Internetweek 2018

インターネットがつながる仕組み

2018.11.27

越後ネットワーク・オペレーターズ・グループ（ENOG）
株式会社新潟通信サービス
櫻井　佑樹

自己紹介

■ 氏名
　櫻井　佑樹（さくらい　ゆうき）

櫻井 佑樹(yuki.sakurai.7311)

聖ん(@hiji1ing)

■ 所属
　株式会社　新潟通信サービス
　新潟県新発田市
　地方ISP
　専用線・ホスティング・ハウジング・光未提供地域への独自FTTHの提供

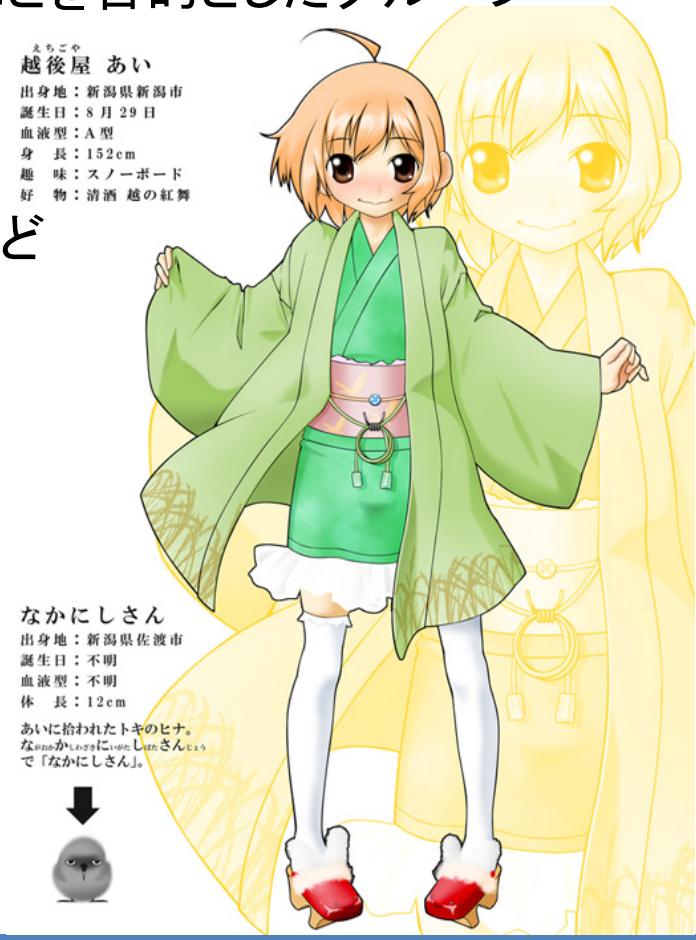
■ お仕事
　レイヤー1～レイヤー8まで何でも

●2010年よりENOG(越後ネットワーク・オペレーターズ・グループ)に参加

ENOG(The Echigo Network Operators' Group)

- 「越後ネットワーク・オペレーターズ・グループ(ENOG)」は、インターネットに於ける技術的事項、および、それにまつわるオペレーションに関する事項を議論、検討、紹介することにより新潟県内、およびその近辺のインターネット技術者、および、利用者に貢献することを目的としたグループです。
- 2ヵ月に1回ペースの勉強会
  過去53回開催
  新発田・新潟・三条・長岡・柏崎・上越・佐渡など
  県内のみならず、県外・東京からも多数参加

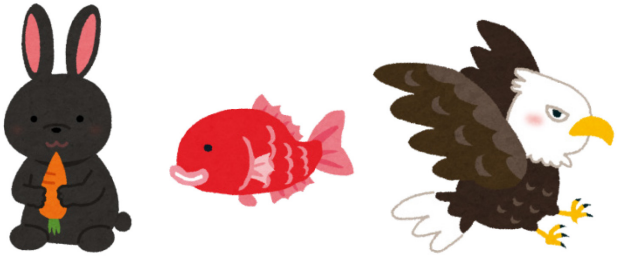
- Echigo-IX の運営・管理

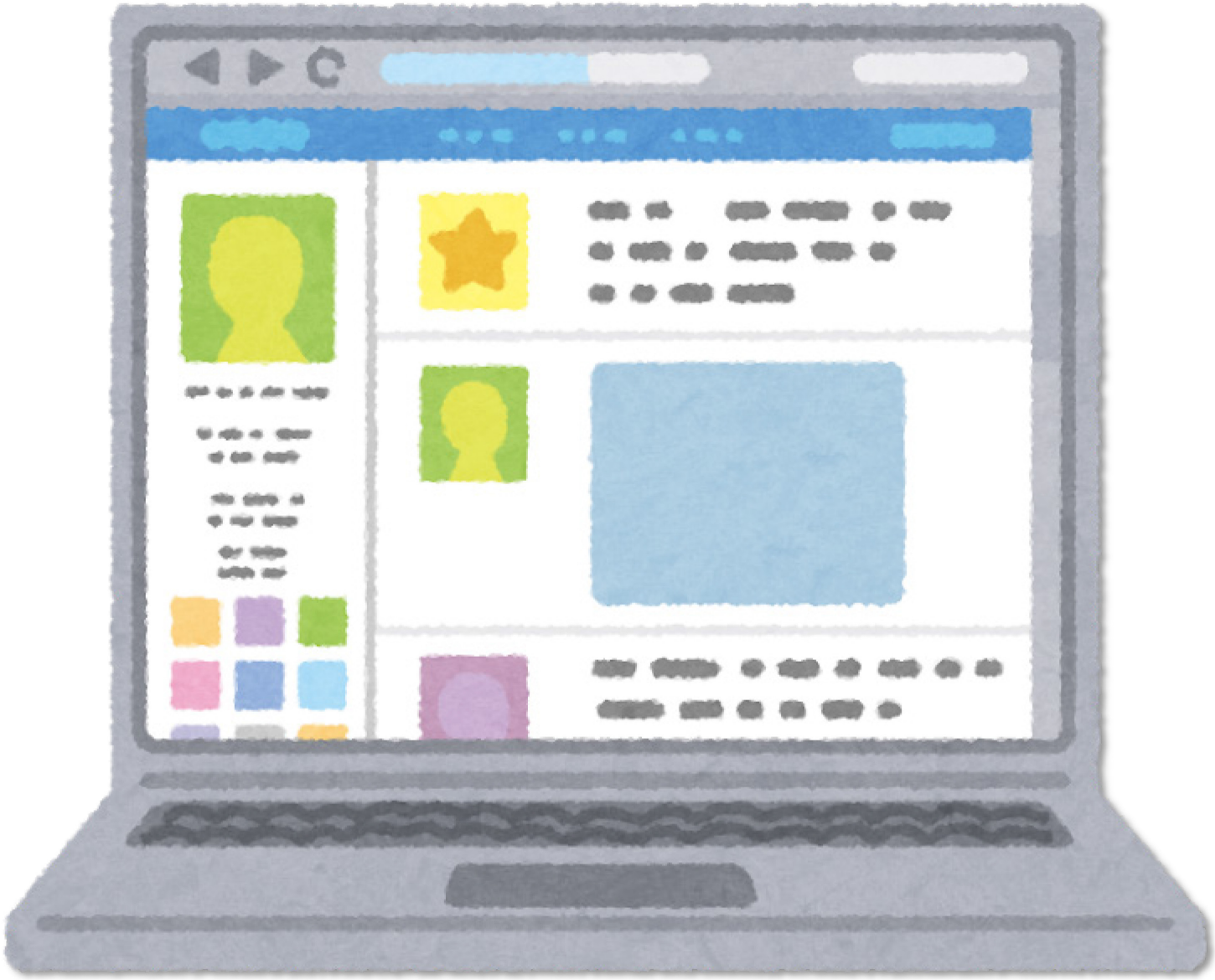


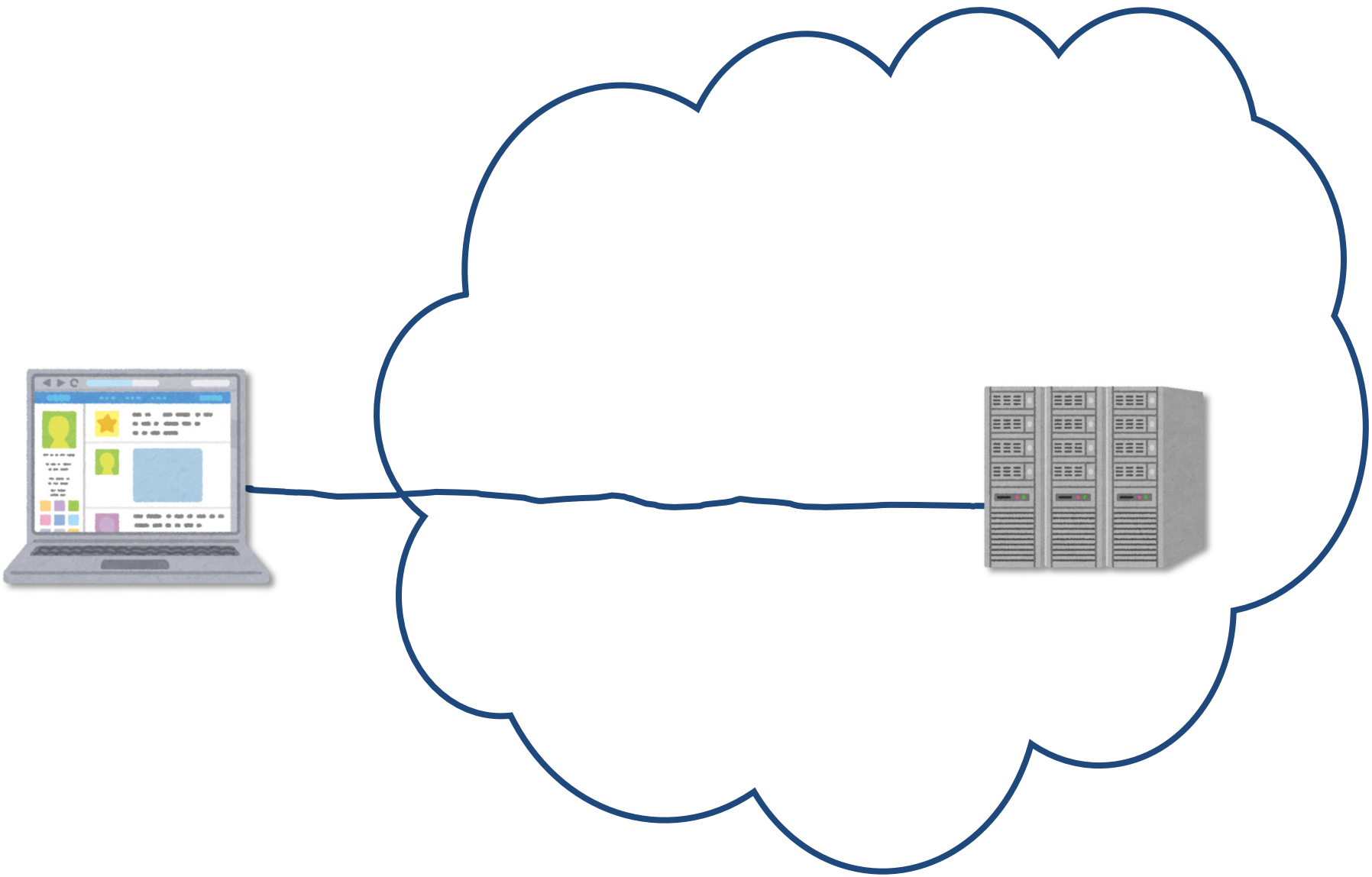
注意事項

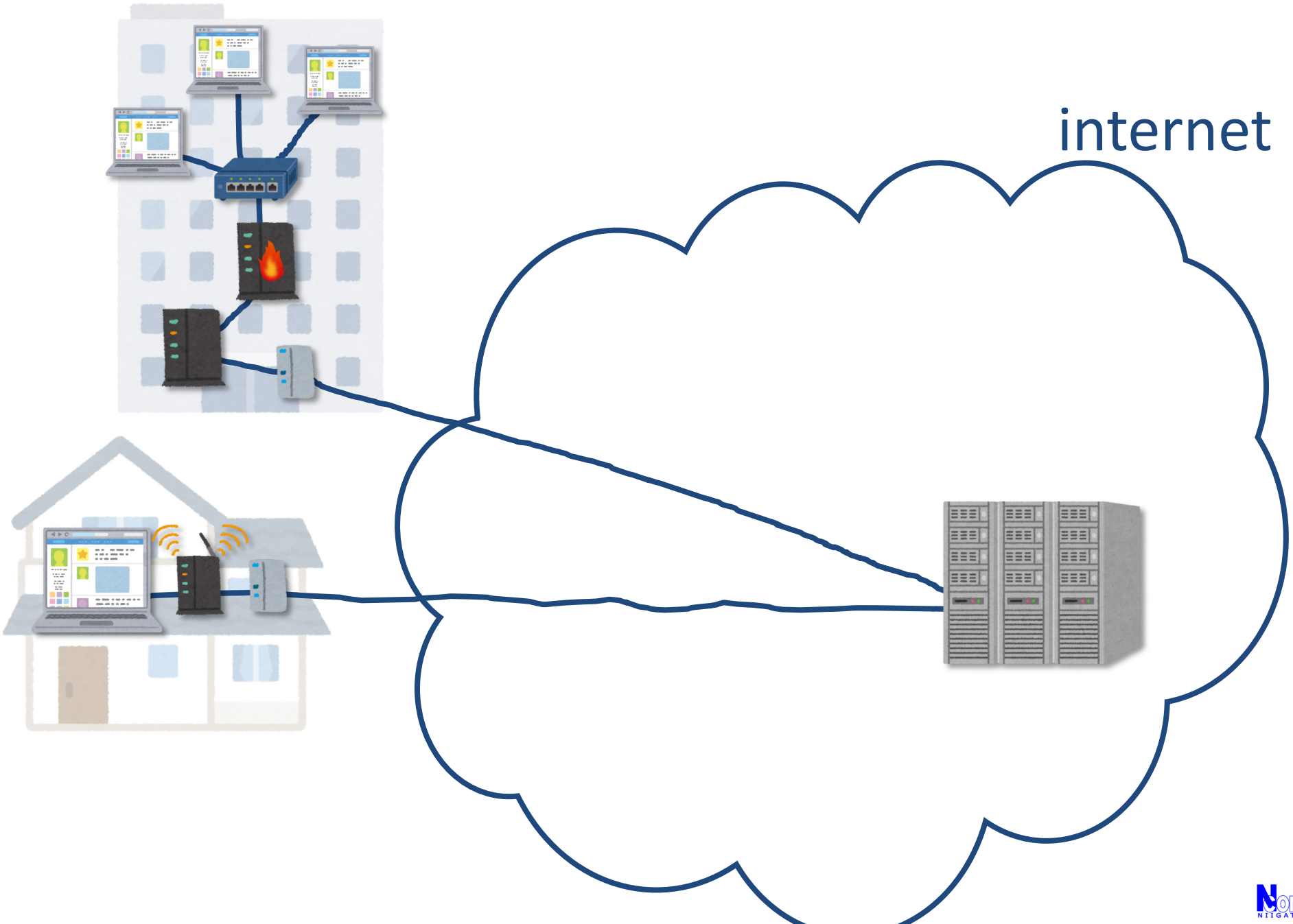
- 特定の業者名が出ることがありますが、広告・宣伝する意図はありません。あくまで例として聞いてください。

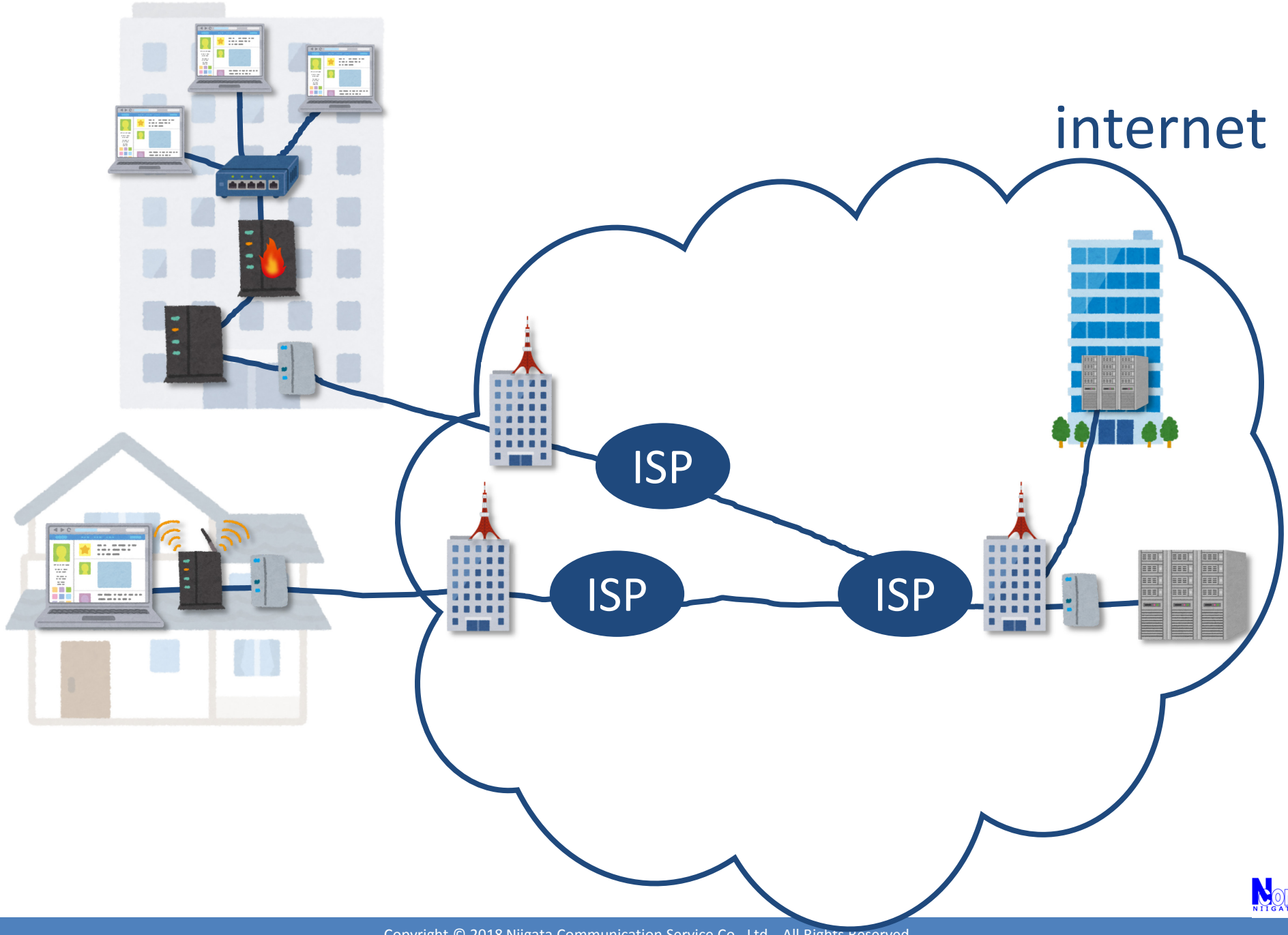
- できるだけ内容をシンプルに、わかりやすくするために、解説のニュアンスが実際の内容と異なる場合があるかもしれません。JAR〇には電話せず、あとでこっそりググったり上司に確認したりしてください。

