AWS基盤
インフラ仕様書

トランコムITS ISグループ

0.1版
2019年 6月

改版履歴

版数	概要	改版シート	内容
0.1	新規作成	-	-

目次

- 本資料の目的
- ネットワーク構成概要
- サーバ環境基本仕様
- 共通機能一覧(インフラ管理)
  - パフォーマンスモニタ項目(リソース管理)
  - セキュリティグループ方針(セキュリティ対策)
  - 社外からのアクセスについて(リモートアクセス)
- 責任境界の考え方
- 個別インフラ機能について

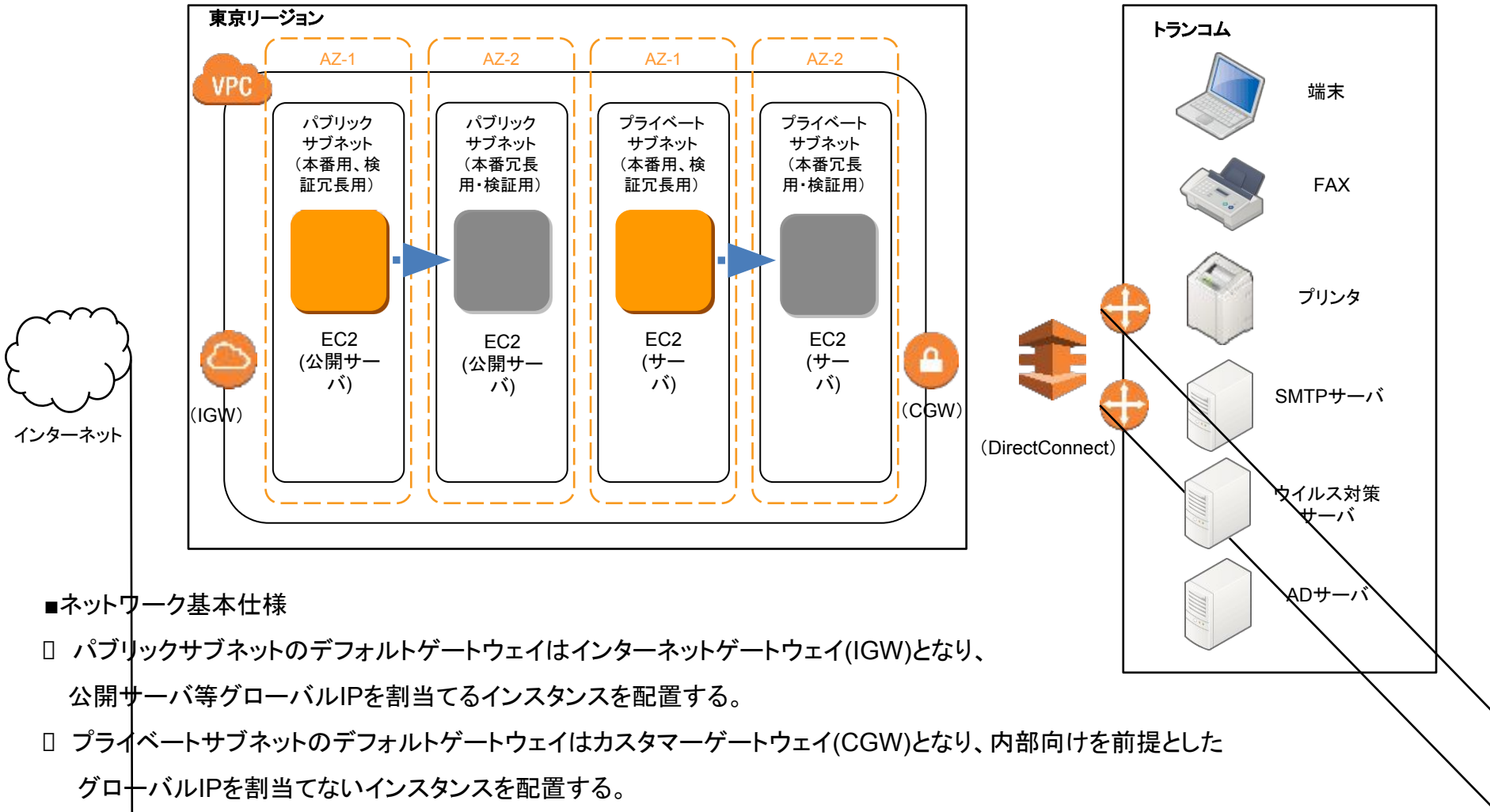
本資料の目的

本資料は、トランコムグループで利用しているAWSのインフラ面における仕様や共通的に適用する機能を明示しています。

トランコムグループでは新システムに対して、AWS上にシステム構築する事を
標準として定め、AWS上に構築するシステムに対して、本資料で説明する
共通的なインフラ機能を標準化し、インフラ部門にて実装しております。

仕様を明示する目的は、社内開発メンバー及び
SIベンダー様(NDA等締結済)が、
インフラ面で考慮すべき事 / 検討すべき事 / 実施すべき事を把握し、
システム導入の検討を補完頂く事を期待するものとなります。

ネットワーク構成概要



■ネットワーク基本仕様

- パブリックサブネットのデフォルトゲートウェイはインターネットゲートウェイ(IGW)となり、
  公開サーバ等グローバルIPを割当てるインスタンスを配置する。
- プライベートサブネットのデフォルトゲートウェイはカスタマーゲートウェイ(CGW)となり、内部向けを前提とした
  グローバルIPを割当てないインスタンスを配置する。
- それぞれのサブネットは冗長用のサブネットが存在している。冗長構成とする場合はこのサブネットを利用する。
- 社内ネットワークへの接続は CGWからDirectConnect 接続を用いており、社内網のネットワークに直収されている。

サーバ環境基本仕様

■サーバ(EC2)基本仕様

- システム領域、データ領域ごとに ストレージを分ける
- システム領域、データ領域の ストレージタイプ、サイズは業務要件により検討
- トランコムグループで共通運用となる監視 /ジョブ管理エージェント、ウィルス対策 S/W、資産管理S/Wを導入とする。

※ウィルス対策 S/W、資産管理S/WはWindowsのみ

