# 冗長構成ネットワークにおける外部プログラムを用いた動的ルーティング手法

山井成良† 宮下卓也†

複数の基幹ネットワークを持つ組織では，耐故障性を高めるために支線ネットワークを複数の基幹ネットワークに接続した冗長構成がよく採用されている．このような構成では動的ルーティングが不可欠であるが，従来の動的ルーティングでは直接接続されたインタフェースをつねに優先して利用するために，高速の迂回路を優先利用できないなどの問題があった．そこで本稿では冗長構成ネットワークにおいて，インタフェースの有効・無効状態など，インタフェースの設定を外部プログラムを用いて変更する動的ルーティング手法を提案する．これにより，通常時には優先すべき通信経路を選択しながら，障害時には直接接続されたインタフェースを用いて障害箇所を迂回することが可能となる．また，外部プログラムを実装して岡山大学の学内ネットワーク上で運用することによりその有効性を確認した．

# A Dynamic Routing Method of Redundant Network with an External Program

Nariyoshi Yamai† and Takuya Miyashita†

Redundant network is a common structure for organizations with multiple backbones to construct a fault tolerant network. To tolerate network troubles on such a structure, a dynamic routing method is essential. However, existing dynamic routing methods have some problems. For example, with existing methods, packets to a subnet are always sent via the direct interface to that subnet even if there exists another faster route. In this paper, we propose a new dynamic routing method with an external program called a *routing program*, which controls some properties of interfaces such as up/down states and subnet masks. With this method, a faster route is usually used and when this route has some troubles, the direct interface is activated. We also have introduced a routing program to the campus network of Okayama University, and have confirmed that this program works well.

## 1. はじめに

近年のネットワーク技術の急速な進展にともない，イーサネット，FDDI，ATMなど多くの種類のネットワークが次々に開発され，LANとして用いられてきた．これらのネットワークは機能・性能の面で異なった特徴を持つため，複数の種類の基幹ネットワークを敷設し，用途に応じてこれらを使い分けている組織も多い．たとえば，筆者らの所属する岡山大学ではFDDIネットワークとATMネットワーク（OC-3）の2種類の基幹ネットワークが敷設されており，前者は主に一般通信用，後者は主にマルチメディア通信用として利用されている．

ところで，このように複数の基幹ネットワークを持つ組織では，耐故障性を高めるために支線ネットワークを複数の基幹ネットワークに接続した冗長構成がよく採用されている．特に，最近はVLAN（Virtual Local Area Network）技術の普及により，物理的な構成にあまり束縛されることなくネットワークを論理的に比較的自由に構成できるようになったため，上記の冗長構成を容易に実現できるようになっている．

一方，冗長構成ネットワークにおいて実際に耐故障性を高めるためには，ネットワークの状態に応じた動的ルーティングが必要不可欠である．冗長構成ネットワークにおける動的ルーティングについてはこれまでに多くの手法が提案されており，組織内ネットワークでの動的ルーティングにはRIP[1),2)]，OSPF[3)]などのプロトコルが標準的に用いられている．これらのプロトコルを用いると，通常はたとえば最も高速の基幹ネットワークを優先的に利用し，これに障害が発生した場合にはバックアップ用の他の基幹ネットワークに

† 岡山大学総合情報処理センター
Computer Center, Okayama University

迂回することが可能となる．

ところが，現在普及している市販ルータでは，あるインタフェースに直接接続されているネットワークへのパケット送出にはつねにそのインタフェースが用いられ，上記のようなプロトコルを用いても動的ルーティングは行われない．そのため，たとえばあるルータにおいて支線ネットワークとの接続に低速のインタフェースが用いられている場合，このルータからこの支線ネットワークへのパケット送出には，ほかにさらに高速の通信経路が存在してもこのインタフェースが用いられることになる．これは，耐故障性は高まるものの通信速度の低下を招くことになり，好ましくない．

そこで，本稿では上記のような冗長構成ネットワークにおいて，外部プログラムを用いた動的ルーティング手法を提案する．本手法では，インタフェースのアップ・ダウンなど従来の動的ルーティング手法では制御の対象とならなかったインタフェースの設定を変更することにより，通常時には優先すべき通信経路を選択しながら，障害時には直接接続されたインタフェースを用いて障害箇所を迂回し，耐故障性を高めることが可能となる．

以下，2 章では対象となるネットワーク構成とその問題点を明らかにし，3 章では本手法の原理と動作手順を示す．4 章では筆者らが所属する岡山大学における運用例を紹介する．最後に 5 章でまとめと今後の課題を述べる．

