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横断的な可視化とセキュリティを実現！安全な運用のためのポイント

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

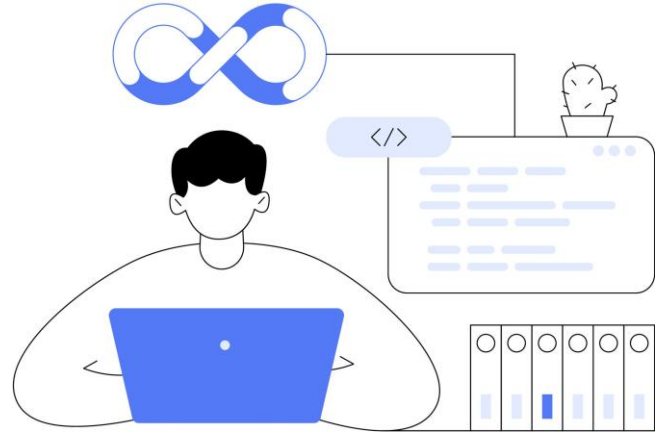
Connect Beyond

クラウドセキュリティ

東京エレクトロン デバイス

クラウドに集まる利用者の目線

アプリインフラ管理
情シス、SRE



アプリ開発者

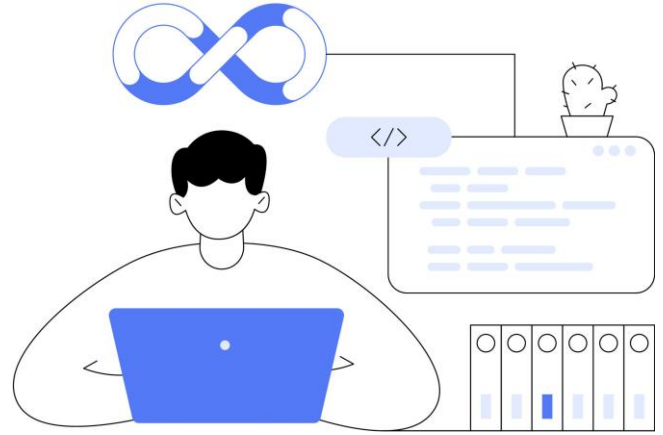
クラウドサービス
IaaS, PaaS, SaaS

