JANOG 52　2023/07/06

CGN/Firewall for 5GC Fabric

ソフトバンク株式会社
黒澤 潔裕

本日の内容

SoftBank

1. キャリアバックボーンとClos Fabric
   - 5GSAのアーキテクチャをIP Clos Fabricで表現してみよう＋

2. Clos Fabric
   - Fabricを作る際に考慮することをディスカッション

➡ 3. CGN/Firewall for 5GC Fabric
   - 5GC FabricのSecurityを支える技術

自己紹介

- 名前:
  黒澤 潔裕(Kurosawa Kiyohiro)

- 出身:
  神奈川県横浜市

- お仕事:
  下記を中心とした設計業務全般
  - インターネットPE
  - SGi/N6網 ← 先のsession(5GC Fabric)
  - インターネット接続用CGN/FW ← このsession

- JANOG歴: 4回目(初登壇)

CGN/FW for 5GC Fabric

1. CGN/FWとは？
2. 我々に求められる在り方
3. 快適な環境を追い求めて
4. 将来のCGN/FWを考えて

CGN/FW for 5GC Fabric

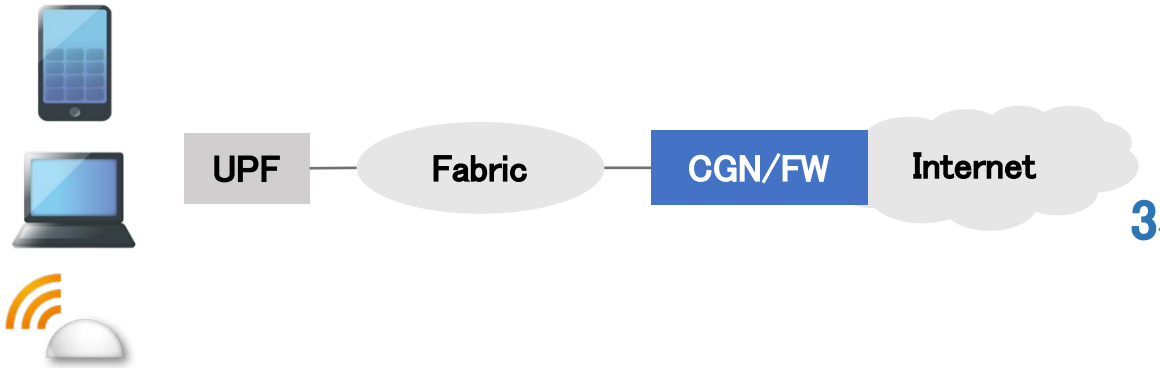
1 CGN/FWとは？

2 我々に求められる在り方

3 快適な環境を追い求めて

4 将来のCGN/FWを考えて

CGN/FWとは



多様なサービスを擁している

- スマートフォン
- PC
- IoT機器　　etc...

3種類のアドレス帯を提供

- IPv4 Private Address
- IPv4 Global Address
- IPv6 Address

すべての環境における「接続性」「安全性」→ CGN/FWを活用

みなさんに質問です

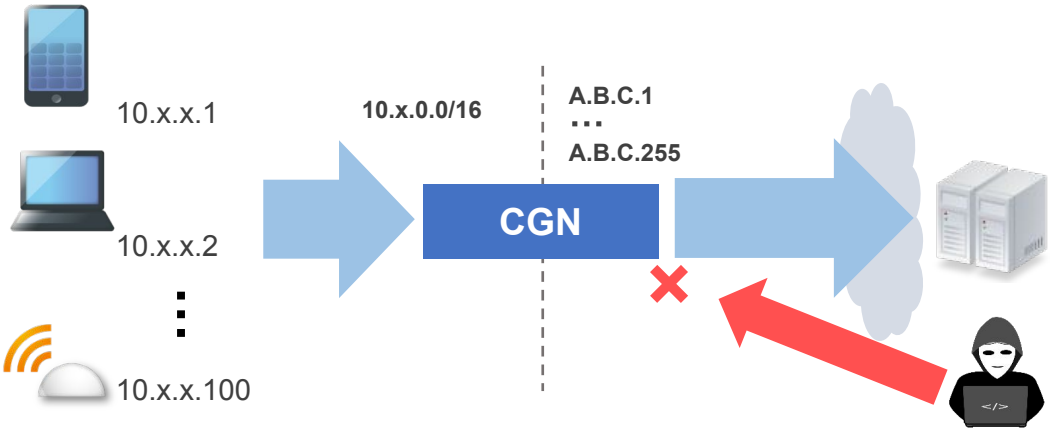
C G N

Carrier Grade NAT

きいたことありますか？

Carrier Grade NAT

Private IPを持つ複数の端末でグローバルIPを共有するための巨大NAPT



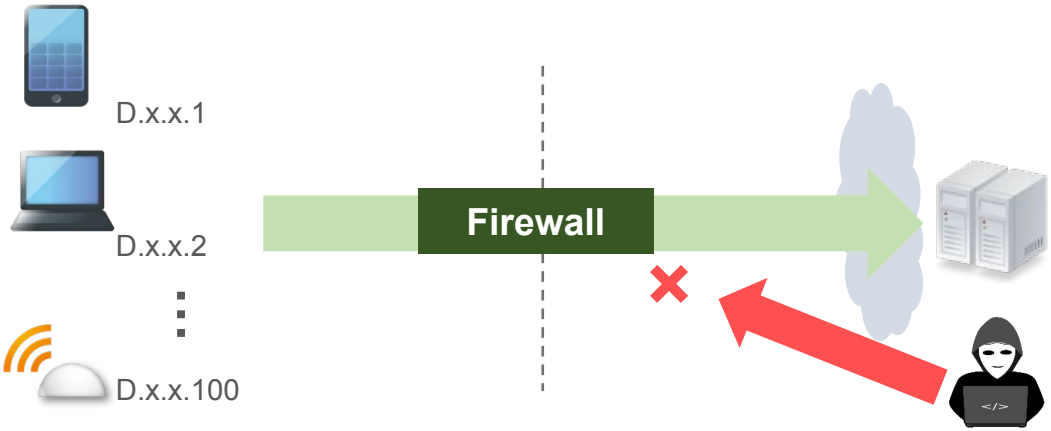
Src IP	Src Port	Dst IP	Dst Port	Translated Src IP	Tranlated Src Port	Dst IP	Dst Port
10.x.x.1	65001	5.6.7.8	80	A.B.C.1	50000	5.6.7.8	80
10.x.x.1	65002	2.3.4.5	30000	A.B.C.1	23000	2.3.4.5	30000
10.x.x.2	65001	1.2.3.4	443	A.B.C.200	50000	1.2.3.4	443
10.x.x.100	65001	9.8.7.6	443	A.B.C.10	54000	9.8.7.6	443

