(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4779639号
(P4779639)
(45)発行日　平成23年9月28日(2011.9.28)　(24)登録日　平成23年7月15日(2011.7.15)

(51)Int.Cl.　F I
H04L 12/46 (2006.01)　H04L 12/46　Z

請求項の数 4　(全 12 頁)

(21)出願番号　特願2005-368200 (P2005-368200)
(22)出願日　平成17年12月21日 (2005.12.21)
(65)公開番号　特開2007-174209 (P2007-174209A)
(43)公開日　平成19年7月5日 (2007.7.5)
審査請求日　平成20年9月11日 (2008.9.11)

(73)特許権者　000005832
パナソニック電工株式会社
大阪府門真市大字門真１０４８番地
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100108707
弁理士　中村　友之
(74)代理人　100095500
弁理士　伊藤　正和
(72)発明者　福田　尚弘
大阪府門真市大字門真１０４８番地　松下電工株式会社内

審査官　岩田　玲彦

最終頁に続く

(54)【発明の名称】セキュリティ通信システム

(57)【特許請求の範囲】
【請求項１】
通信を行う機器間においてデータリンク層のセキュリティ設定を行う第１のセキュリティ手段と、
通信を行う機器間において前記データリンク層よりも上位のプロトコル階層のセキュリティ設定を行う第２のセキュリティ手段とを有し、
前記第１のセキュリティ手段は、前記第２のセキュリティ手段でセキュリティ設定が行われた複数の機器を識別した場合に、当該複数の機器間で前記データリンク層のセキュリティ設定を行うことを特徴とするセキュリティ通信システム。
【請求項２】
前記データリンク層のアドレスを参照してデータの転送をする集線装置を備え、
前記第２のセキュリティ手段は、前記集線装置に接続された複数の機器間においてセキュリティ設定を行い、前記第１のセキュリティ手段は、当該第２のセキュリティ手段によってセキュリティ設定が行われた複数の機器が接続されたポートを識別し、当該ポートのパス制御を前記集線装置に行わせることを特徴とする請求項１に記載のセキュリティ通信システム。
【請求項３】
前記データリンク層のアドレスを参照してデータの転送をする集線装置を備え、
前記第２のセキュリティ手段は、複数の機器の機器認証処理を管理する機器認証サーバであって、機器認証がされた複数の機器のデータリンク層のアドレスを前記第１のセキュ

リティ手段に送信し、
前記第１のセキュリティ手段は、機器認証がされた複数の機器のデータリンク層のアドレスに基づいて、当該複数の機器間におけるパス制御を前記集線装置に行わせることを特徴とする請求項１又は請求項２に記載のセキュリティ通信システム。
【請求項４】
パス制御の対象となる複数のポート番号とを対応付けたアドレステーブルを参照して、前記データリンク層のアドレスを参照してデータの転送をする集線装置を備え、
前記第１のセキュリティ手段は、前記機器認証サーバからの機器認証がされた複数の機器のデータリンク層のアドレスに対してグループ識別子を生成し、前記集線装置に記憶されている前記アドレステーブルに、パス制御の対象となる機器が接続されている複数のポートに対応付けてグループ識別子を設定させることを特徴とする請求項１又は請求項２に記載のセキュリティ通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機器間でセキュアな通信を行うために、相互の機器間にデータリンク層のセキュリティ設定を行うセキュリティ通信システムに関する。
【背景技術】
【０００２】
従来より、ハブ等の集線装置によってポートＶＬＡＮ（virtual LAN）を実現する技術としては、下記の特許文献１に記載された技術などが知られている。
【０００３】
この技術は、機器Ａ，Ｂ間でＶＬＡＮを構築する場合に、ＬＡＮスイッチに機器の情報を登録する。機器Ａから、ＬＡＮスイッチを介して機器Ｂに通信を行う場合、先ず、機器Ａは、自身のＭＡＣアドレスＭＡＣ－Ａ及びＩＰアドレスＩＰ－Ａ、相手の機器ＢのＭＡＣアドレスＭＡＣ－Ｂ及びＩＰアドレスＩＰ－Ｂをイーサーフレームに入れて、送信フレームＦＲ－Ａを生成し、送信を行う。
【０００４】
そして、ＬＡＮスイッチは、ポートからの入力フレームＦＲ－Ａから、送信元のＭＡＣアドレスＭＡＣ－Ａを読み取り、装置内に確保されたＭＡＣアドレステーブルに登録する。このＭＡＣアドレステーブルは、ポート番号（例えばポート「１」）とＭＡＣアドレスＭＡＣ－Ａの対応関係を保持している。
【０００５】
このＬＡＮスイッチは、当該ＭＡＣアドレステーブルに、機器ＢのＭＡＣアドレスを待たないので、該入力パケットを関連する全ポートにブロードキャストをして、ブロードキャストされたフレームＦＲ－Ａを受信した機器Ｂは、受信したフレームＦＲ－Ａの宛先ＭＡＣが、自身のＭＡＣアドレスＭＡＣ－Ｂに一致するので、自身のＭＡＣアドレスＭＡＣ－Ｂ及びＩＰアドレスＩＰ－Ｂ、相手先のＭＡＣアドレスＭＡＣ－Ａ及びＩＰアドレスＩＰ－Ａを入れて、イーサーフレームＦＲ－Ｂの返信を行う。
【０００６】
例えば機器ＢがＬＡＮスイッチのポート「５」に接続されている場合、ＬＡＮスイッチは、イーサーフレームＦＲ－Ｂをポート「５」を介して受信することになる。そこで、ＬＡＮスイッチは、送信元のＭＡＣアドレスＭＡＣ－Ｂを読み取り、ＭＡＣアドレステーブルに登録する。これによって、ＬＡＮスイッチによって、ＭＡＣアドレステーブルに、ポートとＭＡＣアドレスＭＡＣ－Ｂとの対応関係を保持する。
【０００７】
その後、機器Ａと機器Ｂ間の通信は、ＬＡＮスイッチのＭＡＣアドレステーブルに、両方の端末機器のアドレスが登録されたので１対１の通信が行ってポートＶＬＡＮを実現する。そして、一連の通信が終了し、所定時間（例えば５分）が過ぎると、ＬＡＮスイッチ内のＭＡＣアドレステーブルに登録されたポートと送信元ＭＡＣアドレスとの対応関係は

