

# セキュリティに関連するデジタル社会推進 標準ガイドラインの改定について CI/CDパイプラインにおけるセキュリティの 留意点に関する技術レポートの改定について

2025/3/25    セキュリティ・危機管理担当

# ガイドライン/技術レポート（セキュリティ）

[https://www.digital.go.jp/resources/standard\\_guidelines/#security](https://www.digital.go.jp/resources/standard_guidelines/#security)

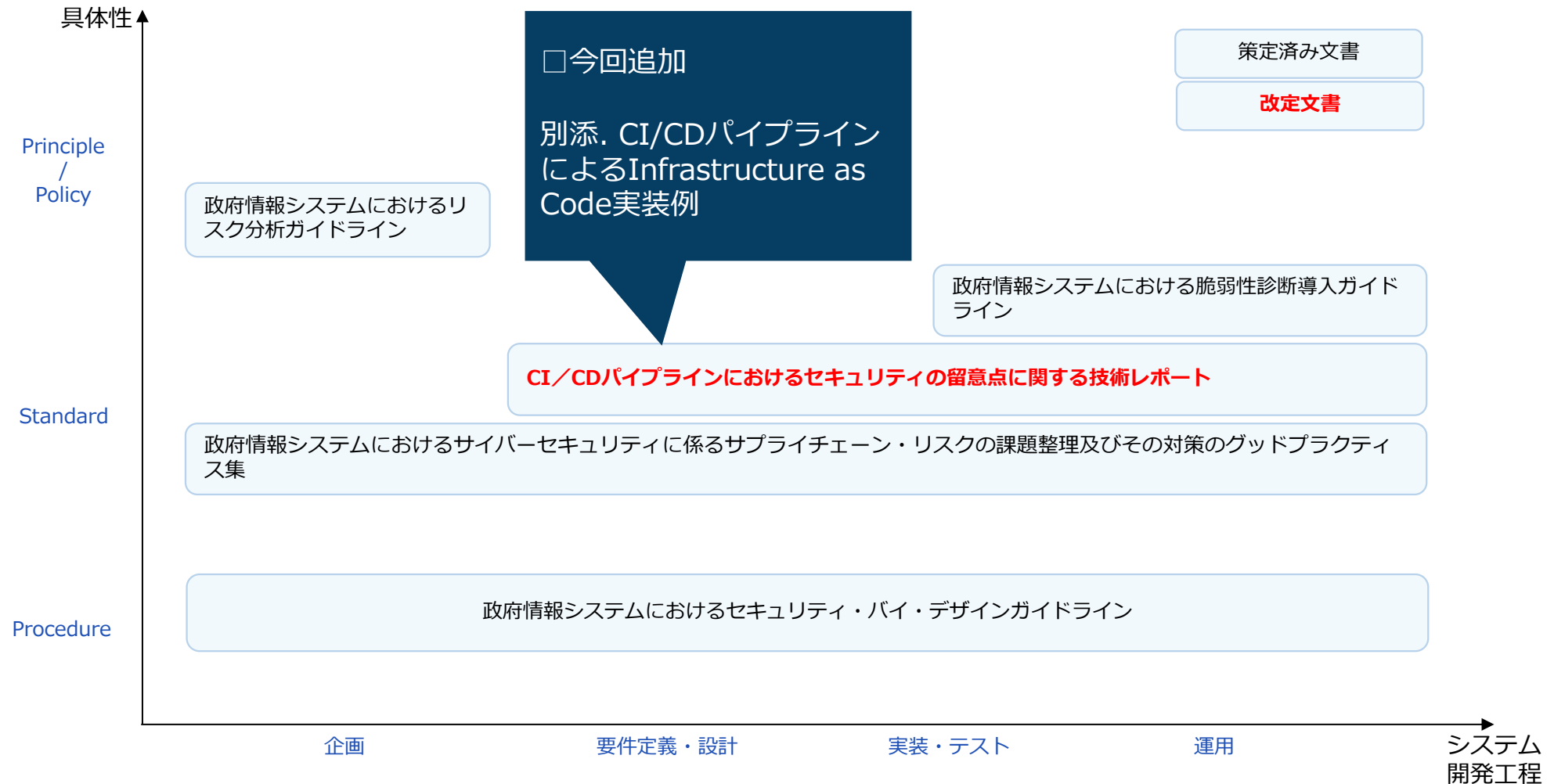
セキュリティに関連する標準ガイドラインの公開状況

## これまで9件のガイドライン・技術レポートを公開しているところ、今回、新たに1件の技術レポートを改定する

項番	タイトル	公開日	最終改定日
DS-200	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	2022/6/30	2024/1/31
DS-201	政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～	2023/3/31	—
<b>DS-202</b>	<b>CI/CDパイプラインにおけるセキュリティの留意点に関する技術レポート</b>	<b>2024/3/29</b>	<b>—</b>
DS-203	政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集	未定（※）	—
DS-210	ゼロトラストアーキテクチャ適用方針	2022/6/30	—
DS-211	常時リスク診断・対処（CRSA）アーキテクチャ	2022/6/30	2024/1/31
DS-212	ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート	2023/3/31	—
DS-220	政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート	2023/3/31	—
DS-221	政府情報システムにおける脆弱性診断導入ガイドライン	2023/3/31	2024/2/6
DS-231	セキュリティ統制のカタログ化に関する技術レポート	2023/3/31	—

（※）2月25日開催の技術検討会議で審議済みだが、DS-203では、「DS-310 政府情報システムにおけるクラウドサービスの利用に係る基本方針」の公開予定の改定版から引用しているところ、現在においてもDS-310が関係者間での協議中であることから公開未定である。そのため、DS-310が公開され次第、DS-203も公開する予定。

# セキュリティ技術ガイドラインのシステム開発、運用に関する文書の体系整理



# CI/CDパイプラインにおけるセキュリティの留意点に関する技術レポート - 別添: CI/CDパイプラインによる Infrastructure as Code実装例

令和7年3月25日

セキュリティ危機管理チーム

デジタル庁

## 背景 – 政府情報システムの提供形態の変化

「**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**」より、政府情報システムでは「効率性」や「セキュリティ水準」等の非機能要件を向上する必要性を述べている。

