第XXII部

ＷＩＤＥネットワークの現状

第 22 部
WIDEネットワークの現状

第 1 章　TWO wg

本章では、TWO wg の今年度の活動報告を行う。各 WIDE NOC における今年度の状況報告と、今年度特に目立った WIDE バックボーンへの DoS 攻撃の傾向についてまとめを行う。

1.1 WIDE NOC

本節では、WIDE NOC のトポロジと接続組織、および、昨年度の変更作業状況を示す。

1.1.1 旭川

- (2002/7/15) 2001/9/11 から運用していた JGN 経由の T1 を廃止、IPv4 を cisco1.nezu との間で GRE トンネルへ

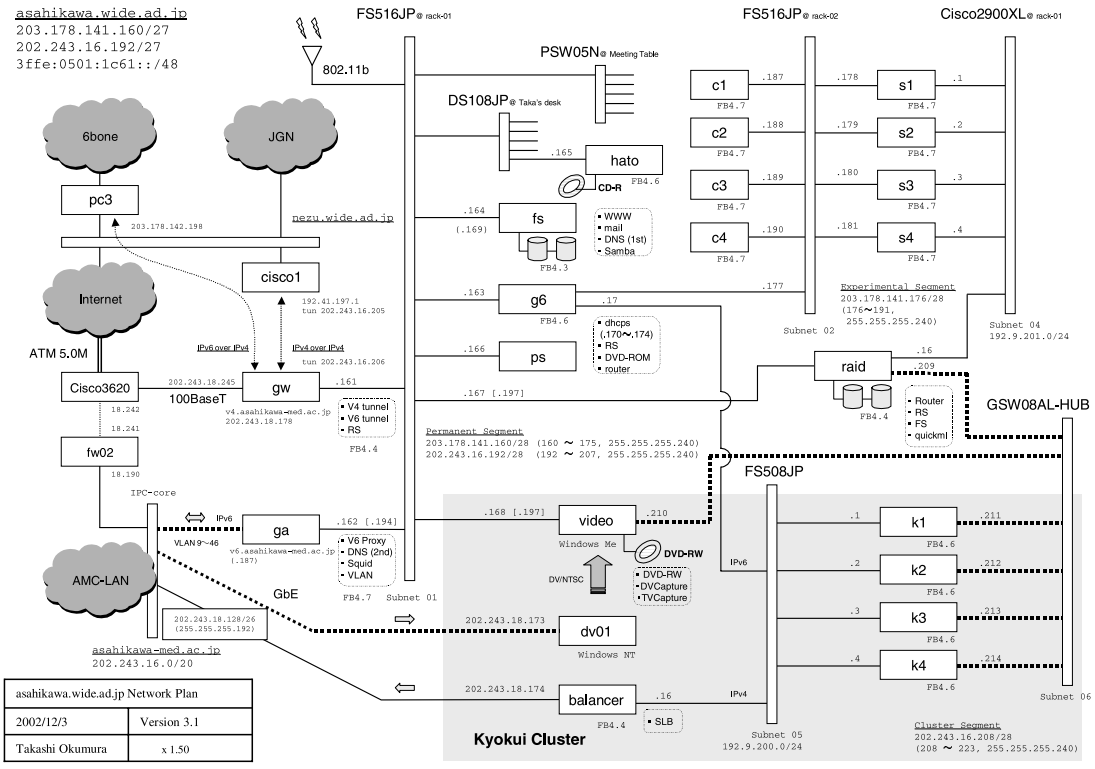

図 1.1.　旭川 NOC

1.1.2 京都

- (2002/4) Cisco7500 を Juniper M5 に更新
- (2002/11) news.kyoto.wide.ad.jp 廃止 (左京へ)
- (2002/12) trans-nt.com との接続を廃止 (左京へ)

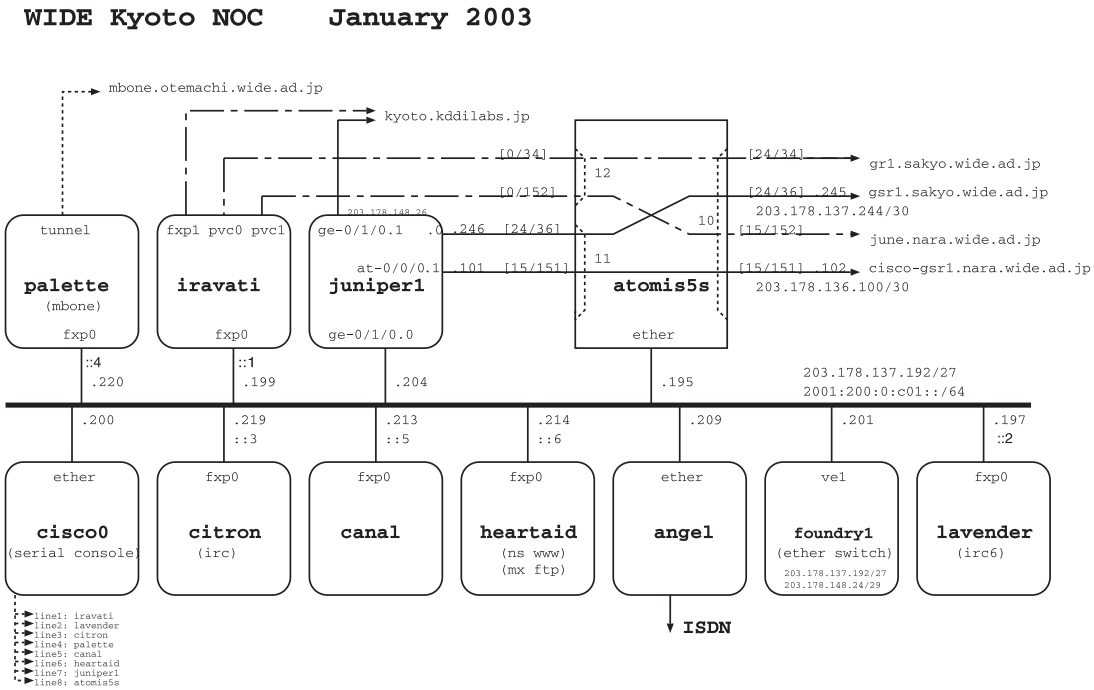

図 1.2.　京都 NOC

1.1.3 広島

- 大きな変更なし

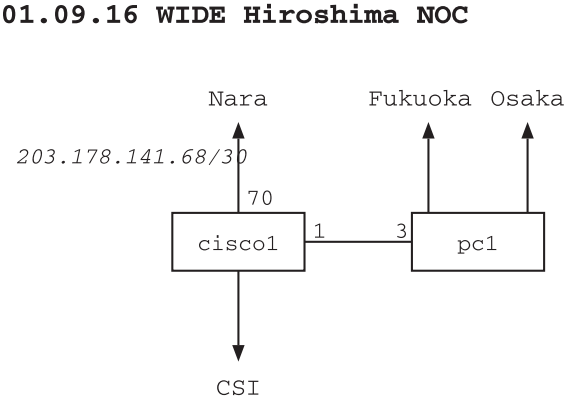

図 1.3. 広島 NOC

1.1.4 左京

- (2002/4) 左京 NOC–京都 NOC 間を BBCC 線 (OC-3) から DF(OC-12) に変更
- (2002/6) gr1.sakyo.wide.ad.jp 設置 (GR2000-4, WIDE 6bone 用)
- (2002/9) sakyo–nezu(IPv6) link up(JGN 経由)
- (2002/10) news.sakyo.wide.ad.jp 設置 (newsfeed.media.kyoto-u.ac.jp)(10 月)
- (2002/12) trans-nt.com と接続

