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

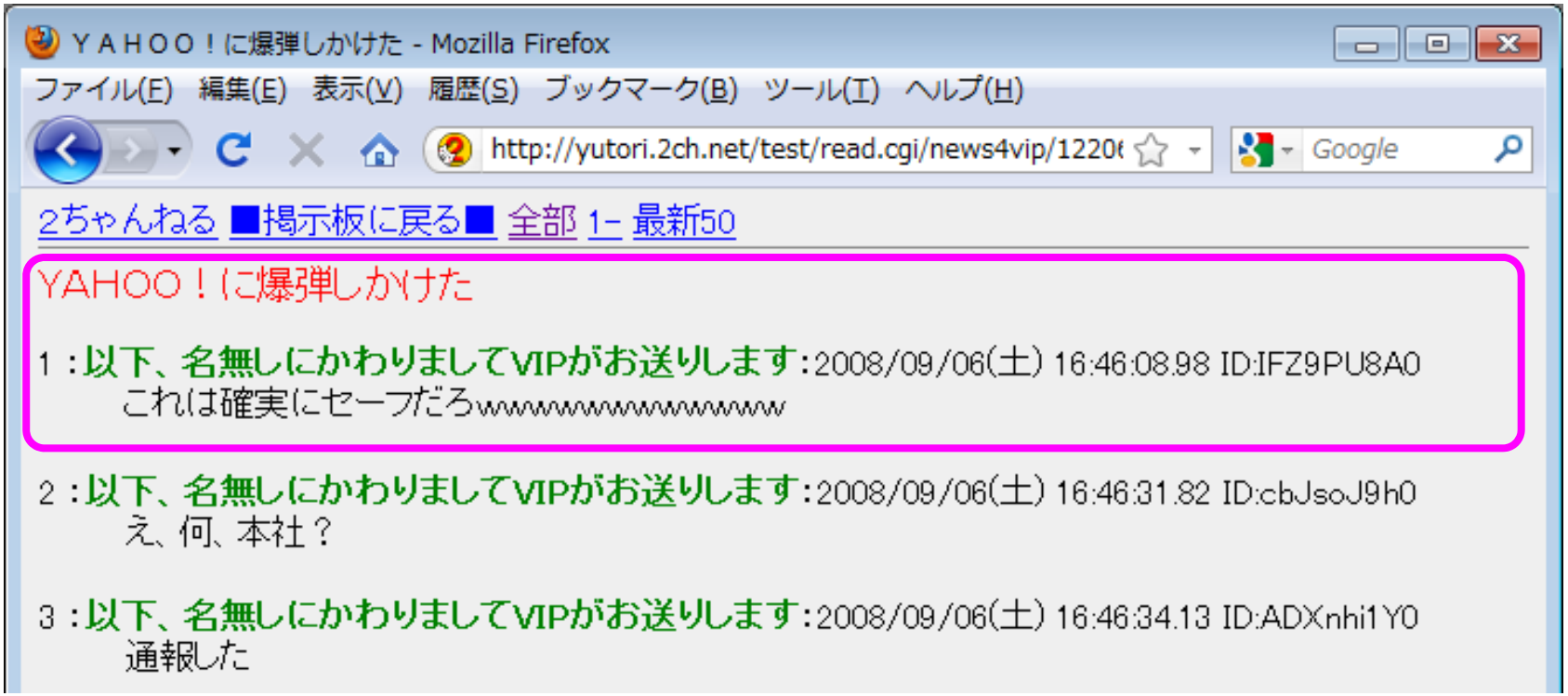
トピックス

［1］ IPアドレス

［2］ ドメイン名 / ホスト名

［3］ ポート番号

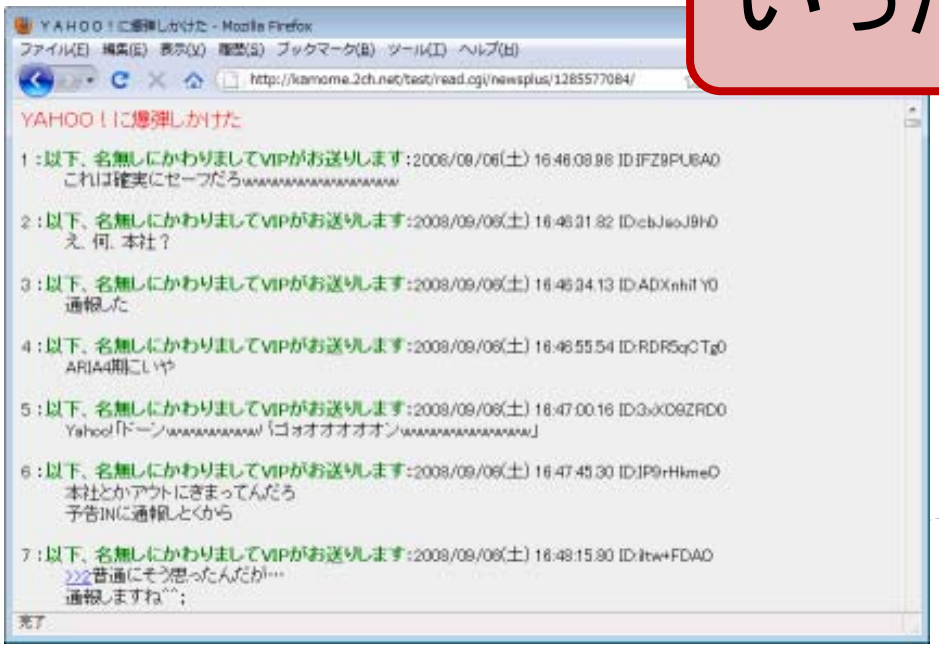
事例1：匿名掲示板での犯罪予告



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



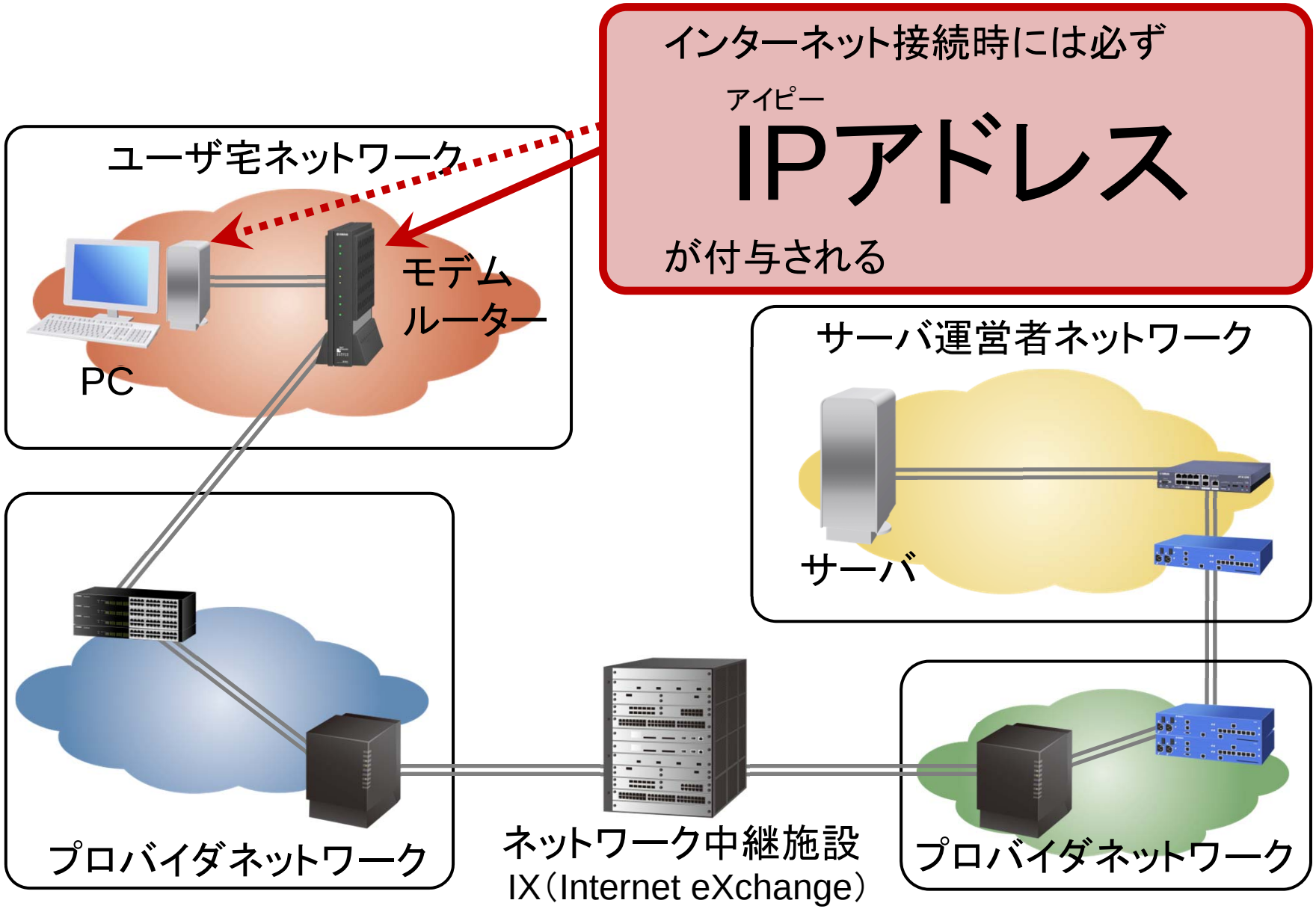
いったい何が記録?