削除される。
【０００８】
また、ＶＰＮ(Virtual Private Network)においては、下記の特許文献２のＳＳＬ（Secure Sockets Layer）またはＲＦＣ（Request For Comments）２４０１－２４０９、他に代表されるＩＰｓｅｃ、ＭＩＴ（マサチューセッツ工科大学）のＫｅｒｂｅｒｏｓ、ＩＢＭ（登録商標）のＫｒｙｐｔｏＫｎｉｇｈｔなどの技術が知られており、これら暗号プロトコルでは、各暗号通信において通信セッションの状態を通信アドレスまたは通信のソケットの単位で管理している。暗号通信を確立するには、暗号通信主体は事前に暗号化する通信セッションの暗号化のネゴシエーション（調停）を行い、暗号通信化が可能であれば暗号通信を確立する。
【特許文献１】特開２００５－７３２３０号公報
【特許文献２】米国特許第５６５７３９０号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００９】
しかしながら、上述の従来の技術は、通信アドレスを偽造するＤｏＳ攻撃に対しては脆弱であった。たとえばＶＰＮによる暗号セッションを確立してもアドレスを偽造することで暗号セッションへのＤｏＳ攻撃が可能である。ＶＰＮによってはＤｏＳ攻撃を受けても耐性を持たせて耐えることも可能であるが、その攻撃量が多ければ問題となる。
【００１０】
そこで、本発明は、上述した実情に鑑みて提案されたものであり、セキュアな通信を行う機器同士を確実に識別してデータリンク層におけるセキュリティ設定を行うセキュリティ通信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】
【００１１】
本発明に係るセキュリティ通信システムは、通信を行う機器間においてデータリンク層のセキュリティ設定を行う第１のセキュリティ手段と、通信を行う機器間において前記データリンク層よりも上位のプロトコル階層のセキュリティ設定を行う第２のセキュリティ手段とを有し、上述の課題を解決するために、第１のセキュリティ手段は、第２のセキュリティ手段でセキュリティ設定が行われた複数の機器を識別した場合に、当該複数の機器間で前記データリンク層のセキュリティ設定を行う。
【発明の効果】
【００１２】
本発明に係るセキュリティ通信システムによれば、第２のセキュリティ手段によってセキュリティ設定がなされた場合に第１のセキュリティ手段によってデータリンク層におけるセキュリティ設定を行うので、第２のセキュリティ手段によって機器が識別された上でデータリンク層におけるセキュリティ設定を行うことができ、セキュアな通信を行う機器同士を確実に識別してデータリンク層におけるセキュリティ設定を行うことができる。
【発明を実施するための最良の形態】
【００１３】
以下、本発明の実施の形態について図面を参照して説明する。
【００１４】
本発明は、図１に示すように、集線装置１に、ＶＰＮ（Virtual Private Network）サーバ２、ＲＡＤＩＵＳ（Remote Authentication Dial-In-User-Service）サーバ３、セキュアな通信を行う機器Ｄ１，機器Ｄ２が接続されたセキュリティ通信システムに適用される。このセキュリティ通信システムは、機器Ｄ１，Ｄ２間で通信を行うに際して、集線装置１に接続されて、機器Ｄ１，Ｄ２間でＯＳＩ（Open Systems Interconnection）参照モデルにおけるデータリンク層（Layer2，Ｌ２）でセキュアな通信を実現するために、機器Ｄ１，Ｄ２間でポートＶＬＡＮ（virtual LAN）を構築するものである。このポートＶＬＡＮを構築するために、セキュリティ通信システムは、データリンク層よりも上位の階層

