



マルチアカウント環境のガバナンス実現方法 + BLEA概説

アマゾン ウェブ サービス ジャパン 合同会社
部長/シニアソリューションアーキテクト
大村 幸敬 (ohmurayu@amazon.co.jp)

2024/06/20

アジェンダ

1. クラウドを活かすガバナンスの考え方
2. スケールするガバナンスの実現方針ガバナンスの実現方針
3. 中央集権で管理する範囲を広げる場合の考え方と注意点
 - ネットワーク設定に対するガバナンスの例
4. Baseline Environment on AWSの概要
 1. BLEAが提供するガバナンスの具体例
 2. ベースラインの展開パターン
 3. BLEAのカスタマイズ
 4. BLEA利用時に必要なスキルおよび運用タスク
 5. 参考資料

クラウドを活かすガバナンスの考え方

クラウドが提供する価値

Builderを支えるセルフサービスプラットフォーム



Builder（手が動く開発者）に自由を与え、承認なく適切な箇所で適切なツールを使えるようにする
それによって柔軟・迅速にビジネス価値を実現できる

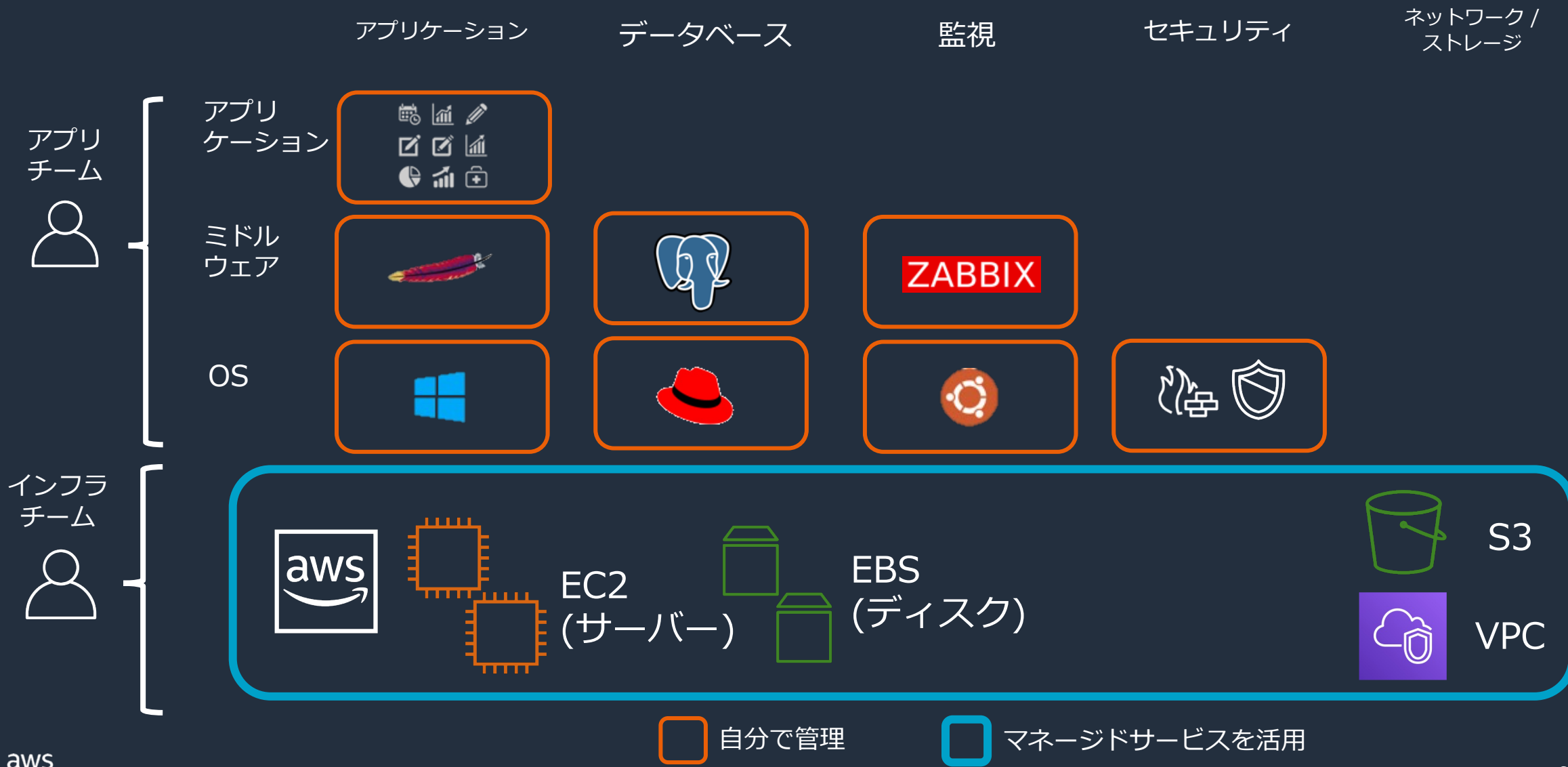
オンプレミスのシステム構成例



 自分で管理

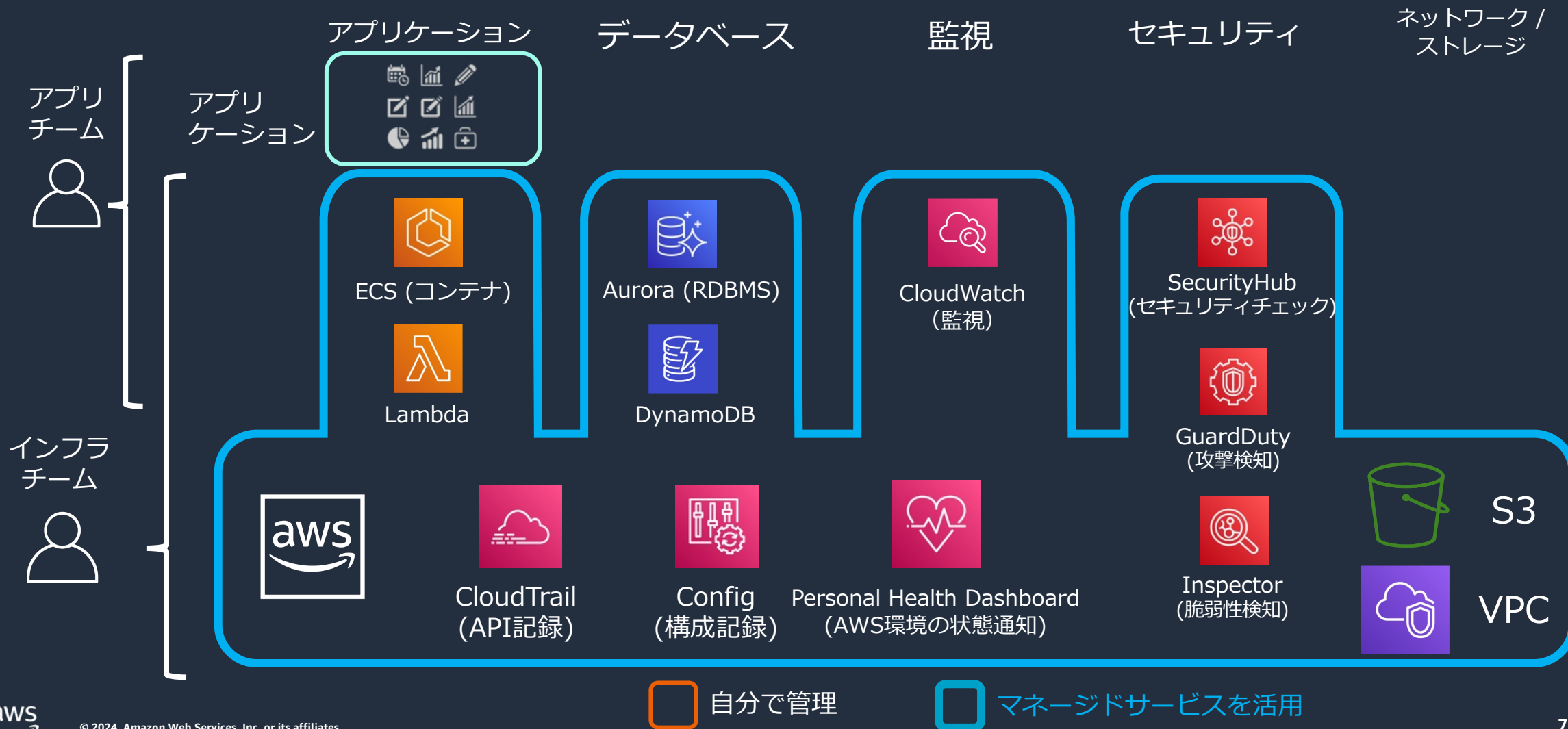
 マネージドサービスを活用

クラウドのシステム構成例 (Liftパターン)



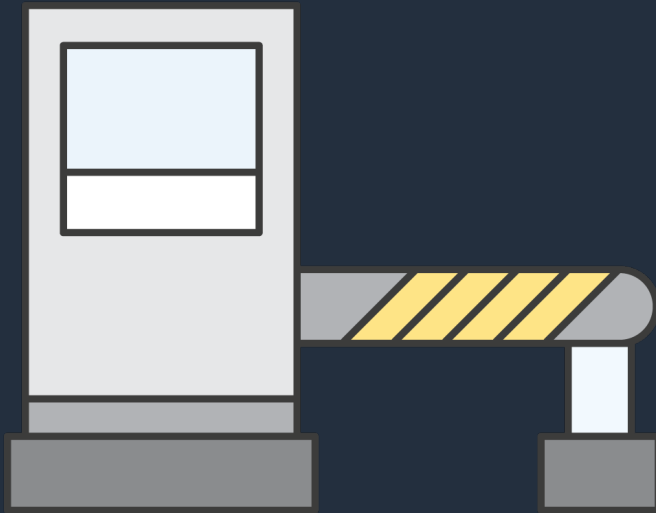
クラウドをフル活用したシステム構成例

マネージドサービス活用により コスト効率よくビジネス価値を実現することに集中



Builderに必要なガバナンス

Gatekeeper



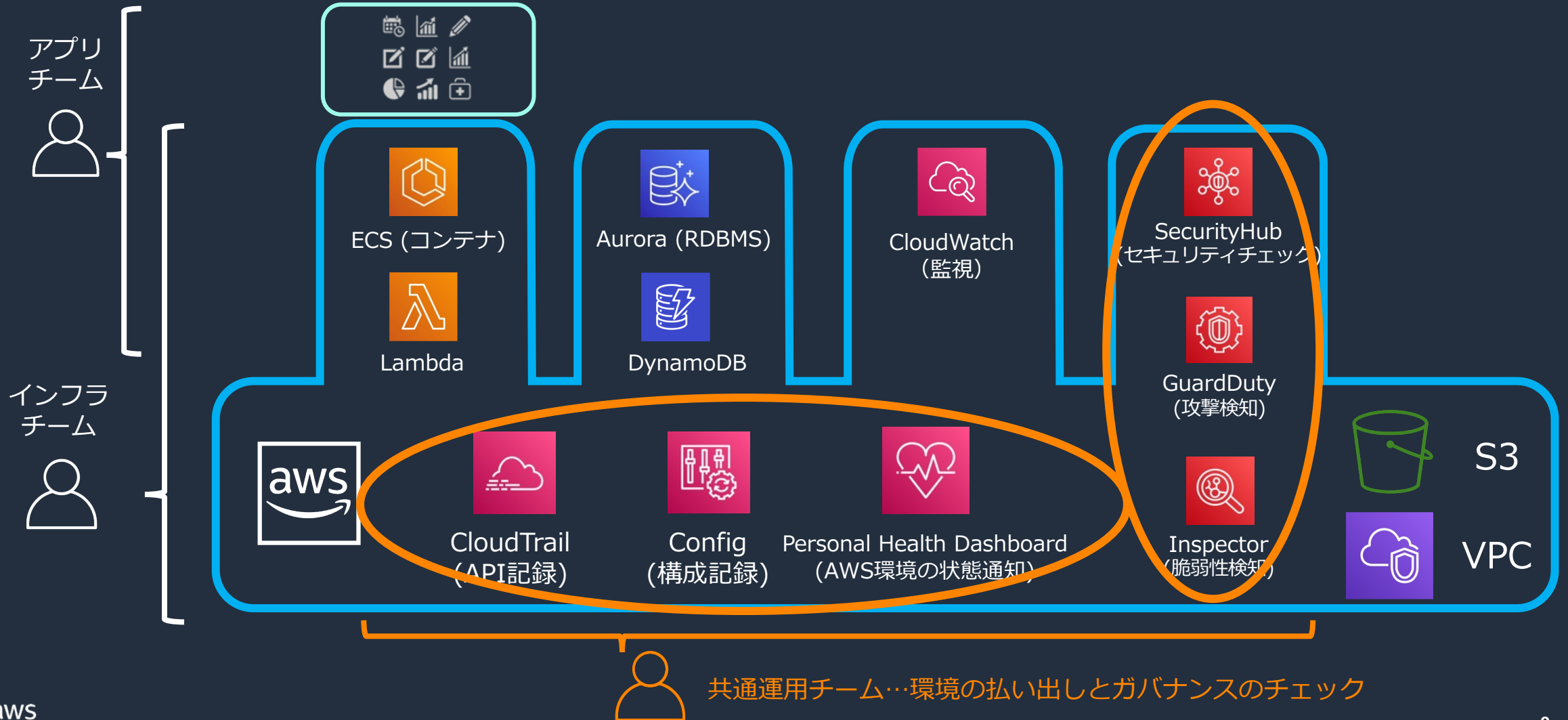
V.S.

Guardrail



ツールの利用を事前承認(Gatekeeper)すると管理業務がボトルネックになる。
各システムで自由に使わせる一方で、Builderを守るためガードレール(Guardrail)を用意する。
やってはいけない操作を未然に防ぐこと（予防的統制）、逸脱を検知すること（発見的統制）の2種類。

セキュリティサービスを活用したガードレールの実現

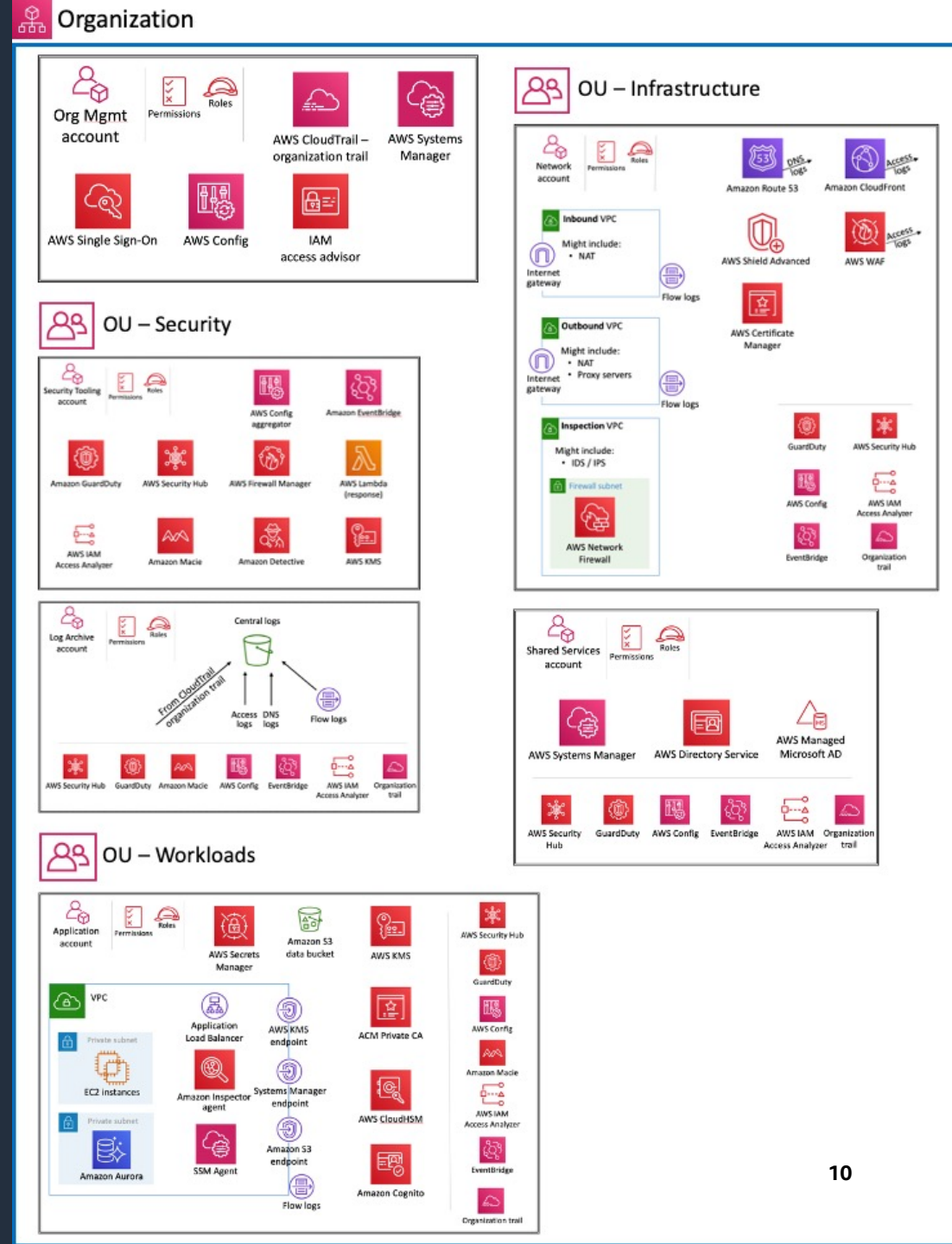
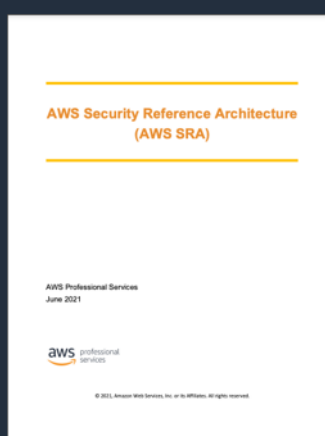


AWS Security Reference Architecture (AWS SRA)

AWSのセキュリティサービスをフル活用する際のガイダンスと実装例
(多くの場合すべてを実装する必要はない)

- セキュリティガバナンス
- セキュリティ監査
- 脅威検出
- 脆弱性管理
- インフラストラクチャ保護
- データ保護
- アプリケーションセキュリティ
- インシデントレスポンス

<https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html>



アカウントに対して ベースラインとして設定を推奨する セキュリティサービス

The screenshot shows the AWS IAM console interface for a 'Guest Account'. A grey box highlights the recommended baseline services: CloudTrail, Config, and ControlTower. Below this box, other security services are listed with their functions.

