L-022

ALC を用いた集約可能なアドレス割り当て手法の提案
Method of allocation addresses that can be aggregated using the ALC

相川　雅英 †
Masahide Aikawa

今泉　貴史 ‡†
Takashi Imaizumi

1. はじめに

ネットワークの管理作業において、各端末の管理はアドレスを基に行われている。このアドレスは、ホストの追加に伴い順次つけられるため、一般的には、まとめて管理できるようなものではない。一方、新規のネットワークであれば、自由なアドレスの設定を行えるため、端末の特性に応じたアドレス設定も可能となる。ところが、個別のホストにアドレスを設定するのではなく、通常は DHCP などを用いたアドレス配布を用いるため、実際には端末の特性を考慮したアドレス設定はあまり行われていない。

本研究では、新規のネットワークを構築する際に、同じ扱いをするホスト群をマスクを用いてまとめて表現できるようにアドレスを割り当てる方法を提案する。このために、アクセスリストを自動生成する ALC[1] を利用する。ALC では、生成するアクセスリストをコンパクトにする際に、同じ扱いをするホスト群をまとめて扱えるようにアドレスを振り直す機能を持っている [2]。この機能を、新規のネットワーク構築の際にも利用できるようにすることで、アドレス割当てを実現する。ALC では、既に割り当てられているアドレスを用いてネットワークの構造を認識しているため、新たに構造を表現するための記述も導入する。

2. アクセスリスト生成システム (ALC)

ALC は、パケットフィルタの設定に関する管理者の負担を軽減することを目的としたシステムである。パケットフィルタリングでは、アクセスリストの生成に手間がかかり管理者の負担を増やしてしまうという欠点がある。しかし、ALC を用いることで、アクセスリストを容易に生成できる。ALC のシステム構成を図 1 に示す。システムは 3 つの記述言語の入力により処理を行う。

- トポロジーの記述
  ネットワークの構造を記述する。network で使用するネットワークを示し、router でルータがどのネットワークに接続しているかを示す。alias はホストやネットワーク群の別名を記述する。
- サービスの記述
  提供または利用したいサービスの情報を記述する。

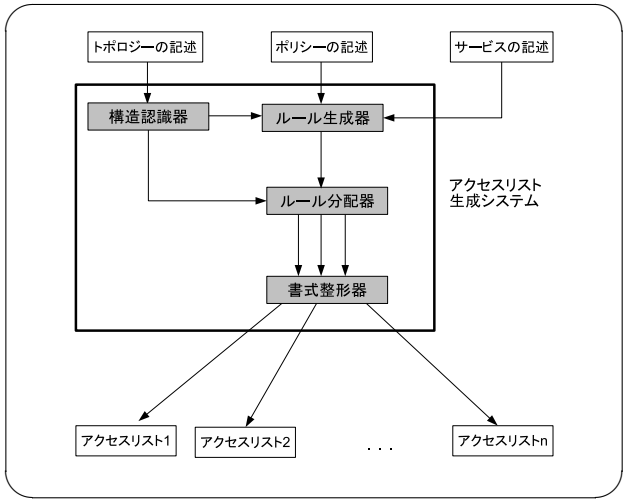

図 1: ALC システム

```
network {
    outside {IPv4 0.0.0.0/0;}
    dmz {IPv4 133.82.180.28/30;}
    inside {IPv4 133.82.0.0/16;}
}
router {
    R0:portmaster3 {
        outside.*;
        dmz.*;
    }
    R1:cisco {
        dmz.*;
        inside.*;
    }
}
alias {
    hostA {IPv4 133.82.180.30/32;}
}
```

リスト 1: トポロジーの記述例

†千葉大学大学院融合科学研究科
‡千葉大学総合メディア基盤センター

```
servise {
    ssh {
          from 1024-65535 to 22 / tcp;
    }
    www {
          from 1024-65535 to 80 / tcp;
          from 1024-65535 to 8080 / tcp;
    }
}
```

リスト 2: サービスの記述例

```
default deny ;
permit from inside ;
permit ssh between outside and hostA
```

リスト 3: ポリシーの記述例

サービスの情報は、サービスの名前、送信元ポート番号、宛て先ポート番号、プロトコルから構成される。

- ポリシーの記述
  実現したいセキュリティポリシーを記述する。許可, 禁止したいサービスと、それをどの範囲で行うかを設定する。範囲やサービスはトポロジーやサービスで指定した名前を使用する。

