aws-three-tier-parameter-sheet.xlsx ／ 00_概要

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E
1	分類	項目	内容	値の区分	補足
2	基本情報	システム名	AWS三層構成 Webアプリケーション（設計サンプル）	Work 01準拠	Work 01 と同じ環境を対象にする
3	基本情報	環境名	sample（ポートフォリオ用の設計サンプル）	設計上の仮値	本番環境・検証環境ではない
4	基本情報	AWSリージョン	ap-northeast-1（東京）	Work 01準拠	Work 01 構成図・資料1.
5	基本情報	構成概要	1つのVPCで2つのAZを使い、Web層（ALB）／アプリケーション層（EC2×2）／データベース層（RDS for MySQL・Single-AZ）を配置する。インターネットに公開するのはALBだけ。NAT Gatewayは置かず、管理用のSSHは EC2 Instance Connect Endpoint、OSの更新は S3 の Gateway VPC Endpoint を経由する	Work 01準拠	Work 01 資料1.〜4.
6	基本情報	使用サービス	Amazon VPC（Public / Private Subnet、ルートテーブル）、Internet Gateway、Application Load Balancer、Amazon EC2、Amazon RDS for MySQL、Security Group、EC2 Instance Connect Endpoint、Gateway VPC Endpoint（S3）	Work 01準拠	Work 01 資料3.
7	基本情報	作成日	2026-11-06		
8	基本情報	作成者	Nami		
9	基本情報	資料の区分	自主制作サンプル（ポートフォリオ用）		実際の業務案件で作成したものではない
10	基本情報	構築状況	AWSアカウントへの構築・動作確認は行っていない		VPC ID・Security Group ID などのリソースIDは、実環境がないと決まらないため記載していない
11	基本情報	対象の構成図	Work 01「AWS三層構成アーキテクチャ図」（portfolio/three-tier-architecture/）		
12	共通設定	命名規則	sample-3tier-<種類>-<役割>-<AZ>（例：sample-3tier-subnet-app-a）	設計上の仮値	Work 01 には名前の記載がないため仮に決めた規則。名前（黄色のセル）はすべて設計上の仮値
13	共通設定	VPCのDNS解決	有効	Work 01準拠	Gateway VPC Endpoint とRDSのエンドポイント（DNS名）を使うために必要（Work 01 資料10.）
14	共通設定	VPCのDNSホスト名	有効	Work 01準拠	Work 01 資料10.
15	共通設定	NAT Gateway	配置しない	Work 01準拠	EC2からインターネットへは直接通信できない（Work 01 資料9.）
16	共通設定	SGの既定の送信ルール	作成時に自動で入る「すべての送信を許可」ルールは削除し、03_SecurityGroup のルールだけにする	Work 01準拠	Security Groupは必要最小限の通信だけを許可する（Work 01 資料6.）
	共通設定	このシートの対象外	ALBのリスナー・証明書・ターゲットグループの詳細、IAMポリシーの内容、ドメイ	要確認	要件が決まってから追加する

17			ンとDNSレコード		
18	**凡例**	**値の区分：Work 01準拠**	Work 01 の構成図・構成説明資料に書かれている値	**Work 01準拠**	
19	**凡例**	**値の区分：設計上の仮値**	Work 01 に記載がなく、説明のために仮に決めた値。構築時に見直す	**設計上の仮値**	セルは黄色
20	**凡例**	**値の区分：要確認**	実環境や要件が決まらないと確定できない値。推測で値を入れていない	**要確認**	セルは赤
21	**凡例**	**列の色**	濃紺の見出し＝設定値の列、青の見出しと灰色のセル＝根拠・説明の列		値の区分は一覧から選べる（入力規則）
22	**集計**	**Work 01準拠の件数**	**49件**		00〜06シートの「値の区分」を数える（数式）
23	**集計**	**設計上の仮値の件数**	**14件**		同上
24	**集計**	**要確認の件数**	**11件**		構築前に確認・決定が必要な項目の数
25	**集計**	**インターネットからの受信を許可しているSGルール**	**1件**		03_SecurityGroup から数える。この構成では SG-ALB の443番の1件だけ
26	**集計**	**そのうち443番以外のルール**	**0件**		0件であること（1件以上なら03_SecurityGroupの「要注意」の行を確認）

