NATのしくみと NAT越え技術

150441104　成瀬　哲

概要

- NAT：Network Address Translation(ネットワークアドレス変換)
- 末端機器(PC)とインターネットの間で、パケット中のIPアドレス(とポート番号)を変換する技術
  - プライベートIPアドレスを持つ機器が、インターネットと双方向通信することが可能になる
- 分類
  - 静的・動的
  - Symmetric型・Cone型

プライベートIPアドレスについて

- インターネットに対して非公開のコンピュータネットワーク内で用いられるIPアドレス
- ネットワーク内では一意だが、他ネットワークでは重複している可能性がある

- 利点
  - グローバルIPアドレスの浪費を防ぐ
  - セキュリティ確保
  - IPアドレス管理団体の許可が不要

概要

- NAT：Network Address Translation(ネットワークアドレス変換)
- 末端機器(PC)とインターネットの間で、パケット中のIPアドレス(とポート番号)を変換する技術
  - プライベートIPアドレスを持つ機器が、インターネットと双方向通信することが可能になる
- 分類
  - 静的・動的
  - Symmetric型・Cone型

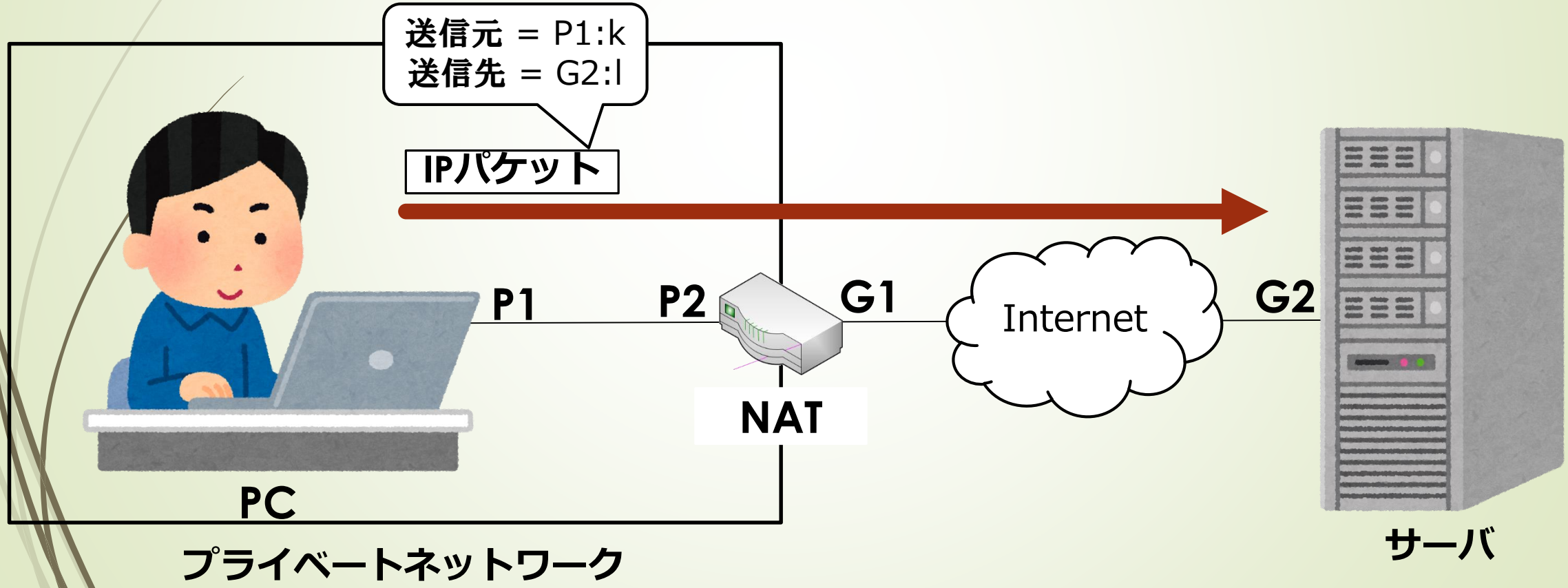
分類について

- 静的・動的
  - 静的：管理者があらかじめ変換を設定しておく方法
  - 動的：NATで使用するIPアドレスのプールを設定する方法

- Symmetric型・Cone型
  - Symmetric型：宛先ごとにアドレス変換を生成
  - Cone型：宛先に関わらず、唯一のアドレス変換を生成

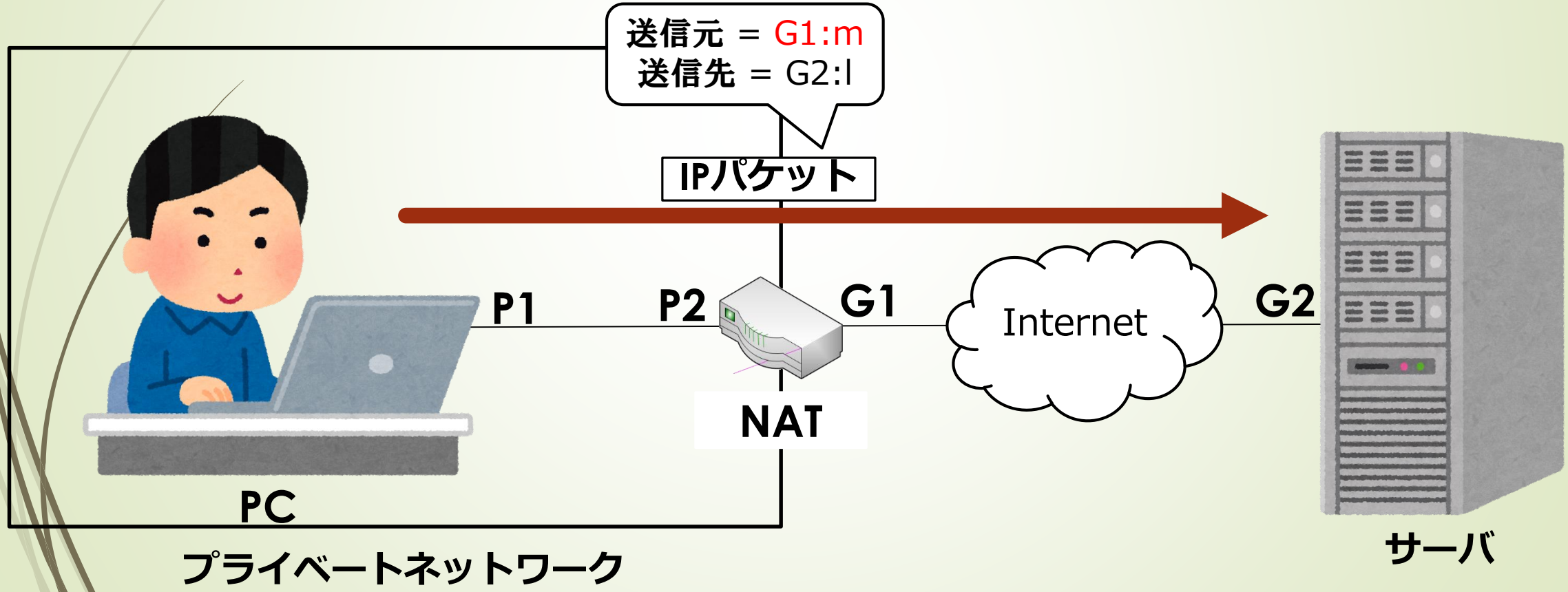
Symmetric型の動作(送信の場合)

①PCからプライベートIPアドレスを用いて、
インターネット上のサーバにパケットを送信する



Symmetric型の動作(送信の場合)

②NAT通過時、パケットの送信元アドレスとポート番号を変換して転送する

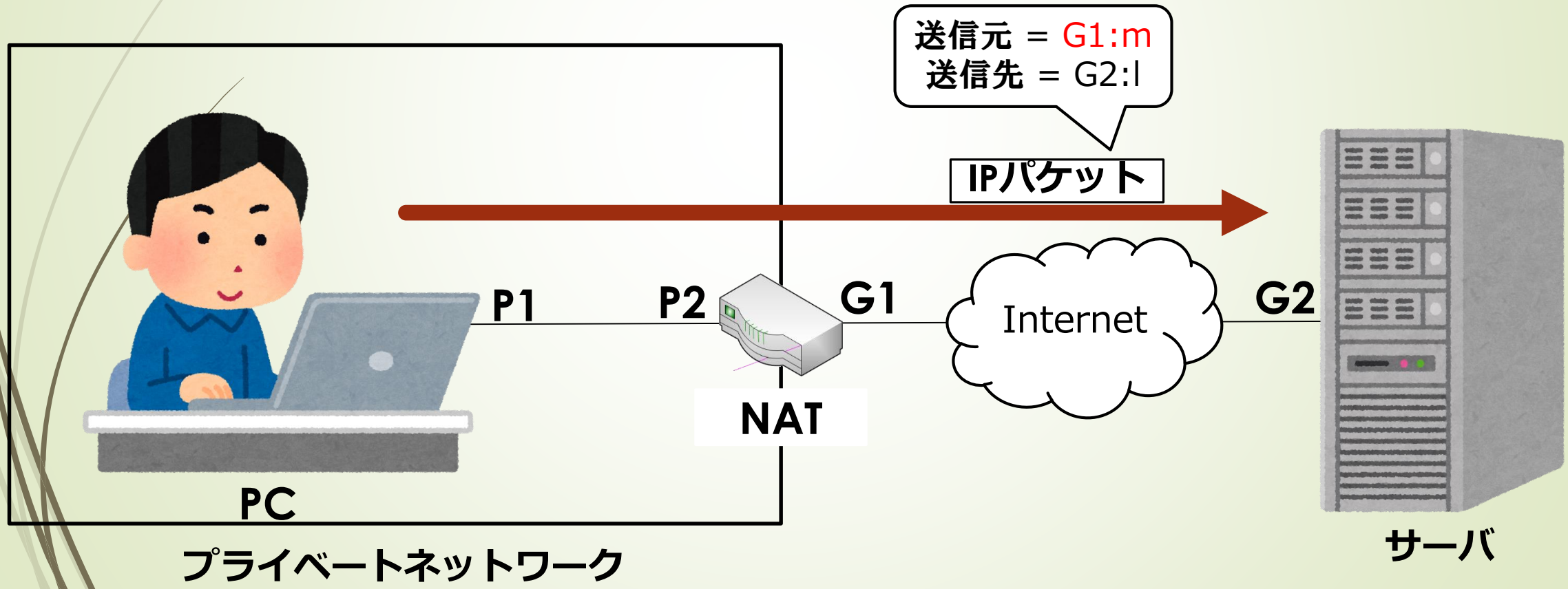


Symmetric型の動作(送信の場合)

③NATテーブルに
変換情報とフィルタリングを記述する

NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m

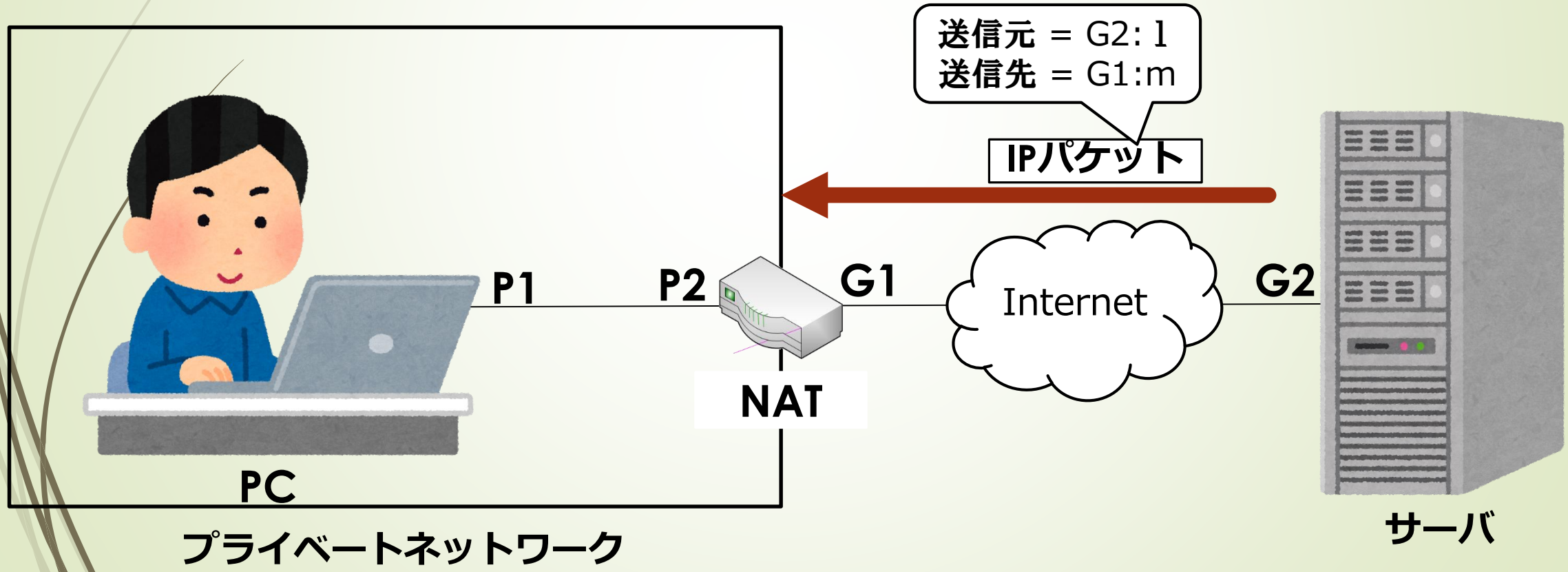


Symmetric型の動作(受信の場合)

