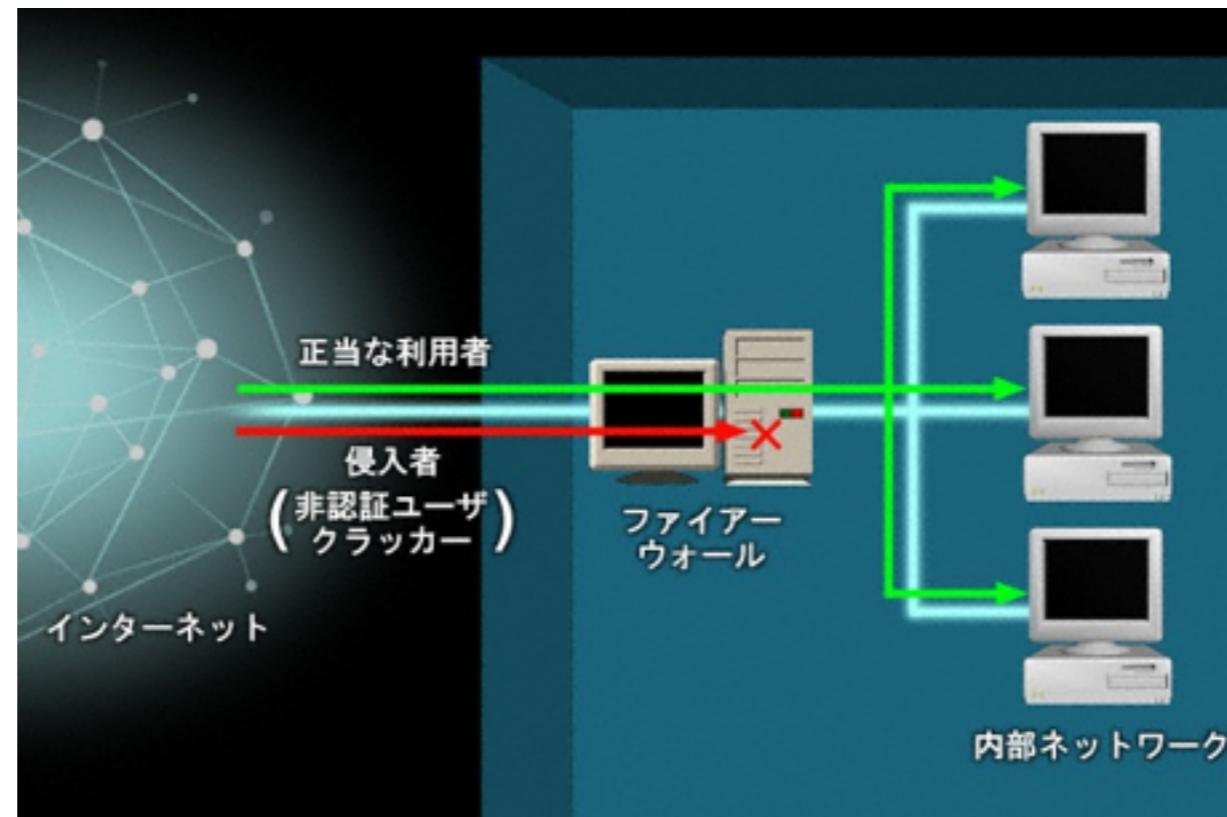


Network Security Firewall

総合情報学科
セキュリティ情報学コース

Firewallとは？

- Networkの境界点でアクセス制御を行うシステム
- 境界を流れるデータを監視し、定義された規則に基づき、不正なアクセスを排除、必要な通信のみ通過させる



図引用) IPA, 教育用画像素材集より: <http://www2.edu.ipa.go.jp/gz/>

Firewallとは? (cont.)

- 名称：「防火壁」 ⇒ 実態は「城壁+城門+検査員」
 - 例：「Passport Control」
- 設置場所: Networkの境界点
 - Firewall は Networkを分割 ⇒ 「保護領域内(内部)」と「外部」
 - 保護領域内を外部の脅威から保護
- Network構造の隠蔽
 - 内部のnetwork構造を外部から隠蔽
- Software / Hardware実装ともにある
 - 高性能が必要 ⇒ 専用Hardware (Appliance : アプライアンス)

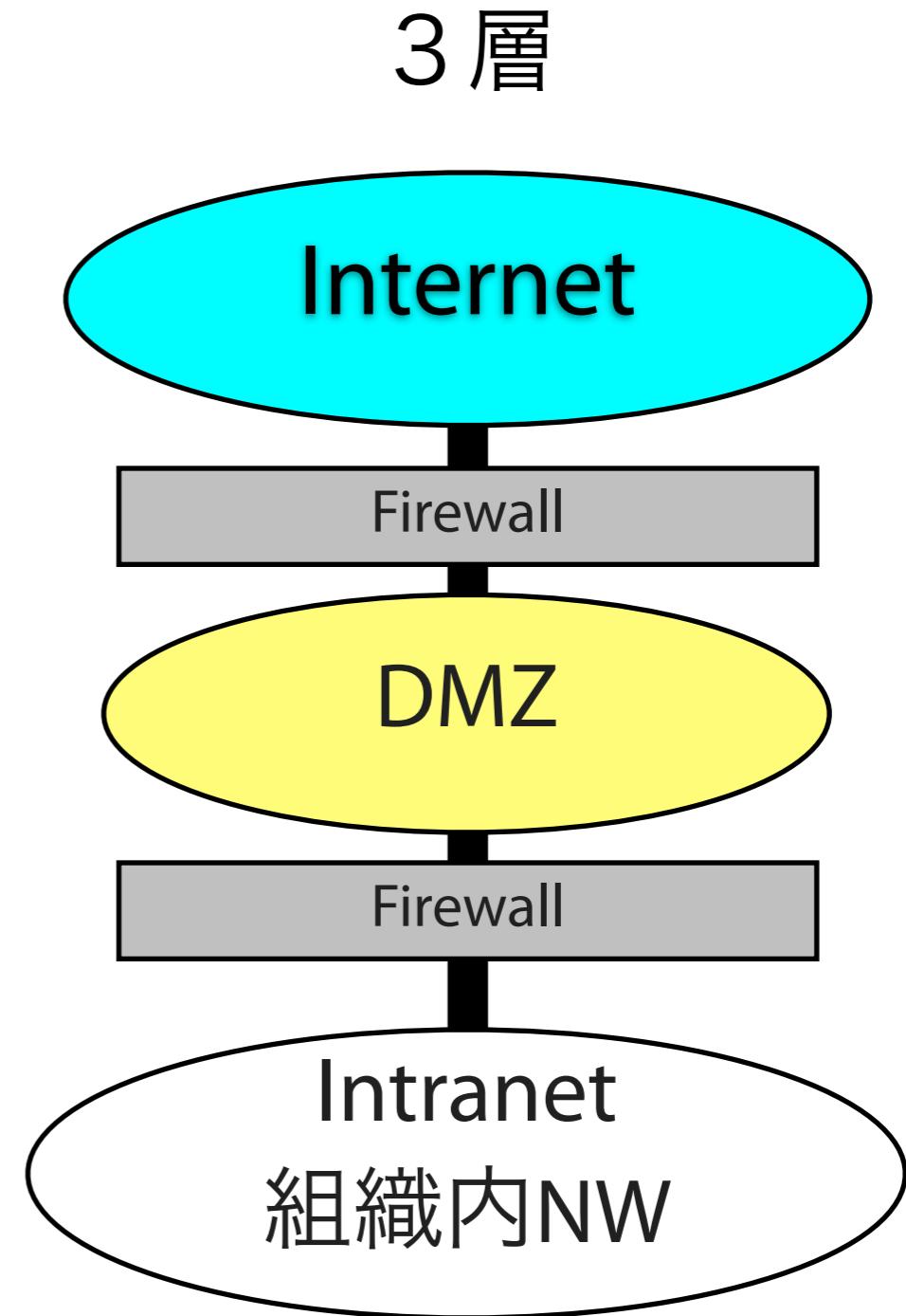
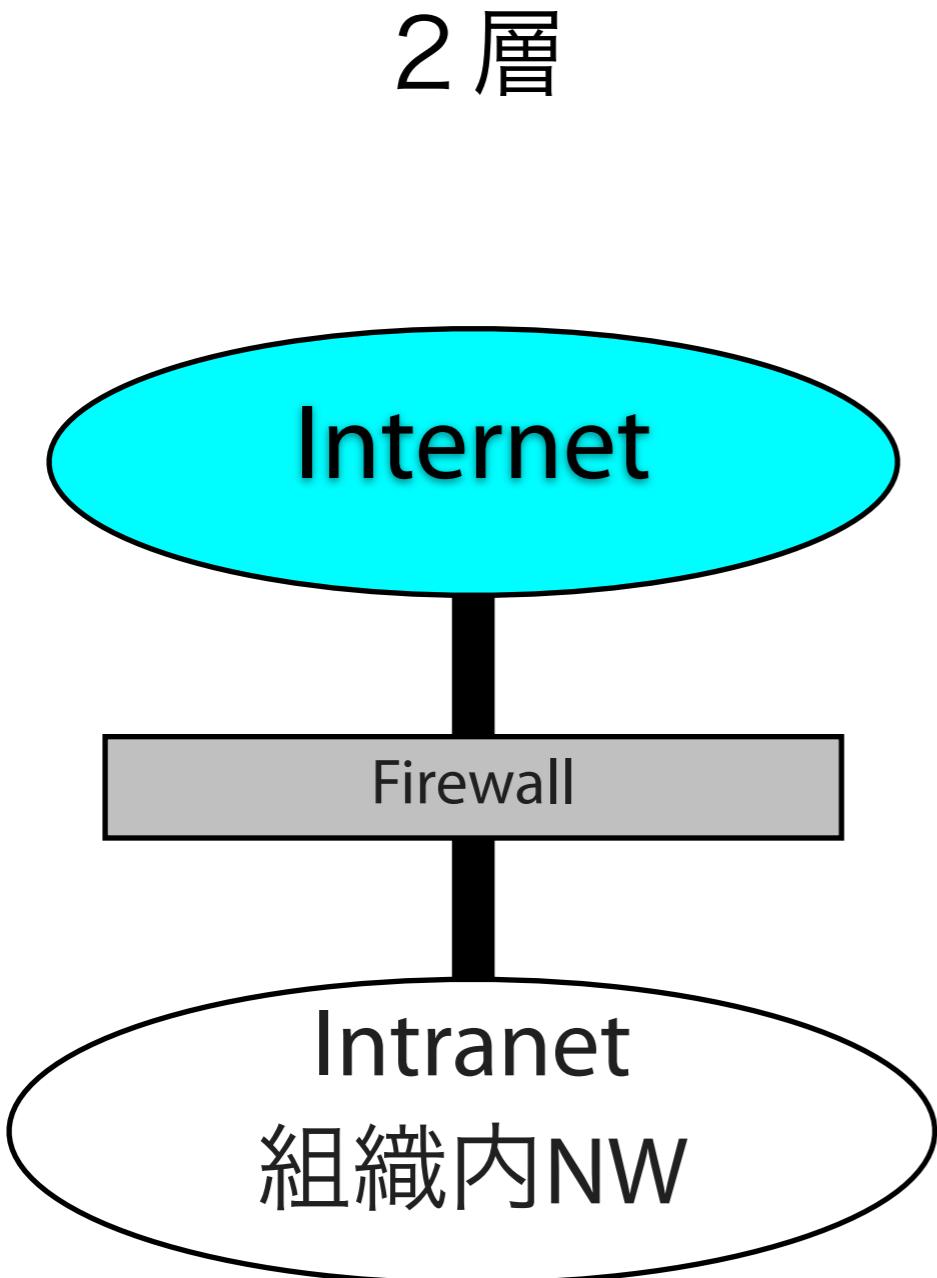


