動的に対象サーバの切り替えを行う。

【００５４】

なお、宅内ＬＡＮとインターネットとの間にルータ等が介在することで、起動通知をセンターサーバＳ３から宅内ＬＡＮ上のデバイスＤ１～Ｄ３に直接送信できない場合には、宅内サーバＳ１が定期的にインターネット上のセキュリティ管理サーバを検索し、セキュリティ管理サーバの検出時に、宅内サーバＳ１からデバイスＤ１～Ｄ３に対してブロードキャスト方式あるいはマルチキャスト方式で起動通知を転送するようにしてもよい。

【００５５】

ここにおいて、デバイスＤ１はダイヤルアップ回線でセンターサーバＳ３と接続されるものであって、そのためデバイスＤ１とセンターサーバＳ３との間のインターネット通信は不安定になりやすいものと仮定する。この場合、インターネット通信が途絶えてデバイスＤ１－センターサーバＳ３間の通信が一時的に途絶えると、デバイスＤ１はネットワークからセンターサーバＳ３が離脱したと判断し、対象サーバをセンターサーバＳ３から他のセキュリティ管理サーバに切り替える。その後、デバイスＤ１－センターサーバＳ３間の通信が復旧すると、デバイスＤ１はセンターサーバＳ３が起動したと判断して、対象サーバを再びセンターサーバＳ３に切り替えることとなる。このように、通信路（ダイヤルアップ回線）の状況により対象サーバが頻繁に切り替わると、対象サーバの切替時に一時的にシステムが停止することにより不具合を生じる可能性がある。

【００５６】

そこで、本実施形態では、デバイスＤ１は、サーバ管理手段５にてセキュリティ管理サーバとの通信信頼性を評価し、当該評価値をサーバ選択手段４での対象サーバの判断基準に加味するものとする。すなわち、デバイスＤ１は、図８に示すように対象サーバとして選択されているセキュリティ管理サーバ（ここではセンターサーバＳ３）の稼働状況の異常（サーバが起動／停止を繰り返して安定しない、ダイヤルアップ回線などで通信路が安定しない等）を検知すると、このように稼働状況に異常のあるセキュリティ管理サーバを除くセキュリティ管理サーバの中で、最もセキュリティレベルの高いセキュリティ管理サーバ（ここでは宅内サーバＳ１）を対象サーバに選択する。これにより、デバイスＤ１が利用可能なセキュリティ管理サーバの中に、通信信頼性に問題のあるセキュリティ管理サ

ーバが含まれていても、当該問題のあるセキュリティ管理サーバが対象サーバとして選択されることを回避できる。

【００５７】

また、デバイスＤ１においてセキュリティ管理サーバとの通信信頼性を評価するためには、図９に示すようにセキュリティ管理サーバの持つサーバ属性情報を利用するようにしてもよい。図９の例では、宅内サーバＳ１とセンターサーバＳ３とは情報保持手段９に保持したサーバ属性情報のうちセキュリティレベルに関する項目は共通である（ここでは、いずれも「セキュリティレベル：高」、「機器固有の暗号鍵を使用」、「暗号鍵の鍵長：２５６ｂｉｔ」、「乱数の精度は高い」）が、宅内サーバＳ１のサーバ属性情報には「宅内ＬＡＮ上に設置」を含んでいるのに対し、センターサーバＳ３のサーバ属性情報には「インターネット上に設置」を含んでいる。

【００５８】

この場合、デバイスＤ１は、両セキュリティ管理サーバのセキュリティレベルが同じであるため、各セキュリティ管理サーバの設置されている場所を比較し、宅内ＬＡＮ上の宅内サーバＳ１とインターネット上のセンターサーバＳ３とでは、宅内ＬＡＮ上の宅内サーバＳ１の方が通信信頼性（安定性）に優れていると判断する。そのため、デバイスＤ１は宅内サーバＳ１を対象サーバに選択して利用する。このように、セキュリティ管理サーバの実際の通信状況を評価しなくても、サーバ属性情報として予め与えられているセキュリティ管理サーバの通信信頼性を加味することで、対象サーバが頻繁に切り替わることを回避できる。