におけるネットワーク層（Layer3，Ｌ３）における処理を利用してセキュアな通信を行う機器Ｄ１，Ｄ２間を識別して、ポートＶＬＡＮを設定することを特徴とするものである。

【００１５】

集線装置１は、例えばＩＥＥＥ（The Institute of Electrical and Electronics Engineers）８０２．１Ｘ、ＲＡＤＩＵＳに対応した有線ＬＡＮ（Local Area Network）スイッチであり、ＲＡＤＩＵＳサーバ３に対するＲＡＤＩＵＳクライアントとして機能する。ここでは有線ＬＡＮによる例を挙げるが、無線ＬＡＮの環境の場合は図２に示す構成となる。この場合、無線ＬＡＮのアクセスポイントＡＰ１，ＡＰ２はそれぞれ集線装置１の各ポートＰ１，Ｐ２に接続され、機器Ｄ１，Ｄ２では無線ＬＡＮのインターフェースを装着するものとする。ここでは機器Ｄ１，Ｄ２と集線装置１との間の通信が無線メディアになるか有線メディアになるかの違いであり、無線ＬＡＮ環境においても同様に動作する。

【００１６】

この集線装置１は、データリンク層における機器Ｄ１，Ｄ２の識別子であるＭＡＣアドレスを参照して、パス制御を行う。この集線装置１には、後述の処理によって、機器Ｄ１，Ｄ２が接続されているポート番号と、機器Ｄ１，Ｄ２のＭＡＣアドレスと、セキュアな通信を行う機器群を識別するグループＩＤとを対応付けたアドレステーブル１ａが記憶されている。集線装置１は、機器Ｄ１，Ｄ２からフレームデータを受信した場合、当該フレームデータを受信したポートの番号と、フレームデータ送信元のＭＡＣアドレスと、フレームデータ送信先のＭＡＣアドレスと、グループＩＤとを参照して、フレームデータの転送を行う。

【００１７】

ＶＰＮサーバ２は、データリンク層よりも上位の階層であるネットワーク層におけるセキュリティ設定処理として、ＫｒｙｐｔｏＫｎｉｇｈｔに準拠した機器認証処理及び暗号キーの設定処理を行う。ＶＰＮサーバ２は、機器Ｄ１，Ｄ２からのＶＰＮ設定要求を受けると、機器Ｄ１，Ｄ２の機器認証処理、機器Ｄ１，Ｄ２に対して暗号キーの設定処理を行う。ＶＰＮサーバ２は、機器Ｄ１，Ｄ２の機器認証が完了した場合に、機器Ｄ１，Ｄ２で使用する暗号キーを設定するネゴシエーションを行って、機器Ｄ１，Ｄ２に暗号キーを付与する。

【００１８】

ここではＫｒｙｐｔｏＫｎｉｇｈｔの例を示したが、ＩＰｓｅｃ、ＳＳＬ、Ｋｅｒｂｅｒｏｓなどの暗号プロトコルを用いても暗号化セッションの管理部分において同様に扱える。

【００１９】

また、ＶＰＮサーバ２は、機器Ｄ１，Ｄ２間における機器認証処理及び暗号キーの設定処理が完了すると、当該セキュリティ通信を行う機器Ｄ１，Ｄ２のＭＡＣアドレスを ＲＡＤＩＵＳサーバ３に供給する。

【００２０】

このＶＰＮサーバ２は、どの機器同士からネットワーク層におけるセキュリティ設定の要求がなされているかを管理するためのＬ３用管理データベース４が接続されている。このＬ３用管理データベース４は、ＶＰＮサーバ２によって書き換えられる。

【００２１】

ＲＡＤＩＵＳサーバ３は、機器Ｄ１，Ｄ２からＲＡＤＩＵＳ認証処理の要求を受けると、当該要求に含まれるユーザＩＤ、パスワードを判断して、相互のユーザ認証を行う。また、ＲＡＤＩＵＳサーバ３は、ＶＰＮサーバ２から送信された機器Ｄ１，Ｄ２のＭＡＣアドレスから、機器Ｄ１，Ｄ２がネットワーク層におけるセキュリティ設定処理がなされたことを認識する。ＲＡＤＩＵＳサーバ３は、機器Ｄ１，Ｄ２のユーザ認証が完了すると、ＶＰＮサーバ２から受信した機器Ｄ１，Ｄ２のＭＡＣアドレスから、セキュアな通信を行う機器群を識別する。そして、ＲＡＤＩＵＳサーバ３は、集線装置１のアドレステーブル１ａを更新させる。

