アクセス制限のある環境下でのデータ配送手法

3F－8

滝川大介　鈴木健也　増井信彦　稲垣博人
ＮＴＴサイバーソリューション研究所
{takigawa, kenya, masui, inagaki}@aether.hil.ntt.co.jp

1. はじめに

企業内ネットワーク等の内部ネットワークはファイアウォールで外部ネットワークからのアクセスを制限されている。この内部ネットワーク内に接続されたPC等の端末にあるデータを出張先等の外部のネットワーク環境で利用したい場合、予めFD、MO、CD-ROM等の記憶媒体やノートパソコンにデータをコピーし、それらを携帯していた。しかしながら、記憶媒体に必要なデータを記録して携帯することが可能な場合とは、予め必要であることがわかっている時であり、予定外に外部ネットワーク環境でデータが必要になった場合は対処できない。そこで本稿では、外出先等でアクセス権のないネットワークで内部ネットワーク上の自分のデータを利用するため、データ配送元、配送先のネットワークにアクセス制限を設けているサーバに対してアクセス権のある2つのコマンド端末を用いることにより安全にデータを配送する方法を提案する。

2. コマンド端末を介したデータ配送方法

2. 1.アクセス権のあるコマンド端末の導入

内部ネットワーク上のデータをアクセス権のない別の内部ネットワークへインターネット等の広域網を介して配送させる場合、アクセス制限をしながら以下の点を行なわなければならない。

(1)外部ネットワークからデータ配送元となる内部ネットワークへデータ配送要求

(2)配送先、配送元を特定するための認証情報の送信

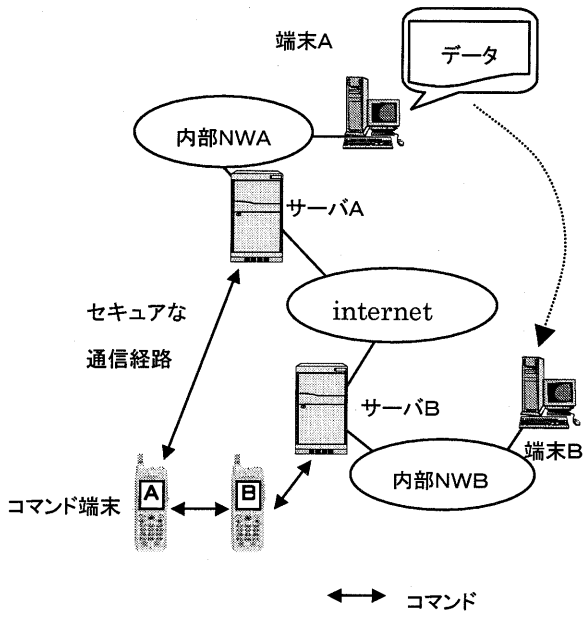

図1　システム概略図

以上の点を解決するため、図1で示されるようなアクセス制限を設ける自サーバに対して外部からアクセス権を持ち、お互いに通信可能なコマンド端末を用いたデータ配送方法を提案する。本稿で提案する方法は以下特徴と持つ。

①コマンド、配送データでの異なる通信経路

認証に必要な情報、及びデータ配送の要求をデータ配送路とは別にアクセス権のあるコマンド端末よりサーバにセキュアな通信経路、例えば無線公衆網、でサーバへ送り、配送データはインターネットを介して送る。

認証に必要な情報のやりとりはコマンド端末を用いた無線ネットワークで行なうが、データリンク層おいて安全性の確立を実現する提案もなされているが[1]、本研究ではその安全性の確立をアプリケーション層で実現させていきたい。

②コマンド端末によるサーバ代理化

A Secure Delivery Method of Data between Private Networks
Daisuke Takigawa, Kenya Suzuki, Masahiko Masui, Hirohiko Inagaki
NTT Cyber Solutions Laboratories, NTT
1-1 Hikarinooka Yokosuka-shi Kanagawa 239-0847 Japan

アクセス権のあるコマンド端末がサーバの代理となり、配送元及び配送先情報、配送データ情報の通知、データ配送要求等のコマンドを受け、それをサーバに送ることにより、アクセス権のない他の内部ネットワークへ必要とするデータを配送することが可能となる。これはコマンド端末がプロキシ機能を持つというイメージである。