サーバ

掲示板に書き込み

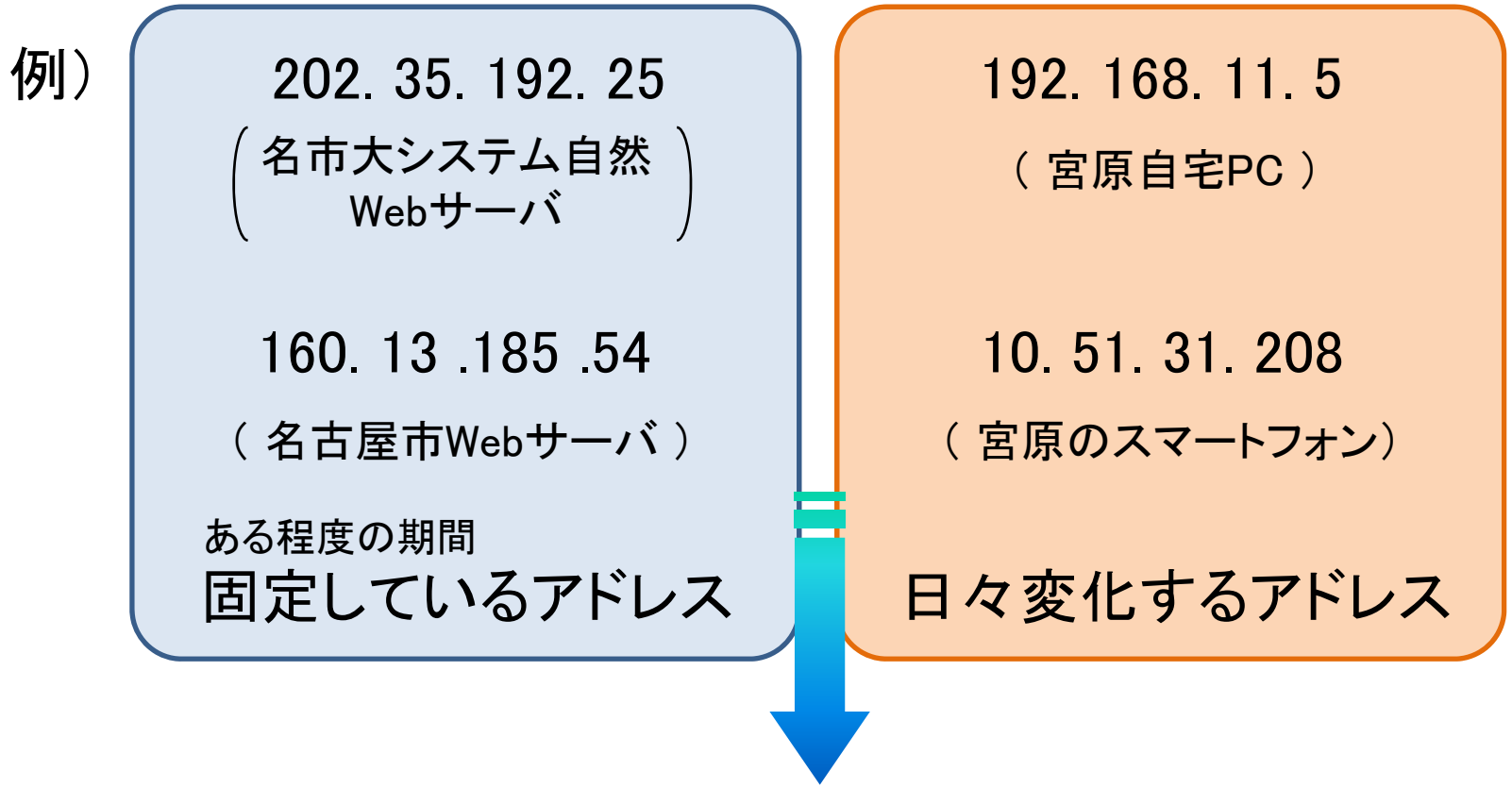
「爆弾しかけたぞ！」

インターネットの接続記録



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



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

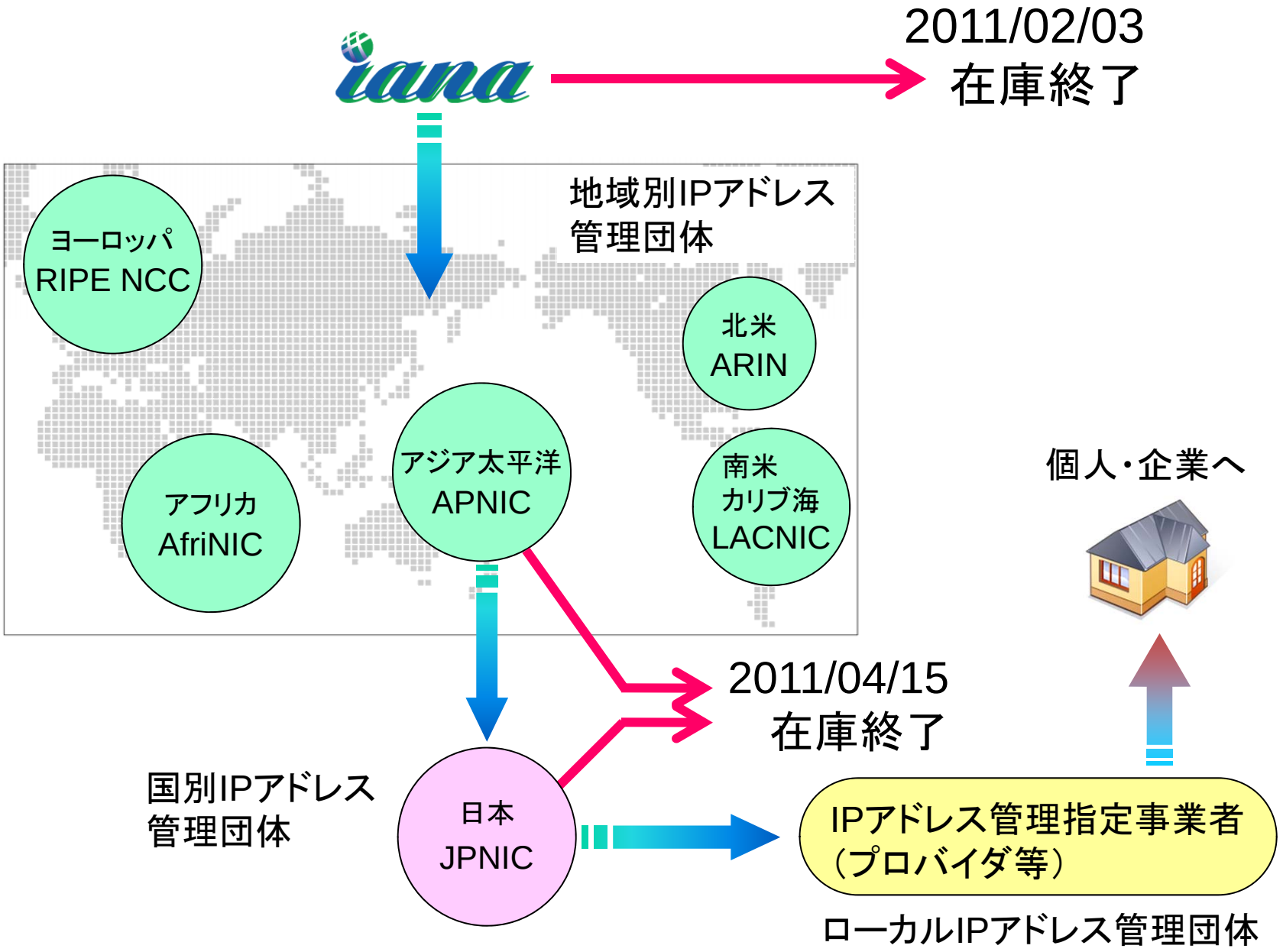
11001010	00100011	11000000	00011001

8ビット毎に10進表記

区切りは．ピリオド

202. 35. 192. 25

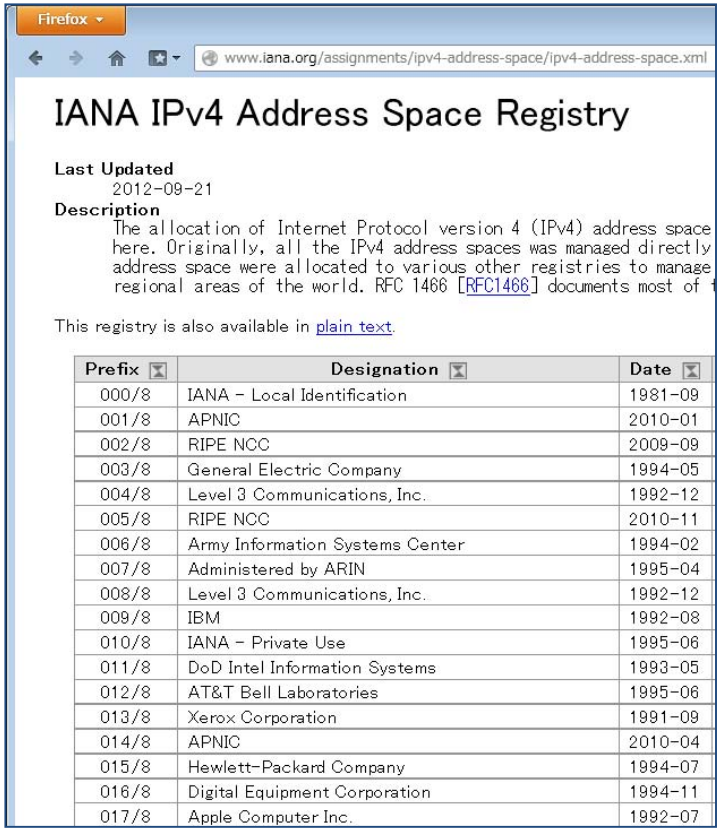
世界における割り当て


2011/02/03
在庫終了
地域別IPアドレス
管理団体
ヨーロッパ
RIPE NCC
北米
ARIN
アジア太平洋
APNIC
アフリカ
AfriNIC
南米
カリブ海
LACNIC
個人・企業へ
2011/04/15
在庫終了
国別IPアドレス
管理団体
日本
JPNIC
IPアドレス管理指定事業者
（プロバイダ等）
ローカルIPアドレス管理団体

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



IANA IPv4 Address Space Registry

Last Updated
2012-09-21

Description
The allocation of Internet Protocol version 4 (IPv4) address space here. Originally, all the IPv4 address spaces was managed directly address space were allocated to various other registries to manage regional areas of the world. RFC 1466 [RFC1466] documents most of t

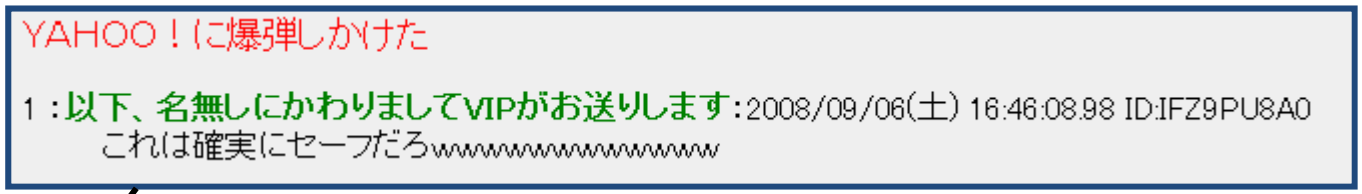
This registry is also available in plain text.