上記を実現するにあたり、政府情報システムを利用者に提供するまでの一連の作業方法の変化、特に「**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**」ことを重視している。

並行して、D庁は一部のプロジェクトで、民間のエンジニアを採用し、内製化した**モダンなシステム開発手法**を進めている。

## 背景 - CI/CDパイプラインの必要性

その例として挙げられている「**CI/CD パイプライン**」は、特にアジャイル開発を採用しているWebアプリケーションやスマートフォンアプリの開発組織にとっては、広く普及したシステム・コンポーネントである

今後、D庁を始めとした政府情報システムの運営でも、CICDパイプラインの利活用が進むことが予測される（※）。

CICDパイプラインはその役割上、**変更管理業務を行う非常に強力な権限**を有する。

※ガバクラ及びエンジニアリングユニットに簡易にヒアリングしたところ、「GitHub Action」を利用していた。

## 背景 - リスクの顕在化

人間による変更作業とは異なり、システムによる自動的な変更作業をするCI/CDパイプライン特有の**考慮すべき脅威・攻撃手法**がある。

そのような保護策について、「統一基準群」を含め政府情報システム向けの**ガイドラインは存在しない**。

近年ではCI/CDパイプラインに対する**侵害事例が増えている**。

特に、2021年における米大統領令の発令の契機ともなった「SolarWinds」に対する**swサプライチェーン攻撃**でも、CI/CDパイプライン侵害も大きな要因となるなど、**侵害に伴う影響も広がっている**。

## CI/CDパイプラインの保護に取り組む意義

1. CI/CDパイプラインへの侵害は**変更権限を奪取されるのと同義**である
2. 政府情報システムのモダン化、そしてシステムのサステナブルな提供にあたり、運営の一環としてCI/CDパイプラインの利用を既に始めている
3. 実際の**政府系システムへの大きな侵害事例**も現れている

- これらの理由から、我が国においてもガイドラインや標準の整備が必要になると考えられる。
- そのための下地を提供する目的で、2024/03に「CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート」を公開した。
- このレポートでは、外観及び用語を整理して、CI/CDパイプラインの各処理、そして必要とされる保護策について技術した。

# 技術レポートの内容

## 1. はじめに

- 1 背景と目的
- 2 適用対象
- 3 位置づけ
- 4 本書の構成
- 5 用語

## 2. CI/CDパイプラインの概要

- 1 CI/CDパイプラインの重要性
- 2 CI/CDパイプラインの全体像
- 3 [コラム] CI/CDを狙った脅威の高まり - SolarWinds

## 3. CI/CDパイプラインにおけるセキュリティ対策

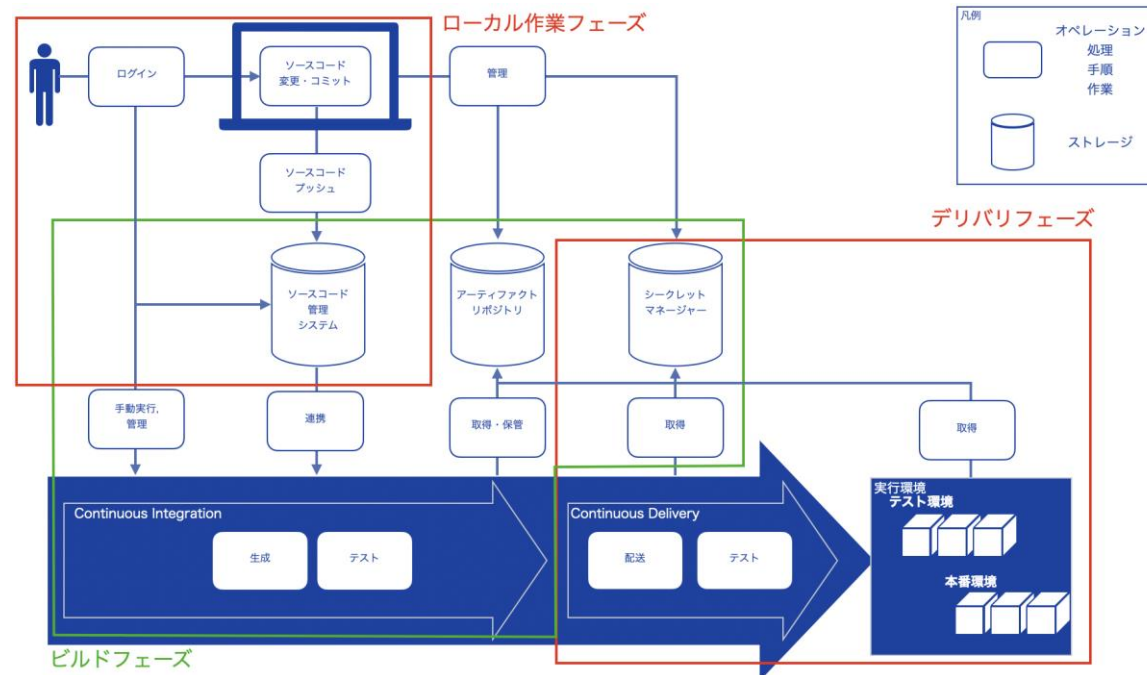
- 1 全フェーズに共通した保護
- 2 ローカル作業フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

## 4. 参考文献

# 技術レポートの概要

CI/CDパイプラインにおける、業務の特性に応じて次のようなフェーズを定義し、各フェーズにおける処理内容と保護策を解説している。

- **ローカル作業フェーズ**: 開発者・運用者・保守者が、手元の端末や統合開発環境（IDE）でソースコードや設定ファイルに対して作業をし、ソースコード管理システム上の「ソースコードリポジトリ」に送信するフェーズである
- **ビルドフェーズ**: 最新のソースコードや設定ファイルを元とした成果物の生成、検証・テスト、保管を行うフェーズである。CI/CDパイプラインのうち、CI（Continuous Integration）がこれに当たる。
- **デリバリフェーズ**: 成果物の実環境への配送と実行を行うフェーズである。CI/CDパイプラインの内、CD（Continuous Delivery）がこれに当たる