## 2. ネットワークの冗長化

### 2.1 対象ネットワーク構成

本稿では，**図 1** のように支線ネットワーク $N$ が 2 つのルータ $R_1$，$R_2$ によりそれぞれ基幹ネットワーク $B_1$，$B_2$ に接続されている構成を対象とする☆．この構成において，支線ネットワーク $N$ とルータ $R_1$ および $R_2$ との接続に用いられるインタフェースをそれぞれ $I_1$，$I_2$，また，これらのインタフェースに接続されているリンクをそれぞれ $L_1$，$L_2$ と記し，$L_2$ が $L_1$ より優先されるものとする．また，ルータ $R_1$ には別のネットワーク $O$ が接続されており，ネットワーク $N$–$O$ 間で通信が行われるものとする☆☆．支線ネットワーク $N$ 内では RIP などのプロトコルを用いて経路

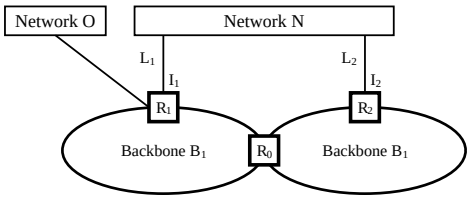


**図 1** 対象ネットワーク構成
Fig. 1 Target network configuration.

情報が広報されており，支線ネットワーク $N$ に接続されている機器はこの経路情報に基づき動的に通信経路を選択するものとする．

このようなネットワーク構成は複数の基幹ネットワークを有する組織ではよく見受けられる．たとえば，基幹ネットワーク $B_1$，$B_2$ としてそれぞれ FDDI とギガビットイーサネットが敷設されており，前者にすべての支線ネットワークが 10 Mbps で接続され，また後者に一部の支線ネットワークが 100 Mbps で接続されているような場合がこれに該当する．

### 2.2 従来の障害対処手法とその問題点

図 1 のような冗長構成ネットワークに関しては，耐故障性を高めるためにこれまでに多くの障害対処手法が提案されてきた．

ルータの冗長化はその手法の 1 つで，この動作を制御するためのプロトコルとして HSRP（Hot Stanby Router Protocol）[4]，VRRP（Virtual Router Redundancy Protocol）[5] などが提案されている．しかし，この手法は複数のルータにおいて各インタフェースが同じネットワークに接続されている構成のみを対象としており，図 1 のように 2 つのルータ $R_1$，$R_2$ が異なる基幹ネットワークに接続されているような構成では適用できない．

また，レイヤ 3 レベルでの経路の冗長化は障害対処手法として最も多く用いられており，ほとんどのルータではこれを行うために RIP，OSPF などの動的ルーティングプロコトルを利用できる．ところが，現在普及している市販ルータでは，あるインタフェースに直接接続されているネットワークへのパケット送出にはつねにそのインタフェースが用いられ，動的ルーティングが行われない．このため，たとえば図 1 においてネットワーク $N$–$O$ 間で通信を行う場合，ルータ $R_1$ から支線ネットワーク $N$ へのパケット送出には，ルータ $R_2$ 経由の方が高速であってもつねにリンク $L_1$ が用いられることになる．

さらに，ネットワークの構成やネットワーク機器の機能によっては，リンク $L_1$ に障害が発生した場合，このリンク経由ではパケットが支線ネットワーク $N$

☆ 支線ネットワークが 3 つ以上の基幹ネットワークに接続されている構成についても本手法は適用可能であるが，簡単化のため本稿では扱わない．

☆☆ ネットワーク $O$ は他のネットワークに接続されていても構わないが，その場合ネットワーク $N$–$O$ 間の通信は通常時はルータ $R_1$ 経由で行われるものとする．

に到達できないにもかかわらず，他の経路に迂回されないことがある．たとえば，リンク $L_1$ においてケーブルが外れるなどの障害が発生してもインタフェース $I_1$ が無効（ダウン）状態にならないようなルータ☆が $R_1$ として用いられた場合，実際にリンク $L_1$ に障害が発生しても，支線ネットワーク $N$ に関する経路情報は他のネットワークに広報され，支線ネットワーク $N$ へのパケットは他の経路に迂回されない．また，たとえばリンク $L_1$ が VLAN などの技術を用いて仮想的に構成されていると，この仮想リンクの途中で障害が発生しても必ずしもルータ $R_1$ でこれを検出できるとは限らず，検出できない場合には上記の例と同様に支線ネットワーク $N$ へのパケットは他の経路に迂回されないことになる．

