【SPring-8データ・ネットワークポータル掲載版】
（ビームラインネットワークの詳細設定に関するページは割愛しています。）

SPring-8イントラネット「ビームラインネットワーク」説明資料集（2024年6月版）

data-net（SPring-8データ・ネットワーク運用担当）

特定の内容のページに移動するためのリンク

基本構成・特徴など → 9ページ目「用語の整理（『ゾーン』構成など）と基本情報（IPアドレスの割り振りなど）」

基本の通信設定など → 27ページ目「基本設定（ビームライン内外・ゾーン間の通信可否）」

利用事例 → 37ページ目「典型的な利用シーンにおいて推奨される接続・使い方について」

移行にあたって行うこと → 57ページ目「現行のネットワークからの切り替えに際するインストラクションに関わる内容について（ビームライン担当者向け）」

特に注意が必要なこと→66ページ目「『ビームラインネットワーク』を安全に使うための運用ルールの作成に向けて」

注意！本資料は「ビームラインネットワーク」の現時点での情報をまとめた資料です。そのため、「ビームラインネットワーク」に関して現段階で未完成の内容も扱っています。
実際に利用する際には最新の情報にご留意願います。（資料中🚧マークを付記）

はじめに

この資料について

対象範囲

- この資料ではSPring-8のイントラネットにおける**「ビームラインネットワーク」**について説明します（用語は改めて後述します）。

目的

- 「ビームラインネットワーク」について**多くのビームラインで共通する一般的な事項**をビームラインの関係者と広く共有し、今後のビームラインへの導入と利用の際に役立てることです。

対象者

- ビームライン（FE、光学機器、**実験**、...）を担当する関係者

これまでの経緯

- SPring-8では2021年度以降、これまでのネットワーク（「BL-USER-LAN」などを含む）に代わる新しい**「ビームラインネットワーク」**の導入がビームライン単位で段階的に進んでいます。
- 具体的には、**「ビームラインネットワーク」**を**「BL-774」**（ビームライン制御・データ収集・オンライン解析プラットフォーム、基幹的なソフトウェアシステムは「774BasicSystem」）※と併せて導入したビームラインには次のものがあります。（※この資料では「BL-774」の詳細は割愛します。）

2021年度	BL09XU
2022年度	BL13XU
2023年度	BL46XU、BL07LSU、BL39XU、BL10XU
2024年度	数ビームラインで計画中（BL15XU、BL16XU、BL28B2ほか）

その後、2028年度夏までに完了を予定しています。
現状の「BL-USER-LAN」は「ビームラインネットワーク」へ移行後に順次廃止予定となっています。

- その他、**データ転送**の用途に、「BL-774」の導入に先行して「ビームラインネットワーク」のみを利用しているビームラインも現時点では存在します。

これまでの経緯

- 所内向けの情報公開
  - 杉本崇, 第2回SPring-8データワークショップ,「ネットワーク高度化計画」, (2021年2月24日)。
    - この後に新たに定義した名称があります。
    - 原則的な考え方は変更ありません。

この資料の構成

基本構成

1. 「ビームラインネットワーク」の**一般事項**について
    a. **用語の整理（「ゾーン」構成など）**と**基本情報（IPアドレスの割り振りなど）**
    b. **基本設定（ビームライン内外・ゾーン間の通信可否）**
2. **典型的な利用シーン**において推奨される接続・使い方について
3. **現行のネットワークからの切り替え**に際するインストラクションに関わる内容について（実験を担当する関係者向け）
4. **安全に使うための運用ルール**の作成に関すること

主要なポイント

- 「ビームラインネットワーク」の設計の背景、ねらい、理由について。これまでのネットワークと何が、どう変わるかについて。
- ビームライン間、ビームライン内外、施設内外の通信可否についての原則的な考え方。
- 利用場所の区分と「ゾーン」の区分の対応。やりたいことと使うべき「ゾーン」の対応。

詳細な情報

- 関心がある箇所によって理解したほうが良い内容が異なることもあるため、説明会時には詳細な情報は紹介程度にとどめます。後程、この資料の公開版をご参照ください。

1. 「ビームラインネットワーク」の一般事項について

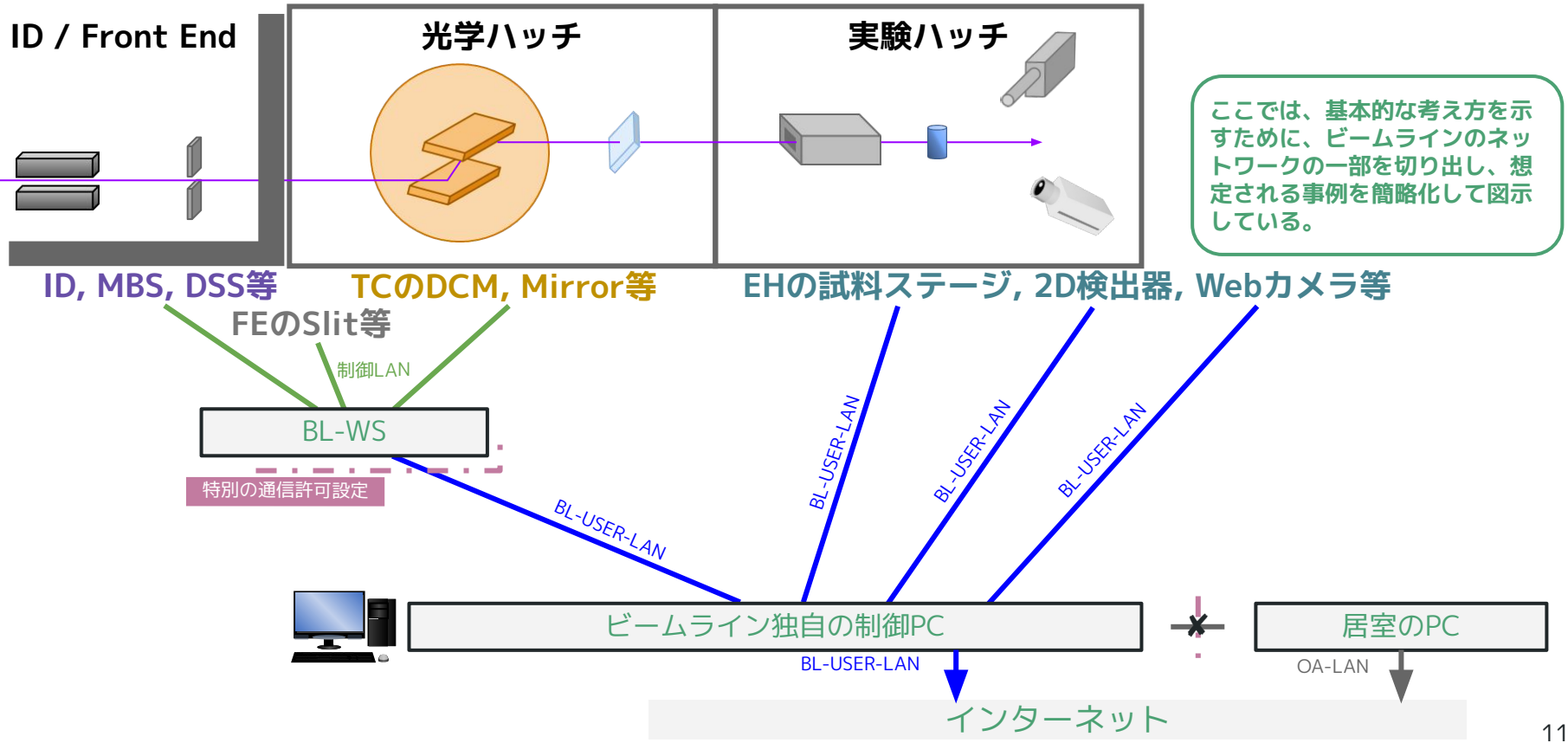
1a. 用語の整理（「ゾーン」の構成など）と基本情報（IPアドレスの割り振りなど）

構内ネットワークにおける「ビームラインネットワーク」の整備

- 目的
  - 用途、使用権限があいまいな現状のOA-LANとBL-USER-LANを発展的に統合・再編する。
  - SPring-8-IIに向けて利用実験に耐えうる性能と拡張性の向上を図る。
- 特徴
  - 用途ごとのゾーン分け
    3つの新しいゾーン**「BL-Core Zone」「User Zone」「Analysis Zone」**で**「ビームラインネットワーク」**を構成
  - 帯域：当初は10Gbpsでスタート
    トラフィック増加傾向を見てアップグレード予定

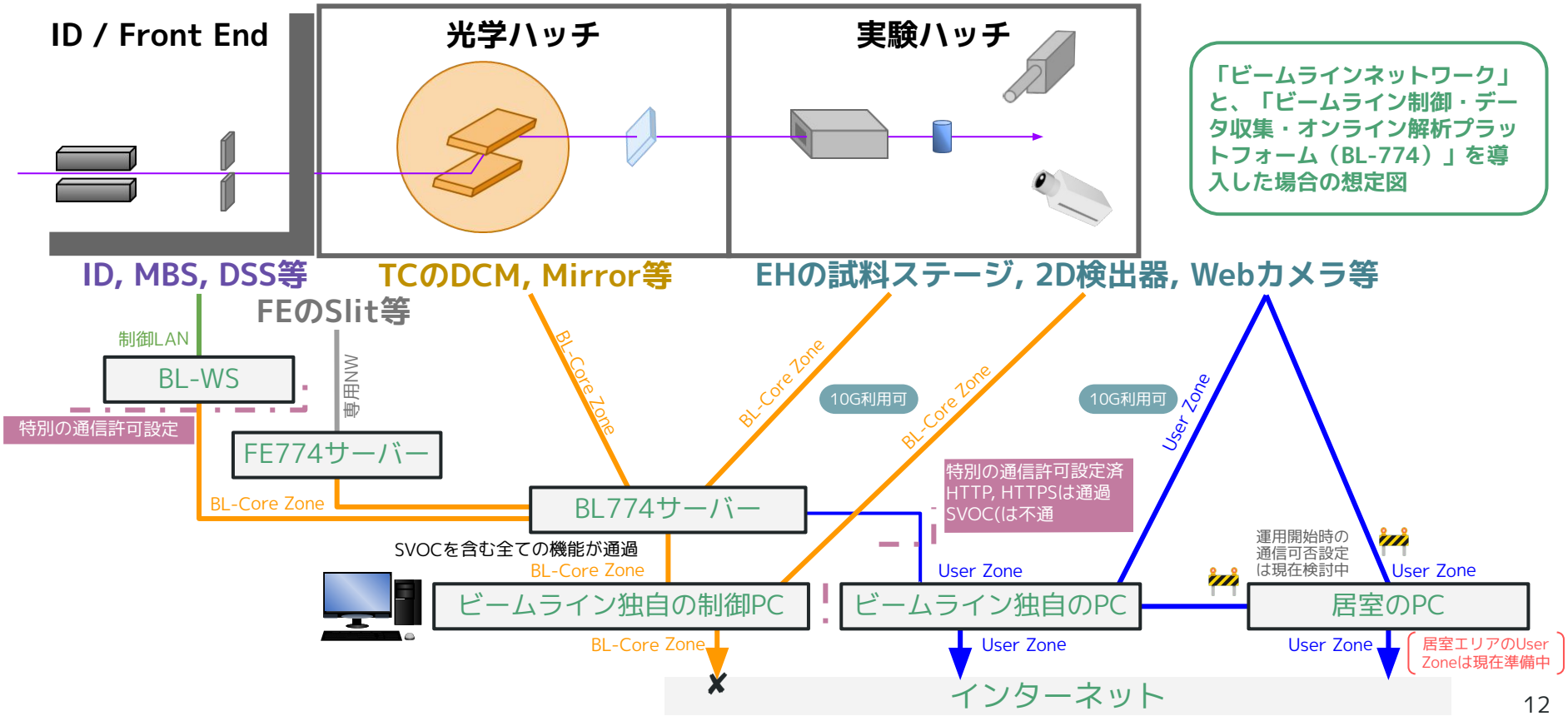
ビームラインで扱う機器と利用するネットワーク移行の典型例（１/２）

これまでのネットワーク接続の概略図



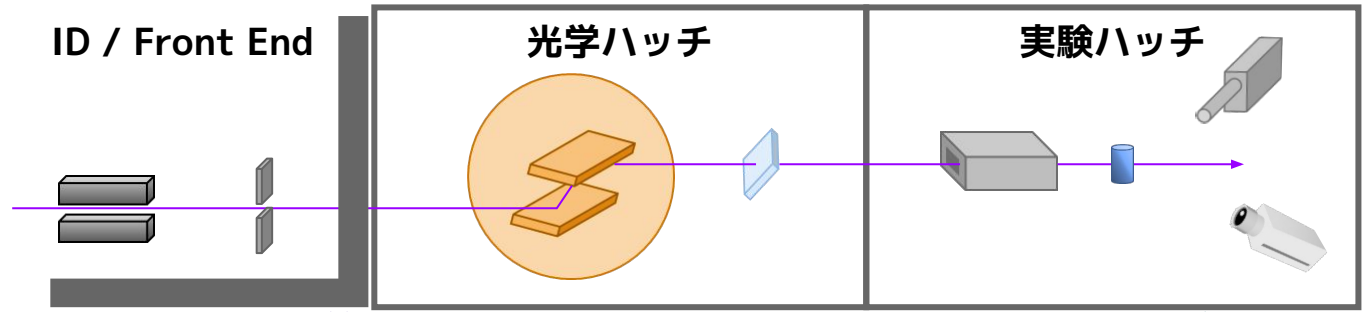
ビームラインで扱う機器と利用するネットワーク移行の典型例（２/２）

これからのネットワーク接続の概略図



ビームラインで扱う機器と利用するネットワーク移行の典型例（２/２）

これからのネットワーク接続の概略図

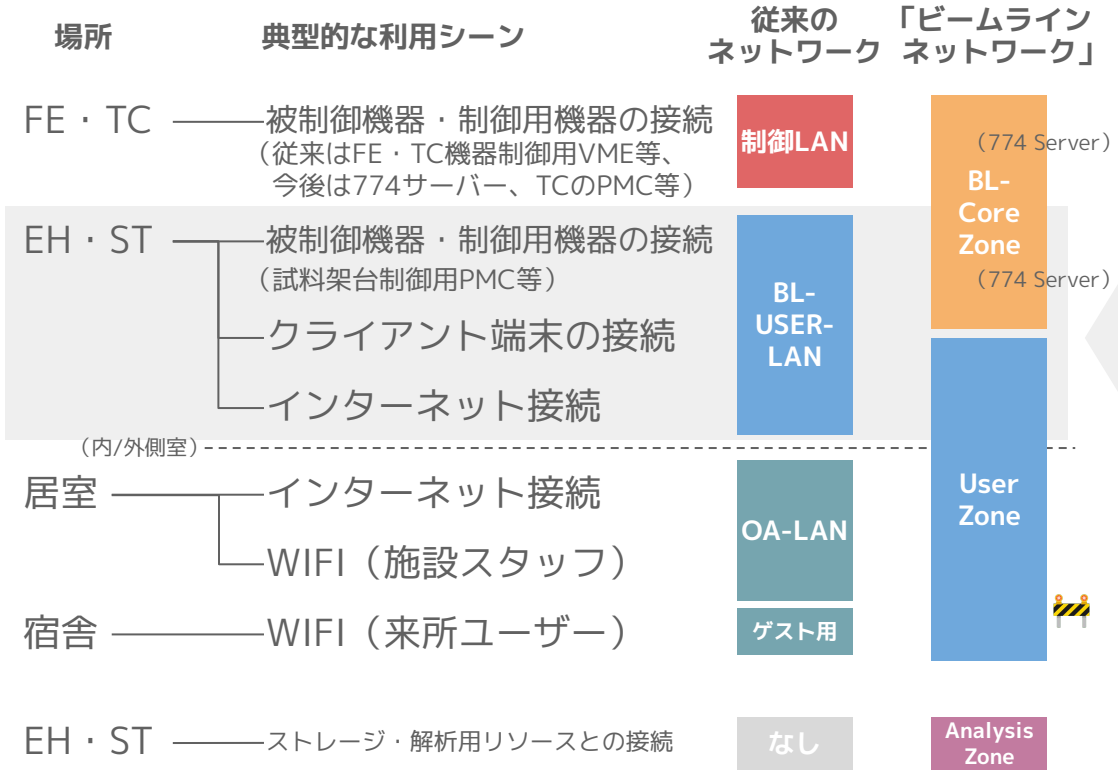


「ビームラインネットワーク」と、「ビームライン制御・データ収集・オンライン解析プラットフォーム（BL-774）」を導入した場合の想定図

ID, MBS, DSS等
TCのDCM, Mirror等
EHの試料ステージ, 2D検出器, Webカメラ等
FEのSlit等
制御LAN
BL-WS
専用NW
特別の通信許可設定
FE774サーバー
BL-Core Zone
BL774サーバー
BL-Core Zone
BL-Core Zone
BL-Core Zone
10G利用可
10G利用可
User Zone
特別の通信許可設定済
HTTP, HTTPSは通過
SVOC(は不通
運用開始時の通信可否設定は現在検討中
User Zone
User Zone
SVOCを含む全ての機能が通過
BL-Core Zone
ビームライン独自のPC
ビームライン独自の制御PC
ビームライン独自のPC
居室のPC
10G利用可
Analysis Zone
BL-Core Zone
User Zone
User Zone
居室エリアのUser Zoneは現在準備中
ストレージ・解析用リソース
インターネット

「ビームラインネットワーク」を構成するゾーンの名称（1 / 4）

SPring-8での用途別の事例でみた新旧のイントラネットの対応関係を示します。「ビームラインネットワーク」では用途に応じて3つの新しいゾーン「BL-Core Zone」「User Zone」「Analysis Zone」が設定されています。



