ここまでやるのは難しい？
AWSのかなりセキュアな運用

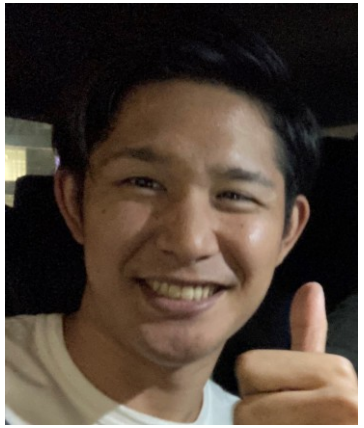
東京エレクトロン デバイス株式会社

2025年4月21日

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

自己紹介

- CN BU CN技術本部
  カスタマーサクセスデザイン部
  中林 稔
- 経歴
  - ネットワーキング,サイバーセキュリティ
  - プライベート/パブリック クラウド
  - HashiCorp製品担当



- CN BU
  ビジネス開発室
  山田 拓明
- 経歴
  - 半導体製品営業
  - ITインフラ、セキュリティ　アカウントセールス
  - セキュリティ、クラウドワークフロー 製品主幹

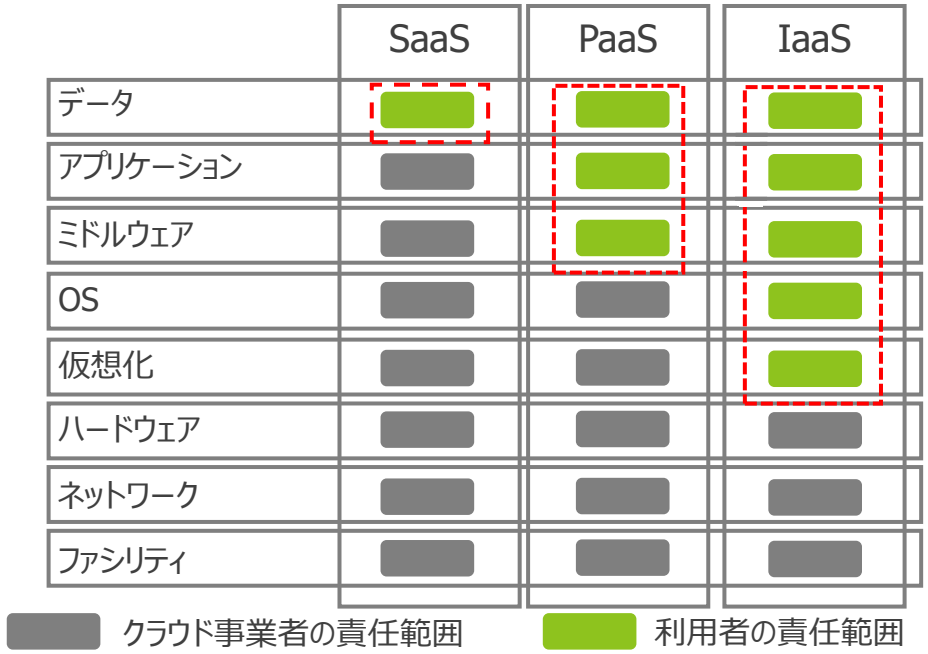
※7月からアメリカ拠点にて新技術のリサーチ業務に従事

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

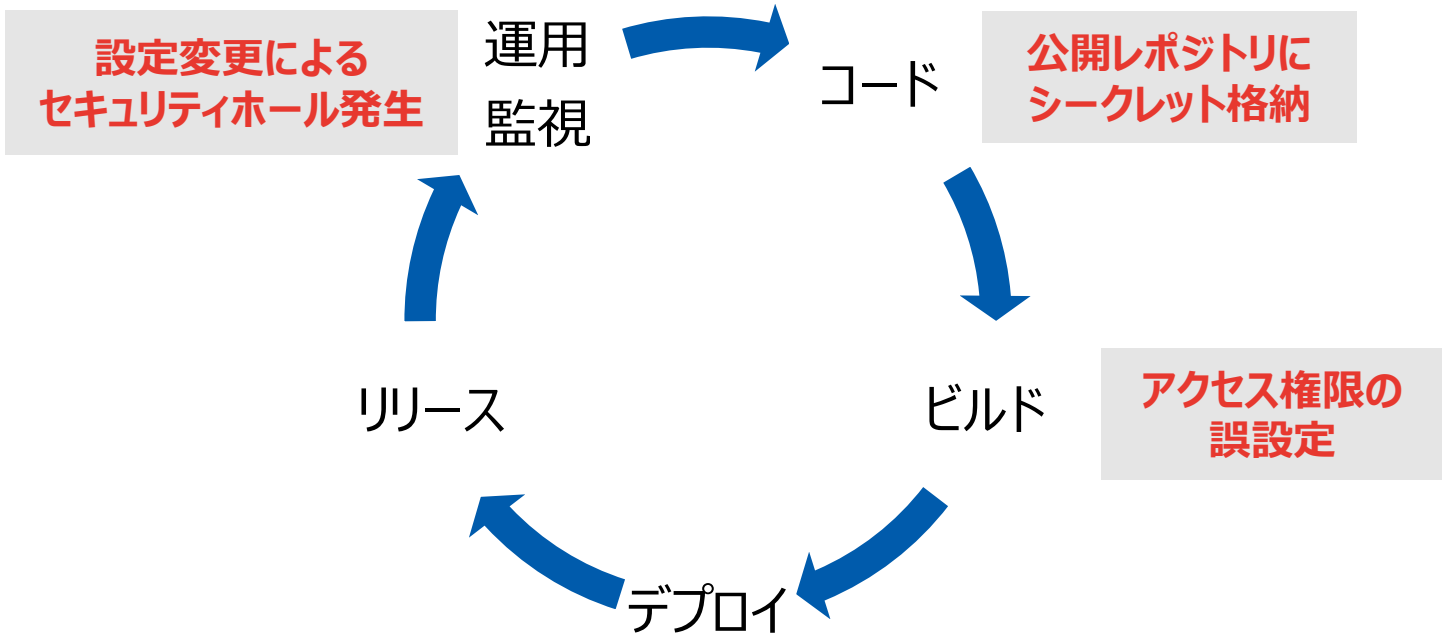
クラウドセキュリティのインシデント要因

セキュリティインシデントはヒューマンエラーが原因

AWSはセキュリティが堅牢
ユーザーの管理する対象が標的に



開発フローにおけるヒューマンエラー



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

AWSセキュリティツールのカバー範囲

AWSが用意しているプロダクト/サービスは33種類*もある

権限管理	証跡管理 ガバナンス	データ保護	脅威検出
Identity and Access Management	CloudTrail	Macie	GuardDuty
IAM アイデンティティセンター	Amazon Inspector	Key Management Service	Amazon Inspector
Cognito	IoT Device Defender	CloudHSM	Security Hub
Verified Permissions	Firewall Manager	Certificate Manager	Security Lake
AWS Directory Service	Shield	Private Certificate Authority	Detective
AWS Resource Access Manager	Artifact	Artifact	Config
AWS Organizations	Audit Manager	Secrets Manager	Security Incident Response
・ ・ ・	・ ・ ・	WAF	・ ・ ・

