参考資料

参考資料１：IPv4 アドレスの国別割り振り状況

（社団法人　日本ネットワークインフォメーションセンター「インターネット資源の管理体制と活用に関する調査研究（平成 20 年３月）」（総務省からの受託調査報告書）４０９ページより抜粋）

IP アドレスの管理原則の一つに、「登録」というものがある。これは、「インターネットアドレス空間の割り当てと割り振りは、インターネットコミュニティの全メンバーがアクセス可能な、公開されているレジストリデータベースに登録されなければならない」という原則を表している。

この原則に従い、RIR では自身の行った割り振り、割り当ての情報をインターネット上に公開している。この章で掲載する統計は、その公開資料を集計したものである。
公開資料の保存箇所は以下の通りである。

AfriNIC：ftp://ftp.afrinic.net/pub/stats/afrinic/
APNIC：ftp://ftp.apnic.net/pub/stats/apnic/
ARIN：ftp://ftp.arin.net/pub/stats/arin/
LACNIC：ftp://ftp.lacnic.net/pub/stats/lacnic/
RIPE NCC：ftp://ftp.ripe.net/ripe/stats/

ここでは上記で提供されている情報をもとに統計をまとめた。なお、本章で集計した統計は全て 2008 年 1 月 31 日現在のデータを使用した。次ページ以降、資源種別（IPv4 アドレス、IPv6 アドレス、AS 番号）毎に、国・地域別の分配状況を示す。

表21： 割り当て済み IPv4 アドレス分配状況 － 国・地域別　全リスト

順位	国・地域	割当数
1	米国(US)	1,409,909,248
2	日本(JP)	141,623,552
3	中国(CN)	136,644,864
4	欧州連合(EU)	120,351,708
5	ｲｷﾞﾘｽ(GB)	83,614,522
6	ﾄﾞｲﾂ(DE)	72,429,360
7	ｶﾅﾀﾞ(CA)	71,920,640
8	ﾌﾗﾝｽ(FR)	67,803,168
9	韓国(KR)	59,456,256
10	ｵｰｽﾄﾗﾘｱ(AU)	33,460,736
11	ｲﾀﾘｱ(IT)	24,046,016
12	ﾌﾞﾗｼﾞﾙ(BR)	23,463,424
13	ﾒｷｼｺ(MX)	21,504,000
14	ｽﾍﾟｲﾝ(ES)	20,551,840
15	ｵﾗﾝﾀﾞ(NL)	19,890,216
16	台湾(TW)	19,865,344
17	ﾛｼｱ(RU)	17,256,328
18	ｽｳｪｰﾃﾞﾝ(SE)	16,891,616
19	ｲﾝﾄﾞ(IN)	13,906,688
20	南ｱﾌﾘｶ共和国(ZA)	13,610,240
21	ﾎﾟｰﾗﾝﾄﾞ(PL)	12,222,732
22	ﾌｨﾝﾗﾝﾄﾞ(FI)	8,638,592
23	ﾄﾙｺ(TR)	8,430,016
24	ﾃﾞﾝﾏｰｸ(DK)	7,902,048
25	ｽｲｽ(CH)	7,537,856
26	香港(HK)	7,246,336
27	ﾉﾙｳｪｰ(NO)	6,731,808
28	ｵｰｽﾄﾘｱ(AT)	6,709,216
29	ﾙｰﾏﾆｱ(RO)	6,675,584
30	ﾍﾞﾙｷﾞｰ(BE)	5,445,504
31	ﾆｭｰｼﾞｰﾗﾝﾄﾞ(NZ)	5,422,336

順位	国・地域	割当数
32	ｱﾙｾﾞﾝﾁﾝ(AR)	5,191,936
33	ﾁｪｺ(CZ)	4,924,800
34	ﾁﾘ(CL)	4,244,736
35	ｼﾝｶﾞﾎﾟｰﾙ(SG)	4,173,312
36	ﾀｲ(TH)	4,076,800
37	ｱｲﾙﾗﾝﾄﾞ(IE)	4,012,800
38	ﾍﾞﾄﾅﾑ(VN)	3,840,256
39	ｲｽﾗｴﾙ(IL)	3,757,248
40	ﾎﾟﾙﾄｶﾞﾙ(PT)	3,552,832
41	ﾍﾞﾈｽﾞｴﾗ(VE)	3,527,168
42	ﾊﾝｶﾞﾘｰ(HU)	3,384,192
43	ﾏﾚｰｼｱ(MY)	3,286,528
44	ｷﾞﾘｼｬ(GR)	3,182,336
45	ｺﾛﾝﾋﾞｱ(CO)	3,099,904
46	ｳｸﾗｲﾅ(UA)	2,881,088
47	ｲﾝﾄﾞﾈｼｱ(ID)	2,814,464
48	ﾌﾞﾙｶﾞﾘｱ(BG)	2,508,800
49	ﾌｨﾘﾋﾟﾝ(PH)	2,376,960
50	ｴｼﾞﾌﾟﾄ(EG)	2,177,280
51	ﾘﾄｱﾆｱ(LT)	1,969,792
52	ｻｳｼﾞｱﾗﾋﾞｱ(SA)	1,706,240
53	ｱﾗﾌﾞ首長国連邦(AE)	1,495,040
54	ｲﾗﾝ(IR)	1,446,400
55	ｽﾛﾊﾞｷｱ(SK)	1,391,104
56	ｺｽﾀﾘｶ(CR)	1,307,392
57	ﾍﾟﾙｰ(PE)	1,253,120
58	ﾗﾄﾋﾞｱ(LV)	1,252,416
59	ｽﾛﾍﾞﾆｱ(SI)	1,097,754
60	ｴｽﾄﾆｱ(EE)	1,003,008
61	ｸﾛｱﾁｱ(HR)	895,072
62	ﾊﾟﾅﾏ(PA)	872,448

順位	国・地域	割当数
63	旧ﾁｪｺｽﾛﾊﾞｷｱ(CS)	763,904
64	ﾊﾟｷｽﾀﾝ(PK)	727,296
65	ﾁｭﾆｼﾞｱ(TN)	631,040
66	ｶｻﾞﾌｽﾀﾝ(KZ)	598,016
67	ﾓﾛｯｺ(MA)	585,984
68	ﾌﾟｴﾙﾄﾘｺ(PR)	572,416
69	ｴｸｱﾄﾞﾙ(EC)	553,216
70	ｸｳｪｰﾄ(KW)	542,208
71	ｱｲｽﾗﾝﾄﾞ(IS)	530,688
72	ｳﾙｸﾞｱｲ(UY)	441,600
73	ｷﾌﾟﾛｽ(CY)	435,232
74	ｱｼﾞｱ太平洋地域(AP)	421,120
75	ﾏｹﾄﾞﾆｱ(MK)	408,320
76	ﾏﾙﾀ(MT)	394,240
77	ﾊﾞﾝｸﾞﾗﾃﾞｼｭ(BD)	382,464
78	ｶﾀｰﾙ(QA)	372,736
79	ﾙｸｾﾝﾌﾞﾙｸﾞ(LU)	351,488
80	ﾎﾞﾘﾋﾞｱ(BO)	343,296
81	ｴﾙｻﾙﾊﾞﾄﾞﾙ(SV)	336,896
82	ﾎﾞｽﾆｱ・ﾍﾙﾂｪｺﾞﾋﾞﾅ(BA)	327,680
83	ｽﾘﾗﾝｶ(LK)	303,104
84	ﾅｲｼﾞｪﾘｱ(NG)	301,568
85	ﾘﾋﾞｱ(LY)	294,912
86	ｱﾙｼﾞｪﾘｱ(DZ)	266,240
87	ﾄﾞﾐﾆｶ共和国(DO)	265,984
88	ｸﾞｱﾃﾏﾗ(GT)	262,144
89	ﾖﾙﾀﾞﾝ(JO)	253,696
90	ｸﾞﾙｼﾞｱ(GE)	249,856
91	ﾄﾘﾆﾀﾞｰﾄﾞ・ﾄﾊﾞｺﾞ(TT)	242,432
92	ﾊﾟﾚｽﾁﾅ(PS)	241,664
93	ｹﾆｱ(KE)	214,016
94	ﾚﾊﾞﾉﾝ(LB)	205,056
95	ﾓｰﾘｼｬｽ(MU)	202,496
96	ｵﾗﾝﾀﾞ領ｱﾝﾃｨﾙ(AN)	200,704

順位	国・地域	割当数
97	ﾓﾙﾄﾞﾊﾞ(MD)	187,136
98	ﾌﾞﾙﾈｲ(BN)	174,592
99	ﾊﾞｰﾚｰﾝ(BH)	165,888
100	ｵﾏｰﾝ(OM)	163,840
101	ﾍﾞﾗﾙｰｼ(BY)	158,720
102	ﾏｶｵ(MO)	146,688
103	ｱｾﾞﾙﾊﾞｲｼﾞｬﾝ(AZ)	141,312
104	ｶﾞｰﾅ(GH)	129,536
105	ｳｽﾞﾍﾞｷｽﾀﾝ(UZ)	129,024
106	ｼﾘｱ(SY)	128,000
107	ﾆｶﾗｸﾞｱ(NI)	124,928
108	ｳｶﾞﾝﾀﾞ(UG)	116,224
109	ｱﾙﾊﾞﾆｱ(AL)	110,848
110	ｱﾙﾒﾆｱ(AM)	109,344
111	ｼﾞｬﾏｲｶ(JM)	105,472
112	ﾊﾞﾙﾊﾞﾄﾞｽ(BB)	103,168
113	ｷｭｰﾊﾞ(CU)	101,376
	ｷﾙｷﾞｽﾀﾝ(KG)	101,376
115	ﾓﾝｺﾞﾙ(MN)	100,608
116	ｶﾝﾎﾞｼﾞｱ(KH)	98,816
117	ｺｰﾄｼﾞﾎﾞｱｰﾙ(CI)	91,392
	ﾌｨｼﾞｰ(FJ)	91,392
119	ﾊﾟﾗｸﾞｱｲ(PY)	90,112
120	ﾈﾊﾟｰﾙ(NP)	88,576
121	米領ﾊﾞｰｼﾞﾝ等(VI)	82,944
122	ﾀﾝｻﾞﾆｱ(TZ)	82,432
123	ﾊﾞｰﾐｭｰﾀﾞ(BM)	79,360
124	ﾙﾜﾝﾀﾞ(RW)	77,824
125	ｸﾞｱﾑ(GU)	73,984
126	ﾎﾞﾂﾜﾅ(BW)	72,704
127	ｽｰﾀﾞﾝ(SD)	67,584
128	ｱﾌｶﾞﾆｽﾀﾝ(AF)	65,536
	ﾊﾞﾊﾏ(BS)	65,536
130	ﾓﾅｺ(MC)	64,832

順位	国・地域	割当数
131	ﾎﾝｼﾞｭﾗｽ(HN)	61,696
132	ﾘﾋﾃﾝｼｭﾀｲﾝ(LI)	55,328
133	ｶﾒﾙｰﾝ(CM)	53,760
134	ｾﾙﾋﾞｱ(RS)	53,504
135	ﾍﾞﾘｰｽﾞ(BZ)	49,664
136	ｼﾞﾌﾞﾗﾙﾀﾙ(GI)	47,104
137	ｱﾝｺﾞﾗ(AO)	46,336
138	ｾﾈｶﾞﾙ(SN)	43,264
139	ﾆｭｰｶﾚﾄﾞﾆｱ(NC)	43,008
140	ﾅﾐﾋﾞｱ(NA)	39,936
141	ﾌﾗﾝｽ領ﾎﾟﾘﾈｼｱ(PF)	39,424
142	ｱﾝﾃｨｸﾞｧ･ﾊﾞｰﾌﾞｰﾀﾞ(AG)	38,912
	ﾓｻﾞﾝﾋﾞｰｸ(MZ)	38,912
144	ﾊﾟﾌﾟｱﾆｭｰｷﾞﾆｱ(PG)	34,560
145	ﾌｪﾛｰ諸島(FO)	33,792
146	ｶﾞﾎﾞﾝ(GA)	33,280
	ｼﾞﾝﾊﾞﾌﾞｴ(ZW)	33,280
148	ﾊｲﾁ(HT)	32,768
	ﾚﾕﾆｵﾝ島(RE)	32,768
150	ｲﾗｸ(IQ)	30,720
151	ﾀｼﾞｷｽﾀﾝ(TJ)	28,672
152	ｱﾝﾄﾞﾗ(AD)	24,576
	ｲｴﾒﾝ(YE)	24,576
154	ﾗｵｽ(LA)	22,784
155	ﾌﾞｰﾀﾝ(BT)	22,528
156	ｽﾜｼﾞﾗﾝﾄﾞ(SZ)	21,248
157	ﾓﾙﾃﾞｨﾌﾞ(MV)	20,992
158	ﾏﾀﾞｶﾞｽｶﾙ(MG)	20,480
	ﾏﾘ(ML)	20,480
	ｻﾝﾏﾘﾉ(SM)	20,480
161	ｽﾘﾅﾑ(SR)	19,456
162	ｱﾙﾊﾞ(AW)	18,432
	ｼｴﾗﾚｵﾈ(SL)	18,432
164	ﾌﾞﾙｷﾅﾌｧｿ(BF)	17,152

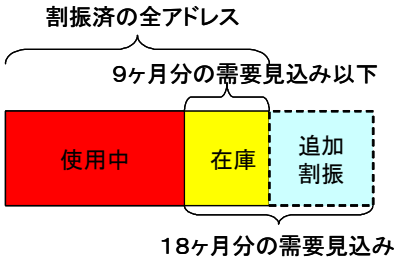
順位	国・地域	割当数
165	ｴﾁｵﾋﾟｱ(ET)	16,384
	ｸﾞﾘｰﾝﾗﾝﾄﾞ(GL)	16,384
	ｶﾞｲｱﾅ(GY)	16,384
	ﾓﾝﾃﾈｸﾞﾛ(ME)	16,384
169	ｻﾞﾝﾋﾞｱ(ZM)	13,568
170	ﾐｬﾝﾏｰ(MM)	12,288
	北ﾏﾘｱﾅﾃ諸島(MP)	12,288
	ｾｲｼｪﾙ(SC)	12,288
	ﾄｰｺﾞ(TG)	12,288
174	西ｻﾓｱ(WS)	11,520
175	ｶﾞﾝﾋﾞｱ(GM)	11,264
176	ｹｲﾏﾝ諸島(KY)	9,216
177	ﾏﾗｳｲ(MW)	8,704
	ｿﾛﾓﾝ諸島(SB)	8,704
179	ｸｯｸ諸島(CK)	8,192
	ﾓｰﾘﾀﾆｱ(MR)	8,192
	ﾅｳﾙ(NR)	8,192
	ﾂﾊﾞﾙ(TV)	8,192
	ﾊﾞﾁｶﾝ市国(VA)	8,192
184	ﾚｿﾄ(LS)	6,400
	ﾊﾞﾇｱﾂ(VU)	6,400
186	ﾍﾞﾅﾝ(BJ)	6,144
	ﾏﾝ島(IM)	6,144
188	ﾄﾝｶﾞ(TO)	4,352
189	ｱﾝｷﾞﾗ(AI)	4,096
	ｱﾒﾘｶﾝｻﾓｱ(AS)	4,096
	ｵｰﾗﾝﾄﾞ諸島(AX)	4,096
	ｶｰﾎﾞﾍﾞﾙﾃﾞ(CV)	4,096
	ｼﾞﾌﾞﾁ(DJ)	4,096
	ｴﾘﾄﾘｱ(ER)	4,096
	ｸﾞｱﾄﾞﾙｰﾌﾟ(GP)	4,096
	ﾊﾟﾗｵ(PW)	4,096
	ﾀｰｸｽ･ｶｲｺｽ諸島(TC)	4,096
	ﾄﾙｸﾒﾆｽﾀﾝ(TM)	4,096