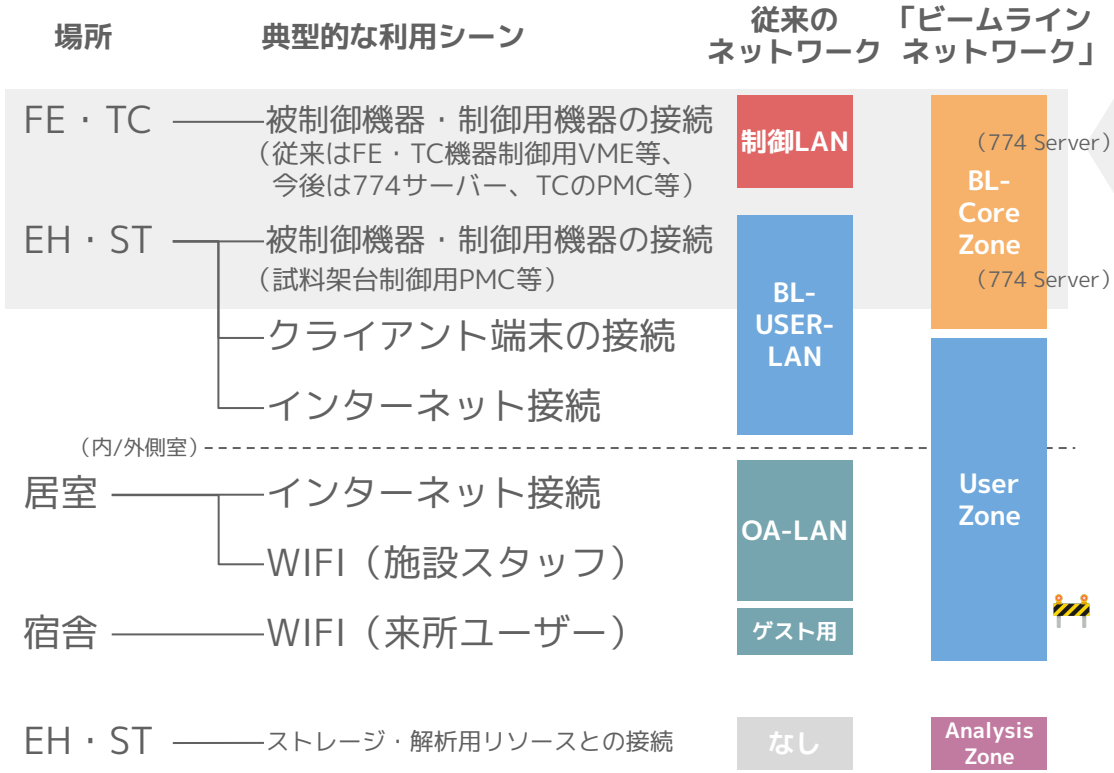
用途別の事例でみた新旧イントラネットの対応関係

- これまでビームラインのEH・STでは「BL-USER-LAN」が用いられてきました。「BL-USER-LAN」は使用目的に応じて「BL-Core Zone」と「User Zone」の2つに分割されました。

- 「BL-Core Zone」は「BL-USER-LAN」に比べてビームラインごとの独立性が高まり、EH・STの制御対象機器だけではなく、従来は「制御LAN」に接続していたFE・TCの制御対象機器※の接続にも使用します。（※この資料では「BL-774」の詳細は割愛します。「BL-774」ではFEの機器の接続には左記以外のローカルネットワークも使用されます。）

「ビームラインネットワーク」を構成するゾーンの名称（2/4）

SPring-8での用途別の事例でみた新旧のイントラネットの対応関係を示します。「ビームラインネットワーク」では用途に応じて3つの新しいゾーン「BL-Core Zone」「User Zone」「Analysis Zone」が設定されています。



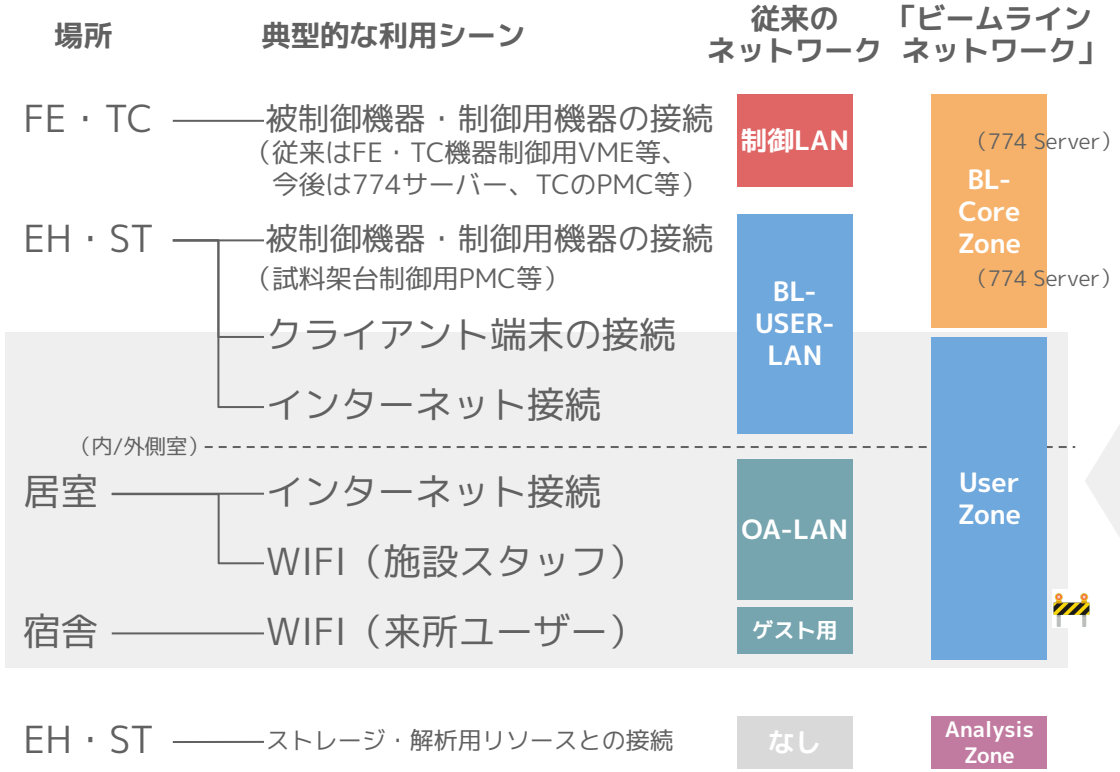
用途別の事例でみた新旧イントラネットの対応関係

- ビームライン（FE・TC・EH・ST）の主要な制御対象機器は「BL-Core Zone」に設置します。これらの機器の制御を担う「BL-774」※の774サーバーも「BL-Core Zone」に設置します。（※この資料では「BL-774」の詳細は割愛します。）

- これまで、FE・TCの機器の制御はBL-WSが担っていて、「BL-USER-LAN」からコマンドを投入するには、**申請**を基づきネットワークをまたぐための通信設定を要していました。
しかし、「BL-Core Zone」内で完結する774制御系では、ビームラインからのコマンド実行にあたり、このような通信設定は要しません。

「ビームラインネットワーク」を構成するゾーンの名称（3 / 4）

SPring-8での用途別の事例でみた新旧のイントラネットの対応関係を示します。「ビームラインネットワーク」では用途に応じて3つの新しいゾーン「BL-Core Zone」「User Zone」「Analysis Zone」が設定されています。



用途別の事例でみた新旧イントラネットの対応関係

- 「User Zone」には操作用のクライアント端末等を設置します。

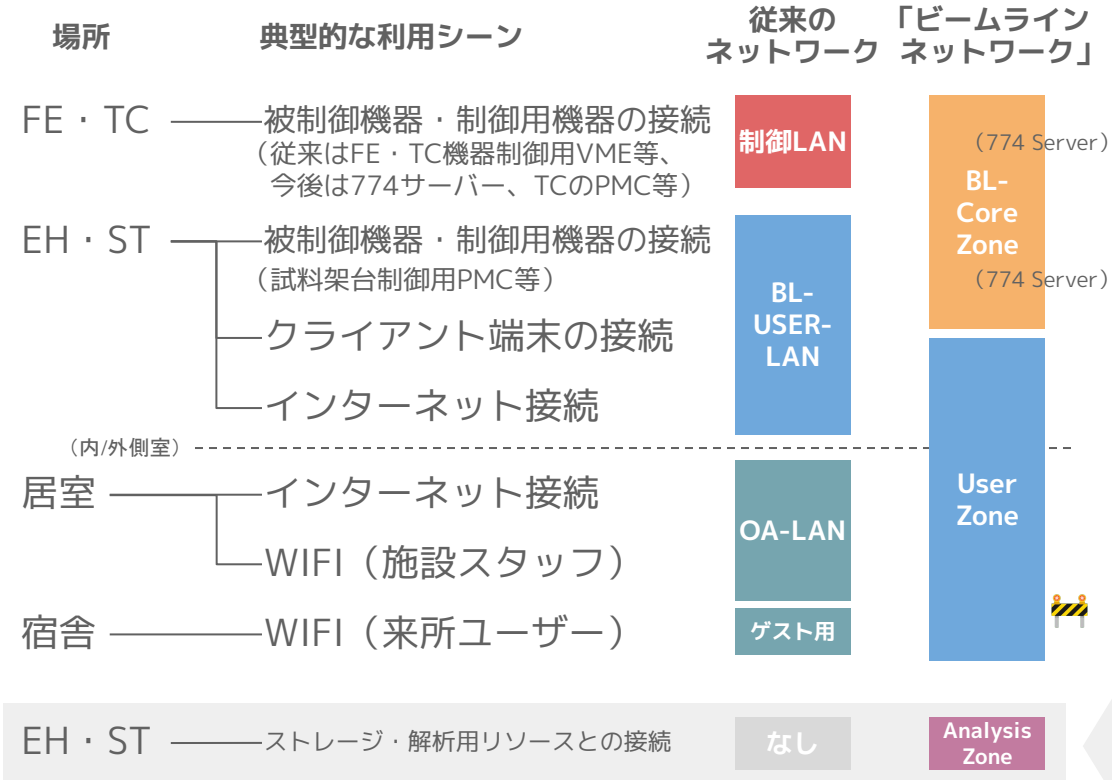
- 「User Zone」はビームラインだけでなくリング棟外の宿舎を含む建屋のエリアにまで展開されます。
- 「User Zone」は、居室等において従来は「OA-LAN」が担ってきた役割も担う（例外はある）ことになります。WIFIによる接続でも来所ユーザーを含めて「User Zone」を利用することになります。

- 「User Zone」については現段階で未定の部分もあるため、今後の周知をご参照ください。

（User Zoneに機器をネットワーク接続するには認証が必要になる予定です。）

「ビームラインネットワーク」を構成するゾーンの名称（4/4）

SPring-8での用途別の事例でみた新旧のイントラネットの対応関係を示します。「ビームラインネットワーク」では用途に応じて3つの新しいゾーン「BL-Core Zone」「User Zone」「Analysis Zone」が設定されています。



用途別の事例でみた新旧イントラネットの対応関係

- 「Analysis Zone」はビームラインからストレージや解析用のリソースへの接続の用途に利用されます。
  （※SPring-8データセンターへはBL-Core ZoneとUser Zoneからの接続も可能です。）
- 現時点では「Analysis Zone」の利用は少数のビームラインであるため、**この資料では深堀しません**。
  「Analysis Zone」については、必要に応じて、他の資料をご参照ください。

- なお、各ゾーンの使い分けについては、ネットワークセキュリティに対する考慮が必要であり、詳細な説明は必要に応じてこの資料の各論をご参照ください。

SPring-8における各ゾーンの配置を示す模式図

Analysis Zone
User Zone
BL-Core Zone

BL◎◎ の Analysis Zone
BL◎◎ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL◎◎ の BL-Core Zone（実験ホール内からのみ接続可能）

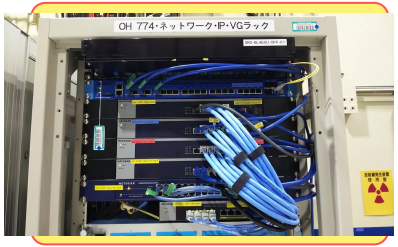
特定のビームラインに属するネットワーク構成単位

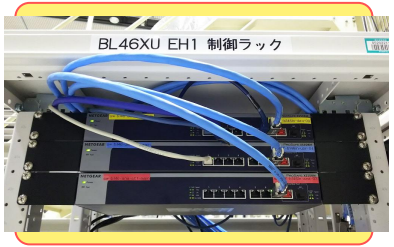
BL※※ の Analysis Zone
BL※※ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL※※ の BL-Core Zone（実験ホール内からのみ接続可能）

「Analysis Zone」についての説明はこの資料では割愛する。

特定のビームラインに属さない領域

Common の Analysis Zone
Common の User Zone
Common の BL-Core Zone





ネットワーク
基幹装置

データセンターのネットワーク

SPring-8データセンター

Wi-Fi

建屋・フロア・居室、
WIFI

SPring-8における各ゾーンの配置を示す模式図

User ZoneとBL-Core Zoneのみを取り出した図

User Zone
BL-Core Zone

BL◎◎ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL◎◎ の BL-Core Zone（実験ホール内からのみ接続可能）

特定のビームラインに属するネットワーク構成単位

BL※※ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL※※ の BL-Core Zone（実験ホール内からのみ接続可能）

特定のビームラインに属さない領域

Common の User Zone
Common の BL-Core Zone

「BL-Core Zone」、「User Zone」(、「Analysis Zone」)には、複数のビームラインで共通して利用するサービス（DNS、NTP、Proxy、…）を配置するために、「common」と呼ばれる領域が設定されている。
ビームライン担当者や実験ユーザーがビームラインネットワークを利用するにあたって、「common」を意識する機会は少ないと予想されるため、この資料での詳細な説明は割愛する。

建屋・フロア・居室、WIFI

1b. 基本設定（ビームライン内外・ゾーン間の通信可否）

SPring-8における各ゾーンの配置を示す模式図

Analysis Zone
User Zone
BL-Core Zone

BL◎◎ の Analysis Zone
BL◎◎ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL◎◎ の BL-Core Zone（実験ホール内からのみ接続可能）

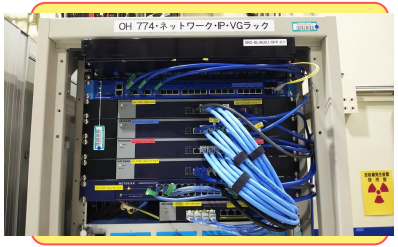
特定のビームラインに属するネットワーク構成単位

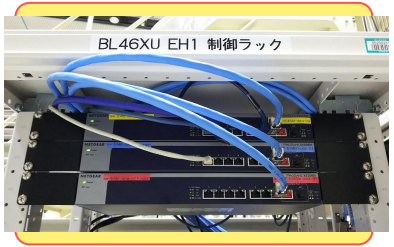
BL※※ の Analysis Zone
BL※※ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）
BL※※ の BL-Core Zone（実験ホール内からのみ接続可能）

「Analysis Zone」についての説明はこの資料では割愛する。

特定のビームラインに属さない領域

Common の Analysis Zone
Common の User Zone
Common の BL-Core Zone





ネットワーク
基幹装置

SPring-8データセンター

Wi-Fi

建屋・フロア・居室、
WIFI

SPring-8における各ゾーンの配置を示す模式図

User ZoneとBL-Core Zoneのみを取り出した図

BL◎◎ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）

BL◎◎ の BL-Core Zone（実験ホール内からのみ接続可能）

特定のビームラインに属するネットワーク構成単位

BL※※ の User Zone（内・外側室にも同じIP範囲の情報コンセントあり）

BL※※ の BL-Core Zone（実験ホール内からのみ接続可能）

特定のビームラインに属さない領域

Common の User Zone

Common の BL-Core Zone

ここでは、Commonの領域を除くUser ZoneとBL-Core Zoneを取り出して、ネットワークレベルの通信可否を見ていきます。

建屋・フロア・居室、WIFI

ゾーン内・ゾーン間のネットワークレベルの通信可否のまとめ

User ZoneとBL-Core Zoneの間の通信可否(Commonの領域を除く)

				送信先							
				User Zone				BL-Core Zone			
				BL※※のUser Zoneに割り当てられたIP		その他のBLのUser Zoneに割り当てられたIP	左以外のUser Zoneに割り当てられたIP	BL※※のBL-Core Zoneに割り当てられたIP		それ以外のBLのBL-Core Zoneに割り当てられたIP	
				全IP	IP=xxx.yyy.zzz.1-8 (zzzは前半2つ) の場合の追加設定	全IP	全IP	全IP	IP=xxx.yyy.zzz.1-8 の場合の追加設定	全IP	IP=xxx.yyy.zzz.1-8 の場合の追加設定
送信元	User Zone	BL※※のUser Zoneに割り当てられたIP	全IP	✓全ての通信		✓全ての通信	✓全ての通信	✗全ての通信	✓HTTP(S) ✓SMB	✗全ての通信	—
		上以外のUser Zoneに割り当てられたIP	全IP	✓全ての通信		✓全ての通信	✓全ての通信	✗全ての通信	—	✗全ての通信	—
	BL-Core Zone	BL※※のBL-Core Zoneに割り当てられたIP	全IP	✗全ての通信	✓HTTP(S) ✓SMB ✓RDP	✗全ての通信	✗全ての通信	✓全ての通信		✗全ての通信	—

この行は後の頁の図(1/3)
この行は後の頁の図(3/3)
この行は後の頁の図(2/3)
この列は後の頁の図(1/3)'
この列は後の頁の図(2/3)'

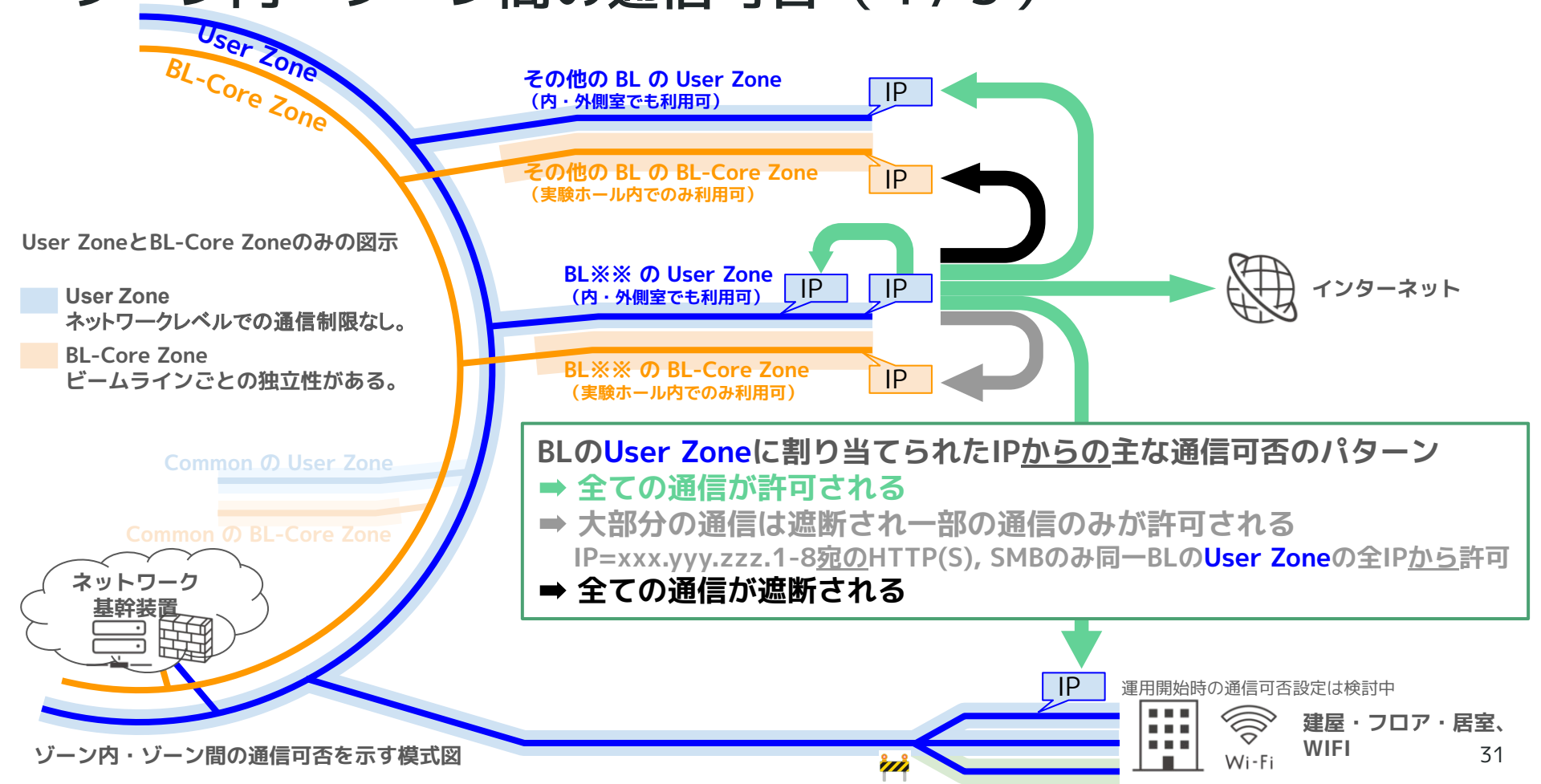
FW設定による許可

考慮する必要のないセル

(上の表ではネットワーク運用上の通信については除く)