*1　AWS webサイトにてセキュリティ、アイデンティティ、およびコンプライアンス製品に位置づけられている製品

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

AWSセキュリティツールのカバー範囲

AWSが用意しているプロダクト/サービスは33種類*もある

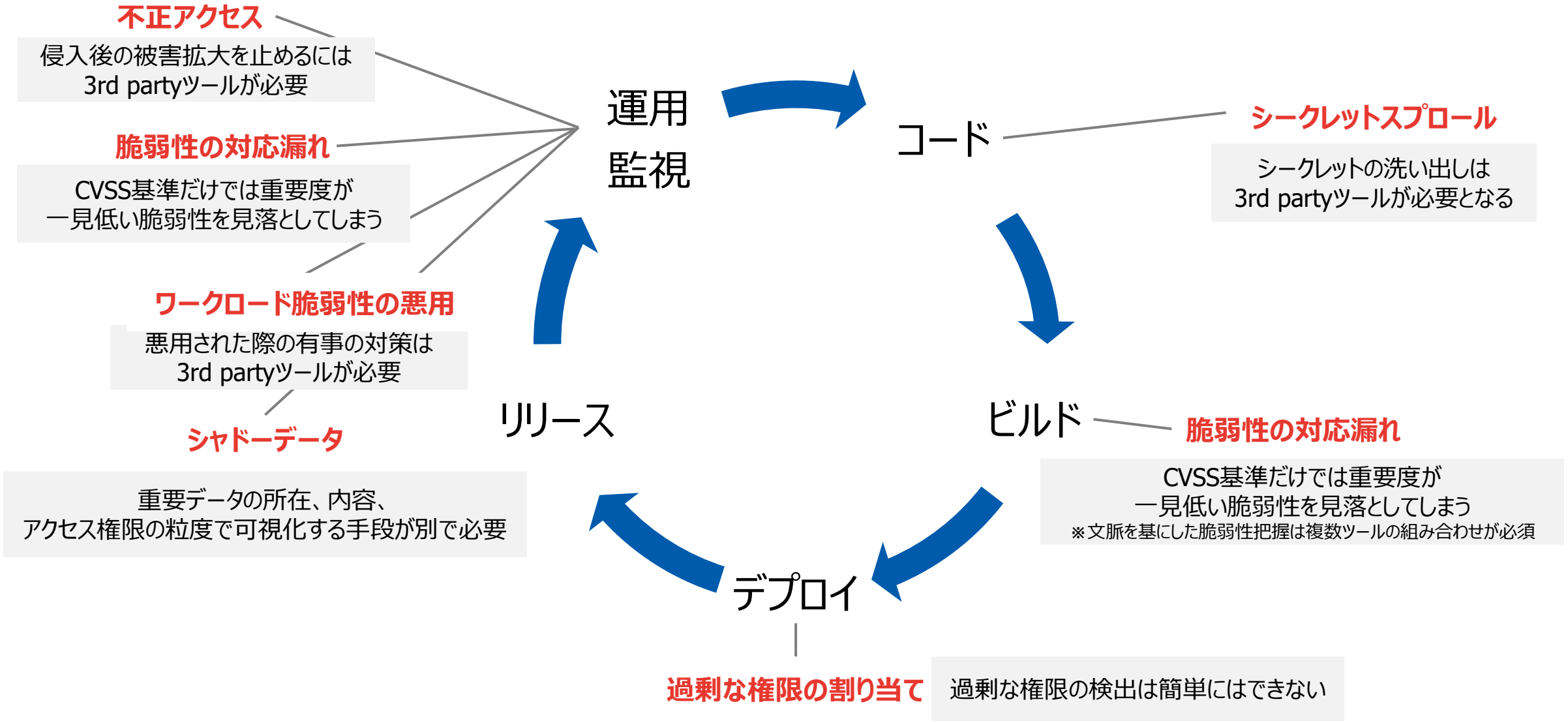
一方、AWSサービス単体では、カバーしきれない**リスク**も**多く**存在

*1　AWS webサイトにてセキュリティ、アイデンティティ、およびコンプライアンス製品に位置づけられている製品

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

AWSのツール以外の方法で対策が必要なリスク

AWSネイティブツールにない他のツールを活用した対応が必要



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

onnect Beyond

ソリューションのご紹介

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

複雑化しがちな組み合わせ対応をシンプル化

クラウド統合セキュリティのCNAPPとガバナンスを考慮したIaCでシンプル化

環境の構築・修復

HCP Terraform

クラウド設定をコード化、**自動化**することで
効率的にセキュアにクラウド環境を運用する

可視化・修復支援

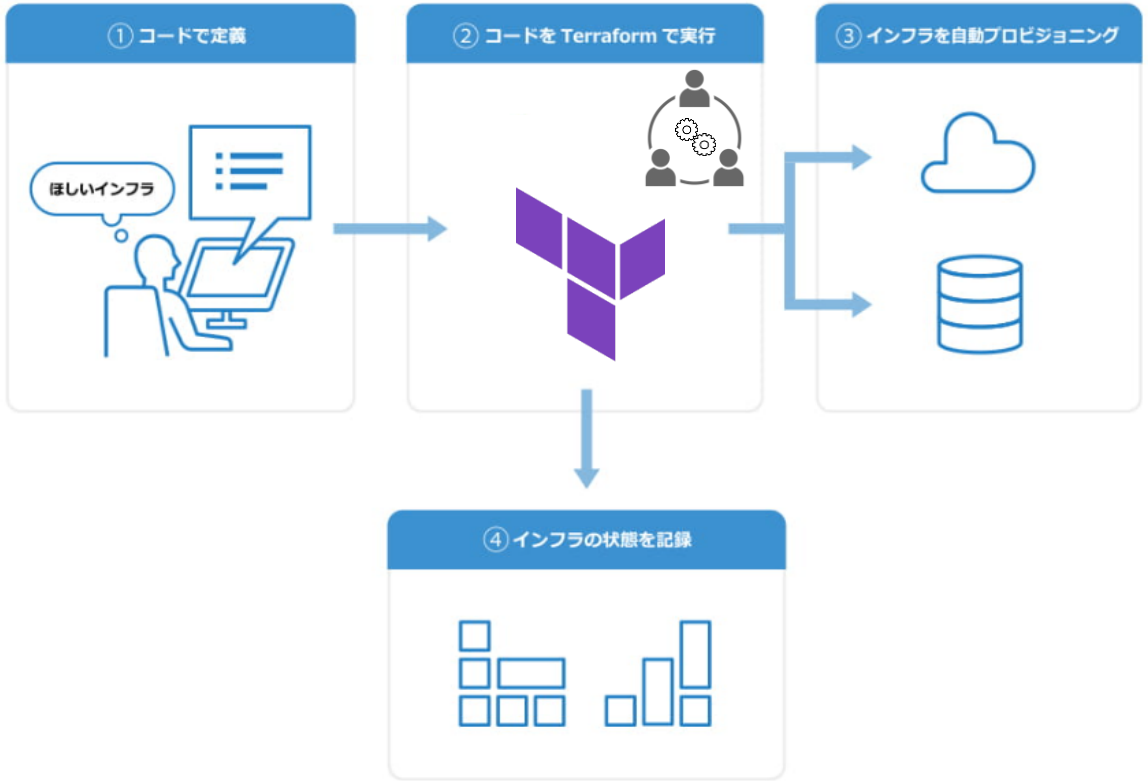
WIZ

設定ミスや脆弱性を継続的に**可視化**、
改善案を提示することで、
セキュリティリスクの管理を支援する

複雑性の回避で対応の抜け漏れも減少

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

IaC（Infrastructure as Code） - インフラをコードで管理



課題

- 他部門で勝手にIaaSなどの利用が始まり、統制が効かない
- 複数クラウドやオンプレでGUI操作が製品ごとに異なる
- マニュアルによる統制の限界

導入後の効果

