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

Wizで実現する、イノベーションを加速させるクラウドセキュリティ

東京エレクトロン デバイス株式会社

Yossy Sakai

自己紹介

- 東京エレクトロン デバイス株式会社
  CN BU　CNビジネス開発室
  マーケティングエンジニア, エバンジェリスト
  酒井 由純
  Yossy Sakai

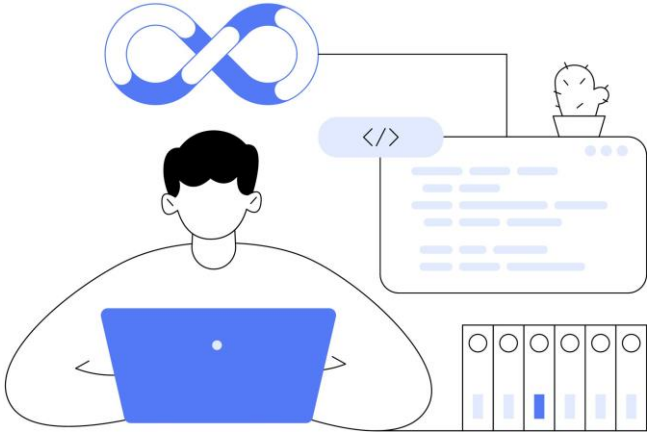
- 経歴
  - ✓ ネットワーキング（L2/L3, エンタープライズやキャンパス）
  - ✓ サイバーセキュリティ
  - ✓ マーケットリサーチ at SF Bay Area
  - ➢ ビジネス開発