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

アプリインフラ管理
情シス、SRE



アプリ開発者

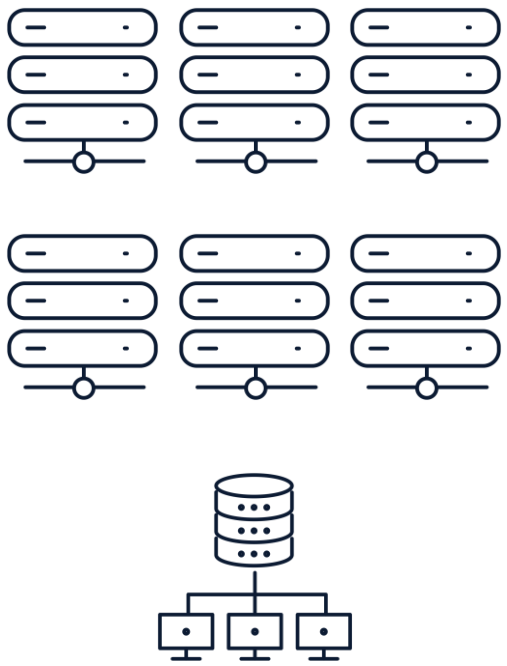
クラウドサービス
IaaS, PaaS, SaaS

アプリ利用
従業員、サプライチェーン

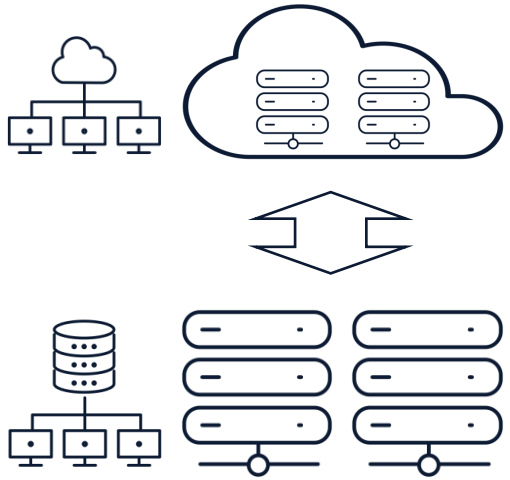
アプリ利用
一般消費者

クラウドの利用状況は様々

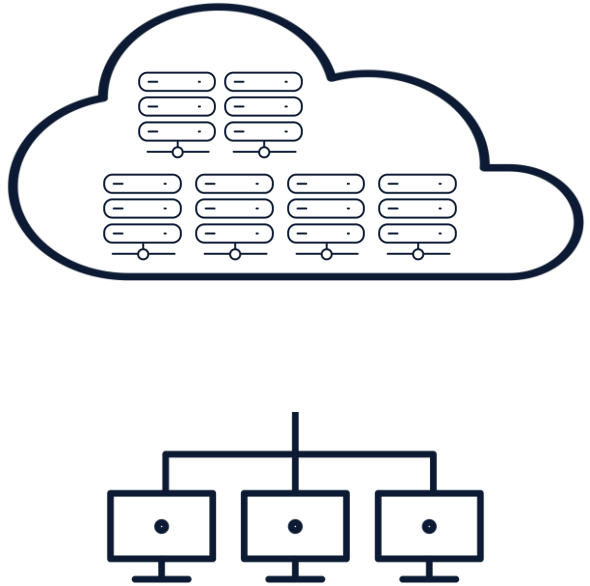
オンプレミス



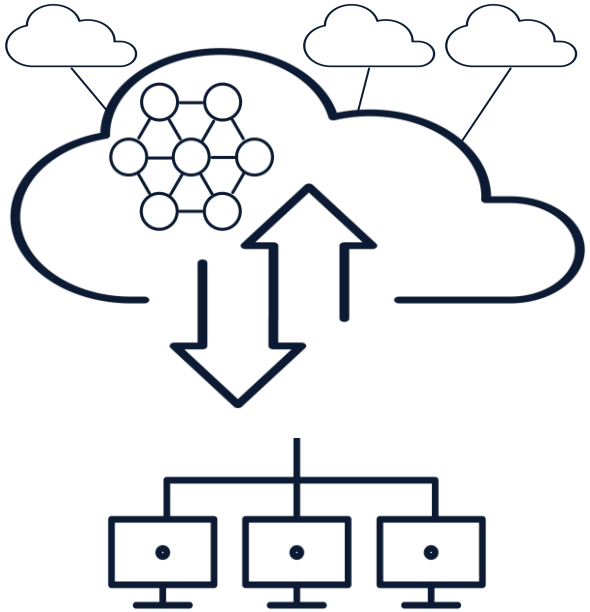
クラウドリフト