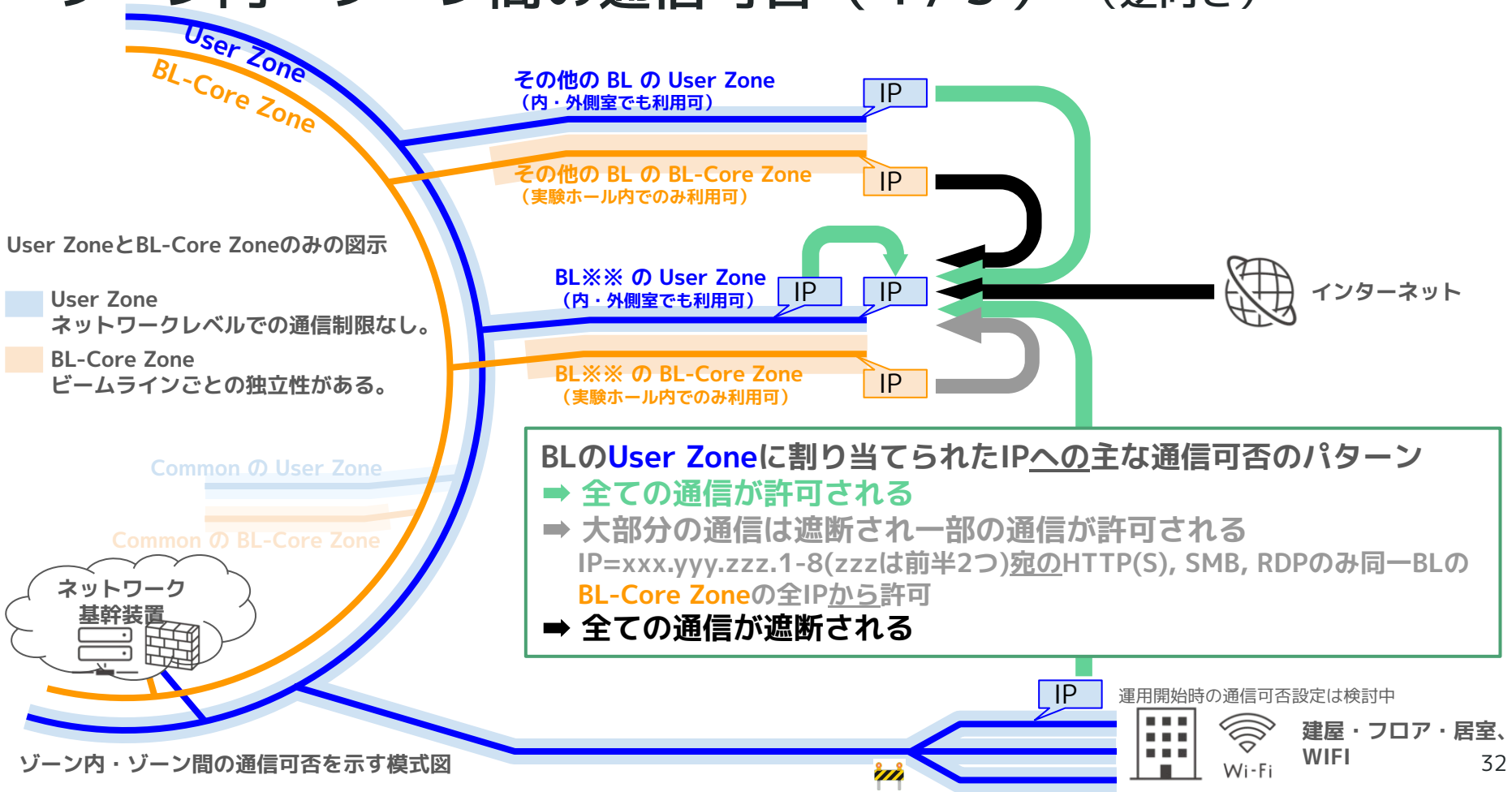
2023年12月時点

ゾーン内・ゾーン間の通信可否（1/3）



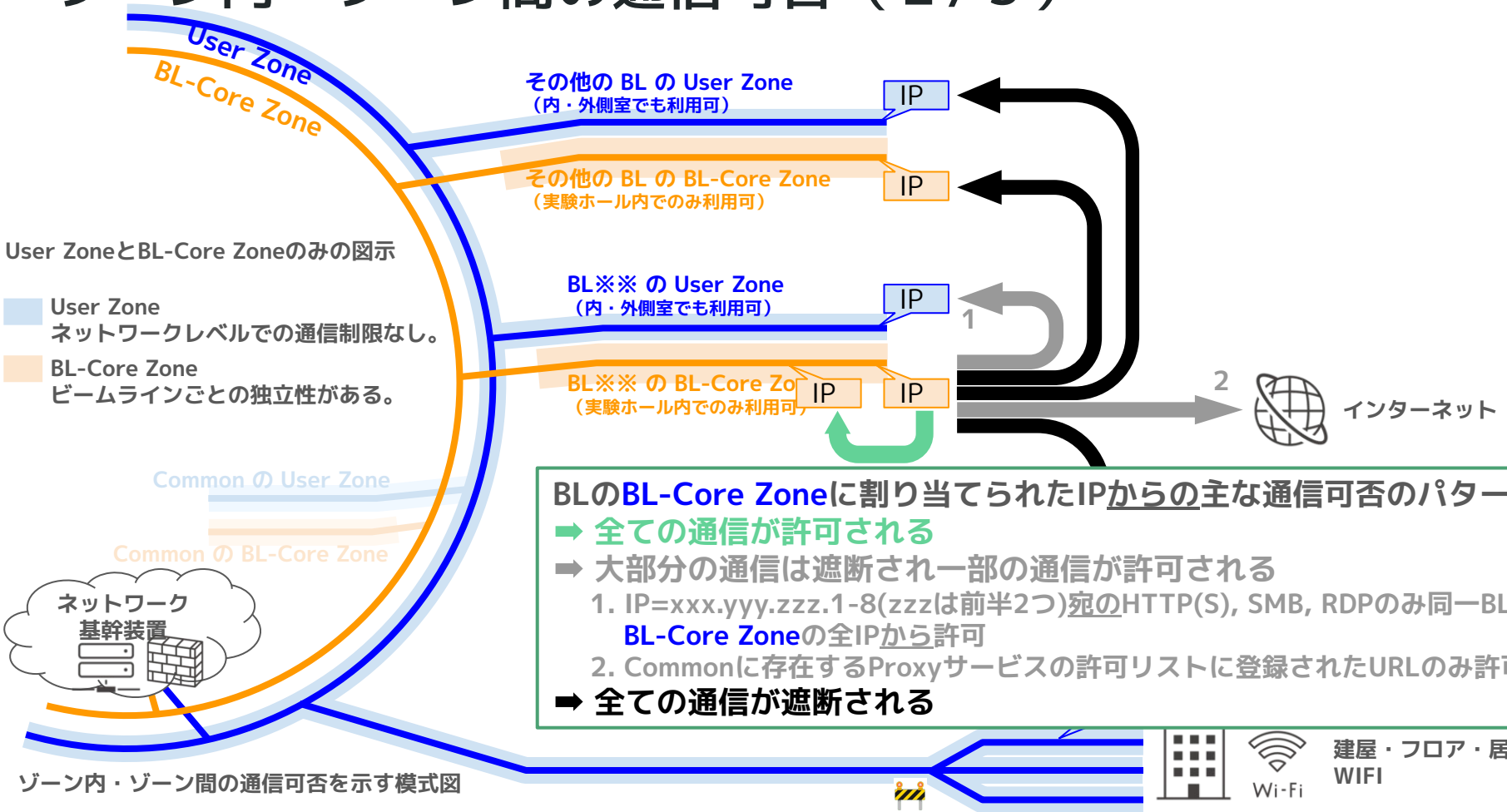
ゾーン内・ゾーン間の通信可否を示す模式図

ゾーン内・ゾーン間の通信可否（１/３）’（逆向き）



ゾーン内・ゾーン間の通信可否を示す模式図

ゾーン内・ゾーン間の通信可否（2/3）



ゾーン内・ゾーン間の通信可否を示す模式図

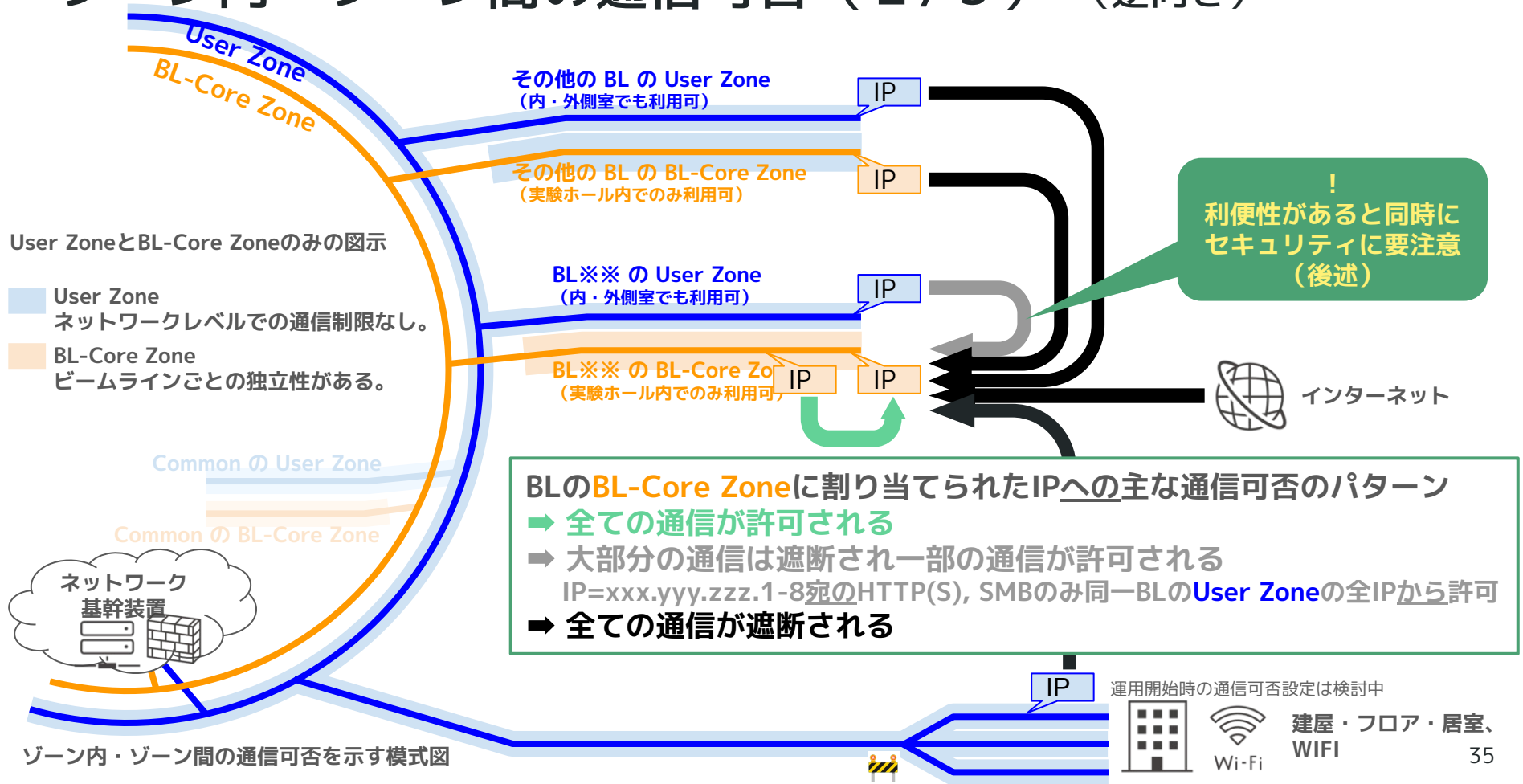
【ご参考】Proxyの許可リストについて

	用途
1	Linux(Ubuntuなど)のアップデート
2	Microsoftのダウンロード
3	Microsoftアカウントへのサインイン
4	Windows Updateへのアクセス
5	Apple製品のサポートサイト
6	Pythonパッケージのダウンロード
7	Anacondaのダウンロード
8	Node.jsパッケージのダウンロード
9	BL-774の開発環境へのアクセス

2023年8月現在のリスト

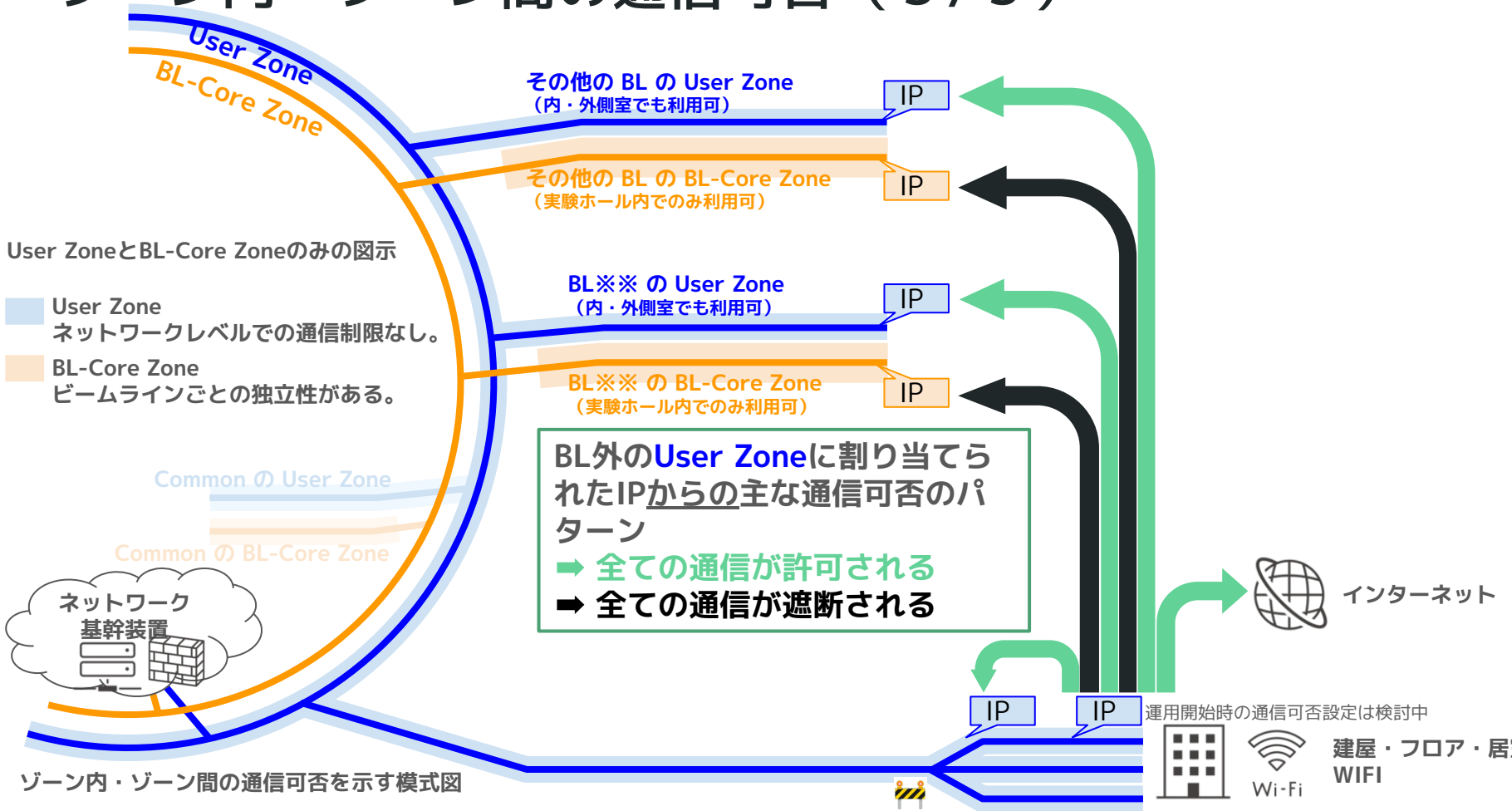
- 表に記載している用途のインターネット接続がBL-Core Zoneからできるように、プロキシサーバーの許可リストにドメインを登録しています。接続できない場合には、ビームラインネットワークの担当者が対応します。ビームラインネットワークの問い合わせ先までご相談ください。
- 左表にない用途（特定の実験機器を使うために必要なライセンスサーバーへのアクセスなど）が必要な際には別途ドメインの登録が必要になります。ビームラインネットワークの問い合わせ先までご相談ください。

