東京エレクトロンデバイス ウェビナー

パブリッククラウドの運用をワンランクアップ！
安全な利活用促進のアプローチ

セキュリティリスクを生ませないクラウド運用！ TerraformとVaultの活用法

東京エレクトロン デバイス株式会社

CNビジネス開発室

小野瀬　翼

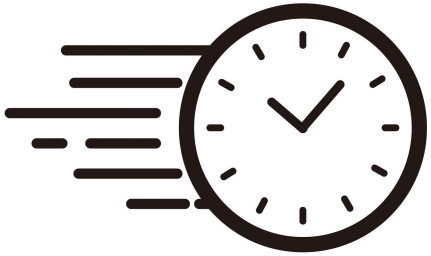
Onose Tsubasa

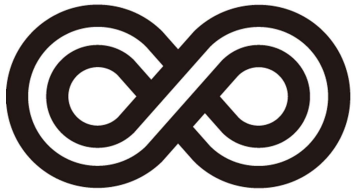
本日のセッション内容は・・・

セキュアなクラウド運用

クラウド運用に求められるもの

- ビジネススピード
  - ✓ 迅速なスケーリング
  - ✓ 開発とデプロイメントの高速化
- 生産性向上
  - ✓ コラボレーションの強化
  - ✓ 自動化と効率化
- 持続性・弾力性
  - ✓ ワークフローの標準化
  - ✓ サービスの継続性





クラウド運用の理想と現実

理想

開発-構築-運用まで統制のある組織

自動化による生産性向上

継続的なサービスデリバリ

ビジネス速度の向上、コスト最適

現実

部分最適化しているが連携が不備

マニュアル作業による事故の発生

一貫性がなく後戻りが多い

ビジネス速度の低下、コストアップ

責任の所在があいまいになりやすく、改善に時間がかかる

スピードを重視すると発生しがちな
「セキュアなクラウド運用」の落とし穴

ビジネス速度を優先することで起こり得るリスク

- セキュリティの後回し
  - セキュリティチェックが不十分で、脆弱な状態が未検出のまま放置されて攻撃者に悪用される
- 不十分なテスト
  - 全開発環境でセキュリティのワークフローが統一されていないと、テスト結果の差が見過ごされ、テストが不十分になる
- ガバナンスのおろそかさ
  - セキュリティのワークフローに統一性がないまま事故が起こると、会社の信頼性の損失につながる
- 設定ミス
  - クラウドサービスやデータベースの認証やセキュリティ設定が適切に行われない
- 自動化の過信
  - 自動化されたプロセスが不適切に設定されていて未検証の場合、ツール自体がセキュリティリスクになる