システムの動きとしては、まずトポロジーの記述よりネットワーク構造認識器がネットワークの構造を認識する。その後、他の記述ファイルを合わせてルール生成器でルールを生成する。さらに、生成したルールは、ルール分配器によってルール毎に適切なルータに分配される。最後に書式整形器によって目的の書式に変換し、直接ルータに設定することが可能なアクセスリストを得る。

3. ルール最適化器

ALC でアクセスリストを作成する際には、宛て先 IP アドレス以外の記述、または送信元 IP アドレス以外の記述が全て同じルールを多数含む可能性がある。ルール最適化器を用いることで、これらのルールをまとめて表現できる。

例えば、outside から同一ネットワーク内の hostA, B, C への通信を許可するアクセスリストを設定する場合を考える。それぞれのルールは、宛て先 IP アドレス以外の情報が一致するため、hostA, B, C は同じ扱いをするホスト群として扱える。この時、アドレスが図 2 の状態であるとする。この場合には、3 つのルールをまとめて、outside から「192.168.20.8/30」というアドレスへの通信を許可することで表現できる。しかし、このネットワークに「192.168.20.11/32」のアドレスを持つ hostD が存在する場合、「192.168.20.8/30」には hostD も含まれてしまうため、本来は許されない hostD への通信も許可されてしまう。このような場合、アドレス群に含まれないように hostD のアドレスを変更することで、複数のルールをまとめて表現できるようにする。

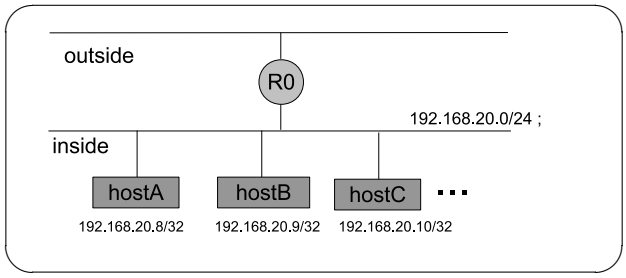

図 2: 論理ネットワーク図の例

IP アドレスは、内部的には図 3 のように分割して割り当てる。

1. ルールから同じ扱いをするホスト群を抽出する
2. 抽出したホスト群をサブネットにより分割してサムグループとする
3. (a) 複数のサムグループに所属するホストがある場合、それらのサムグループをすべてまとめてパーティーとする
   (b) 複数のサムグループに所属するホストのないサムグループは、それ単体でパーティーとする
4. パーティー内のホスト数を出現頻度と見なして、ハフマン木を構築し、パーティーにビット列を割り当てる (ハフマンビット)
5. 複数のサムグループで構築されるパーティーではサムグループ毎にビットを割り当て、各ホストのサムグループへの所属状況を表現する (パーティービット)

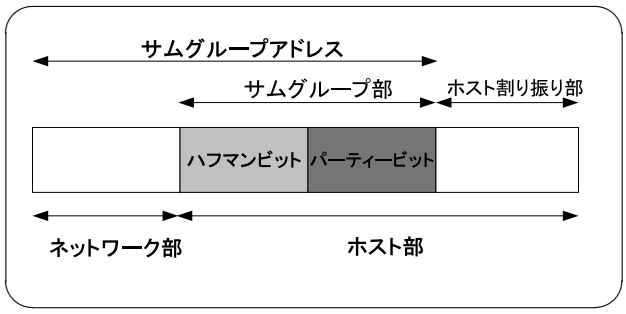

図 3: サムグループのアドレス構造

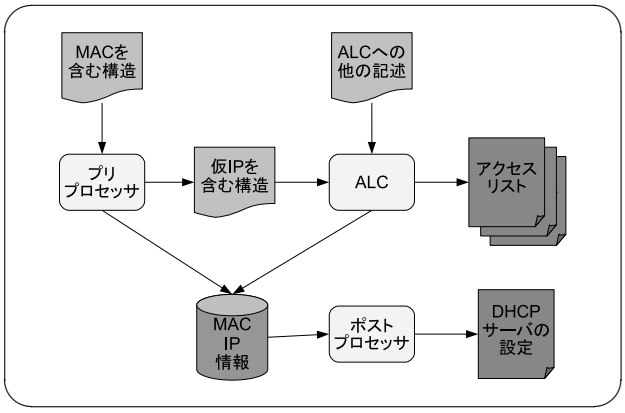

図 4: システムの概要

4.AM(Address Management)