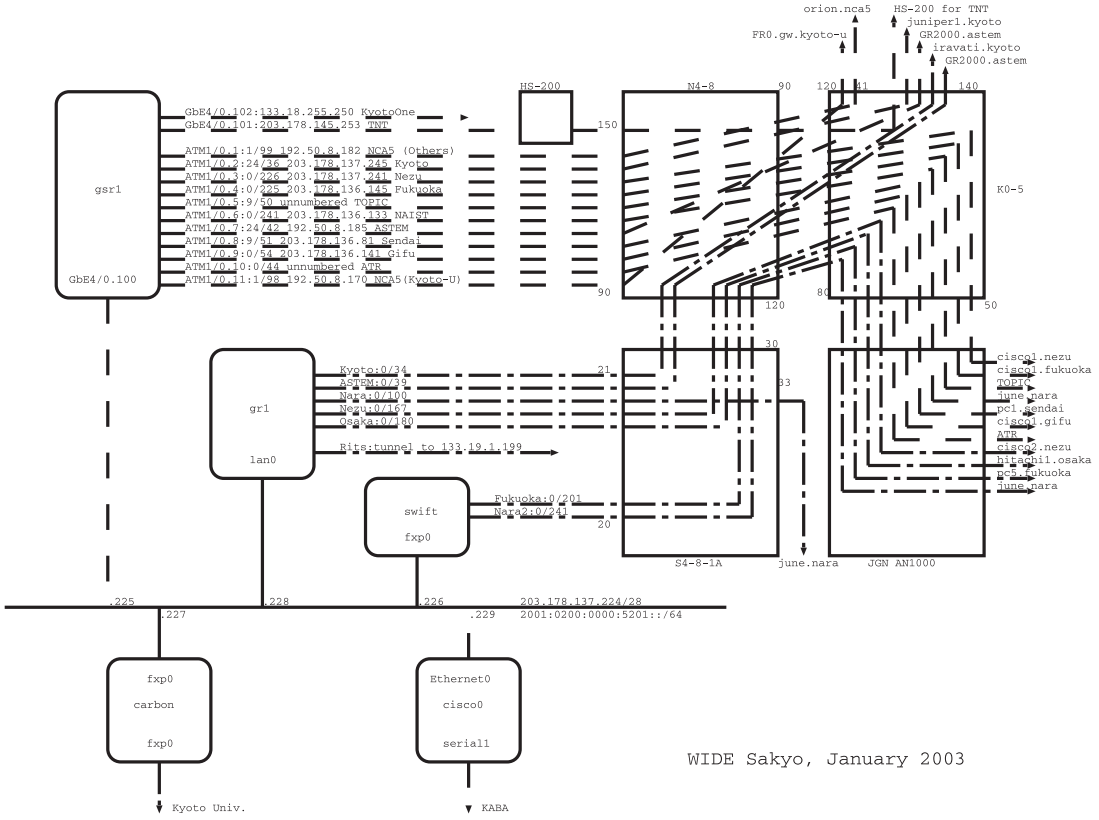

図 1.4.　左京 NOC

1.1.5 小松

- 通信・放送機構・北陸 IT 研究開発支援センター (愛称:StarBed) を下流接続組織として接続
- cisco3.komastu(Cisco7607OSR) の導入
- NOC 内のサーバセグメントの収容先をを cisco1 から cisco3 へ変更
- cisco3 を WIDE バックボーンのルートリフレクタに

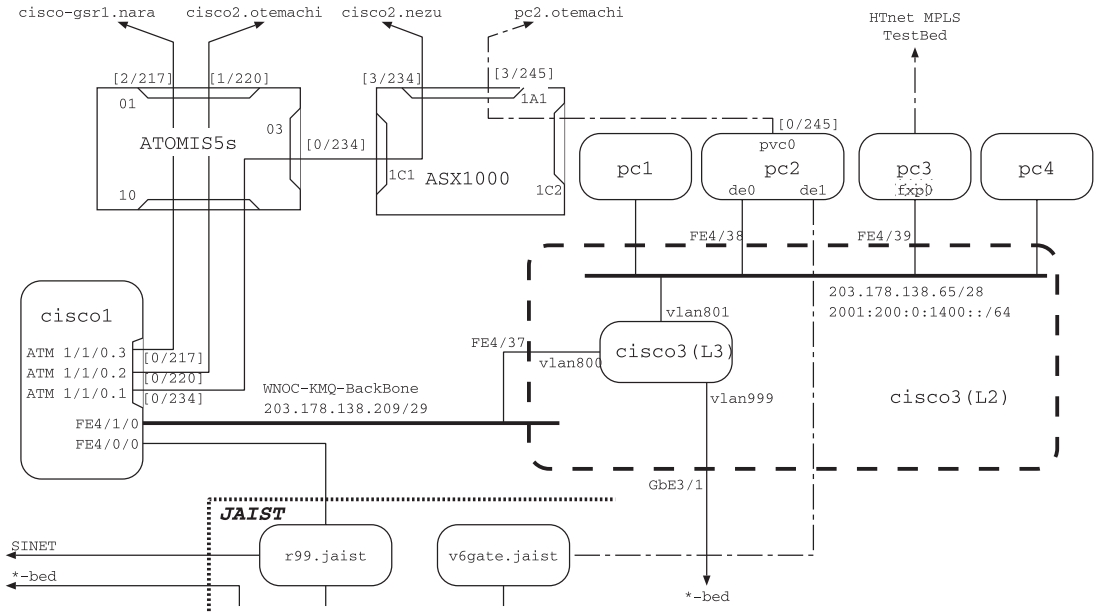

図 1.5. 小松 NOC

1.1.6 仙台

- (2002/9) 仙台 POP として IPv6 接続 (nezu-sendai, UBR44M)
- pc1.sendai 更新 (同様の PC ルータを予定)

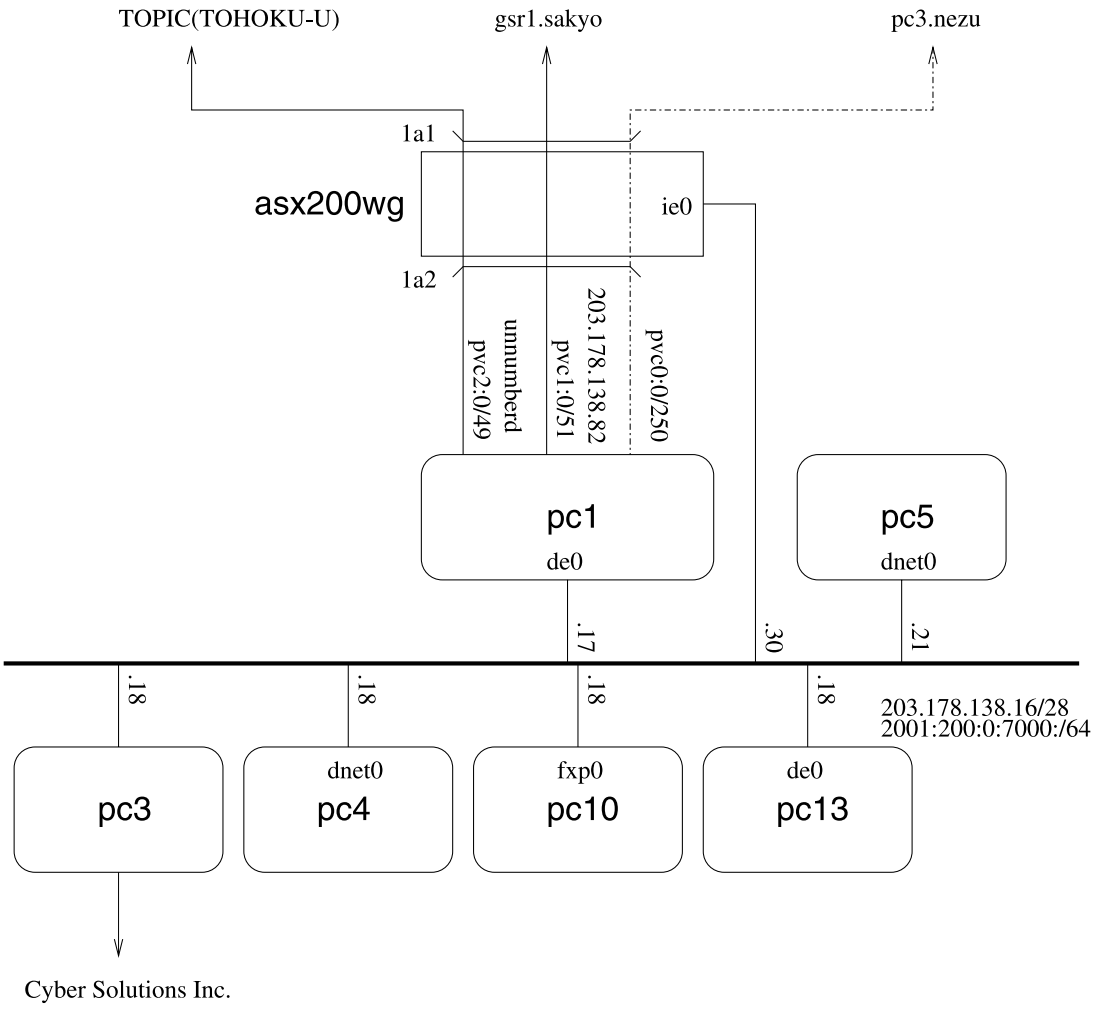

図 1.6.　仙台 NOC

1.1.7 倉敷

- JGN の回線で奈良 (WIDE) 向きに 100 Mbps(ATM UBR) 確保
- 既存の 10 Mbps 回線と同時に juniperM40 で奈良向きに接続して冗長構成に変更
- 美星天文台、美星スペースガードセンターのアドレスをリナンバ、*wide BB アドレス返却 (3/1 予定)

