

明細書

発明の名称
通信装置及び異機種間通信制御方法及び運用管理の専門性の排除方法

5

技術分野
本発明は、通信装置及び異機種間通信制御方法及び運用管理の専門性排除方法に関する物
です。

10

背景技術
1980 年代中頃まではコンピュータは、汎用機と入力端末の組み合わせによって構成され
ており、すべての処理は、中央の汎用機によって処理されると言った閉じた空間での運用
でした。

15

しかし、その後 LAN や WAN によって繋がれた社内ネットワーク環境が導入され、1995 年
頃からインターネットによって繋がれた社内外のネットワーク環境こそがコンピュータシ
ステムへと変化し、昨今はクラウドと言ったサービスが開始され、その形態に益々拍車が
かかり社外のリソースとの接続、さらにビジネスがグローバル化し国境を超えたネットワ
ーク接続が通常の接続となって来ました。今や情報は、国境を越えた安全なネットワーク
を使い伝達される事が重要となっています。

20

クラウドサービスは、インターネットとペアとなり利用いたしますが、インターネット
はセキュリティ面から考えると大変危険な為に、安全なネットワークの構築が必要です。
しかし、安全なネットワーク接続を行うには複雑で多様な接続形態への対応と言った課題
があり、この課題を解決する為には高価な機器、高度なネットワーク設計、その為に高度
なネットワーク専門技術者の確保と言った新たな課題が浮き彫りになり、アドレスの管理、
アドレスの枯渇と言った課題があります。

25

特許文献 1 に示したような先行技術は有るが、この技術ではインターネット、LAN、WAN
等にて定められたアドレスの大きさをプロクシーが独自の大きさのアドレスに変えると言
った事を行っているが、本発明ではこの様なアドレスの大きさを変えることなく、そのネ
ットワーク上で定められた大きさのアドレスのまま利用でき、プロクシー等の設置が不要
と成り運用が格段に簡素化され、企業間合併等にて異なる LAN、WAN 等の結合によってアド
レスが重複すると言った問題が起きた時にもさまざまな問題を解決できます。

30

先行技術文献

35

特許文献
特許文献 1：特許第 4802295 号公報

発明の概要

40

発明が解決しようとする課題
運用管理効率を向上させるためには、自立分散型システムとし、トラフィックを分散さ
せ中継器の負荷を軽減し、自己学習機能により、運用維持管理機能を自動化する必要が有
ります。つまり、インターネット上に暗号化網を独自に構築出来る技術が必要になります。
アドレスが競合するような事が起こり得る異なるネットワークどうしの統合はアドレス
等の管理が必要です。又、現在の技術では、安全なネットワーク設計が容易ではなく、期
待通りに稼働するネットワークを迅速かつ手間なく構築・運用できるようにするには、ネ
ットワーク設計の手法そのものを工夫が必要であり、アプリケーションごとにアドレスの
再配布と言ったネットワーク設計をするのではネットワークはシンプルにならず、ネット
ワーク機器の設定変更を伴うため莫大な投資が必要と言った課題があります。

50

課題を解決するための手段

本発明は、アドレスを集中管理し、端末毎にアドレスを自動付加出来るようにする事や、中継器の自己学習機能により運用維持管理機能の自動化による利用者の専門知識が無くとも安全なネットワークを自由に構築する能力を提供することにより、誰でもが簡単に安全なネットワークを構築出来る事を最も主要な特徴とする技術の提供及び運用方法です。

発明の効果

本発明のネットワーク環境整備システムは、利用者の専門的知識が不要で自由に安全なネットワークを簡単に構築できるという利点があります。

図面の簡単な説明

図 1 は本発明の一例を示す全体構成図

図 2 はデバイスの初期化方法図

図 3 はデバイスの死活状況確認方法図

図 4 はデバイスの管理情報更新方法図

図 5 は管理者通知方法図

図 6 はデバイス接続認証方法図

図 7 は終端ソフト登録方法図

図 8 は終端ソフト接続方法図

図 9 は終端ソフト切断方法図 1

図 10 は終端ソフト切断方法図 2

図 11 は終端ソフト切断方法図 3

図 12 はアドレスの変換方法図

図 13 はアドレス変換例送信図

図 14 はアドレス変換例返信図

発明を実施するための形態

実施例

図 1 は、本発明の実地形態の例であるネットワークシステムの全体概要図である。

本発明は、ネットワーク情報を一元的に管理することにより、これまで煩雑であったネットワーク設計、構成、管理作業量を削減し、効率化の為にインターネットとは論理的に隔離されたネットワークを定義することにより、インターネットからの脅威に対し保護する機能を提供する為に、オペレーションセンター101、認証局 102、コンソール 103 が有り、管理ネットワーク 104 を構成する。