NATテーブルのフィルタリングに記述されている相手からの通信は成立する

NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m

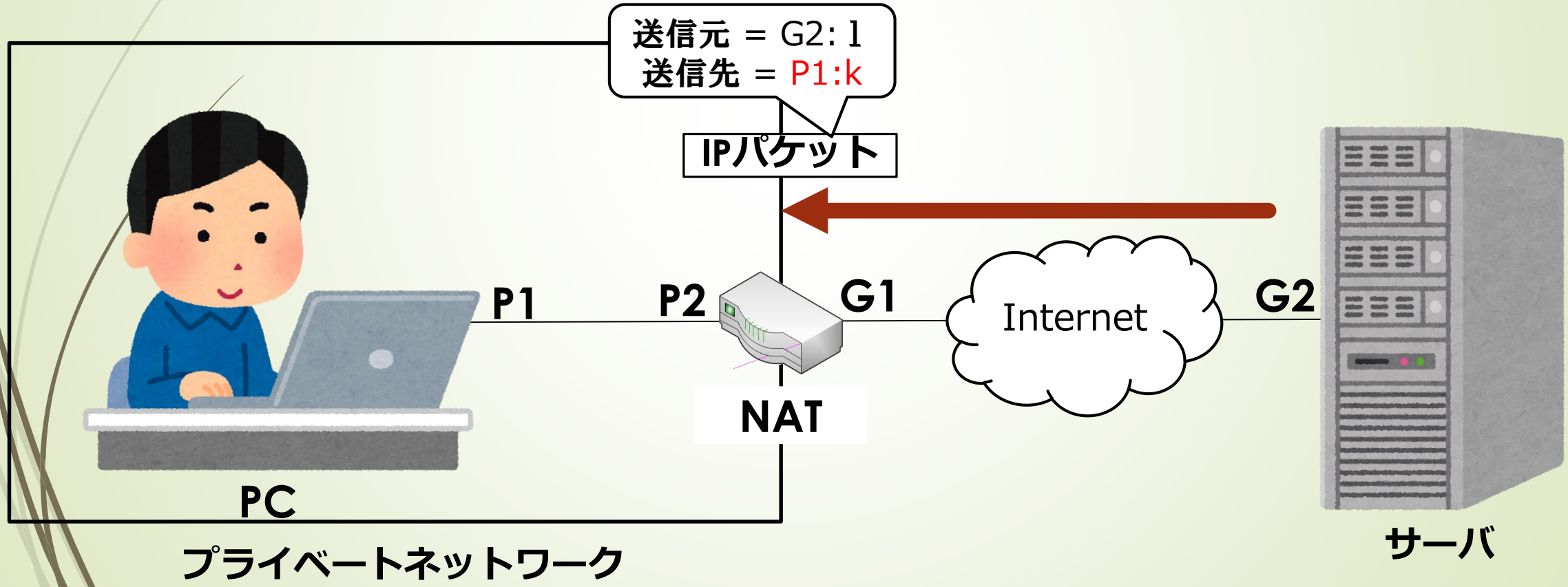


Symmetric型の動作(受信の場合)

NATテーブルのフィルタリングに記述されている相手からの通信は成立する

NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m

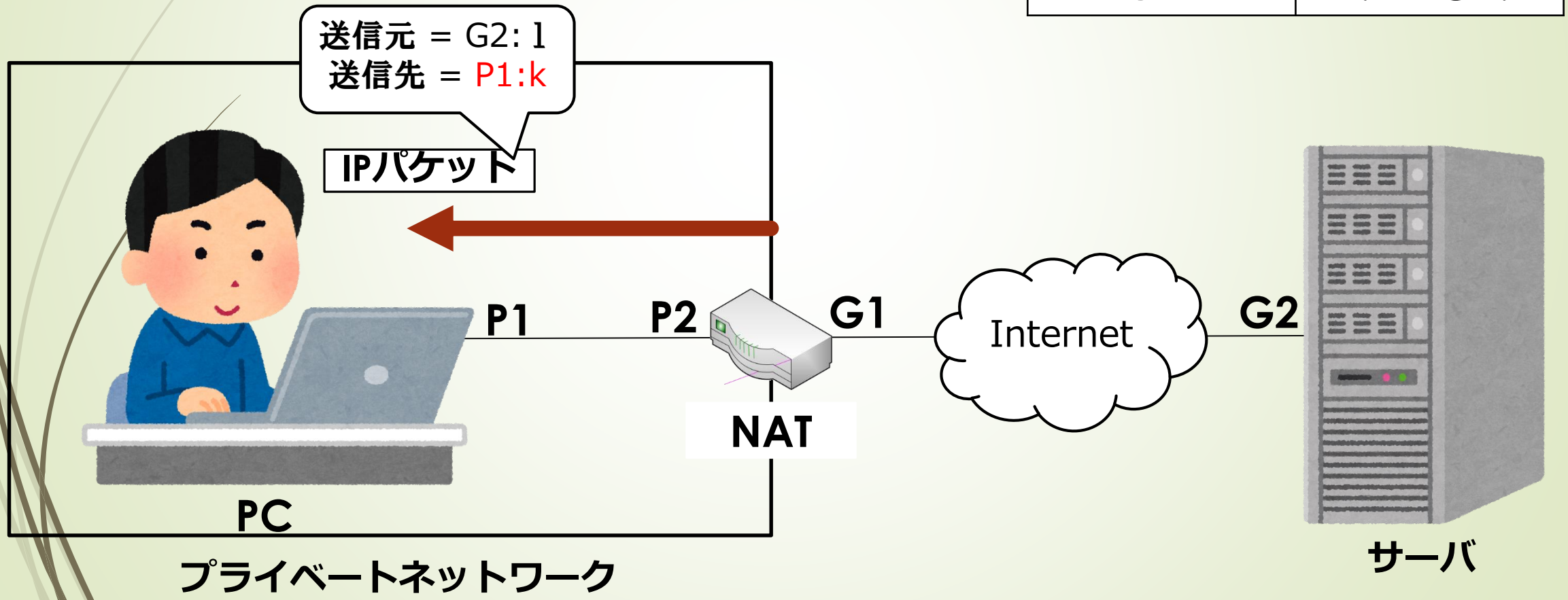


Symmetric型の動作(受信の場合)

NATテーブルのフィルタリングに記述されている相手からの通信は成立する

NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m

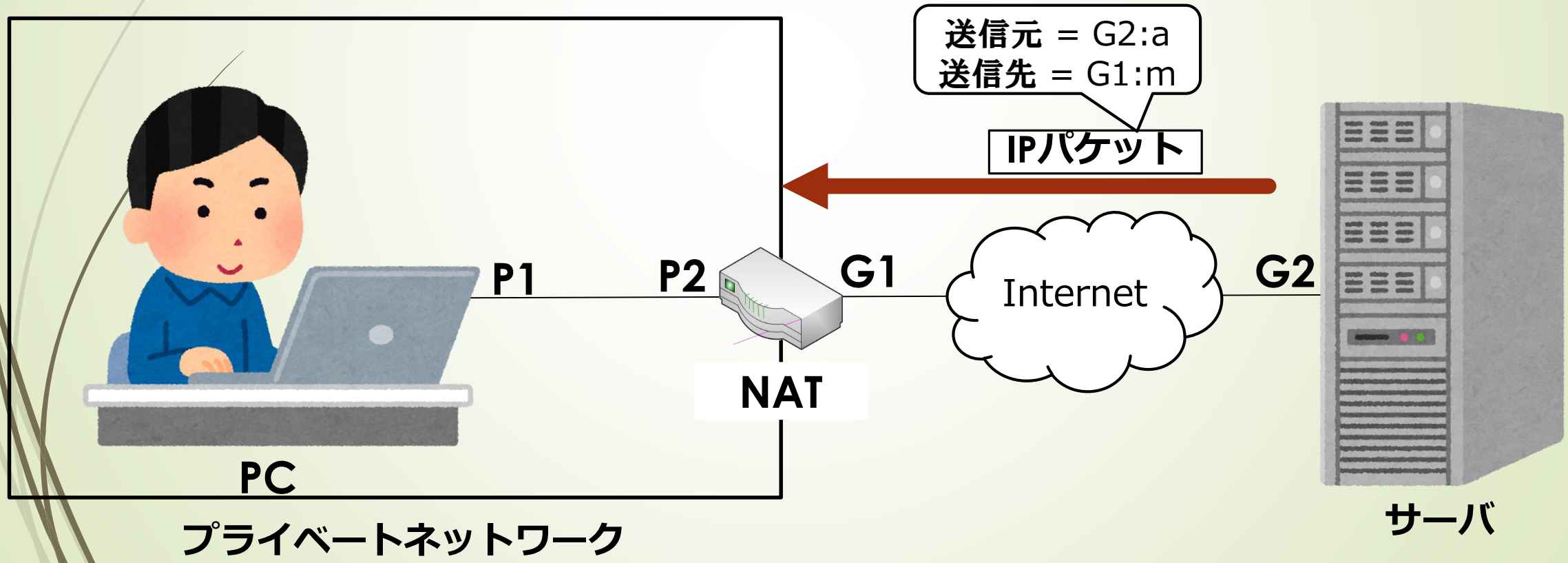


Symmetric型の動作(受信の場合)

NATテーブルのフィルタリングに記述されていない相手からの通信は破棄する

NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m

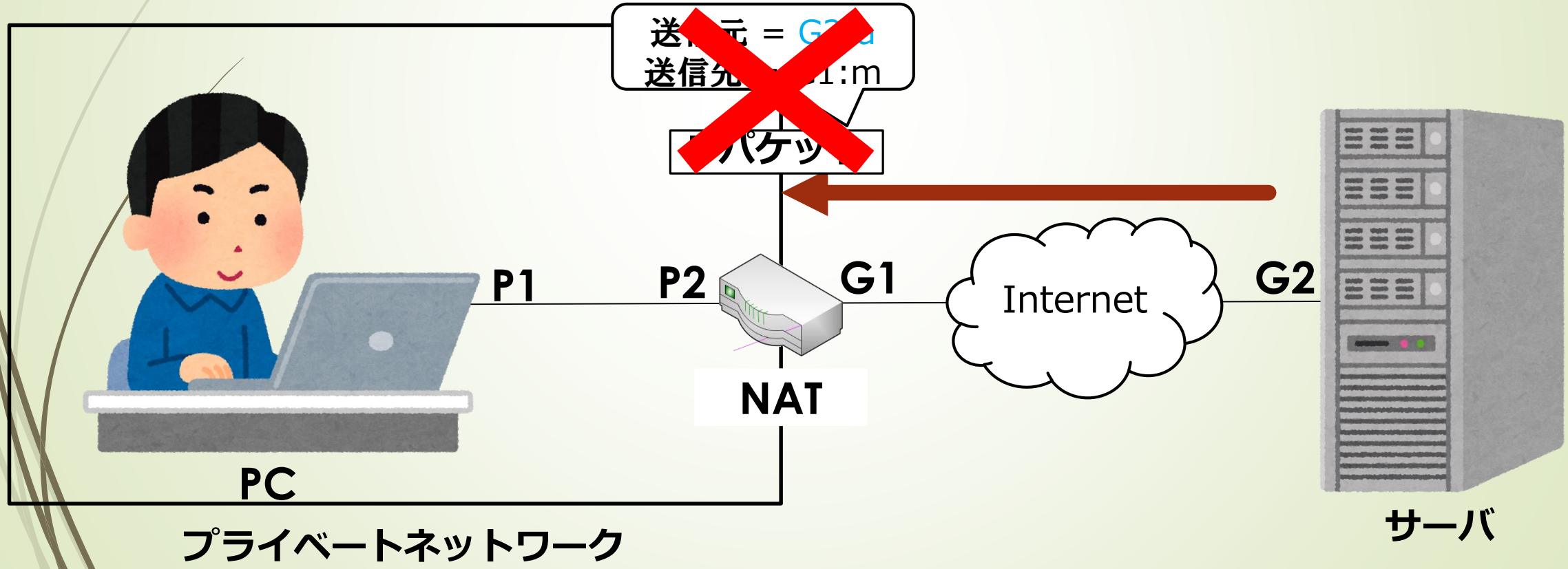


Symmetric型の動作(受信の場合)