【００５９】

なお、サーバ管理手段５での評価値を対象サーバの選択時の判断基準にどの程度加味するかは、デバイスＤ１のセキュリティ属性情報において規定することが可能である。そのため、たとえ宅内サーバＳ１のセキュリティレベルがセンターサーバＳ３のセキュリティ管理サーバより低くても、セキュリティ管理サーバの通信信頼性（安定性）を優先して、センターサーバＤ３ではなく宅内サーバＳ１を対象サーバに選択する設定とすることも可能である。

【００６０】

その他の構成および機能は実施形態１と同様である。

【図面の簡単な説明】

【００６１】

【図１】本発明の実施形態１のシステム構成を示す概略ブロック図である。

【図２】同上のデバイスの構成を示す概略ブロック図である。

【図３】同上のセキュリティ管理サーバの構成を示す概略ブロック図である。

【図４】同上のシステム構成を示す概略ブロック図である。

【図５】同上のシステム構成を示す概略ブロック図である。

【図６】本発明の実施形態２のシステム構成を示す概略ブロック図である。

【図７】同上のシステム構成を示す概略ブロック図である。

【図８】同上のシステム構成を示す概略ブロック図である。

【図９】同上のシステム構成を示す概略ブロック図である。

【図１０】従来例を示す概略ブロック図である。

【図１１】他の従来例を示す概略ブロック図である。

【符号の説明】

【００６２】

２　サーバ検出手段

４　サーバ選択手段

５　サーバ管理手段

Ｄ１～Ｄ３　デバイス

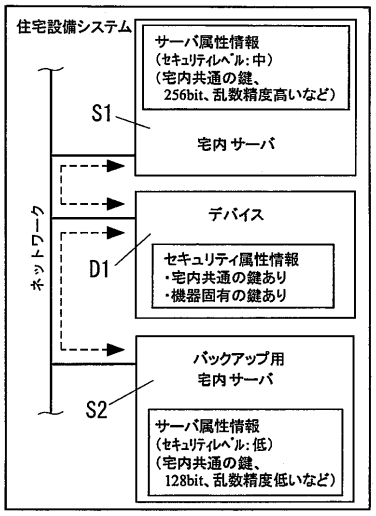
Ｓ１　宅内サーバ（セキュリティ管理サーバ）

Ｓ２　バックアップ用宅内サーバ（セキュリティ管理サーバ）

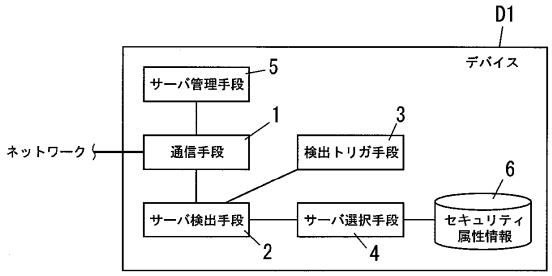
Ｓ３　センターサーバ（セキュリティ管理サーバ）

【図１】

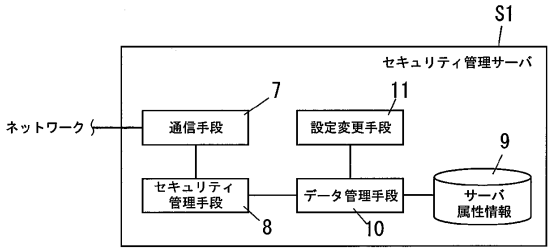
Ｄ１　デバイス
Ｓ１　宅内サーバ（セキュリティ管理サーバ）
Ｓ２　バックアップ用宅内サーバ（セキュリティ管理サーバ）