ゾーン内・ゾーン間の通信可否（２/３）’（逆向き）



ゾーン内・ゾーン間の通信可否を示す模式図

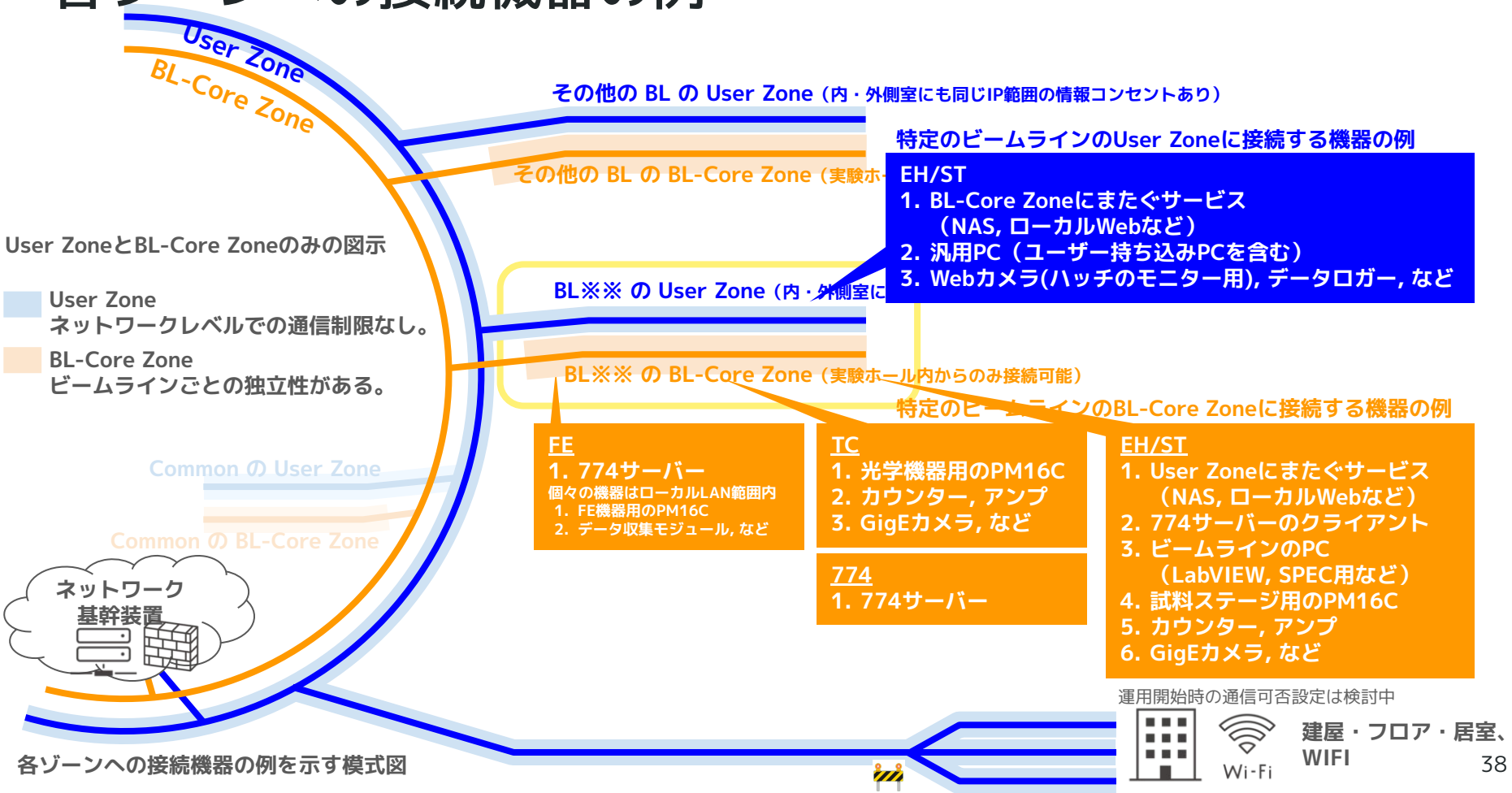
ゾーン内・ゾーン間の通信可否（３/３）



ゾーン内・ゾーン間の通信可否を示す模式図

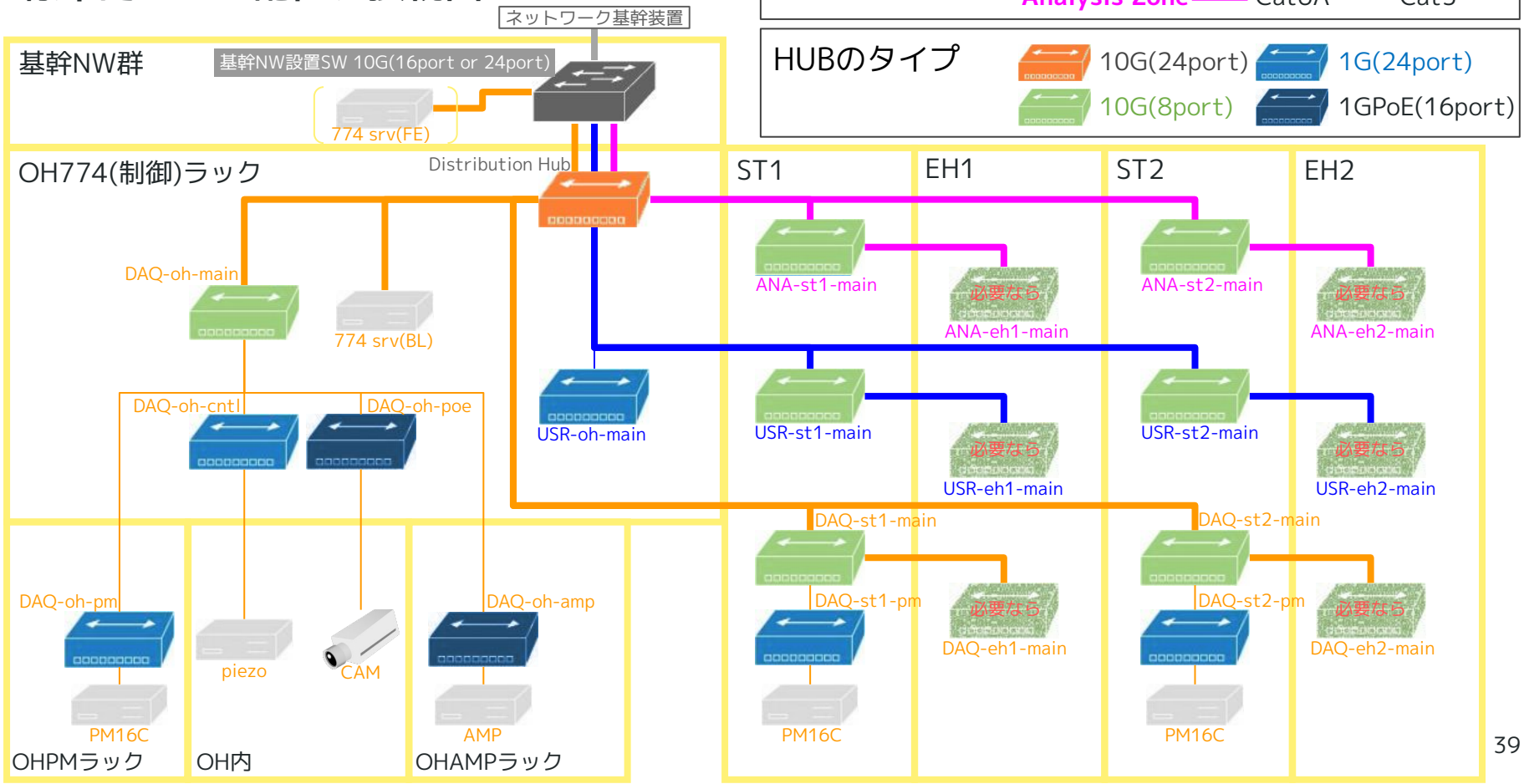
2. 典型的な利用シーンにおいて推奨される接続・使い方について

各ゾーンへの接続機器の例

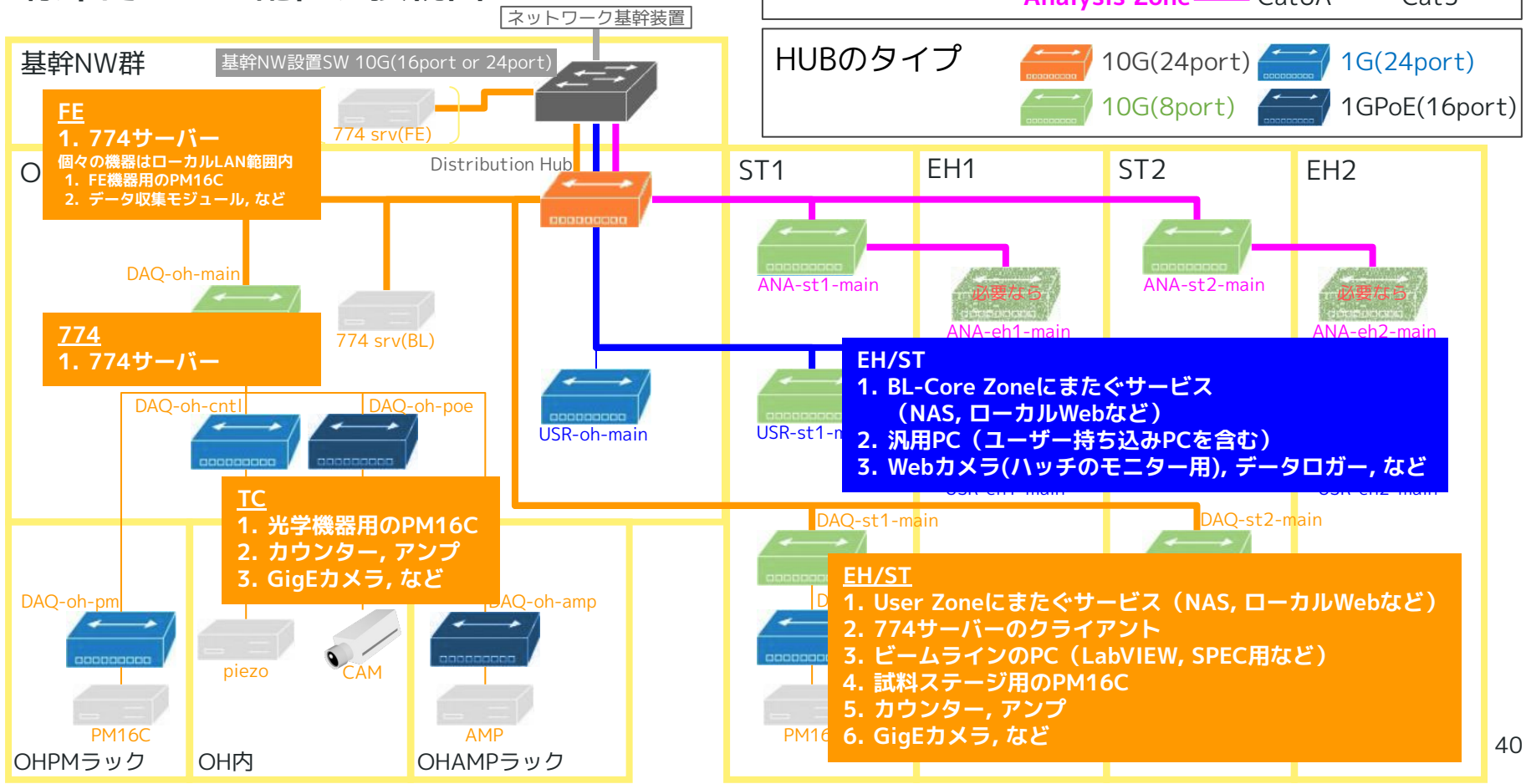


各ゾーンへの接続機器の例を示す模式図

ビームライン内の
標準的なHUB配置、接続図



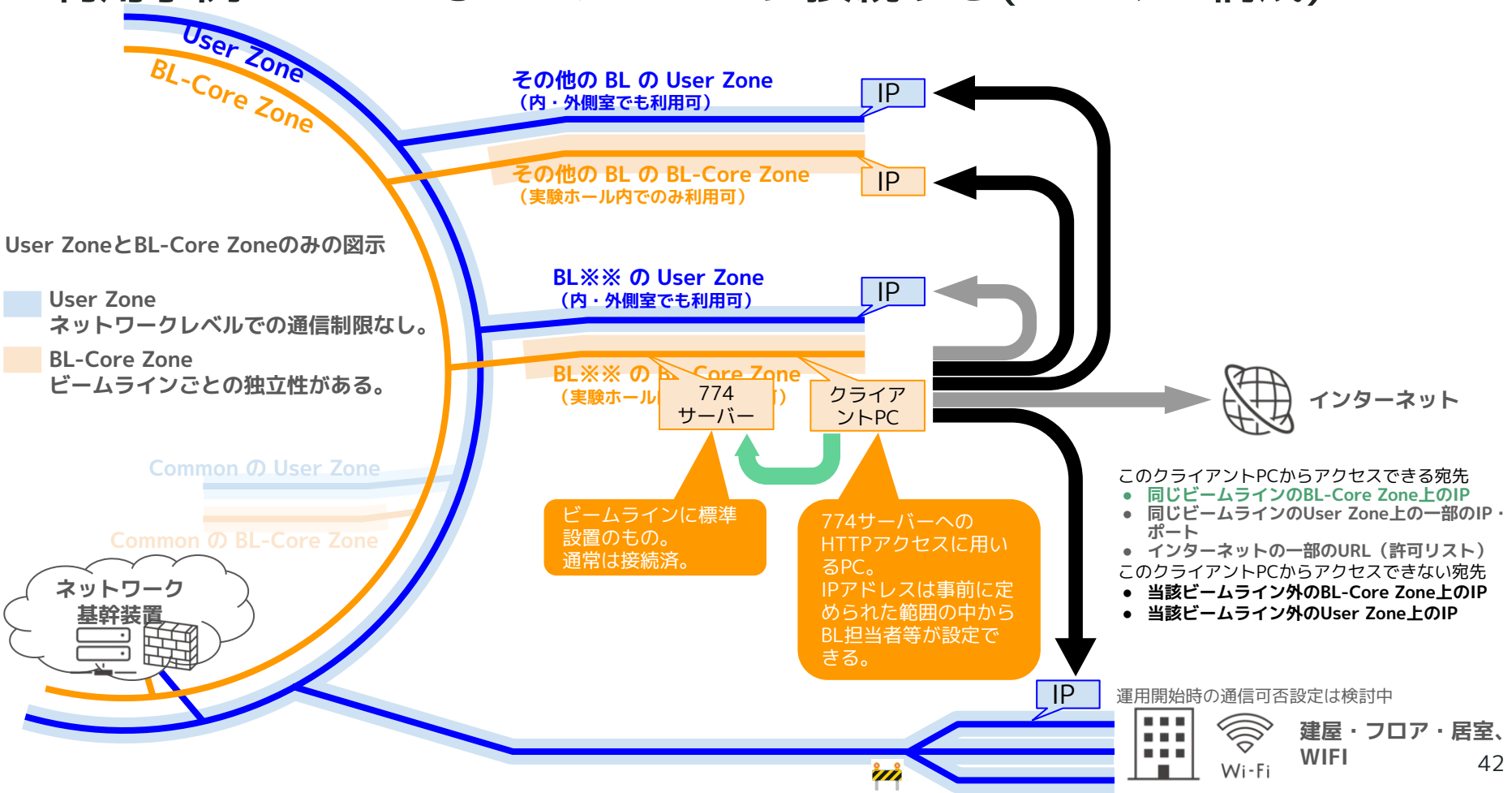
ビームライン内の
標準的なHUB配置、接続図



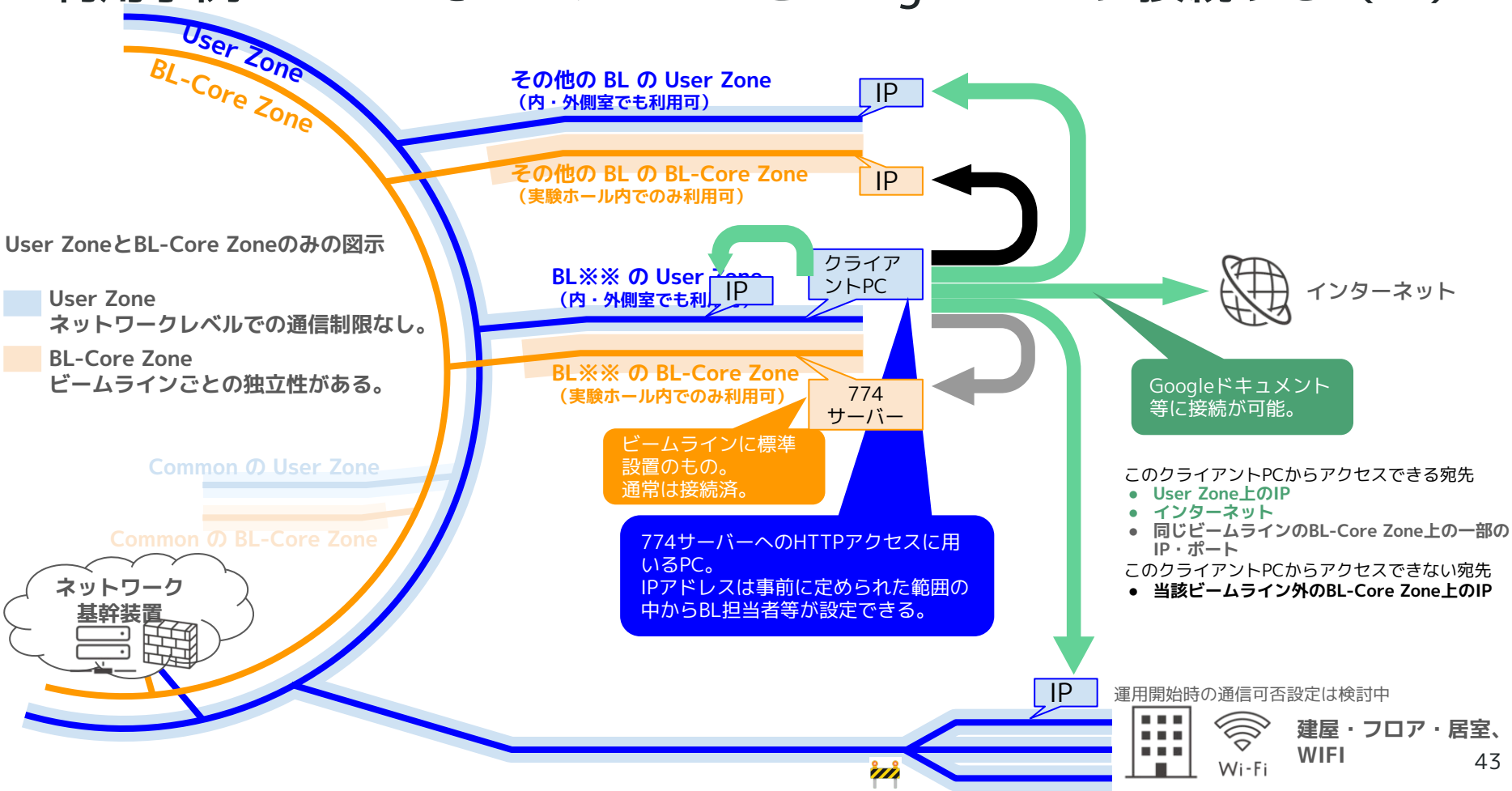
典型的な利用シーンの事例リスト

	接続元		行うこと
1	**EH/ST**	1	EH/STから**ビームラインの774サーバー**にアクセスして操作する（ミニマム構成の例）
		2	EH/STから**ビームラインの774サーバー**にアクセスして操作しつつ**Googleドキュメント**にログを保存する
		3	EH/STからEH内の**試料ステージ用のPM16Cを774で**制御する（ミニマム構成の例）
		4	EH内の**試料ステージ用のPM16CをLabVIEWで**操作する（ミニマム構成の例）
2	**側室**	1	EH内の**ウェブカメラを側室からモニター**する
		2	ビームラインの**774サーバーを側室から（リモート）操作**する
3	**居室**	1	EH内の**ウェブカメラを居室からモニター**する（将来計画の例）🚧
		2	ビームラインの**774サーバーを居室から（リモート）操作**する（将来計画の例）🚧
4	**施設外**	1	インターネット経由で**774サーバーをリモート制御**する（所定の申請手続きの許可後）