レイヤ 2 レベルでの経路の冗長化も障害対処手法の 1 つで，たとえば図 1 ではルータ $R_1$–$R_2$ 間を VLAN などの技術を用いて基幹ネットワーク $B_1$，$B_2$ 経由で仮想的なリンクを設定することにより実現することができる．この場合，IEEE 802.1d spanning tree[6] などのアルゴリズムを用いて冗長リンクのうち実際に用いるリンクが選択される．しかし，このアルゴリズムではルータのインタフェースの MAC アドレスを基にリンク選択が行われるため，必ずしもリンク $L_2$ が優先されるとは限らない．また，たとえリンク $L_2$ を優先するようなアルゴリズムがルータ $R_1$，$R_2$ に実装されていたとしても，基幹ネットワークに用いられている機器が VLAN 機能をサポートしていない場合には $R_1$–$R_2$ 間に仮想的なリンクを設定することができない．

以上のように，従来の障害対処手法には，直接接続されているインタフェースがつねに優先して選択されたり，適用できるネットワーク構成やネットワーク機器に強い制限があったりするなどの点で問題がある．

## 3. 外部プログラムによる動的ルーティング

前章で述べた問題点を考慮した障害対策手法として，本章では外部プログラムを用いた動的ルーティング手法を提案する．この外部プログラムは各ルータの状態を定期的に調べ，その結果通常の通信経路に障害が発生したと判断した場合には代替経路に迂回するように各ルータを制御する役割を果たす．以下では，このプログラムをルーティングプログラムと呼ぶ．

本手法はルータのインタフェースをルーティングプログラムにより直接制御するため，従来の動的ルーティング手法とは異なり直接接続されているインタフェースを経由しない経路を優先することも可能である．また，市販ルータが有する標準的な機能を利用して制御するため，広範囲のネットワークに適用可能であるという特徴も有する．

☆ 少なくとも岡山大学で用いられている FDDI ルータがこれに該当する．

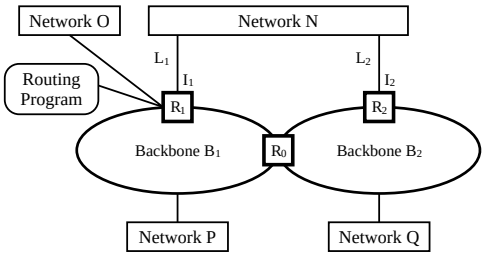


**図 2** ルーティングプログラムを導入した場合のネットワーク構成
Fig. 2 Network configuration with a routing program.

ルーティングプログラムを導入した場合のネットワーク構成を**図 2** に示す．この図において，ルーティングプログラムはルータ $R_1$ に直接接続された計算機上で動作しているが，想定しているような障害が発生してもルータ $R_1$ を制御できる場所であればどこで動作してもかまわない．

この図に示す環境において，障害はルータ $R_0$〜$R_2$，リンク $L_1$，$L_2$（あるいはインタフェース $I_1$，$I_2$），あるいは基幹ネットワーク $B_1$，$B_2$ のいずれか 1 カ所で発生する場合を想定する．すなわち，同時に 2 カ所以上で障害が発生する場合は稀であると考え，本稿では考慮しない．また，支線ネットワーク $N$ におけるリンク $L_1$，$L_2$ 以外の個所での障害発生についてもレイヤ 2 レベルでの冗長化で解決すべき問題であると考え，本稿では考慮しない．

以下では，図 2 において $L_2$ を優先する状況を例にとり，本手法の原理と動作を示す．なお，本手法ではリンク $L_1$，$L_2$ の障害を考慮するかどうかによりルータに必要な機能や動的ルーティングの動作が異なるため，それぞれの場合に分けて述べる．

### 3.1 リンクの障害を考慮しない場合

まず，リンク $L_1$，$L_2$ の障害を考慮しない場合について考える．この場合，考慮の対象となるのは，ルータあるいは基幹ネットワークの障害のみである．ルーティングプログラムはルータ $R_1$ においてインタフェース $I_1$ を適宜有効（アップ）・無効（ダウン）状態に変更することにより動的ルーティングを実現する．

以下に，本手法の具体的な動作手順を示す．

障害が発生していない通常時では，ネットワーク $N$–$O$ 間の通信がリンク $L_1$ を経由せずリンク $L_2$ を

経由するようにしておく必要がある．そのために，本手法では初期状態としてルータ $R_1$ においてインタフェース $I_1$ を通常時は無効状態にしておく．この状態ではルータ $R_1$ はリンク $L_1$ を利用することができず，基幹ネットワークを通じて広報された経路情報に基づきルータ $R_2$ 経由で通信を行うことになる．また，支線ネットワーク $N$ と $O$ 以外のネットワークとの間の通信についても同様に広報された経路情報に基づきルータ $R_2$ 経由で行われることになる．