- DNS参照先は社内ActiveDirectoryサーバとする。(ドメインは基本参加)

※ドメイン不参加のサーバ (Unix系やその他事由)は個別検討とする

- NTP同期先はActiveDirectoryサーバ(ドメイン参加)となる。

※ドメイン不参加のサーバ (Unix系やその他事由)は個別検討とする

- インフラ共通運用で使用するスクリプトを実行する為、 AWS CLI、Pythonの実行環境を導入とする。
- 各サーバごとにセキュリティグループの適用を行う 。

共通運用となる通信は共通のセキュリティグループを割当てて通信許可としており、
後は各システムに必要な通信を個別セキュリティグループとして作成し、割り当てる必要がある。

■その他(AWS関連)

- AWSマネージドコンソールは インフラメンバーの管理下 となります。

AWSのマネージドサービスを利用する場合は 構成からの協議/検討となる

共通機能一覧(インフラ管理)

□　各システムに共通で適用する機能（1／2）

項番	共通機能名	説明
1	リソース管理	サーバのパフォーマンス情報を取得する。パフォーマンスモニタで採取する項目は別ページにて記載（Linuxはsarコマンドで取得可能な項目全て） 基本は1分間隔で取得。
2	ログ管理	Windowsはイベントログとパフォーマンスログ、Linuxは/var/log配下のシスログとパフォーマンスログ。 日次(基本は5:00～6:00実施)で取得し、1年間保存(変更不可)。 ※ログ収集実施時間は業務要件により変更可
3	障害監視	死活監視(5分間隔で監視) リソース閾値監視(毎分監視【通報は5回連続失敗時のみ】) イベントログ(システム、アプリケーション)監視 ※イベントログはリアルタイムで、「重大」「エラー」「警告」を監視
4	ジョブ管理	バックアップ/ログ管理(収集/削除)。運用監視サーバのHinemosから実施。
5	バックアップ・リストア (OSレベル)	AWSのスナップショット機能を利用したシステムバックアップを日次 (基本は6:00～7:00実施)で取得。 ※システムバックアップ取得時間は業務要件により変更可 ※RPOは直近の日次バックアップ、世代数は基本は 2世代(変更可) 静止点確保(DBバックアップ取得)等はシステムバックアップとして 個別機能として検討が必要となります。(外部保存先等は提供可)

