

AWS-24

運用視点で考える AWS の セキュリティ体制強化

辻本 雄哉

技術統括本部 金融ソリューション本部 シニアソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社



自己紹介

名前：辻本 雄哉（つじもと ゆうや）

所属：アマゾン ウェブ サービス ジャパン合同会社

技術統括本部 シニア ソリューションアーキテクト

経歴：外資系 SIer のインフラエンジニアとして金融システムのミッションクリティカルシステムを担当

現在は金融機関のお客様、特に保険業界のお客様のクラウド活用をご支援

好きな AWS サービス：AWS Transit Gateway, AWS Shield

趣味：スノーボード

好きなもの：ドクターペッパー



本日の Agenda

1. はじめに
2. クラウド活用におけるセキュリティ運用の課題
3. 課題解決のポイント
 - ① セキュリティ体制の強化に必要な要素
 - ② AWS サービスを活用したセキュリティ運用
4. まとめ

はじめに

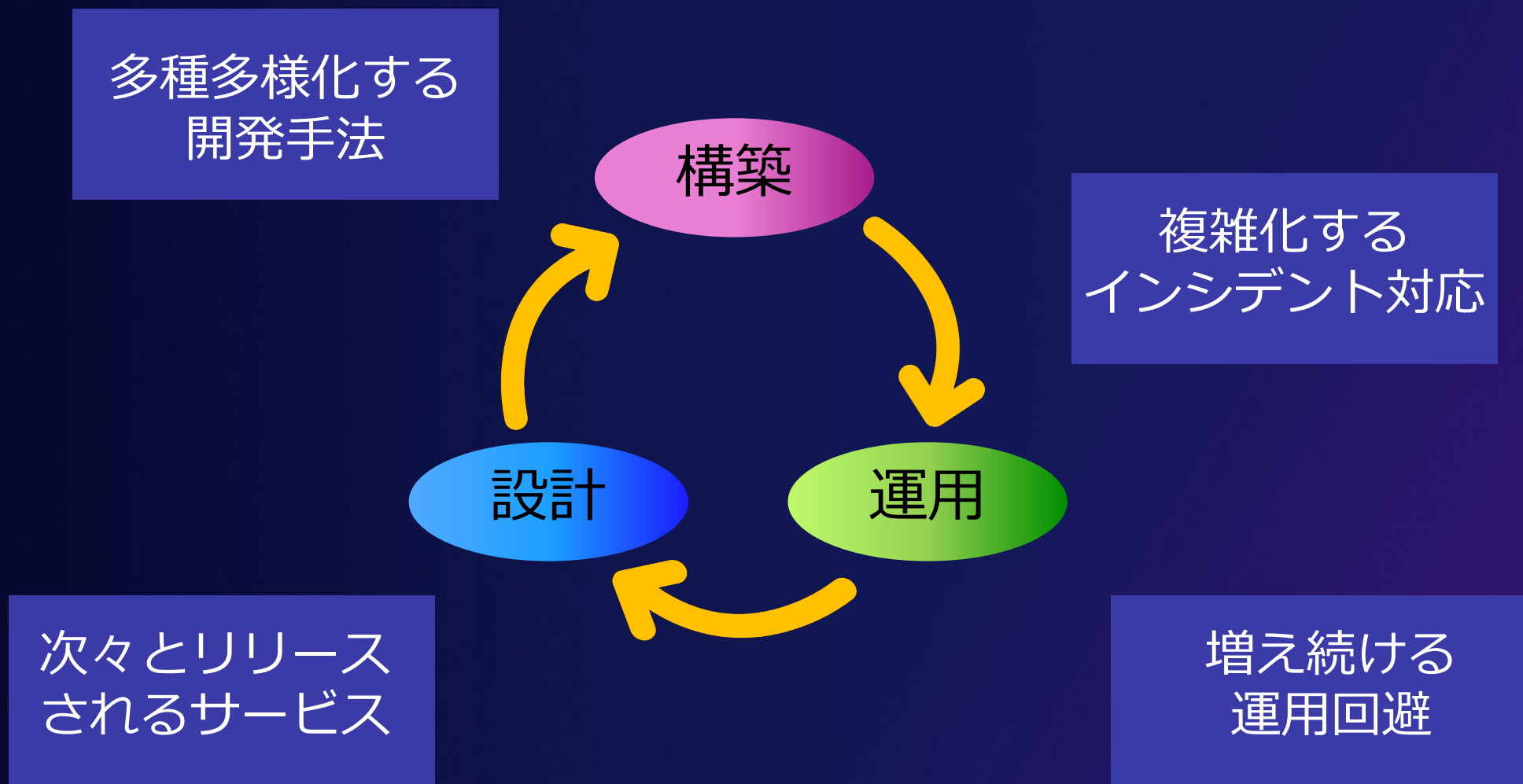
本セッションでは、これから AWS を本格的に活用することを検討している開発チーム／運用チーム／セキュリティチームの方に向け、セキュリティ運用をどのように効率よく実践していくかをご紹介します。

【このような課題感をお持ちの方】

- AWS のアカウントが増えるにつれ、セキュリティ対応が心配
- 運用の効率が良くない
- セキュリティ対応のための作業が増えてきていて、システム開発のスピードが落ちている