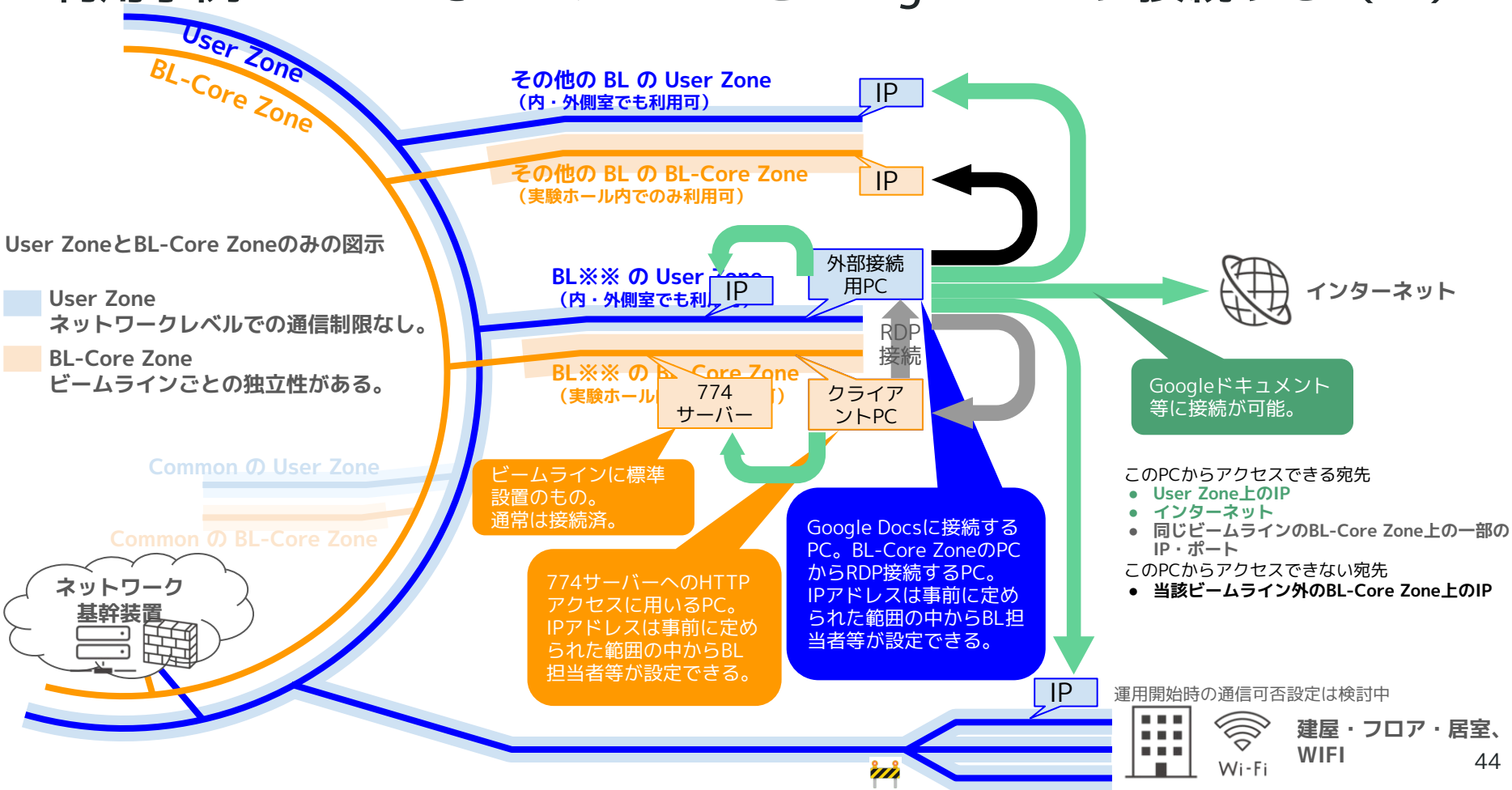
利用事例１.１ STで774サーバーに接続する(ミニマム構成)