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



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**

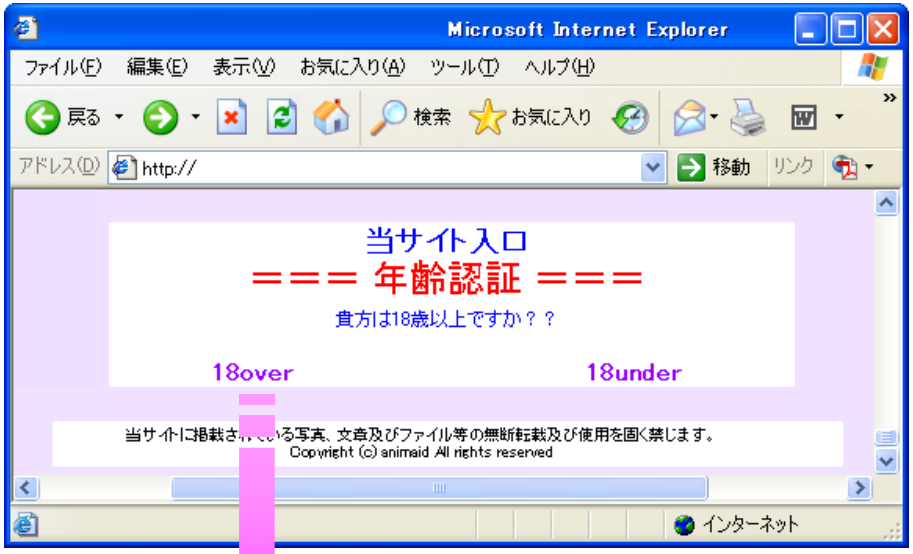
ここまでのまとめ

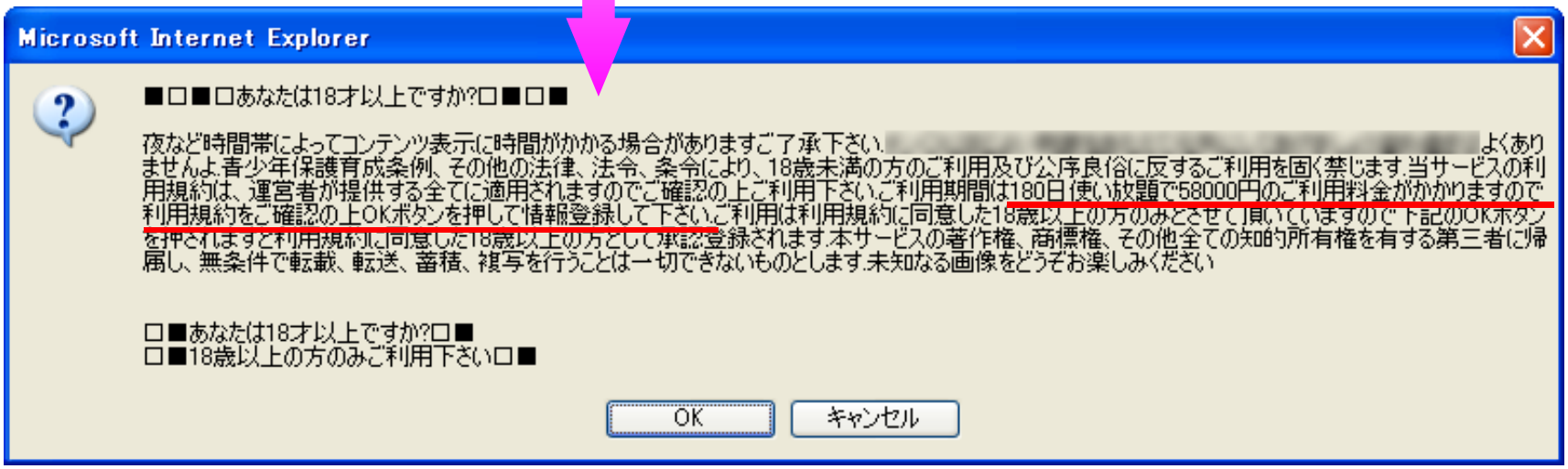
インターネットは匿名か？

否

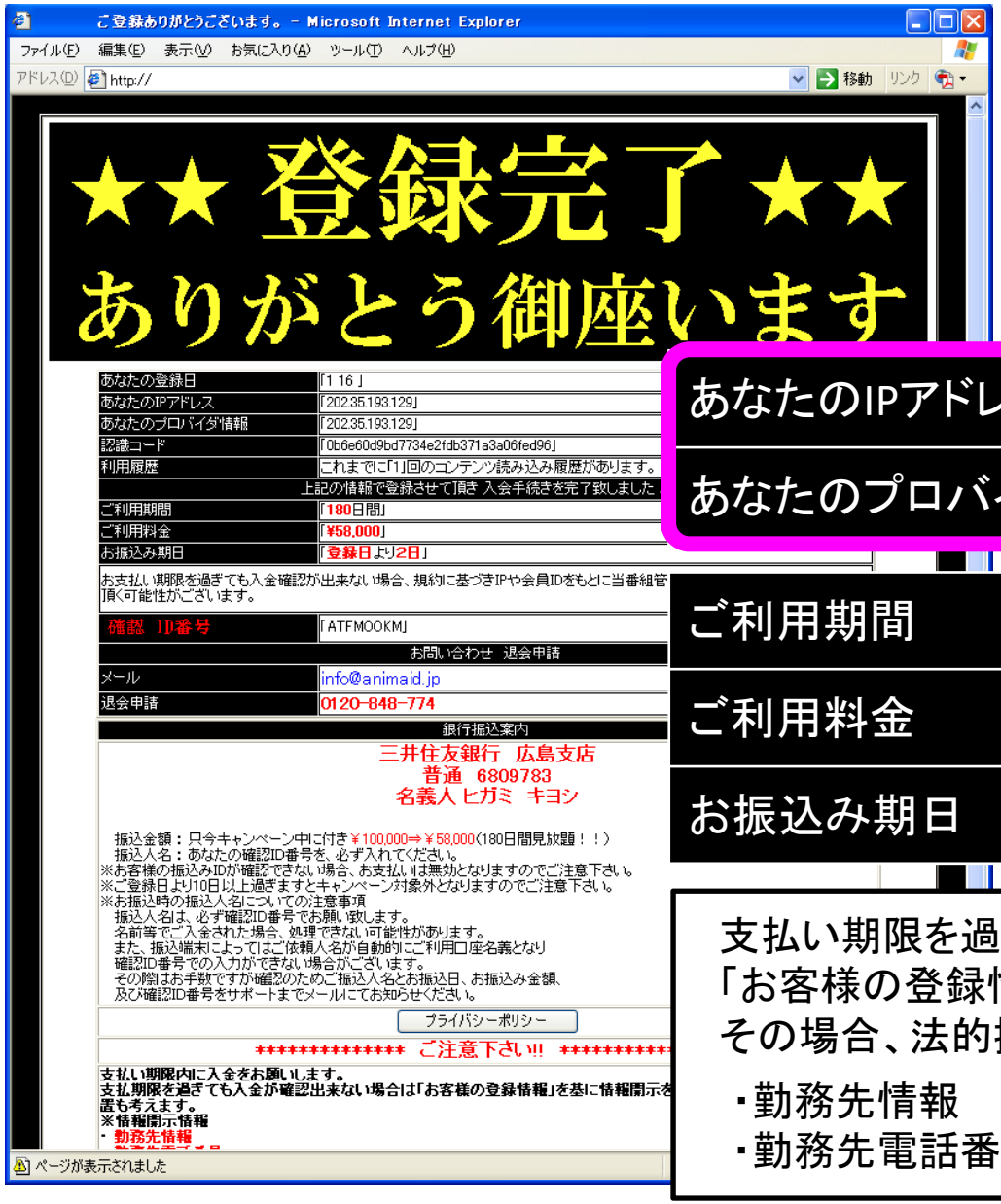
開示請求によって明らかに

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



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！

（ただのハッタリ）

（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