基幹ネットワークやルータに障害が生じ，支線ネットワーク $N$ への通信がルータ $R_2$ 経由では行えなくなった場合，ルーティングプログラムはまずこれを検出する必要がある．この障害の検出についてはいくつかの方法が考えられるが，たとえば SNMP [7]を用いてルータ $R_1$ におけるネットワーク $N$ の経路情報の有無やルータ $R_2$ の反応の有無などを調べることにより検出することが可能である．あるいは，ルータの機種によってはルーティングプログラムが telnet によりルータ $R_1$ を直接制御し，ルータ $R_1$ 上で ICMP echo や telnet を用いてルータ $R_2$ への到達可能性を調べることも可能である．

障害を検出すると，ルーティングプログラムはルータ $R_1$ においてインタフェース $I_1$ を有効状態に変更し，支線ネットワーク $N$ の経路情報を基幹ネットワークに広報する．これにより，ネットワーク $N$–$O$ 間の通信がリンク $L_1$ 経由で行われることになる．また，$O$ 以外のネットワークと支線ネットワーク $N$ との通信については，広報された経路情報に基づきルータ $R_1$ あるいは $R_2$ 経由☆で行われることになる．なお，ルータ $R_1$ から支線ネットワーク $N$ の経路情報を他のネットワークに広報するとき，および他のネットワークの経路情報を支線ネットワーク $N$ に広報する場合には，RIP におけるメトリック値などを調整し，他のルータが支線ネットワーク $N$ の経路情報をルータ $R_2$ からも受け取ったときにルータ $R_2$ を優先するようにすることが望ましい．また，ルータ $R_1$，$R_2$ から視線ネットワーク $N$ へはデフォルトネットワークの経路情報だけでなく他のネットワークの経路情報についても広報し，たとえばルータ $R_0$ に障害が生じた場合でもネットワーク $N$ とネットワーク $P$，$Q$ との間で通信できるようにする．

障害から復旧すると，ルーティングプログラムはこれを検出して再びインタフェース $I_1$ を無効状態に変更する．ここで，ルーティングプログラムがどのように障害復旧を検出するかが問題となる．これについてもいくつかの方法が考えられるが，たとえば SNMP を用いてルータ $R_2$ に支線ネットワーク $N$ や $O$，デフォルトネットワークなどの経路情報を問い合わせ，これにルータ $R_2$ が正しく応答し，かつ問合せ結果が正常であれば障害から復旧したと判断することができる．

以上をまとめると，本手法では次のような手順で動的にルーティングを行うことになる．

(1) 初期状態として，インタフェース $I_1$ を無効状態に，インタフェース $I_2$ を有効状態に設定する．また，ルータ $R_1$，$R_2$ から必要な経路情報を適切な重みを付けて各ネットワークに広報するように設定する．
(2) ルーティングプログラムは定期的にルータ $R_1$，$R_2$ に状態を問い合わせ，支線ネットワーク $N$ との通信に障害が発生していないかどうかを調査する．障害を検出した場合には，次に進む．
(3) ルーティングプログラムは，障害を検出するとインタフェース $I_1$ を有効状態に変更して支線ネットワーク $N$ との通信を行えるようにし，経路情報を広報するようにする．
(4) ルーティングプログラムは，定期的にルータ $R_1$，$R_2$ に状態を問い合わせ，障害が復旧しているかどうかを調査する．障害復旧を検出した場合には，次に進む．
(5) ルーティングプログラムは，インタフェース $I_1$ を無効状態に変更し，(2) に進む．

### 3.2 リンクの障害を考慮した場合

次に，リンク $L_1$，$L_2$ の障害を考慮する場合について考える．

この場合，基本的な動作はリンクの障害を考慮しない場合と同様でよいが，障害発生・復旧の検出は前節の手順をそのまま適用することはできない．たとえば障害発生の検出については，リンク $L_2$ に障害が発生した場合でもルータ $R_2$ が支線ネットワーク $N$ の経路情報を広報し続けるため，前節で述べたようなルータ $R_1$ におけるネットワーク $N$ の経路情報の有無やルータ $R_2$ の反応の有無の確認だけでは障害発生を検出できない．また，障害検出時の動作についても，単にルータ $R_1$ のインタフェース $I_1$ を有効状態にするだけなく，ルータ $R_2$ が支線ネットワーク $N$ との通信にリンク $L_2$ を使わないように設定する必要がある．このとき，前節における初期状態と同様に単にインタフェース $I_2$ を無効状態に設定する方法が考えられる