00_概要 | 01_VPC・Subnet | 02_RouteTable | 03_SecurityGroup | 04_EC2 | 05_RDS | 06_VPC_Endpoint | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 01_VPC・Subnet

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F	G	H	I	J	K
1	**No**	**VPC名**	**CIDR (VPC)**	**Subnet名**	**Availability Zone**	**Subnet CIDR**	**Public / Private**	**用途**	**関連するルートテーブル**	**値の区分**	**根拠・備考**
2	1	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-public-a	ap-northeast-1a	10.0.0.0/24	Public	ALB（AZ-Aのノード）	sample-3tier-rt-public	**Work 01準拠**	Work 01 構成図・資料3.。ALBには2つ以上のAZのサブネットが必要で、各サブネットは /27 以上（/24 で満たす）
3	2	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-public-c	ap-northeast-1c	10.0.1.0/24	Public	ALB（AZ-Cのノード）	sample-3tier-rt-public	**Work 01準拠**	Work 01 構成図・資料3.
4	3	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-app-a	ap-northeast-1a	10.0.10.0/24	Private	EC2（sample-3tier-web-a） EC2 Instance Connect Endpoint	sample-3tier-rt-app	**Work 01準拠**	Work 01 構成図・資料3.。インターネットへの経路を持たない。パブリックIPの自動割り当ては無効にする
5	4	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-app-c	ap-northeast-1c	10.0.11.0/24	Private	EC2（sample-3tier-web-c）	sample-3tier-rt-app	**Work 01準拠**	Work 01 構成図・資料3.。パブリックIPの自動割り当ては無効にする
6	5	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-db-a	ap-northeast-1a	10.0.20.0/24	Private	RDS（Single-AZのDBインスタンス）	sample-3tier-rt-db	**Work 01準拠**	Work 01 構成図・資料3.。DBサブネットグループに含める
7	6	sample-3tier-vpc	10.0.0.0/16	sample-3tier-subnet-db-c	ap-northeast-1c	10.0.21.0/24	Private	DBサブネットグループ用（インスタンスなし。Multi-AZ化するときのスタンバイ配置先）	sample-3tier-rt-db	**Work 01準拠**	Single-AZでも、DBサブネットグループには2つのAZのサブネットが必要（Work 01 資料7.）

00_概要 | **01_VPC・Subnet** | 02_RouteTable | 03_SecurityGroup | 04_EC2 | 05_RDS | 06_VPC_Endpoint | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 02_RouteTable

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F	G	H
1	**No**	**ルートテーブル名**	**関連Subnet**	**Destination**	**Target**	**用途・説明**	**値の区分**	**根拠・備考**
2	1	sample-3tier-rt-public	sample-3tier-subnet-public-a sample-3tier-subnet-public-c	10.0.0.0/16	local	VPC内の通信（ルートテーブル作成時に自動で入る経路）	**Work 01準拠**	Work 01 資料4. ルートテーブル
3	2	sample-3tier-rt-public	sample-3tier-subnet-public-a sample-3tier-subnet-public-c	0.0.0.0/0	Internet Gateway（sample-3tier-igw）	インターネットとの通信。ALBが利用者からのHTTPSを受けるために必要。この経路があるサブネットがPublic Subnet	**Work 01準拠**	Work 01 構成図（RT: 0.0.0.0/0 → IGW）・資料5.
4	3	sample-3tier-rt-app	sample-3tier-subnet-app-a sample-3tier-subnet-app-c	10.0.0.0/16	local	ALB・RDS・EC2 Instance Connect Endpoint との通信	**Work 01準拠**	Work 01 資料4.。NAT Gatewayを置かないため、0.0.0.0/0 の経路は設定しない
5	4	sample-3tier-rt-app	sample-3tier-subnet-app-a sample-3tier-subnet-app-c	S3のプレフィックスリスト（com.amazonaws.ap-northeast-1.s3）	Gateway VPC Endpoint（sample-3tier-vpce-s3）	OSパッケージの更新（dnf）。Gateway Endpointをこのルートテーブルに関連付けると自動で追加される	**Work 01準拠**	Work 01 構成図（RT: S3 → Gateway VPCE）・資料4-3。プレフィックスリストのID（pl-で始まる値）は構築時に決まるため記載しない
6	5	sample-3tier-rt-db	sample-3tier-subnet-db-a sample-3tier-subnet-db-c	10.0.0.0/16	local	VPC内の通信のみ。インターネットへの経路は持たない	**Work 01準拠**	Work 01 構成図（RT: local のみ）・資料4.