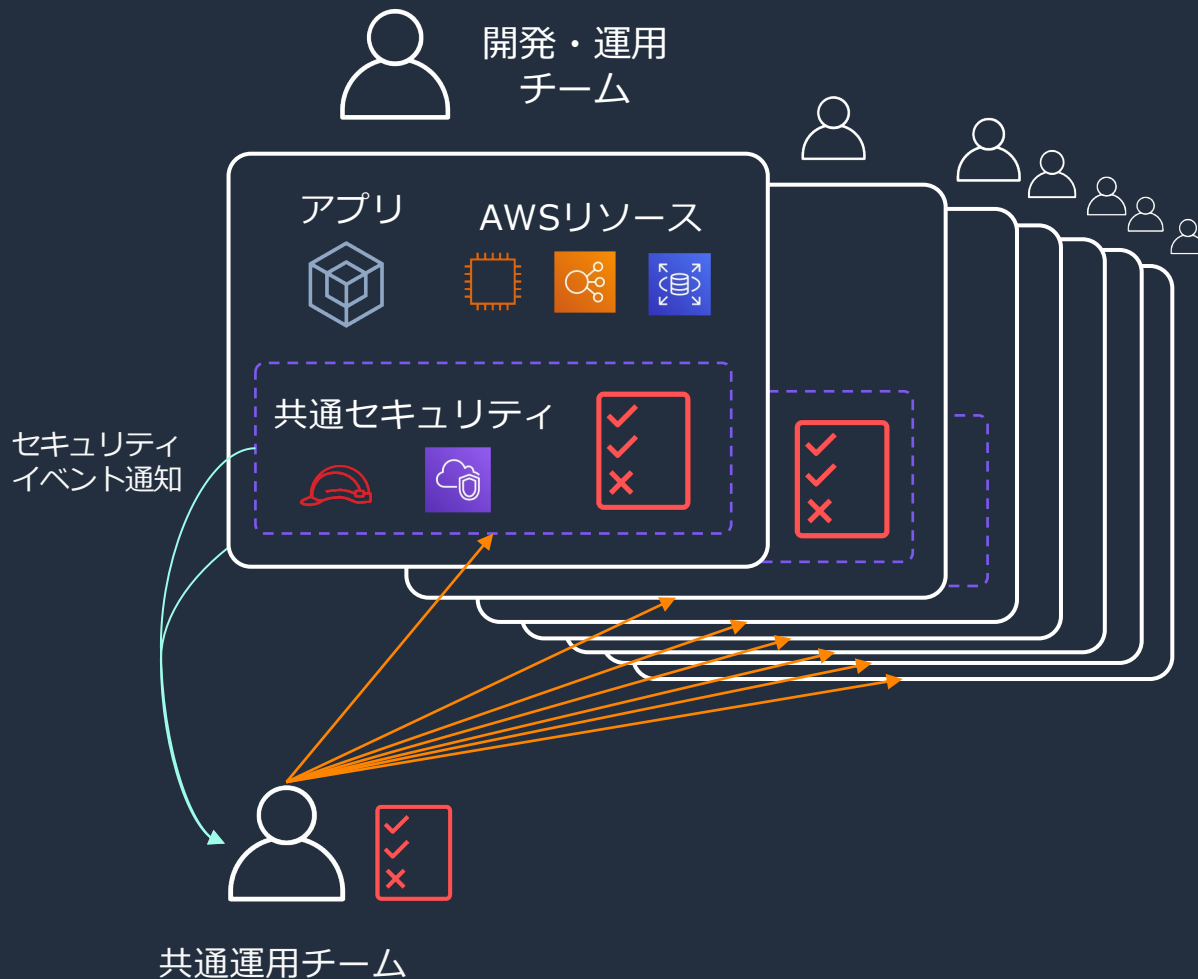
Service	Function
CloudTrail	APIの記録
Config	構成変更の記録
ControlTower	ControlTowerによって有効化
GuardDuty	セキュリティ脅威の検知
SecurityHub	設定がAWSのベストプラクティスに適合しているかのチェック
Inspector	脆弱性の検出

複雑な設定は不要、コストも小さく、稼働するワークロードに影響を与えない
まずはこれらをONにしてセキュリティレベルのベースを上げることを推奨

スケールするガバナンスの実現方針

よくある落とし穴

よくある課題：中央集権管理がクラウドの価値を下げってしまう



中央集権的な管理作業の例

- 共通運用チームが…
 - 1つのセキュリティポリシーを全体へ適用する
 - 各システムのセキュリティ設定を実施する
 - 各システムのセキュリティイベントに対応する
 - 各チームメンバーのアクセス管理を実施する

課題

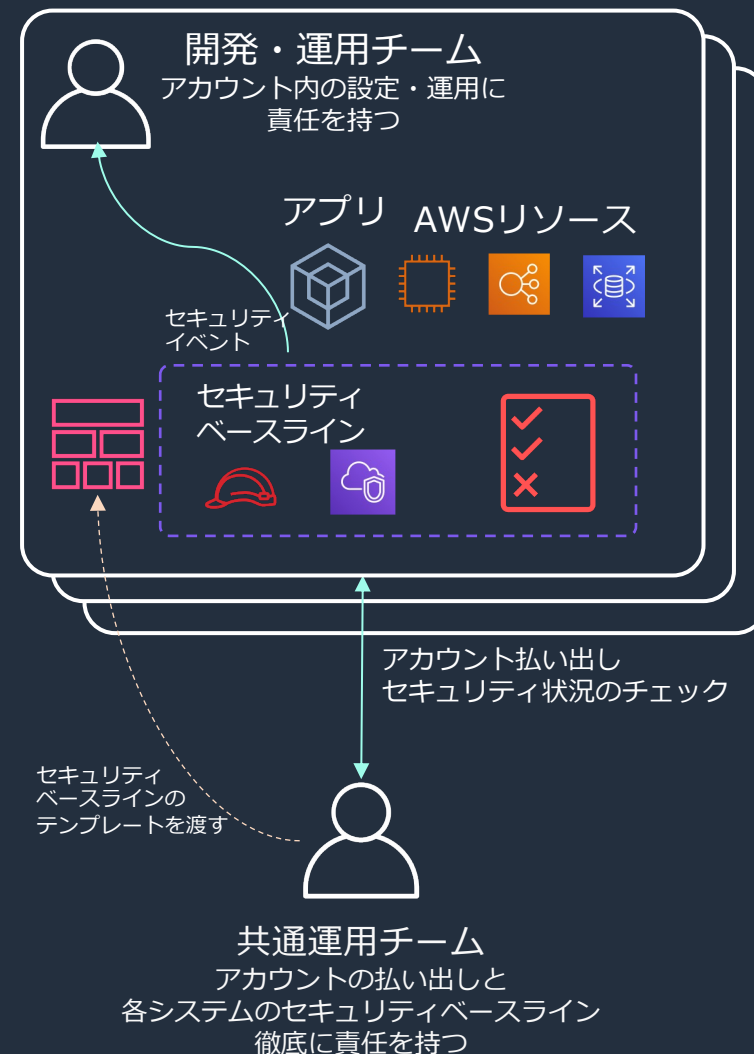
- マネージドサービスが活用できない
 - 共通セキュリティポリシー変更時間に時間を要する
 - AWSの機能拡張にルールが追従できない
- 共通運用チームがボトルネック
 - システム数増加に手動作業が追いつかない
 - 多量のセキュリティイベントに対応できない
 - 個々のシステムで認めた例外の管理が困難

スケールするガバナンスの具体的な実装例

1) アカウントをまるごと渡す

スケールするガバナンスの実現方針

- **環境ごとにアカウントを払い出す**
 - アカウント内は自由にAWSを利用可能（最低限の制限のみ設定）
 - 他のアカウントに影響を与えない
- **払い出したアカウントの管理は開発・運用チームに委ねる**
 - 共通運用チームはセキュリティベースラインを用意して、開発・運用チームが自分でそれを展開
 - 開発・運用チームはアカウント内の各種設定・運用に責任を持つ
- **各アカウントの状況はセキュリティサービスで集約して閲覧**
 - 共通運用チームは自らが望むタイミングでまとめて情報を得る
 - セキュリティイベントは開発・運用チームが自ら受ける

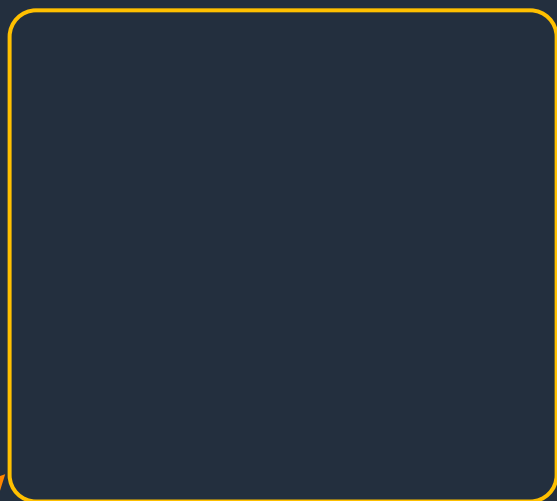


テンプレートを使ったガバナンスの全体像

開発・運用チーム



1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う



1. アカウント払い出し
最低限の
ガードレール設定

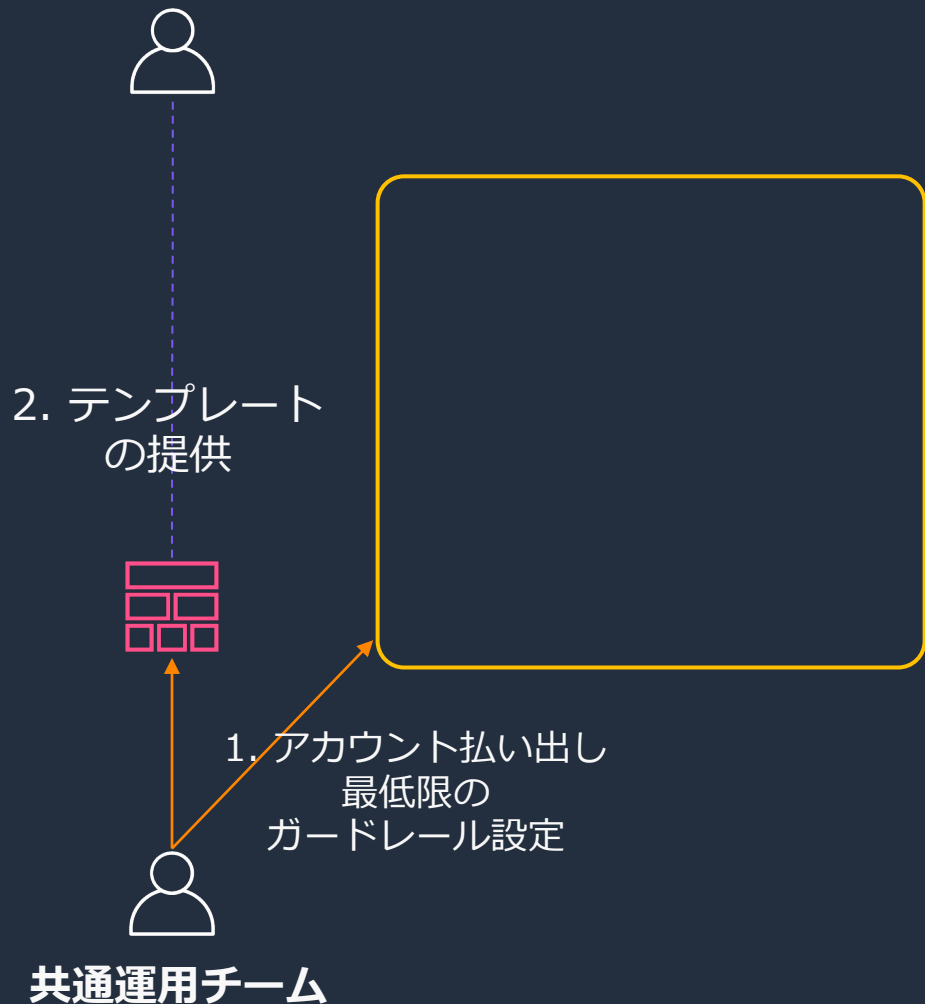


共通運用チーム



テンプレートを使ったガバナンスの全体像

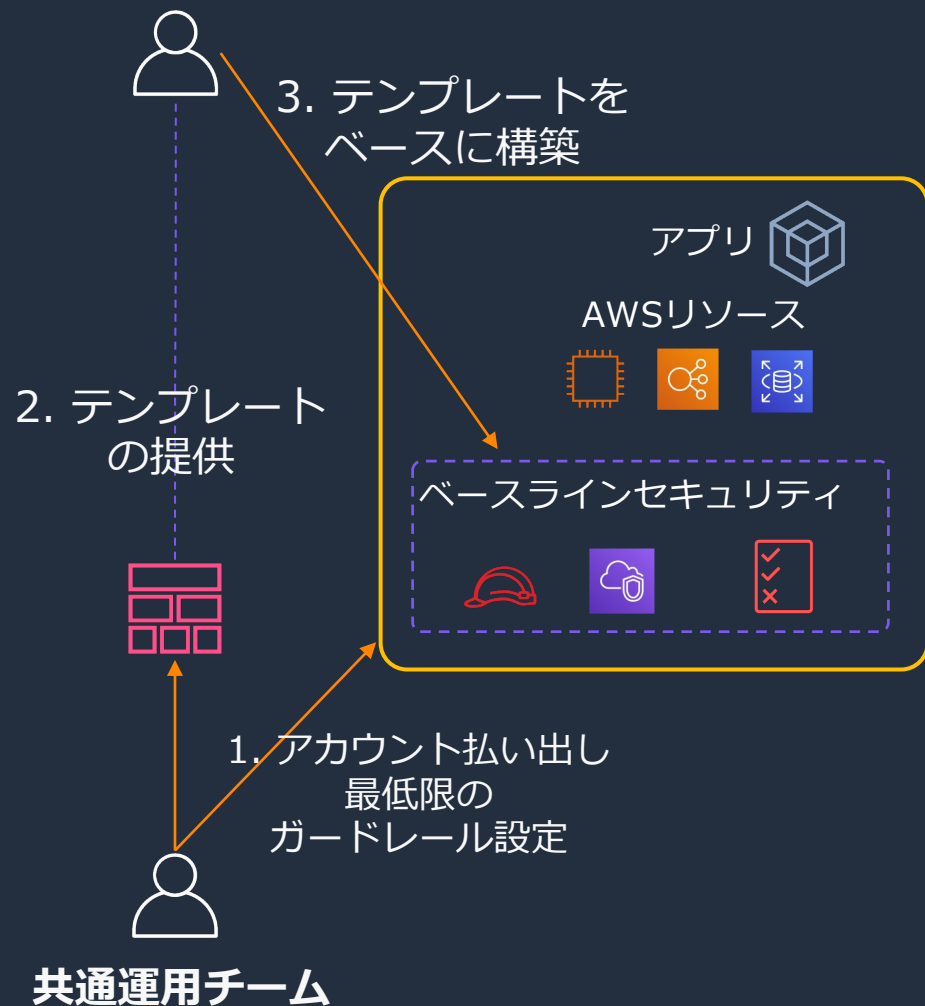
開発・運用チーム



1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う
2. 「実行可能なセキュリティガイド」としてのテンプレートの配布
 - ガイドや手順書ではなく

