NTT

「そのIPv4アドレス共有環境、通信できる？」
ポート数制限下環境での通信影響を緩和する方法の紹介

2012.7.5

NTT ネットワーク基盤技術研究所
内藤　憲吾

今回紹介する方式を、
IETFにて標準化提案しています。
http://tools.ietf.org/html/
draft-naito-nat-resource-optimizing-extension-01

NTT　1.　研究のモチベーション

IPv4アドレスが枯渇し、割り当て可能なアドレスリソースが減少してきています。IPv4通信を延命させるには、今後、より多くの人数でグローバルアドレスとポートを共有する必要が出てくると考えます。

そうすると、ひとりのユーザが使用できるグローバルポートの数が制限され、通信に様々な影響がでてきそうです。

この環境で、通信できる？
やばそうなので、考えてみた

IPv4アドレスたくさん

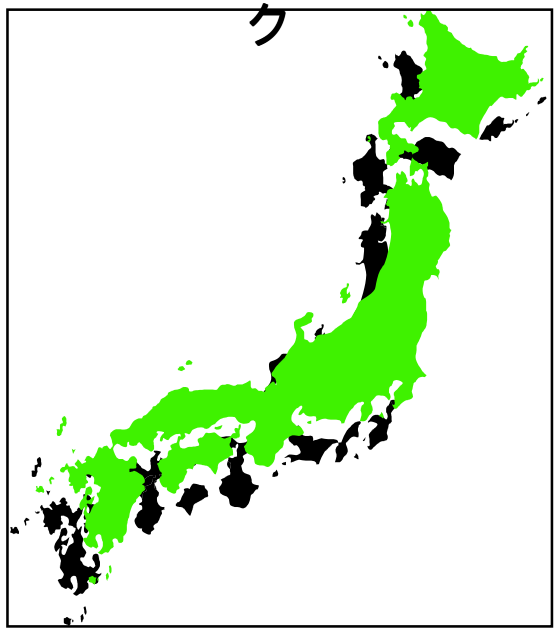
ちょっとアドレス共有

すごく
アドレス共有

NTT　2.　ポート制限による影響

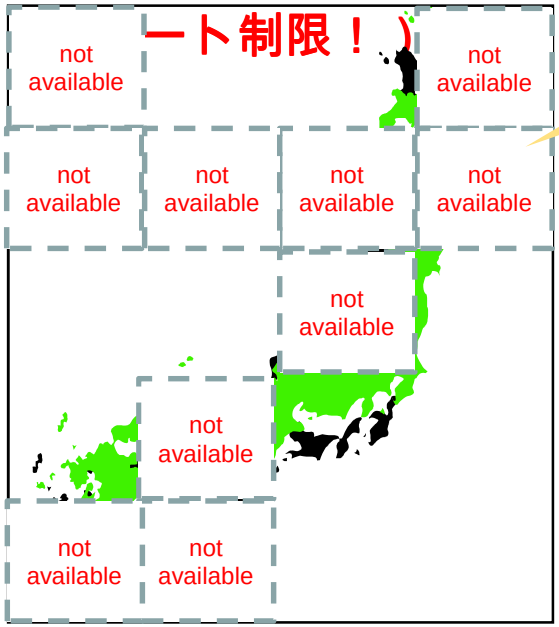
Webサイトなどでは、情報を取得するために、一度に多くのTCPセッションを生成することがあります。必要なセッション数を生成できない場合、情報が欠損し、通信に影響が出るケースがあります。試しにポートを50程度に制限して様々なサイトに通信を試みたところ、40/200サイト程度に影響が見られました。

