

セキュリティから学ぶ インターネット

ネットワークセキュリティ

👉 何を守るのか？

= 自身, 組織の有するデータ, 情報, 財産

👉 何から守るのか？

= インターネットを標的とする犯罪者と, そのためのプログラム

- ✓ ウイルス
- ✓ スパイウェア
- ✓ オンライン詐欺
- ✓ SPAMメール
- ✓ なりすまし
- ✓ 情報漏洩・流出



どのようにして守るのか？

技術だけで防止できるもの
そうでないもの

知識・経験・勘

トピックス

[1] IPアドレス

[2] ドメイン名 / ホスト名

[3] ポート番号

事例1：匿名掲示板での犯罪予告

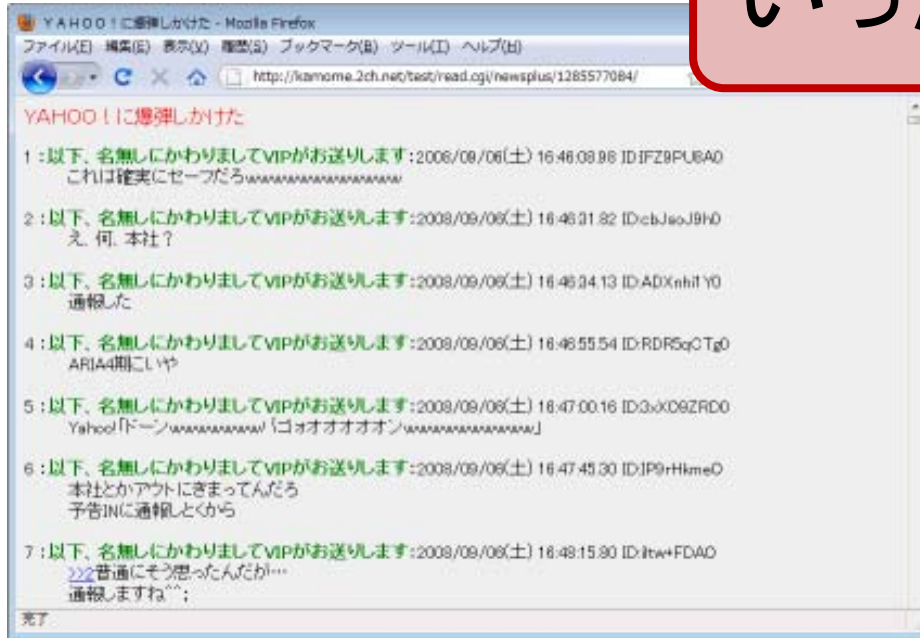


なぜこれだけの情報で逮捕？

前述新聞記事：同社の被害届を受け、インターネットの接続記録などから同容疑者を割り出した。

インターネットの接続記録

いったい何が記録?



サーバ



掲示板に書き込み
「爆弾しかけたぞ！」

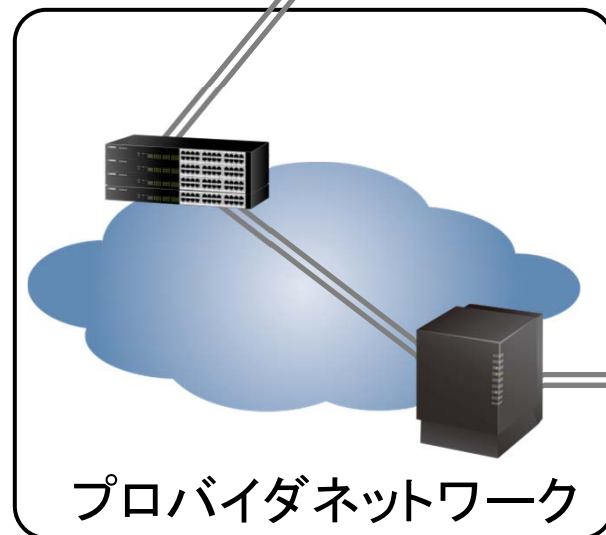
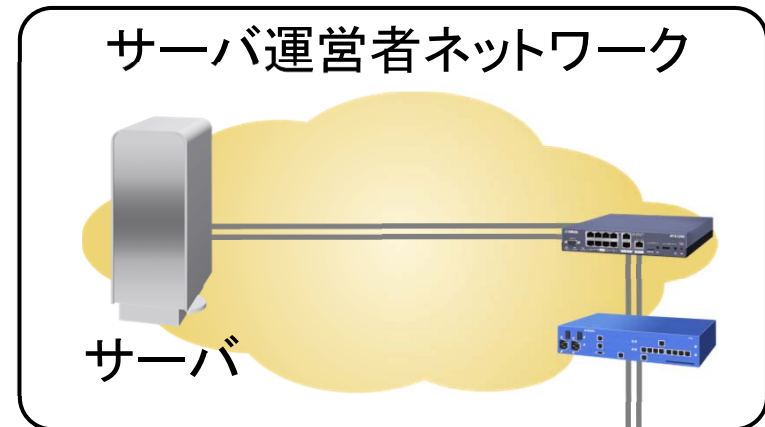
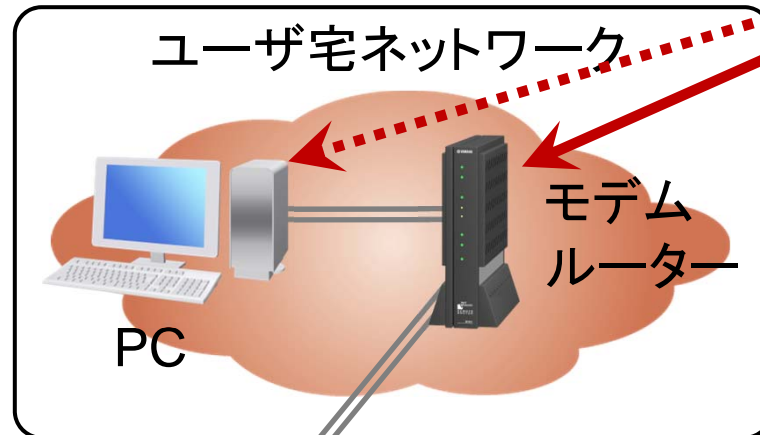
インターネットの接続記録

インターネット接続時には必ず

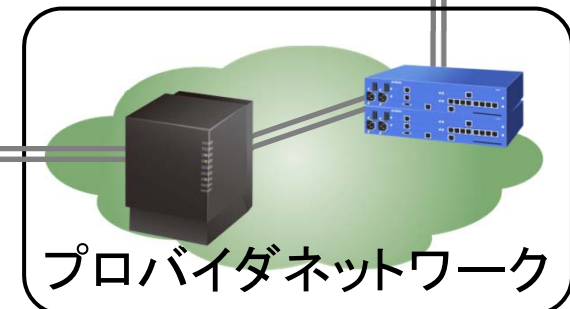
アイピー

IPアドレス

が付与される



ネットワーク中継施設
IX (Internet eXchange)