クラウド活用における セキュリティ運用の課題

セキュリティ運用を取り巻く様々な状況



セキュリティチームの課題

セキュリティ
チーム

開発チーム

運用チーム

単独視点による
弊害

セキュリティチェックシートでの
対応内容は担当者依存

開発・運用チームへの
セキュリティ対応の負担増

調査は運用・開発チーム任せとなり、
対応スピードが鈍化

運用チームの課題

セキュリティ
チーム

開発チーム

運用チーム

単独視点による
弊害

設計フェーズに関与せず、
運用に関する要件が適切に伝わらない

運用回避対応による負担増

運用性の向上とビジネスの成果が
結びつかない

開発チームの課題

セキュリティ
チーム

開発チーム

運用チーム

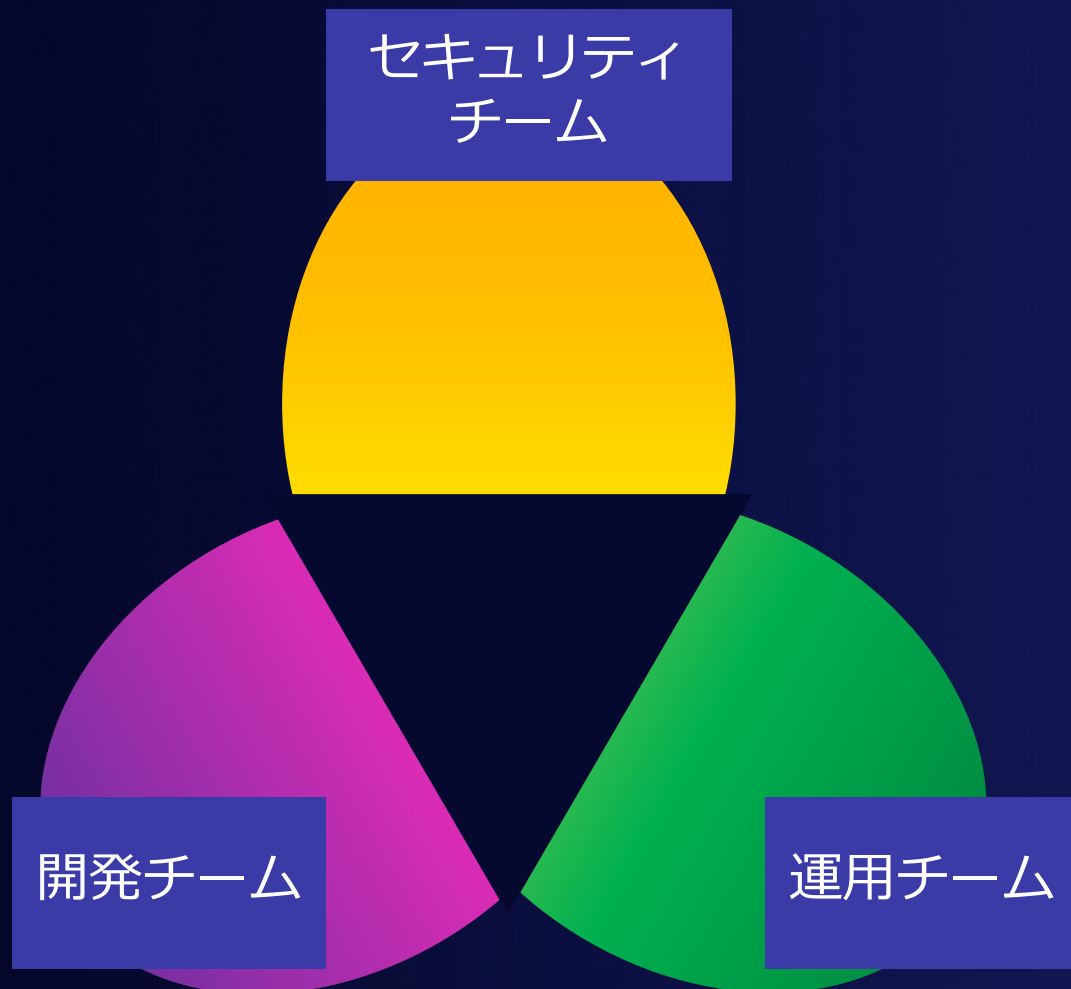
単独視点による
弊害

業務開発を優先し、運用は後回し

開発期間の短縮に伴う作業負荷の増大

最後の手段は「運用回避」

各チームの単独視点による課題



チームをまたがる視認性の欠如

課題・問題の後回し

属人的で非効率な運用

スケールへの対応が困難



運用効率が非常に低下する要因