順位	国・地域	割当数
199	中央ｱﾌﾘｶ共和国(CF)	3,072
	英領ｲﾝﾄﾞ洋地域(IO)	3,072
	ｷﾘﾊﾞｽ(KI)	3,072
	ｾﾝﾄｸﾘｽﾄﾌｧｰ・ﾈｲﾋﾞｽ(KN)	3,072
203	ｺﾝｺﾞ民主共和国(CD)	2,560
204	ﾌﾞﾙﾝｼﾞ(BI)	2,304
205	ﾐｸﾛﾈｼｱ(FM)	2,048
	ﾌﾗﾝｽ領ｷﾞｱﾅ(GF)	2,048
	ｶﾞｰﾝｼﾞｰ(GG)	2,048
	赤道ｷﾞﾆｱ(GQ)	2,048
	ｼﾞｬｰｼﾞｰ(JE)	2,048
	ﾏｰｼｬﾙ諸島(MH)	2,048
	ｾﾝﾄﾋﾞﾝｾﾝﾄ・ｸﾞﾚﾅﾃﾞｨｰﾝ(VC)	2,048
	ﾜﾘｽ・ﾌﾃｭﾅ諸島(WF)	2,048
213	ﾉｰﾌｫｰｸ島(NF)	1,280
214	ｺﾝｺﾞ(CG)	1,024
	ｷﾞﾆｱﾋﾞｻｳ(GW)	1,024
	ﾆｳｴ(NU)	1,024
	米領ﾊﾞｰｼﾞﾝ諸島(VG)	1,024
218	ｸﾞﾚﾅﾀﾞ(GD)	256
	ｾﾝﾄﾙｼｱ(LC)	256
	ﾓﾝﾄｾﾗﾄ(MS)	256

参考資料２：現在の IPv4 アドレス割り振りのルール

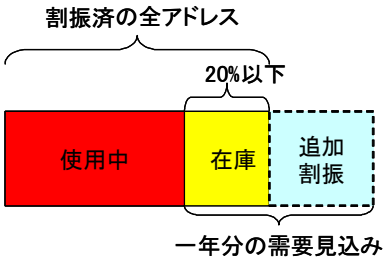
(1) ICANN(IANA)から地域管理団体(RIR ： APNIC 等)への割り振りは、
- RIR の在庫量が「９ヶ月分の需要見込み」を下回ったときに
- 「１８ヶ月分の需要見込み」分を満たすまでアドレスを割り振る

なお、割り振りは、/8(=IPv4 アドレス約 1600 万個)単位で行われる。



(2) RIR から国別管理団体(NIR: JPNIC 等)、または ISP などへの割り振りは、地域によって若干のルールの差はあるが、
- 既に割り振られたアドレスの８０%以上が効率的に利用されているときに
- 「１年分の需要見込み」分を満たすまでアドレスを割り振る

なお、割り振りは、/21(=IP アドレス 2048 個） 単位で行われる



(3) 日本の NIR である JPNIC は、割り振りの必要が生じる毎に、APNIC からアドレス割り振りを受けているので、国内在庫を有していないため、APNIC の在庫がなくなると、JPNIC は新規割り振りができなくなる

割振りルールを踏まえると、枯渇時期（わが国で IPv4 アドレスが不足する時期）の予測については、RIR 毎のアドレス在庫の予測を行い、それを積み上げたものと、IANA のアドレス残数とを照らし合わせることで行うことが適当。

参考資料3 IPv4アドレスの枯渇の影響

No.	対象	具体的な影響	二次的なインパクト	
			対象	影響
01-01	ASP／IDC系事業者	インターネット経由でのVPNサービスにはグローバルIPアドレスが必要なため、インターネットを経由したVPNサービスの新規提供は出来なくなる。 新規のVPNサービスの提供は、閉域網によるIP-VPNサービスのみという制限が生じる。	ユーザ 企業 大学	インターネットを介したVPNサービスを受けることが出来なくなる。この結果、特定事業者の回線に依存したIP-VPNの利用を余儀なくされ、導入コストが高くなる。
01-02		新規のホスティング等の提供が困難になる。バーチャルホスト等の利用もあり得るが、顧客毎にリソースを完全に分離したいという要求に応えることは出来なくなる。	ユーザ	新規では共用型のホスティングサービスしか受けること出来ず、セキュリティポリシーの調整が必要となったり、柔軟なリソース変更が困難になる等、フレキシブルなサイト運営に制限が生じる。
01-03		データセンター／ウェブホスティング事業については、バーチャルホスト等でサービス提供を続けることはできるが、負荷分散等のコストが今まで以上に必要となり、サービスを提供する際のコストが高くなる。		
01-04		セキュリティ確保のためのIPアドレスを用いたアクセス制御の実施は、グローバルアドレスを持たないユーザの増加により、その継続的実施が困難になる。別手段による認証・アクセス制御方法への移行を迫られ、実施形態に制限が生じる。		
01-05		VODサービスなどのグローバルIPアドレスを大量に使うような、新規サービスの開発、提供が出来なくなる。	企業 ユーザ	ASP/SaaS型のサービスが制約されるため、これらを活用した生産性改善や新事業創生の機会に制限が生じる。
02-01	ISP（既存）	動的アドレス割り当てのためのアドレスプールを増やすことが出来なくなり、アドレスの利用率が高まることで、接続時にアドレス取得できないケースが増加する。インターネット接続サービスの品質に制限が生じる。さらに、新規のサービス提供にも制限が生じる。	新規ユーザ	ISPへの加入が困難になる。
			ユーザ	動的アドレスサービスの利用ユーザにおいて、サービスの品質に制限が生じる。
02-02		グローバルIPアドレスを利用するサービス（固定アドレスサービス、IP電話のようなインターネットを介して機器をIPアドレスで同定するようなサービス等）の開発や提供が出来なくなる。	ユーザ	固定アドレスサービスの新規利用が出来なくなる。 その他、新規の便利なサービスの利用が出来なくなる。
02-03		グローバルアドレスを必要とするサービスの提供維持のためのグローバルアドレスとプライベートアドレスの再配置を含むネットワーク構成の再編や、アドレス不足から来るアドレス空間の細分化による経路情報の増加により、現在運用中のルータの処理能力を超える可能性がある。この場合、CPU・メモリのアップグレード、若しくは機種交換が必要となり、コストが高くなる。		
02-04		自社の提供網において、プライベートアドレスの利用ユーザとグローバルアドレスの利用ユーザが混在することによって、自社の提供するサーバやアプリケーションへのアクセス経路、認証等において工夫が必要となり、コストが高くなる。	ユーザ	プライベートアドレスしか提供されないユーザの場合、一部のインターネットアプリケーションの利用に制限が生じる。

参考資料3-2

02-05		ISPによって現在保持しているIPv4アドレスの余裕率に違いがあるため、当面の間サービス継続可能なところと、すみやかな対策が必要なところとに分かれる。ただし、対策を講じたとしても、場合によってはサービス内容に制限が生じる。	ユーザ	加入しているISPのサービス内容が変わる場合は、その対応や、場合によってはISPを変更する等しなければならなくなる。その結果、サービス品質に制限が生じたり、コストが高くなったりする。
02-06		ホールセール事業者の対応が必要となり、コストが高くなる。対応の時期や内容次第では、事業の継続そのものが困難になる。		
03-01	ISP(新規)	IPv4インターネットへの新たな接続を自ら提供することができないため、新規のISP事業の開始が困難である。上位ISPの取次ぎ程度しか出来ず、事業展開に制限が生じる。	ユーザ	新規参入によるISP間の競争が期待できないため、長期的にはコストが高くなる。
04-01	企業ネットワーク 大学ネットワーク	インターネットVPNの新規利用が出来なくなるため、既存の企業ネットワーク(大学ネットワーク)と新規拠点(支社、分校)の間のWAN接続ではインターネット経由の利用が出来なくなる。IP-VPNや専用線等での接続が必須となり、コストが高くなる。		
04-02		新設の企業、大学等において、グローバルアドレスがもらえないため、自営ネットワークを利用したサービス提供や活動に制限が生じる。研究開発型の組織においては、柔軟で十分な活動機会が得られないことで、成果をあげることが困難になる。		
05-01	SOHOネットワーク 家庭ネットワーク	通常はISPを経由して宅外のネットワークにつながるため、ISPのサービスに依存した部分が大きい。ISPのサービスの制約にともない、インターネットの利用に制限が生じる。		
06-01	エンドノード (非PC機器、センサー等)	センサーネットワーク等の実用、提供が困難になる。	ユーザ	リモートセンシング、遠隔制御等、今後登場すると期待される新規のネットワークサービスが提供されないまま、利用することが出来なくなる。
07-01	運用スタッフ	ISPのネットワークが複雑化する等により、運用負荷が高まり、労働条件の維持が困難になる。	ISP ユーザ	システムの運用コストが高くなる。さらにこのコストがサービス料金にも影響を与え、その提供や利用に係わるコストが高くなる。
08-01	SIer	ネットワーク利用システムにおいて、利用可能なネットワーク形態が制限され、提案の幅が限られるので、最適なソリューションを提供することが出来なくなる。	ユーザ 企業	ネットワーク利用システムにおいて、利用可能なソリューションに制限が生じる。
08-02		ASP/SaaS型サービスの優劣が、サービス内容よりもアドレスの提供力に依存するようになり、価格体系にゆがみが生じる。このため、シェアードサービスを利用するよりはクローズドなシステムによるソリューションを目指すようになり、ソリューションの提供形態に制限が生じ、コストが高くなる。	ユーザ 企業	プラットフォーム的なシェアードサービスの利用が困難となり、小規模企業では事業維持のオーバーヘッドが増大してコストが高くなる。
09-01	ベンダ	ネットワークを活用した新機能提供や機器保守等においてアドレス不足を前提とした新たな設計手法を開発する必要があり、その分コストが高くなる。	ユーザ 企業	新機能利用、機器保守等においてアドレス不足を想定した利用形態についても考慮した導入、運用・保守を行う必要があり、その分コストが高くなる。
09-02		アドレス変換、冗長化等の保守・運用手段に関して新たな技術開発が必要となり、その分コストが高くなる。		

09-03		アドレス不足回避技術の寿命見通しが不透明(IPv6等の導入により、いつ不要になるか予測困難)であるため、これらの技術の開発・採用リスクが大きく、経営の意思決定が困難になる。		
10-01	ユーザ	P2P接続を要するアプリケーションが使用できない、新規分野のサーバ系サービスが提供されない、仮に提供されても通信相手がそのサービスを利用出来ない等により、インターネットを介したコミュニケーション手段の一部が活用出来なくなる。	ユーザ 経済	インターネット上でのユーザ間の情報交流が制限されることにより、情報が充実していることによって保たれていたインターネットを利用した購買意欲が低下し、インターネット経済の拡大が困難になる。
10-02		技術的・コスト的負担がユーザにまで転嫁され、ユーザが負担するコストが高くなる。		
11-01	IP電話	グローバルIPアドレスを利用するインターネット電話の利用拡大が出来なくなる。インターネット電話にかかわるキャリア内ネットワーク構成が、プライベートアドレスの併用等により複雑化し、その維持運用のためコストが高くなる。	企業 ISP	プライベートアドレスを利用した対応可能性はあるが、中小企業等ではゲートウェイ設置の分コストが高くなる。ISP側でもセントレックス利用等の管理コスト増によりコストが高くなる。
11-02		インターネットTV会議システム等、相手にグローバルアドレスを要求するVoIPアプリケーションの利用拡大が出来なくなる。		
12-01	新規サービス事業	健康・医療・福祉・介護等をサポートするサービス、生産・施設・都市管理等のマネジメントサービス、セキュリティサービス、コンテンツ提供・ゲーム等の双方向サービス等、これまでインターネットを利用していなかったが、今後新しく利用しようとしている産業や地域が参入することが出来なくなる。	ユーザ	企業による新規インターネットサービスの提供を受けることが出来なくなる。
			マクロ経済	インターネット上の新規サービスが提供できなくなり、経済のインターネット経済への移転が進まなくなるため、拡大を続けるはずだったインターネット経済が、これ以上拡大することが出来なくなる。
12-02		車載ネットワークをはじめとするモビリティ要素が高い今後のネットワークサービスにおいても、想定されるサービス内容に制限が生じる。		
12-03		ホームネットワークにおいても、宅内の家電を外部からHGW経由で操作や監視を行うサービスの提供に制限が生じる。		
13-01	マクロ経済	インターネット利用サービスが頭打ちになることで、ICT利用による生産性向上を原動力とする潜在成長率に制限が生じる。	マクロ経済	インターネット経済の拡大の恩恵を最も受ける企業群においては、成長性への不安から、株価の維持が困難になる。
14-01	その他	IPv4アドレスを取引するブラックマーケットが出現した場合、アドレス利用の正当性を証明できずに、インターネット全体への到達性を確保出来ないアドレス領域が生じる可能性がある。IPv4インターネット全体の到達性や信頼性を維持することが困難になる。		
14-02		現在のインターネットの普及率が固定化され、地域格差が生じる。都市部では引き続きインターネットを利用できるが、地方ではインターネット利用の拡大が困難になる。		

参考資料4：
IPv4アドレス在庫の枯渇時期の予測について

● IPv4アドレス在庫の枯渇時期の予測

1．予測の前提

- 予測に当っては、不確定要素を排除するため、特段の事情変更がないまま、粛々とアドレス割り振りがなされていくことを前提とする。すなわち、下記の３点を前提条件とした上で予測を行う。

1. 国際的なアドレス割り振りのルール（次頁参照）が変化しないこと
2. 割り振りを受けたIPv4アドレスを維持するためのルールが変化しないこと
3. アドレス割り振りを受ける者が、恣意的に余剰アドレスの確保を図らないこと