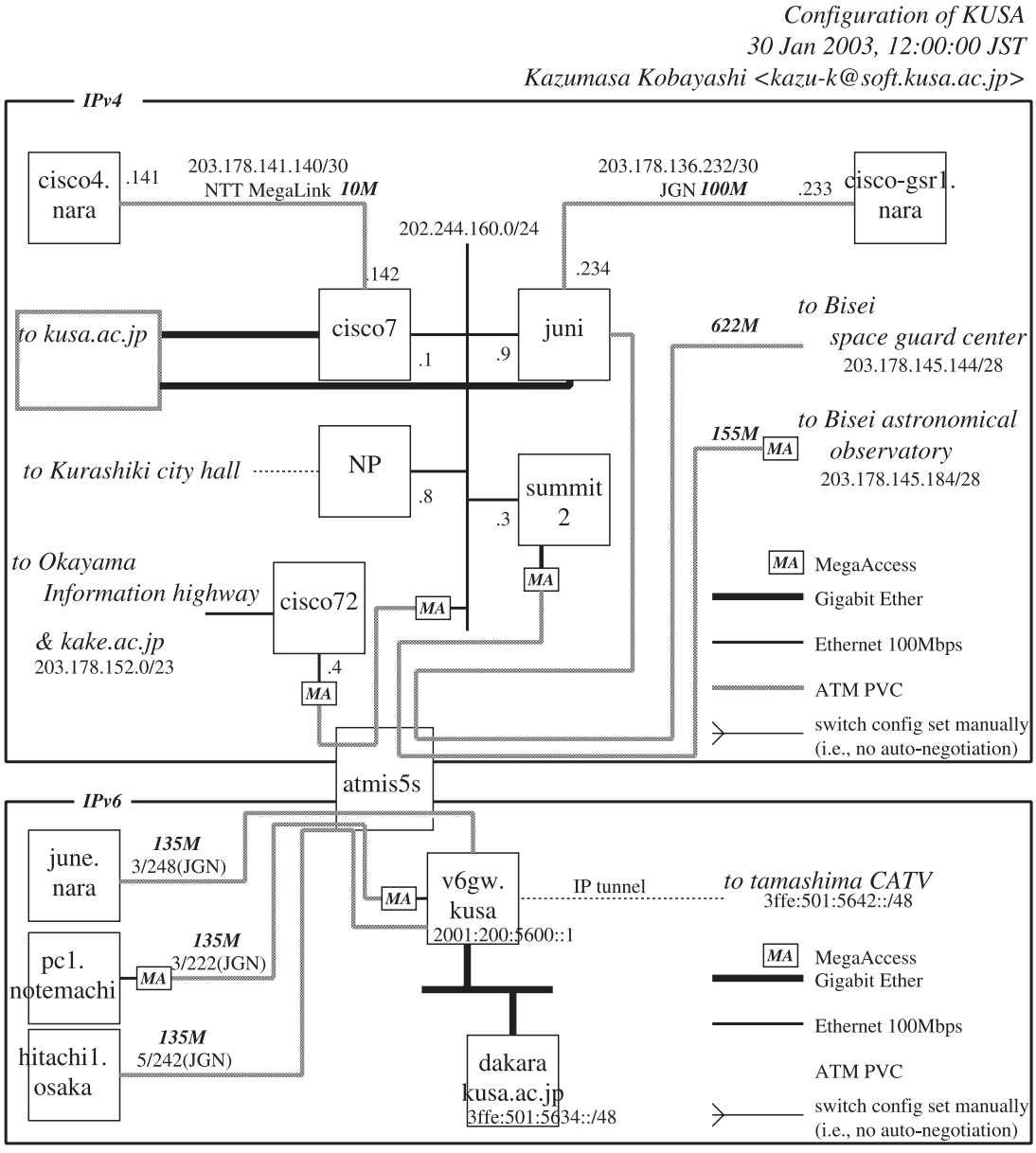

図 1.7. 倉敷 NOC

1.1.8 大阪

- 奈良–大阪を BBCC から JGN に回線変更
- csr-core1.osaka(IPv4)，　csr-core2.osaka(IPv6)
  を廃止
- hitachi1.osaka を設置

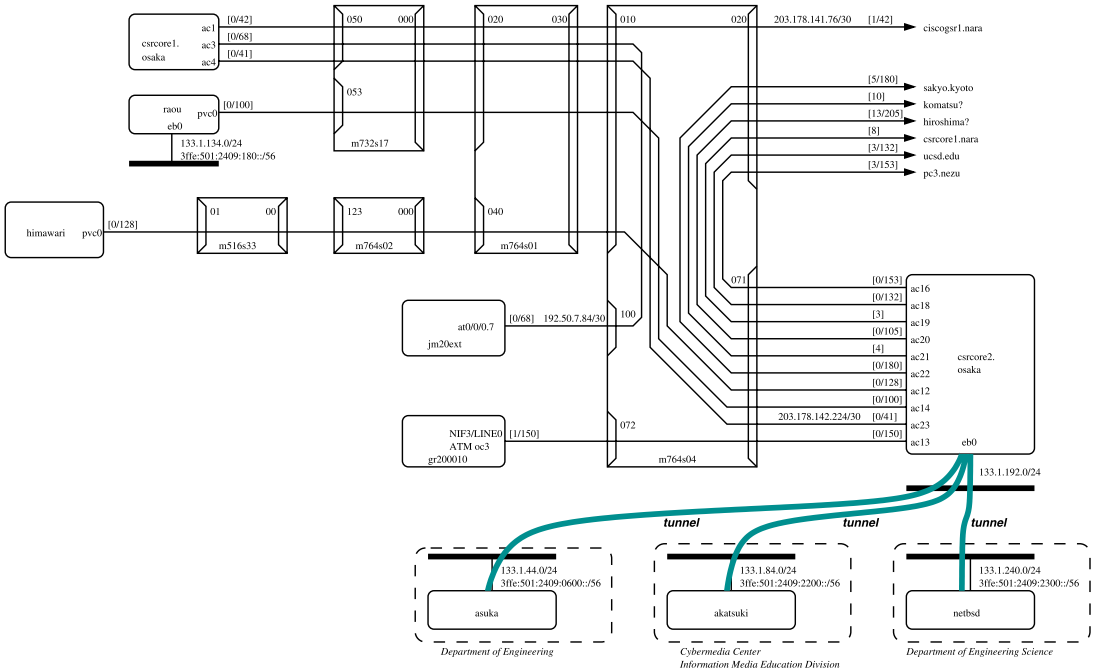

図 1.8.　大阪 NOC

1.1.9 東京

東京 NOC はもともと WIDE の最も古い NOC であり、そのトポロジーが非常に複雑であった。また、利用していた機器なども古く、台数も多かったため、管理コストが増大していた。そのため、2001 年初頭からネットワークの構成変更を行ってきたが、この度ネットワークの再構築が概ね終了した。

本構成変更の最終的な目的は、Leaf 収容に利用するネットワークとサービスを提供するネットワークの分離、IPv4/v6 ともに利用できる環境、中心部分を遠隔地から制御できるようにするための電源供給部分の改善、及び接続の冗長化である。現在の段階で上記目的はほぼ達成された。今後は情報収集をスムーズに行えるような仕組みの実装を行う予定である。

- (2002/1/18) irc.tokyo.wide.ad.jp 移設
- (2002/1/21) Eden による監視試験開始
- (2002/3/29) News サーバーの移設
- (2002/5/2) ネットワークの構成変更、経路制御の修正
- (2002/10/22) ホスト等のリナンバーを行った
- (2002/10/30) Powerdcom 回線の引き込み
- (2002/10/31) WIDE CA サーバーの設置
- (2002/11/28) 広域 Ether 網への接続、GR2000, Summit1i の運び込み
- (2002/12/1) NOC の法定点検
- (2003/1/23) FDDI 回線撤去
- その他暫時各 Leaf サイトの収容変更及び Dual-Stack への移行
  各種セキュリティーホールへの対応