課題解決のポイント

課題解決のために重要となる要素は 「視認性の向上」と「セキュリティ体制の強化」



クラウドベースのワークロードとアプリケーションの運用効率を向上させる



視認性の向上



セキュリティ体制の強化

運用効率の向上に必要な要素



クラウドのメリットを
活かした運用

- セキュリティ・開発・運用
チームで可視化を統合
- 運用の自動化でセキュリティ
対応を高度化



AWSセキュリティサービスを
活用し、効率化

- 継続的な脅威の検出
- ワークフローの最適化
- 修復時間の最小化



クラウドのメリットを
活かした運用

- セキュリティ・開発・運用
チームで可視化を統合
- 運用の自動化でセキュリティ
対応を高度化



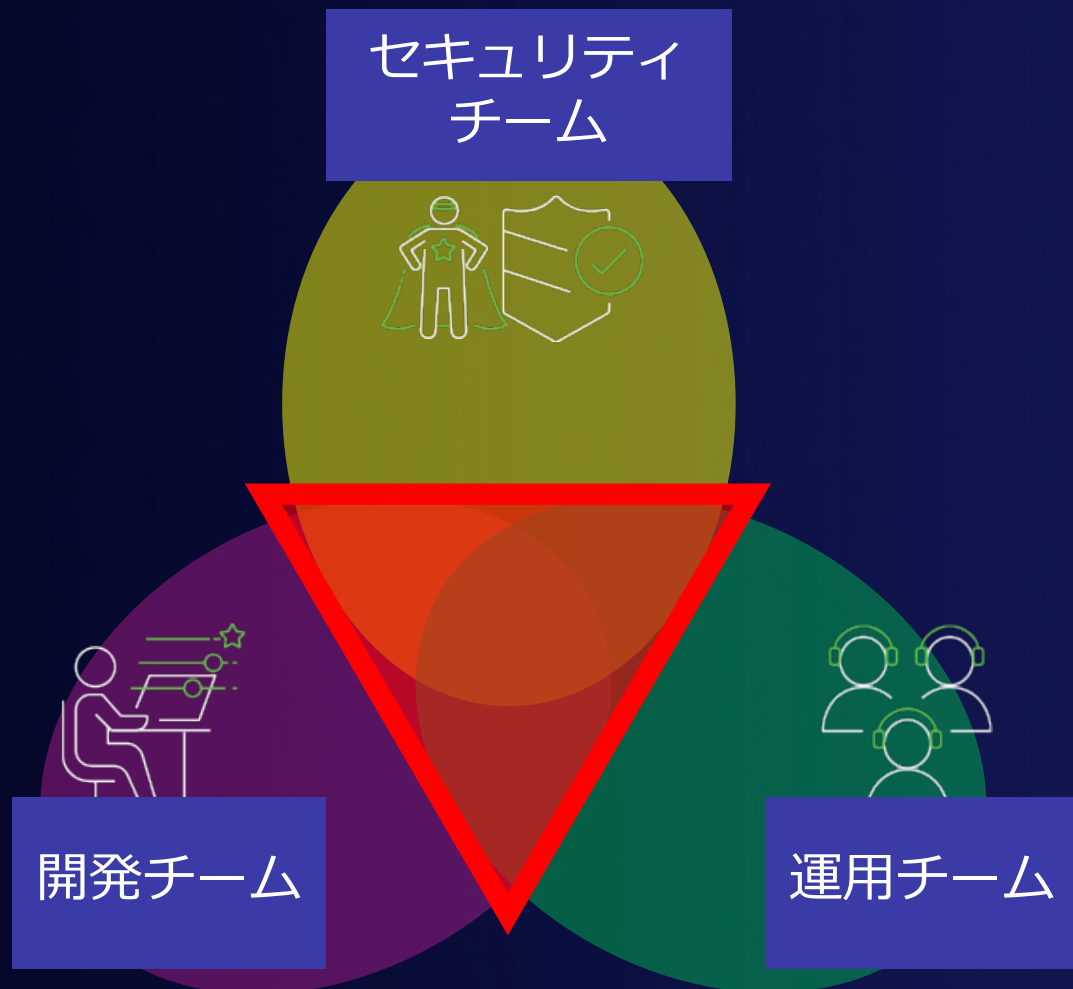
AWSセキュリティサービスを
活用し、効率化

- 継続的な脅威の検出
- ワークフローの最適化
- 修復時間の最小化

課題解決のポイント①

クラウドのメリットを活かした運用

開発・運用・セキュリティチームで共通の視点を



システムのライフサイクル全体を
意識した視認性の共有

システムのライフサイクル全体の
