# セキュリティに関連する標準ガイドラインの策定について

令和6年3月22日

セキュリティ危機管理チーム

デジタル庁

# ガイドライン/技術レポート（セキュリティ）

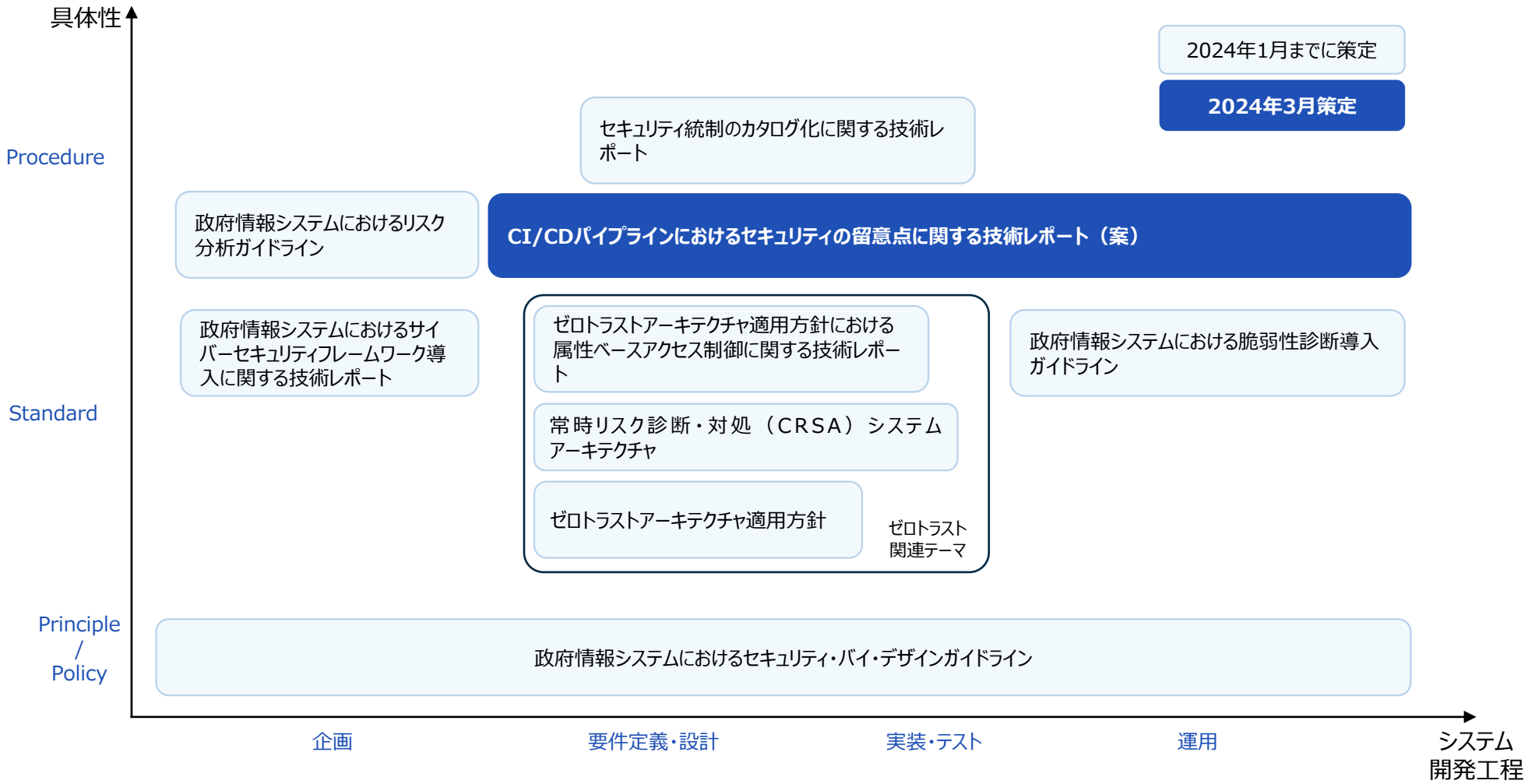
https://www.digital.go.jp/resources/standard_guidelines/#security