本日のお話は

クラウドセキュリティ

クラウドに集まる利用者の目線

インフラ運用・管理
情シス、CCoE、SRE



アプリ開発者

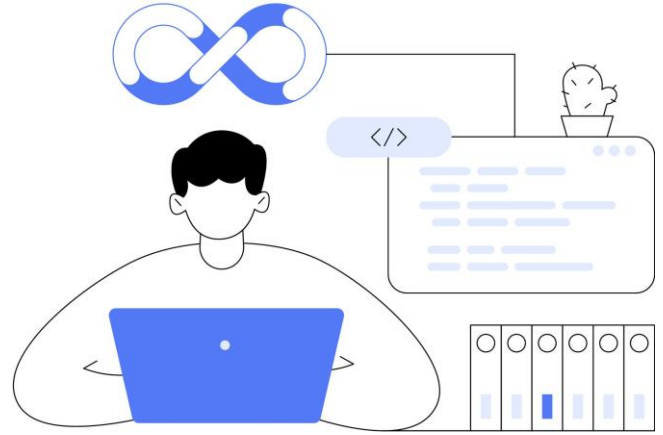
クラウドサービス
IaaS, PaaS, SaaS

アプリ利用
従業員、サプライチェーン

アプリ利用
一般消費者

今回のお話の主な対象は

インフラ運用・管理
情シス、CCoE、SRE



アプリ開発者

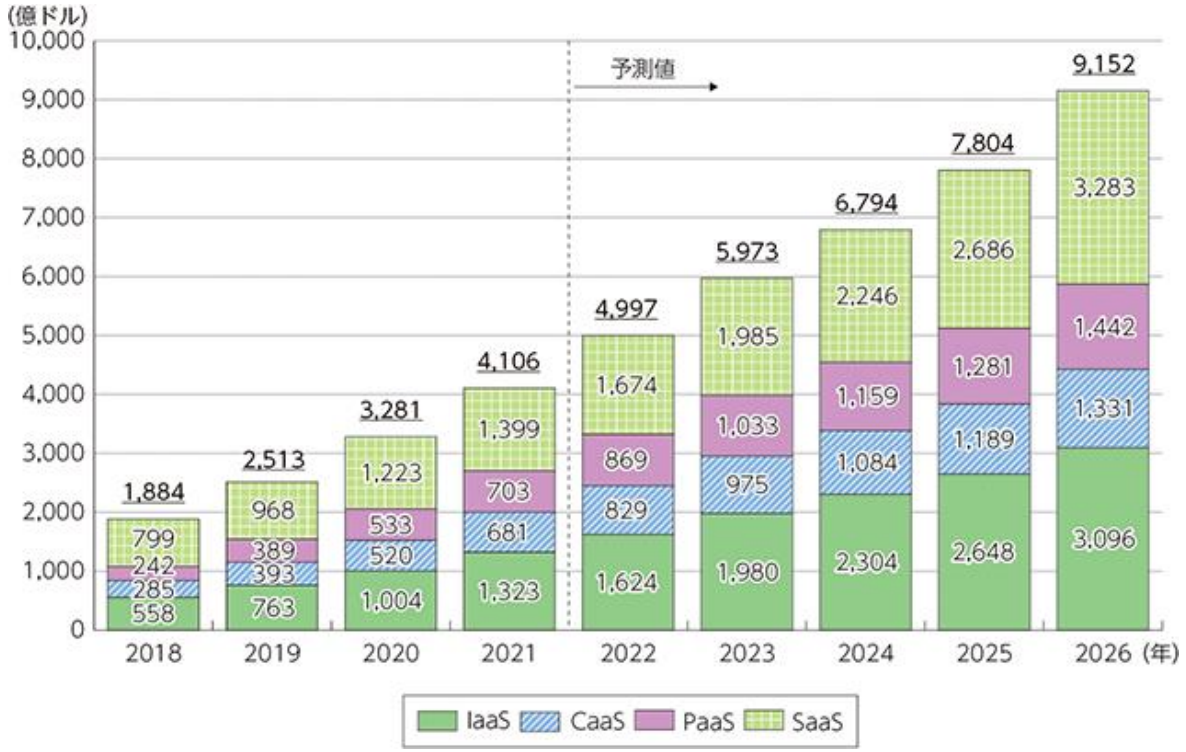
クラウドサービス
IaaS, PaaS, SaaS

アプリ利用
従業員、サプライチェーン

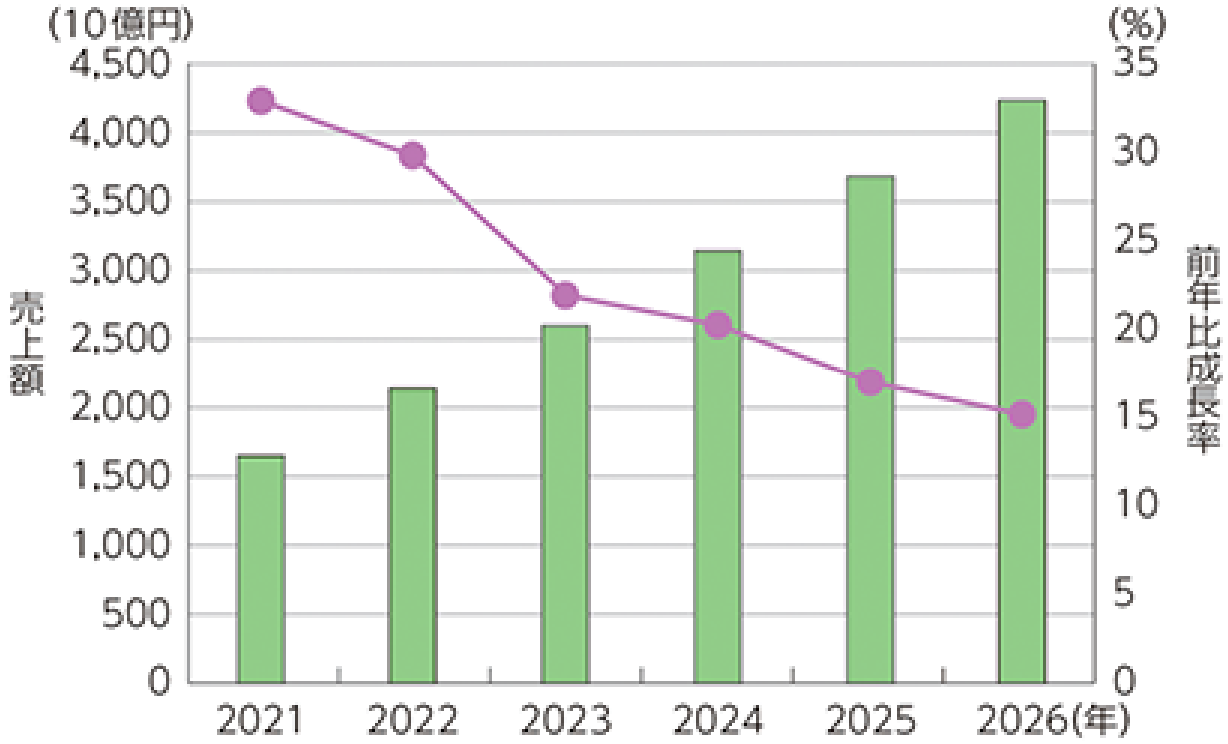
アプリ利用
一般消費者

世界でも日本でも 市場は拡大

世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測



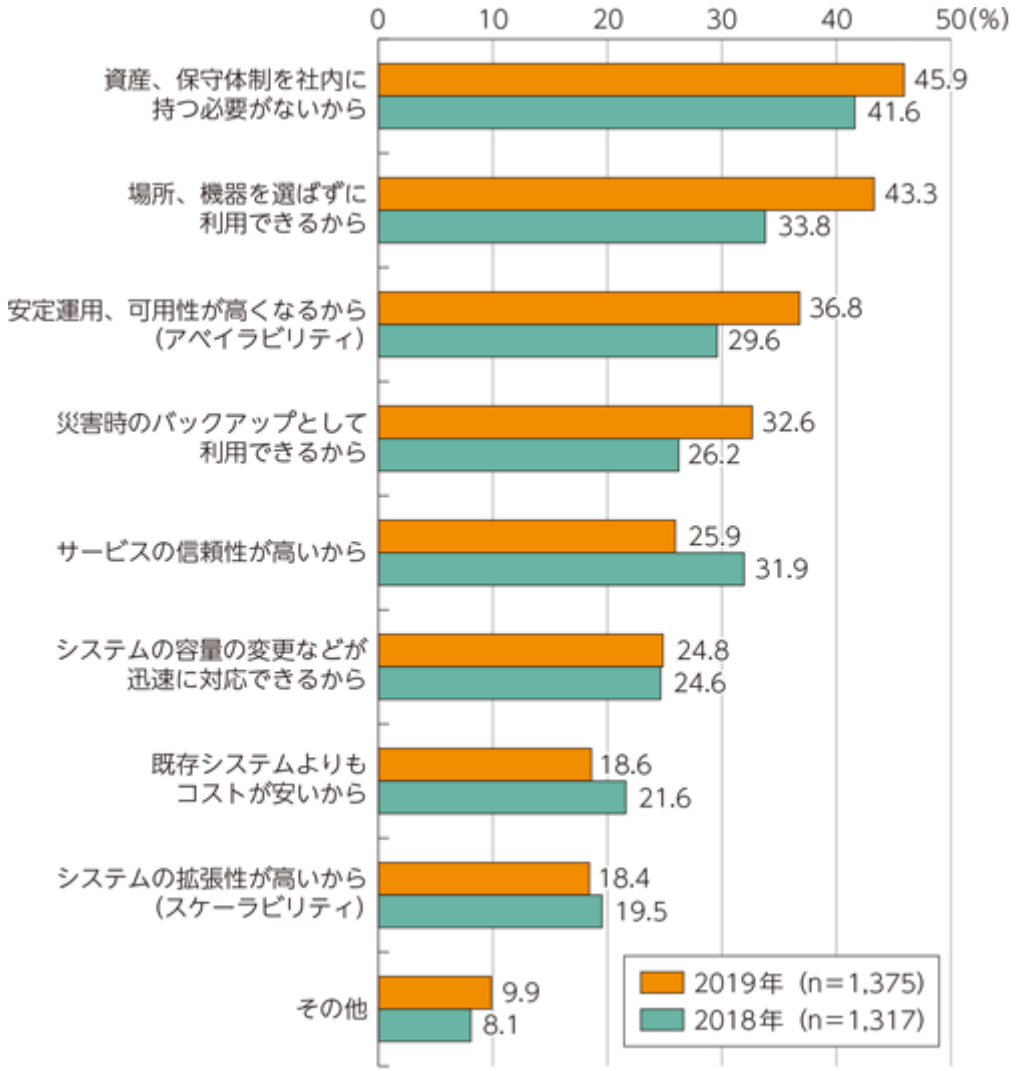
日本のパブリッククラウドサービス市場規模（売上高）の推移及び予測



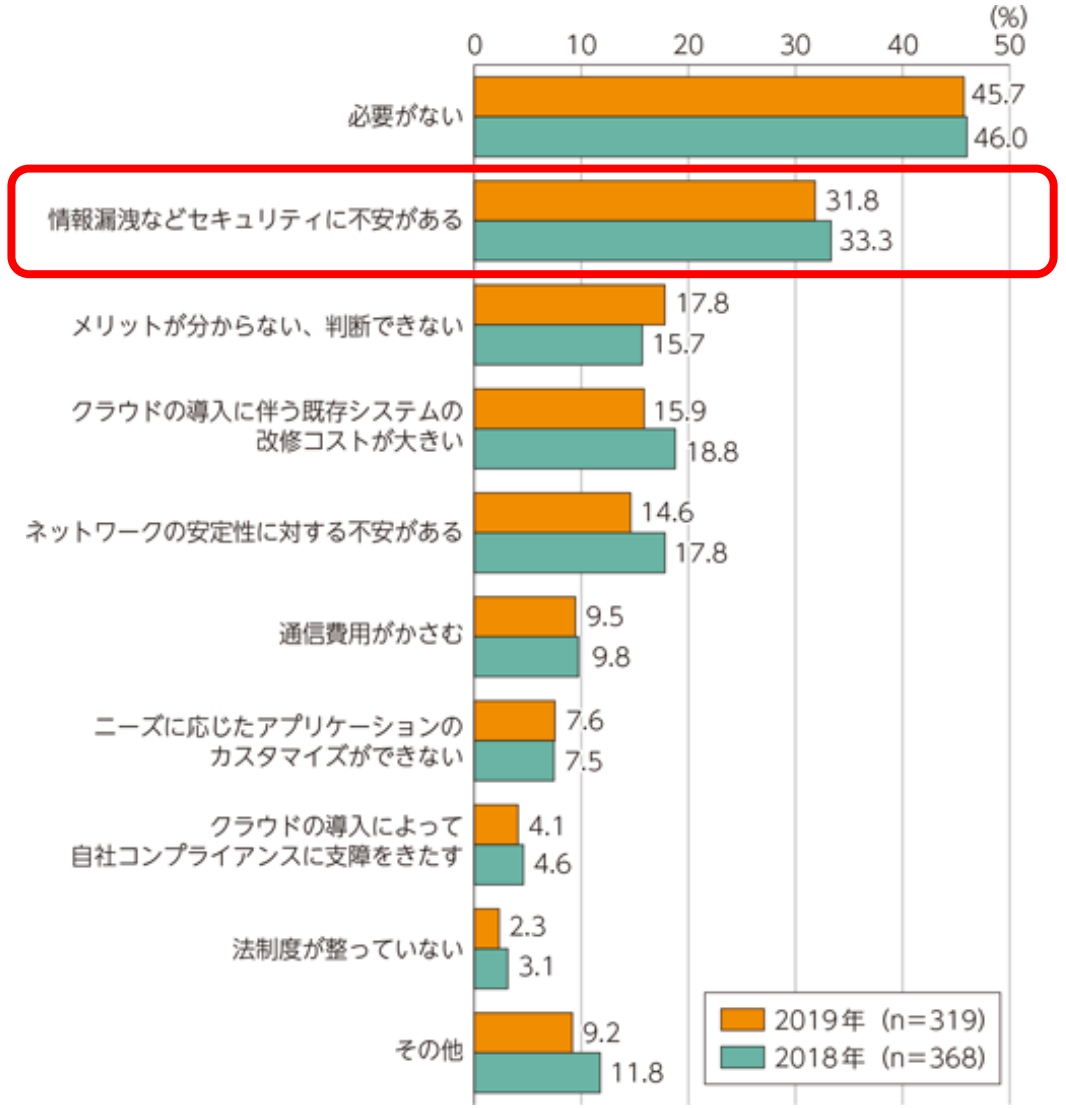
出典: 総務省 情報通信白書 令和5年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd248200.html

イノベーションを加速させるクラウドサービス

クラウドを 利用する理由 と 利用しない理由



※「場所、機器を選ばずに利用できるから」の2018年の数値は、「どこでもサービスを利用できるから」のもの。



出典: 総務省 情報通信白書 令和2年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd252140.html

海外のセキュリティインシデント事例

内部機密データを誤って インターネットに公開

- ✓ 過剰なアクセススコープ
- ✓ 過剰なアクセストークンへの権限
- ✓ 意図せずインターネットに公開

出典: 38TB of data accidentally exposed by Microsoft AI researchers (2023/9/18)
https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers

国内のセキュリティインシデント事例

ヘルスケア系サービスプロバイダーで ノーウェアランサム被害

- ✓ 委託先企業の不適切なアクセスキー管理
- ✓ アクセスキーの漏えい
- ✓ 漏えいした情報を不正アクセスへ悪用被害
- ✓ 利用者のPII/PHIなどが流出

クラウドサービス利用時の注意点

- 障害などによりデータが消失する

クラウドセキュリティ

- 預けているデータが外部に漏えいする
- クラウドサービスのアカウントが第三者に悪用される

出典: 総務省 クラウドサービス利用上の注意点 | 国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_security02_06.html