NATテーブルのフィルタリングに記述されていない相手からの通信は破棄する

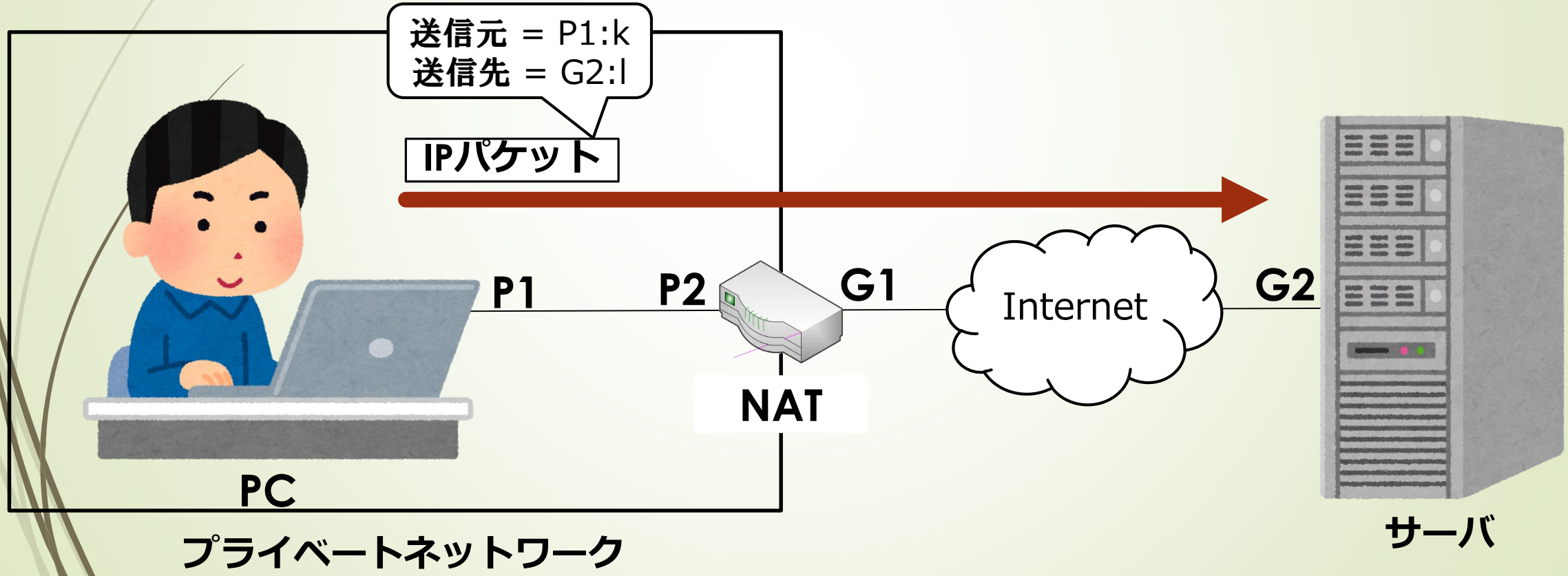
NATテーブル

フィルタリング	変換情報
G2:l	P1:k⇔G1:m



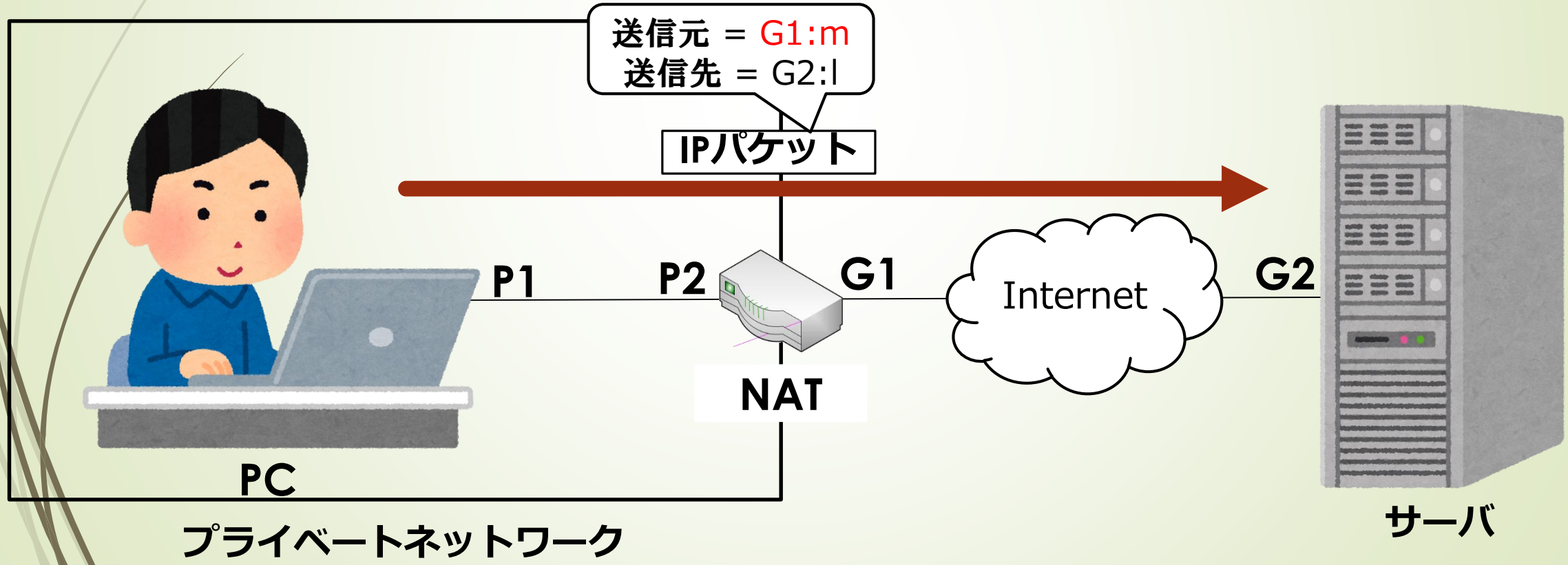
Cone型の動作(送信の場合)

①PCからプライベートIPアドレスを用いて、
インターネット上のサーバにパケットを送信する



Cone型の動作(送信の場合)

②NAT通過時、パケットの送信元アドレスとポート番号を変換して転送する

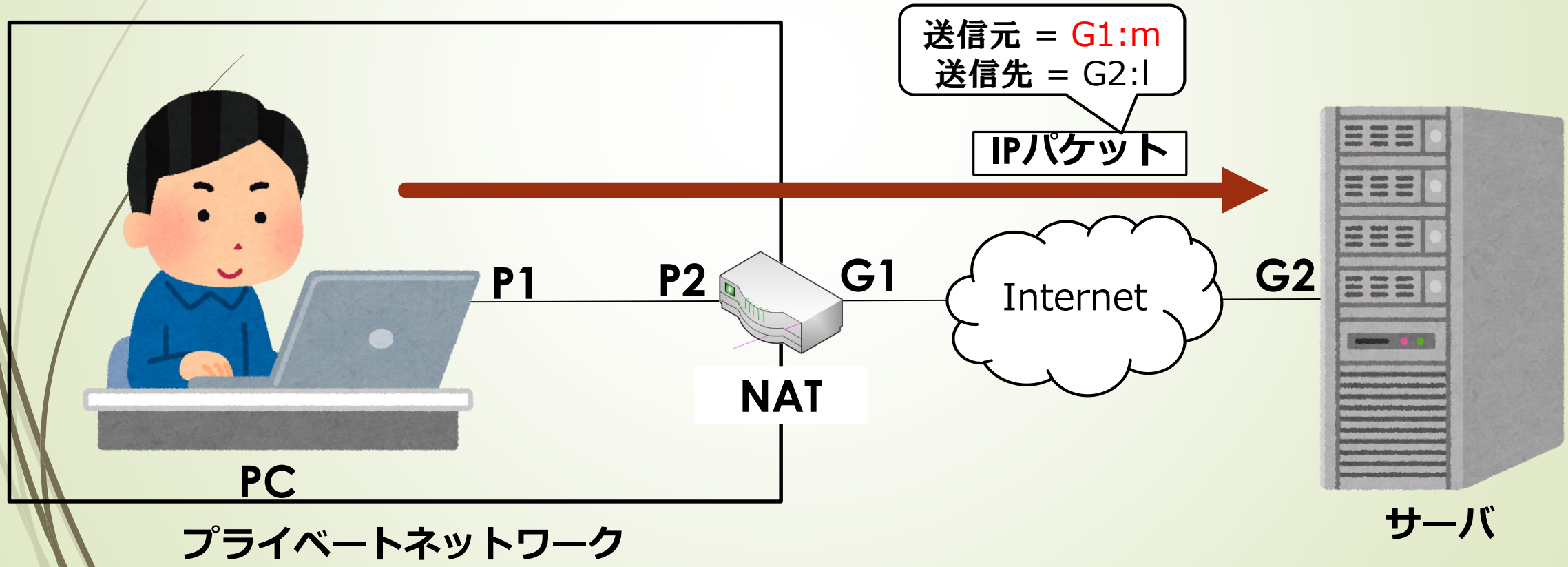


Cone型の動作(送信の場合)

③NATテーブルに変換情報を記述する
(フィルタリングには何も記述しない)

