AWS Summit Japan 2026 ミニセッション
多くの現場で学んだ、
AWS共通基盤を「定着」させる7つのポイント

2026/6/25-6/26

株式会社NTTデータ

自己紹介

奥村 康晃（Okumura Yasuaki）

NTTデータ クラウド&データセンタ事業部 エグゼクティブITスペシャリスト

ミッション：

クラウド領域における技術リード

先進技術を用いた新規サービスの創出

クラウド人財育成

社外活動：

- 2022-25 APN AWS Top Engineers / 2023-25 AWS Ambassadors
  2025 AWS Top Ambassador(日本唯一)
- AWS Summit Tokyo 2023登壇など
- CodeZine:これだけは押さえておきたい！ AWSサービス最新アップデート[連載中]
- マイナビ Tech+:AWS Organizations連携サービス最新情報＆セットアップのコツ[連載中]

保有資格：

本セッションにおける「共通基盤」とは？

■ 定義

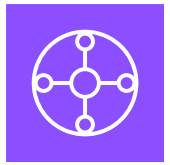
アマゾン ウェブ サービス（AWS）を全社／グループ横断で利用する際に**共通的に必要となる機能・ルール・標準構成の総称**

■ 含まれるもの

① 共通機能（システム基盤）

- アカウント管理（Control Tower等）機能
- 共通ネットワーク機能
- ログ・監視基盤
- セキュリティガードレール　など

AWS Control Tower



AWS Transit Gateway

AWS CloudTrail

② 共通ルール・ガイドライン

- アーキテクチャ標準
- 守るべきセキュリティポリシー
- IaCテンプレート　など

標準ガイドライン

セキュリティポリシー

IaC

共通基盤、こんなことで悩みませんか？

何から決めるべきか**わからない**

作っても**使われない**

セキュリティと利便性の**板挟み**

本日は、本当に使われる共通基盤を作るためのポイントについてお話しします！

アジェンダ

なぜ今、共通基盤が求められるのか
立ち上げの『罠』を避ける
設計の『要』を押さえる
運用の『責任』と『普及』
まとめ

アジェンダ

なぜ今、共通基盤が求められるのか

立ち上げの『罠』を避ける

設計の『要』を押さえる

運用の『責任』と『普及』

まとめ

なぜ今、共通基盤が求められるのか

まだ共通基盤がないケース

- 個別プロジェクト（部署）でパブリッククラウド利用が進んでおり、全社としてのガバナンスが維持できているかが不安
- 個別プロジェクトで同じような機能を作っていて、コスト最適の点で課題を感じている

もう共通基盤があるケース

- 最新のベストプラクティスに沿っているか不安なので作り直したい
- 既存の共通基盤の維持運用が辛く、マネージドサービスでの実現を考えたい

状況によらず、共通基盤を作るニーズが高まっている

アジェンダ

なぜ今、共通基盤が求められるのか

立ち上げの『罠』を避ける

設計の『要』を押さえる

運用の『責任』と『普及』

まとめ

ポイント１ ：ゼロから車輪の再発明をしない 1/2

- AWSから提示されている**「AWS 利用標準化ガイドライン策定のベストプラクティス」**をスタートラインとすることを推奨
- ガイドラインの章立て例も提示されており、共通基盤として求められる内容の網羅的な検討に役に立つ

AWS ブログ　ホーム　カテゴリ　エディション

Amazon Web Services ブログ

AWS 利用標準化ガイドライン策定のベストプラクティス

by Jumpei Noda | on 30 9月 2022 | in Best Practices, Enterprise governance and control, Management & Governance | Permalink | Share

組織で横断的に AWS の展開を進めていくにあたり、クラウド環境の統制、セキュリティ対策、品質の確保にお悩みではありませんか？

組織で AWS の利用を拡大する際には、それぞれの環境において確実に統制を効かせ、適切なセキュリティ対策を行い、品質のばらつきを抑えることが欠かせません。その際に有効なアプローチが AWS 利用標準化ガイドライン（以下「ガイドライン」と記載）の活用です。本ブログではガイドラインを策定し、有効に活用するためのベストプラクティスをご紹介します。