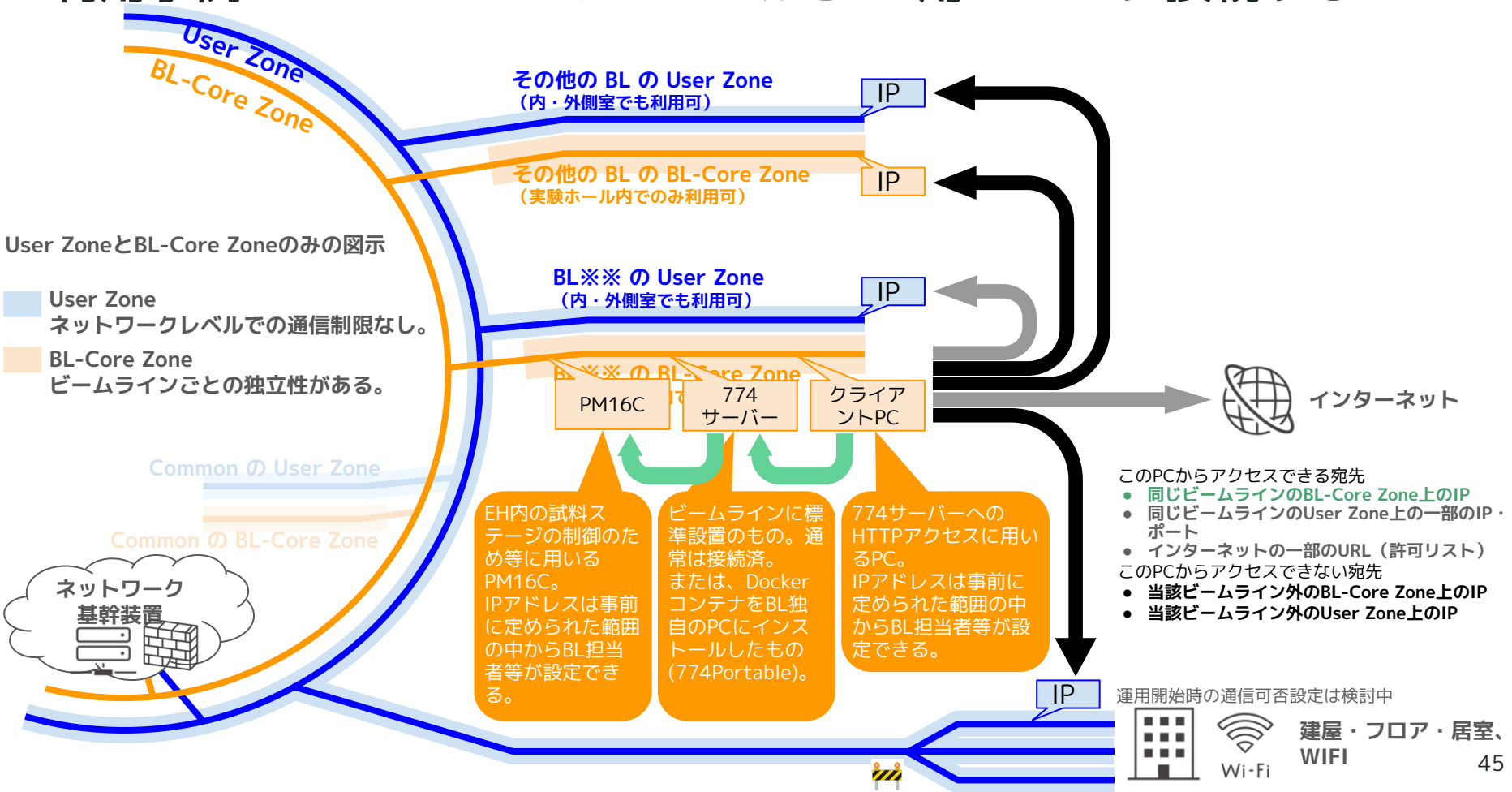
利用事例１.２ STで774サーバーとGoogle Docsに接続する（１）



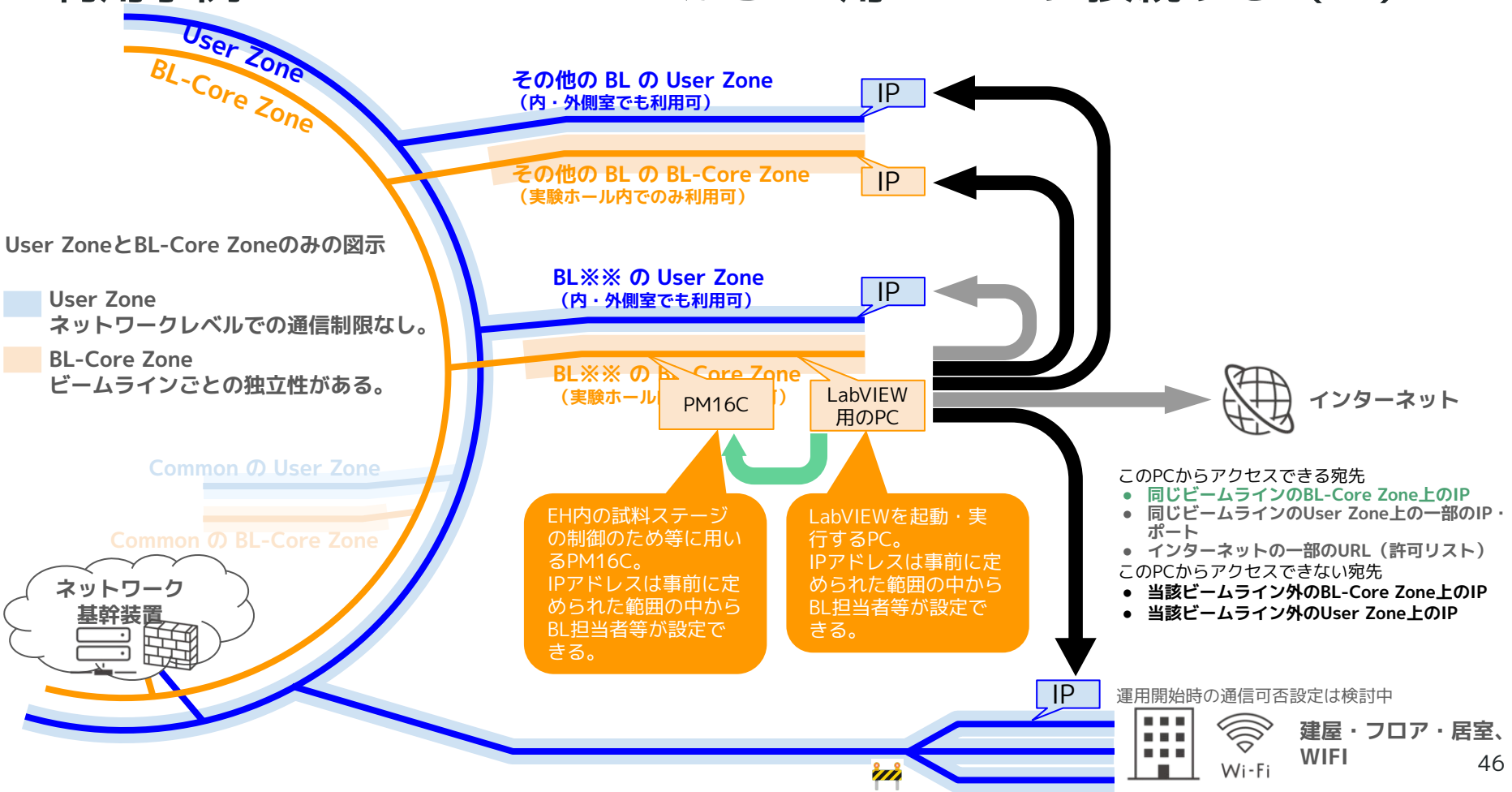
利用事例１.２ STで774サーバーとGoogle Docsに接続する（２）



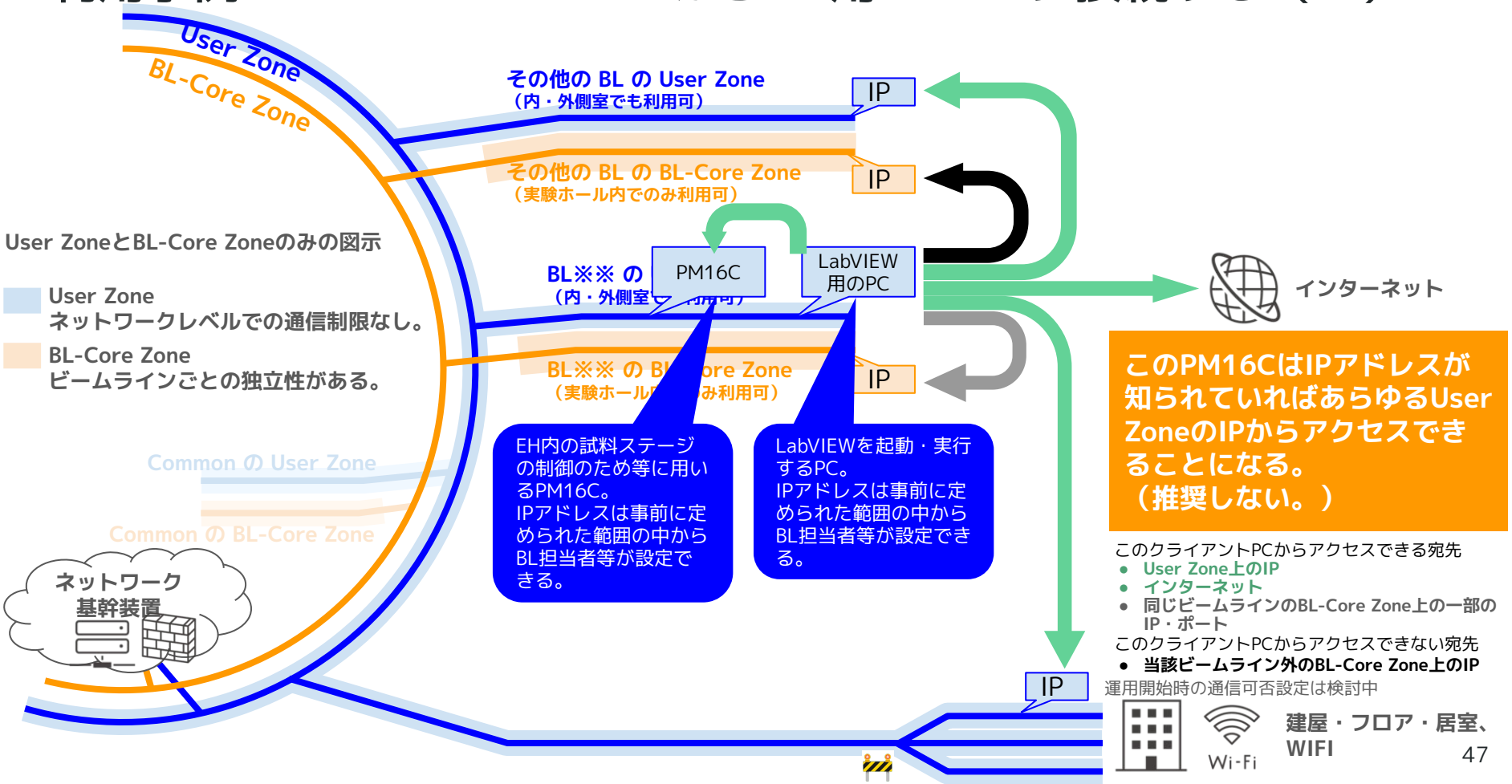
利用事例１.３ STの774サーバーからEH用のPMCに接続する



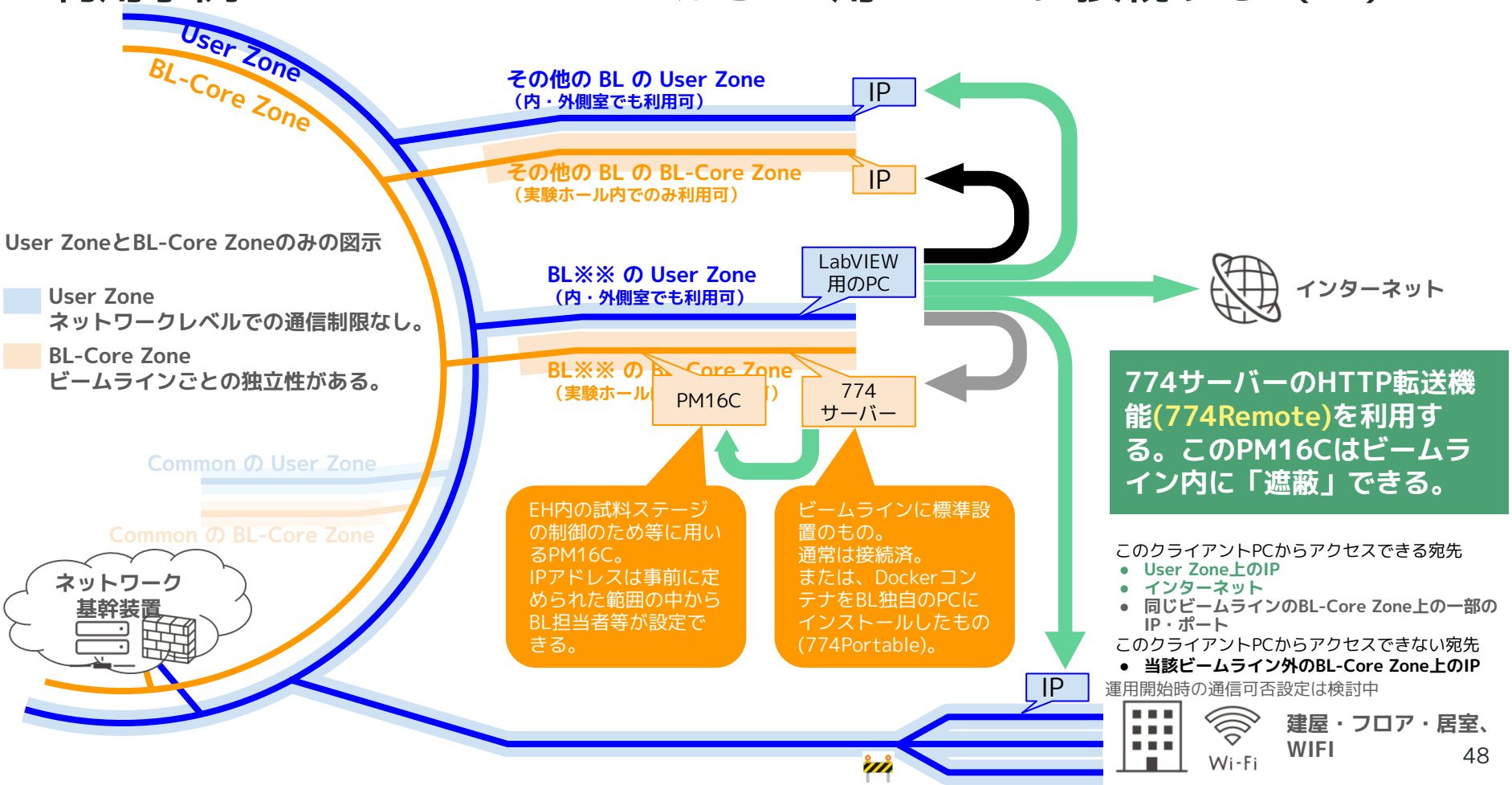
利用事例１.４ STのLabVIEWからEH用のPMCに接続する（１）



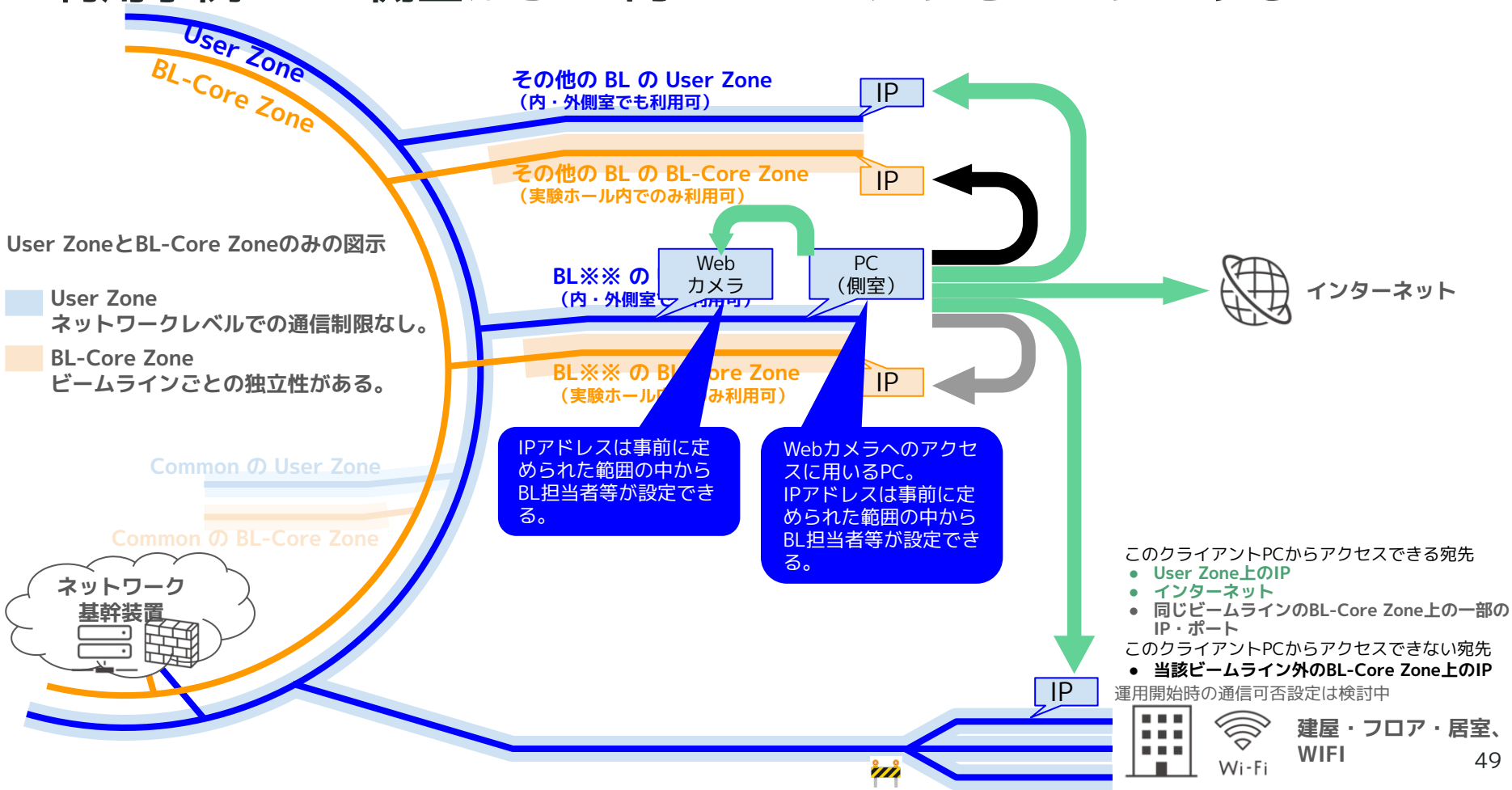
利用事例１.４ STのLabVIEWからEH用のPMCに接続する（２）



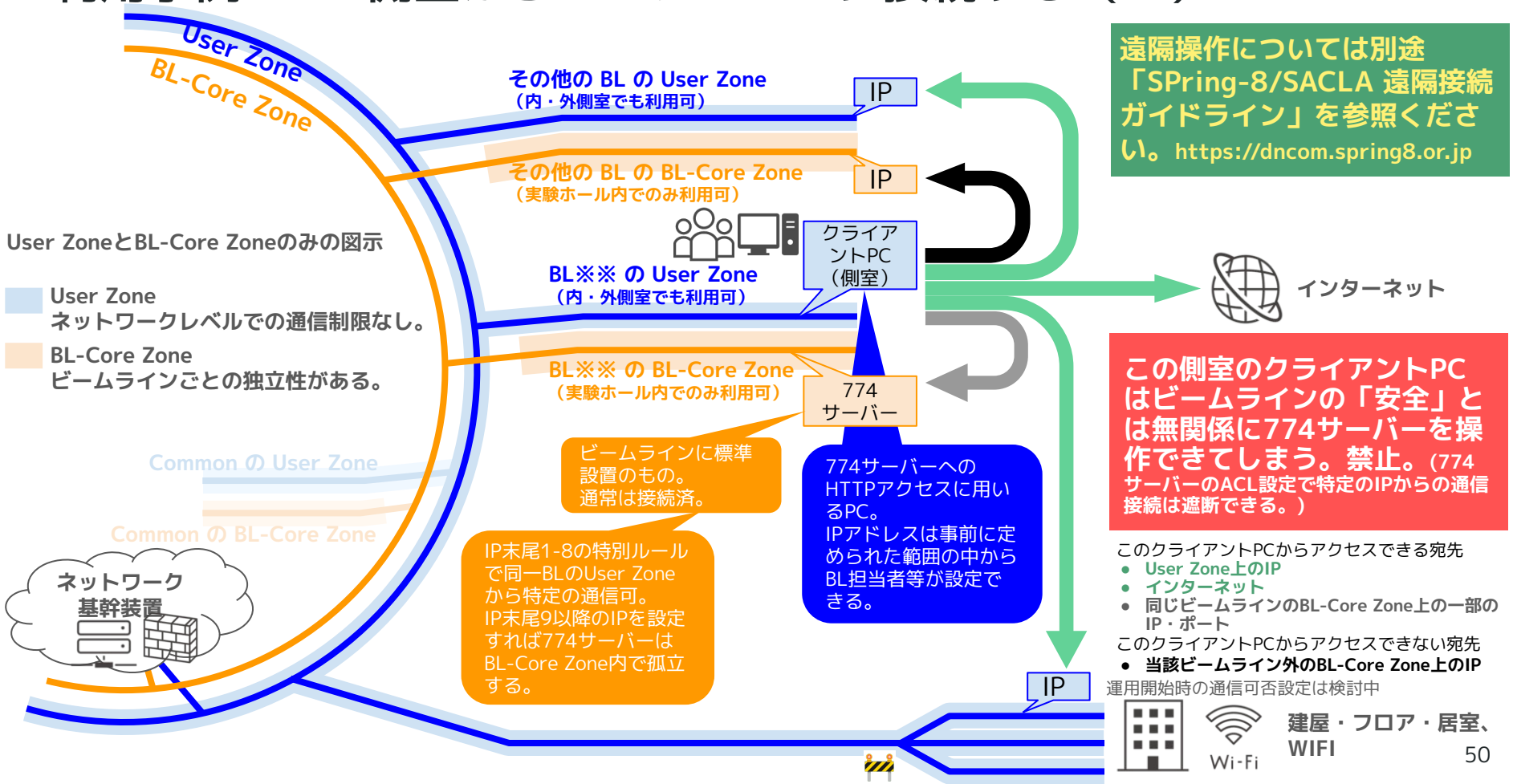
利用事例１.４ STのLabVIEWからEH用のPMCに接続する（３）



利用事例２.１ 側室からEH内のWebカメラをモニターする



利用事例２.２ 側室から774サーバーに接続する（１）



遠隔操作については別途「SPring-8/SACLA 遠隔接続ガイドライン」を参照ください。https://dncom.spring8.or.jp

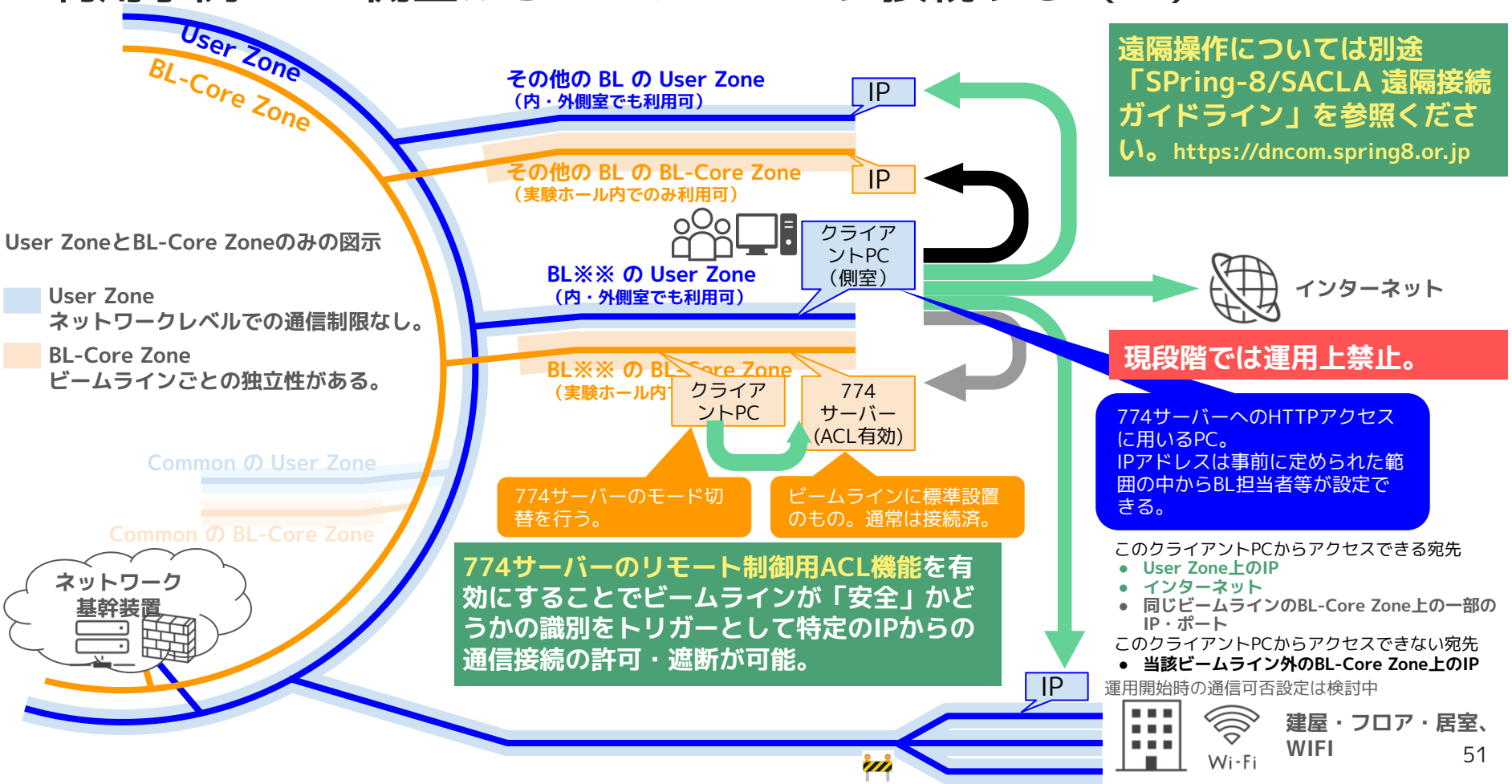
この側室のクライアントPCはビームラインの「安全」とは無関係に774サーバーを操作できてしまう。禁止。（774サーバーのACL設定で特定のIPからの通信接続は遮断できる。）

このクライアントPCからアクセスできる宛先
- User Zone上のIP
- インターネット
- 同じビームラインのBL-Core Zone上の一部のIP・ポート

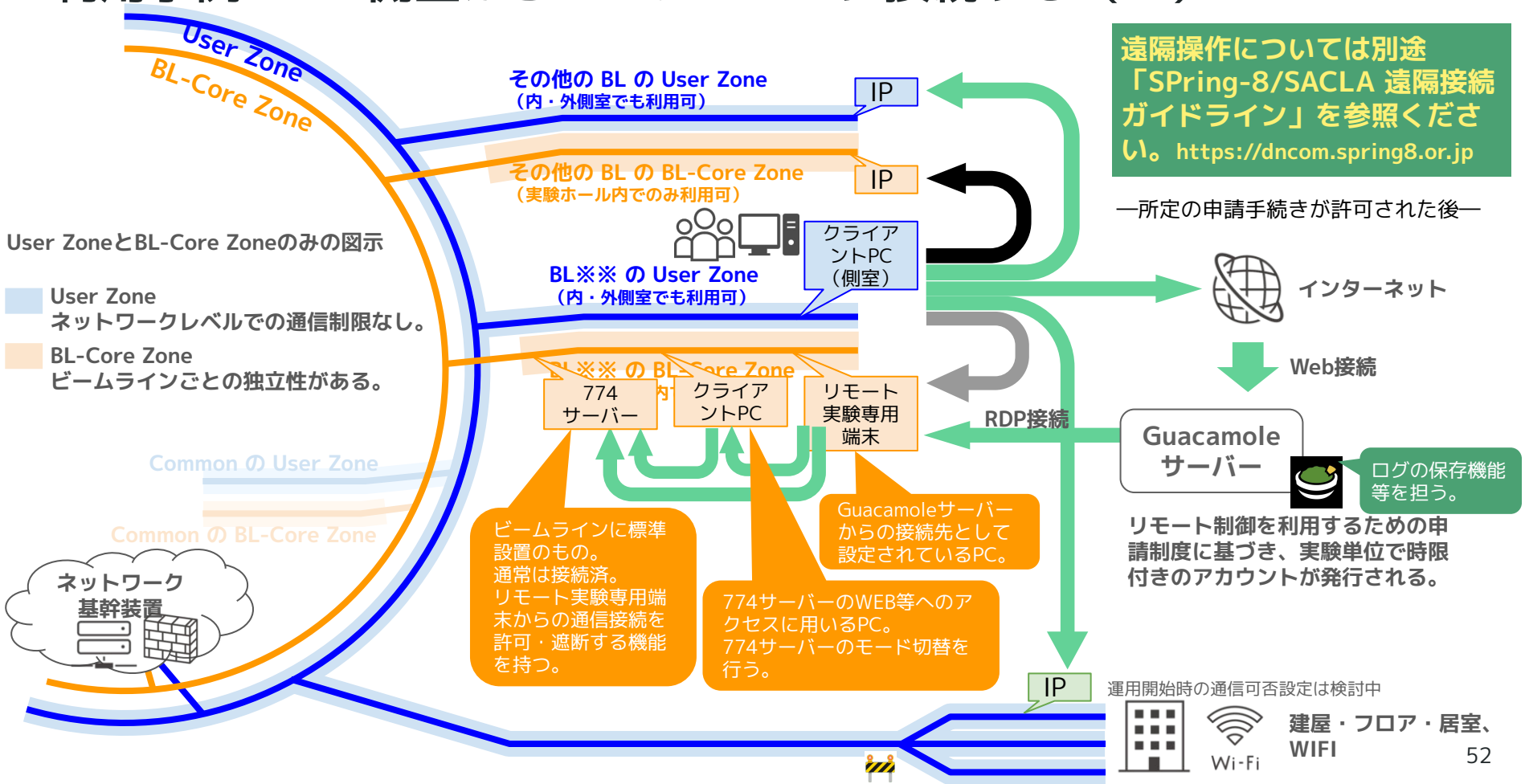
このクライアントPCからアクセスできない宛先
- **当該ビームライン外のBL-Core Zone上のIP**