Points

アドレスの有効活用
☞ IPv4=限られた資源

不正な通信をblock
☞ 安全な環境の実現

アドレス変換不要のケース(Global IP v4/v6)も不正な通信から保護



Src IP	Src Port	Dst IP	Dst Port
D.x.x.1	65001	5.6.7.8	80
D.x.x.1	65002	2.3.4.5	30000
D.x.x.2	65001	1.2.3.4	443
D.x.x.100	65001	9.8.7.6	443

Points

アドレスは変換なし

不正な通信をblock
☞ 安全な環境の実現

CGN/FW for 5GC Fabric

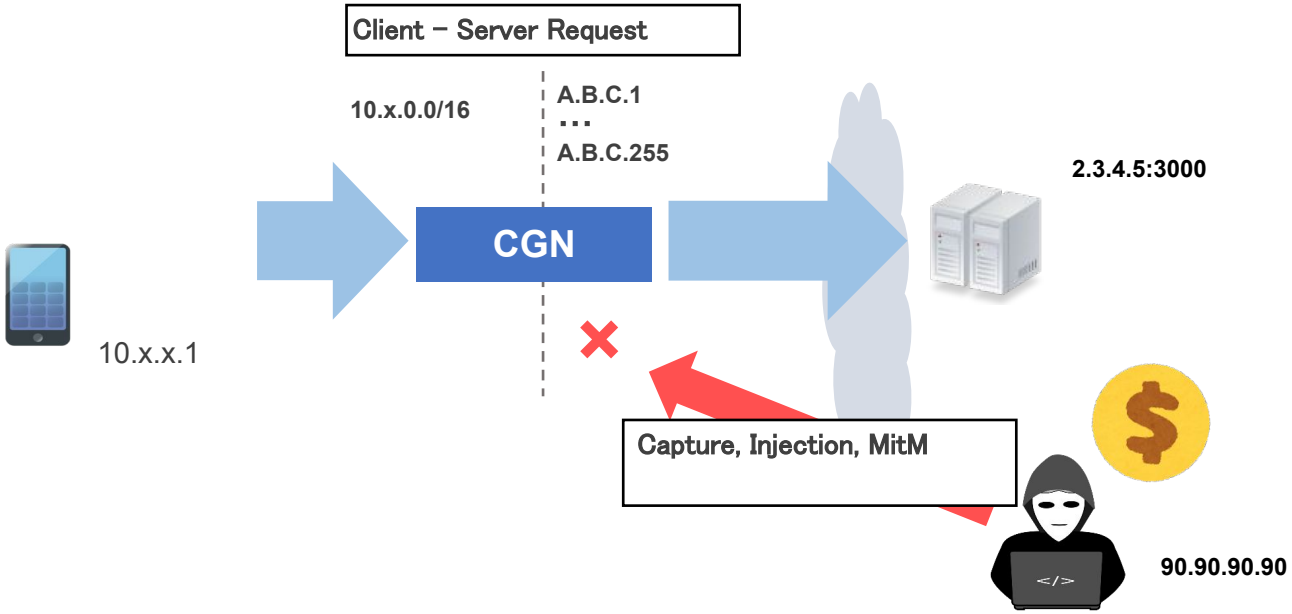
1 CGN/FWとは？

2 我々に求められる在り方

3 快適な環境を追い求めて

4 将来のCGN/FWを考えて

一般的なパターン



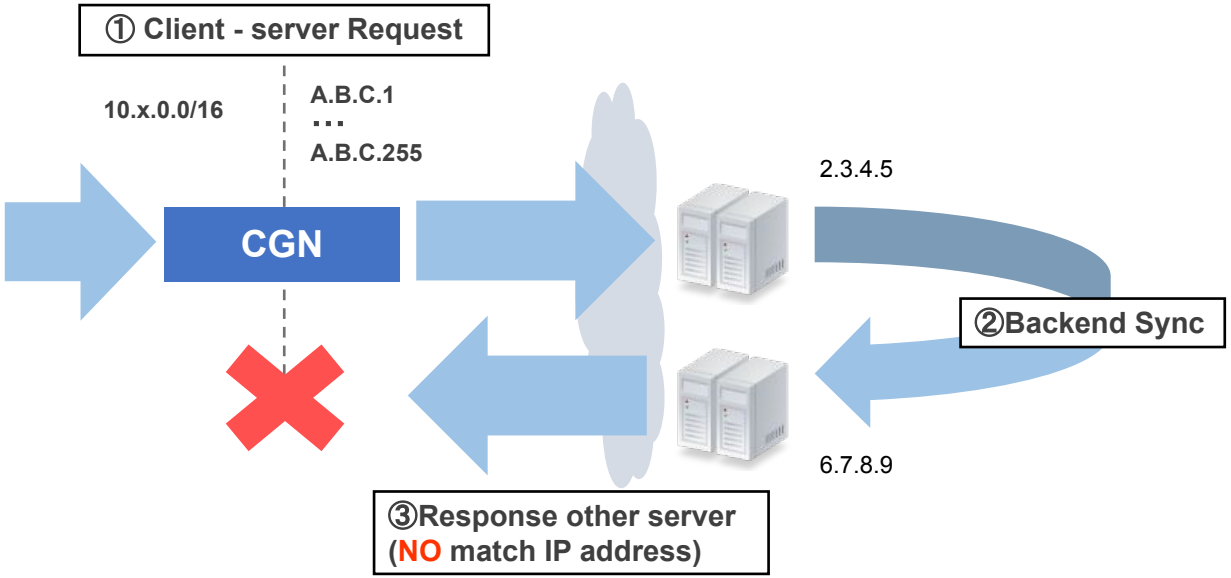
Src IP	Src Port	Dst IP	Dst Port	Translated Src IP	Tranlated Src Port	Dst IP	Dst Port
10.x.x.1	65001	5.6.7.8	80	A.B.C.1	50000	5.6.7.8	80
10.x.x.1	65002	2.3.4.5	30000	A.B.C.1	23000	2.3.4.5	30000
10.x.x.2	65001	1.2.3.4	443	A.B.C.200	50000	1.2.3.4	443
10.x.x.100	65001	9.8.7.6	443	A.B.C.10	54000	9.8.7.6	443