HCP Terraform

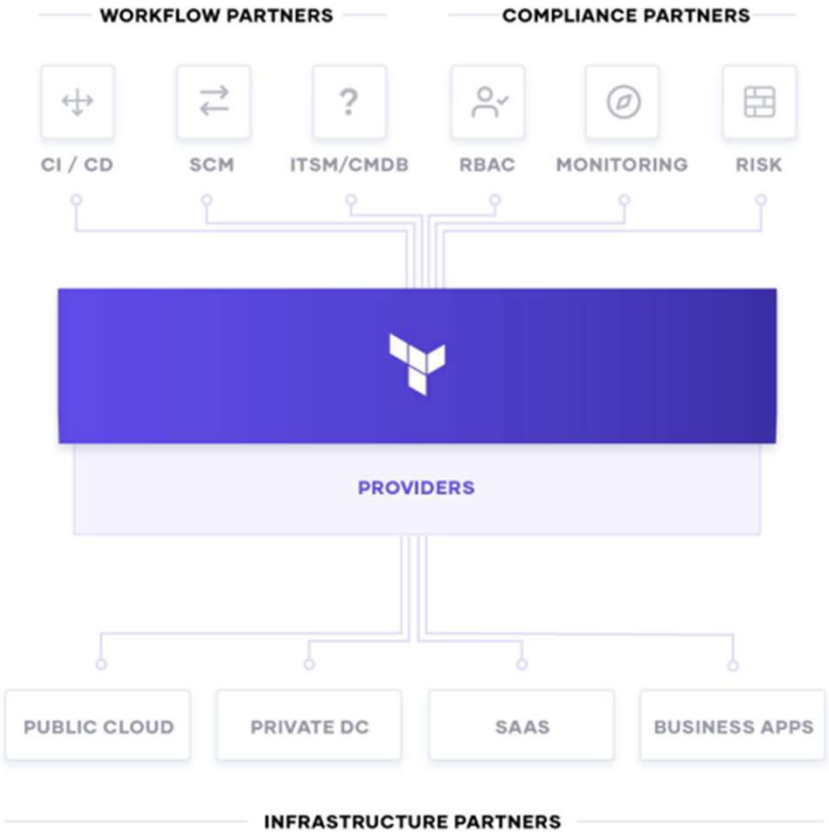
HCP Vault

そこで HashiCorp製品で課題を解決

HCP Terraform

HCP Terraform

- IaCソフトウェアツールの**デファクトスタンダード**
- 個人利用向け無償版と、組織利用向け有償版
- **多種多様なサービスやプラットフォームに対応**
- 一貫したワークフローでインフラを自動設定・構築

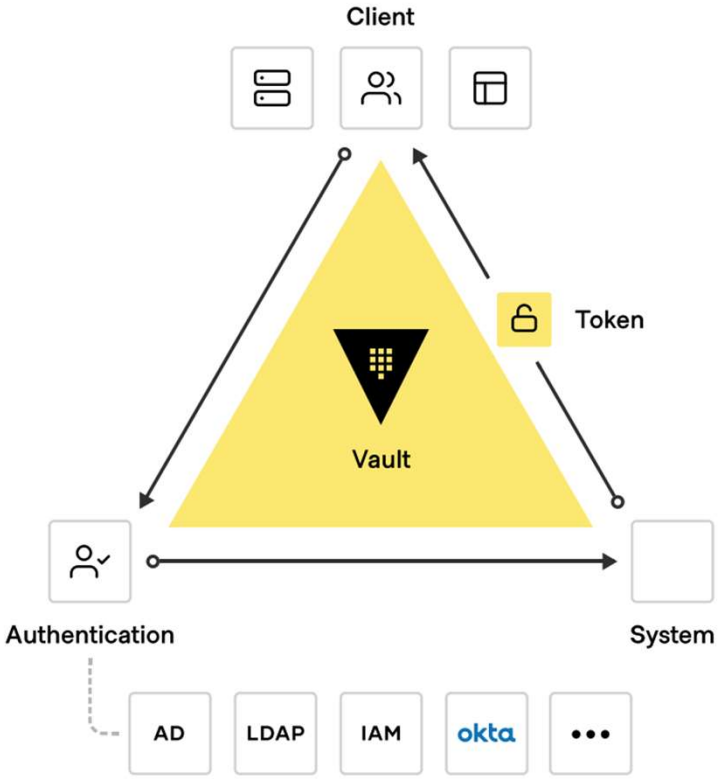


HCP Vault

Connect Beyond

HCP Vault

- クラウド運用における**シークレット運用管理**
- データを安全に保つ**クラウドセキュリティ自働化の基盤**
- 散逸しがちなシークレットを一元的に管理する
- シークレットの長期利用・使い回しを抑制



