

情報セキュリティ特論

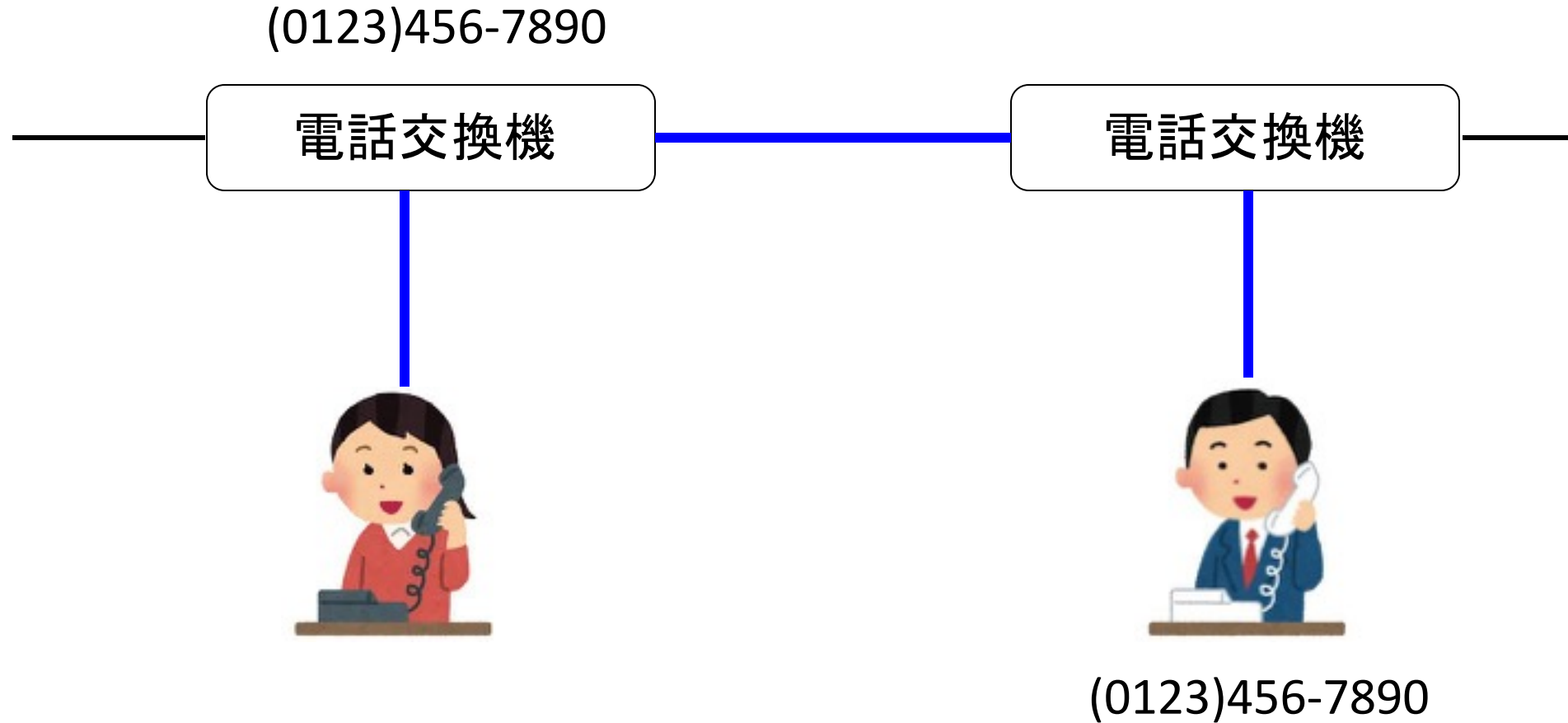
第3回

第3回：アクセス制御

今回の目標

- ・ ネットワーク
- ・ アクセス制御

電話のしくみ



ネットワーク通信

ネットワーク層

相手先のハードウェア的信息

送信元のハードウェア的信息

ネットワークの情報

送信元のIPアドレス

相手先のIPアドレス

プロトコルの情報

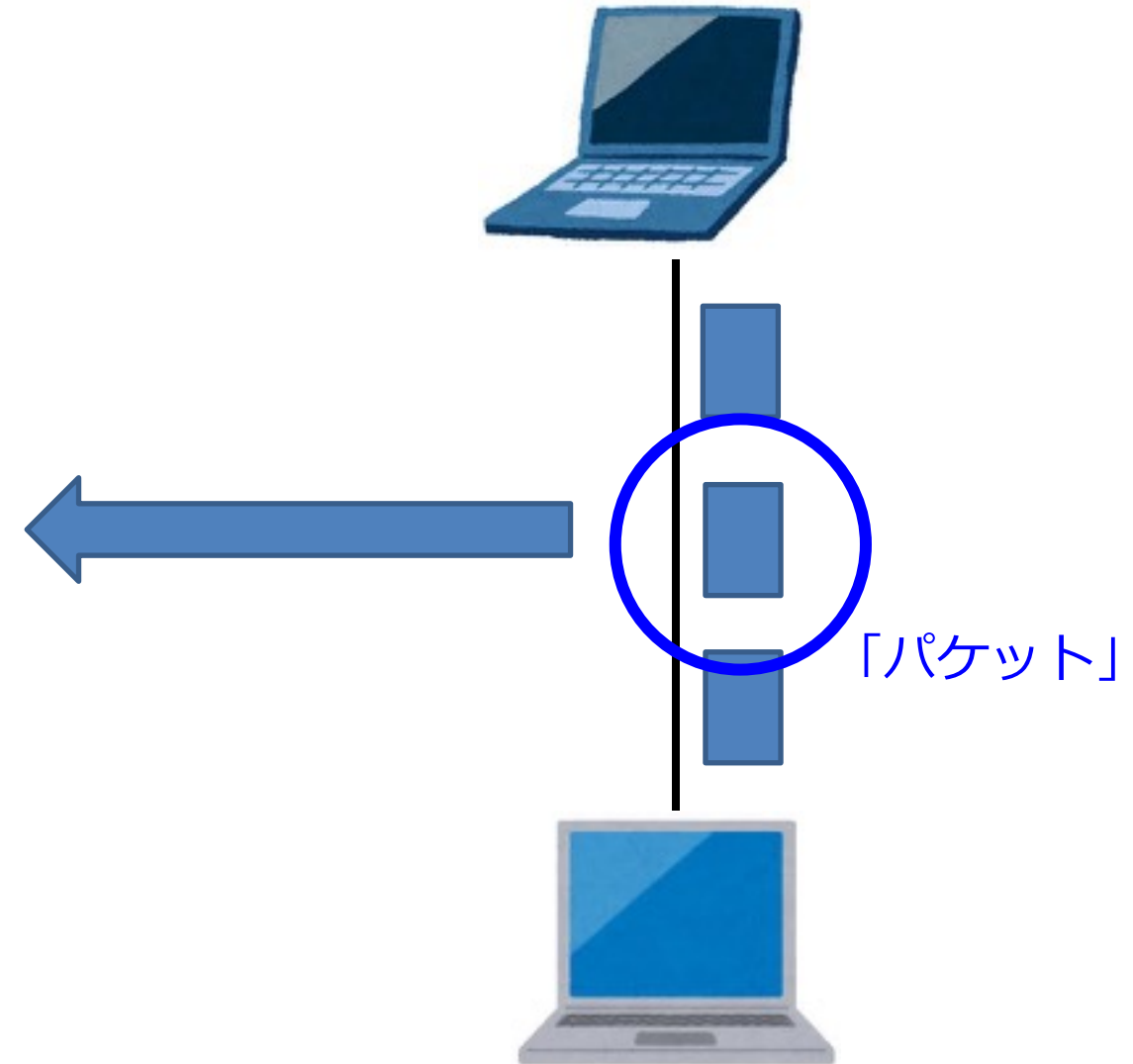
送信元のポート情報

相手先のポート情報

データ

FCS

トランスポート層



ネットワーク上の通信

パケットの通信にはTCP/IP（またはUDP）という規格での通信を行うのが一般的

Transmission Control Protocol / Internet Protocol

トランスポート層

ネットワーク層

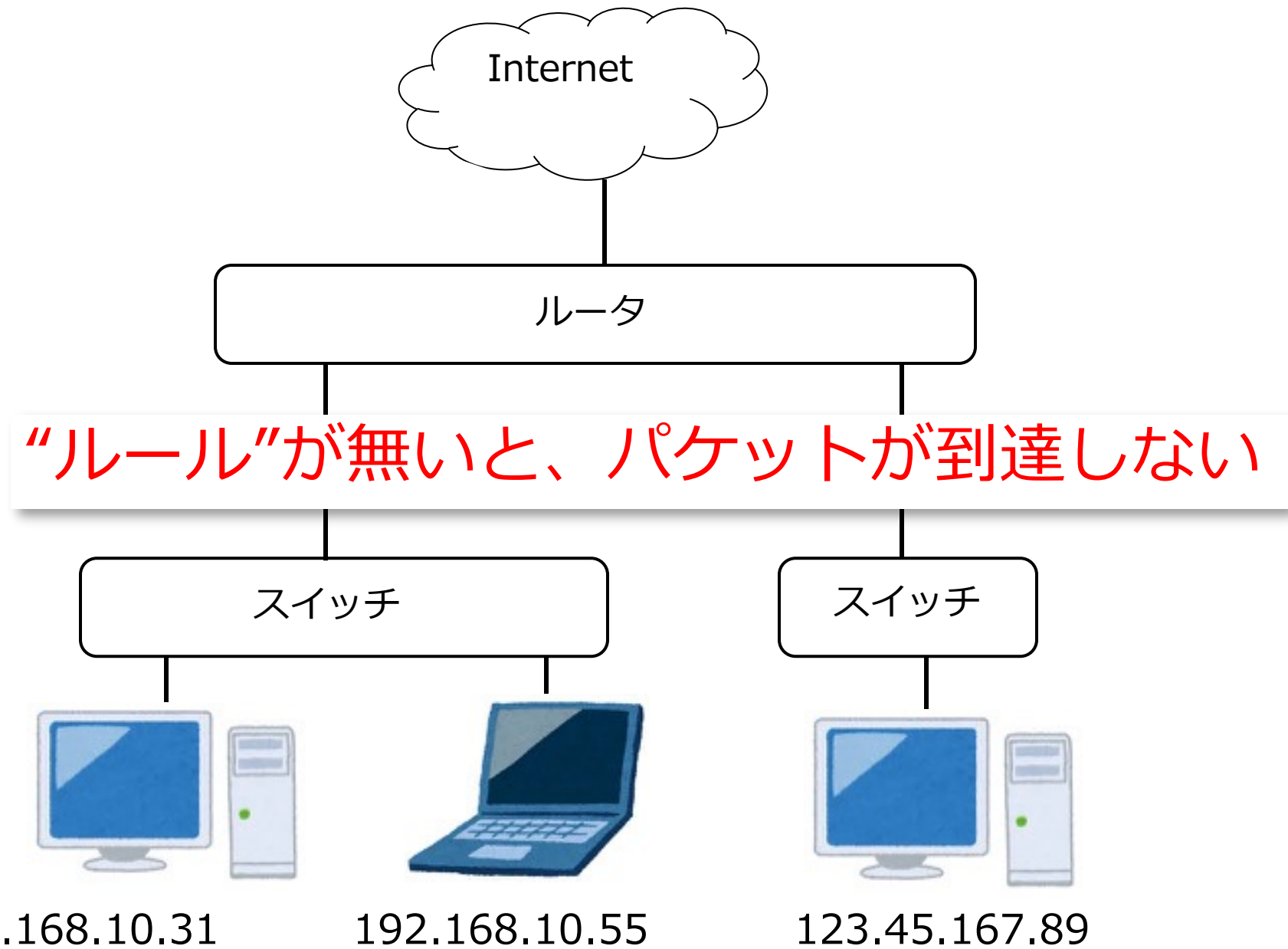
- ネットワーク層