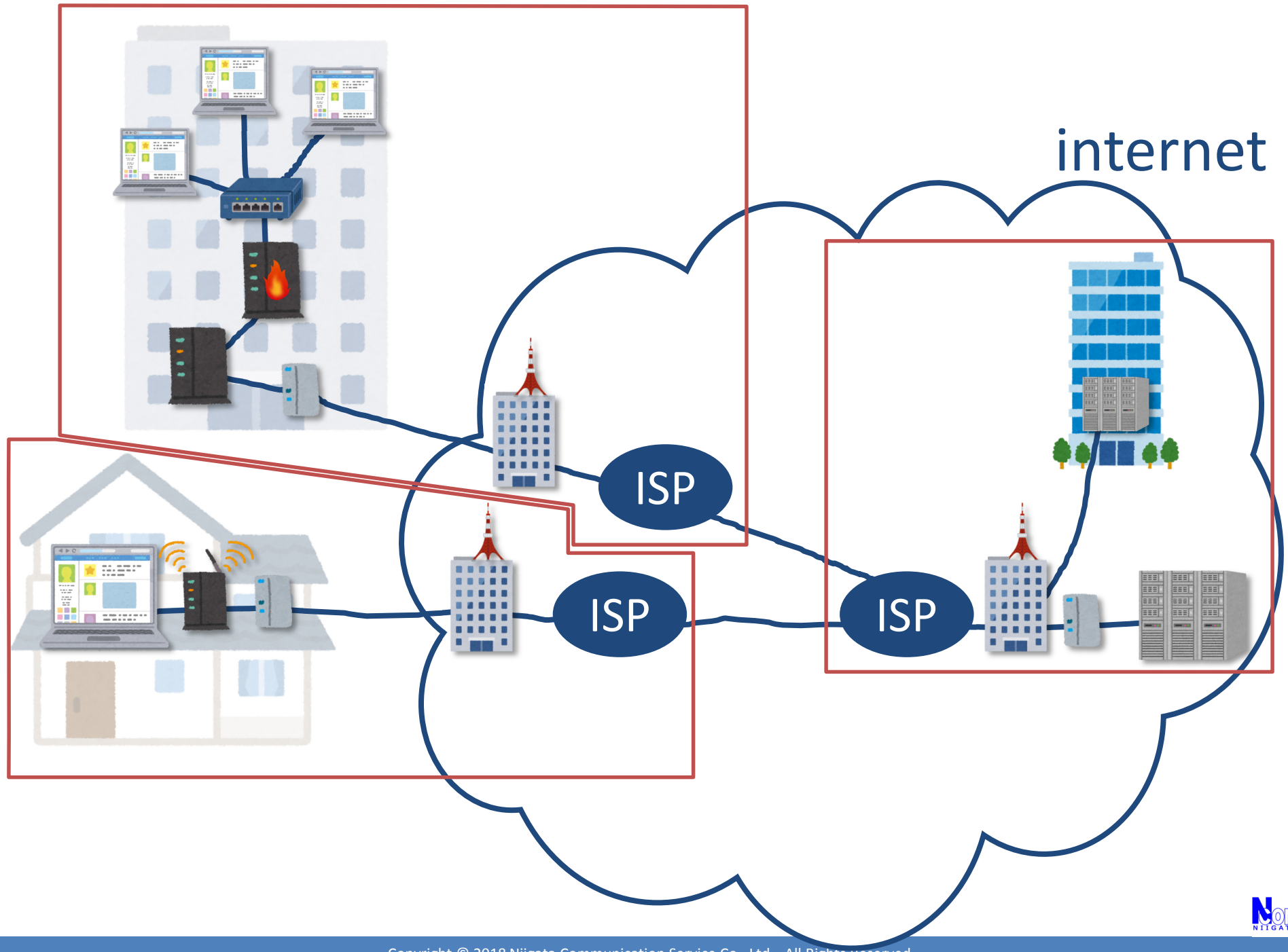


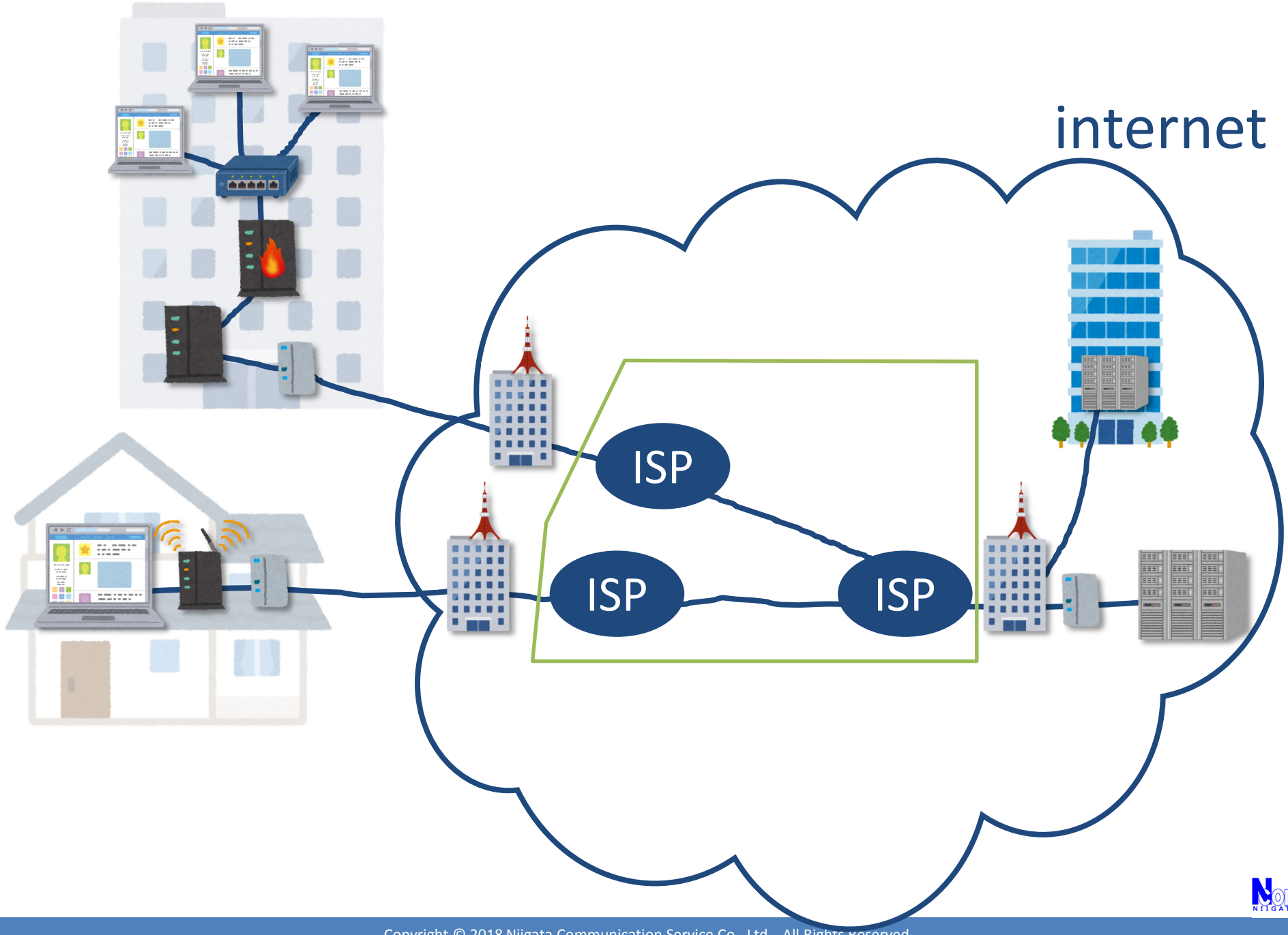




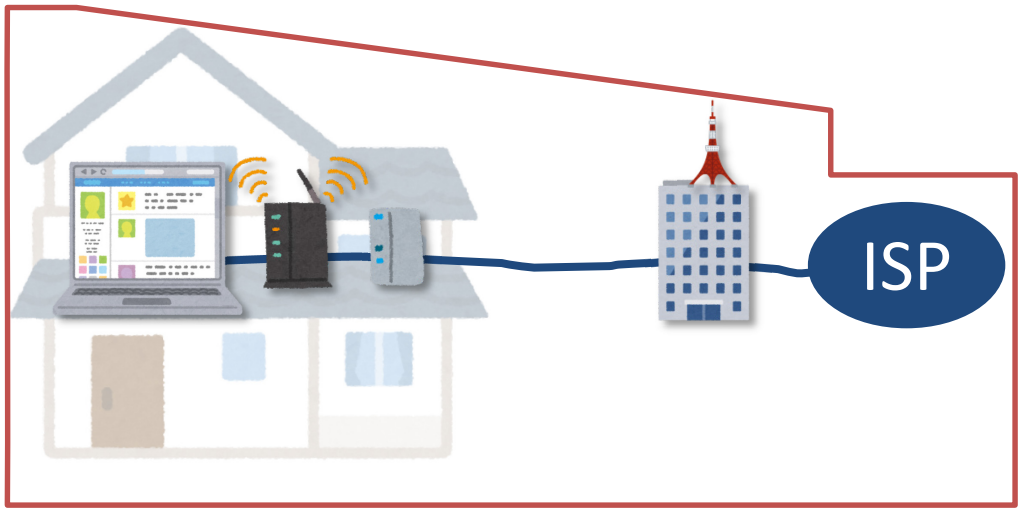








端末～ISPまでのお話



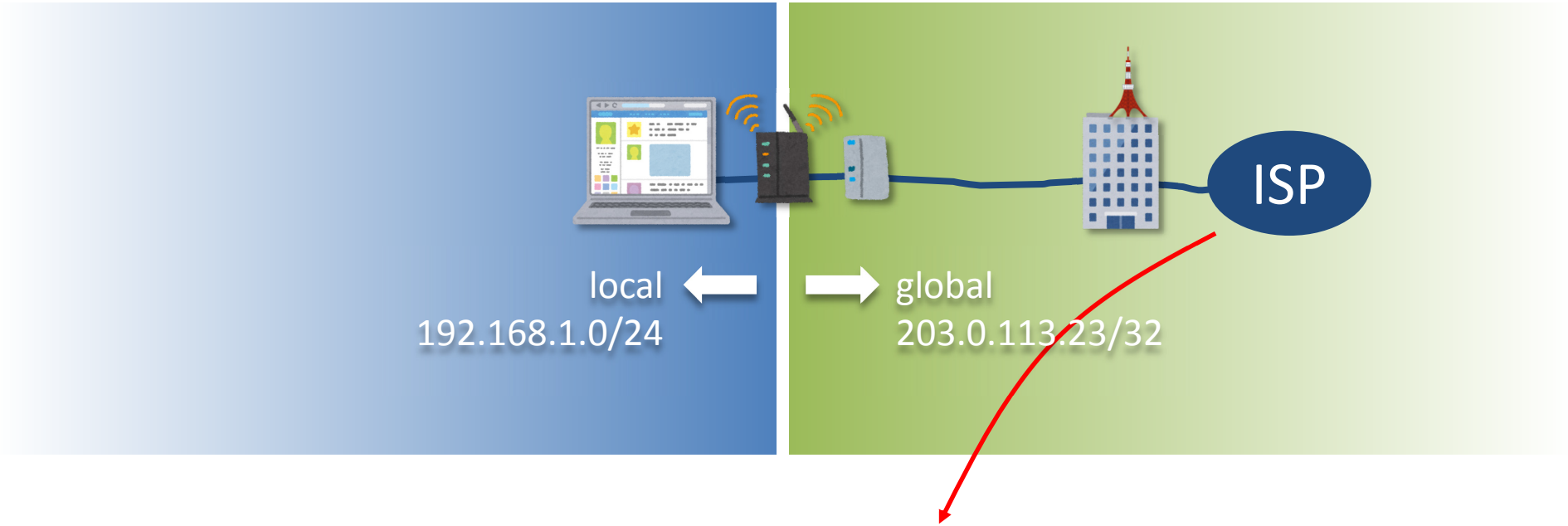
プレイヤー

回線事業者

ISP

お客様サポート

IPアドレスをもらおう

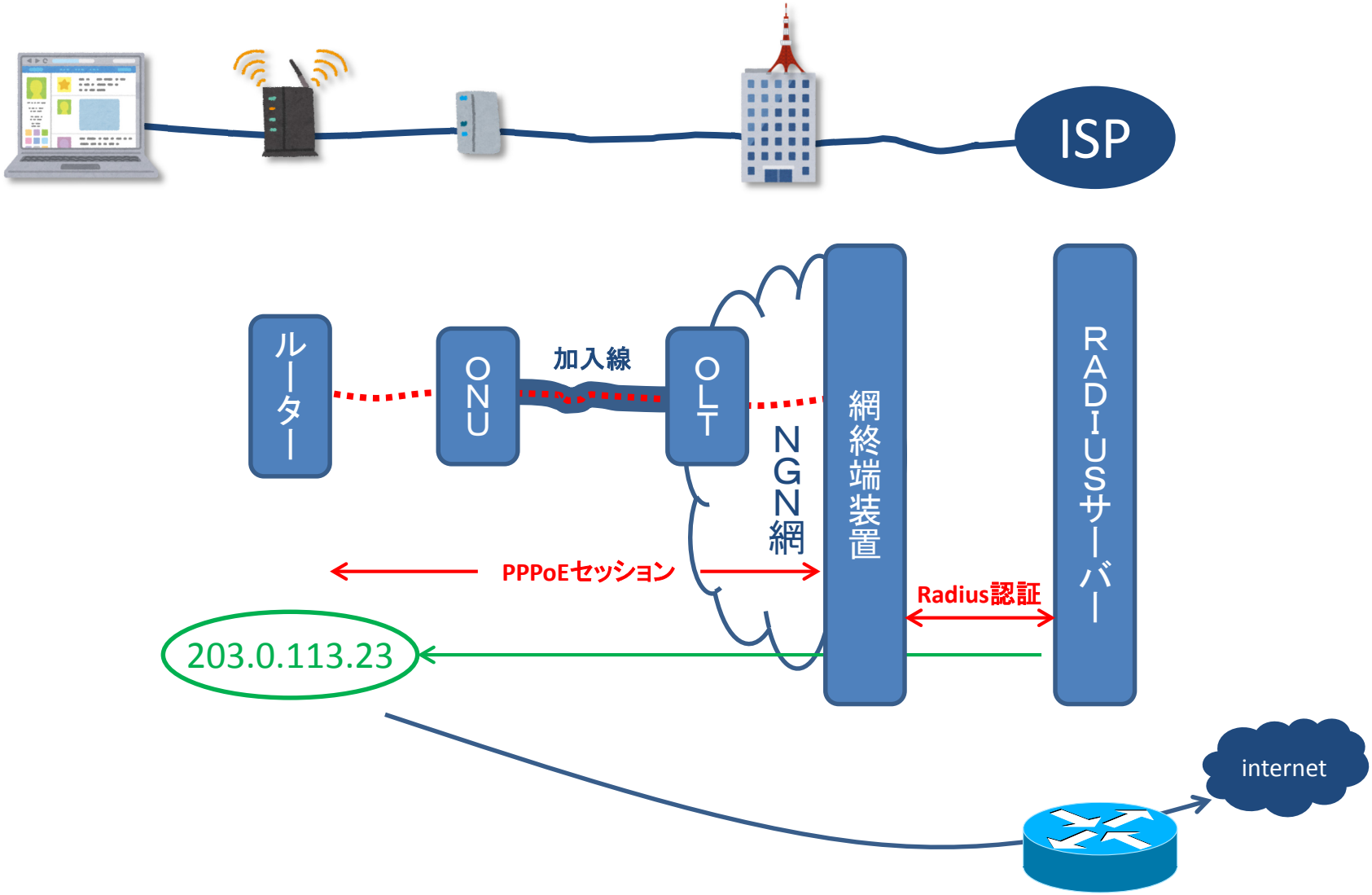


PPPoE

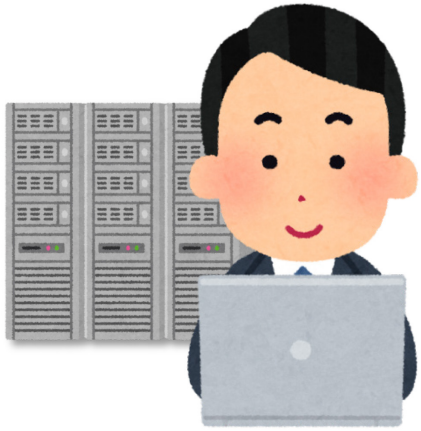
Point-to-**P**oint **P**rotocol **o**ver **E**thernet

「ユーザー名」と「パスワード」を用いて認証することで
インターネットにつながるようにしてくれるすごいヤツ

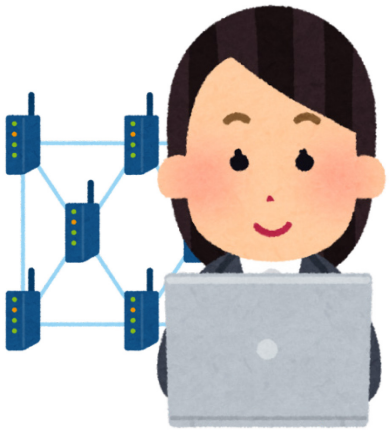
PPPoE(フレッツ光の場合)