NAT tableに
matchしない
→ 不正としてReject

こんなパターンも は許されない

⑥ User Angry

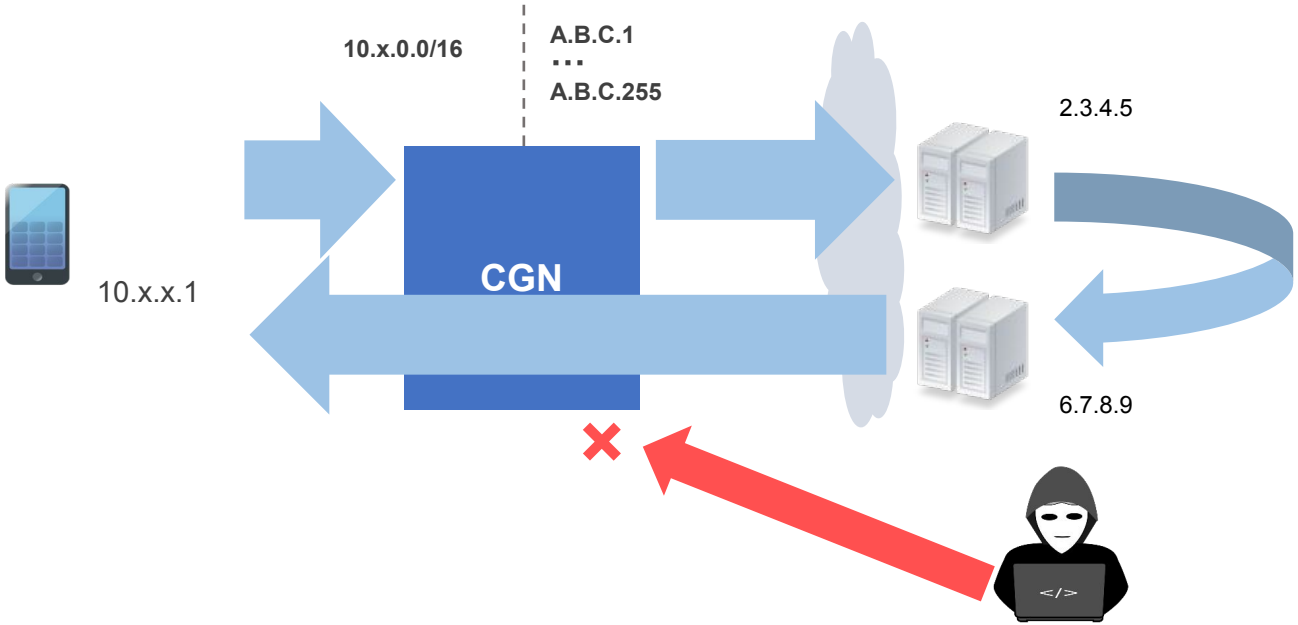
10.x.x.1



Src IP	Src Port	Dst IP	Dst Port	Translated Src IP	Tranlated Src Port	Dst IP	Dst Port
10.x.x.1	65001	5.6.7.8	80	A.B.C.1	50000	5.6.7.8	80
10.x.x.1	65002	2.3.4.5	30000	A.B.C.1	23000	2.3.4.5	30000
10.x.x.2	65001	1.2.3.4	443	A.B.C.200	50000	1.2.3.4	443
10.x.x.100	65001	9.8.7.6	443	A.B.C.10	54000	9.8.7.6	443

④NAT tableに
matchしない
→ 不正としてReject

目指すところ。。。



不特定の悪意ある通信から利用者を保護しつつ、
不特定のバックエンド連携やP2Pは通してあげる　そんな難易度HELLの世界
☞キャリアにおいては「防ぎすぎることも害悪」になる