東京エレクトロン デバイス

HCP Terraform / Vaultで実現できること

Connect Beyond

HCP Terraform

HCP Vault

- ポリシーによるインフラの自動監査
- プロビジョニング後の運用までカバーする機能
- ノーコードで設定・構築

- サービスとしての暗号化
- シークレットの自動ローテーション
- 高度なデータ保護

ポリシーによるインフラの自動監査

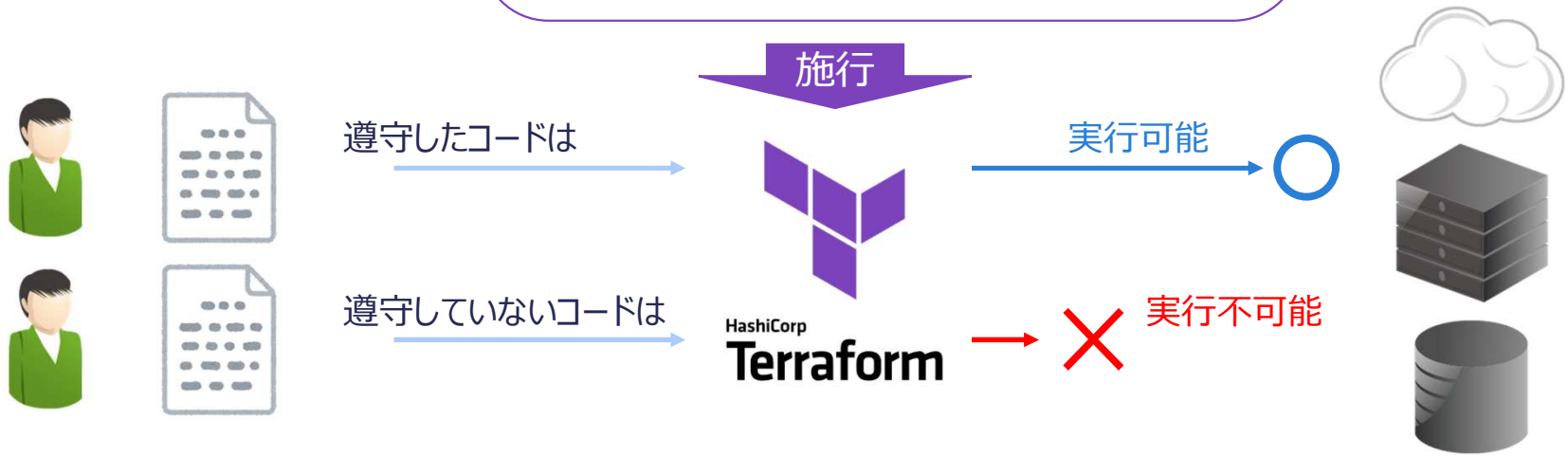
HCP Terraform

コードによるポリシー定義 (Policy-as-Code)

ポリシー記述は独自言語HCLを使う Sentinel または
OSSの汎用言語 OPA(Open Policy Agent) に対応

規定のポリシーをコードで定義し、自動監査

- 運用上の規定
  - ✓ 分類用の必須タグが無いリソースを禁止
  - ✓ 特定時間帯の作業の禁止
  - など
- セキュリティ上の規定
  - ✓ 通信ポリシーで送信元無制限の受信ルール禁止
  - ✓ 脆弱な認証方式の禁止
  - など