クラウドのリスクマネジメントで「把握」すべき6つの事項

onnect Beyond

資源 資産
を把握する

- クラウドリソース
- 機密データ
- SBOM

など

危険
を把握する

- クラウドの構成
- 脆弱性
- マルウェア
- ユーザーと権限

など

被害
を把握する

- リモートコードの実行
- IDや権限の悪用
- ラテラルムーブメント

など

影響
を把握する

- 機密データの漏えい
- アカウントの悪用
- 影響の重大度

対策
を把握する

- 修正すべき構成と内容
- バージョンアップ手順
- 適切な運用方法

状況
を把握する

- 対策前後の効果
- 構成や状況の変化
- 新しいアカウント
- 新しい脅威
- コンプライアンス

クラウドのセキュリティ統制の現況

なにを？

セキュリティの向上・統制

だれが？

情報セキュリティ担当者

- ✓ 情シス部門が兼務も多い
- ✓ クラウドを直接管理・利用する部門ではないことが多い

どうやって？

1. なにもできていない(現場任せ)
2. チェックシート
3. CSP等のサービス・ツール

イノベーションの
足を引っ張る可能性が！

セキュリティがクラウドによるイノベーションの足を引っ張る？

クラウドチームのチェック・回答

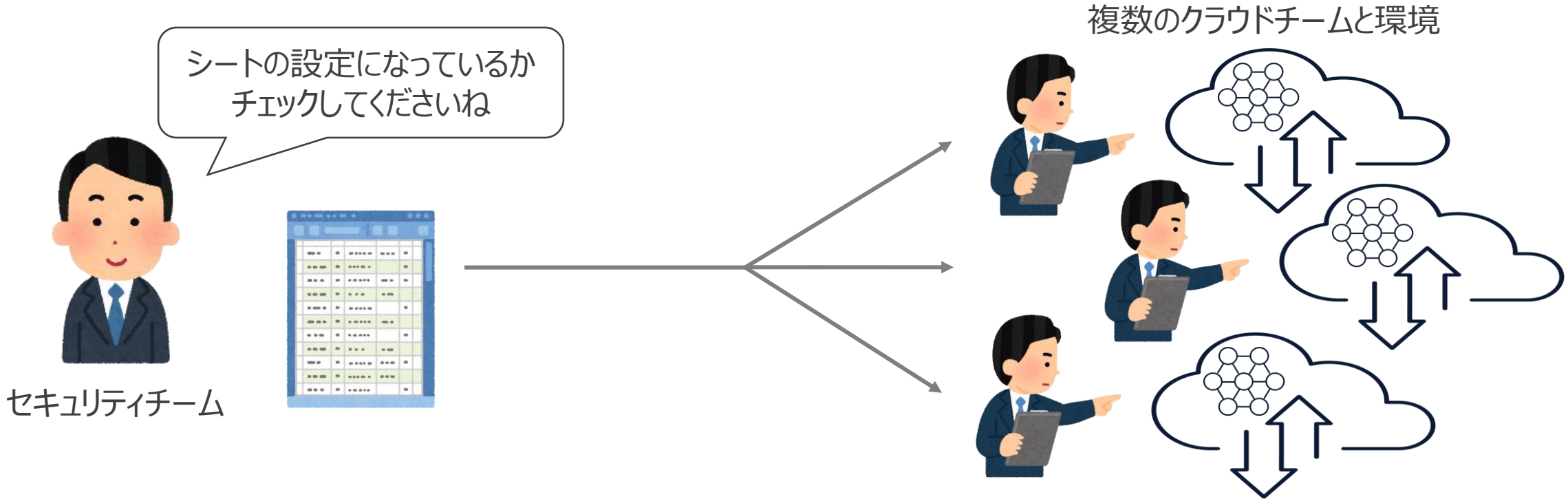
ベストプラクティス準拠の確認

セキュリティがクラウドによるイノベーションの足を引っ張る？

クラウドチームのチェック・回答

ベストプラクティス準拠の確認

現場の手作業チェックではスケールしない！



問題点

- ✓ チェックシートのメンテナンス
- ✓ チームごと異なるセキュリティ知識
- ✓ クラウドチームの業務を停める作業

セキュリティがクラウドによるイノベーションの足を引っ張る？

クラウドチームのチェック・回答

ベストプラクティス準拠の確認

ベストプラクティスだけでは環境ごとの差異を吸収できない！

AWS Foundational Security Best Practices (FSBP)
Microsoft Cloud Security Benchmark (MCSB)
CIS AWS Foundations Benchmark
CIS Microsoft Azure Benchmarks
CIS Google Cloud Computing Platform Benchmarks
など