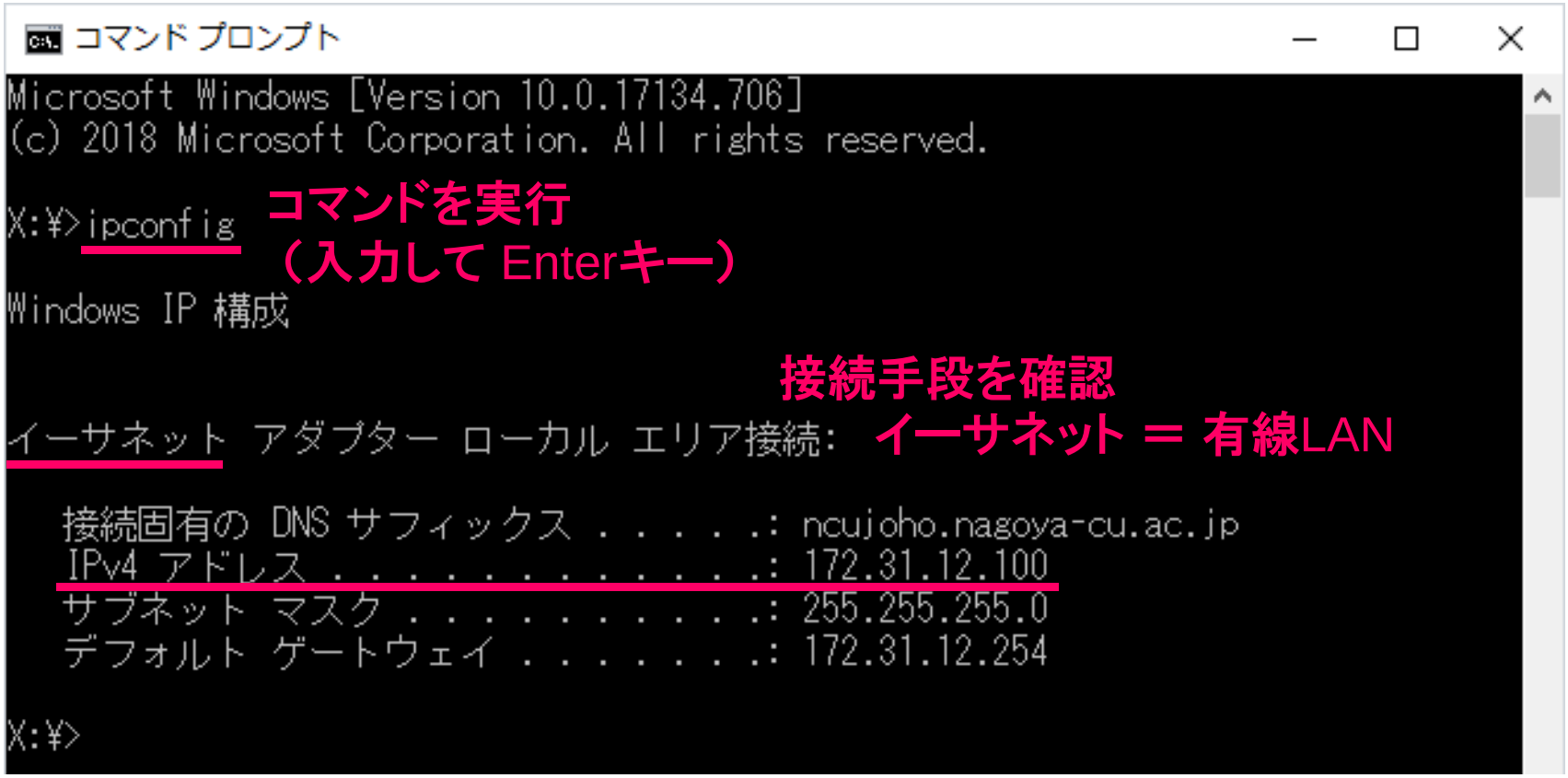
（４）ケータイ版、スマートフォン版サイトも存在

（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

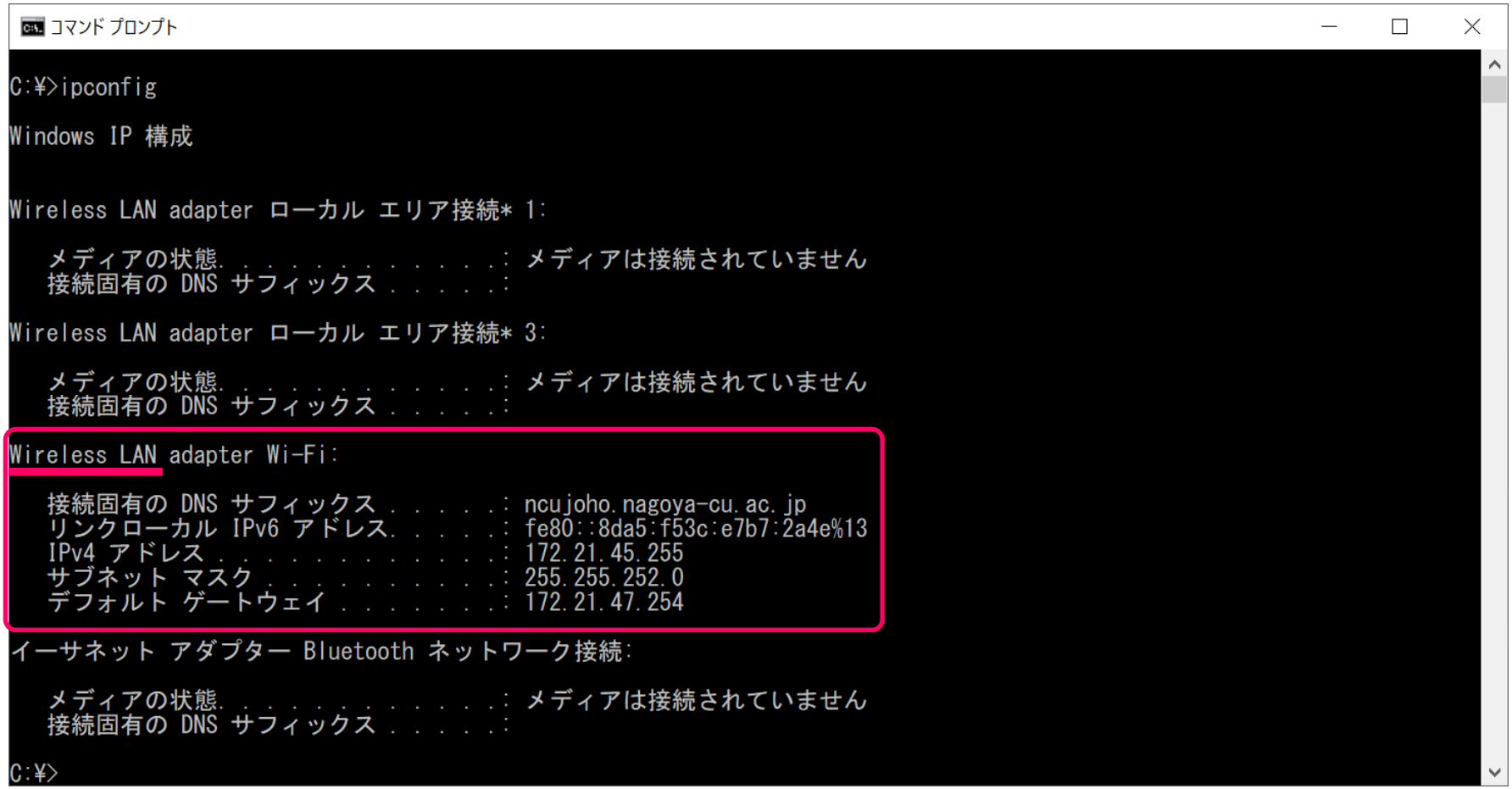
スタートメニュー
⇒ Windows システムツール
⇒ コマンドプロンプト

⇒ 本教室では Windows アクセサリ



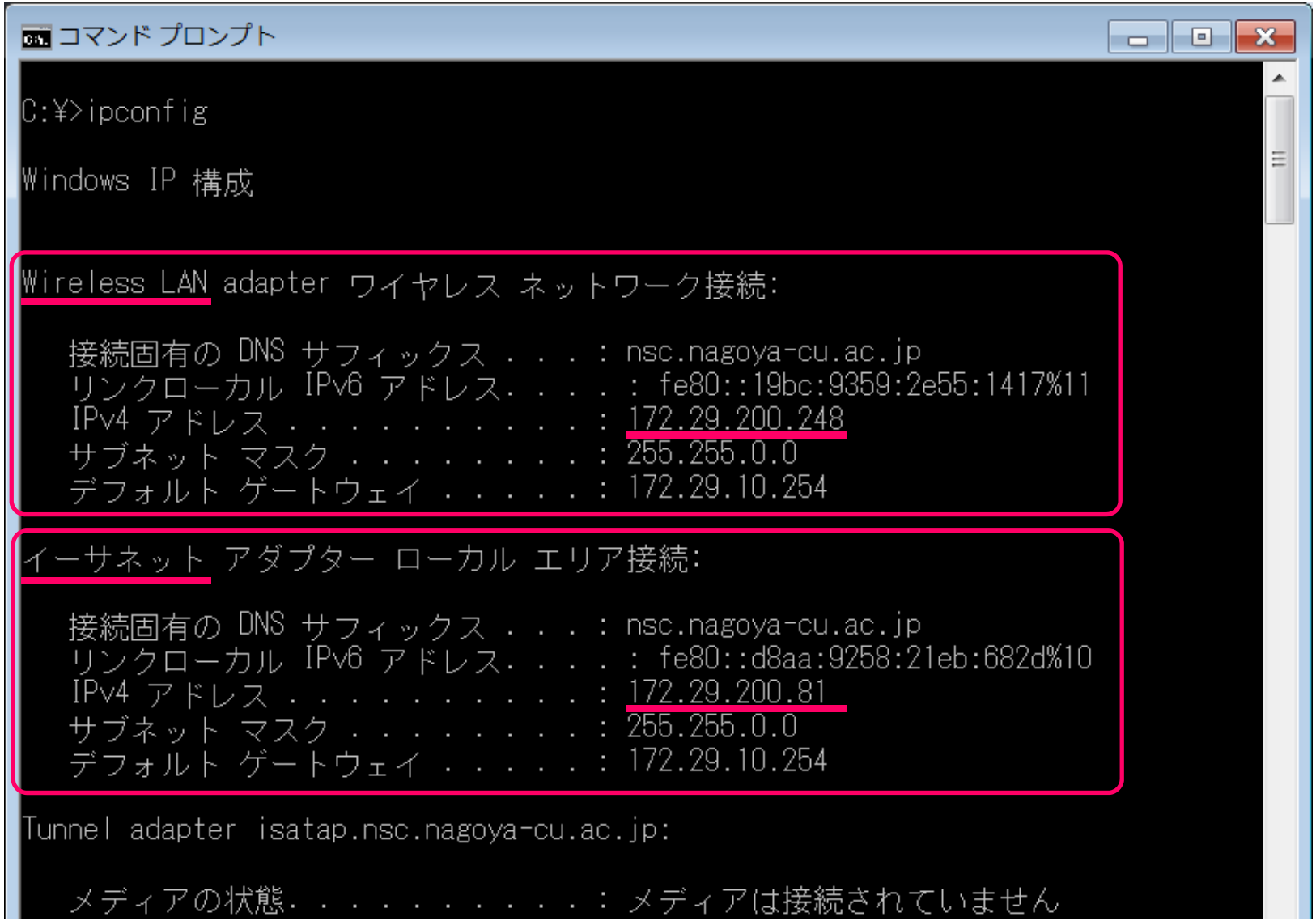
有線LAN接続のみのシンプルな構成

IPアドレスの調べ方



無線LAN（ncu wifi）のみ接続

IPアドレスの調べ方



有線LAN、無線LAN、双方を設定

IPアドレスの調べ方

設定

⇒ ネットワークとインターネット

⇒ ネットワークのプロパティを表示

⇒ 適切なアダプタの項目

IPアドレスの調べ方