IPアドレス

インターネットに接続された機器を識別するための固有の番号

例)

202. 35. 192. 25

(名市大システム自然
Webサーバ)

160. 13 .185 .54

(名古屋市Webサーバ)

ある程度の期間
固定しているアドレス

192. 168. 11. 5

(宮原自宅PC)

10. 51. 31. 208

(宮原のスマートフォン)

日々変化するアドレス



IPアドレスが付いていないと通信できない

IPアドレスの形式

32ビットで表現

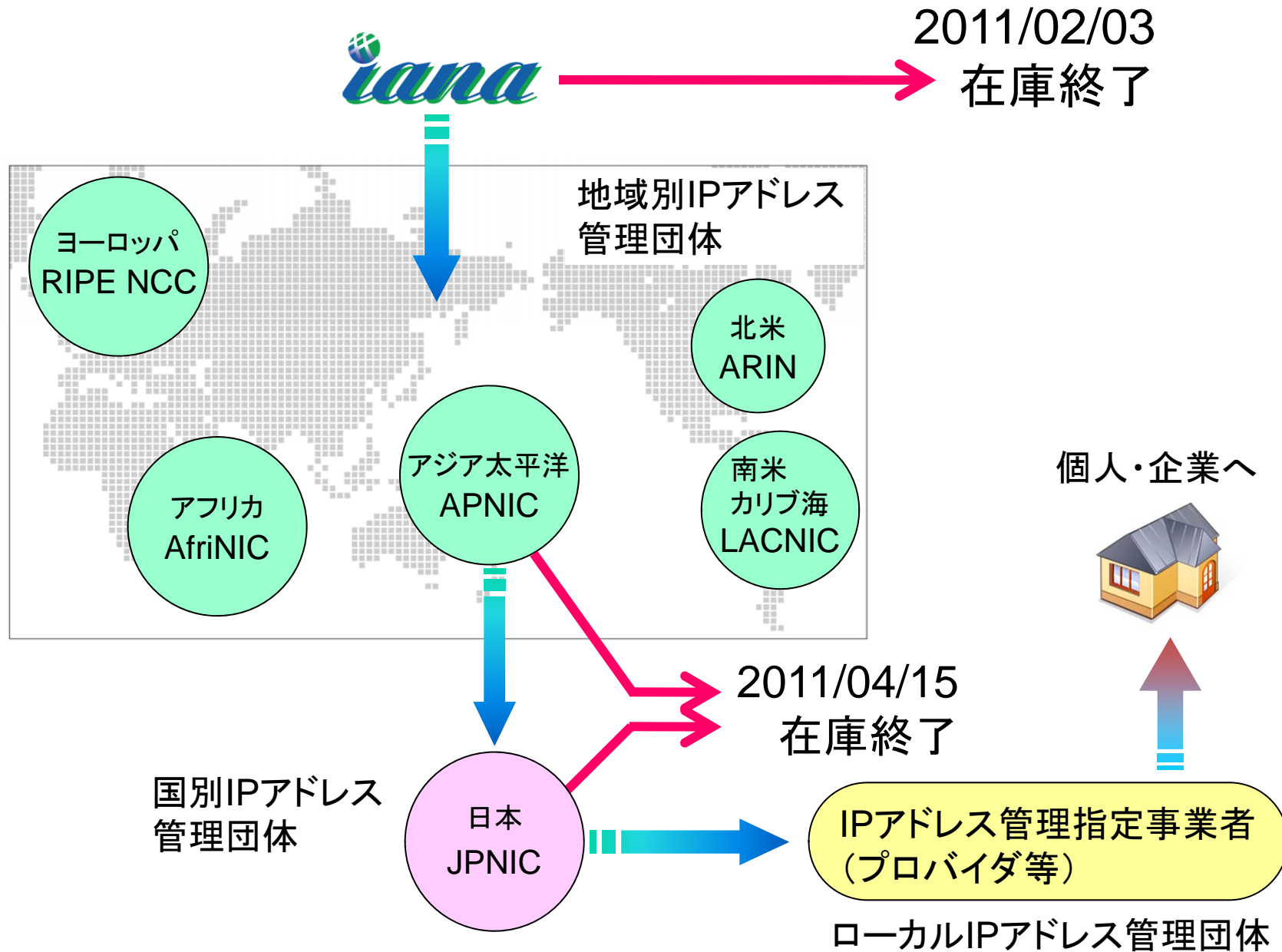
11001010	00100011	11000000	00011001
----------	----------	----------	----------

8ビット毎に10進表記

区切りは . ピリオド

202. 35. 192. 25

世界における割り当て



IPアドレス割当を調べる



- ➡ IP Addresses & AS Numbers (中段)
- ➡ Internet Protocol v4 Address Space
- ➡ 1ブロック目から割当地域を調べる



各地域NICにて whois 検索

Prefix	Designation	Date
000/8	IANA - Local Identification	1981-09
001/8	APNIC	2010-01
002/8	RIPE NCC	2009-09
003/8	General Electric Company	1994-05
004/8	Level 3 Communications, Inc.	1992-12
005/8	RIPE NCC	2010-11
006/8	Army Information Systems Center	1994-02
007/8	Administered by ARIN	1995-04
008/8	Level 3 Communications, Inc.	1992-12
009/8	IBM	1992-08
010/8	IANA - Private Use	1995-06
011/8	DoD Intel Information Systems	1993-05
012/8	AT&T Bell Laboratories	1995-06
013/8	Xerox Corporation	1991-09
014/8	APNIC	2010-04
015/8	Hewlett-Packard Company	1994-07
016/8	Digital Equipment Corporation	1994-11
017/8	Apple Computer Inc.	1992-07

課題: ひとつ選び検索

68.71.220.23

133.6.1.1

128.97.27.37

27.110.42.248

133.29.251.222

211.16.112.216

195.224.71.221

160.111.244.48

203.32.178.10

接続記録を追う

YAHOO! に爆弾しかけた

1: 以下、名無しにかわりましてVIPがお送りします:2008/09/06(土) 16:46:08.98 ID:IFZ9PU8A0
これは確実にセーフだろwwwwwwwwwwwwwwwwwwww

掲示板サイトのサーバには、書き込み元 IPアドレスが記録

(例えば、180.42.178.1) ← サーバ運営会社から得るには法に基づいた
開示請求 が必要

IPアドレスから、ネットワーク組織を特定

インターネットの知識があれば
誰でも可能

(例えば、上記アドレスは、OCN という
プロバイダに割当てられている)