# セキュリティ技術ガイドラインの公開

これまで8本のガイドライン・技術レポートを公開

- 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
- 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～
- DS-210
  ゼロトラストアーキテクチャ適用方針
- DS-211
  常時リスク診断・対処（CRSA）アーキテクチャ
- 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
- 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
- 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
- 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

# セキュリティ技術ガイドライン全体の構造整理



新規

# DS-202
# 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（案）

デジタル庁

# 本レポートの背景

- **「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」**は、政府情報システムにおける「効率性」と「セキュリティ」等の非機能要件を向上する上で、**「アジャイル的な手法」**及び「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
- その例として挙げられている「**CI/CD パイプライン化**」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。
- 一方、業務要件上、CI/CDパイプラインはサーバやアクセス管理等のリソースに対して変更を行える高い権限を有し、本質的に**リスクの高い**システム・コンポーネントでもある。
- その重要度及びリスクへの注目、そして実際に発生したCI/CDパイプラインに侵害するインシデントの事例から、**米国におけるCI/CDパイプラインの保護に関するガイドラインが急増**しており、今後政府情報システムの運営においても**ガイドラインが必要になることが予想**される。

# 本レポートの目的

- 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している。
- 統一基準はないが、今後、米国等の影響から、**ガイドラインあるいは標準の整備が必要になることが予想**される。**本技術レポートは、その検討に必要な下地を提供**する。
- 具体的には、CI/CDパイプラインに関する**外観及び用語を整理**しつつ、情報システムの開発からリリースまでの一連の業務に対して、**CI/CDパイプラインが担う処理を紹介**する。また、CI/CDパイプラインにおいて**必要とされる対策について記述**する。

# 目次

# 2. CI/CDパイプライン（以降、CI/CD）の概要

CI/CDの重要性:

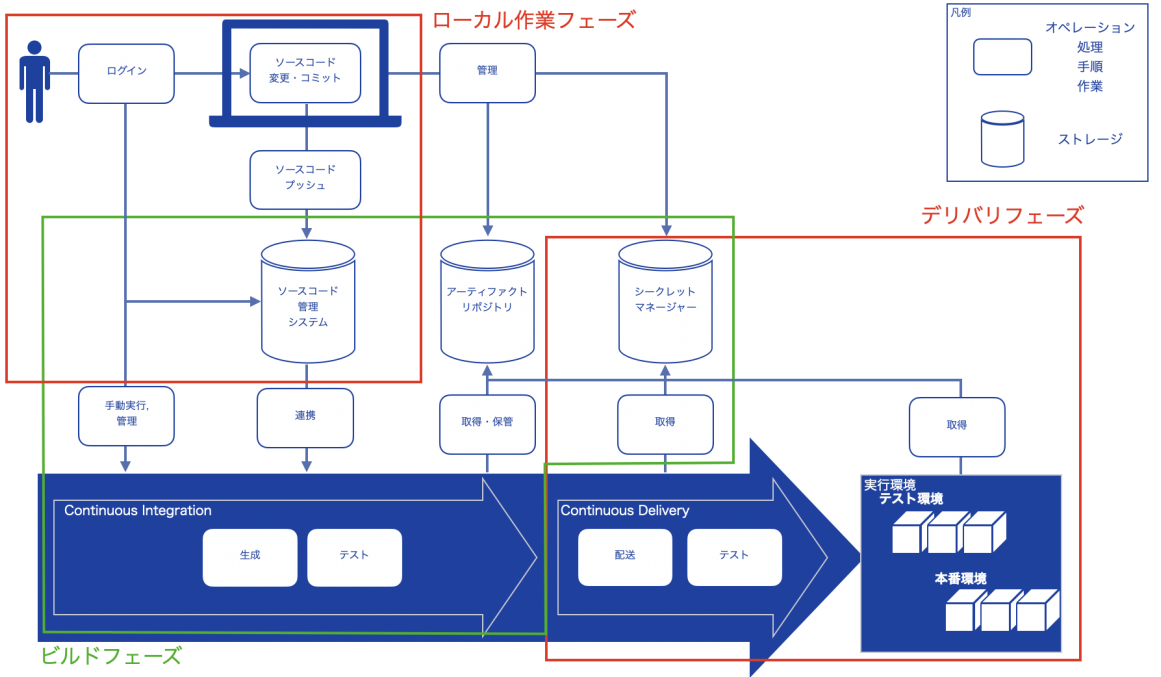
- クラウド上で稼働するモダンアプリケーションを継続的に提供・改善するにあたり、欠かせないシステムコンポーネントがCI/CDである
- CI/CDは元となる**ソースコードや設定ファイルに対して作業を実施し、成果物の生成と実行環境への配送及び実行といった業務プロセスを自動化**する。
- CI/CDは**変更管理や構成管理をする能力を有するだけでなく、インフラそのものの設定ファイルを処理することができるためである**。その業務を執行するにあたって**特権に近い権限**を持つ。従って**本来はリスクが高いシステムコンポーネント**である。
- 実際にそのような経路を狙った侵害事例も発生しており、特に著名なものは2020年の「Solar Winds」である。

