

防災アプリケーション基本提案書（第3版）  
【別冊2】

APPLIC-0003\_2-2008

# 防災ネットワーク整備ガイドライン

財団法人全国地域情報化推進協会  
アプリケーション委員会

2008年3月

## 【目次】

<b>1. はじめに</b> .....	<b>3</b>
1.1 防災ネットワークの要件.....	3
<b>2. ネットワーク物理設計（物理的冗長化設計）</b> .....	<b>5</b>
2.1 ネットワークの多ルート化.....	5
(1) スター型構成.....	5
(2) リング型構成.....	5
(3) メッシュ型構成.....	6
2.2 バックアップ回線.....	7
(1) 地上系無線.....	8
(2) 衛星通信ネットワーク.....	9
<b>3. ネットワーク論理設計（論理的冗長化設計）</b> .....	<b>10</b>
3.1 冗長化技術の適用イメージ.....	10
3.2 冗長化技術.....	11
(1) レイヤ2の冗長化技術.....	11
(2) レイヤ3の冗長化技術.....	14
3.3 IPV6の防災ネットワークへの活用.....	15
<b>4. ネットワーク機器</b> .....	<b>17</b>
4.1 ネットワーク機器の冗長化.....	17
(1) ネットワーク機器内部の冗長化.....	17
(2) ネットワーク機器の冗長化.....	17
4.2 ネットワーク機器選定のポイント.....	18
(1) ネットワーク機器の性能・信頼性の確認.....	18
(2) 対応プロトコル・ルータ機能の確認.....	18
(3) 接続インターフェースの確認.....	18
<b>5. 輻輳、パーストラフィック対策</b> .....	<b>19</b>
5.1 優先制御.....	19
(1) QoS.....	19
(2) 優先制御の仕組み.....	20
(3) 帯域制御装置.....	21
5.2 マルチキャスト通信.....	21
<b>6. セキュリティ対策</b> .....	<b>23</b>
6.1 ネットワーク論理分割.....	23
6.2 セキュリティ対策.....	23
6.3 リモート接続.....	23
<b>7. ファシリティ関連</b> .....	<b>25</b>

7.1	ファシリティの信頼性向上策.....	25
(1)	回線敷設時の対策.....	25
(2)	機器の耐災害対策.....	25
(3)	電源対策.....	25
<b>8.</b>	<b>推進体制.....</b>	<b>27</b>
8.1	推進体制に関する留意点.....	27
<b>9.</b>	<b>付録.....</b>	<b>28</b>
9.1	防災ネットワーク 耐災害性チェックリスト.....	28

## 1. はじめに

---

本ガイドラインにおける防災ネットワークとは、団体内において防災業務に関連する情報を流通させるための IP ベースのネットワーク基盤と定義する。防災ネットワークを利用することにより、防災データの共有を実現することが可能になる。団体間のデータ連携の標準化や防災アプリケーションの標準化の動向を勘案して、防災ネットワークの基本要件や整備方法について検討を進めると、「地域公共ネットワークに係る標準仕様」の記載内容と同様に、標準化されたオープンな技術の採用および市販されている一般的な機器調達の実施がポイントになる。

### 1.1 防災ネットワークの要件

災害発生時には次のような情報のやり取りが必要となり、被災後の脆弱と考えられる環境においても、これらの流通が確保される防災ネットワークを構築することが求められる。

- ・被災住民の情報連絡、情報収集
- ・団体内における関連部門担当者間の情報連絡(状況把握、対策検討、対策実施)
- ・一般市民、マスメディア等への情報提供

防災ネットワークに求められる要件は以下の通り。

- ・被災時に確実に動作し、利用できること
- ・被災者への情報提供、団体の防災担当者間の連絡、被災状況等の発信が支障なく実施できること
- ・被災時のネットワーク利用形態に合わせた利用ができること

また災害時のケーブル断線やネットワーク機器の故障発生について考慮しなくてはならない。このような回線断や機器故障を前提とした状況において、ネットワーク整備計画時に想定した通信が実施できる環境を維持することが、防災ネットワークの信頼性向上の観点から求められる。そのためには、一箇所の障害がネットワーク全体に影響することがないようにすること、つまり、ネットワーク上にある単一故障ポイントをなくすための「冗長化」を実施していくことが防災ネットワークに求められる。

これらを勘案して防災ネットワークを他業務のネットワークと比較した場合、通常のネットワーク要件に加え考慮すべきポイントとしては下記の通りで、防災ネットワーク特有の要件と考えられる。

- (1) ネットワークの信頼性向上  
物理面での信頼性向上、論理面での信頼性向上
- (2) ネットワーク機器多重化
- (3) 輻輳、バーストラフィック対策

- (4) 機密情報を保護するためのセキュリティ対策
- (5) ファシリティ関連
- (6) 推進体制

これらのポイントは通常のネットワークにおいても考慮すべき事項であるが、災害発生時に防災情報の共有を行う防災ネットワークにおいては、特別な考慮や対策が必要である。

防災ネットワーク特有の要件と本ガイドラインの構成の対応について以下に示す。

表 1-1 防災ネットワーク特有の要件と本ガイドラインの構成

防災ネットワーク特有の要件	本ガイドラインの構成
(1) ネットワークの信頼性向上 物理面での信頼性向上	2 章 ネットワーク物理設計 (物理的冗長化設計)
(1) ネットワークの信頼性向上 論理面での信頼性向上	3 章 ネットワーク論理設計 (論理的冗長化設計)
(2) ネットワーク機器多重化	4 章 ネットワーク機器
(3) 輻輳、バーストラフィック対策	5 章 輻輳、バーストラフィック対策
(4) 機密情報を保護するための セキュリティ対策	6 章 セキュリティ対策
(5) ファシリティ関連	7 章 ファシリティ関連
(6) 推進体制	8 章 推進体制

なお、本書の使用方法については、2 章から順番に読み進めていくという方法も可能であるが、9 章の「防災ネットワーク 耐災害性チェックシート」を使用して、災害対策が不足している項目について重点的に確認し、その対策を検討するという方法も可能である。

## 2. ネットワーク物理設計(物理的冗長化設計)

防災ネットワークはその特性上、災害時の回線途絶に備え、ネットワークの信頼性向上策が必須となる。本章では、ネットワークの多ルート化およびバックアップ回線を利用した信頼性向上策について紹介する。

### 2.1 ネットワークの多ルート化

ネットワーク回線が途絶した場合、物理的な通信が不可能となりシステム全体の機能が果たせなくなる。物理面でのネットワーク回線の障害性を考えた場合、ネットワーク経路の多重化を実施し、ネットワーク回線の信頼性向上に努めることが望まれる。ここではネットワーク回線の信頼性向上策を紹介する。

#### (1) スター型構成

ネットワークの拡張性や柔軟性に優れている最も一般的な構成である。ネットワークの拡張時の構成変更に関わる作業、コストが小さく、柔軟且つ迅速な対応が可能である。ただし、本方式は障害に対して弱いため、防災ネットワークにおいては、リング型構成やメッシュ型構成を取り入れる等の冗長化構成をとることが必要である。

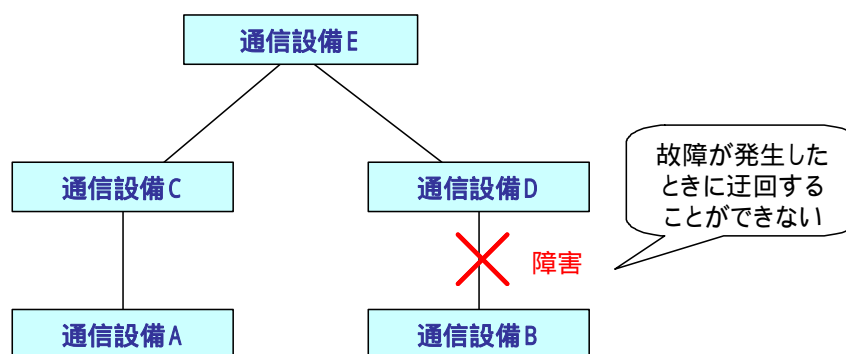


図 2-1 スター型トポロジー

#### (2) リング型構成

ネットワークトポロジーをリング型にすることにより、バス型、スター型のネットワーク構成と比較し冗長性があり災害に強いネットワークを構築することができる。ただし本方式はネットワークの構築に比較的成本がかかるため、大規模ネットワークの基幹回線等で採用される場合が多い。