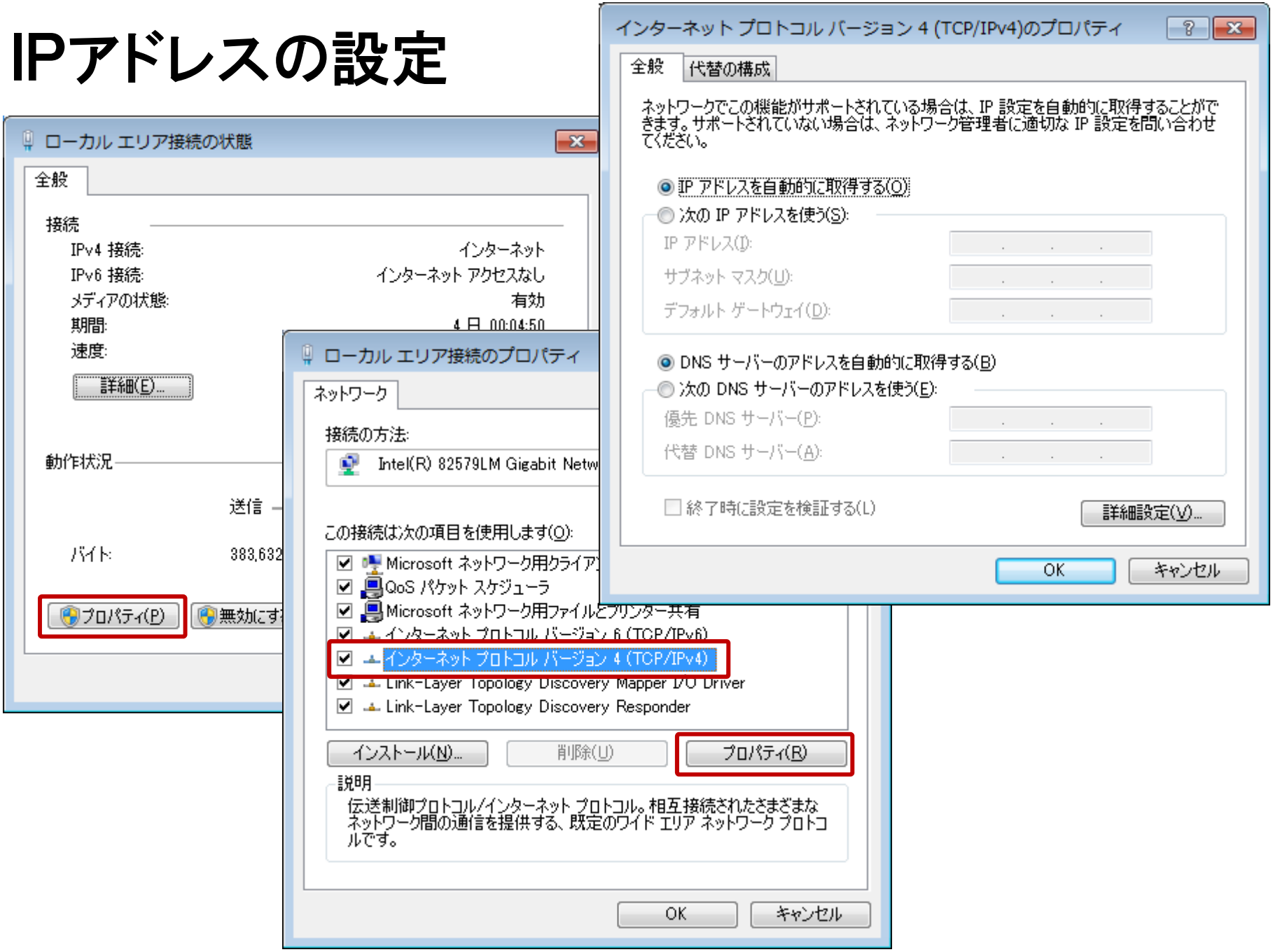
システムプロファイラ

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

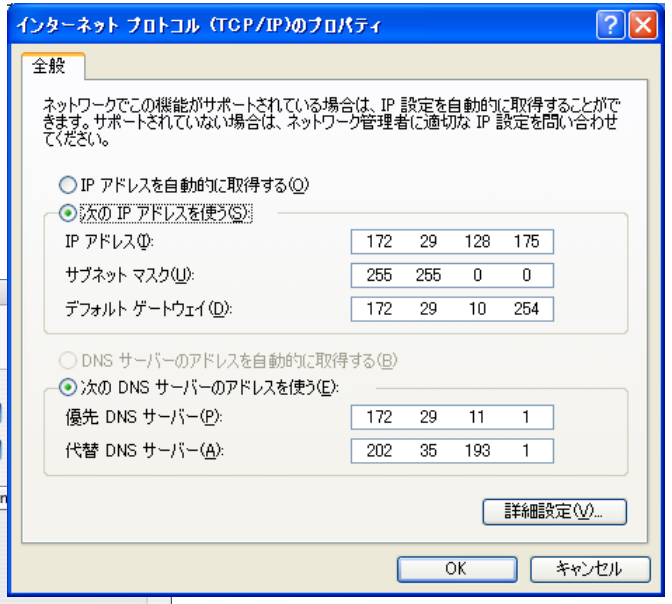
無線LANの場合
Wi-Fi を選択

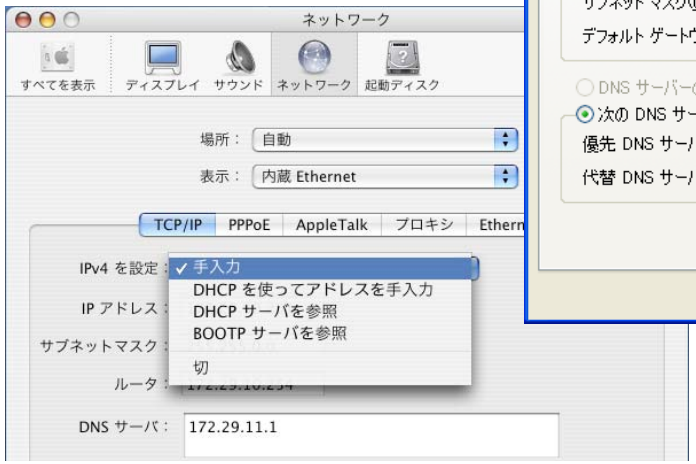
ネットワークユーティリティ
（ Spotlightで検索 ）

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:
速度:
詳細(E)...
動作状況
送信
バイト:
383,632
プロパティ(P)
無効にす
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
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