# 2. CI/CDパイプラインの概要

CI/CDの全体像 - ①:

- CI/CDは、その**業務の特性に応じて次の図のようにフェーズを分類**できる。
  - **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

    ※Continuous Deployも存在するが、変更のリリースといった側面が強く、技術レポートの範囲では大きくContinuous Deliveryと変わらないため、本文書では省略する。



# 2. CI/CDパイプラインの概要

CI/CDの全体像 - ②:

- CI/CDにおける**ストレージに**は次のものがあげられる
  - **ソースコード管理システム（SCM）:** ソースコードのバージョン管理をするシステムである。ソースコードを変更した主体と差分を変更履歴として保存する。
  - **アーティファクトリポジトリ**:ビルドフェーズで生成した成果物を保管するシステムである。
  - **シークレットマネージャー**:アクセストークンやサービス同士の通信で利用するサービスアカウントのシークレットを保管する。
- 図の記載はないが、CI/CDパイプライン、CI/CD、各種ストレージは、それぞれがアクセス制御管理機能を有する
- **提供形態**は、SaaSのような第三者によるサービス提供や政府情報システム管理下の**サーバやコンテナホスト等でホスティング する形態が主**に考えられるが、これらに限定されるものではない

# 3. CI/CDパイプラインにおけるセキュリティ対策

概要

- CI/CDおける対策は、大きく分類し、**全体に共通する対策**と**各フェーズ特有の対策**がある
- CI/CD特有のリスクや考え方については、次のガイドラインを基礎にする
  - メイン

    CISA、FBI:「Defending Continuous Integration/Continuous Delivery (CI/CD) Environments」