プレイヤー



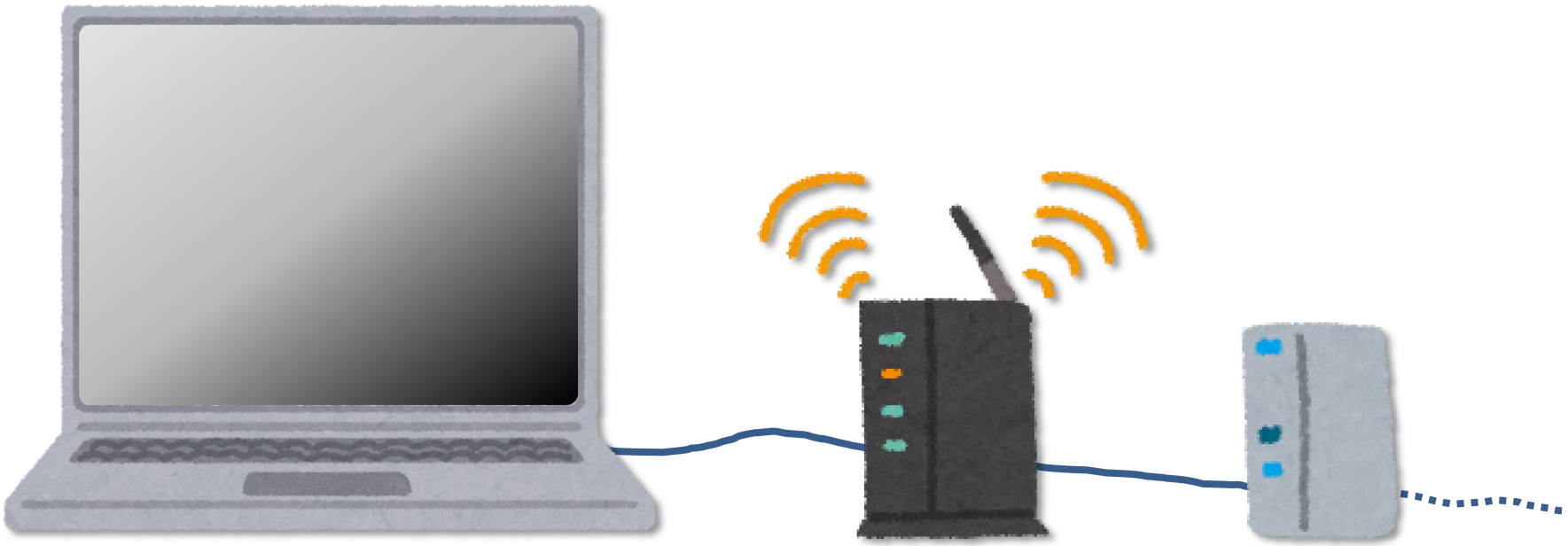
サーバーエンジニア



ネットワークエンジニア

準備はできた

準備はできた



ん？

http://example.com

DNSによる

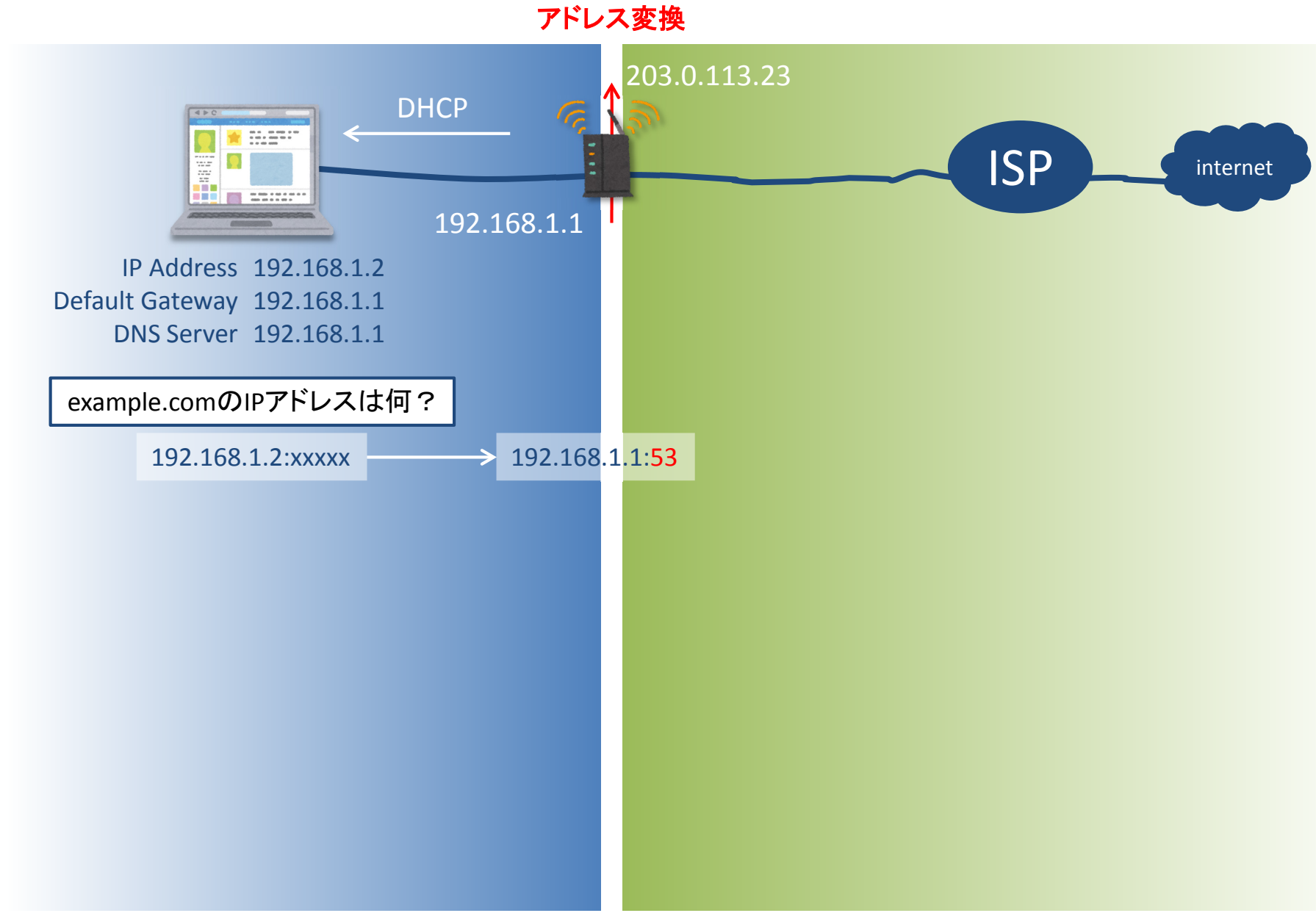
名前解決

http://example.com

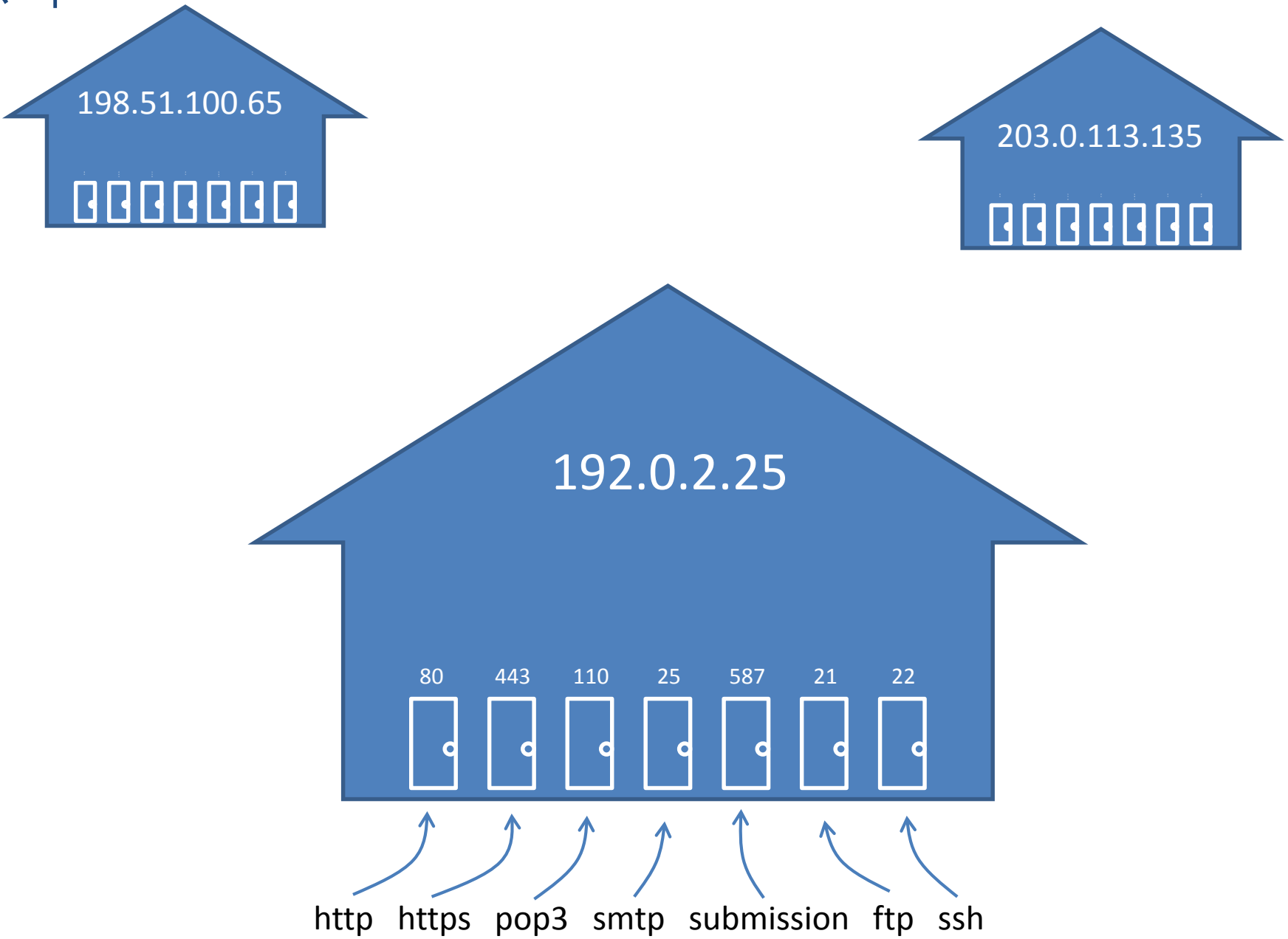
↓

IPアドレス

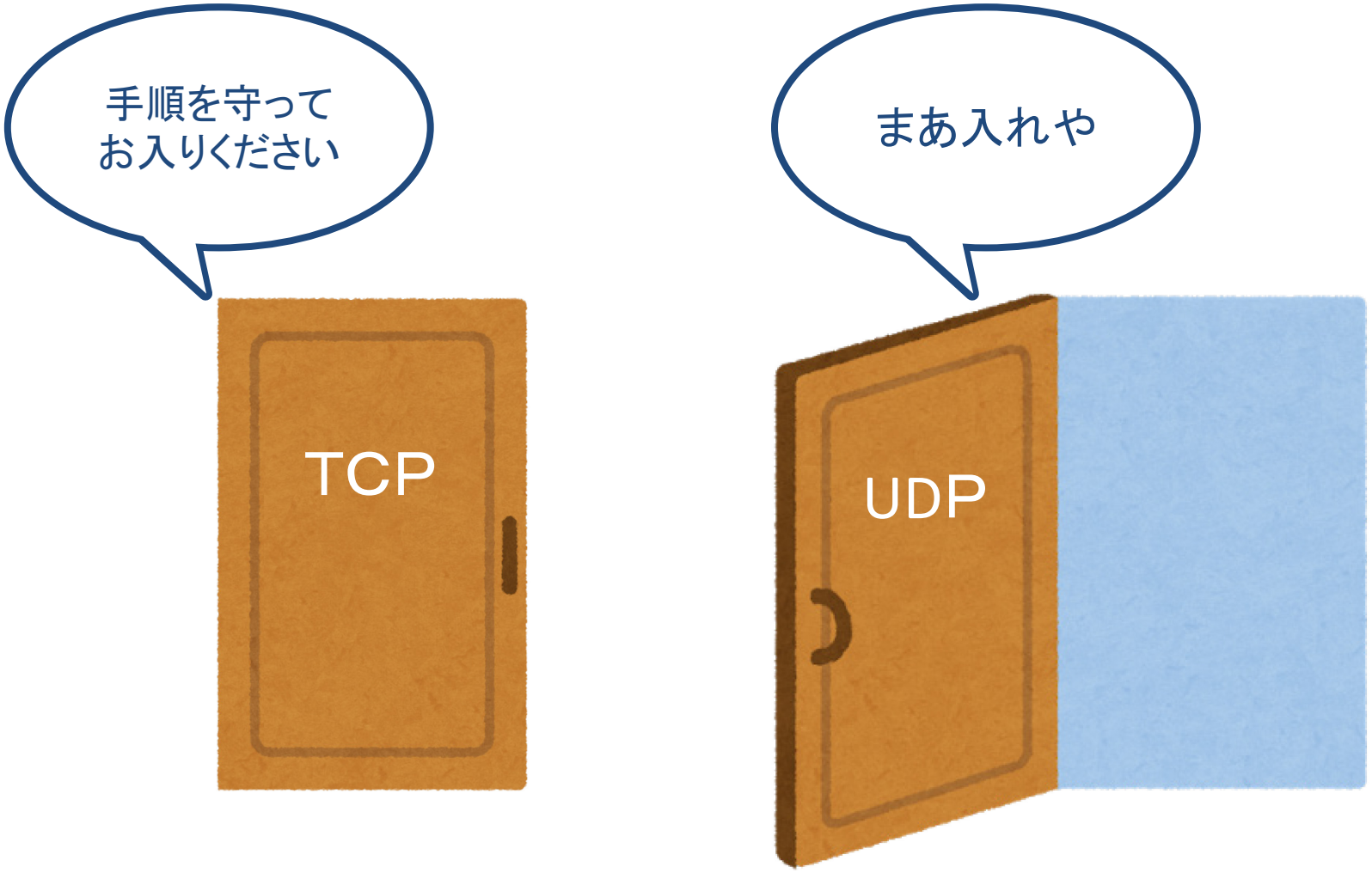
名前解決



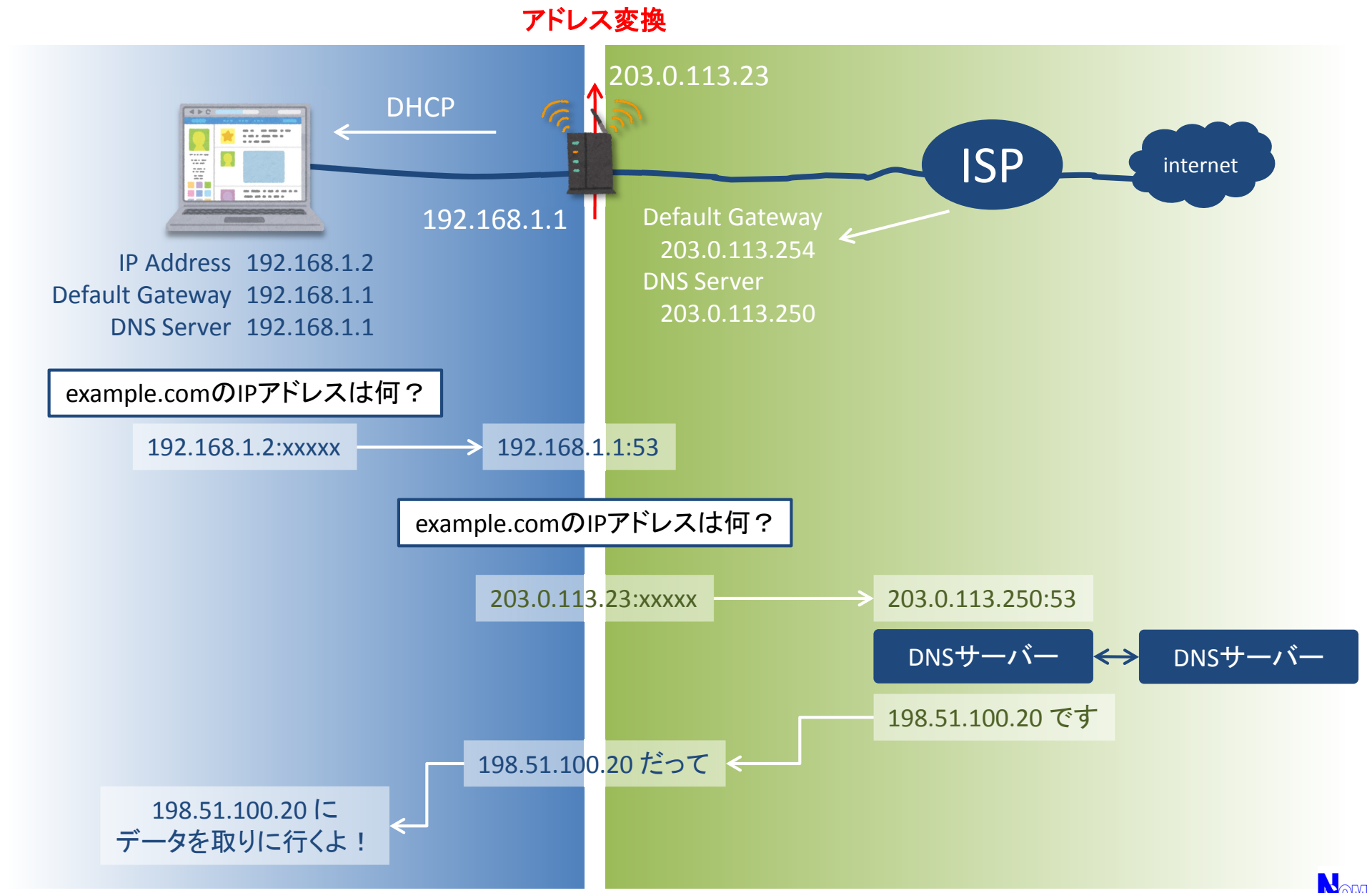
ポート



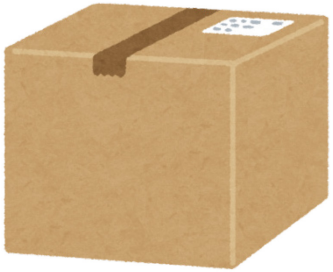
レイヤー4：トランスポート層



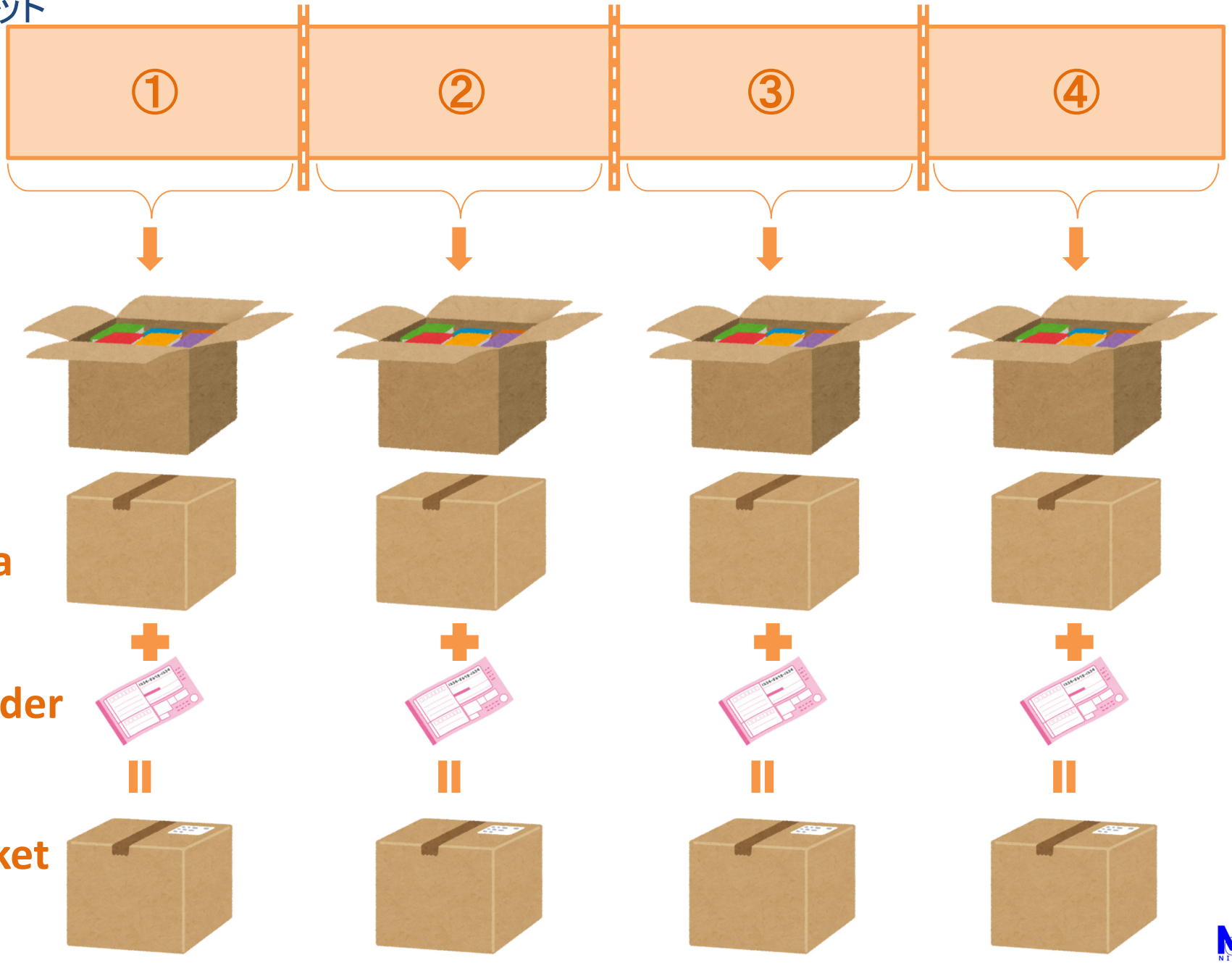
名前解決



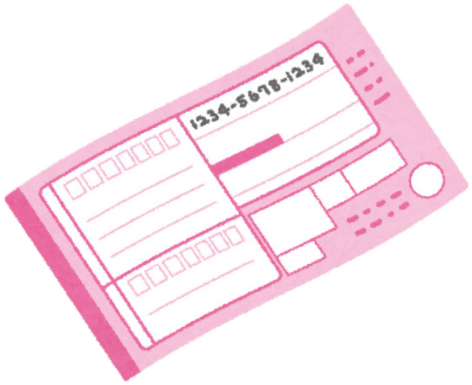
パケット



パケット

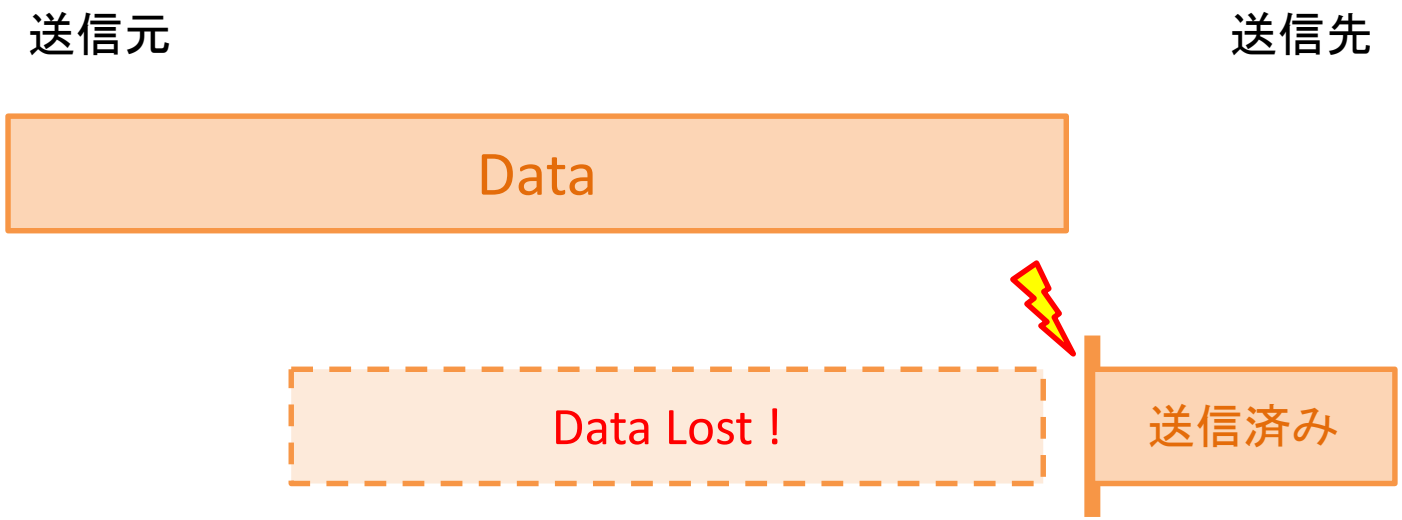


ヘッダ

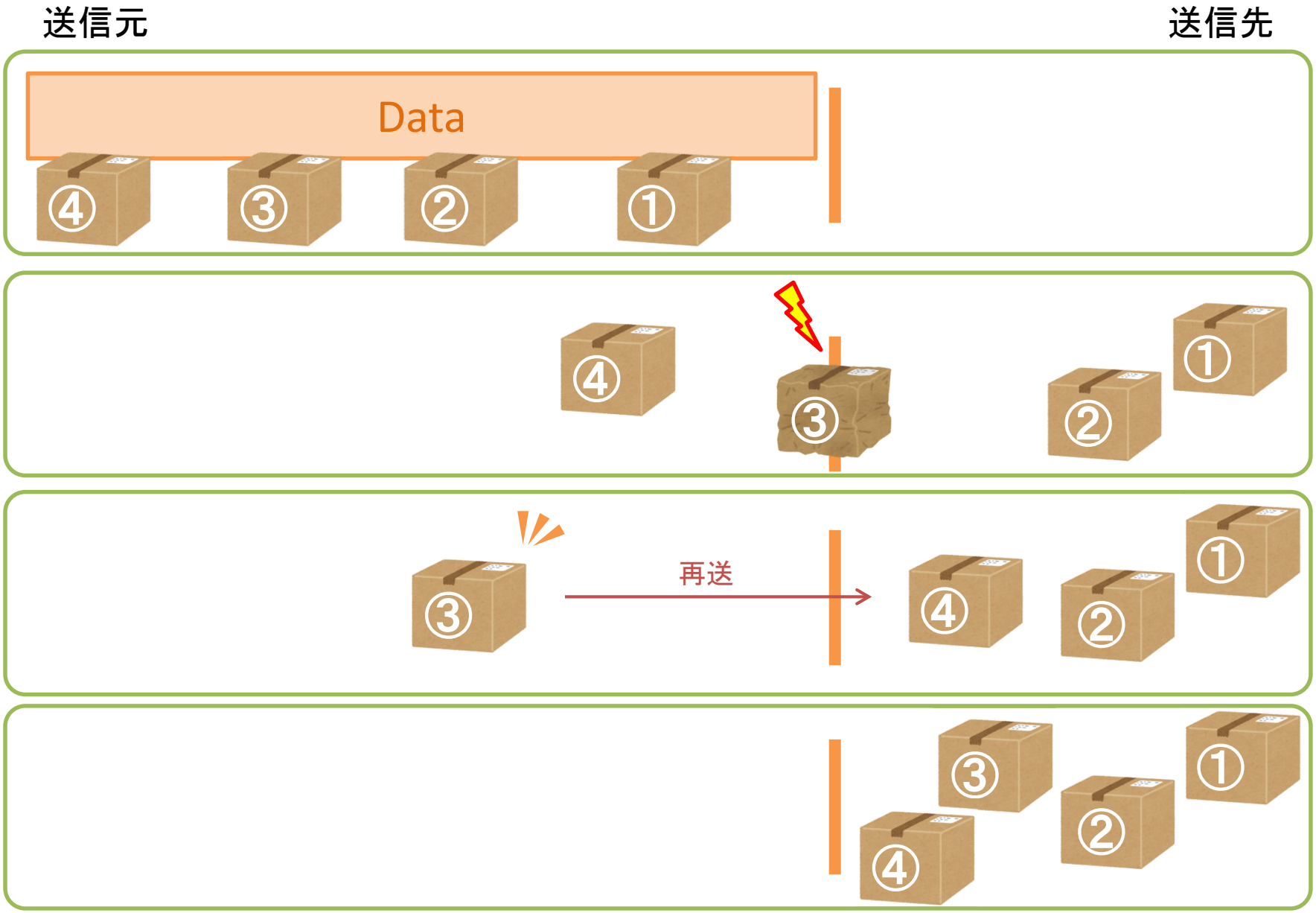


フィールド	内容
バージョン	IPのバージョンは4だよ
ヘッダ長	オプション使わないので20Byteだよ
サービスタイプ	略
全長	このパケットは全部で32KByteだよ
ID	分割されたパケットのうちの②番だよ
フラグ	略
フラグメントオフセット	略
TTL	略
プロトコル番号	TCPのパケットだよ
ヘッダチェックサム	ヘッダが壊れてないか確認するよ
送信元IP	203.0.113.23 からのパケットだよ
送信先IP	198.51.100.20 行きのパケットだよ
オプション	略

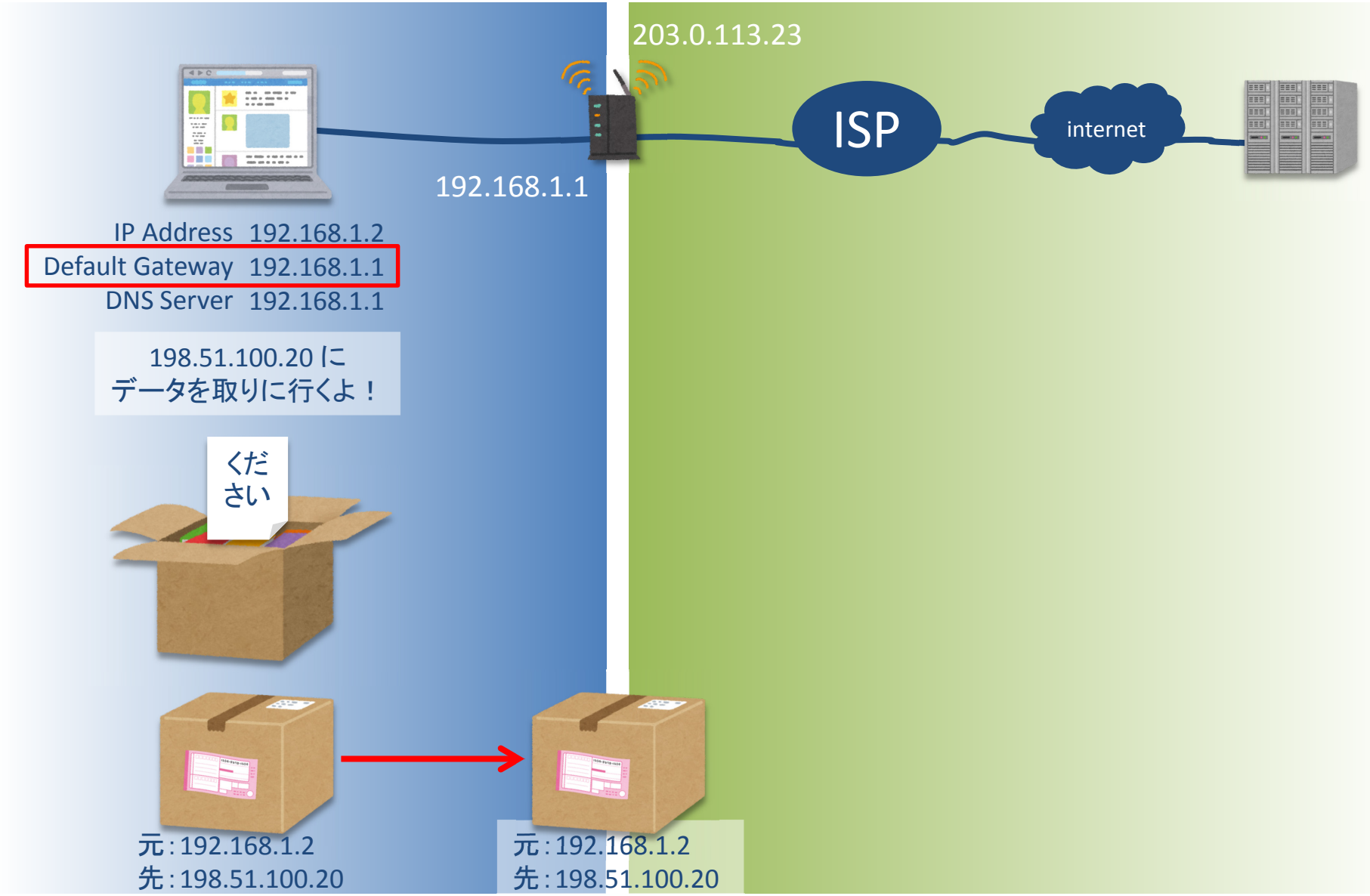
パケットにしないと



パケットなら



パケットを送ろう



パケットを送ろう

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

192.168.1.1

203.0.113.23

ISP

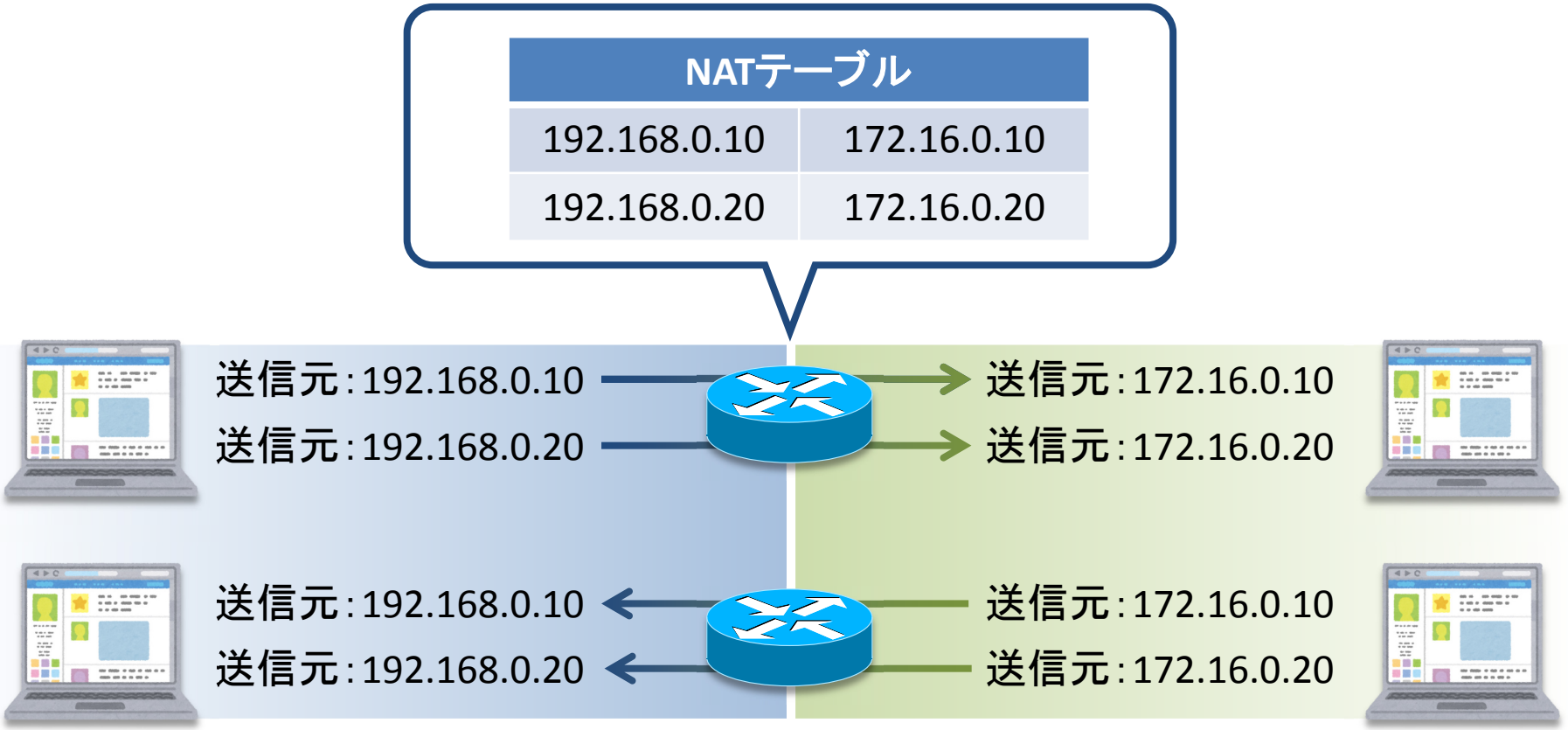
internet

NAT(NAPT)