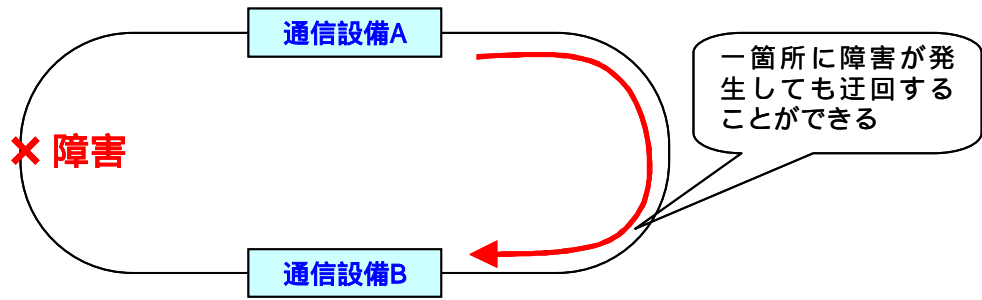


図 2-2 リング型ネットワークポロジ

(3) メッシュ型構成

特定の LAN 内等で安価にネットワークの信頼性を向上させるネットワークポロジとしてメッシュ型の構成を紹介する。ただし本方式は通信機器やホストのネットワーク設定が複雑になりやすいため設定ノウハウが必要である。

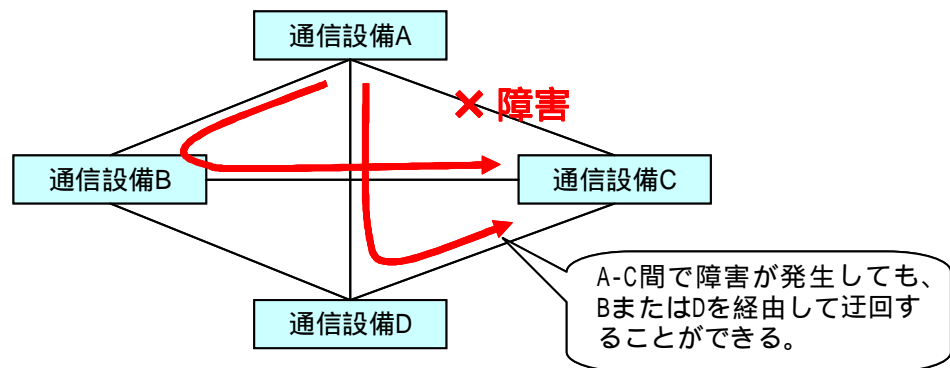


図 2-3 メッシュ型ネットワークポロジ

## 2.2 バックアップ回線

通常利用するメイン回線の他にバックアップ回線として複数の回線を用意しておき、メイン回線断絶時にはバックアップ回線に切り替えて通信を継続する方式が有効である。同一種類の回線をバックアップ回線とする場合もあるが、回線サービス全体が停止するリスクを考えるとバックアップ回線はできるだけ異なる種類の回線を選定するのが望ましい、またバックアップ回線は最低限のネットワーク要件を洗い出し、メイン回線より性能の低い回線を選んでもよい。以下で紹介する「無線ネットワーク」は有線回線のバックアップ通信経路として適している。

防災分野におけるネットワークというと、防災行政無線を中心とする音声系の無線が多く導入されている。防災行政無線においては近年デジタル化が推進されており非常に注目度が高い。防災行政無線がデジタル化されるとデータ転送が可能となるが、現在の仕様では32～64kbpsの少ない帯域しか確保することができない。迅速な音声通信を目的とする防災行政無線(デジタル)を、防災ネットワークのバックアップ回線とすることは、データ転送が帯域を占有し、円滑な音声通信を妨げる可能性があることから望ましくない。本項目では防災行政無線は本来用途の音声通信に特化して利用することを前提として検討対象外とし、大容量のIP通信のバックアップ回線として利用可能な無線ネットワークの技術を中心に紹介する。

無線ネットワークは広帯域伝送の有線ネットワークと比較して伝送容量が少ないが、通信ケーブルを敷設する必要がないため、災害に強いネットワークである。そのため、有線ネットワークのバックアップ回線として無線ネットワークを併用することは、災害時の接続を保証する必要がある防災ネットワークの信頼性を確保する方法として有効な手段である。

有線ネットワークのバックアップ回線として無線ネットワークを用いる場合は、バックアップする無線区間、必要伝送容量(速度)などについて検討し、最適な無線方式を選定する必要がある。

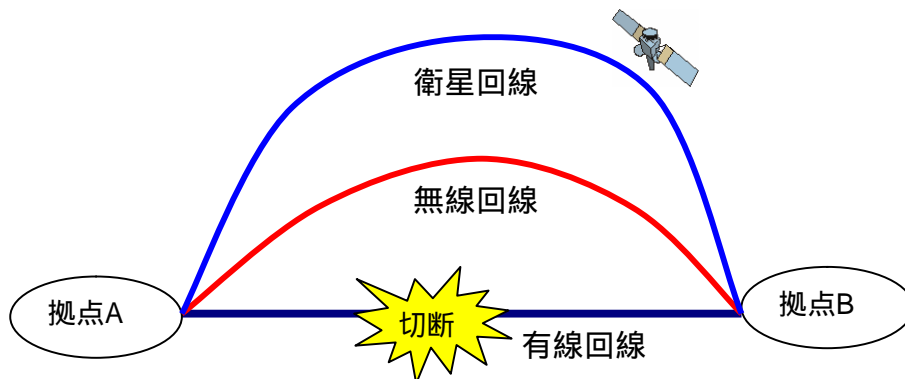


図 2-4 無線回線によるバックアップイメージ

無線ネットワークは大きく地上系無線と衛星系無線に分けることができる。それぞれの方式の特徴とバックアップ回線としての活用が想定される代表的な方式を紹介する。

(1) 地上系無線

地上系無線システムを利用する場合、無線通信方式のそれぞれの特徴を考慮する必要がある。無線通信には次の2通りの方法が考えられる。

表 2-1 地上系無線

方式	概要
固定無線アクセス FWA ( Fixed Wireless Access) 通信	<p>公共業務用無線(18GHz 帯)を使って、地域自治体ネットワークの山間地域や離島への回線作成に利用されているが、有線ネットワークのバックアップ回線として利用も可能である。</p> <p>特徴としては、最大伝送容量が 156Mbps、数キロから 10km 程度での高速無線アクセス回線が作成できる。</p>
無線 LAN	<p>現在広く普及している無線 LAN を使っての有線ネットワークのバックアップ回線を作成する方法がある。</p> <p>特徴としては、設備が簡易で安価であり、小型なために構築が容易である。可搬性が良く、無線局免許が必要なく利用できる。通信のセキュリティについては IEEE802.11i などのセキュリティ対策が必要である。</p> <p>また、無線 LAN の使用する無線帯域も IEEE802.11 b/g の 2.4GHz 帯や IEEE802.11a の 5GHz 帯(2.4GHz 帯よりもノイズの影響が少ない帯域)の製品があり、高利得アンテナを用いた屋外長距離利用の製品も商品化されている。</p> <p>その他、無線 LAN の通信エリアを面的に広げる方法としてメッシュ型の無線 LAN やアドホックネットワークなどにより災害地の通信を確保する事が可能である。</p>

## (2) 衛星通信ネットワーク

衛星通信ネットワークを利用する場合、それぞれの方式の特徴を考慮する必要がある。衛星通信ネットワークには次の2通りの方法が考えられる。

表 2-2 衛星通信ネットワーク

方式	概要
地域衛星通信ネットワーク	<p>各自治体では(財)自治体衛星通信機構の地域衛星通信ネットワークを導入しており、デジタル化(IP化)を進めている状況である。</p> <p>第二世代システム配備後は各自治体内の各関係機関(導入局)間を庁内 LAN に接続して IP 通信による有線ネットワークのバックアップ回線としても活用可能である。また、地域衛星通信第二世代システムには可搬型の送信設備もあり、この設備を利用して臨時に災害地～庁内 LAN との回線作成により災害現地本部との防災情報通信を行える。</p> <p>特徴としては、第二世代システムが配備済み自治体では通常時の利用の他、有線ネットワークのバックアップ回線としてすぐにも利用できる。</p> <p>各自治体は、ほぼ全国的に地域衛星通信ネットワークは導入されており(約4700局)世界最大級のネットワークを作っているが、IP 通信化した第二世代化の全国的な配備には時間が掛かりそうである。</p>
民間衛星通信会社の衛星サービス利用	<p>民間衛星通信会社の VSAT 装置を使って衛星回線を利用しインターネット回線(VPN 利用)に接続して通信回線を作成することができる。</p> <p>特徴は、VSAT 装置は小型で可搬性に優れている、また、操作性が良く、無線技術者でなくても簡単 2Mbps 程度の回線が作成できる。ただし、事前に回線契約(費用)が必要である。</p>

### 3. ネットワーク論理設計(論理的冗長化設計)

防災ネットワークの論理設計を実施する際は、各団体間を柔軟に接続できる拡張性、各種アプリケーションの動作を保証する汎用性、標準規格としての経済性の観点から、採用技術について検討する必要がある。これらを勘案して検討した結果、OSI 参照モデルのレイヤ 2 にあたるローカルエリアネットワーク(LAN)においてはイーサネット(Ethernet)、レイヤ 3 においてはインターネットプロトコル(IP)の採用が推奨される。本章では、Ethernet 及び IP 技術を用いてネットワークの論理的冗長化設計を行う際に考慮すべきポイントについて紹介する。