図引用: <http://www.checkpoint.co.jp/>

Firewallの機能

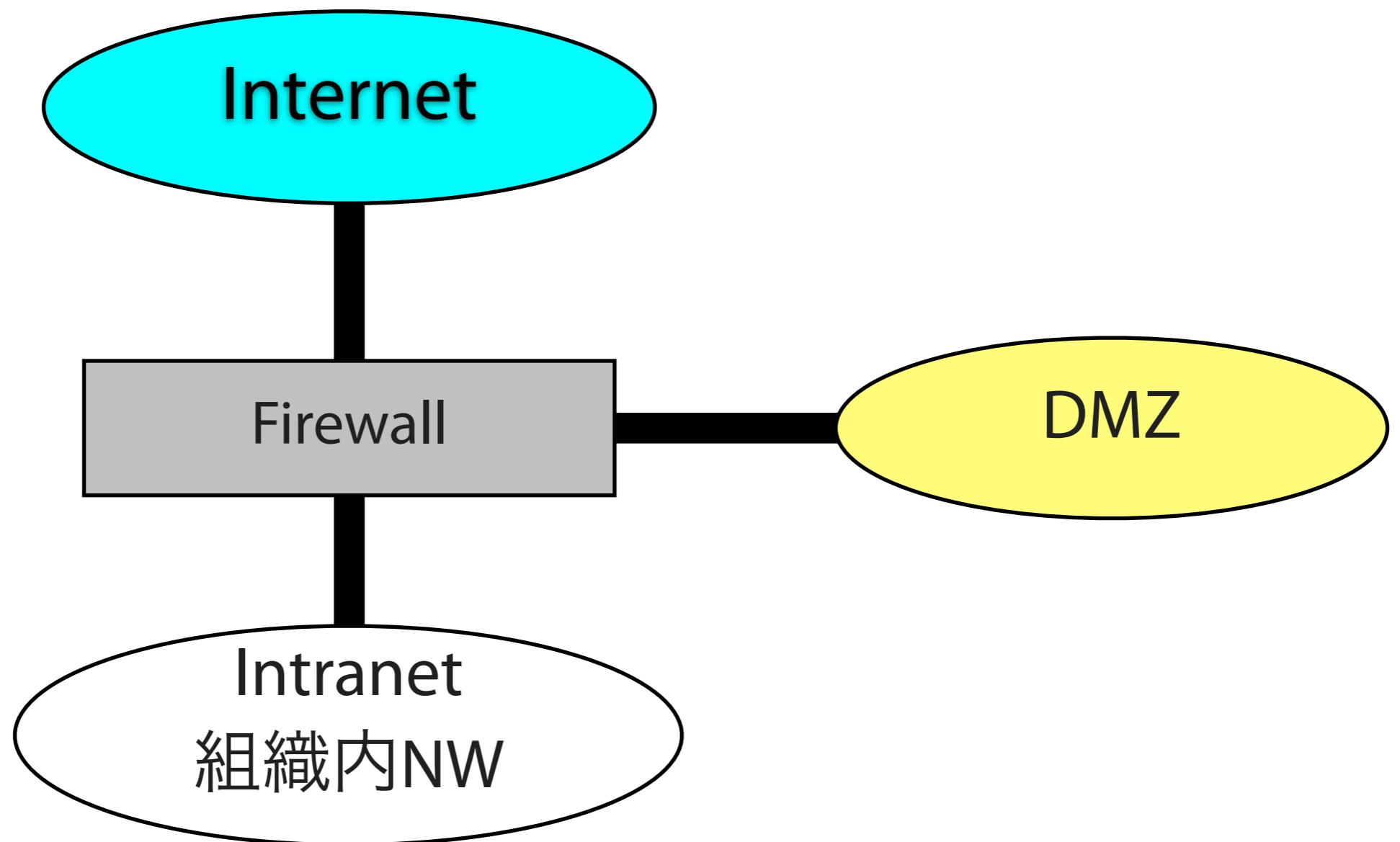
- 隘路 (check point) : 防御すべき点を限定する
- 仕切り (screening) : 外部と内部を仕切る
- 隠蔽 (conceal) : 内側の状況を外側から隠蔽する
- 検問 (filtering) : 条件に応じて通行を制御
- 記録 (logging) : 入出力を記録

組織Networkの複層化



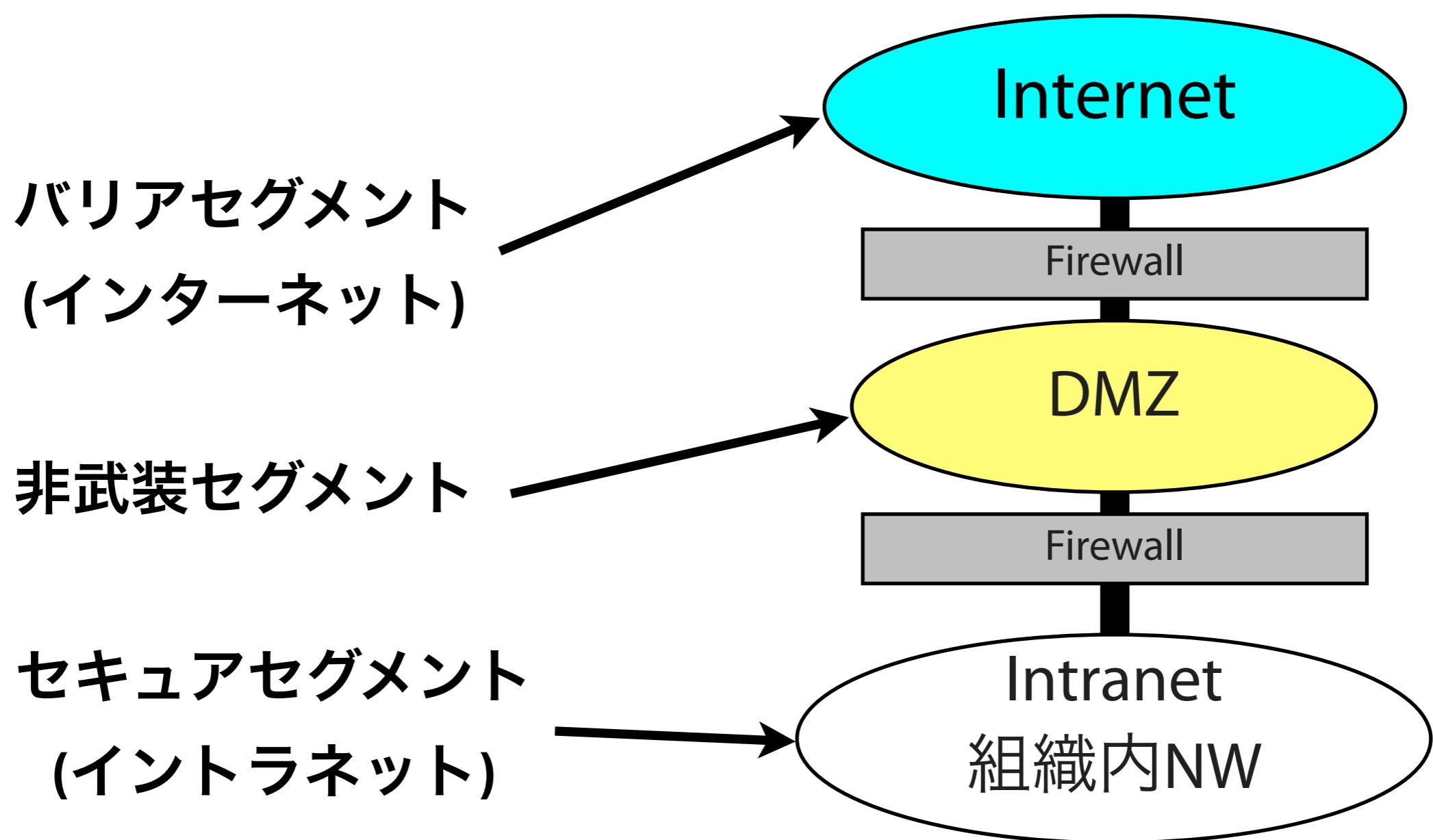
NW=Network

別形式での3層Network



NW=Network

各network(segment)の呼称



NW=Network

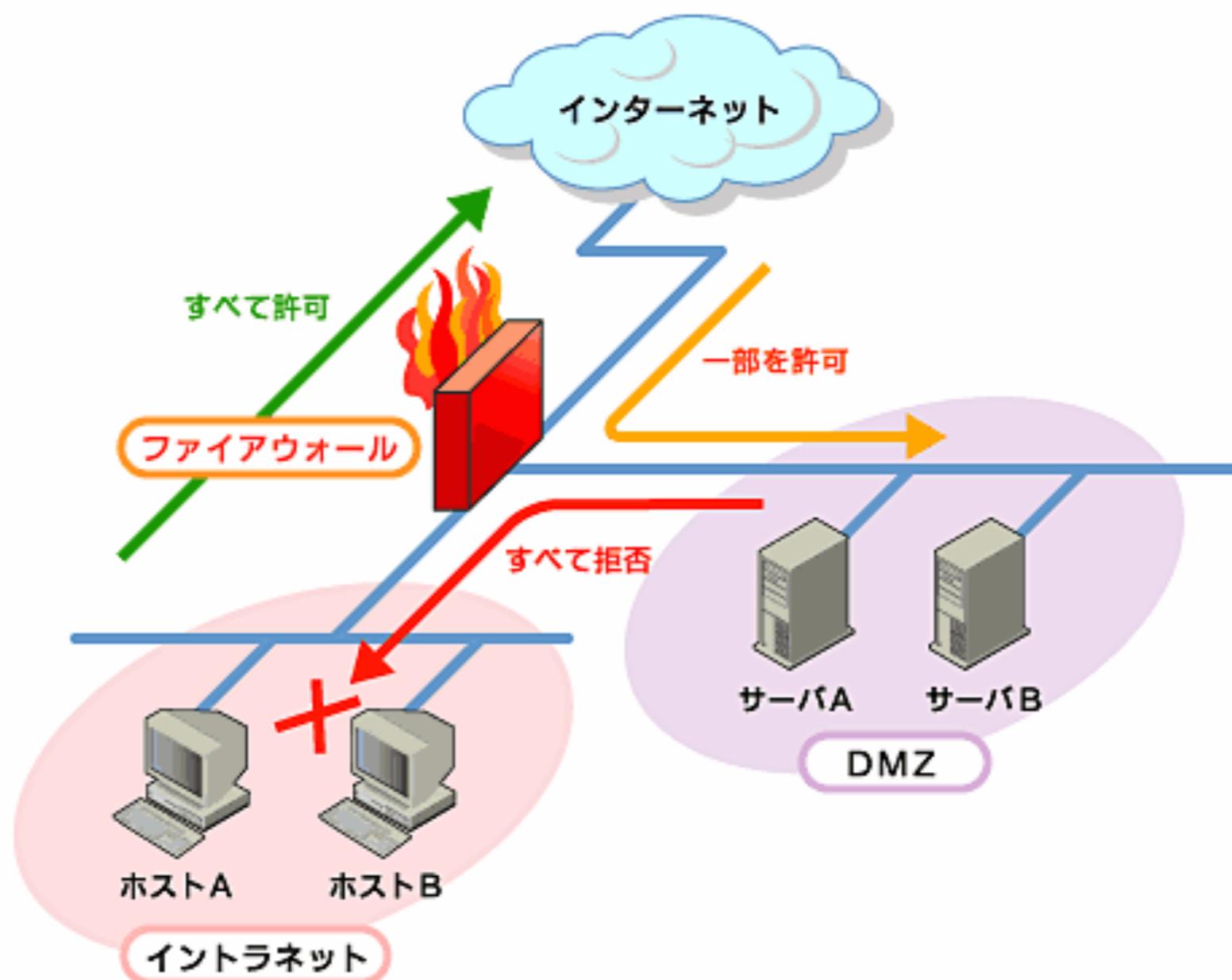
イントラネット (Intranet)

- 組織内networkの一呼称
 - 組織内networkを標準技術(TCP/IP)で実現
- Internetを“**Extranet**” ⇔ 組織内net.を“**Intranet**”
- 別名: 「セキュアセグメント」 「武装セグメント」

DMZ (Demilitarized Zone)

- Demilitarized Zone = 「非武装地帯」
 - Intranet内のnetworkの1つ
- Internet(外部)から/へのアクセスが必要な、以下の2種類の組織内設備をDMZ内に設置
 - 組織外(Internet)にサービスを提供する計算機：
(E-mail, Web, DNS, FTP)
 - 組織内network保護のためのシステム：
(Proxy, VPN, Content Filter, IDS)
- **Perimeter network** (境界ネットワーク) とも呼ばれる
@IT, セキュリティ用語辞典, 非武装地帯 DMZ (DeMilitarized Zone)
<http://www.atmarkit.co.jp/aig/02security/dmz.html>