共通機能一覧(インフラ管理)

□　各システムに共通で適用する機能（2／2）

項番	共通機能名	説明
6	メール送信 (通知)	社内共通のリレーサーバにて上記運用の通知メールをサポートデスク宛へ送信 システムからメール送信を行う場合は利用可否含め、個別検討 とする
7	セキュリティ対策	エンドポイントのウイルス対策はトランコム標準のS/W(Symantec Endpoint Protection)にて実施。 またセキュリティグループにてアクセス制御を実施。共通機能で必要となる通信許可はされており、上記以外のインバウンド・アウトバンド通信は個別に設定が必要。
8	リモートアクセス	SI開発ベンダー様などを想定したトランコム社外からのアクセスは、 踏み台サーバ経由でのアクセスのみを許可 とさせて頂きます。 送信元IPを特定(固定グローバル)とSSH通信が利用可能な環境が前提となります。 トランコム社内からのアクセスは、直接サーバへログイン可能
9	その他共通管理	ドメイン参加(Windowsのみ)、資産管理、時刻同期など

上記以外の機能はシステム個別に検討する必要あり

【参考】パフォーマンスモニタ項目(リソース管理)

TRANCOM VISION 2020

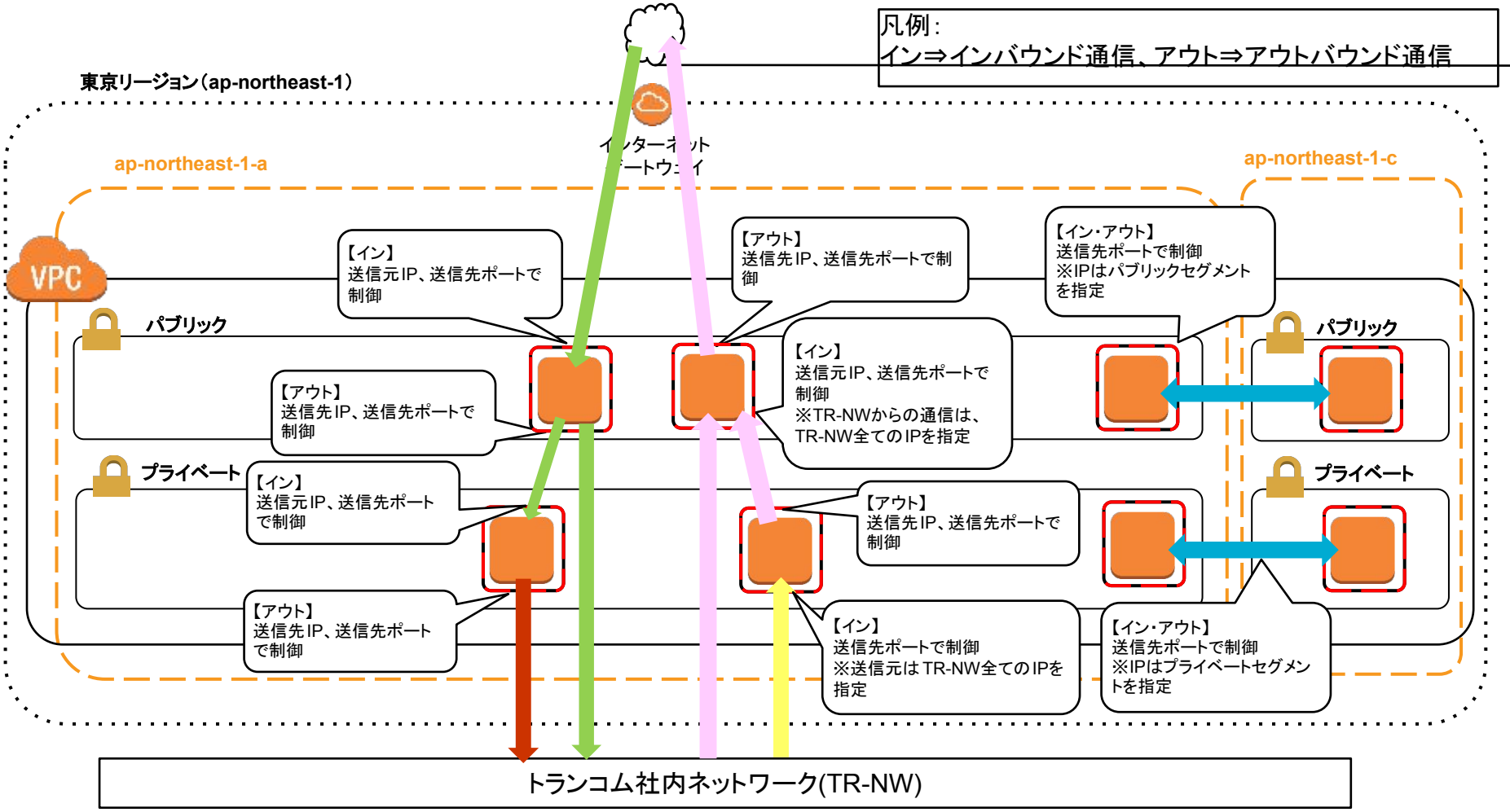
パフォーマンスモニタ(Windows)で取得する項目

項番	項目	説明	SQL Server 未導入サーバ	SQL Server 導入サーバ
1	LogicalDisk(*)\Avg. Disk Queue Length	ディスク読み書き待ち数	○	○
2	LogicalDisk(*)\Disk Transfers/sec	秒あたりのI/Oリクエスト数(IOPS)	○	○
3	LogicalDisk(*)\% Free Space	ディスクの空き率	○	○
4	Memory\Available Kbytes	メモリの空き容量(単位はByte)	○	○
5	Memory\Pool Nonpaged Bytes	物理メモリ内に存在するオブジェクト用のシステムメモリサイズ(単位はByte)	○	○