運用開始時の通信可否設定は検討中

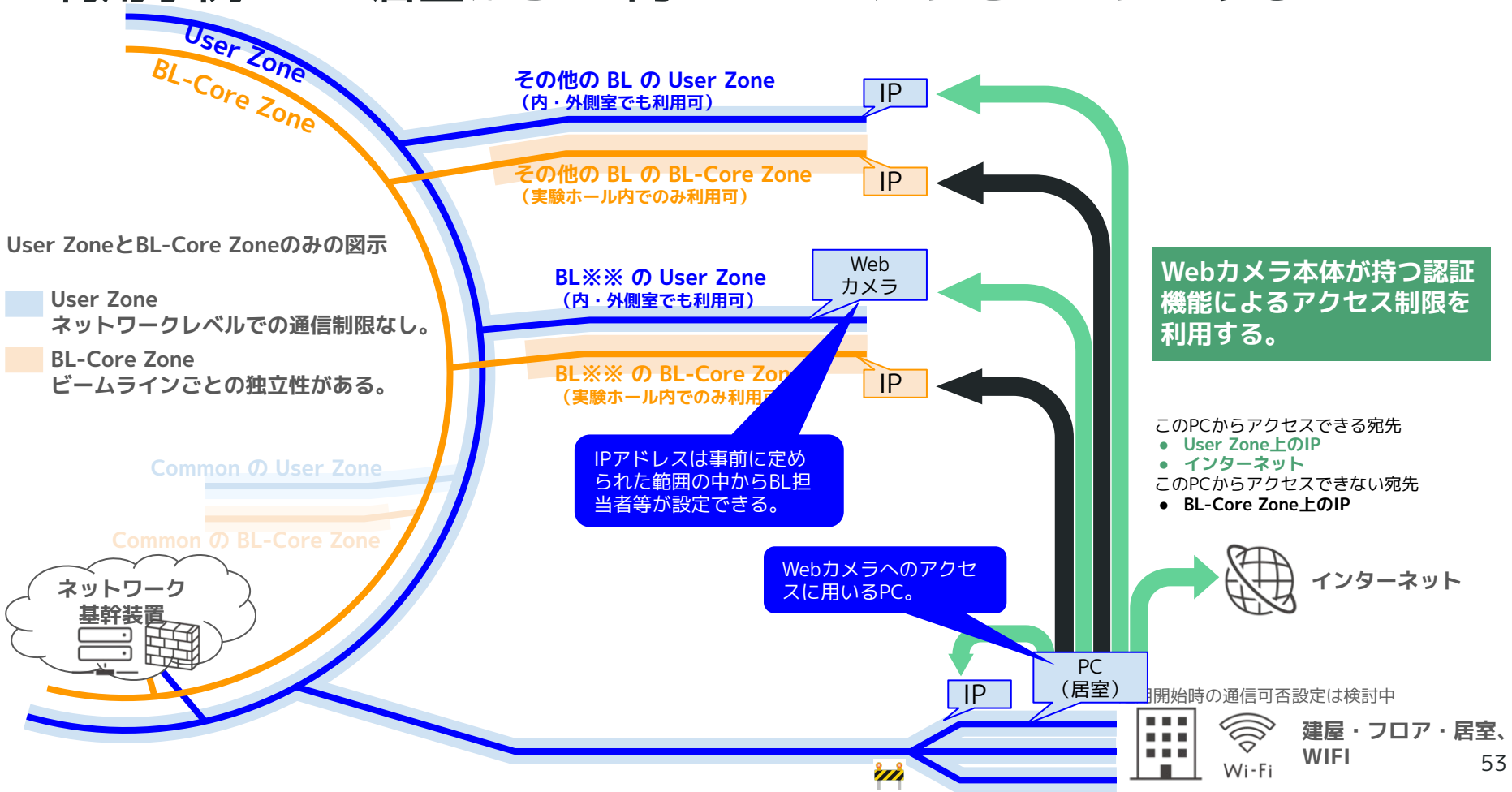
利用事例２.２ 側室から774サーバーに接続する（２）



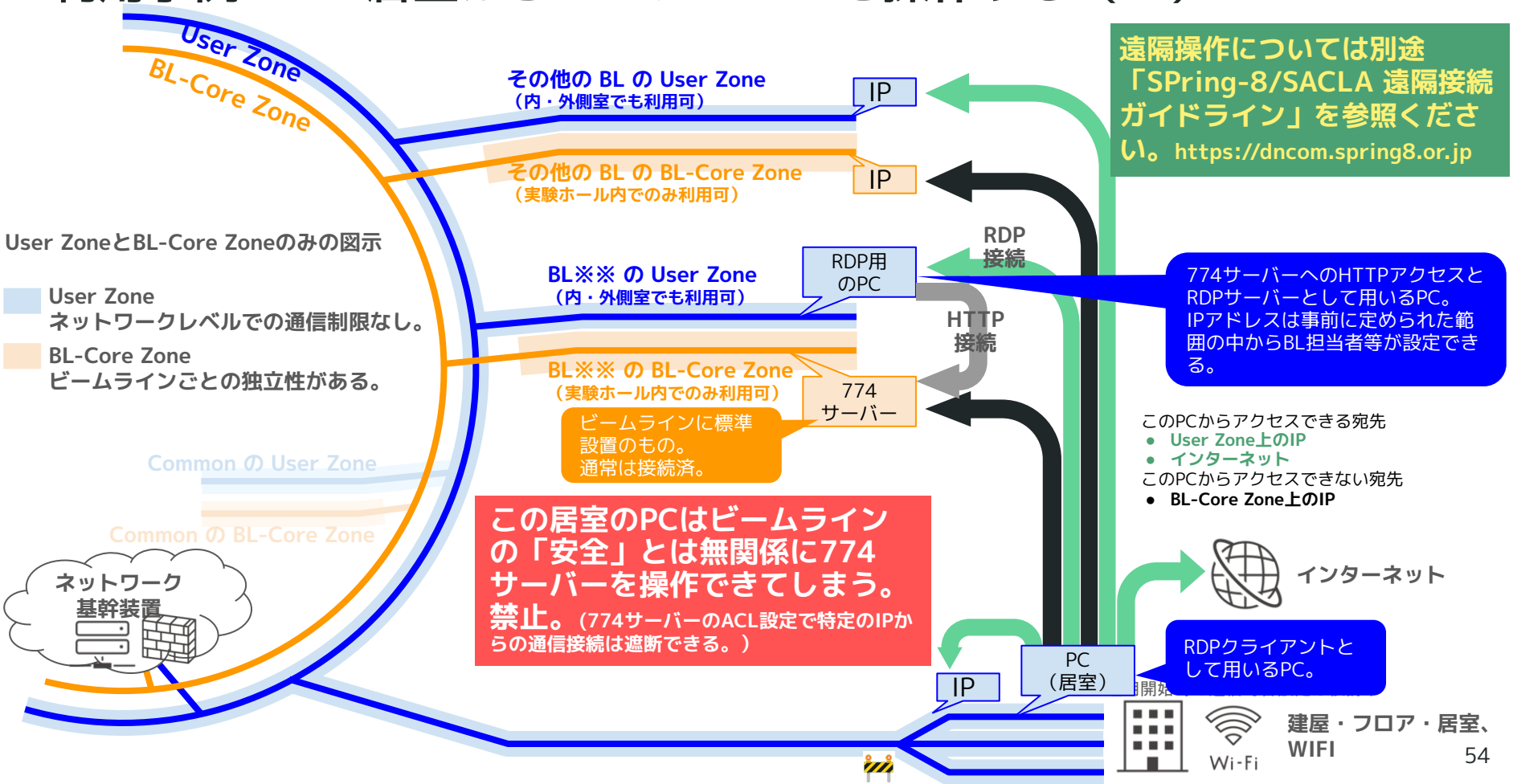
利用事例２.２ 側室から774サーバーに接続する（３）



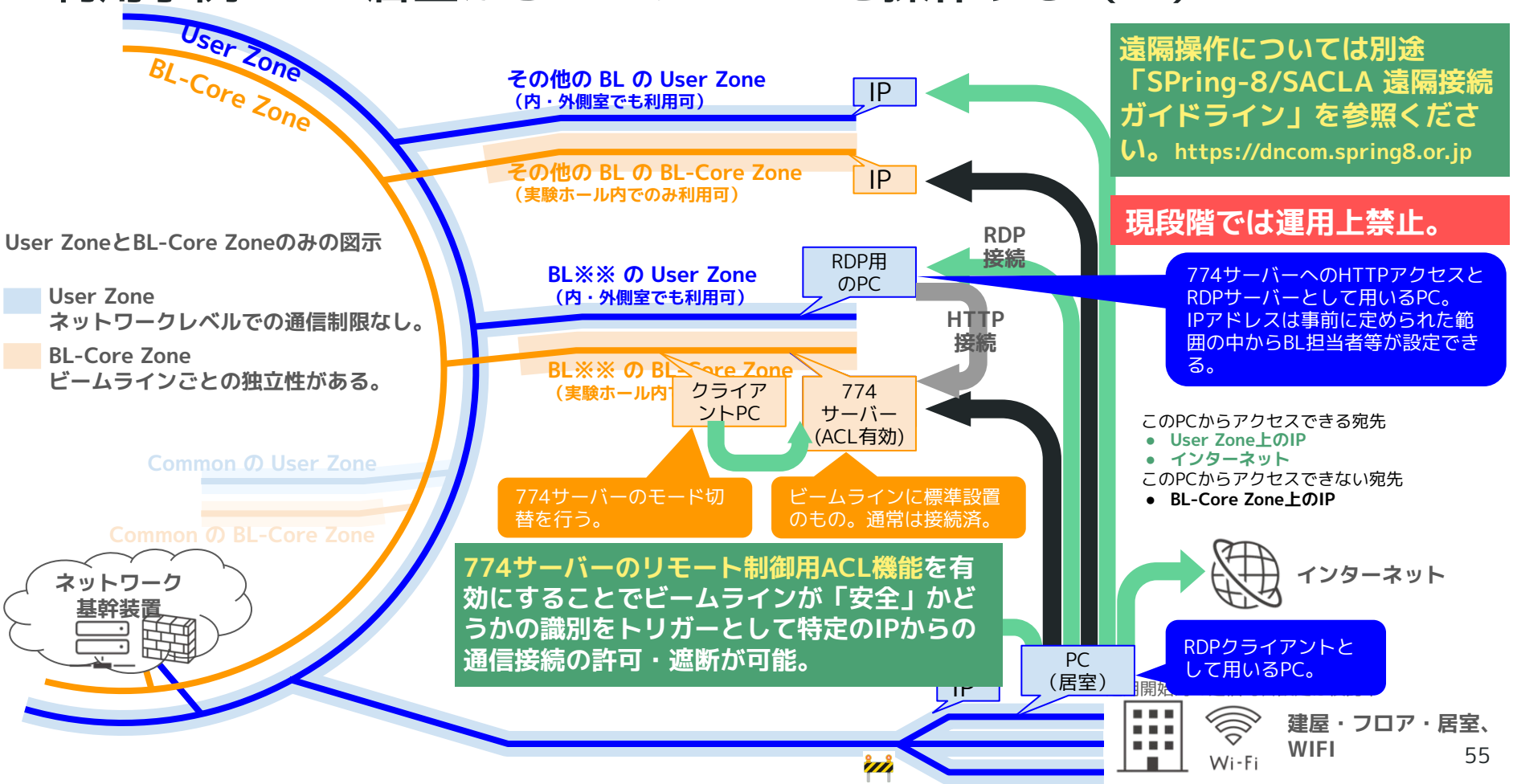
利用事例３.１ 居室からEH内のWebカメラをモニターする



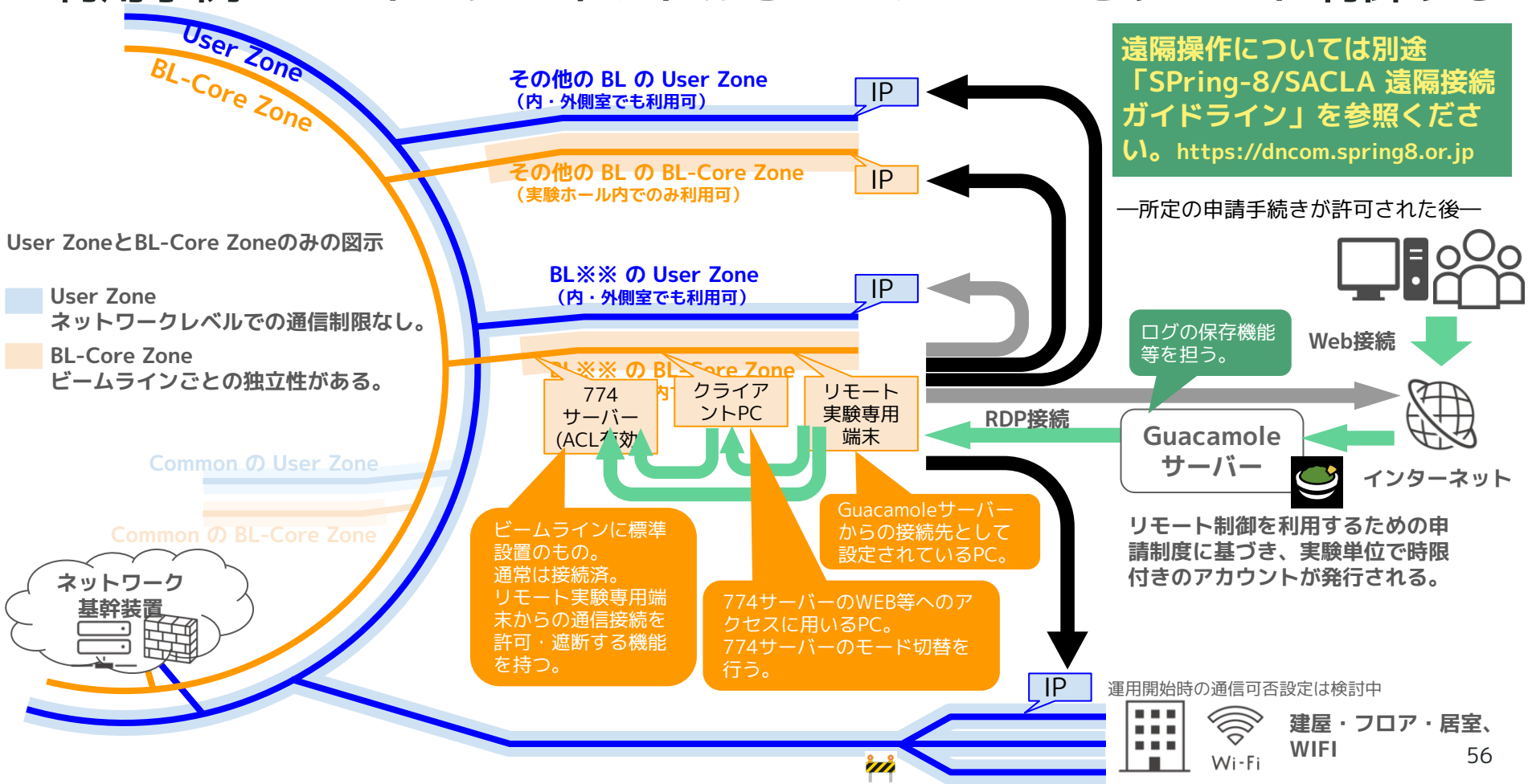
利用事例３.２ 居室から774サーバーを操作する（１）



利用事例３.２ 居室から774サーバーを操作する（２）



利用事例４.１ インターネットから774サーバーをリモート制御する



3. 現行のネットワークからの切り替えに際するインストラクションに関わる内容について（ビームライン担当者向け）

「ビームラインネットワーク」の導入タイミング

背景

- **「BL-774」**（ビームライン制御・データ収集・オンライン解析プラットフォーム）のソフトウェアシステム**「774BasicSystem」**はビームラインへのインテグレーションにおいて**「ビームラインネットワーク」の利用を前提にシステム設計**がされています。
- そのため、ビームラインで「BL-774」（774BasicSystem）の機能を全て有効活用するためには**「ビームラインネットワーク」の導入が不可欠**です。

「ビームラインネットワーク」＋「BL-774」の導入タイミングの主なパターン

- **主に光学装置の改造を伴うケース**
  - **半年程度のシャットダウン期間**を伴うことが多く、その期間の中での作業タイミングを調整して実施を計画します。
- **主に光学装置の改造を伴わないケース**
  - **夏期、（冬期）、年度末の停止期間中**での作業タイミングを調整して実施を計画します。

【参考】「ビームラインネットワーク」導入の作業分担（理研BL・共用BLの場合）

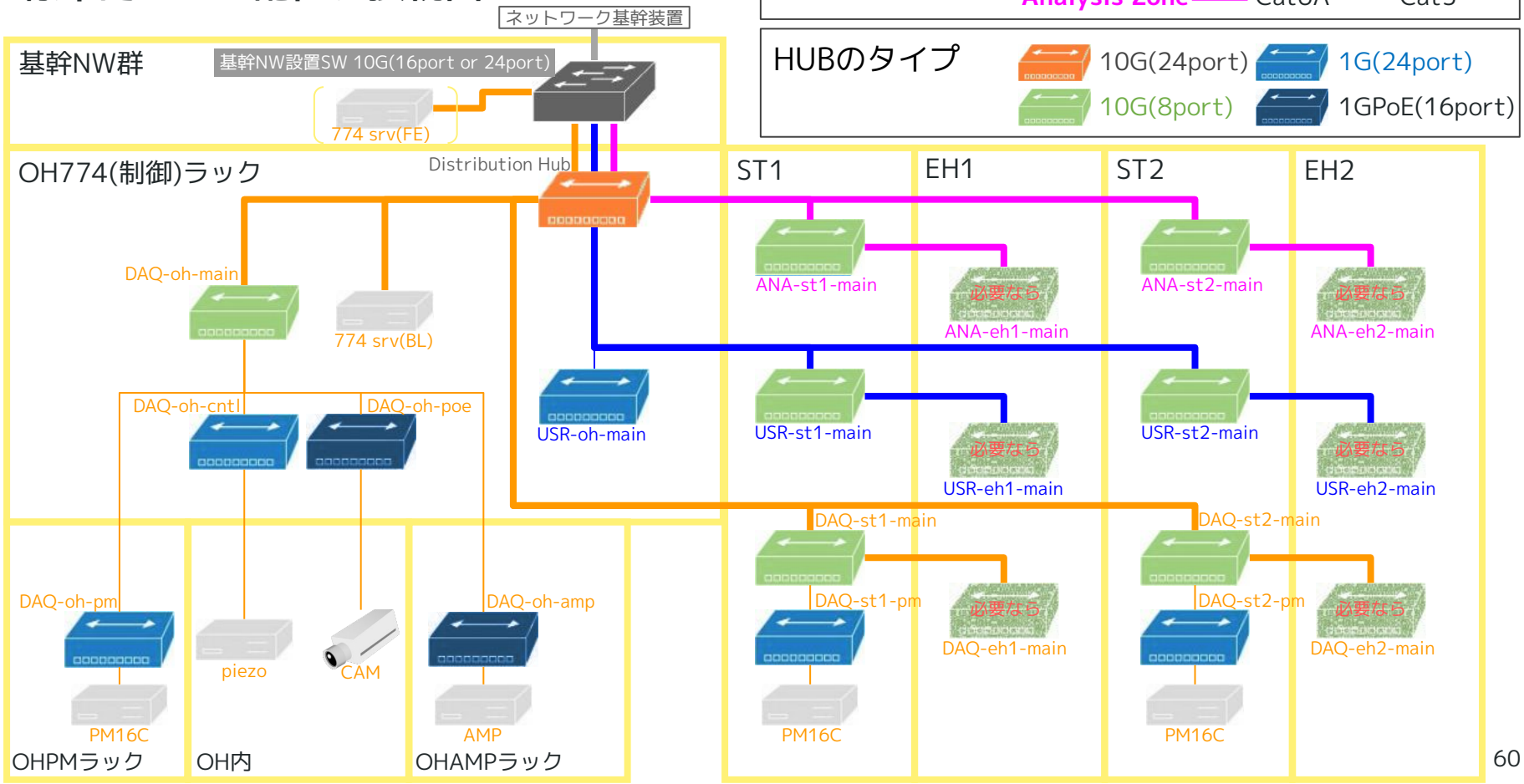
3つのステップで作業が進められる。

1. **基幹ネットワーク** ← **この後の図①**
   ネットワーク基幹装置からビームラインまでの光配線、ビームラインへのエッジスイッチの設置と接続、基幹装置側で行うゾーン関係の設定。（ビームラインの側室を含む）
   - エッジスイッチの設置場所：典型的にはデッキ上のラック内、従来VMEの筐体がある付近。
   - 調達発注／役務発注／現地作業の担当者：ネットワークの担当者
   - この段階で実現すること：3つのゾーンが利用できるネットワークポートを有するエッジスイッチがそのビームラインで稼働する。User zoneが利用できる情報コンセントがビームラインの側室で稼働する。
2. **ローカルネットワーク** ← **この後の図①②**
   ビームラインのエッジスイッチより下流のHUBの設置、エッジスイッチからそれらのHUBまでのネットワーク配線。
   - HUBの設置場所：概ねデッキ上、各実験ハッチ・実験ステーションに各ゾーンに対応するHUBを1台ずつ。
   - 調達発注／役務発注／現地作業の担当者：Engチーム（DAQ Hard）の担当者
   - この段階で実現すること：各エリアで3つのゾーンを利用できるHUBが稼働する。
3. **機器接続** ← **この後の図③**
   末端のHUBへのネットワーク機器の接続、ネットワーク機器のIPアドレスの割り当て、設定、疎通確認。（必要に応じてHUBの追加を含む）

3.1. FE・TCのネットワーク機器に対する作業の場合（FE機器・光学機器関連）
- 調達発注／（役務発注）／現地作業の担当者：Engチーム（DAQ Hard）の担当者

3.2. **EH・STのネットワーク機器に対する作業の場合（ビームライン実験関連）**
- **調達発注／（役務発注）／現地作業の担当者：各ビームラインの担当者**
- この段階で実現すること：各ネットワーク機器が割り当てたIPアドレスで稼働する。

ビームライン内の
標準的なHUB配置、接続図



ビームライン内の
標準的なHUB配置、接続図①

ゾーンの区分
- User Zone — Cat6A — Cat5
- BL-Core Zone — Cat6A — Cat5
- Analysis Zone — Cat6A — Cat5