動作概念



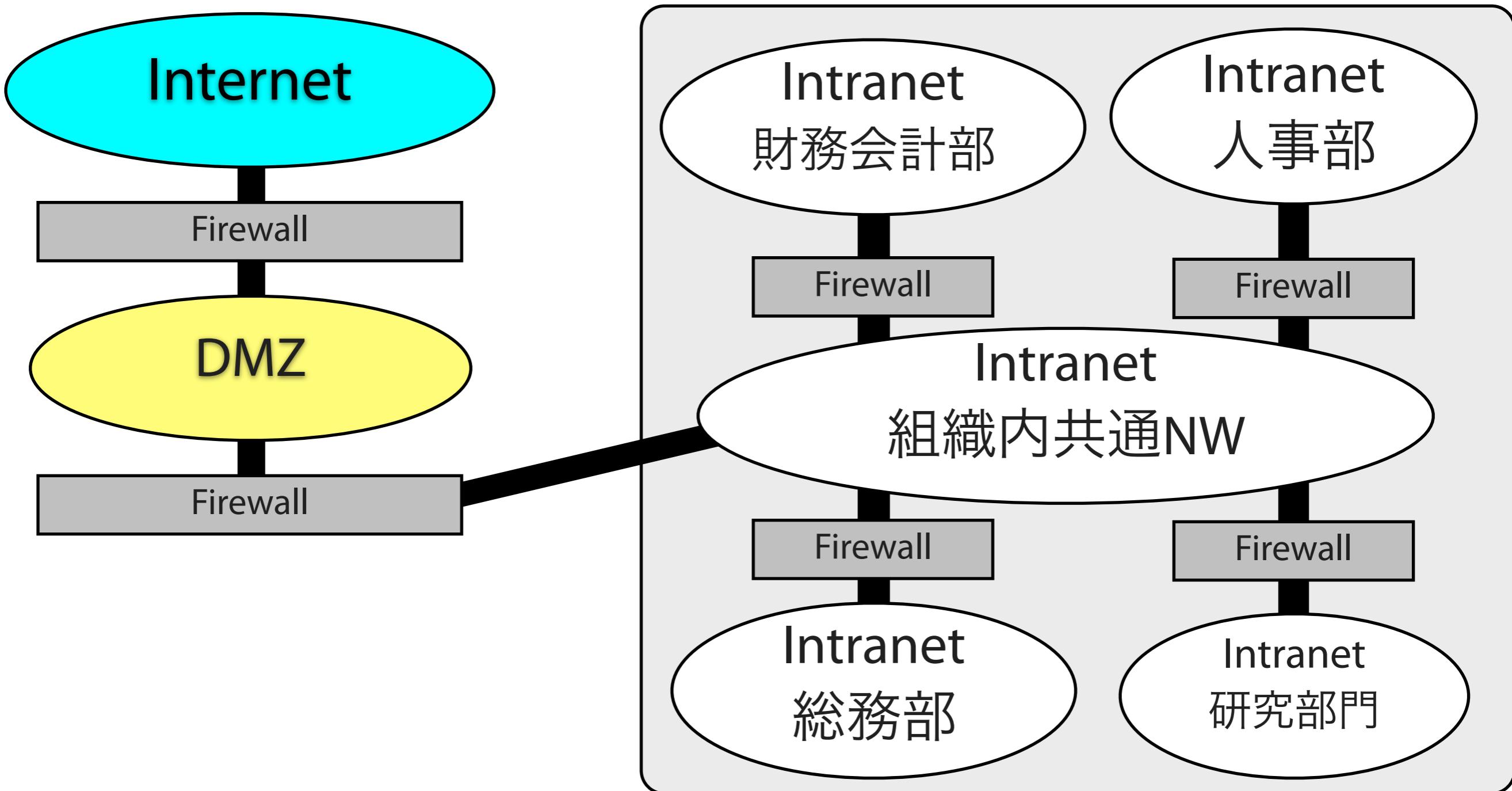
図引用) Firewall運用の基礎: 第1回 Firewallの基礎知識, (2001/05/17),
<http://www.atmarkit.co.jp/fsecurity/rensai/fw01/fw01.html>

よくあるルール

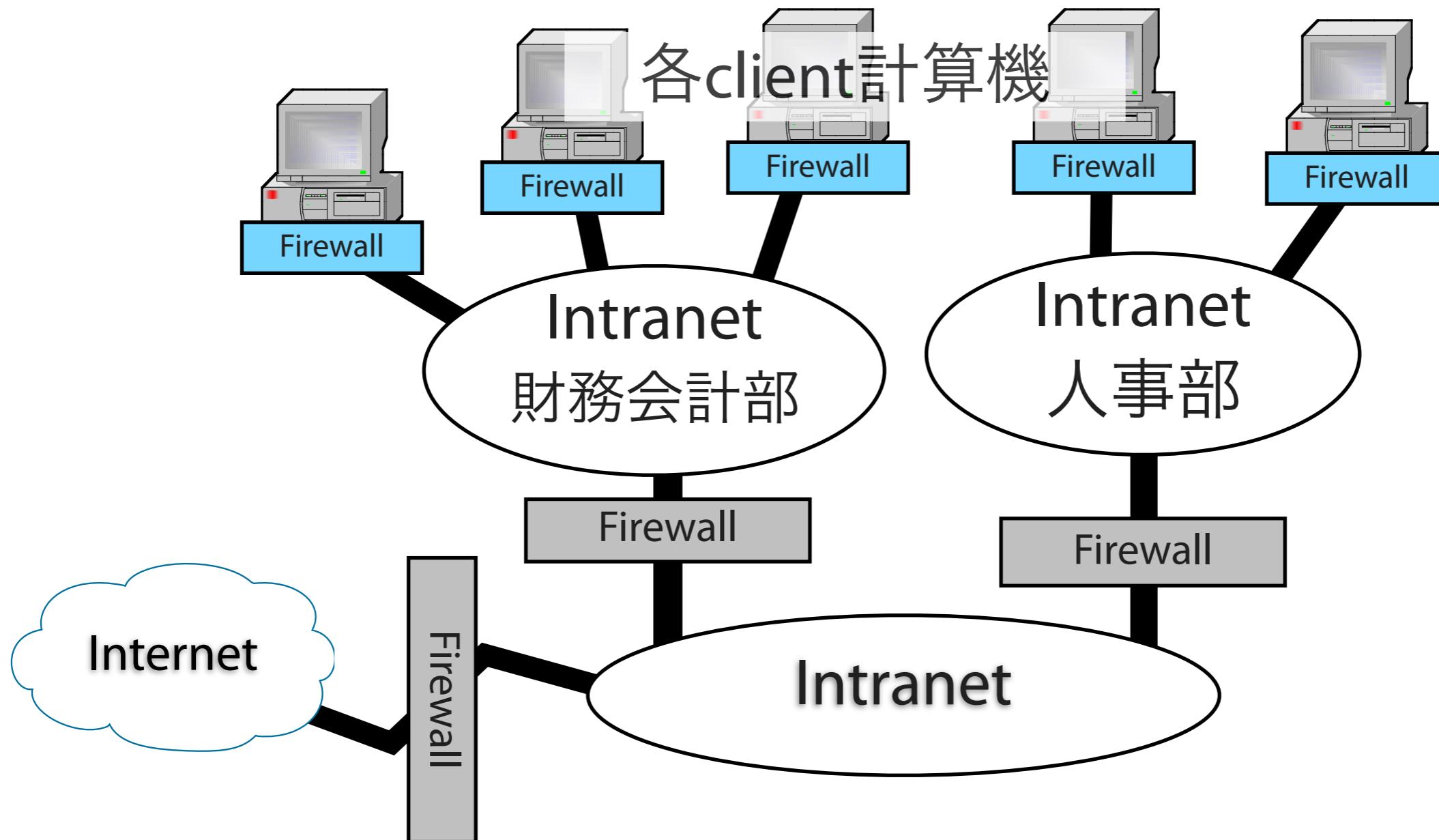
基本: Internet ⇒ Intranet、 DMZ ⇒ Intranetは
直接通信できないようにする

From	To	通信可否
Internet	DMZ	○
Internet	Intranet	×
DMZ	Internet	○
DMZ	Intranet	△
Intranet	Internet	×
Intranet	DMZ	△

組織Networkは多層化へ



そしてあらゆるシステムへ



Majorなクライアント OSにはfirewall機能が搭載
⇒ **Personal Firewall**

ネットワークアドレス変換

- NAT (Network Address Translation)
- NAPT (Network Address and Port Translation)
 - 言葉の使われ方が錯綜
 - NAT ≈ NAPT と一般的に理解されている
 - 別名: IP masquerading, many-to-one NAT, SNAT, DNAT

主目的：IP address枯渇への対応

private network/internet間接続におけるGlobal IP addr.の共有

副次的効果として疑似Firewallとして機能

Network Address Translation(NAT)

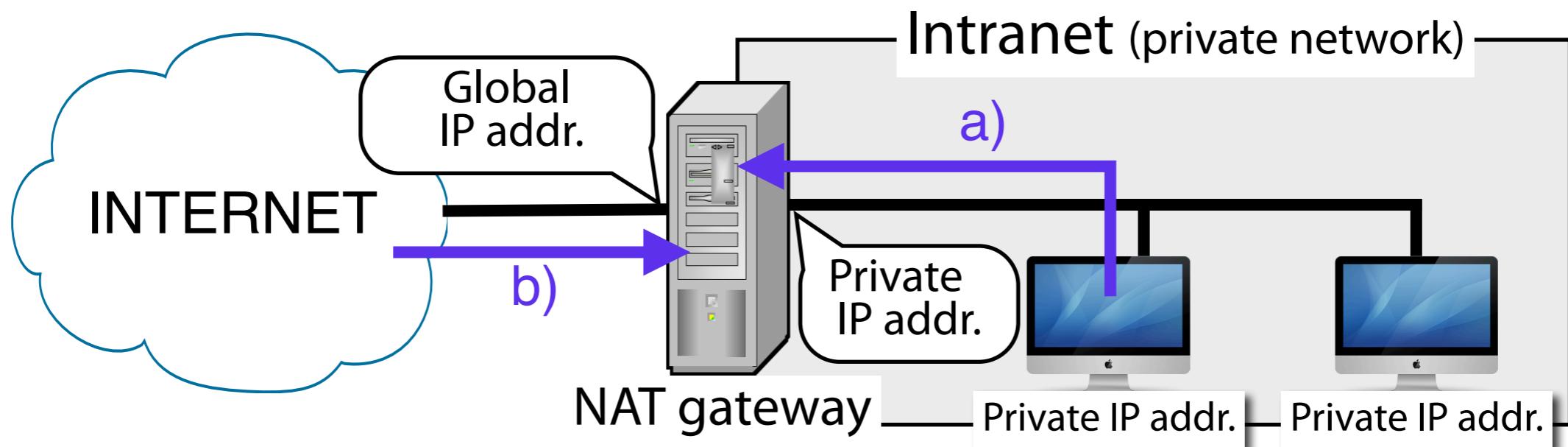
- Private IP addr.のNetworkをInternetと通信可能にしたい
 - Global IP addr.を必要台数分取得すればよい
⇒ 取得は手間とコストがかかる
 - 社内/家庭内のNetworkはPrivate IP addr.で十分
⇒ 決められた範囲内で自由にIP addr.を利用可能
 - ただ、社内/家からもInternetにもアクセスしたい
⇒ Internetに接続するにはGlobal IP addr.が必要
 - どうにかならないか？ ⇒ NATの利用

Network Address Translation(NAT)