- このため、下記のような事象は、今後のアドレス管理等にかかる国際的議論の結果として起こりうるものであるが、本予測ではこれら事象の影響は見込んでいない。
  - ➢ アドレス在庫の枯渇がより早まる事象
    - – IPv4アドレスの国際的在庫が一定数を下回ったときに、残数全てを各地域に平等に、若しくは特定地域に優先的に配布する
    - – IPv4アドレスの枯渇を見越し、恣意的に割り振り済みアドレスの無駄遣いを行うことで、「当面の必要量」を大きく見せるなど、必要以上のアドレス割り振りが要求される
  - ➢ アドレス在庫の枯渇が遅くなる事象
    - – アドレス保有単価が大幅に引き上げられる
    - – アドレス割り振りの際に、割り振るアドレス数が現在よりも少なくなる
    - – IPv4アドレスをアドレス保持者同士が相対で取引できるようになる

2. 枯渇時期予測手法

- 現在枯渇時期予測の手法としては、一般に下記の手法が用いられている。

1. IPアドレス割り振り、経路広告に関する実績値、及びIPv4アドレスプールに関するデータ等を利用
2. 直近の過去1200日の経路広告を元に、Fitting modelを決定
3. 直近の過去1200日の割り振り実績データを元に、Fitting modelにあわせた推計式を導出
4. 導出した式を元に、今後のアドレス消費量を予測

参考資料4－3

本予測は、アドレスの需要は「今までと同様か、更に伸びる方向にある」という検討結果を踏まえ、

① 上記手法をそのまま利用することで「直近の傾向のままアドレス消費が伸びつづける」場合に相当し、また国際的にも一般的な予測として用いられているGeoff Huston氏（APNICのChief Scientist）のモデル（Geoffモデル）

② アドレスの需要は「今までと同様か、さらに伸びる方向にある」という検討結果のうち、最もアドレスの消費速度が遅い「需要が一定」の場合に相当する線形モデル（モデレートモデル）

の2つの方法を用いて、IPv4アドレス在庫の枯渇時期を予測するものである。

※なお、本予測にて用いている過去の実績データは、2007年9月30日（日）現在のものである

3. Geoffモデルによる予測（1）

（http://www.potaroo.net/tools/ipv4/index.html）

(1) 経路広告されたアドレス空間数の一次微分からFitting modelを絞り込み

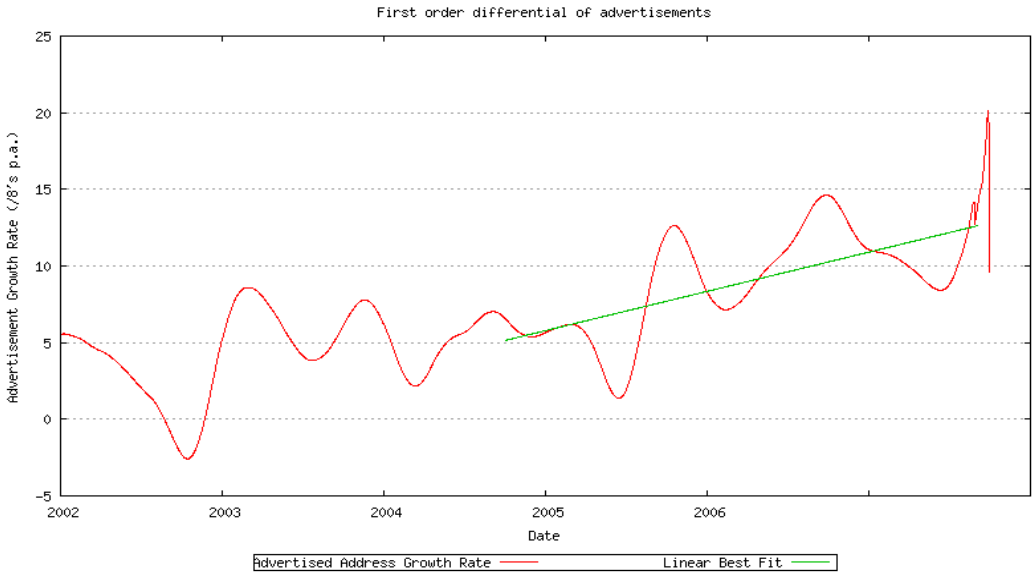
→ 実利用アドレスの増加数が増していることから、Fitting modelとして一次関数（新規需要一定）を排除

(2) さらに各RIRの割り振りブロック数の一次微分からFitting modelを決定

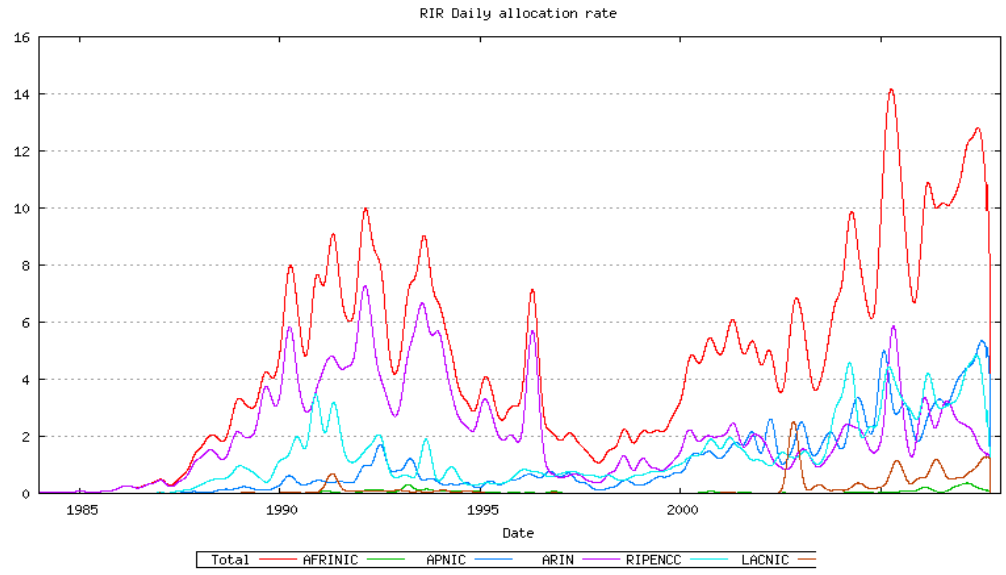
各年の伸びが一定ではない → 上記による一次関数排除の正当性を支持
増加数の伸びが著しい → n次関数よりも指数関数が適していることを示唆

→ 指数関数モデルを採用

参考資料4－4



経路広告されたアドレススペースの増加の一次微分



各RIRの割り振りブロック数の一次微分

3. Geoffモデルによる予測（2）

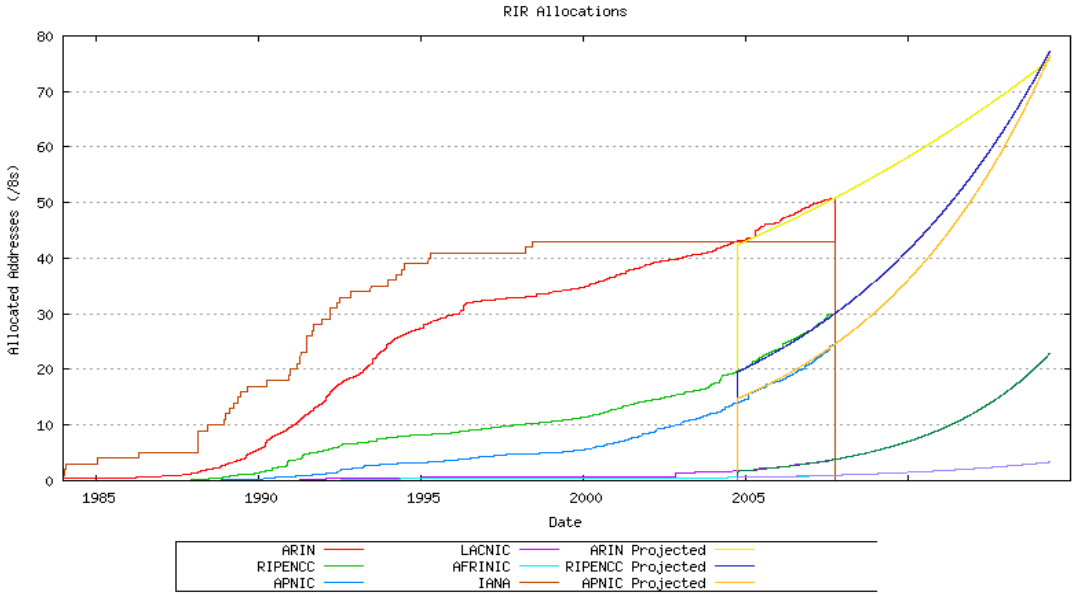
(3) RIRによるアドレス割り振りの予測

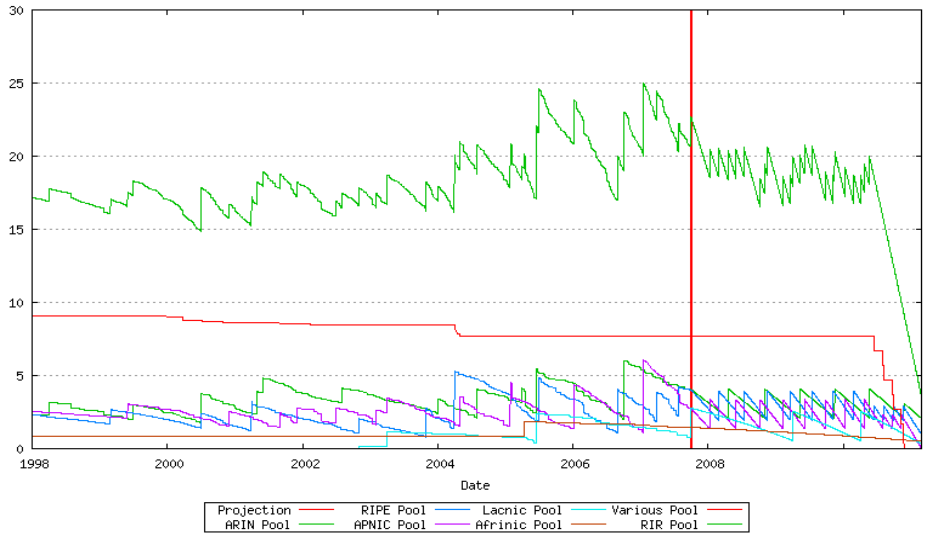
指数関数モデルにより各RIRのアドレス割り振りの実績及び過去1200日のデータとのfittingにより予測したデータを左下のグラフに示す。

(4) RIRにおける在庫アドレスの挙動の予測

上記を踏まえ、アドレス割り振りルールを元に各RIRの在庫アドレスの挙動の予測し、あわせて全RIRの在庫アドレス数を合算したものを、右下のグラフに示す。

参考資料4－5



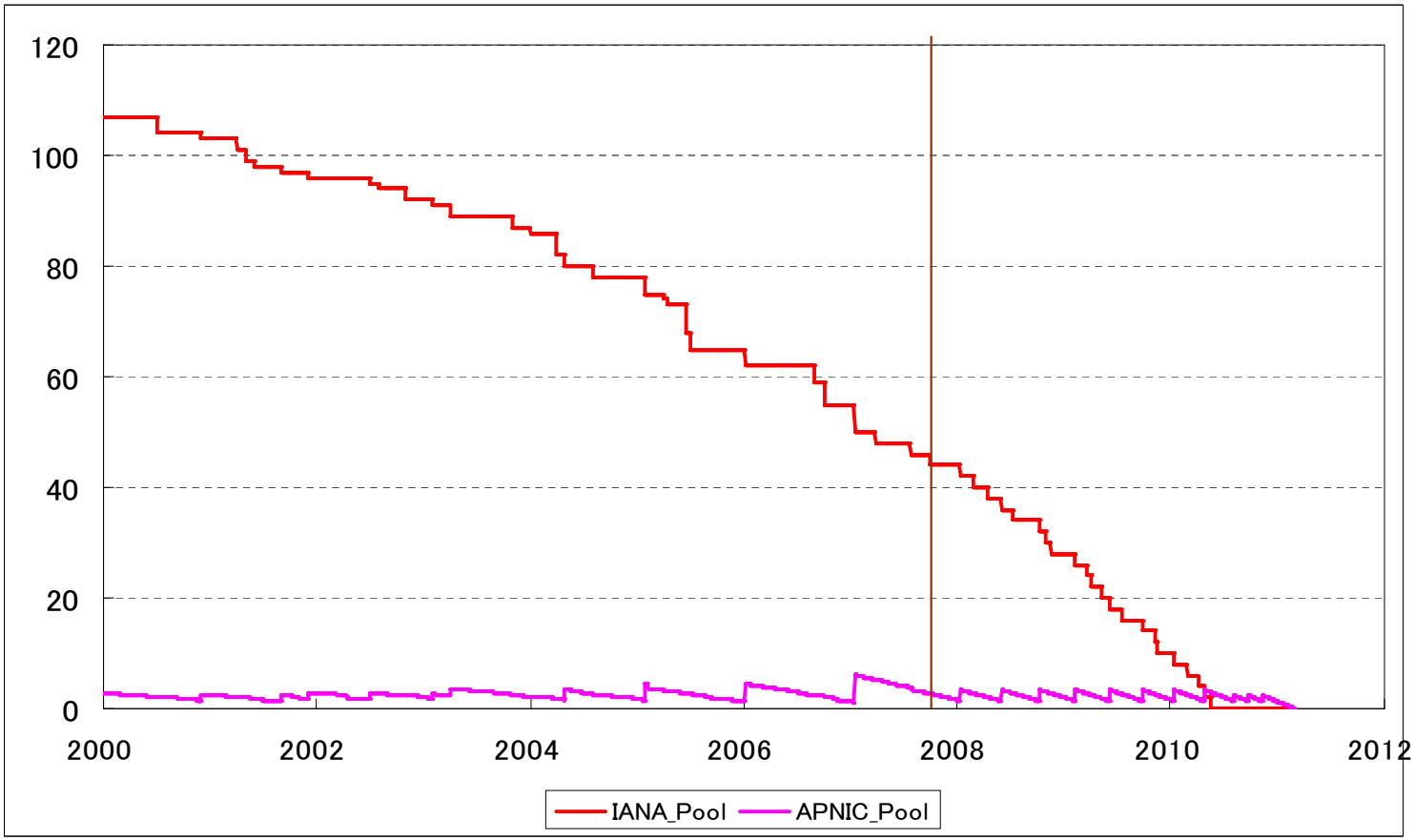


3. Geoffモデルによる予測（3）

(5) IANA残存ブロックの予測

- (4)の全RIRの在庫アドレス数の変動を、IANAの在庫アドレス状況に反映させたものを、IPv4アドレスの国際的在庫残（IANA Pool）の予測とする。
- これより、IANAにおける在庫アドレスは、2010年6月頃にゼロになると予想される。
- 同様に、APNICにおける在庫アドレスも、2011年3月末頃にゼロになると予想される。

参考資料4－6



4. モデレートモデルによる予測（1）

(1) 線形推計モデルによる予測

- 各RIRごとに、直近の過去1200日のIPアドレス割り振りに関する実績データから、回帰分析により推計式を導出
- 導出した式を元に、今後のアドレス消費量を予測