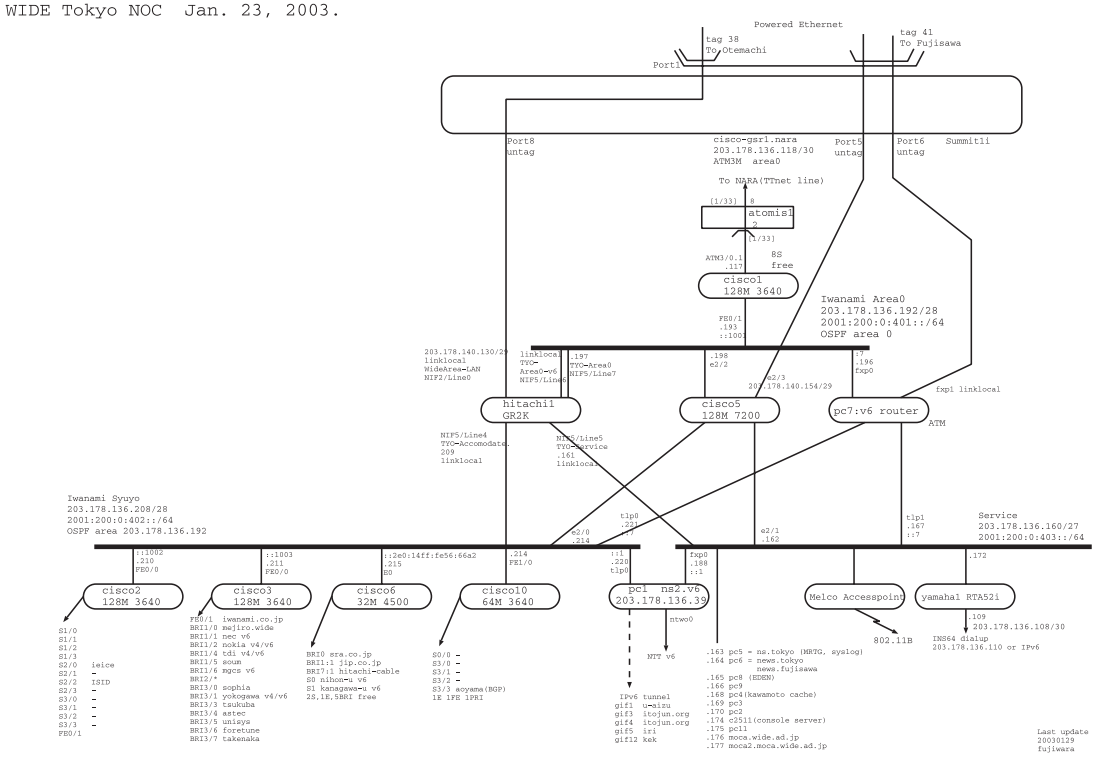

図 1.9. 東京 NOC

1.1.10 藤沢

- otemachi-fujisawa ATM 線廃止
- gifu-fujisawa HSD 線廃止
- 7 拠点ネットワークを otemachi-fujisawa ATM 線にかわる
- バックアップ回線として設定
- foundry1.fujisawa に M4 を導入し L3SW に設定
- juniper2.fujisawa を設置 (NTT 東日本 Flets IPv6 実験用)
- atomis5s*2, atomis7m を atomis7 に移行
- JGNv6 用 MegaAccess*4 を nezu に移動
- cisco1.fujisawa, cisco8.fujisawa, cisco15.fujiswa を撤去
- キヤノン: 廃止
- 湘南国際女子短期大学: 廃止
- 東芝: yagami に移動
- 日立ソフトウェア: tokyo に移動
- gsr1.fujisawa において AI3 と IPv6 BGP peering を開始
- AI3 用 NDNNYF セグメントの設定 (奈良との通信用)
- AI3 用 KNNYF セグメントの設定 (APAN との BGP peering 用)

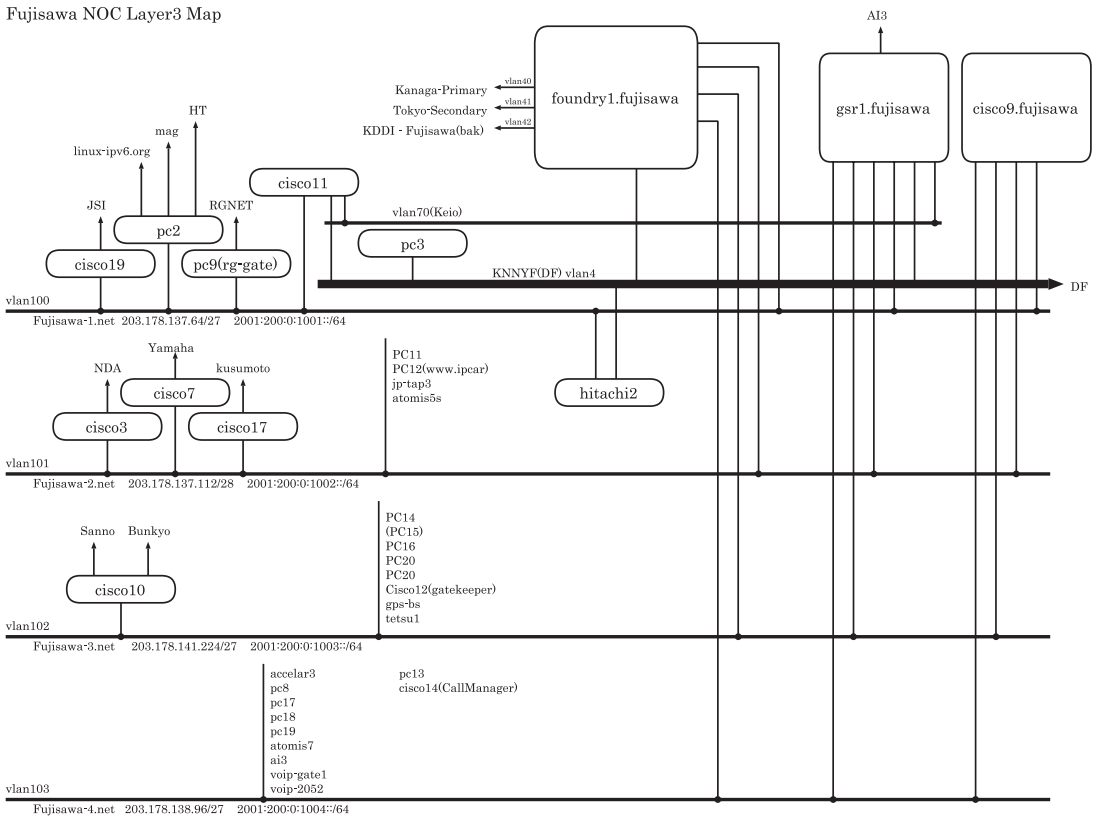

図 1.10.　藤沢 NOC

1.1.11 堂島

- 堂島第 3 ビルフロア移転中 (4F から 5F)

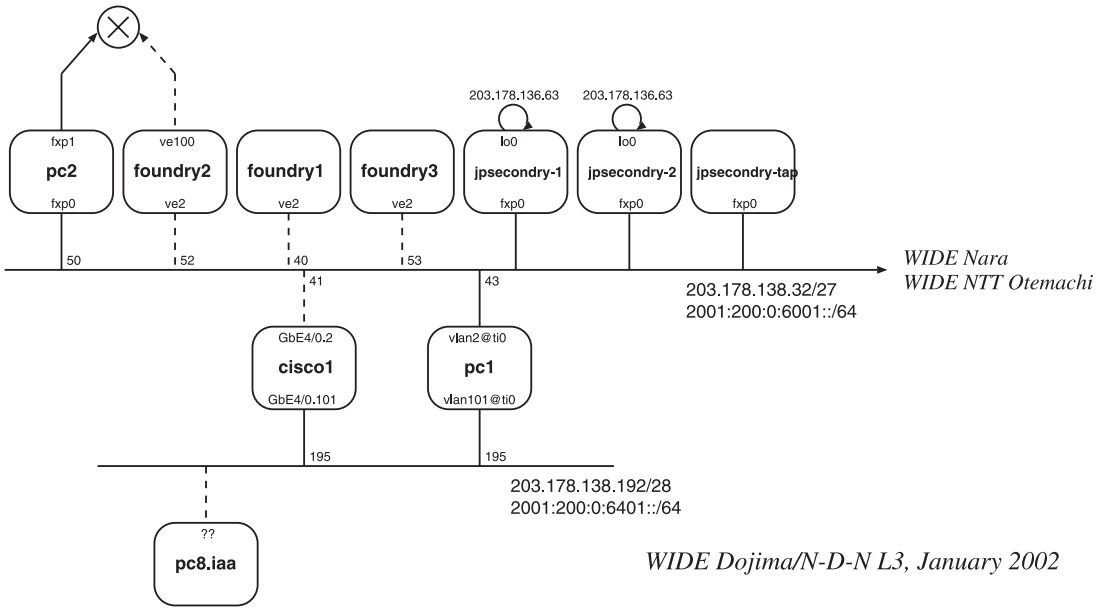

図 1.11. 堂島 NOC

1.1.12 奈良

- (2002/4) cisco6.nara (AI3 接続) 設置
- (2002/4) 松下接続廃止、cisco8.nara(松下接続) 撤去
- (2002/6) 奈良–大阪を BBCC から JGN に回線変更、csr-core1.nara, csr-edge1.nara(大阪 IPv6 接続) 撤去、pc5.nara(大阪 IPv6 接続) 設置
- (2002/9) GPS NTP サーバ ntp.nara 設置
- (2002/11) hitach1.nara(NIIT 接続) 設置
- (2002/12) TAO 奈良リサーチセンターを接続 (IPv4)