- IP address (=Network address)を変換することで Private IP Net.とInternet間での通信を可能にする

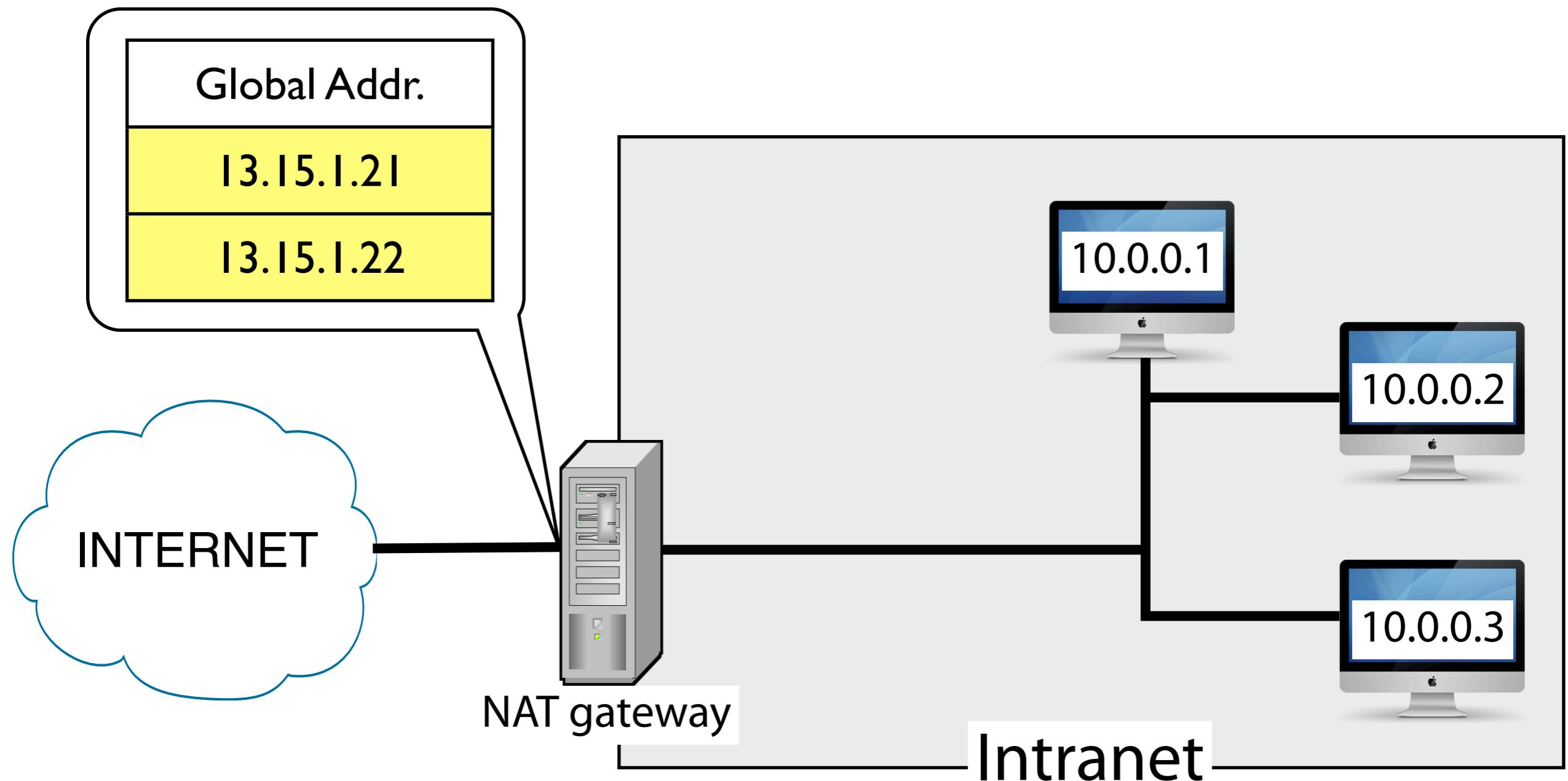
問題点

- Private IP addr.をInternet内通信で利用できない
(⇒そのままだと Internet内のRouterで破棄)
- Global IP addr.でGatewayに届いたpacketを誰に届けたら良いのか？