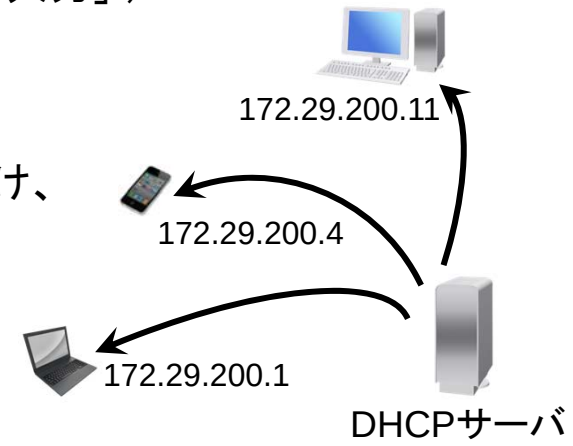
取得方法

- ✓ 接続プロバイダから貸与
- ✓ 所属組織から貸与

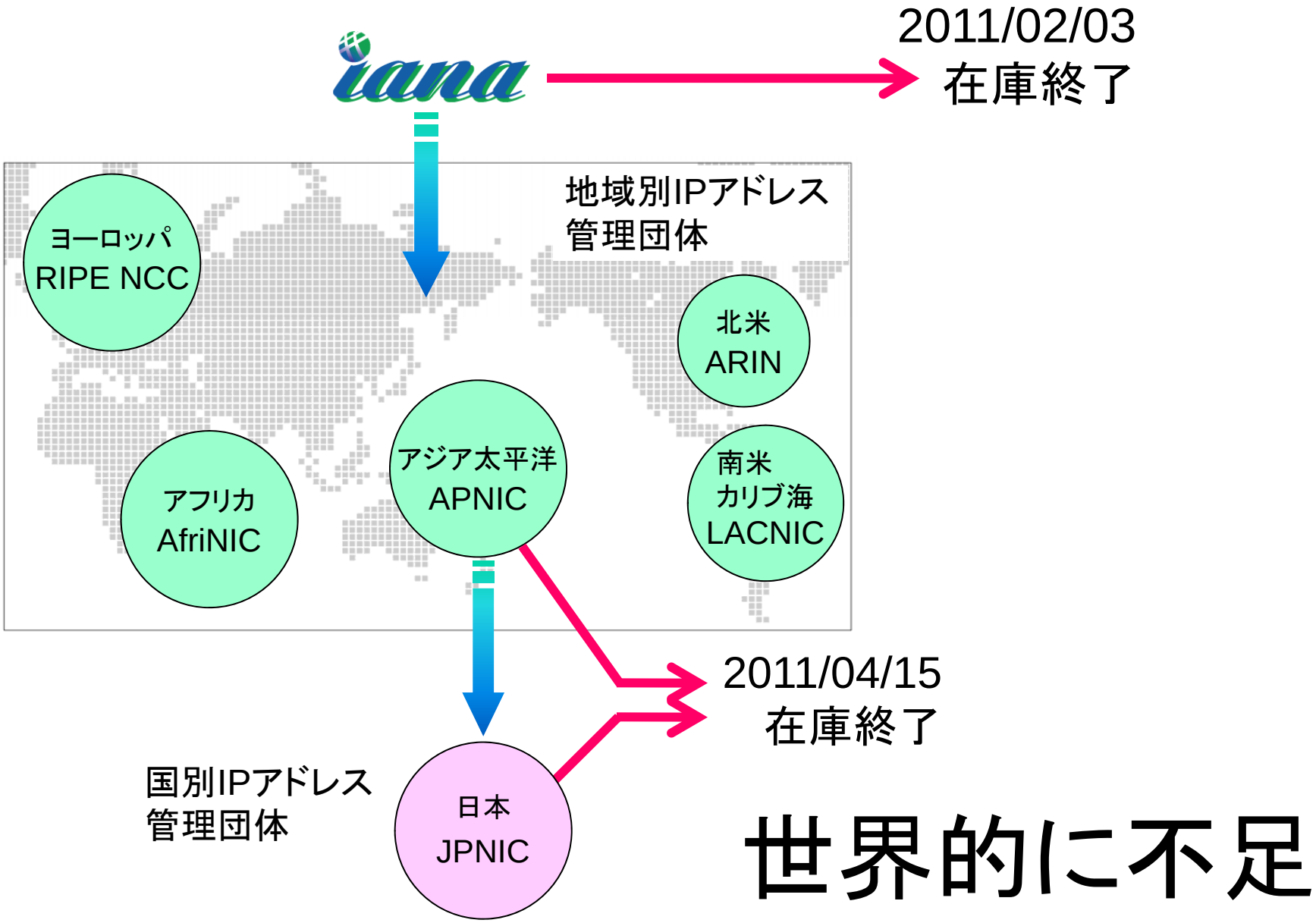
2通りの設定方法

- ✓ 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澗個 ）

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

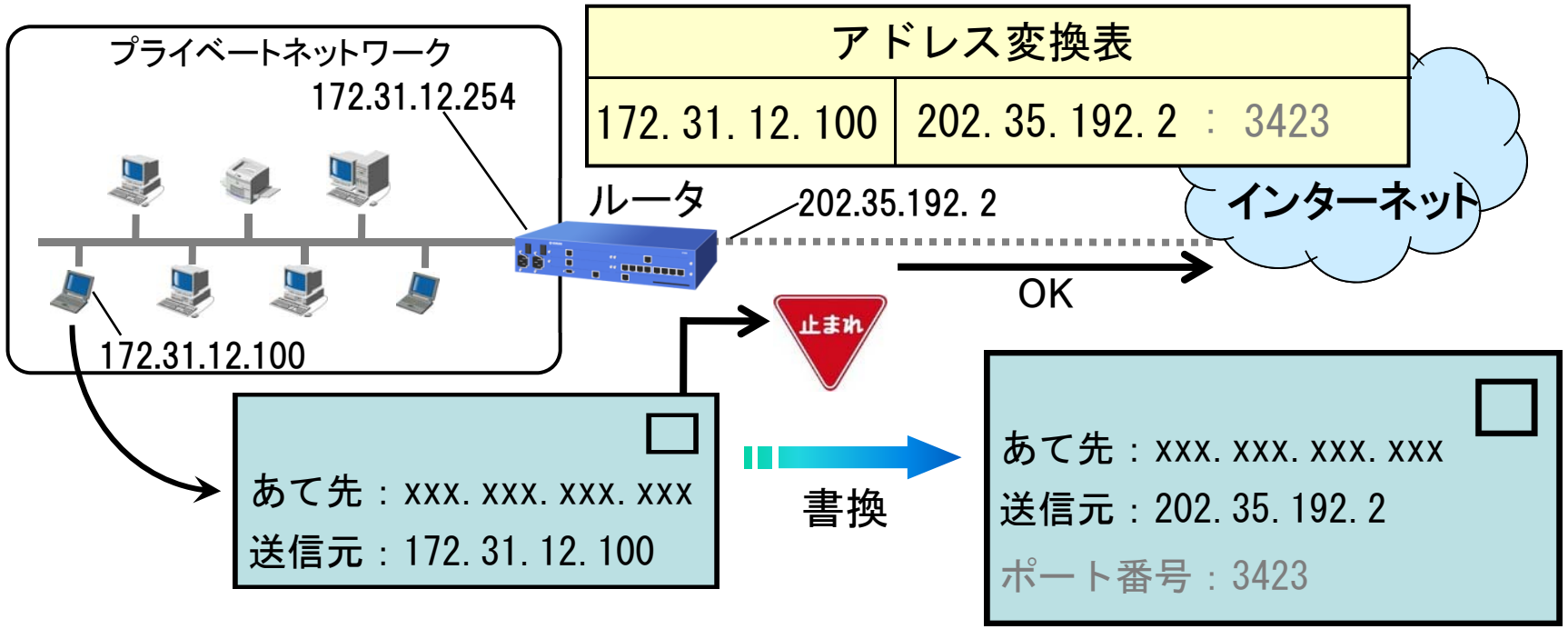
☞ プライベートアドレスとアドレス変換
（NAT：Network Address Translation）