プロバイダの接続記録から契約者を特定 ← **開示請求**

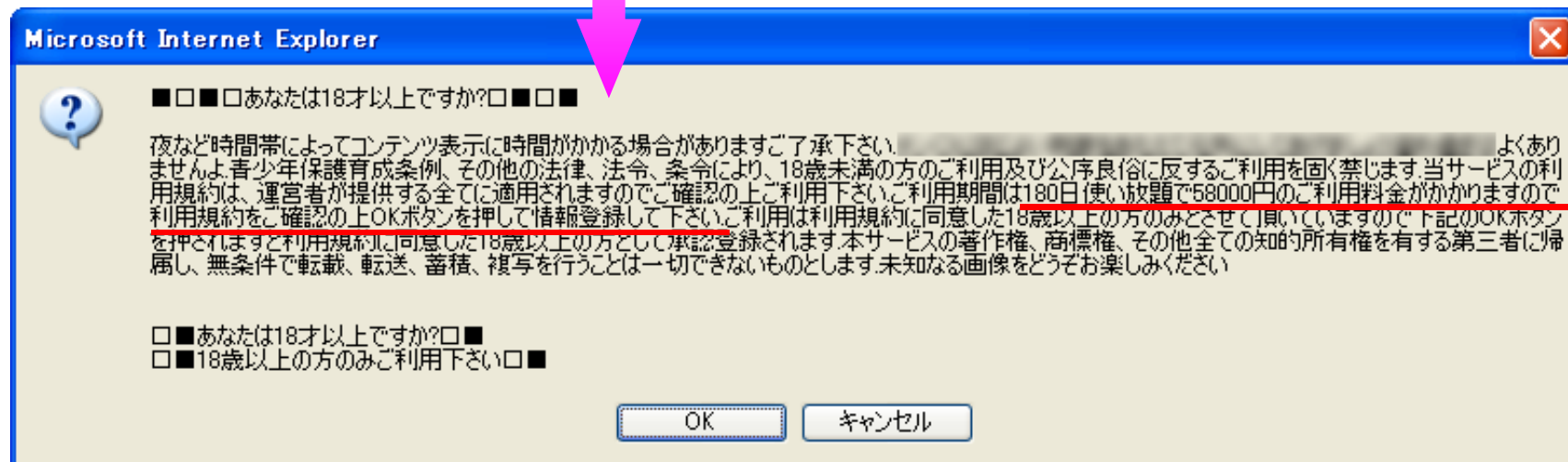
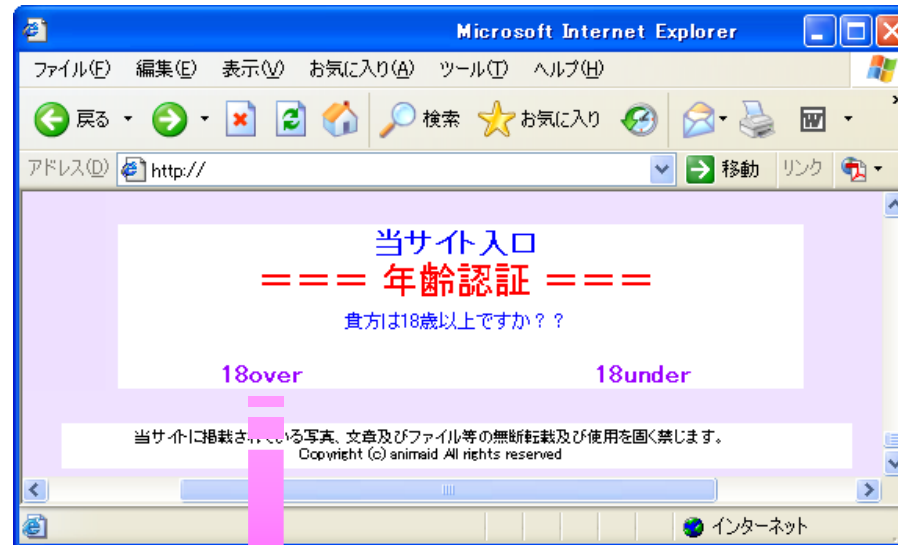
ここまでのまとめ

インターネットは匿名か？

否

開示請求によって明らかに

事例2: ワンクリック不当請求サイト



事例2: ワンクリック不当請求サイト

ご登録ありがとうございます。 - Microsoft Internet Explorer

アドレス http://

★★ 登録完了★★ ありがとうございます

あなたの登録日	[16日]
あなたのIPアドレス	[202.35.193.129]
あなたのプロバイダ情報	[202.35.193.129]
認識コード	[0b6e60d9bd7734e2fdb371a3a06fed96]
利用履歴	これまでに[1]回のコンテンツ読み込み履歴があります。 上記の情報で登録させて頂き、入会手続きを完了致しました。
ご利用期間	[180日間]
ご利用料金	[¥58,000]
お振込み期日	[登録日より2日]

お支払い期限を過ぎても入金確認が出来ない場合、規約に基づきIPや会員IDをもとに当番館まで頂く可能性があります。

確認 ID番号 [ATFM00KM]

お問い合わせ 退会申請

メール info@animaid.jp

退会申請 0120-848-774

銀行振込案内

三井住友銀行 広島支店
普通 6809783
名義人 ヒガミ キヨシ

振込金額: 只今キャンペーン中につき ¥100,000 ⇒ ¥58,000 (180日間見放題!!)
振込人名: あなたの確認ID番号を、必ず入れてください。
※お客様の振込みIDが確認できない場合、お支払いは無効となりますのでご注意ください。
※ご登録日より10日以上経過するとキャンペーン対象外となりますのでご注意ください。
※お振込時の振込人名についての注意事項
振込人名は、必ず確認ID番号でお願致します。
名前等でご入金された場合、処理できない可能性があります。
また、振込漏れによってご依頼人名が自動的にご利用口座名義となり、確認ID番号での入力ができない場合がございます。
その際はお手数ですが確認のためご振込人名とお振込日、お振込み金額、及び確認ID番号をサポートまでメールにてお知らせください。

プライバシーポリシー

***** ご注意下さい!! *****

支払い期限内に入金をお願いします。
支払い期限を過ぎても入金確認出来ない場合は「お客様の登録情報」を基に情報開示を
も考えます。
※情報開示情報
・勤務先情報

ページが表示されました

あなたのIPアドレス 202.35.193.129

あなたのプロバイダ情報 202.35.193.129

ご利用期間 180日間

ご利用料金 ¥58,000

お振込み期日 登録日より2日

支払い期限を過ぎても入金が確認できない場合は「お客様の登録情報」を基に情報開示を求めます。その場合、法的措置も考えます。

- ・勤務先情報
- ・勤務先電話番号

接続記録を追う

あなたの登録日	[1 16]
あなたのIPアドレス	[202.35.193.129]
あなたのプロバイダ情報	[202.35.193.129]
認識コード	[0b6e60d9bd7734e2fdb371a3a06fed96]
利用履歴	これまでに「1」回のコンテンツ読み込み履歴があります。