参考資料4－7

(2) 各RIR毎の推計式

- AFRINIC　　y ＝ 0.130109 x － 260.296
- APNIC　　y ＝ 3.238200 x － 6477.77
- ARIN　　y ＝ 2.762047 x － 5494.11
- RIPE　　y ＝ 3.433282 x － 6863.29　　（x ＝ 西暦年）
- LACNIC　　y ＝ 0.661448 x － 1324.38　　（y ＝ /8の個数）

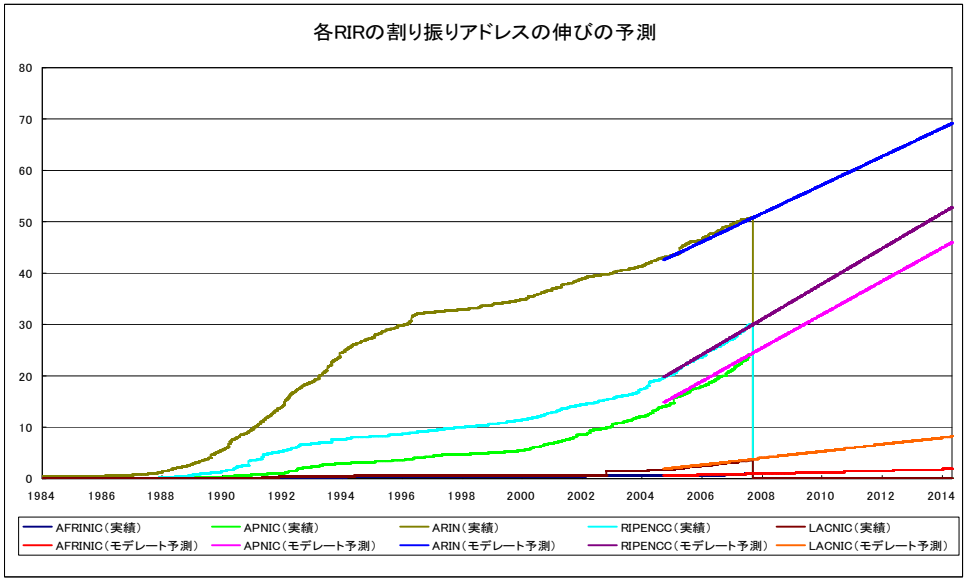
4. モデレートモデルによる予測（2）

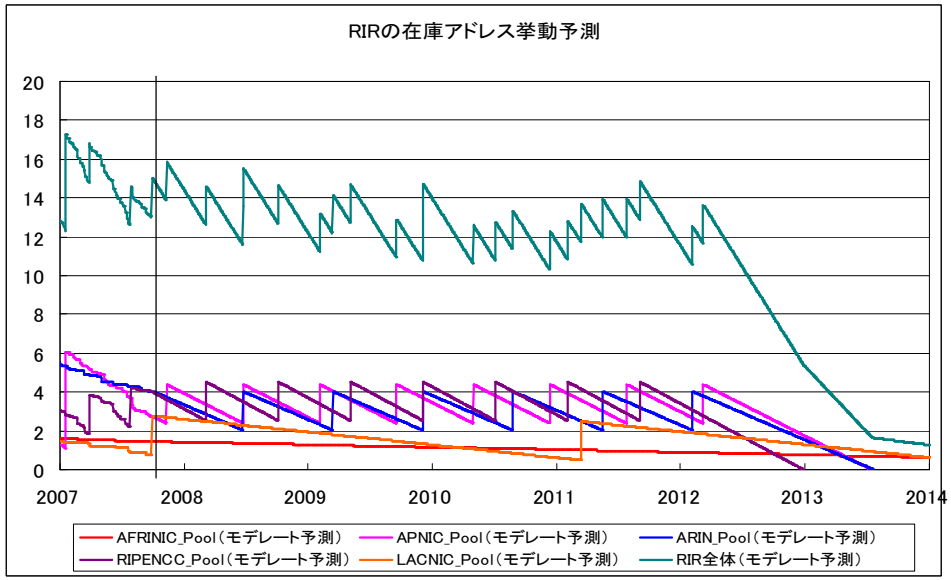
(3) 各RIRの割り振りアドレスの伸びの予測

各RIRへの割り振りアドレスの実績及び(2)の推計式により予測したデータを左下のグラフに示す。

(4) RIRにおける在庫アドレスの挙動の予測

上記を踏まえ、アドレス割り振りルールを元に各RIRの在庫アドレスの挙動の予測し、あわせて全RIRの在庫アドレス数を合算したものを、右下のグラフに示す。



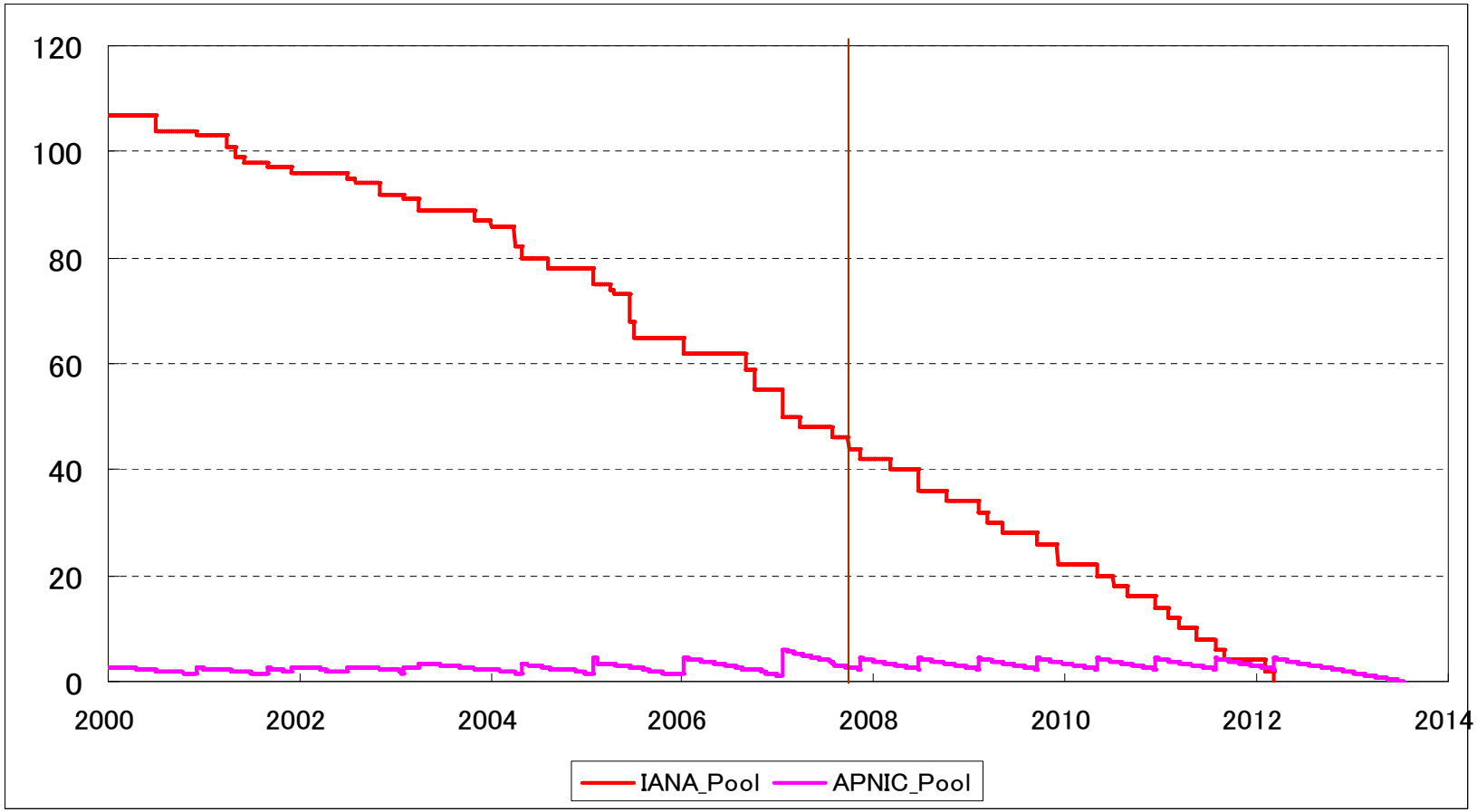


4. モデレートモデルによる予測（3）

(5) IANA残存ブロックの予測

- (4)の全RIRの在庫アドレス数の変動を、IANAの在庫アドレス状況に反映させたものを、IPv4アドレスの国際的在庫残（IANA Pool）の予測とする。
- これより、IANAにおける在庫アドレスは、2012年2月頃にゼロになると予想される。
- 同様に、APNICにおける在庫アドレスも、2013年7月頃にゼロになると予想される。

参考資料4－9



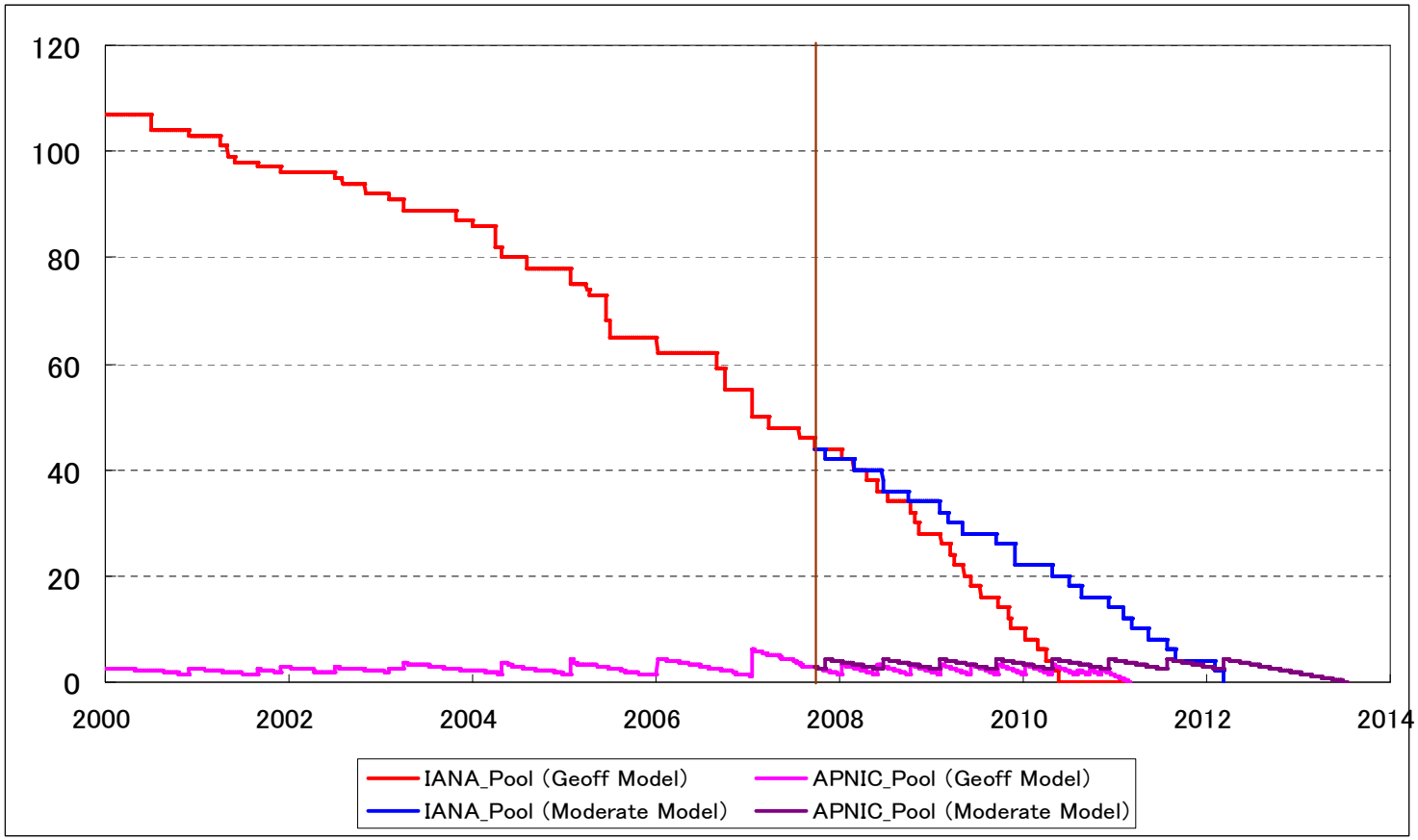
5. IPv4アドレス在庫の枯渇時期

- これらより、特段の事情変更がない場合、即ち、国際的なアドレス割り振りやアドレス維持に係るルールに変化がなく、またアドレス割り振りを受ける者も恣意的に余剰アドレスの確保を図らないとした場合には、

> **・国際的在庫（IANA Pool）の枯渇は、2010年半ば～2012年初頭**
> **・日本国内で利用するアドレスの補充が不可能となるのは、2011年初頭～2013年半ば**

と予測される。

参考資料4－10



参考資料　５：IPv6 インターネット接続サービスの提供状況

（株式会社　三菱総合研究所「ＩＰｖ６接続サービスの提供状況に関する調査の結果の概要（平成 20 年３月）」（総務省からの受託調査報告書概要版）より抜粋）

総務省では、株式会社三菱総合研究所へ調査研究の請負を行い、同社が事務局を務める IPv6 普及・高度化推進協議会のチャネルを通じて、昨年度に引き続き、IPv6 接続サービスの提供状況について調査を行いました。この調査では、主要な商用 IPv6 接続サービスについて Web による検索調査を行うとともに、主要なインターネットサービスプロバイダー（以下「ISP」）約 190 社を対象としたアンケート調査を実施しました。

1. 商用 IPv6 接続サービスの状況

大手主要 ISP に関して Web 上でのサービスメニューの確認を行い、さらにインターネット上の検索エンジンを利用して、主要な商用 IPv6 接続サービスについて検索を行った結果が以下の表となります。

このように、全国レベルのプロバイダにおいては、個人、法人ともに、IPv6 接続サービスが利用可能となっています。なお、前回調査に比べて数が増えていますが、これは前回調査で発見できなかったサービス（下表の下線を付加したサービス）の追加であり、この１年で新規にサービスをはじめた事業者ではありません。ただし、この１年でサービス提供の開始を発表した ISP が 2 社ありますので、欄外に記載いたします。