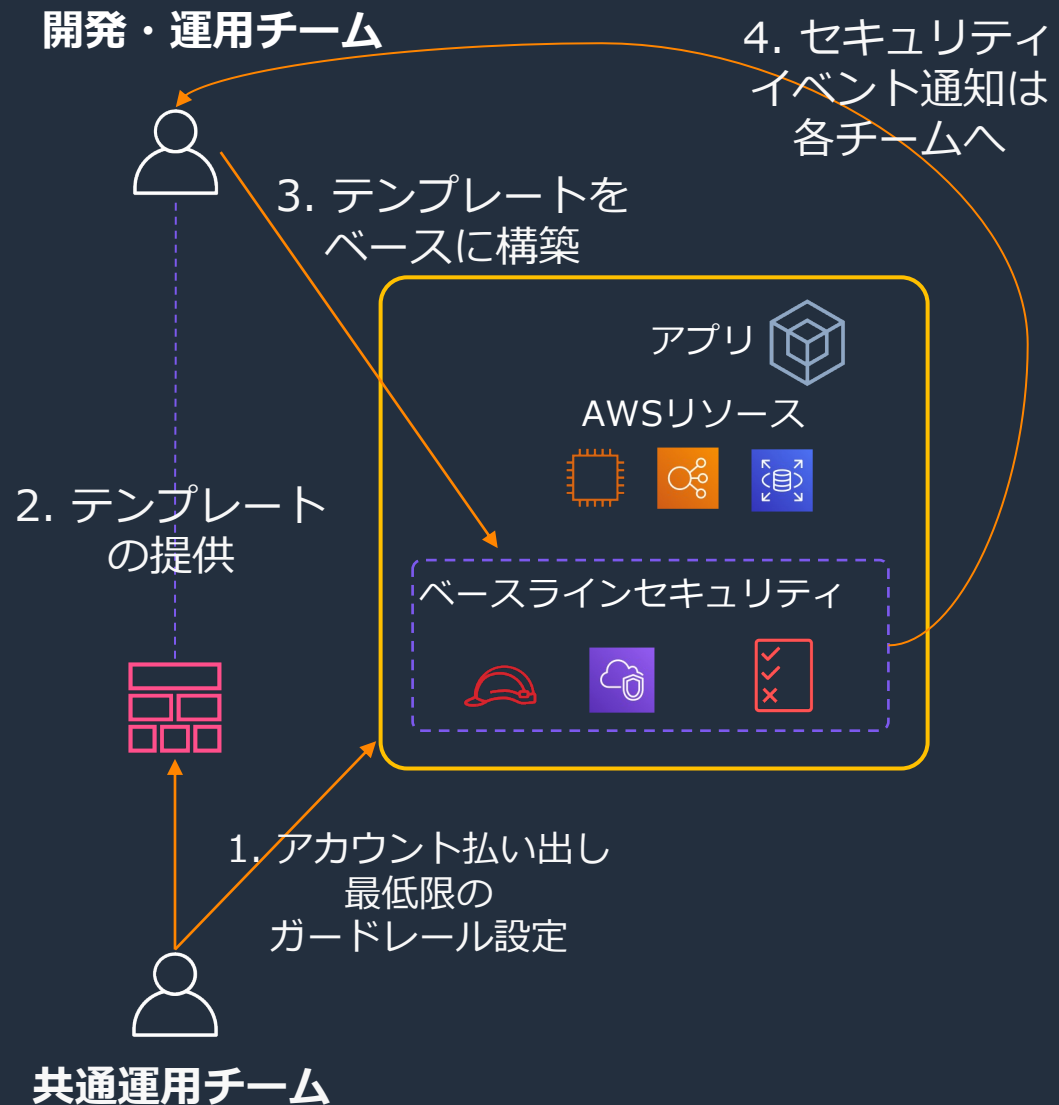
テンプレートを使ったガバナンスの全体像

開発・運用チーム



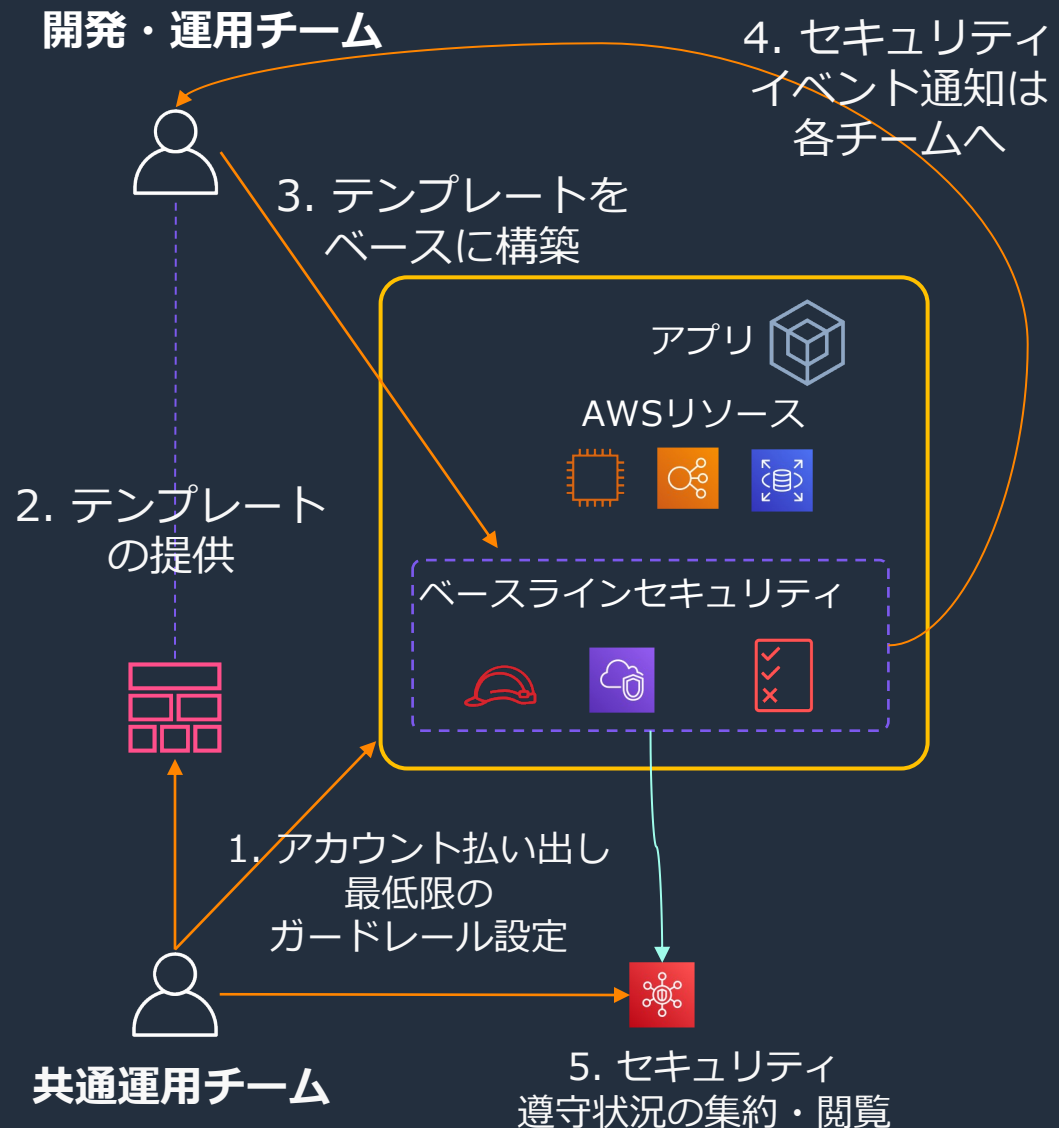
1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う
2. 「実行可能なセキュリティガイド」としてのテンプレートの配布
 - ガイドや手順書ではなく
3. 各アカウントの管理責任は各チームが負い、テンプレートも各チームの責任で管理する (カスタマイズやメンテナンスも行う)

テンプレートを使ったガバナンスの全体像



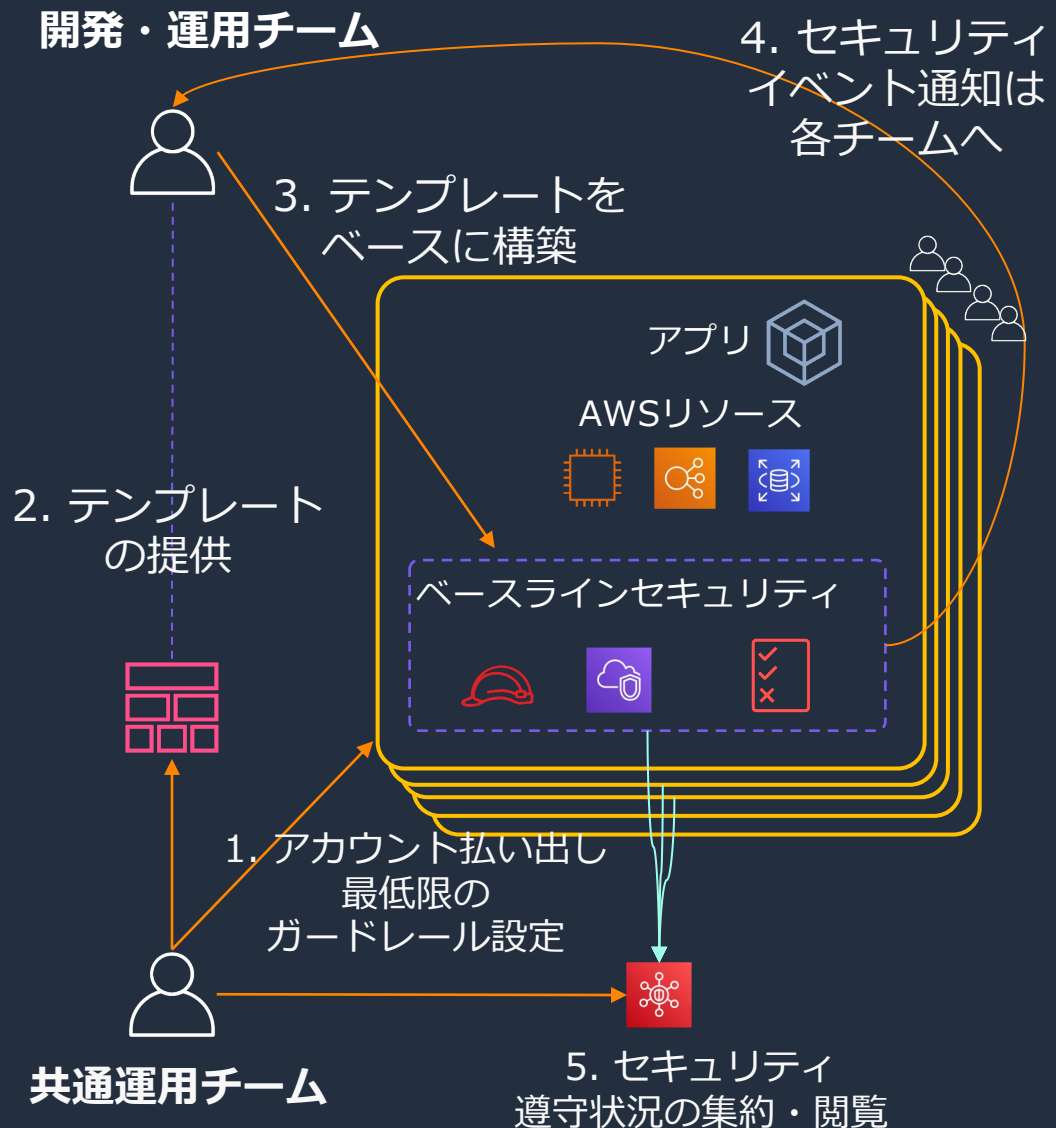
1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う
2. 「実行可能なセキュリティガイド」としてのテンプレートの配布
 - ガイドや手順書ではなく
3. 各アカウントの管理責任は各チームが負い、テンプレートも各チームの責任で管理する（カスタマイズやメンテナンスも行う）
4. セキュリティイベントの即時通知は各チームで対処

テンプレートを使ったガバナンスの全体像



1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う
2. 「実行可能なセキュリティガイド」としてのテンプレートの配布
 - ガイドや手順書ではなく
3. 各アカウントの管理責任は各チームが負い、テンプレートも各チームの責任で管理する（カスタマイズやメンテナンスも行う）
4. セキュリティイベントの即時通知は各チームで対処
5. 重要なセキュリティイベントや定期的な遵守状況の確認は共通運用チームが実施

テンプレートを使ったガバナンスの全体像



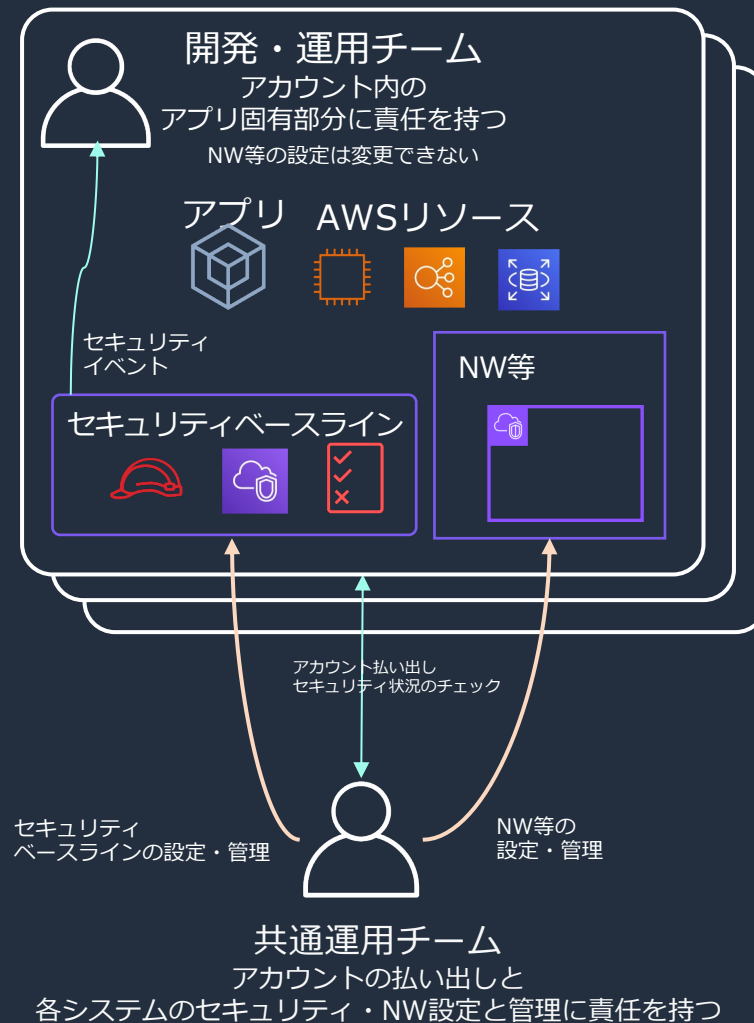
1. 共通運用チームはアカウントの払い出しと最低限のガードレール設定のみを行う
2. 「実行可能なセキュリティガイド」としてのテンプレートの配布
 - ガイドや手順書ではなく
3. 各アカウントの管理責任は各チームが負い、テンプレートも各チームの責任で管理する（カスタマイズやメンテナンスも行う）
4. セキュリティイベントの即時通知は各チームで対処
5. 重要なセキュリティイベントや定期的な遵守状況の確認は共通運用チームが実施

中央集権で管理する範囲を広げる場合の 考え方と注意事項

中央集権でベースラインを管理するガバナンスの実現方針（例）

アカウントが増えた場合に、管理し切れるか、あとから設定変更可能かよく検討する

- 環境ごとにアカウントを払い出す
 - アカウント内は自由にAWSを利用可能
ただしNWやセキュリティベースラインの設定は変更不可
 - 他のアカウントに影響を与えない
- 払い出したアカウントの**アプリ固有部分のみ**開発・運用チームに委ねる
 - 共通運用チームがセキュリティベースラインとNW等を設定
全アカウントの当該設定を共通運用チームで管理
 - 開発・運用チームはアカウント内のアプリ固有部分のみ
設定・運用に責任を持つ（サーバ、Lambda等を含む）
- 各アカウントの状況は**セキュリティサービスで集約して閲覧**
 - 共通運用チームは自らが望むタイミングでまとめて情報を得る
 - セキュリティイベントは開発・運用チームが自ら受ける



ネットワーク設定に対するガバナンスの例

ネットワーク設定を集中管理する場合のガバナンス（例）

- 予防的統制
 - ゲストアカウトで、ネットワーク設定を変更できないよう制限
 - SCP（OUまたはアカウント単位） / IAM Policy (boundary) で設定
 - VPC等はタグを付与して、中央管理者のみ変更可能、他のエンティティは変更不可
 - 例) IGWのアタッチ、VPCやサブネットの作成、EIPのアタッチなどを禁止する
- 発見的統制（こちらを強化することを推奨）
 - ゲストアカウトで、ルールを逸脱した設定を検知して通知
 - SecurityHubやConfig rulesを設定（これらの設定を無効化できないようIAM等で制限）
 - ゲストアカウト管理者に通知、悪質なものは中央管理者に通知 or レポーティング
 - 例) 許可されないVPCのIGWアタッチ、EIPがアタッチされたインスタンスを検知

ネットワーク設定を集中管理する具体的な設定例

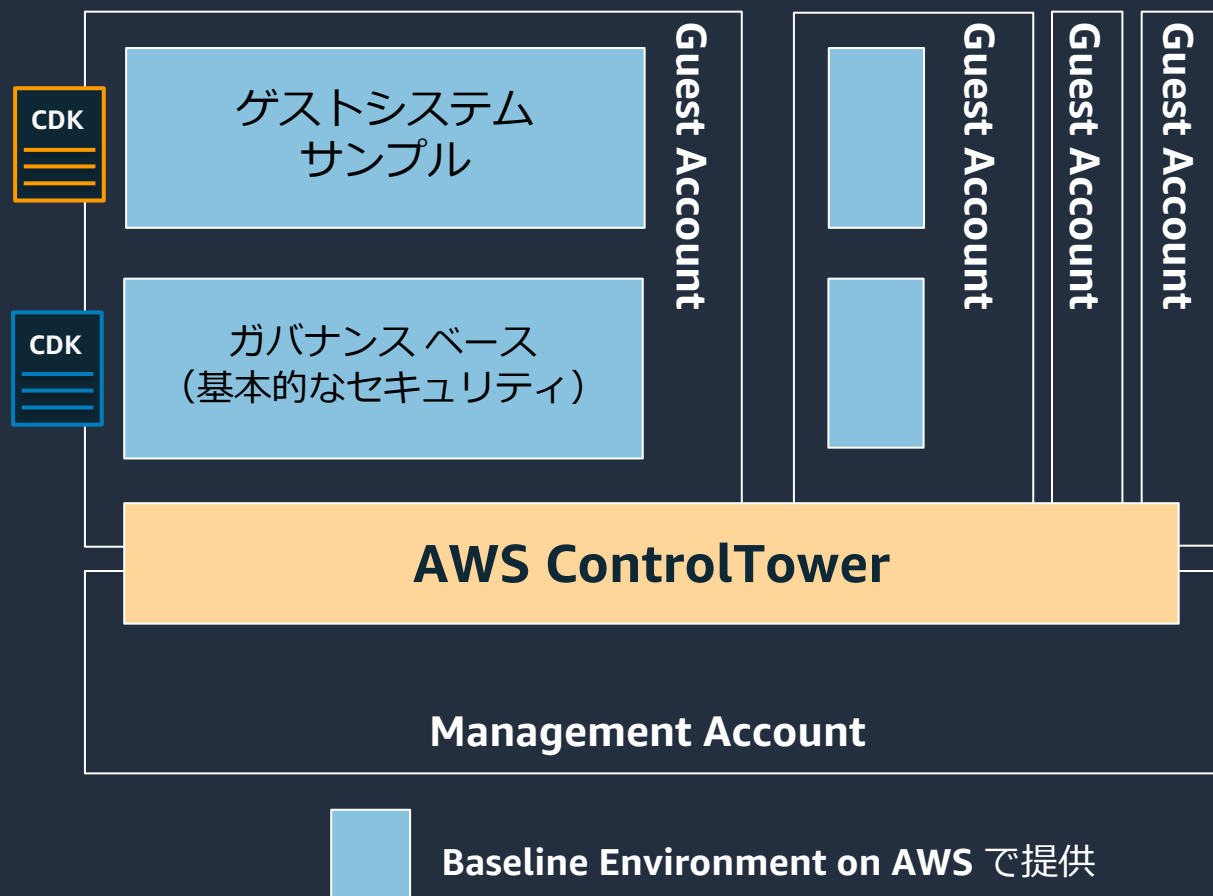
- 予防的統制
 - [Amazon VPC ポリシーの例](#)
 - [SCPを利用して複数AWSアカウントのEC2へのパブリックIP付与を禁止する](#)
- 発見的統制（こちらを強化することを推奨）
 - SecurityHub
 - [\[EC2.9\] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします](#)
 - [\[EC2.15\] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします](#)
 - [\[EC2.18\] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします](#)
 - [\[EC2.19\] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません](#)
 - Config Managed Rules
 - [eip-attached](#)
 - [internet-gateway-authorized-vpc-only](#)

Baseline Environment on AWS の概要

Baseline Environment on AWS

AWSのセキュリティベストプラクティスを実装したサンプルテンプレート

<https://github.com/aws-samples/baseline-environment-on-aws>



- **セキュリティのベースラインを提供**
 - ControlTowerの機能をベースに足りない部分を **ガバナンスベース** で提供
 - AWSのセキュリティサービスをフル利用
- **ゲストシステムのサンプルを提供**
 - ガバナンスベースを土台として構築するWebアプリケーションなどのサンプル
 - **AWSセキュリティベストプラクティスを実装**
- **AWS CDK*** で提供 *Cloud Development Kit
 - AWS JapanのSAが**オープンソース**で公開
 - CDKのリファレンスや学習利用を想定
 - シンプル、引き継ぎやすさを重視

BLEAについてよくある質問

Q: BLEAは公共機関や金融機関など高いセキュリティレベルを実現するための重厚な仕組みなのですか

A: いいえ。逆です。むしろ俊敏性を必要とする環境において最低限のセキュリティを提供するための薄い仕組みです。より高いセキュリティのための第一ステップを容易に実現します。