ネットワークにおいて通信経路の選択。

- トランスポート層

ネットワークにおける通信管理。

TCPは、セッションという形で1対1の通信を実現し、エラー訂正機能などを持つ。



TCP/IPによる通信

“ルール”を設定して、パケットを目的のコンピュータへ届けるために

- 
- (I) IPアドレス
自分のアドレス
 - (II) サブネットマスク
ネットワークの「外側」と「内側」の区別
 - (III) デフォルトゲートウェイ（またはゲートウェイ）
パケットの「出口」のアドレス

この3つが最低でも必要

各項目の説明

(I) IPアドレス (IPv4の場合)

ネットワーク上のアドレス (電話番号や住所の様なもの)

“123.45.167.89” 4区画の数字の羅列で記述される。

IPv4では32bitなので各区画8bitずつになる (0-255)。

(原則として) 1つのIPは世界中で1つ (0.0.0.0 - 255.255.255.255)



原理的には約43億個で枯渇する

IPv6 : 128bit

3.4×10^{38} 個

「IPアドレス」は電話番号みたいなもの。
(市外局番や国番号といった部分も含む)

IPアドレス: 123.45.167.89



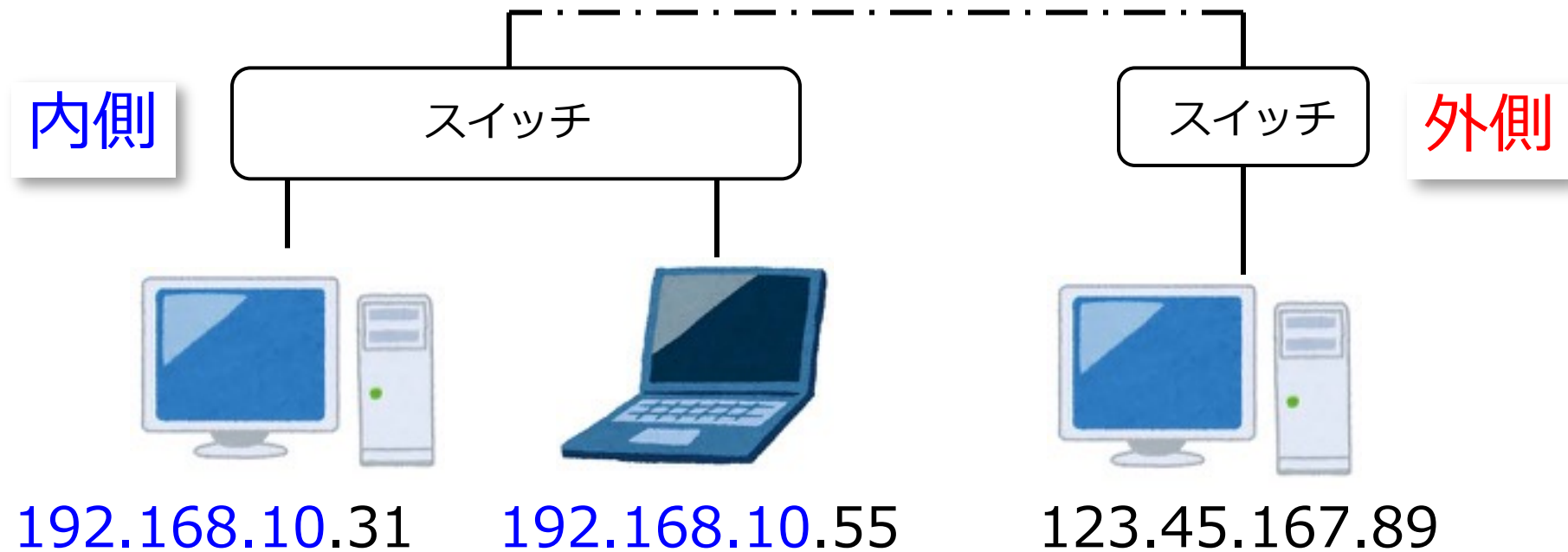
電話番号: +81-123-456-7890

国番号+市外局番+番号

(II) サブネットマスク

ネットワークの**内側**と**外側**を分けるマスク処理の為の数字

この数字と自分のIPアドレスの数字を2進数でAND処理し、出てきた数字が**ネットワークアドレス**、その他がホストアドレスとなる。



ネットワークの「内側」と「外側」

自分のIPアドレス: 192.168.10.31

サブネットマスク: 255.255.255.0

2進数に変換: 11000000.10101000.00001010.00001111 (192.168.10.31)
 11111111.11111111.11111111.00000000 (255.255.255.0)

AND処理 (1と1のとき1、それ以外は0)