【００２２】

このＲＡＤＩＵＳサーバ３は、集線装置１を介して通信を行う機器についてユーザ認証を行うためのデータベース、どの機器同士からデータリンク層におけるセキュリティ設定の要求がなされているかを管理するためのテーブル等を記憶するＬ２用管理データベース５が接続されている。このＬ２用管理データベース５は、ＶＰＮサーバ２からＲＡＤＩＵＳサーバ３にネットワーク層におけるセキュリティ設定がなされたことを示す暗号通信情報が供給された場合に、ＲＡＤＩＵＳサーバ３によって書き換えられる。

【００２３】

尚、ここでは機器Ｄ１，Ｄ２のユーザ認証を含めての例を示したが、機器Ｄ１，Ｄ２の管理によってはユーザの認証が必要ない場合がある。たとえば、機器Ｄ１，Ｄ２の管理が機器のIDまたはグループごとに行われる場合である。この場合はユーザ認証の認証子（ユーザのID、パスワードなど）を利用せず、機器Ｄ１，Ｄ２のIDとして機器Ｄ１，Ｄ２のMACアドレスまたは機器Ｄ１，Ｄ２のMACアドレスの上位、下位数ビットをグループとして認証して実施することも可能である。尚、機器Ｄ１，Ｄ２のIDはRadiusによる認証技術で一般的に用いられるMACアドレスを挙げたが、Radius側での認証子の設定を変更することで機器Ｄ１，Ｄ２のIDとしてはEMITのOID（Object Identification)を利用することもできる。

【００２４】

このようなセキュリティ通信システムは、例えば、所謂ＥＭＩＴ（Embedded Micro Internetworking Technology）と称されるネットワーク技術を利用して、機器Ｄ１，Ｄ２を制御・監視するものである。このＥＭＩＴ技術は、機器Ｄ１，Ｄ２、集線装置１といったネットワーク機器にＥＭＩＴミドルウェアを組み込み、当該ＥＭＩＴミドルウェア同士の通信によって通信接続を実現するものである。

【００２５】

なお、詳細は後述するが、集線装置１には、ＥＭＩＴミドルウェア間におけるルーティング処理、機器Ｄ１，Ｄ２の認識処理等を行うＯＡＳ（Object Access Server）機能部が実装され、機器Ｄ１，Ｄ２には、ＥＭＩＴミドルウェア間で各種機器Ｄ１，Ｄ２の制御信号や機器Ｄ１，Ｄ２の状態信号等を送受するＭＯＳ（Micro Object Server）機能部が実装され、機器Ｄ１，Ｄ２の動作を遠隔で制御・監視するパーソナルコンピュータには、制御対象の機器Ｄ１，Ｄ２への制御・監視リクエストを出力すると共に機器Ｄ１，Ｄ２の状態表示等を行うＯＡＬ（Object Access Library）機能部（図示せず）が実装されている。

【００２６】

このような機器Ｄ１，Ｄ２及び集線装置１は、図３に示すように構成される。

【００２７】

機器Ｄ１，Ｄ２は、ＭＯＳ機能部１１に、アプリケーション処理部１２、インターフェースモジュール１３が接続されている。

【００２８】

アプリケーション処理部１２は、例えば照明として機能する場合に、例えば照度値を調整するアプリケーションコードが記憶されており、照度値を保持してＭＯＳ機能部１１に受け渡す。

【００２９】

インターフェースモジュール１３は、ＯＳＩ参照モデルにおけるデータリンク層、ネットワーク層、トランスポート層の処理を行う。例えばデータリンク層においてイーサネット（登録商標）に従った処理を行い、ネットワーク層においてＩＰ（Internet Protocol）に従った処理を行い、トランスポート層においてＴＣＰ（Transmission Control Protocol）に従った処理を行う。このインターフェースモジュール１３は、ＲＡＤＩＵＳサーバ３にＲＡＤＩＵＳ認証処理の要求を送信すると共に、ＶＰＮサーバ２にＶＰＮ設定要求を送信する機能を有する。

【００３０】

インターフェースモジュール１３の通信プロトコルバージョン、通信速度といった能力

は、能力テーブル１４に格納されて、集線装置１のＯＡＳ機能部２１によって取得可能となっている。

【００３１】

ＭＯＳ機能部１１は、アプリケーション処理部１２によるアプリケーション層とインターフェースモジュール１３によるトランスポート層との間のＥＭＩＴミドルウェアとして機能する。このＭＯＳ機能部１１には、集線装置１のＯＡＳ機能部２１によって、機器Ｄ１，Ｄ２がＥＭＩＴにおけるオブジェクトであることを識別するために、オブジェクトＩＤ１１ｄが与えられている。このオブジェクトＩＤ１１ｄは、ＯＡＳ機能部２１と通信するに際して、集線装置１に送信するフレームデータに格納される。

【００３２】

ＭＯＳ機能部１１は、機能（function、関数）１１ａ、イベント（event）１１ｂ、変数（variable）１１ｃで定義された動作を行う。このＭＯＳ機能部１１の動作は、サービステーブル１１ｅして定義されており、集線装置１のＯＡＳ機能部２１によって取得可能となっている。