# 技術レポート単体の限界

ガイドラインはない状況下で、**各政府情報システムの担当者は**、実運用における**留意点や保護策を具体化する必要**がある。この**負担は大きい**と予想される

実際に、デジタル庁内の技術レポートレビューでも、**具体例を欲する要求**が多かった

上記の状況を踏まえ、想定読者である各システム担当者の理解を補助する目的で、  
具体的な実装例や保護策を整理した文書を別添として作成した。  
本別添では、インフラの構成管理のCI/CDパイプラインを具体例として提供する。  
アプリケーションのCI/CDパイプラインに関する具体例は今後、検討する。

# 別添の内容

## 1. はじめに

## 2. シナリオ

1 組織構成

---

2 本シナリオでの概要図および詳細図

---

## 3. プラットフォームチームのCI/CDパイプライン

1 全フェーズに共通した保護

---

2 ローカル開発フェーズの保護

---

3 ビルドフェーズの保護

---

4 デリバリフェーズの保護

---

## 4. サービスチームのCI/CDパイプライン

1 全フェーズに共通した保護

---

2 ローカル開発フェーズの保護

---

3 ビルドフェーズの保護

---

4 デリバリフェーズの保護

---

# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

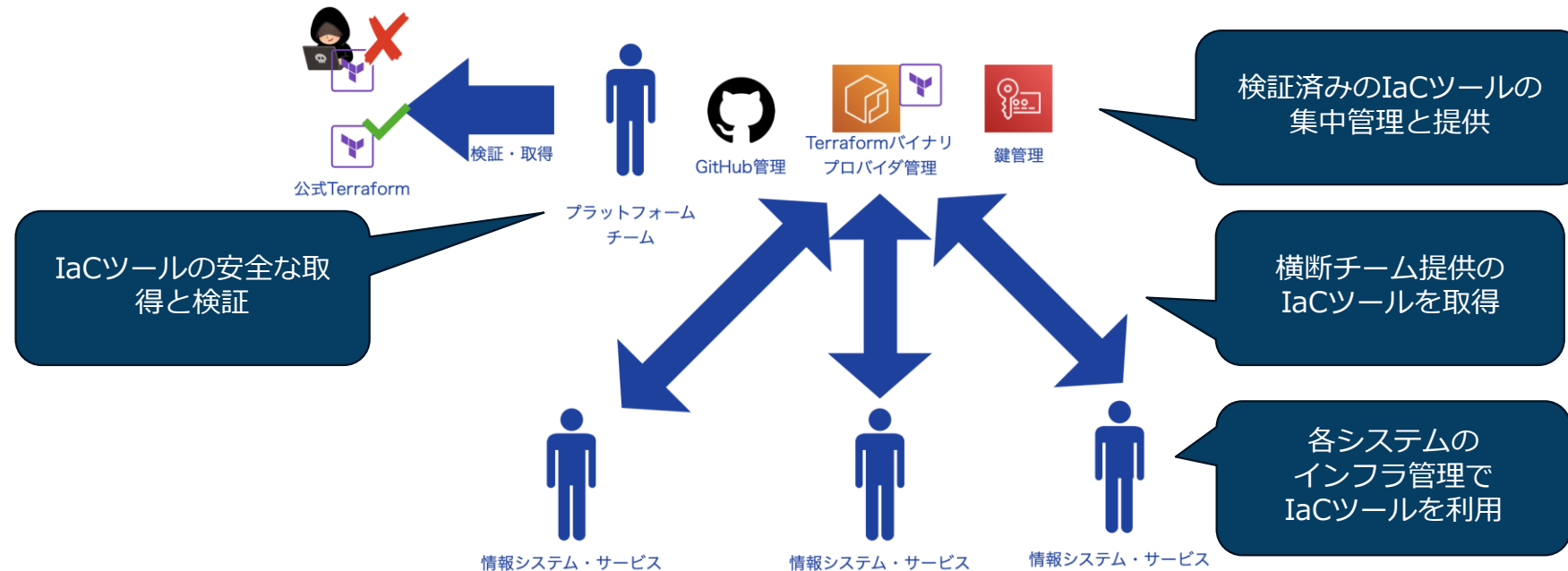
本シナリオで扱うシナリオ  
および  
具体例で利用するツール名

# シナリオ

インフラの構成管理の自動化において、複数のチームが共通したIaCツールを利用することが予想される  
このツールを、安全に取得・検証・利用することがSWサプライチェーンの観点では重要である

各チームが個別にプロセスを実行する状態は効率化や品質の平準化の観点で理想的ではないため、**IaCツールの安全な取得・検証・提供を担う横断チームの設置**が想定される。

本書では、**横断チーム**のCI/CDパイプラインがIaCツールを安全に取得・検証・提供し、**各情報システムチーム**のCI/CDパイプラインがツールを取得・利用し、情報システムを提供するシナリオを提示する



# 実装例で取り上げるサービス及びツール

機能	サービス・ツール
バージョン管理	git (git version 2.39.3 (Apple Git-146))
Gitリポジトリホスティング	GitHub (クラウド、Team Plan)
CI/CDパイプライン	GitHub Actions、AWS CodeBuild
Infrastructure as Code	Terraform (v1.10.2)
シークレットスキャン	Trivy (v0.57.1)
脆弱性スキャン/誤設定スキャン	同上
メタデータ生成 - Software Bill of Material (SBOM)	同上
成果物署名、署名検証	Cosign (v2.4.1)
メタデータ生成	同上
他	AWSの各種サービス

# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

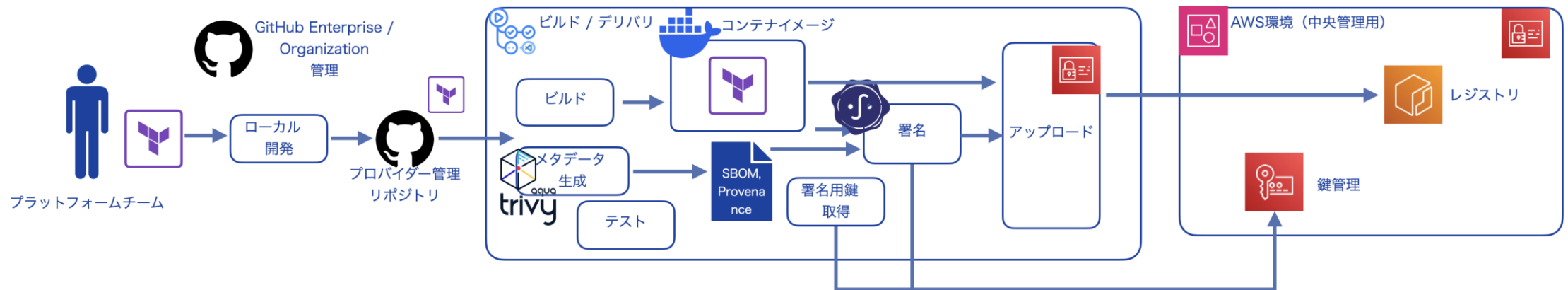
## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

一元的に管理するTerraformバイナリおよびAWSプロバイダーを、サービスチームに提供するCI/CDパイプラインにおける保護策。  
具体的には、資産管理、脆弱性管理を含む運用・保守、環境への対策、シークレットの保護、CI/CDパイプラインを通じた信頼性の確保である。

# プラットフォームチームのCI/CDパイプライン - 全フェーズに共通した保護

- 資産管理、脆弱性管理を含む・運用保守
  - 成果物の構成内容、脆弱性情報、来歴情報といったメタデータの提供  
※ 3.34) 「依存物の安全性の担保」での具体的な対応策解説
- シークレットの保護
  - AWS IAMアクセスキーを利用し、AWS Web API を介した GitHub と AWS 間の連携
  - GitHub リポジトリの「Secrets」機能 を利用したアクセスキーの安全な管理
  - サービスチームからのアクセスについてはクロスAWSアカウントアクセスを想定
- CI/CD パイプラインを通じた信頼性の確保
  - 小規模チームによるソースコードからデリバリまでの管理のため、チーム差の不存在による 高い信頼性を想定



# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

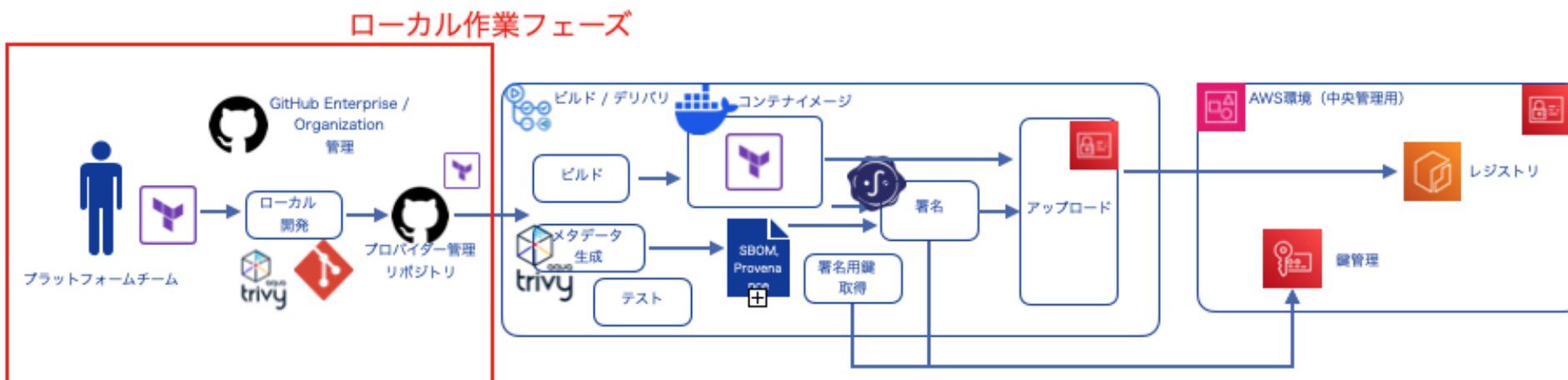
## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

主にソースコード管理システムとそのリポジトリ、ブランチに対する対策の具体例を挙げる

# プラットフォームチームのCI/CDパイプライン - ローカル開発フェーズの保護

- GitHub Organizationおよびリポジトリの権限最小化
- GitHubのRulesets機能による強制的な取り込み予防
- GitHubに対する2FA強制、またはSSOの検討
- コミットへの署名強制による作業内容と作業者の紐づけ
- Git HooksとTrivyを利用したシークレットのコミット予防



# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

ビルドフェーズでは、サービスチームに提供するための検証済みTerraformツールを成果物として生成し、その信頼性と安全性を確保するにあたって、次の具体的な保護策を挙げる。

# プラットフォームチームのCI/CDパイプライン – ビルドフェーズの保護

## シークレット情報の漏洩対策

- Trivyを使った誤コミット検知
- GitHub Secretsによるシークレット保存とログ出力時のマスク

## ソースコード・成果物の信頼性の担保

- GitHubのCode Ownersの指定と、branch ruleの構成によるレビュー必須化
- Trivyによる構成ミス及び脆弱性のスキャン
- SBOMとSLSA Provenanceの生成と署名