ALC のルール最適化器が行う作業は、逆の見方をすると、同じ扱いをするホスト群に対して、マスクで表現しやすい IP アドレスを割り当てる作業と見ることができる。本研究では、この機能を新規のネットワークに適用できるようにする。しかし、新規のネットワークに対しては ALC は利用できない。これは、ALC では、IP アドレスにより各ホストの識別だけでなく所属するネットワークの識別も行っているため、必ずホストには IP アドレスが割り当てられている必要があった。しかし新規のネットワークでは、必ずしも扱うすべてのホストに IP アドレスが割り振られているとは限らない。そのため、新規のネットワークであっても、このアドレスを割り当てる機能を利用できるようする必要がある。

そのために、既存の ALC に対してプリプロセッサとポストプロセッサを追加した (図 4)。プリプロセッサでは、IP アドレスによらないネットワークの構造認識を行い、ALC で処理できるように仮の IP アドレスの割り振りを行う。ポストプロセッサでは、実際の運用時に IP アドレスの割り当てをするために、DHCP サーバに設定するファイルの生成を行う。

4.1. プリプロセッサ

プリプロセッサでは、新たな記述を加えたネットワーク構造情報からネットワークトポロジーを認識する。認識後、ALC で処理できるように仮のアドレスの割り当てを行う。

例えば、図 5 のようなネットワークの構築を行うとする。この場合、ネットワーク内は、複数のサブネットに分割される。さらに、各サブネット内にはいくつかのホストが存在し、その中の各ホストは同じ扱いをするグループとして表現できる。本システムでは、これらのネットワーク、サブネット、グループ、ホストの関係を包含関係を用いて表現する。これらの包含関係はネットワークの記述より識別される。

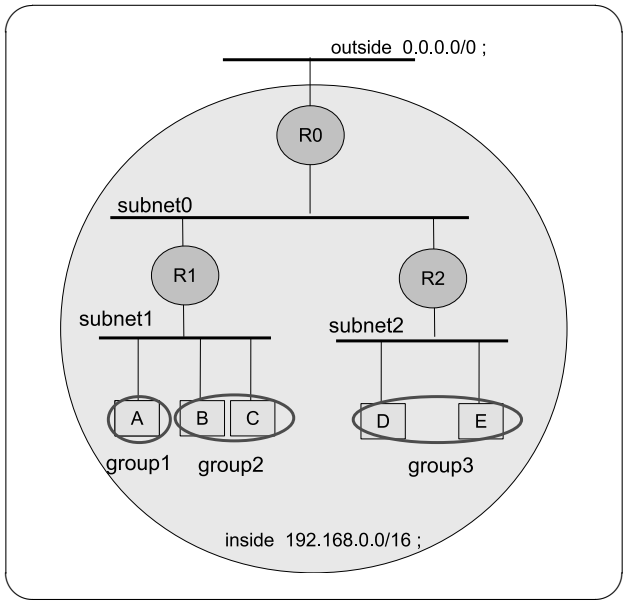

図 5: ネットワークの例

ネットワーク構造の記述は、ALC が扱う 3 つの部分と包含関係のための 2 つの部分から成る。今回の記述では、包含関係を明記する必要があるため、「:」を用いて新たに包含関係を表す記述を定義した。「:」の左側は右側に含まれるという包含関係を表す。

- 既存の ALC と同様の記述

  ネットワークの記述 設定を行うネットワークの構成をネットワーク名、IP アドレスと prefix 長の組で指定する。この時、IP アドレスは IPv4、IPv6 どちらも使用できる。

  ルータの記述 ルータがどのサブネットに接続しているかを記述する。ここで既存の ALC では、上記で定義したネットワーク名を使用して、それにルータが接続していると記述していたが、本システムでは複雑な内部のネットワーク構造を IP アドレスを使用しなくても表現できるようにするために、ルータはネットワークやサブネットに接続しているものとして表現する。

  ホストの記述 ネットワーク内に存在する、グループとして扱いたいホストを記述する。既存の ALC ではホストを IP アドレスで指定をしていたが、本記述では MAC アドレスでも行うことができる。