00_概要 | 01_VPC・Subnet | **02_RouteTable** | 03_SecurityGroup | 04_EC2 | 05_RDS | 06_VPC_Endpoint | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 03_SecurityGroup

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F	G	H	I	J	K
1	No	Security Group名	対象リソース	Inbound / Outbound	プロトコル	ポート番号	送信元・宛先	許可理由	インターネット公開チェック	値の区分	根拠・備考
2	1	SG-ALB	Application Load Balancer	Inbound	TCP	443	0.0.0.0/0	利用者からのHTTPSを受け付ける。インターネットに公開するのはこのルールだけ	公開（HTTPSのみ）	Work 01準拠	Work 01 資料6.
3	2	SG-ALB	Application Load Balancer	Outbound	TCP	80	SG-App	EC2への転送とヘルスチェック	—	Work 01準拠	Work 01 資料6.。AWSのALB推奨ルール（宛先はインスタンスのSG）に沿う
4	3	SG-App	EC2（sample-3tier-web-a / sample-3tier-web-c）	Inbound	TCP	80	SG-ALB	ALBからの転送とヘルスチェックだけを受ける	—	Work 01準拠	Work 01 資料6.
5	4	SG-App	EC2（sample-3tier-web-a / sample-3tier-web-c）	Inbound	TCP	22	SG-EICE	管理者のSSH。EC2 Instance Connect Endpoint からだけ受ける（インターネットには開けない）	—	Work 01準拠	Work 01 資料6.
6	5	SG-App	EC2（sample-3tier-web-a / sample-3tier-web-c）	Outbound	TCP	3306	SG-DB	RDS（MySQL）への接続	—	Work 01準拠	Work 01 資料6.
7	6	SG-App	EC2（sample-3tier-web-a / sample-3tier-web-c）	Outbound	TCP	443	S3のプレフィックスリスト（com.amazonaws.ap-northeast-1.s3）	OSパッケージの更新（Gateway VPC Endpoint 経由でS3へ）	—	Work 01準拠	Work 01 資料6.。AWSの手順ではHTTPとHTTPSの送信許可が案内されているため、80番が必要な場合は同じ宛先に80/TCPを追加する
8	7	SG-DB	RDS（sample-3tier-db）	Inbound	TCP	3306	SG-App	EC2のアプリケーションからのDB接続だけを受ける	—	Work 01準拠	Work 01 資料6.
9	8	SG-DB	RDS（sample-3tier-db）	Outbound	—	—	（ルールなし）	送信ルールは不要（SGはステートフルのため、応答は自動で返る）	—	Work 01準拠	Work 01 資料6.
10	9	SG-EICE	EC2 Instance Connect Endpoint	Inbound	—	—	（ルールなし）	受信ルールは不要（エンドポイントへの接続はSGにかかわらず届き、接続できる人はIAMで制御する）	—	Work 01準拠	Work 01 資料6.（AWS公式ドキュメントに基づく）
11	10	SG-EICE	EC2 Instance Connect Endpoint	Outbound	TCP	22	SG-App	EC2へのSSH	—	Work 01準拠	Work 01 資料6.