11000000.10101000.00001010.00000000

ネットワークアドレス: 192.168.10.0

相手先IPアドレス: 192.168.10.55 「内側」

相手先IPアドレス: 123.45.167.89 「外側」

ネットワークの「内側」と「外側」

自分のIPアドレス: 192.168.10.31

ネットワークアドレス: 192.168.10.0

相手先IPアドレス: 192.168.10.55

ネットワークアドレスが同じなので「内側」
つまり、同じサブネット内に存在

相手先IPアドレス: 123.45.167.89

ネットワークアドレスが違うので「外側」
つまり、別のサブネットに存在



「外側」のときはパケットの出口の指定が必要

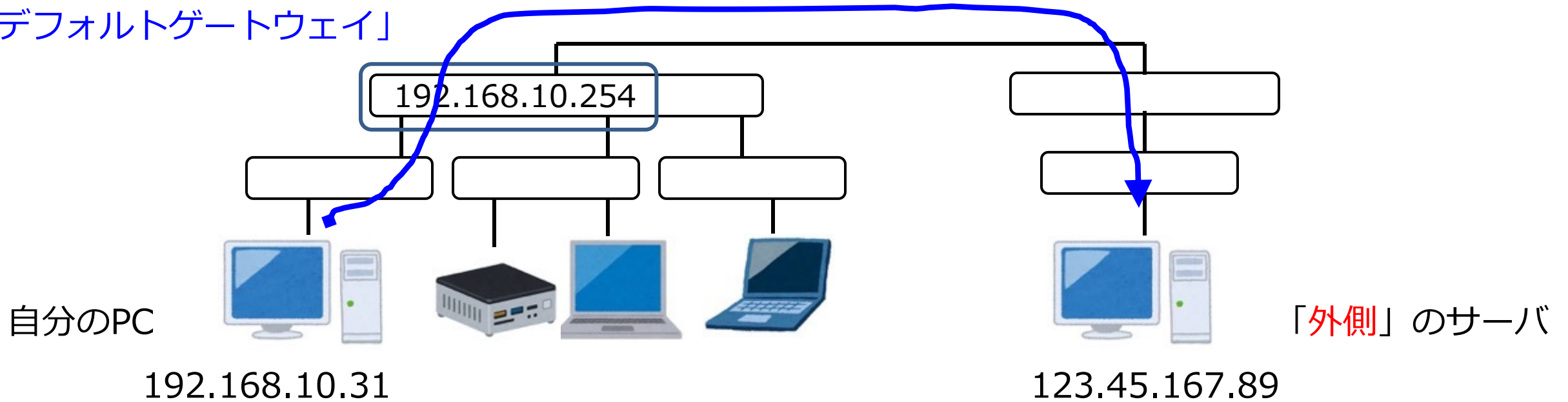
(III) デフォルトゲートウェイ

パケットがどこを**通って外に出るか**を決めるもの。

192.168.10.254

となっている場合、「192.168.10.254」のIPアドレスが
パケットを外に出すための出口になる。

「デフォルトゲートウェイ」



TCP/IPによる通信

“ルール”を設定して、パケットを目的のコンピュータへ届けるために

- 
- (I) IPアドレス
自分のアドレス
 - (II) サブネットマスク
「外側」と「内側」の区別
 - (III) デフォルトゲートウェイ (またはゲートウェイ)
パケットの出口はどこか