- 本システム独自の記述

  サブネットの記述 ネットワークに存在するサブネットを記述する。これにより、内部のネットワーク構造を細かく表現することができる。また、ホストの記述と同様に包含関係を使用して、サブネットが属すネットワークを表す。

グループの記述 サブネット内で同じ扱いをしたい集まりを記述する。これはグループという表現を用いて、同じ扱いをするホストをまとめて表現できる。これも同様に、包含関係により、グループが属すサブネットを表す。

これらの記述により、ネットワーク、サブネット、グループ、ホストは包含関係で表すことができる。ここで、各ホストは、複数のグループに属すことは可能だが、サブネットは 1 つにしか存在できない。この包含関係により、例えば hostA は group1 に属し、group1 は subnet1 に属し、subnet1 は inside に属すことがわかる。これにより、hostA は inside に属すことがわかる。これをすべてのホストに行うことで、正確にネットワークの構造を認識できるようになる。

さらに、全てのホストやサブネットに対して仮の IP アドレスを割り当てることで、記述を ALC で処理可能にする。グループに対する IP アドレスは、ルールの最適化の際に割り当てられる。

4.2. ポストプロセッサ

ポストプロセッサでは、実際の運用局面で各ホストに IP アドレスを割り当てるために、DHCP サーバの設定ファイルを生成する。まずプリプロセッサで得られる、MAC アドレスと仮 IP アドレスの対応を取得する。さらに、ALC の処理で得られる、仮 IP アドレスと本 IP アドレスの対応を取得する。これらの情報を合わせることで、必要な MAC アドレスと本 IP アドレスの対応を得ることができる。これらの情報から DHCP サーバの設定ファイルを生成でき、DHCP サーバによる IP アドレスの配布により付けられるアドレスは、マスクによる表現が可能なアドレスとなる。

4.3. 本システムの動作例

本システムの動作を示す。図 5 のネットワーク構造を想定する。この場合、ネットワークの構造を表す記述はリスト 4 のようになる。

プリプロセッサでは、ネットワークの構造を認識し、サブネットにアドレスを割り当てる。さらに、各ホストのアドレスを、属するサブネットに含まれるように仮の IP アドレスを割り当てる (図 6)。この時割り当てるのは仮の IP アドレスであるため、マスクでホスト群を表すことができるアドレス構造にはなっていない。そのため、プリプロセッサの動作時にはグループのアドレスの割り当ては行われていない。

その後、ALC の処理により、同じ扱いをするホスト群のアドレスが決まるため、このホスト群をマスクで表現したグループのアドレスが決まる。さらに、グループのアドレスが決まるので、グループに属すように各ホストに割り振るべき本 IP アドレスが決まる。例えば ALC の処理後、図 6 の hostB, C のグループは 192.168.64.128/25 というグループのアドレスが決まる。さらに、hostB, C にはそれぞれ、192.168.64.130/32,

```
network{
   outside{ 0.0.0.0/0;}
   inside{ 192.168.0.0/16;}
}
subnet{
    subnet0 : inside;
    subnet1 : inside;
    subnet2 : inside;
}
group{
    group1 : subnet1;
    group2 : subnet1;
    group3 : subnet2;
}
host{
    hostA { 11-11-11-22-22-22;} : group1
    hostB { 22-22-22-33-33-33;} : group2
    hostC { 33-33-33-44-44-44;} : group2
    hostD { 44-44-44-55-55-55;} : group3
    hostE { 192.168.96.2;} : group3
}
router{
    R0:cisco{
        outside;
        subnet0;
    }
    R1:cisco{
        subnet0;
        subnet1;
    }
    R2:cisco{
        subnet0;
        subnet2;
    }
}
```

リスト 4: ネットワーク構造の記述例

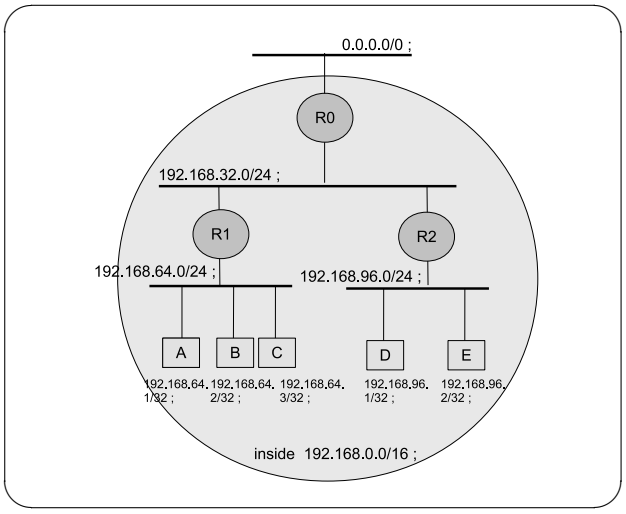

図 6: 仮の IP を含むネットワーク

192.168.64.131/32 という本 IP アドレスが振り直される。これにより、hostB, C は 192.168.64.128/25 というマスクで表現できる。