はじめに

多くの企業や政府機関において、クラウドの活用を加速する動きが加速しています。しかし、その過程において以下のような課題に直面するケースがあります。

- 設計・運用方針がバラバラで統制が取れていない
- セキュリティ対策が十分に実装されていない
- 担当者によって品質にバラつきがある
- 基盤機能が重複しており非効率

https://aws.amazon.com/jp/blogs/news/standardization-guideline-bestpractice-jp/

＜ガイドラインの章立て（例）＞

No	項目	含める内容	関連する AWS サービス
1	標準化ガイドライン	• ガイドラインの目的 • ガイドラインの対象範囲 • ガイドラインの運用	ー
2	アカウント設計	• AWS アカウントの構成 • アカウントの展開方法 • 組織・アカウント単位で行う統制の方針	AWS Organizations, AWS Control Tower
3	ネットワーク設計	• AWS 環境内のネットワーク構成 • オンプレミス環境との接続 • インターネット接続構成	Amazon VPC, AWS Transit Gateway, AWS Direct Connect, Amazon Route 53
4	アイデンティティ管理とアクセス管理	• AWS 環境における認証・認可 • 権限設計の方針 • ユーザー管理	AWS IAM, AWS IAM Identity Center(旧 AWS SSO)
5	発見的統制	• セキュリティ監視	AWS CloudTrail, AWS Config, Amazon GuardDuty, AWS Security Hub, Amazon Inspector
6	インフラストラクチャ保護	• データ漏洩対策 • インバウンド通信の保護 • アウトバウンド通信の制御	AWS Shield, AWS WAF, AWS Network Firewall
7	データ保護	• データの管理方法(アクセス制御, 保管設定) • 保管データの暗号化 • 通信データの暗号化	Amazon S3, Amazon Key Management Service(KMS), Amazon Certificate Manager(ACM)
8	監視	• AWS サービス稼働状況の監視 • リソースの稼働状況の監視	Amazon CloudWatch, AWS Trusted Advisor, AWS Health
9	ログ管理	• 取得するログ • ログの保管・管理	Amazon CloudWatch, Amazon S3
10	インシデント対応	• インシデント発生時の運用	Amazon EventBridge, AWS Config

ポイント１：ゼロから車輪の再発明をしない 2/2

- すべてをしっかりと検討すると時間を要するため、全項目を同じレベルで検討するのではなく、AWSアカウントの作成時に必要となる下記青色箇所を中心に検討いただくことを推奨

No	項目	含める内容	関連する AWS サービス
1	標準化ガイドライン	•ガイドラインの目的 •ガイドラインの対象範囲 •ガイドラインの運用	–
2	アカウント設計	•AWS アカウントの構成 •アカウントの展開方法 •組織・アカウント単位で行う統制の方針	AWS Organizations, AWS Control Tower
3	ネットワーク設計	•AWS 環境内のネットワーク構成 •オンプレミス環境との接続 •インターネット接続構成	Amazon VPC, AWS Transit Gateway, AWS Direct Connect, Amazon Route 53
4	アイデンティティ管理とアクセス管理	•AWS 環境における認証・認可 •権限設計の方針 •ユーザー管理	AWS IAM, AWS IAM Identity Center
5	発見的統制	•セキュリティ監視	AWS CloudTrail, AWS Config, Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector
6	インフラストラクチャ保護	•データ漏洩対策 •インバウンド通信の保護 •アウトバウンド通信の制御	AWS Shield, AWS WAF, AWS Network Firewall

No	項目	含める内容	関連する AWS サービス
7	データ保護	•データの管理方法(アクセス制御保管設定) •保管データの暗号化 •通信データの暗号化	Amazon S3, AWS Key Management Service (AWS KMS), AWS Certificate Manager (ACM)
8	監視	•AWS サービス稼働状況の監視 •リソースの稼働状況の監視	Amazon CloudWatch, AWS Trusted Advisor, AWS Health
9	ログ管理	•取得するログ •ログの保管・管理	Amazon CloudWatch, Amazon S3
10	インシデント対応	•インシデント発生時の運用	Amazon EventBridge, AWS Config
11	災害対策とバックアップ/リストア	•災害対策 •バックアップ/リストア	AWS Elastic Disaster Recovery, AWS Backup
12	インフラプロビジョニング	•リソースのプロビジョニング方法 •AWS サービスのコード化	AWS CloudFormation, AWS Cloud Development Kit(CDK)
13	運用管理	•インスタンス管理 •運用ジョブの実行形式 •タグの管理 •サポートの利用	AWS Systems Manager, AWS Support
14	コスト管理	•コスト管理 •コスト最適化	AWS Billing and Cost Management, AWS Compute Optimizer

ポイント２ ：最初から「100点」を目指さない

■ よくある失敗

- 全てのユースケースや将来拡張を網羅しようとする
- 全部門の合意形成を待ってしまう

→ 結果：議論だけで半年が過ぎ、**何もリリースできない**

■ 推奨アプローチ

- 「完成形」ではなく「実用最小限」でスタートする
- まずは特定のプロジェクトで小さく始め、実績を作る

■ 現場のリアル

- AWSの進化は速く、今日の100点は来年の80点になる
- 共通基盤は「作りきるもの」ではなく、**走りながら「育てるもの」**

ポイント３ ：セキュリティ・オンプレネットワーク担当へのアプローチ

■ よくある失敗

- セキュリティ担当にゼロから相談して先に進まない
- オンプレネットワークの現場担当と調整し、方針が定まらず膠着する
  → 技術検証は終わっているのに、**組織の壁で前に進まない**