東京エレクトロン デバイス

プロビジョニング後の運用までカバーする機能

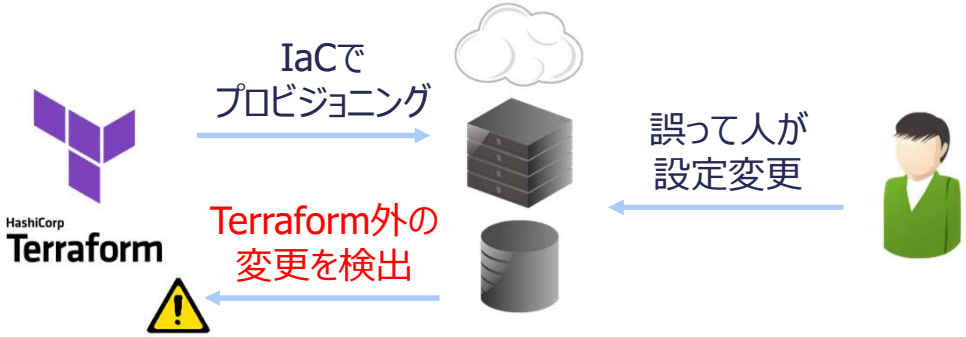
HCP Terraform

Connect Beyond

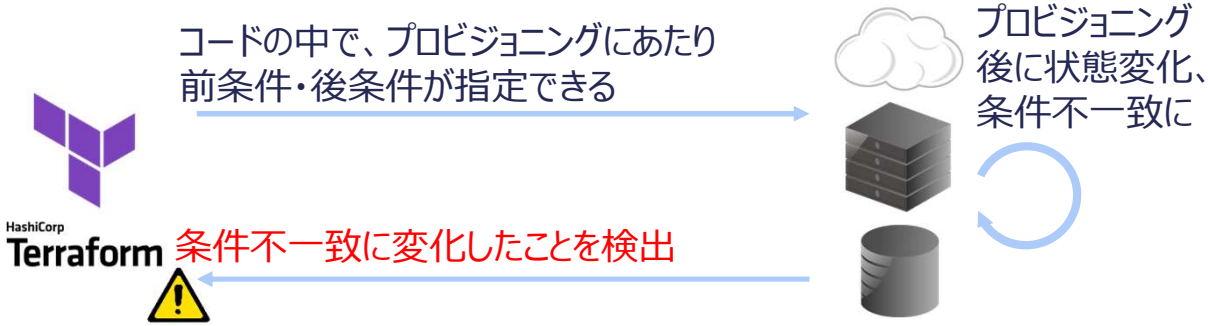
Terraformが行った設定内容を記録する

ステートファイル

ドリフト検出 (Drift Detection)



継続的検証 (Continuous Validation)

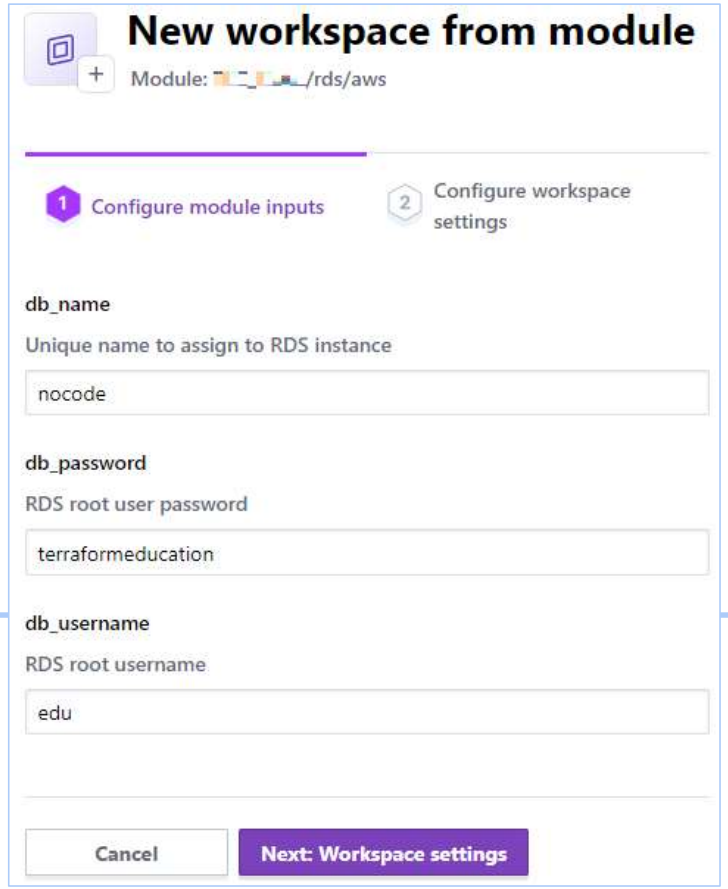


東京エレクトロン デバイス

ノーコード

HCP Terraform

ノーコードモジュールによる設定・構築



設定・構築を行う作業者はコードを記述しない。
ブラウザの画面からパラメーターを指定するだけでITインフラの設定・構築ができる。

東京エレクトロン デバイス

サービスとしての暗号化(Encryption as-a-Service)