セキュリティサービス

自動チェック

チェックシート運用の課題を解決！

問題点

- ✓ 被害と影響を無視
- ✓ 膨大な数のアラート
- ✓ 構成以外のリスクは対象外

必要なのはクラウドのイノベーションを阻害しないセキュリティ！

多面的な情報を分析に活かせる

資源資産　危険　被害　影響　対策　状況　を分析できる

影響を基準とした優先度を付けられる

把握すべきチームだけが把握できる

上記がすべて**自動**で**継続的に**行われる

目指すべきクラウドセキュリティの姿を実現するソリューション

それが……

です

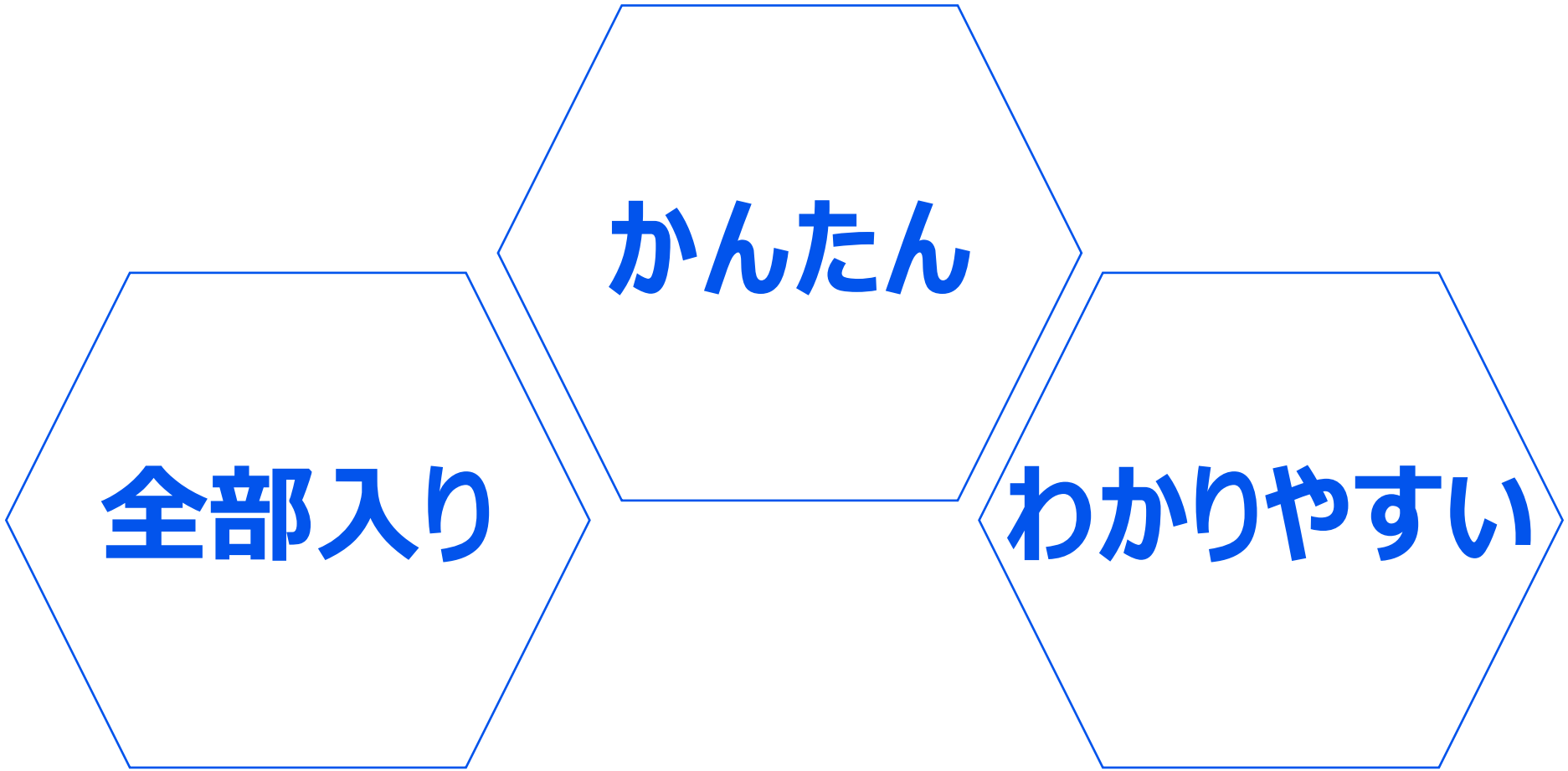
パブリッククラウド向けセキュリティソリューション

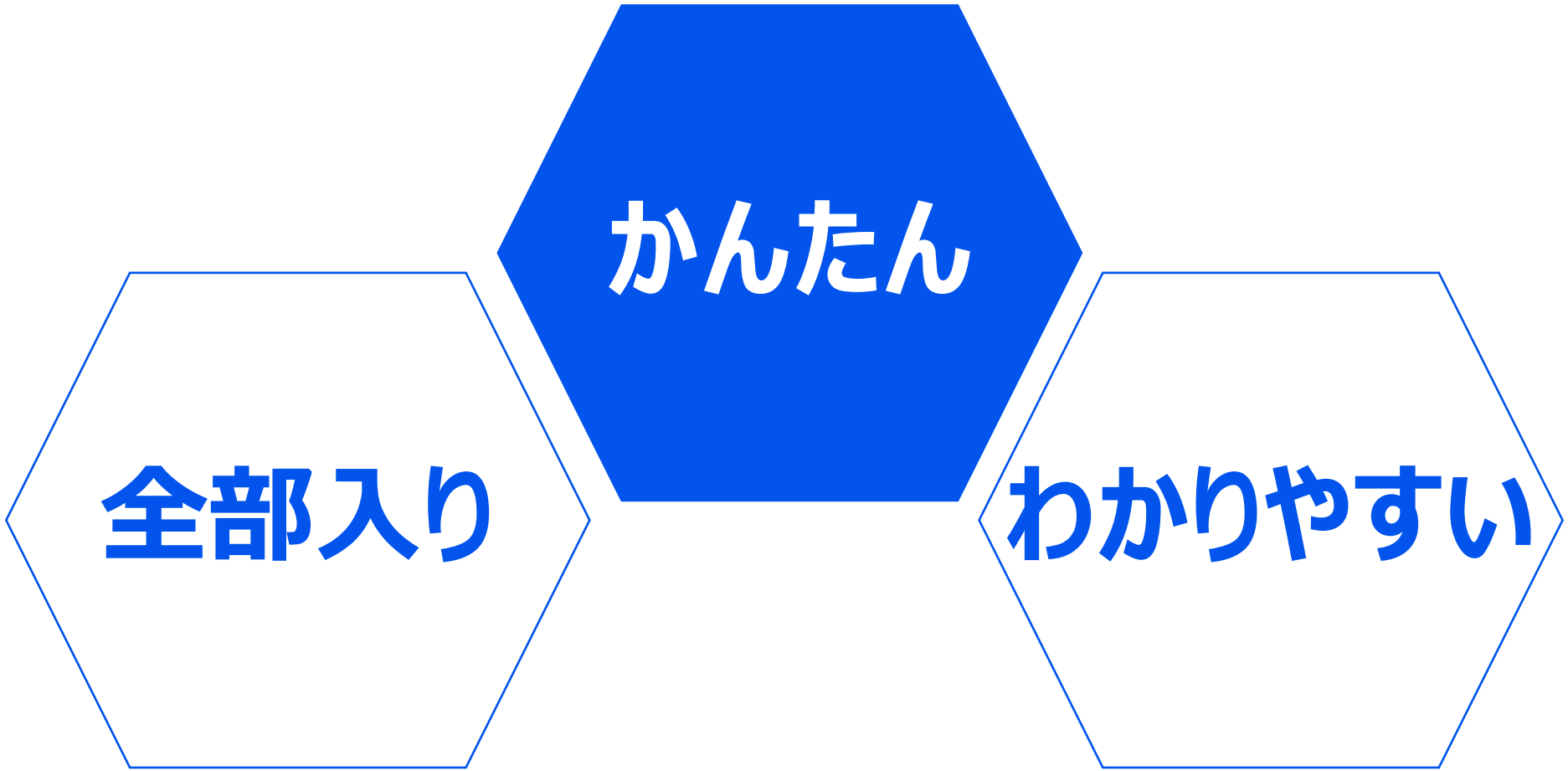
東京エレクトロン デバイス

東京エレクトロン デバイス

WIZ

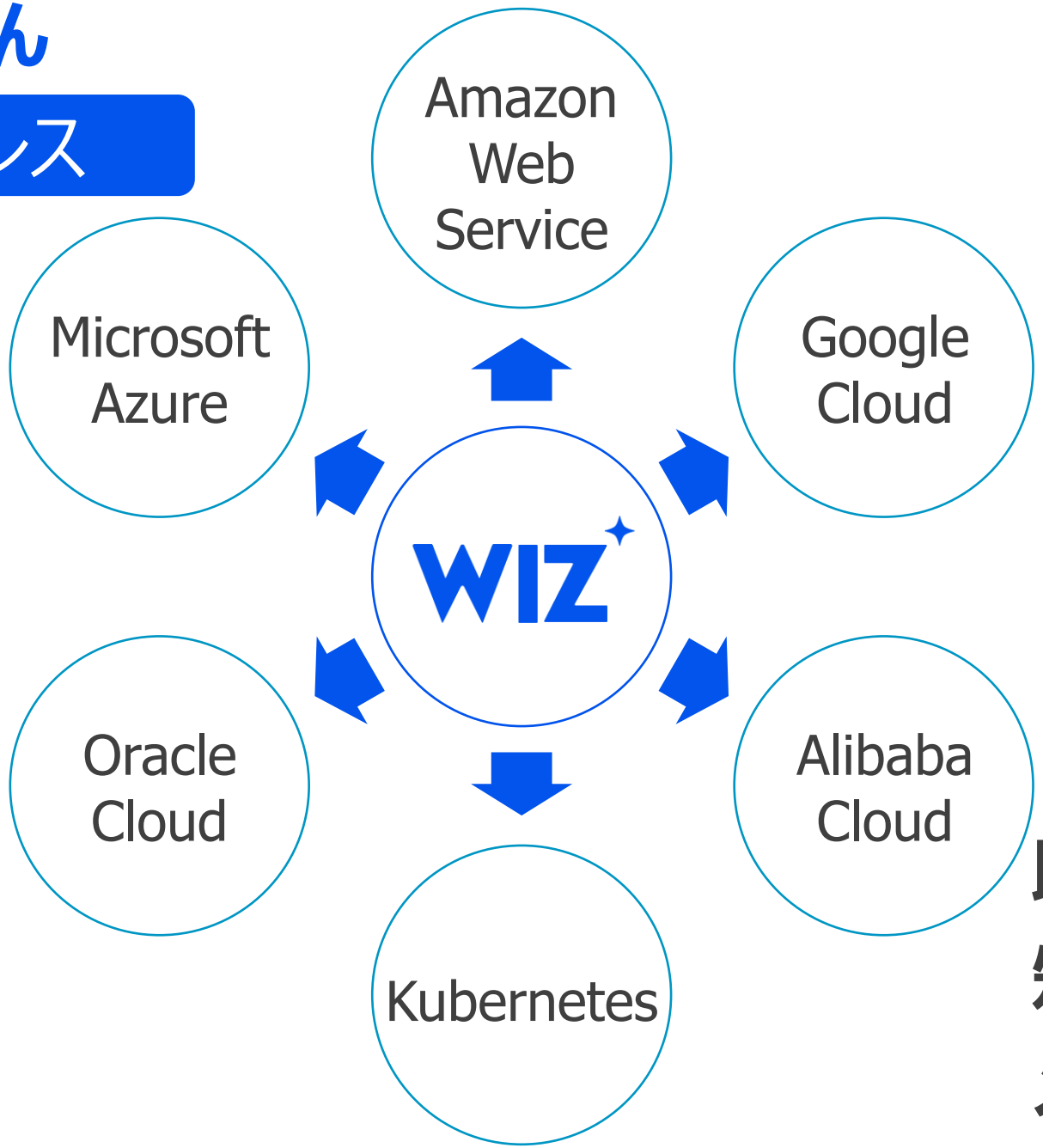
3つの特徴





特徴1: かんたん

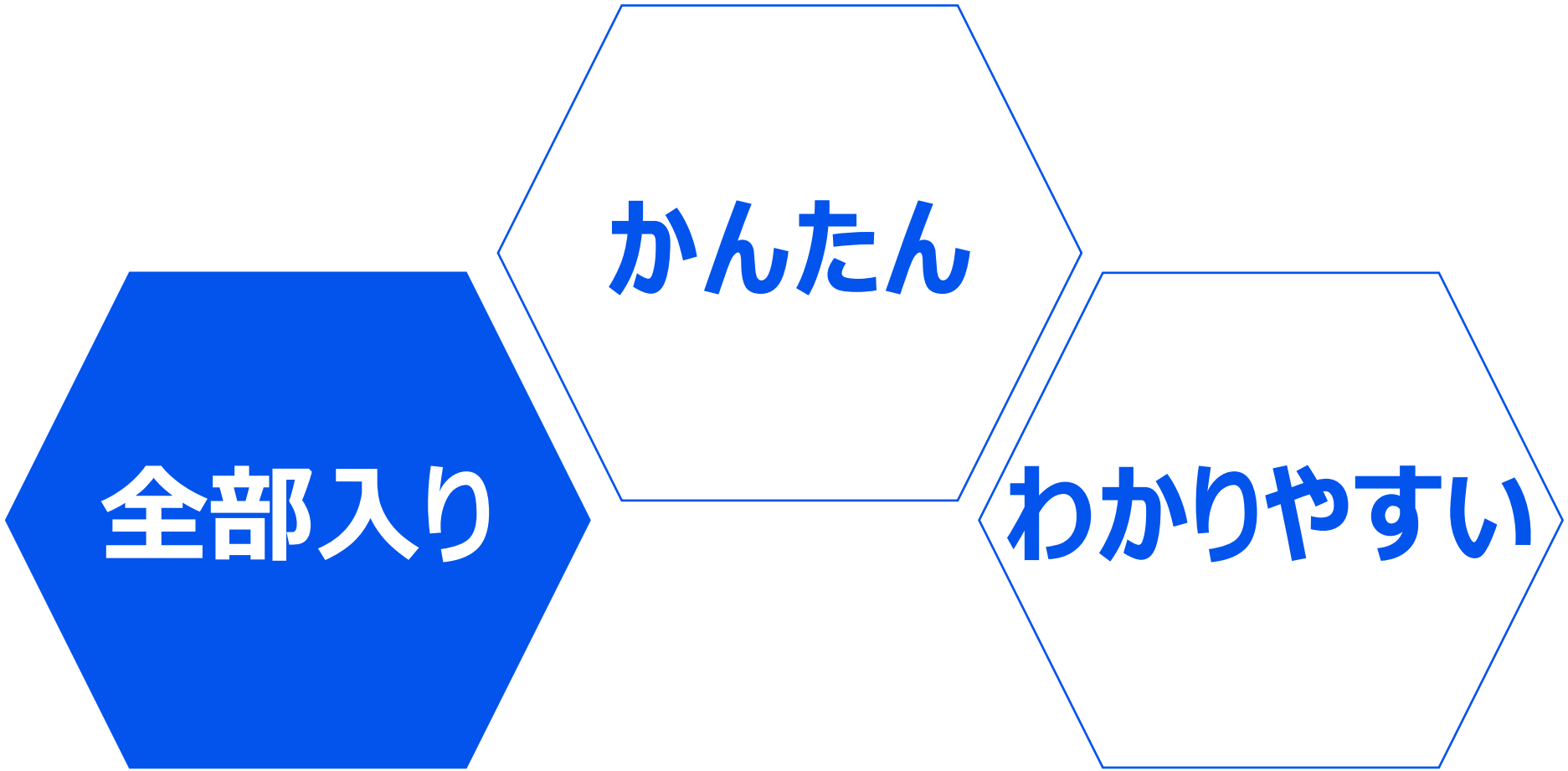