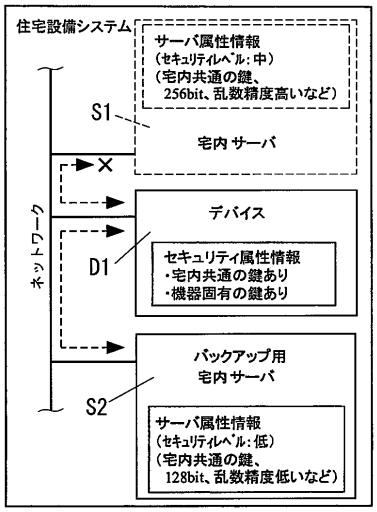
【図２】



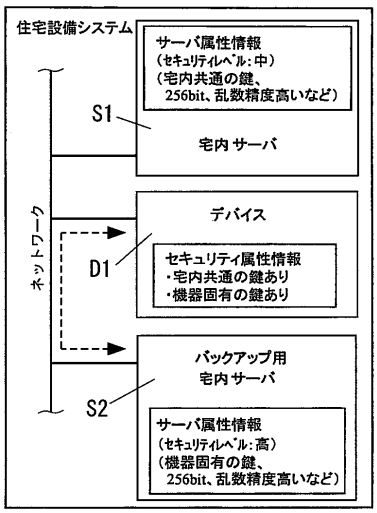
【図３】



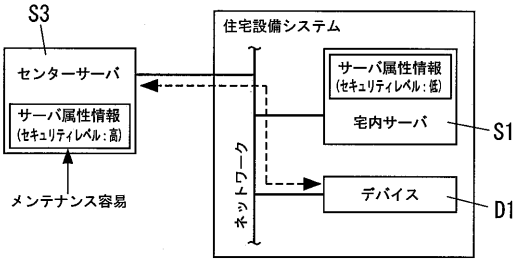
【図４】


住宅設備システム
サーバ属性情報
（セキュリティレベル：中）
（宅内共通の鍵、
256bit、乱数精度高いなど）
S1
宅内 サーバ
ネットワーク
デバイス
D1
セキュリティ属性情報
・宅内共通の鍵あり
・機器固有の鍵あり
バックアップ用
宅内サーバ
S2
サーバ属性情報
（セキュリティレベル：低）
（宅内共通の鍵、
128bit、乱数精度低いなど）

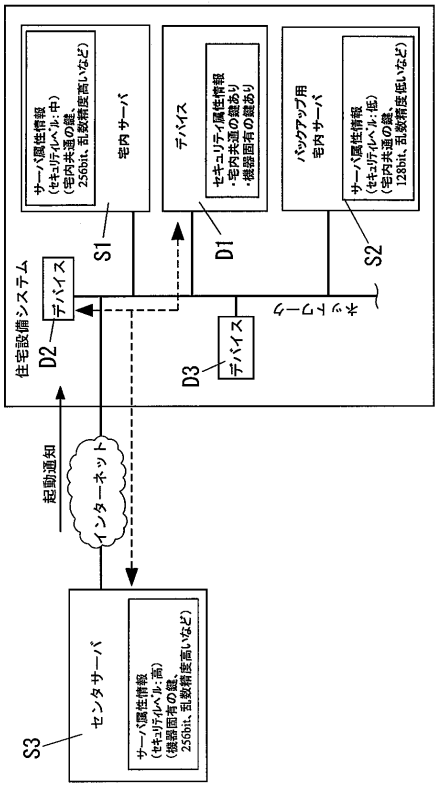
【図５】


住宅設備システム
サーバ属性情報
（セキュリティレベル：中）
（宅内共通の鍵、
256bit、乱数精度高いなど）
S1
宅内 サーバ
ネットワーク
デバイス
D1
セキュリティ属性情報
・宅内共通の鍵あり
・機器固有の鍵あり
バックアップ用
宅内サーバ
S2
サーバ属性情報
（セキュリティレベル：高）
（機器固有の鍵、
256bit、乱数精度高いなど）

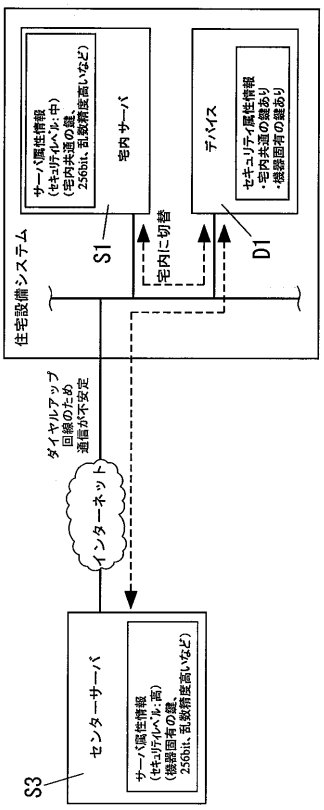
【図６】


S3
センターサーバ
サーバ属性情報
（セキュリティレベル：高）
メンテナンス容易
住宅設備システム
サーバ属性情報
（セキュリティレベル：低）
宅内サーバ
S1
ネットワーク
デバイス
D1