#### 3.1 冗長化技術の適用イメージ

Ethernet 及び IP には冗長化のための様々な技術が存在する。これらの技術を組み合わせることで信頼性の高い防災ネットワークを構築することが可能となる。

団体の拠点内ネットワーク、拠点間ネットワーク(WAN)、インターネット接続という 3 つの領域における冗長化技術の適用イメージを図 3-1 に示す。レイヤ 2(Ethernet)およびレイヤ 3(IP)に分類して、冗長化のために使用するプロトコルを記載した。

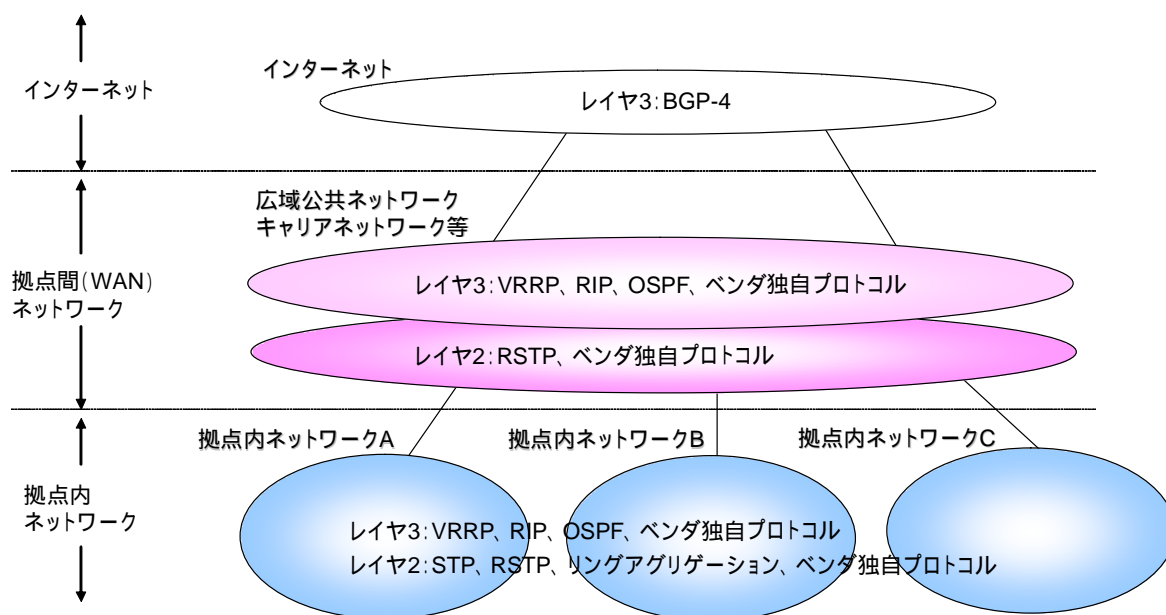


図 3-1 冗長化技術の適用イメージ

表 3-1 冗長化に使用されるプロトコル

	レイヤ 2	レイヤ 3
インターネット	-	BGP-4
拠点間ネットワーク (WAN)	RSTP ベンダ独自プロトコル	VRRP RIP OSPF ベンダ独自プロトコル
拠点内ネットワーク	STP RSTP リングアグリゲーション ベンダ独自プロトコル	VRRP RIP OSPF ベンダ独自プロトコル

### 3.2 冗長化技術

冗長化技術として、レイヤ 2 及びレイヤ 3 において使用されるプロトコルについて解説する。

#### (1) レイヤ 2 の冗長化技術

スパニングツリープロトコル (STP: Spanning Tree Protocol)

図 3-2 に示すように Ethernet の基本的トポロジはある機器を中心にして放射状に機器を接続したスター型トポロジである。冗長化するためには、スイッチ A と C をつなぎループ構成にする必要がある。しかし、Ethernet はループ構成にすると仕様上ブロードキャストパケットがネットワーク内を永久に巡回するブロードキャストストーム状態となり、ネットワークをダウンさせてしまう。したがって、Ethernet においてループ構成は許容されない。

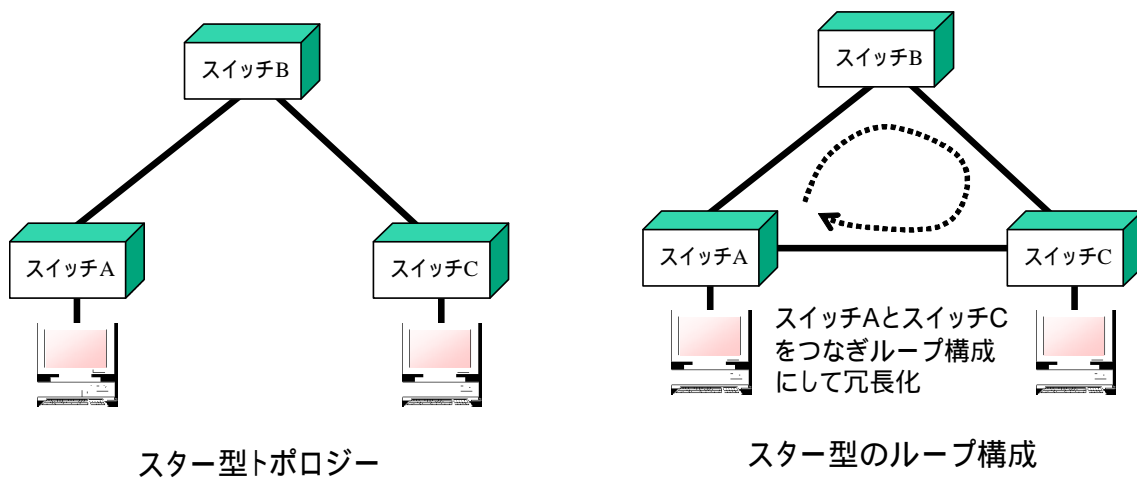


図 3-2 スター型のループ構成

ループを回避しネットワークを冗長化するためにはスパニングツリープロトコル(STP)と呼ばれる経路の冗長化プロトコルを用いる。STP による経路冗長化の仕組みは次のとおりである。(図 3-3 参照)

- 1) スイッチ同士が情報を交換し、スイッチ C のスイッチ A 側ポートをブロックすることにより、経路をスイッチ A B C の 1 つに絞り込む。
- 2) スイッチ A ~ B 間で故障が発生した場合には自動的にスイッチ C のスイッチ A 側ポートが開放され、スイッチ A C の経路により通信を継続する。

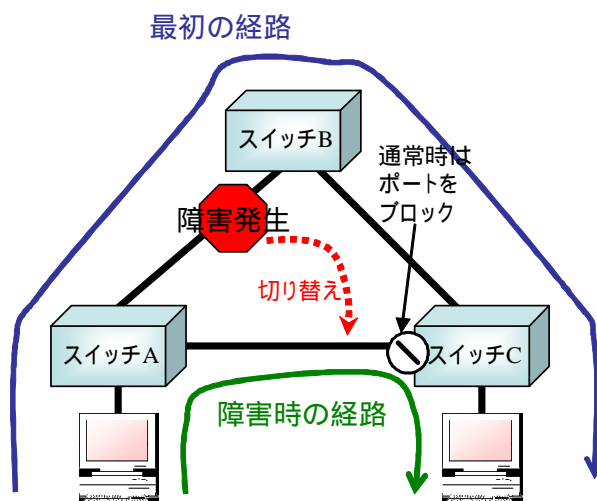


図 3-3 STP の仕組み

STP はスイッチの黎明期から使用されている技術であるが、障害発生からトポロジー変更および切替えまでの収束処理に時間がかかるという弱点がある。収束を高速化した RSTP (Rapid STP) が標準化されており、防災ネットワークの要求条件により RSTP に準拠したスイッチを使用しネットワークに実装する方法を検討する必要がある。

### リンクアグリゲーション

リンクアグリゲーションは図 3-4 に示すように複数本の物理回線を束ねて論理的にひとつのリンクとして扱う技術である。物理回線を複数本束ねることにより広帯域化を図ることができる。また、複数本のリンクの 1 回線に障害が発生しても、残りのリンクで通信を継続することができる。