☆ たとえばルータ $R_0$ が故障した場合，基幹ネットワーク $B_2$ に接続されている支線ネットワークから $N$ への通信はルータ $R_2$ 経由で行われる．

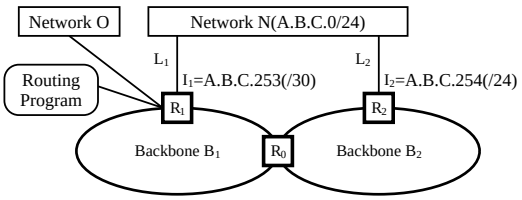


**図 3** リンクの障害を考慮する場合のネットワーク構成
Fig. 3 Network configuration for link failure recovery function.

が，この方法ではリンク $L_2$ が障害から復旧したことを検出することが困難である．

そこで，本手法ではインタフェース $I_2$ を有効状態のままで支線ネットワーク $N$ との通信に用いられないようにするため，ルータ $R_1$，$R_2$ においてインタフェース $I_1$，$I_2$ のサブネットマスクを適宜変更する．このとき，サブネットマスクを変更したインタフェースは支線ネットワーク $N$ に対して経路情報を広報するためのみに用い，これを利用して障害発生・復旧の検出を行う．

以下では，**図 3** の環境を例にとって本手法の具体的な手順を示す．図 3 では，支線ネットワークのアドレスとして A.B.C.0/24 が用いられているものとする．このとき，インタフェース $I_1$ にアドレス A.B.C.253 を，またインタフェース $I_2$ にアドレス A.B.C.254 を割り当てる．また，アドレス A.B.C.252 は使用禁止とする．なお，ルータの機能によってはこの割当てに必ずしも従わなくてもよい場合があるが，これについては後述する．

初期状態では，ルータ $R_1$ が支線ネットワーク $N$ との通信にリンク $L_1$ を用いないようにしなければならない．そこで，ルータ $R_1$ ではインタフェース $I_1$ のサブネットマスクを/30 に設定する．この設定では，インタフェース $I_1$ 経由で通信できるのは A.B.C.252〜A.B.C.255 の範囲に限られ，このうち A.B.C.252 は使用禁止であり，また A.B.C.255 は支線ネットワーク $N$ の同報アドレスであるため，支線ネットワーク $N$ 内にある一般のホストとの通信にはインタフェース $I_1$ が用いられることはない．また，この状態でルータ $R_1$ は自身が持つ経路情報を低優先度で支線ネットワーク $N$ に広報する．逆に，ルータ $R_2$ から広報される経路情報はルータ $R_1$ では低優先度のものとして扱う．なお，サブネットマスクの変更による影響を避けるため，支線ネットワーク $N$ での経路情報の広報には RIP1 [1]のような可変長サブネットマスク（VLSM: Variable Length Subnet Mask）を考慮しないプロトコルを用いないようにするか，用いたとしてもたとえばルータ $R_1$ ではこれを無視するように設定する必要がある．これを怠ると，ルータ $R_2$ から支線ネットワーク $N$ 経由で広報された経路情報は，ルータ $R_1$ ではすべて/30 のサブネットマスクを持つ別のサブネットに関するものと見なされ基幹ネットワークや他の支線ネットワークに広報される．これにより，これらのサブネットに属するアドレスに宛てたパケットは，まずルータ $R_1$ で受け取られて支線ネットワーク $N$ 経由でルータ $R_2$ に送られ，またルータ $R_2$ ではこれを幹線ネットワーク経由でルータ $R_1$ に送り返すため，ルータ $R_1$，$R_2$ 間で循環してしまう結果を招くことになる．

障害の検出では，ルータ $R_2$ に障害が発生した場合（障害 1），基幹ネットワーク（たとえばルータ $R_0$）に障害が発生した場合（障害 2），およびリンク $L_2$ に障害が発生した場合（障害 3）のそれぞれの場合についてこれを検出できる必要がある．このうち，障害 1 については前節と同様にルータ $R_1$ における A.B.C.0/24 の経路情報の有無で検出可能である．障害 2 については，RIP のように A.B.C.0/24 の経路情報を支線ネットワーク $N$ 自身に広報しないプロトコルを用いる場合にはルータ $R_1$ における A.B.C.0/24 の経路情報の有無で検出可能であり，そうでない場合にはルータ $R_1$ における A.B.C.0/24 の経路情報のうち中継先がルータ $R_2$ のアドレス A.B.C.254 であるかどうかで検出可能である．また，障害 3 については，インタフェース $I_1$ で受信するパケットがあるにもかかわらず，インタフェース $I_2$ で受信するパケットがなくなったかどうかで検出可能である．