    OWASP: Top10 CI/CD Security Risks
  - 補助

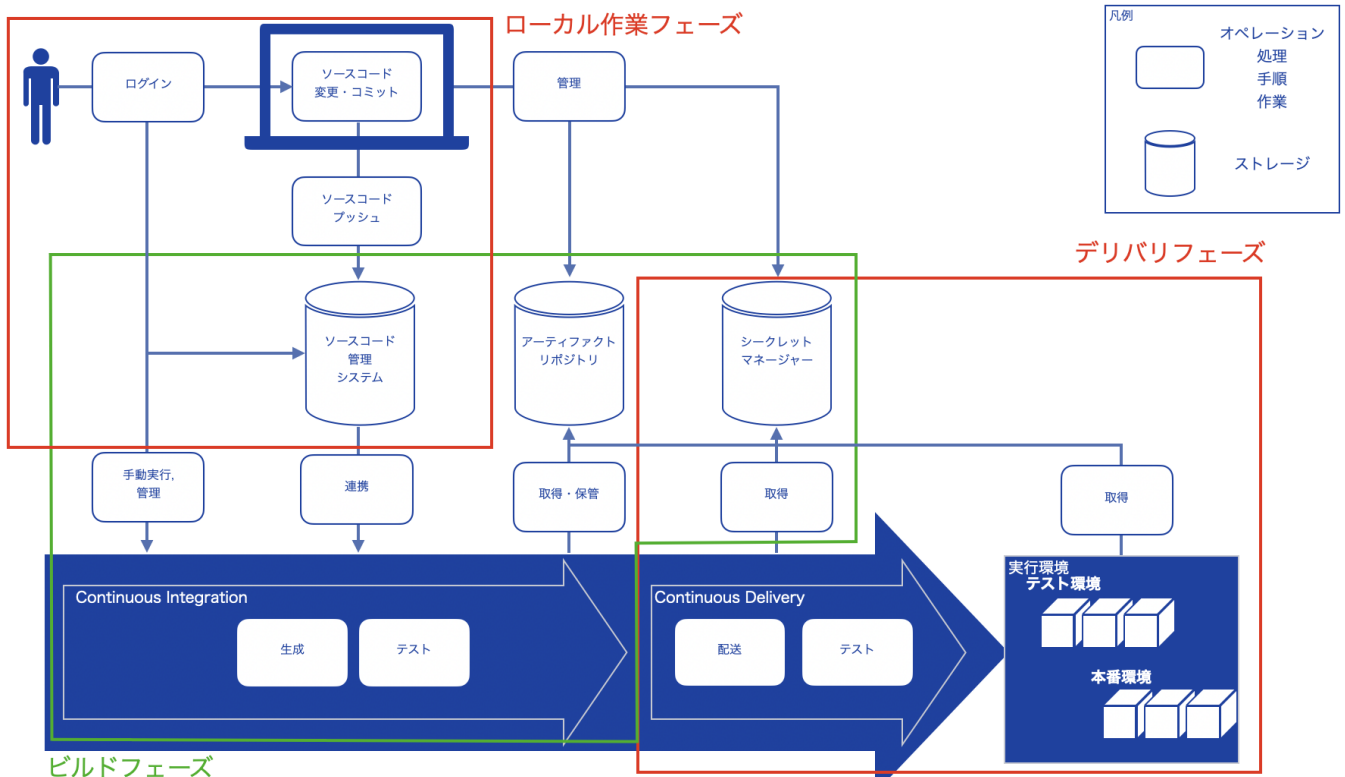
    DoD:「DevSecOps Fundamental Guide Book」

    Microsoft:「DevOps threat matrix」開発フェーズの脅威とコントロール
- 最終的に基準・ガイドラインに参照・拡張されることを考慮し、文言等は基本的に統一基準のものを参照する。

# 3. CI/CDパイプラインにおけるセキュリティ対策

CI/CD全フェーズに共通した保護

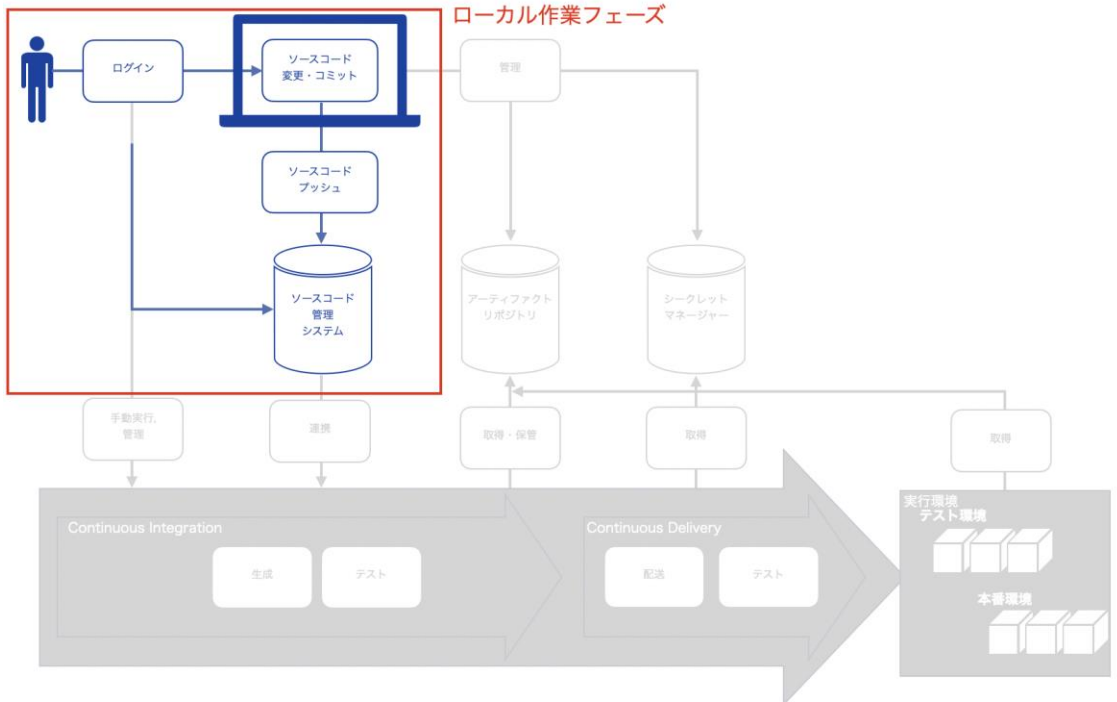
- 資産管理
  - 自組織の資産の状況を把握し、台帳に記録することが重要である。
  - 各システムのプラグインや連携しているサードパーティ製アプリ、オープンソースソフトウェア（以降、OSS）といったものも対象となる。
- 脆弱性管理を含む運用・保守
  - 上記資産に関する脆弱性を管理する。
  - もしクラウドサービスである場合、設定不備・構成不備に留意する。
- 環境への対策
  - 次の点について留意が必要になる。
    - シークレットの保護
    - アカウント管理・アクセス制御
    - ログの取得・管理
    - トラストチェンの確保