IEEE802.3ad で標準化されており、制御プロトコル(LACP: Link Aggregation Control Protocol) が規定されている。

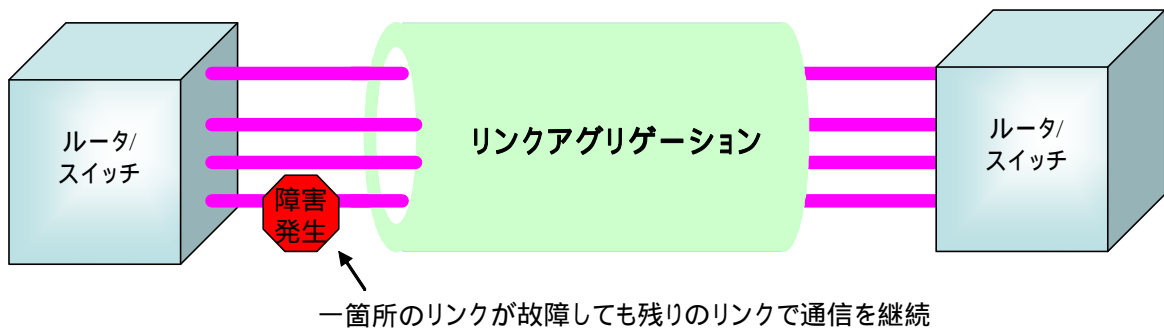


図 3-4 リンクアグリゲーション

### ベンダ独自プロトコル(デュアルホーム構成)

デュアルホーム構成は図 3-5 に示すように、スイッチにおいてマスタ、スレーブという主従関係を作る。正常時はマスタ側のスイッチを使用して通信を行う。障害時には自動的にスレーブ側に切り替わり通信を継続する。正常時にはスレーブ側ポートはブロックされるために経路がループすることはない仕組みとなっている。デュアルホーム構成は図 3-5 のようなメッシュ型のトポロジーのネットワークに適用される。

なお、デュアルホーム構成を実現するプロトコルはベンダ独自であるため、異なるベンダ間の相互接続性はない。

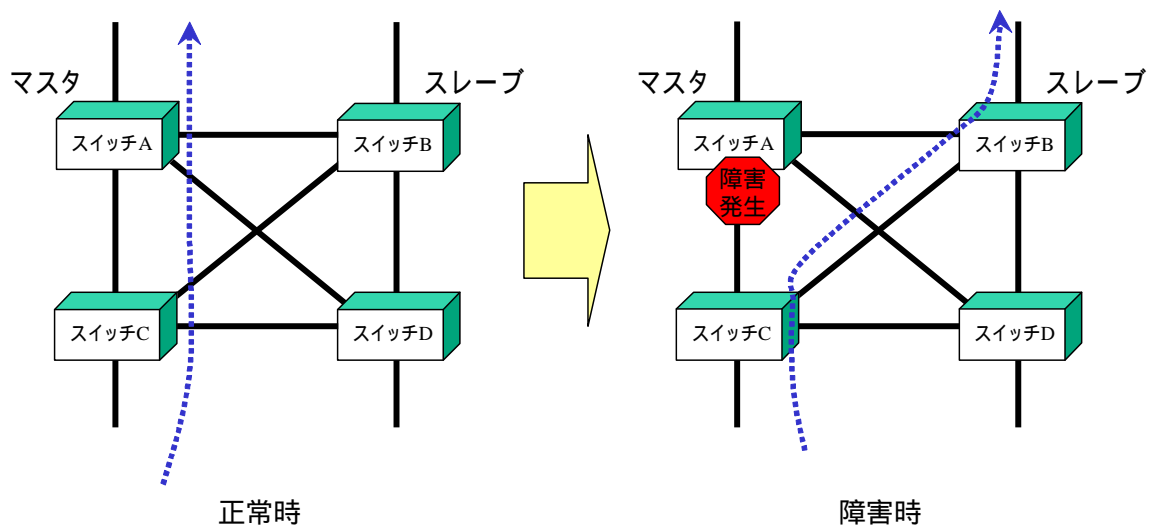


図 3-5 デュアルホーム構成

## (2) レイヤ 3 の冗長化技術

機器冗長化のためのプロトコル(VRRP: Virtual Router Redundancy Protocol)

ルータやレイヤ3スイッチ等の機器冗長化のために使用される方式がVRRPプロトコルである。

VRRPには仮想のIPアドレスとMACアドレスを持つ仮想ルータが存在する。図3-6に示すとおり、VRRPが動作しているルータ(ルータB及びルータC)のうち、マスタとなっているルータBが仮想IPアドレスとMACアドレスを使用して動作する。ルータCはバックアップとして動作し、マスタ(ルータB)が故障した場合には速やかに仮想IPアドレス及びMACアドレスをバックアップであるルータCが引き継いで、仮想ルータが存在し続けているかのように動作する。各PCにおいてデフォルトGWとして仮想ルータを設定することにより、各PCはマスタ(ルータB)が故障等によりダウンしてもバックアップ(ルータC)を経由して通信を継続することができる。

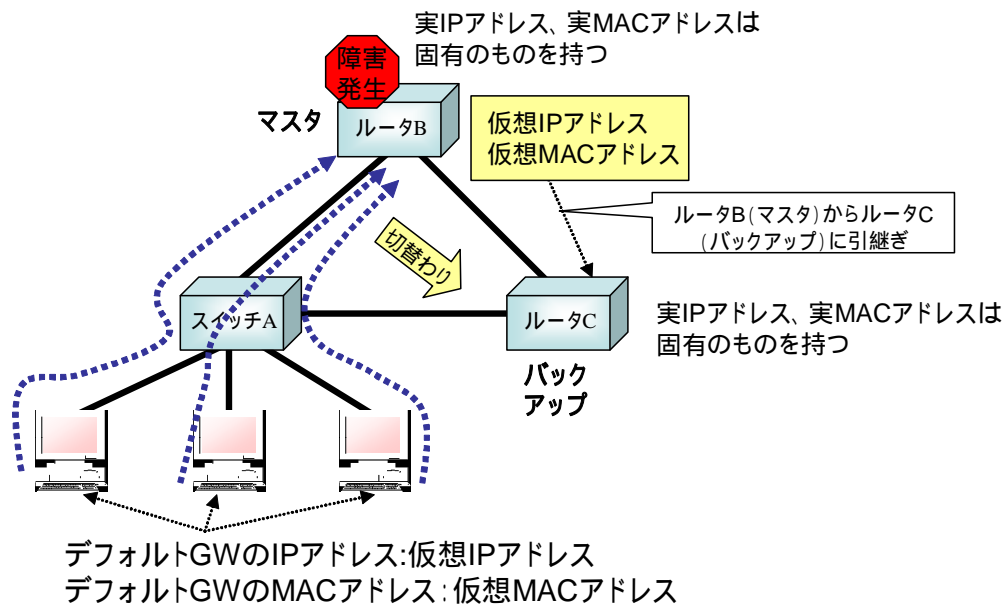


図 3-6 VRRP の仕組み

## 経路冗長化のためのプロトコル

ダイナミックルーティングを用いることによりレイヤ3ネットワークを冗長化することができる。ダイナミックルーティングはルーティングプロトコルを用いてルータやレイヤ3スイッチが動的に経路情報を学習し、最適な経路を選択するものである。ルータやスイッチは一定時間間隔毎に情報を交換することにより、回線断や構成変更によるネットワークの状態変化を常に把握する。そのため、経路のどこかで障害が発生した場合も、最適な迂回経路を自動で選択することができる。

ダイナミックルーティングを実現するためのプロトコルは大きくIGP(Interior Gateway Protocol)とEGP(Exterior Gateway Protocol)の2つに分類される。IGPは団体内におけるLAN等、管理組織内のルータ及びレイヤ3スイッチの経路制御に利用されるプロトコルであり、RIP、OSPFなどが

代表的である。EGP は団体等、管理組織間の経路制御に使用されるプロトコルであり、一般的にはサービスプロバイダ間で使用される。主に使用されるプロトコルは BGP-4 である。ダイナミックルーティングの分類を表 3-2 に示す。

表 3-2 ダイナミックルーティングの分類

代表的プロトコル	管理組織内		管理組織間
	IGP		EGP
	RIP	OSPF	BGP-4
概要	隣接ホストと動的に経路を交換し、目的ネットワークにたどり着くまでに経由するルータをホップ数という値で数値化し、最短となる経路を決定する方式。距離と方向に基づいて最適なルートを計算するディスタンスベクタ型のプロトコルであり、実装が比較的容易でサポートしている機器が多いことから比較的小規模なネットワークでの利用に適している。	各ルータの持つリンク情報をデータベース化し、最短経路を計算するリンクステート型のプロトコルである。RIP に比べネットワーク変更時の収束時間が短いことや、情報のやり取りに必要な帯域幅が小さいことなど数多くの利点を持つ。一方、ルータの処理負荷が高く、実装が複雑なことから、一般的に中～大規模ネットワークにおいて利用されるプロトコルである。	異なる管理ポリシーにより運営される自律システム(AS:Autonomous System)間をルーティングするために利用されるプロトコルである。防災ネットワークにおいては、各自治体等にまたがる複数の OSPF ネットワークの接続等に利用できるほか、BGP-4 を利用してネットワークの冗長性向上や負荷分散を実現できる。