エージェントレス



既存環境に影響なし

短期導入

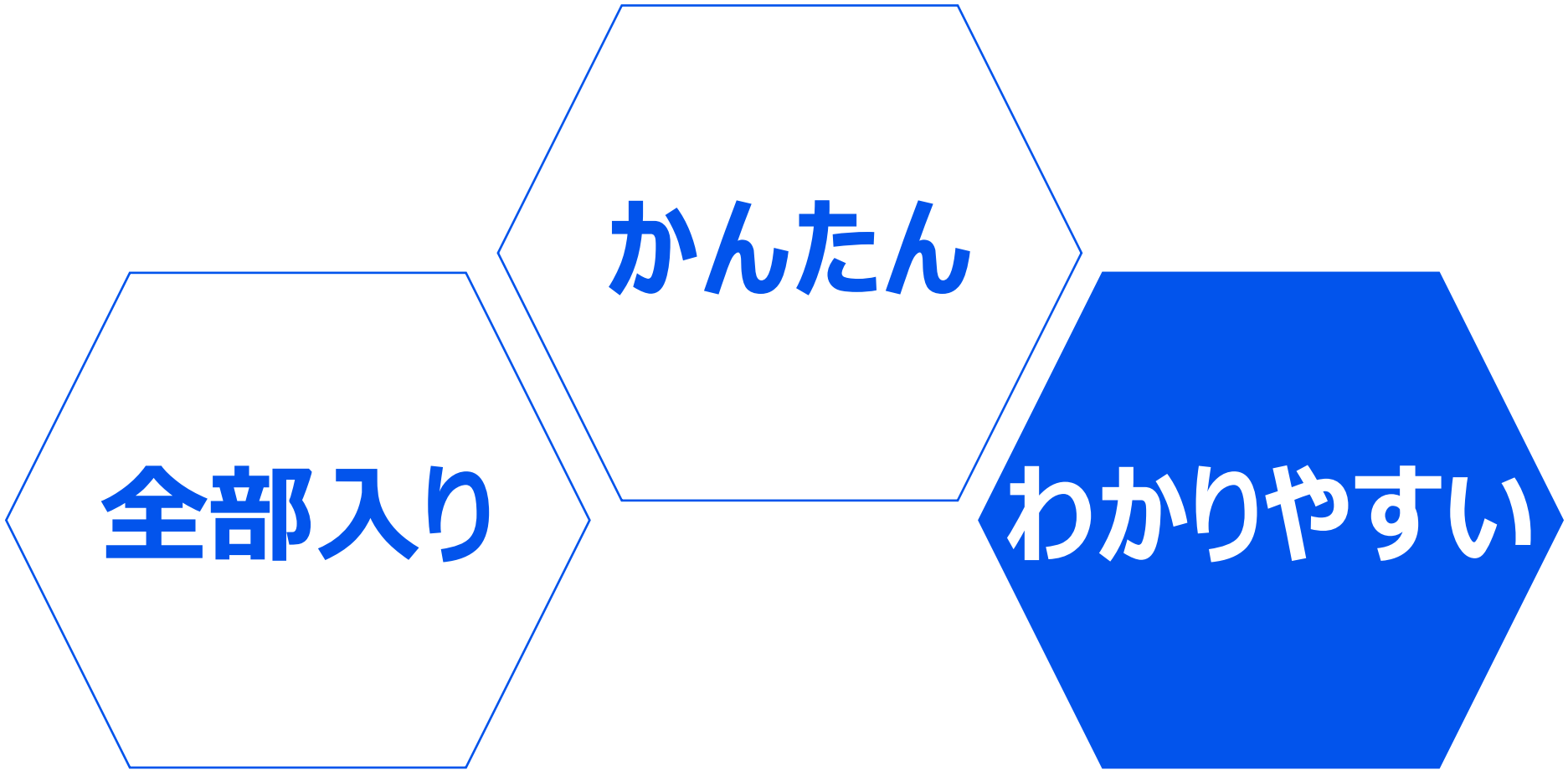
メンテナンス不要



特徴2: 全部入り

CNAPP - クラウドネイティブアプリケーション保護プラットフォーム

CSPM	CWPP
CIEM	サーバーレスセキュリティ
コンプライアンスレポーティング	クラウド構成管理
ネットワークアーキテクチャ	IaCスキャニング
コンテナセキュリティ	シークレットスキャニング
ホスト構成管理	脆弱性管理
DSPM - データセキュリティ	CDR



特徴3: わかりやすい

Connect Beyond

CSPM
- ミスコンフィグ診断・管理
  - SSH等TCPポートの開放
  - バケットへのアクセス設定
  - など

CWPP
- ワークロード保護
  - VM/コンテナ/サーバーレス
  - 脆弱性診断・管理
  - マルウェア診断
  - など

CIEM
- クラウドのID権限管理
  - IAMユーザーの運用
  - アクセス権限
  - など

データ保護