この3つが最低でも必要

しかし通常は「IPアドレスを自動的に取得する」とすることが多い

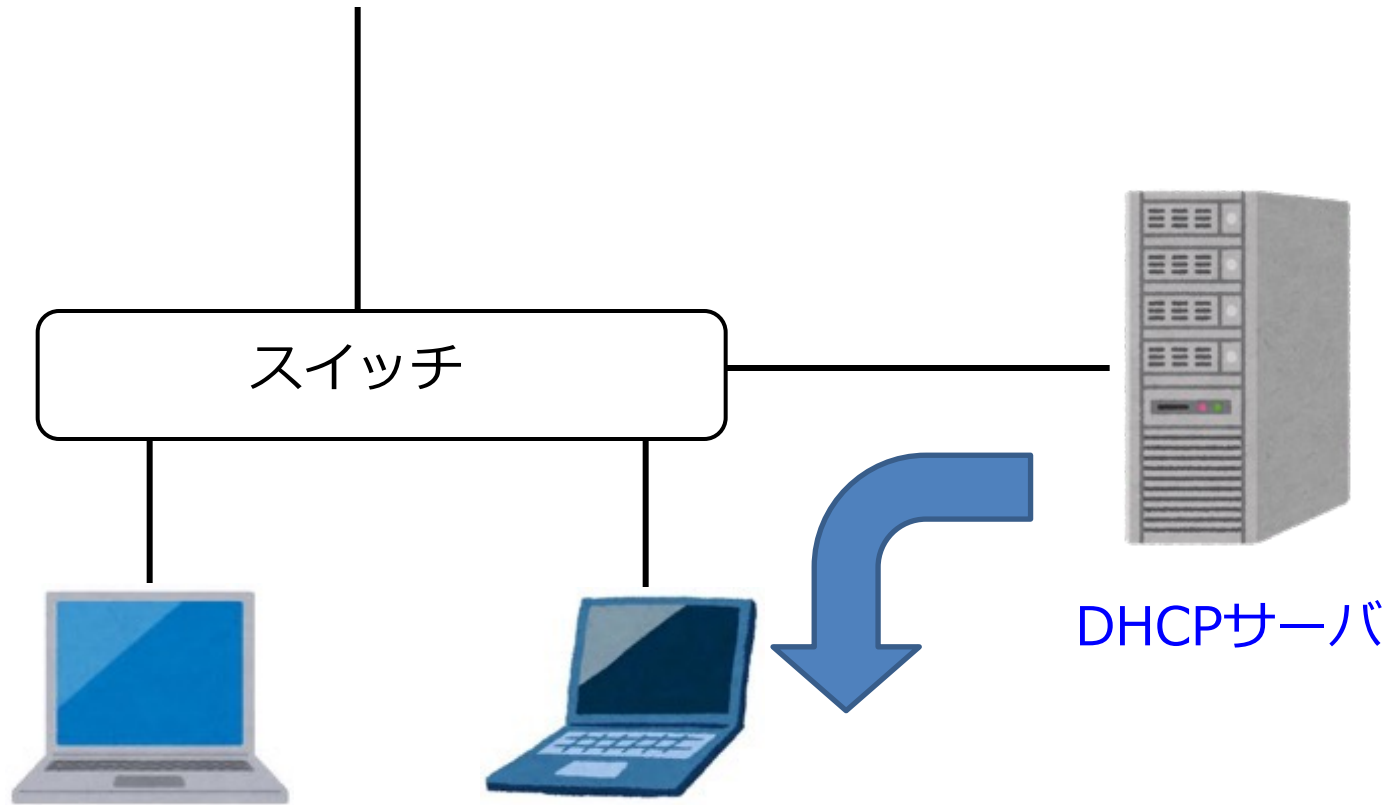


インターネット通信に必要な設定を自動で取得する仕組みがある

DHCPとよばれるプロトコルを使い、

- (I) IPアドレス
- (II) サブネットマスク
- (III) デフォルトゲートウェイ

を自動的に設定する。



“自動的に取得する”

- | | |
|--------------|----------------|
| •IPアドレス | 192.168.10.55 |
| •サブネットマスク | 255.255.255.0 |
| •デフォルトゲートウェイ | 192.168.10.254 |

さらに、「IPアドレス」を直接使わない

そんな、IPアドレス指定なんかまどろっこしくてやってられない、、、

www.kitami-it.ac.jp

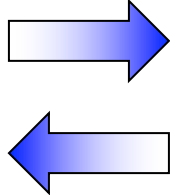
www.amazon.com

youtube.com

等、IPではなく名前でアクセスするのが普通

ネームサーバ

そこで、名前からIPアドレス(あるいはその逆)に変換してくれるサーバが必要。

www.hogehoge.ac.jp  123.45.167.89

この機能を持つサーバを

DNS(Domain Name Server)

「ドメインネームサーバ」と呼ぶ

“Domain(ドメイン)”

インターネットにおける住所のようなもの

www.hogehoge.ac.jp

jp: トップレベルドメイン

.jp、.uk、.fr等の国と、
.com、.org等の一般的分類がある。

ac: セカンドレベルドメイン

各トップドメインの管轄下で決められた分類

.acは4年大学が中心

2. アクセス制御

システムアクセス制御

「認証」と「認可」

認証:

ユーザがログインできるか識別すること

通常、IDとパスワード等で識別（前回の他要素認証）

認可:

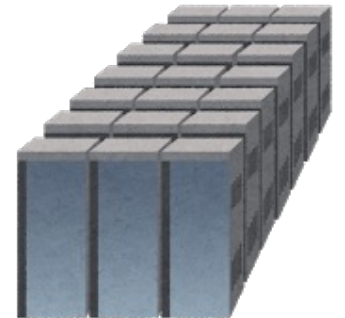
そのユーザにどのシステム（機能）を利用させるか決定すること

通常、認証後に行われる

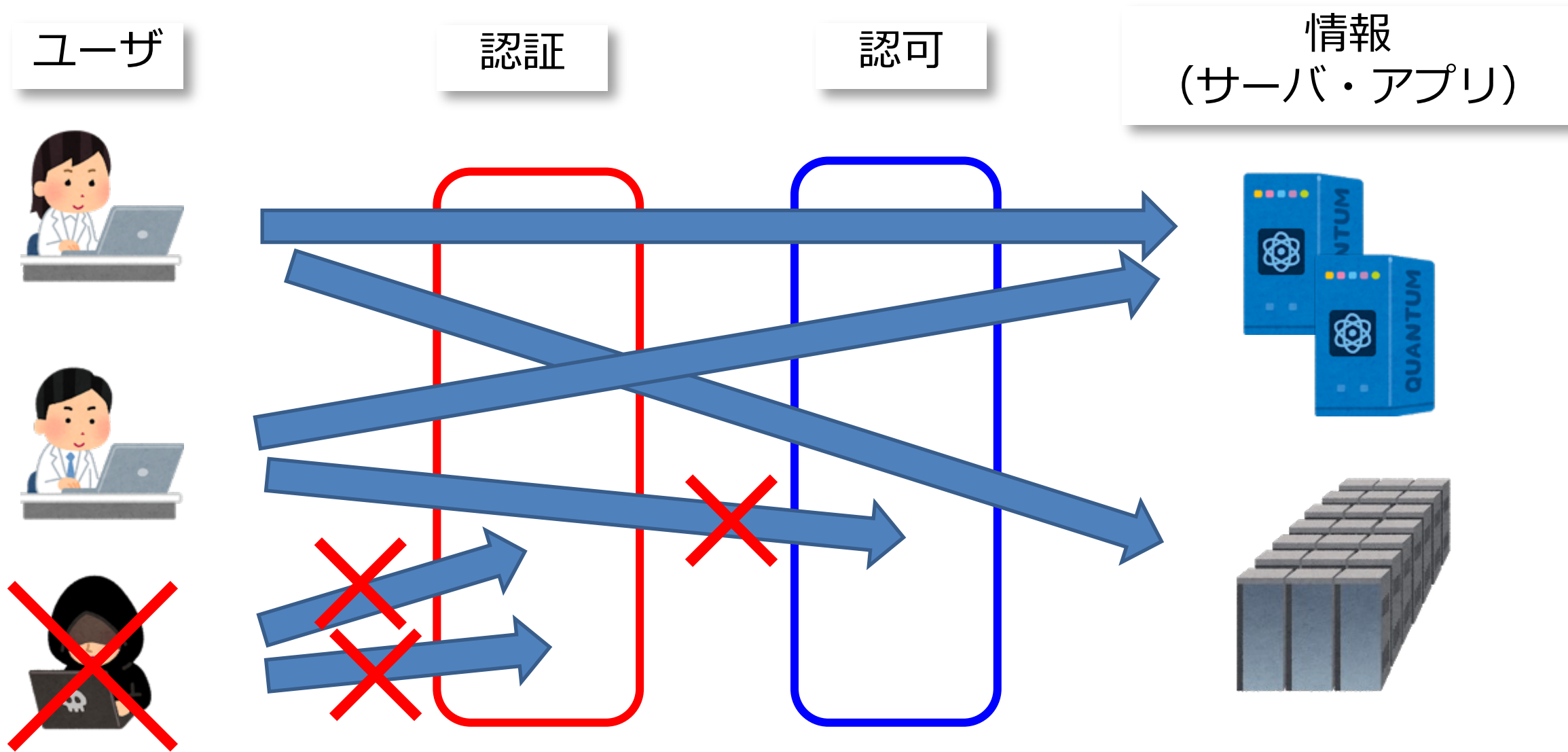
ユーザ



情報
(サーバ・アプリ)



全てのユーザが全ての情報へアクセスできてしまう



ユーザ毎に利用できる情報を制御

認証：ログインのアクセス制御

ID管理

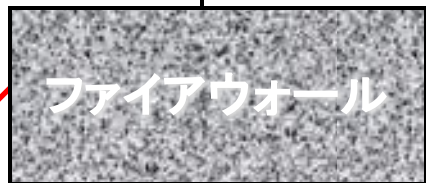
パスワード管理

認証方式の複雑化（多要素認証）

- ・ 簡単な文字列にしない
- ・ 初期パスワードのままにしない
「定期的な変更」は必ずしも良い結果になるとは限らない
- ・ 同じパスワードを別サービスで使わない
- ・ 他人に教えない、紙に書いておかない

- WWW (http)
- メール (SMTP)
- その他の通信

遮断



- WWW (http)
- メール (SMTP)
- その他公開できるもの

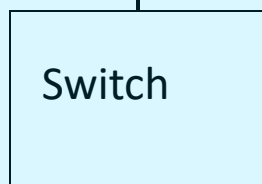
公開用区画

- Webサーバ
- メールサーバ

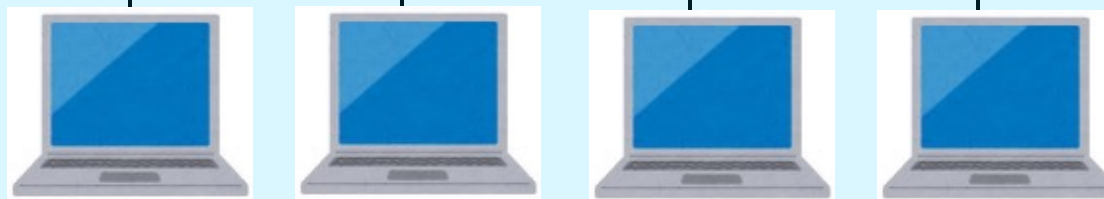
「公開用区画」との
アクセスのみ許可

- WWW (http)
- メール (SMTP)

学内ネットワークが安全に保たれる



学内ネットワーク



ネットワークのアクセス制御

- ・ファイアウォール

ネットワーク上の通信を制御

- ・ネットワークアドレス変換

外部からIPアドレスを指定してアクセスできないようにする

IPv4のIP枯渇問題を解消する

NAT: Network Address Translation

NAPT: Network Address Port Translation

今は一般的に「NAT」と呼ぶ

各項目の説明

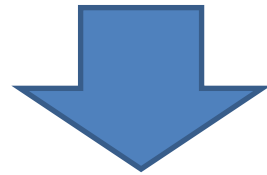
(I) IPアドレス (IPv4の場合)

ネットワーク上のアドレス (電話番号や住所の様なもの)

“123.45.167.89” 4区画の数字の羅列で記述される。

IPv4では32bitなので各区画8bitずつになる (0-255)。

(原則として) 1つのIPは世界中で1つ (0.0.0.0 - 255.255.255.255)