不当請求サイトのサーバに、IPアドレスが記録



→ 202.35.193.129

IPアドレスから、ネットワーク組織を特定（WHOIS検索）



→ 名古屋市立大学

開示請求……できない ……………（どうすることもできない）

不当請求サイト: 対策



それらしい情報を表示し、不安を募らせる

この類のサイトに個人は特定できない！

(ただのハッター)

- (1) 基本は無視、絶対に振り込まない
- (2) 問合せ、登録解除依頼といった連絡もしない
- (3) ネットの掲示板で相談、似た事例を検索
- (4) ケータイ版、スマートフォン版サイトも存在

(ただ、無視できないケースもでてきた……)

IPアドレスの調べ方

スタートメニュー

⇒ Windows システムツール

⇒ コマンドプロンプト

⇒ 本教室では Windows アクセサリ

```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

X:¥> ipconfig
Windows IP 構成

イーサネット アダプター ローカル エリア接続:
    接続固有の DNS サフィックス . . . . . : ncujoho.nagoya-cu.ac.jp
    IPv4 アドレス . . . . . : 172.31.12.100
    サブネット マスク . . . . . : 255.255.255.0
    デフォルト ゲートウェイ . . . . . : 172.31.12.254

X:¥>
```

有線LAN接続のみのシンプルな構成

IPアドレスの調べ方

```
コマンド プロンプト
C:\>ipconfig

Windows IP 構成

Wireless LAN adapter ローカル エリア接続* 1:

    メディアの状態. . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :

Wireless LAN adapter ローカル エリア接続* 3:

    メディアの状態. . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :

Wireless LAN adapter Wi-Fi:

    接続固有の DNS サフィックス . . . . . : ncu.joho.nagoya-cu.ac.jp
    リンクローカル IPv6 アドレス. . . . . : fe80::8da5:f53c:e7b7:2a4e%13
    IPv4 アドレス. . . . . : 172.21.45.255
    サブネット マスク . . . . . : 255.255.252.0
    デフォルト ゲートウェイ . . . . . : 172.21.47.254

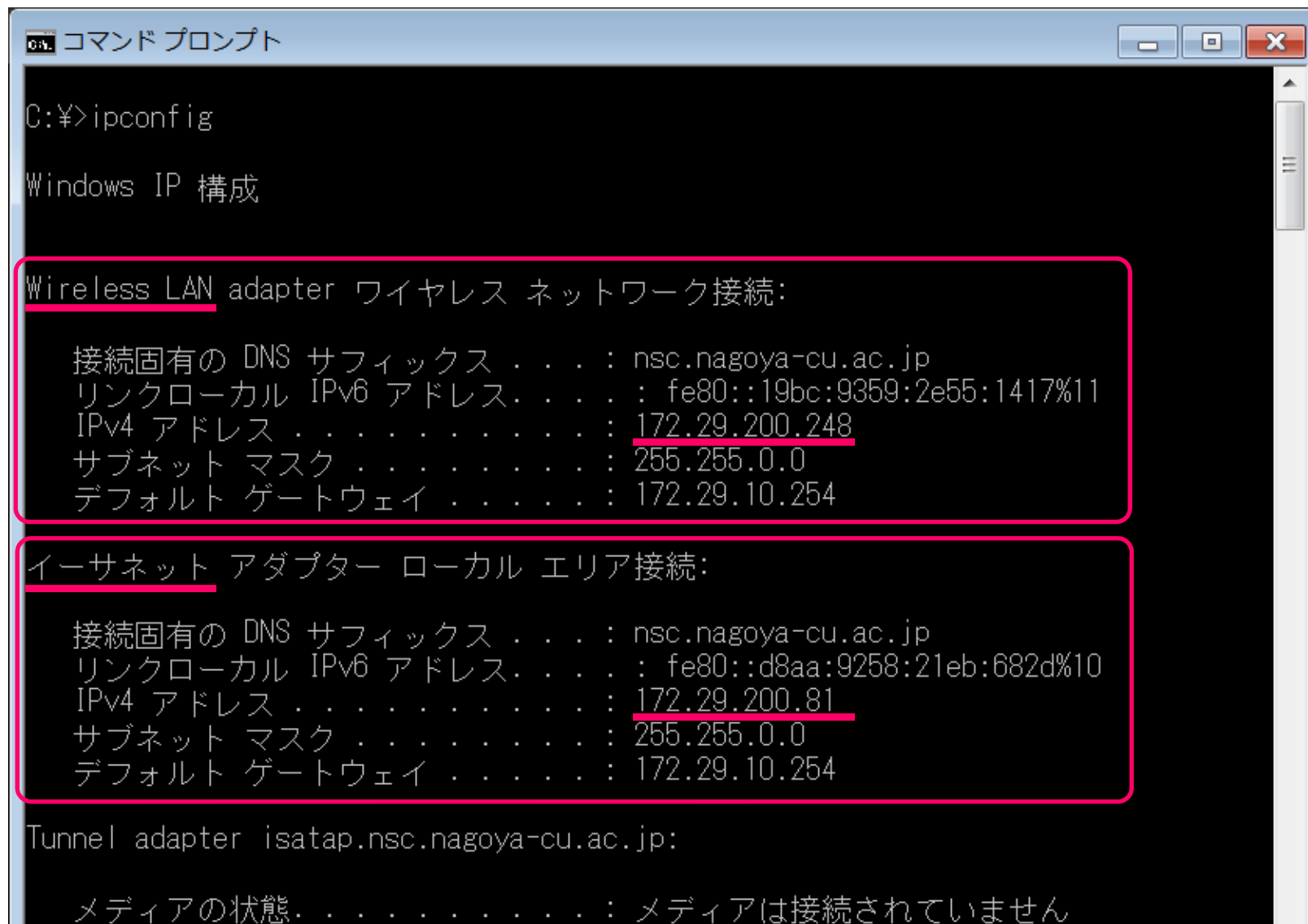
イーサネット アダプター Bluetooth ネットワーク接続:

    メディアの状態. . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :

C:\>
```

無線LAN (ncu wifi) のみ接続

IPアドレスの調べ方



```
コマンドプロンプト
C:\>ipconfig

Windows IP 構成

Wireless LAN adapter ワイヤレス ネットワーク接続:

    接続固有の DNS サフィックス . . . . : nsc.nagoya-cu.ac.jp
    リンクローカル IPv6 アドレス . . . . : fe80::19bc:9359:2e55:1417%11
    IPv4 アドレス . . . . . : 172.29.200.248
    サブネット マスク . . . . . : 255.255.0.0
    デフォルト ゲートウェイ . . . . . : 172.29.10.254

イーサネット アダプター ローカル エリア接続:

    接続固有の DNS サフィックス . . . . : nsc.nagoya-cu.ac.jp
    リンクローカル IPv6 アドレス . . . . : fe80::d8aa:9258:21eb:682d%10
    IPv4 アドレス . . . . . : 172.29.200.81
    サブネット マスク . . . . . : 255.255.0.0
    デフォルト ゲートウェイ . . . . . : 172.29.10.254

Tunnel adapter isatap.nsc.nagoya-cu.ac.jp:

    メディアの状態 . . . . . : メディアは接続されていません
```