バランスを均一化し、効率化

システムのライフサイクルで考える

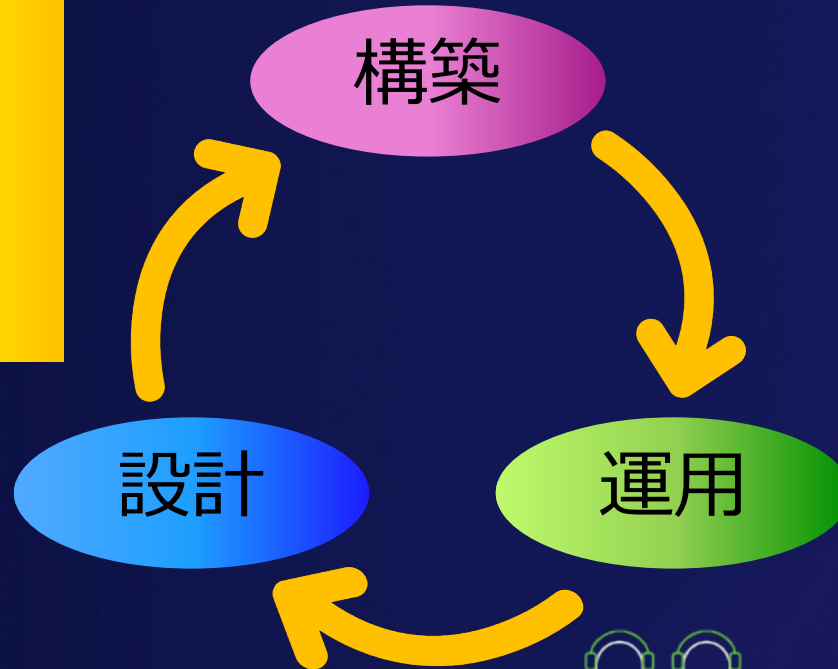


開発チーム

- 監査への主体性を持つ
- 情報収集、分析の仕組みを持つ



セキュリティ
チーム



- フィードバックを受けるために必要な Output を実装
- 運用を意識した開発



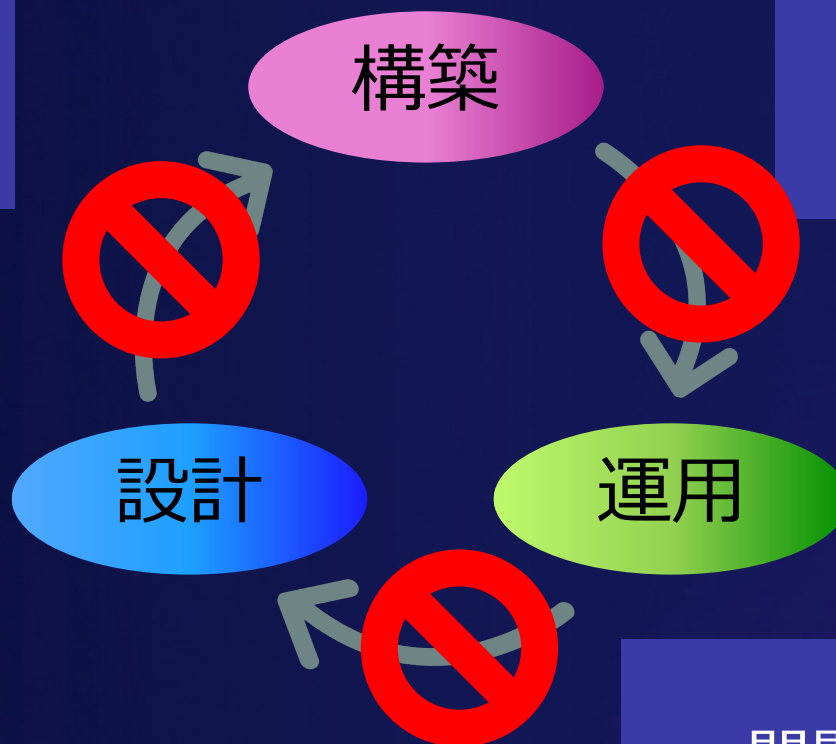
運用チーム

- 業務に対する適切なフィードバックを提供
- 設計への積極的な関与

セキュリティ対応が負担になっていませんか

開発前のセキュリティ
チェック

リリース直前の
セキュリティチェック

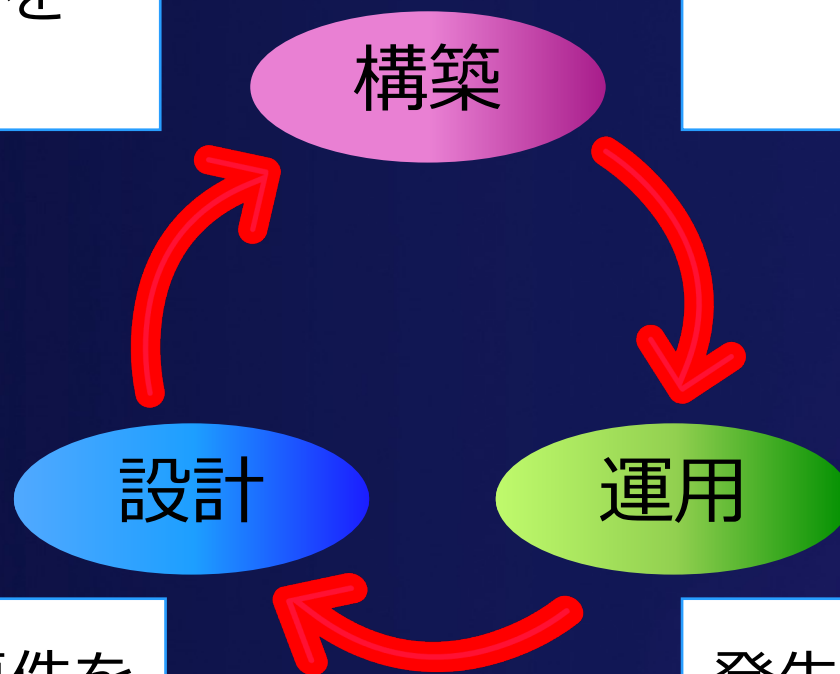


問題が発生した場合は
チェック項目を追加

立ち止まらず、進み続けるために

CI/CD パイプラインに
セキュリティチェックを
組み込み、自動化

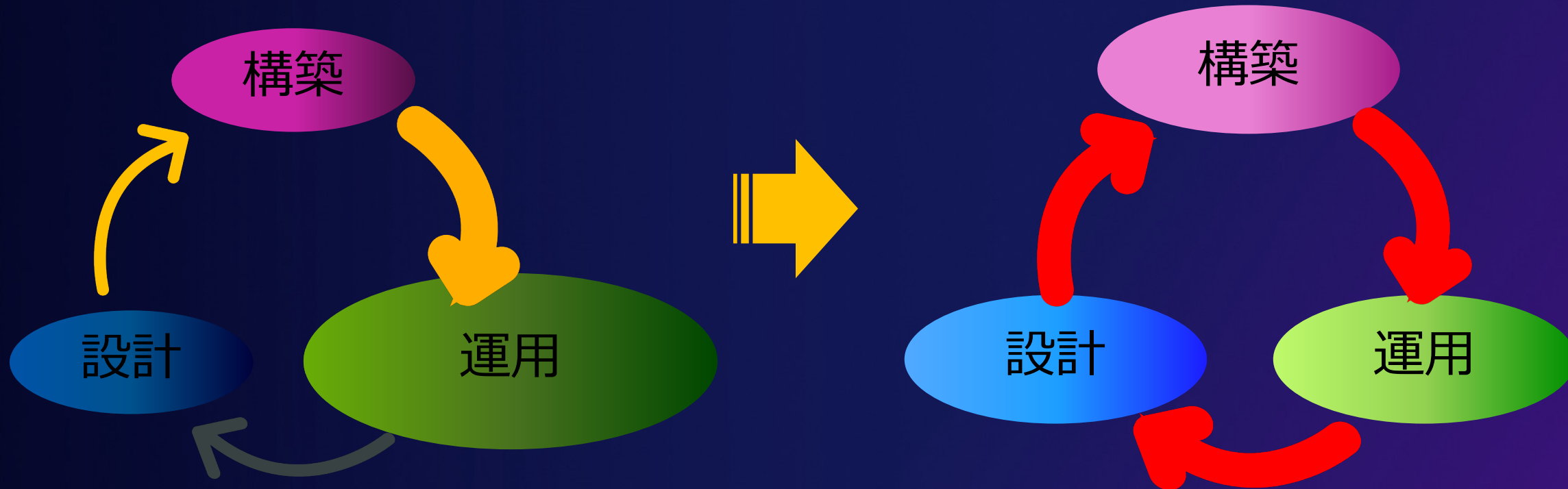
承認プロセスにセキュリティ
の観点を加える



設計時にセキュリティ要件を
整理。全体で共通認識を持つ

発生した問題はツールとして
対応し、負担を軽減

開発「サイクル」の回転を強めるために



クラウドのメリットを活かした運用による解決

チームをまたがる視点の欠如

課題・問題の後回し

属人的で非効率な運用

スケールへの対応が困難

システムのライフサイクル全体を
意識した視認性の共有

システムのライフサイクル全体の
バランスを均一化し、効率化



クラウドのメリットを
活かした運用

- セキュリティ・開発・運用
チームで可視化を統合
- 運用の自動化でセキュリティ
対応を高度化



AWSセキュリティサービスを
活用し、効率化

- 継続的な脅威の検出
- ワークフローの最適化
- 修復時間の最小化

課題解決のポイント②

AWS サービスを活用した セキュリティ運用

AWSサービスを活用し、クラウド環境のセキュリティで優れた運用性を実現



- 脅威の検出と監視を一元化
- セキュリティポスチャ評価の改善
- 脆弱性管理を最適化
- 根本原因分析を合理化
- 機密データの発見を改善
- 既存フローとのスムーズな連携
- 検出結果に対する優先順位付け
- 修復の自動化
- スケールする利用環境への対応