## ビルド上での実行範囲の制限

- GitHubにおけるPush rulesetsの構成によるビルド定義ファイルの保護
- 信頼できる提供元の公式ソフトウェアのみの利用

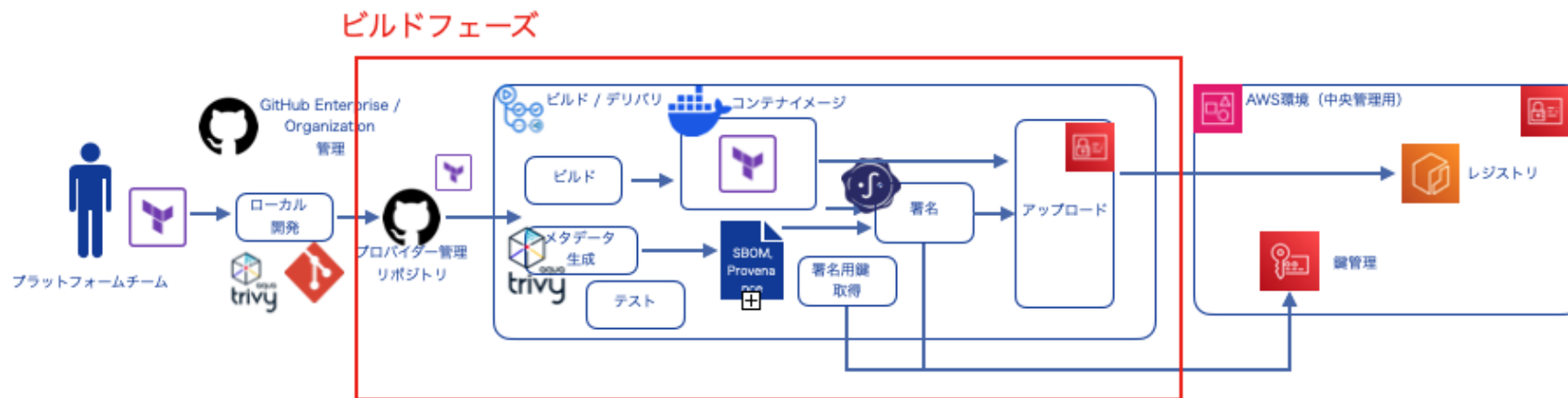
- ビルドフェーズにおける最小権限の実現

## 依存物の安全性の担保

- 前述の対策
- GitHub Actionsのcommit hashによるバージョン固定

## ストレージ内の成果物の保護

- ECRのリソースポリシーやKMSキーポリシーによる権限最小化



# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

デリバリフェーズでは、Terraformツール、メタデータ、それぞれの署名をストレージ（レジストリ）にアップロードする。この際の保護実装例は次の通りである。

# プラットフォームチームのCI/CDパイプライン – デリバリフェーズの保護

## デリバリ時に利用する主体の保護

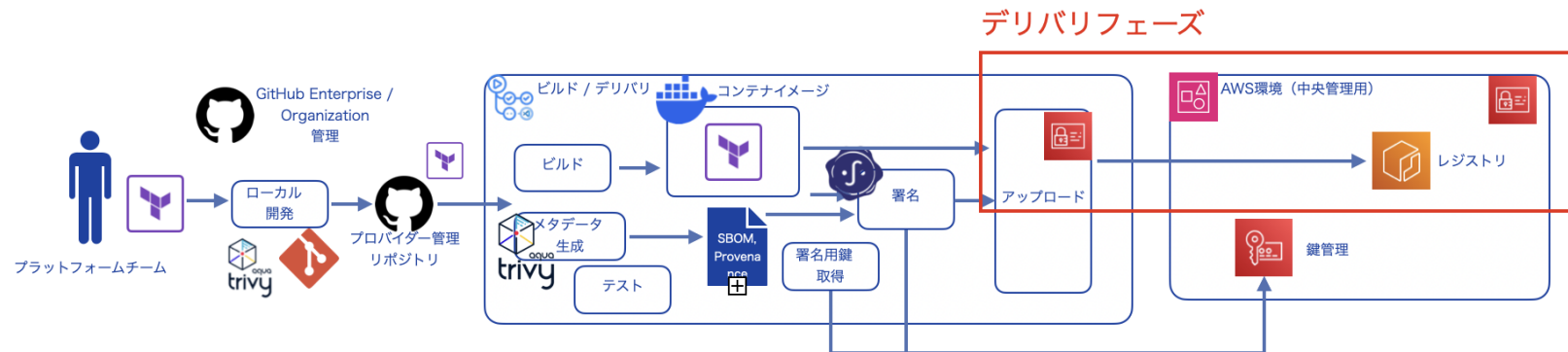
- ローカル開発フェーズの保護例と同等のため省略

## 信頼できる成果物をデリバリするための保護

- ビルドフェーズの保護例と同等のため省略

## デリバリ時の証跡

- 成果物としての ECR 上のコンテナイメージ
- GitHub 上のソースコードの Zip ファイル
- GitHub Actions のワークフロー履歴
- AWS CloudTrail における ECR 操作の記録 (データイベント有効時)