会社名	個人向けサービス	法人向けサービス
㈱インターネットイニシアティブ	IPv6 トンネリングサービス（フレッツ、ADSL 利用）	IPv6 インターネット接続（トンネル接続（ADSL、B フレッツ/フレッツ光プレミアム）、IPv6 デュアルスタック接続(専用線））
(株)NTT-ME		IPv6 インターネット接続（専用線、トンネル接続・デュアルスタック接続・ネイティブ接続）
NTT コミュニケーションズ㈱	IPv6 インターネット接続（トンネル接続、ADSL・光接続・ISDN・専用線・無線 LAN、PHS 又はダイヤルアップを用いた IPv6 インターネット接続、情報家電利用等）	IPv6 インターネット接続（トンネル接続、ADSL・光接続・ISDN・専用線・ハウジング）、<u>マルチポリシーVPN サービス</u>
KDDI(株)		IPv6 インターネット接続（トンネル接続）
西日本電信電話株式会社	IPv6 閉域網（光ファイバを用いた、映像マルチキャスト､テレビ電話､VOD 等）	IPv6 VPN（光ファイバを用いた、テレビ電話、マルチキャスト通信、コンビニ情報端末へのデータ配信等）
ニフティ㈱	IPv6 インターネット接続（ADSL 利用）	
東日本電信電話株式会社	IPv6 閉域網（光ファイバを用いた、映像マルチキャスト､テレビ電話､VOD 等）	IPv6 VPN（光ファイバを用いた、テレビ電話、マルチキャスト通信、コンビニ情報端末へのデータ配信等）
フリービット㈱	FB Feel6 接続サービス(トンネル接続)	
三菱電機情報ネットワーク㈱		<u>インターネット接続サービス（(トンネル接続)、専用線（IPv6 ネイティブ接続)）</u>
メディアエクスチェンジ㈱		<u>インターネット接続サービス(イーサネットタイプ)</u>

※　Web 検索では、検索キーワード「ＩＰｖ６」、「接続」、「サービス」による結果をもとにしている

（参考）今後、IPv6 接続サービスを提供することを発表している企業

- (株)エネルギアコミュニケーションズ：

  法人向け IPv4/IPv6 デュアルスタックサービス

  開始予定：2008 年 4 月

- (株)電算

  法人/個人向け、データセンタ内接続（IPv6 ネイティブ、IPv4/IPv6 デュアル）フレッツ固定 IP 接続(トンネル接続)

  開始予定：2008 年 4 月

2. ISP へのアンケート調査結果

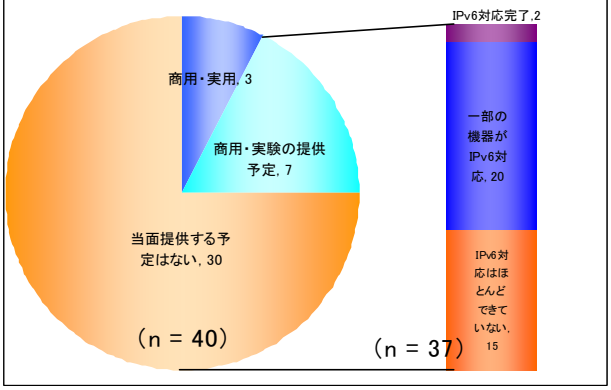
複数都道府県にわたるエリアをカバーしてサービスを提供している主要なインターネットサービスプロバイダー（以下「ISP」）約 190 社を対象に、IPv6 接続サービス（VPN サービスを含む）の提供状況、準備状況、検討状況、IPv6 接続サービスのターゲット、IPv6 接続サービス提供のための課題等について、Web アンケート調査を行いました。その結果、40 社（3 月 12 日現在）より回答を得ましたので、その分析結果を下記にご紹介します。

（１）IPv6 接続サービスの提供実態と予定

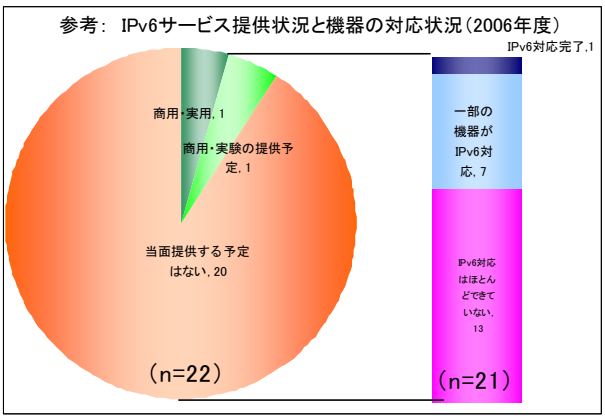
～徐々に IPv6 対応を進めつつ、IPv6 サービスの提供に向けた計画策定を開始しつつある～

回答を得た ISP のうち、商用または実験での IPv6 接続サービスを行っている ISP は 3 社と少ないですが、商用あるいは実験での IPv6 接続サービスを予定している ISP は 7 社と、大きく増えています。依然として 3/4 の ISP については具体的な IPv6 接続サービス提供時期について未定という状況にあるものの、昨年よりも多くの企業が少なくとも計画段階に入っており、そのうち 6 社は 2008～2010 年の商用サービスの提供を予定しているなど、IPv4 在庫アドレスの枯渇の対策として IPv6 対応が進み始めていることが伺われます。なお、今回は VPN による接続サービスの提供状況についても調査を行いました。現在、IPv6 接続サービスを提供している 3 社はいずれも VPN サービスを提供しておらず、IPv6 提供予定の 7 社では 2 社が IPv6 での VPN サービスの提供を予定していましたが、通常のデュアルスタックサービス等とあわせての提供を想定していると

図1： IPv6サービス提供状況と機器の対応状況（2007年度）



参考： IPv6サービス提供状況と機器の対応状況（2006年度）



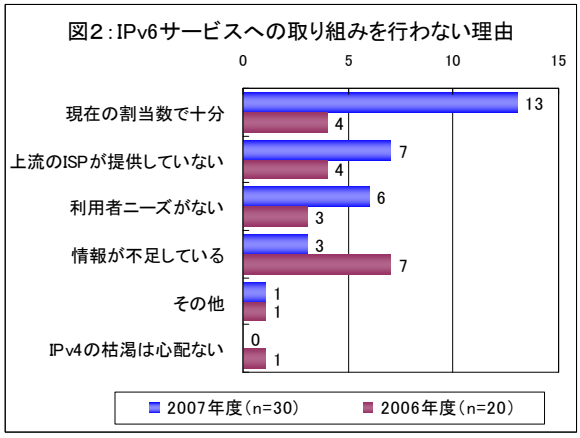
いう状況であり、まずはインターネット接続を考えている事業者が多いことがわかりました。

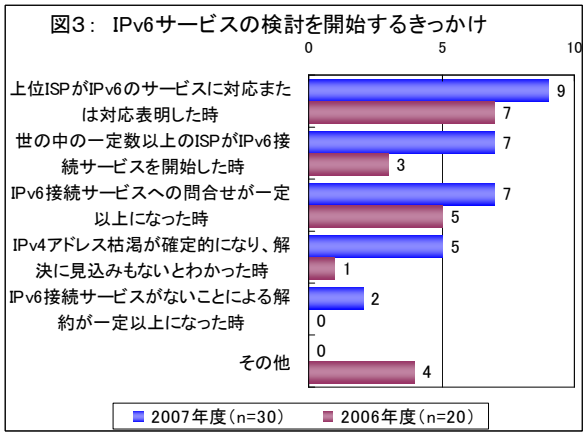
また、商用あるいは実験でのサービスを行っていない 37 社のうち半数以上の 22 社、提供時期が未定という 30 社だけでみても、半数以上の 16 社について、自社設備について何らかの IPv6 対応が進められているとの回答がありました。

これは IPv6 サービスの提供を計画していなくとも、機器の更新などのタイミングに IPv6 対応のものを導入した、あるいは最新機種を購入したところ IPv6 にも対応していた等の事由によって徐々に IPv6 対応が進みつつあることが考えられます。

なお、依然として IPv6 接続サービスに踏み切らない理由としては、現在の IPv4 アドレスの割当数で当面の事業に支障はきたさないという理由が最も多く、また、IPv6 接続サービスを提供するきっかけとなる理由として、上位 ISP が IPv6 に対応するか、世の中の一定数以上の ISP が IPv6 接続サービスを開始するという理由をあわせると半数以上（16 社）に達していることから、対応を検討していない ISP の多くは現時点では様子を見ていると推察されます。

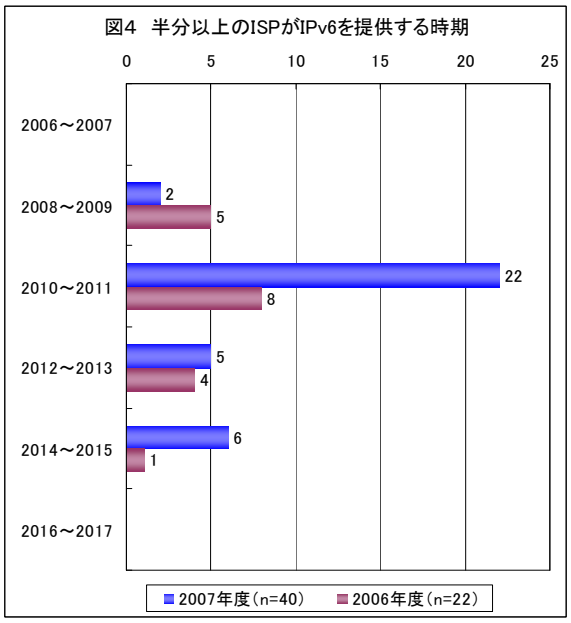
また、IPv6 サービスに取り組まない理由として、情報が不足しているという回答が昨年に比べて大きく減少しており、2007 年度に行われた、IPv4 アドレスの在庫枯渇等に関する情報提供活動によって、多くの ISP が IPv6 化の必要性についての情報を入手していることが伺えます。





IPv6 接続サービス提供時期の想定としては、「半分以上の ISP が IPv6 を提供する時期」について、2010～2011 年という回答が 22 社と最も多く、半数以上になります。多くの事業者がこの時期までに対応すると設定しているのは昨年と変わっておらず、この時期が ISP の IPv6 対応のピークと想定されます。

これは、「インターネットの円滑な IPv6 移行に関する調査研究会」で公表した資料に記載した IPv4 アドレス枯渇想定時期ともリンクするタイミングであり、現在具体的な予定を想定していない ISP についても、2010 年から 2011 年頃を目処に IPv6 接続サービスへの対応を考えていることが予測されます。

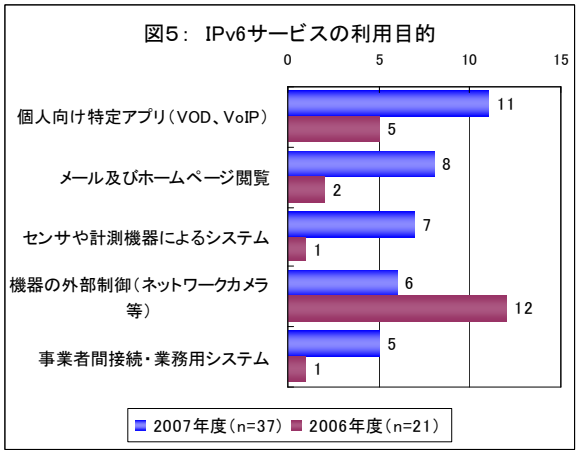


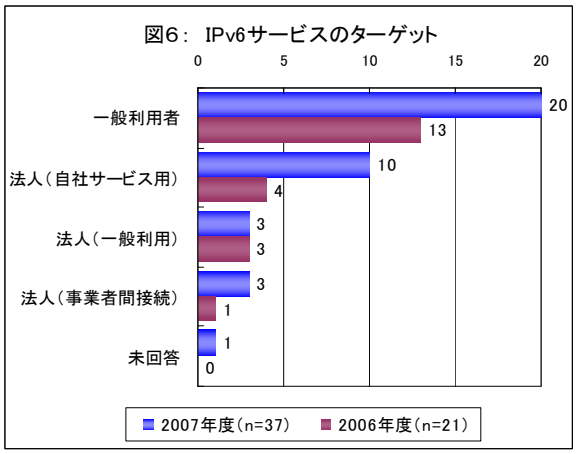
（２）サービス概要と利用状況

～利用者嗜好はつかめず、きっかけ待ちであるが IPv4 とは異なる利用が期待されている～

回答を得た ISP のなかで IPv6 接続サービスを提供していたのは 3 社であり、IPv6 接続サービスの利用実態や利用者の傾向についてはアンケートから想定できる状況とはいえません。なお、その 3 社のケースで想定される IPv6 の利用動機は、「メール及びホームページ閲覧」を 2 社、「端末や機器の外部制御での利用（ネットワークカメラ等）」を 1 社が挙げている状況であり、IPv4 の置き換えという面が強い状況です。

これに対し、現在提供していない事業者（37 社）の意見を見ると、「メール及びホームページ閲覧」だけでなく、「個人向けの特定アプリ（VOD、VoIP）」やセンサネットワーク等の、IPv6 ならではの使い方への期待が伺えます。なお、昨年度と比べると、「端末や機器の外部制御での利用」が減少し、「個人向け特定アプリ」が伸びていますが、これは、2008 年 3 月以降 NTT 東日本の「FLET'S 光」加入者が映像配信サービスを標準で受けられるようになるという報道や、同じく 2008 年 3 月の NGN の開始に併せて地上波デジタルテレビ放送の IPv6 マルチキャストによる IP 再送信が行われるようになるという報道等の影響によることが想定されます。なお、「個人向けの特定アプリ（VOD、VoIP）」を選んでいる事業者は、11 社全てが想定ターゲットとして「一般利用者」を考えており、映像配信サービスが一般利用者向けのキラーアプリとして期待されていることが伺えます。これに対して、法人をターゲットとしてあげている事業者（16 社）については、「センサや計測機器等を大量に接続したシステムでの利用」（6 社）や、「メール及びホームページ閲覧」（5 社）、「事業者間接続・業務用システムでの利用」（4 社）等、多様な選択をしており、まだメリットとしてどの部分に着目するかが定まっていないように見受けられます。



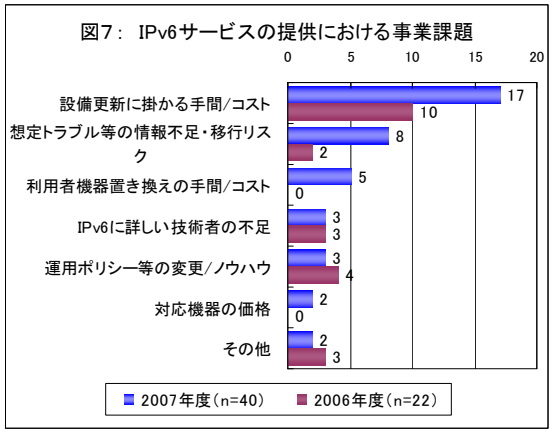


また、IPv6 接続サービスのターゲットとしては、現在の IPv4 サービスと同様に一般利用者へのサービスが期待として挙げられています。

しかし今回 IPv6 接続サービスを提供していると答えた 3 社は、全て法人顧客をターゲットとしたサービスを展開しており、一般利用者向けのサービスを実際に提供するには、まだ課題があることが伺えます。