### 3.3 IPv6 の防災ネットワークへの活用

現在一般的に利用されている IPv4 に代わるものとして開発された次世代のインターネットプロトコルである IPv6 は防災ネットワークを実現する上で以下のとおり数多くの利点をもつ。

- ・災害時にアドホックネットワークを利用したネットワーク再構築が容易  
被災によるネットワーク切断箇所にいち早く無線アクセスポイントを多数設置し、プラグアンドプレイや Mobile IPv6 により、緊急用ネットワークを早急に再構築することが出来る。
- ・災害時の現場把握が容易  
グローバルアドレスを持った多数のフィールド監視カメラを利用することにより、災害対策本部等から被災地のカメラ映像を直接呼び出すことが可能である。
- ・広域災害に対応したネットワーク構築が容易  
IPv6 では事実上無限ともいえる多数の IP アドレスが利用できるため、地域ネットワークがそれぞれ異なるグローバルアドレスを利用することができ、複数の地域ネットワークを統合接続しても、アドレスの重複等の不整合が発生しない。

・同じ物理ネットワーク上で複数のアプリケーションがセキュアに並立

IPv6 では、マルチホーム技術、マルチプレフィックス技術や m2m-x 等のアクセス制御技術により、1 つの IPv6 基盤ネットワーク上に目的ベースの様々なオーバーレイネットワークを共存させることが可能である。したがって、災害時に必要な人だけが必要な機器にアクセスするというグルーピングされた複数の仮想閉域ネットワークを同時稼動することが可能である。

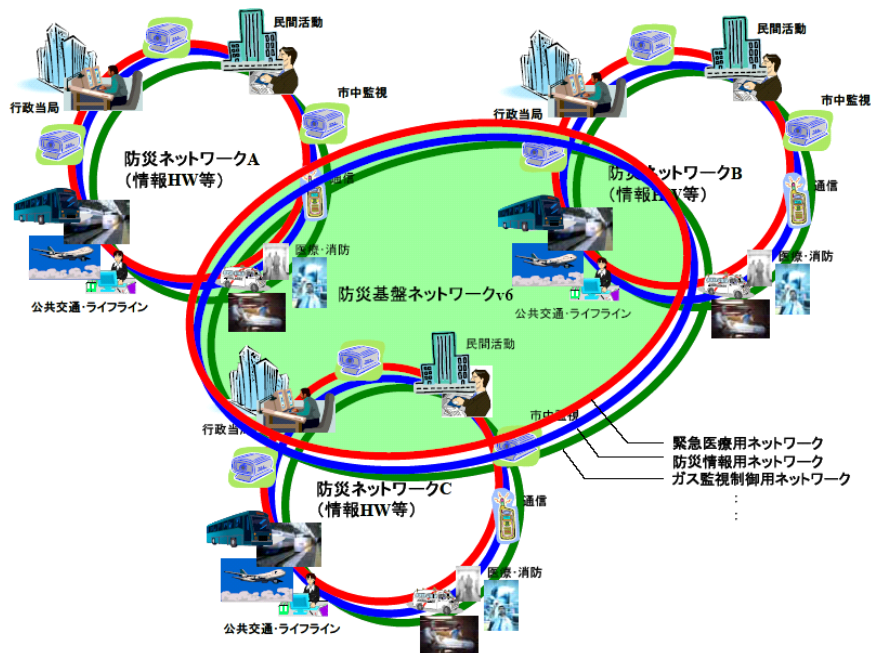


図 3-7 防災用セキュアオーバーレイネットワークのイメージ

また、IPv4は数年のうちにIPアドレスが枯渇することが想定されており、約 $3.4 \times 10^{38}$ 個というほぼ無限ともいえるIPアドレスを持つIPv6への近い将来の移行は不可避でもある。さらに、重点計画 2006(平成18年7月26日 IT戦略本部)において、「各府省は、原則として2008年度までに、各情報システムの新たな開発(導入)又は更改に合わせて、情報通信機器及びソフトウェアのIPv6対応を図る」とされていることから、国のネットワークへの接続の可能性を考慮する面からも、現時点でのIPv6利用の有無を問わず、防災ネットワークの設計に際してはIPv6に対応した機器を選定すべきである。

ネットワークに関しても、IPv6端末とIPv4端末間の通信はできないため、両機器が併用される移行期間については、デュアルスタックの設定によりIPv4とIPv6の両ネットワークを運用する必要がある。ただし物理的にネットワークを二重構築することはコスト面、運用面から最適とはいえないため、1つのアクセス回線でIPv6/IPv4両方の論理ネットワークを構築する方法が推奨される。このためIPv6/IPv4デュアルスタックに対応したネットワークサービスを予め選定しておくことが重要となる。

## 4. ネットワーク機器

---

防災ネットワークを構成するネットワーク機器は、その特性を踏まえた機器選定が必要となる。本章では、防災ネットワーク機器冗長化に使用する技術およびネットワークの機器選定のポイントについて紹介する。

### 4.1 ネットワーク機器の冗長化

ネットワーク機器の冗長化には大きく分けて 2 つの方法がある。1 つはネットワーク機器内部の二重化である。もう 1 つはネットワーク機器の二重配備を行い、現用ネットワーク機器が故障した場合につなぎ換える方法である。

#### (1) ネットワーク機器内部の冗長化

防災ネットワークの信頼性向上のためには、ネットワーク機器内部の主要部品の二重化が必要となる。特にバックボーンルータやスイッチにおいてはインタフェースパッケージ及び故障頻度の高い電源と冷却ファンの二重化は必須となる。また、故障時に待機している部品に自動的に切り替る、電源 ON の状態で部品を交換できる等の機能を実装しているネットワーク機器を採用することにより信頼性をさらに高めることができる。

#### (2) ネットワーク機器の冗長化

ネットワーク機器は災害時の衝撃等により停止してしまう可能性がある。ネットワーク機器が停止した際の通信維持に関する対策としては、ネットワーク機器の二重化が有効である。本項目では機器を冗長化し、障害発生時に動的切替えを行う際の技術を紹介する。

##### スパニングツリープロトコル(STP)

障害に備え 2 系統のスイッチ及び経路を用意した構成において、本技術を利用することにより、通常時にループ構成とならないように、冗長経路をブロックすることが可能となる。また障害時に通常の経路が利用不可となった場合に、自動的に冗長化された経路に切替え通信を継続することが可能となる。STP の技術内容については、「3.2 章 (1) レイヤ 2 の冗長化技術 スパニングツリープロトコル(STP)」を参照されたい。

##### VRRP(ルータ冗長化用プロトコル)

VRRP の技術内容については、「3.2 章 (2) レイヤ 3 の冗長化技術 機器冗長化のためのプロトコル(VRRP)」を参照されたい。

ネットワーク機器を二重化し、それらを動的に切り替えるよう動作させるためには、上記2つのプロトコルを適切に設定することが必要となる。ただし機器の運用管理方法が複雑になるため、単一構成と比較すると設定・運用コストが高くなることが多い。予算等に制約がある場合には、同一機能を有するネットワーク機器を予備で用意しておき、障害発生時に手作業で機器を置き換える方策も代替案として効果的である。

## 4.2 ネットワーク機器選定のポイント

防災ネットワークの特性を鑑み、ネットワーク機器選定にあたっては、通常のネットワーク機器選定要件に加え、以下のポイントを考慮する必要がある。

### (1) ネットワーク機器の性能・信頼性の確認

防災ネットワークにおいては、災害時の集中的なアクセスの際にもネットワーク機器がボトルネックとならないよう、装置の処理能力の的確な把握と需要の適切な予測にもとづき、十分な性能を持つ機器を選定すべきである。また、MTBF(平均故障間隔)、MTTR(平均修復間隔)等の数値を元に、必要な信頼性を満たす機器であることを確認し、必要であれば4.1項で説明した機器の冗長化等の対策を実施する必要がある。

### (2) 対応プロトコル・ルータ機能の確認

機器選定の際には、利用が想定されるプロトコルに対応していることを確認した上で調達する必要がある。特に災害による回線途絶時に、迂回回線へ自動切替が可能な各種ルーティングプロトコルへ対応した機器を選定することは重要である。また将来防災業務への活用が期待されるIPv6に対応した機器を選定しておくことも推奨される。

### (3) 接続インターフェースの確認

接続インターフェースの規格にはイーサネット、ATM、I インターフェース等、複数の規格が存在する。このためネットワークと接続する機器を選定する際には、利用するネットワークに応じた接続インターフェースを持つ機器を選定する必要がある。