CGN/FW for 5GC Fabric

1 CGN/FWとは？

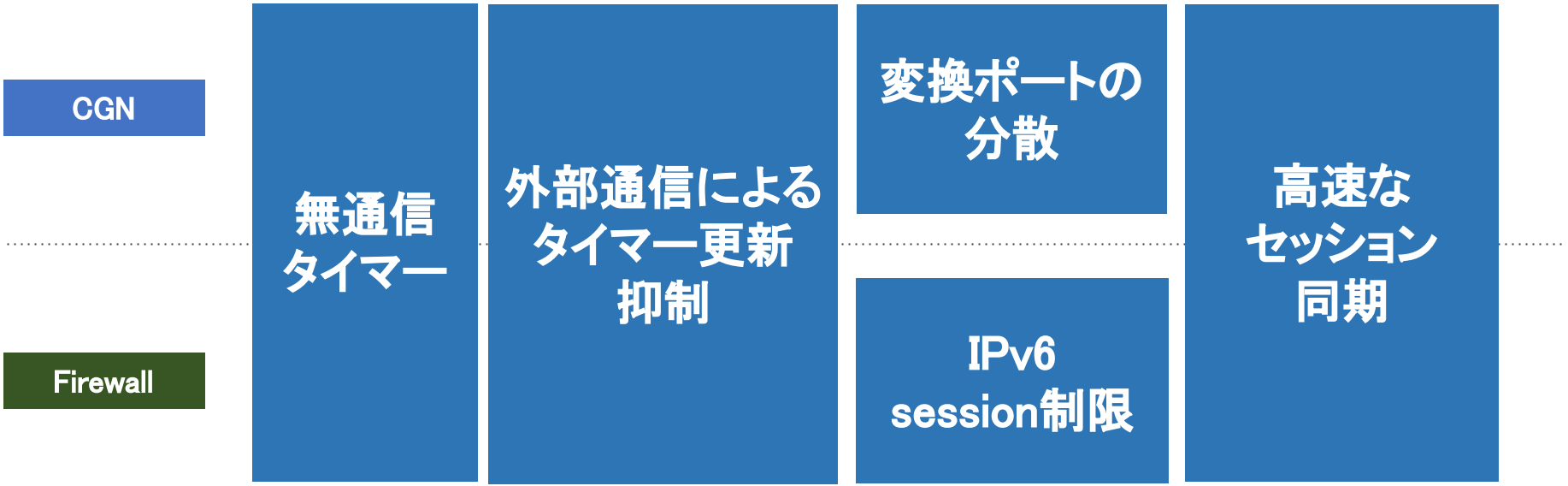
2 我々に求められる在り方

3 **快適な環境を追い求めて**

4 将来のCGN/FWを考えて

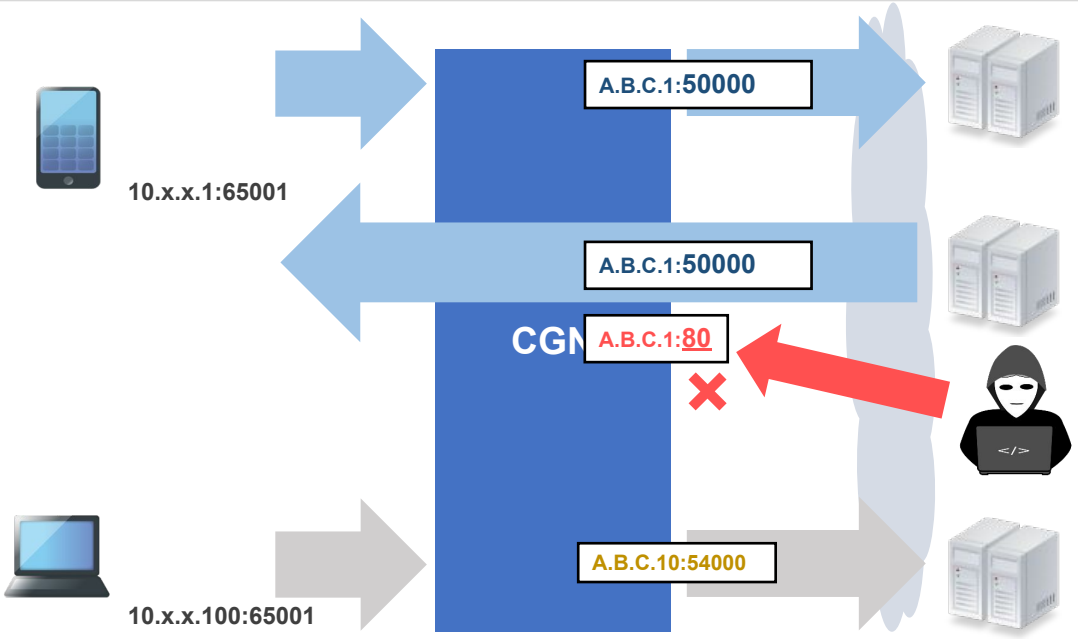
快適な通信を追い求めて

Fullcone通信の採用、関連機能を徹底的にチューン



FullConeの実装

CGN



Src IP	Src Port	Dst IP	Dst Port	Translated Src IP	Tranlated Src Port	Dst IP	Dst Port
10.x.x.1	65001	5.6.7.8	80	A.B.C.1	50000	5.6.7.8	80
10.x.x.1	65002	2.3.4.5	30000	A.B.C.1	23000	2.3.4.5	30000
10.x.x.2	65001	1.2.3.4	443	A.B.C.200	50000	1.2.3.4	443
10.x.x.100	65001	9.8.7.6	443	A.B.C.10	54000	9.8.7.6	443