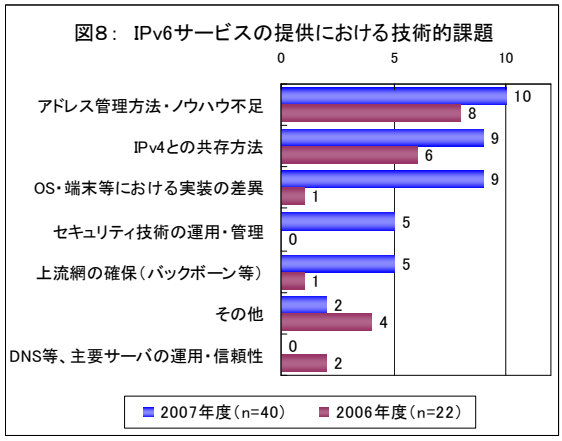
（３）その他

～IPv6 接続サービス対応の促進に向け、技術サポートを含めた情報提供等の普及促進が必要～



今後の IPv6 接続サービスの普及に向け、ISP が考えている課題についての回答をみると、昨年度と同様、事業的な課題としては設備更新のコストと手間が圧倒的で、次いで想定されるトラブルの情報やノウハウの不足が挙げられています。特に設備更新のコストについては、当初の機器更新計画から逸脱した早期更新はなかなかむずかしく、ある程度の余裕を持った IPv6 への対応期間が必要になることはやむを得ないと考えられます。

一方、技術的課題についても、昨年度と同様アドレス管理ノウハウ、IPv4 との共存方法があげられていますが、それに加えて、「OS 等における実装の差異」が昨年度よりもかなり増加しています。いずれも運用に絡んだノウハウや経験、情報の不足といえますが、前述の通り IPv6 化の必要性の周知が進んできたことと併せて考えると、IPv6 化が必要であるということについての情報は周知されてきているものの、いざ実装を行おうとすると不明な情報が多いという、情報不足という壁にぶつかっている事業者が多いことが想定されます。このような状況が、現在の様子見状態を招いているものとも考えられます。



以上、実装上の差異についての情報や、移行の際のテクニック、完全移行に至るまでの運用ノウハウ等を対象とした情報の発信と共有に基づく普及促進活動の継続が必要と考えられます。

以上

参考資料６：
IPv4アドレス在庫枯渇に対する３つの対応方策に対する評価結果

参考６－１

NAT/NAPTの利用

	肯定的意見	否定的意見
利用スタイル	①　外部からのアクセスに制限が生じるため、セキュリティ対策の一部として機能する。	①　Private IP Addressのみを払い出された利用者間の通信が困難になる 【理由】NAT/NAPTのLAN内にあるノードをWAN側から特定することが困難なため。ただし、Global IP Addressをもつサーバに中継させることによって、ある程度解決可能である。 ②　アドレス変換実施に伴う通信速度低下 【理由】NAT/NAPTではアドレス変換用の情報を管理する必要があるが、大規模な運用をした場合、当該情報が膨大になり、アドレス変換に要する時間が増大する。 ③　アドレス情報埋め込み型の通信について個別に対処が必要となる 【理由】SIP、IPsec等のアドレス情報が埋め込まれた、あるいはGWで変更困難なプロトコルに対しては、NAT/NAPTを超えた通信のためには個別のALGが必要となる。しかしながら、全ての通信アプリケーションについて対応することは実質不可能である。 ④　アドレスの重複が起きる 【理由】NAT/NAPT内に配置されたノード間の通信の際に、複数のノードが同一のPrivate IP Addressを利用している可能性があり、通信アプリケーションによっては、通信が不能となる怖れがある。 ⑤　悪い意味で匿名性が向上する 【理由】NAT/NAPTのログ保存コストは非常に高いため、短期間で破棄せざるを得ない。そのため同一Global IP Addressを共有している利用者のうち、悪意の行為を行った利用者を特定する事が困難となる。

ネットワーク構成	①　現在の機器をそのまま利用できる 【理由】現在と同様にIPv4アドレスを利用するため、NAT/NAPT用設備の追加もしくは設定変更で対応可能である。	⑥　IPアドレスのリナンバリングが必要になる 【理由】NAT/NAPTの導入に伴いアドレス体系を変更する必要が生ずる。 ⑦　Private IPv4 Addressの拡張の検討が必要である 【理由】大規模にNAT/NAPTを利用することを考慮すると、Private IPv4 Addressを増加させることを予め検討しておくことが望まれる。
運用	②　技術的な蓄積がある 【理由】NAT/NAPTは現時点で広く使われている技術であるため。	⑧　大規模ネットワークをNAT/NAPTを用いた場合の運用可能性が不明 【理由】現在はCATVや企業内での利用等の比較的小規模ネットワークでの利用が殆どであり、大規模ネットワークでの運用経験が薄い。このため、どの程度の大規模集約化が可能であるか不明であると共に、ノウハウ構築が必要な可能性がある。 ⑨　多段NATについては、運用可能性が不明である 【理由】現在、多段NATを利用した大規模ネットワークの運用経験が薄いため、実現性が不明である。 ⑩　アドレス節約ができる者と、できない者とが存在する 【理由】Webサイトなど、広く一般からのアクセスを求める者には利用できないが、それらの者が別の部門等でNAT/NAPTを利用できない。その一方で、インターネット接続事業者などはNAT/NAPTの利用により、多量のGlobal IPv4 Addressの余剰を生み出すことが出来る可能性がある。 ⑪　特許問題への注意が必要である。 【理由】NAT/NAPTは、個別通信アプリケーションに対するALGと組み合わせて利用する必要が生じることから、技術のつぎはぎの結果、予想外の特許に抵触する可能性がある。

コスト	③　プロトコルを変更するコストがかからない 【理由】今までと同様にIPv4アドレスで運用するため。	⑫　事業者の投資負担が大きくなる 【理由】一定数の配下ユーザ毎に装置を設置する必要がある。また、集約が進むにつれコストが増加するため、最終的に必要なコストを見積もる事が困難。

参考６－２

割り振り済みのIPv4アドレスの再配分

	肯定的意見	否定的意見
利用スタイル		
ネット構成	①　現在の機器をそのまま利用できる 【理由】今までと同様にIPv4アドレスで運用するため。	①　正当なアドレス利用者を知らしめる仕組みの構築が必要 【理由】通信中継の判断の正当性を担保するため、アドレス利用者が誰であるか担保し続けるための仕組みを新たに構築する事が必要。
運用	②　アドレス割り振りポリシの変更に伴い、利用可能なアドレスが増加する可能性がある。	②　アドレス需要への対応力が低い 【理由】現在の全世界における新規アドレス需要はアドレス全体の5%にも達しており、直近の需要を満たすことも困難。特に余剰アドレスの返還に際しては相当なシステム回収コストが必要と見込まれるため、相当に強力なのインセンティブ若しくは強制力が必要。 ③　アドレス割り振りポリシの変更に係る合意形成時期が不明 ④　アドレスがいつかは無くなる 【理由】現在の全世界における新規アドレス需要はアドレス全体の5%にも達しており、配分を効率化してもいつかはアドレスが無くなる。 ⑤　ルーティング経路のマネージメントが困難になる 【理由】アドレスが細分化され、かつ、地域に関係なく割り当てられるようになると、経路情報のマネージメントが困難になる。

コスト	③　プロトコルを変更するコストがかからない 【理由】今までと同様にIPv4アドレスで運用するため。	⑥　ルーティング経路のマネージメントが困難になる 【理由】アドレスが細分化され、かつ、地域に関係なく割り当てられるようになると、経路情報のマネージメントが困難となり、全てのネットワーク運用者にとってコスト増となる。

参考６－３

IPv6への移行

	肯定的意見	否定的意見
利用スタイル	①　IPアドレスを潤沢に利用することが可能になる 【理由】IPv6アドレスは2の128乗個という膨大な数があるため。 ②　End　to　Endで運用することを前提とした機器/アプリケーションが利用しやすくなる	①　IPv6に対応していない機器/アプリケーションがある 【理由】特に古い機器やアプリケーションなどでは、IPv4にのみしか対応していないものが多くある。また、IPv6化が行われている機器でも、基本機能は実装されているが、冗長化などの実環境ネットワークで必要な機能が実装されていないことが多い。 ②　IPv6の実装がまだ枯れておらず、安定していない.
ネット構成	④　IPv6導入の際に、現在の利用方法に適した効率的で使いやすいネットワークを作成できる 【理由】IPv4のネットワークは旧来のものにつぎはぎで作り続けてきたネットワークであるが、新技術への移行にあわせて、現在の利用方法に適したものを作成することができるため。 ⑤　ネットワーク設計(アドレス設計)が容易になる 【理由】IPv6アドレスは潤沢に存在するため。 ⑥　より大規模なネットワーク利用への発展が容易になる 【理由】アドレス管理やルーティング管理がシンプル化されるため。	③　ネットワークの再デザインが必要になる。 【理由】ネットワーク機器にIPv6機能を追加することによって増加する負荷に見合ったサイジングをする必要がある。 ④　サーバ側には引き続きIPv4が必須という課題がある 【理由】クライアント側にIPv4が存在する限り、サーバ側はｸﾞﾛｰﾊﾞﾙIPv4が引き続き必要となる。
運用	⑦　ネットワーク管理が容易になる 【理由】IPv6 ネットワークはアドレスを潤沢に利用し、機能を活かした管理しやすいネットワークとして構築することが可能であるため。	⑤　IPv4 ネットワークと IPv6 ネットワークを並行して運用する期間が存在する 【理由】IPv4 アドレスが瞬時に IPv6 アドレスに切り替わるとは想定できず、数年から数十年の移行期間が発生すると考えられる。それまでの期間、ISP 等は、IPv4/IPv6 デュアルスタックのネットワークを運用するか、もしくは、IPv4 ネットワークと IPv6 ネットワークを接続するためのトランスレータ等

		を運用するかを考える必要がある。IPv4/IPv6 デュアルスタックネットワークを運用する場合は、設計･構築･試験の稼動が(倍にはならなくても)多くかかる。 ⑥　利用者への影響が最も大きくなるので、事業者側の対応が必要 【理由】利用者の対応負担に応じて、サービスを提供する事業者側の対応も必要になるが、現状では事業者側で IPv6 対応するコストの回収が見込めないため、IPv6 対応が進まないことが起こり得る。 ⑦　IPv6 導入の方法を考える必要がある 【内容】既存の IPv4 ネットワークを積極的に排除しつつ IPv6 へ移行するのか、あるいは細々とリファインしつつ共存させていき、やがてはニーズがなくなった時点で終焉させるのかを考える必要がある。 ⑧　技術的な蓄積が薄く、技術者の数も少ない 【理由】IPv6 の運用はまだ広く行われているとはいえないため、運用経験が十分蓄積されていない。また、IPv4/IPv6 ネットワークの設計や構築は可能でも、障害切り分けができる運用管理エンジニアが殆どいない。そのため、技術者の教育等が必要になる。 ⑨　ユーザサポートに手間がかかる 【理由】ユーザには IPv4 を使用しているという認識は無い。そのため、IPv6 に変わることの説明及び変わった後の技術的なサポートを実施する必要がある。 ⑩　運用面、セキュリティ面での対応に時間がかかる

		【理由】IP トランスポートそのものよりも、ネットワークセキュリティの考え方や保守・運用面で IPv4 との差違が大きくなると考えられるものがあり、その周知徹底や環境構築に時間がかかる。 ⑪　サービス差が出ないように配慮する必要がある 【理由】経営的には、IPv6 接続ユーザが受けられるサービスと IPv4 接続ユーザが受けられるサービスについて、差が出ないようにする必要がある。
コスト		⑫　ネットワーク機器の値段がIPv4に比して高価 【理由】IPv6対応機器は、IPv4にも対応しているため、IPv6対応機器のコストはIPv4のみに対応した機器よりも高い。 ⑬　移行費用が多大である 【理由】機器やアプリケーションのIPv6仕様への対応度により、機材等の新規導入/改修費用、機器導入にかかるチェック費用などが移行費用としてかかる。

参考資料７：
IPv4アドレス在庫枯渇への対応に向けた課題の整理表

参考資料7－1：インターネットのIPv6化に伴う課題

区分 a 特段の課題なし
b 製品はあるが、運用能力が無い／運用経験が足りない
c 製品はあるが、運用ツールが足りない
d 技術はあるが、製品がない
e 技術がない

注：上記の製品の有無については、構成員が現実的に知りうる範囲での有無による
また、自社製作を含め、汎用品以外を使っている可能性が高いものについては、「製品」を「もの」に、「ない」を「改造が必要」に読み替える。

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
コンシューマー・ユーザ	機器	PC	a/b	・OSを始めとして最新のソフトウェアであれば可能 例：WindowsであればVista以上が必要(WindowsXPではIPv6ではDNSやファイル共有が不能) ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い
		ネットワーク家電	a/d	・DLNAを始めとして、現状ではIPv4のみ対応の機器が多数 ・出荷後のアップデートが困難なものもあり、IPv4が必須であり続ける可能性有り	a/d	・現状でIPv6対応の機器は稀有 ・冗長化時のステート同期に不安（安定性を欠く恐れ） ・映像などについてパフォーマンスが確保できない怖れ	a/d	・現状でIPv6対応の機器は稀有 ・冗長化時のステート同期に不安（安定性を欠く恐れ） ・映像などについてパフォーマンスが確保できない怖れ
		ゲーム機など特殊なportを使う蓋然性が高い機器	a/d	・現状ではIPv4のみ対応の機器が多数 ・出荷後のアップデートが困難なものもあり、IPv4が必須であり続ける可能性有り	a/d	・現状でIPv6対応の機器は稀有 ・冗長化時のステート同期に不安（安定性を欠く恐れ） ・通信のリアルタイム性が確保できない怖れ	a/d	・現状でIPv6対応の機器は稀有 ・冗長化時のステート同期に不安（安定性を欠く恐れ） ・通信のリアルタイム性が確保できない怖れ

		フィールド	IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
コンシューマー・ユーザ	機器	CPE	a/b/c/d	・求められる機能がネットワークアーキテクチャ依存。 ・DSLモデムを始めとして、現時点ではIPv6未対応かつ開発計画もない製品も存在 ・IPv6経由でのリモート監視機能の開発が必要 ・現状機器では、IPv6については、パススルーのみ対応のものが殆どであり、IPv6のルーティングができず、IPv6対応機器の管理が困難 ・IPv4と比較してIPv6はスループットが劣る ・実効上ファイアウォールとしても機能しているNATが無くなる ・現状機器では、セキュリティに関連する機能（パケットフィルタ、SPI、IDS、ファイアウォール）が劣る ・家庭内の古いIPv4のみ対応機器をIPv6対応可する機能が必要となる可能性あり				
	アプリケーション	メール	a/b	・最新のソフトウェアであれば一般に可能 例：Thunderbird, Becky!, Winbiffなど ・DNSに依存する問題ではあるが、フォールバックのおそれ有り	a/b		a/b	
		Web閲覧	a/b	・最新のソフトウェアであれば一般に可能 例：Internet Explore, Firefox, Operaなど ・DNSに依存する問題ではあるが、	a/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/d	・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		VoIP	a/b/d	・製品に依存 ・IPv4/v6それぞれに対応したDNSがネットワークにより提供されることが必要	a/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/d	・サービス側が個別アプリケーションごとのトランスレータを用意することが必要