- 人手からコードへの移行により、インフラ構築ミスの大幅削減
- 属人化の撤廃
- 学習コストの削減

特徴

- パブリッククラウド、SaaS、オンプレまでマルチにサポート
- Terraformのみ覚えれば良いため学習コスト削減

オールインワンのインフラ作成機能を提供

※HCPとはHashiCorp Cloud Platformの略で、HashiCorpが管理するSaaSサービス

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Wiz とは？
アプリと実行環境を包括的に守るCNAPP

過去に遡ってリスクを予防

Wiz Code
セキュアなクラウド開発

現在あるリスクへの対策

Wiz Cloud
セキュリティポスチャー管理

将来起こりうる脅威への対策

Wiz Defend
クラウド脅威への対応

シークレット　脆弱性　データセキュリティ　アイデンティティセキュリティ　構成管理　インターネット公開

セキュリティ対策のシフトレフトを支援

コードやバージョン管理システムの構成における
重大なセキュリティリスクを特定。

CI/CDパイプラインを調査し、潜在的な脆弱性、設定ミス、シークレット、機密データを検出し、設計段階からセキュリティを強化します。

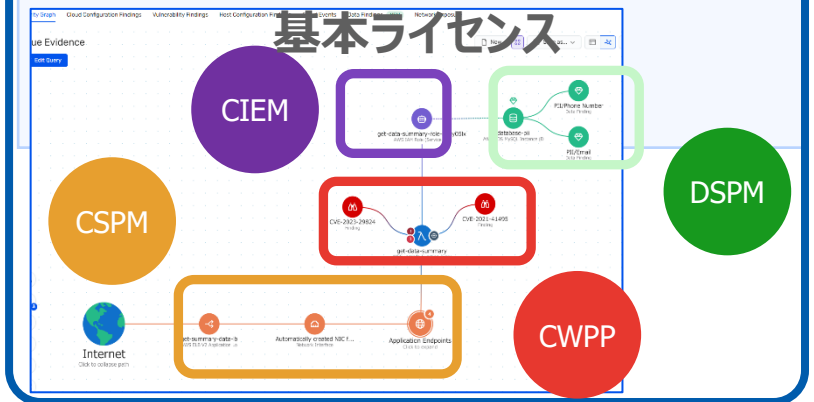
オプションライセンス

オールインワンのCNAPPを提供

ワークロード、VM、データベース、アプリケーションなど、お客様のクラウドテクノロジースタックのすべてのレイヤーからデータをエージェントレスで収集。

取得したデータを分析してリスクと設定ミスを関連付け、最も重大な問題を特定し、クラウド環境全体の攻撃対象領域をプロアクティブに削減。

基本ライセンス



リアルタイム脅威検知を提供

コードとクラウドログを使用してリアルタイムで脅威を検知し、
疑わしい活動の根本原因を調査・特定。

SecOps、CloudSec、開発者間の連携を促進し、インシデント対応者がプラットフォームからアクションを発行して脅威を封じ込めることを可能にします。

オプションライセンス

Copyright © Tokyo Electron Device LTD. All rights reserved.