クラウドシフト



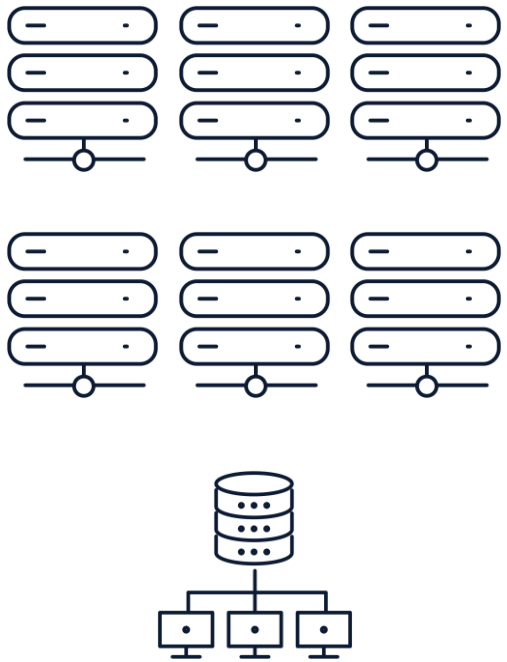
クラウドネイティブ



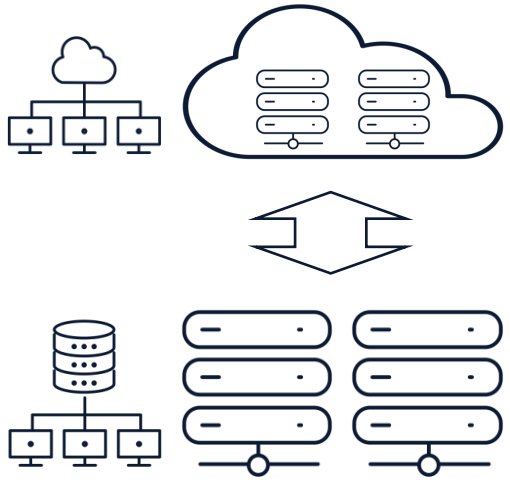
クラウドジャーニー

パブリッククラウドをご利用の方々向けです

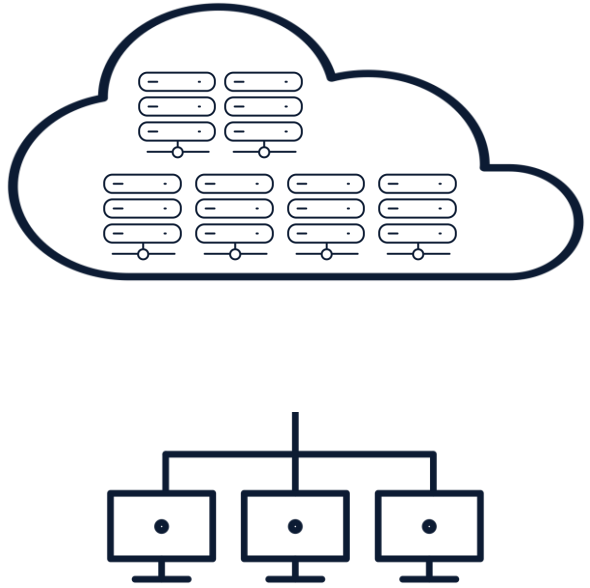
オンプレミス



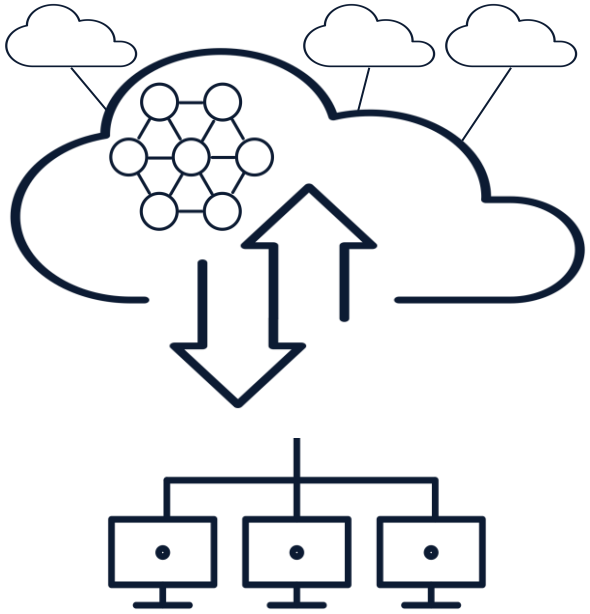
クラウドリフト



クラウドシフト



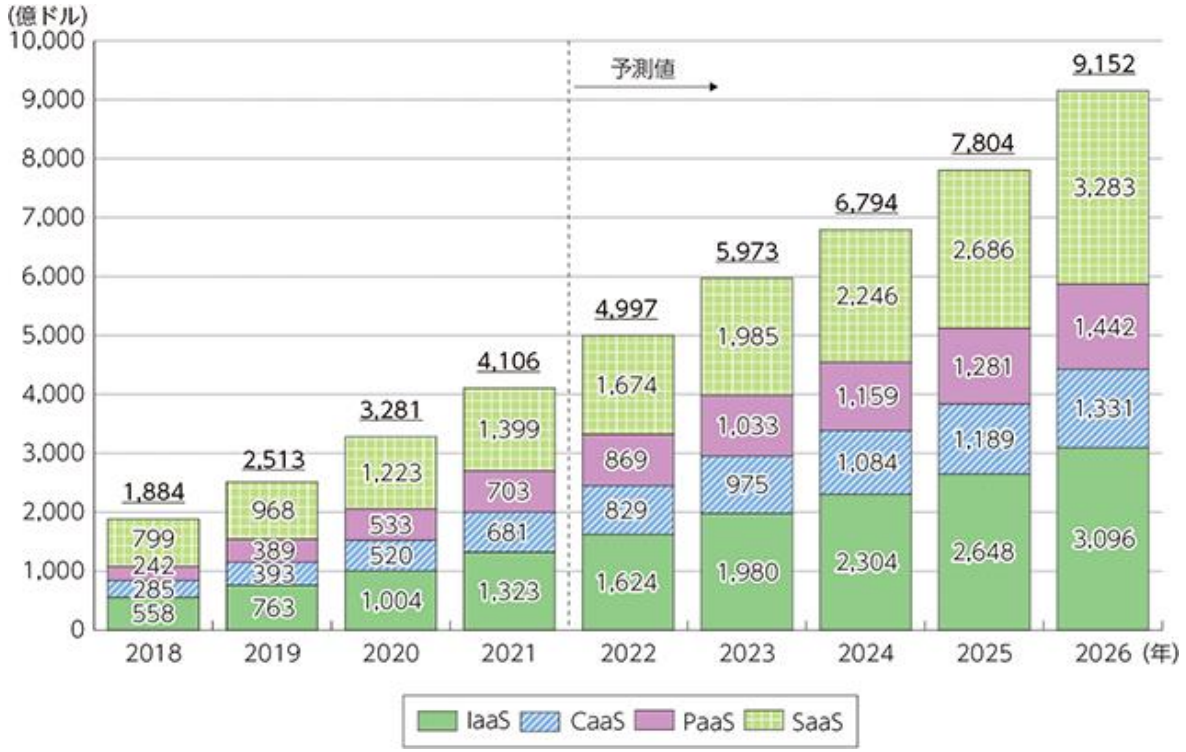
クラウドネイティブ



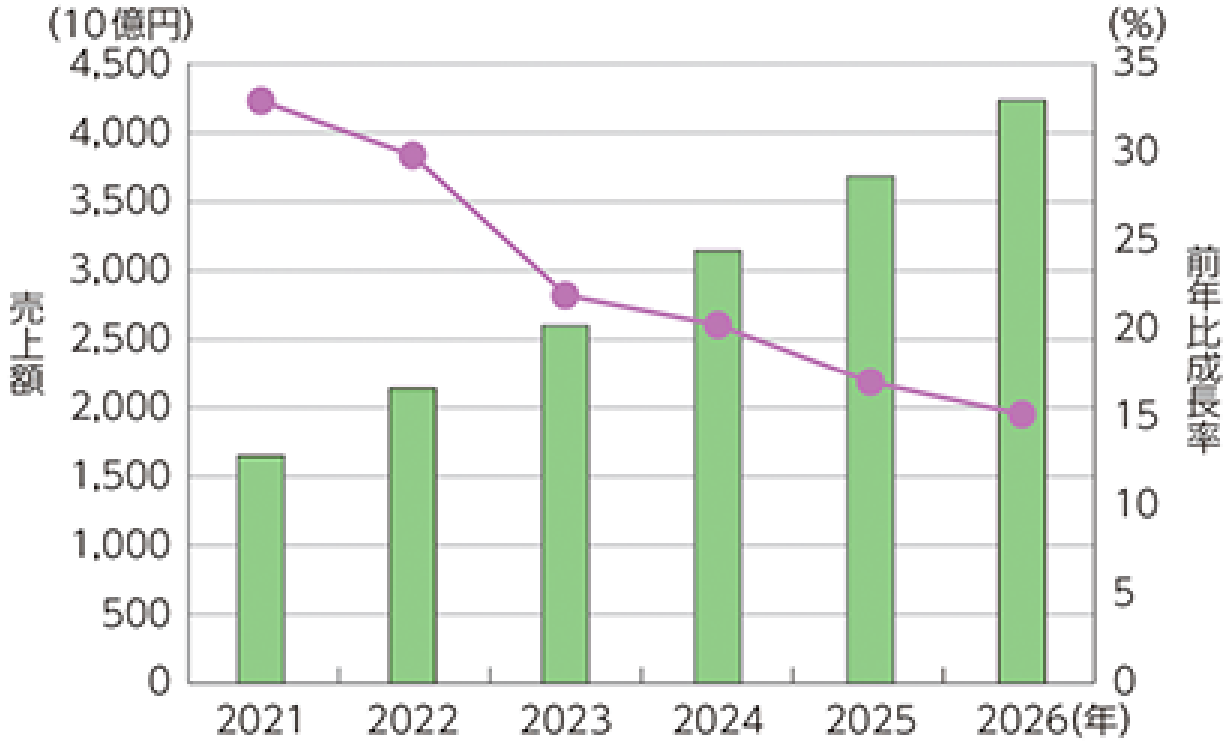