	フィールド		IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
コンシューマー・ユーザ	アプリケーション	ストリーミング	a/d	・製品に依存 ・IPv4/v6それぞれに対応したDNSがネットワークにより提供されることが必要	a/d		a/d	・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		ダイナミックDNS	d					
		P2Pアプリケーション	a/d	・アプリケーション依存	a/d	・アプリケーション依存 ・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		NTP	a		a	・通信のリアルタイム性が確保できない怖れ	a	・通信のリアルタイム性が確保できない怖れ
		パーソナルファイアウォール	a	・最新のソフトウェアであれば一般に可能				
中規模ユーザ	機器	PC	a/b	・OSを始めとして最新のソフトウェアであれば可能 例：WindowsであればVista以上が必要(WindowsXPではIPv6ではDNSやファイル共有が不能) ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・リモートメンテナンスツールが不足	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い
		サーバー類	a/b/d	・OSを始めとして最新のソフトウェアであれば可能 例：Windows Serverであれば2008以上が必要 ・ソフトウェアのアップグレードが必要なケース多 ・ミドルウェア類などについては、改修が必要な可能性大 ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・リモートメンテナンスツールが不足	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い

		フィールド	IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
中規模ユーザ	機器	ルータ／スイッチ	a/b/c	・IPv6経由での管理機能の開発が必要 ・リモートメンテナンスツールが不足 ・既利用機器はIPv6未対応製品であること多。買い替えが必要となる可能性大 ・対応製品であっても、安定性低下の可能性あり。特に古い機器の場合、処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・サーバ収容ルータ／スイッチの冗長構成に難があるもの有り(ALAXALA, NEC, Nokiaは実装済) ・IPv6はアドレス長が長いため、セキュリティに関連する機能(パケット				
		ファイアウォール	b/c	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・IPv6拡張ヘッダに対する制御に問題がある可能性あり（RFC4942） ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
中規模ユーザ	機器	IDS／IPS	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明
		アンチウイルスゲートウェイ	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・DNS-based Blackhole ListがIPv6に対応していないものあり ・冗長化時のステート同期などが困難	d	・アドレスベースのポリシを正当に記載可能か不明	d	・アドレスベースのポリシを正当に記載可能か不明
		プロクシサーバ	b/c/d	・Proxy単体での製品は存在。 ・Web ServerにProxy機能を持つものも存在。 例：apache, IIS2003 ・アプライアンス組み込み型のプロクシサーバは、未対応のものが多い ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・きめ細かいフィルタリング条件の設	b/c/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	b/c/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合
			区分	備考	区分	備考	区分	備考
中規模ユーザ	機器	VPN機器	a/b	・運用ノウハウの再構築が必要	a/b	・正常に動作しないおそれ有り ・SSL VPNは可能。 ・IPsec VPNは、自動鍵を利用する場合は（鍵交換でトラヒックセレクタを折衝するので）不可能だが、手動鍵であれば可能。	a/b	・正常に動作しないおそれ有り ・SSL VPNは可能。 ・IPsec VPNは、自動鍵を利用する場合は（鍵交換でトラヒックセレクタを折衝するので）不可能だが、手動鍵であれば可能。
		オフィス機器	b	・対応製品が少ない	b		b	
	アプリケーション	メール（含むコンテンツDNS）	a/b	・最新のソフトウェアであれば一般に可能 例：sendmail,bind ・DNSツリー全体がIPv4、IPv6に両対応している必要有 ・運用ノウハウの再構築が必要 ・IPv4/v6それぞれに対応したDNSが必要 ・DNSが、通信相手にフォールバックを起こすおそれ有り	a/b		a/b	
		Web閲覧	a/b/d	・最新のソフトウェアであれば一般に可能 例：IE,Firefox,Opera ・運用ノウハウの再構築が必要 ・IPv4/v6それぞれに対応したDNSが必要	a/b	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/b	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		VoIP	a/b/d	・運用ノウハウの再構築が必要 ・IPv4/v6それぞれに対応したDNSが必要	a/b	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/b	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意すること
		DHCP	a/b/c/d	・最新のソフトウェアであれば一般に可能 例：Windows-Vista,ISC-DHCP,WIDE-DHCPv6,Dibbler ・但し、フルスペックに対応したものは無い ・運用ノウハウの再構築が必要				

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
中規模ユーザ	アプリケーション	認証	a/b/d	・RADIUSは対応製品有り 例：fullflex RADIUS ・Active Directory認証が未対応 ・検疫ネットワークやL2スイッチによるフィルタが機能しない可能性有り ・運用ノウハウの再構築が必要	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り ・man-in-the-middle問題が発生する怖れ有	a/b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要 ・man-in-the-middle問題が発生する怖れ有
		DB	b/d	・最新のDBMSであれば一般に可能 例：DB2, PostgreSQL,IBM DB2（Oracleは未サポート） ・DBMSが対応していたとしても、DBそのものの個別改修が必要な可能性も大。 ・DBフロントのみのv6化は可能 ・運用ノウハウの再構築が必要	b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		NTP	a	例：ntpd	a	・通信のリアルタイム性が確保できない怖れ	a	・通信のリアルタイム性が確保できない怖れ
大規模ユーザ	機器	PC	a/b	・OSを始めとして最新のソフトウェアであれば可能 例：WindowsであればVista以上が必要(WindowsXPではIPv6ではDNSやファイル共有が不能) ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・リモートメンテナンスツールが不足	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い
		サーバー類	a/b/d	・OSを始めとして最新のソフトウェアであれば可能 例：Windows Serverであれば2008以上が必要 ・ソフトウェアのアップグレードが必要なケース多 ・ミドルウェア類などについては、改修が必要な可能性大 ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・リモートメンテナンスツールが不足	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い

		フィールド	IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
大規模ユーザ	機器	ルータ／スイッチ	a/b/c	・IPv6経由での管理機能の開発が必要 ・リモートメンテナンスツールが不足 ・既利用機器はIPv6未対応製品であること多。買い替えが必要となる可能性大 ・対応製品であっても、安定性低下の可能性あり。特に古い機器の場合、処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・サーバ収容ルータ／スイッチの冗長構成に難があるもの有り(ALAXALA, NEC, Nokiaは実装済) ・IPv6はアドレス長が長いため、セキュリティに関連する機能(パケット				
		ファイアウォール	b/c	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・IPv6拡張ヘッダに対する制御に問題がある可能性あり（RFC4942） ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
大規模ユーザ	機器	IDS／IPS	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明
		アンチウイルスゲートウェイ	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・DNS-based Blackhole ListがIPv6に対応していないものあり ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	d	・アドレスベースのポリシを正当に記載可能か不明	d	・アドレスベースのポリシを正当に記載可能か不明

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
大規模ユーザ	機器	プロクシサーバ	b/c/d	・Proxy単体での製品は存在。 ・Web ServerにProxy機能を持つものも存在。 例：apache, IIS2003 ・アプライアンス組み込み型のプロクシサーバは、未対応のものが多い ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は大きく落ちる恐れ有り ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv4と比較してIPv6はスケールしない可能性有り				
		帯域制御装置	b/c/d	・製品は存在するが専用製品は稀有 例：専用製品としてはPureFlow。その他ルータに機能実装している例は多い。				
		VPN機器	a/b/d	・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる恐れ有り ・マルチキャスト対応はIPv4のみのこと多し	a/b	・正常に動作しないおそれ有り ・SSL VPNは可能。 ・IPsec VPNは、自動鍵を利用する場合は（鍵交換でトラヒックセレクタを折衝するので）不可能だが、手動鍵であれば可能。	a/b	・正常に動作しないおそれ有り ・SSL VPNは可能。 ・IPsec VPNは、自動鍵を利用する場合は（鍵交換でトラヒックセレクタを折衝するので）不可能だが、手動鍵であれば可能。
		オフィス機器	b	・対応製品が少ない	b		b	

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
大規模ユーザ	アプリケーション	メール（含むコンテンツDNS）	a/b	・最新のソフトウェアであれば一般に可能 例：sendmail,bind ・DNSツリー全体がIPv6に対応している必要有 ・IPv4/v6それぞれに対応したDNSが必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・きめ細かいフィルタリング条件の設定ができない可能性有 ・DNSが、通信相手にフォールバックを起こすおそれ有り ・運用ノウハウの再構築が必要	a/b		a/b	
		Web閲覧	a/b	・最新のソフトウェアであれば一般に可能 例：IE,Firefox,Opera ・運用ノウハウの再構築が必要 ・IPv4/v6それぞれに対応したDNSが必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・宛先アドレスに応じてproxyを変更する設定ができない可能性有り	a/b	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/b	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		VoIP	a/b/d	・IPv4/v6それぞれに対応したDNSが必要 ・コール・エージェントの再構築が必要 ・処理能力がIPv4と比較してIPv6は	a/b	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/b	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
大規模ユーザ	アプリケーション	DHCP	a/b/c/d	・最新のソフトウェアであれば一般に可能 例：Windows-Vista,ISC-DHCP,WIDE-DHCPv6,Dibbler ・但し、フルスペックに対応したものは無い ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り				
		認証	a/b/d	・Active Directory認証が未対応 ・RADIUSは対応製品有り。 例：fullflex RADIUS ・ただし、RADIUSとして求められるパラメータについて、一部標準化議論中の部分が残っている ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・検疫ネットワークやL2スイッチによるフィルタが機能しない可能性有り	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り ・man-in-the-middle問題が発生する怖れ有	a/b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要 ・man-in-the-middle問題が発生する怖れ有
		DB	b/d	・最新のDBMSであれば一般に可能 ・DBMSが対応していたとしても、DBそのものの個別改修が必要な可能性も大。 ・DBフロントのみのv6化は比較的容易 ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は	b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
		業務系アプリケーション	d	・改修が必要な可能性大	d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意すること
		NTP	a		a	・通信のリアルタイム性が確保できない怖れ	a	・通信のリアルタイム性が確保できない怖れ

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
ネットワーク（インターネット）	機器	ルータ／スイッチ	a/b	・運用経験が不足していることが多いが、学術系や一部ISPは既に運用中 ・IPv6関連機能のバグや脆弱性が枯れておらず、緊急アップデート等の運用稼働が増加する可能性あり。 ・運用ノウハウの再構築が必要 ・旧型機器は買い替えが必要 ・リモートメンテナンスツールが不足 ・安定性低下の可能性 ・古い機器、中小規模向けの場合、処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・サーバ収容ルータ／スイッチの冗長構成に難があるもの有り(ALAXALA, NEC, Nokiaは実装済) ・IPv6はアドレス長が長いため、セキュリティに関連する機能(パケットフィルタ、SPI、IPsecなど)についてきめ細かい設定が困難な可能性有。				
		収容装置	a/d	・アーキテクチャ依存 ・非対応製品の設備更改が必要 ・CATV業界ではケーブルラボ認定(DOCSIS3.0)製品が必要				
		サーバー類	a/b/d	・運用経験が不足していることが多い ・運用ノウハウの再構築が必要 ・非対応製品の設備更改が必要 ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い
		監視装置	d	・製品の機能が不足 ・非対応製品の設備更改が必要 ・IPv6経由での監視機能の開発が必				

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
ネットワーク（インターネット）	アプリケーション	キャッシュDNS	b/c	・最新のソフトウェアであれば一般に可能 ・運用経験が不足していることが多い ・運用ノウハウの再構築が必要 ・DNSツリー全体がIPv6に対応している必要有 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・DNSが、通信相手にフォールバックを起こすおそれ有り	b		b	
		メンテナンス／運用ツール	c/d	・IPv6経由での監視機能の開発が必要 ・レポート機能等に制限有り（フロー				
		認証	c/d	・対応製品有り。 例：fullflex RADIUS ・ただし、RADIUSとして求められるパラメータについて、一部標準化議論中の部分が残っている ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り ・man-in-the-middle問題が発生する怖れ有	a/b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要 ・man-in-the-middle問題が発生する怖れ有
		DHCP	b/c/d	・最新のソフトウェアであれば一般に可能 例：Windows-Vista,ISC-DHCP,WIDE-DHCPv6,Dibbler ・但し、フルスペックに対応したものは無い ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り				
		アクセス解析	b/c/d/e	・DNS逆引きベースのアクセス解析はほぼ不可能 ・データベースに基づくアクセス解析は技術的には可能				

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
サービス提供者	機器	ルータ／スイッチ	a/b	・運用経験が不足していることが多いが、学術系や一部ISPは既に運用中 ・IPv6関連機能のバグや脆弱性が枯れておらず、緊急アップデート等の運用稼働が増加する可能性あり。 ・運用ノウハウの再構築が必要 ・旧型機器は買い替えが必要 ・リモートメンテナンスツールが不足 ・安定性低下の可能性 ・古い機器、中小規模向けの場合、処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・サーバ収容ルータ／スイッチの冗長構成に難があるもの有り(ALAXALA, NEC, Nokiaは実装済) ・IPv6はアドレス長が長いため、セキュリティに関連する機能(パケットフィルタ、SPI、IPsecなど)についてきめ細かい設定が困難な可能性有。				
		サーバー類	a/b/d	・OSを始めとして最新のソフトウェアであれば可能 例：Windows Serverであれば2008以上が必要 ・サーバー内に収容するミドルウェア／コンテンツについては個別検証が必要。 ・運用経験が不足していることが多い ・運用ノウハウの再構築が必要 ・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い ・リモートメンテナンスツールが不足	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い	a/b/d	・v4、v6混在環境下での適切な通信方法選択の仕組みが弱い

	フィールド	IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
		区分	備考	区分	備考	区分	備考
サービス提供者	機器						
	ロードバランサ	b/d	・製品は存在するが稀有 例：BIG-IP ・IPv6経由での管理機能の開発が必要 ・運用ノウハウの再構築が必要 ・リモートメンテナンスツールが不足 ・処理能力がIPv4と比較してIPv6は				
	ファイアウォール	b/c	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・IPv6拡張ヘッダに対する制御に問題がある可能性あり（RFC4942） ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明
	IDS／IPS	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかを始めとして、対応レベルも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	b	・アドレスベースのポリシを正当に記載可能か不明	b	・アドレスベースのポリシを正当に記載可能か不明

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
サービス提供者	機器	アンチウイルスゲートウェイ	b/c/d	・対応製品が少ない ・製品によっては、アドレスによるポリシルールをIPv6環境下でも作れるのかも不明 ・きめ細かいフィルタリング条件の設定ができない可能性有り ・IPv6経由での管理機能の開発が必要 ・DNS-based Blackhole ListがIPv6に対応していないものあり ・冗長化時のステート同期などが困難 ・処理能力がIPv4と比較してIPv6は	d	・アドレスベースのポリシを正当に記載可能か不明	d	・アドレスベースのポリシを正当に記載可能か不明
		トランスレータ（NAT-PT）（レイヤ4以下でIPv4⇔IPv6の相互変換をする装置）			d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り		
		トランスレータ(ALG)（レイヤ5以上を参照してIPv4⇔IPv6の相互変換をする装					d/e	・個別アプリケーションごとのトランスレータを用意することが必要