■ 推奨アプローチ

- セキュリティ：AWS推奨構成で案を作り、**追認（承認）のみ求める**
- ネットワーク：現場ではなく、インフラ部門責任者と**トップダウンで握る**

■ 現場のリアル

- 相談ではなく「既成事実化」が最も早い合意形成である
- 技術課題ではなく「全社方針」として承認を取り付ける

アジェンダ

なぜ今、共通基盤が求められるのか

立ち上げの『罠』を避ける

設計の『要』を押さえる

運用の『責任』と『普及』

まとめ

ポイント４：無理に統合しない。あえて新旧並走させる

■ よくある失敗

- 既存ルールの維持や既存の共通基盤との互換性にこだわりすぎる
  → **調整コストが肥大化**し、共通基盤の検討そのものが進まなくなる

■ 推奨アプローチ

- 既存環境（技術的負債）を取り込まず、**新設（グリーンフィールド）**する
- 既存環境を切り離し、これから新設するシステムでの要件/ベストプラクティスに基づき設計する

■ 現場のリアル

- 一時的な「二重管理」は、プロジェクト成功の必要経費と割り切る
- 不便な既存と快適な新設の**併存期間**を設け、強制せずに、利便性の差で自然な移行を進ませる

ポイント５：技術的な最大の急所は踏み台サーバ

■ よくある失敗

- Session Manager導入前提で検討し、SSH(AWS-StartSSHSessionドキュメントを使用したSSH接続)やポートフォワーディングを意図せず許可

→ SSHトンネルや転送通信の中身は記録されないため、踏み台が**監査の死角**になり、再検討へ

■ 推奨アプローチ

- SSHトンネル（ポートフォワーディング）は原則禁止し、OS操作はSSMシェルを利用
- 業務上やむを得ない場合のみ例外として設計

■ 現場のリアル

- Session ManagerはSSMシェル利用時にはOS操作ログはCloudWatch Logs等へ記録可能
- 自社の要件によっては、特権管理ソリューションの導入も検討する必要がある

アジェンダ

なぜ今、共通基盤が求められるのか

立ち上げの『罠』を避ける

設計の『要』を押さえる

運用の『責任』と『普及』

まとめ

ポイント６ ：セキュリティ運用は誰が担うのか

■ **よくある失敗**

- GuardDuty / Security Hub CSPMのアラートは時間とともに増加し、CCoEの運用負荷が肥大化する
  → アラートの**発見が遅れたり、放置**される

■ **推奨アプローチ**

- **CCoEは検知・可視化までを提供**し、修正は利用者側の責任とする
- セキュリティ部門は是正状況を統制・監督する

→ 責任を分解して設計する

■ **現場のリアル**

- 利用者が少ない間はCCoEによる手厚い支援が可能
- しかしAWSアカウントが50超になると個別支援は限界
- 各AWSアカウントのセキュリティ違反は、利用者自身が是正する前提にしないとスケールしない

ポイント7 ：良い基盤も、知られなければ無価値

■ よくある失敗

- 共通基盤の仕様やガイドラインがPowerPoint／PDFで作成され、配布されて終わる
- ドキュメント同士が相互参照だらけになっている
- タイトルから内容が判断できない

→ **情報が分散**し、どれが正解か分からなくなる
→ 現場は独自解釈し、共通基盤が利用されなくなる

■ 推奨アプローチ

- 最初に**共通基盤ポータル**を作り、極力すべての情報をそこに集約する
- 関係性はWebページのリンクで表現し、ファイルとして配布することはしない

■ 現場のリアル

- 共通基盤の検討はPowerPointやExcelで行われがちで、その成果物をそのまま利用者に展開してしまいがち
- 手間はかかるが、Webサイトで提供したほうが利用者目線では圧倒的に使いやすく、最新情報も伝わりやすい

アジェンダ

なぜ今、共通基盤が求められるのか

立ち上げの『罠』を避ける

設計の『要』を押さえる

運用の『責任』と『普及』

まとめ

まとめ

立ち上げ

1．AWS社公式ガイドライン活用
2．最初から100点を目指さない
3．NW・セキュリティ担当の効果的な巻き込み方

設計

4．新設環境で作り、新旧併存を許容する
5．踏み台は操作ログ取得に注意を払う

運用

6．セキュリティ運用の責任分界点の合意
7．ポータルによる情報展開


NTT DATA