障害検出時の動作についても障害の発生個所により異なる．障害 1〜3 のいずれの場合についてもインタフェース $I_1$ のサブネットマスクを/24 に変更するが，障害 2，3 ではさらにインタフェース $I_2$ のサブネットマスクを/30 に変更する．このとき，必要であればルータ $R_2$ ではルータ $R_1$ から支線ネットワーク $N$ 経由で広報される経路情報を無視するように設定する．

障害復旧の検出については，たとえば SNMP を用いてルータ $R_2$ に A.B.C.0/24 の中継先ならびにインタフェース $I_2$ の受信パケット数を問い合わせ，これにルータ $R_2$ が正しく応答し，A.B.C.0/24 の中継先が基幹ネットワークのルータ（たとえばルータ $R_0$）であり，インタフェース $I_2$ の受信パケット数が前回の結果より増加していれば障害から復旧したと判断することができる．

以上をまとめると，本手法では次のような手順で動的にルーティングを行うことになる．

(1) 初期状態として，支線ネットワークに接続されるインタフェースのサブネットマスクを，インタフェース $I_1$ については/30に，インタフェース $I_2$ については/24に設定する．また，ルータ $R_1$，$R_2$ から必要な経路情報を適切な重みを付けて各ネットワークに広報するように設定する．

(2) ルーティングプログラムは定期的にルータ $R_1$，$R_2$ に状態を問い合わせ，支線ネットワーク $N$ との通信に障害が発生していないかどうかを調査する．障害を検出した場合には，どのような種類の障害であるかを確認して次に進む．

(3) ルーティングプログラムは，障害を検出するとインタフェース $I_1$ のサブネットマスクを/24に変更して支線ネットワーク $N$ との通信を行えるようにし，またルータ $R_2$ 自身に障害が発生している場合以外はインタフェース $I_2$ のサブネットマスクを/30に変更する．

(4) ルーティングプログラムは，定期的にルータ $R_1$，$R_2$ に状態を問い合わせ，障害が復旧しているかどうかを調査する．障害復旧を検出した場合には，次に進む．

(5) ルーティングプログラムは，インタフェース $I_1$ のサブネットマスクを/30に，インタフェース $I_2$ のサブネットマスクを/24に変更し，(2)に進む．

なお，ルーティングプログラムの動作場所については，想定している障害が発生した場合でもルータ $R_1$，$R_2$ をともに制御できる場所が望ましいが，ルータ $R_1$ からルータ $R_2$ へは基幹ネットワーク経由，支線ネットワーク経由の両方の経路に障害が発生しない限り通信可能であるため，ルータ $R_1$ が制御可能であれば事実上十分であると思われる．また，インタフェース $I_1$，$I_2$ に割り当てるアドレスについては必ずしもA.B.C.253，A.B.C.254に限られるものではなく，たとえばそれぞれにA.B.C.1，A.B.C.2を割り当ててもかまわない．ただし，この場合はA.B.C.0とA.B.C.3が使用禁止となるとともに，インタフェースのサブネットマスクを/30に変更する場合にはあわせて同報アドレスをA.B.C.255に設定する必要があることに注意する．

## 4. ルーティングプログラムの実装と運用

我々は岡山大学の学内ネットワークOUnetを対象として，前章で述べた手法に基づいたルーティングプログラムを実装し，運用を行っている．本章ではこの実装方法と運用結果について述べる．