00_概要 | 01_VPC・Subnet | 02_RouteTable | **03_SecurityGroup** | 04_EC2 | 05_RDS | 06_VPC_Endpoint | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 04_EC2　　自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F
1	分類	項目	EC2 #1（AZ-A）	EC2 #2（AZ-C）	値の区分	根拠・説明
2	基本	インスタンス名	sample-3tier-web-a	sample-3tier-web-c	設計上の仮値	00_概要の命名規則に沿った仮の名前
3	基本	AMI（OS）	Amazon Linux 2023	Amazon Linux 2023	Work 01準拠	Work 01 資料4-3の前提。OSの更新を S3 の Gateway VPC Endpoint 経由で行うため
4	基本	AMI ID	構築時に最新のAMI IDを確認	構築時に最新のAMI IDを確認	要確認	AMI IDは実環境で確認する値のため、推測で記載しない
5	基本	インスタンスタイプ	t3.micro	t3.micro	設計上の仮値	説明用の仮の値。アプリの負荷と料金（EC2の料金ページ）を確認して決める
6	ネットワーク	配置Subnet	sample-3tier-subnet-app-a（10.0.10.0/24）	sample-3tier-subnet-app-c（10.0.11.0/24）	Work 01準拠	Work 01 構成図・資料3.（Private Subnet（App））
7	ネットワーク	Availability Zone	ap-northeast-1a	ap-northeast-1c	Work 01準拠	Work 01 構成図
8	ネットワーク	Security Group	SG-App	SG-App	Work 01準拠	Work 01 資料6.（詳細は 03_SecurityGroup）
9	ネットワーク	パブリックIP設定	割り当てない	割り当てない	Work 01準拠	インターネットから直接アクセスさせない（Work 01 資料2.）
10	ストレージ（EBS）	ボリュームタイプ	gp3	gp3	設計上の仮値	説明用の仮の値
11	ストレージ（EBS）	サイズ	20 GiB	20 GiB	設計上の仮値	説明用の仮の値。アプリとログの容量で決める
12	ストレージ（EBS）	暗号化	有効	有効	Work 01準拠	Work 01 資料8.-4
13	ストレージ（EBS）	終了時に削除	有効	有効	設計上の仮値	説明用の仮の値
14	権限	IAMロール	sample-3tier-ec2-role（付与する権限は要確認）	sample-3tier-ec2-role（付与する権限は要確認）	要確認	必要最小限の権限にする（Work 01 資料8.-6）。権限の内容はアプリの要件が決まってから決める。ロール名は仮の名前
15	その他	管理者の接続方法	EC2 Instance Connect Endpoin	EC2 Instance Connect Endpoin	Work 01準拠	Work 01 資料4-2。AZ-CのEC2もAZ-AのEndpointから接続する

			t 経由のSSH（22）	t 経由のSSH（22）		
16	**その他**	**キーペア**	要確認	要確認	**要確認**	EC2 Instance Connect で一時的な鍵を送るか、キーペアを使うかを構築時に決める（Work 01 資料10.）
17	**その他**	**インスタンスメタデータ**	IMDSv2 を必須にする	IMDSv2 を必須にする	**設計上の仮値**	Work 01 に記載なし。セキュリティを考えた仮の設定
18	**その他**	**Webサーバーの待ち受けポート**	80（HTTP）	80（HTTP）	**Work 01準拠**	ALBからHTTP 80で転送される（Work 01 資料4-1）
19	**その他**	**ALBのターゲット登録**	登録する（HTTP:80）	登録する（HTTP:80）	**Work 01準拠**	ヘルスチェックのパスはアプリが決まってから設定する（要確認）