## 5. 輻輳、バーストラフィック対策

---

防災ネットワークの特徴として、平常時のトラフィックは比較的少ないが、災害時はシステムへのアクセス集中等によりネットワーク負荷が増大することが挙げられる。

災害時のネットワーク負荷増大についての対策としては、十分な許容量・耐久性を持ったネットワークの構築が理想的であるが、費用対効果の関係により困難な場合もある。このような場合は優先制御による通信制御が有効となる。この技術を用いることにより、災害時に団体の防災業務に関するトラフィックを優先することや画像・映像等広帯域を必要とするアプリケーションのトラフィックを制限すること等が可能となる。

本章では、限られたネットワーク資源を有効活用し、災害時のネットワーク負荷集中を解決するために有効な通信制御技術を紹介する。

### 5.1 優先制御

#### (1) QoS

ネットワーク上で特定の通信のための帯域を優先確保し、特定の通信だけに一定の通信速度を保証する際に使用する技術である。具体的には、動画の転送やメール転送、データ交換などの通信トラフィックが混在する中で、特定の通信(例:テキストデータの交換)を優先させるといった制御が可能となる。突発的に大量のトラフィックが発生する中で、重要な通信を確保する必要がある防災ネットワークの特性を鑑みても欠かすことのできない技術である。通信事業者のネットワークサービスを利用する場合、QoS に対応した制御ができることを確認しておく必要がある。

またインターネットなど複数の回線が混在する中で送信先までの帯域を制御し、通信品質を確保する RSVP (Resource reSerVation Protocol) というプロトコルもある。RSVP はホストとルータ、またはルータ同士が QoS 制御に必要な情報を交換するためのプロトコルである。実際にルータ上で QoS を保証するためのアルゴリズム(トラフィック制御、ポリシー制御)は独立して存在しており QoS 保証の仕組みは、個々のルータの実装に依存する。

これら技術を導入するためには QoS や RSVP に対応したネットワーク機器を購入する必要がある。防災ネットワークを整備する際には将来の拡張性を見据え、これらの機能を有するネットワーク・機器を選定しておくことが望ましい。

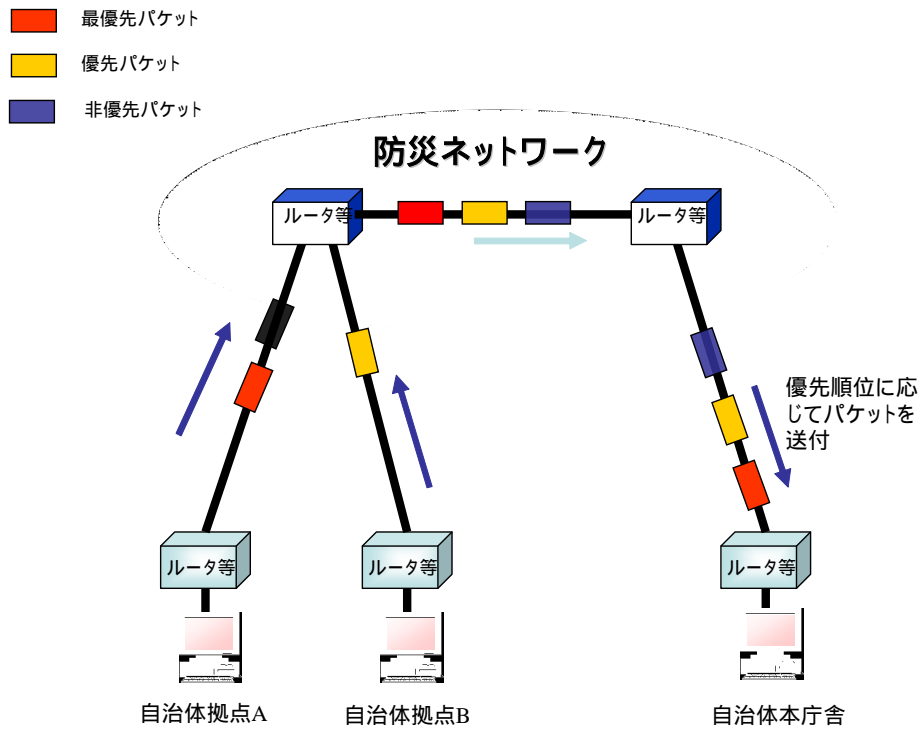


図 5-1 優先制御のイメージ

## (2) 優先制御の仕組み

優先制御を実施する際に、IP パケットのどのフィールドを使用して制御が行われるのかについて以下で説明する。具体的には、ポート番号、および IP アドレス、ToS フィールド、CoS フィールドという 4 つの設定パラメータを使用することにより優先制御を実施している。

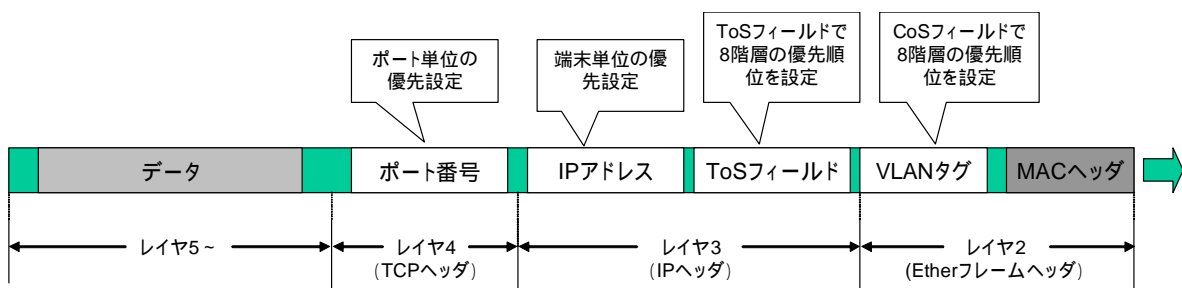


図 5-2 IP パケットにおける優先制御パラメータ

### ポート番号による優先設定

Web 通信を優先したい場合には 80 番ポート (HTTP) を優先設定、メール通信を優先したい場合には 25 番ポートを優先設定する等の TCP ポート番号により優先設定を実施することができる。

### IP アドレスによる優先設定

IP アドレスによる優先設定は機器毎の優先設定に利用される。設定例として、IP アドレス 192.168.50.10 の端末からのパケットを優先する、IP アドレス 192.168.100.20 のサーバへの転送を優先するといった設定が考えられる。

### ToS (Type of Service) による優先設定

IP ヘッダで定義された ToS フィールド(8 ビット)の上位 3 ビットを利用して優先度を設定する。2 の 3 乗 = 8 段階の優先度を設定可能である。レイヤ 3 である IP ヘッダでの設定値であるので、セグメント分割されたネットワークにおいても利用することができる。ToS フィールドは QoS 専用のパラメータであり、利用者の設定によりカスタマイズした優先制御を実現できる。

### CoS (Class of Service) による優先設定

レイヤ 2 の Ethernet フレームで定義された CoS フィールドで優先度を設定する。3 ビットのフィールドであり 2 の 3 乗 = 8 段階での優先度を設定できる。レイヤ 3 でルーティングされる際には失われるフィールドであり、レイヤ 2 通信のセグメント内で利用される。CoS フィールドは ToS フィールド同様 QoS 専用のパラメータであり、利用者の設定によりカスタマイズした優先制御を実現できる。

## (3) 帯域制御装置

QoS では特定のプロトコルレベルまでしか制御出来ず、同種のプロトコルが混在する環境下では有効に機能を発揮できない。帯域制御装置ではネットワークを流れるデータの中身を解析し、設定されたポリシーを基に詳細な帯域制御を実現することができる。また製品によっては詳細なフローコントロール、レートコントロールが可能で、ネットワーク帯域を最大限有効に利用するための制御を行うことができる。ただし帯域制御装置は一般的に高価で、設定・維持管理に関するノウハウが必要であるため導入の難易度は高い。また帯域制御装置に加え、アプリケーション制御や制度整備により、災害時に利用可能なシステムやユーザの利用等を制限する方策についても検討する必要がある。

## 5.2 マルチキャスト通信

マルチキャスト通信とは決められた複数の配信先に対して一対多で効率的に通信を行う技術である。通常の 1 対 1 の通信に用いられるユニキャスト通信を複数実施する場合と比較して、限られた回線帯域を有効に活用できる(図 5-3 参照)。防災業務における災害現場の動画ライブ配信や同報型一斉配信等を実現する際に適した技術であるため、防災ネットワークを整備する際には、あらかじめ対応するネットワークや機器を選定しておくことが推奨される。