元：203.0.113.23
先：198.51.100.20

NAT(Network Address Translation)

ある範囲のIPアドレスを別の範囲のIPアドレスと対応付け、
送受信するIPパケットのヘッダ部のIPアドレスを、
対応付けられた範囲で変換する技術



変換には1対1のアドレス数が必要

NAPT(Network Address and Port Translation)

別名「IPマスカレード(IP Masquerade)」

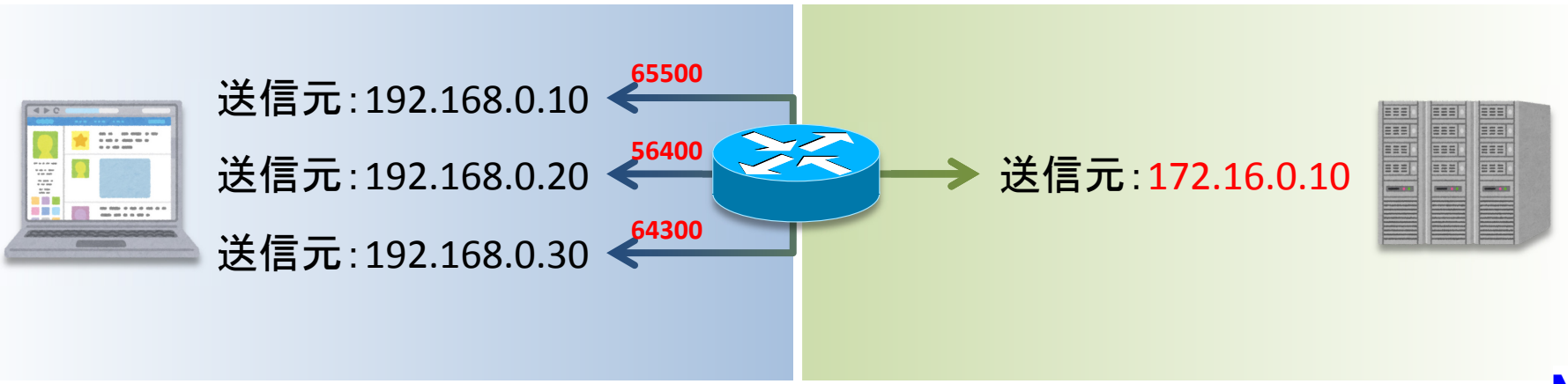
我々の想像するIPマスカレード

NAPT(Network Address and Port Translation)

別名「IPマスカレード(IP Masquerade)」

IPアドレスに加えてTCP/UDPのポートも変換することで、
1つのアドレスに対して複数のアドレスを対応付け、
変換させる技術

NATテーブル	
192.168.0.10:65500	172.16.0.10:65500
192.168.0.20:56400	172.16.0.10:56400
192.168.0.30:64300	172.16.0.10:64300



パケットを送ろう

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

192.168.1.1

203.0.113.23

ISP

internet

元：203.0.113.23
先：198.51.100.20

元：203.0.113.23
先：198.51.100.20

パケットを送ろう

192.168.1.1

203.0.113.23

ISP

internet

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

ください

元：203.0.113.23
先：198.51.100.20

パケットを送ろう

192.168.1.1

203.0.113.23

ISP

internet

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

元：203.0.113.23
先：198.51.100.20

パケットを送ろう

192.168.1.1

203.0.113.23

ISP

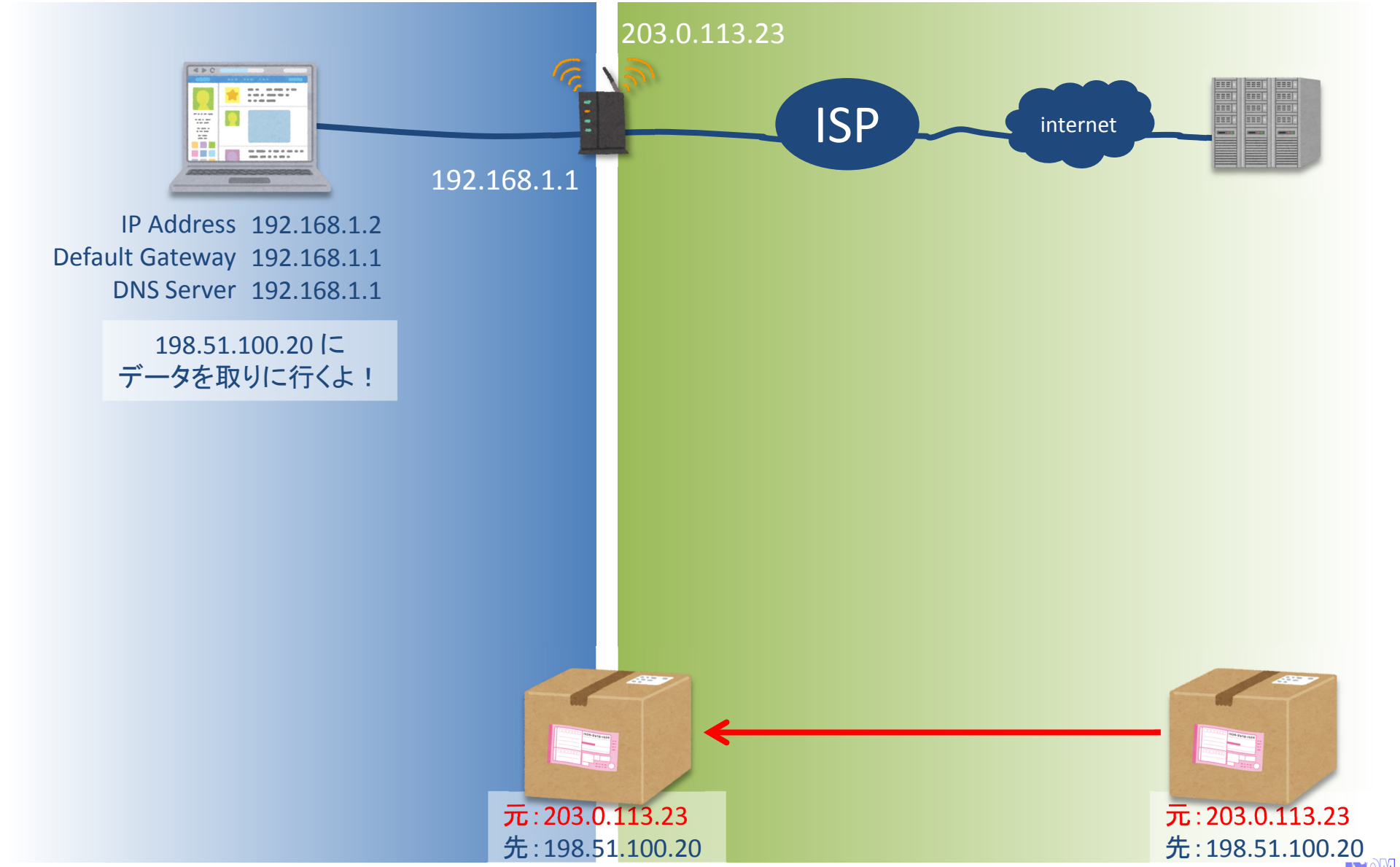
internet

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

元：203.0.113.23
先：198.51.100.20

パケットを送ろう



パケットを送ろう

IP Address 192.168.1.2
Default Gateway 192.168.1.1
DNS Server 192.168.1.1

198.51.100.20 に
データを取りに行くよ！

192.168.1.1

203.0.113.23

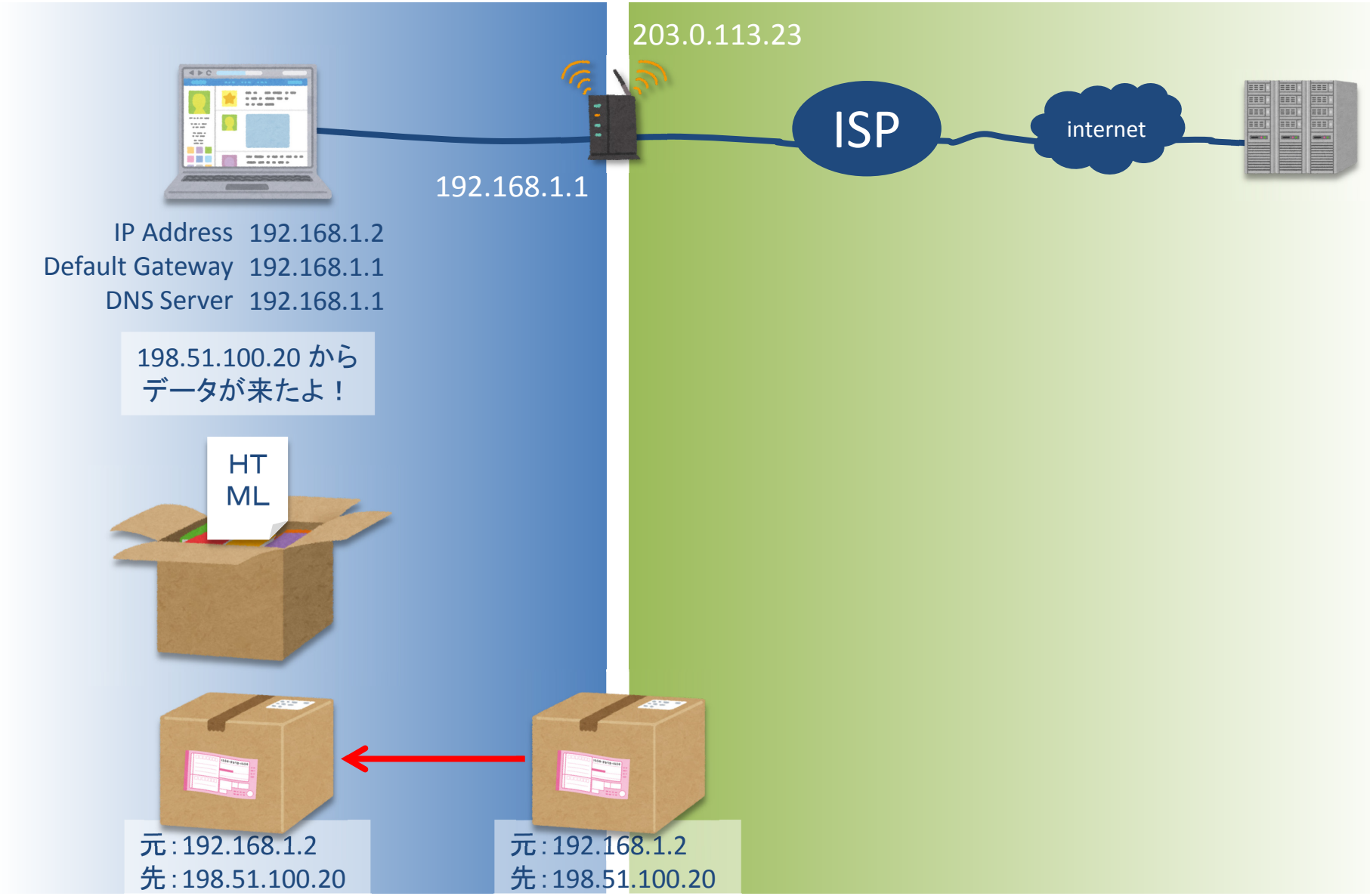
ISP

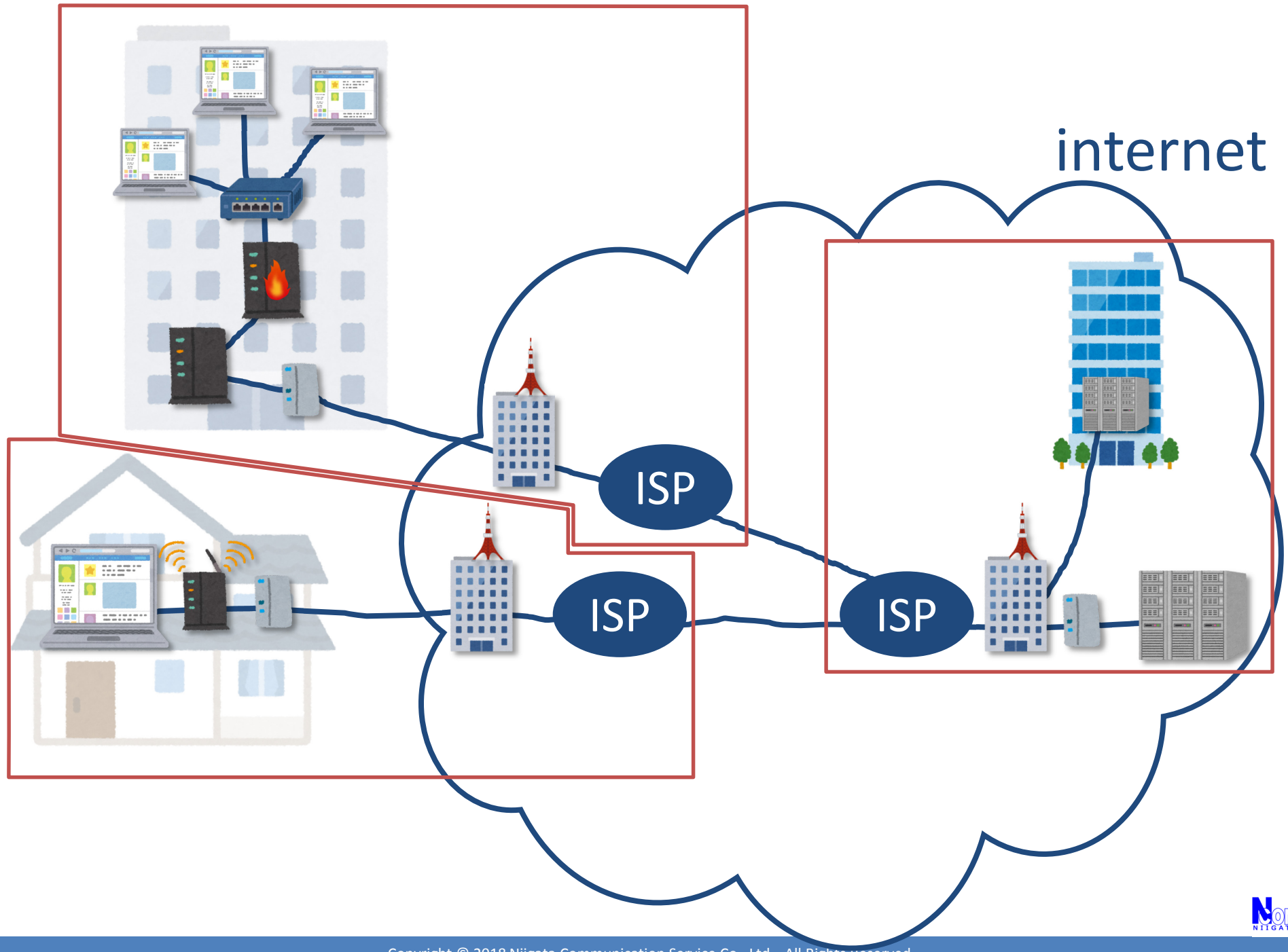
internet

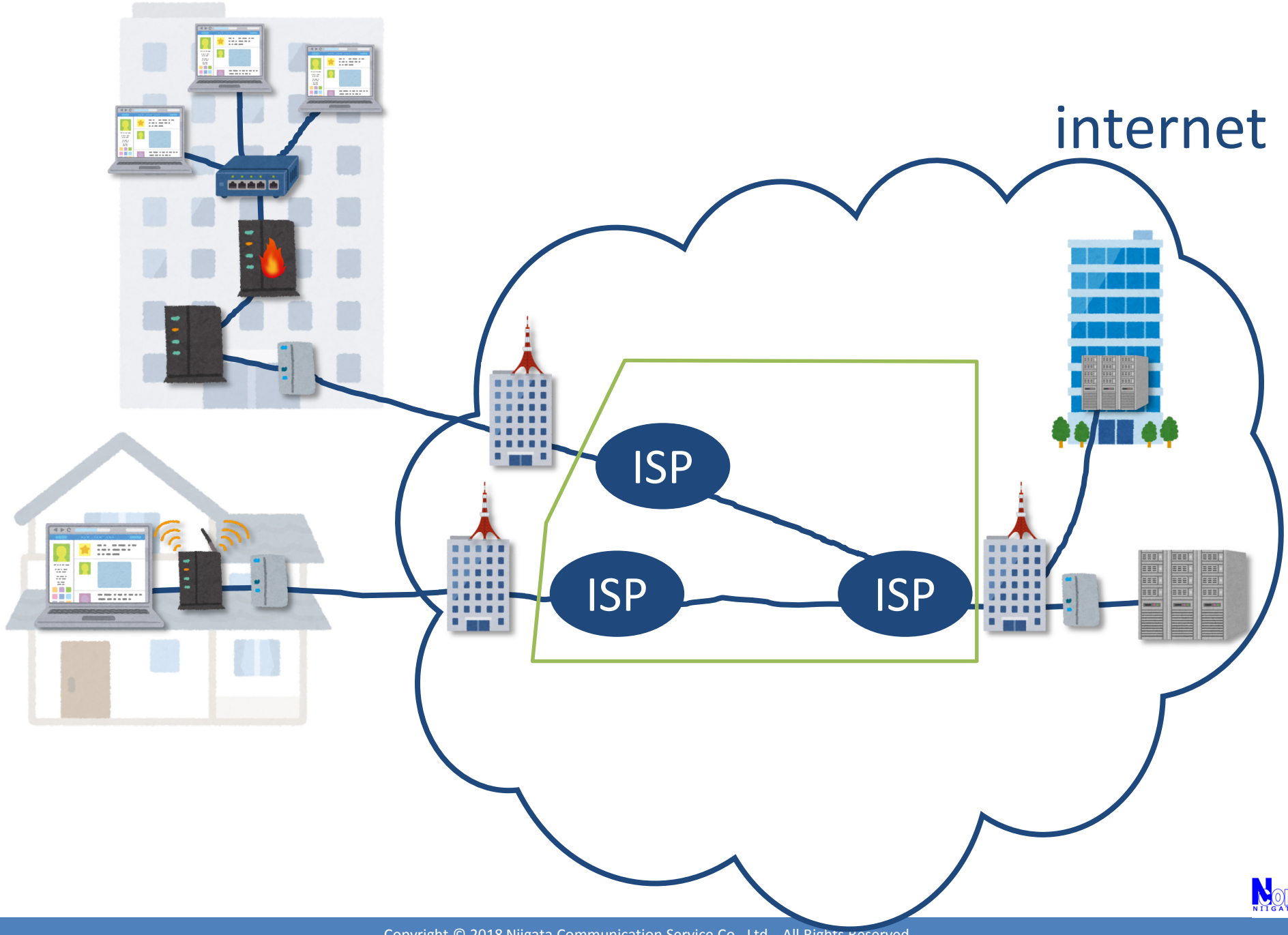
NAT(NAPT)

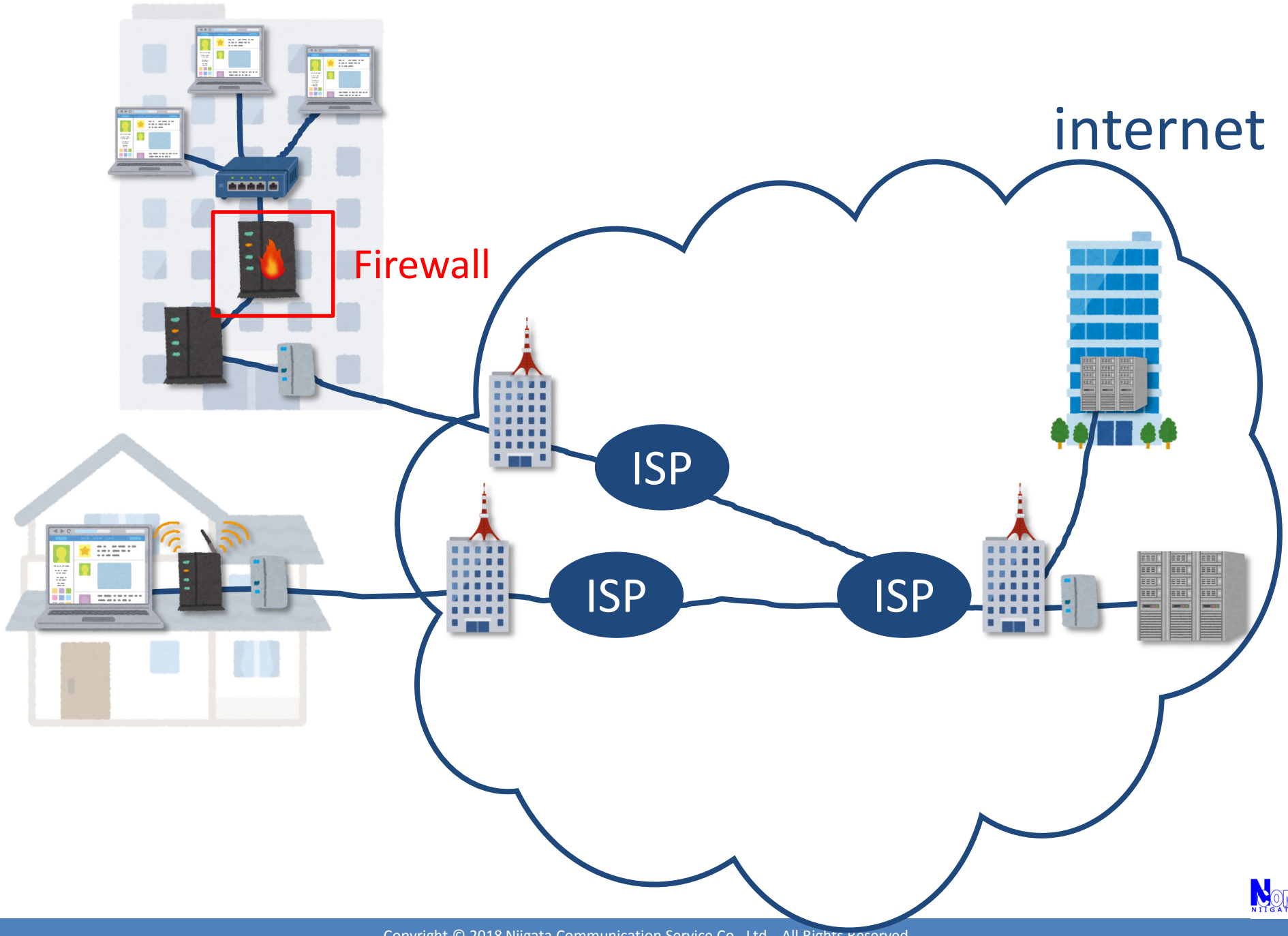
元：192.168.1.2
先：198.51.100.20

パケットを送ろう

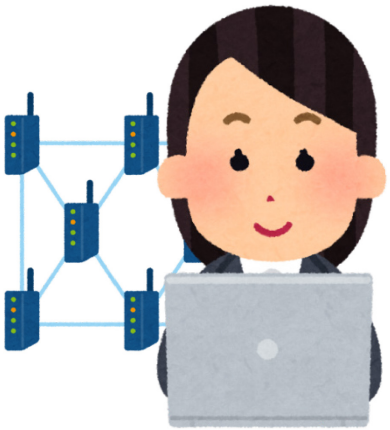








プレイヤー

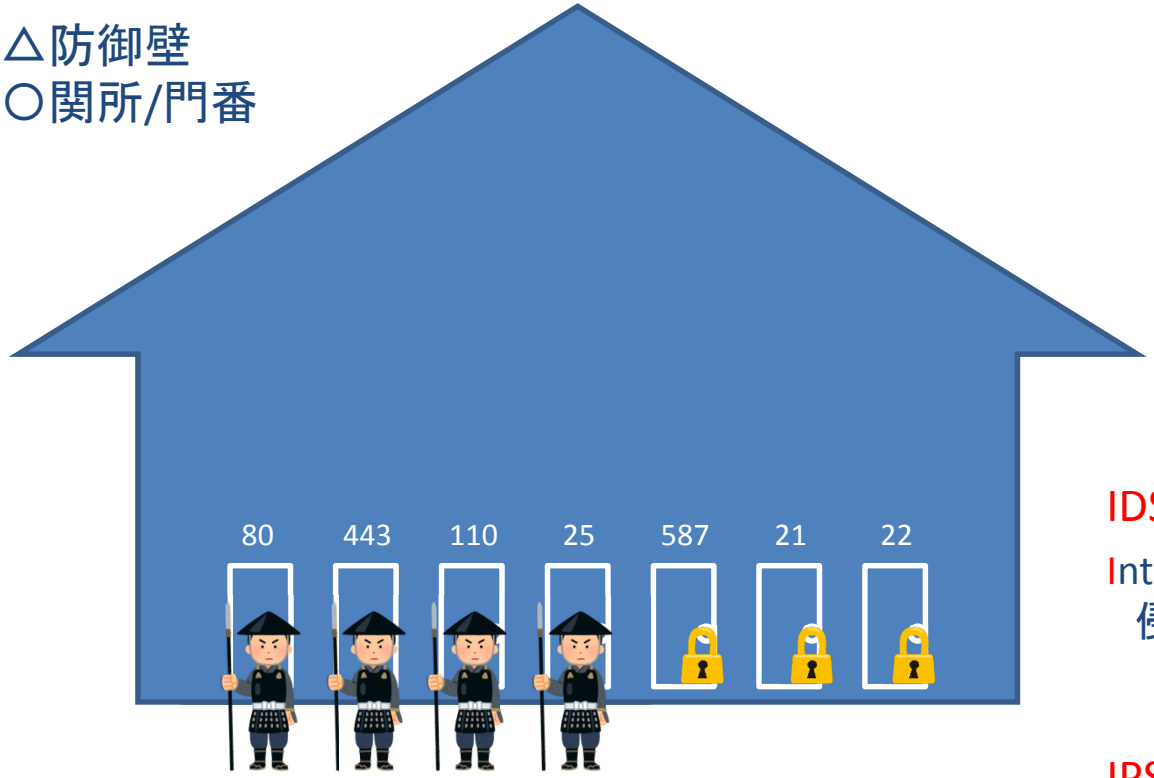


ネットワークエンジニア

セキュリティエンジニア

Firewall

△防御壁
〇関所/門番



・特定のIPアドレスからなら許可/不許可
・特定のIPアドレス宛てなら許可/不許可
・特定のパケットの種類なら不許可
・特定の頻度以上なら不許可
・特定のパケットは記録
・特定の記録は通報