Q: BLEAを使うためにはBLEAそのものに関する習熟が必要ですか。

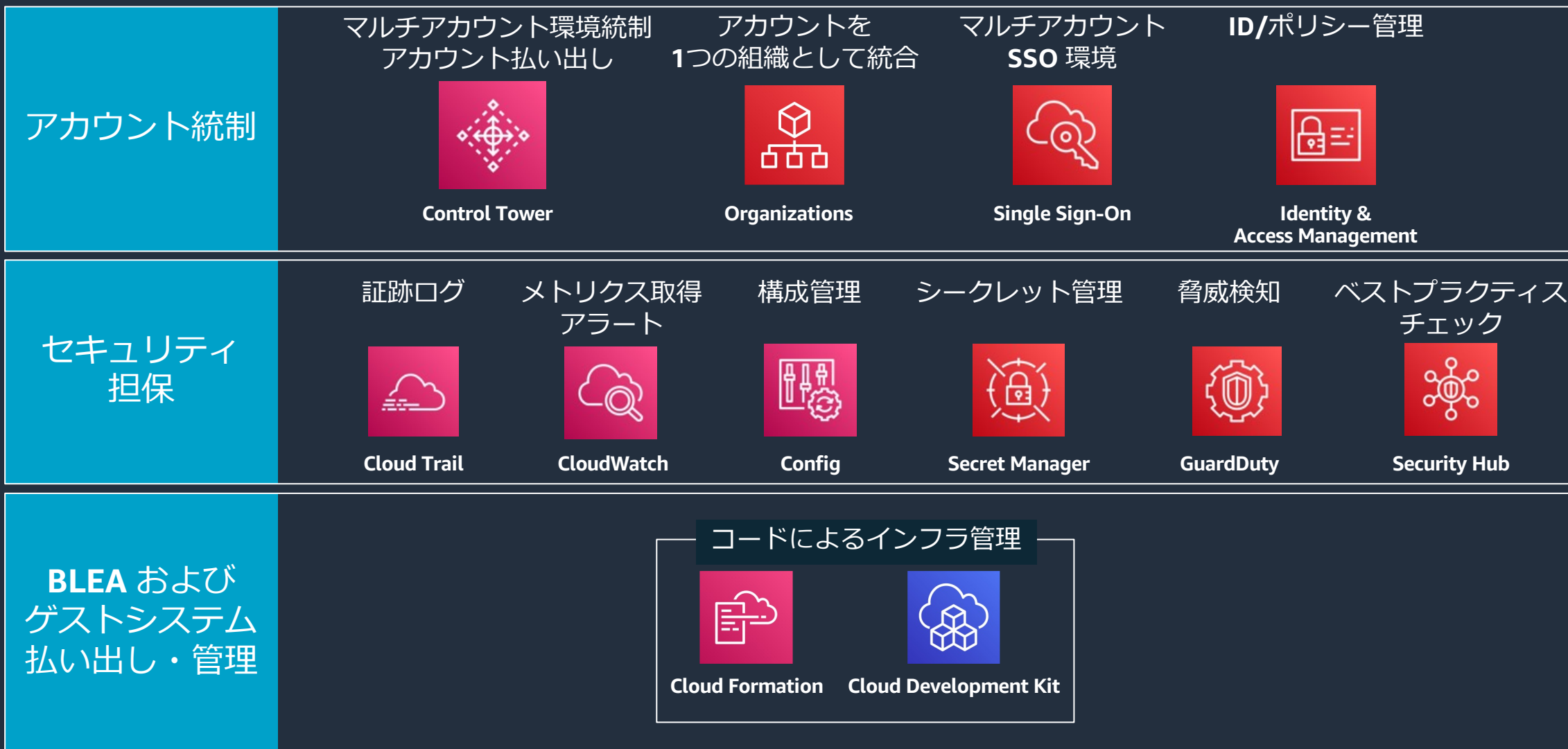
A: いいえ。BLEAは極力独自の仕組みを作るのではなく、AWSのセキュリティサービスをそのまま使っています。AWSの標準的な知識だけで理解できるよう作られています。

Q: 開発者がCDKを利用できないと使えませんか。

A: いいえ。管理者が Service Catalog にベースラインを登録し、開発者がそれを使ってベースラインを展開する方法があります。

BLEAが提供するガバナンスの具体例

BLEA で使用している主要 AWS サービス



BLEAマルチアカウント版 管理タスクと利用サービス対応表

(ver. 2023/03/20)

AWS ControlTower

Governance Base for CT Guest

Guest System

	管理タスク	Management Account	Audit Account	LogArchive Account	Shared Svc Account*	Guest Account
1	アカウント払い出し	CT-Org	(Created by CT)	(Created by CT)	(Created by CT)	(Created by CT)
2	アクセス制御	CT-SSO/Admin + AD	CT-Admin	CT-Admin	CT-Admin	CT-Admin
3	予防的統制	CT-SCP	CT-SCP	CT-SCP	CT-SCP	CT-SCP
4	発見的統制(Config)	CT-ConfigRules作成	CT-ConfigRules	CT-ConfigRules	CT-ConfigRules	CT-ConfigRules
5	ロギング	CT-Trail for Organization	CT-Config Aggregator	CT-Bucket for Logs	CT-CloudTrail/Config	CT-CloudTrail/Config
6	通知 (CT)	(CT-Audit Topic)	CT-Audit Topic	(To Audit Topic)	(To Audit Topic)	(To Audit Topic)
7	発見的統制 (挙動)		MNL-SecurityHub MNL-GuardDuty MNL-Inspector			Member-SecurityHub Member-GuardDuty
8	セキュリティ分析		MNL-IAM-AccessAnalyzer			Member-IAMAccessAnalyzer
9	共有ネットワーク				TMPL-VPC/DNS/VPCEP *	(Use Shared Svc Account)
10	サーバ管理					MNL-SSM QuickSetup
11	通知 (Security)+Chat					TMPL-Security Alarm
12	アクセス制御 (for Guest)					TMPL-IAM
13	発見的統制 (for Guest)					TMPL-ConfigRules
14	ロギング (for Guest)					TMPL-FlowLogs/ALB Logs etc.
15	ネットワーク (for Guest)					TMPL-VPC
16	鍵管理 (for Guest)					TMPL-KMS
17	通知 (Monitoring)+Chat					TMPL-Monitor Alarm
18	リソース + バックアップ					TMPL-EC2/Serverless etc.
19	デプロイメント					TMPL-CI/CD


CT- : Managed by ControlTower / TMPL- : Provide Templates (CDK) / MNL-: Manual / *: Not implemented





管理タスクの主体


管理される側










BLEA マルチアカウント版 – セキュリティベースラインの全体像



 Management Account

-  AWS Contrl Tower
-  CloudTrail (Organization Trail)
-  CloudWatch Logs (Log Stream of CloudTrail)
-  Trusted Advisor Org view

 Audit Account

-  Config Aggregator
-  Organizations Delegated Admins
-  GuardDuty
-  Inspector
-  SecurityHub
-  IAM AccessAnalyzer

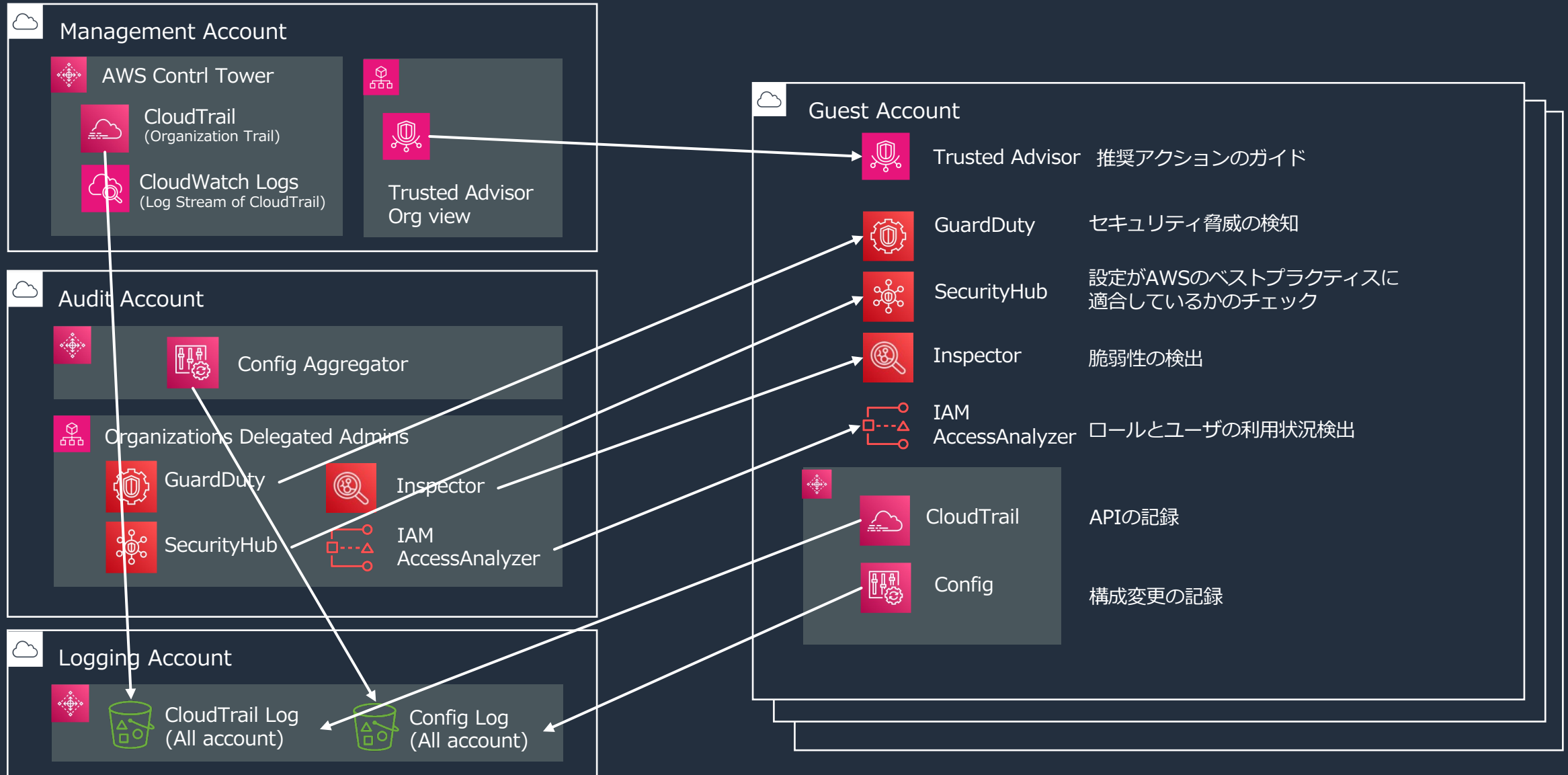
 Logging Account

-  CloudTrail Log (All account)
-  Config Log (All account)

 Guest Account

-  Trusted Advisor 推奨アクションのガイド
-  GuardDuty セキュリティ脅威の検知
-  SecurityHub 設定がAWSのベストプラクティスに適合しているかのチェック
-  Inspector 脆弱性の検出
-  IAM AccessAnalyzer ロールとユーザの利用状況検出
-  CloudTrail APIの記録
-  Config 構成変更の記録

BLEA マルチアカウント版 – セキュリティベースラインの全体像



Trusted Advisor – Organizations View

Trusted Advisor <

Trusted Advisor > 組織ビュー

概略

レポートのチェック結果を確認します。このレポートをダウンロードして組織と共有し、影響を受ける AWS アカウント、対処する必要があるサービス、およびパフォーマンスを改善するために削除または最適化できるリソースを特定できます。

MyOrgTrustedAdvisorReport 概略 レポートをダウンロード

アカウント数	作成日	形式
15	success (April 03, 2024 04:42:42)	JSON

⊗ 45 推奨されるアクション 情報	⚠ 157 調査が推奨されます 情報	☑ 217 問題が検出されなかったチェック項目 情報
コスト最適化 1	コスト最適化 5	コスト最適化 6
パフォーマンス 1	パフォーマンス 3	パフォーマンス 9
セキュリティ 39	セキュリティ 136	セキュリティ 122
耐障害性 4	耐障害性 10	耐障害性 30
サービスの制限 0	サービスの制限 2	サービスの制限 49
	運用上の優秀性 1	運用上の優秀性 1

月額料金節約の可能性
\$31.37

GuardDuty – Organization summary

GuardDuty

Amazon GuardDuty では、生成された検出結果について集約されたインサイトを表示する新しいエクスペリエンスが提供されています。このページの改善に役立つように、フィードバックを送信することをお勧めします。

GuardDuty > 要約

要約

以下のインサイトは、AWS 環境で生成された最新の 5,000 件の検出結果に基づいています。

数秒前 で更新済み 今日

概要

合計検出結果	高い 重大度の検出結果	検出結果を含むリソース	検出結果を含むアカウント
0	0	0	0
すべての検出結果を表示	高い重大度の検出結果をすべて表示		

重大度別の検出結果

最も一般的な検出結果タイプ

アカウント

設定

リスト

最新情報

パートナー

GuardDuty

要約 新規

検出結果

使用状況

マルウェアスキャン

保護プラン

- S3 Protection
- EKS Protection
- ランタイムモニタリング 新規
- Malware Protection
- RDS Protection
- Lambda 保護

アカウント

設定

リスト

GuardDuty > アカウント

アカウント

Total member accounts 15/15 (Updated 12時間前)

新しいアカウントの自動有効化 編集 招待によるアカウントの追加

組織の管理アカウントでは、委任された管理者が、メンバーアカウントで GuardDuty Malware Protection 機能を有効にするための関連する許可をアタッチすることは許可されていません。こちらの指示に従ってください。

Accounts (15)

保護プランを編集 アクション

アカウント ID、アカウント名を検索またはフィルタ条件を追加

<input type="checkbox"/>	アカウント ID	名前	タイプ	ステータス	最終更新日	保護プラン
<input type="checkbox"/>	197680276259 [ohmurayu+able2-guest6@amazon.co.jp]	GuestSystem6	Via Organizations	有効	2年前	0/6
<input type="checkbox"/>	719457743686 [ohmurayu+able2-guest3-root@amazon.co.jp]	able2-guest3	Via Organizations	有効	2年前	0/6
<input type="checkbox"/>	128784423201 [ohmurayu+able2-asgapp@amazon.co.jp]	asgapp	Via Organizations	有効	2年前	0/6
<input type="checkbox"/>	108286923059 [ohmurayu+able2-shared@amazon.co.jp]	Shared	Via Organizations	有効	1年前	0/6
<input type="checkbox"/>	525269670137 [ohmurayu+able2-guset4@amazon.co.jp]	GuestSystem4-osaka	Via Organizations	有効	2年前	0/6



Security Hub – Organization view

Security Hub ×

概要

コントロール
セキュリティ基準

インサイト

検出結果
統合

▼ 管理

オートメーション
カスタムアクション

▼ 設定

一般
リージョン
設定 **新規**
使用

最新機能

[Security Hub](#) > 概要

概要 Info

Reset to default layout + Add widget

Choose a filter set Filter data

Workflow status = NEW Workflow status = NOTIFIED Record state = ACTIVE Clear filters

Security standards Info

概要セキュリティスコアと標準セキュリティスコアでクラウドセキュリティ態勢を追跡できます。このウィジェットには、フィルタリングされていない完全なデータが常に表示されます。

セキュリティスコア

69%

198 / 285 コントロール 合格

標準	成功	失敗	スコア ▲
CIS AWS Foundations Benchmark v1.2.0	11	32	26%
AWS 基礎セキュリティのベストプラクティス v1.0.0	181	52	78%
NIST Special Publication 800-53 Revision 5	199	56	78%
CIS AWS Foundations Benchmark v1.4.0			有効化
PCI DSS v3.2.1			有効化

[すべての規格を表示](#)

調査結果が最も多い資産 Info

最もリスクの高い資産に優先順位を付けて評価します。

リソース	アカウント	[アプリケーション]	
リソース	重大度別	リソースタイプ別	調査結果の総数
arn:aws:cloudtrail:ap-northeast-1:771002807239:trail/a- ws-controltower-BaselineCloudTrail	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #c4582c, #c4582c);"></div>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #4169e1, #4169e1);"></div>	32
AWS:::Account:3443161- 97558	<div style="width: 50%; height: 10px; background: linear-gradient(to right, #c4582c, #c4582c);"></div>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #4169e1, #4169e1);"></div>	31
AWS:::Account:3883750- 43318	<div style="width: 50%; height: 10px; background: linear-gradient(to right, #c4582c, #c4582c);"></div>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #4169e1, #4169e1);"></div>	31
AWS:::Account:7194577- 43686	<div style="width: 50%; height: 10px; background: linear-gradient(to right, #c4582c, #c4582c);"></div>	<div style="width: 100%; height: 10px; background: linear-gradient(to right, #4169e1, #4169e1);"></div>	31

[インサイトを表示](#)

IAM Access Analyzer – Organization activity

Identity and Access Management (IAM)

ダッシュボード

- ▼ アクセス管理
 - ユーザーグループ
 - ユーザー
 - ロール
 - ポリシー
 - ID プロバイダー
 - アカウント設定
- ▼ アクセスレポート
 - アクセスアナライザー**
 - 外部アクセス
 - 未使用のアクセス
 - アナライザーの設定
 - 認証情報レポート
 - 組織のアクティビティ
 - サービスコントロールポリシー (SCP)

AWS account ID:
992860067891

IAM > 概要

概要 情報

分析したロールとユーザーの数によっては、検出結果の更新がサマリーに反映されるまでに時間がかかることがあります。

外部アクセスに関する検出結果

最終更新日: 22 時間前 | 信頼ゾーン: 現在の組織

外部アクセスアナライザー
ConsoleAnalyzer-5ef07913-3db1-4f33-a9c3-a9d910b94c6f

アクティブな検出結果

パブリックアクセス

0

組織外のアクセス

177

検出結果の概要

177
アクティブな検出結果

組織外のアクセス

IAM > Access Analyzer > 外部アクセス

外部アクセス 情報

アナライザー

最終スキャン日: 2 時間前

ConsoleAnalyzer-5ef07913-3db1-4f33-a9c3-a9d910b94c6f
信頼ゾーン: 現在の組織 (o-rx6pstlmg)

検出結果 (177)