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
サービス提供者	アプリケーション	コンテンツDNS	a/b	・最新のソフトウェアであれば一般に可能 例：bind ・運用経験が不足していることが多い ・運用ノウハウの再構築が必要 ・DNSツリー全体がIPv6に対応している必要有 ・レジストラの登録用webがIPv6に対応する事が必要 ・ドメインのNSサーバに対してAAAAレコードを登録するインタフェースが用意されているドメイン登録事業者が少ない ・処理能力がIPv4と比較してIPv6は	a/b		a/b	
		メール（含むコンテンツDNS）	a/b	・最新のソフトウェアであれば一般に可能 例：sendmail ・運用ノウハウの再構築が必要 ・迷惑メールなどのアクセス制御ができない ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・IPv4/v6それぞれに対応したDNSが必要 ・DNSが、通信相手にフォールバックを起こすおそれ有り	a/b		a/b	
		認証	a/b/d	・対応製品有り。 例：fullflex RADIUS ・ただし、RADIUSとして求められるパラメータについて、一部標準化議論中の部分が残っている ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り ・man-in-the-middle問題が発生する怖れ有	a/b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要 ・man-in-the-middle問題が発生する怖れ有

フィールド		IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
		区分	備考	区分	備考	区分	備考
サービス提供者	アプリケーション html／ファイル	a/b	・最新のサーバーソフトウェアであれば一般に可能 例：IIS,apache ・サーバーソフトウェアが対応していたとしても、コンテンツそのものの個別改修が必要な可能性も大 ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・コンテンツ配信の対象地域を利用者のIPアドレスを元に限定することができない可能性あり	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	a/b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
	DB	b/d	・最新のDBMSであれば一般に可能 ・DBMSが対応していたとしても、DBそのものの個別改修が必要な可能性も大。 ・運用ノウハウの再構築が必要 ・本当にIPv6化が必要か検討が必要（バックエンドであれば、そのままIPv4のみ対応のままで利用可能な可能性） ・処理能力がIPv4と比較してIPv6は	b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	b/d	・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要
	アプリケーションサーバー	b	・最新のサーバーソフトウェアであれば一般に可能 ・サーバーソフトウェアが対応していたとしても、アプリケーションそのものの個別改修が必要な可能性も大 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	b	・開発が必要 ・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り	b	・開発が必要 ・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意することが必要

フィールド			IPv4とIPv6の双方が利用可能な環境で、IPv4、IPv6それぞれの通信を実現させる場合（IPv4、IPv6間の通信なし）		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（IPv4=IPv6変換）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合		IPv4とIPv6の双方が利用可能な環境で、トランスレータ（ALG）がサービスとして提供されている際に、IPv4=IPv6間の通信を実現させる場合	
			区分	備考	区分	備考	区分	備考
サービス提供者	アプリケーション	ストリーミング	a/b/d	・製品に依存 ・運用経験が不足していることが多い ・運用ノウハウの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り ・コンテンツ配信の対象地域を利用者のIPアドレスを元に限定することができない可能性あり	a/b/d	・トランスレータでは対応できないコンテンツ（ペイロード部にアドレスを含むものなど）が多数存在するおそれ有り ・冗長化時のステート同期に不安（安定性を欠く恐れ） ・映像などについてパフォーマンスが確保できない怖れ	a/b/d	・冗長化時のステート同期に不安（安定性を欠く恐れ） ・映像などについてパフォーマンスが確保できない怖れ
		VoIP	b/d	・運用ノウハウの再構築が必要 ・コール・エージェントの再構築が必要 ・処理能力がIPv4と比較してIPv6は大きく落ちる怖れ有り	b/d	・コール・エージェントの再構築が必要 ・トランスレータでは対応できない通信アプリケーション（ペイロード部にアドレスを含むものなど）が多数存在す	b/d	・コール・エージェントの再構築が必要 ・アプリケーション依存 ・サービス側が個別アプリケーションごとのトランスレータを用意すること
		NTP	a	例：ntpd, セイコープレシジョンタイムサーバ	a	・通信のリアルタイム性が確保できない怖れ	a	・通信のリアルタイム性が確保できない怖れ

参考資料7－2：ネットワーク内へのNAT導入に伴う課題

区分 a 可能
b 製品はあるが、運用能力が無い／運用経験が足りない
c 製品はあるが、運用ツールが足りない
d 技術はあるが、製品がない
e 技術がない

注：上記の製品の有無については、構成員が現実的に知りうる範囲での有無による
また、自社製作を含め、汎用品以外を使っている可能性が高いものについては、「製品」を「もの」に、「ない」を「改造が必要」に読み替える。

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
コンシューマー・ユーザ	機器	PC	a	・アプリケーション依存	a/b	・アプリケーションに依存
		ネットワーク家電	a/b	・DDNSやポートフォワーディングの利用やCPEを介して制御等となるため、機能が限定される ・レイヤ4以上でIPアドレスを使用する場合は不可	a/b/c/d/e	・DDNSやポートフォワーディングの利用やCPEを介して制御等となるため、片方がGlobal IPアドレスを持つ場合以上に機能が限定される ・レイヤ4以上でIPアドレスを使用する場合は不可
		ゲーム機など特殊なportを使う蓋然性が高い機器	a/b	・DDNSやポートフォワーディングの利用やCPEを介して制御等となるため、機能が限定される ・レイヤ4以上でIPアドレスを使用する場合は不可	a/b/c/d/e	・DDNSやポートフォワーディングの利用やCPEを介して制御等となるため、片方がGlobal IPアドレスを持つ場合以上に機能が限定される ・レイヤ4以上でIPアドレスを使用する場合は不可
		CPE	a/b	・ホールセール事業者において、ISPからエンドユーザへのプライベートアドレス割当ができることが必要	a/b/c/d/e	・プロトコルやアーキテクチャに依存 ・ホールセール事業者において、ISPからエンドユーザへのプライベートアドレス割当ができることが必要
	アプリケーション	メール	a/b		a/b	・メールサーバーがGlobal IPアドレスを持っているのであれば、特段の問題は生じない ・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
		Web閲覧	a/b	・レイヤ4以上でIPアドレスを使用する場合は不可	a/b	・レイヤ4以上でIPアドレスを使用する場合は不可 ・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
		VoIP	a/b/c	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存	a/b/c	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存 ・サービスの安定性低下が危惧される

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
コンシューマー・ユーザ	アプリケーション	ストリーミング	a/b		a/b	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。 ・サービスの安定性と転送性能面での低下が危惧される
		ダイナミックDNS	a/d		a/d	
		P2Pアプリケーション	a/b		a/b	・アプリケーション依存
		NTP	a/b		a/b	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
		パーソナルファイアウォー	a/b		a/b	
中規模ユーザ	機器	PC	a		a/b	・アプリケーションに依存
		サーバー類	a		a/b/c	・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		ルータ／スイッチ	a		a/b/c	・NAT機能を提供する製品について、機能やスケールに起因する置き換えが必要となる可能性もある
		ファイアウォール	a		a/b/c	・運用の見直しが必要である可能性がある
		IDS／IPS	a		a/b/c	・運用の見直しが必要である可能性がある
		アンチウイルスゲートウェ	a		a/b/c	・運用の見直しが必要である可能性がある
		プロクシサーバ	a		a/b/c	・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		VPN機器	a/d/e	・ユーザから始動の場合は可能 ・相手から始動の場合、ユーザが静的NAT配下であれば可能 ・IPsec利用の場合、NATトラバーサル機能のサポートが必須 ・IPsec利用の場合、NAPT配下の複数機器を扱えるかは機器に依存 ・IPsec(AH)は利用不可	b/c/d/e	・ユーザから始動の場合、相手側が静的NAT配下であれば可能 ・IPsec利用の場合、NATトラバーサル機能のサポートが必須 ・IPsec利用の場合、NAPT配下の複数機器を扱えるかは機器に依存 ・IPsec(AH)は利用不可
		オフィス機器	a/b	・NATが間に入ることを想定していない一部の機能が利用できない可能性あり	a/b/c	・NATが間に入ることを想定していない一部の機能が利用できない可能性あり

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
中規模ユーザ	アプリケーション	メール（含むコンテンツDNS）	a		a/b/c	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。 ・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		Web閲覧	a		a/e	・レイヤ4以上でIPアドレスを使用する場合は不可 ・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
		VoIP	b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存	b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存 ・サービスの安定性低下が危惧される
		DHCP	a		a/b	・DHCP Relay中継などが必要と考えられる
		認証	d	・プロトコルやアーキテクチャに依存	d	・プロトコルやアーキテクチャに依存
		DB	a	・プロトコルやアーキテクチャに依存	a	・プロトコルやアーキテクチャに依存
		NTP	a		a/b/c	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
大規模ユーザ	機器	PC	a		a/b	・アプリケーションに依存
		サーバー類	a		a/b/c	・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		ルータ／スイッチ	a		a/b/c	・NAT機能を提供する製品について、機能やスケールに起因する置き換えが必要となる可能性もある
		ファイアウォール	a		a/b/c	・運用の見直しが必要である可能性がある
		IDS／IPS	a		a/b/c	・運用の見直しが必要である可能性がある
		アンチウイルスゲートウェ	a		a/b/c	・運用の見直しが必要である可能性がある
		プロクシサーバ	a		a/b/c	・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		帯域制御装置	a/b/c		a/b/c/e	・多段NATの影響により、運用者が想定した帯域制御が行われるかどうか、非常に疑問

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
大規模ユーザ	機器	VPN機器	a/d/e	・ユーザから始動の場合は可能 ・相手から始動の場合、ユーザが静的NAT配下であれば可能 ・IPsec利用の場合、NATトラバーサル機能のサポートが必須 ・IPsec利用の場合、NAPT配下の複数機器を扱えるかは機器に依存 ・IPsec(AH)は利用不可	b/c/d/e	・ユーザから始動の場合、相手側が静的NAT配下であれば可能 ・IPsec利用の場合、NATトラバーサル機能のサポートが必須 ・IPsec利用の場合、NAPT配下の複数機器を扱えるかは機器に依存 ・IPsec(AH)は利用不可
		オフィス機器	a/b	・NATが間に入ることを想定していない一部の機能が利用できない可能性あり	a/b/c	・NATが間に入ることを想定していない一部の機能が利用できない可能性あり
		NTP	a		a/b/c	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
	アプリケーション	メール(含むコンテンツDNS)	a		a/b/c	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。 ・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		Web閲覧	a		a	・レイヤ4以上でIPアドレスを使用する場合は不可 ・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。
		VoIP	b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存	b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存 ・サービスの安定性低下が危惧される
		DHCP	a		a/b	・DHCP Relay中継などが必要と考えられる
		認証	d	・プロトコルやアーキテクチャに依存	d	・プロトコルやアーキテクチャに依存
		DB	a	・プロトコルやアーキテクチャに依存	a	・プロトコルやアーキテクチャに依存
		業務系アプリケーション	a	・プロトコルやアーキテクチャに依存	a	・プロトコルやアーキテクチャに依存

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
ネットワーク（インターネット）	機器	ルータ／スイッチ	a/b	・NATルータのスケール問題が発生する可能性あり	a/b/c	・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		収容装置	a	・既存IPv4対応機器で可能	a/b	
		サーバー類	a	・サーバはグローバルIPv4を付与という前提	a/b/c	・NAT下にあるサーバーへのアクセスを可能とするには、Static NATやGlobal IPアドレスを持つ中継サーバなどを利用することが必要。 ・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		監視装置	a/b/c	・NAT配下に存在する装置の監視が不可となる可能性がある	b/c/e	・NAT配下に存在する装置の監視が不可となる可能性がある
		NAPT	d/e	・基本的なNAT技術・製品はあるが、キャリア向け相当の大規模なNATの実現技術、製品が存在しない。	d/e	・基本的なNAT技術・製品はあるが、キャリア向け相当の大規模なNATの実現技術、製品が存在しない。
	アプリケーション	キャッシュDNS	a		a/b/c	・企業内のシステムで実績あり ・サーバ自体がNAT配下へ置かれると、ポートフォワーディング等の運用面やスケール、安定性などの課題が浮上する可能性がある
		メンテナンス／運用ツール	a	・NAT配下に存在する装置の監視が不可となる可能性がある	a/b/c/e	・NAT配下に存在する装置の監視が不可となる可能性がある
		認証	a/d	・プロトコルやアーキテクチャに依存	b/d	・プロトコルやアーキテクチャに依存
		DHCP	a		a/b	
		アクセス解析	a/d/e	・大規模NATのログ解析が困難と想定	a/b/c/e	・NAT配下に存在する装置の監視が不可となる可能性がある。 ・匿名性が向上するため、そもそも解析不能となるケースも考えられる

フィールド			NAT下に収容されたユーザーが、Global IPアドレスをもつ相手と通信する場合		NAT下に収容されたユーザーが、NAT下の相手と通信する場合	
			区分	備考	区分	備考
サービス提供者	機器	ルータ／スイッチ	a		a/b/c	・NATボックスとして利用している製品の、機能やスケールに起因する置き換えが必要となる可能性もある
		サーバー類	a/d/e	・DoSアタックへの対処が困難	a/b/c	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		ロードバランサ	a		a/b	・サーバーの直前に置くことが必要となる
		ファイアウォール	a/e	・多人数が同じアドレスでアクセスしてくる可能性があるため、問題が生ずる可能性あり	a/b/c	・運用の見直しが必要である可能性がある ・多人数が同じアドレスでアクセスしてくる可能性があるため、問題が生ずる可能性あり
		IDS／IPS	a/e	・多人数が同じアドレスでアクセスしてくる可能性があるため、問題が生ずる可能性あり	a/b/c/e	・運用の見直しが必要である可能性がある ・多人数が同じアドレスでアクセスしてくる可能性があるため、問題が生ずる可能性あり
		アンチウイルスゲートウェ	a		a/b/c	・運用の見直しが必要である可能性もある
	アプリケーション	コンテンツDNS	a/d	・スケール問題が発生する可能性あり ・DDNSへの対応方法が確立していない。	a/b/c	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		メール（含むコンテンツDNS）	a	・スケール問題が発生する可能性あり	a/b/c	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		認証	a/d	・プロトコルやアーキテクチャに依存 ・スケール問題が発生する可能性あり	a/d	・プロトコルやアーキテクチャに依存
		html／ファイル	a	・レイヤ4以上でIPアドレスを使用する場合は不可 ・スケール問題が発生する可能性あり	a/b/c	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		DB	a	・プロトコルやアーキテクチャに依存 ・スケール問題が発生する可能性あり	a	・プロトコルやアーキテクチャに依存
		アプリケーションサーバー	a	・スケール問題が発生する可能性あり	a	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		ストリーミング	a	・スケール問題が発生する可能性あり	a/d	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される
		VoIP	a/b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存 ・スケール問題が発生する可能性あり	a/b/c/d	・利用する製品とそれらの組み合わせに依存 ・SIPとNATの相性(タイマ周り等)やSIP-NAT機能のサポートなどに依存 ・サービスの安定性低下が危惧される ・スケールが課題
		NTP	a	・スケール問題が発生する可能性あり	a/b/c	・サーバー類をNAT下に設置した場合、外部からのアクセスが困難となることが想定される