IDS

Intrusion Detection System
侵入検知システム

IPS

×iPS(induced pluripotent stem)細胞
〇Intrusion Prevention System
侵入防止システム

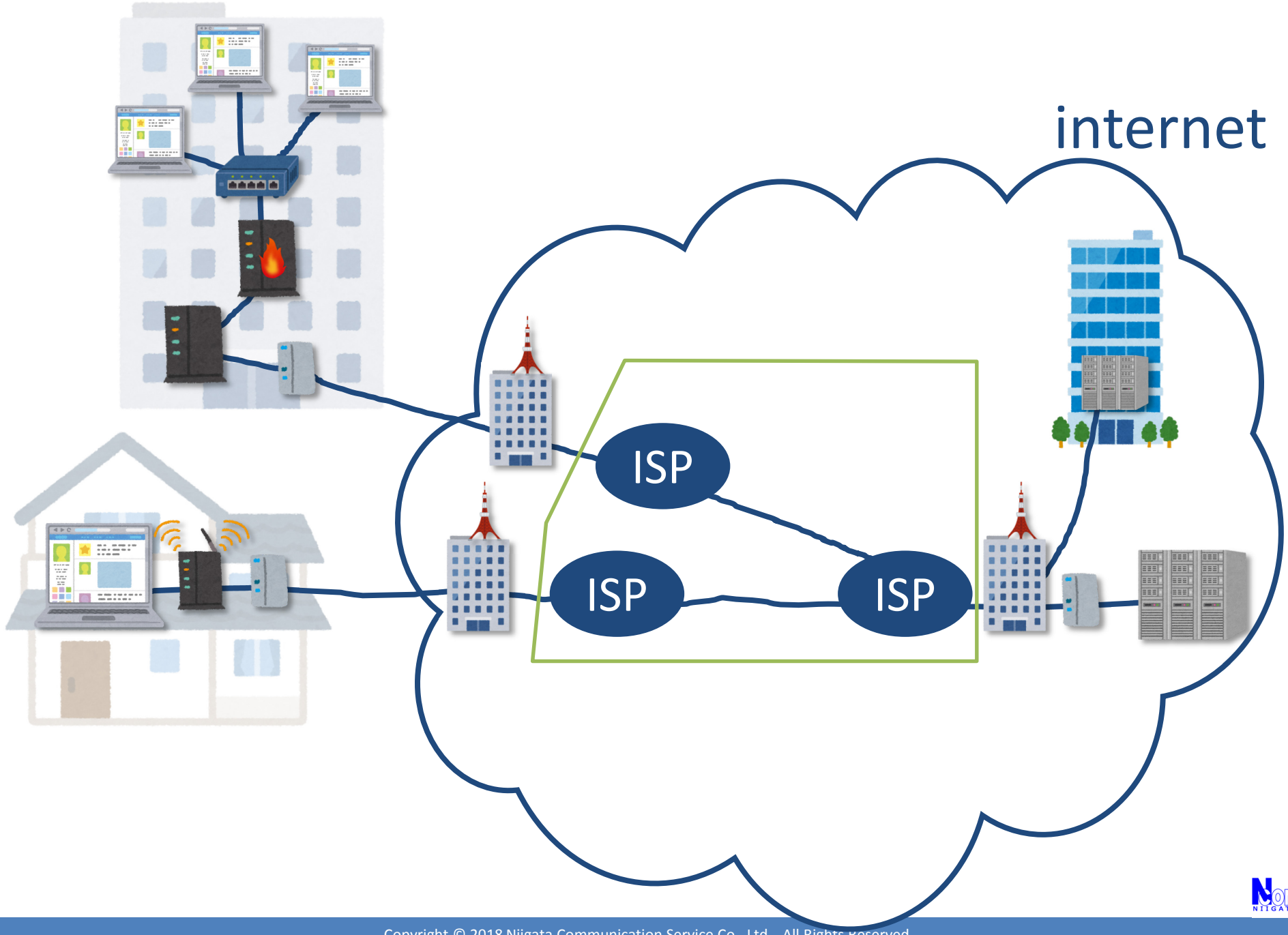
UTM

Unified Threat Management
総合脅威管理

CSIRT

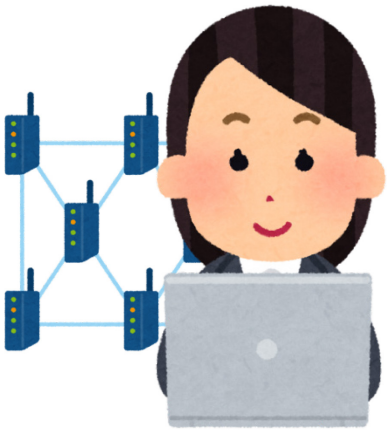
Computer Security Incident Response Team
コンピューターセキュリティインシデント（セキュリティ的に何かヤバいことがあった）の際に対応活動を行う組織。
専門の部署がある場合もあるが、インシデント発生時にのみ組織される場合もある。

- 情報収集
- 分析
- 解析/解明
- 対処
- 対応
- 評価
- 提言



プレイヤー

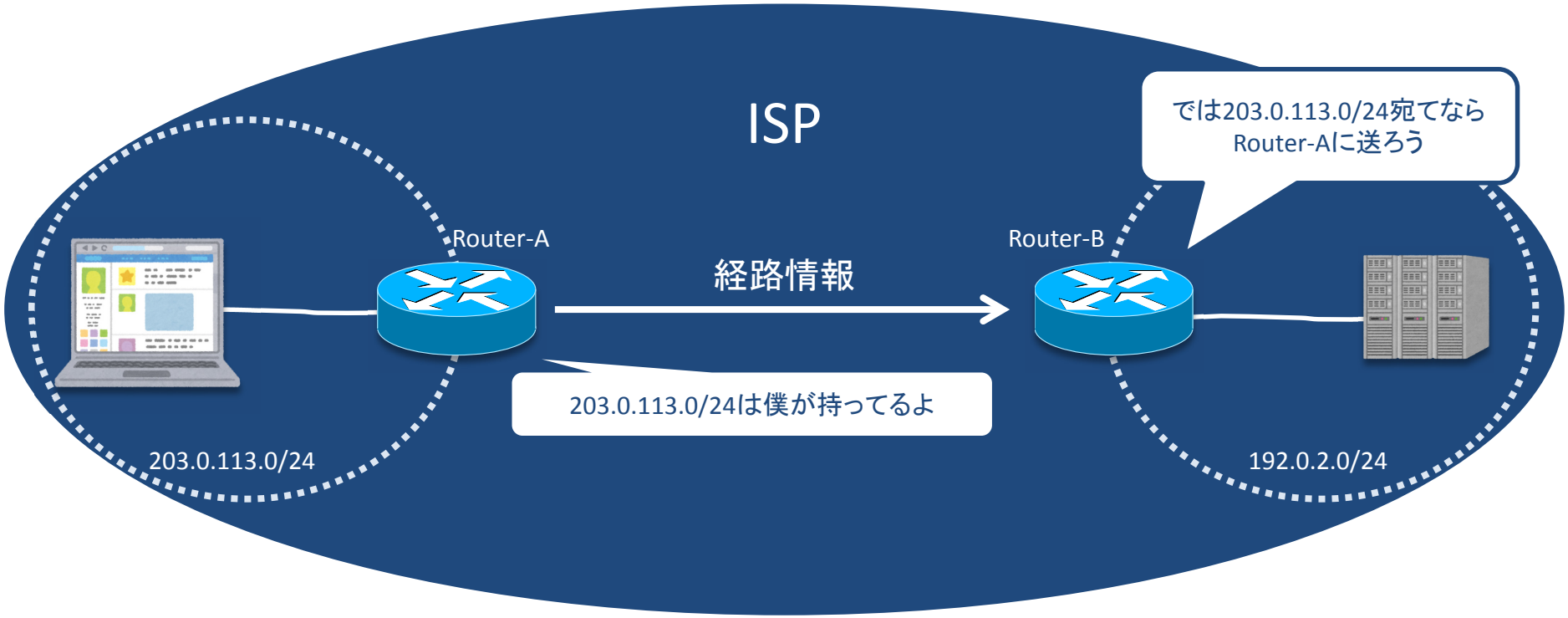
ISP



ネットワークエンジニア

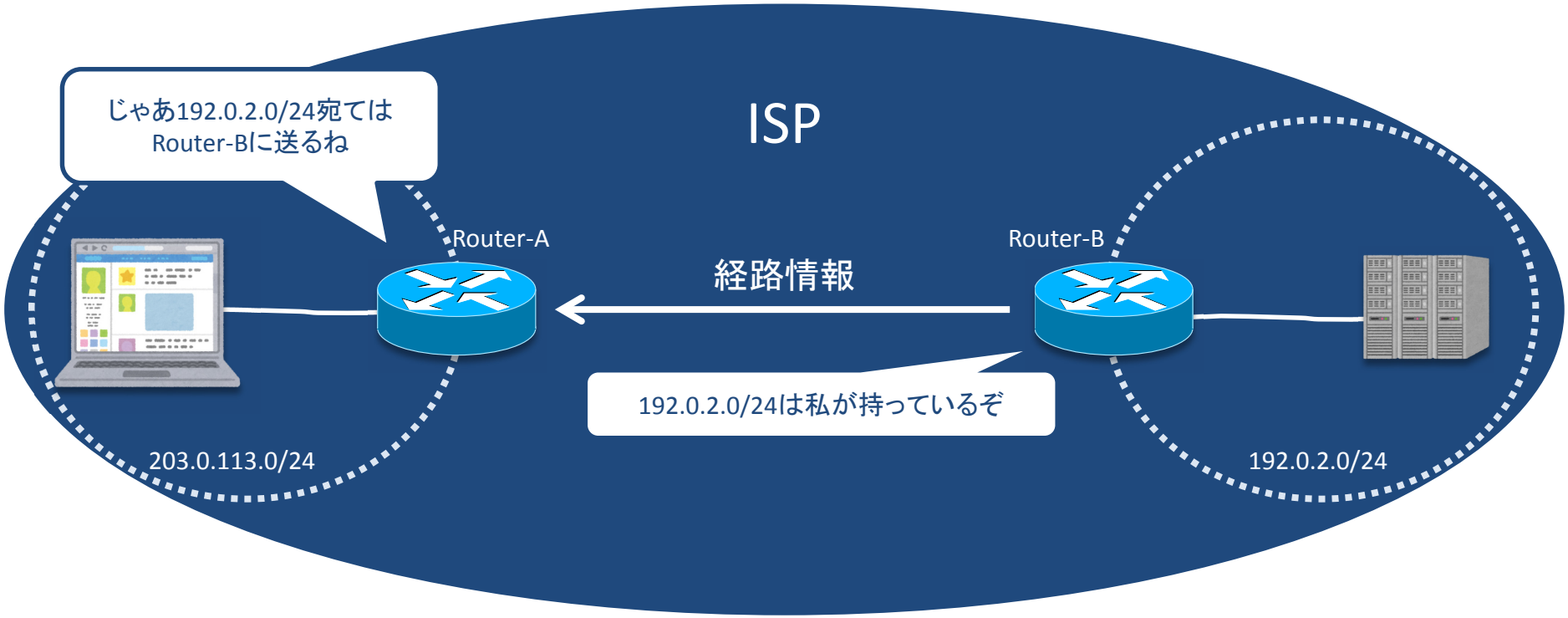
営業

経路を伝える（ISP内）



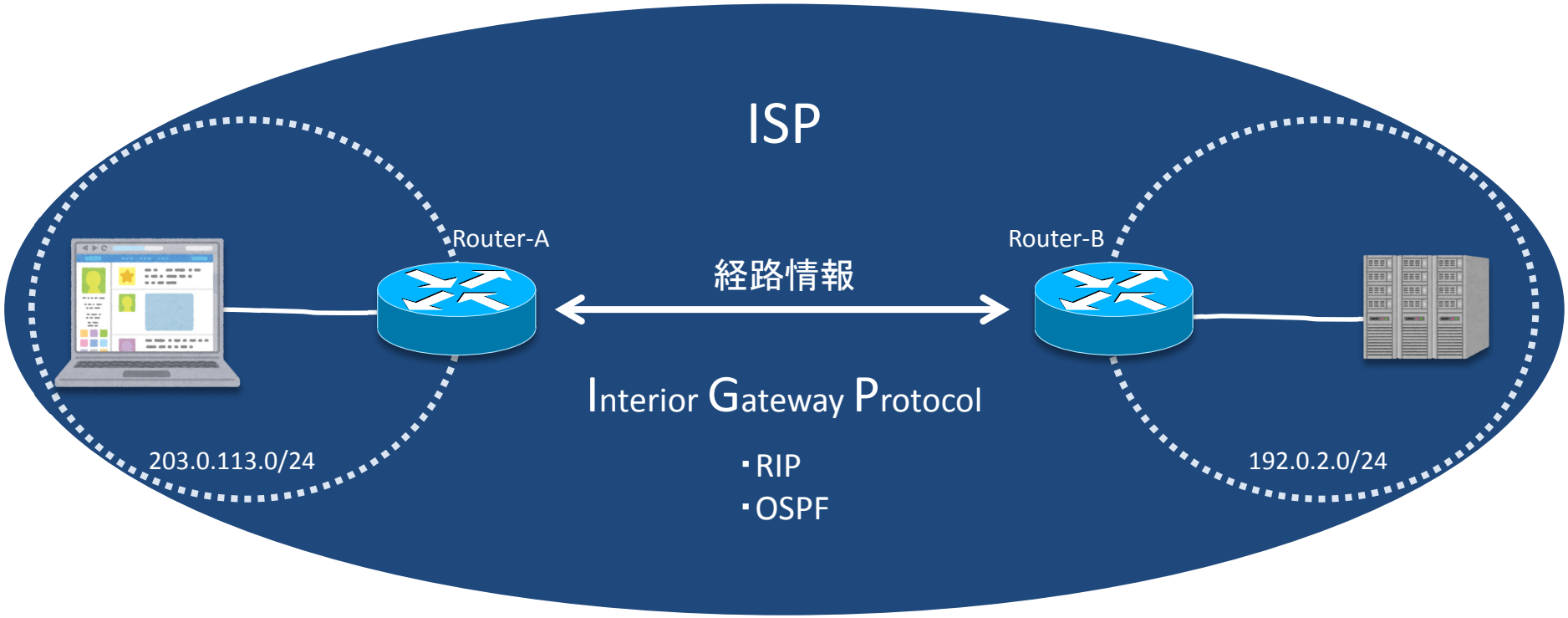
Router-A：加入者向けRouter
Router-B：サーバー群用Router

経路を伝える（ISP内）



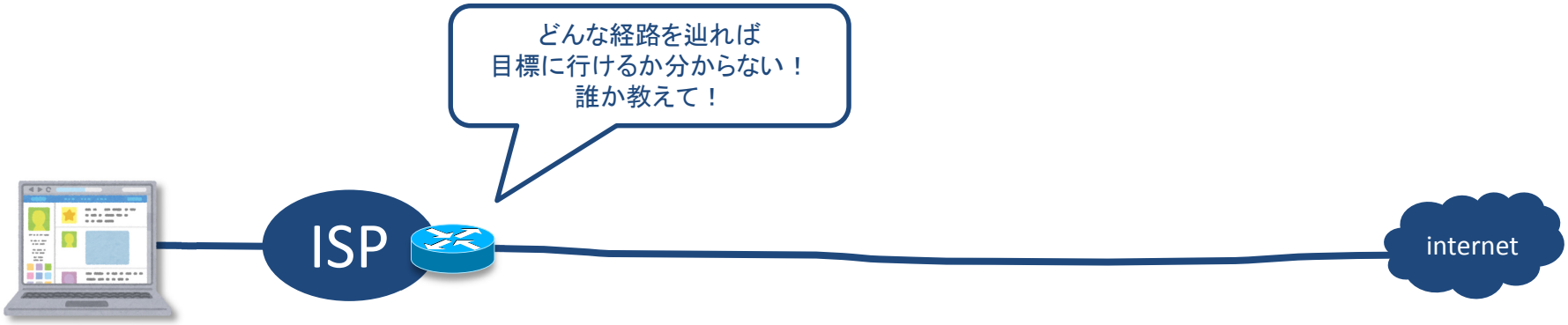
Router-A：加入者向けRouter
Router-B：サーバー群用Router