ステータス: アクティブ

177 件の一致

パブリックアクセス = false

フィルターをクリア

<input type="checkbox"/>	検出結果 ID	リソース	リソース所有...	外部プリンシパル	条件	次を介し...	アクセス...	最終更...
<input type="checkbox"/>	681942a0-1285-43b4-ada6-f...	aws-reserved/sso.amazonaws.com IAM Role	128784423201	フェデレーションユーザー arn:aws:iam::1287...	-	-	Write, Tag...	579 日前
<input type="checkbox"/>	62214664-91a1-41b6-ae09-9...	aws-reserved/sso.amazonaws.com IAM Role	128784423201	フェデレーションユーザー arn:aws:iam::1287...	-	-	Write, Tag...	579 日前
<input type="checkbox"/>	dc3e69b7-45b7-4dc2-b333-6...	aws-reserved/sso.amazonaws.com IAM Role	128784423201	フェデレーションユーザー arn:aws:iam::1287...	-	-	Write, Tag...	579 日前

CloudTrail – Organization Trail

CloudTrail > 証跡 > arn:aws:cloudtrail:ap-northeast-1:771002807239:trail/aws-controltower-BaselineCloudTrail

aws-controltower-BaselineCloudTrail

削除

ログ記録の停止

全般的な詳細

編集

証跡のログ記録

✔ ログ記録

証跡名

aws-controltower-
BaselineCloudTrail

マルチリージョンの証跡

はい

組織に証跡を適用

すべてのアカウントで有効

証跡ログの場所

aws-controltower-logs-
194650547258-ap-northeast-1/o-
rx6pstlemg/AWSLogs/o-
rx6pstlemg/771002807239

配信された最後のログファイル

4月 03, 2024, 13:42:01 (UTC+09:00)

ログファイルの SSE-KMS 暗号化

有効になっていません

ログファイルの検証

有効

最後に配信されたファイル検証の結果

4月 03, 2024, 13:39:20 (UTC+09:00)

SNS 通知の配信

arn:aws:sns:ap-northeast-
1:992860067891:aws-
controltower-AllConfigNotifications

最後の SNS 通知

4月 03, 2024, 13:42:01 (UTC+09:00)

CloudWatch Logs

編集

ロググループ

aws-controltower/CloudTrailLogs

IAM ロール

arn:aws:iam::771002807239:role/service-
role/AWSControlTowerCloudTrailRole

AWS Config – Organizations Aggregator

AWS Config

- ダッシュボード
- 適合パック
- ルール
- リソース
- ▼ **アグリゲータ**
 - コンプライアンスダッシュボード
 - 適合パック
 - ルール
 - インベントリダッシュボード
 - リソース
 - 認証
 - 高度なクエリ
 - 設定
 - 最新情報
- ドキュメント
- パートナー
- よくある質問
- 料金表

AWS Config > アグリゲータ

アグリゲータ

アグリゲータは、複数のアカウントおよびリージョンから AWS Config データを収集する AWS Config リソースタイプです。アグリゲータを使用して、複数のアカウントおよびリージョンについて AWS Config に記録されたリソース設定とコンプライアンスデータを表示します。

アグリゲータ

アグリゲータを作成

アクション

アグリゲータ名	ソースアカウント	ソースタイプ
aws-controltower-GuardrailsComplianceAggregator	15 アカウント	個々のアカウント

aws-controltower-GuardrailsComplianceAggregator のアグリゲータ概要

ダッシュボードに表示されるデータは複数の集約ソースから受信したものであり、異なる間隔で更新されます。データは数分遅れている可能性があります。

AWS リージョンまたはアカウント ID でフィルタリング

すべてのソースアカウントおよびリージョンからのデータ収集が、完全ではありません。 [詳細はこちら](#)

詳細を表示

リソースのインベントリ (4,297)

タイプ	リソース数
Config ResourceCompliance	1,564
IAM Role	739

コンプライアンス状況

43.54%

Config ルールのコンプライアンス

⚠️ 520 非準拠ルール

BLEA セキュリティ通知 1) 注意が必要な操作

Slackへの通知例

BLEAベースラインにより以下の注意が必要な操作を検知

- IAM Policyの変更
- セキュリティグループの変更
- NetworkACLの変更
- CloudTrailの設定変更
- API認証エラー
- アクセスキーの作成
- Root ユーザーによる操作

aws アプリ 19:33

CloudWatch Alarm | BLEA-BASE-SecurityAlarm-IAMPolicyChangeAlarm014E790D-1D70STFTL5XVA | ap-northeast-1 | Account: [redacted]

Threshold Crossed: 1 out of the last 1 datapoints [1.0 (30/07/21 10:28:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).

Metric Alarm Name	Alarm State
BLEA-BASE-SecurityAlarm-IAMPolicyChangeAlarm014E790D-1D70STFTL5XVA	ALARM
Namespace	Metric
CloudTrailMetrics	IAMPolicyEventCount

AWS API Call via CloudTrail | ap-northeast-1 | Account: [redacted]

The API 'aws.ec2 AuthorizeSecurityGroupIngress' was invoked in ap-northeast-1 by user 'arn:aws:sts::[redacted]:assumed-role/AWSReservedSSO_AWSAdministratorAccess_49066d74300efbfa/ohmurayu+abl[redacted].co.jp'.

User identity arn:aws:sts::946064424231:assumed-role/AWSReservedSSO_AWSAdministratorAccess_49066d74300efbfa/ohmurayu+abl[redacted].co.jp

User agent cloudformation.amazonaws.com

API AuthorizeSecurityGroupIngress

Event ID c0145e5d-1eac-49ed-beea-c50cc09f6844

Event time Fri, 30 Jul 2021 10:21:06 GMT

BLEA セキュリティ通知 2) セキュリティサービスの通知

Slackへの通知例

BLEAベースラインにより以下のAWSセキュリティサービス通知を受ける

- SecurityHub
 - CIS Benchmark および AWS Security Foundational Best Practices の Critical/Highレベル検知
- GuardDuty
 - Medium~Highの検出結果
- AWS Health
 - 稼働中リソースに影響するAWSイベントの発生

! Security Hub Finding | ap-northeast-1 | Account: [REDACTED]

EC2.2 The VPC default security group should not allow inbound and outbound traffic

This AWS control checks that the default security group of a VPC does not allow inbound or outbound traffic.

Finding Type: Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Be...

[続きを見る](#)

First Seen	Last Seen
Fri, 30 Jul 2021 07:45:34 GMT	Fri, 30 Jul 2021 07:45:36 GMT
Affected Resource	Severity
arn:aws:ec2:ap-northeast-1:[REDACTED]:security-group/sg-082d28fc71e2c2577	High

aws APP 3:07 PM

🚩 AWS Health Event | ap-northeast-1 | Account: [REDACTED] | open

Event type code: AWS_VPC_OPERATIONAL_NOTIFICATION

English follows Japanese

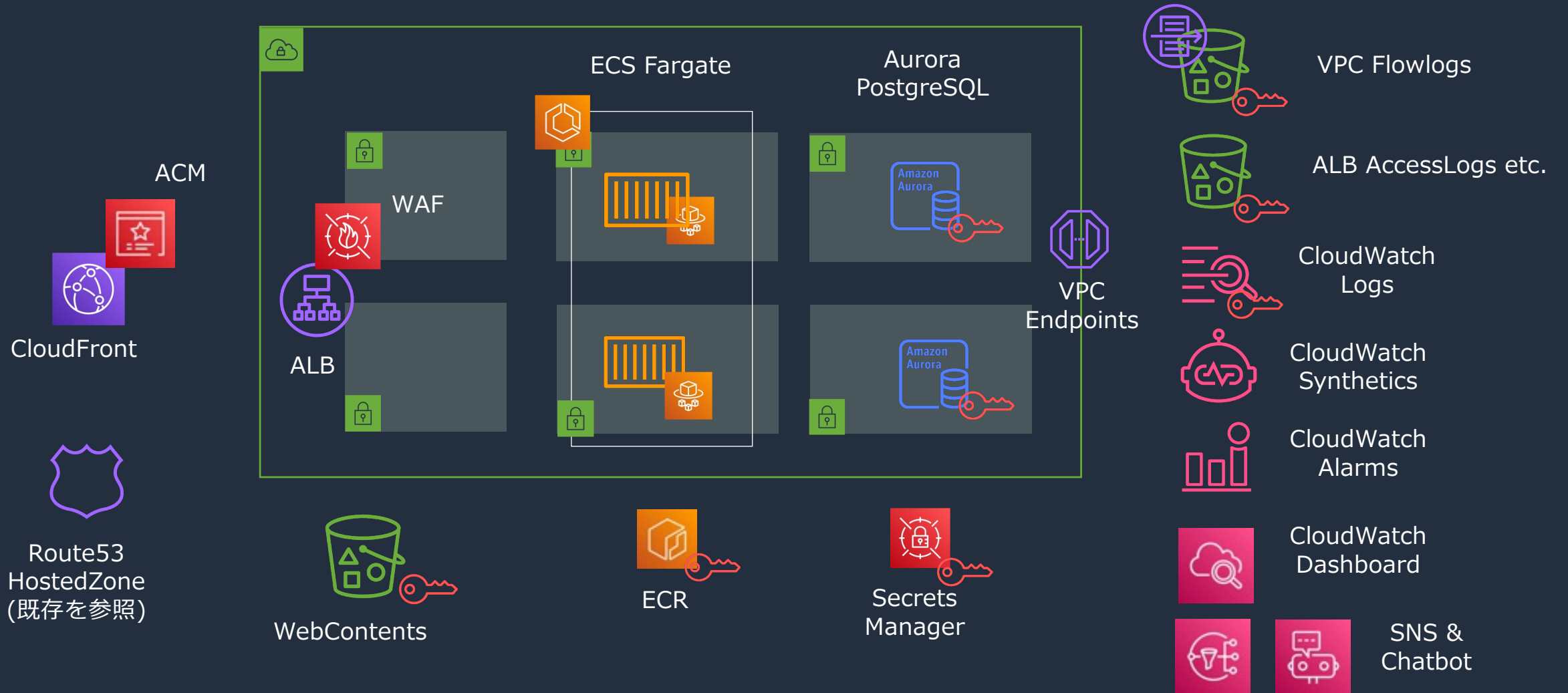
いつもお世話になっております。

AP-NORTHEAST-1 リージョンのお客様の AWS アカウントの VPC フローログリソースが、日本標準時間 2021 年 6 月 8 日午前 9:30 から 2021 年 6 月 13 日午前 11:04 まで、イベントの影響を受けていたため、ご連絡いたします。このイベント中に、S3 オブジェクト名にプレフィックスの 'day' セクションが追加された、誤ってフォーマットされた S3 プレフィックスを使用して口...

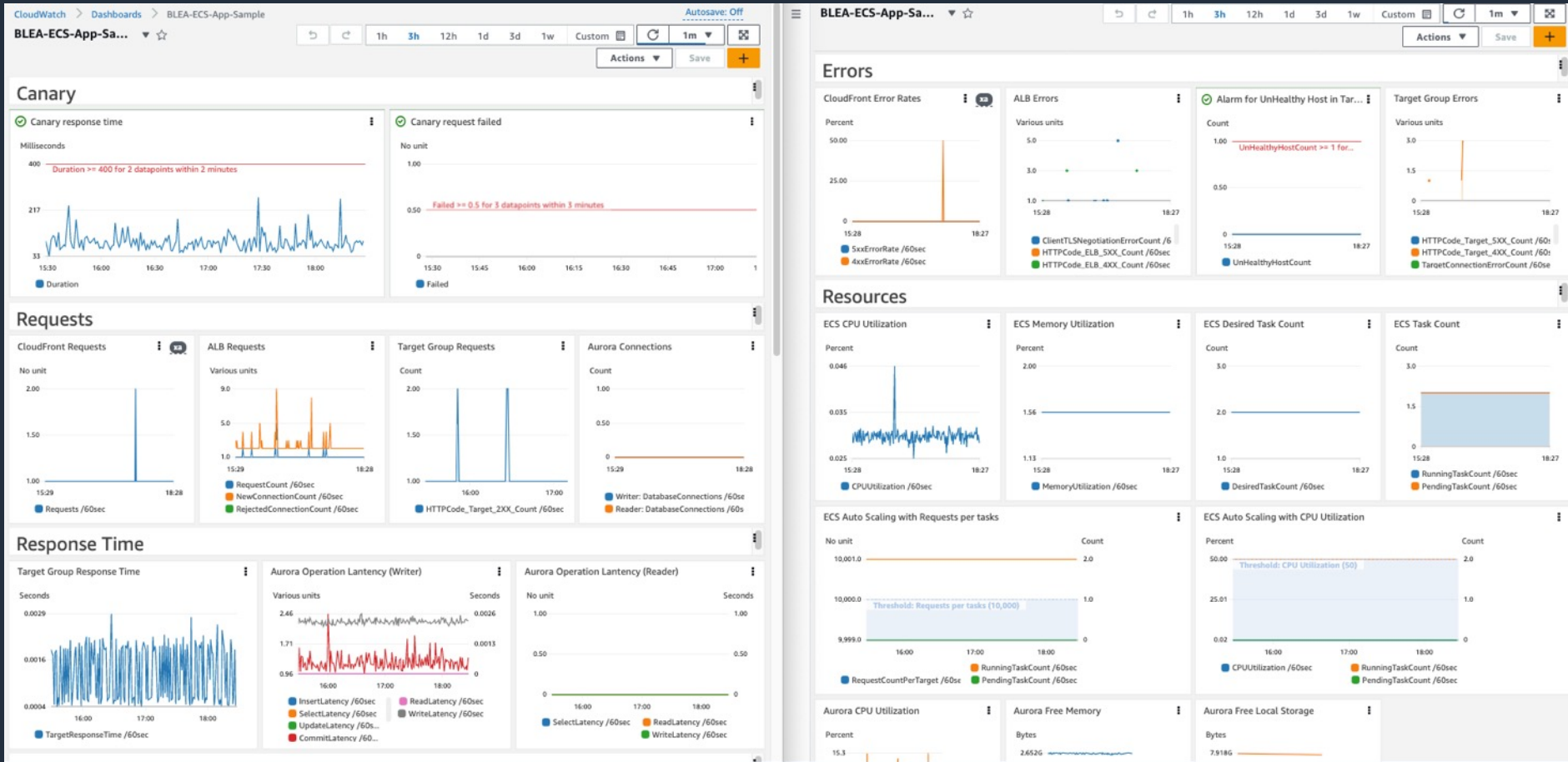
[See more](#)

BLEA ゲストシステム例 : Webアプリケーション (ECS+SSL)

(ver. 2021/10/26)

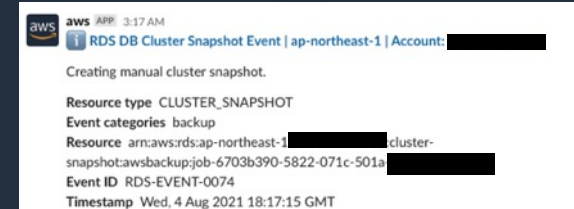
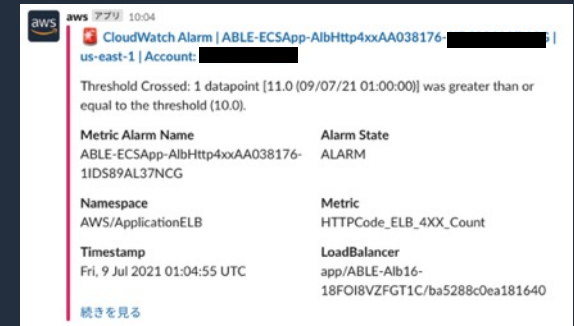


モニタリングアラートの通知とダッシュボード



サンプルアプリケーションの通知実装

- ECS/Fargate Service 平均CPU使用率
- ECS/Fargate Service タスク数
- ALB レスポンスタイム
- ALB HTTP 4XXエラー数
- ALB HTTP 5XXエラー数
- ALB HealthyHost数
- Aurora CPU使用率
- RDS イベント



※リソースの変更にCloudWatchダッシュボードを追従させるのは IaCでないとかかなり煩雑

ゲストシステムのセキュリティ実装

- アプリケーション用KMSキーによる各ストレージ暗号化（データ消去管理）
- ALBアクセスログバケットの暗号化（SSEのみ）と権限設定の最小化
- Webコンテンツバケット暗号化（SSEのみ）
- AWS外部で取得した独自ドメインによるHTTPS通信
- ECS FargateクラスタをProtected サブネットに配置
- ECRリポジトリのプライベートアクセス（Pull through cache 対応）とイメージスキャン有効化
- ECSサービスおよびデプロイメントイベントの通知
- Aurora クラスタおよびインスタンスの重要イベント通知
- Aurora 監査ログの出力
- Aurora ログインパスワードのSecret Manager登録
- Aurora Performance Insightの有効化とデータの暗号化

参考：Chatへのフロー情報集約の例

CloudWatch Eventsが
対応する
200以上のサービス群

EventBridge
(CloudWatch Events)



AWS Chatbot個別対応サービス

CloudWatch
Metrics



CloudWatch Alarm



CloudFormation



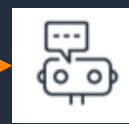
Developer
Services



AWS Budget



SNS Topic
(Chatbot用)