IPv4アドレスたくさんネットワーク



すごくアドレス共有ネットワーク

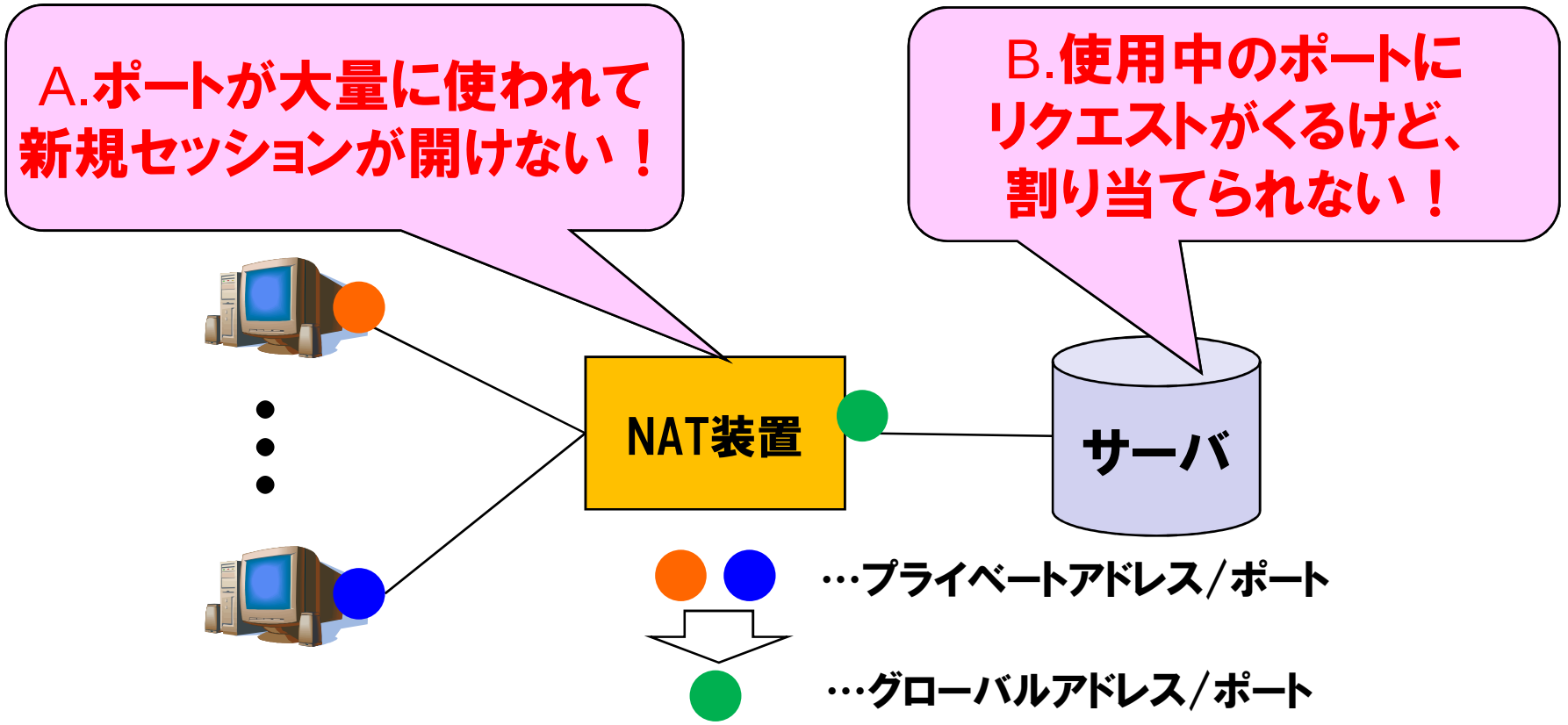
ート制限！）



情報欠損！！

3.　なぜ通信影響が生じる？　（1/3）

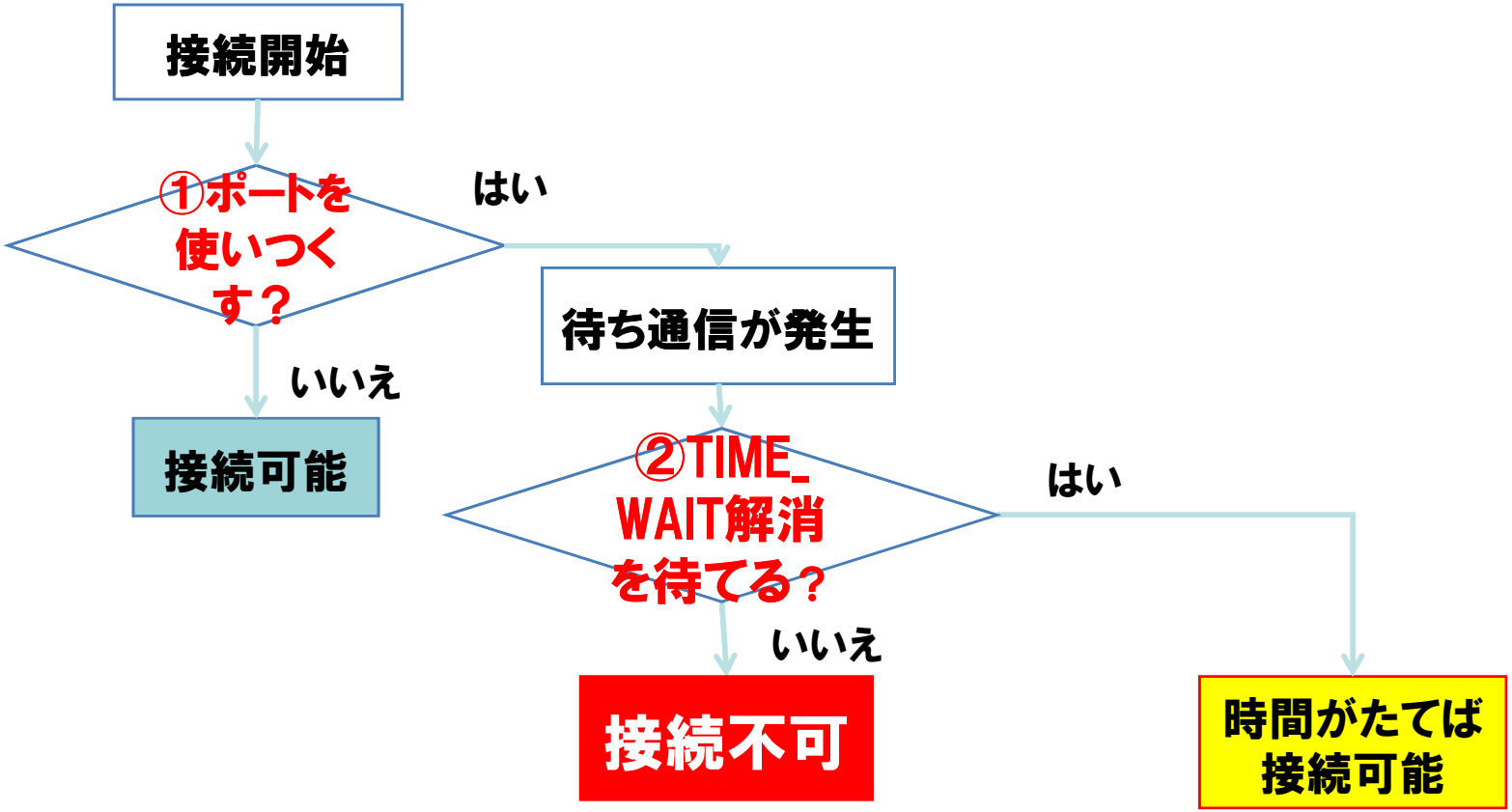
A.クライアント側（下図の場合はNAT装置）とB. サーバ側それぞれで対処を考える必要があります。ポート制限時の通信影響の主な原因のひとつは、ポート制限によって必要な数のTCPセッションが開けないことです。



使えるポートが少なくても、
どんどん使い回していけば、
いいんじゃないの？

NTT 3. なぜ通信影響が生じる？ (3/3)

TCPセッションは情報取得後にTIME_WAIT(*1)状態となり、すぐにはポートを解放しない(*2)
古い情報の混入防止と、LAST ACK喪失時もセッションを正常に閉じるためのTCPの仕様です。ポートが解放されれば、次の通信に再利用できますが、再送時間内で空きポートが作れない場合は、情報取得に失敗します。