終端ソフト 108 は PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等の端末にインストールされた本発明ソフトウェアであり、PC109 はネットワークに接続された本発明ソフトウェアがインストールされていない PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等である。終端ソフト 108 と PC109 や LAN110 やインターネット 106 を経由しデバイス 107 に接続し、デバイス 107 が管理ネットワーク 104 を経由しオペレーションセンター101 に接続し認証局 103 で正規ユーザーである事が認証されると、デバイス 107 とうしが実ネットワーク 105 を構築し、終端ソフト 108 や PC109 などとメッシュ状の実ネットワーク 105 にて暗号通信を行い安全なデータ交換を行う。

発明者及び出願人が独自に名称を付している、各々のソフトウェアおよび装置によって本発明の実ネットワークを構築するので下記に記載する。

・オペレーションセンター101

ネットワーク情報を管理し、既存のネットワークとは論理的に隔離されたネットワークを構成する為に必要な本発明の実ネットワーク内だけで使用する実アドレス管理機能を持ち、ネットワークシステム 100 内で発生する事象をログとして記録する機能や認証局 102 を持ち、管理者に対し GUI による操作を可能とするコンソール 103 を持つ。

前記、実アドレスとは本発明が新たに作成管理し、本発明内で運用される通信機器等がデータを送信する際、送り先の装置、機器、サービス、ソフトウェア等を特定する為の識別子。

・認証局 102

5 デバイス 107、終端ソフト 108、PC109 等が実ネットワーク 105 を利用するにあたって、正規ユーザーか判断する証明書を管理する、公開鍵証明書発行管理機能を持つ認証局。

・コンソール 103

10 オペレーションセンター101 への GUI クライアントであり、オペレーションセンター101 へのデータ入力、更新、削除、参照処理及びオペレーションセンター101 情報を活用し必要なデータを作成する。

・管理ネットワーク 104

本発明の実ネットワークを運営管理する為、コンソール 103 がオペレーションセンター101 に接続し、終端ソフト 108、PC109 などがオペレーションセンター101 を経由し認証局 102 に認証を受けるための暗号化された安全な通信経路。

15 ・実ネットワーク 105

デバイス 107 や終端ソフト 108、PC109 などの間で暗号通信を行う本発明の安全な通信経路。

・インターネット 106

インターネットプロトコルを利用したコンピュータネットワーク。

20 ・デバイス 107

オペレーションセンター101 と通信する機能を持ち、セキュリティ機能、実ネットワーク 105 の制御機能を提供し、終端ソフト 108 及び PC109 からの通信を制御する。

・終端ソフト 108

25 PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等を実装する本発明のクライアントソフトウェア。

・PC 109

PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等の汎用装置。

・LAN 110

30 一般的なローカルエリアネットワーク。

図2は、本発明の初期設定について記載した図である。初期設定の目的は、新規に安全な本発明の実ネットワークを構築する際、オペレーションセンター101 に安全な本発明の実ネットワークのオーナー情報を設定し、オーナー配下のグループを構成する。各設置先に
35 配備されるデバイス 107 の初期設定は、各設置先でデバイス 107 をインターネットに接続し、初期化鍵をデバイス 107 に読み込ませ自動設定させることにより、デバイス 107 が管理ネットワークに接続されるようにセットアップする事である。

図2のオーナー情報入力 201 は、オペレーションセンター101 のオーナー情報として担当者、部門名、メールアドレス、FAX 番号、TEL 番号、一般的なアドレス等の情報を入力し、
40 入力されたオーナー情報を受信したオーナー情報登録 202 は、一般的なアドレスから本発明の実ネットワークで使用するユニークな実アドレスにハッシュ関数を使い変換し、実ネットワーク名などの実ネットワーク内で使用される実ネットワーク情報を自動生成し、オーナー情報と実ネットワーク情報をオペレーションセンター101 の管理情報に登録する。デバイス情報入力 203 は、デバイス 107 のデバイス情報として設置場所、シリアル番号、一般のネットワークへの接続条件等を入力し、入力されたデバイス情報を受信したデバイス
45 情報登録 204 は、デバイス 107 がオペレーションセンター101 に対し接続する際の情報としてプロトコル、ゲートウェイ等をオペレーションセンター101 のデータベースに接続情報として登録し、自動生成した仮 ID、パスワード、証明書情報等を認証局 102 の暗号データベースに認証情報として登録する。接続情報を暗号化 206 は、デバイス 107 がオペレーション
50 センター101 に対し接続する際の接続情報を共通鍵暗号方式にて暗号化し、暗号化した情報を媒体に書き込む。この事によりデバイス 107 がオペレーションセンター101 に対し接続