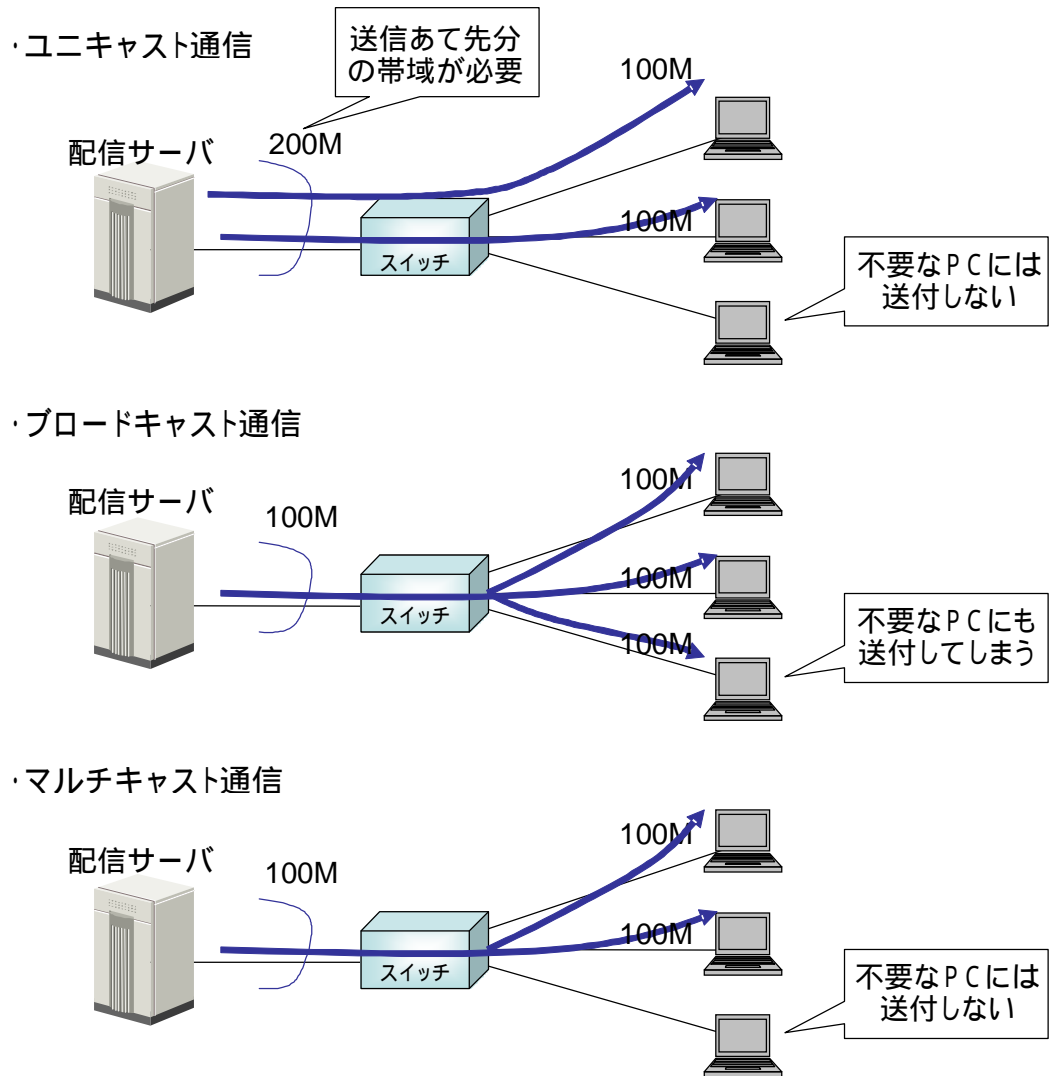


図 5-3 ユニキャスト、ブロードキャスト、マルチキャスト通信の違い

## 6. セキュリティ対策

---

防災ネットワークは平常時と災害時の両方を想定したセキュリティ対策が求められる。本章では、ネットワークの論理分割、および他団体接続に関するセキュリティ対策について紹介する。

### 6.1 ネットワーク論理分割

1 つの物理回線を論理分割し、異なるセキュリティポリシーのネットワークを混在させるための技術である。ネットワークの新規整備が難しい場合、この技術により既設の公共ネットワークやインターネット、民間回線を用いて安価にネットワークを構築することが可能である。推奨される方法としては VPN や VLAN 等がある。

なお、ネットワーク論理分割については、「地域公共ネットワークに係る標準仕様(平成 19 年 4 月改訂版)」(総務省情報通信政策局地域通信振興課 / [http://www.soumu.go.jp/joho\\_tsusin/manual/ck\\_network/pdf/01.pdf](http://www.soumu.go.jp/joho_tsusin/manual/ck_network/pdf/01.pdf))等を参考とすることが望ましい。

### 6.2 セキュリティ対策

インターネットとの接続点がある場合の対策として、不正侵入、攻撃、ウイルス感染等のリスクを軽減するために、ファイアウォールによる通信制御、ウイルス対策ゲートウェイ、不正侵入検知装置等の導入が有効である。

なおセキュリティ対策については、「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成 18 年 9 月策定)」3.6 技術的セキュリティ(総務省自治行政局地域情報政策室 / [http://www.soumu.go.jp/s-news/2006/pdf/060929\\_8\\_1.pdf](http://www.soumu.go.jp/s-news/2006/pdf/060929_8_1.pdf))等を参考とすることが望ましい。

### 6.3 リモート接続

関連機関が団体の防災ネットワークに接続して防災情報をやりとりする手段として、リモート接続が挙げられる。このように外部機関と接続する際には、セキュリティの確保が特に重要となる。その際の簡易な接続方法としてインターネット VPN が有効である。この方法は安価なインターネット接続サービスを利用し、仮想的閉域網を構築することでセキュリティを確保することが可能である。リモート接続に利用される技術である IPSec と SSL-VPN について、その特徴を次に示す。

表 6-1 IPsec と SSL-VPN

名称	IPsec (IP Security Protocol)	SSL-VPN (Secure Socket Layer VPN)
暗号化手法	ネットワーク層の暗号化技術 IP パケットとして暗号化するため、 上位層のプロトコルの制限なし	セッション層の暗号化技術 アプリケーション層はHTTPSをサポート するものに限定される
ソフトウェア	専用のクライアントソフトが必要	通常のブラウザで利用可能
その他	対応 VPN 間でトンネルを構成	端末毎に Web ブラウザと VPN 装置間で トンネルを構成

## 7. ファシリティ関連

災害に備えた防災ネットワーク自体の信頼性向上に加え、その基盤となるファシリティについても信頼性向上が必要とされる。本章では、ファシリティの信頼性向上策について紹介する。

### 7.1 ファシリティの信頼性向上策

#### (1) 回線敷設時の対策

事務室に通信ケーブル等を配線する際に、ケーブルを剥き出しにしたままにしておくと、踏まれるなどして損壊する可能性が高くなる。このような場合、配線収納管等を利用し、通信ケーブル等の損壊を防ぐ必要がある。また配線の不燃化、構内回線の引き込み口等に延焼防止、耐火等の措置を講じる。ノイズの多い場所で使用する通信ケーブルについては、シールドされた STP ケーブルを使用するようにする。

#### (2) 機器の耐災害対策

ネットワーク機器の耐災害対策の重要なポイントとしては、機器の設置要件に関するものが多い。機器を設置する際は、機器製造業者が推奨する方法を採用して固定し、「情報システム安全対策基準(平成9年9月最終改正)」5 設置基準(通商産業省告示第536号 / <http://www.meti.go.jp/policy/netsecurity/downloadfiles/eseu03j.pdf>)や「公共建築工事標準仕様書」で記載された基準に準じた設置工事を行うことが重要である。

機器の対災害対策として有効な方法について以下に示す。

表 7-1 機器の対災害対策

災害名称	対策内容
地震	機器に対して架台の使用、耐震ベースの使用、床直接固定などの転倒防止措置を講じる。 機器、関連設備に連動して運転制御をする地震感知器を設置する。
水害	水害に備え、床下防水加工、防水堤、漏水検知機等の漏水・浸水対策も実施する。
落雷	端末やモデムなどの通信設備に避雷措置を講じる。
火災	災害時における火災に備え、窒素ガス消火設備等、機器に対する影響が少ない消火設備が整備された施設に設置するようにする。

#### (3) 電源対策

ネットワーク停止の事例としては災害時の停電や瞬断によるネットワーク機器の故障が多い。多くのネットワーク機器は安定的な電源供給を前提として動作するため、電源対策は非常に重要となる。

電源対策としては、自家用発電装置を保有することが理想的であるが、導入コストが高くなる場合が多い。また建物の設置環境等により導入が難しい場合もある。

簡易な電源対策としては、無停電電源装置(UPS)等のバッテリータイプの機器導入が効果的である。この場合の留意点としては、あくまで短時間の電源対策であるため応急処置に過ぎず、電源が正常に供給されるまで対策が有効に実施される保証はないことである。

また落雷等による過電流から機器を保護する措置として、避雷器の導入が有効である。

電源対策はネットワーク機器だけでなく、防災システムを構成するサーバや端末等、全てのハードウェアを対象とした総合的な対策である必要がある。ただし全てのハードウェアの電源対策がコスト上難しい場合は、優先度の高いものに限定して実施することが有効である。