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

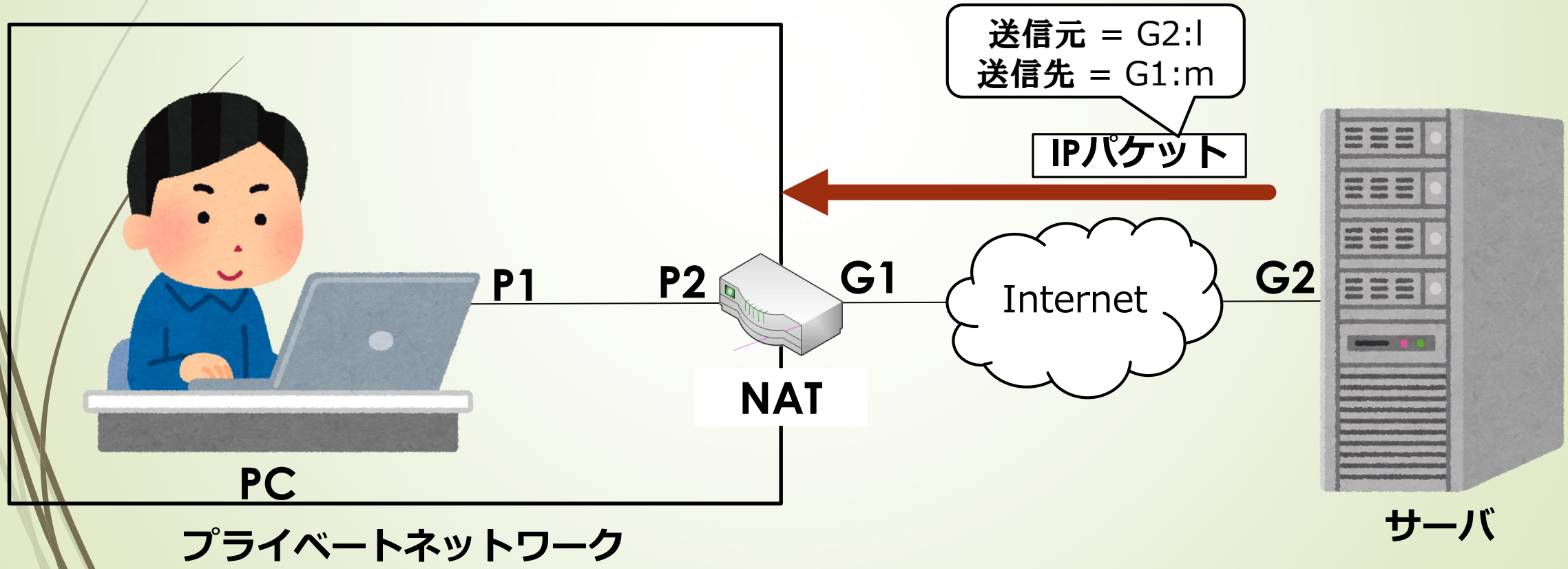


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

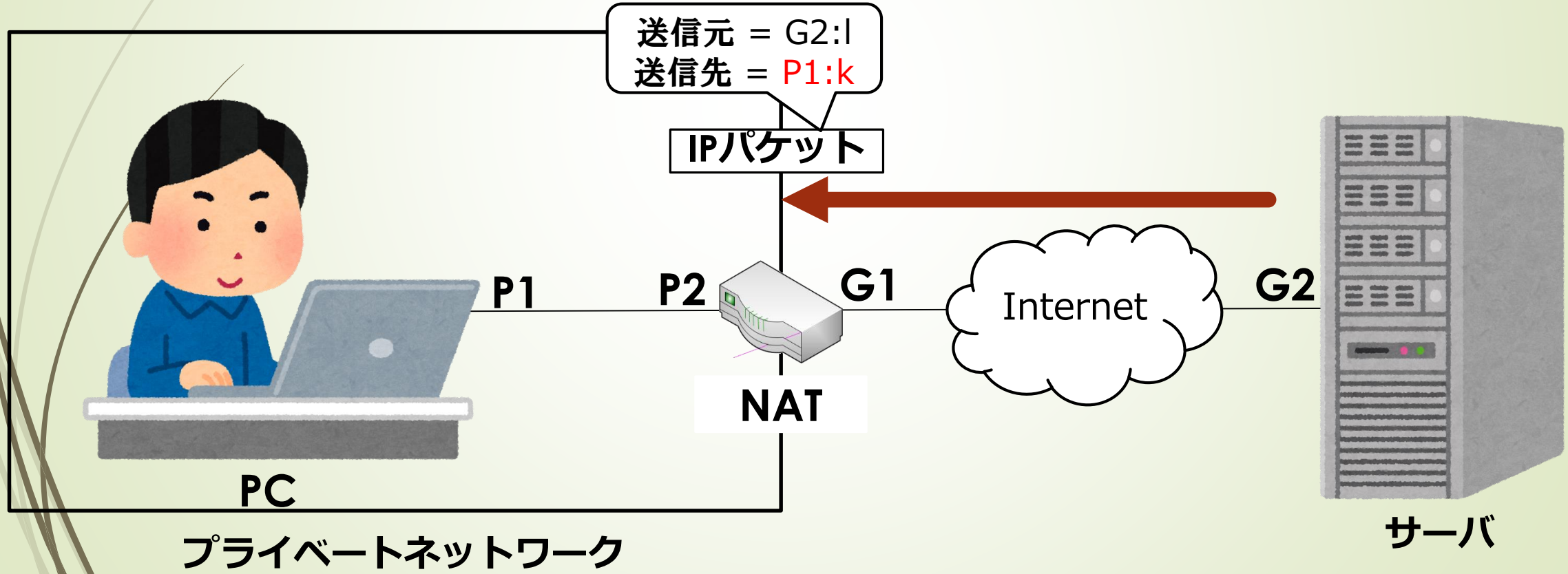


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

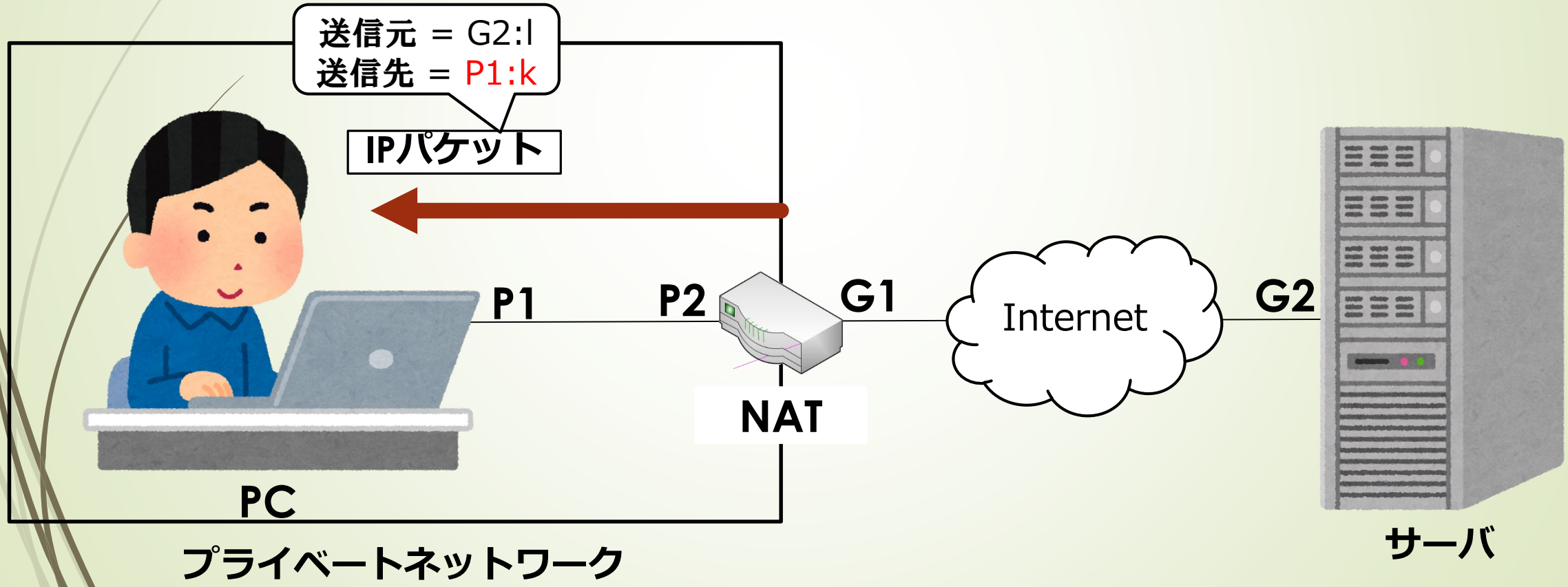


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

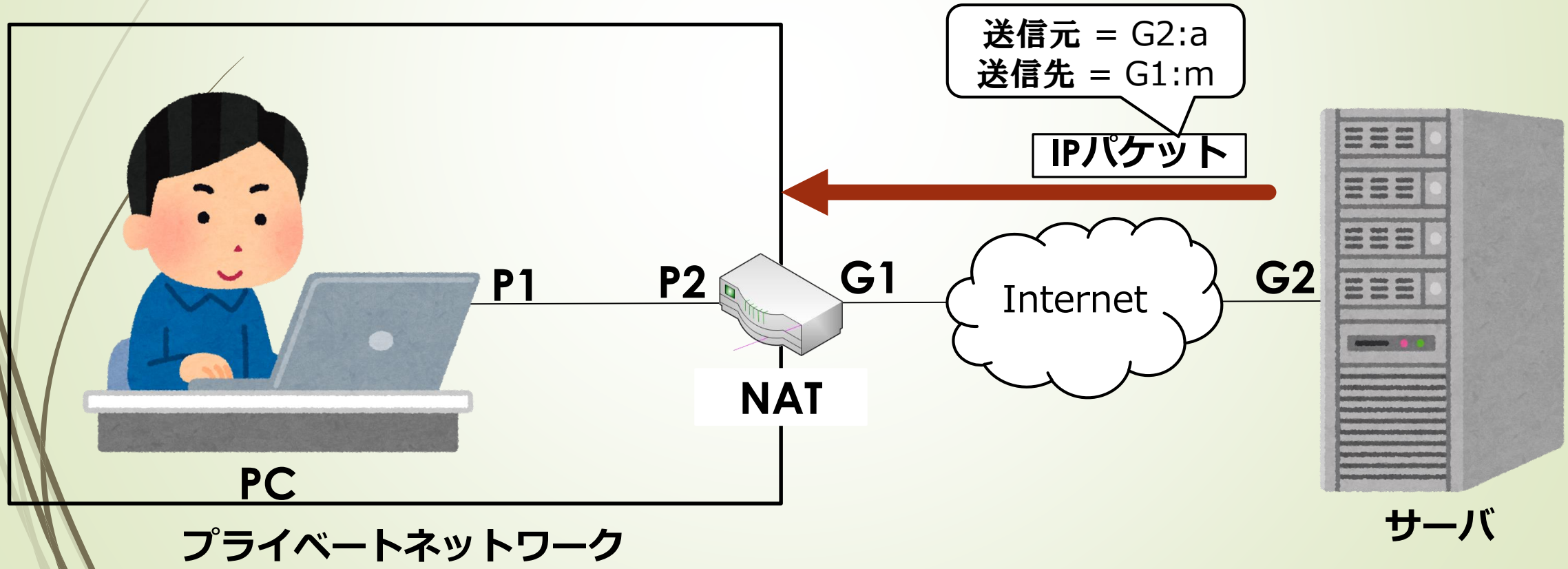


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

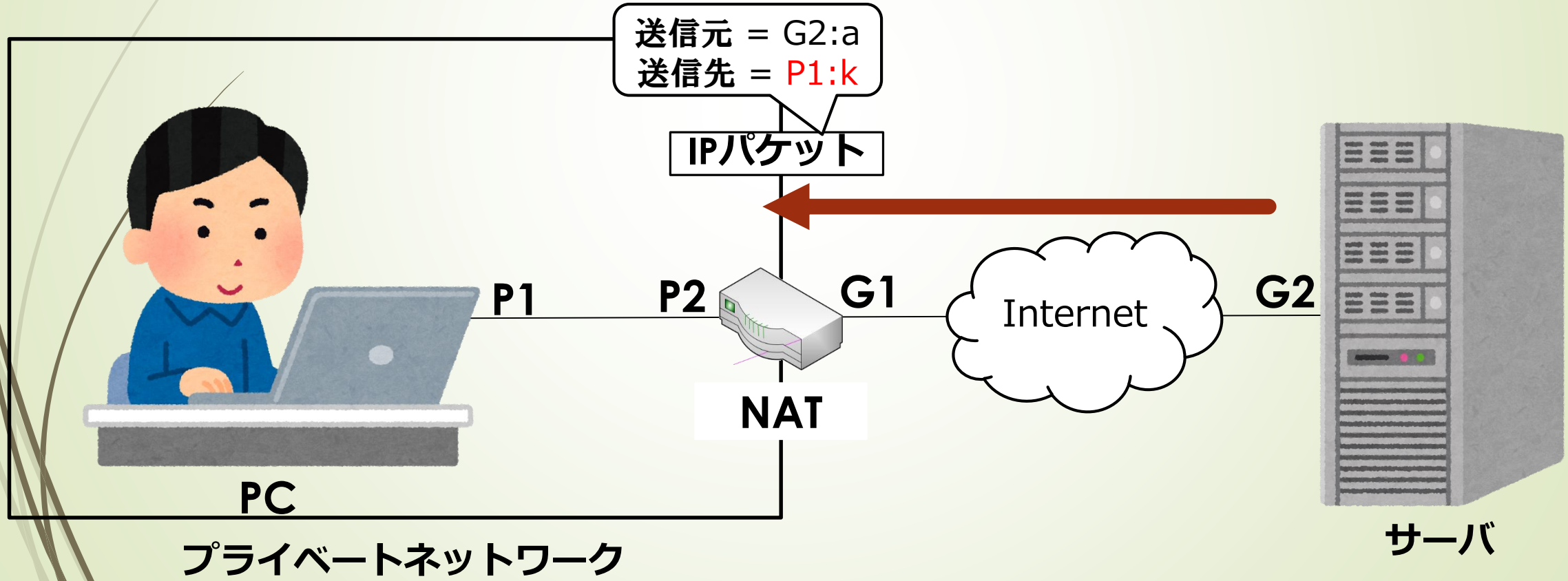


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

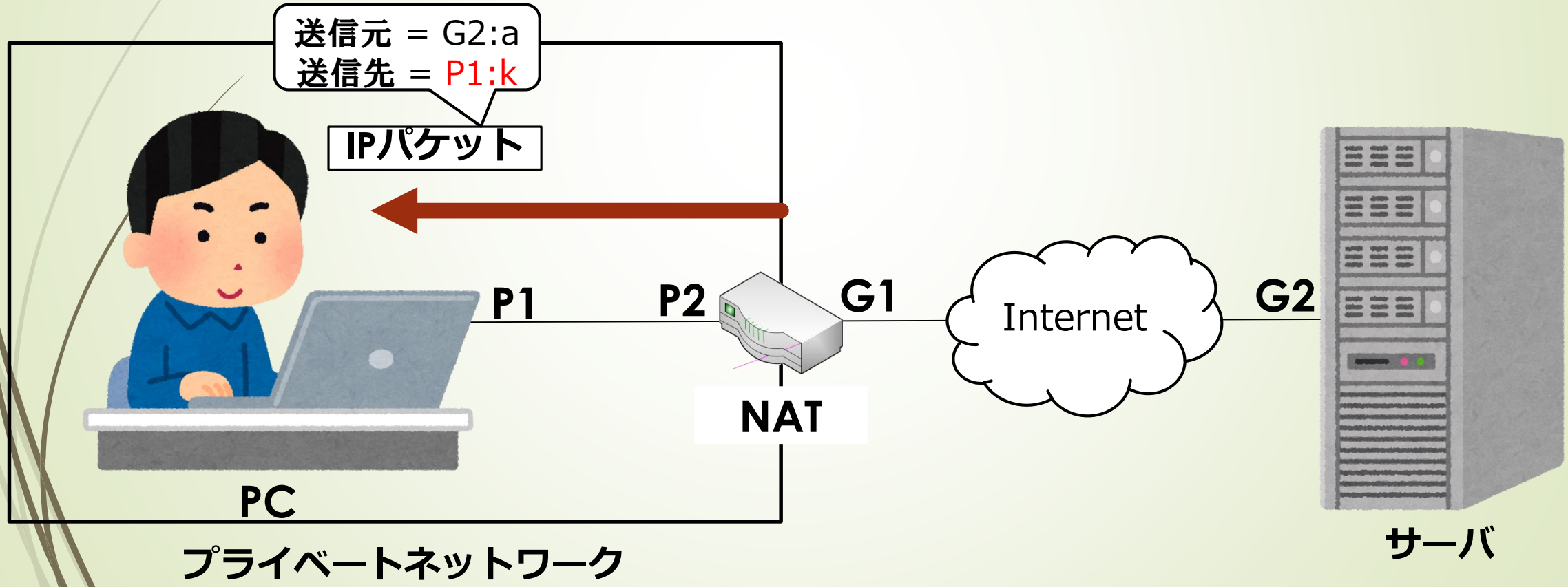


Cone型の動作(受信の場合)