する際の接続情報作成作業をコンソール 103 の設置場所であればどこでも行えるので作業の効率化を図る事が出来る。さらに、本発明では、この接続情報を使用しデバイス 107 がオペレーションセンター101 に接続する際の初期化鍵と成るのでこの暗号化した接続情報を初期化鍵と言う。初期化鍵メール送信 207 は、初期化鍵をデバイス設置先の管理者にメール等にて送信する。接続情報を暗号化 206 にて接続情報を暗号化する為に使用した暗号鍵は独自のアルゴリズムにて生成し、共有される。郵送 208 は、デバイス 107 を郵送にてオペレーションセンター101の管理情報に書き込まれたデバイス107の設置場所管理者に郵送する。情報取り込み 210 は、デバイス 107 の設置場所に届いたデバイス 107 とメール等にて届いた初期化鍵を外部記憶媒体に書き込み、初期化鍵の復号化 211 にて、デバイス 107 に前記外部記憶媒体を接続させ外部記憶媒体に記憶されている初期化鍵と共通暗号化鍵を読み込む。初期化鍵の復号化 211 は、外部記憶媒体の共通暗号鍵を使用し、外部記憶媒体の暗号化された初期化鍵を復号化させ、オペレーションセンター101にデバイス 107 が接続するための情報を取り出す。オペレーションセンター接続 212 は、復号化された初期化鍵にてデバイス 107 が、オペレーションセンター101 と暗号通信にて接続する。認証 213 は、デバイス 107 から送信された仮 ID、パスワード、証明書にてデバイス 107 を確認する。正規だと認証できなかった時、エラー処理 214 を実行しエラー内容をログに出力する。認証できた場合は、実ネットワーク送信 215 にてデバイス 107 に対して、既存アドレス、本発明の実アドレス等を作成し本発明の実ネットワーク情報をデバイス 107 に対し送信する。

デバイス 107 は実ネットワーク受信処理 216 により実ネットワーク情報を受信し、デバイス構成処理 217 にてデバイス自身が実ネットワークに接続できるように初期設定を行う。

図 3 は、本発明のデバイスの死活監視について記載した図である。

デバイス 107 の死活状況をオペレーションセンター101 及び他デバイス 107 が認識し、実ネットワークのメンバーとして適切で無いとオペレーションセンター101 及び他デバイス 107 が判断した場合、対象となるデバイス 107 を実ネットワークから取り除き、残されたデバイス 107 にて本発明の実ネットワークを再構築し、実行状況をログに残し、管理者に状況を通ずる事を目的とする。

図 3 の状況チェック 301 は、定期的にデバイス 107 がデバイス 107 自身のセルフチェックを行い、デバイス 107 自身の状況を確認し、あらかじめオペレーションセンター101 と取り決めた稼働状況をコード化する。状況通知 305 は、コード化した稼働状況を定期的にオペレーションセンター101 に送信する。通知チェック 306 は、あらかじめ決められた一定期間、デバイス 107 からの稼働状況通知を待ち、一定期間内にデバイス 107 から稼働状況通知が無い場合は、デバイス 107 に対し稼働状況通知要求を行いそれでもデバイス 107 から稼働状況通知が無い場合、そのデバイス 107 の設置場所や本発明で取り決めたデバイス 107 の実アドレス等のデバイス 107 が特定出来る情報を、稼働状況通知無し情報としてエラーログに出力する。デバイス 107 からの稼働状況通知は有ったものの稼働状況通知内容がエラーだった場合もそのデバイス 107 が特定出来る情報をエラー情報としてエラーログに出力する。デバイス 107 からの稼働状況通知情報が致命的なエラーの場合は、デバイス致命的エラーとして管理情報に記録し、今回通知の有ったデバイス 107 以外のデバイス 107 に対し今回通知の有ったデバイス 107 が使用不可能な為、実ネットワークから排除する為の情報として活用する。通知チェック 306 に対し、一定期間内にデバイス 107 から稼働状況通知が有るかその稼働状況通知がエラーでは無く、デバイス 107 の設定内容が変化しと言った情報の場合、オペレーションセンター101 は、自身が保存しているデバイス 107 の情報と比較し変化の有った情報を新たなデバイス 107 情報とし情報変更処理 314 にてオペレーションセンター101 の管理情報を更新する。