各チームに閉じた視点により生じる課題への対応

チームをまたがる視認性の欠如

課題・問題の後回し

属人的で非効率な運用

スケールへの対応が困難

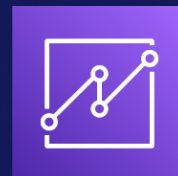
解決 1. チーム横断での可視化

チームをまたがる視認性の欠如

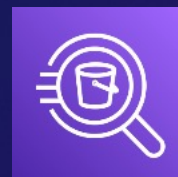
課題・問題の後回し

属人的で非効率な運用

スケールへの対応が困難

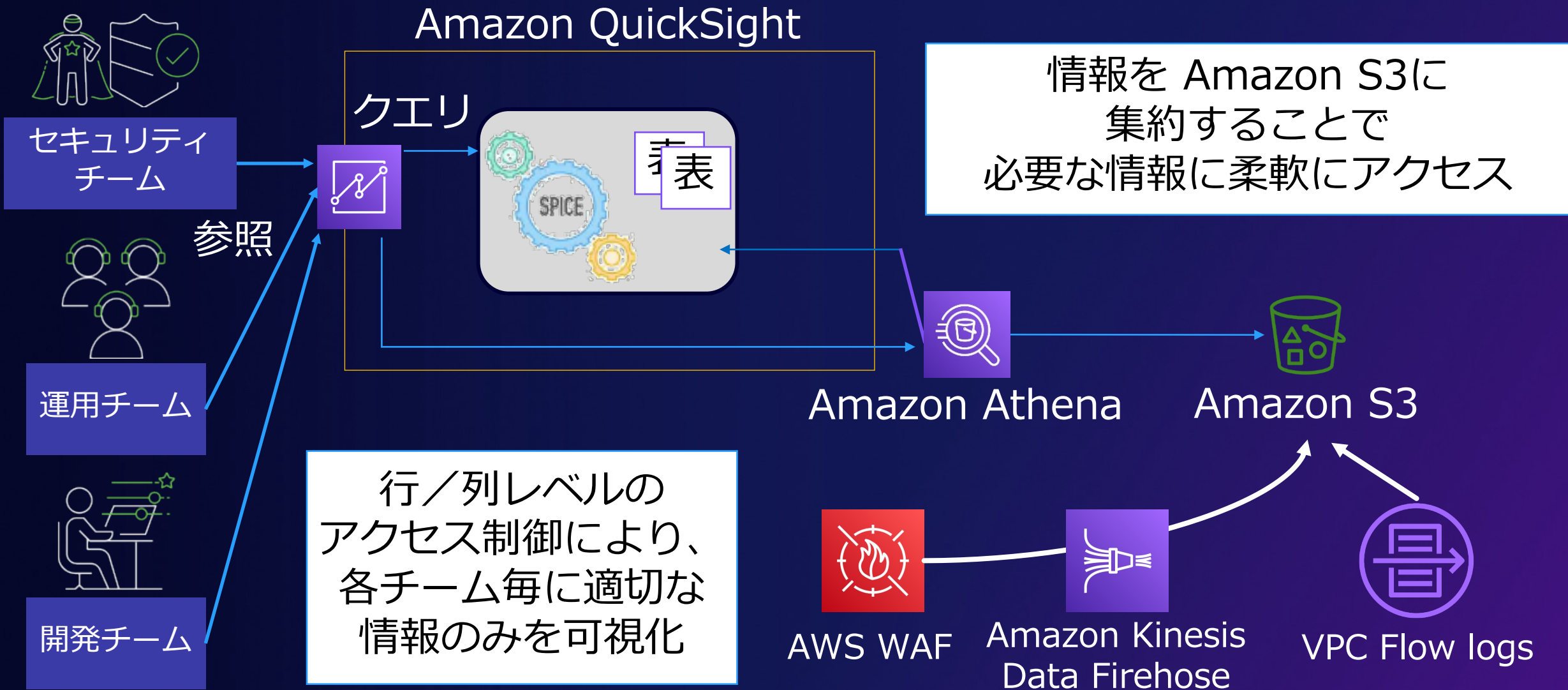


Amazon QuickSight
クラウドネイティブの
サーバーレスなビジネス
インテリジェンスサービス



Amazon Athena
Amazon Simple Storage Service
(Amazon S3) 内のデータを
標準 SQL を使用して簡単に分析

例) Amazon S3 に集約されたログの可視化



AWS サービス活用のメリット



セキュリティ
チーム

調査は運用・開発チーム任せとなり、対応スピードが鈍化



開発チーム

業務開発を優先し、
運用は後回し

最後の手段は「運用回避」



運用チーム

運用回避対応による負担増

運用性の向上とビジネスの
成果が結びつかない

各チームが必要となる情報
に必要なタイミングで
アクセスできるようにする
ことで適切なフィード
バックを実現

解決2. 属人性を排除し、効率的な開発

チームをまたがる視認性の欠如

必要な情報にアクセスできない

属人的で非効率な運用

スケールへの対応が困難



Amazon Inspector

AWS ワークロードをスキャンする
自動化された継続的な
脆弱性管理サービス



Amazon
EC2



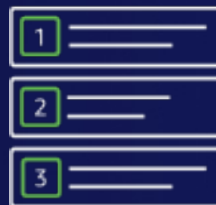
Amazon
ECR

例) 自動化を活用した属人性の排除



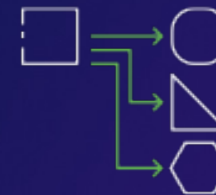