AWS
Chatbot

独自フォーマットが
必要なサービス



Slack #citical



SLOに影響が出ている
即時確認と対応が必要

ストック情報は
Wikiやチケットに記録



Slack #error

放置するとSLOに影響する
平日の朝夕に確認して
その日に対応方針を決めれば良い



Slack #info

長期的な方針検討に必要な情報
イテレーション(2weekなど)ごとに確認
必要な時に時系列で見ればよい

ベースラインの展開パターン

ベースラインの展開パターン

A. テンプレート配布方式（Pull型）

- テンプレートのみを提供。開発・運用チームがコードから展開する

B. サービスカタログ方式（Pull型）

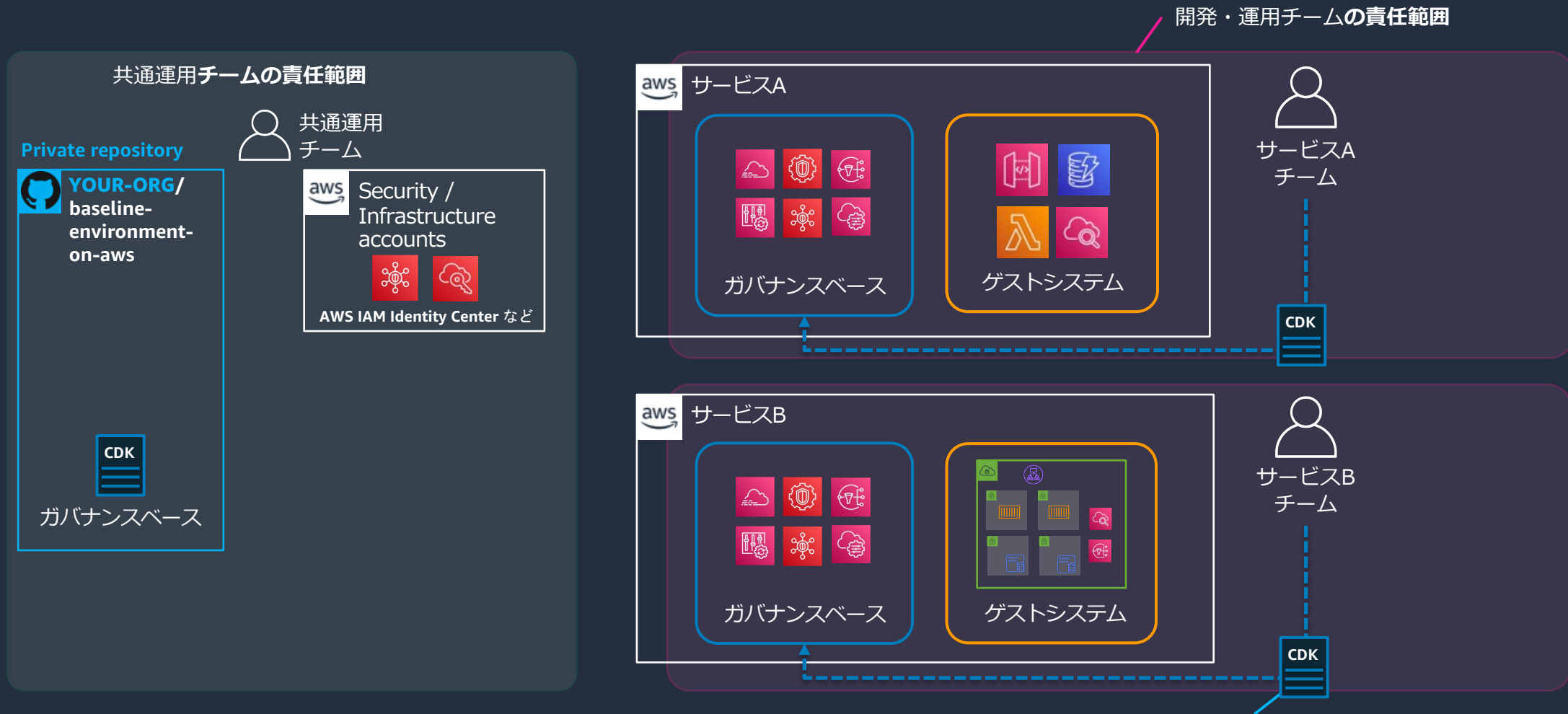
- Service Catalogを提供。開発・運用チームが自らデプロイする

C. AFC方式（Push型）

- 中央集権で共通運用チームがベースラインをデプロイ・管理する

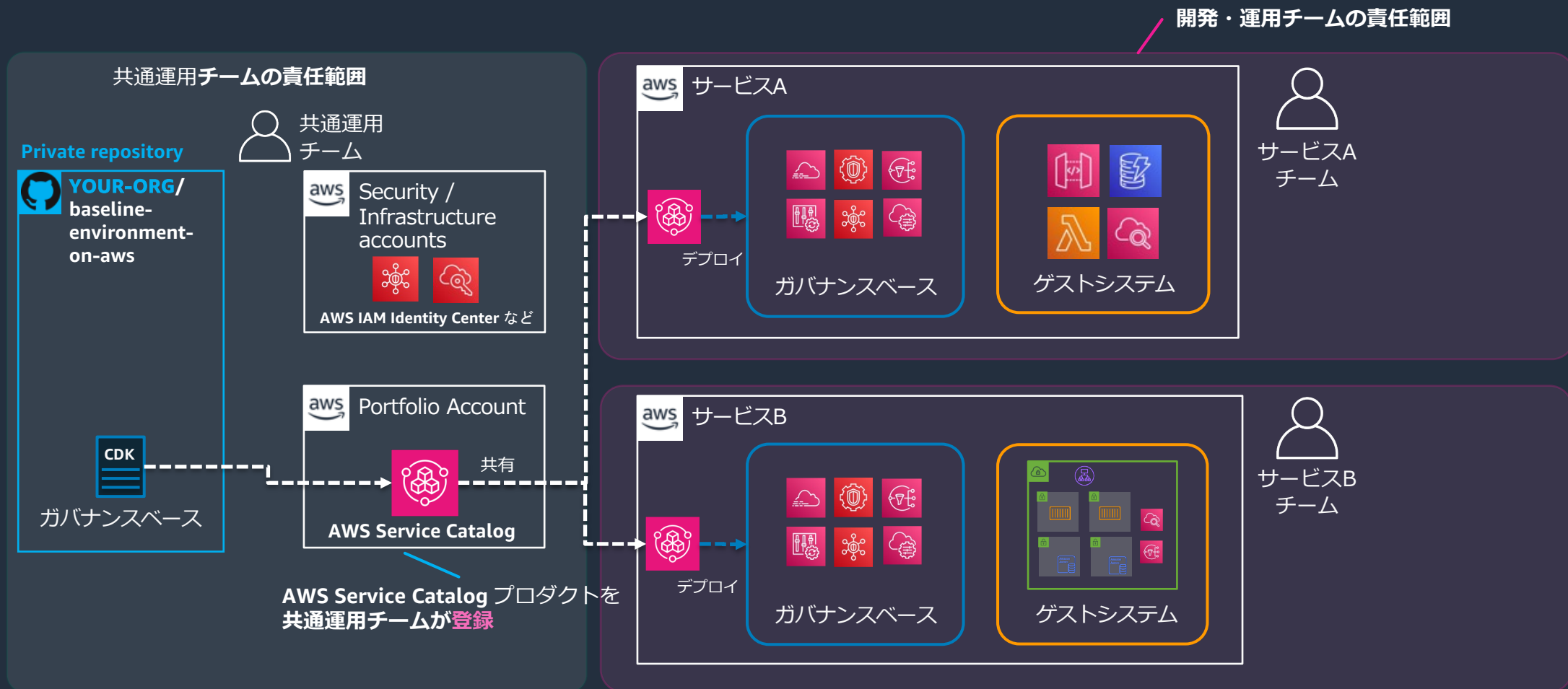
ベースラインの展開パターン A. テンプレート配布方式

- ガバナンスベースはテンプレート（コード）で提供し、開発・運用チーム自身がデプロイする基本の運用モデル
- 共通運用チームはガバナンスベースのコードをメンテナンス・配布する



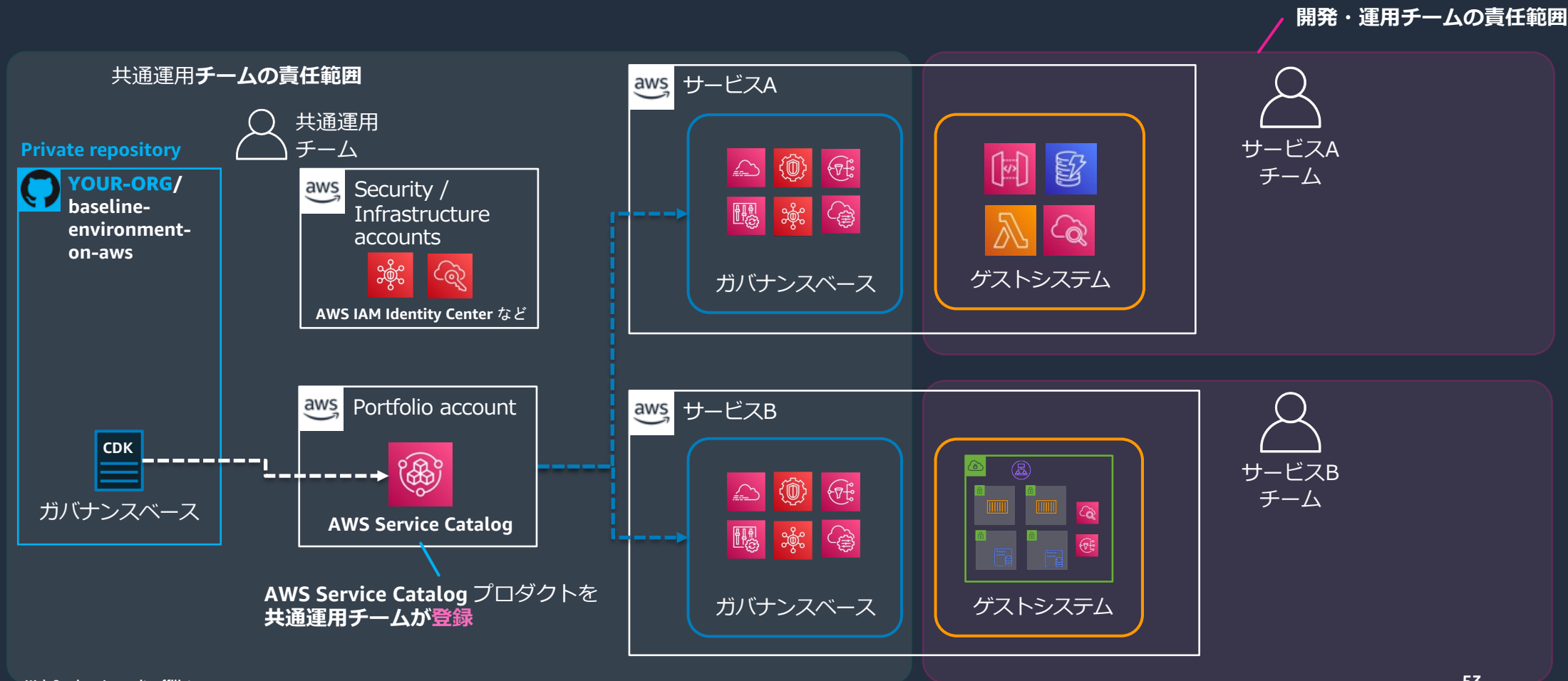
ベースラインの展開パターン B. サービスカタログ方式

- 共有されたService Catalogを使って、開発・運用チームがガバナンスベースを自分のアカウントへデプロイする（Pull型）



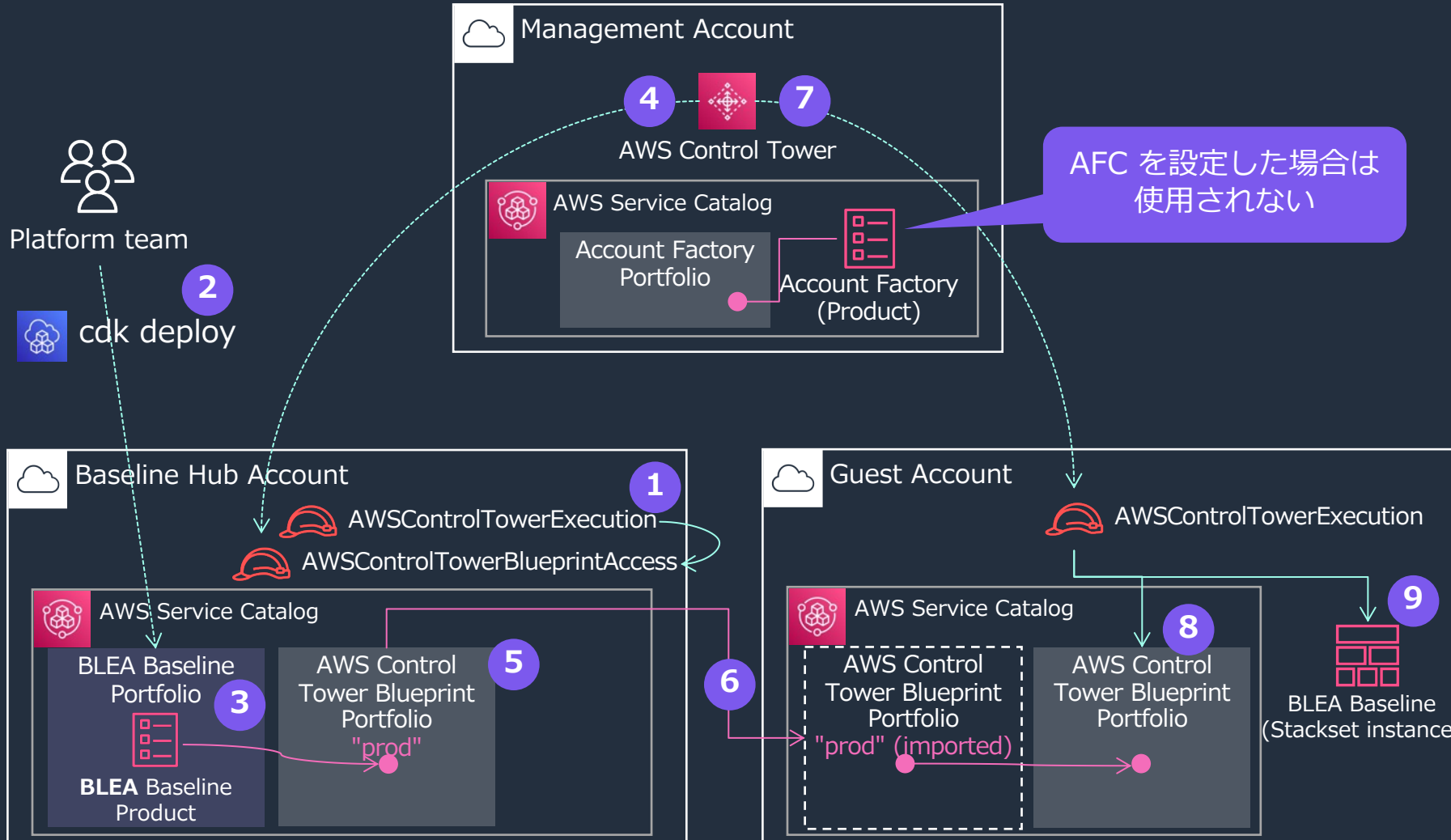
ベースラインの展開パターン C. AFC方式

- AWS Control Tower Account Factory Customization (AFC) でアカウント発行時に自動適用 (Push型)
- ガバナンスベースの更新も、共通運用チームが Control Towerから実施 (Push型)



参考 : Account Factory Customization (AFC) の動作

* CT = AWS Control Tower



- 1 (事前準備) CT 用のロールを作成
- 2 CDK コマンドでガバナンスベースをデプロイ
- 3 CDK から Service Catalog 製品とポートフォリオを作成
- 4 CT でブループリントを設定して Account Factory を実行
- 5 CT 用のポートフォリオを作成し指定された製品を紐付け
- 6 CT がポートフォリオをゲストアカウントに共有
- 7 CT がゲストアカウントでポートフォリオの共有を受入れ
ゲストアカウント用のポートフォリオを作成して共有済みの製品を紐付け
- 8 ポートフォリオを作成して共有済みの製品を紐付け
- 9 Service Catalog 製品をプロビジョニング (StackSet)

BLEA のカスタマイズ

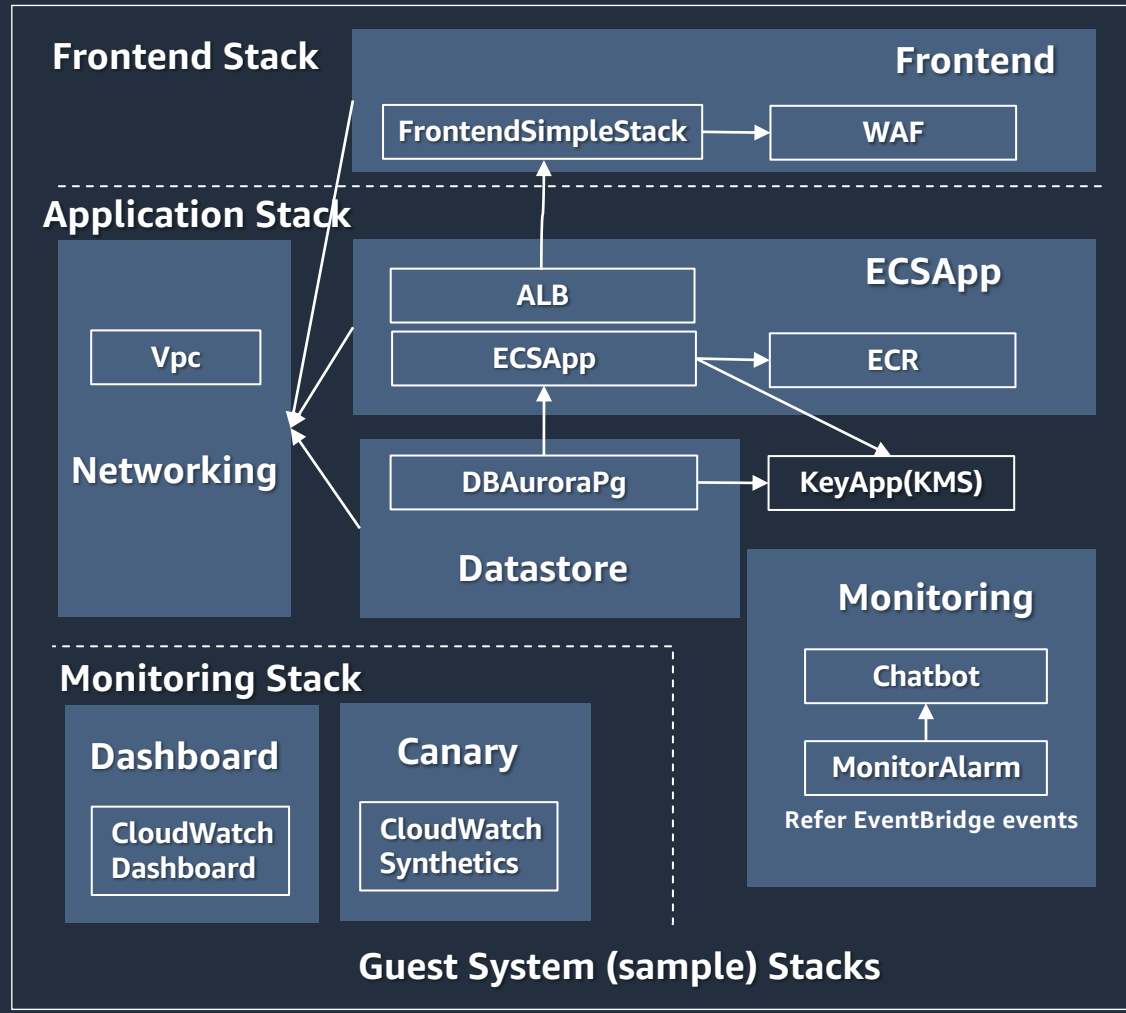
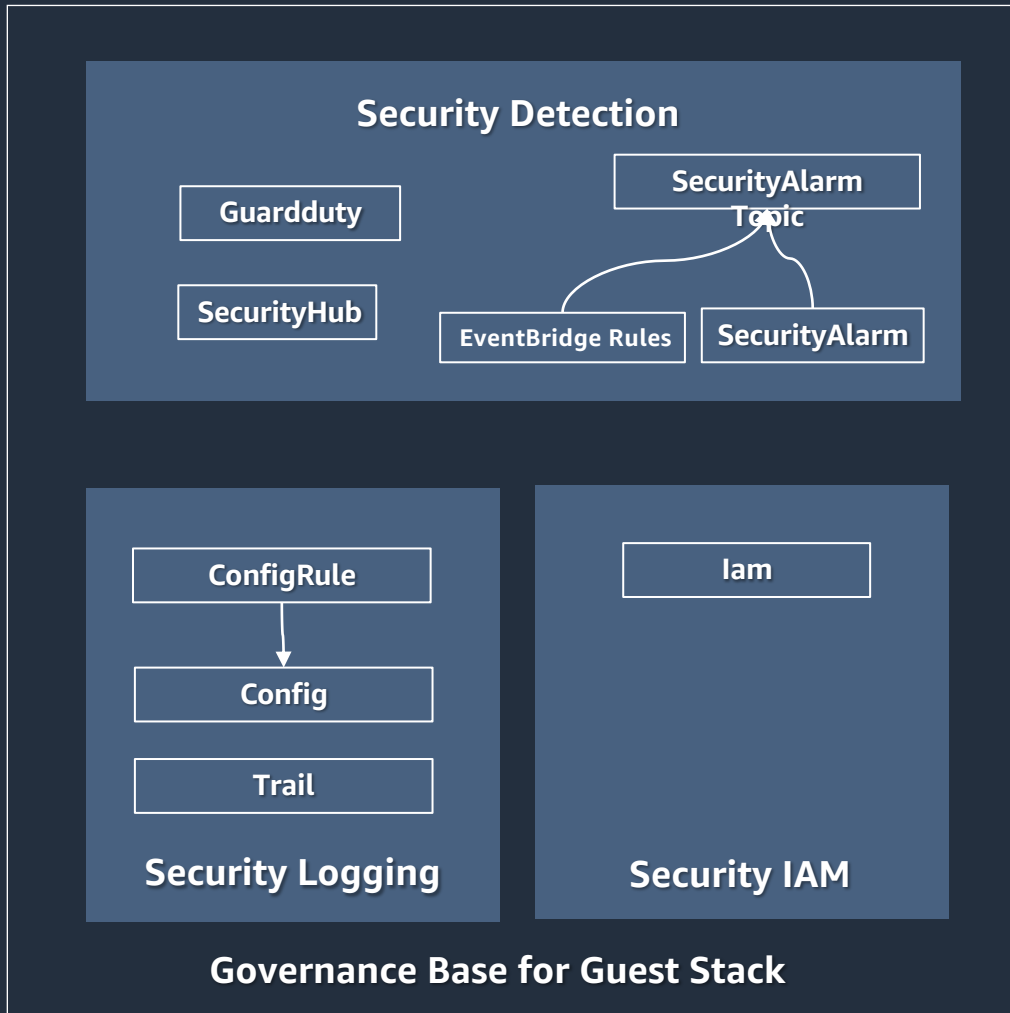