ポストプロセッサでは、ALC の処理の前後の情報から与えるべき IP アドレスと MAC の対応の情報が得られるので、各ホストにアドレスの割り当てを行うために、DHCP サーバの設定ファイルの生成を行う。DHCP はリレーエージェントの機能を使用し、集中管理することを想定しているため、各サブネットごとの設定ファイルの出力をする。この例の場合に出力される、各サブネット毎の ISC の DHCP サーバの設定ファイルの例を示す (リスト 5, 6)。

5. 考察

本システムでは、ホスト群をマスクを用いてまとめて表すため、アクセスリストで通信が許可されていても実際にはそのアドレスを持つホストが存在しない場合もある。特別な権限が付加されたアドレスが不正に利用されてしまうと、本来、そのホストが取得できる権限より高い権限で通信が行えてしまう恐れがある。そのため、権限の付加されたアドレスを不正に使用できないようにする必要がある。これは、未使用のアドレスをすべて使用しているかのようにふるまうホストを準備することで、不正にアドレスの取得を行えないようにすることが可能となる [3]。また、未使用 IP アドレスをハニーポットに割り当てる研究も提案されている [4]。これはハニーポットのサーバと DHCP サーバが連帯することで機能する。これを用いることで、未使用のアドレスはハニーポットに割り当てられるため、不正なアドレス取得を防ぐことができる。さらに、ハニーポットのアドレスに向けた不正アクセスなどを監視することができる。この手法は DHCP サーバとの連帯で行われるため、DHCP セグメントの変化に対応して管理を行うことが可能となる。今回は、未使用なアドレスを使用できないようにすることが目的であるの

```
ddns-update-style none;
subnet 192.168.64.0 netmask 255.255.255.0 {
    range 192.168.64.1 192.168.64.63;
    option broadcast-address 192.168.64.255;
    option routers 192.168.64.254;
    option subnet-mask 255.255.255.0;
    default-lease-time 6000;
    max-lease-time 72000;
}
    host A{
        hardware ethernet 11:11:11:22:22:22 ;
        fixed-address 192.168.64.100;
    }
    host B{
        hardware ethernet 22:22:22:33:33:33 ;
        fixed-address 192.168.64.130;
    }
    host C{
        hardware ethernet 33:33:33:44:44:44 ;
        fixed-address 192.168.64.131;
    }
```

リスト 5: 192.168.64.0/24 のサブネットにおける DHCP サーバの設定例

```
ddns-update-style none;
subnet 192.168.96.0 netmask 255.255.255.0 {
    range 192.168.96.1 192.168.96.127;
    option broadcast-address 192.168.96.255;
    option routers 192.168.96.254;
    option subnet-mask 255.255.255.0;
    default-lease-time 6000;
    max-lease-time 72000;
}
    host D{
        hardware ethernet 44:44:44:55:55:55 ;
        fixed-address 192.168.96.130;
    }
    host E{
        hardware ethernet 55:55:55:66:66:66 ;
        fixed-address 192.168.64.131;
    }
```

リスト 6: 192.168.96.0/24 のサブネットにおける DHCP サーバの設定例

で、[3] の方法で十分であるが、ネットワークの管理・運用を行う場合は、[4] の方法も有効である。どちらの手法も、未使用なアドレスを使用しているかのようにして管理を行うが、未使用なアドレスが膨大に存在した場合、そのすべてを管理する必要があり、機器に負荷がかかるなど問題が残る。これらの機器に対しては、未使用領域はどこなのかを示す情報を提供する必要があるが、これらはポストプロセッサの処理の際に集めた情報から生成できるため、これらのシステムに対する設定も自動生成することは可能と考える。