aws-three-tier-parameter-sheet.xlsx ／ 05_RDS

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E
1	分類	項目	設定値	値の区分	根拠・説明
2	基本	DB識別子	sample-3tier-db	設計上の仮値	00_概要の命名規則に沿った仮の名前
3	基本	エンジン	MySQL（Amazon RDS for MySQL）	Work 01準拠	Work 01 構成図・資料3.
4	基本	エンジンのバージョン	要確認	要確認	サポート期間とアプリの対応状況を確認して決める
5	基本	インスタンスクラス	db.t3.micro	設計上の仮値	説明用の仮の値。利用できるクラスと料金を構築時に確認する
6	ネットワーク	DBサブネットグループ	sample-3tier-db-subnet-group（sample-3tier-subnet-db-a / sample-3tier-subnet-db-c）	Work 01準拠	Single-AZでも2つのAZのサブネットが必要（Work 01 資料7.）。名前は仮の名前
7	ネットワーク	配置AZ	ap-northeast-1a	Work 01準拠	Work 01 構成図（AZ-AのPrivate Subnet（DB））
8	ネットワーク	Security Group	SG-DB	Work 01準拠	Work 01 資料6.（詳細は 03_SecurityGroup）
9	ネットワーク	パブリックアクセス	なし	Work 01準拠	Work 01 資料8.-1
10	ネットワーク	ポート	3306	Work 01準拠	MySQLのポート（Work 01 資料4-1・6.）
11	ネットワーク	接続先	エンドポイント（DNS名）で接続する	Work 01準拠	IPアドレスではなくDNS名で接続する（Work 01 資料7.）。エンドポイント名は構築時に決まる
12	ストレージ	ストレージタイプ	gp3	設計上の仮値	説明用の仮の値
13	ストレージ	割り当て容量	20 GiB	設計上の仮値	説明用の仮の値。データ量の見込みで決める
14	ストレージ	ストレージの暗号化	有効	Work 01準拠	Work 01 資料8.-4
15	ストレージ	ストレージの自動拡張	要確認	要確認	データ量の増え方と費用を見て決める

16	バックアップ	自動バックアップ	有効	Work 01準拠	Work 01 資料7.（スナップショット・特定時点への復元）
17	バックアップ	バックアップの保持期間	7日	設計上の仮値	説明用の仮の値。保存容量に料金がかかる場合がある
18	バックアップ	バックアップの時間帯	要確認	要確認	利用の少ない時間帯を要件から決める
19	可用性	Multi-AZ設定	使用しない（Single-AZ）	Work 01準拠	費用を優先（Work 01 資料2.・9.）。AZ-Aの障害時はDBが止まる。止められないサービスではMulti-AZ配置にする
20	運用	メンテナンスの時間帯	要確認	要確認	利用の少ない時間帯を要件から決める
21	運用	削除保護	有効	設計上の仮値	Work 01 に記載なし。誤って削除しないための仮の設定
22	認証	マスターユーザー名	要確認	要確認	構築時に決める
23	認証	パスワードの管理	コードやサーバー上のファイルに直接書かない（保管方法は要確認）	要確認	AWS Secrets Manager などの利用は、費用と要件で判断する（Work 01 資料8.-5）

00_概要 | 01_VPC・Subnet | 02_RouteTable | 03_SecurityGroup | 04_EC2 | **05_RDS** | 06_VPC_Endpoint | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 06_VPC_Endpoint

自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F	G	H	I	J	K
1	No	Endpoint名	サービス名	Endpointタイプ	接続先	関連ルートテーブル またはSubnet	Security Group	用途	エンドポイント ポリシー	値の区分	根拠・備考
2	1	sample-3tier-eice	EC2 Instance Connect Endpoint	EC2 Instance Connect Endpoint	VPC内のEC2（sample-3tier-web-a / sample-3tier-web-c）へのSSH（22）	Subnet：sample-3tier-subnet-app-a（10.0.10.0/24・ap-northeast-1a）	SG-EICE	管理者がEC2に接続する入口。踏み台サーバーが不要	—（接続できる人はIAMポリシーで制御）	Work 01準拠	Work 01 資料3.・4-2。VPCに1つまで。同時接続は20まで、1回の接続は最大1時間。追加料金なし（AZをまたぐデータ転送は課金）
3	2	sample-3tier-vpce-s3	com.amazonaws.ap-northeast-1.s3	Gateway	Amazon S3（Amazon Linux 2023 のパッケージリポジトリ）	ルートテーブル：sample-3tier-rt-app	—（Gateway型は Security Group を使わない）	EC2のOSパッケージ更新（dnf）。インターネットを通らずにS3へ接続する	要確認：既定はフルアクセス。絞る場合は、Amazon Linux 2023 のリポジトリ用バケット（al2023-repos-ap-northeast-1-de612dc2）の読み取りを許可する	要確認	Work 01 資料3.・4-3。追加料金なし。バケット名は AWS re:Post Knowledge Center の手順に基づく。ポリシーの内容は構築時に確認する