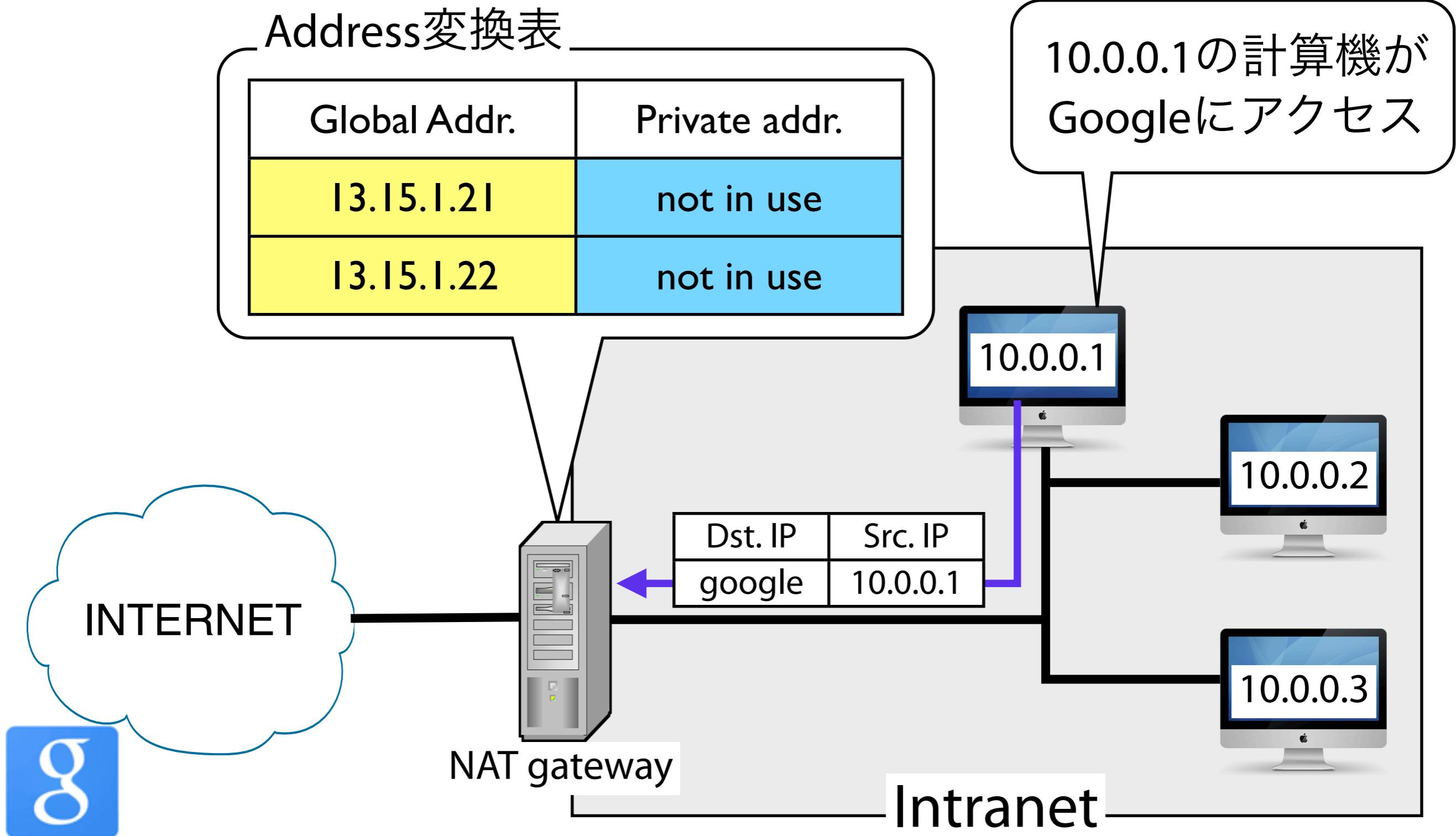


NATの仕組み

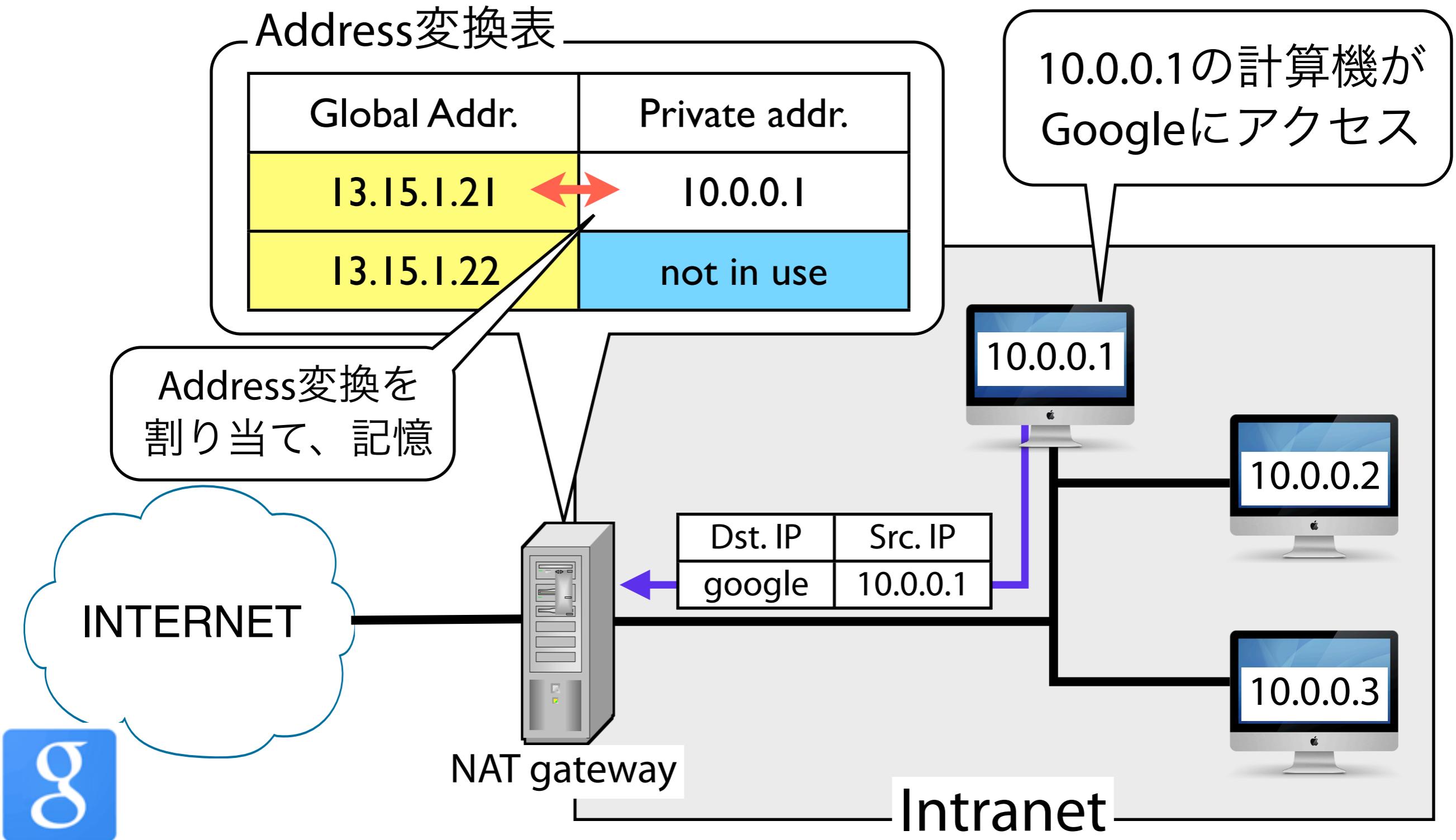
前提条件：NAT GWは2つのGlobal IP addr.を利用可能



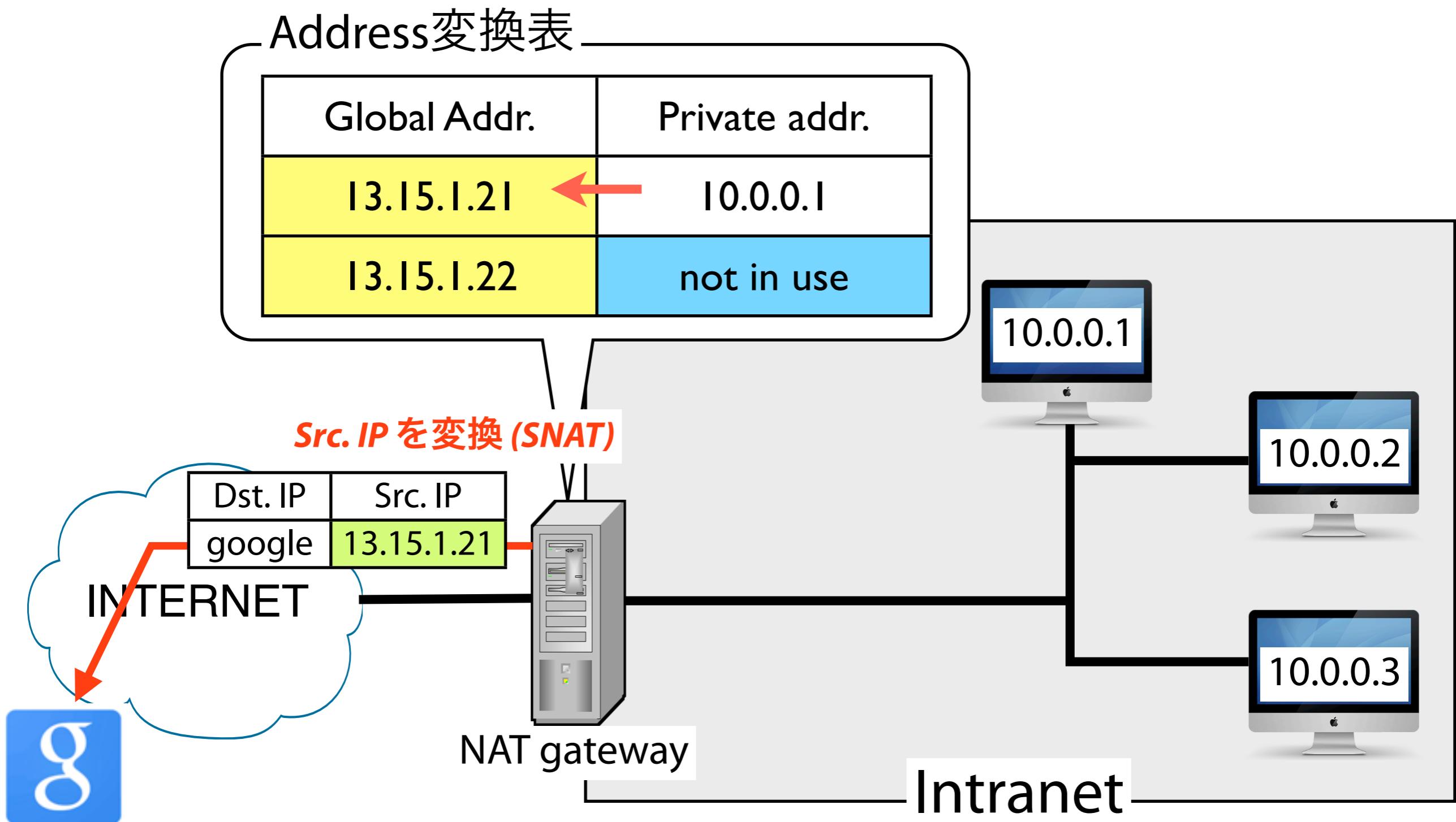
NATの仕組み



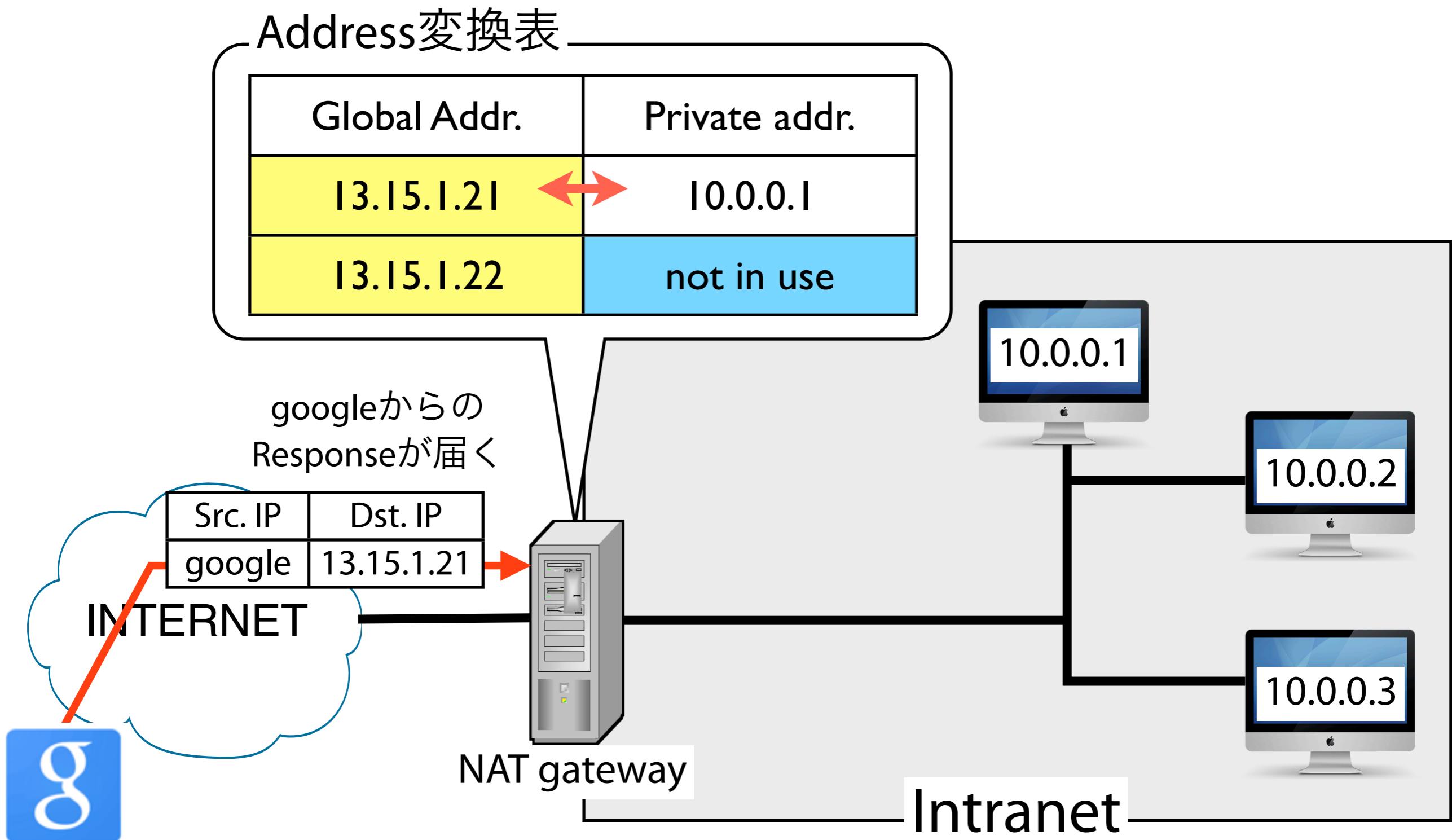
NATの仕組み



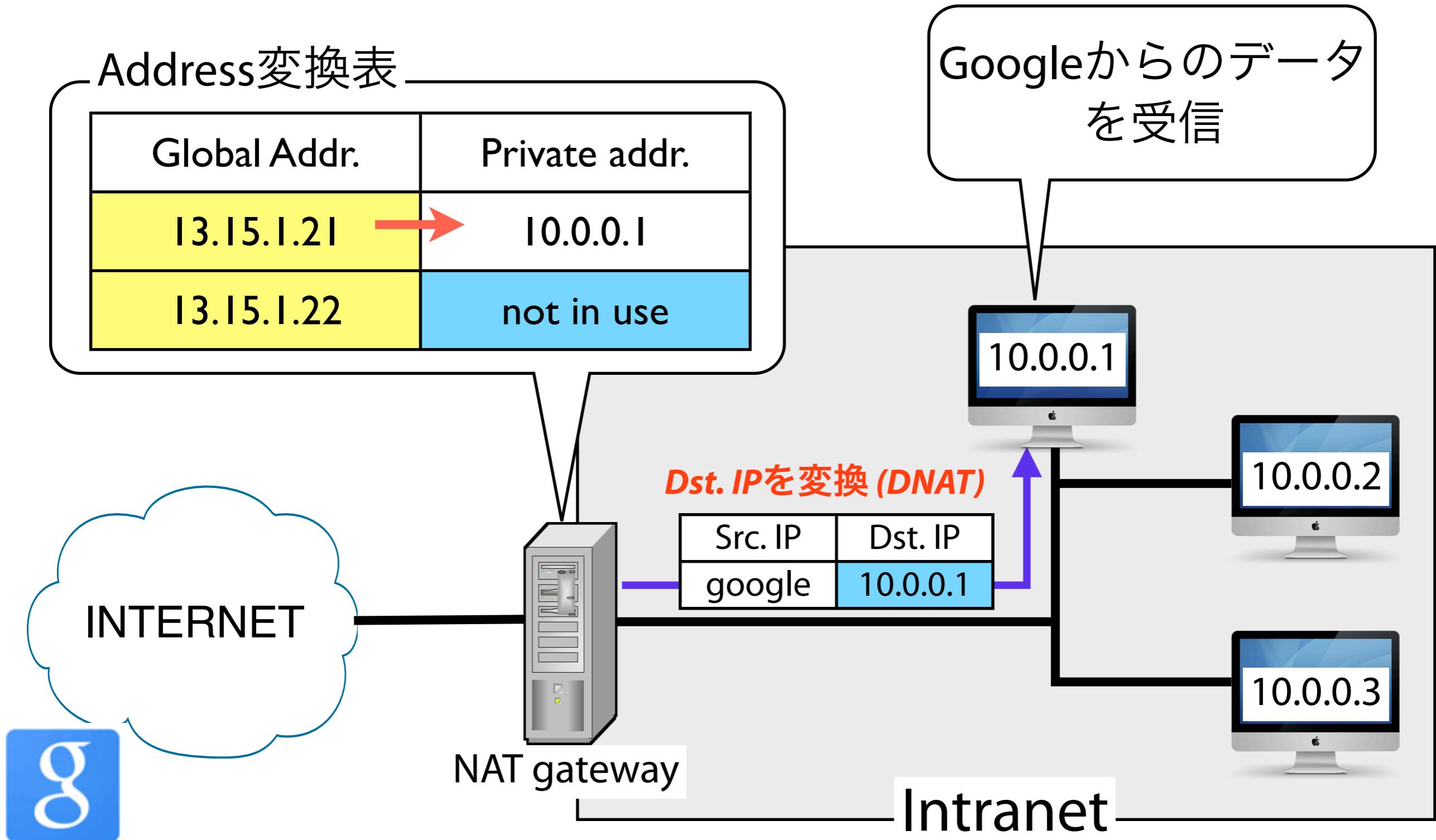
NATの仕組み



NATの仕組み

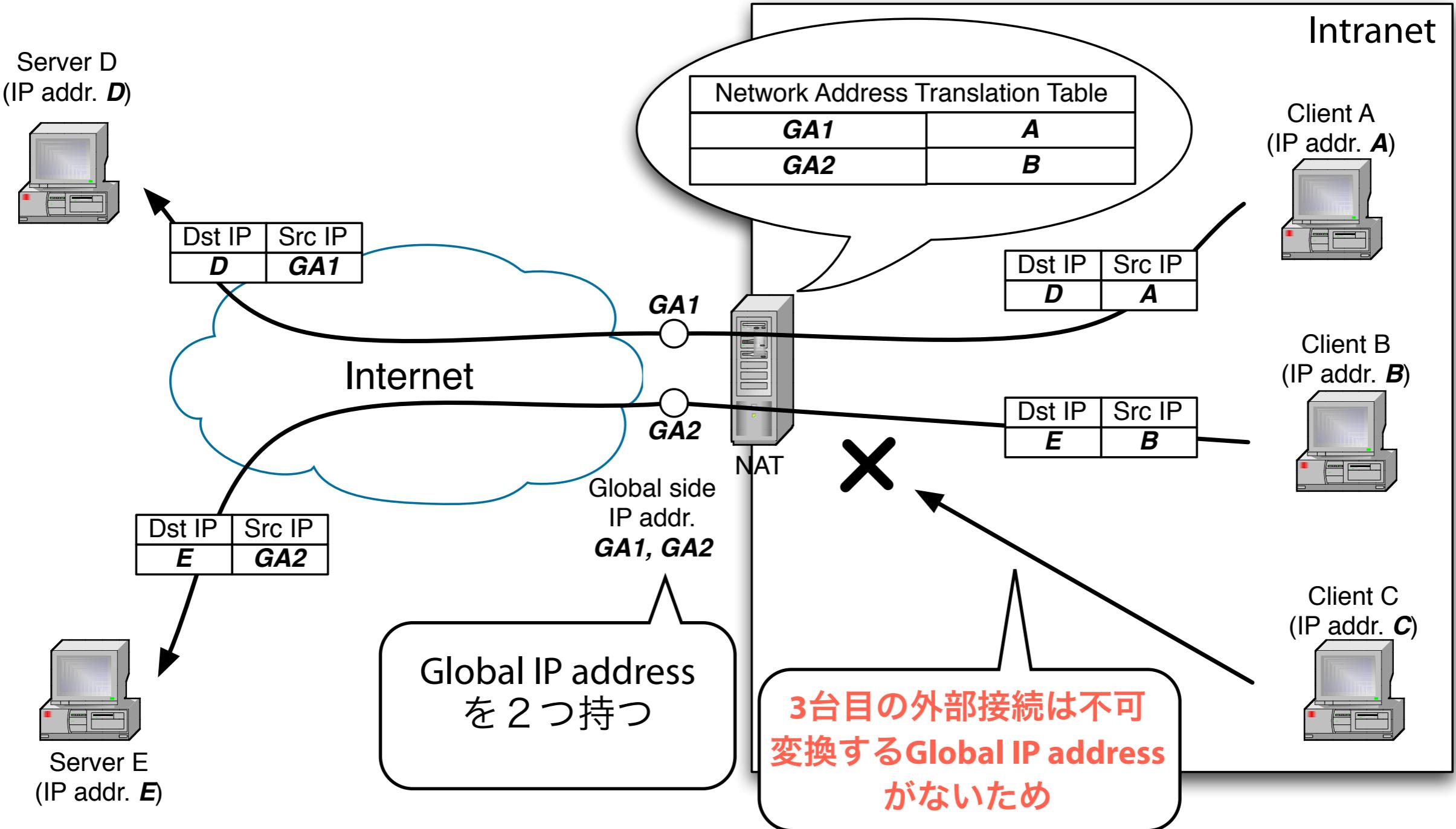


NATの仕組み



Network Address Translation(NAT)

- IP address枯渇への対応は限定的
⇒ 「Private IP addr. ⇄ Global IP addr.」 を一対一変換
 - Private network内的一台の計算機がGlobal IP addr. 1つを**占有**
 - NATのGlobal IP address数 = Private net.からInternetへの同時接続可能数
 - 対外接続数はGlobal IP addr.数で制限される (上限)