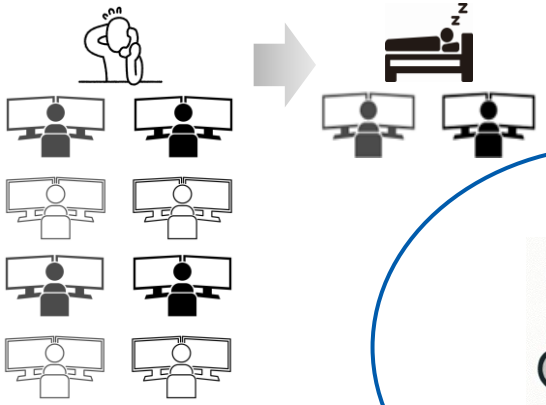
東京エレクトロン デバイス

具体的な解決策の説明

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

変化に強いアプリケーションのライフサイクル

「眠れる」セキュリティ運用



運用

開発

AWS

WIZ ×

コード開発

VCS

シークレット、機密データの露出防止

ビルド

アーティファクトの脆弱性を検出

デプロイ

コンプライアンス遵守

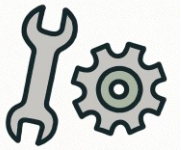
リリース

一貫性の維持

監視・分析

新たな脆弱性の発見、ドリフト検出

修復



即応または計画メンテナンスの判断を支援

監査

通知

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

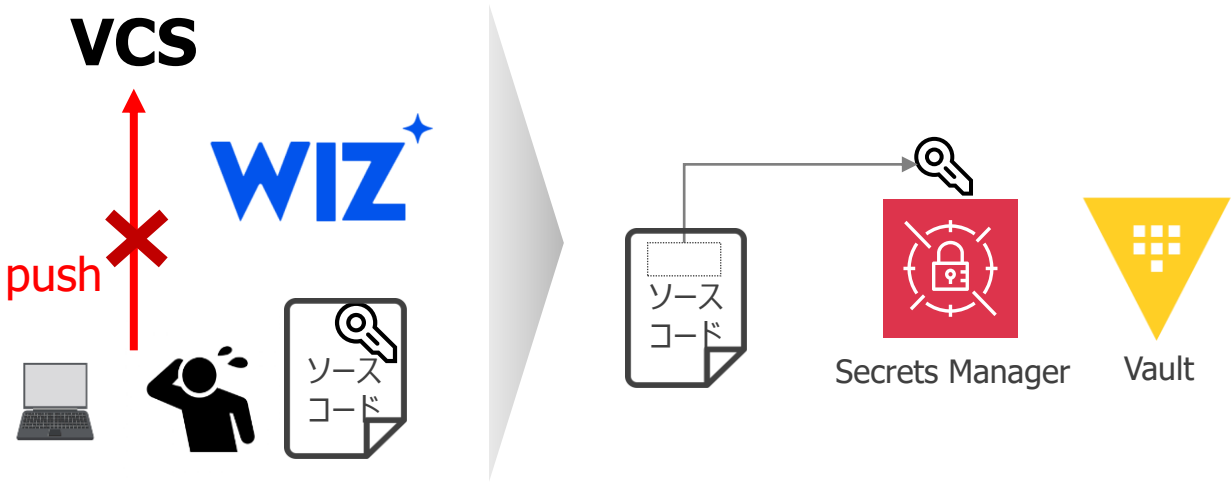
コードを守る

コード開発時のシークレット露出を防止

シークレットスプロールの対策

- ✓ **IDE（VS Code）上**でシークレットを検出し、Wizが提案した修正案をもとにコミット前に対応
- ✓ **プルリクエスト時**にシークレットを発見し、レビュー段階で漏えいを防止することも可能
- ✓ 検出されたシークレットは AWS Secrets Manager や HashiCorp Vault に移行し安全に管理
- ✓ 管理されたシークレットは、定期的に自動でローテーションしてセキュリティを維持

シークレットの種類	ファイルの種類
パスワード	ソースコード
シークレットアクセスキー	設定ファイル
APIキー	スクリプト
アクセス・トークン	IaCコード
SSHキー	テキストファイル
一般的なシークレット	テストデータ



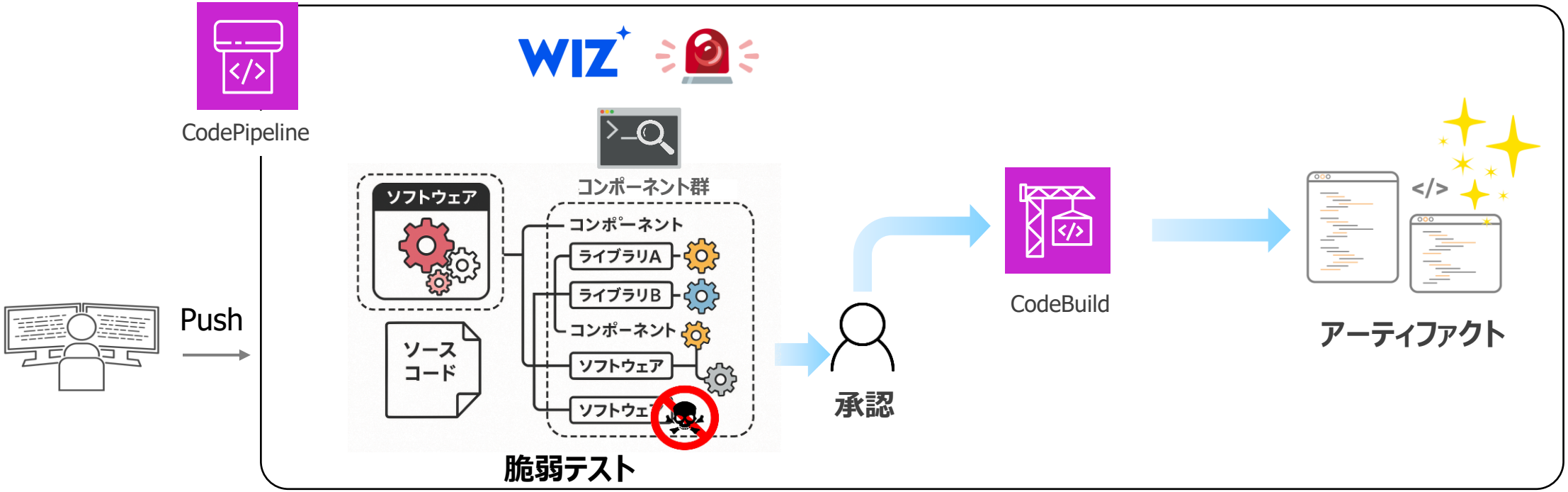
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