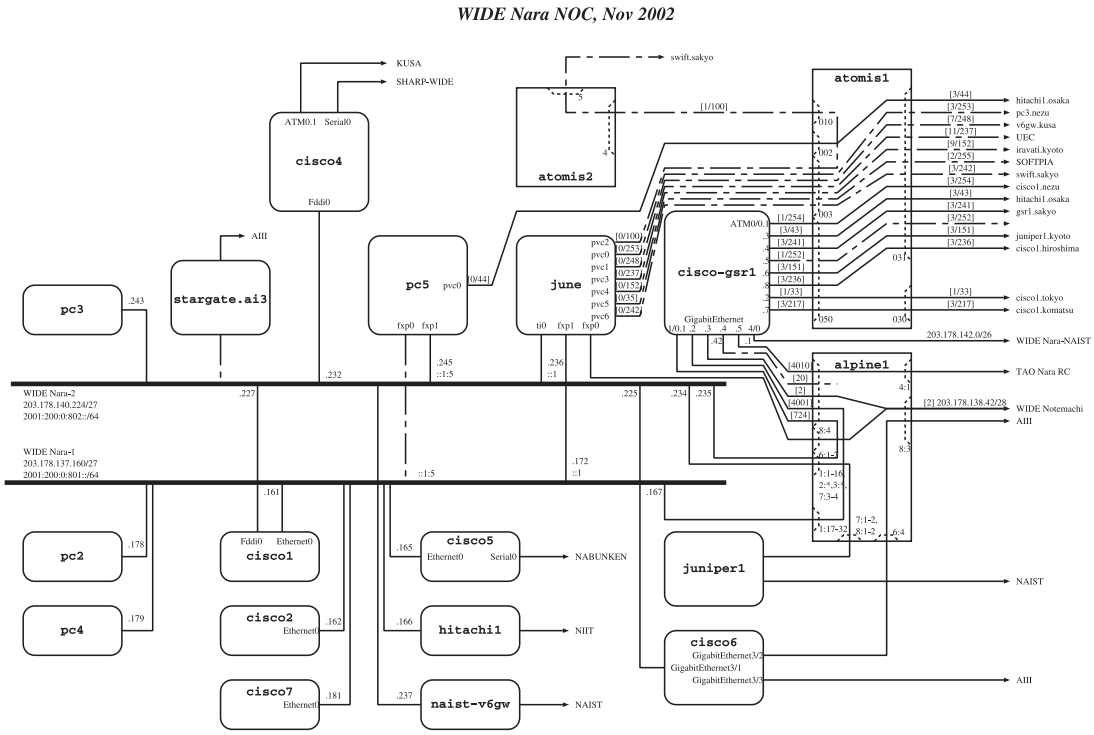

図 1.12.　奈良 NOC

1.1.13 八王子

- 大手町の v6 の受け口が pc8.otemachi から pc11.otemachi になった

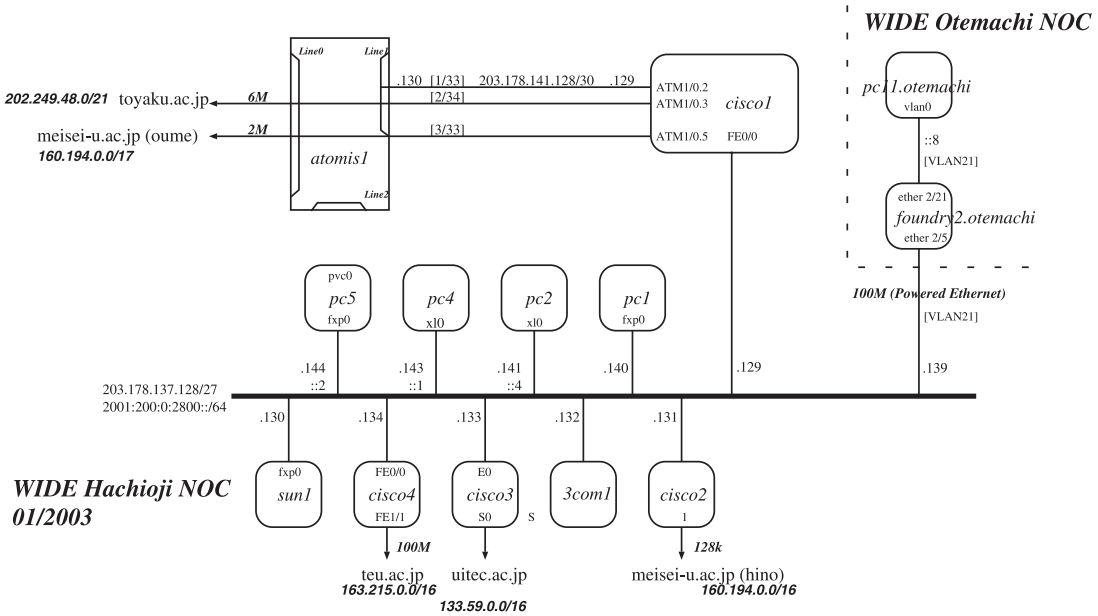

図 1.13. 八王子 NOC

1.1.14 福岡

- pc1.fukuoka.wide.ad.jp 撤去 (福工大 WIDE 回線休止のため)
- pc4.fukuoka.wide.ad.jp 撤去/ cisco4.fukuoka.wide.ad.jp 撤去 (ISIT のレンタル期限超過のため)
- 福工大休止
- 九州大学 peer が切れた状態 (復旧作業は近々行う予定)
- QGPOP/GENKAI(as2523) との peering について今後接続作業を進める予定

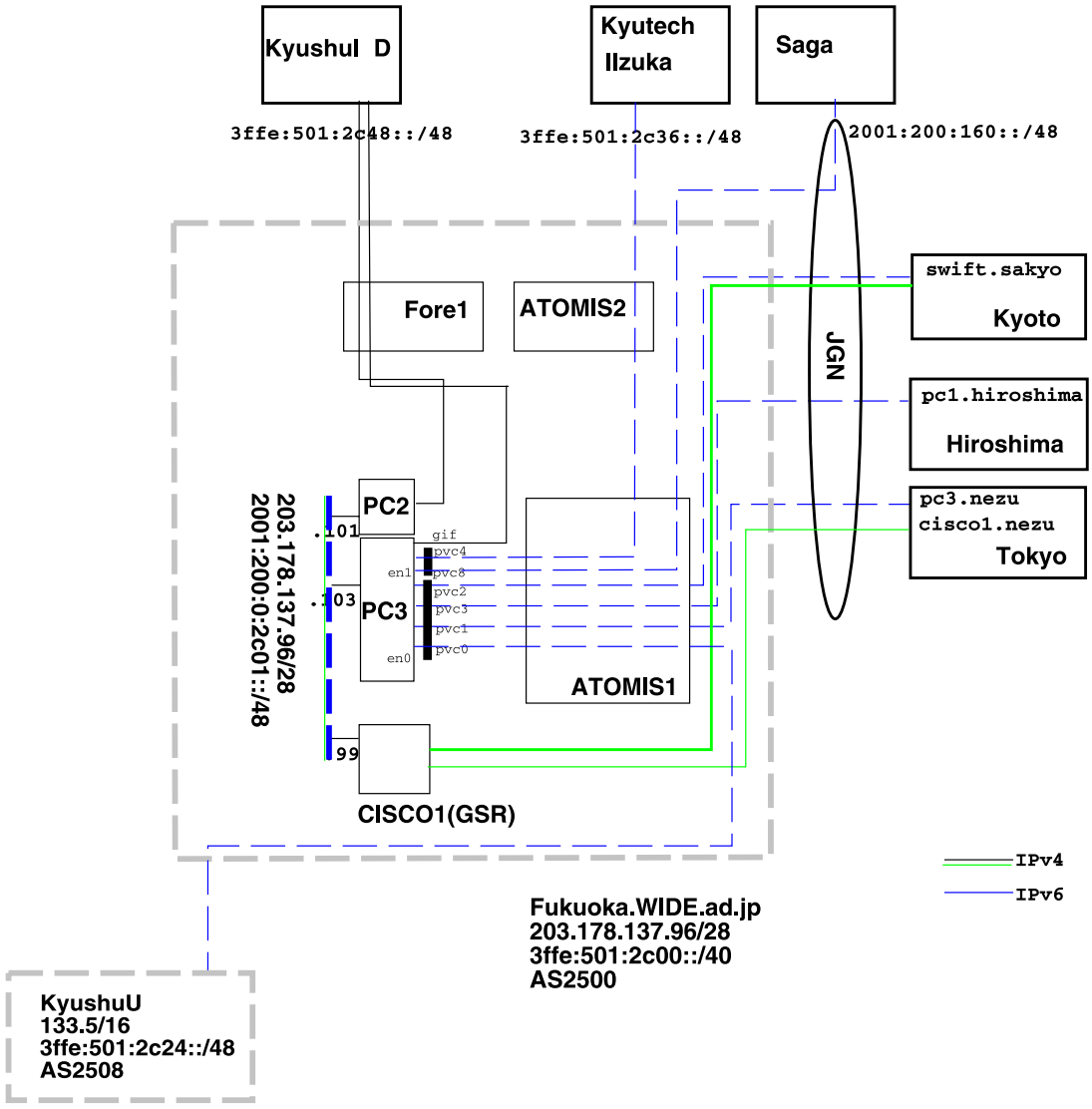

図 1.14.　福岡 NOC

1.1.15 矢上

- (2002/2/22) GSR1(cisco 12000) 設置 (電源の準備が間に合わなかったので設置のみ)
- (2002/2/22) IA-Server 設置
- (2002/3/15) NTT 東日本メトロイーサ開通、GSR1 設定
- (2002/3/28) Flets 網 ATM Megalink 開通、Atomis 設置
- (2002/4/5) cisco1(cisco 7400) 設置
- (2002/8/26) IA-Server リプレース
- (2002/10/5) パワードコム七拠点イーサネット開通