BLEAのカスタマイズガイド

- **ガバナンスベース**は基本的に修正不要
 - 最低限必要なセキュリティ設定を有効化
- **ゲスト基盤**は現状の設定をベースに必要な機能を追加する
 - セキュリティ要件に合わせてSecurityHubやAWSConfigのCompliance状態を確認
- **ゲストシステム**は用途に合わせて選択、カスタマイズが前提
 - よく使いそうなコード素材がサンプルの中に散りばめられている
 - コピーしてパラメータ変更でできる部分を多く
- フラットなコード構成
 - クラス化による隠蔽より、設定のわかりやすさを優先
 - 自社用には独自の仕様を埋め込んだクラスを作ってもよい
- サンプルがどこまで実装しているか
 - サンプルテンプレートはSecurityHubの「AWSのベストプラクティス」および「CISベンチマーク」で、「すぐに対処が必要 (CRITICAL)」 「優先して対処が必要 (HIGH)」がないよう実装

Baseline Environment on AWS – Component dependency

- Governance Base and Guest System can deploy independently



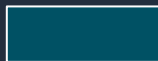
テンプレートを利用した開発の例



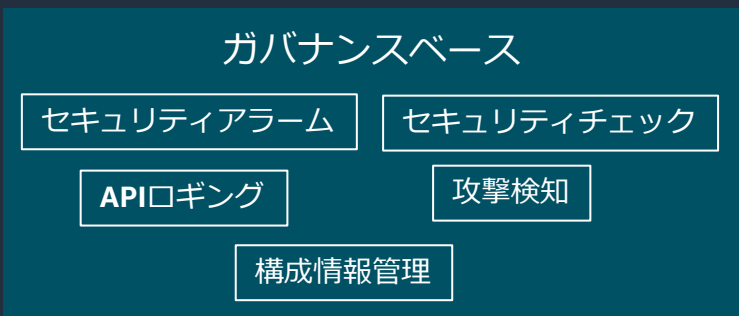
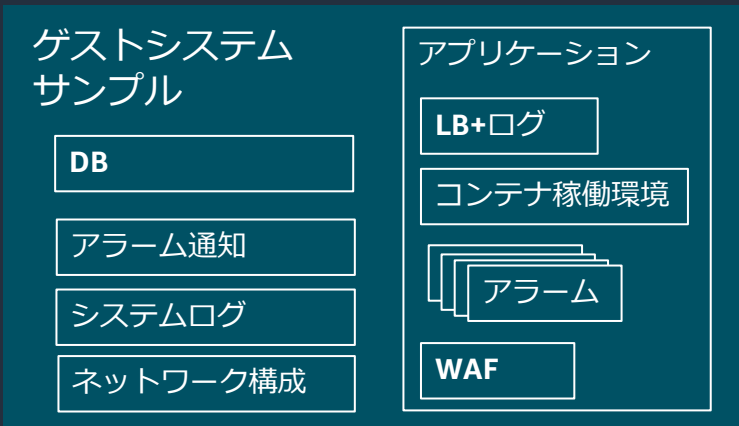
新しいコードの作成



テンプレートコードのパラメータを変更



変更なし（そのまま利用）

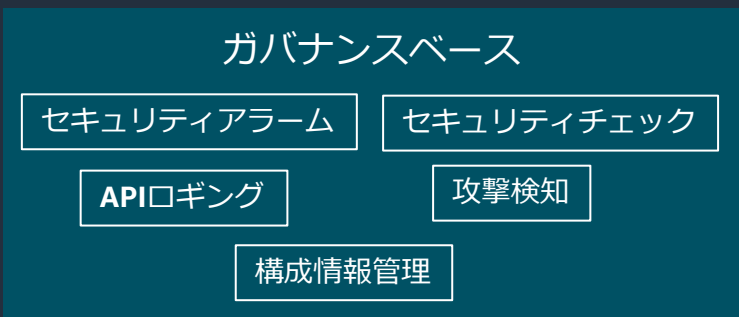
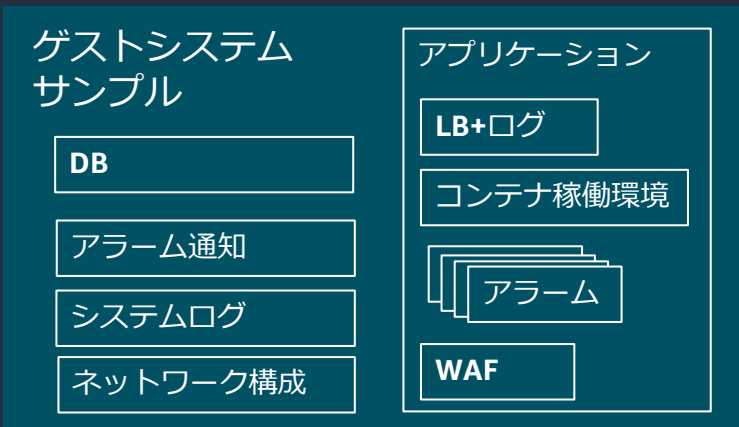


BLEAテンプレート



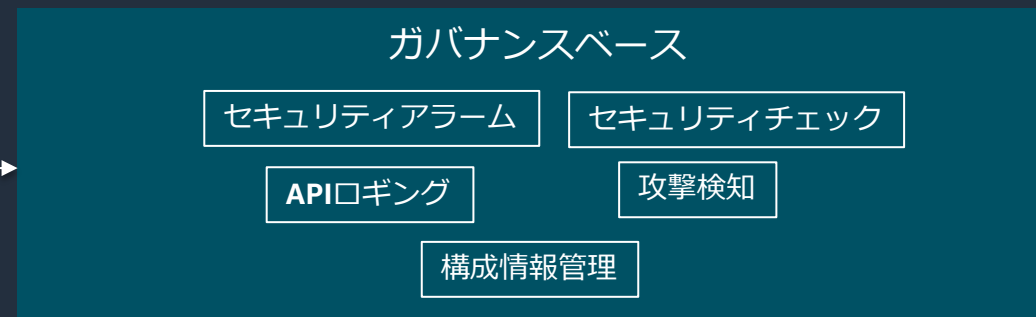
テンプレートを利用した開発の例

- 新しいコードの作成
- テンプレートコードのパラメータを変更
- 変更なし（そのまま利用）



BLEAテンプレート

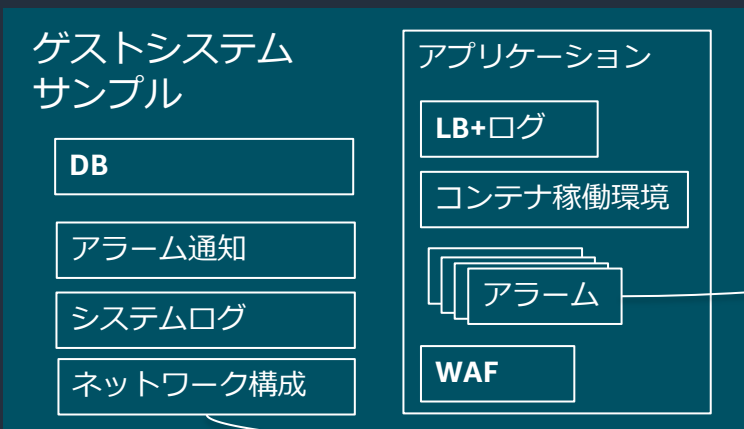
ガバナンスベースはそのまま利用



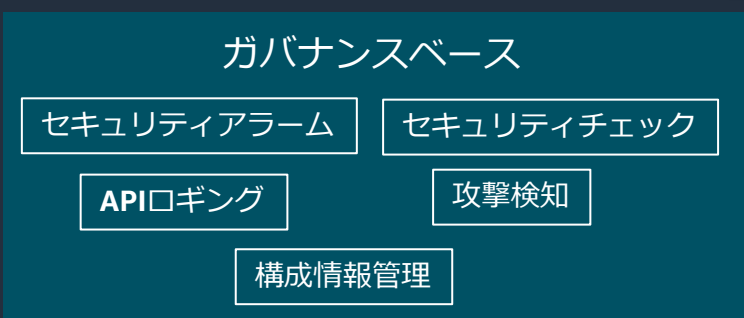
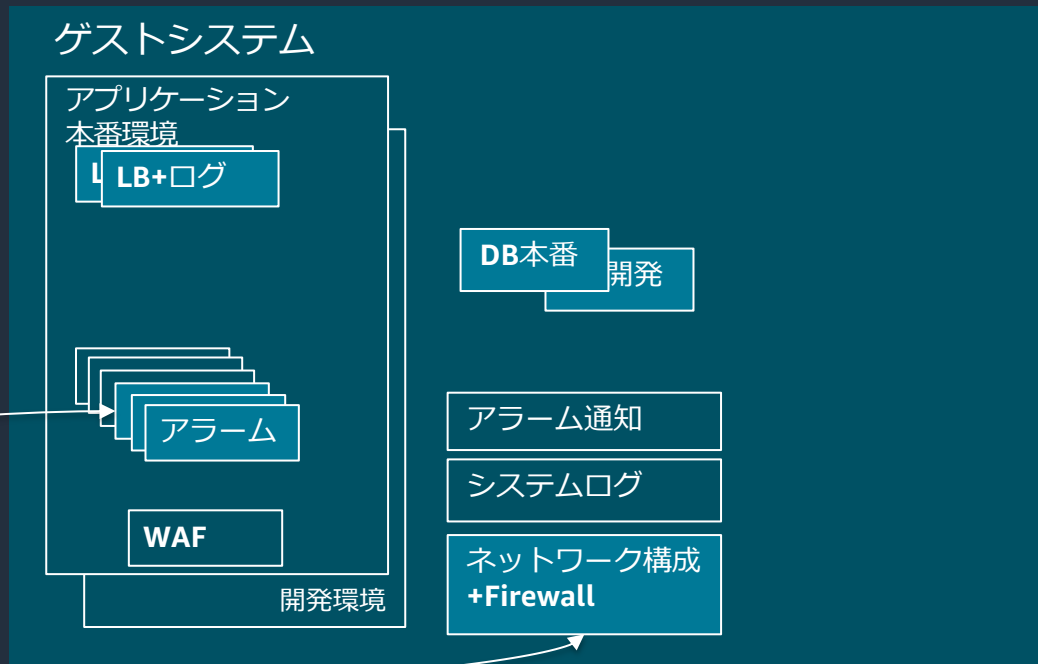
個別システム

テンプレートを利用した開発の例

- 新しいコードの作成
- テンプレートコードのパラメータを変更
- 変更なし（そのまま利用）

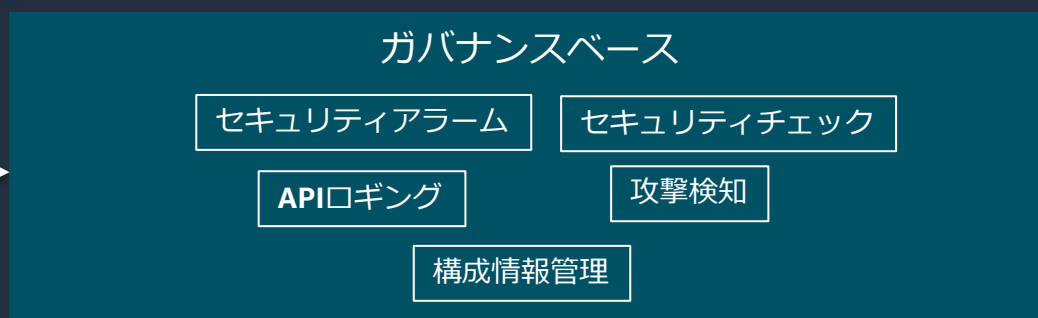


コピー+パラメータ変更で
監視項目を追加



ログやネットワーク構成は
一部改変してそのまま利用

ガバナンスベースは
そのまま利用

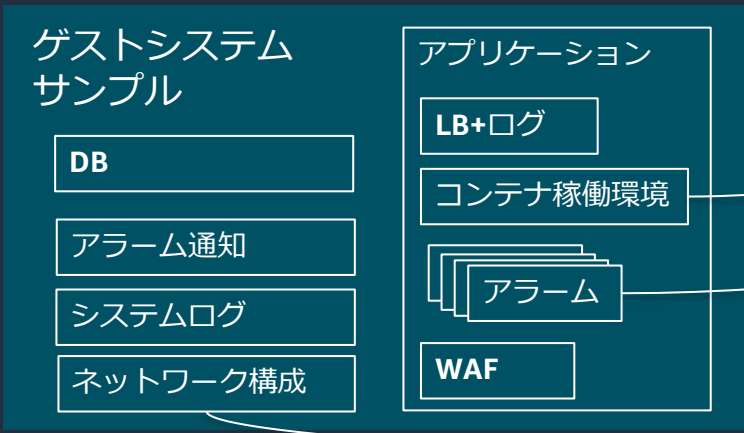


BLEAテンプレート

個別システム

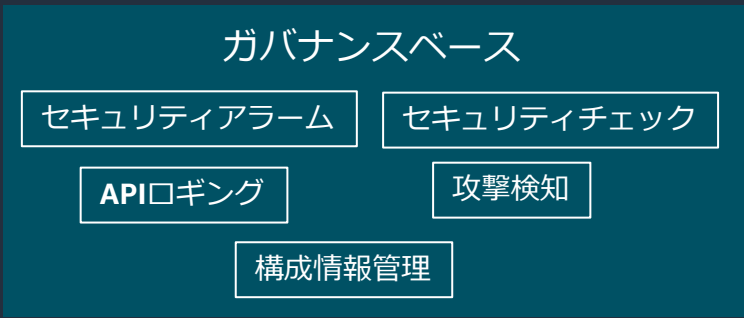
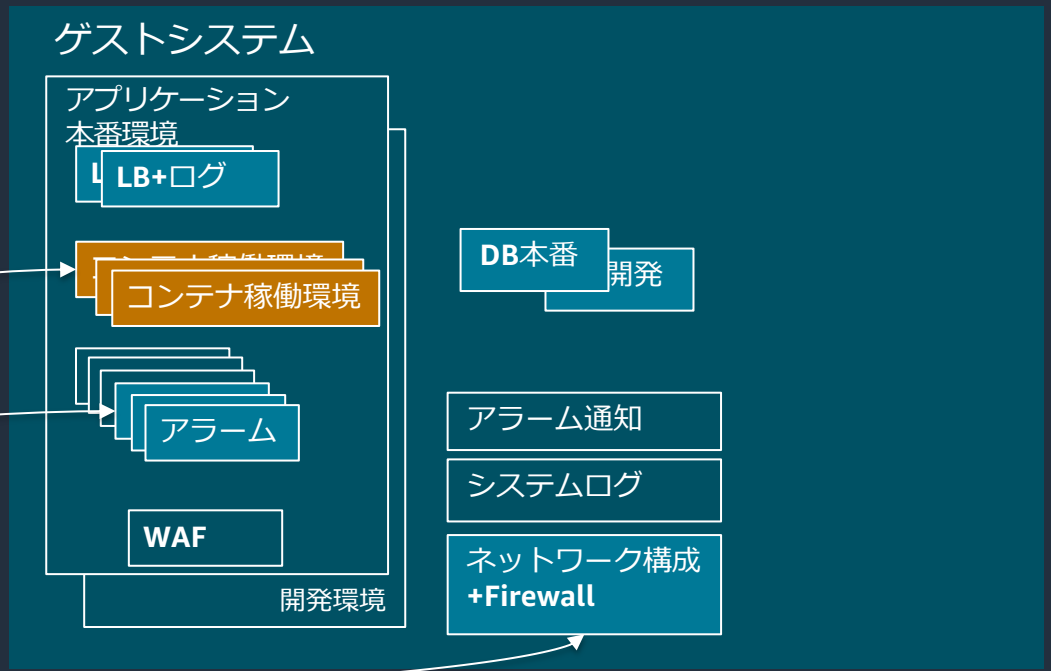
テンプレートを利用した開発の例