図 4 は、オペレーションセンター101 の管理情報が更新された場合、同一グループのデバイス 107 はオペレーションセンター101 から管理情報を取り込み、新たな実ネットワークを構築する事を目的とする。

管理情報が更新されているか管理情報判断 401 にて判断し、管理情報が更新されていると判断した場合、管理情報変換 402 は、管理情報を送信データとし作成する。デバイス 107 の管理情報送信依頼 403 よりオペレーションセンター101 に対し管理情報の送信を依頼し、依頼を受けたオペレーションセンター101 は管理情報送信 404 にてデバイス 107 に対し管理

情報を送信する。管理情報を受け取ったデバイス 107 は、デバイス 107 の OS に対し通信状況の確認コマンドを実行し、デバイス 107 自身の通信状況がどの様に成っているか最新情報を取得し、受信した管理情報とデバイス 107 自身の通信状況と比較し他デバイス 107 の増減を認識し、管理情報から削除された他デバイス 107 が有ったときは、対象と成るデバイス 107 との一切の通信を行えないよう処理し、対象デバイス除外報告を除外処理終了報告 410 にてオペレーションセンター101 に対し通知する。

この時、増加したデバイスが有った場合、デバイス追加処理を行う。(図 6 参照)

コンソールよりの強制切断 412 にてデバイス 107 の強制排除処理を行った場合、強制排除されたデバイス 107 が所属していたグループの他デバイス 107 に対しデバイス 107 を強制排除した事を一斉に通知する。この通知を受けたコンソール 107 は即座に強制排除されたデバイス 107 と一切の通信を行えないよう処理し、対象デバイス除外報告を除外処理終了報告 410 にてオペレーションセンター101 に対し通知する。

図 5 は、オペレーションセンター101 の最新ログから緊急状態を確認した時、管理者に緊急性の有るエラーを報告する事を目的とする。

オペレーションセンター101 のログ処理では、定期的にオペレーションセンター101 のデータベースに確保されているログの確認を行い、ログが前回確認した時より新たに追加されている時、新たなログを読み取りそのログ内容に緊急性が有ると緊急性判断処理 503 にて判断した時、その緊急内容を通知内容編集処理 504 にて編集し、通知先を通知先確保処理 505 にて確保し、管理者にメール等にて通知する。

図 6 は、同一グループ内に新規デバイス 107 が追加された時、そのデバイス 107 を他のデバイス 107 が物理的に接続されたことを確認認証し新たな実ネットワークの構成メンバーとする事を目的とする。

死活確認等の処理にて新たなデバイス 107 が追加された時、ファイアウォール設定 601、ファイアウォール設定 603 にて相手のデバイス 107 と通信が行えるようにファイアウォールの設定を変更する。接続要求 602 は、相手のデバイス 107 に対し通信接続要求を行い、通信接続要求はお互いに行うが、通信接続要求を受けた側は、接続応答 604 に即座に切り替える。接続応答 604 は、相手側デバイス 107 に対し接続準備完了を通知する。接続準備完了を受けたデバイス 107 は相手側デバイス 107 に対し、オペレーションセンター101 から受信した変更管理情報からパスワード認証 605 によって相手側デバイス 107 に対し ID、パスワード、証明書等を送信する。ID、パスワード、証明書等を受信したデバイス 107 は、ID、パスワード、証明書をオペレーションセンター101 から受信した変更管理情報から認証 OK606 によって照合確認し、照合確認できない時は、FW 通信不可 607 によりファイアウォールの設定を変更し、相手側デバイス 107 との通信を強制切断する。照合確認できた時は、通信許可 608 によって相手側デバイス 107 に対し通信許可を与え、暗号接続 609 と暗号接続 610 にて暗号通信を確立し、デバイス 107 にて、暗号接続済報告 611 と暗号接続済報告 612 にて暗号通信が確立した事をオペレーションセンター101 に報告し、オペレーションセンター101 では暗号接続済報告受信 613 にて受信しデバイス追加処理完了記録 614 によってオペレーションセンター101 の管理情報にデバイス追加完了を記録する。