00_概要 | 01_VPC・Subnet | 02_RouteTable | 03_SecurityGroup | 04_EC2 | 05_RDS | **06_VPC_Endpoint** | 07_設定一覧

aws-three-tier-parameter-sheet.xlsx ／ 07_設定一覧　　自主制作サンプル（AWSへの構築は行っていない設計サンプル）・Excelの内容から作成したプレビュー

	A	B	C	D	E	F
1	No	カテゴリ	項目	設定値（各シートから参照）	値の区分	参照元シート
2	1	概要	AWSリージョン	ap-northeast-1（東京）	Work 01準拠	00_概要
3	2	概要	環境名	sample（ポートフォリオ用の設計サンプル）	設計上の仮値	00_概要
4	3	概要	命名規則	sample-3tier-<種類>-<役割>-<AZ>（例：sample-3tier-subnet-app-a）	設計上の仮値	00_概要
5	4	VPC	VPC CIDR	10.0.0.0/16	Work 01準拠	01_VPC・Subnet
6	5	VPC	DNS設定	DNS解決：有効 ／ DNSホスト名：有効	Work 01準拠	00_概要
7	6	VPC	NAT Gateway	配置しない	Work 01準拠	00_概要
8	7	Subnet	Public Subnet（AZ-A）	10.0.0.0/24（ap-northeast-1a・Public）	Work 01準拠	01_VPC・Subnet
9	8	Subnet	Public Subnet（AZ-C）	10.0.1.0/24（ap-northeast-1c・Public）	Work 01準拠	01_VPC・Subnet
10	9	Subnet	Private Subnet（App・AZ-A）	10.0.10.0/24（ap-northeast-1a・Private）	Work 01準拠	01_VPC・Subnet
11	10	Subnet	Private Subnet（App・AZ-C）	10.0.11.0/24（ap-northeast-1c・Private）	Work 01準拠	01_VPC・Subnet
12	11	Subnet	Private Subnet（DB・AZ-A）	10.0.20.0/24（ap-northeast-1a・Private）	Work 01準拠	01_VPC・Subnet
13	12	Subnet	Private Subnet（DB・AZ-C）	10.0.21.0/24（ap-northeast-1c・Private）	Work 01準拠	01_VPC・Subnet
14	13	RouteTable	経路 1	sample-3tier-rt-public：10.0.0.0/16 → local	Work 01準拠	02_RouteTable
15	14	RouteTable	経路 2	sample-3tier-rt-public：0.0.0.0/0 → Internet Gateway（sample-3tier-igw）	Work 01準拠	02_RouteTable
16	15	RouteTable	経路 3	sample-3tier-rt-app：10.0.0.0/16 → local	Work 01準拠	02_RouteTable
17	16	RouteTable	経路 4	sample-3tier-rt-app：S3のプレフィックスリスト（com.amazonaws.ap-northeast-1.s3） → Gateway VPC Endpoint（sample-3tier-vpce-s3）	Work 01準拠	02_RouteTable
18	17	RouteTable	経路 5	sample-3tier-rt-db：10.0.0.0/16 → local	Work 01準拠	02_RouteTable
19	18	SecurityGroup	ルール 1	SG-ALB Inbound：TCP/443 ← 0.0.0.0/0	Work 01準拠	03_SecurityGroup
20	19	SecurityGroup	ルール 2	SG-ALB Outbound：TCP/80 → SG-App	Work 01準拠	03_SecurityGroup
21	20	SecurityGroup	ルール 3	SG-App Inbound：TCP/80 ← SG-ALB	Work 01準拠	03_SecurityGroup
22	21	SecurityGroup	ルール 4	SG-App Inbound：TCP/22 ← SG-EICE	Work 01準拠	03_SecurityGroup
23	22	SecurityGroup	ルール 5	SG-App Outbound：TCP/3306 → SG-DB	Work 01準拠	03_SecurityGroup
24	23	SecurityGroup	ルール 6	SG-App Outbound：TCP/443 → S3のプレフィックスリスト（com.amazonaws.ap-northeast-1.s3）	Work 01準拠	03_SecurityGroup