【００３３】

機器Ｄ１，Ｄ２が照明である場合、機能１１ａは、オンオフ値の出力機能となり、イベント１１ｂは、例えば照度値が所定値以下となったらオンを出力するイベントとなり、変数１１ｃは、現状のオンオフ値そのものとなる。

【００３４】

また、機器Ｄ１，Ｄ２は、ＭＯＳ機能部１１によって、オブジェクトＩＤ１１ｄ、機器属性情報（class）、機能情報、変数情報、イベント情報等を送信させても良く、集線装置１からの要求に応じてオブジェクトＩＤ１１ｄ等を送信しても良い。

【００３５】

集線装置１は、機器Ｄ１，Ｄ２を制御・監視するものであって、セキュリティ通信システムにおいてはアドレステーブル１ａを参照したパス制御を行うパス制御部２２を備えている。この集線装置１は、ＯＡＳ機能部２１に、パス制御部２２、通信モジュール２３が接続されている。

【００３６】

パス制御部２２は、アドレステーブル１ａを有し、ＲＡＤＩＵＳサーバ３によってアドレステーブル１ａが書き換えられる。パス制御部２２は、通信モジュール２３を介してフレームデータ及び当該フレームデータを受信したポート番号を入力した場合に、当該フレームデータの送信先ＭＡＣアドレスに対応したポート番号をアドレステーブル１ａから取得して、当該ポート番号からフレームデータを送信させる。

【００３７】

また、パス制御部２２は、入力したフレームデータにグループＩＤが含まれている場合、同じグループＩＤと対応付けられてアドレステーブル１ａに登録された機器が送信先ＭＡＣアドレスとなっている場合のみにフレームデータを転送する。これによって、パス制御部２２は、ポートＶＬＡＮを実現する。

【００３８】

通信モジュール２３は、機器Ｄ１，Ｄ２のインターフェースモジュール１３との間で通信を行うと共に、ＶＰＮサーバ２，ＲＡＤＩＵＳサーバ３との間で通信を行う。この通信モジュール２３は、ＯＳＩ参照モデルにおけるデータリンク層、ネットワーク層、トランスポート層の処理を行う。例えばデータリンク層においてイーサネット（登録商標）に従った処理を行い、ネットワーク層においてＩＰに従った処理を行い、トランスポート層においてＴＣＰに従った処理を行う。個々の機器Ｄ１，Ｄ２が様々なインターフェースモジュール１３で構成されている場合、通信モジュール２３は、デバイスアクセスコントローラ２１ｃの制御に従って、機器Ｄ１，Ｄ２ごとの通信プロトコルバージョン、通信速度といった機器Ｄ１，Ｄ２の能力に応じた通信処理を行う。

【００３９】

この通信モジュール２３は、集線装置１に設けられた物理的なポートを有する。通信モ

ジュール２３は、機器Ｄ１，Ｄ２からフレームデータを受信した場合、当該フレームデータにポート番号を付加してパス制御部２２に供給する。また、通信モジュール２３は、ＲＡＤＩＵＳサーバ３からのアドレステーブル１ａの書き換え命令を受信した場合には、当該命令をパス制御部２２に出力する。

【００４０】

ＯＡＳ機能部２１は、パス制御部２２の処理と通信モジュール２３によるトランスポート層処理との間のＥＭＩＴミドルウェアとして機能する。このＯＡＳ機能部２１は、デバイスアクセスサーバ２１ａ、所定のメモリに格納されたサービス情報２１ｂ、デバイスアクセスコントローラ２１ｃを備えて構成されている。

【００４１】

デバイスアクセスサーバ２１ａは、集線装置１に接続された機器の情報を取得して、機器Ｄ１，Ｄ２ごとに、オブジェクトＩＤ１１ｄ、機能１１ａ、イベント１１ｂ、変数１１ｃを管理している。例えば、集線装置１に接続された機器に対してクライアント（ＯＡＬ）からリクエストが発生した場合には、制御先のオブジェクトＩＤとサービス情報とを参照して制御対象の機器を判定する。そして、デバイスアクセスサーバ２１ａは、ＭＯＳ機能部１１に対してリクエストに応じた動作をするように制御信号をデバイスアクセスコントローラ２１ｃから送信させる。

【００４２】

つぎに、このように構成されたセキュリティ通信システムにおいて、機器Ｄ１，Ｄ２からの要求に応じて、機器Ｄ１，Ｄ２間でポートＶＬＡＮを構築する手順について図４のフローチャート及び図５乃至図７のテーブルを参照して説明する。

【００４３】

先ず、ステップＳ１で集線装置１に機器Ｄ１，Ｄ２が接続されると、ステップＳ２において、集線装置１は、ＭＡＣアドレス（１）の機器Ｄ１がポート番号（Ｐ１）のポートに接続され、ＭＡＣアドレス（２）の機器Ｄ２がポート番号（Ｐ２）のポートに接続されていることを認識する。これにより、集線装置１は、ポート番号（Ｐ１）とＭＡＣアドレス（１）とを対応付け、且つ、ポート番号（Ｐ２）とＭＡＣアドレス（２）とを対応付けるようにアドレステーブル１ａを更新する。