有線LAN、無線LAN、双方を設定

IPアドレスの調べ方



IPアドレスの調べ方

システムプロファイラ

アップルメニュー

⇒ このMacについて

⇒ システムレポート

⇒ ネットワーク

MacBook Pro

動作中のサービス	種類	ハードウェア	BSD 装置名	IPv4 アドレス
Bluetooth DUN	PPP (PPPSerial)	モデム	Bluetooth-Modem	
Bluetooth PAN	Ethernet	Ethernet	en3	
Thunderbolt Bridge	Ethernet	Ethernet	bridge0	
USB Network Interface	Ethernet	Ethernet	en4	
Wi-Fi	AirMac	AirMac	en0	172.29.200.34

無線LANの場合
Wi-Fi を選択

Wi-Fi :

種類 : AirMac
ハードウェア : AirMac
BSD 装置名 : en0
IPv4 アドレス : 172.29.200.34

IPv4 :

AdditionalRoutes :

DestinationAddress : 172.29.200.34
SubnetMask : 255.255.255.255
DestinationAddress : 169.254.0.0
SubnetMask : 255.255.0.0

アドレス : 172.29.200.34
ARPResolvedHardwareAddress : 00:23:26:ee:a5:ac
ARPResolvedIPAddress : 172.29.10.254
構成方法 : DHCP
ConfirmedInterfaceName : en0
インターフェイス名 : en0
ネットワーク署名 :
IPv4.Router=172.29.10.254;IP:a5:ac
ルーター : 172.29.10.254

ネットワークユーティリティ

Info Netstat Ping Lookup Traceroute Whois Finger Portscan

情報を取得する対象となるネットワークインターフェイスを選んでください。

Wi-Fi (en0)

インターフェイス情報

ハードウェア・アドレス : 20:c9:d0:7a:06:3f
IP アドレス : 172.29.200.34
リンク速度 : 54 Mbit/秒
リンクの状況 : 動作中
製造元 : Apple
モデル : Wireless Network Adapter (802.11 a/b/g/n)

転送の統計情報

送信パケット数 : 27,665
送信エラー数 : 0
受信パケット数 : 103,033
受信エラー数 : 0
衝突 : 0

ネットワークユーティリティ
(Spotlightで検索)

IPアドレスの設定

ローカルエリア接続の状態

全般

接続

IPv4 接続:	インターネット
IPv6 接続:	インターネット アクセスなし
メディアの状態:	有効
期間:	4 日 00:04:50
速度:	

動作状況

送信	
バイト	383,632

詳細(E)...

プロパティ(P)

ローカルエリア接続のプロパティ

ネットワーク

接続の方法:

Intel(R) 82579LM Gigabit Netw

この接続は次の項目を使用します(O):

- Microsoft ネットワーク用クライアント
- QoS パケット スケジューラ
- Microsoft ネットワーク用ファイルとプリンター共有
- インターネット プロトコル バージョン 6 (TCP/IPv6)
- インターネット プロトコル バージョン 4 (TCP/IPv4)
- Link-Layer Topology Discovery Mapper I/O Driver
- Link-Layer Topology Discovery Responder

インストール(N)... 削除(U) プロパティ(R)

説明

伝送制御プロトコル/インターネット プロトコル。相互接続されたさまざまなネットワーク間の通信を提供する、既定のワイド エリア ネットワーク プロトコルです。

OK キャンセル

インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

IP アドレスを自動的に取得する(O)

次の IP アドレスを使う(S):

IP アドレス(I):

サブネット マスク(U):

デフォルト ゲートウェイ(D):

DNS サーバーのアドレスを自動的に取得する(B)

次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P):

代替 DNS サーバー(A):

終了時に設定を検証する(L)

詳細設定(V)...

OK キャンセル

IPアドレス取得と設定

取得方法

- ✓ 接続プロバイダから貸与
- ✓ 所属組織から貸与

2通りの設定方法

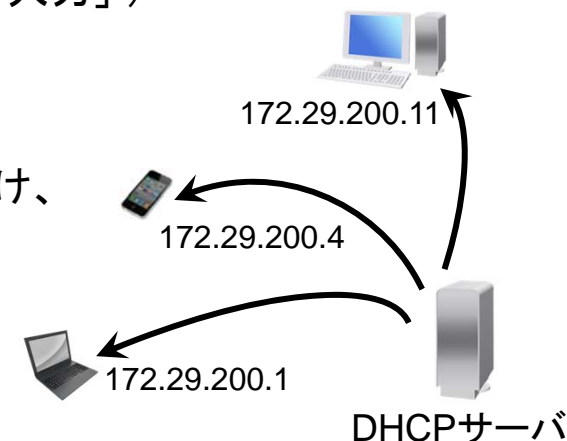
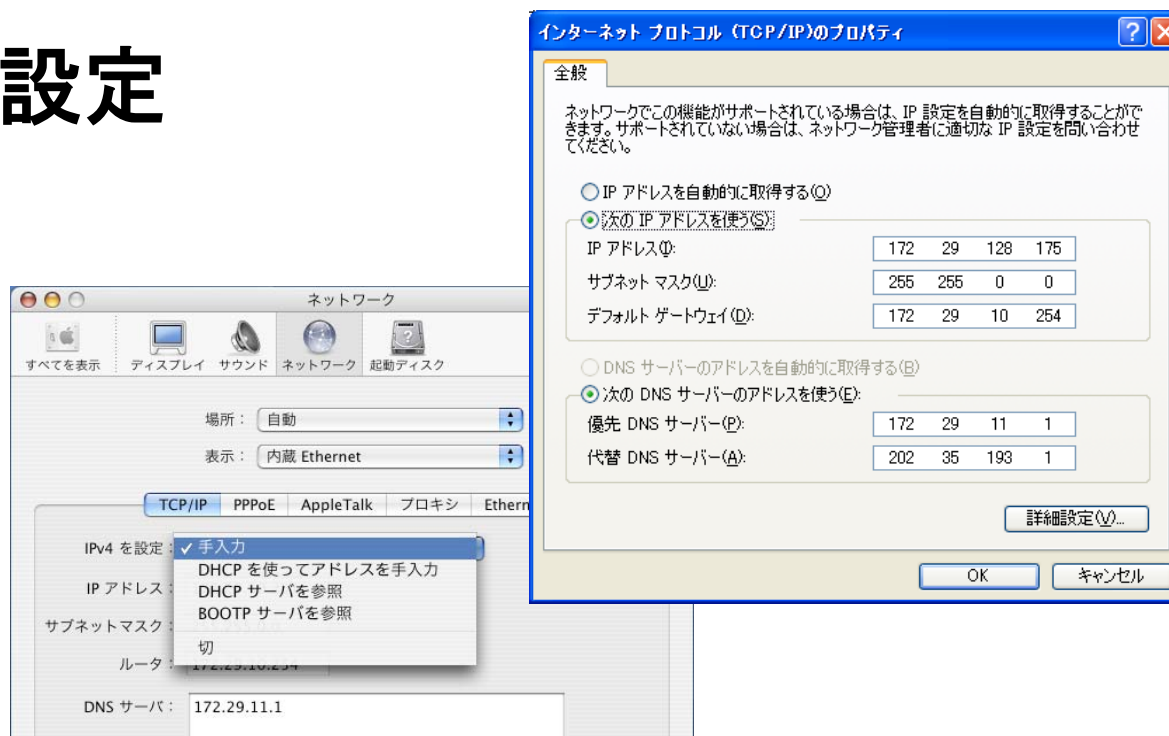
✓ 固定アドレス