# 3. CI/CDパイプラインにおけるセキュリティ対策

## ローカル作業フェーズの保護

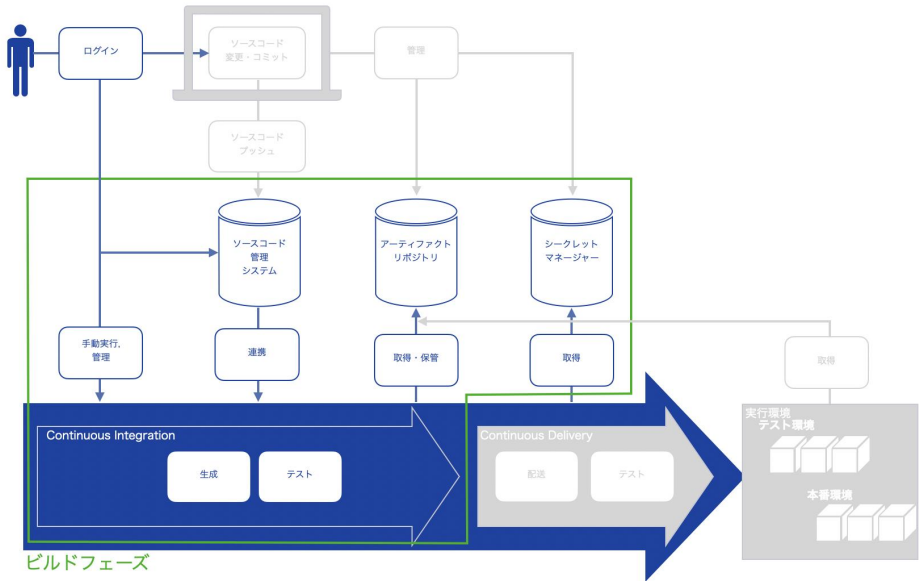
- 利用者やエンドポイントにおける対策
  - 開発者・運用者・保守者が作業を行う**端末およびアカウントを適切に管理**し、初期アクセスの脅威から保護する。
- ソースコード管理システム、そのリポジトリ及びブランチの保護
  - **アクセス権限の設定や強制的な変更の取り込みを禁ずる**などの保護策を実装する。
- ソースコード管理システムの公私共用なユーザーアカウントの管理
  - 組織テナントに**個人アカウントを招待する運用を取る際、有償機能の検討も含め、適切な対策**を検討する。
- 作業内容と作業者の紐付き
  - ソースコードや設定ファイルに対する作業が、確かに作業者のものであるか、その**真正性を署名によって担保**する。
- ソースコード管理システムに対するシークレットの記録予防
  - シークレットを**作業履歴に取り込まないよう予防措置**をとる
    - なお、検知措置についてはビルドフェーズに記載している
  - **万が一取り込んでしまった場合は、早急にローテーション**をする