ビルドを守る

リスクを排除したアーティファクトで、安全な環境を確保

□ 脆弱性の対応漏れの対策

- ✓ コンテナイメージやライブラリに脆弱性スキャナを適用し、CVEやライセンスリスクを検出
- ✓ OSSの依存関係を可視化し、脆弱性の有無を診断。リスクのあるコンポーネントを特定
- ✓ ビルド前に**CLI**でスキャンを実行し、手動承認後に安全なアーティファクトを生成



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

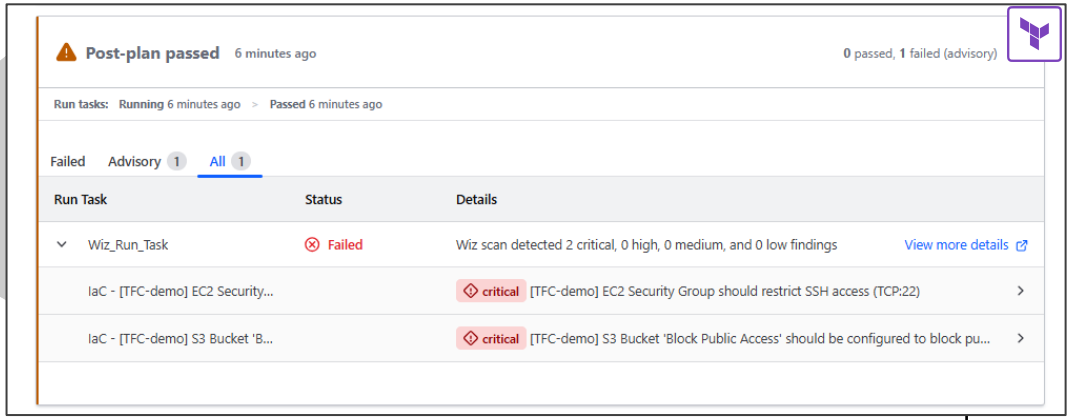
インフラ適用前に過剰な権限をブロック

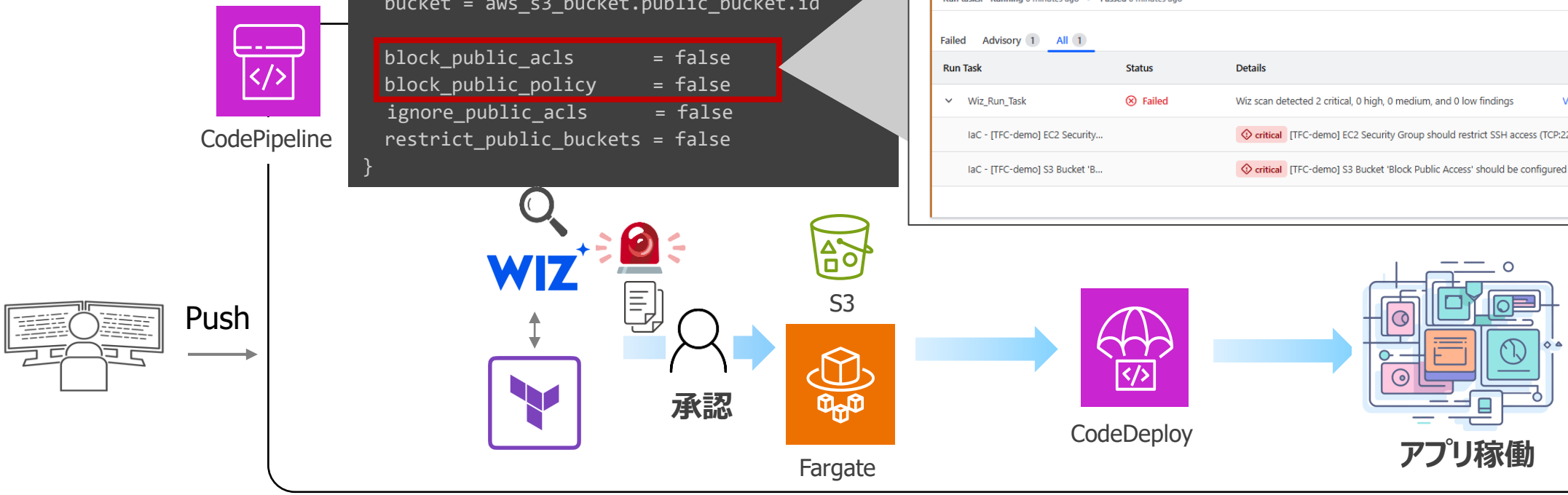
◻ 過剰な権限の割り当ての対策

- ✓ WizがTerraformコードをスキャンし、過剰な権限設定がインフラに適用されるのを未然にブロック
- ✓ これまで目視で行っていたIAMポリシーなどの確認作業を、自動化・省力化

```
resource "aws_s3_bucket_public_access_block" ¥
 "allow_public_access" {
  bucket = aws_s3_bucket.public_bucket.id

  block_public_acls       = false
  block_public_policy     = false
  ignore_public_acls      = false
  restrict_public_buckets = false
}
```





Copyright © Tokyo Electron Device LTD. All Rights Reserved.