他の通信で生成したNATテーブルを用いて、グローバルアドレス側から通信可能

NATテーブル

フィルタリング	変換情報
※：※	P1:k⇔G1:m

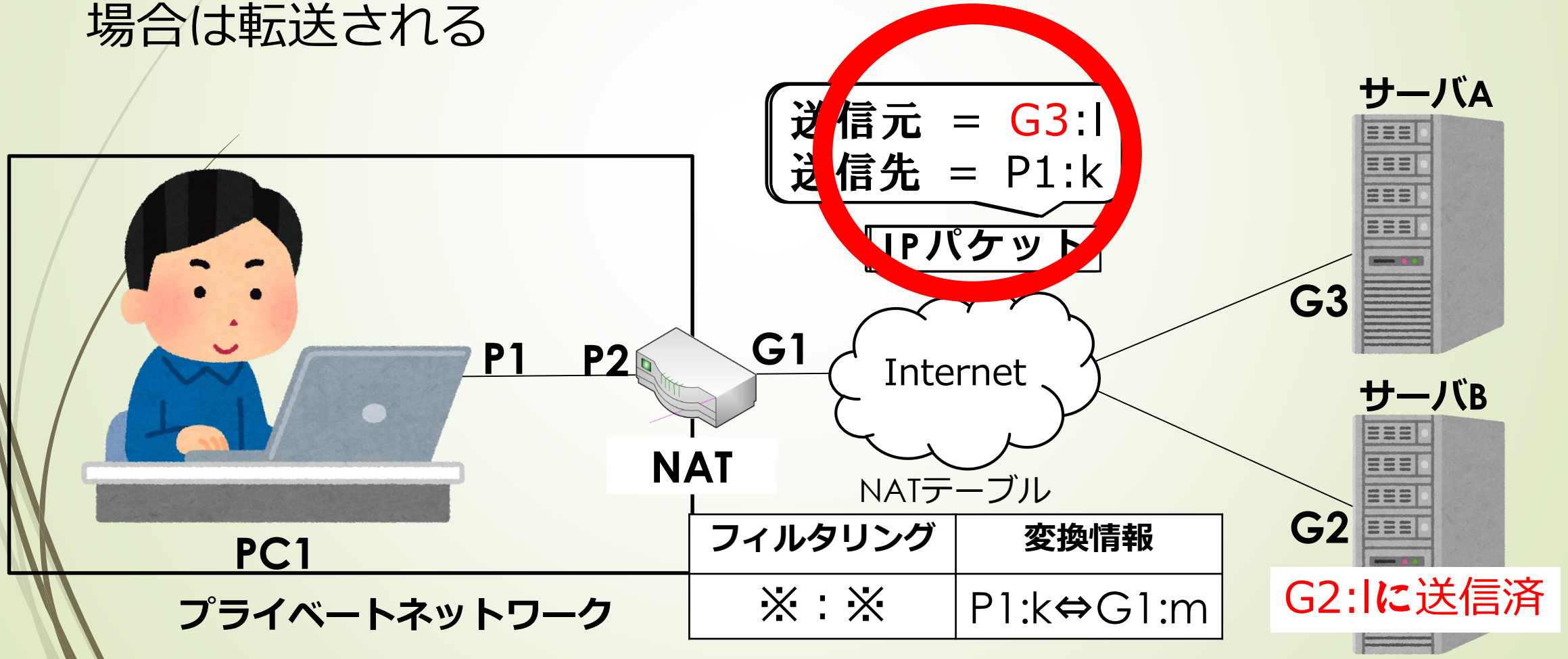


Cone型NATの分類

- Full Cone NAT
  - 一度も送信したことのないWAN側からのパケットも、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される
- Address-Restricted Cone NAT
  - 一度送信したことのあるIPアドレスからのパケットであれば、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される
- Port Restricted Cone NAT
  - 一度送信したことのあるIPアドレス・ポート番号からのパケットであれば、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される

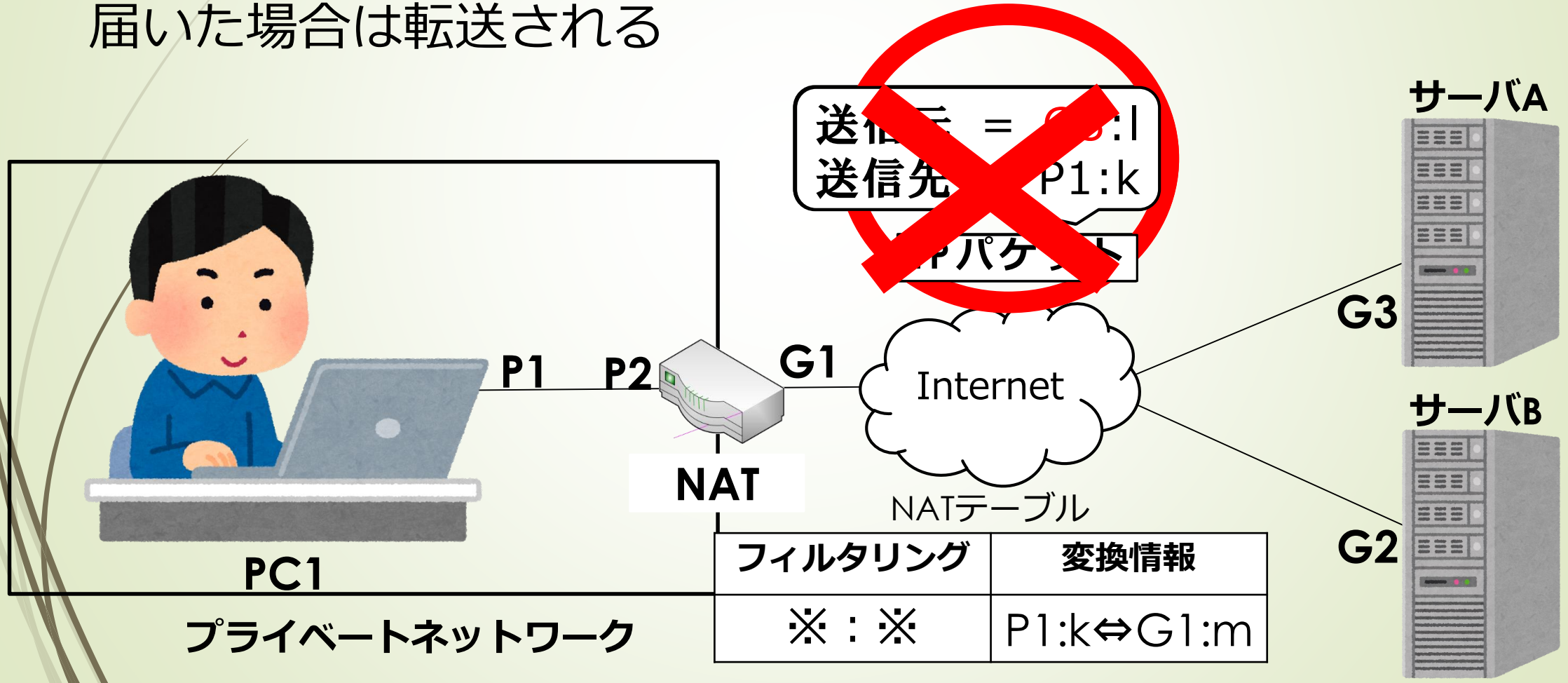
Full Cone NAT

一度も送信したことのないWAN側からのパケットも、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される



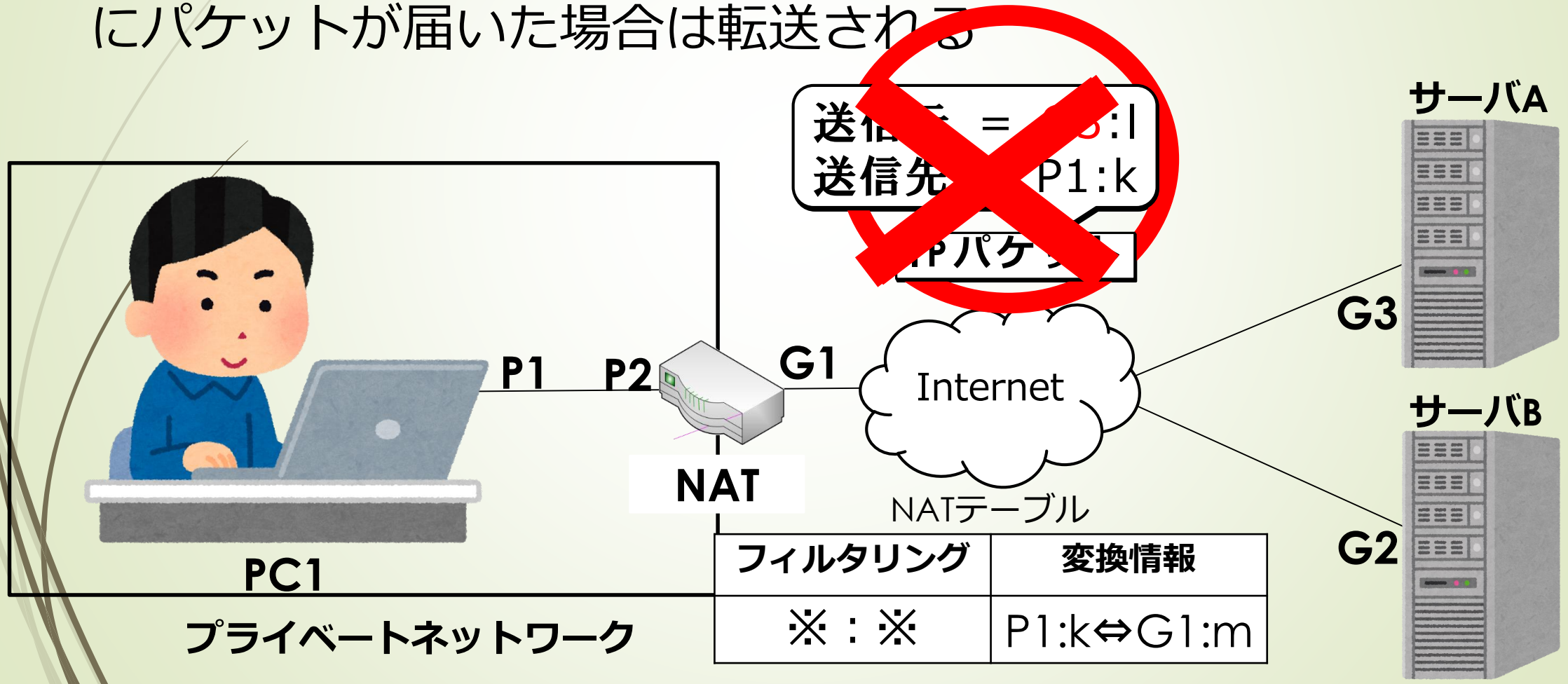
Address-Restricted Cone NAT

一度送信したことのあるIPアドレスからのパケットであれば、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される