- 新しいコードの作成
- テンプレートコードのパラメータを変更
- 変更なし（そのまま利用）



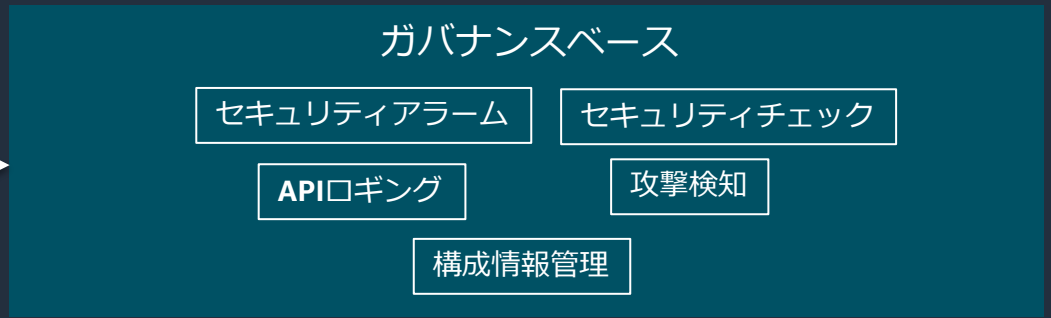
アプリ仕様に合わせて
コードをカスタマイズして開発

コピー+パラメータ変更で
監視項目を追加



ログやネットワーク構成は
一部改変してそのまま利用

ガバナンスベースは
そのまま利用

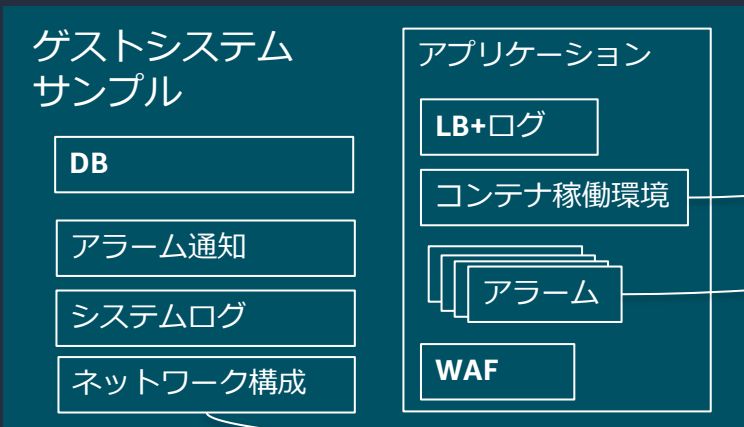


BLEAテンプレート

個別システム

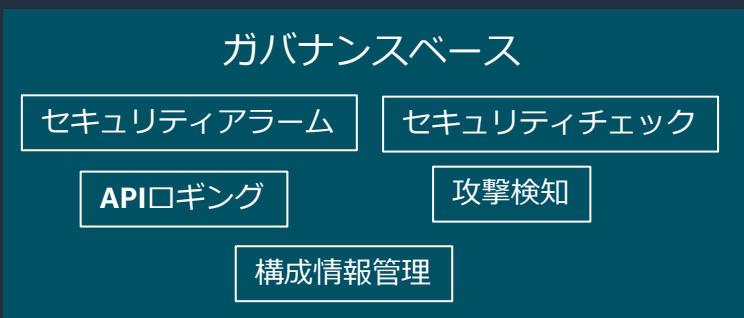
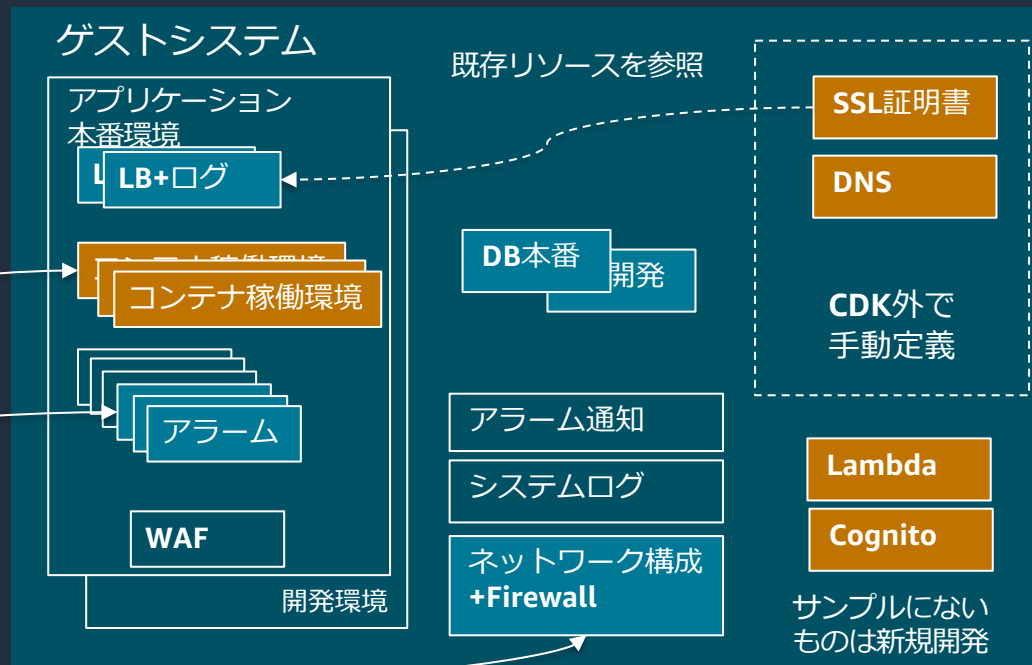
テンプレートを利用した開発の例

- 新しいコードの作成
- テンプレートコードのパラメータを変更
- 変更なし（そのまま利用）



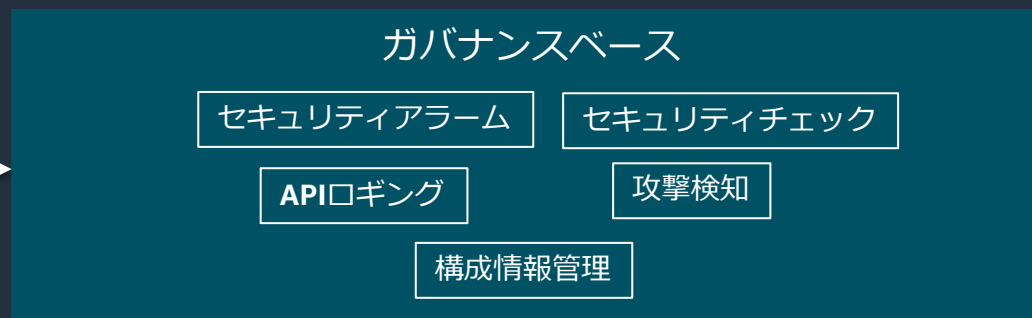
アプリ仕様に合わせて
コードをカスタマイズして開発

コピー+パラメータ変更で
監視項目を追加



ログやネットワーク構成は
一部改変してそのまま利用

ガバナンスベースは
そのまま利用



BLEAテンプレート

個別システム

參考資料



BLEA（関連）公開資料

- BLEA
 - <https://github.com/aws-samples/baseline-environment-on-aws>
- AWS資料
 - [テンプレートによるAWS環境のガバナンス](#)（AWS Summit 2022 発表資料）
 - [BLEA 開発チームが学んだ AWS CDKの開発プラクティス](#)（CDK Conference 2023 発表資料）
- ユーザー様資料
 - [みずほリサーチ&テクノロジーズが AWS CDK で実装したマルチアカウント管理の仕組み](#)
 - [オンプレシシステムのクラウドリフトにおいてBLEAを利用してセキュリティのベースラインを確保した話](#)

閉域網での利用を前提としたCDKのサンプルテンプレート

Amazon Web Services ブログ

閉域網での利用を前提としたCDKのサンプルテンプレートを公開しました

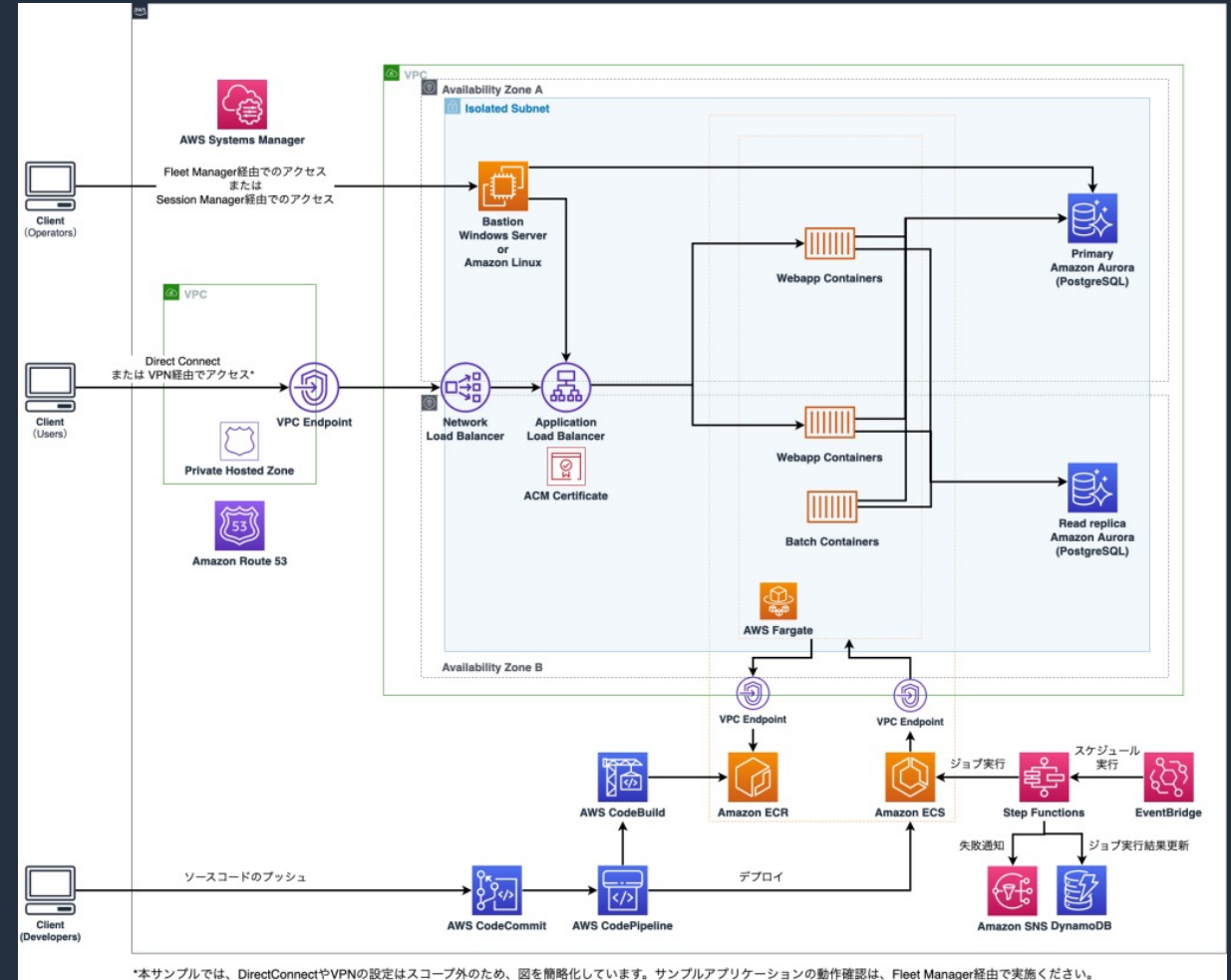
by Yozo Suzuki | on 10 3月 2023 | in General, Government, Public Sector, State Or Local Government, Technical How-To | Permalink | Share

こんにちは、公共部門でプロトタイプSAをしている鈴木です。

デジタル庁が整備するガバメントクラウドではAWSが採択されており、中央省庁や地方自治体等でAWSをご利用いただくお客さまが増えてきました。

このブログではこれからAWSを利用し始めるお客さまやアプリケーションのモダナイズをご検討されているお客さま向けに開発した、閉域網での利用を前提としたサンプルテンプレートについてご紹介します。

BLEAのゲストシステムサンプルとして利用可能



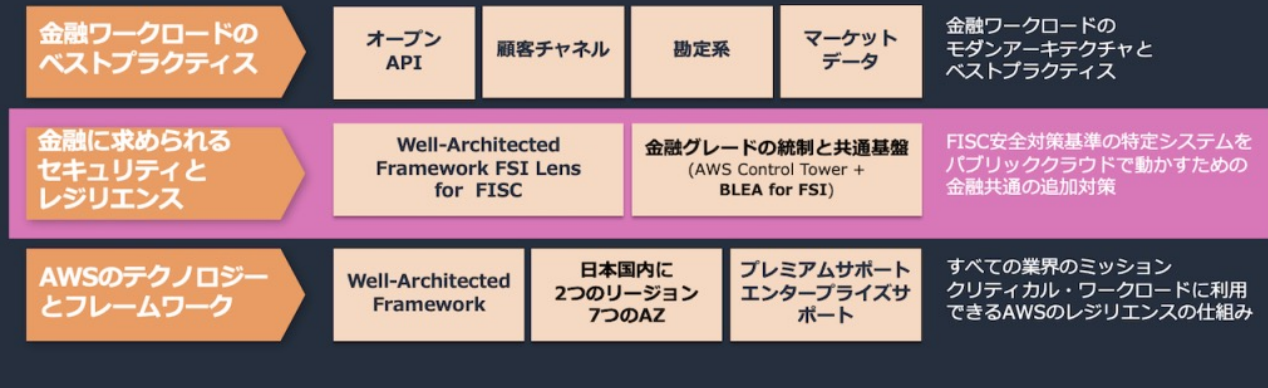
<https://aws.amazon.com/jp/blogs/news/announcing-template-for-closed-network-system-workloads-on-aws/>
<https://github.com/aws-samples/template-for-closed-network-system-workloads-on-aws>



金融リファレンスアーキテクチャ

金融リファレンスアーキテクチャ日本版

日本の金融インダストリーの高信頼性を担保するフレームワーク



BaseLine Environment on AWS for Financial Services Institute (BLEA for FSI)

BLEA for FSI は [BLEA](#) をベースとして、FISC 準拠が求められる 金融グレードの統制と共通基盤のベースラインとなる CDK のテンプレートを提供します。マルチアカウント AWS 環境をセキュアに構築・管理するための AWS Control Tower環境を前提とし、ゲストAWSアカウントに FISC 実務基準に対応したガードレールを組み込むことを強力にサポートします。BLEA for FSI は共通の統制基盤を構築する Control Tower ベースのガバナンスベースと金融ワークロード サンプルアプリケーションから構成されます。※ BLEA for FSI で提供するCDK コードはサンプル実装となるため、実際の構築・運用にあたってはお客様側でのカスタマイズおよび検証が必要となります。

<https://aws.amazon.com/jp/blogs/news/financereferencearchitectureproductionseminar202210/>

<https://github.com/aws-samples/baseline-environment-on-aws-for-financial-services-institute>



日本が目指すデジタル社会の姿と、それを実現するために必要な考え方と取り組みについて(SP-01)

ガバメントクラウド テックブログ

♡ 76

デジタル庁 ガバメントクラウド
2022年1月24日 17:11



「政府共通のクラウドサービスの利用環境です。クラウドサービスの利点を最大限に活用することで、迅速、柔軟、かつセキュアでコスト効率の高いシステムを構築可能とし、利用者にとって利便性の高いサービスをいち早く提供し改善していくことを目指します」

- **Cost (コスト効率、最適化)** : 投資対効率
- **Elasticity (弾力性)** : 伸張性、拡張性を支える性能
- **Performance (パフォーマンス)** : システム全体のパフォーマンス
- **Agility (俊敏性)** : 変化への追従性
- **Velocity (ベロシティ)** : 実行の加速度
- **Security (セキュリティ)** : セキュリティ性能
- **Resiliency (レジリエンシー)** : 復旧や回復性能
- **Observability (可観測性)** : システムの内部状況の把握性能
- **Transparency (透明性)** : 目的に対する貢献度合いの可視化性
- **Improvability (改善性)** : 改善のしやすさ
- **Automation (自動化)** : 自動化のしやすさ

「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」の改定について

2022年5月24日
ガバメントクラウドチーム

参考

- [ガバメントクラウド テックブログ](#)
- [「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」の改定について](#)

改定の概要

- 旧方針（2018年6月に初版）は、クラウドファースト（まずはクラウドの利用を検討する）だったが、本方針では**クラウドスマート**（クラウドを賢く適切に利用する）を目的とする。
- スマートとは**モダン技術**の利用であり「**マネージドサービス**」と「**IaC (Infrastructure as Code)**」が中心。

「3.4 アプリケーションとシステム刷新」より抜粋

- アプリケーションとインフラを分離した調達は、アプリケーションのモダン化とスマートなクラウド利用を阻害する要因となるため、クラウドでは見直しが必要となる。（中略）クラウド移行に向けた刷新においては、**インフラとアプリケーションを同時に刷新**することが合理的である。また、事業者や調達についても**インフラとアプリケーションを原則として分離**するべきではない。
- オンプレミスにおけるアプリケーションとクラウド上のアプリケーションでは、以下で大きく異なるので、新規開発時やアプリケーション刷新時には特に留意されたい。
 - **モダンアプリケーションとする**
 - オンプレミス時代の旧来技術・運用を単純に踏襲しない
 - オンプレミス時代の人海戦術的な方式を踏襲せず自動化する
 - 単なるシステム監視ではなく定量的計測を行う
 - セキュリティ対策もクラウドに最適化させる
 - 開発プロセスをクラウドに最適化させる
 - 稼働日で完成ではなく日々の運用で改善していく



ガバメントクラウドにおけるIaC(Infrastructure as Code)の考え方

♥ 96

デジタル庁 ガバメントクラウド
2022年1月24日 17:12



デジタル庁クラウドチーム

Cloud Architect 山本教仁

ガバメントクラウドでは、コスト効率、迅速性、柔軟性、セキュリティを基本的指標にしています。第1回では、この指標を実現するための技術要素の1つであるInfrastructure as Code（以下、IaC）についてガバメントクラウドにおける考え方を説明します。

IaCのメリット

IaCのコードはいったん作成すればそれを何回でも別の環境でも流用可能です。典型的なインフラ構成をコード記述し、それをマスターテンプレートとして使い回すことで、(1)インフラ構成を迅速に作れ、(2)設計工数と期間を短縮することでインフラ構築コスト削減につながり、(3)手元のコードに記述された内容がインフラ構成のすべてなのでブラックボックス化を防ぎ頻繁なアプリケーションの改善リリースに対しても柔軟に対応でき、(4)マスターテンプレートの一部を強制することでガバナンスを効かせてセキュリティレベルを保持でき、(5)IaCを徹底すればインフラ（OS）へのログインがなくなるためセキュリティ機能や運用もシンプルになる、という5つのメリットがあります。



Thank you!