経路を伝える（ISP内）

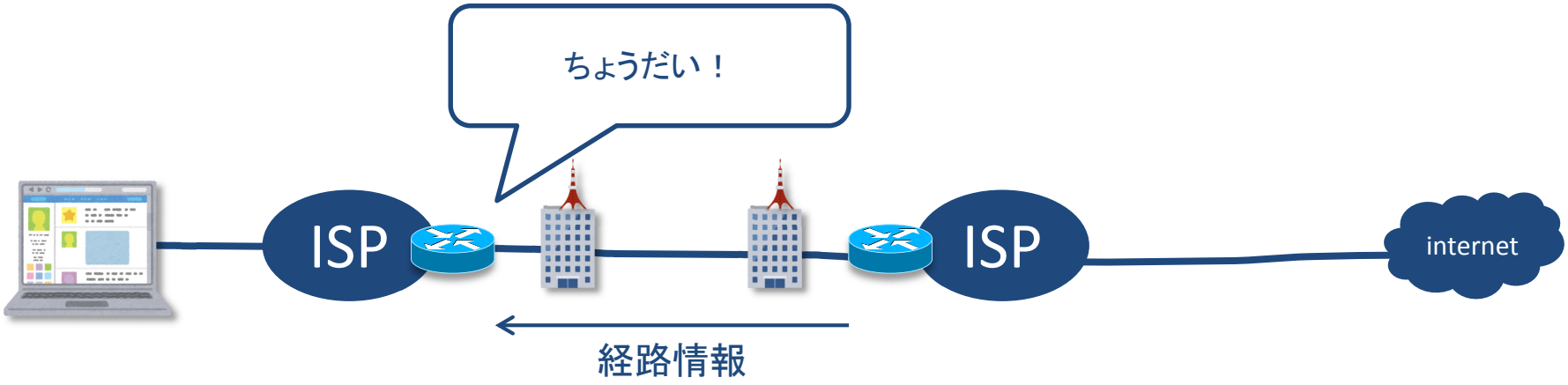


Router-A：加入者向けRouter
Router-B：サーバー群用Router

経路を伝えて

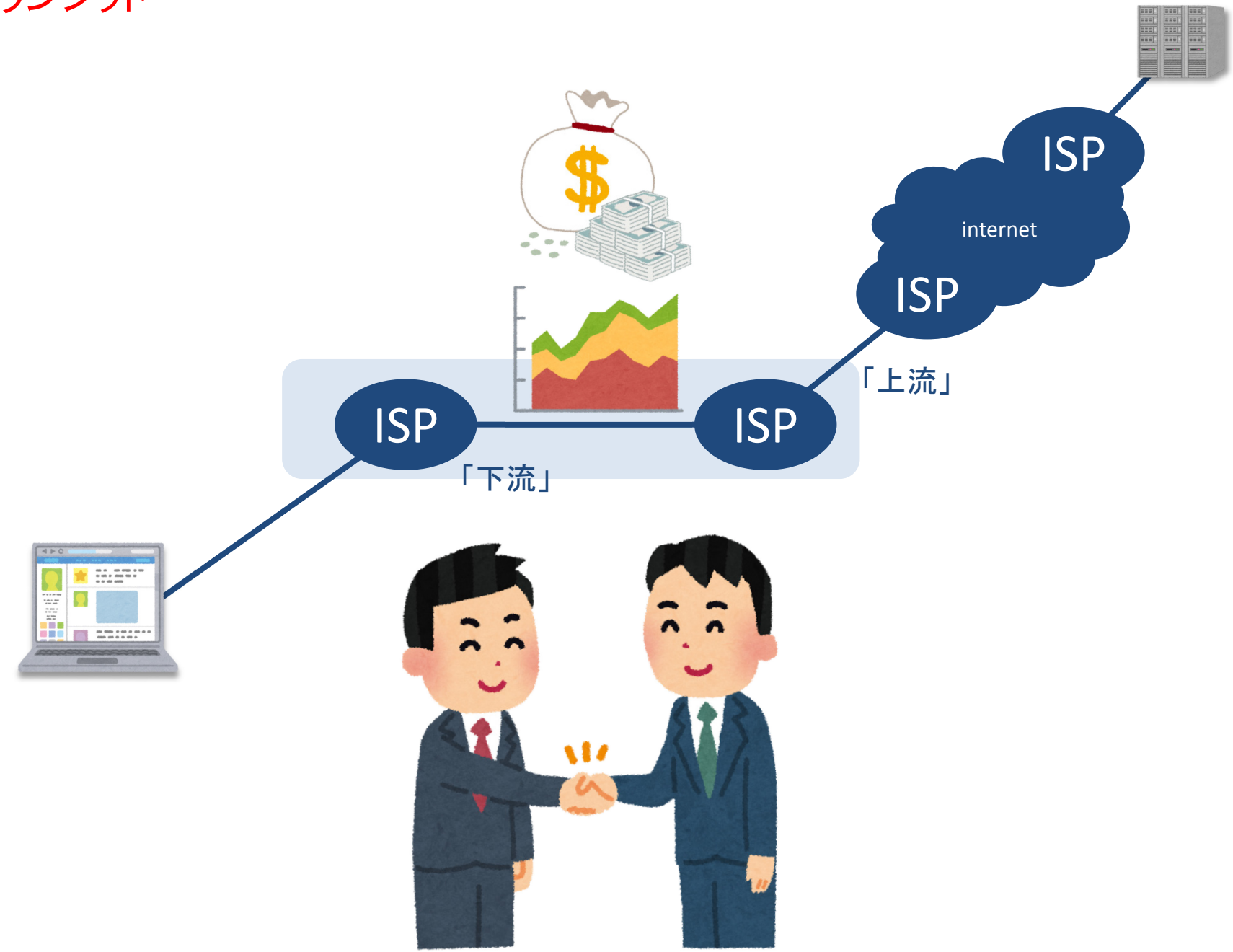


経路をください

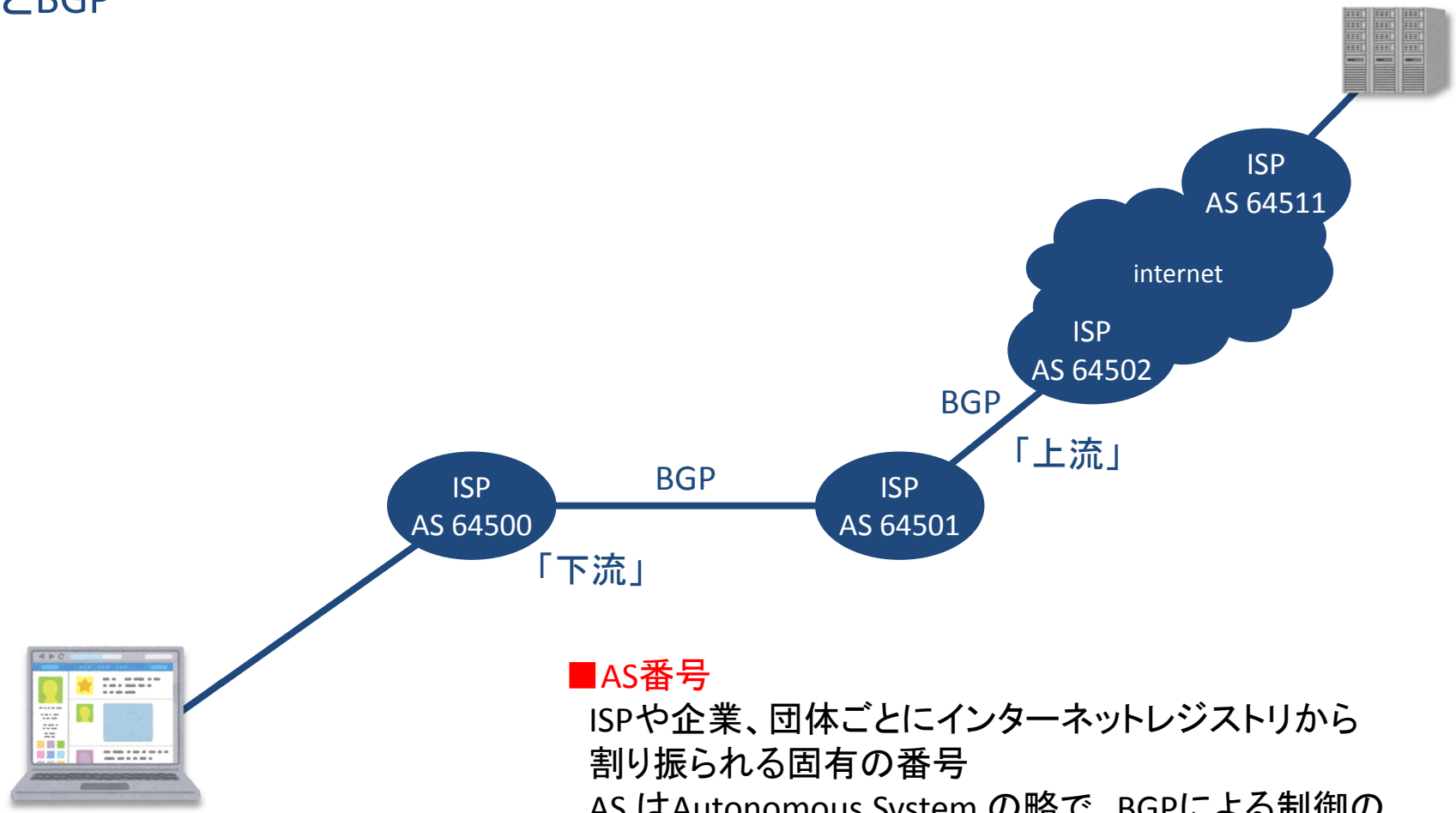


トランジット

トランジット



ASとBGP



■AS番号

ISPや企業、団体ごとにインターネットレジストリから割り振られる固有の番号
AS はAutonomous System の略で、BGPによる制御の単位となる

■BGP

ASを単位として、お互いの経路情報をやり取りするための制御プロトコルで、Border Gateway Protocol の略
ORIGIN属性、AS-PATH属性、NEXT-HOP属性、LOCAL-PREF属性などを交換する　EGP（Exterior Gateway Protocol）

AS-PATH

198.51.100.20

ISP
AS 64511

internet

ISP
AS 64502

198.51.100.0/24は
私の向こうの
AS 64502 の向こうの
（中略）の向こうの
AS 64511 が持ってるよ

198.51.100.0/24は
AS 64501 の向こうの
AS 64502 の向こうの
（中略）の向こうの
AS 64511 が持ってるよ

BGP

「上流」

198.51.100.0/24は
私の向こうの
（中略）の向こうの
AS 64511 が持ってるよ

ISP
AS 64500

BGP

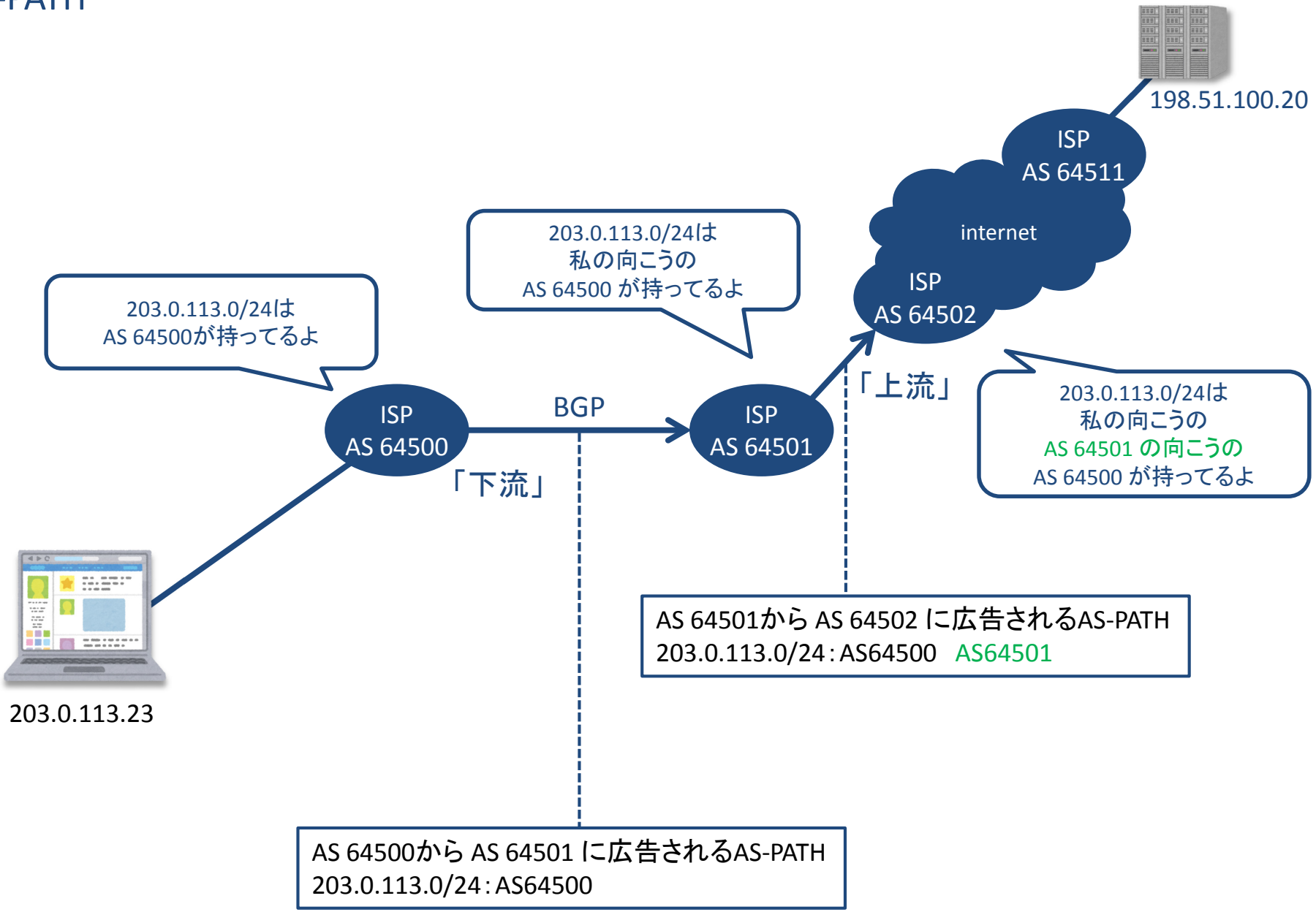
ISP
AS 64501

「下流」

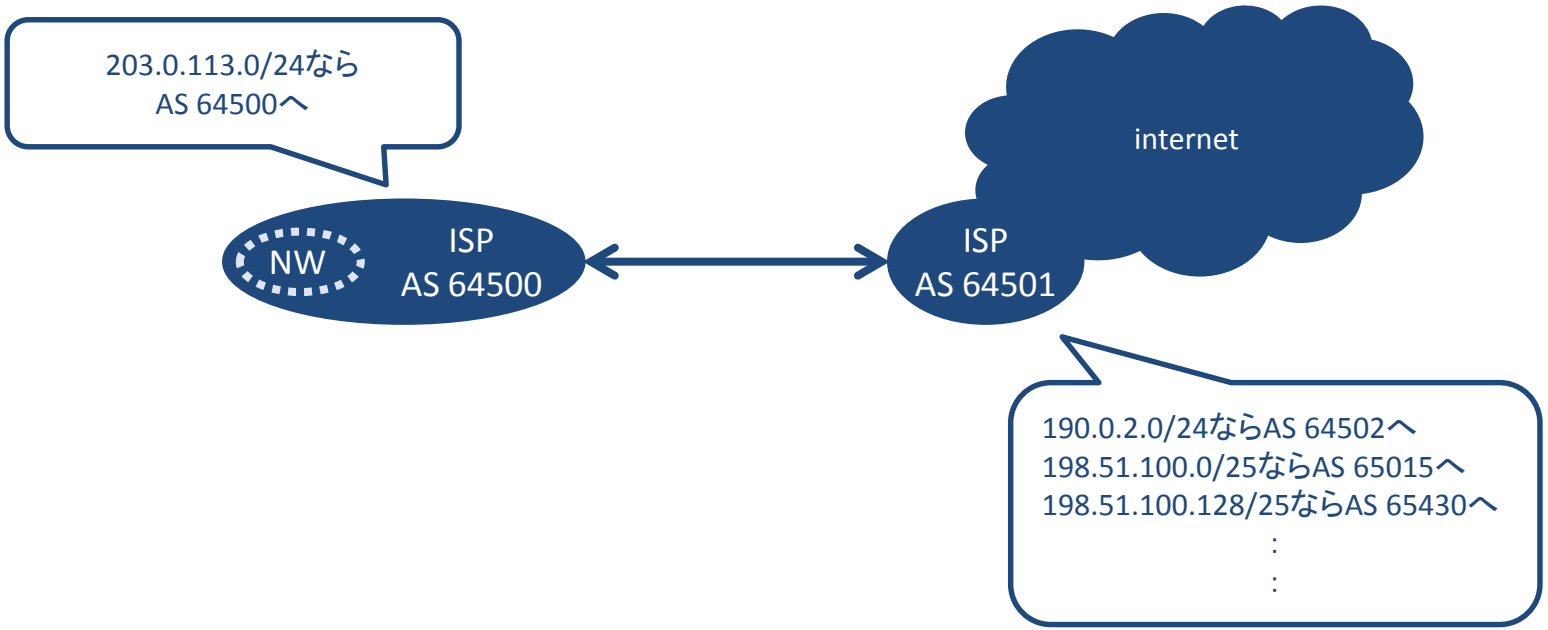
AS 64502から AS 64501 に広告されるAS-PATH
198.51.100.0/24：AS64511　(中略)　AS64502

