

# コンテナプラットフォーム(kubernetes)環境における セキュリティ対策について

## 主な内容

kubernetesなどのCloud Nativeなシステムのセキュリティ対策は多くの技術要素が組み合わさっている為、とても複雑である。また、kubernetes本体の各種デフォルト設定値のまま導入・運用する事はセキュリティ対策が不十分であるのが定説となっている。弊社では、考慮すべきセキュリティ対策を「セキュリティカテゴリ」と「セキュリティ境界」の2つの軸で整理した。

## 目次

- 1 エンタープライズ企業がプロダクション環境でkubernetes互換のコンテナプラットフォームを動かす際の選択肢について
- 2 AWSなどのパブリッククラウドでコンテナプラットフォーム環境を導入し運用する際に考慮すべきセキュリティ対策について
- 3 kubernetes のコンテナプラットフォーム環境におけるセキュリティ対策について
- 4 セキュリティカテゴリ毎の対策詳細について
  - (1) 認証
  - (2) 認可及びAdmission Control
  - (3) ファイアウォール
  - (4) ワークロード分離(物理/論理)
  - (5) シークレット管理
  - (6) 暗号化 (ネットワーク通信/ステートフルなデータ)
  - (7) バックアップ
  - (8) 脆弱性対策
  - (9) モニタリング
  - (10) ガバナンス/コンプライアンス
- 5 kubernetesなどのCloud Nativeなコンテナプラットフォーム向けセキュリティ対策ツールについて

申し込みする