- クラウド上のデータ管理
  - シークレットの特定
  - データ特性と所在の把握
  - など

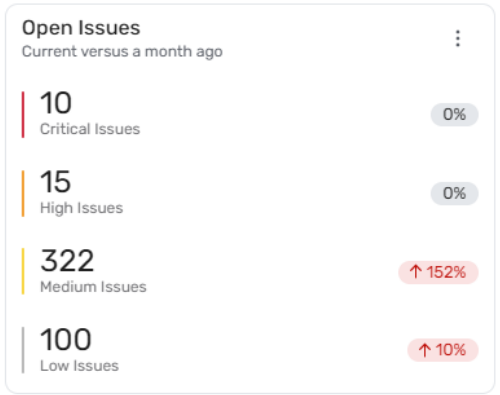
Wiz CNAPP

Wizのコンテキスト化

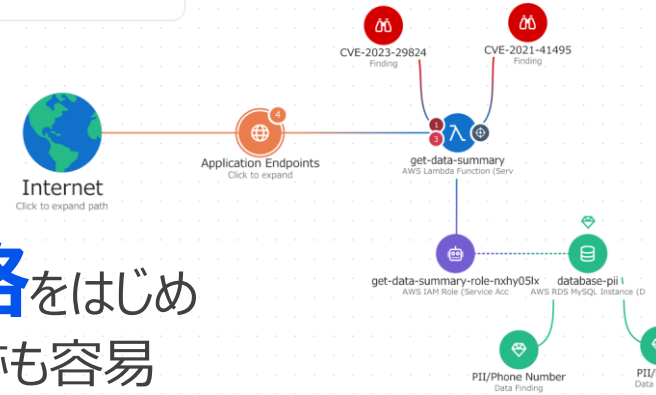
それぞれの分析結果を相関付けて

資源資産 / 危険 / 被害 / 影響 / 対策 / 状況

を分析



影響を元に
重要度を識別！



攻撃経路をはじめ
6事項の追跡も容易

東京エレクトロン デバイス

クラウド環境をセグメント化するWizプロジェクト

Connect Beyond

Wizプロジェクト

セキュリティチーム

全体の
統制・管理

WIZ

- AWSアカウント
- AWSアカウント
- AWSアカウント
- AWSアカウント
- Azureサブスクリプション
- Google Cloudプロジェクト

管理
通知

クラウドチームA

管理
通知

クラウドチームB

管理
通知

クラウドチームC管理者

閲覧のみ

クラウドチームCゲスト

CNAPPとして**多面的な分析**を提供

資源 資産 / 危険 / 被害 / 影響 / 対策 / 状況 を分析して情報提供

影響を基準として問題の重要度を提示

プロジェクトにより**管理領域の分割**、**個別通知**

上記すべて**自動**で**継続的**に実行

イノベーションを加速させるセキュリティを Wizで実現！

日本国内のお客様の声

○某テクノロジー系企業様
他社ソリューションでは埋もれていた**重要なセキュリティリスクを特定**
Wizの言うクリティカルは**本当にクリティカルな問題**

○某情報通信系企業様
他社ソリューション比で**カバー範囲とリスク検知性能が圧倒的**
重要度により**本当に重要な問題がひと目でわかる**ため、運用面で安心

○某エンターテインメント系企業様
エージェントレスで**既存環境への影響が無く導入できる**ことが重要
検知リスクの説明がわかりやすく**運用しやすい**

クラウドに構築し、実行する
すべてのものを守る

東京エレクトロン デバイス

Connect Beyond

共に創る 新たな価値を

東京エレクトロン デバイス