—— あらかじめ決められた IP アドレスを借り受け、それを手動で設定
(Windows:「次のIPアドレスを使う」 MacOS:「手入力」)

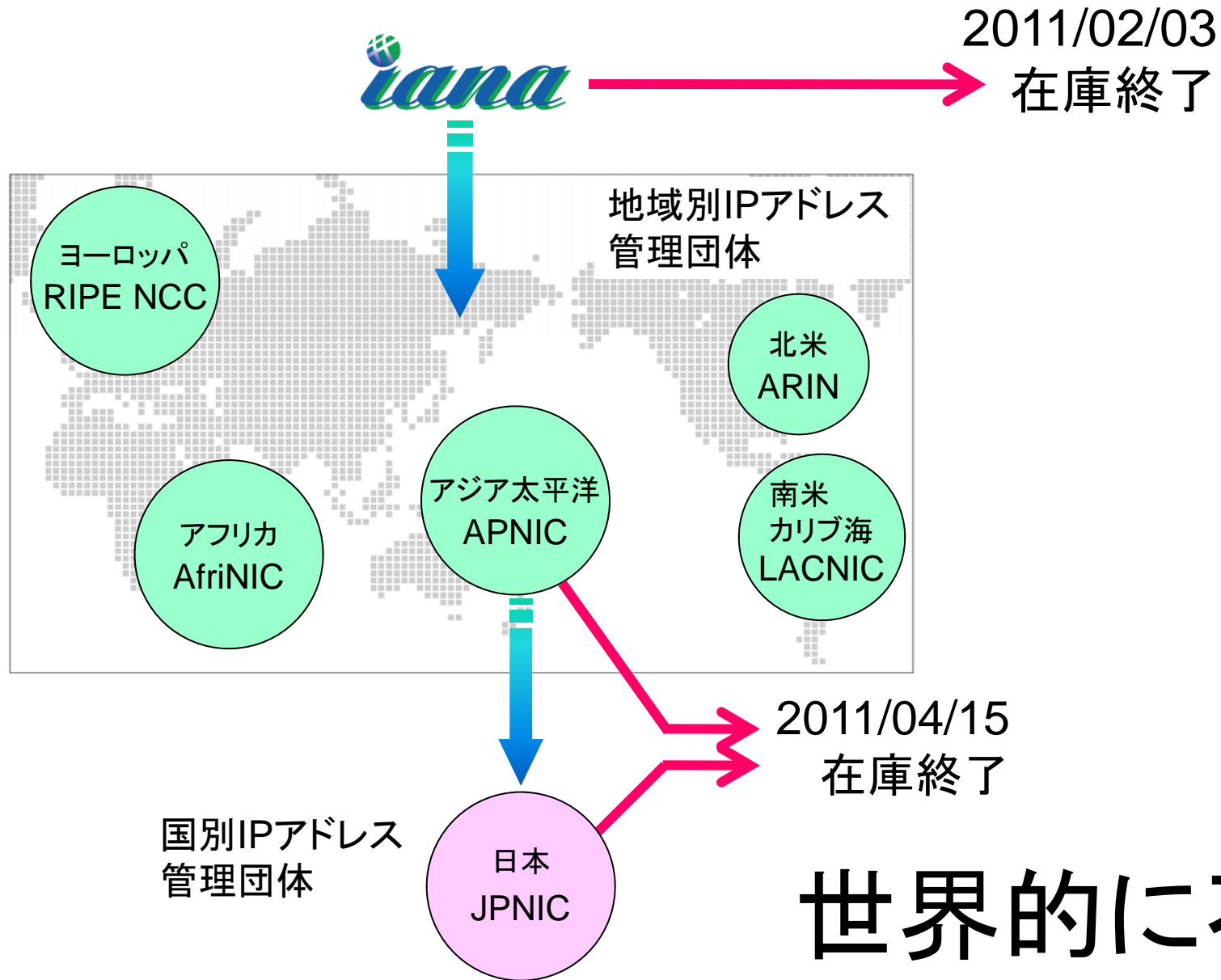
✓ 動的アドレス (DHCP)

—— 起動時に専用サーバからIP アドレスひとつを借り受け、自動で設定

(Windows: 「IPアドレスを自動的に取得する」
MacOS: 「DHCPサーバを使用」)



世界における割り当て



世界的に不足

IPアドレス不足への対応

☞ 次世代版IPアドレス (IPv6)

128ビットのアドレス空間

(340282366920938463463374607431768211456個 = 約340潤個)