グローバル　or　プライベート？

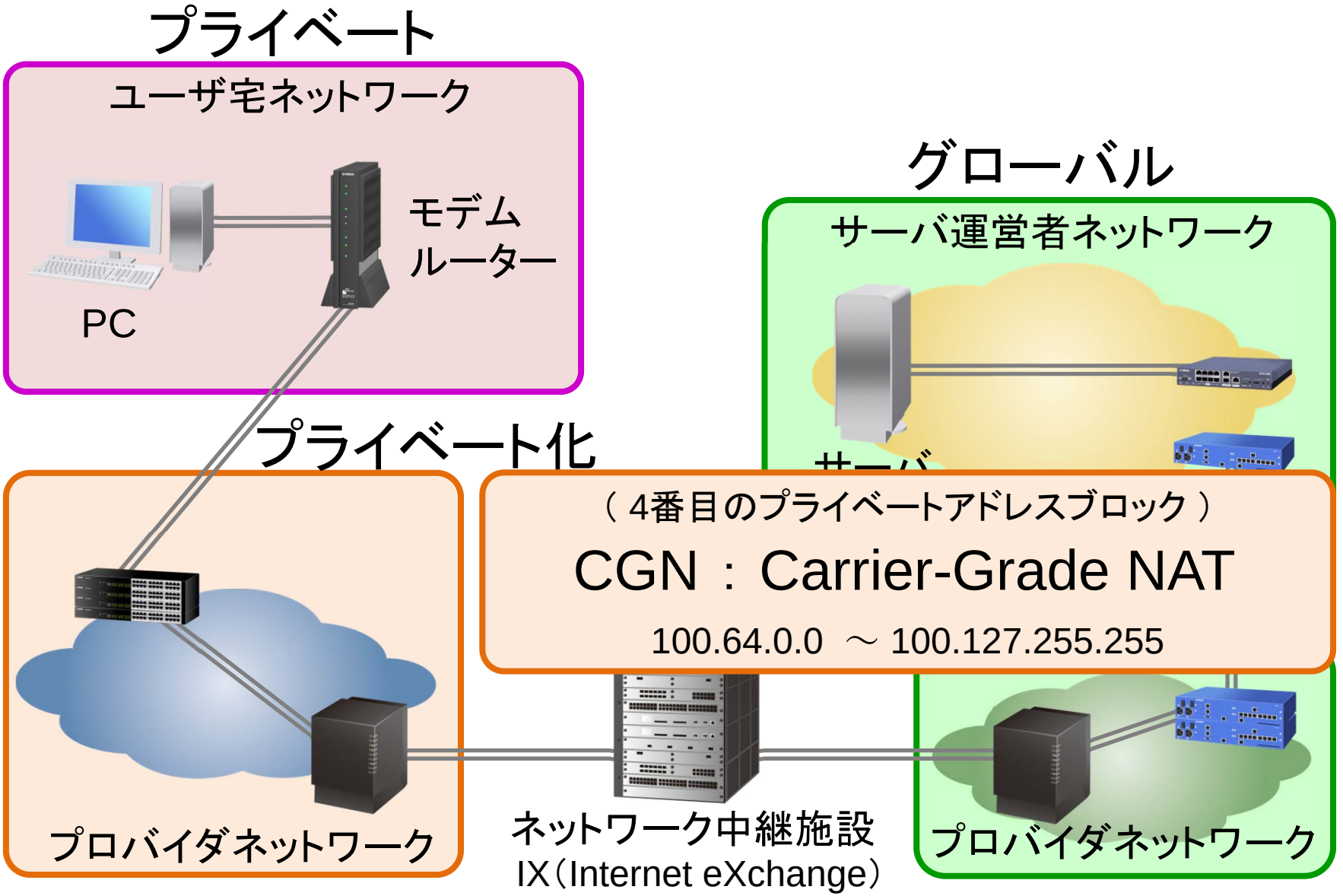
- グローバルIPアドレス
  ＝ 世界に通じるIPアドレス

- 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 ）

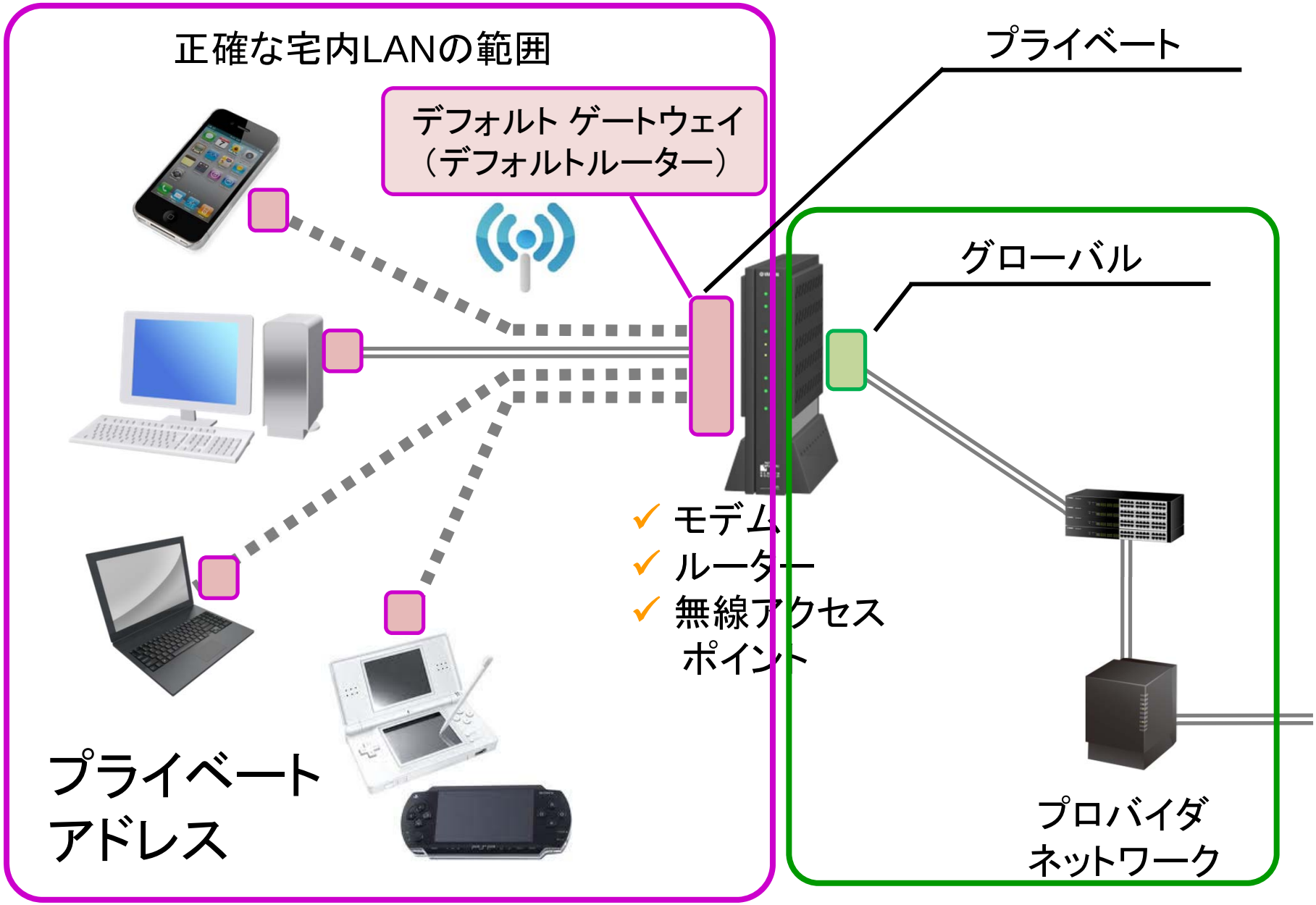
10.0.0.0　～ 10.255.255.255
172.16.0.0　～ 172.31.255.255
192.168.0.0　～ 192.168.255.255