HCP Vault

onnect Beyond

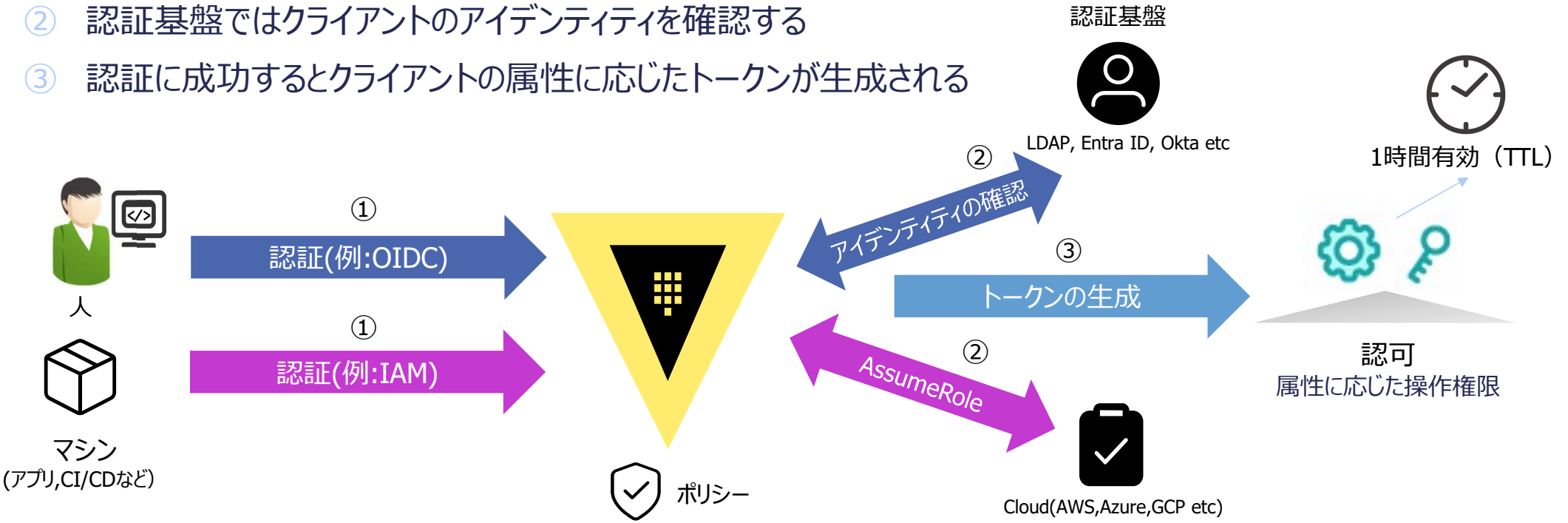
厳格なアクセス制限(1/2)

認証・認可

① クライアントはVaultを利用するために信頼された認証基盤で認証する

② 認証基盤ではクライアントのアイデンティティを確認する

③ 認証に成功するとクライアントの属性に応じたトークンが生成される



東京エレクトロン デバイス

サービスとしての暗号化(Encryption as-a-Service)