# 別添の内容

## 1. はじめに

## 2. シナリオ

1 組織構成

2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

1 全フェーズに共通した保護

2 ローカル開発フェーズの保護

3 ビルドフェーズの保護

4 デリバリフェーズの保護

## 4. サービスチームのCI/CDパイプライン

1 全フェーズに共通した保護

2 ローカル開発フェーズの保護

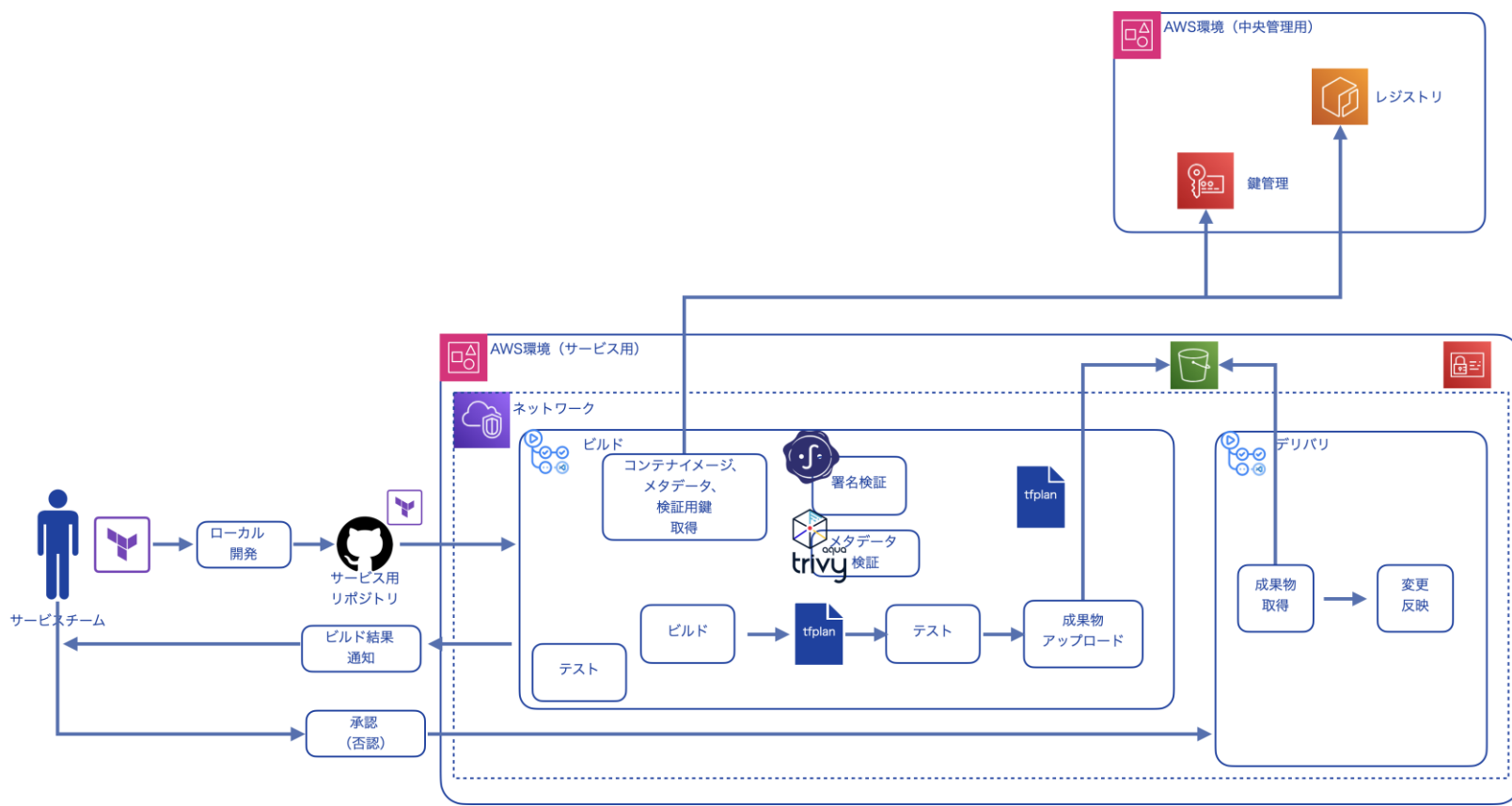
3 ビルドフェーズの保護

4 デリバリフェーズの保護

プラットフォームチーム提供の  
Terraformを用いたAWS環境を管理する  
CI/CDパイプラインにおける保護策

# サービスチームのCI/CDパイプライン - 全フェーズに共通した保護

これは、実際に政府情報システムを提供する特定サービスチームのパイプラインであり、パイプラインAから提供されるTerraform関連のソフトウェアおよびメタデータを取得・検証・利用しながら、自身のIaCファイルを用いてAWS環境の構成管理を行う。