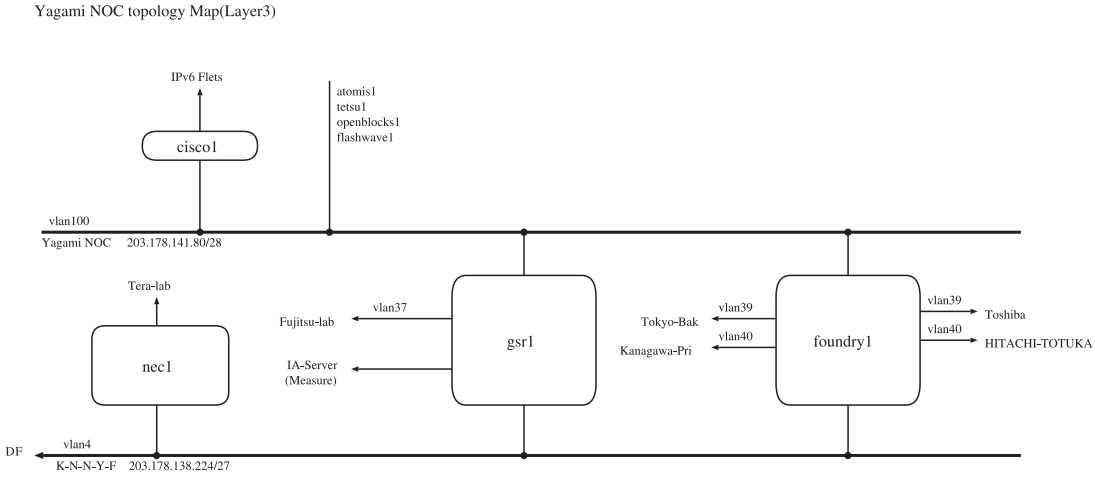

図 1.15. 矢上 NOC

1.1.16 KDDI 大手町

- otemachi-hachioji ATM 廃止
- いくつかの接続組織が Ethernet サービスに移行
- LosAngeles への国際線が OC-3 になる

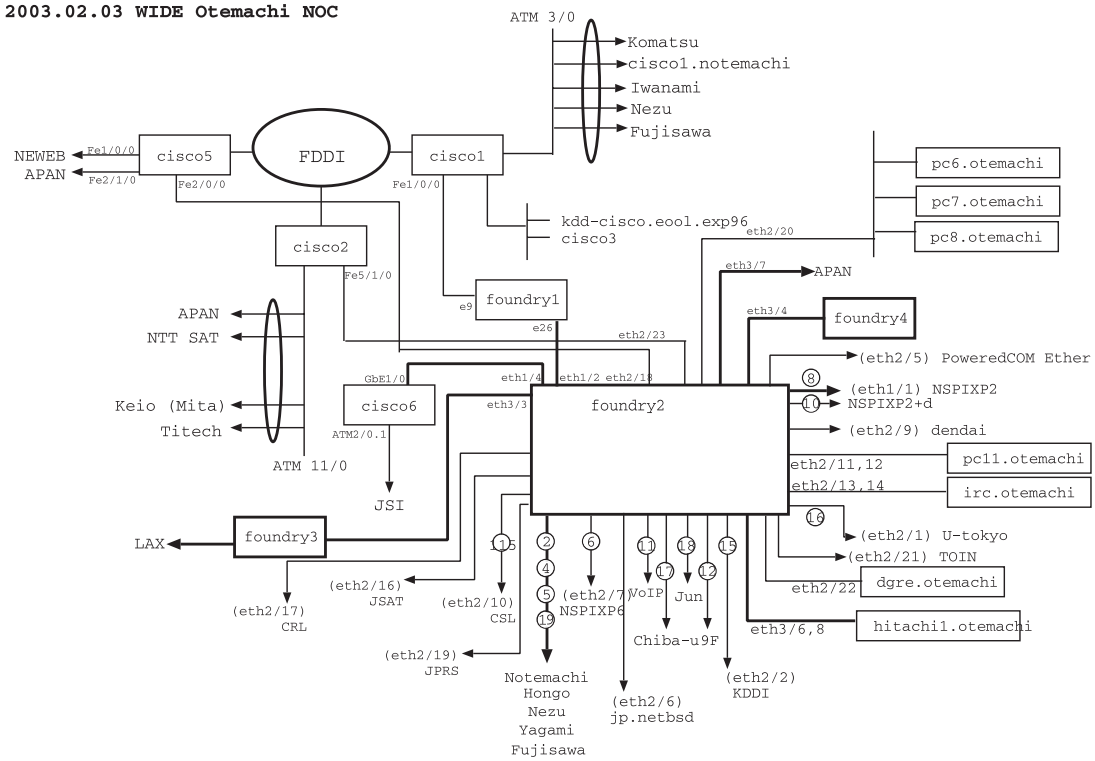

図 1.16.　KDDI 大手町 NOC

1.1.17 根津

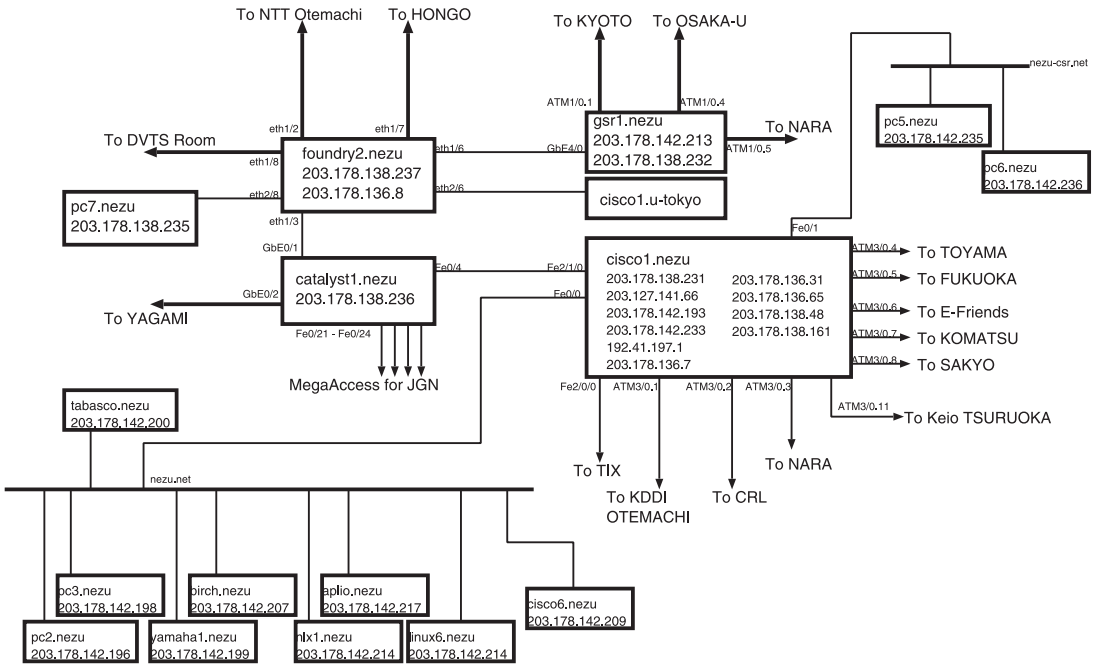

図 1.17. 根津 NOC

1.1.18 LosAngeles

- JAPANNET への接続停止
- UUnet への接続開始

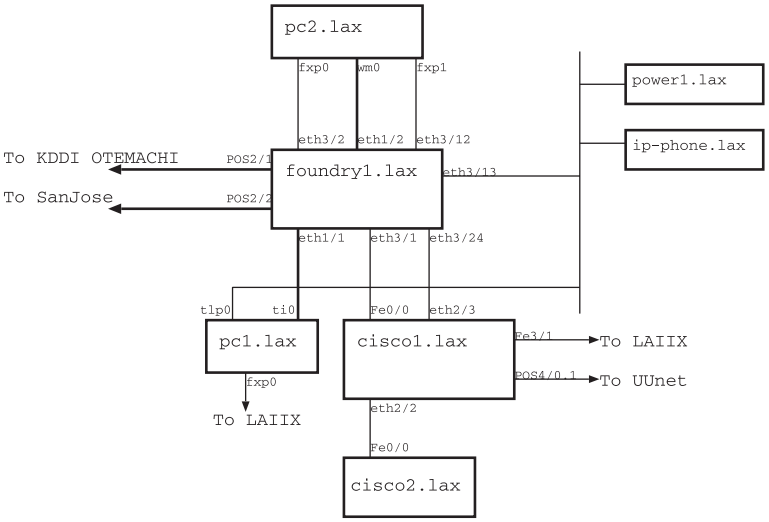

図 1.18.　LosAngeles NOC

1.1.19 NTT 大手町

- C 社製品機器不具合にから field notice に基づき line card の変更
- 分散 NSPIXP2 用の機器 (10GE-LR/BI8000) 設置/実験
- IEEAF 収容回線 (10GE-LR/10GE-ER/OC-12POS) および機器 9(foundry4) 設置