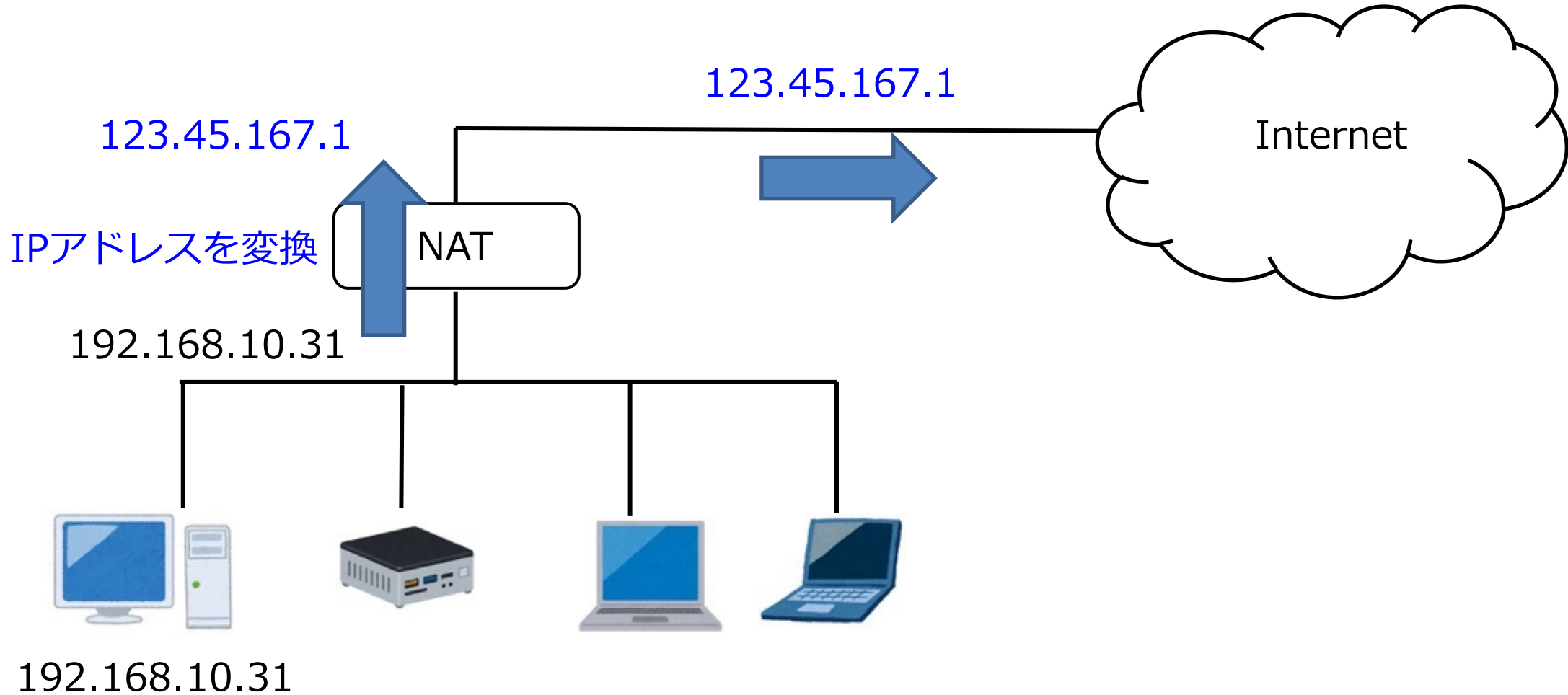
原理的に約43億個で枯渇する

IPv6 : 128bit

3.4×10^{38} 個

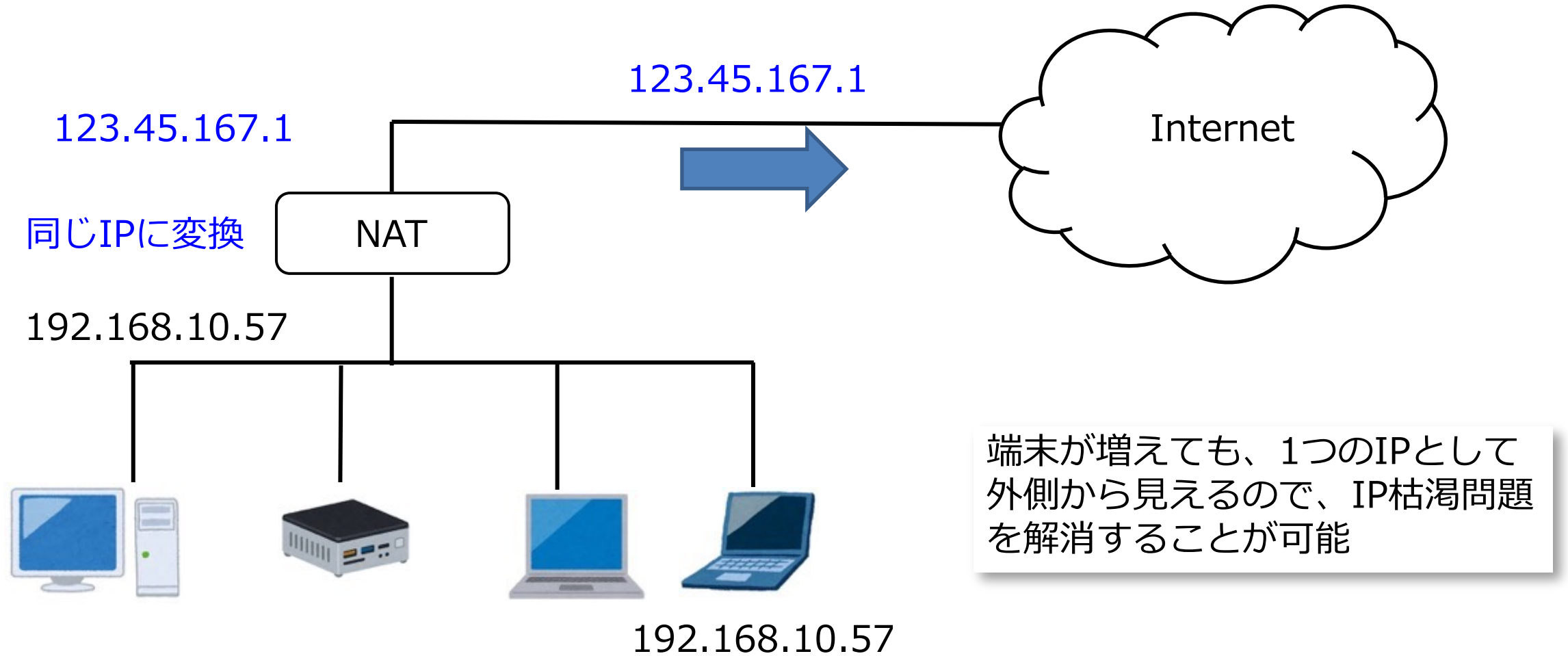
NAT

ネットワークの「内側」と「外側」でIPアドレスを変換する技術



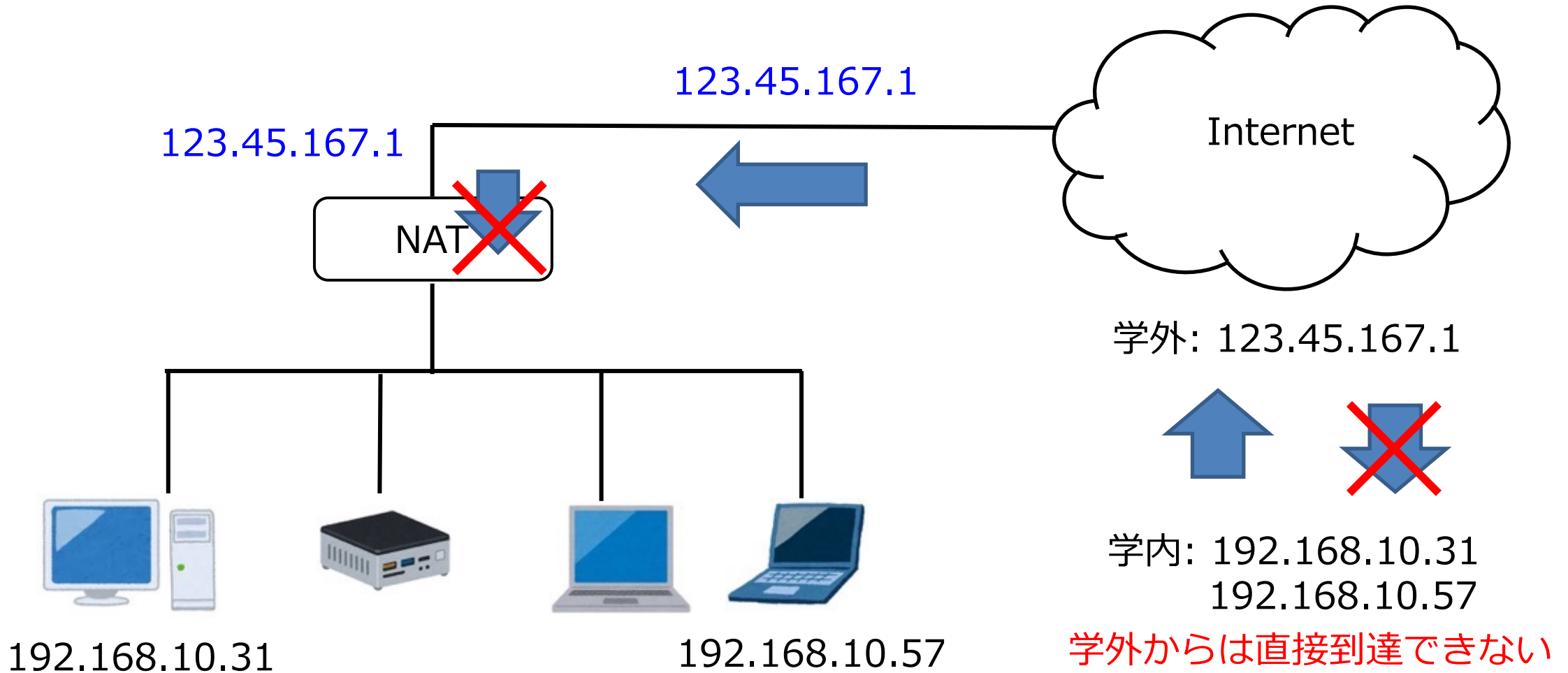
NAT

ネットワークの「内側」と「外側」でIPアドレスを変換する技術



NAT

ネットワークの「内側」と「外側」でIPアドレスを変換する技術



VPN