# 別添の内容

## 1. はじめに

## 2. シナリオ

1 組織構成

---

2 本シナリオでの概要図および詳細図

---

## 3. プラットフォームチームのCI/CDパイプライン

1 全フェーズに共通した保護

---

2 ローカル開発フェーズの保護

---

3 ビルドフェーズの保護

---

4 デリバリフェーズの保護

---

## 4. サービスチームのCI/CDパイプライン

1 全フェーズに共通した保護

---

2 ローカル開発フェーズの保護

---

3 ビルドフェーズの保護

---

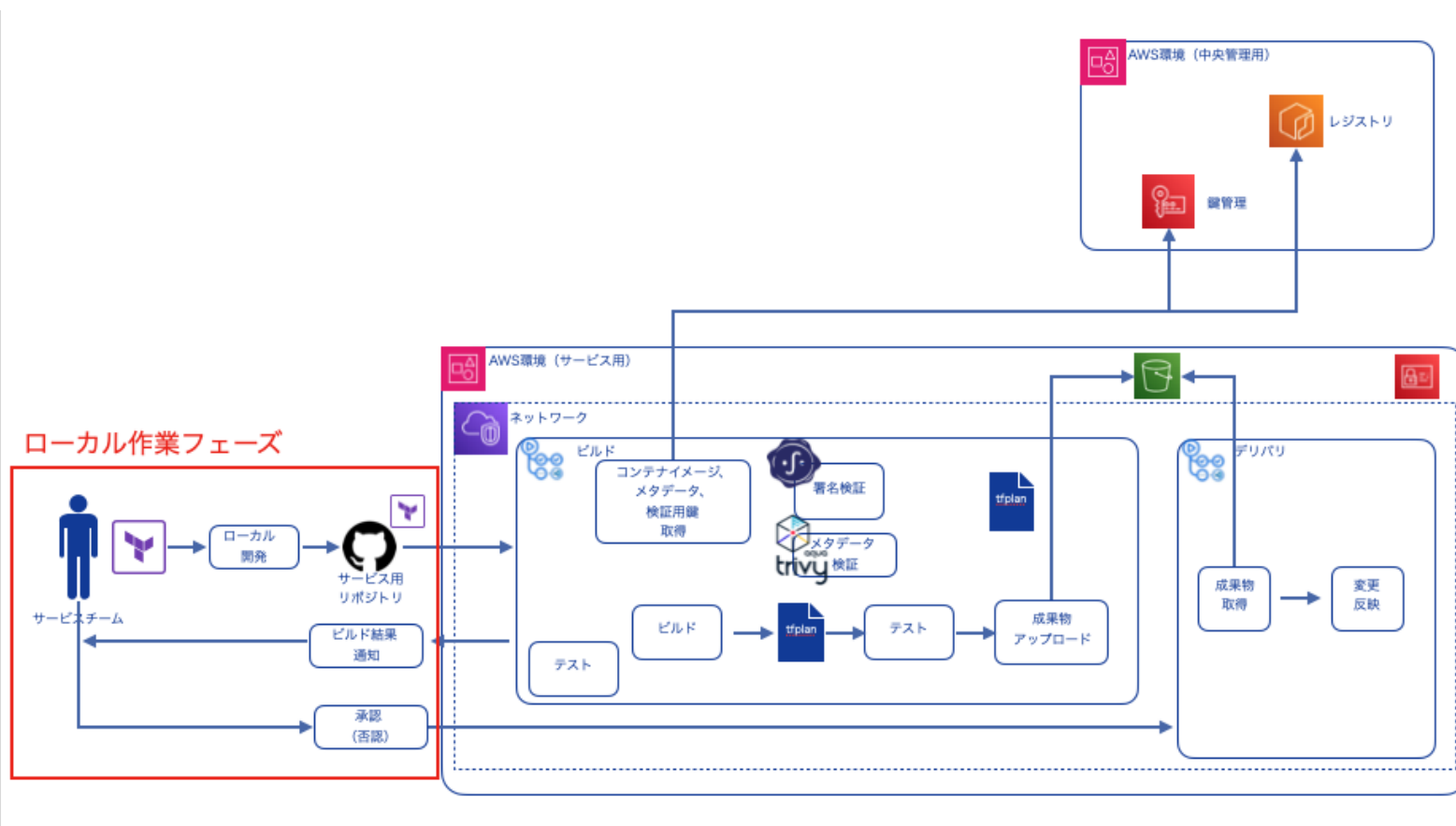
4 デリバリフェーズの保護

---

若干の違いはあるものの、基本的な設定はプラットフォームチームのCI/CDパイプラインと類似しているため、詳細な説明は省略している。

# サービスチームのCI/CDパイプライン - ローカル開発フェーズの保護

基本的に省略



# 別添の内容

## 1. はじめに

## 2. シナリオ

- 1 組織構成
- 2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

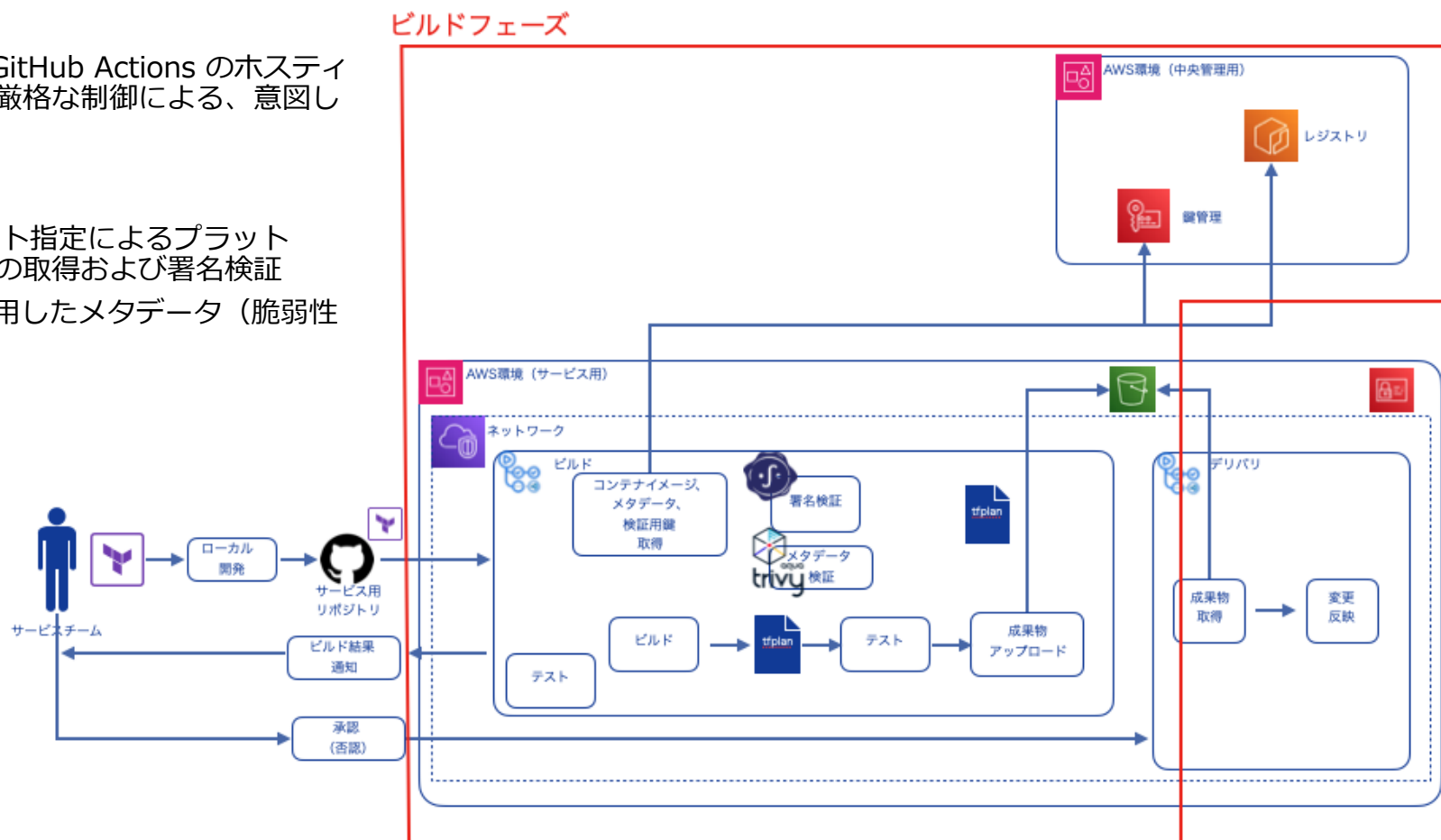
## 4. サービスチームのCI/CDパイプライン

- 1 全フェーズに共通した保護
- 2 ローカル開発フェーズの保護
- 3 ビルドフェーズの保護
- 4 デリバリフェーズの保護

ソースコード・成果物の信頼性の担保、ビルド上での実行範囲の制限、そして依存物であるTerraformの安全性を検証する保護策について説明する。

# サービスチームのCI/CDパイプライン – ビルドフェーズの保護

- ソースコード・成果物の信頼性の担保
  - TrivyによるTerraformファイルにおける構成ミスを検出
  - GitHubリポジトリのRulesetsによるアクセス権限やレビュー強制
- ビルド上での実行範囲の制限
  - VPC 上の AWS CodeBuild における GitHub Actions のホスティングと、ネットワーク的な外部通信の厳格な制御による、意図しないパイロード取得の防止
- 依存物の安全性の担保
  - Cosignを利用したイメージダイジェスト指定によるプラットフォームチーム成果物及びメタデータの取得および署名検証
  - Cosign, Trivy, SLSA Provenanceを利用したメタデータ（脆弱性情報、構成環境）の検証