WIDE Notemachi NOC Jan. 17, 2003

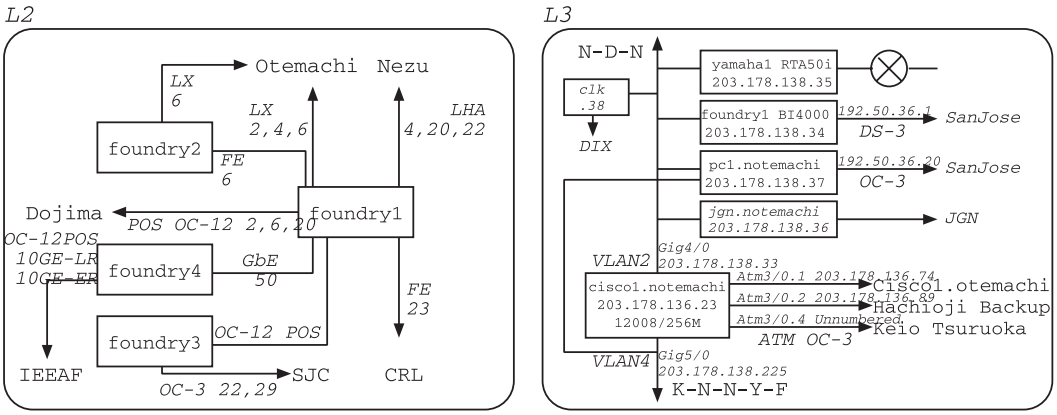

図 1.19. NTT 大手町 NOC

1.1.20 SanJose

- Internet2(Abilene) 収容回線 (DS-3 から OC-3)/機器 (C7206 から GSR) の変更
- NTTMCL 回線 (DS-3) 収容 L2SW(Summit から BI4000) の変更

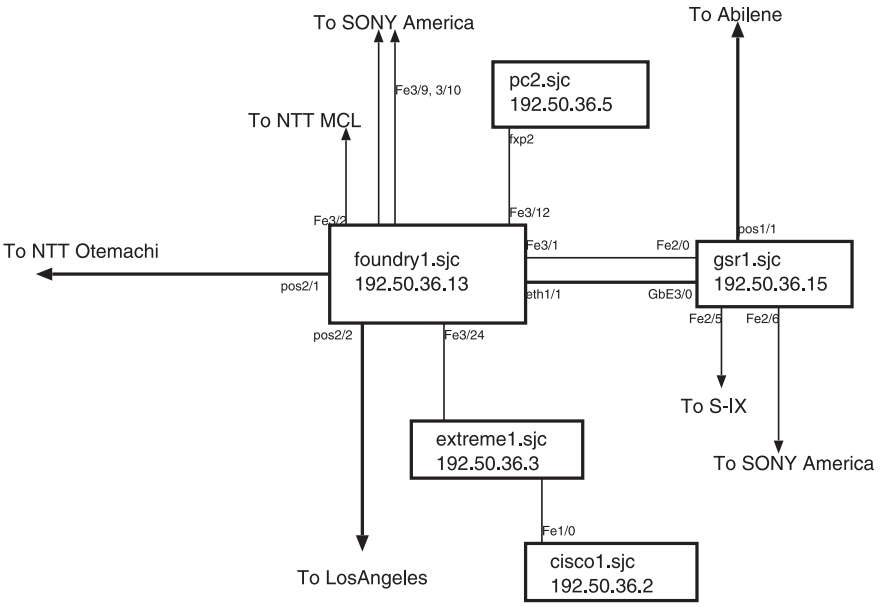

図 1.20.　SanJoseNOC

1.1.21 7 拠点広域イーサネット

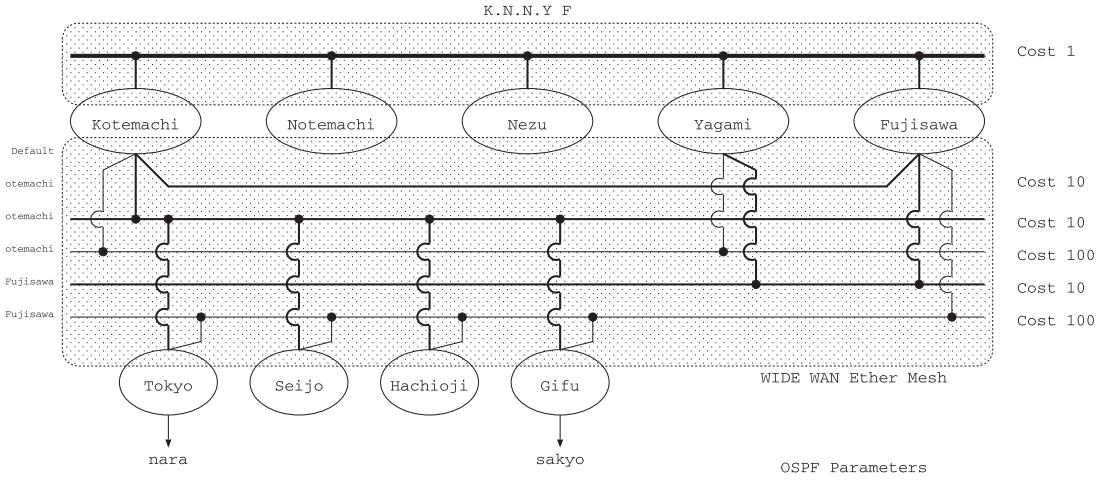

図 1.21. 7 拠点広域イーサネット

1.2 WIDE バックボーンに対する DoS 攻撃の傾向

1.2.1 DoS 攻撃

インターネットにおける Denial of Service(以下、DoS) 攻撃とは、大量のデータを送信することで、対象となるホストまたは途中経路のネットワーク資源を使い尽し、サービスを妨害および拒否する攻撃である。DoS 攻撃は大きく分て、logic 攻撃と flooding 攻撃の 2 種類に分類される [134]。

- logic 攻撃

  Operating System やソフトウェアのセキュリティホールにつけこみ、システムの停止やサービスの低下を引き起こす攻撃である。この logic 攻撃は OS やソフトウェアをアップデートする、もしくは、特定パターンのパケットをフィルタリングすることによって防ぐことができる。

- flooding 攻撃

  大量のパケットを送信することによって、ネットワーク資源やホストの計算機資源を占有しサービス不能状態にする攻撃である。この flooding 攻撃は、一つ一つのパケットは通常のトラフィックと比較した場合に特徴がなく、ただパケット量が多いだけである。そのため、logic 攻撃と同等の手法で flooding 攻撃を防ぐことはできない。更に flooding 攻撃の被害を受ける対象で分類した場合、ホストの計算機資源とネットワーク資源の 2 つに分類することができる。

WIDE インターネットでは、後者の flooding 攻撃によるネットワーク資源の占有を最小限に抑え、ユーザに対して快適なネットワーク環境を提供する必要がある。

1.2.2 WIDE インターネットにおける対応

WIDE インターネットは、flooding 攻撃によるネットワーク資源の占有によって、BGP の peer の切断などの被害を受けている。

そのため、WIDE プロジェクト/two ワーキンググループでは、AGURI[86] による flooding 攻撃の観測を定常的に行った。また、その観測結果に基づいて filtering による flooding 攻撃対策を行った。

WIDE インターネットは 2 本の国際線によって 2 社の ISP と接続している。この 2 本の国際線は 2 つの特徴を持っている。

1) 国際線が WIDE インターネットの出入り口であること
2) 国際線の回線帯域と国内バックボーンの回線帯域の格差が存在することである。

第一に、WIDE インターネットは外部組織との接続を、この 2 本の国際回線と NSPIXP2 などの国内 IX による相互接続によって実現している。flooding 攻撃の検知を考えた場合、攻撃は一般的に外部から来るため組織の出入り口でデータを収集するのが適当である。

第二に、WIDE インターネットの主要な国内バックボーンは Gigabit Ethernet で構成されている、しかし、2 本の国際専用線環境はそれより劣っている。そのため、この 2 本の国際線のデータを収集し、flooding 攻撃の観測を行った。この収集ポイントを以下の図 1.22 に示す。

