大規模組織における仮想ネットワーク構築に関する研究開発（041108001）

Researches on configuration method of virtual networks for large scale organizations

研究代表者

山井成良　岡山大学総合情報基盤センター

Nariyoshi Yamai, Information Technology Center, Okayama University

研究分担者

松浦敏雄†　石橋勇人†　安倍広多†　岡山聖彦††　河野圭太††

Toshio Matsuura†　Hayato Ishibashi†　Kota Abe†

Kiyohiko Okayama††　Keita Kawano††

†大阪市立大学大学院創造都市研究科　††岡山大学総合情報基盤センター

†Graduate School of Creative Cities, Osaka City University

††Information Technology Center, Okayama University

研究期間　平成 16 年度～平成 18 年度

本研究開発の概要

最近、組織外から組織内ネットワークへの安全な通信や、物理的形状に依存しないネットワーク構成を実現する技術として、VPN(Virtual Private Network)、VLAN(Virtual Local Area Network)等の仮想ネットワーク構成技術が注目されている。ところが、従来の仮想ネットワーク構成技術を大規模組織で用いる場合には、例えば組織外・下部組織間の通信や異なる下部組織同士間の通信等複数のセキュリティゲートウェイを経由する通信が柔軟に行えない等の問題があった。本研究開発では、このように独立してネットワーク管理を行うような下部組織を多数有する大規模組織において、正規の利用者であれば組織外あるいは他の下部組織からでも、自由にかつ安全に下部組織ネットワークにアクセスできるような仮想ネットワーク構築技術の確立を目指す。

Abstract

In recent years, virtual network technologies such as VPNs or VLANs, which can configure logical networks independent of the physical network structure, attract much attention. However, especially in large scale organizations having many departments, existing technologies have many problems such as poor flexibility, inefficiency, and so on, in case that two or more security gateways mediate communication. In our researches, we have developed some configuration methods of virtual networks where valid users can securely and seamlessly access to their department networks either from the Internet or from other departments.

１．まえがき

最近、組織外から組織内ネットワークへの安全な通信や、物理的形状に依存しないネットワーク構成を実現する技術として、VPN（Virtual Private Network）、VLAN（Virtual Local Area Network）等の仮想ネットワークが注目されている。ところが、従来技術を大規模組織で用いる場合には、様々な問題が生じる。

例えば、VPN は組織外からセキュリティゲートウェイ（以下、SGW）で守られた組織内ネットワークへの安全な通信を実現する技術であるが、総合大学における附属病院等、独自 SGW を設置する下部組織が存在する場合、従来の VPN 技術では、例えば附属病院と開業医の間で複数の SGW を経由するような通信を実現できなかった。また、VLAN は主に組織内ネットワークの物理的形状に依存しない高速な論理ネットワークを構成する技術であるが、多くの VLAN を持つ大規模組織では、VLAN-ID の割当てが困難であったり管理が複雑になったりする。

本研究では、このように独立した管理主体（下部組織）を多数有する大規模組織において、正規利用者であれば組織外や他の下部組織から自由に下部組織ネットワークにアクセスできるような仮想ネットワーク構築技術の確立を目指す。具体的には、(1)柔軟な構成を可能にする仮想ネットワーク構築技術の確立、(2)柔軟かつ管理が容易なアクセス制御手法の確立、(3)空間的・時間的にシームレスな接続を可能にする技術の確立という目標を設定し、VPN および VLAN それぞれに関する研究開発を行った。

２．研究内容及び成果

2.1　VPN に関する研究

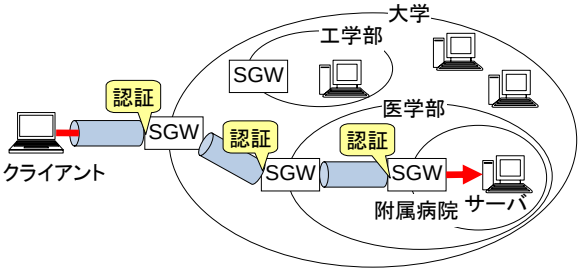

図 1　階層型 VPN の構成例

VPN では、組織等同一のアクセスポリシを持つネットワークの範囲をドメインとみなし、ドメインの境界に SGW を設置して通信を制御する。階層型 VPN ではドメインが階層的に構成されるため、組織外から部局内にアクセスするには複数の SGW を順番に辿ることになる（図 1）。