図 7 の目的は、新たに端末ソフト 108 を設置する際、コンソール 103 よりオペレーションセンター101 に指示することにより、オペレーションセンター101 が端末ソフト 108 用の証明書を発行し、発行した証明書を暗号化する。暗号化された証明書と接続情報を新たに端末ソフト 108 として追加される PC 等の管理者に受け渡す事。

クライアント証明書発行指示 701 とクライアント証明書発行 702 は、新規の端末ソフトを PC、タブレット型コンピュータやスマートフォンを含む携帯型多機能情報端末等にセットアップする時、コンソール 103 よりオペレーションセンター101 や認証局 102 に対しクライアント証明書発行処理 702 を起動し、証明書作成のバージョン、認証局 102 がユニークに割り当てるシリアル番号を採番し、公開鍵証明書の署名方式などを端末ソフト 108 用の証明書として作成する。設定情報連結 703 は、前記処理、クライアント証明書発行 702 にて発行した証明書とオペレーションセンター情報、拡張設定情報を連結し端末ソフト接続情報とし、暗号化 704 にて端末ソフト接続情報を暗号化し、端末ソフト接続情報 705 にて、

5 5 終端ソフト 103 の管理者に対して終端ソフト接続情報メール等送信 705 にてメール等の通信手段あるいは、外部記憶媒体に暗号化した終端ソフト接続情報を書き込み郵送等の手段にて送付し、終端ソフト 103 の管理者は、終端ソフト接続情報メール等受信 706 にてメール等の通信手段あるいは、郵送等の手段にて受け取る。終端ソフト 103 の管理者は、終端ソフトインストール 707 の処理を行い該当の PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等に終端ソフトをインストールする。次に、終端ソフト 103 の管理者は、接続情報複号化 708 にて暗号化されている終端ソフト接続情報を該当の PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等に取り込ませ復号化し、終端ソフト 103 の設定を行い、ID 作成 710 にて終端ソフトが設定された PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等のユニークな ID 等を作成する。終端ソフト接続情報を使用し終端ソフトコントロールセンター認証 711 にてオペレーションセンター101 に対し接続し、認証要求を行い、認証 OK712 にて認証確認を行い、認証確認できた時、端末ソフト登録 713 にて端末ソフトを登録情報として、オペレーションセンター101 のデータベースに終端ソフトの設定が完了した PC、タブレット型コンピュータやスマートホンを含む携帯型多機能情報端末等の個別情報等を登録し、終端ソフト 108 に対し登録完了を通知する。認証 OK712 にて認証できなかったときはエラーログに認証できなかった事を出し、該当の終端ソフトとの通信を切断する。

20 図 8 は、終端ソフト 108 がデバイス 107 経由で実ネットワークに接続切断するときの動作及びコンソール 103 からデバイス 107 の追加削除やデバイス 107 の不具合等の要素から変化した場合、その変化に影響を受けるデバイス 107 に対し新たな状況をオペレーションセンター101 がブッシュ型で通知する場合の処理や、定期的にデバイス 107 がオペレーションセンター101 に対しての問い合わせに対し、オペレーションセンター101 が回答する事を目的とする。

25 図 8 の認証要求 801 は、終端ソフト 108 からオペレーションセンター101 に接続し認証要求を行い、認証された場合、オペレーションセンター101 は接続先デバイス確認 803 によって終端ソフト 108 が接続するデバイス 107 の有無をチェックし、接続するデバイス 107 が無い時は、接続先無を終端ソフト 108 に伝え回線を切断する。接続するデバイス 107 が複数あるときは、最適デバイス検索 804 にて、現時点の最小接続数等から最適なデバイス 107 を決定し、そのデバイス 107 に対し終端ソフト 108 のグローバル IP アドレス等の接続情報を接続許可指示 806 によりデバイス 107 に伝え、接続準備処理 807 により終端ソフト 108 からの通信を受け入れられるようファイアウォール等の設定を変更させ、設定が完了した段階で接続準備完了報告 808 によりオペレーションセンター101 と終端ソフト 108 に対し接続準備完了を報告する。オペレーションセンター101 は、接続先デバイス通知 809 にて終端ソフト 108 に対しデバイス 107 の一般的なアドレス等の接続方法を指示し、終端ソフト 108 は受け取った接続方法に従って通信プロトコルを決め接続認証情報送信 810 によって ID、パスワード、証明書等をデバイス 107 に送信し、オペレーションセンター101 は受け取った ID、パスワード、証明書等を確認し承認出来れば終端ソフト 108 に承認できた事を伝える。終端ソフト 108 は、暗号データ通信 812 によってデバイス 107 の暗号データ通信 813 と暗号通信を行い、デバイス 107 は受け取ったデータを宛先に送信する。