AS 64501から AS 64500 に広告されるAS-PATH
198.51.100.0/24：AS64511　(中略)　AS64502　AS64501

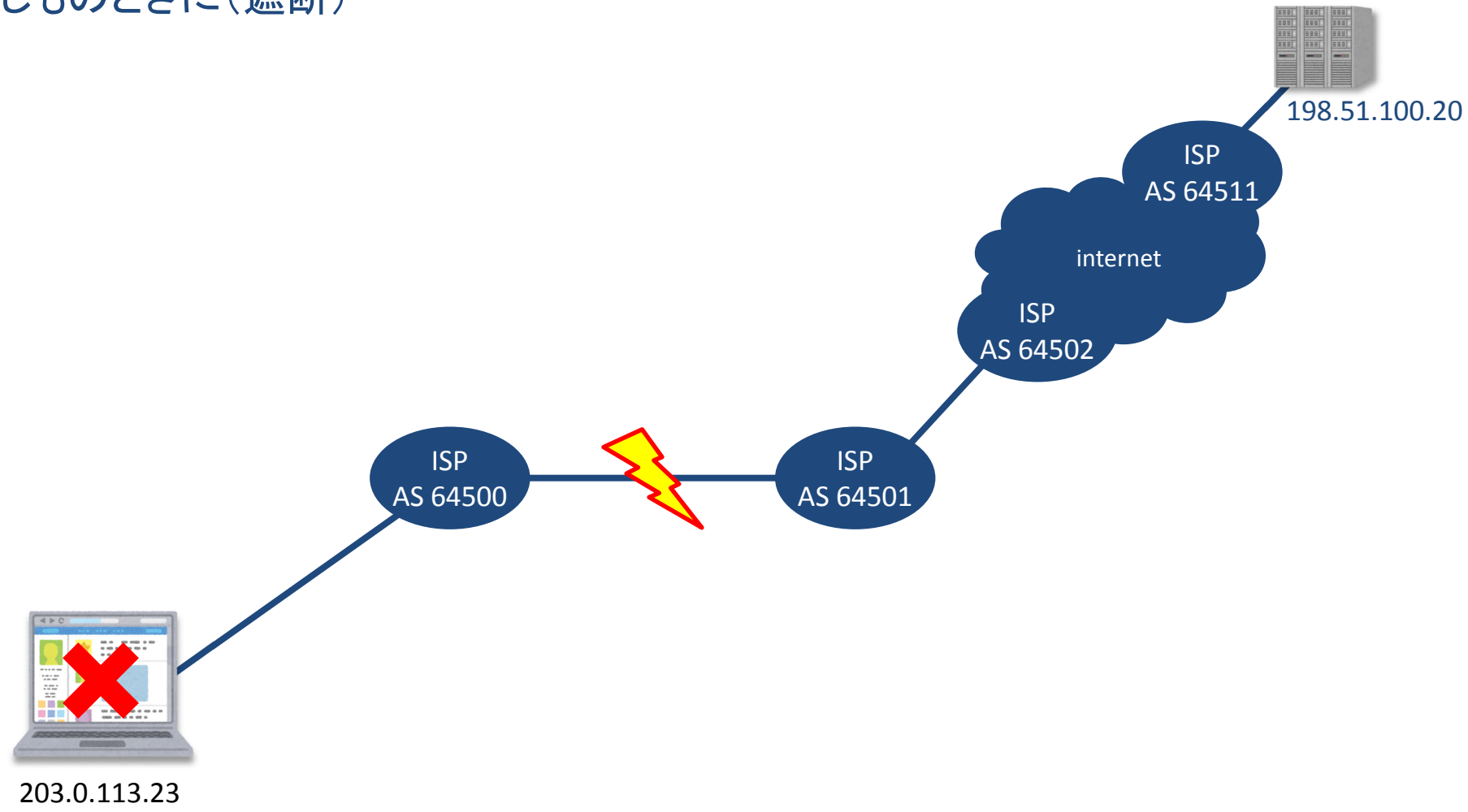
AS-PATH



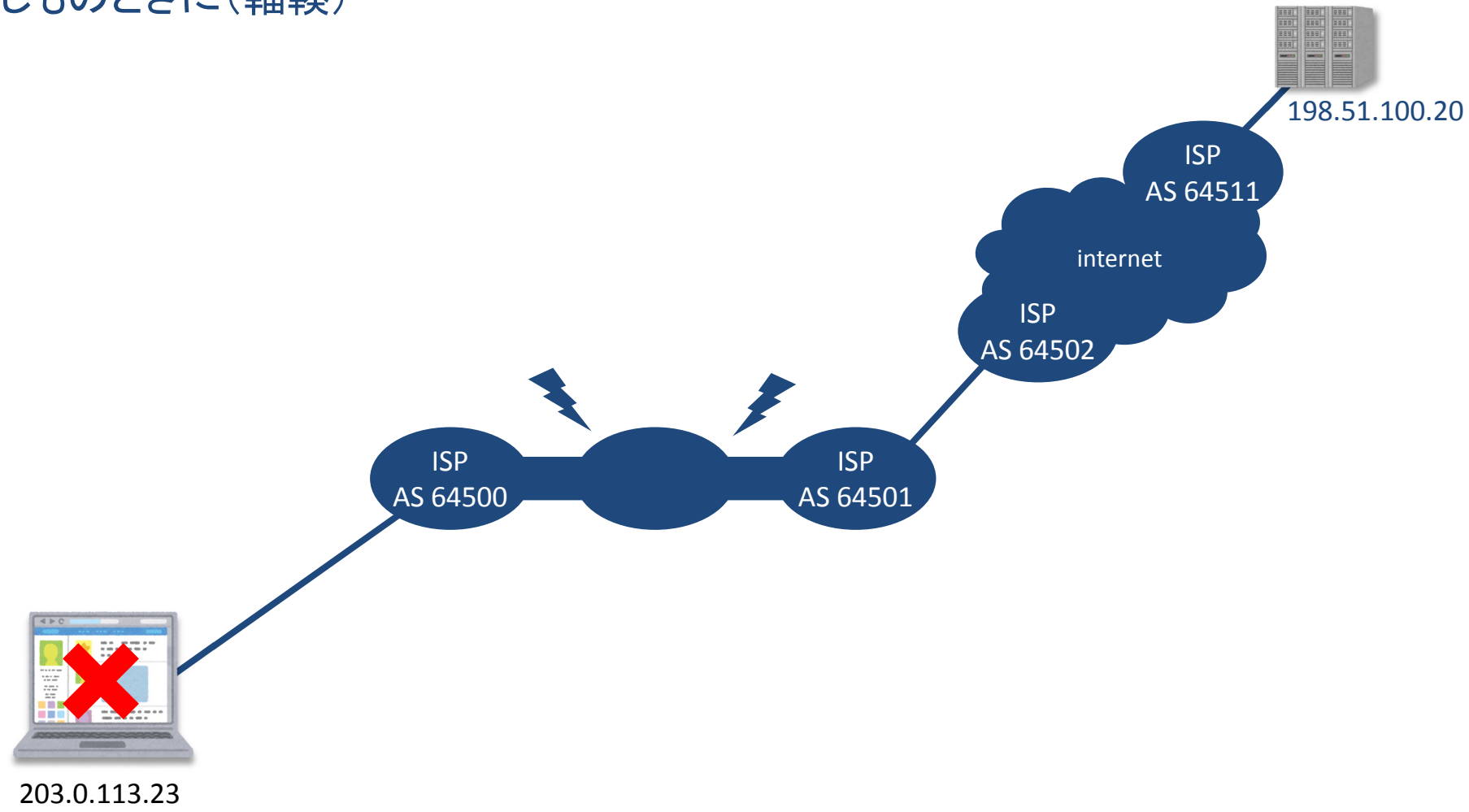
トランジット



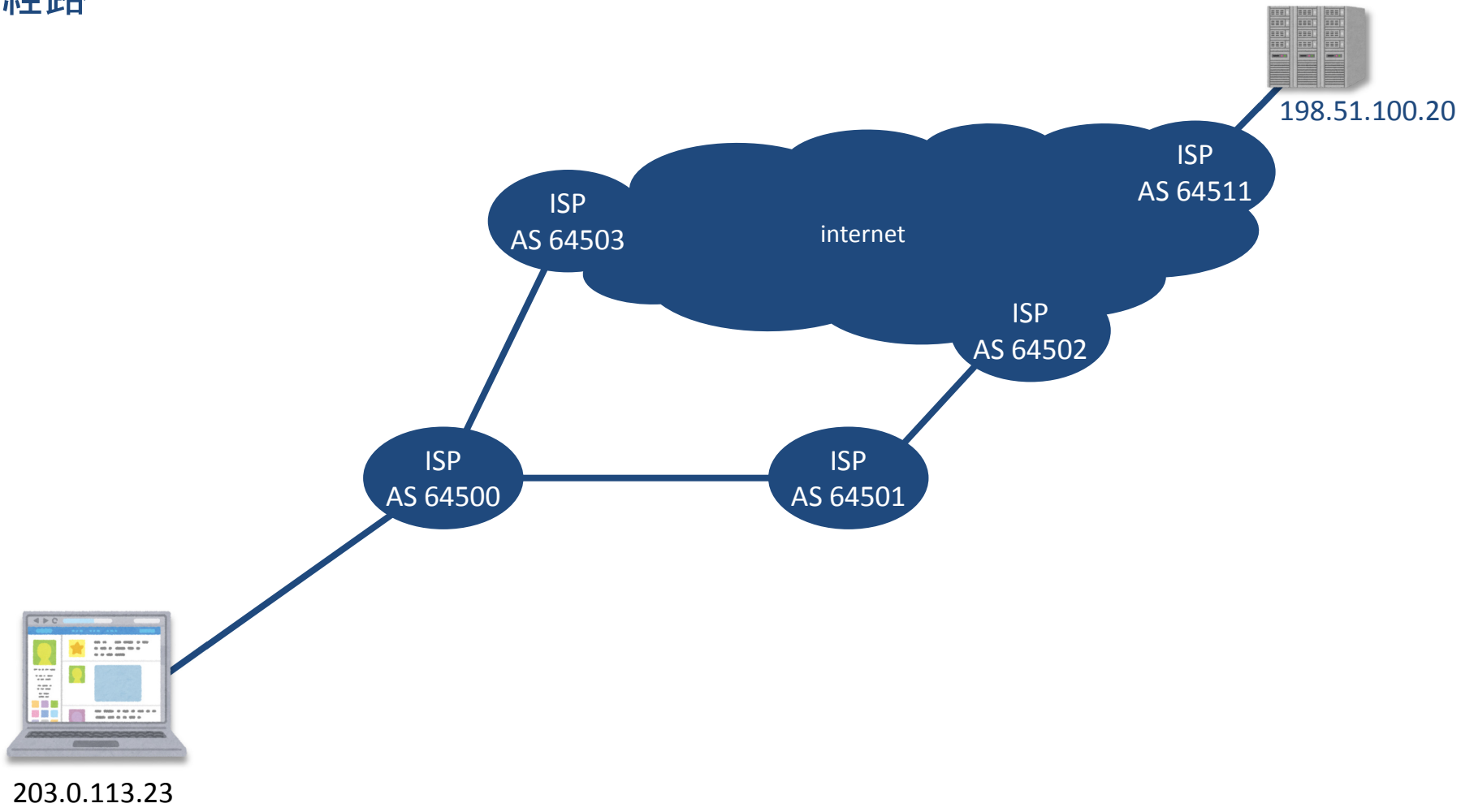
もしものときに（遮断）



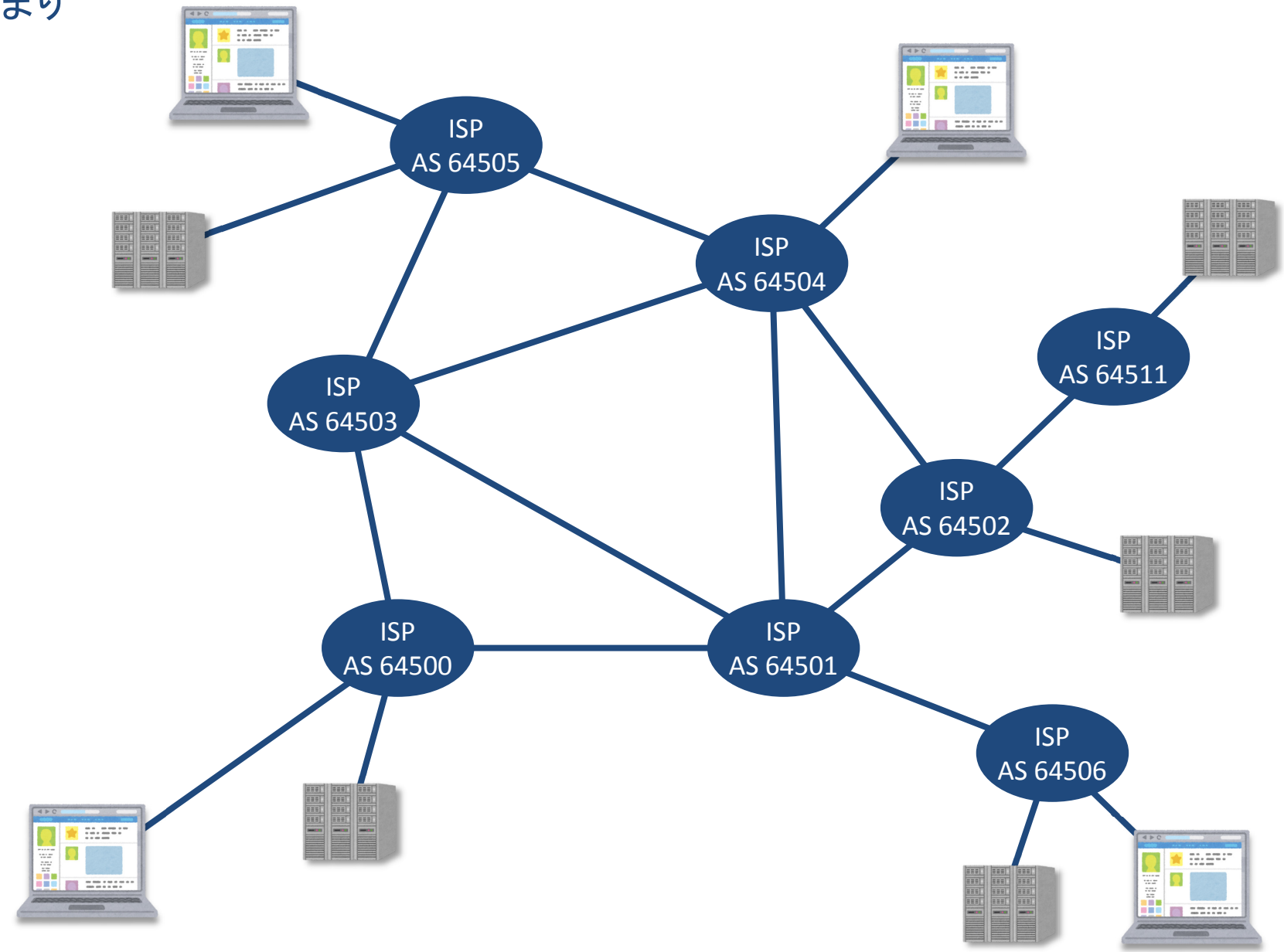
もしものときに（輻輳）



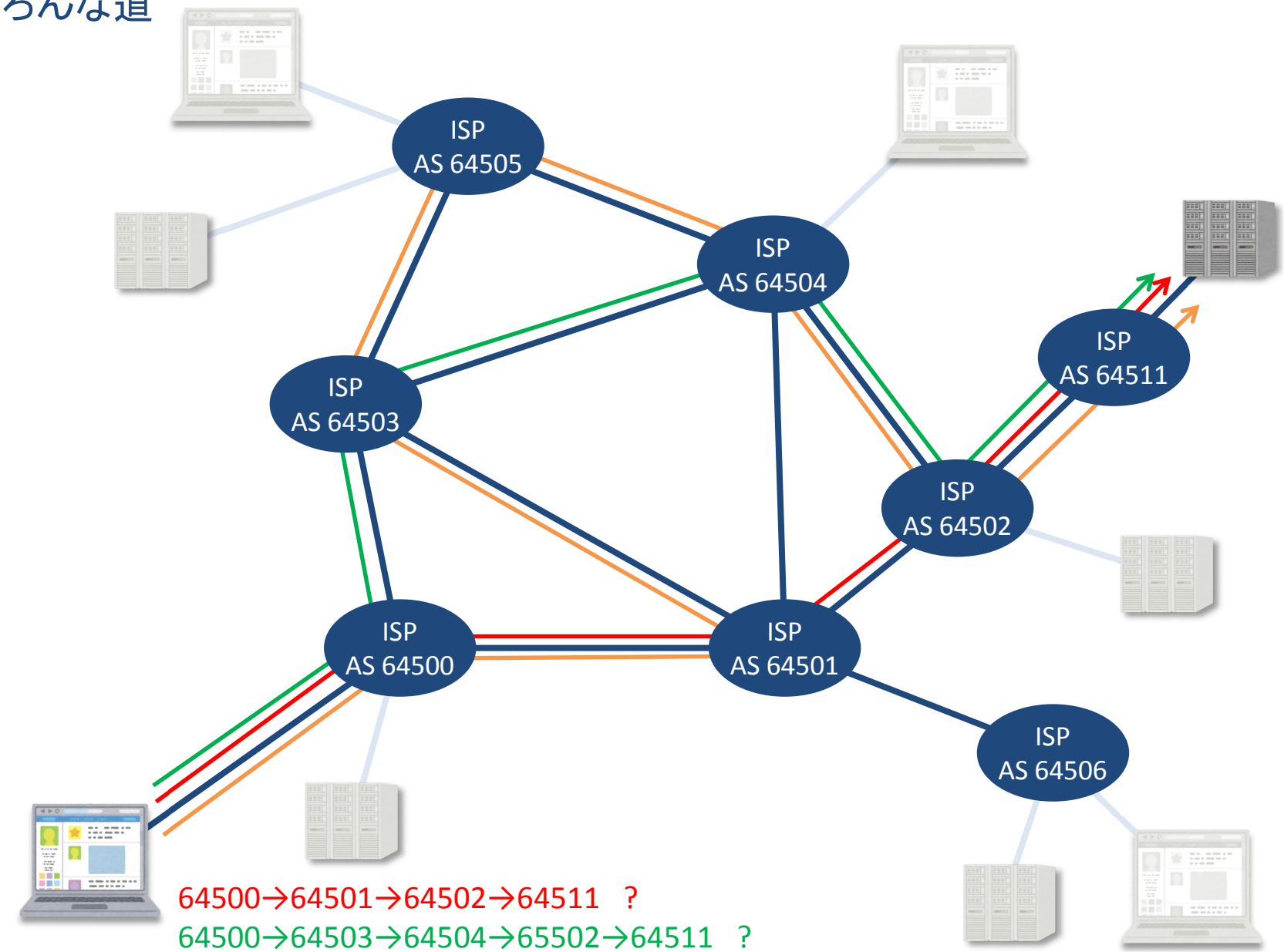
別経路



つまり



いろんな道



64500→64501→64502→64511 ?

64500→64503→64504→65502→64511 ?

64500→64501→64503→65505→65504→64502→64511 ?

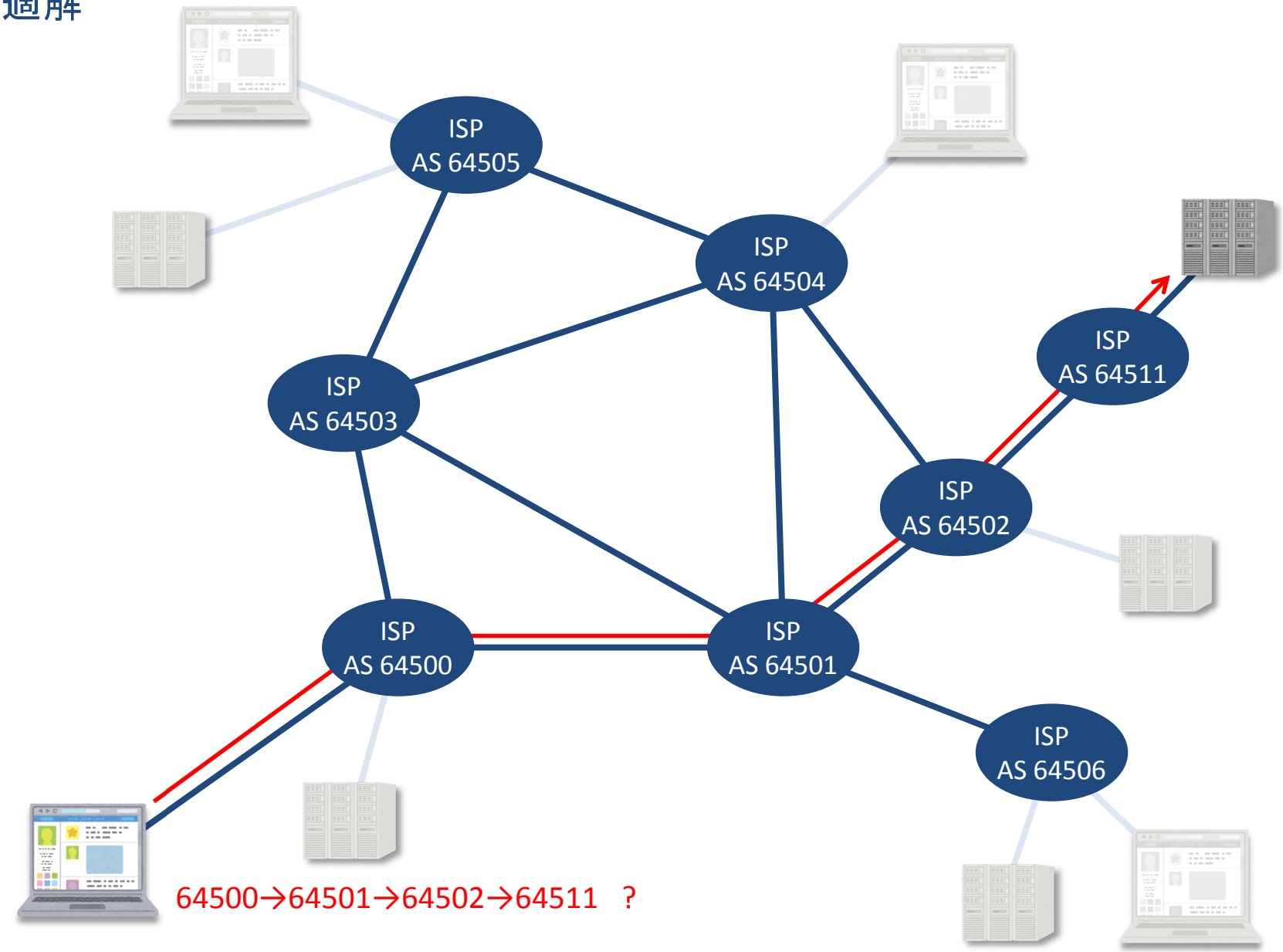
経路選択の優先度

↑ 優先度高

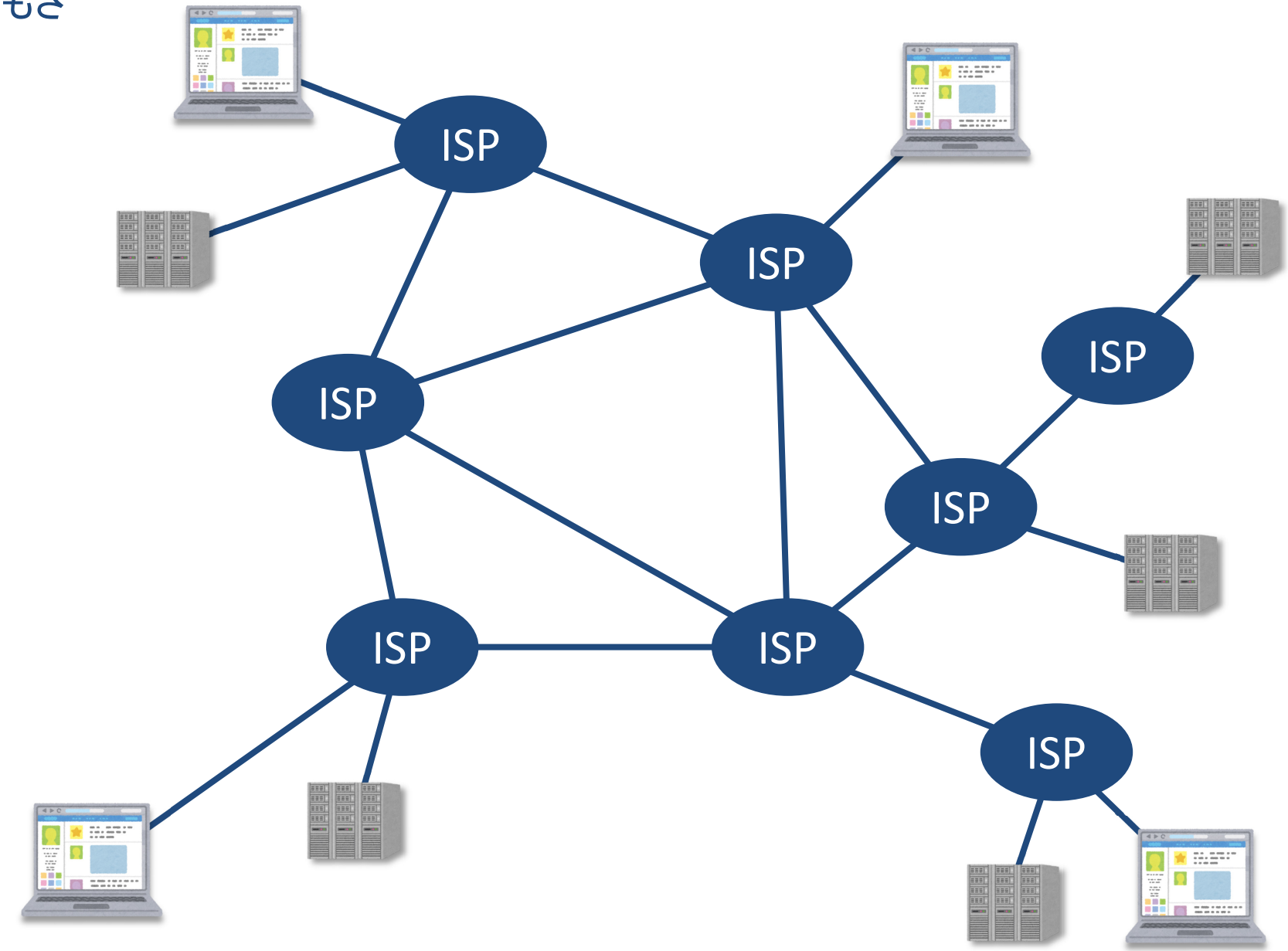
1. ネクストホップへのIGPルートを持っていない経路は無視されます。
2. weightパラメータを持つルータはweightパラメータ値が最大の経路を選択します。
3. LOCAL_PREF属性の値の最も高い経路を選択します。
4. AS_PATH属性のリストの長さが最も短い経路を選択します。
5. ORIGIN属性のタイプが最も低い経路を選択します。（IGP<EGP<INCOMPLETEの順）
6. ルートが同じASから取得し、複数存在する時にはMULTI_EXIT_DISC属性の低い経路を優先します。
7. iBGPよりもeBGPで取得した経路を優先します。
8. ネクストホップへIGPで最も近い経路を優先します。
9. ルータIDが最も低いピアから学習した経路を優先します。
   （ルータIDは通常、ルータのインタフェースから自動的に生成されます）

↓ 優先度低

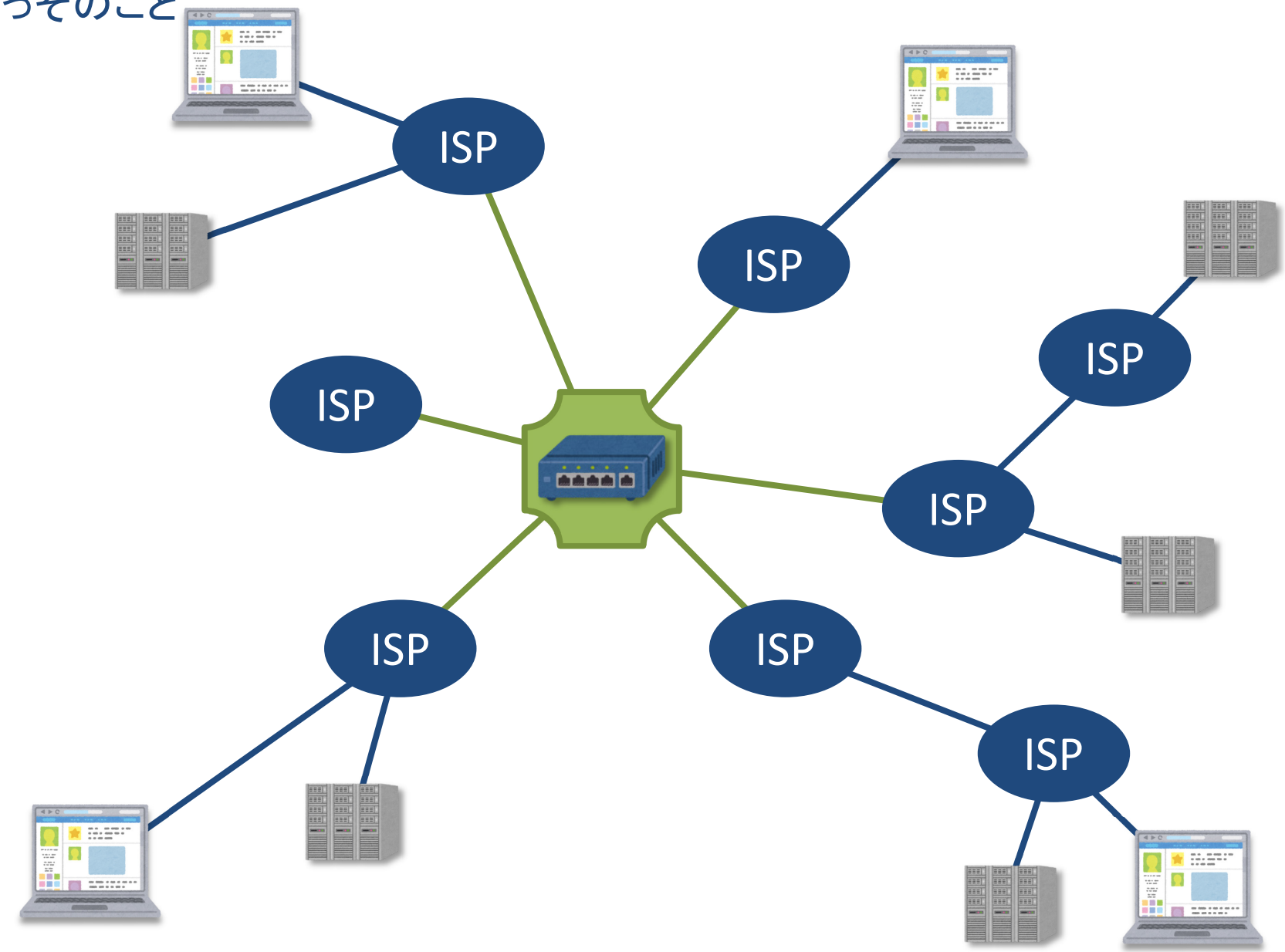
最適解



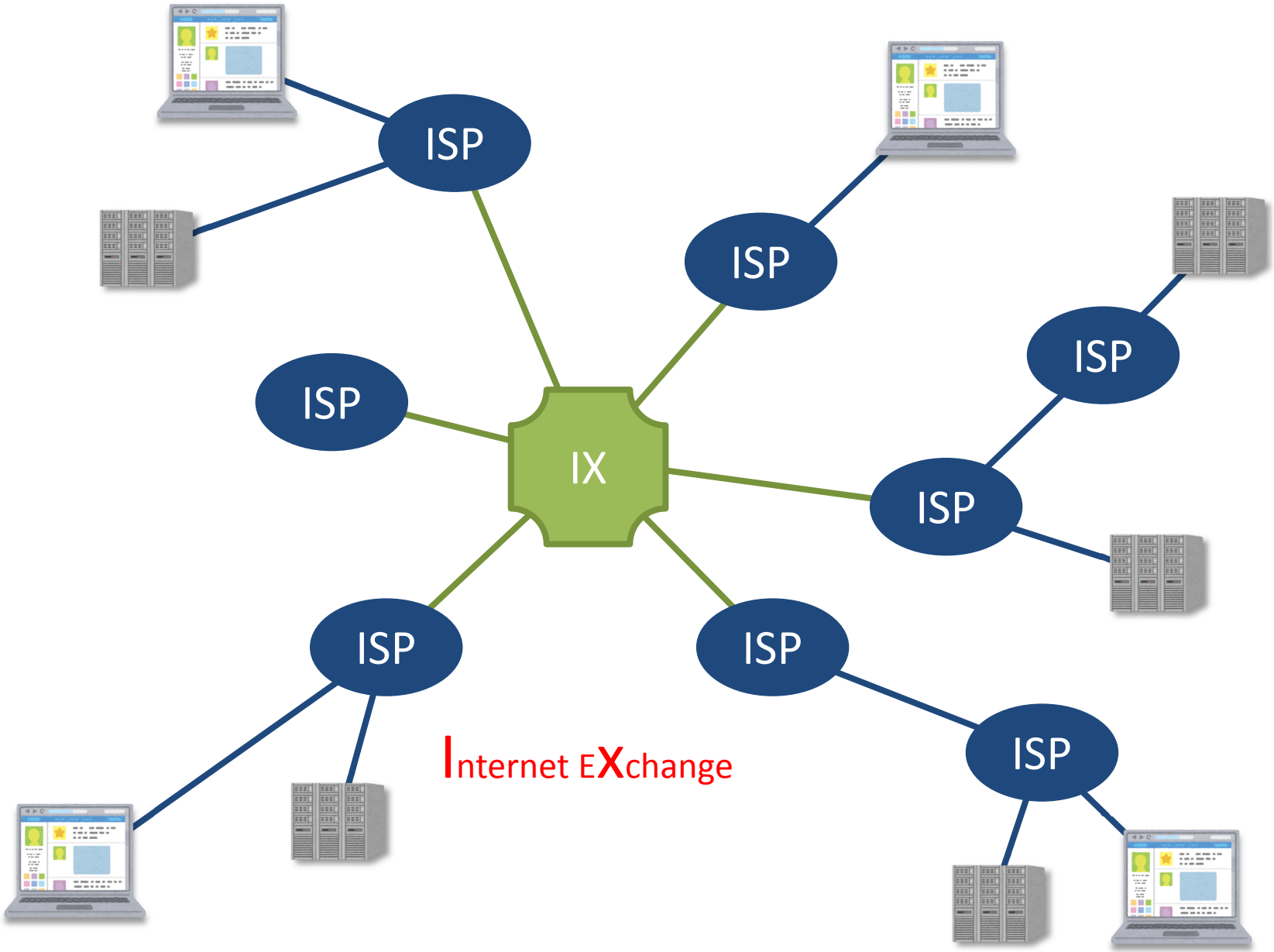
でもさ



いっそのこと



IX



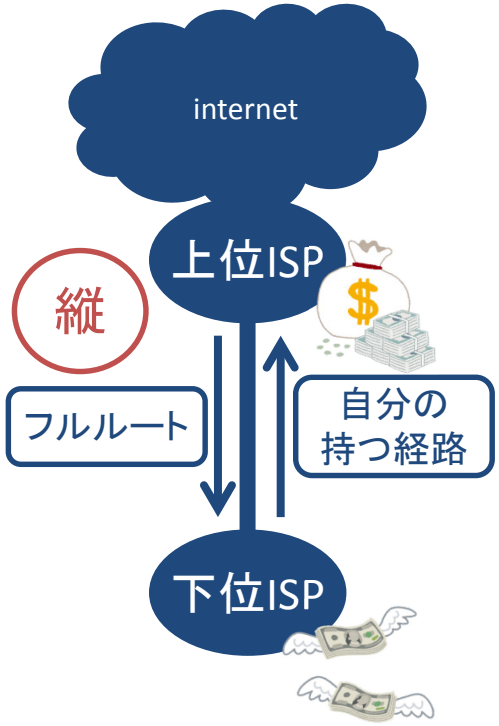
トランジットとIX

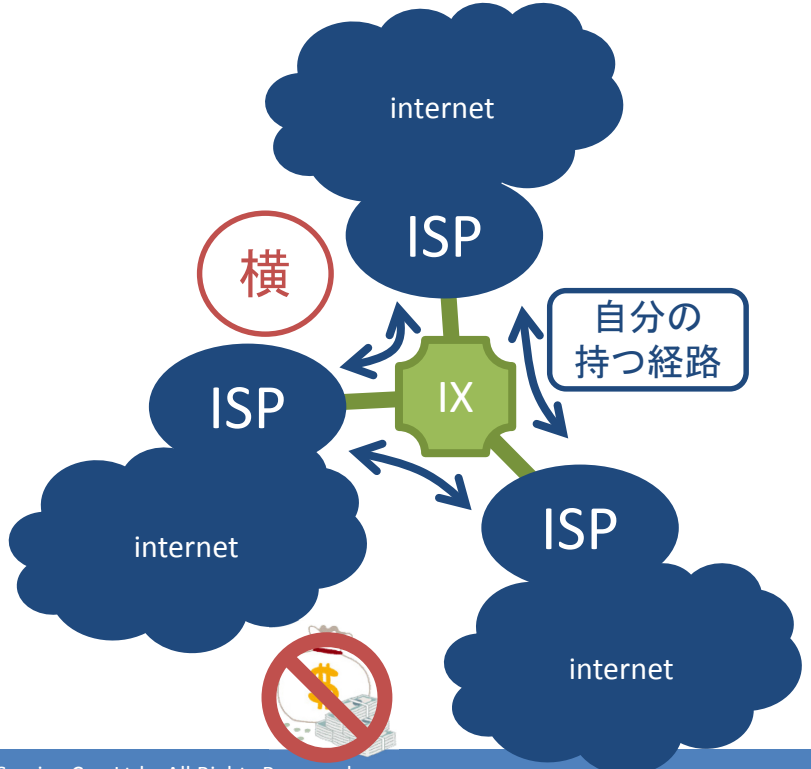
	トランジット	IXによるピアリング
経路情報	上位ISPが下位ISPにフルルートを流し、下位は上位に自分持っている経路を流す	お互いに自分の持っている経路を流す
接続相手との関係性	縦の関係	横の関係
お金	下位ISPが上位ISPにお金を払う	IX事業者に使用料を払えば、利用ASどうしは無料