アドレス表記の例) 2001:0db8:bd05:01d2:288a:1fc0:0001:10ee

IPv4 との互換性、移行方法、共存が課題

 実験的サービスや限定利用にとどまる

☞ プライベートアドレスとアドレス変換

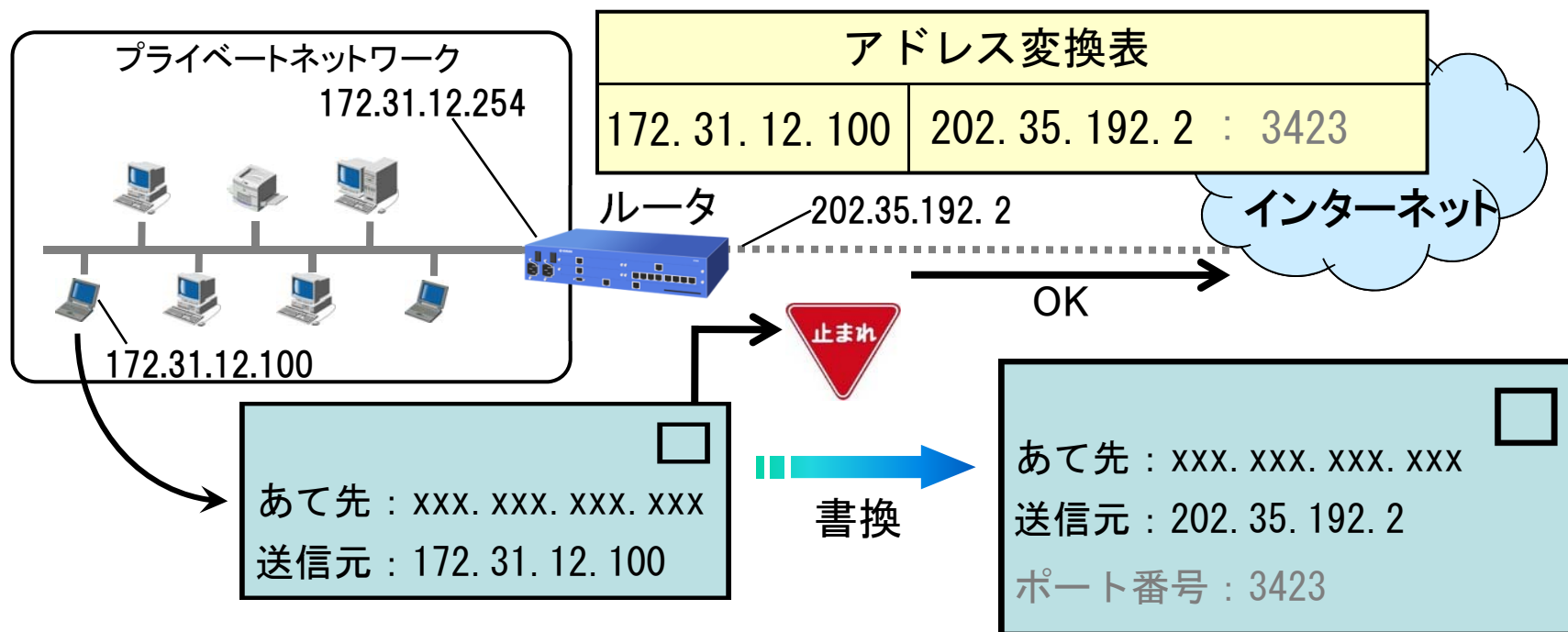
(NAT: Network Address Translation)

グローバル or プライベート？

👉 グローバルIPアドレス
= 世界に通じるIPアドレス

👉 プライベートIPアドレス →
= 組織内に限って使用可能
(外に行くときはグローバル使ってネ)

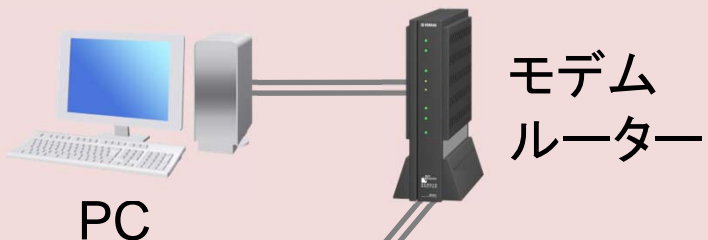
10.0.0.0	~ 10.255.255.255
172.16.0.0	~ 172.31.255.255
192.168.0.0	~ 192.168.255.255



グローバル or プライベート？

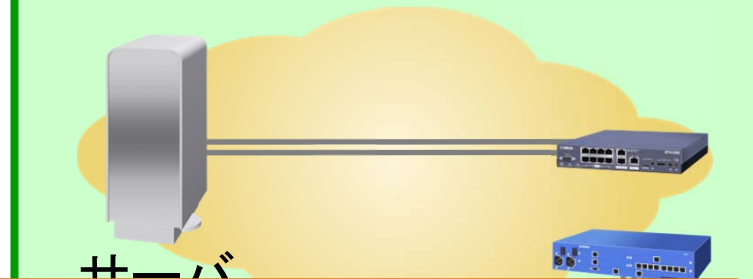
プライベート

ユーザ宅ネットワーク



グローバル

サーバ運営者ネットワーク



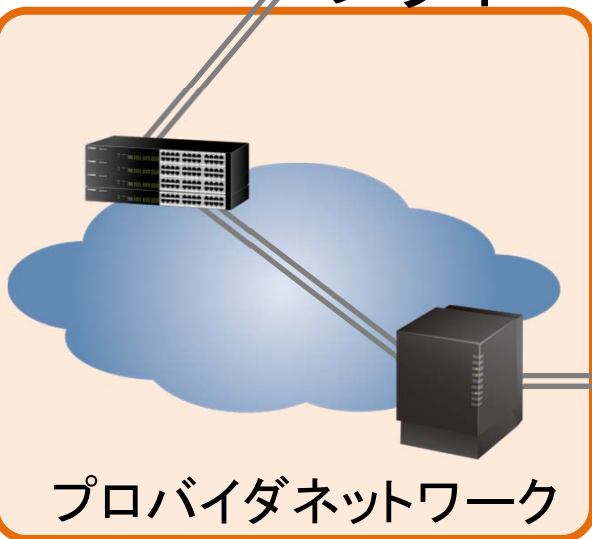
プライベート化

(4番目のプライベートアドレスブロック)