【００４４】

次に機器Ｄ１と機器Ｄ２とがポートＶＬＡＮを構築するために、機器Ｄ１、機器Ｄ２は、ステップＳ３において、集線装置１を介して、ＲＡＤＩＵＳ認証処理の要求をＲＡＤＩＵＳサーバ３に送信する。ここで、集線装置１は、ＲＡＤＩＵＳサーバ３が接続されたポートを開放（ＯＰＥＮ）状態にしているので、当該ポートからＲＡＤＩＵＳ認証処理の要求を転送できる。また、機器Ｄ１から送信されたＲＡＤＩＵＳ認証処理の要求には、機器Ｄ１のユーザＩＤ、パスワードが含まれており、機器Ｄ２から送信されたＲＡＤＩＵＳ認証処理の要求には、機器Ｄ２のユーザＩＤ、パスワードが含まれている。集線装置１は、機器Ｄ１からの ＲＡＤＩＵＳ認証処理の要求に、機器Ｄ１が接続されているポート番号（Ｐ１）を付加して転送し、機器Ｄ２からのＲＡＤＩＵＳ認証処理の要求に、機器Ｄ２が接続されているポート番号（Ｐ２）を付加して転送する。

【００４５】

ＲＡＤＩＵＳサーバ３は、ＲＡＤＩＵＳ認証処理の要求をそれぞれ受信すると、当該ＲＡＤＩＵＳ認証処理の要求に含まれるＭＡＣアドレス（１）、ＭＡＣアドレス（２）をそれぞれ取り出す。そして、ＲＡＤＩＵＳサーバ３は、図５に示すように、機器Ｄ１，機器Ｄ２ごとに、ユーザＩＤ、パスワード、ポート番号、ＭＡＣアドレスが対応付けられたＲＡＤＩＵＳ認証用のテーブルを作成して、Ｌ２用管理データベース５に格納させる。

【００４６】

次に、機器Ｄ１、機器Ｄ２は、ステップＳ４において、ネットワーク層におけるセキュリティ設定を行うために、集線装置１を介してＶＰＮサーバ２にＶＰＮ設定要求を送信する。ここで、集線装置１は、ＶＰＮサーバ２が接続されたポートを開放（ＯＰＥＮ）状態にしているので、当該ポートからＶＰＮ設定要求を転送できる。

【００４７】
ＶＰＮサーバ２は、ＶＰＮ設定要求をそれぞれ受信すると、当該ＶＰＮ設定要求に含まれるＭＡＣアドレス（１）、ＭＡＣアドレス（２）をそれぞれ取り出す。そして、ＶＰＮサーバ２は、図６に示すように、機器Ｄ１，機器Ｄ２ごとに、ＶＰＮ番号、ＭＡＣアドレスが対応付けられたＶＰＮ設定用のテーブルを作成して、Ｌ３用管理データベース４に格納させる。このＶＰＮ番号は、機器Ｄ１、機器Ｄ２とが相互にＶＰＮ通信をするので、同一の値（２００）が機器Ｄ１，機器Ｄ２それぞれの ＭＡＣアドレスに対応して格納される。

【００４８】
そして、ＶＰＮサーバ２は、機器Ｄ１と機器Ｄ２との間でＶＰＮ接続することを検知したことに応じて、ＭＡＣアドレス（１）の機器Ｄ１とＭＡＣアドレス（２）の機器Ｄ２とがＶＰＮ通信を行うことを示すＶＰＮ通信情報をＲＡＤＩＵＳサーバ３に送信する。

【００４９】
次に、ＲＡＤＩＵＳサーバ３は、ステップＳ５において、ＶＰＮ通信情報を受信したことに応じてＭＡＣアドレス（１）の機器Ｄ１とＭＡＣアドレス（２）の機器Ｄ２とがＶＰＮ通信を行うことを認識し、当該機器Ｄ１と機器Ｄ２間でポートＶＬＡＮを構築するために、グループＩＤを生成する。このグループＩＤは、図７に示すように、ＲＡＤＩＵＳサーバ３によって、集線装置１におけるポートＶＬＡＮを管理するテーブルに格納される。図７に示すように、ＲＡＤＩＵＳサーバ３は、集線装置１のＩＤ（１）と、グループＩＤ（１００）と、集線装置１のポート番号（Ｐ１）が接続状態であることを示す値（１）、集線装置１のポート番号（Ｐ２）が接続状態であることを示す値（１）とを対応付けたテーブルを作成する。