6	Memory\Pages/sec	秒あたりのページング回数(単位は回数)	○	○
7	Network Interface(*)\Bytes Received/sec	秒あたりの受信バイト数	○	○
8	Network Interface(*)\Bytes Total/sec	秒あたりの送受信バイト数	○	○
9	Process(*)\IO Data Operations/sec	プロセスがファイルやネットワークに対してI/O処理を実施している数(全プロセスの合計数)	○	○
10	Process(*)\% Processor Time	プロセス毎のCPU使用率	○	○
11	Process(*)\Working Set	プロセス毎のメモリ使用量(単位 Byte)。Private BytesとSharable Bytesの合計。	○	○
12	Processor(*)\% User Time	アプリケーションのCPU使用率	○	○
13	Processor(*)\% Privileged Time	OSのCPU使用率	○	○
14	Processor(*)\% Idle Time	CPU空き率	○	○
15	System\Processor Queue Length	プロセッサの実行待ちの回数	○	○
16	SQLServer:Buffer Manager\Buffer cache hit ratio	キャッシュヒット率(ディスクから読み取る必要がないページの比率)	―	○
17	SQLServer:Memory Manager\Total Server Memory (KB)	SQL Serverがコミット(使っているか否かにかかわらず確保)したサイズ	―	○
18	SQLServer:Transactions\Transactions	現在のアクティブなトランザクション数	―	○

【参考】セキュリティグループ方針(セキュリティ対策)

セキュリティグループ設計

- インバウンド、アウトバウンドともに、原則通信不可とし、 必要なアクセスのみ 許可する
- OS標準のファイアウォール機能は 使用しない



【参考】社外からのアクセスについて(リモートアクセス)