HCP Vault

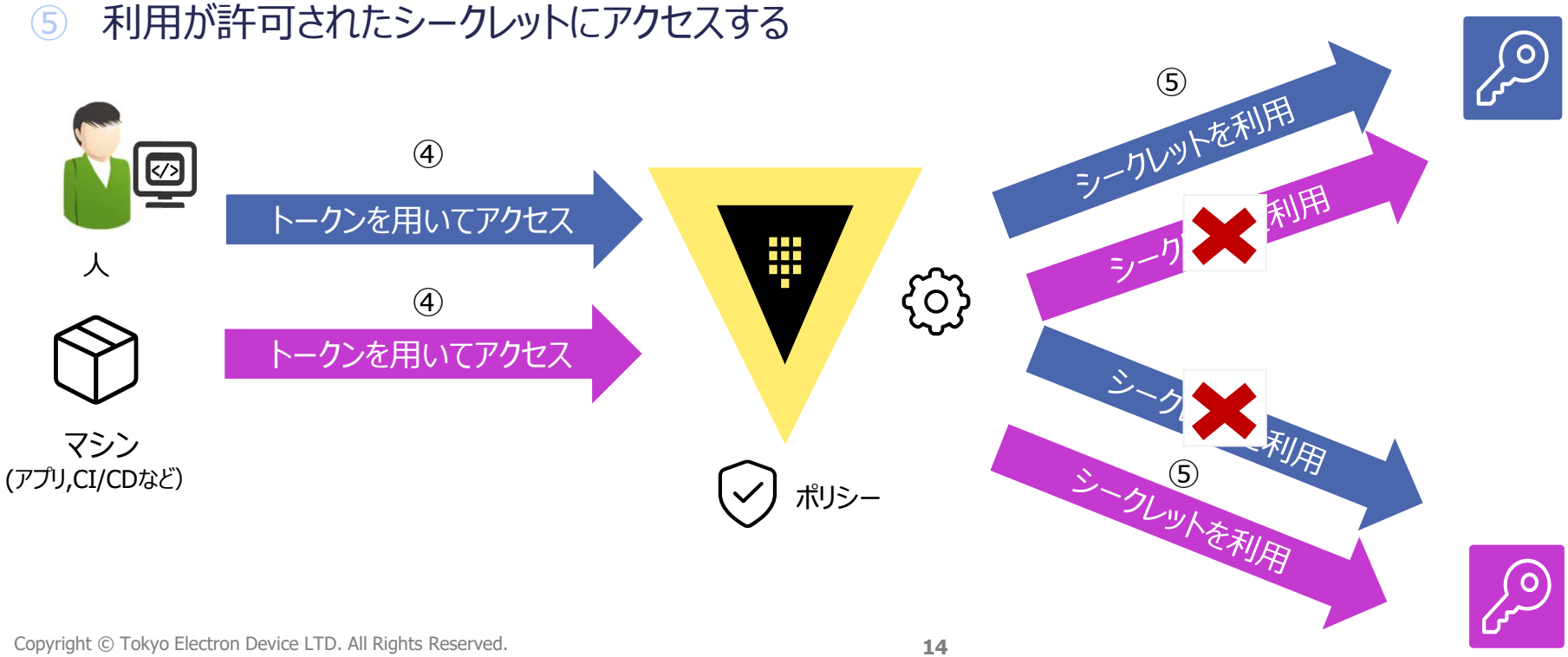
Connect Beyond

厳格なアクセス制限(2/2)