 - Global IPを1個しか持っていない
⇒ 自宅からは機器1台しかInternetに接続できない!!!



- NATは*Network address translation table*(アドレス変換表)を持つ
通過するIP headerの IP address をその都度変換
- 最大 Internet 同時接続数 = NATの所有Global IP address数

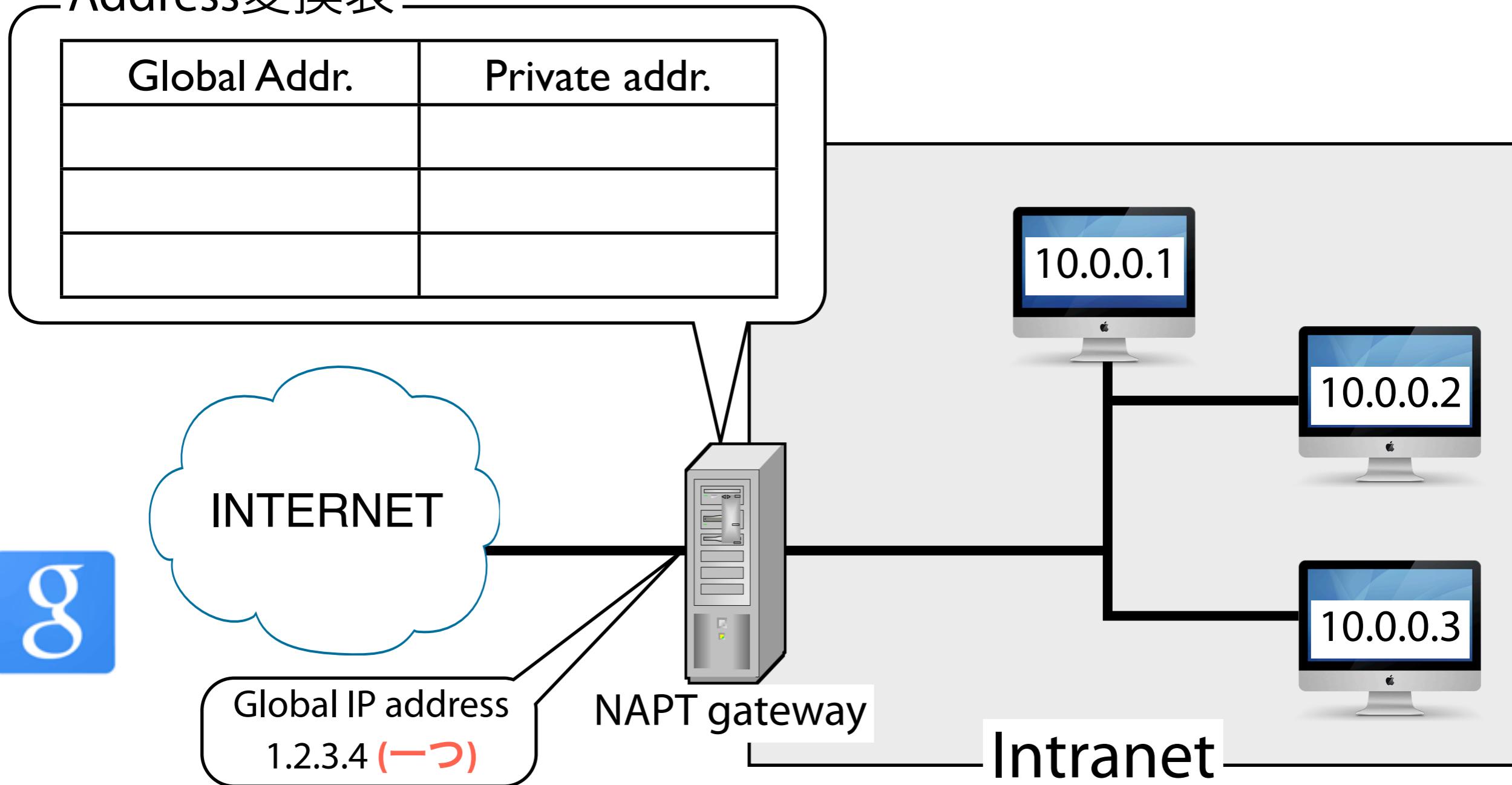
Network Address and Port Translation (NAPT)

- Global IP address 1つで Private networkから Internet に多数同時接続したい！ ⇒ NAPT
- (IP address, Port番号)の組みによるアドレス変換 ⇒ Private IP addr. から Internetへのアクセス時 2つのアドレス値を用いて Address変換する 「“Global IP addr.” + とあるPort番号」
- 要するに “Port番号” を活用 ⇒ Global IP addr. 1つでも複数の接続点を提供可能 ⇒ 1 IP addr. で60,000超の接続点を用意可能 (理論的)