【００５０】
次にＲＡＤＩＵＳサーバ３は、ステップＳ６において、ポート番号（Ｐ１）とポート番号（Ｐ２）との間でポートＶＬＡＮを構築する命令を集線装置１に送信する。この命令には、図７におけるグループＩＤを含む。これにより、集線装置１は、ステップＳ２で作成したアドレステーブル１ａを、ポート番号（Ｐ１）に機器Ｄ１のＭＡＣアドレス（１）とグループＩＤ（１００）とを対応付け、ポート番号（Ｐ２）に機器Ｄ２のＭＡＣアドレス（２）とグループＩＤ（１００）とを対応付けたアドレステーブル１ａに更新する。

【００５１】
その後、集線装置１は、ポート番号（Ｐ１）からフレームデータを入力した場合には、アドレステーブル１ａを参照して同じグループＩＤの機器Ｄ２が接続されているポート番号（Ｐ２）からのみフレームデータを転送し、逆に、ポート番号（Ｐ２）からフレームデータを入力した場合には、アドレステーブル１ａを参照して同じグループＩＤの機器Ｄ１が接続されているポート番号（Ｐ１）からのみフレームデータを転送する。

【００５２】
以上のように、本発明を適用したセキュリティ通信システムは、ポートＶＬＡＮを構築するために、ＲＡＤＩＵＳサーバ３によって、ＶＰＮサーバ２によるＶＰＮ設定がなされたことを検知した場合に、機器Ｄ１，機器Ｄ２間でデータリンク層のセキュリティ設定を行うので、機器Ｄ１、機器Ｄ２が相互にネットワーク層におけるセキュリティを保持したい場合のみにポートＶＬＡＮを設定でき、セキュアな通信を行う機器同士を確実に識別してポートＶＬＡＮを構築できる。

【００５３】
また、このセキュリティ通信システムによれば、ＲＡＤＩＵＳサーバ３によって、ＶＰＮサーバ２によってＶＰＮ設定がなされ、且つ集線装置１のポートに接続された機器Ｄ１，機器Ｄ２を識別して、集線装置１のアドレステーブル１ａを書き換えてパス制御をさせるので、ＶＰＮ設定の設定結果をアドレステーブル１ａに反映させてパス制御を行わせることができる。

【００５４】
なお、上述の実施の形態は本発明の一例である。このため、本発明は、上述の実施形態

に限定されることはなく、この実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

【図面の簡単な説明】

【００５５】

【図１】本発明を適用したセキュリティ通信システムの構成を示すシステム図である。

【図２】本発明を適用したセキュリティ通信システムの他の構成を示すシステム図である。

【図３】集線装置及び機器の構成を示すブロック図である。

【図４】機器間でポートＶＬＡＮを構築するときの処理手順を示すフローチャートである。

【図５】ＲＡＤＩＵＳサーバに記憶される、ユーザＩＤ、パスワード、ポート番号、ＭＡＣアドレスを対応付けたテーブルを示す図である。

【図６】ＶＰＮサーバに記憶される、ＶＰＮ番号、ＭＡＣアドレスを対応付けたテーブルを示す図である。

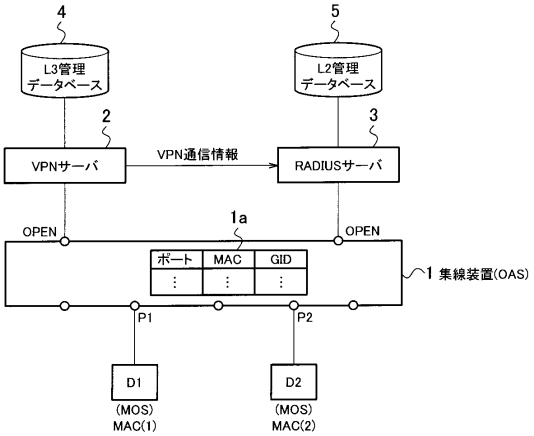
【図７】ＲＡＤＩＵＳサーバに記憶される、集線装置のＩＤ、グループＩＤ、ポートの接続状態を対応付けたテーブルを示す図である。