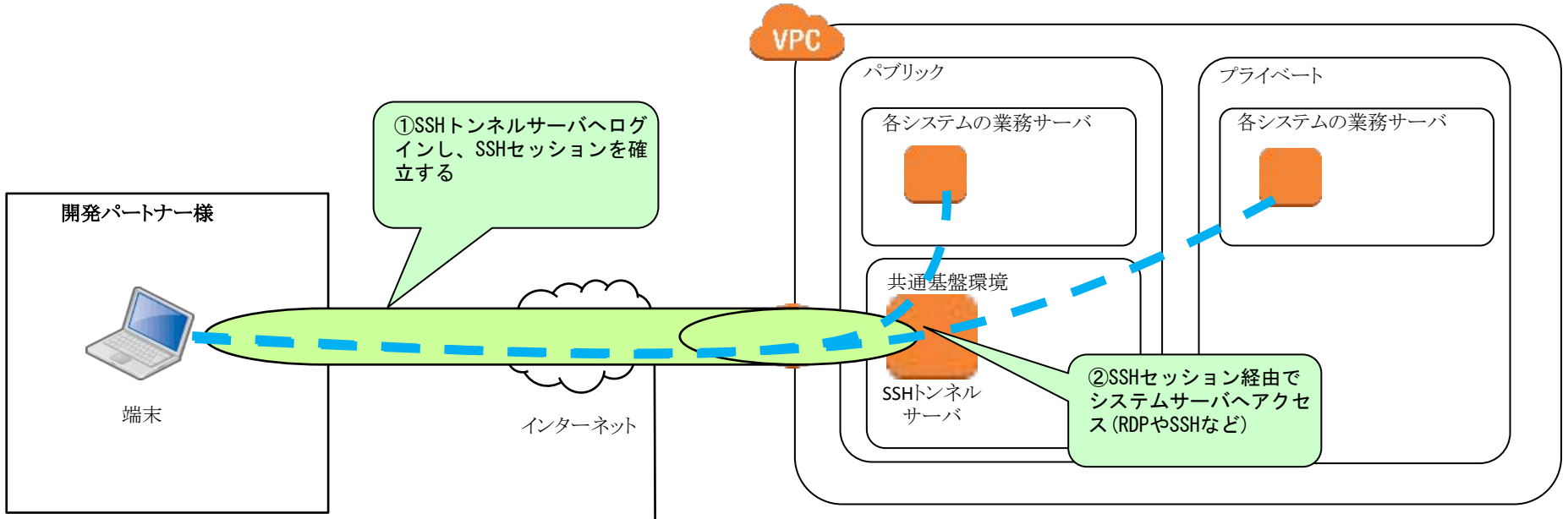
リモートアクセス機能の提供について

開発パートナー様向けなど、外部からの保守用アクセスに対応する為、 SSHポートフォワーディング機能を使って

リモート接続環境を提供します。大まかな接続条件は以下となります。

・送信元を特定する為、固定のグローバル IPからのアクセスである事

・弊社が用意する公開踏み台サーバ (SSHトンネルサーバ)へのSSH接続(TCP/22)が可能な事



※本接続を実施する際には簡易の手順書等をお渡しいたします

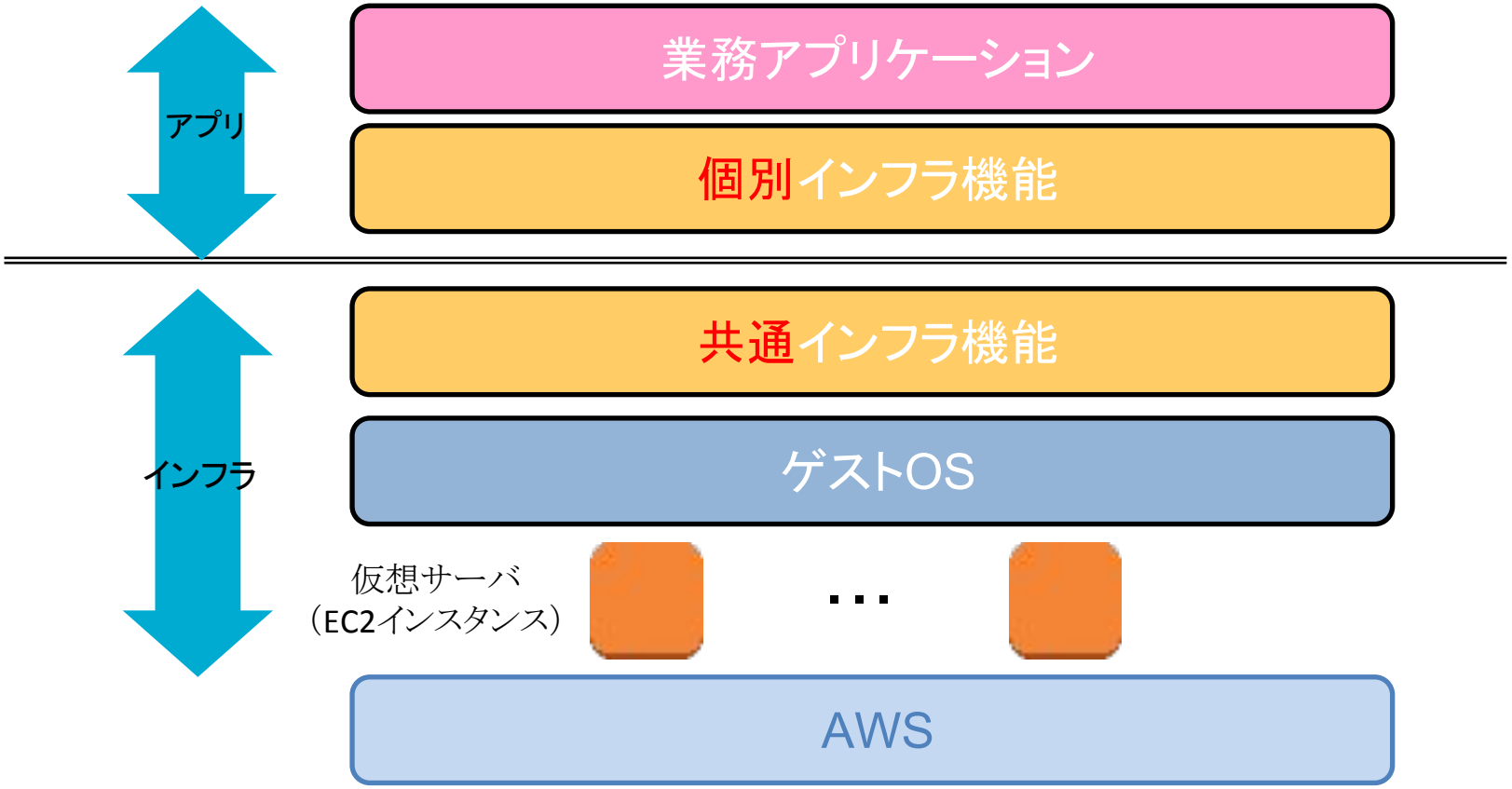
責任境界の考え方

責任境界の考え方

インフラ: AWS上に仮想サーバを切り出し、共通インフラ機能の導入設定までを行う。

アプリ: 各システムの要件により導入要否や設計内容が異なるインフラ機能の個別対応 (※)を行う

※アプリが全てを実施すると言う事では無く、システムとして必要な要件を確認し、インフラと共に実装する



個別インフラ機能について

TRANCOM VISION 2020

- 下記はシステム個別で検討が必要なインフラ機能の例です。

項番	機能名	説明