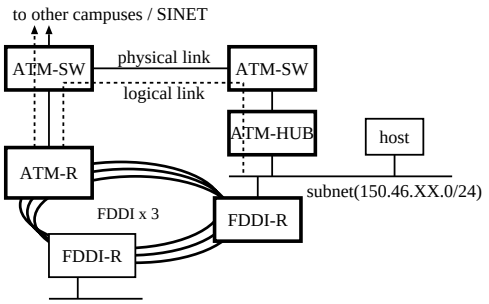


**図4** 津島キャンパスにおけるOUnetの構成
Fig. 4 Network structure of OUnet in Tsushima Campus.

まず，OUnetの構成を示す．岡山大学には9学部を擁する津島キャンパスと2学部を擁する鹿田キャンパスの2つの主要なキャンパスがあり，どちらのキャンパスにおいてもFDDI，ATMの2種類の基幹ネットワークと，これらに接続されている支線ネットワークから構成されている．このうちFDDIネットワークは研究系，図書系，事務系の3系統のループが敷設されており，多くの建物にはルータが設置され，支線ネットワークとして10Base5が接続されている．一方，ATMネットワークについては主要な建物にのみATM交換機（NEC ATOMIS-7ならびにATOMIS-5）とATMハブ（NEC ES10e C5000）が設置されており，導入当初はマルチメディア端末など一部の計算機が接続されていただけであったが，平成11年3月にFDDIの支線ネットワークの大半が接続された．2種類の基幹ネットワークの相互接続は各キャンパスに1台設置されているATMルータ（NEC IP45/650 SSP）が担当している．このルータはさらに上記の支線ネットワークをLANE（LAN Emulation）方式で接続しているほか，キャンパス間接続や対外ネットワークとの接続も担当している．津島キャンパスにおけるOUnetの構成を**図4**に示す．

この図のような構成では，多くの支線ネットワークが論理的には直接ATMルータに接続されているため，従来の動的ルーティングではATMルータを経由して支線ネットワークへ向かう通信がATMネットワークに集中することになる．そこで前章で述べた手法によりFDDIネットワークを優先するようなルーティングプログラムを実装した．支線ネットワークにおけるルーティングプロコトルには支線ネットワークで用いられている機器の関係からRIP1を用いた．なお，FDDIルータはインタフェースの設定変更に再起動を必要とする，あるいは可変長サブネットマスクをサポートしていないなどの理由により，実装したルーティングプ

ログラムではリンクの故障は考慮していない．

ルーティングプログラムはシェルスクリプトで記述されており，60本の支線ネットワークについて順に障害が発生していないかどうか調査するようになっている．障害発生・復旧の検出はSNMPを用いてMIB-II[8]に規定されるいくつかの状態を問い合わせることにより行った．すなわち，各FDDIルータの状態をSNMPを用いて問い合わせ，問合せに対して応答しない状態あるいは以下の条件を1つでも満たしていない状態が3回連続すれば障害が発生していると判断した．また，障害発生中に問合せに対して応答を返し，かつ応答が以下の条件をすべて満たす状態が1度でもあれば，その時点で障害から復旧したと判断した．

(1) 支線ネットワークのインタフェースに対応するifOperStatusがup(1)である．
(2) 支線ネットワークのipRouteTypeがdirect(3)である．
(3) 支線ネットワークのipRouteNextHopがFDDIルータ自身を指している．
(4) デフォルトネットワークのipRouteNextHopがFDDIを経由するものになっている．

障害発生・復旧を検出すると，ルーティングプログラムはexpect[9]を用いてATMルータの当該支線ネットワークに対応するLANEインタフェースを有効状態あるいは無効状態に設定するようにした．これはATMルータではLANEインタフェースの制御をSNMPを用いて行うことができなかったためである．また，ルーティングプログラムには障害発生・復旧の検出時に管理者に電子メールで通知する機能も組み込んだ．

ルーティングプログラムの設定では，各ルータの属する基幹ネットワーク，各ルータに接続されている支線ネットワーク，各支線ネットワークに対応するLANEインタフェースなど，対象となるネットワークの構造をネットワーク管理者が把握しておく必要がある．しかし，これは本プログラムとは無関係にネットワーク管理者が当然把握しておくべき内容であり，管理の負担とはならないと考えられる．また，岡山大学のネットワーク環境では各支線ネットワークに対するFDDIルータのインタフェースアドレスやATMルータのLANEインタフェースの名前およびアドレスを一定の規則に従って割り当てているため，1つの支線ネットワークの制御に必要な情報はサブネットアドレス，対応するFDDIルータ名，FDDIルータが属する幹線ネットワークの3つ組だけであり，新しい支線ネットワークの追加も容易である．

次に，ルーティングプログラムの運用結果について述べる．平成11年6月にルーティングプログラムを導入してから平成13年4月までの間に約40件のFDDIルータ障害が発生した．このうちの多くは休日や夜間に発生しており，ルーティングプログラムが基幹ネットワークの可用性の向上に大きく貢献しているといえる．基幹ネットワークの切替えに要する時間は，障害発生時で約3分，障害復旧時で約1分であるが，これはルーティングプログラムがすべての支線ネットワークの状態調査に約1分を要するためであり，たとえば複数の計算機上でルーティングプログラムを動作させて複数の支線ネットワークを並行して調査するようにすれば短縮を図ることが可能であると思われる．なお，岡山大学のネットワーク環境では1つのATMルータに多くの支線ネットワークが集中的に接続されているため，支線ネットワーク数が増加すると，たとえばATMルータのFDDIインタフェースに障害が発生した場合にすべての支線ネットワークをATMでの接続に切り替えるためにかなりの時間を要するなど，スケーラビリティの面で若干の問題がある．しかし，これはネットワークの構成上の問題であり，ルーティングプログラム自身は各支線ネットワークに関する経路制御を独立して行えるため分散配置して動作させることが可能で，本方式は原理的にはさらに大規模なネットワークにも適用可能である．