階層型 VPN に対応する従来の VPN 技術はいくつかあるが、ドメイン間で認証情報の共有を含む柔軟なアクセスポリシ管理ができないことや、複数の経路が存在する場合を考慮していないといった問題がある。そこで本研究では、主に以下の 2 点について研究開発を行った。

(1)柔軟なアクセスポリシ管理

階層型 VPN では、各 SGW が通信元・通信先に応じてアクセスの可否や認証の有無等を決定する。例えば図 1 において、他組織の医師に附属病院サーバへのアクセスを

許す場合には、大学や部局の SGW では認証を行わないといった設定を施す必要が生じる。しかし、従来技術では各 SGW の管理者間でアクセスポリシの調整を行う必要があり、管理の手間が大きい。

これを解決するため、本研究では上位ドメインのアクセスポリシ決定権を下位に委譲する手法を考案した。提案手法では、接続先が権限委譲先ドメインならば、当該ドメインの SGW は下位 SGW に問い合わせ、その結果に基づいて認証動作等を決定する。さらに、従来はドメイン毎に独自管理される認証情報を、電子認証技術（PKI）を活用して、証明書に認証情報を格納するようにした。ドメイン毎に異なるユーザ名は別名として証明書に埋め込むことにより、ユーザは 1 つの証明書を保持するだけでよい。

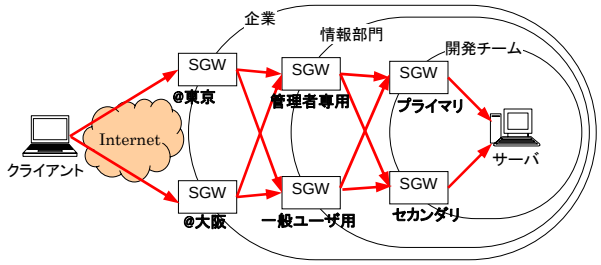

図 2　複数の経路が存在する場合

(2)仮想リンク確立のための経路制御

大規模組織では、例えば地域的に分散した本社・支社または下部組織のネットワークが個別の SGW を有する場合等が想定され（図 2）、クライアントがどの SGW を経由して仮想リンクを確立すればよいかが問題となる。

本研究では、QoS 指標として RTT（Round Trip Time）および利用可能帯域を扱うものとし、ユーザが重視する指標に基づいて経路選択を行う手法を考案した。一般に、組織外のクライアントは組織内部に直接アクセスできないため、提案手法では SGW がバケツリレー方式で指標値を収集してクライアントに通知する。このとき、SGW はユーザ名に基づいてアクセスポリシを検索し、当該ユーザがアクセスできない SGW については指標値を返さないことにより、ユーザの誤選択を防止している。

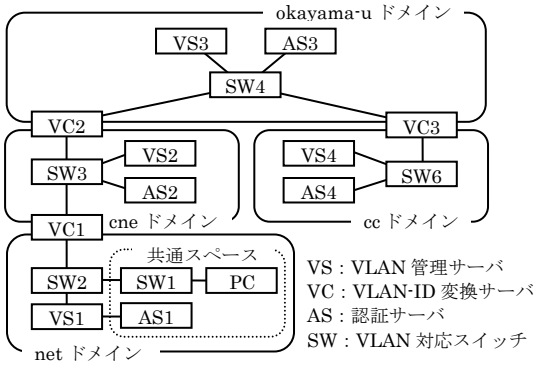

図 3　前提とするネットワーク環境

2.2 VLAN に関する研究

VLAN に関する研究では、VLAN が下部組織等複数の管理主体（以下、ドメインという）に独立して管理されるような大規模組織を対象として、VLAN-ID の不足や衝突を回避するための VLAN 相互接続方式を開発した。