ファシリティに関する詳細については、「地方公共団体における情報セキュリティポリシーに関するガイドライン(平成18年9月策定)」3.4 物理セキュリティ(総務省自治行政局地域情報政策室 / [http://www.soumu.go.jp/s-news/2006/pdf/060929\\_8\\_1.pdf](http://www.soumu.go.jp/s-news/2006/pdf/060929_8_1.pdf))、及び「地方公共団体における情報セキュリティ対策に関する調査研究報告書」2.1 ファシリティ管理(平成14年2月地方公共団体における情報セキュリティ対策に関する調査研究会 / <http://www.soumu.go.jp/singi/security.pdf>)等を参考とすることが望ましい。

## 8. 推進体制

### 8.1 推進体制に関する留意点

防災ネットワークは、企画・設計、構築、運用保守の各段階において、その推進体制に関する留意点がある。本章では、推進体制に関する留意点について紹介する。

表 8-1 推進体制に関する留意点

段階	留意点
企画・設計	<ul style="list-style-type: none"> <li>・災害時の行動計画・対応計画について検討する担当者を設置する</li> <li>・設計内容について専門家の耐災害評価を受ける</li> <li>・災害発生時の回線途絶や機器破損に関する対策が企画書や設計書に含まれていることをチェックする</li> <li>・防災ネットワーク途絶時の対応を、あらかじめ設計書等に盛り込んでおく (例)メイン回線途絶時に、手動でバックアップ回線に切り替える</li> <li>・入札に対して業者から提案を受ける際は、構築金額だけを重視するのではなく、ネットワークの信頼性、災害対応、保守サポート等の観点から、総合的に評価する</li> </ul>
構築	<ul style="list-style-type: none"> <li>・構築の責任者、責任部門を明確にする</li> <li>・構築開始後に設計変更が発生した場合は、耐災害性について再度評価する</li> <li>・試験段階において、災害発生を想定した切り替えテストを実施する</li> <li>・防災ネットワークが完成した段階で、耐災害性を評価する</li> <li>・ネットワーク障害発生を想定した訓練・教育を実施する(構築段階に限らず、運用保守段階においても実施する)</li> </ul>
運用保守	<ul style="list-style-type: none"> <li>・防災ネットワークの運用責任者を設置する</li> <li>・ネットワーク障害発生時に復旧を行う担当者、及び管理者を明確にし、障害発生時の連絡体制を明確化しておく</li> <li>・ネットワークの構成変更や増設を実施した際は、必ず設計書等を更新する。また設計文書の管理責任者・担当者を明確にする</li> <li>・災害発生時の復旧手順、及び正常性確認手順を明確化し、文書として作成する。またそれらの実施体制を構築しておく</li> <li>・ネットワーク回線・機器に関する保守契約・内容について確認し、製造業者やサービス提供業者の連絡先・連絡方法を明確にしておく</li> <li>・ネットワーク障害発生を想定した訓練・教育を実施する</li> <li>・定期的に防災ネットワークの耐災害性を評価し、防災ネットワークの改善を検討する</li> </ul>

推進体制に関する詳細については、「地域公共ネットワークに係る標準仕様(平成 19 年 4 月改訂版)」(総務省情報通信政策局地域通信振興課 / [http://www.soumu.go.jp/joho\\_tsusin/manual/ck\\_network/pdf/01.pdf](http://www.soumu.go.jp/joho_tsusin/manual/ck_network/pdf/01.pdf))等を参考とすることが望ましい。

## 9. 付録

### 9.1 防災ネットワーク 耐災害性チェックリスト

既存の防災ネットワークや新たに設計する防災ネットワークの耐災害性を判定するためのチェックリストを下記に示す。入札仕様書作成時のチェックリストとしての利用も想定している。

全ての項目についてチェックを行い、対災害性を判定する。チェックの結果、実施されていない項目については、そのリスクについて理解し、対策を実施することが推奨される。

表 9-1 対災害性チェックリスト

No	チェック項目	未実施の場合のリスク	対策
1	メイン回線以外に、複数ルートの回線が準備されているか？	回線途絶時に通信が中断し、情報共有が実施できなくなる。	2 章を参照し、多ルート化、バックアップ回線を検討する。
2	回線が複数ルート準備されている場合、回線途絶やネットワーク機器故障が発生した際に、自動的に切り替わるか？	手動切り替えの場合、迅速に対応できない場合があり、多ルート化、バックアップ回線の準備を実施したにも関わらず、長期間ネットワークが停止する可能性がある。	3 章を参照し、自動的に経路選択を行うネットワーク機器の導入、および対応したルーティング設定を検討する。 また 4 章を参照し、ネットワーク機器の冗長化を行い、故障時に自動的に切り替わるように設定する。
3	ネットワークの拡張性や相互接続について考慮されているか？	拡張性のないネットワーク構成の場合、将来的にネットワークの拡張や相互接続のニーズが発生した際に対応できず、ネットワークを再構築しなければならない可能性がある。	3 章を参照し、拡張性、相互接続を考慮して、ネットワーク設計を実施する。 また 4 章を参照し、ネットワーク機器選定時に拡張性のあるネットワーク機器を選定する。 また 6 章を参照し、将来的に相互接続を実施する場合を見据えて、ネットワーク論理分割が可能な VLAN、VPN 等に対応したネットワーク機器を選定しておく。
4	パーストラフィックの対策が考慮されているか？	平常時はあまり利用されていない回線であっても、災害発生時にアクセスが集中し、ネットワークの輻輳により、防災情報の共有が実施できないリスクがある。	5 章を参照し、優先制御技術の導入について検討する。 すぐに導入しない場合でも QoS や帯域制御機能を有するネットワーク機器を選定し、必要に応じて迅速に導入できる状態にしておく。
5	ネットワーク機器設置、回線工事の際に、耐震対策が考慮されているか？	災害発生時にネットワーク機器が故障し、ネットワークが停止してしまう可能性がある。	7 章を参照し、機器設置要件、回線敷設工事の内容を確認し、可能な範囲内で耐震対策を実施する。

6	ネットワーク機器の電源対策が実施されているか？	ネットワーク機器は、バッテリーが搭載されていない製品が多いため、停電発生時に回線が途絶していない場合でも、ネットワークが停止してしまう。	7章を参照し、ネットワーク機器の電源対策について見直しを行う。特に基幹線等、優先度の高いネットワークの機器については重点的に対策を実施する。
7	ネットワーク機器の冗長化または予備機の準備が実施されているか？	冗長化や予備機について考慮されていない場合、ネットワーク機器が故障した際に、長期間ネットワークが停止する可能性がある。	4章を参照し、ネットワーク機器の二重化、予備機の設置等、信頼性対策について検討し、設置箇所に応じた対策を実施する。
8	運用保守時において、災害発生時の正常性確認、復旧対応に関する体制・手順が明確になっているか？	平常時から運用保守の体制・手順を明確にしていない場合、災害発生時に運用担当者が混乱し、有効な対処を行うことができず、ネットワークが長期間停止する可能性がある。	8章を参照し、運用保守時の体制・手順の見直しを実施する。特に災害発生時の対応について平常時に十分に検討を行い、体制・手順を整備しておく、災害発生時の対応が迅速になる。
9	回線やネットワーク機器について、業者と保守契約を結んでいるか？	業者と保守契約を結んでいない場合、災害発生時に自組織内の要員で対応するしかない。	8章を参照し、保守運用体制を検討する。業務内容によっては、必要に応じ専門業者と保守契約やSLA等を締結し、業務を委託する。
10	採用しているネットワーク機器は、保守可能な製品か？	古いネットワーク機器や、安価なネットワーク機器の場合、故障・障害が発生しても、製造業者で修理・サポートが行えない場合がある。	8章を参照し、使用しているネットワーク機器について精査を行い、サポートが切れた機器は更改を検討する。
11	運用保守時に、定期的に防災ネットワークの耐災害性の評価を行っているか？	ネットワーク拡張や構成の変更により、防災ネットワークの信頼性や耐災害性が著しく低下し、災害発生時に支障をきたす場合がある。	年1回を目標に、防災ネットワークの耐災害性評価を定期的に行い、耐災害性の強化を検討する。必要な対策については予算化を検討する。 機器更改や設定変更等、比較的簡易に実施できる対策も多々ある。
12	構築および運用保守の実施体制に、防災部門と情報部門の両方が含まれているか？	災害発生時に、防災業務を行う防災部門とネットワークや情報システムを主管する情報部門が綿密に連携できていないと、ネットワークを用いた情報収集や情報共有に支障をきたす可能性がある。	8章を参照し、設計時、構築時、運用保守時の体制を検討する。特に防災部門と情報部門が相互に連携できる体制を構築する。