リンクの障害を考慮したルーティングプログラムについては，上記の理由により実際の運用は行っていないが，FDDIルータの設定を変更せず，ATMルータのサブネットマスクの変更のみを行う方法については動作試験を行っている．その結果，FDDIルータと支線ネットワークとを接続するリンクに障害が発生すると，ATMルータを経由しない通信は障害個所を迂回できないが，学外との通信などATMルータを経由する通信は利用する基幹ネットワークがFDDIネットワークからATMネットワークに切り替わり障害個所を迂回することが確認された．また，障害から復旧すると，すべての通信がFDDIルータ経由で行われることも確認された．なお，その際，今回使用したATMルータでは標準でproxy arp機能[10]が有効になるように設定されているが，支線ネットワークが接続されているLANEインタフェースに関してはこれを無効にする必要があった．これはこの機能を無効にしないとFDDIルータから支線ネットワークに接続されているホストへのMACアドレス問合せに対してATMルータが応答を返すためである．

## 5. ま と め

本稿では支線ネットワークを複数の基幹ネットワークに接続した冗長構成ネットワークにおいて，インタフェースの有効・無効状態やサブネットマスクなど，従来の動的ルーティング手法では制御の対象とならなかったインタフェースの設定を外部プログラムを用いて変更する動的ルーティング手法を提案した．これにより，通常時には優先すべき通信経路を選択しながら，障害時には直接接続されたインタフェースを用いて障害箇所を迂回し，耐故障性を高めることが可能となった．また，外部プログラムを実装して岡山大学の学内ネットワーク上で運用することによりその有効性を確認した．

今後の課題としては，リンクの障害を考慮したルーティングプログラムを実際のネットワーク上で運用し，その有効性を検証することがあげられる．

## 参 考 文 献


1) Hedrick, C.: Routing Information Protocol, RFC1058, IETF (1988).
2) Malkin, G.: RIP Version 2, RFC2453, IETF (1998).
3) Moy, J.: OSPF Version 2, RFC2328, IETF (1990).
4) Li, T., Cole, B., Morton, P. and Li, D.: Cisco Hot Standby Router Protocol (HSRP), RFC2281, IETF (1998).
5) Knight, S., Weaver, D., Whipple, D., Hinden, R., Mitzel, D., Hunt, P., Higginson, P., Shand, M. and Lindem, A.: Virtual Router Redundancy Protocol, RFC2338, IETF (1998).
6) IEEE: Media Access Control (MAC) Bridges, *ISO/IEC 15802-3:1993 ANSI/IEEE Std 802.1D* (1993).
7) Case, J., Fedor, M., Schoffstall, M. and Davin, J.: A Simple Network Management Protocol (SNMP), RFC1157, IETF (1990).
8) McCloghrie, K. and Rose, M.: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, RFC1213, IETF (1991).
9) Libes, Don: *Exploring Expect*, O'Reilly & Associates, Inc. (1994).
10) Braden, R. and Postel, J.: Requirements for Internet Gateways, RFC1009, IETF (1987).
11) 山井成良，大隅淑弘，宮下卓也，岡本卓爾：岡山大学における基幹ネットワークの構成と運用，情報処理学会分散システム/インターネット運用技術研究会研究報告，2000-DSM-19-6, pp.31–36 (2000).


(平成 13 年 5 月 8 日受付)
(平成 13 年 10 月 16 日採録)

**山井 成良**（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師を経て，現在岡山大学総合情報処理センター助教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

**宮下 卓也**

平成 3 年岡山大学工学部電気電子工学科卒業．平成 5 年同大学大学院工学研究科（電気電子工学専攻）修了．平成 8 年同大学院自然科学研究科（知能開発科学専攻）修了．平成 9 年東京農工大学ベンチャービジネスラボラトリー博士研究員．平成 10 年岡山大学総合情報処理センター助手．主にディジタル機器からの放射電磁雑音の計算機シミュレーションの研究に従事．情報処理教育，マルチメディア，高速ネットワーク等に興味を持つ．博士（工学）．IEEE，電子情報通信学会，エレクトロニクス実装学会各会員．