【符号の説明】

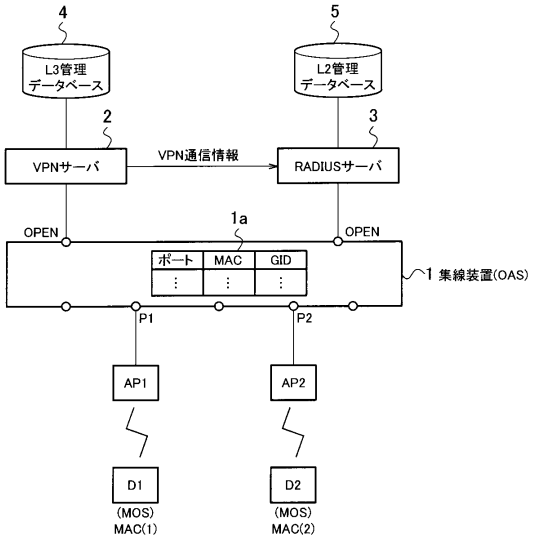
【００５６】

１　集線装置
１ａ　アドレステーブル
２　ＶＰＮサーバ
２　ＲＡＤＩＵＳサーバ
３　ＲＡＤＩＵＳサーバ
４　Ｌ３用管理データベース
５　Ｌ２用管理データベース
１１　ＭＯＳ機能部
１１ａ　機能
１１ｂ　イベント
１１ｃ　変数
１１ｄ　オブジェクトＩＤ
１１ｅ　サービステーブル
１２　アプリケーション処理部
１３　インターフェースモジュール
１４　能力テーブル
２１　ＯＡＳ機能部
２１ａ　デバイスアクセスサーバ
２１ｂ　サービス情報
２１ｃ　デバイスアクセスコントローラ
２２　パス制御部
２３　通信モジュール

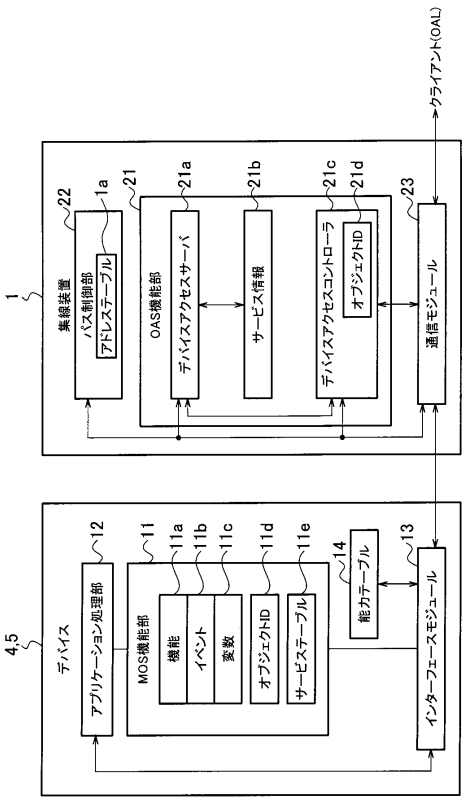
【図１】


4
L3管理データベース
5
L2管理データベース
2
VPNサーバ
VPN通信情報
3
RADIUSサーバ
OPEN
1a
OPEN
ポート
MAC
GID
1 集線装置(OAS)
P1
P2
D1
(MOS)
MAC(1)
D2
(MOS)
MAC(2)

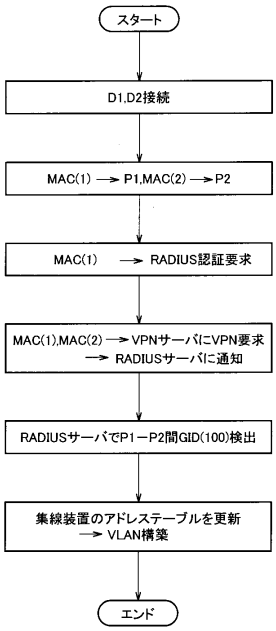
【図２】


4
L3管理データベース
5
L2管理データベース
2
VPNサーバ
VPN通信情報
3
RADIUSサーバ
1a
OPEN
OPEN
ポート
MAC
GID
1 集線装置(OAS)
P1
P2
AP1
AP2
D1
(MOS)
MAC(1)
D2
(MOS)
MAC(2)

【図３】


クライアント(OAL)
1
集線装置
22
1a
21
21a
21b
21c
21d
23
パス制御部
アドレステーブル
OAS機能部
デバイスアクセスサーバ
サービス情報
デバイスアクセスコントローラ
オブジェクトID
通信モジュール
4,5
デバイス
12
11
11a
11b
11c
11d
11e
14
13
アプリケーション処理部
MOS機能部
機能
イベント
変数
オブジェクトID
サービステーブル
能力テーブル
インターフェースモジュール

【図４】


スタート
D1,D2接続
MAC(1) → P1,MAC(2) → P2
MAC(1) → RADIUS認証要求
MAC(1),MAC(2) → VPNサーバにVPN要求
→ RADIUSサーバに通知
RADIUSサーバでP1－P2間GID(100)検出
集線装置のアドレステーブルを更新
→ VLAN構築
エンド

【図５】

RADIUS認証テーブル

ユーザID	パスワード	ポート番号	MACアドレス
△△	×××	P1	MAC(1)
□□	○○○	P2	MAC(2)
⋮	⋮	⋮	⋮

【図６】

L3用サーバ管理テーブル

No.	VPN番号	MAC	MAC
1	200	MAC(1)	MAC(2)
⋮	⋮	⋮	⋮

【図７】

L2用データベース(RADIUSサーバ)

No.	SWID	GID	P1	P2	…	Pn
1	1	100	1 (接続)	1 (接続)	…	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮

フロントページの続き

(56)参考文献 特開２００４－３０４５７４（ＪＰ，Ａ）
特開２００２－３１４５７３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／４６