ネットワーク基幹装置

基幹NW群

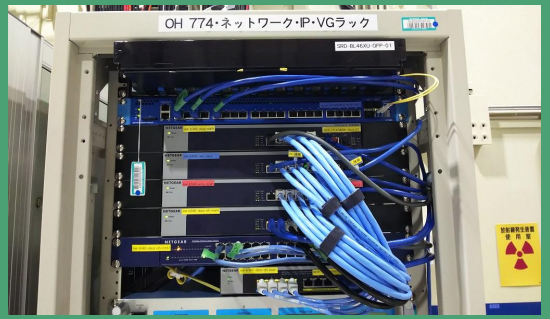
基幹NW設置SW 10G(16port or 24port)

774 srv(FE)

Distribution Hub

OH774(制御)ラック

設置例(BL46XU)



エッジスイッチ
ApresiaNP4000 (経緯により他機種の場合もあり)

「ビームラインネットワーク」として設置する
（場所：これまでFE・TCの機器制御に用いてきたVMEのクレートが設置されているラック内）

エッジスイッチの標準的なポート割り当て
- Port1　：User zone
- Port3, 4：BL-core zone
- Port5　：Analysis zone

USR-st1-main

USR-st2-main

必要なら
USR-eh1-main

必要なら
USR-eh2-main

DAQ-st1-main

DAQ-st2-main

エッジスイッチから各EH・ST等へのメインのネットワーク配線

各ビームラインのハッチ構成に合わせて「ビームラインネットワーク」として設置する

PM16C

AMP

OHPMラック

OH内

OHAMPラック

ビームライン内の
標準的なHUB配置、接続図②

ゾーンの区分

User Zone	Cat6A	Cat5
BL-Core Zone	Cat6A	Cat5
Analysis Zone	Cat6A	Cat5

HUBのタイプ

10G(24port) 1G(24port)
10G(8port) 1GPoE(16port)

ネットワーク基幹装置

基幹NW群

基幹NW設置SW 10G(16port or 24port)

NETGEAR, XS724EM-100AJS
10G/マルチギガビット24ポート
アンマネージプラススイッチ
100M/1G/2.5G/5G/10G RJ-45ポート：24
SFP+ポート：2 (コンボ)

「ビームラインネットワーク」
として設置する

ST1

ANA-st1-main

USR-st1-main

NETGEAR, XS508M-100AJS
10G/マルチギガ8ポート アンマネージスイッチ
100M/1G/2.5G/5G/10G RJ-45ポート：7
10GBASE-T(10G/1G) ポート：1
10G SFP+ポート： 10G/1G SFP+×1 (コンボポート)

「ビームラインネットワーク」
として設置する

DAQ-oh-cntl

DAQ-oh-poe

USR-oh-main

NETGEAR, GS516PP-100AJS
PoE+対応 (260W) ギガビット16ポート アンマネージスイッチ
10/100/1000 Mbpsギガビットイーサネットポート：16
PoEポート：802.3at PoE+ × 16ポート (1ポートあたり30W)
PoE合計出力：260W

各場所での必要の有無に応じて
「ビームラインネットワーク」
として設置する

DAQ-st1-ma

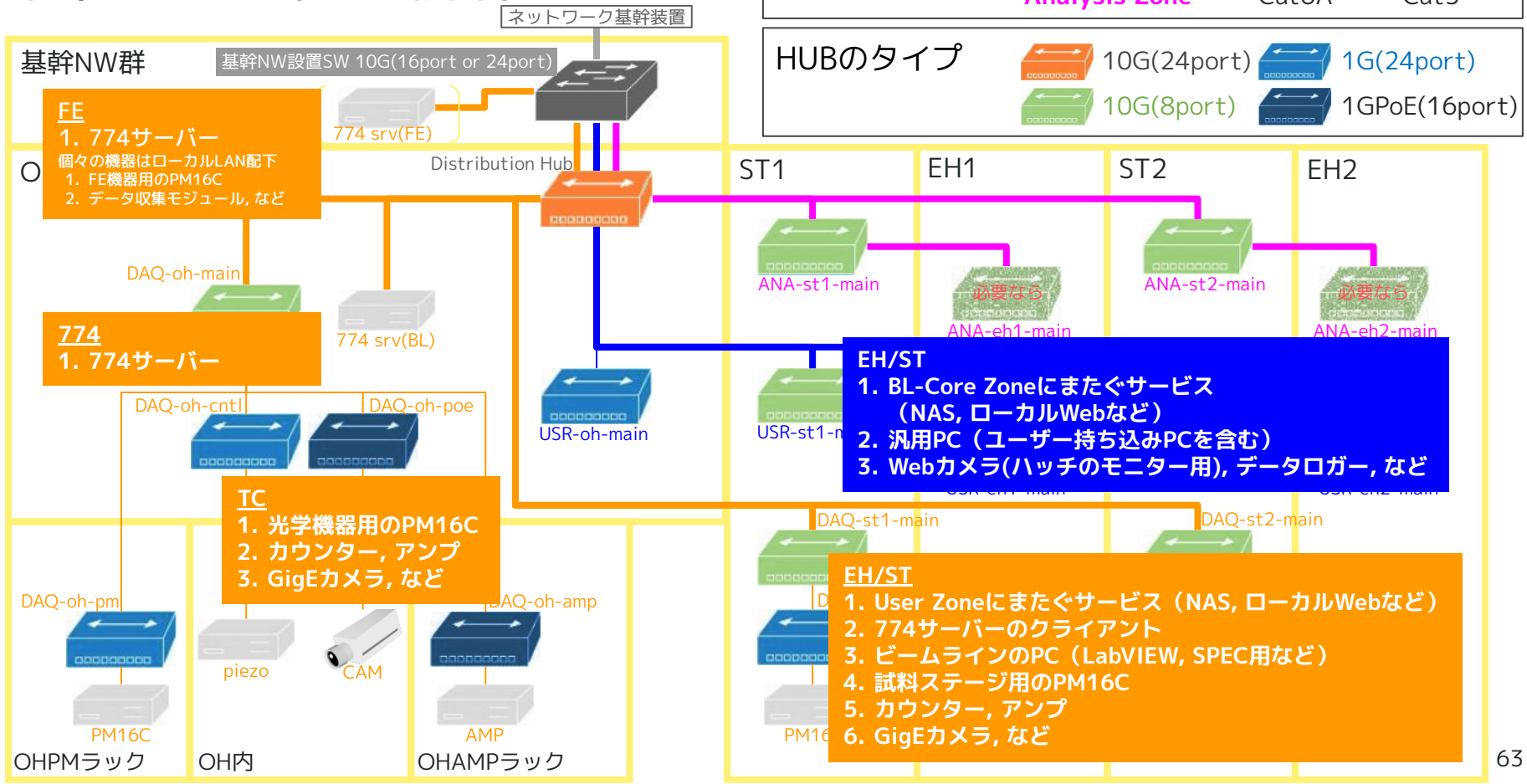
DAQ-st1-pm

PM16C

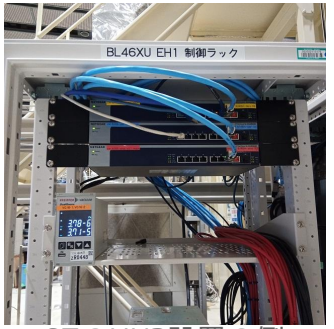
NETGEAR JGS524-300JPS
ギガビット24ポート アンマネージスイッチ
10/100/1000Mbps ギガビットイーサネット ポート数：24
PoEポート：-
ループ検出：-

各場所での必要の有無に応じて
「ビームラインネットワーク」
として設置する

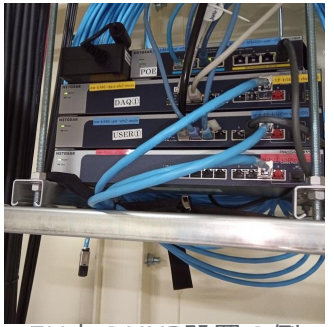
ビームライン内の
標準的なHUB配置、接続図③



ビームライン担当者が行うこと（共用BL・理研BL）



STのHUB設置の例


EH内のHUB設置の例

停止期間作業前に実施すること

- 各ST、EHに配置する各ゾーンのHUBの**設置位置の最終決定**
  - 設置と敷設は理研エンジニアリングチームがヒアリングの上、行ないます。
  - 具体的な構成はヒアリングの際にご紹介します。
- 「ビームラインネットワーク」に接続する機器の**IPリストの作成**
  - 事例. これまでのビームラインで適用したIPリストの例
    （「説明資料集」にBL46XU（EH・STの機器）の事例を記載しています。）

停止期間作業中に実施すること

- 各ST、EHに設置される各ゾーンのHUBと機器間の**ケーブル接続**
  - 標準で設置されるHUB以外のHUBを独自に設置する場合のHUBの設置と接続
- 機器への**IP設定変更、通信確認**
  - 「ビームラインネットワーク」の稼働後に通信が有効になります。
- その他「BL-774」※の導入を含めて、プログラム内のIP設定の変更など
  - BL-WSのIPアドレスを774サーバーのIPアドレスに変更するなど
    （※この資料では「BL-774」の詳細は割愛します。）

「ビームラインネットワーク」の導入に関連する事項

これまで使用してきたBL-USER-LANの扱い

- ビームラインごとにBL-USER-LANを使わず「ビームラインネットワーク」のみを利用した実験の実施に移行できたと判断できた段階で**BL-USER-LANは廃止**していきます。
  - data-net@spring8.or.jpへご連絡ください。
  - ネットワーク基幹装置での設定を変更し、物理的な配線は複数のビームラインをまとめて対処する方針です。

4.「ビームラインネットワーク」を安全に使うための運用ルールの作成に向けて

「ビームラインネットワーク」のメリット・デメリットの整理

メリット

- **BL-Core Zone**
  - 遠隔実験の申請により、自宅からもネットワーク接続をしてユーザー対応ができる仕組みを提供します。
  - 原則としてビームライン内外からのアクセス制限がされていますので、BL-Core Zone内の**制御用PCと被制御機器に対するセキュリティ・リスクを低減する**ことができます。
  - 10Gbpsの帯域でデータセンターと接続しているため、高速の**データ転送**が可能です。
- **User Zone**
  - ビームライン・実験ホール外にも疎通しているため、**ビームライン・実験ホール外からビームライン内の情報を閲覧**する用途に有効です。
  - 10Gbpsの帯域でデータセンターと接続しているため、高速の**データ転送**が可能です。
- **Analysis Zone（参考）**
  - ビームラインでのストレージや解析用のリソースへの接続に利用可能です。

デメリット

- 今までビームラインで使っていたBL-USER-LANのみに比べると、ネットワーク構成が複雑になり、**各ゾーンの役割に応じた機器の設置や設定が必要**になります。
- ゾーン間・ビームライン内外のネットワーク接続が適切でない場合には、セキュリティ（security）・セーフティ（safety）両面でリスクが高まります。
  - 典型的には側室のUser ZoneとBL-Core Zoneの間の通信接続など。（後述）

「ビームラインネットワーク」を使う上での基本方針

～「ビームラインネットワーク」の「心」～

- 技術的には、様々な利用実態に合わせることができるように、いろいろな設定ができるようにしてあります。
- 原則としては、従来通り、**セーフティ（safety）**の観点から
  - ◆ **人命優先**
  - ◆ **機器保護**

  の２点に反しないようにビームラインの機器を接続してください。
- これには**情報セキュリティ（security）**に対する扱いも関連します。
  - その中でゾーンの設定やゾーン間の通信可否設定など、ネットワークレベルでできる対策を行っています。
  - 従来通り、機器のログイン認証の設定など、個々にできる対策の実施をお願いします。

- その上で指針となる**運用ルール**を今後まとめていきますのでご協力ください。

リモート制御、遠隔操作の詳細については別途
「SPring-8/SACLA 遠隔接続ガイドライン」を参照ください。
https://dncom.spring8.or.jp

【補足】「リモート制御」における「安全」について

「リモート制御」の仕組みが満たす必要のある原則：「安全」が担保されている時のみリモート制御ができる。

- ここでの「安全」である時：ハッチが閉まっている時。人はハッチ中にはいない。
  ハッチ内で負傷はしない。（ここでは機器の保護とは別の意味合い。）
- ここでの「安全」でない時：ハッチが開いている時。人がハッチ中に入っているかもしれない。
  ハッチ内で負傷の恐れがある。

この資料の後半で「BL774」を利用する場合のリモート制御の構成例を示します。

- この構成では、上記の原則は「774サーバー」が標準で持つ仕組みが担います。
  - 「安全」であるときのみ、あるIPから774サーバーへの通信接続を許可し、「安全」でないと判断したときには、そのIPからの通信接続を遮断する機能を有効にする。
- その「774サーバー」にインターネットから到達するには基幹部の「Guacamoleサーバー」を経由させます。
- 「Guacamoleサーバー」からの接続先を絞るために「リモート制御専用端末」をビームラインごとに1台設定し、ここから「774サーバー」にRDP接続する設計になっています。
- 運用面では、この「774サーバー」の仕組みが揃っているビームラインに「Guacamoleサーバー」用のアカウントが発行できることになっています。

側室や居室からの操作であってもリモート制御と同等に「安全」に関するリスクの背景が存在します。

- 現段階では「SPring-8/SACLA 遠隔接続ガイドライン」によらない操作は禁止されます。
- 今後の運用は検討中です（インターネット経由とイントラネット経由で同じ申請手続きかなど）。

【補足】ビームライン内外・ゾーン間通信の扱いに関して

A. これまでビームライン・実験ホール内で用いられてきたBL-USER-LANは**ビームライン・実験ホール外からのアクセス**は不可であったが、**User Zoneでは可**となる。また、**ビームライン内でUser ZoneからBL-Core Zoneへの特定の通信が可**となる。

	通信元		通信先
A.	**ビームライン外のUser Zone(居室等)**	→	**ビームラインの管理区域内のUser Zone** のIP(全IP)を持つ機器への通信
	ビームラインの外側室のUser Zone	→	
		→	**ビームラインのBL-Core Zone** のIP**(末尾1-8のみ)**を持つ機器への通信**(HTTP(S), SMBのみ)**

B. ビームラインの機器との通信には一般に、**機器の制御操作と機器の情報閲覧**が存在するが、両者の性格は異なる。ビームラインの「安全」の観点では、ビームライン・実験ホール外からビームライン・実験ホール内の**機器制御は不可、情報閲覧は可**を原則とすべきである。

C. しかし、制御操作と情報閲覧の通信をファイアーウォールやアクセスコントロールなど**ネットワークが持つ仕組みのみで100%の精度で識別し許可・遮断することは現実的に不可能**である。

D. 「安全」が担保されている状況かの判断をトリガーとして特定のIPからの通信を許可・遮断する仕組みは**774サーバーの「リモート制御」**の機能として実現している。ビームライン・実験ホール外から（インターネット経由であるかを問わず）ビームライン・実験ホール内の機器を制御する必要がある際にはこの仕組みを使用することが原則となる。

E. なお、もともと情報の閲覧に特化し、制御機能は限定的な機器（Webカメラなど）は「リモート制御」の仕組みによらずビームライン・実験ホール外からビームライン・実験ホール内にアクセスすることが許容される機器となる。

	状態	対象となる機器	機器制御		情報閲覧	備考
B.	原則的に実現されているべき状態	制御可能な全ての機器	×不可 (774の有無によらず)		○可	システムのみでは解決せず"運用"を伴う必要がある。
C.	ネットワークの設定のみで実現する状態	制御可能な全ての機器	○可		○可	—
D.	**774サーバーの「リモート制御」**の機能を用いて実現する状態	774サーバーを介して通信する機器	「安全」担保下	○	○	774サーバーが特定のIPからの通信を動的に許可・遮断する。
			「安全」担保外	×	○/×	
E.	機器が備えている機能が限定的な場合の状態	特定の機器 (Webカメラ等)	△限定的/×不可 (首振り等のみ)		○可	上のようなソリューションは必要なくアクセスできる。

「ビームラインネットワーク」の運用ルール作りに向けて

- 人命優先・機器保護の原則を効果的に実践するためには「ビームラインネットワーク」を利用していく上でのルール作りが不可欠です。
  - 現状、「ビームラインネットワーク」レベルでの細かいルールは明文化されていません。
- 次ページに大枠案を示します。ビームラインに関わる方々で実際の利用を踏まえた細かい運用ルール案のリスト化を希望します。
- それらを基に、ネットワーク関係者も関与して整理していきます。
  - ルールの具体的な記述、ルールの位置づけの整理（「ビームラインネットワーク」固有のルールとするか、一般にネットワーク共通のルールとして扱うかなど）も図ります。
- ビームラインに関わる方から数名程度、ビームラインからの案のとりまとめやネットワーク関係者との検討に参加していただくことを希望します。

リスト編集中

「ビームラインネットワーク」の運用ルールの大枠案

各ゾーンでの機器の接続、通信について

- User Zoneに実験機器を接続して実験に利用しない（Webカメラや持ち込み装置のような例外はあるので例外を決める。）
- 従来のBL-USER-LANと同じように、全ての機器やPCをBL-Core Zoneに接続して、ビームライン外からのアクセスを行わない運用も可能であるが、逆にTC・FEの制御系へのリスクが高まるので避ける。
- いわゆる「ユーザー持ち込み機器」をBL-Core Zoneに接続しない。
- IPアドレスの使い方の例（制御PCはIPの末尾100番台、機器は200番台、ユーザーPCは末尾100以降に割り振るなど。）
- ネットワークスキャンやポートスキャンをする機器の接続を禁止する。
- User Zoneでのポーリング等のルール（パケットの流し過ぎ禁止。居室から早い周期で値の参照などをする可能性。）
- 他のビームラインへのアクセス時のルール（むやみに知らない人が実験しているビームラインに接続しない。）
- 成果占有などは外部からの接続ができること自体を嫌いそうなのでその際の対策（一時的にビームラインのUser Zoneを切り離すなど。）

運用上の相談について

- ネットワークの特定のポートに対する通信可否設定の変更に関する申請の手続き方法を決める。（共用BLであれば上長のOKを取ってネットワーク関係者に申請するなど。）
- 接続の可否が分からない場合にはネットワーク関係者に相談を行って欲しい。
- ビームライン側の協議で決まらなかった点も上げてもらってネットワーク関係者で検討を一緒に行う。

おわりに

まとめ

- SPring-8のイントラネットにおける**「ビームラインネットワーク」**について多くのビームラインに共通する一般的な事項についてご説明しました。
- **用途別に提供される3つのゾーンを選択的に利用する**ことにより、さまざまな機能が標準で可能になります。
  - インターネット環境からのリモート制御、実験の進行状況の所内外からのモニターなど。
- 「ビームラインネットワーク」の**ビームラインへの導入の流れ**についてご説明しました。
  - 「BL-774」（774BasicSystem）の導入と同じタイミングで導入が必要になります。
  - ビームラインによってシャットダウンを伴う期間に作業を行う場合と、停止期間中のみに作業を行う場合があります。
- 「ビームラインネットワーク」を**安全に利用するための運用ルール**作りに向けてのご説明をしました。

情報公開、問い合わせ先

- **この資料の公開場所**
  - 下に記載のポータルサイト内
- **問い合わせ先**
  - SPring-8のイントラネットに関すること：data-net@spring8.or.jp
  - BL-774、774BasicSystemに関すること：blict@spring8.or.jp
  - 遠隔実験のWeb申請：SPring-8 データ・ネットワークポータル https://dncom.spring8.or.jp/

ご覧いただきありがとうございました。