自動検出と継続的な スキャン

- リソースの自動検出
- 脆弱性とネットワーク到達可能性の継続的スキャン



スコア算出による 優先順位付け

- コンテキストを考慮した実用的なリスクスコアを算出
- 対策措置の優先順位を列挙



対策措置の ワークフロー自動化

- API で操作可能
- Amazon EventBridge と連携
- AWS Security Hub と統合

AWS サービス活用のメリット



セキュリティ
チーム

セキュリティチェックシート
での対応内容は担当者依存

開発・運用チームへの
セキュリティ対応の負担増



開発チーム

開発期間の短縮に伴う
作業負担の増大



運用チーム

運用回避対応による負担増

マネージドサービスの活用で
対応工数を削減
機械的なチェックにより、
属人性を排除し、安定的な
品質を確保

解決3. スケールへの対応

チームをまたがる視認性の欠如

必要な情報にアクセスできない

属人的で非効率な運用

スケールへの対応が困難



AWS Security Hub

組織内の様々なセキュリティデータを
を集約して、一元的に可視化



AWS Organizations

AWS リソースの増加やスケーリング
に合わせて、環境を一元的に管理し、
統制するサービス

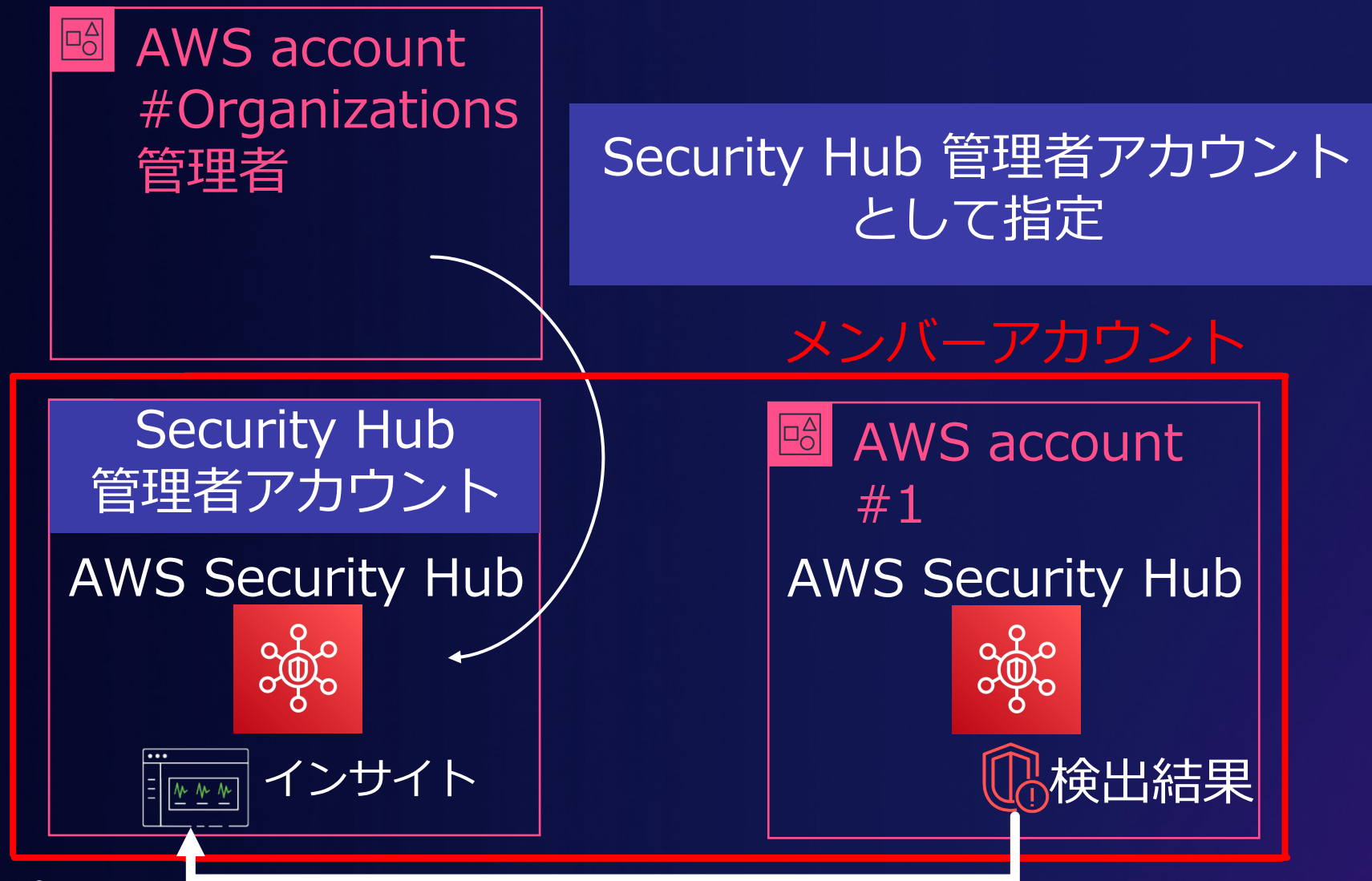
例) AWS Security Hub のマルチアカウント対応



メンバーアカウントに追加・招待を実施することで
複数アカウントの検出結果を集約することは可能

アカウント追加の都度、追加・招待のオペレーションが必要

例) AWS Organizations との統合



例) AWS Organizations との統合



AWS account
#Organizations
管理者

Organizations に新規に追加されるアカウントは自動で
集約対象として追加。検出結果の一括確認が可能