CGN : Carrier-Grade NAT

100.64.0.0 ~ 100.127.255.255

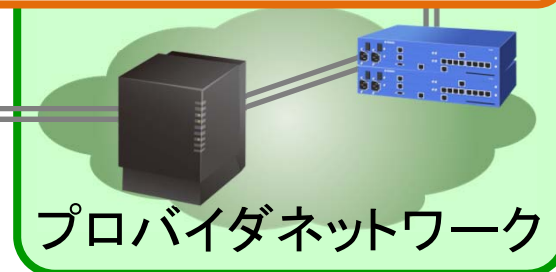
プロバイダネットワーク



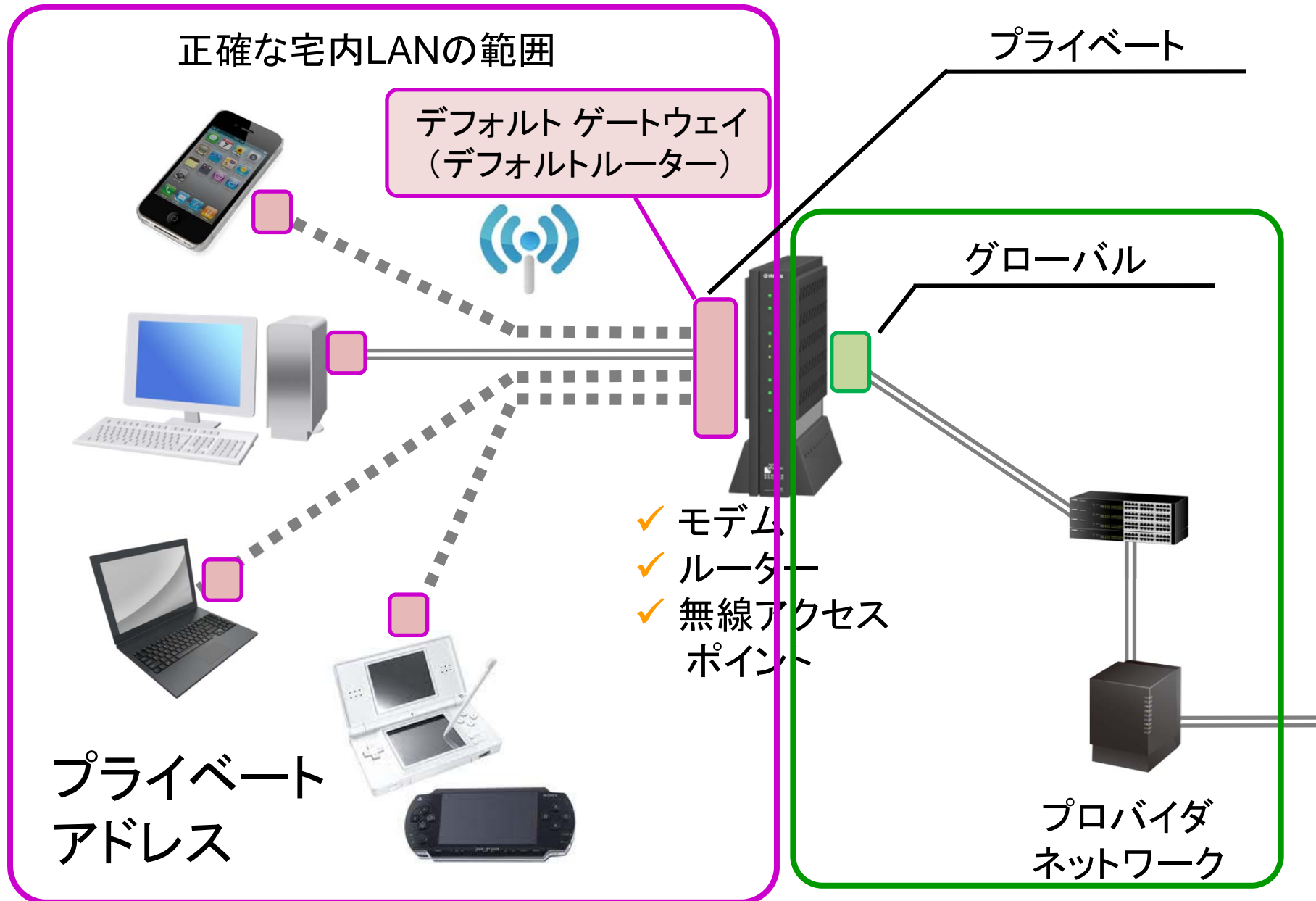
ネットワーク中継施設
IX(Internet eXchange)



プロバイダネットワーク



どこにIPアドレスが付くか？



どこにIPアドレスが付くか？

```
cmd コマンドプロンプト
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

X:¥>ipconfig

Windows IP 構成

イーサネット アダプター ローカル エリア接続:

接続固有の DNS サフィックス . . . . . : ncuioho.nagoya-c
IPv4 アドレス . . . . . : 172.31.12.100
サブネット マスク . . . . . : 255.255.255.0
デフォルト ゲートウェイ . . . . . : 172.31.12.254

X:¥>
```

確認くん

https://www.ugtop.com/spill.sht

あなたの情報 (確認くん)

情報を取得した時間	2019年 04月 26日 PM 12 時 47分 05秒
現在接続している場所(Server)	www.ugtop.com
あなたのIPアドレス(IPv4)	202.35.192.2
ゲートウェイの名前	(none)
OSの解像度	1280 x 1024pix
現在のブラウザ	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101 Firefox/60.0 表示サイズ : 905 x 714pix
クライアントの場所	(none) / (none)
クライアントID	(none)
ユーザ名	(none)
どこのURLから来たか	https://www.google.com/
Proxyのバージョン等	(none)
Proxyのステータス	(none) / (none) / (none)
Proxyの効果	(none)
MIMEの仕様	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
FORMの情報	GET

どこにIPアドレスが付くか？



端末の設定画面から確認

10.50.151.190

プライベートアドレス



外部Webサイトで確認

110.163.12.77

NTT DoCoMoに割当て

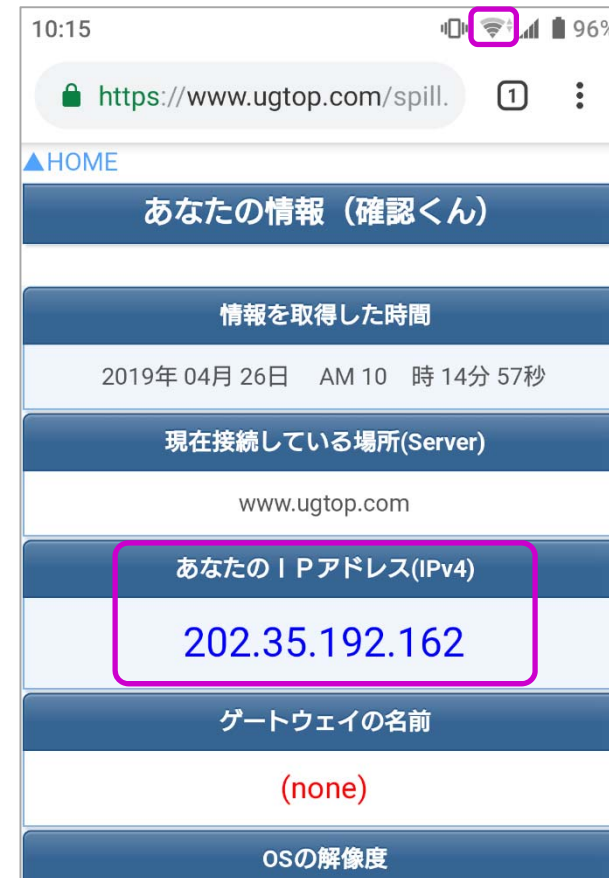
どこにIPアドレスが付くか？



端末の設定画面から確認

172.21.44.211

ncuwifi 割当のプライベートアドレス



外部Webサイトで確認

202.35.192.162

名古屋市立大学に割当て

まとめ

インターネット・必須知識(1)

IPアドレス

- (1) インターネット接続時には必ず付与
- (2) XXX.XXX.XXX.XXX という形式 (XXX = 0 ~ 255)
- (3) IPアドレスから個人(住所、氏名、電話番号)が特定されることは、まずない
- (4) 組織内のみ有効なプライベートアドレス