Points

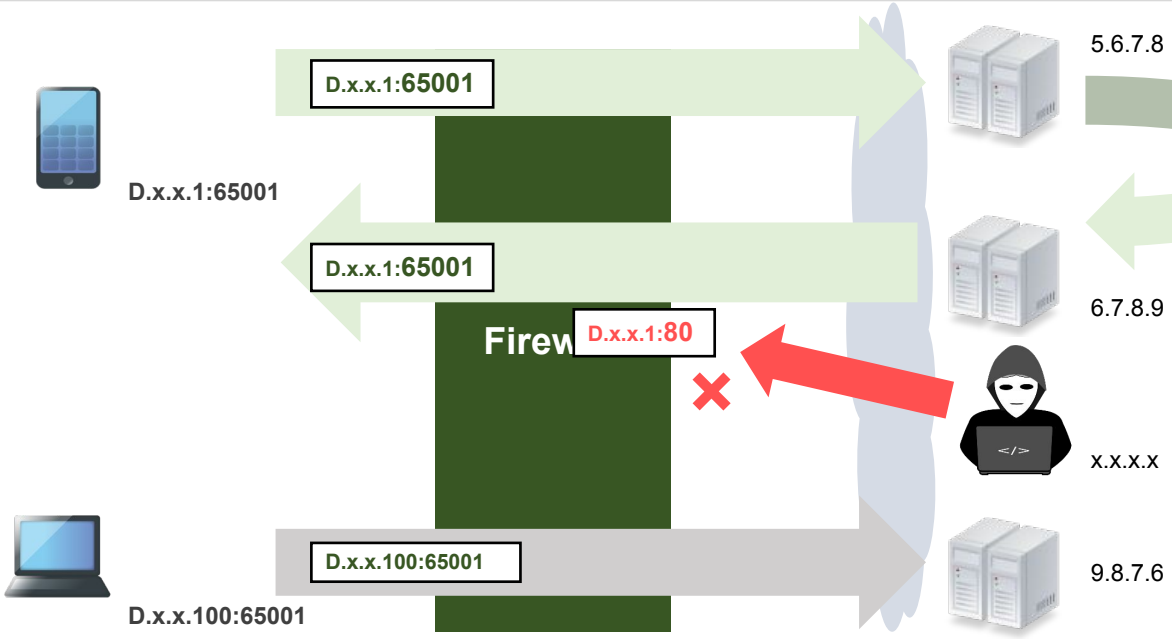
Fullconeと呼ばれる機能を実装

☞同一Src IPは
同一Global IPに変換（EIM）

☞通信済みのIP/Portに対して
他のIPのアクセス許可（EIF）

FullConeの実装

Firewall



Src IP	Src Port	Dst IP	Dst Port
D.x.x.1	65001	5.6.7.8	80
D.x.x.1	65002	2.3.4.5	30000
D.x.x.2	65001	1.2.3.4	443
D.x.x.100	65001	9.8.7.6	443