1	冗長化	ロードバランサーを使った負荷分散やDRの構築といった冗長構成を組み、サーバが1台停止してもサービス停止しないようにする。
2	アプリケーション 実行環境	Tomcatなど、業務アプリケーションを実行する環境。 Webアクセス時のhttps利用(サーバ証明書)要否。
3	ジョブ実行環境	業務バッチを実行する環境。(インフラで運用の Hinemosを利用も可)
4	データベース環境	Oracleなど、データベース環境。EC2(仮想サーバ)の構築方法とRDS(AWSのマネージドサービス)の構築方法等あり
5	ログ管理	システム管理対象ログファイル等の管理 インフラ共通の仕掛けを使って 収集対象ディレクトリへ格納頂く事で自動収集が可能 となります。
6	障害監視	ログファイル監視(リアルタイムでキーワード出力有無を監視) サービス監視(5分間隔など、定期的にサービスの死活を監視) プロセス(5分間隔など、定期的にプロセスの死活を監視) URL(5分間隔など、定期的にURLのレスポンスタイムを監視)
7	バックアップ・リストア (データ)	データベースなど、システムデータのバックアップ。 保管先としてはAmazon S3を用意可能 。(保管・世代管理も含む)
8	セキュリティ対策	システムで必要となる通信(インバウンドおよびアウトバウンド)を 個別セキュリティグループとして設定 する。

以　　上