40 図 9、図 10、図 11 は、何らかの指示、又は回線状況の悪化によって回線を切断する事を目的とする。

45 図 9 は、終端ソフト 108 の回線切断指示 901 にて回線切断指示が有った時、回線切断メッセージ 902 にてデバイス 107 に対し回線切断メッセージを送信し、回線切断指示を受けたデバイス 107 は回線切断処理 903 にて回線切断を行い、終端ソフト 108 との接続ポートを遮断し、切断報告 904 にてオペレーションセンター101 に終端ソフト 108 との回線を切断した事を報告する。

50 図 10 は、終端ソフト 108 とデバイス 107 との間での通信中に、回線接続状況の悪化等によってデバイス 107 が終端ソフト 108 と通信が行えない現象が発生し、応答なし 1001 にて回線不通可能性ありと判断した場合、確認 1002 にてデバイス 107 が終端ソフト 108 に死活監視を行い、一定期間通信が行えない時にデバイス 107 は、切断 1004 にて切断処理を行い、切断報告 1005 にてオペレーションセンター101 に対し切断報告を送信する。

図 11 は、コンソール 103 より切断指示 1101 にて端末ソフト 108 とデバイス 107 との切断指示が行われた時、オペレーションセンターを経由し端末ソフト 108 と接続しているデバイス 107 に指示を行い、指示を受けたデバイス 107 は、端末ソフト切断 1104 にて切断処理を行い、オペレーションセンター 101 に対し切断報告を送信する。

図 12 は、異なる技術思想の基に作成された複数の異なるネットワークを単一のネットワークに統合する際に発生するネットワークアドレスの重複と言った課題を解決するとともに、異なるアドレスを持つ複数サーバーのアドレスを単一の本発明の実アドレスでアクセス出来る様にする事により、アドレスの数を減らしコストを削減し運用管理を簡便にする事を目的とする。

端末ソフト 108 や PC109 よりデータを異なるネットワーク上に配置されたサーバー 112 にデータを送信する際の説明図と成る。端末ソフト 108 や PC109 のデータ送信 1201 にてデバイス 107 に送信されたデータは、データフォーマット解析 1202 によって送信データを解析し、本発明内に設置されているサーバー等に対する送信又は、一般の外部ネットワークに送信するかを判断する。判断方法は、送信データの送信先アドレスを予めデバイス 107 が保持する変換テーブルと突き合わせ、登録されている時は本発明内に対する送信、登録されていない時は一般の外部送信とする。データフォーマット解析 1202 によって一般の外部送信と判断した時は、一般的なネットワーク処理を行い外部にデータを送信する。

本発明内に対する送信と判断した場合、端末ソフト 108 や PC109 からサーバーへの通信は、対向デバイス 107 が持つ実アドレスに向け実行される。この実アドレスは送信元と成る端末ソフト 108 や PC109 が所属するネットワーク内に存在しないアドレスである。この方法を用いる事により、端末ソフト 108 や PC109 とサーバーが所属するネットワークが重複しアドレスが重複する場合においても、通信を行うことを可能とする。