③許可証の発行

コンテンツデータの受け渡しはサーバ間で安全に行なう必要があり、渡す側のコマンド端末が相手のコマンド端末に許可証を発行し、それを元にサーバ間で目的とするデータの配送のみの通信を行なう。許可証の構成として、配送データ名、コマンド端末の ID、ワンタイムパスワード、配送元サーバのアドレス、配送先サーバのアドレス等を用いる。コマンド端末が発行するデータ配送前のサーバ間の認証の流れを図2に示す。

まず配送データを渡す側のコマンド端末は二つの許可証を発行し、配送データのある内部ネットワーク側のサーバと、配送先のサーバ側へアクセス権のあるコマンド端末 B にそれぞれ渡す。許可証1には、どのコンテンツを誰が取りにくるか、という情報や、コマンド端末 B→サーバ B 経由でサーバ A に送られてくる許可証2を認証するためのパスワード等が含まれている。コマンド端末 B はコマンド端末 A から渡された許可証2をサーバ B に渡し、その許可証2を用いてインターネット経由でサーバ A に接続要求する。サーバ A は二つの許可証を合わせてサーバ B を認証し、配送データをサーバ B に送信する。このように予め、アクセス権のあるコマンド端末よりセキュアな通信経路でサーバBを認証するための情報を渡すため、配送データの受け渡し以外の不正アクセスを防止できる。

2.2. データ配送手順

内部ネットワークBにある端末Bに端末Aにあるデータを渡す場合、まずコマンド端末AによりサーバAに接続し、目的のデータを検索しデータの格納場所情報であるディレクトリ情報、ここでは端末名及び当該端末のディレクトリ情報等、を取得し、配送データを選択する。

次にデータの配送先となる内部ネットワークBへのアクセス権のあるコマンド端末Bに接続する。コマンド端末

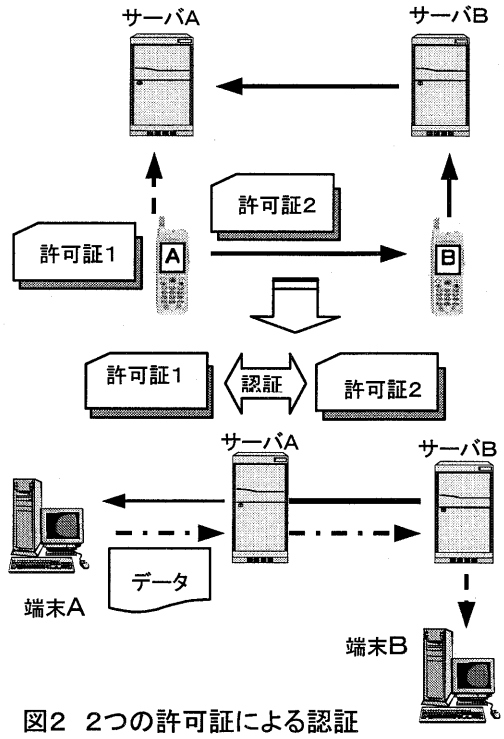

図2 2つの許可証による認証

Bはデータの配送先情報をコマンド端末Aに送信する。

コマンド端末Aは配送元の情報と配送先情報を用いて許可証のペアを作成し、コマンド端末Bに対して内部ネットワークAにアクセスするための許可証1を、サーバAに対して許可証2を送信する。

サーバAは二つの経路から送信されてきた許可証1、2を用いて認証し、端末Aからデータを取り出しサーバBに配送する。

サーバBは、配送されたデータを端末Bに送り、データ配送を終了する。

3. おわりに

本稿では、データ配送を内部ネットワークに要求するコマンド端末を用いた、異なる内部ネットワーク間でのデータ配送手法を提案した。今後コマンド端末が複数台ある場合のコマンド端末同志の特定方法を検討していきたい。

参考文献

[1]新井他：移動透過型通信環境を実現するためのセキュリティ機構の設計と実装，情報処理学会第 59 回（平成 11 年後期）全国大会論文集(3),pp247-248,1999