日本のIX

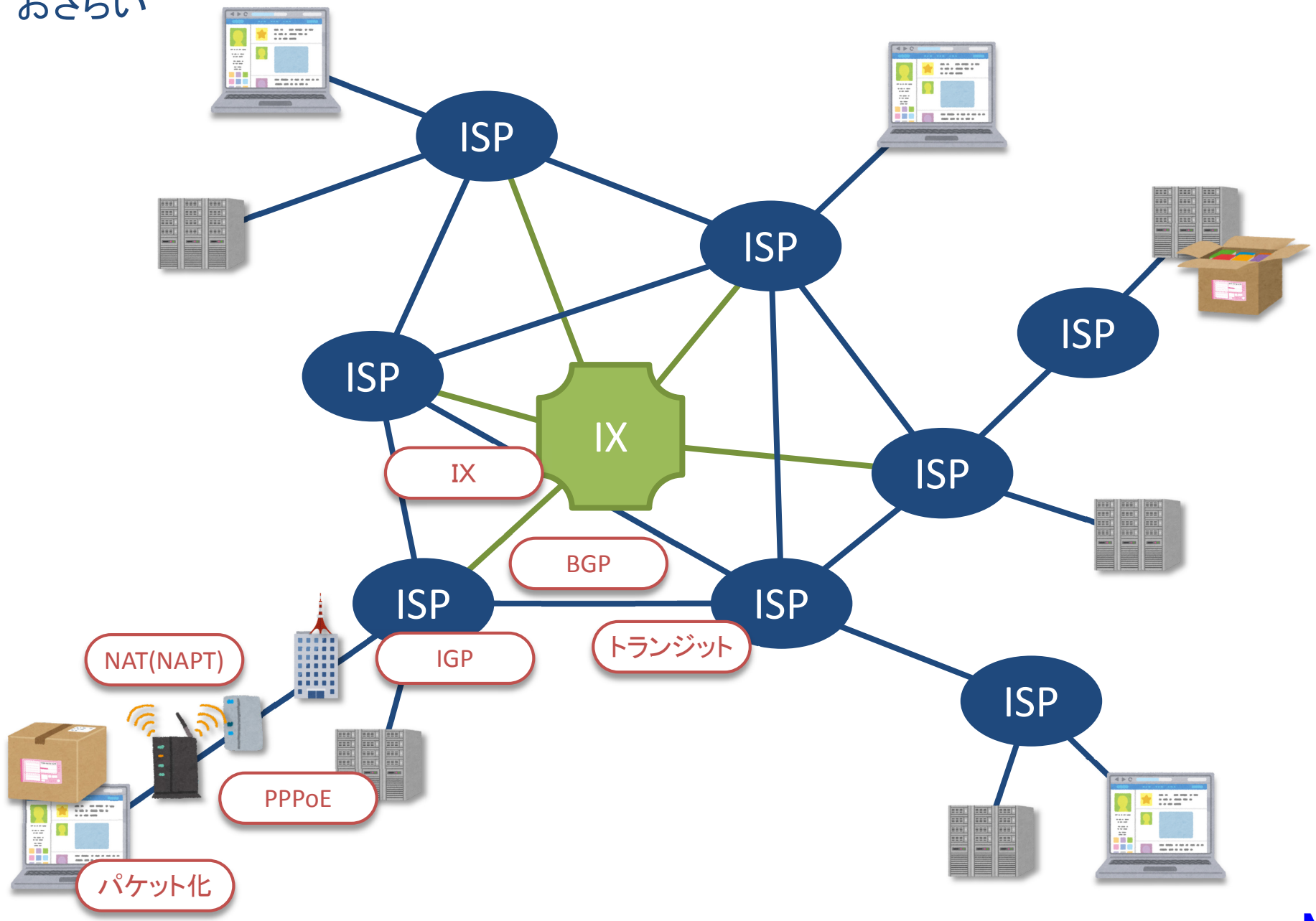
【広域】
BBIX
JPIX
JPNAP
他

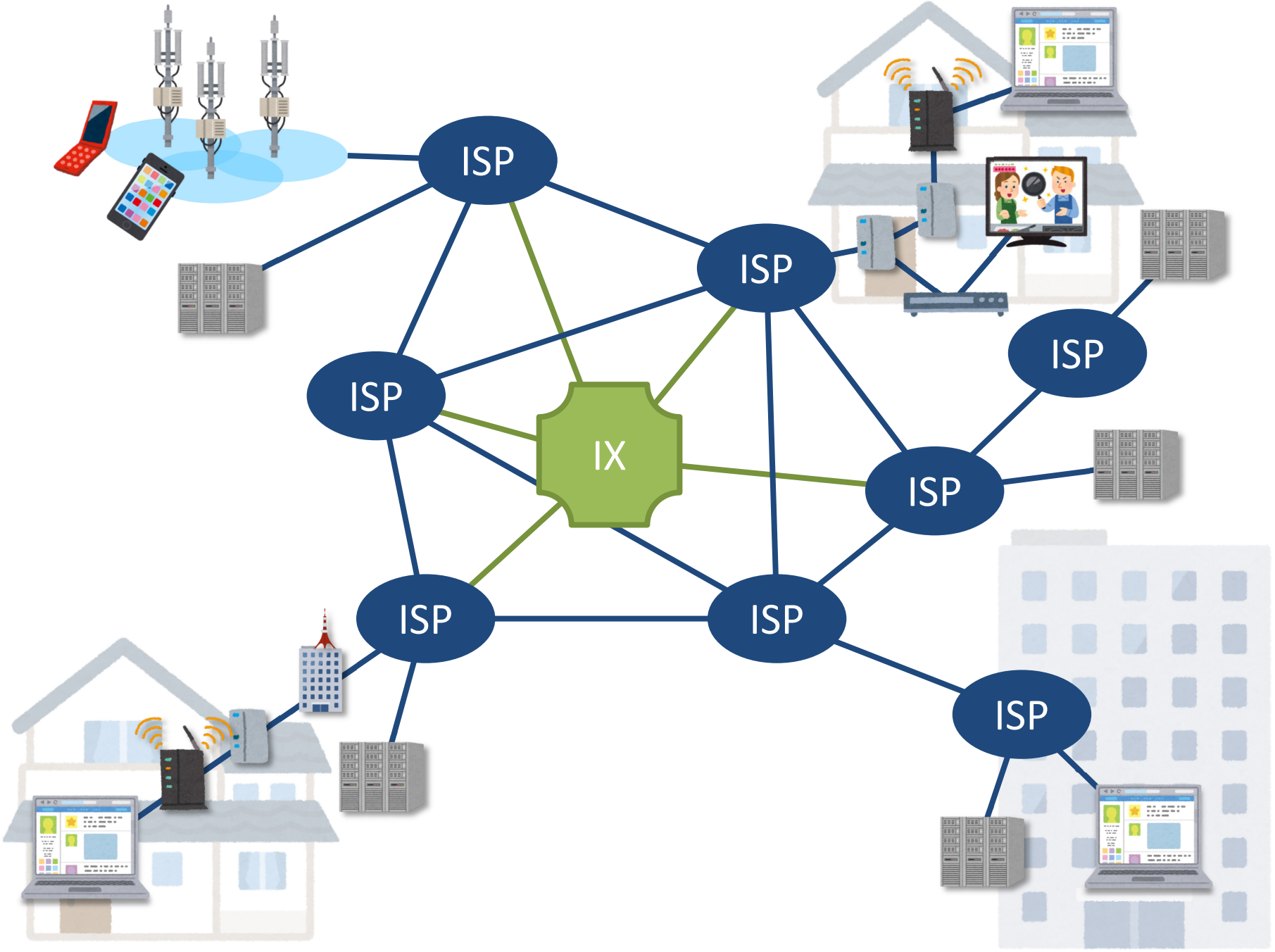
【地域】
Echigo-IX(新潟県)
OIX(沖縄県)
OKIX(岡山県)
YSN(山口県)
他





おさらい

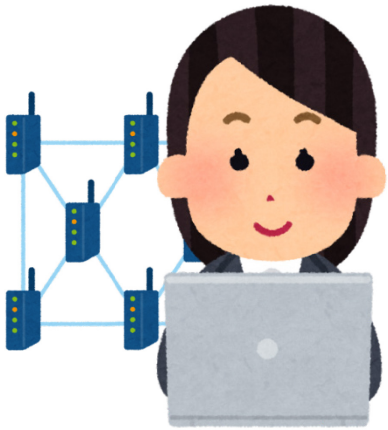




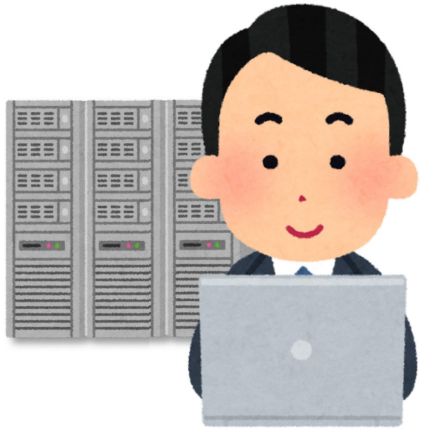
おまけ

CDN
Content Delivery Network

CDN事業者

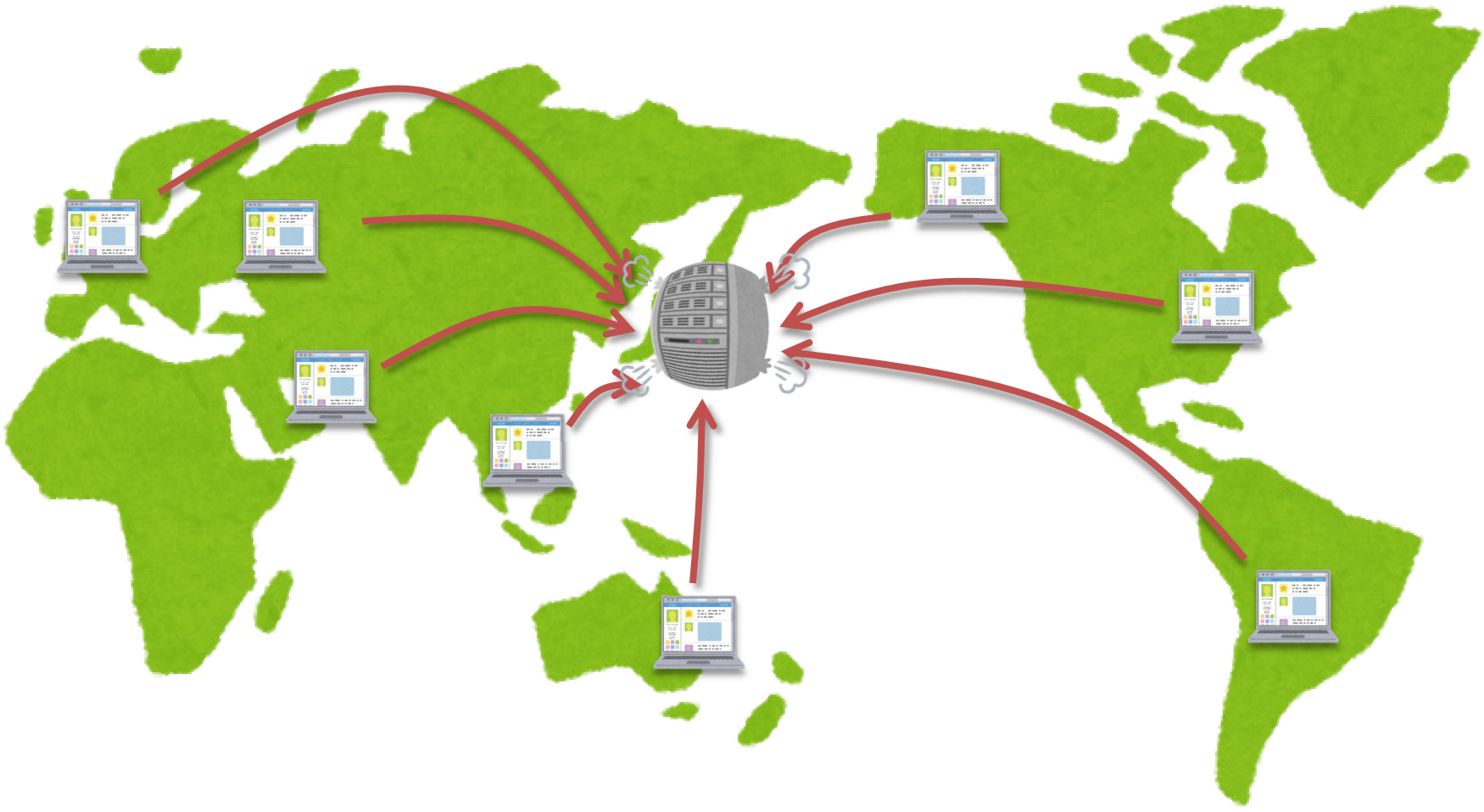


ネットワークエンジニア

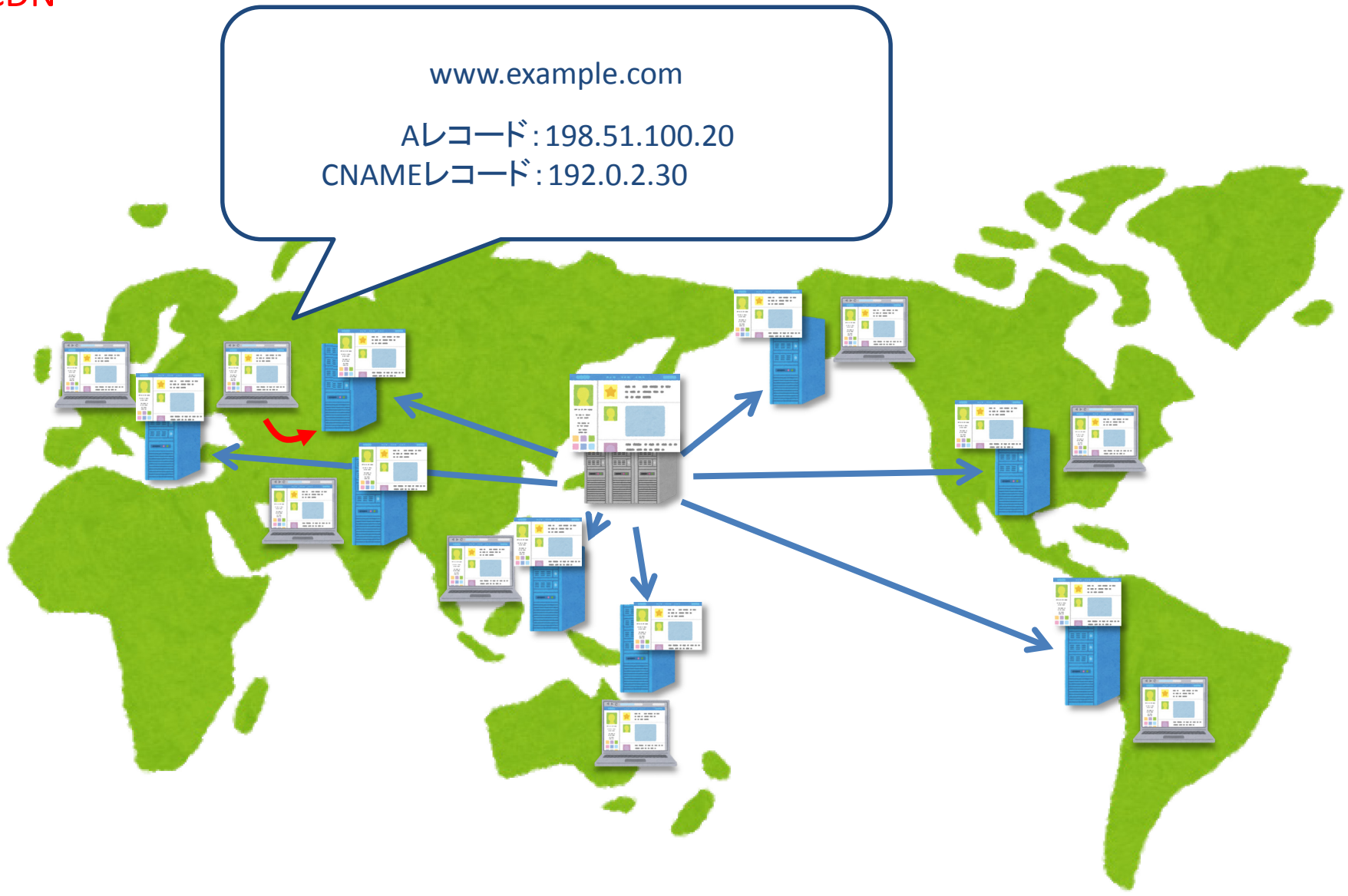


サーバーエンジニア

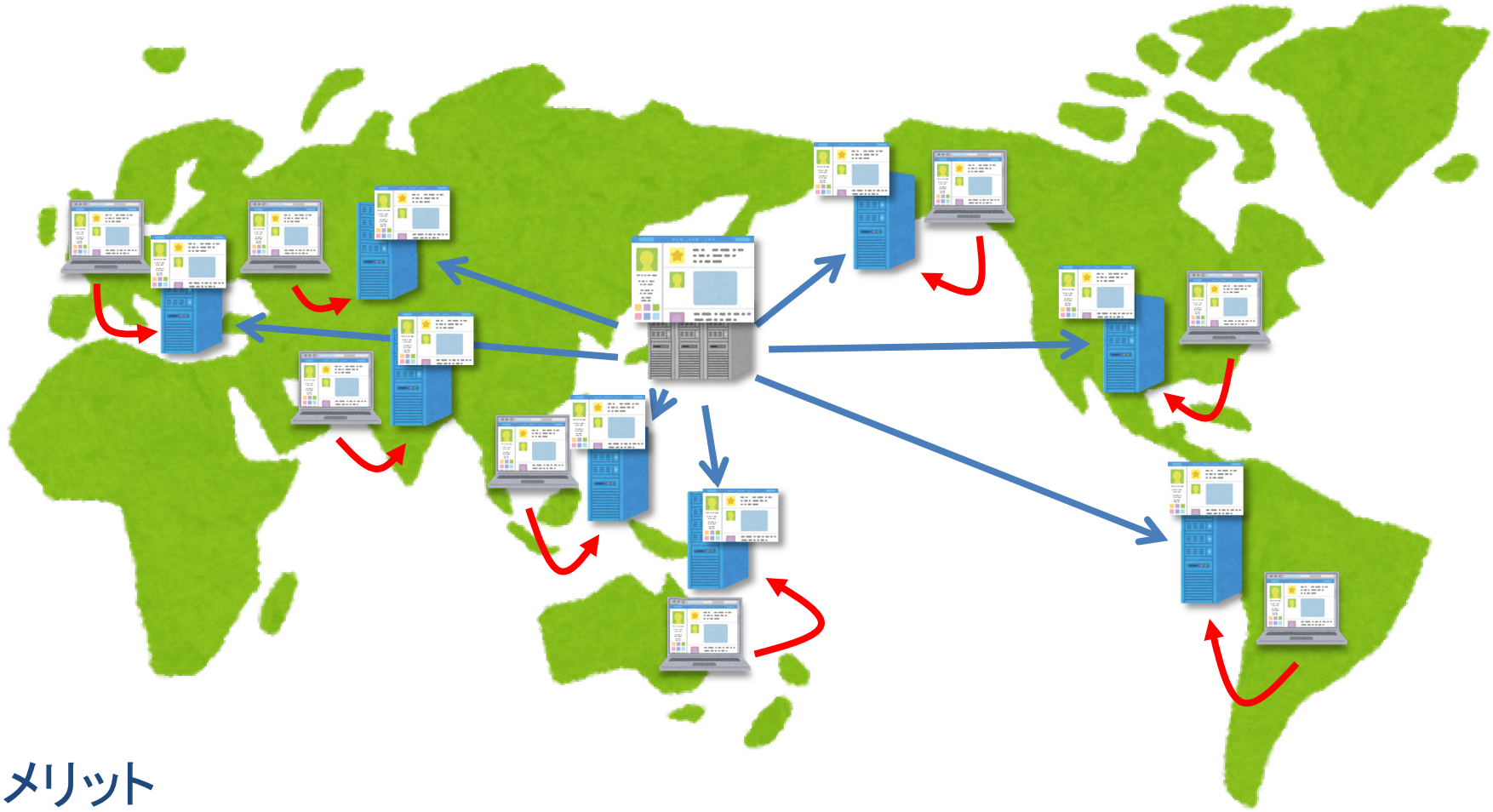
CDN



CDN



CDN



メリット

□レスポンスの向上
□ダウンロード速度の向上
■オリジンサーバーへのトラフィック集中回避
■サービスの耐障害性の向上

ご清聴ありがとうございました