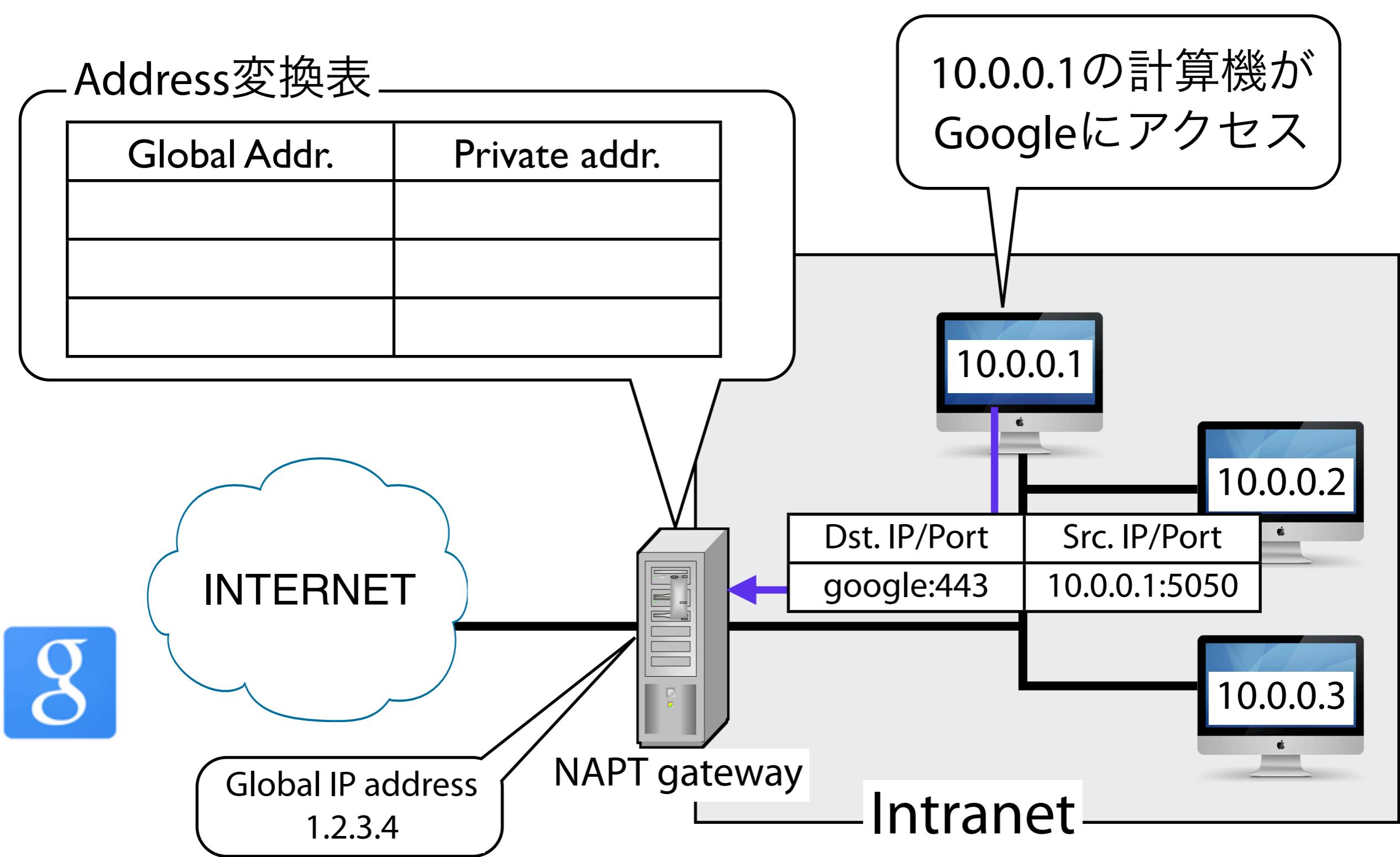
NAPTの仕組み

前提条件: NAPT gatewayはGlobal IP addr.を1つ利用可能

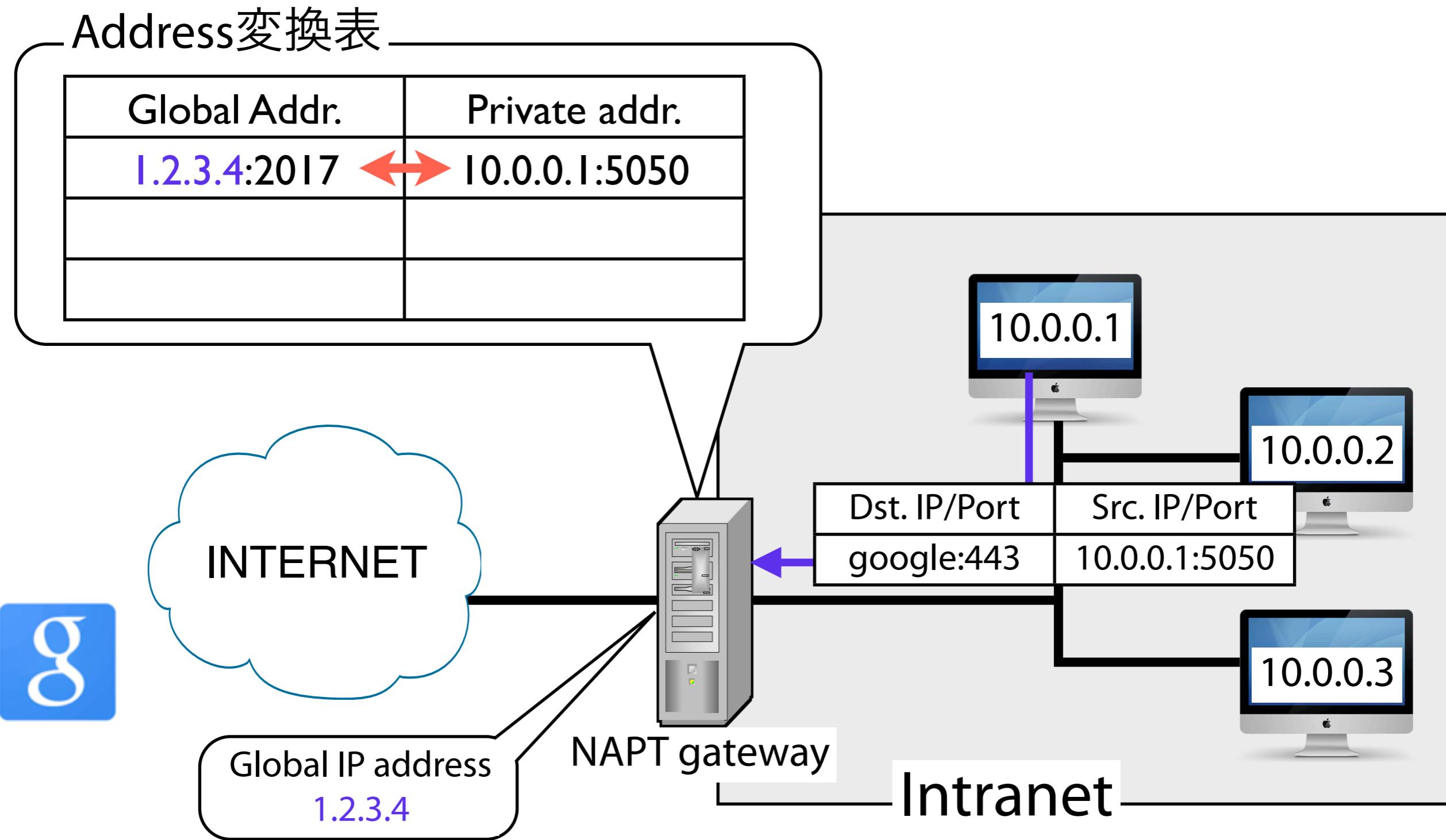
Address変換表



NAPTの仕組み

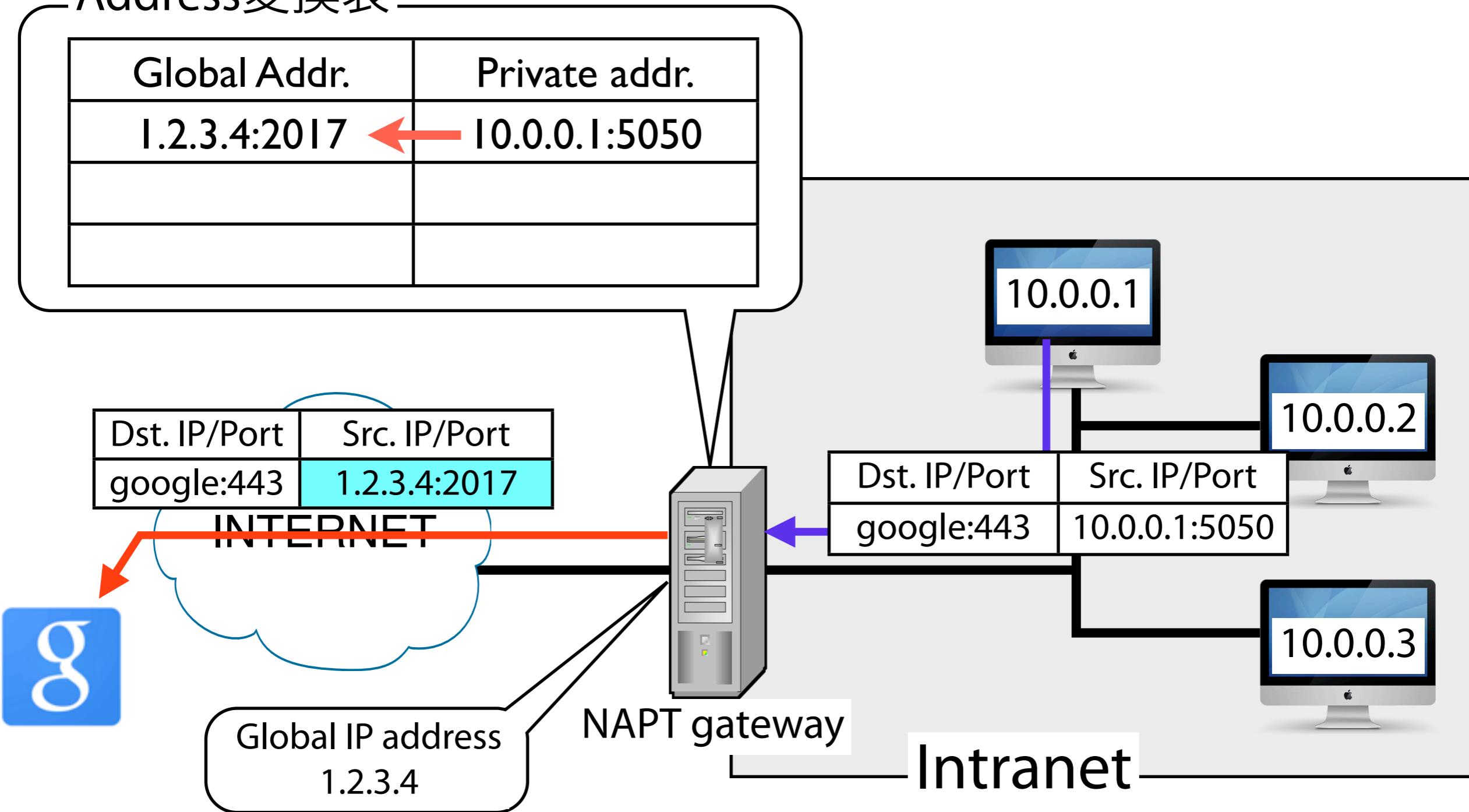


NAPTの仕組み



NAPTの仕組み

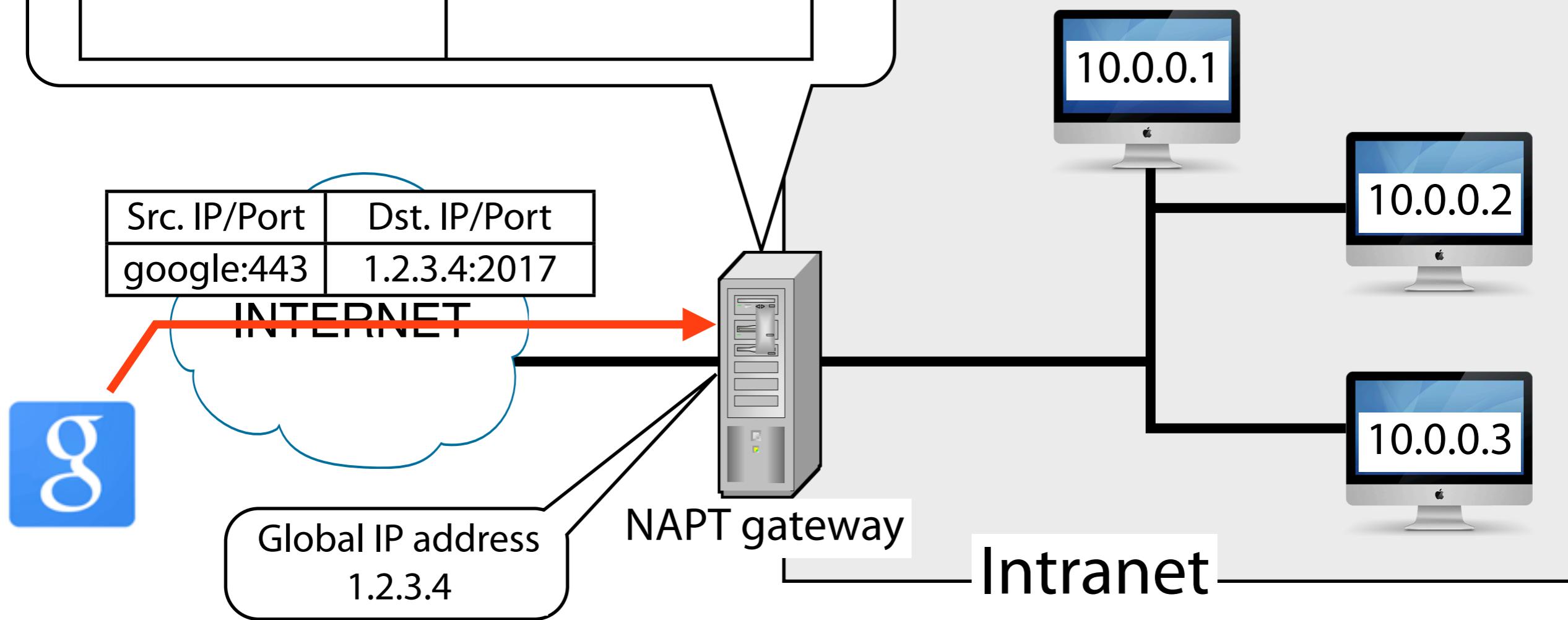
Address変換表 Addr.変換して、変換情報を記憶しておく



NAPTの仕組み

Address変換表

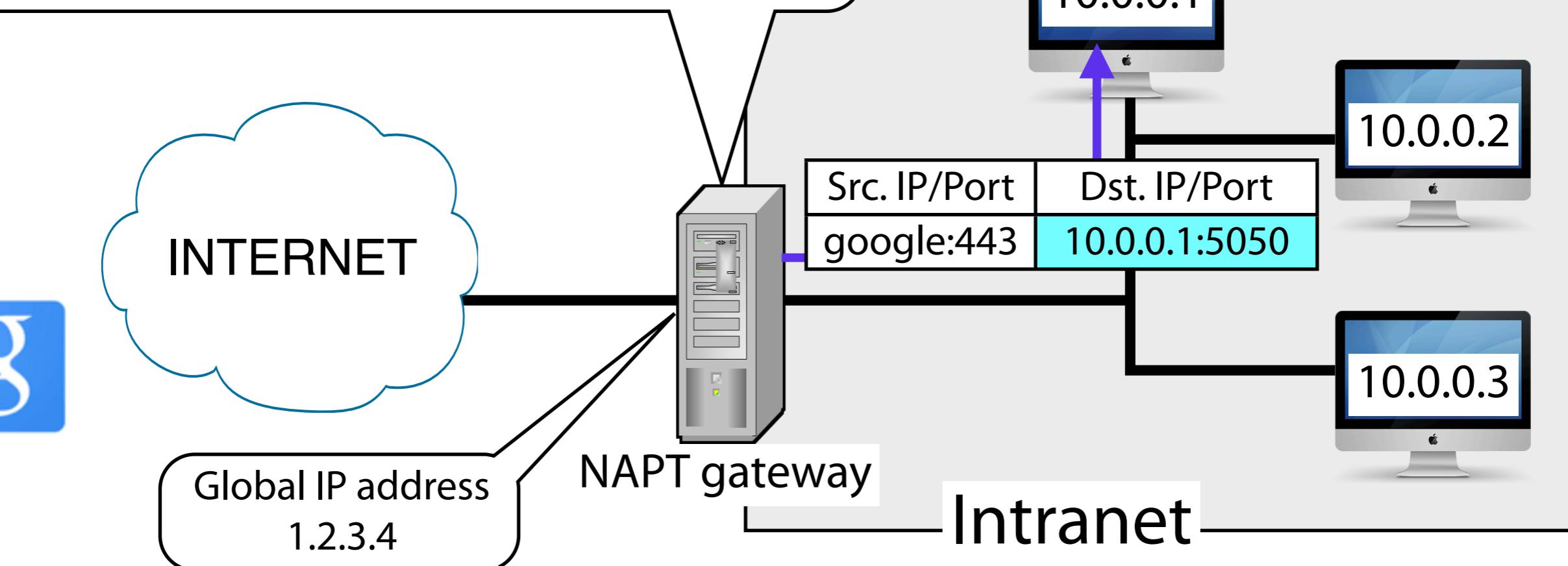
Global Addr.	Private addr.
1.2.3.4:2017	10.0.0.1:5050