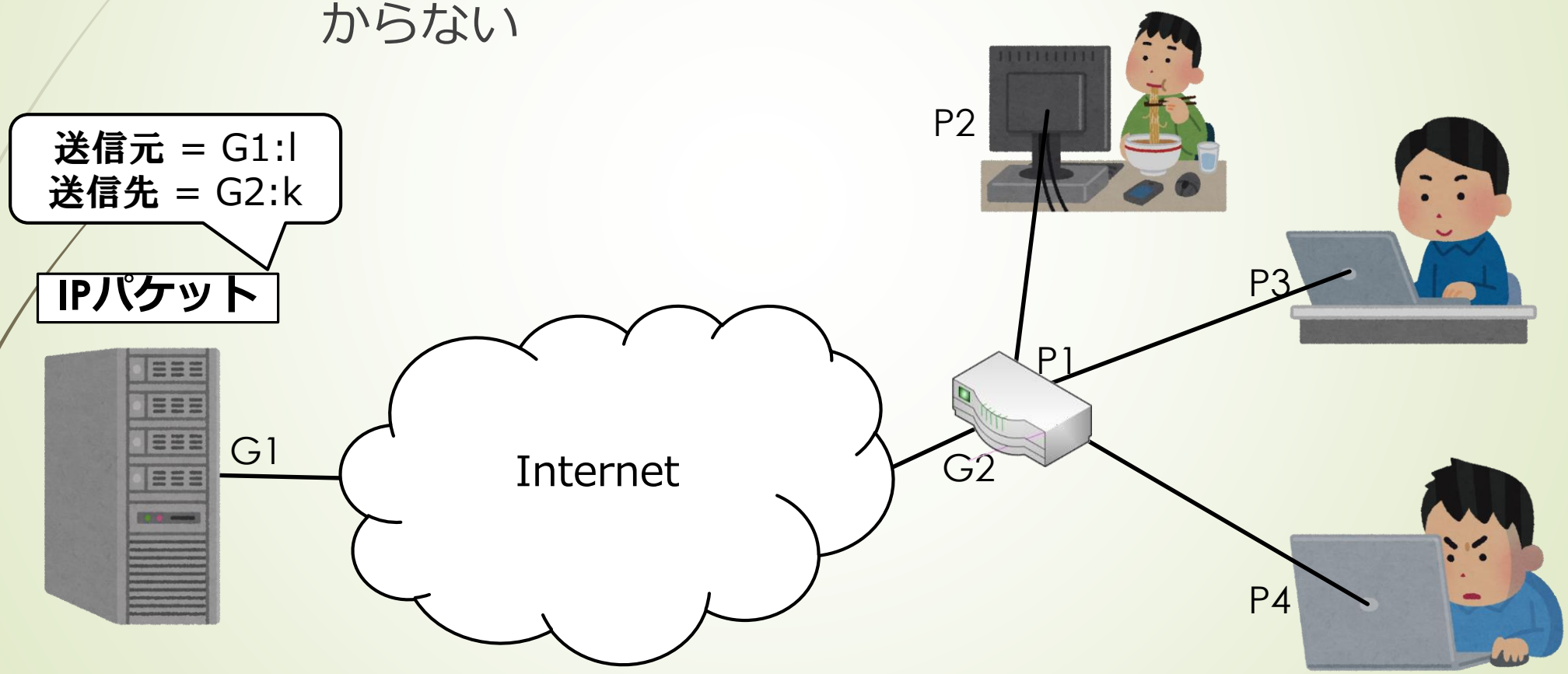
Port Restricted Cone NAT

一度送信したことのあるIPアドレス・ポート番号からのパケットであれば、変換情報が存在するIPアドレス・ポート番号宛てにパケットが届いた場合は転送される



NATが抱える問題

- グローバルアドレス側からの通信開始が不可能
  - NATテーブルがなく、NAT配下の誰に送信すればよいかわからない

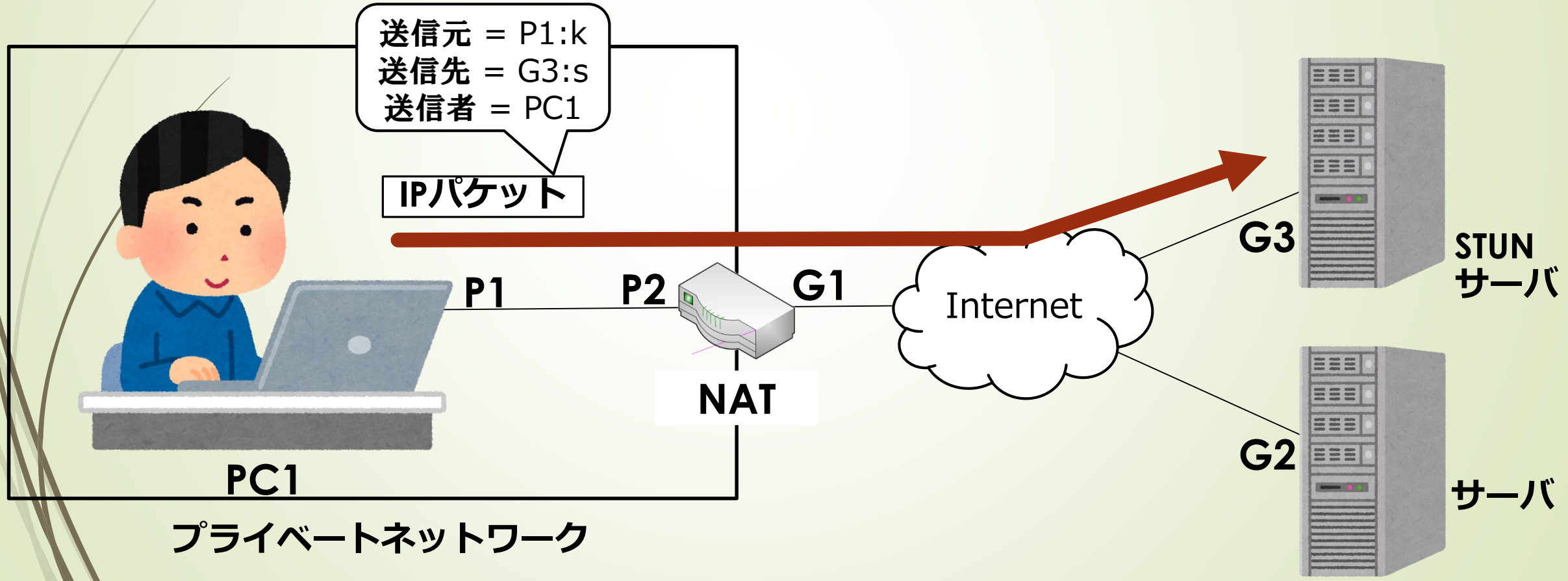


NAT越え技術

- STUN(Simple Traversal of UDP through NATs)
- TURN(Traversal Using Relay NAT)
- ICE(Interactive Connectivity Establishment)

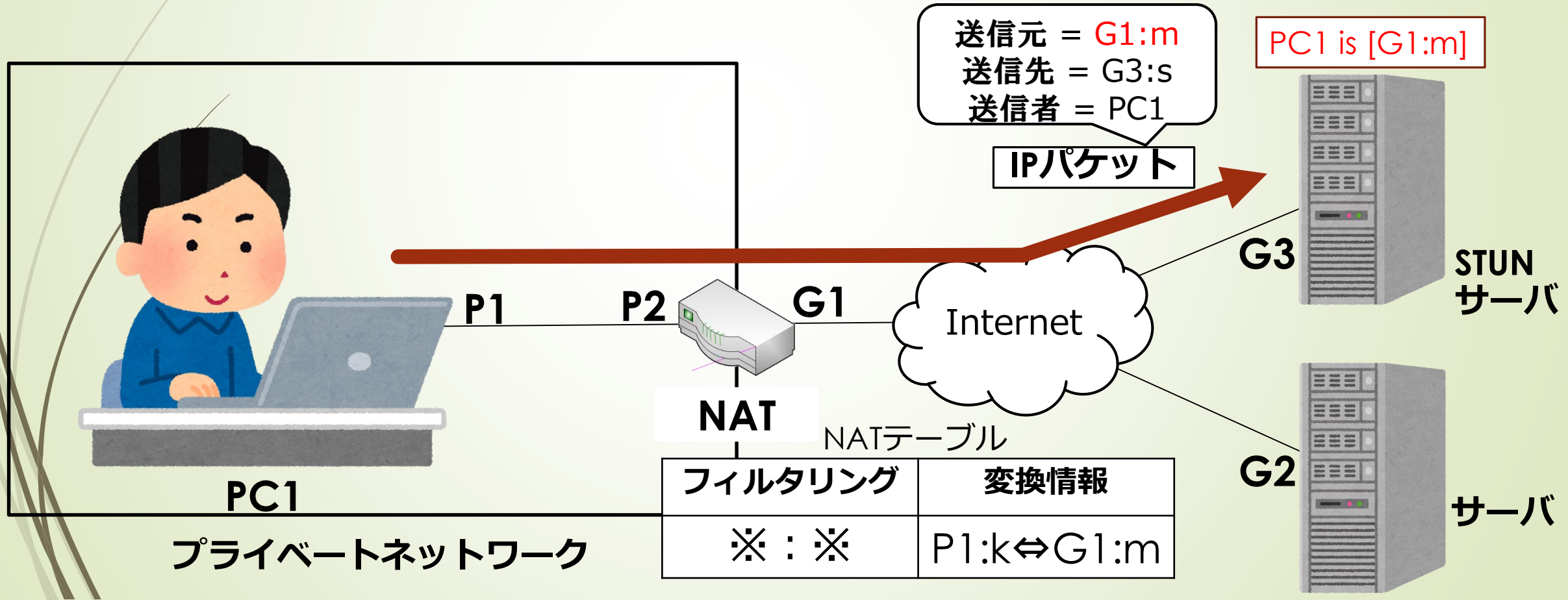
Cone型NATの場合のSTUNの動作(準備)

①PC1からプライベートIPアドレスを用いて、
STUNサーバにパケットを送信する(STUN Binding Request)



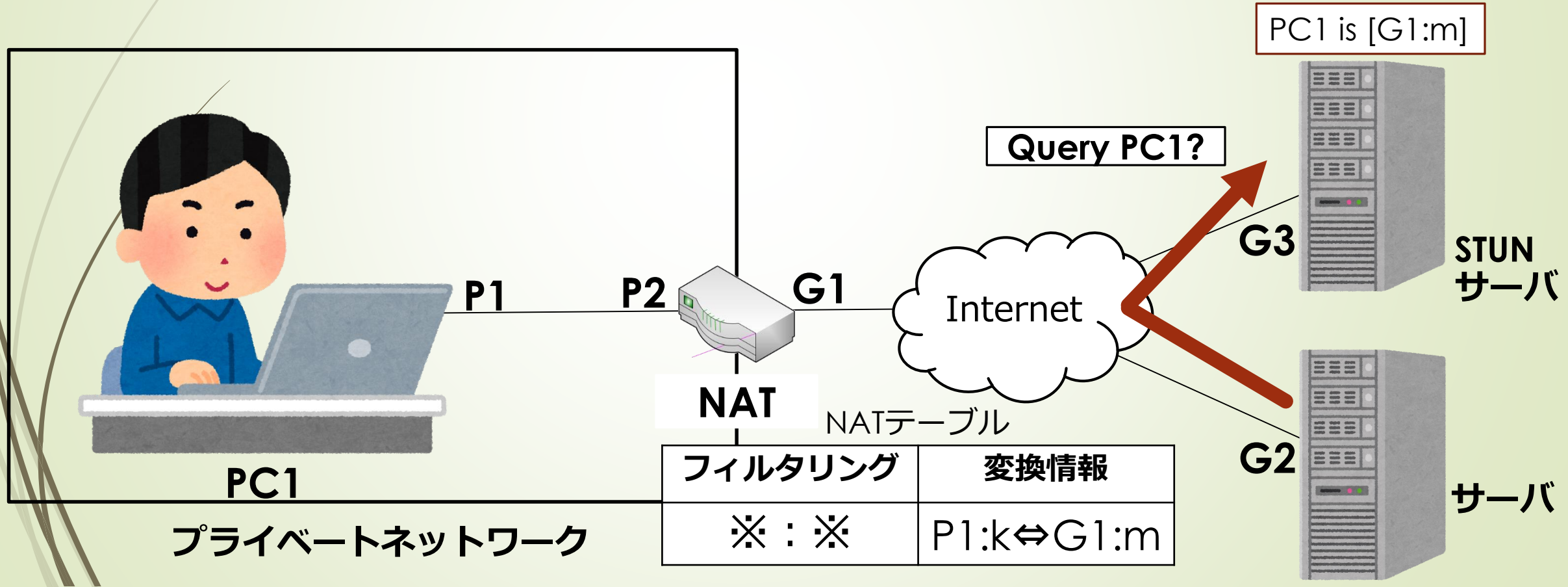
Cone型NATの場合のSTUNの動作(準備)