本来、論理的なトポロジーと物理的なトポロジーは一致しない。そのため本システムは、物理的なトポロジーを考慮した上で、論理的なトポロジーを考えた。つまり、端末の物理的な位置による制限によりサブネットを分割し、その中でマスクの表現を使用した。しかし、実際のネットワークは一般的に VLAN が使用されている。そのため、VLAN の機能を考慮してアドレス付けを行えるようにすることで、異なるサブネットに存在するが、同じ扱いをするグループをさらにまとめることが可能となる。これにより、ネットワーク内のグループの膨張を防ぐことができる。さらにネットワークをサブネットなどの制限がなく自由に表現することができる。本システムで VLAN の機能を利用するには、VLAN を使用する場合のサブネットの表現について拡張する必要がある。現在の記述の範囲では対応することは困難だが、新たな記述を導入することで対応できると考えている。

本手法では、マスクで管理できるアドレス構造にするため、ネットワーク内で使用されないアドレス数が増加し、サブネット内のアドレスの使用率が下がってしまう。そのため、アドレス資源に余裕がない状態では使用が困難な恐れがある。本手法で利用したマスクの表現をより活用するためには、VLSM に対応させることが必要である。これは、ホスト数に合わせてプレフィックス長を変更することで、未使用のアドレス数を削減することになる。これにより、IP アドレスの無駄を防ぎ、さらにグループのアドレスによる経路の集約も行うことができると思われる。ただし、現在の ALC は VLSM に対応していないため、VLSM に対応するためには ALC 本体を含めた修正が必要となる。

6. おわりに

本研究では、ホストの識別に MAC アドレスを用い、ネットワークの包含関係を別に指定することで、ALC を新規ネットワークの構築の際にも利用できるようにした。これにより、同じ扱いをするホスト群をマスクを用いてまとめて指定できるアドレス付けが行える。ホスト群の記述は様々な設定に使用できるので、ネットワークの管理が行いやすくなったと言える。

今回は、ホスト群を表すグループをネットワークの包含関係の中で表現したため、複数のサブネットにまたがるようなホスト群を表現することはできない。しかし、同じ扱いをするグループが異なるサブネットに存在していることも多い。これらの構造を正確に表現できれば、さらにホスト群をまとめることができると思われる。

参考文献

[1] 谷津 文平, 今泉 貴史. セキュアな IPv6 ネットワーク構築のためのアクセスリスト生成システム. 情報科学技術フォーラム. 2002.

[2] 加瀬 智博, 今泉 貴史. アクセスリストコンパイラにおけるルール最適化手法. 情報科学技術フォーラム. 2010.

[3] CounterACT. http://www.soliton.co.jp/products/net_security/counteract/index.html.

[4] 溝口 誠一郎, Le Malecot Erwan, 堀 良彰, 櫻井 幸一. DHCP によって管理されたセグメントに存在する未使用 IP アドレスの監視手法. 情報処理学会研究報告. CSEC, [コンピュータセキュリティ]. 2008.

[5] RFC2131. Dynamic Host Configuration Protocol. http://www.ietf.org/rfc/rfc2131.txt.

[6] DHCP4.2.4(ISC). http://www.isc.org/software/dhcp.

[7] マルチメディア通信研究会編 笠野 英松 監修. インターネット RFC 事典. アスキー出版局. 1998.

[8] 村井 純・楠本 博之 訳 Dougles E.Comer 著. TCP/IP によるネットワーク構築 Vol. (第 4 版)-原理・プロトコルアーキテクチャー. 共立出版株式会社. 2002.

[9] 井上 尚司 監訳 W リチャードスティーヴンス 著. 詳解 TCP/IP Vol.1 プロトコル. 株式会社ピアソンエデュケーション. 2000.

[10] IRI・ユビキタス研究所 共著. マスタリング TCP/IP IPv6 編. 株式会社オーム社. 2005.

[11] D.Brent Chapman Elizabeth D.Zwichy 共著, 歌代 和正 監訳, 鈴木 克彦 訳. ファイアウォール構築 インターネット・セキュリティ. 株式会社ピアソンエデュケーション. 2002.

[12] 片岡 巌. ファイアウォール&ネットワークセキュリティ 実戦テクニック. 株式会社技術評論社. 2001.

[13] VLSM とは. http://www.7key.jp/nw/routing/vlsm.html.

[14] VLAN とは. http://www.7key.jp/nw/lan/vpn/vlan.html.