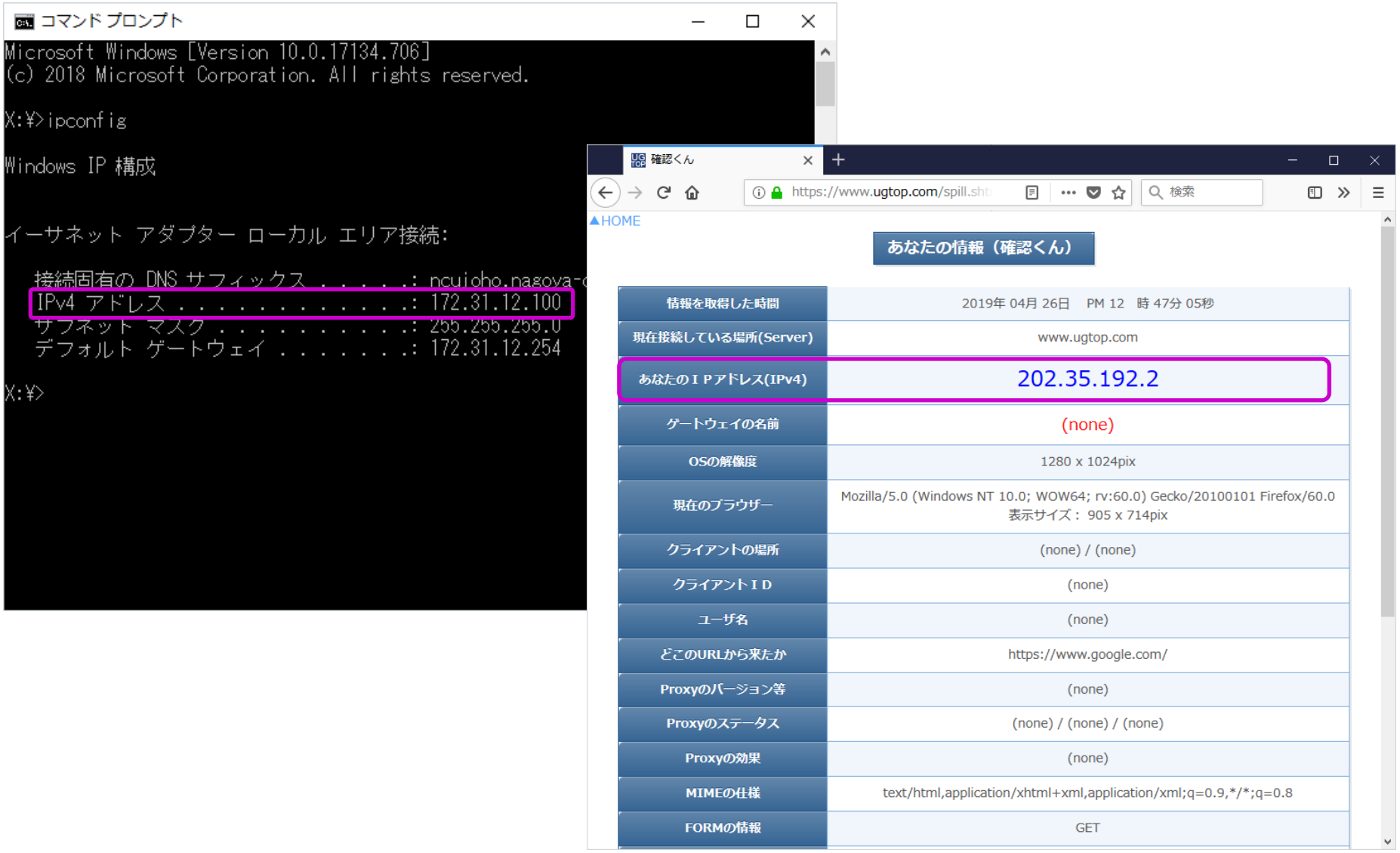
グローバル　or　プライベート？



どこにIPアドレスが付くか?



どこにIPアドレスが付くか?



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

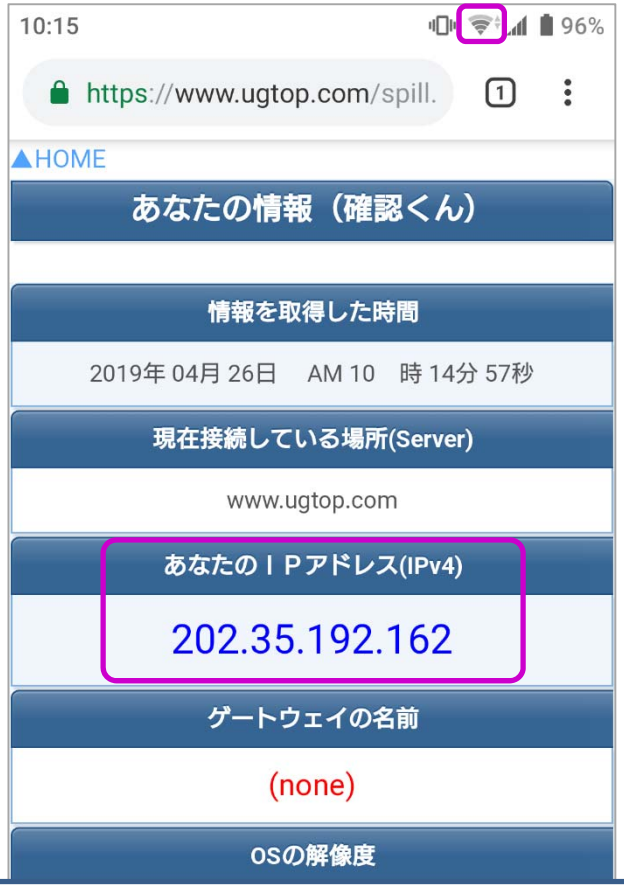
プライベートアドレス

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