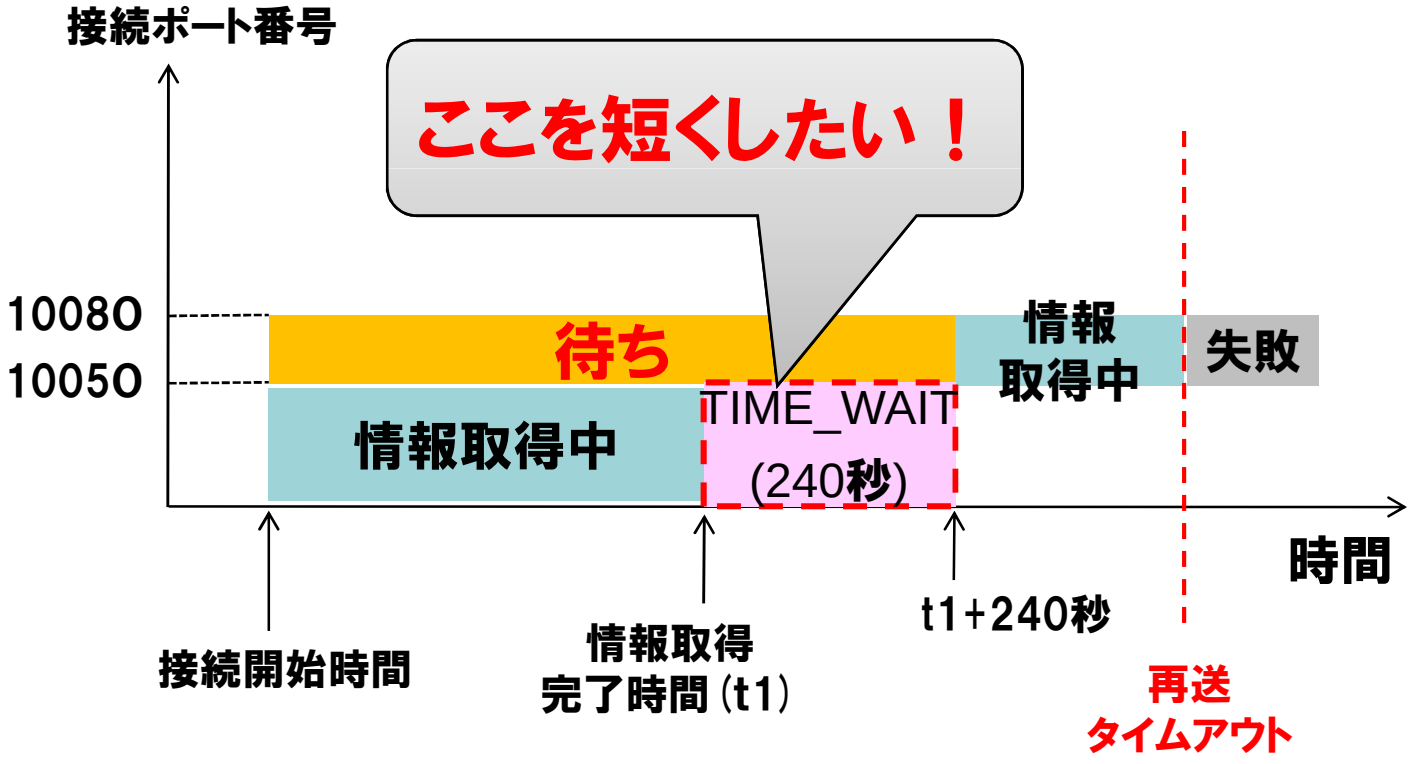


*1:旧パケットの混入防止、LastACK喪失時に対応するため情報取得後も一定時間、ポートを解放しない
*2:具体的には、2×MSL秒。(Max Segment Life:パケットの最大生存時間)。2×MSLはOSにより60秒～240秒程度。

NTT 4.　緩和方式その1：　TIME_WAIT「0」 方式

おもいきって、TIME_WAIT値を0にコンフィグする。
→影響は緩和できるけど、別の問題が起こらないかは、要検討。。。

例）
1ユーザあたりの使用可能ポート数が50に制限された環境で、80ポートが必要な接続を行った場合



4. 緩和方式その2
①RFC6191/②1323 PAWS to NAT方式

①Timestamp値およびシーケンス番号が新しい通信に、TIME_WAIT状態のセッションを解放して割り当てる。 → RFC6191の動作

②最新パケットのTimestamp値/シーケンス番号より小さい値を持つパケットを破棄する。

FIN+ACKが再送された際に、ACKを返す実装をすれば、LAST ACK喪失対応も可能です。なお、サーバ側は、①相当の挙動を示すものが多いため、NATを通過するパケットの値を単調増加するように書き換えてあげれば、影響を緩和可能と考えます。