Virtual Private Network

- ・ファイアウォールを跨いで仮想ネットワークを構築する技術
- ・暗号化通信と組み合わせ、安全に通信を確立するのに用いられる

使用例)

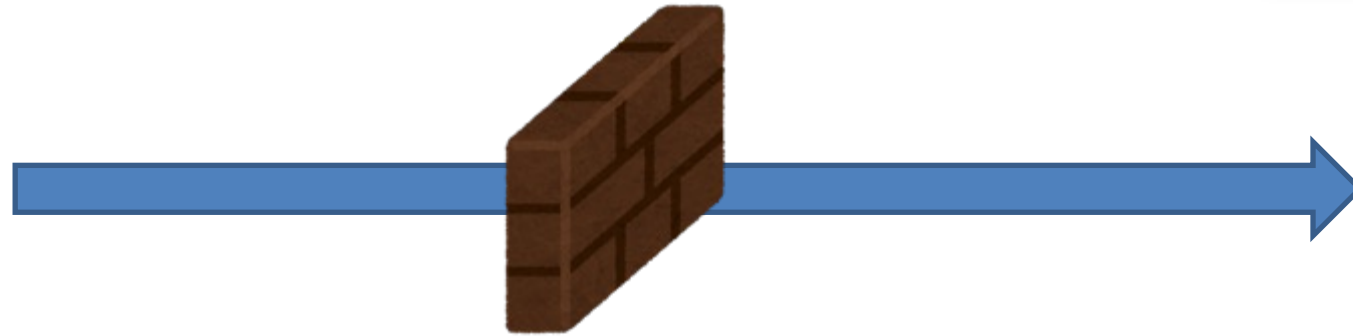
学外から学内の重要なサーバへログインする

大学間で同じネットワーク（IPアドレス帯）を使う

ユーザ



ファイアウォール



情報
(サーバ・アプリ)



通常はファイアウォールで
通信が遮断される

ファイアウォールまたはVPN専用装置に
認証情報を与え（ログイン等）、ユーザ
と「情報」の間に特別な通信を作成する。