②NATテーブルが作成され、
STUNサーバにPC1とG1:mの関係が登録される



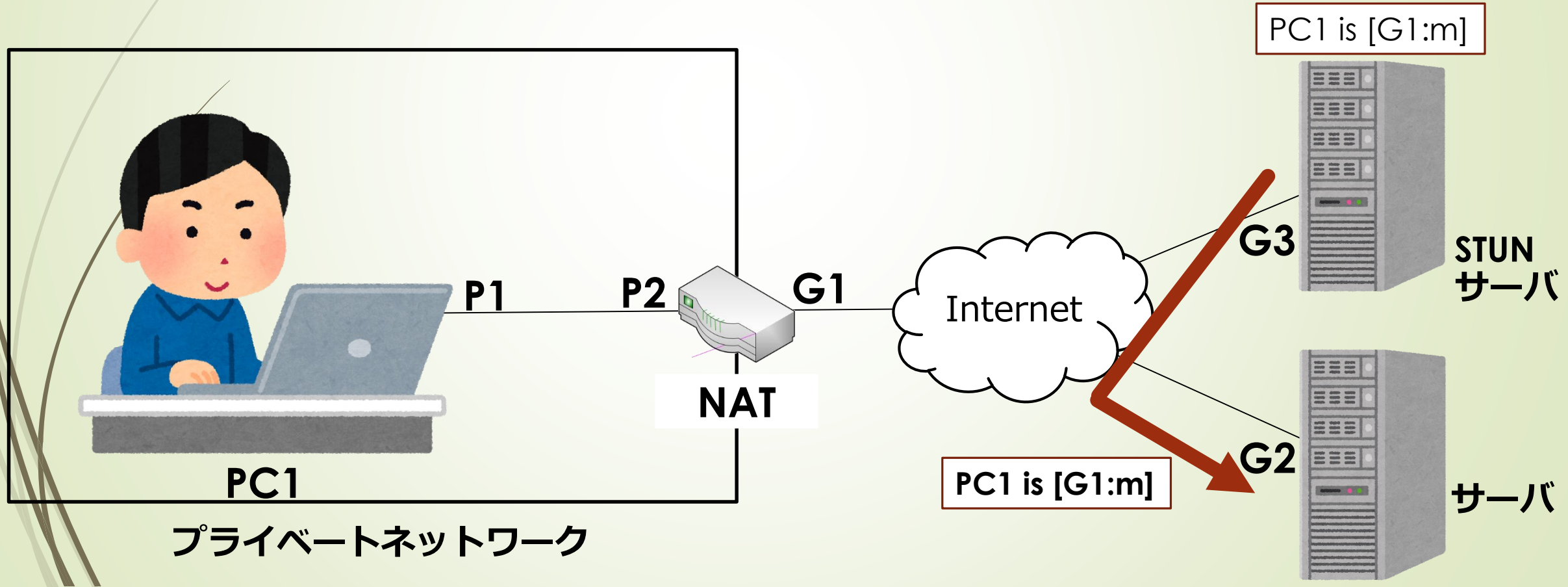
Cone型NATの場合のSTUNの動作

①サーバはSTUNサーバにPC1の情報を問い合わせる



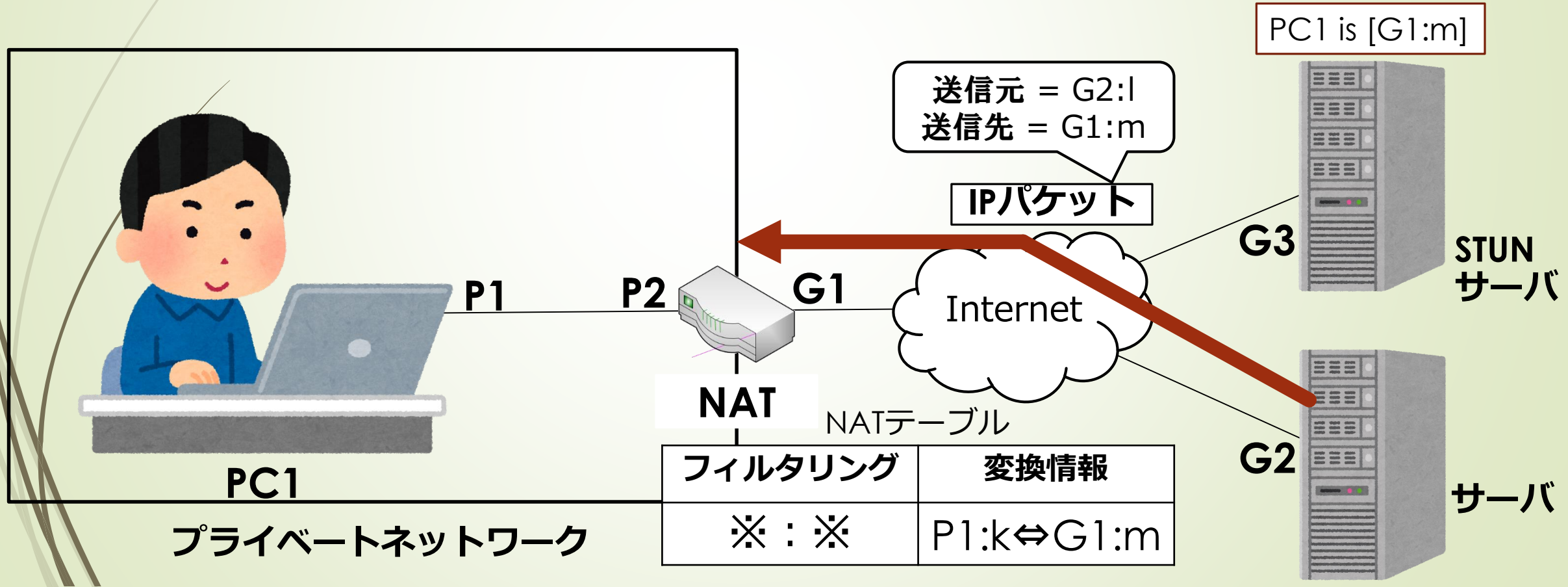
Cone型NATの場合のSTUNの動作

②STUNサーバは自信のもつPC1の情報をサーバに答える



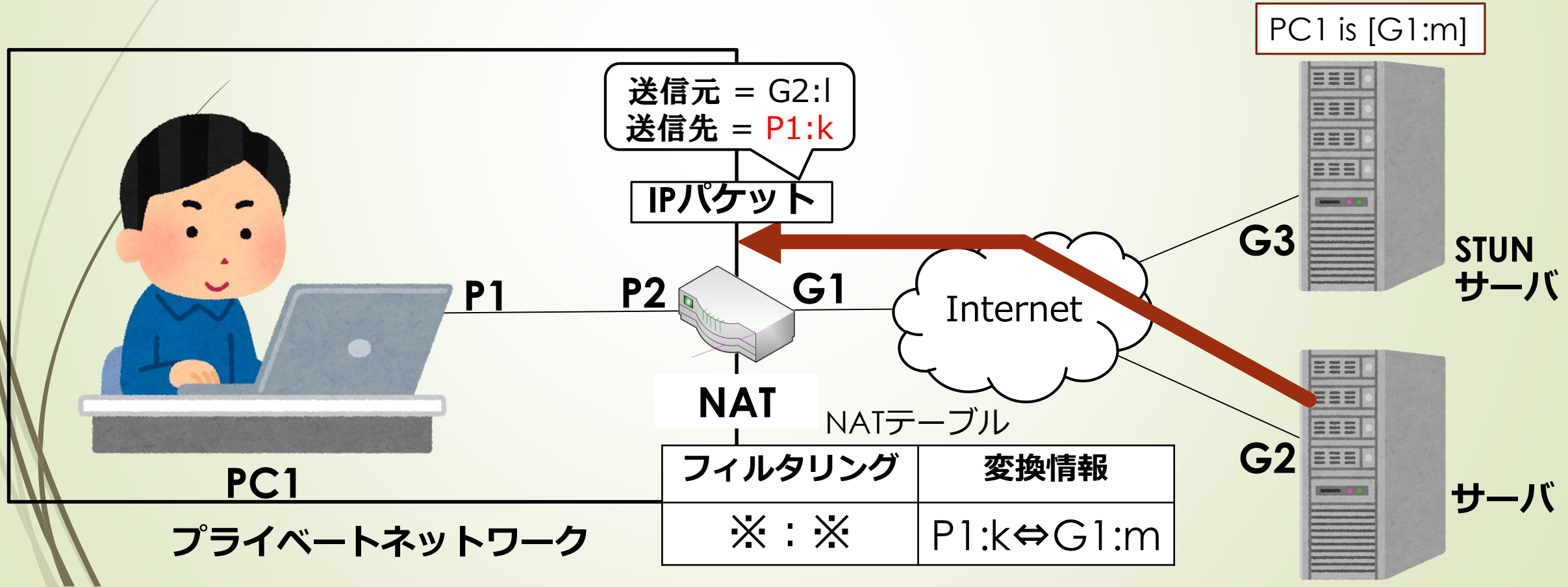
Cone型NATの場合のSTUNの動作

③受信したPC1のアドレスとポート番号を用いて、パケットを送信する



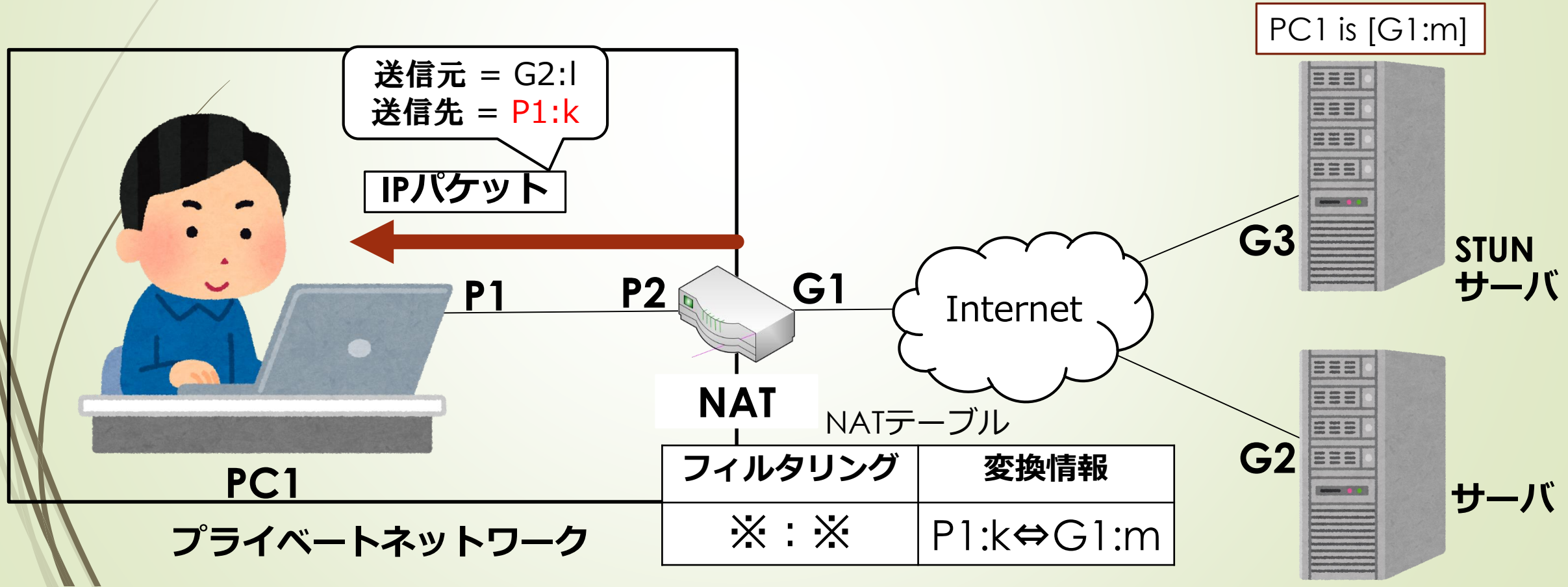
Cone型NATの場合のSTUNの動作

④Cone型NATのため破棄されることなく通信が行われる



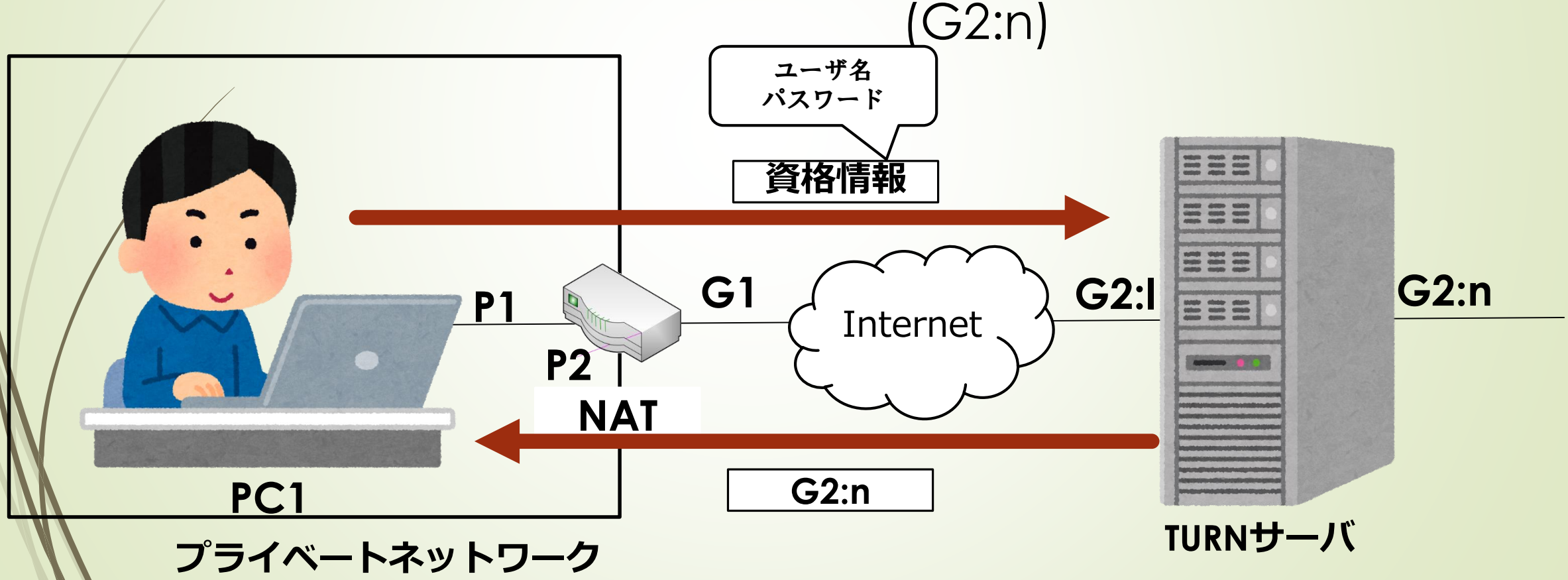
Cone型NATの場合のSTUNの動作

④Cone型NATのため破棄されることなく通信が行われる



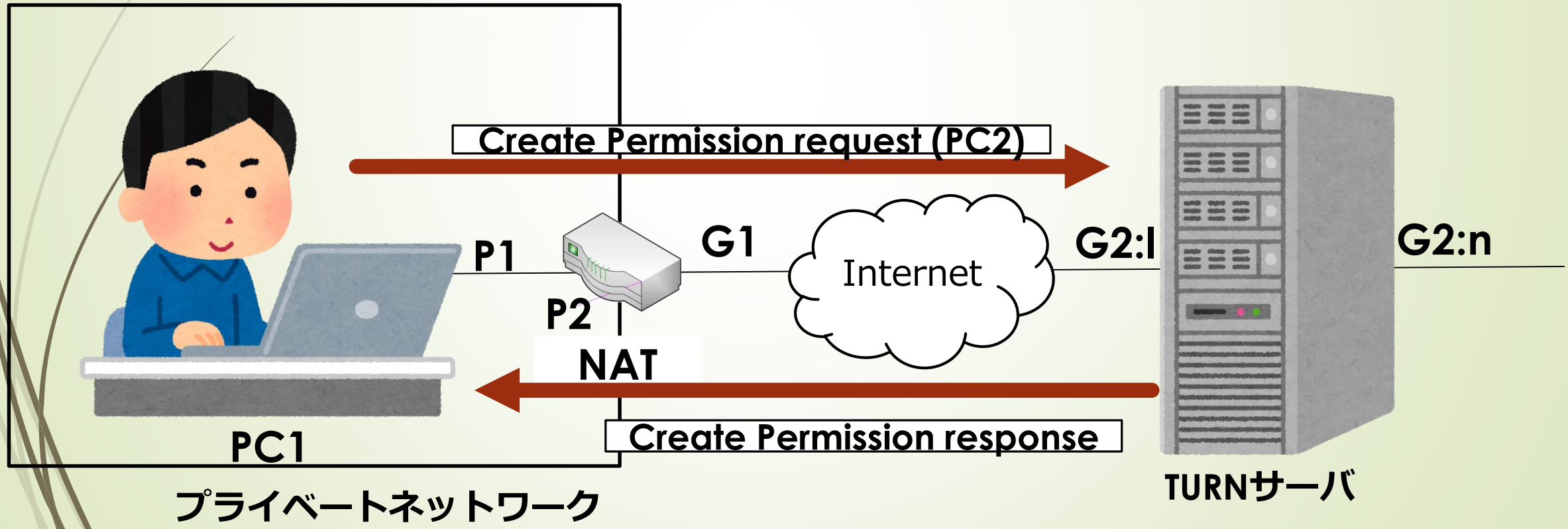
TURNの動作(割り当て)