本報告書では、収集ポイント A で収集したデータを “データ A”、収集ポイント B で収集したデータを “データ B”、収集ポイント C で収集したデータを “データ C” とする。

flooding 攻撃を抽出し傾向を把握するためには、攻撃パケットをフロー単位に集約する必要がある。なぜなら、logic 攻撃の場合と異なり、flooding 攻撃はパケット一つ一つを観察した場合には通常のトラフィックと差別化することができないからである。そのため、パケットの集合であるフロー単位でトラフィックを観察することにより、初めて flooding 攻撃を検知することができる。

一般的にフローは、5-tipuls と呼ばれる以下に示す 5 つの要素が同一のパケットの集合と定義される場合が多い。

1. source ip address
2. destination ip address
3. source port number
4. destination port number
5. protocol

しかし、flooding 攻撃を観測する上で 5-tipuls を用いたフローの定義を適応することは適切ではない。なぜなら、攻撃者によるネットワーク資源を占有は、port scan に代表される異なる port 番号のパケットによる攻撃や、複数のソースアドレスを詐称した攻撃によって引き起こすことができるからである。このような攻撃手法を用いた場合、5-tipuls のフロー定義では、大量のフローが検出されるだけで、攻撃自体の特徴を抽出することはできない。

そこで、本研究では、flooding 攻撃の定義をトラフィッ

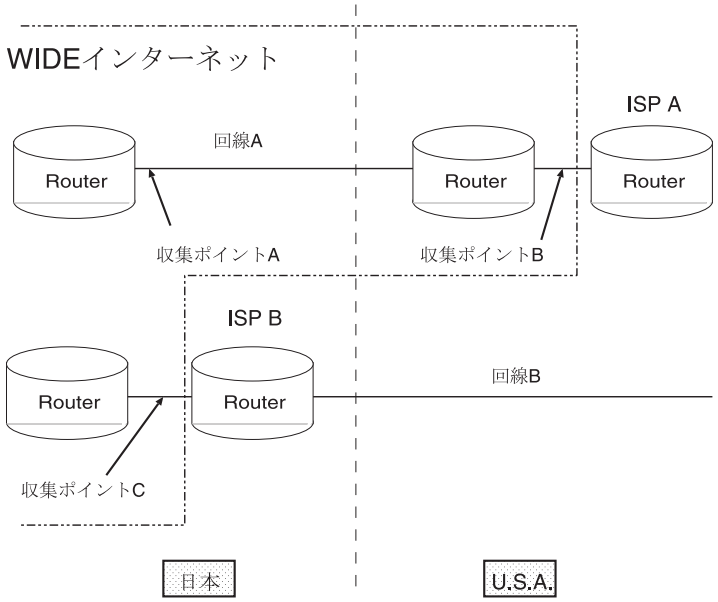

図 1.22. データ収集ポイント

ク傾向に現れる症状を基に柔軟に行う。具体的には以下に示す 4 つの条件を一つでもみたしたものを flooding 攻撃フローと定義する。

1. AGURI データ (source ip address) 内で、総トラフィックの 20%以上を占有するフロー
   AGURI では、IP アドレス空間からの流量とホストからの流量の両者を抽出することができる。そのため、抽出されたホストの IP アドレスが、同じく IP アドレス空間に含まれる場合がある。本研究では、この場合最長適合を用い、ホストからの流量を採用する。例えば、“192.168.0.5” というホストの IP アドレスと、“192.168.0/24” という IP アドレス空間を抽出した場合、本研究では最長適合する “192.168.0.5” をフローとして採択する。
   また、抽出された IP アドレス空間が “10.0.0.0/8” のように、あまりに広大である場合、その IP アドレス空間から分散してトラフィックが送信されたことを意味し、flooding 攻撃の特徴として捕らえるには現実的ではない。そのため、本研究では “/24” より狭い IP アドレス空間のみをフローの対象とする。
2. AGURI データ (destination ip address) 内で、総トラフィックの 20%以上を占有するフロー
   source ip address の AGURI データと同様の定義を行う。
3. AGURI データ (source port) 内で、総トラフィックの 20%以上を占有するフロー
   AGURI では、IP のバージョン、使用されるプロトコル、ポート番号を抽出することができる。しかし、IP のバージョンが同様であるだけ、使用されるプロトコルが同様であるだけでフローを定義すると、ほぼ全てのパケットがわずかなフローに集約される。そのため、本研究では、ポート番号まで同一のパケットの集合を同一フローであると定義する。
4. AGURI データ (destination port) 内で、総トラフィックの 20%以上を占有するフロー
   source port の AGURI データと同様の定義を行う。

上記の 4 つ条件はいずれも、総トラフィックの 20%以上のフローを検出することである。総トラフィックの 20%以上の流量のあるフローを検出するためには、全てのフローの中から、流量の多いフローを上位 5 つ抽出することで可能になる。

フローの開始からフローの終了は AGURI によるトラフィックデータの収集を基に行い、AGURI による検出が始まった瞬間から検出ができなくなった時点までを 1 つのフローとして扱う。これを、以下の図 1.23 を用いて説明する。

1 時 6 分頃から hostB 宛の flooding 攻撃が始まり、1 時 18 分頃に収束した。その後、改めて 1 時 36 分

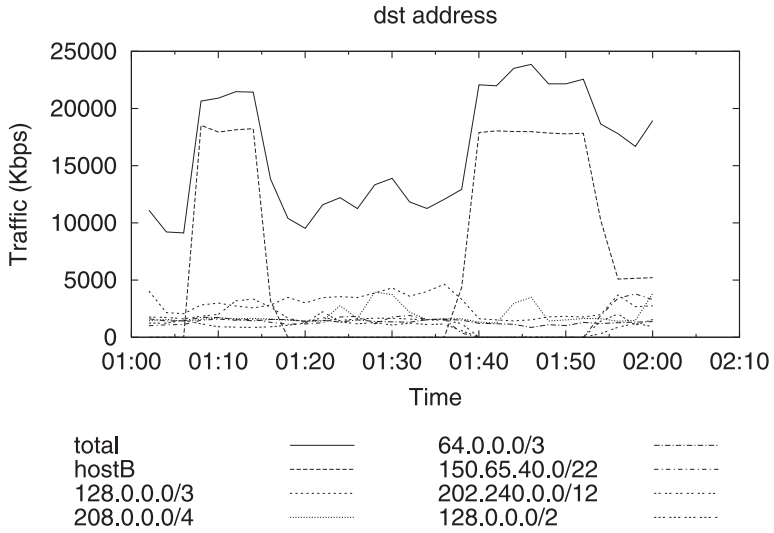

図 1.23.　2 回の flooding 攻撃例

表 1.1.　データ A における flooding 攻撃発生件数

年	月	回数
2002 年		306
	1 月	45
	2 月	39
	3 月	62
	4 月	32
	5 月	34
	6 月	36
	7 月	43
	8 月	2
	9 月	2
	10 月	1
	11 月	2
	12 月	8

頃から同様の flooding 攻撃が始まり、2 時にいたっても収束していない。

この場合、本研究の定義では、この flooding 攻撃は 1 時 18 分に一度終了し、1 時 36 分から新しい flooding 攻撃が来たと判断し、2 回の flooding 攻撃があったものとする。

上記の定義に基づいて、データ A、データ B、データ C のそれぞれのデータから flooding 攻撃の発生回数を集計した。データ A についての攻撃発生回数を以下の表 1.1 に、データ B についての攻撃発生回数を以下の表 1.2 に、データ C についての攻撃発生回数を以下の表 1.3 に示す。

表 1.2.　データ B における flooding 攻撃発生件数

年	月	回数
2002 年		11
	10 月	1
	11 月	2
	12 月	8

表 1.3.　データ C における flooding 攻撃発生件数

年	月	回数	年	月	回数
2001 年		184	2002 年		149
	1 月			1 月	18
	2 月	15		2 月	12
	3 月	27		3 月	25
	4 月	21		4 月	9
	5 月	19		5 月	12
	6 月	8		6 月	23
	7 月	27		7 月	29
	8 月	6		8 月	12
	9 月	13		9 月	3
	10 月	18		10 月	0
	11 月	14		11 月	1
	12 月	16		12 月	5

上記の表 1.1、表 1.2、表 1.3 に示されたように、2002 年の 8 月を境に flooding 攻撃の発生件数が激減している。また、2002 年の 12 月にかけて再び flooding

攻撃の発生件数が増加しはじめている。
これは、WIDE インターネットのネットワーク運用における flooding 攻撃対策の影響である。WIDE インターネットでは頻発する flooding 攻撃対策として、2002 年 8 月 12 日と 8 月 21 日に、それぞれ接続している ISP に特定の IP アドレスを送信先とするパケットのに対するフィルタ記述を依頼した。そのため、9 月以降は flooding 攻撃がほとんど検出されなかった。その後、2002 年 12 月に入ってから、フィルタ依頼をしていない別の IP アドレスを送信先とするパケットを用いた攻撃が発生したため、再び flooding 攻撃が検出されるようになった。