25	24	**SecurityGroup**	**ルール 7**	SG-DB Inbound：TCP/3306 ← SG-App	**Work 01準拠**	03_SecurityGroup
26	25	**SecurityGroup**	**ルール 8**	SG-DB Outbound：ルールなし	**Work 01準拠**	03_SecurityGroup
27	26	**SecurityGroup**	**ルール 9**	SG-EICE Inbound：ルールなし	**Work 01準拠**	03_SecurityGroup
28	27	**SecurityGroup**	**ルール 10**	SG-EICE Outbound：TCP/22 → SG-App	**Work 01準拠**	03_SecurityGroup
29	28	**EC2**	**インスタンス名**	sample-3tier-web-a ／ sample-3tier-web-c	**設計上の仮値**	04_EC2
30	29	**EC2**	**AMI（OS）**	Amazon Linux 2023 ／ Amazon Linux 2023	**Work 01準拠**	04_EC2
31	30	**EC2**	**インスタンスタイプ**	t3.micro ／ t3.micro	**設計上の仮値**	04_EC2
32	31	**EC2**	**配置Subnet**	sample-3tier-subnet-app-a （10.0.10.0/24） ／ sample-3tier-subnet-app-c （10.0.11.0/24）	**Work 01準拠**	04_EC2
33	32	**EC2**	**パブリックIP**	割り当てない ／ 割り当てない	**Work 01準拠**	04_EC2
34	33	**EC2**	**EBSの暗号化**	有効 ／ 有効	**Work 01準拠**	04_EC2
35	34	**EC2**	**IAMロール**	sample-3tier-ec2-role （付与する権限は要確認） ／ sample-3tier-ec2-role （付与する権限は要確認）	**要確認**	04_EC2
36	35	**RDS**	**エンジン**	MySQL（Amazon RDS for MySQL）	**Work 01準拠**	05_RDS
37	36	**RDS**	**インスタンスクラス**	db.t3.micro	**設計上の仮値**	05_RDS
38	37	**RDS**	**DBサブネットグループ**	sample-3tier-db-subnet-group （sample-3tier-subnet-db-a / sample-3tier-subnet-db-c）	**Work 01準拠**	05_RDS
39	38	**RDS**	**配置AZ**	ap-northeast-1a	**Work 01準拠**	05_RDS
40	39	**RDS**	**Multi-AZ設定**	使用しない（Single-AZ）	**Work 01準拠**	05_RDS
41	40	**RDS**	**パブリックアクセス**	なし	**Work 01準拠**	05_RDS
42	41	**RDS**	**ポート**	3306	**Work 01準拠**	05_RDS
43	42	**RDS**	**ストレージの暗号化**	有効	**Work 01準拠**	05_RDS
44	43	**RDS**	**自動バックアップ**	有効	**Work 01準拠**	05_RDS
45	44	**RDS**	**バックアップの保持期間**	7日	**設計上の仮値**	05_RDS
46	45	**VPC Endpoint**	**EC2 Instance Connect Endpoint**	sample-3tier-eice（EC2 Instance Connect Endpoint） ／ Subnet：sample-3tier-subnet-app-a （10.0.10.0/24・ap-northeast-1a）	**Work 01準拠**	06_VPC_Endpoint

47	46	**VPC Endpoint**	**S3 Gateway VPC Endpoint**	sample-3tier-vpce-s3（Gateway）／ ルートテーブル：sample-3tier-rt-app	**要確認**	06_VPC_Endpoint