アクセス制御

④ クライアントは認証成功時に取得したトークンを用いてVaultにアクセスする

⑤ 利用が許可されたシークレットにアクセスする



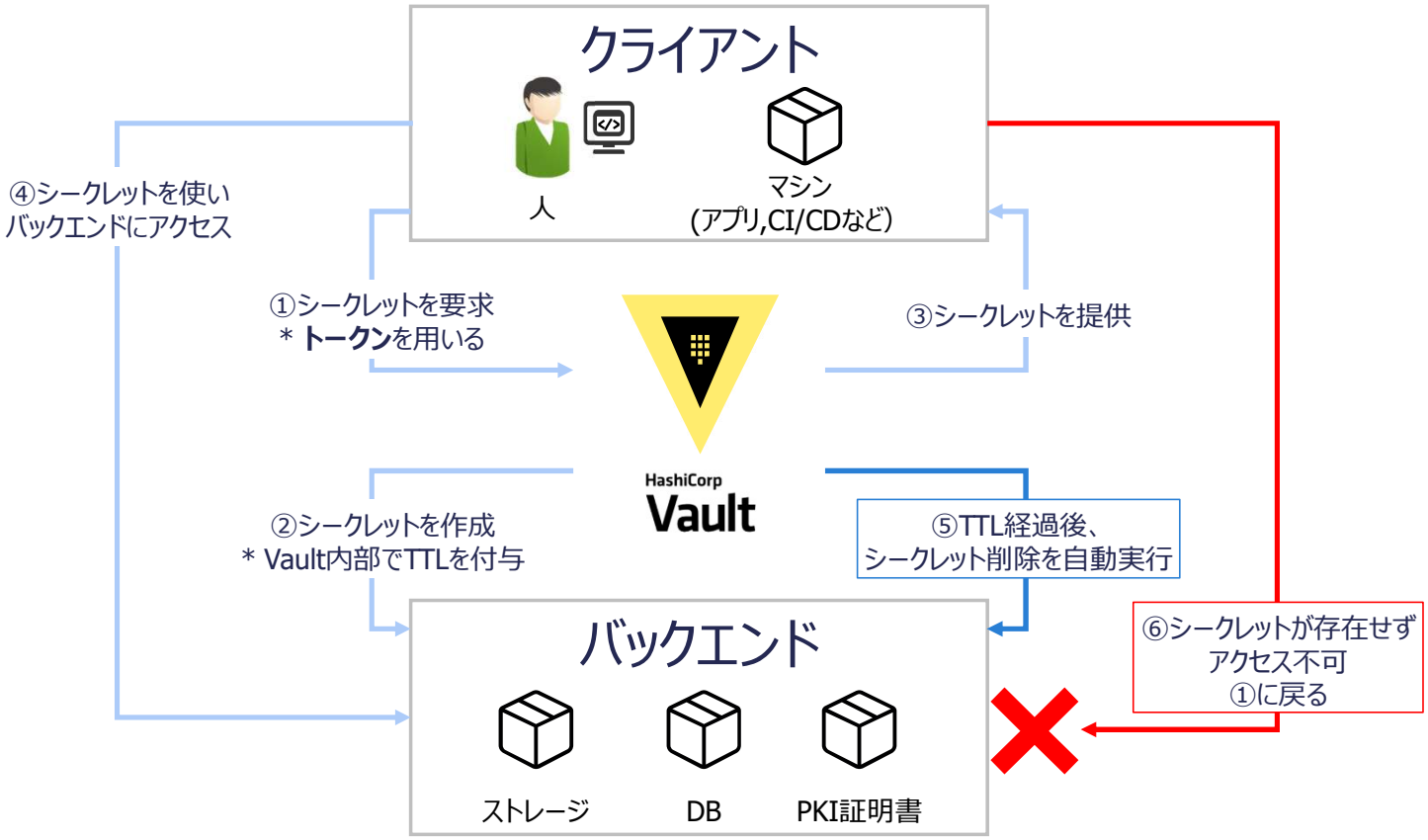
東京エレクトロン デバイス

TS0

シークレットの自動ローテーション

HCP Vault

Connect Beyond



動的シークレット

- ユニークかつ最小権限かつ有効期限(TTL)付きシークレットを必要な時のみ生成

- ファイルへのシークレット記入が不要
- 各クライアントごとにユニークなシークレットを利用可能
- 一定の期間でシークレットをローテーション

長期利用、使い回しを抑制。
自動ローテーションを委任できる

東京エレクトロン デバイス

スライド 15

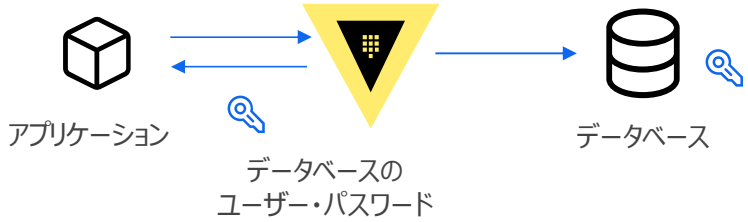
TS0 [@TED CBD Onose Tsubasa]
他社のロゴ使用許可が取れていない場合には、ロゴはテキスト入力に変更いただけますでしょうか。
よろしくお願いいたします。
TED CBD Nagasawa Sayaka, 2024-07-23T02:42:54.661