アドレス変換 A1205 にてアドレスを予めデバイス 107 が保持する変換テーブルに従いアドレス変換を行い、対向するデバイス 107 に送信する。変換方法の例が図 13 に記載されている。変換理由は、対向デバイス 107 に送信する経路が一般のインターネットなどの通信経路を使用するために一般的な通信機器が対向デバイス 107 にデータを送信出来る様にする為である。データ受信したデバイス 107 は、宛先が予め保持する変換テーブルに合致したアドレスの場合、アドレス変換 B1206 にて変換テーブルに従いアドレスを変換し宛先と成るサーバー 112 にデータを送信する。本説明のケースの場合は必ず宛先が変換テーブルに合致し、データは複数のパケットに分割され送受信される為、ステートフル処理を行う。データを受信したサーバー 112 は受信データをデータ受信 1207 にて処理し返信データをデータ返信 1208 にて作成する。返信データの送信先アドレスは受信データの送信元とし、送信元はサーバー自身のアドレスとし、返信データをデバイス 107 に送信する。返信データを受信したデバイス 107 はアドレス変換 C1209 にてステートフル処理を行い、アドレスを変換しデータを対向デバイス 107 に送信する。変換方法の例が図 14 に記載されている。返信データを受信したデバイス 107 はアドレス変換 D1210 にてステートフル処理にてアドレス変換を行い宛先と成る端末ソフト 108 や PC109 に送信し、端末ソフト 108 や PC109 はデータ受信 1211 にてデータを受信する。

産業上の利用可能性

今後、ますます盛んになる事が予想されるクラウドサービスの安全な機密通信技術や日本国内外と言った空間を越え、設置にかかる労力を特別な知識を不要とし、簡単に設置運用する事が出来る設置運用技術。

請求の範囲

【請求項 1】

既に個々の PC やサーバー等にアドレスが設定されている既存ネットワークに対し、自動的にユニークに成るアドレスを付与するシステムであって、

PC やサーバー等に既に設定されていたアドレスと本発明にて設定されたアドレスの 2 つのアドレスを管理し、

既に設定されているアドレスを修正変更する事無く、既に設定されているアドレスや本発明にて設定するアドレスにて安全な機密性を持たせ通信する通信技術。

【請求項 2】

デバイスを配布する際、デバイスが設置されるネットワークが持つアドレスをデバイスに設定し、デバイスに設定したアドレスをコントロールセンターにて保管し、

デバイスに設定したアドレスを基に複数の実アドレスを作成しデバイス、コントロールセンターに保管し、

保管した複数の実アドレスをデバイスに接続する PC、サーバー等用の実アドレスとし、前記 PC、サーバー等が元々既存のネットワークから割り当てられているアドレスとを合わせて二重管理するアドレス管理技術。

【請求項 3】

既存のネットワークに割り当てられているアドレスを基に使用中のアドレスとポート番号や識別子を自動的に調査分析し、未使用のアドレスとポート番号や識別子を洗い出し、アドレスとポート番号や識別子にて新たなアドレスとする自動アドレス生成技術。

【請求項 4】

異なる技術思想の基に作成された複数の異なるネットワークを単一のネットワークに統合しデータに安全な機密性を持たせ通信する技術であって、

サーバーや PC、端末ソフト等からの送信依頼データをデバイスが受信し、前記デバイスが受信したデータを解析し、

前記デバイスが保持する変換テーブルと突き合わせ、

送信先アドレスが登録されている時は、本発明内に設置されているサーバーや PC 等に対する送信とし、

送信先アドレスが登録されていない時は、一般の外部ネットワークに送信とし、一般の外部ネットワークに送信する際は、一般的な通信機器と同様の動作を行い一般のネットワークにデータを送信する。

本発明内に設置されているサーバーや PC 等に対し送信する場合は、

一般ネットワーク上を通過するデータが、一般通信機器が持つアドレスとの重複や一般通信機器の規約違反を避ける為に、前記デバイスに保存されているユニークで一般通信機器が目的の対向デバイスにデータを送信できるアドレスにデータの送信先アドレス、送信元アドレスを変換し対向デバイスにデータを送信し、

前記対向デバイスがデータを受信し、

受信したデータの送信先アドレスを解析し、前記対向デバイスが所属するネットワーク内部にて認識できるアドレスに前記デバイスが保存しているテーブルを使用し、送信先アドレスをアドレスに変換し、目的のサーバーや PC 等にデータを送信し、前記サーバーや PC 等がデータを受信する。

前記、データ受信したサーバーや PC 等が一般的なネットワーク通信と同じ方法にて返信データを作成し、

この時受信データの送信元を送信先、送信先を前記サーバーや PC 等が持つアドレスに設定し、前記対向デバイスに返信データを送信するので、前記対向デバイスは返信データを受信しステートフル処理を行い、アドレスを変換し返信データを前記デバイスに送信し、返信データを受信した前記デバイスもステートフル処理にてアドレス変換を行い宛先と成る送信元のサーバーや PC、端末ソフト等にデータを送信し、

送信元のサーバーや PC、端末ソフト等はデータを受信する通信技術。