サーバ使用権限を持っていることを示す資格情報を送信する
認証成功後、TURNサーバが用いる転送アドレスが返される。



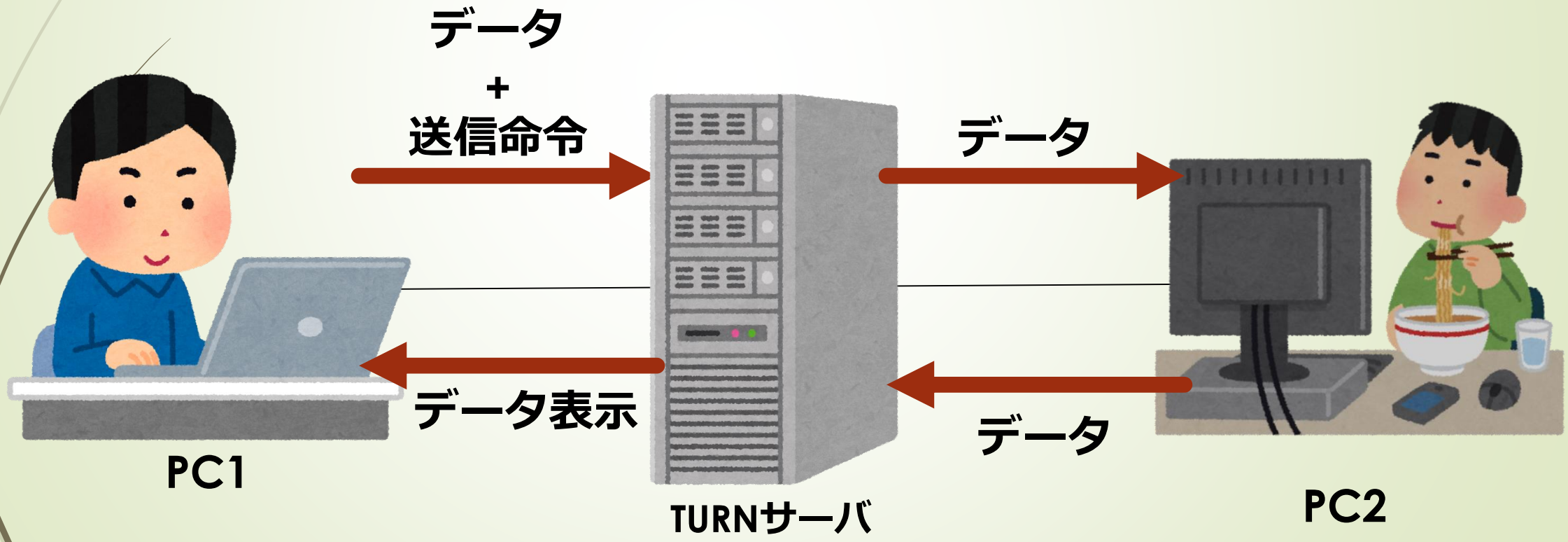
TURNの動作(送信メカニズム)

①TURNサーバに接続作成要求を送信する(接続先をPC2とする)
アクセスが許可された場合、レスポンスが返ってくる。



TURNの動作(送信メカニズム)

②TURNサーバを介してデータの送受信を行う

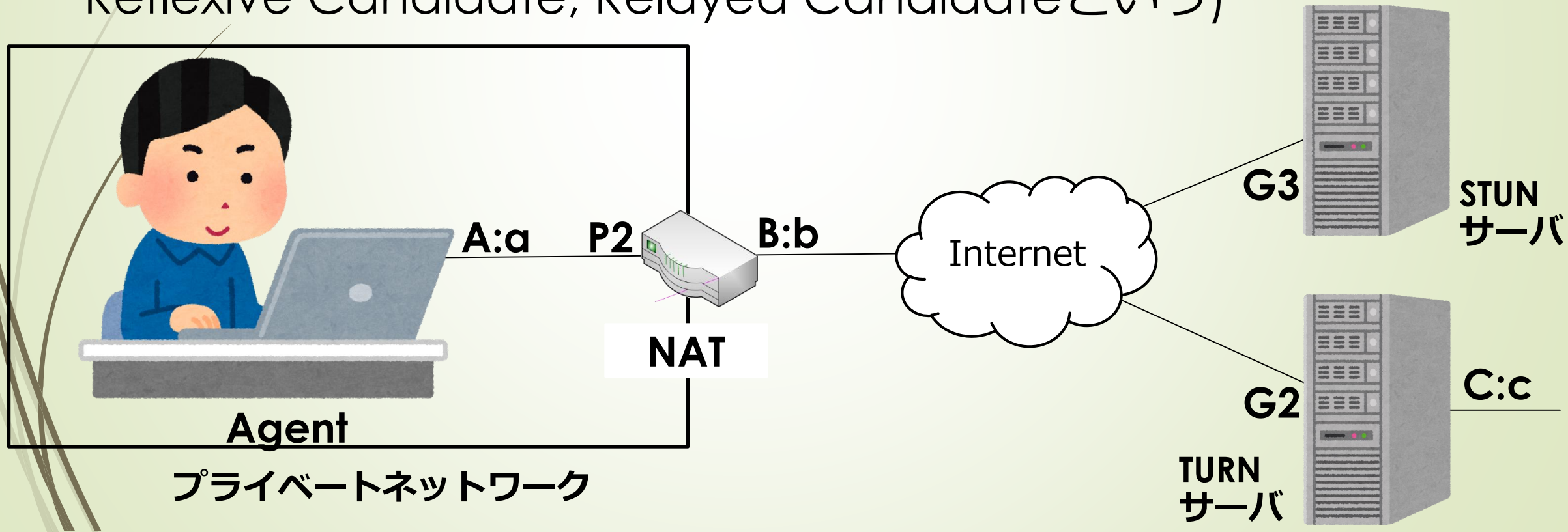


ICEについて

- STUNとTURNを組み合わせたようなもの
- 互いの通信できそうな候補の組み合わせの中から接続可能なものを探し、その中で最も良いものを使用する
- 以下のように進む
  1. 準備：候補の準備
  2. 交換：自信と相手の候補リストを交換
  3. 整頓：候補をペアにする
  4. 確認：接続可能性を確認
  5. 完結：どのペアを用いるか決定する

候補の収集

Agentのローカルアドレス、STUNよりNATのグローバルIPアドレスとポート番号、TURNサーバの中継用グローバルIPアドレスとポート番号を入手する(順にHost Candidate, Server Reflexive Candidate, Relayed Candidateという)

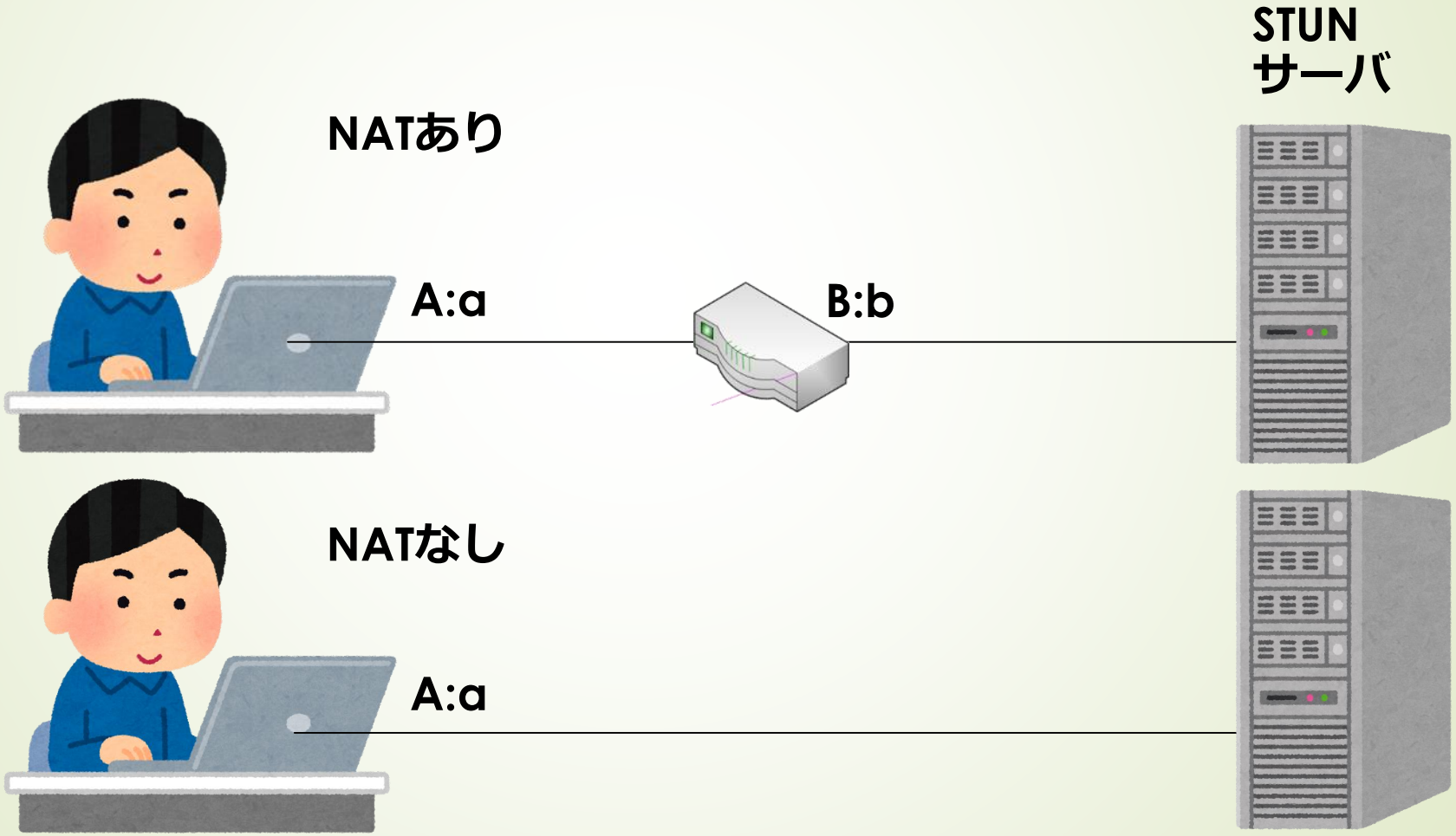


候補の優先順位付けと冗長削除

- 優先度は以下の式で求める
  - Priority = $2^{24} \times (type\ preference) + 2^{8} \times (local\ preference) + 2^{0} \times (256 - componentID)$
    - Type preference:候補のタイプごとの優先度
      - HOST…126(最高値),SERVER REFLEXIVE…100, RELAYED…0（最低値）
    - Local preference:IPアドレスの優先順位
      - NATのグローバルIPアドレスとポート番号が複数存在する場合に用いる
    - Component ID:1~256までの値
      - RTPの場合1、RTCPの場合2

候補の優先順位付けと冗長削除

- 冗長削除について



候補情報の交換・整頓

- SDP(Session Description Protocol)を用いて交換する
- 自身と相手の候補を以下のようなペアにする

IP Address	Port	Protocol	Type	IP Address	Port	Protocol	Type
A_L	a_L	UDP	HOST	A_R	a_R	UDP	HOST
A_L	a_L	UDP	HOST	B_R	b_R	UDP	SERVER
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
C_L	c_L	UDP	RELAYED	C_R	c_R	UDP	RELAYED

※Agent LをControlling Agent，Agent RをControlled Agentとする

接続可能性の確認

- 各候補間の接続性を、STUN　Binding request/responseにより確認する
- STUN Binding responseが以下の条件を満たす場合，

  接続可能と判定する
  - 成功応答(success response)である
  - 送信元IPアドレスとポート番号がBinding requestした宛先IPアドレスとポート番号に一致する
  - 宛先IPアドレスとポート番号がBinding requestした送信元IPアドレスとポート番号に一致する

使用するペアの決定

- 以下二種類のいずれかを用いて、使用するペアを決定する
  - Regular Nomination：接続可能なペアのうちいずれかに決定し、Flag付きSTUN Binding requestにより通知
  - Aggressive Nomination：確認段階でFlag付きSTUN Binding requestを送信し、接続可能なペアが発見された場合、それを使用する。

まとめ

- NATとは：末端機器(PC)とインターネットの間で、パケット中のIPアドレス(とポート番号)を変換する技術
- 分類
  - 静的・動的
  - Symmetric型・Cone型
- NAT越え技術
  - STUN
  - TURN
  - ICE

参考文献

- RFC 5245 “Interactive Connectivity Establishment (ICE) : A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols”
  - https://tools.ietf.org/html/rfc5245 (2018/04/12)
- Symmetric NAT における NAT 越え実現方式
  - http://www.wata-lab.meijo-u.ac.jp/file/mthesis/2009/2009-MT-Hui_Li.pdf (2018/04/11)
- 輪講資料 ICE（Interactive Connectivity Establishment）
  - http://www.wata-lab.meijo-u.ac.jp/file/seminar/2017/2017-Semi1-Yuma_Kamoshita.pdf (2018/04/13)
- WebRTCのICEについて知る
  - https://www.slideshare.net/iwashi86/webrtcice (2018/04/11)
- NAT 基礎講座
  - www.shudo.net/publications/20080627-NAT/shudo-NAT-20080627.pdf (2018/04/11)