Points

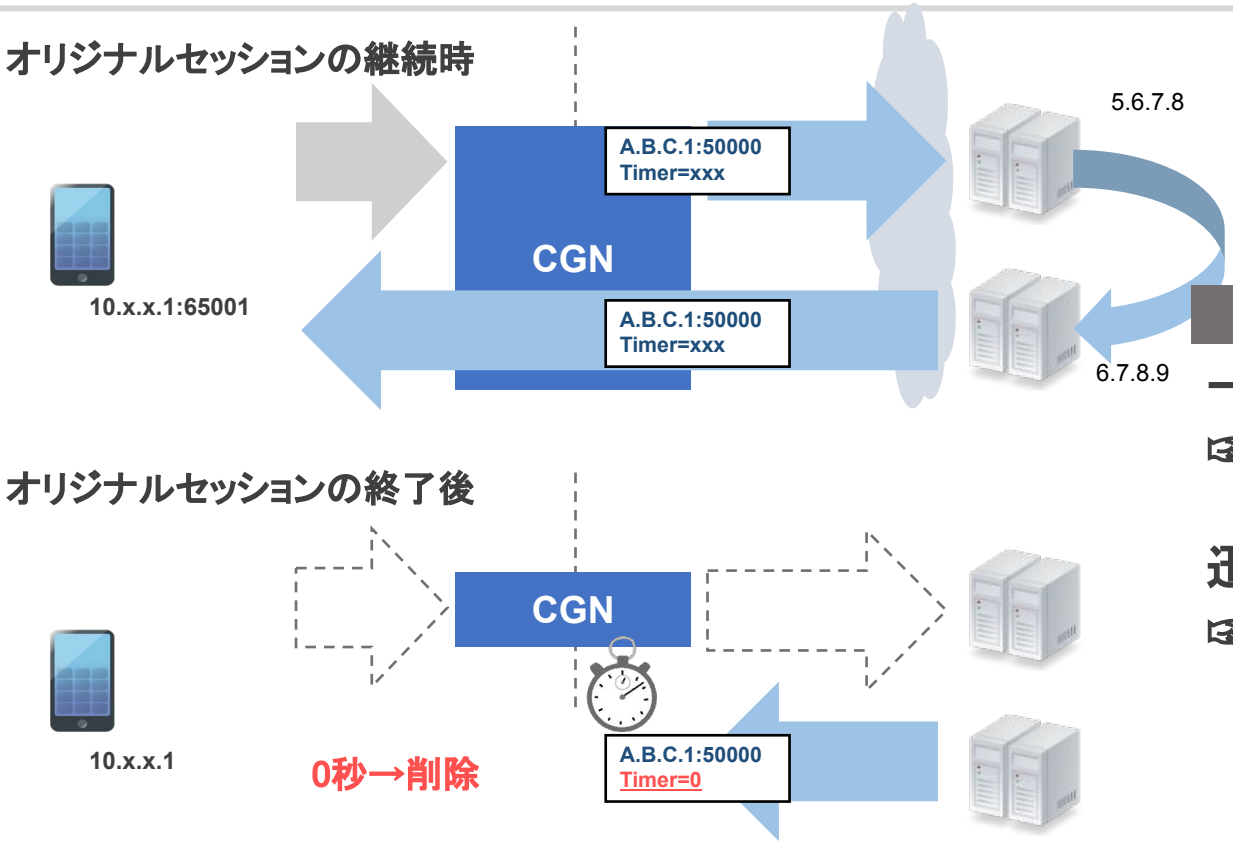
Fullconeの世界観をFWに導入

☞通信済みのIP/Portは
他のIPからのアクセスも許可

→通信劣化を防止

無通信タイマーの実装

CGN　Firewall



Points

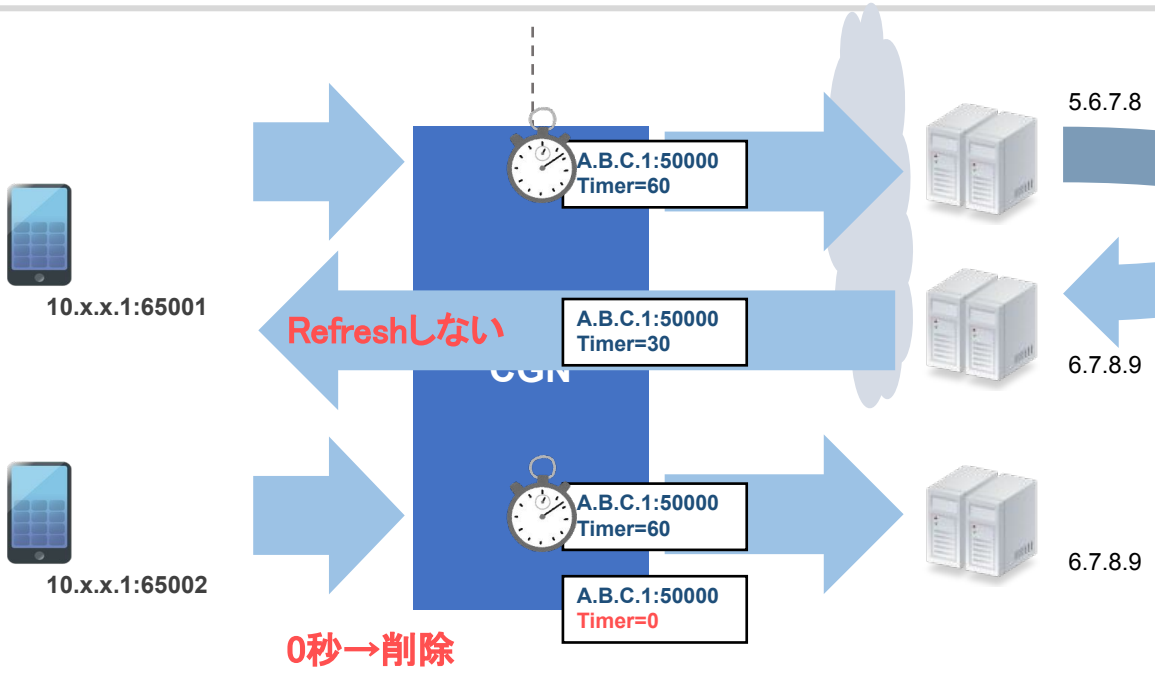
一定時間経過後Fullcone解除
☞安全性の確保

迅速に切れば良い？：NO
☞Retry, Timeout, latency

アプリケーション単位
の検討が必要
（QUICを見据えた見直し時期?）

外部通信によるタイマー更新抑制

CGN　Firewall



Points

Full cone＝不特定多数の受付

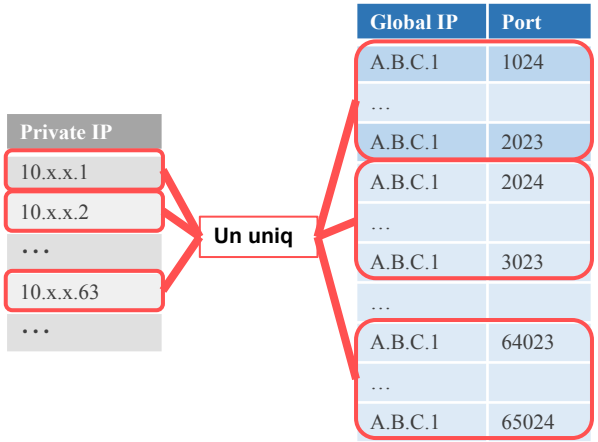
☞Sessionが**無限に増え得る**

外部通信で
タイマーが更新されない
仕組みが必要

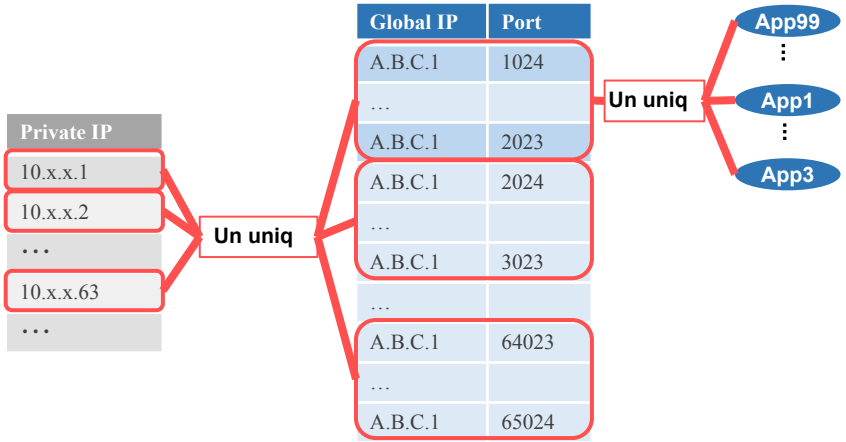