前提とするネットワーク環境を図 3 に示す。提案方式では、あるドメインの共通スペース（会議室等）から自ドメインに一時接続するような用法を想定する。例えば、cc ドメイン所属のユーザが net ドメインの共通スペースから自ドメインに接続する場合、認証を受けた後、両ドメインを結ぶ全ドメインで一時 VLAN が自動構築される。このとき、各ドメインの VLAN-ID が異なるため、ドメイン境界で相互変換することにより、ドメインを跨いだレイヤ 2 レベルの高速通信を提供する。本研究では、提案方式を構成する各サーバ（VLAN 管理サーバ、VLAN-ID 変換サーバ、認証サーバ）の設計と実装を行い、図 3 と同様の実験環境上で動作を確認すると共に、VLAN-ID 変換サーバをソフトウェアで実現しているにもかかわらず、VPN に比して高スループットが得られることを確認している。

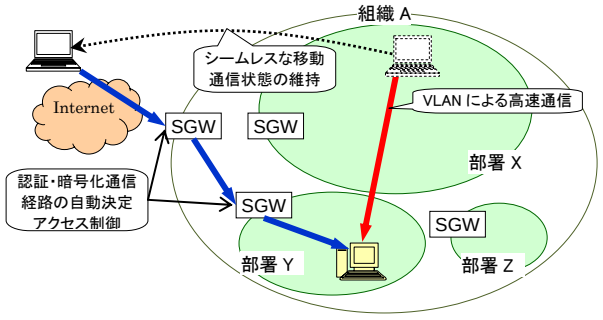

図 4　シームレス接続の例

2.3 シームレス接続に関する研究

VPN および VLAN に関する研究成果を統合し、仮想ネットワークを利用して組織内外からシームレスに接続する方式を提案した。シームレス接続の例を図 4 に示す。提案方式は、ノート PC で利用されるサスペンド機能を TCP 通信に拡張したものであり、ノート PC をサスペンドしてネットワーク上の任意の場所に移動後、レジューム時に PC の状態のみならず TCP コネクションも復元する。本研究では、(1)プロクシによる移動中の TCP 通信維持および移動後の再開機能、(2)IP アドレスに基づいた接続手段（VLAN/VPN）の自動選択機能等を設計および実装し、実験ネットワーク上の動作確認実験により、サスペンド後、数時間以上ノート PC を放置しても、TCP 通信が正常に再開できることを確認している。

3．むすび

本研究は大規模組織のセキュリティ強化と利用者の利便性を両立させるための次世代ネットワーク基盤技術に関するものであり、例えば移動端末から組織内ネットワークへのシームレスなアクセスや在宅勤務を可能とし、今後の高度情報通信社会に与える影響が大きいと予想される。

また、本研究では既存技術に基づくネットワーク機器をそのまま利用することを前提としているが、本研究を通じて大規模組織を対象とした仮想ネットワーク構築技術の重要性が認識され、現行の規格の拡張や新規格の提案、あるいは新製品の開発につながることが期待される。

【誌上発表リスト】

[1] 岡山聖彦、山井成良、二串信弘、河野圭太、岡本卓爾、“大規模 VLAN 環境における VLAN の相互接続方式”、情報処理学会論文誌 Vol.48 No.4 pp.1584-1594（平成 19 年 4 月）

[2] 岡山聖彦、山井成良、石橋勇人、安倍広多、松浦敏雄、“階層型 VPN における効率的なアクセスポリシ管理手法”、情報処理学会論文誌 Vol.47 No.4 pp.1136-1145（平成 18 年 4 月）

[3] 木澤政雄、二串信弘、岡山聖彦、山井成良、横平徳美、“利用者端末の広域移動を考慮した TCP 通信の維持”、電子情報通信学会技術研究報告 IN2006-187 pp.43-48（平成 19 年 3 月）