リリースを守る

再現性のあるインフラで、スムーズに本番リリース

- テストと本番の差異を抑えた、一貫性のあるインフラ構成
  - ✓ 十分に検証された環境を本番に適用できるため、手戻りの少ない安全なリリースを実現

Terraformによる本番環境のインフラ適用の流れ

①インフラの設定への変更をVCSにコミット

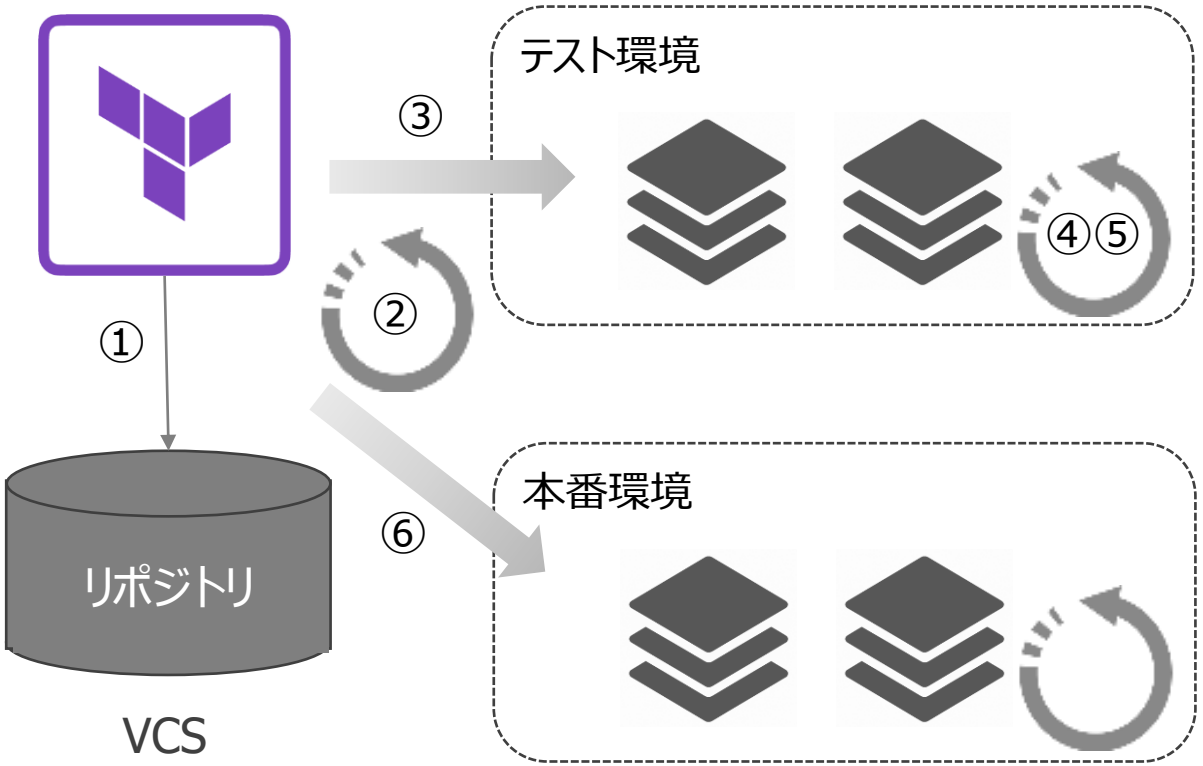
②単体テストを実行し、フォーマットや設定をチェック

③テスト環境に変更を加えたリソースを作成・更新

④テスト環境のリソースに結合テストを実行

⑤テスト環境のリソースにE2Eテスト実行

⑥テスト環境と同じ流れを本番環境にも適用

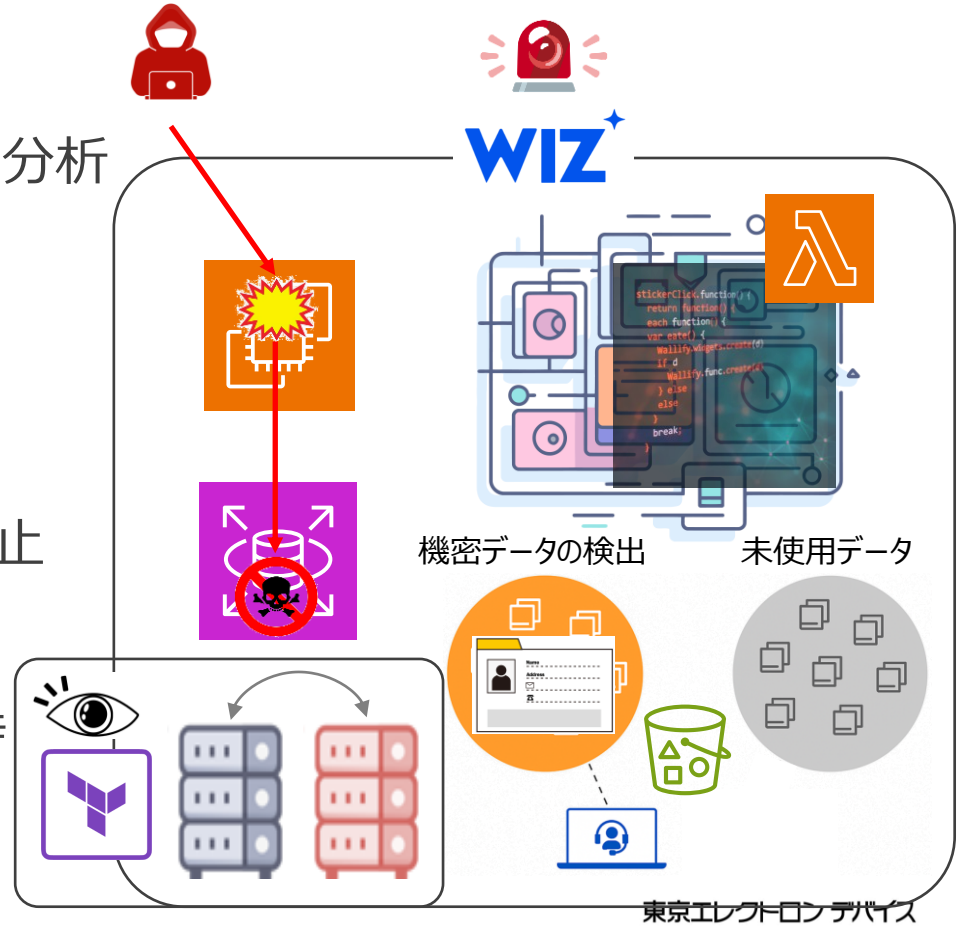


Copyright © Tokyo Electron Device LTD. All Rights Reserved.

運用を守る

変化するリスクを見逃さず、常にセキュアな状態を維持

- ワークロード脆弱性の悪用対策
  - ✓ ランタイムでの挙動監視と振る舞い検知により、実際の攻撃や不審なプロセスを検出
- 不正アクセスの対策
  - ✓ 誰が何にアクセスできるかを見える化し、潜在的なリスクを管理・分析
- シャドー・データの対応
  - ✓ 機密データを自動で検出・分類し、休眠データも特定
- 脆弱性の対応漏れの対策
  - ✓ 継続的な脅威検出と優先度に基づく対策で、大きな事故を防止
- ドリフト検出と対策
  - ✓ 意図しない設定変更を検知し、構成の一貫性と安全性を維持



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まとめ

セキュリティリスクを最小限に抑えつつ、スピードと統制を両立する

フェーズ	Wiz × HCP Terraform の主な機能	具体的なメリット
開発	継続的インテグレーション（CI） • シークレットスキャン • 脆弱性スキャン • リアルタイムフィードバック	• 機密情報の漏えい防止 • 早期のセキュリティリスク発見 • 手戻りを抑え、開発効率を最大化
	継続的デリバリ（CD） • ポリシーチェック • IaCコードスキャニング • IaCコードの標準化	• ガードレールによるガバナンス強化 • コンプライアンスの早期確保 • 再現性の高いインフラでリリースを高速化
運用	リスクの発見と対応 • 継続的セキュリティ監視 • リスク分析・優先順位付け・修復提案 • 設定ドリフト検出	• 新たな脅威の早期検知 • 効率的な問題対応 • インフラの一貫性を持続的に維持

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Connect Beyond

共に創る 新たな価値を

東京エレクトロン デバイス

Copyright © Tokyo Electron Device LTD. All Rights Reserved.