変換Portの分散

CGN

Address単位で重複回避



Blockごとに重複回避

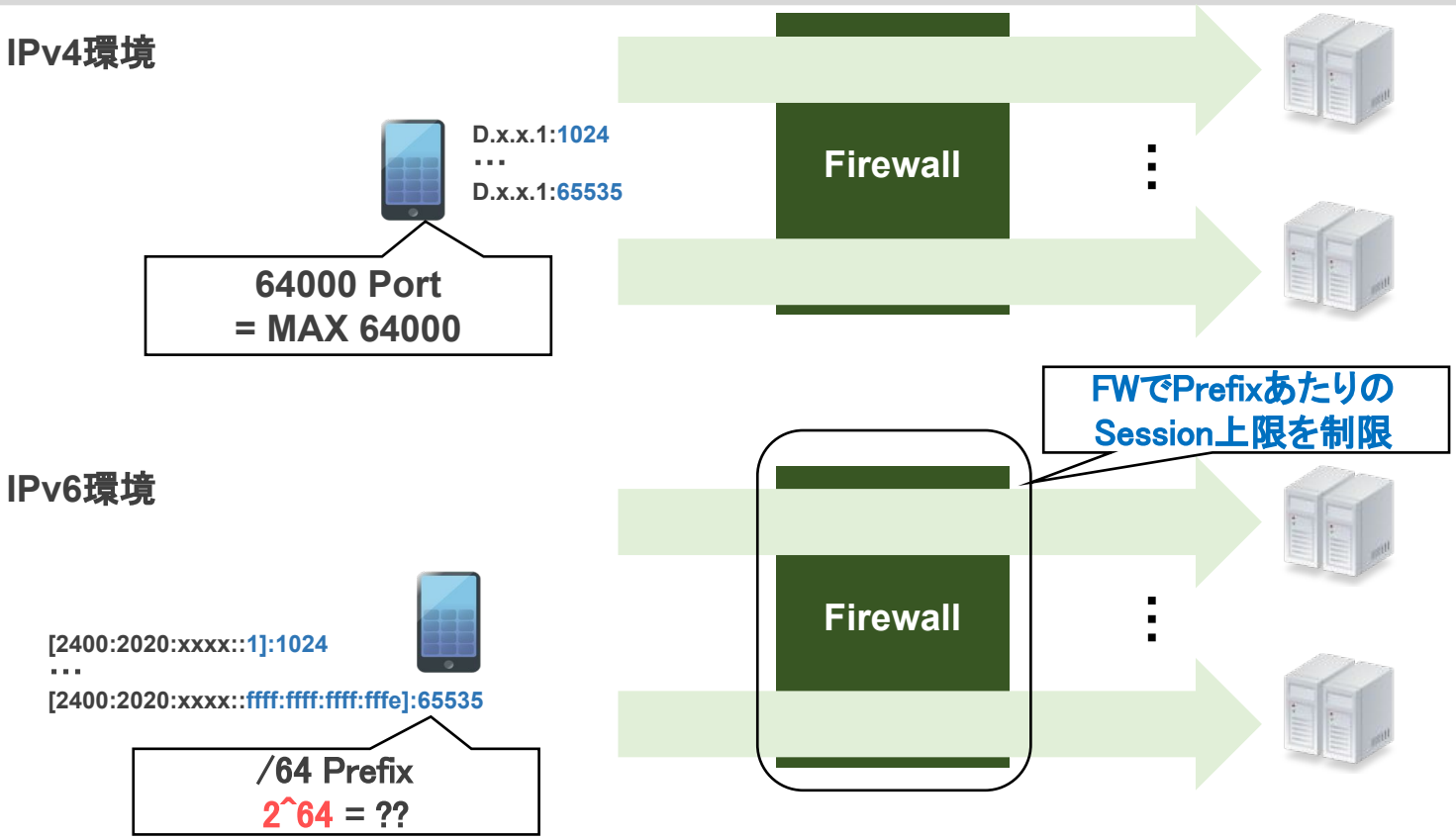


等々・・・

利用Portの偏りを減らす → 利用率向上、類推困難に

IPv6セッション数の制限

Firewall

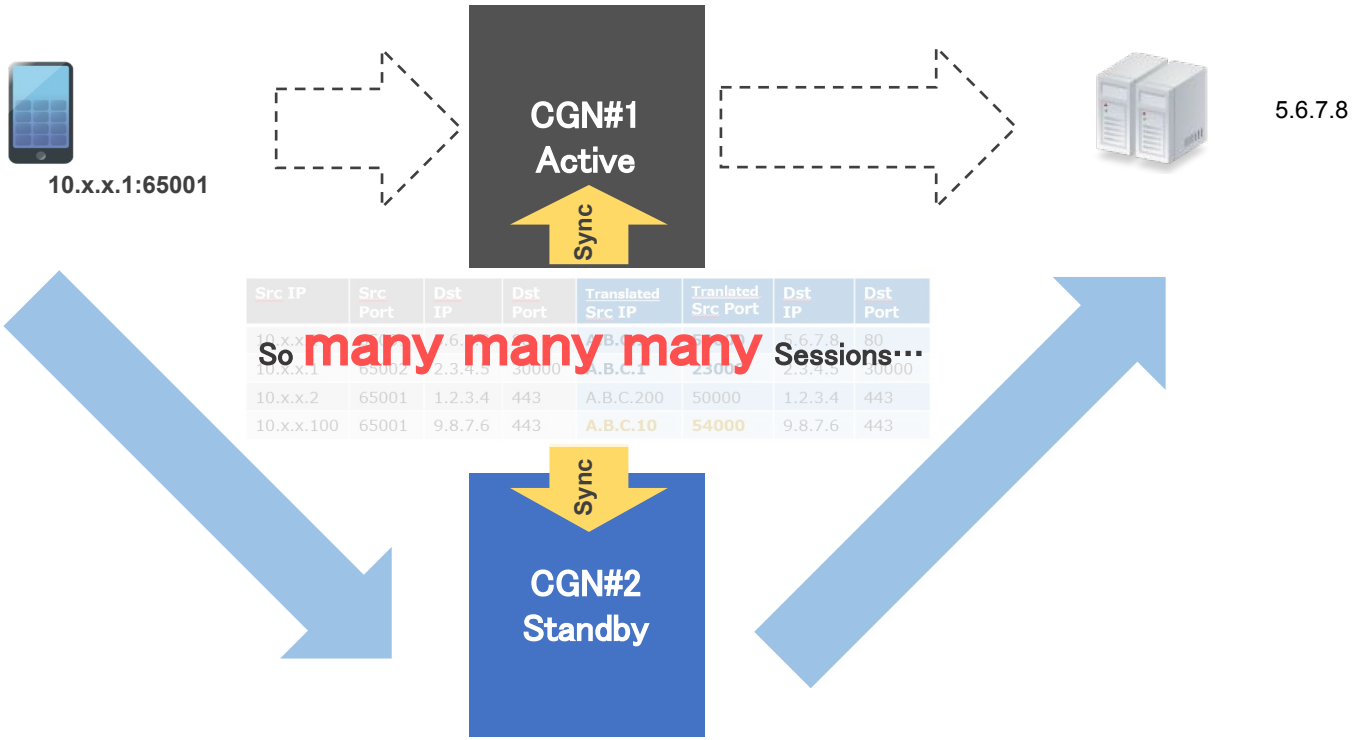


IPv6の場合セッション数増大を防ぐ必要がある

セッション情報の高速同期

CGN

Firewall



Src IP	Src Port	Dst IP	Dst Port	Translated Src IP	Tranlated Src Port	Dst IP	Dst Port
10.x.x.2	65001	1.2.3.4	443	A.B.C.200	50000	1.2.3.4	443
10.x.x.100	65001	9.8.7.6	443	A.B.C.10	54000	9.8.7.6	443