# 3. CI/CDパイプラインにおけるセキュリティ対策

## ビルドフェーズの保護

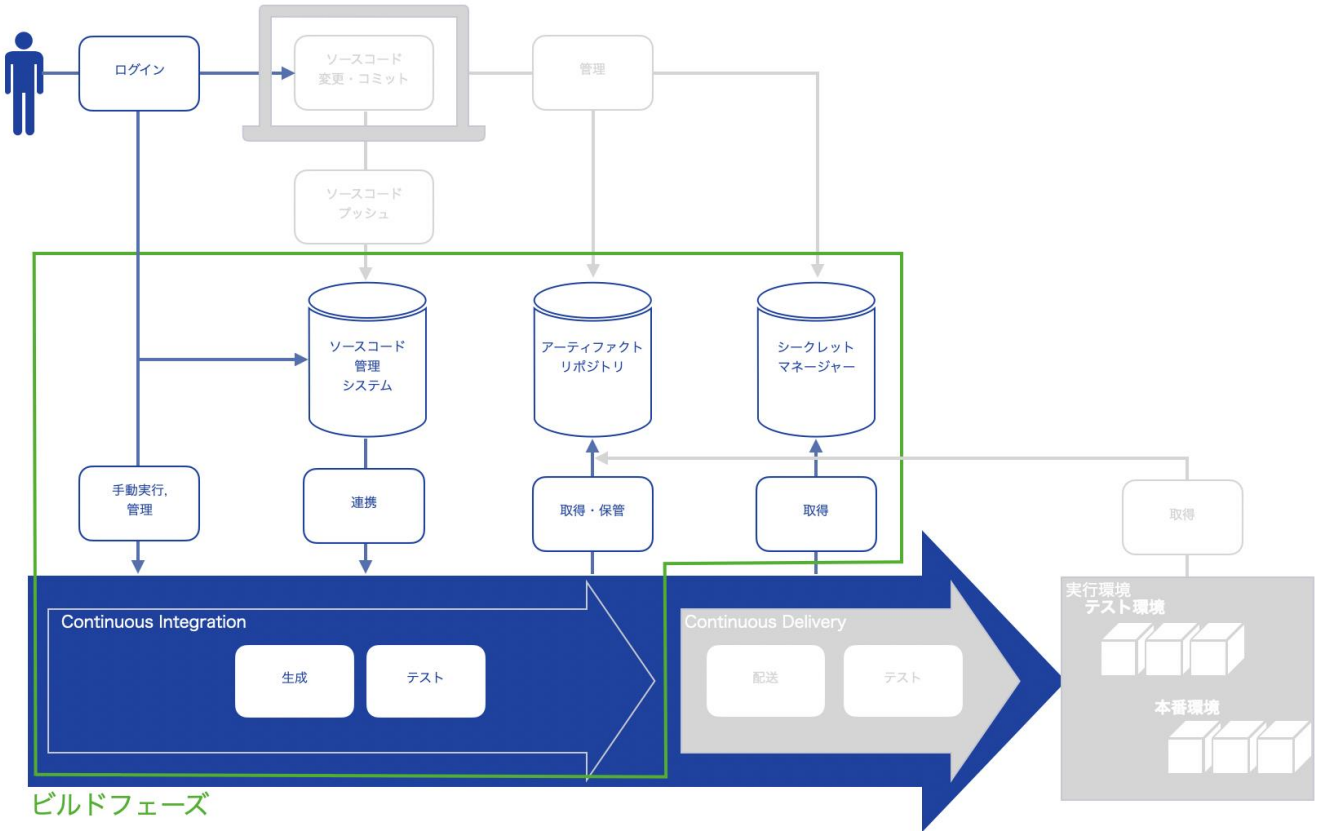
- ビルド上での実行範囲の制限
  - アクセス可能なネットワークを制限したり、利用可能なツールやモジュールを事前にホワイトリスト化することで、取り込み前のCI環境上での活動制限を適用する。
- シークレット情報の漏洩対策
  - シークレットがログ上に出力されないようマスキングしたり、作業対象のファイルの変更差分にシークレットが含まれてないことを検出するといった対策が有効である。
- ソースコード・成果物の信頼性の担保
  - 上位者による承認や、脆弱性スキャンによる瑕疵の検出等により、品質を担保する。
- 依存物の安全性の担保
  - サードパーティによるパッケージやツールに脆弱性などの瑕疵がないか、それらのサードパーティが信頼された提供元であるか等を確認する。
- ストレージ内の成果物の保護
  - ストレージそのもののアクセス管理を強固にすることで、成果物を保護する。
  - 成果物へのデジタル署名で完全性と神聖性を担保する。