メンバーアカウント

Security Hub
管理者アカウント

AWS Security Hub



インサイト



AWS account
#1

AWS Security Hub

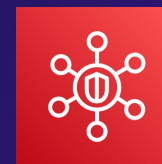


検出結果



AWS account
#2

AWS Security Hub



検出結果

AWS サービス活用のメリット



セキュリティ
チーム

開発・運用チームへの
セキュリティ対応の負担増

調査は運用・開発チーム任せと
なり、対応スピードが鈍化



開発チーム

開発期間の短縮に伴う
作業負荷の増大



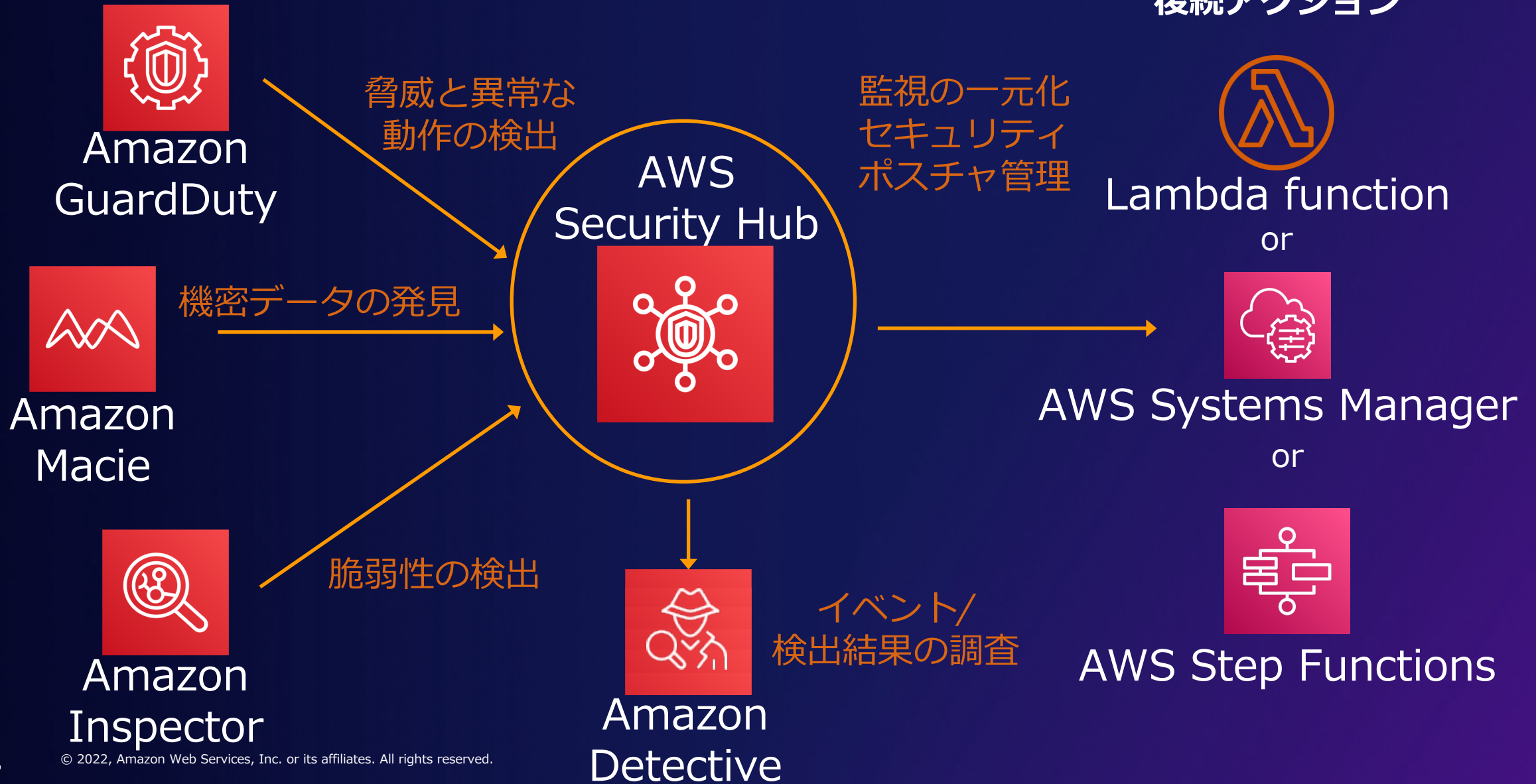
運用チーム

運用回避対応による負担増

Organizations /
Security Hub の機能により
スケール時の自動追加や
一元管理を実現することで
各チームの作業負荷を軽減

AWS Security Hub を中心としたセキュリティ運用

後続アクション



まとめ

セキュリティ運用の課題とポイント

各チームの 単独視点による弊害

チームをまたがる
視点の欠如

課題・問題の後回し

属人的で非効率な運用

スケールへの
対応が困難

クラウドのメリットを 活かした運用

システムのライフサイクル
を意識した視認性の共有

システムのライフサイクル
全体のバランスを
均一化し、効率化


AWSサービスを活用 したセキュリティ運用

Organizations /
Security Hub との統合に
よるスケール対応

Athena / QuickSight
による可視化

Amazon Inspector によ
る自動化

セキュリティはブレーキではない



「セキュリティ体制の強化」は非効率な対応から解放し、加速させるものである。決して開発や運用を縛り、自由とスピードを奪うものではない

Thank you!

辻本 雄哉

技術統括本部 金融事業本部