# 別添の内容

## 1. はじめに

## 2. シナリオ

1 組織構成

2 本シナリオでの概要図および詳細図

## 3. プラットフォームチームのCI/CDパイプライン

1 全フェーズに共通した保護

2 ローカル開発フェーズの保護

3 ビルドフェーズの保護

4 デリバリフェーズの保護

## 4. サービスチームのCI/CDパイプライン

1 全フェーズに共通した保護

2 ローカル開発フェーズの保護

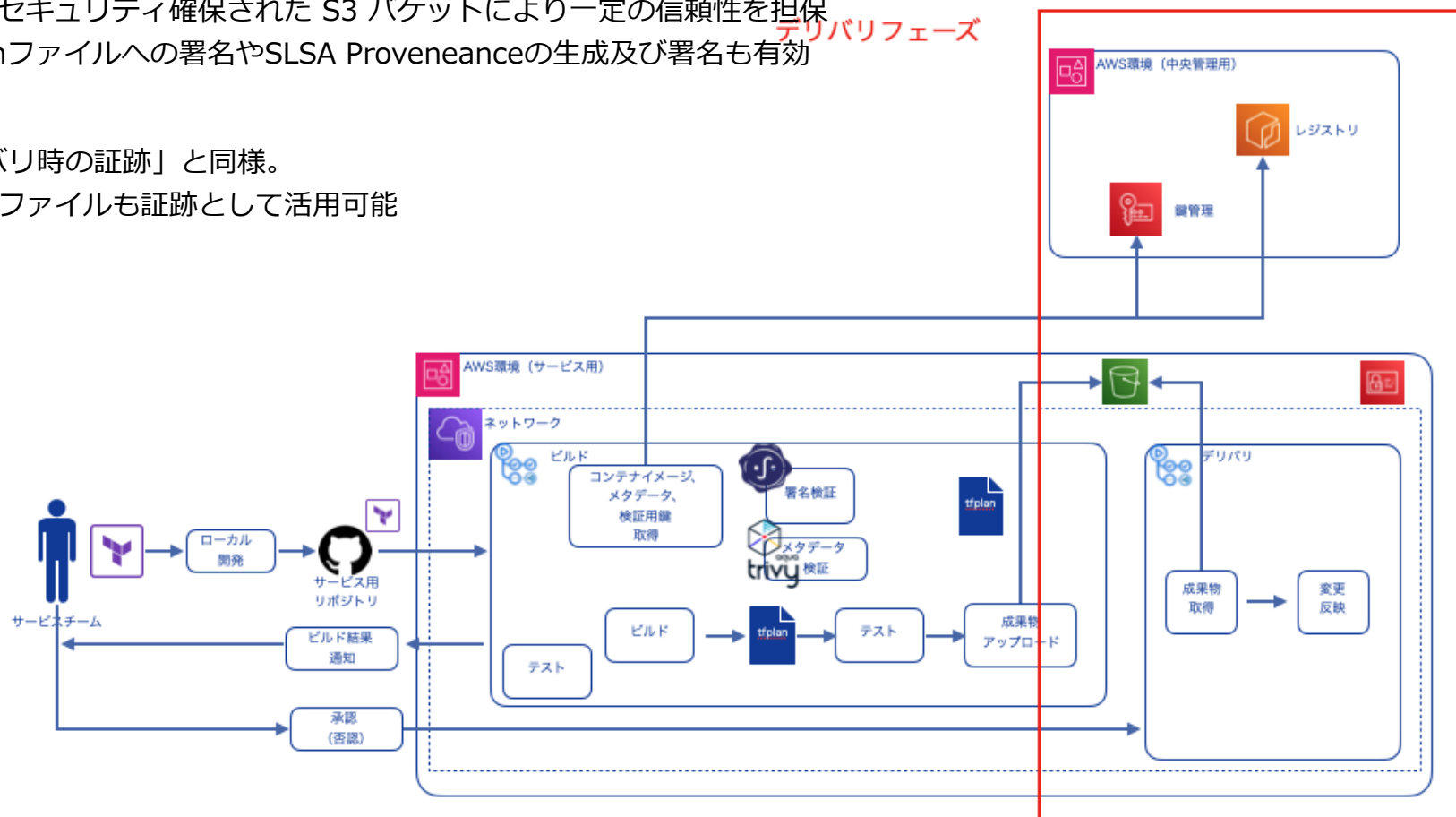
3 ビルドフェーズの保護

4 デリバリフェーズの保護

デリバリ時に利用する主体の保護、信頼できる成果物をデリバリするための保護、そしてデリバリ時の証跡について説明する。

# サービスチームのCI/CDパイプライン – デリバリフェーズの保護

- デリバリ時に利用する主体の保護
  - AWS CodeBuildに割り当てるIAMロールの権限最小化による保護
- 頼できる成果物をデリバリするための保護
  - 検証済みの Tfplan ファイルと適切にセキュリティ確保された S3 バケットにより一定の信頼性を担保
  - 本文書では実施していないが、Tfplanファイルへの署名やSLSA Provenanceの生成及び署名も有効
- デリバリ時の証跡
  - GitHub 上での確認は3.43)「デリバリ時の証跡」と同様。
  - ビルドフェーズで生成された Tfplan ファイルも証跡として活用可能



**デジタル庁**