# 3. CI/CDパイプラインにおけるセキュリティ対策

## ビルドフェーズの保護

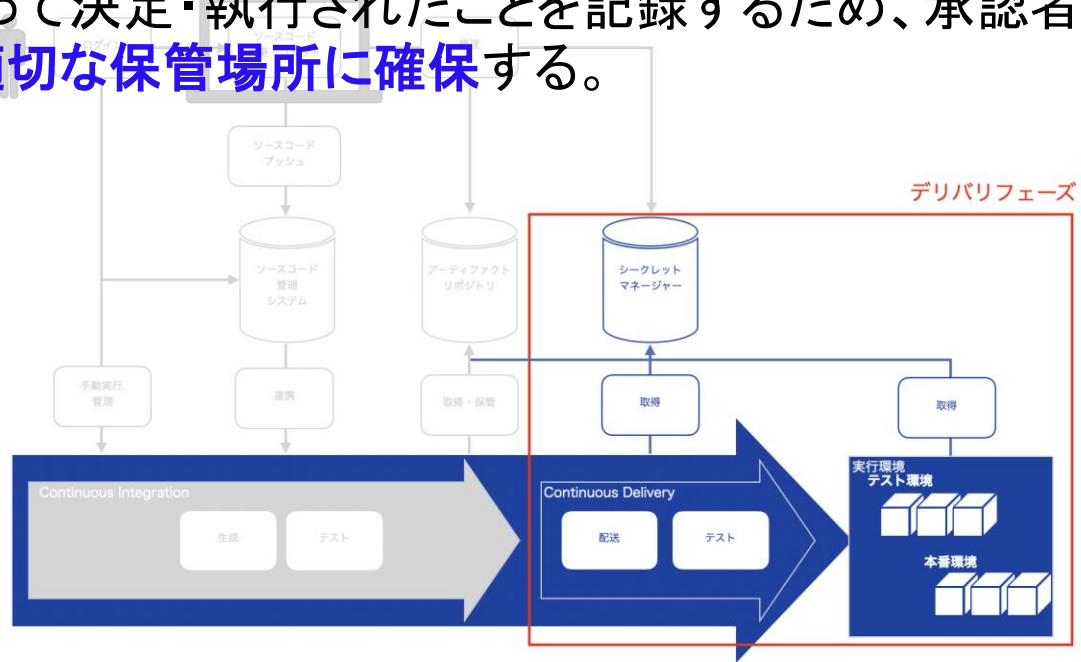
- 特定のイベントをトリガーとして処理を実行する**Webhookのクレデンシャル・トークンを保護**する
- ビルド環境の**ログ等に環境変数やクレデンシャルが記録されない様に留意**する。
- ソースコードや設定ファイルの依存する**外部パッケージにリスクがないか、脆弱性の有無などを検証**する。
- ソースコード、設定ファイルの改ざんの有無を検知するため、**開発フェーズにおける署名を検証**する。
- 生成したイメージ、成果物の**真正性を確立するため、署名**をする。
- イメージや成果物を保管する**ストレージを保護**する。



# 3. CI/CDパイプラインにおけるセキュリティ対策

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
  - 実質的に本番環境を変更する権限を有する主体であるため、**他フェーズでの使い回しを避けたり、より強固な認証手法などで保護**されなければならない。
- 信頼できる成果物をデリバリするための保護
  - 成果物やイメージを動作環境へデリバリする前に、**改ざんの有無を検知するため、ビルドフェーズにおける署名を検証**する。
- デリバリ時の証跡
  - 成果物やイメージのリリースが正しいプロセスに則って決定・執行されたことを記録するため、承認者による**承認の形跡や、その後の作業ログを取得し、適切な保管場所に確保**する。



デジタル庁