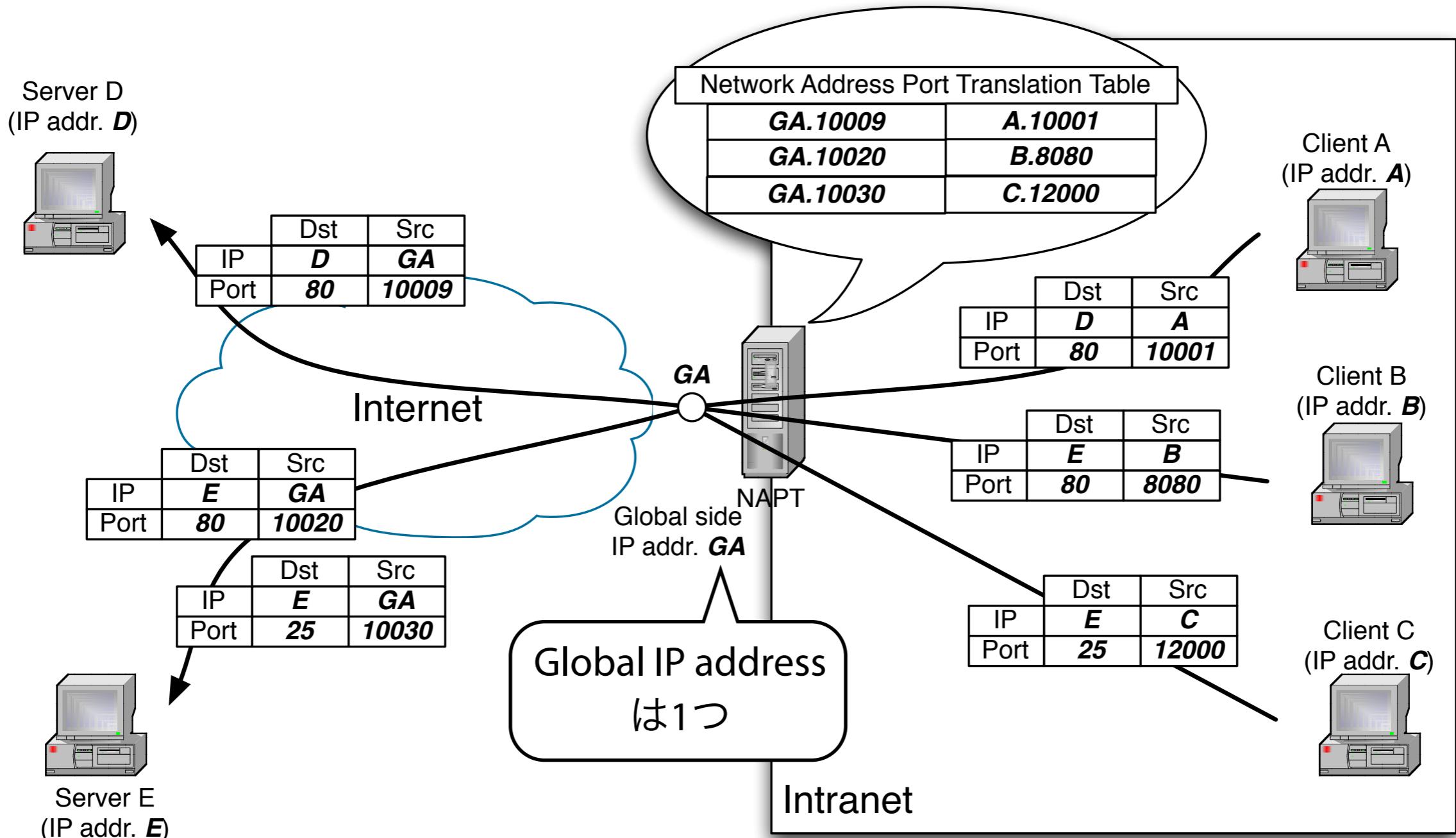
NAPTの仕組み

Address変換表

Global Addr.	Private addr.
1.2.3.4:2017	10.0.0.1:5050

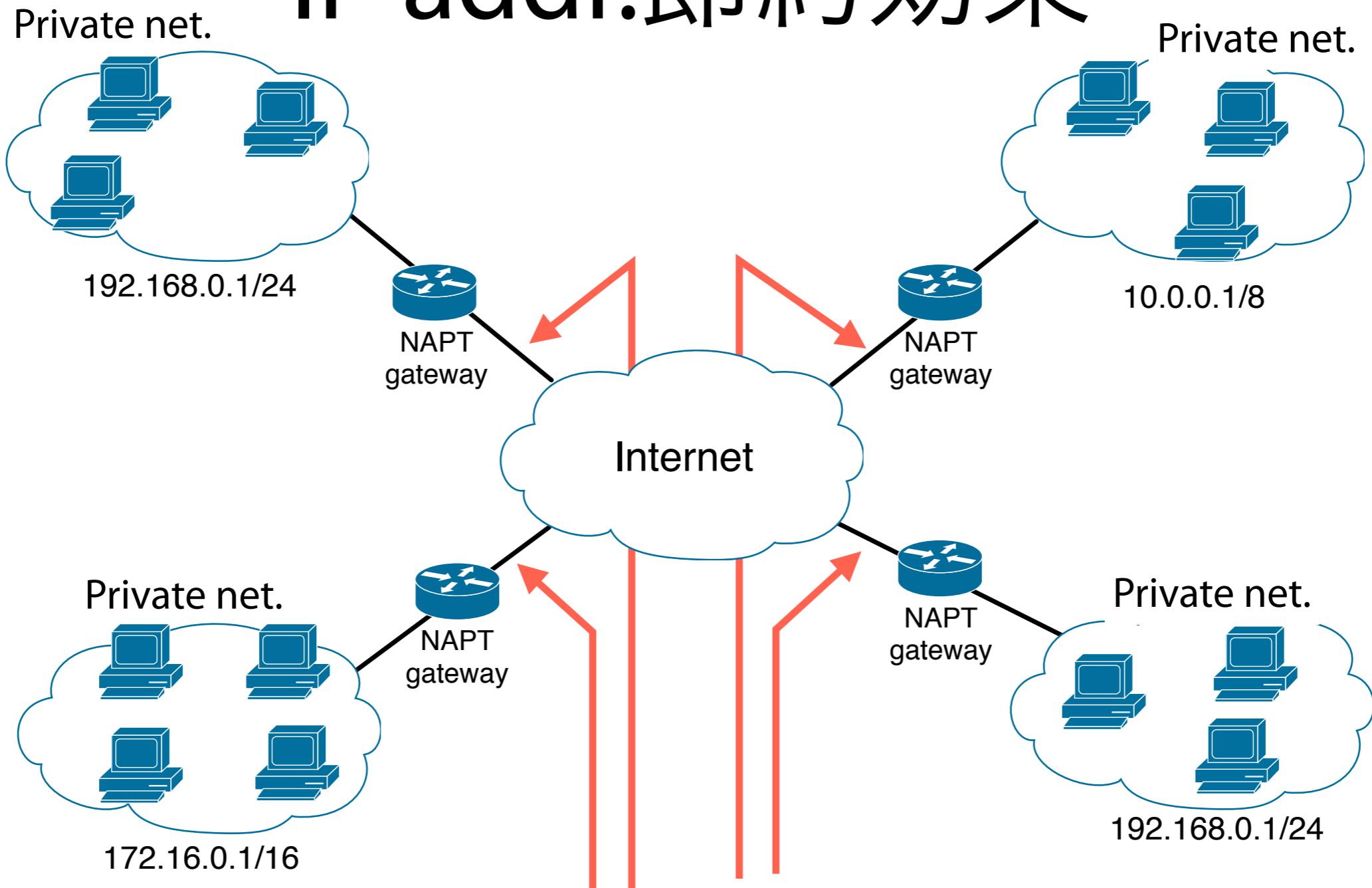


NAPTは“Network address port translation table”
 (アドレス&ポート変換表)を持ち、アドレス変換を実施



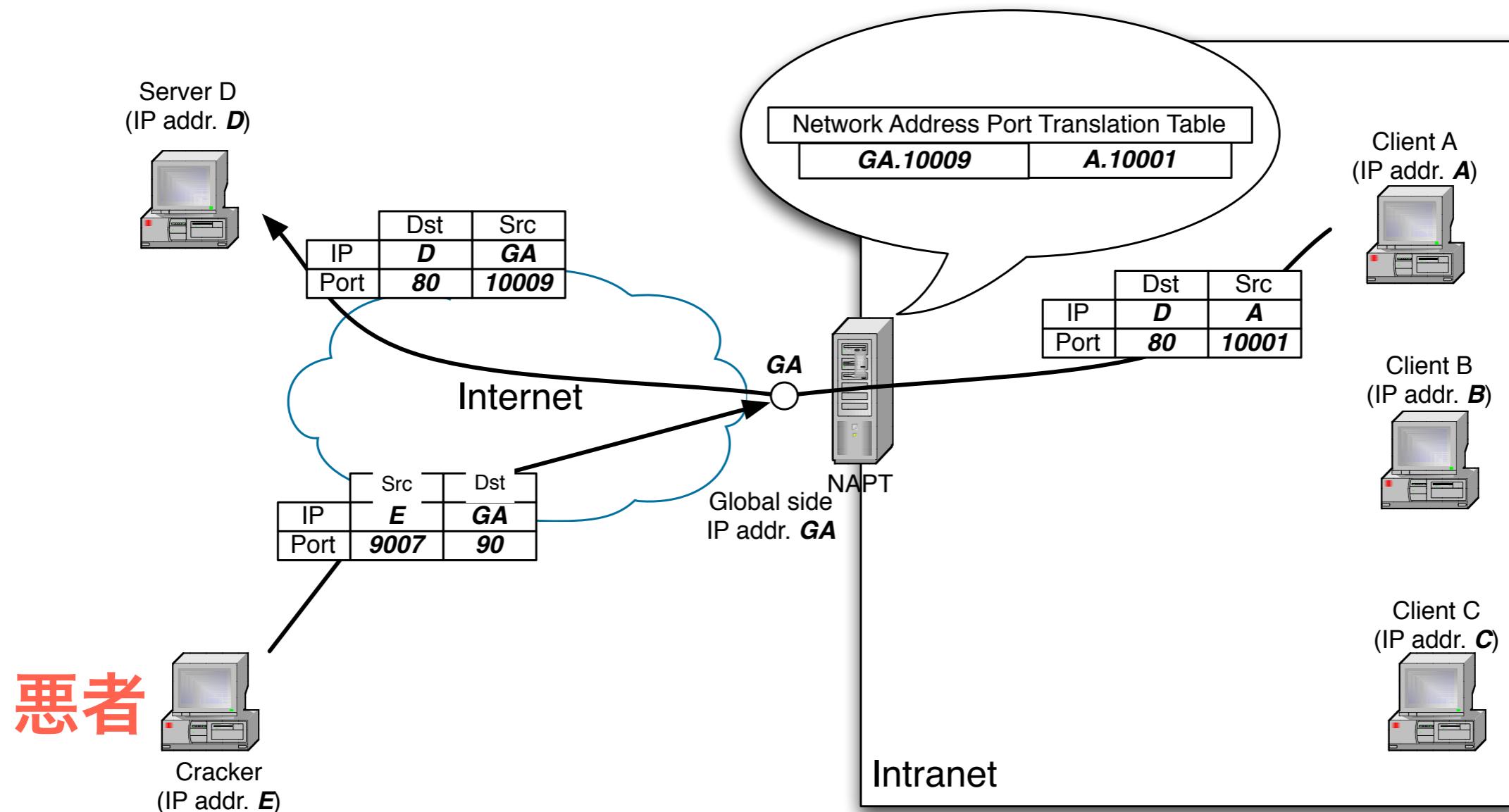
NAPTでは、Global IP address1つでもInternetへの
 同時複数接続が可能 ⇒ IP addr.枯渇問題に有効

IP addr.節約効果



4つのprivate network / 計13台の計算機を
4つのGlobal IP addressでInternet経由で接続可能

NAT/NAPT の 疑似Firewall効果



アドレス変換Tableに変換情報がなければ
外部(Internet)からIntranet内の計算機には接続不能

しかもRuleは自動生成