動的シークレットの利用シーン

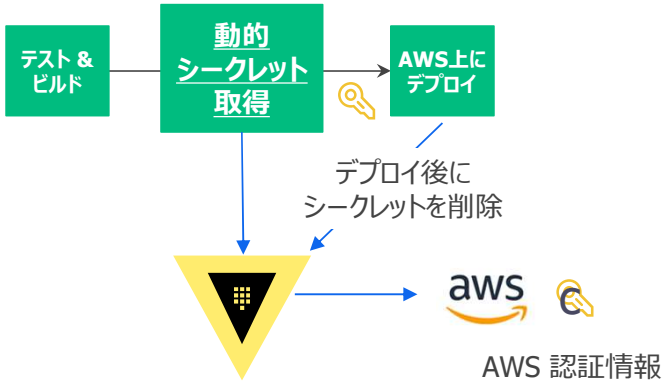
HCP Vault

onnect Beyond

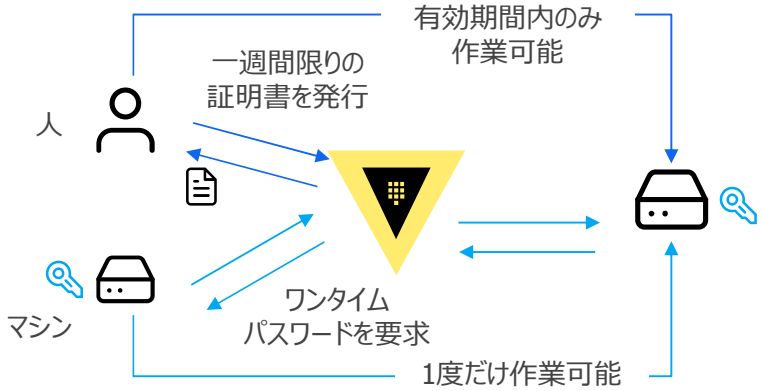
アプリケーションからの利用



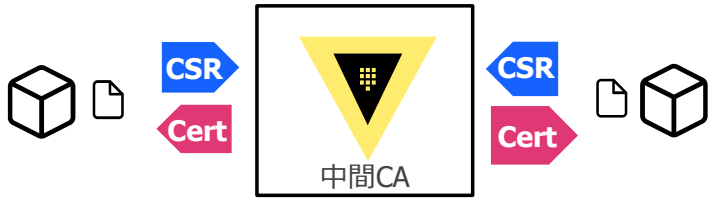
CI/CDからのデプロイ先への認証



SSH ログインでの利用



証明書管理



- 証明書の取得
- 証明書の破棄
- 権限管理
- 証明書の期限管理

東京エレクトロン デバイス

高度なデータ保護

HCP Vault

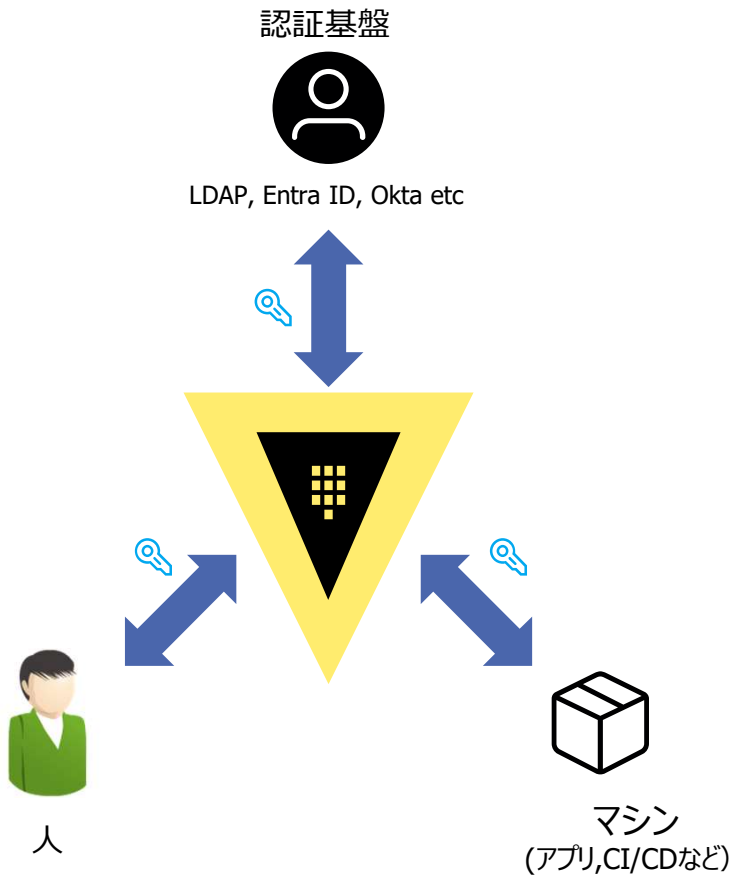
Connect Beyond

よりセキュアな運用を支援

セキュアなシークレットエンジン

- 鍵管理シークレットエンジン（KMSE）
  - さまざまな鍵管理サービス (KMS) プロバイダーの暗号鍵の配布
  - シークレットライフサイクル管理のための一貫したワークフローを提供

- KMIP(*)シークレットエンジン
  - Vaultが鍵管理相互運用プロトコル（KMIP） サーバーとして機能
  - KMIP管理対象シークレットのセキュアなライフサイクル処理を実現



*鍵管理サービスとクライアント間での相互運用性を確保するための通信プロトコル

セキュリティを後回しにしない！

最初から最後まで守り抜くインフラ！

不十分なテストを一掃！

堅牢なインフラ、確実なデプロイ！

ガバナンスを強化！

すべてのリソースを一元管理！

設定ミスゼロへ！

自動化されたポリシーで安心のデプロイ！

自動化を賢く活用！

シークレット管理で安心のオペレーション！

HCP Terraform　HCP Vault

を活用して、

セキュリティリスクを生まないクラウド運用を促進しましょう！

onnect Beyond

共に創る 新たな価値を

東京エレクトロン デバイス