高速なセッション同期をすることでfailover時の影響を抑制

CGN/FW for 5GC Fabric

1 CGN/FWとは？

2 我々に求められる在り方

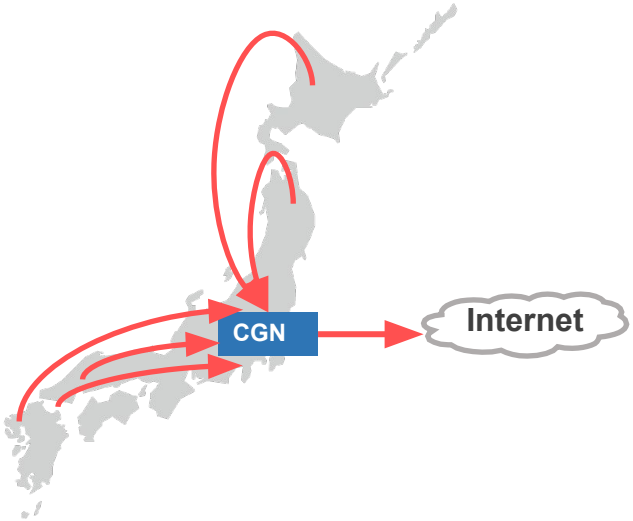
3 快適な環境を追い求めて

4 **将来のCGN/FWを考えて**

将来のCGN/FWを考えて

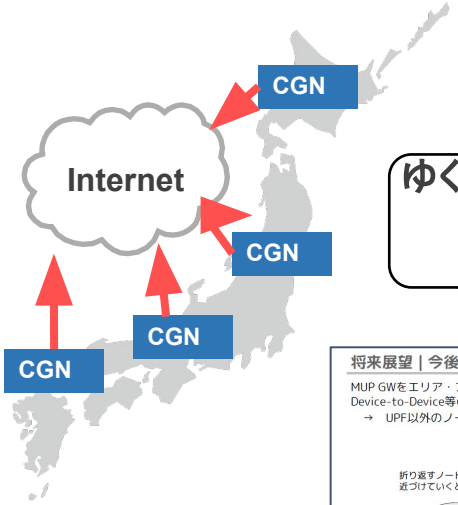
AS-IS

特定のセンターに一括集中
→ Overheadの存在

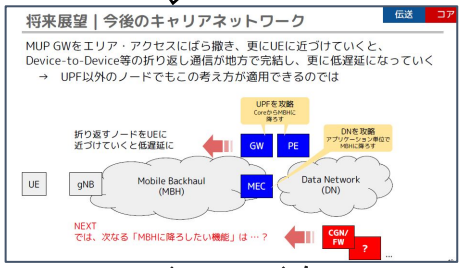


TO-BE

地方センターへの分散配置
→ トラフィックの地産地消化
（Overhead減・耐障害性向上）



ゆくゆくはMUPやMECとの連携も視野に・・・？

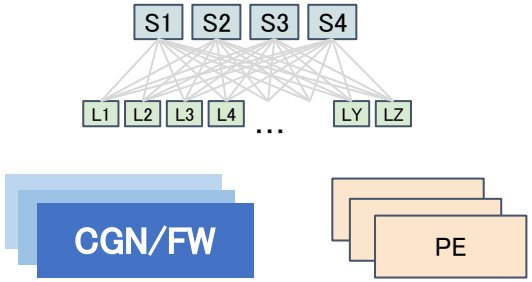


Day2
SRv6 Mobile User Plane (SRv6 MUP) を
商用 NW に入れてみた

将来のCGN/FWを考えて

AS-IS

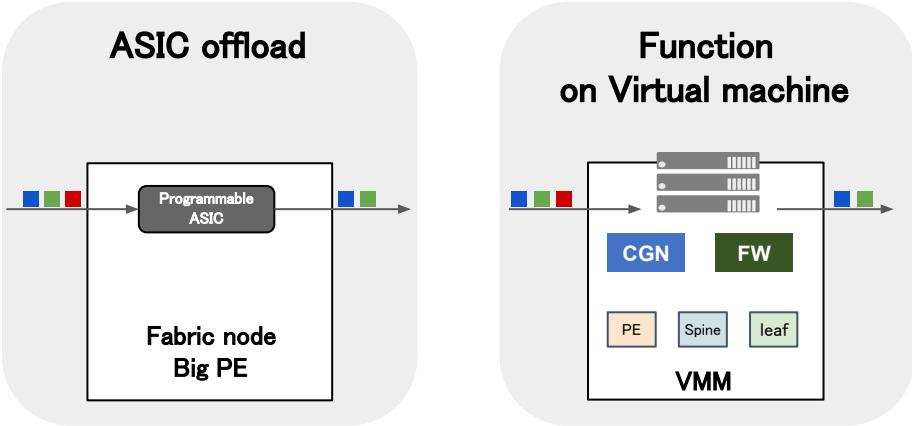
Fabricとは別に専用HWを用意



運用コストの増大、Topology制約

TO-BE

展開性の高いNetwork Function



運用コスト低減、CGNの可搬性向上

CGN/FW for 5GC Fabric

1 CGN/FWとは？

2 我々に求められる在り方

3 快適な環境を追い求めて

4 将来のCGN/FWを考えて

～全体を通して～皆様と議論したいこと

～全体を通して～皆様と議論したいこと

キャリアバックボーンとClos Fabric

- 6G時代はどんなネットワークになるんだろう？
- Fabric Leaf/ToR/PPの、ぼくがかんがえた最強の物理配置はどんなのがある？
- 日本全体をみたEast-West通信のBreakoutに関する課題感共有認知大会

Clos Fabric

- Fabricの作り方をどうしていますか？課題はありますか？
- DC/リージョン内のサイジングや冗長の考え方はありますか？
- PBR等特殊な制御は行ってますか？

CGN/Firewall

- Fullcone使っていますか？見合ったbenefitは得られていますか？
- 高速failover/session同期は大事（メーカー様いつもありがとうございます）
- NF/Edge化する未来の現実性（他に良い手法はある？）

SoftBank

ご清聴ありがとうございました