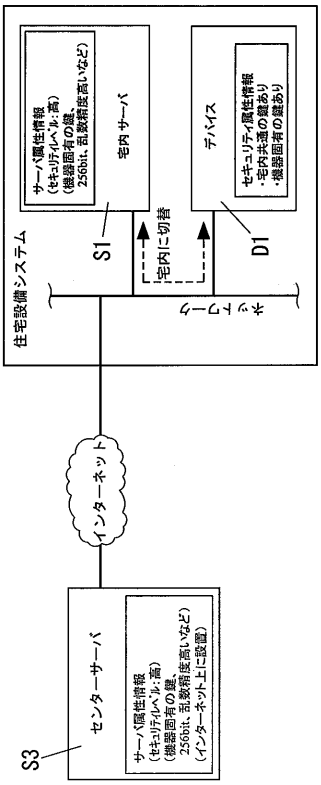
【図７】


サーバ属性情報
（セキュリティレベル：中）
（宅内共通の鍵、
256bit、乱数精度高いなど）
宅内 サーバ
デバイス
セキュリティ属性情報
・宅内共通の鍵あり
・機器固有の鍵あり
バックアップ用
宅内サーバ
サーバ属性情報
（セキュリティレベル：低）
（宅内共通の鍵、
128bit、乱数精度低いなど）
S1
D1
S2
住宅設備システム
デバイス
D2
デバイス
D3
ネットワーク
起動通知
インターネット
センタサーバ
サーバ属性情報
（セキュリティレベル：高）
（機器固有の鍵、
256bit、乱数精度高いなど）
S3

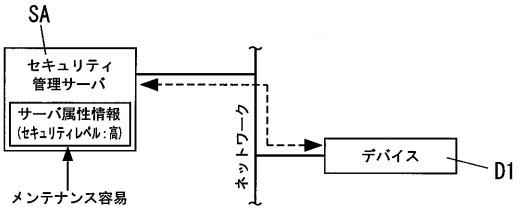
【図８】


サーバ属性情報
（セキュリティレベル：中）
（宅内共通の鍵、
256bit、乱数精度高いなど）
宅内 サーバ
デバイス
セキュリティ属性情報
・宅内共通の鍵あり
・機器固有の鍵あり
住宅設備システム
S1
宅内に切替
D1
ダイヤルアップ
回線のため
通信が不安定
インターネット
センターサーバ
サーバ属性情報
（セキュリティレベル：高）
（機器固有の鍵、
256bit、乱数精度高いなど）
S3

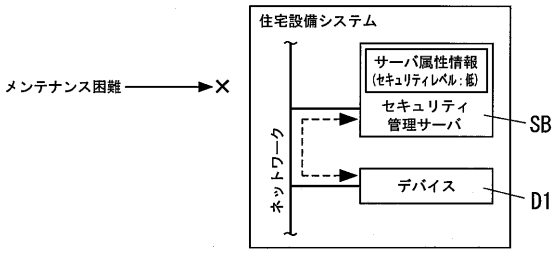
【図９】


住宅設備システム
サーバ属性情報
(セキュリティレベル:高、
機器固有の鍵、
256bit、乱数精度高いなど)
宅内 サーバ
S1
宅内に切替
デバイス
セキュリティ属性情報
・宅内共通の鍵あり
・機器固有の鍵あり
D1
ネットワーク
インターネット
センターサーバ
サーバ属性情報
(セキュリティレベル:高、
機器固有の鍵、
256bit、乱数精度高いなど)
(インターネット上に設置)
S3

【図１０】


SA
セキュリティ
管理サーバ
サーバ属性情報
(セキュリティレベル:高)
メンテナンス容易
ネットワーク
デバイス
D1

【図１１】


メンテナンス困難
住宅設備システム
サーバ属性情報
(セキュリティレベル:低)
セキュリティ
管理サーバ
SB
ネットワーク
デバイス
D1

フロントページの続き

(56)参考文献 特開２００１－１８８７５８（ＪＰ，Ａ）
特開２００２－１４０４１４（ＪＰ，Ａ）
特開２００６－３３９８５５（ＪＰ，Ａ）
特開２０００－０２０２６４（ＪＰ，Ａ）
特開２００２－２６９０６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１