クラウドジャーニー

世界でも日本でも

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



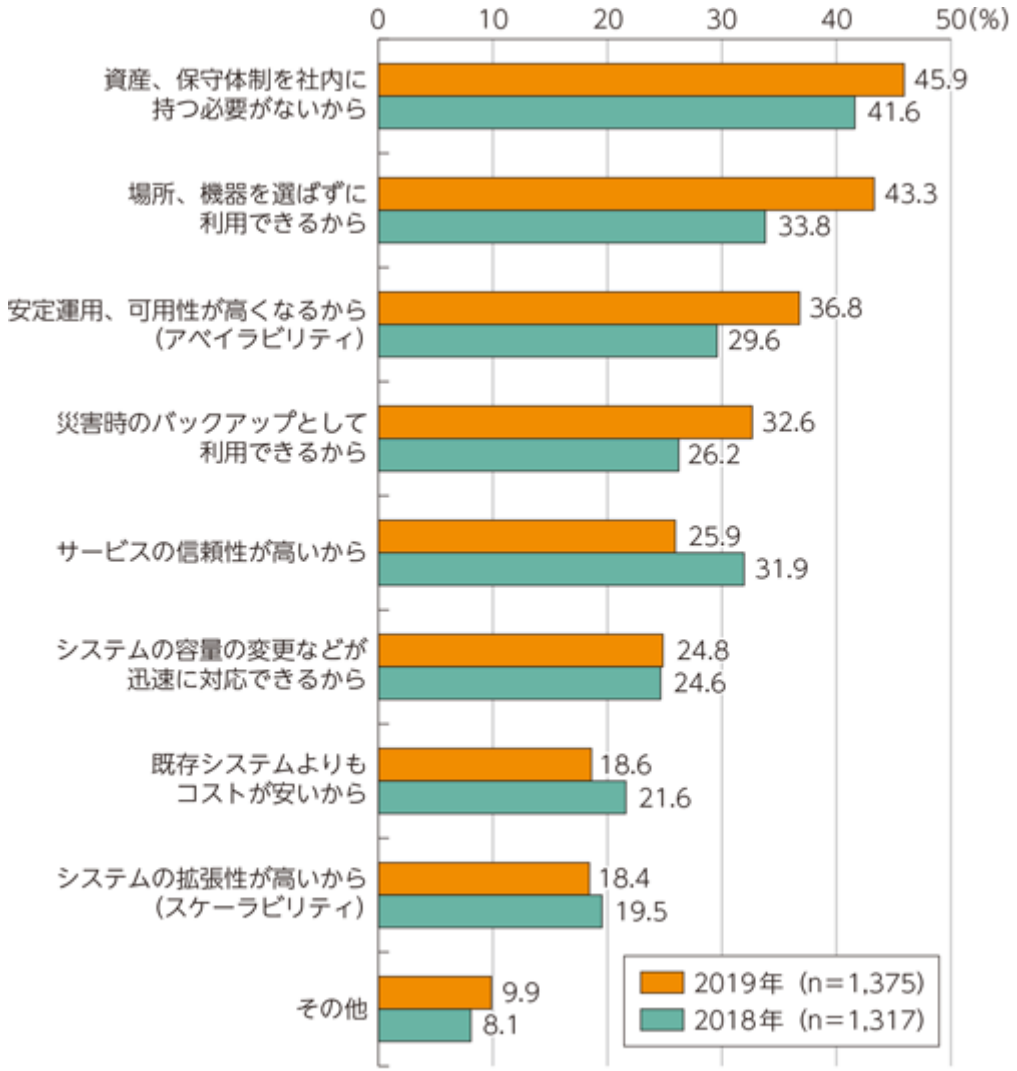
日本のパブリッククラウドサービス市場規模（売上高）の推移及び予測



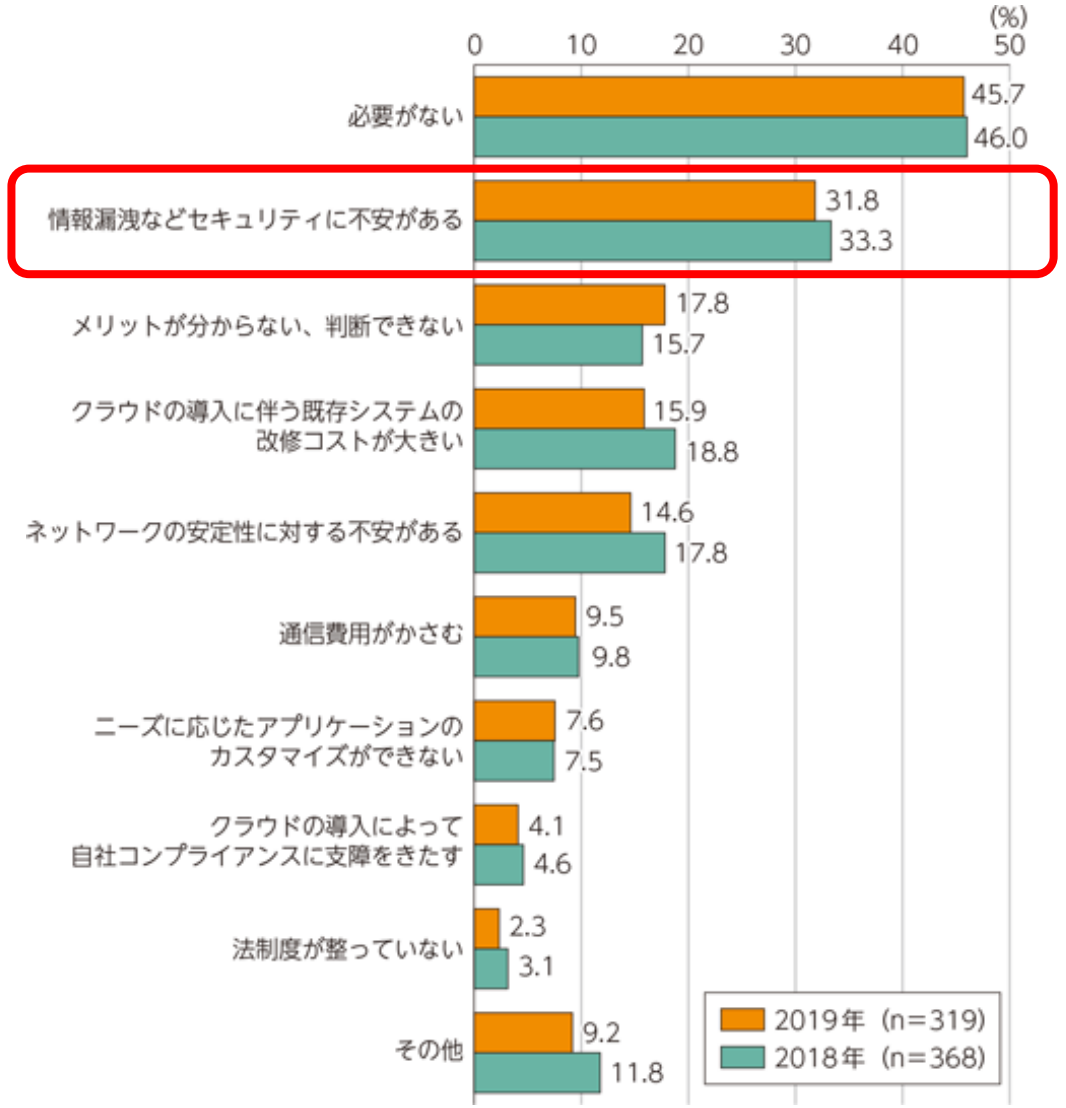
出典: 総務省 情報通信白書 令和5年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/nd248200.html

拡大するクラウドサービスの活用

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

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
- 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

クラウドの責任共有モデル

ユーザー管理
プロバイダー管理

オンプレミス	IaaS	PaaS	SaaS
データ	アプリケーション	アプリケーション	アプリケーション
アプリケーション	データ	データ	データ
ランタイム	ランタイム	ランタイム	ランタイム
ミドルウェア	ミドルウェア	ミドルウェア	ミドルウェア
OS	OS	OS	OS
仮想化	仮想化	仮想化	仮想化
サーバー	ストレージ	ストレージ	ストレージ
ストレージ	サーバー	サーバー	サーバー
ネットワーク	ネットワーク	ネットワーク	ネットワーク
データセンター	データセンター	データセンター	データセンター

クラウド利用に伴うセキュリティ上の課題

新しいサービスの利用に伴う
リスクが把握できず採用を躊躇

アタックサーフェスや侵入経路が
把握できておらず対策が打てない

利用者が自由勝手にリソースを
作るので全体像の把握が困難

日々登場する新しいリスクの
優先順位付けに苦慮

どこにリスクがあるか把握する
のが難しい

マルチアカウント横断の資産管理
やリスク分析ができていない

機密情報へのアクセス経路に
抜けがないか心配

マルチクラウド横断の資産管理や
リスク分析ができていない

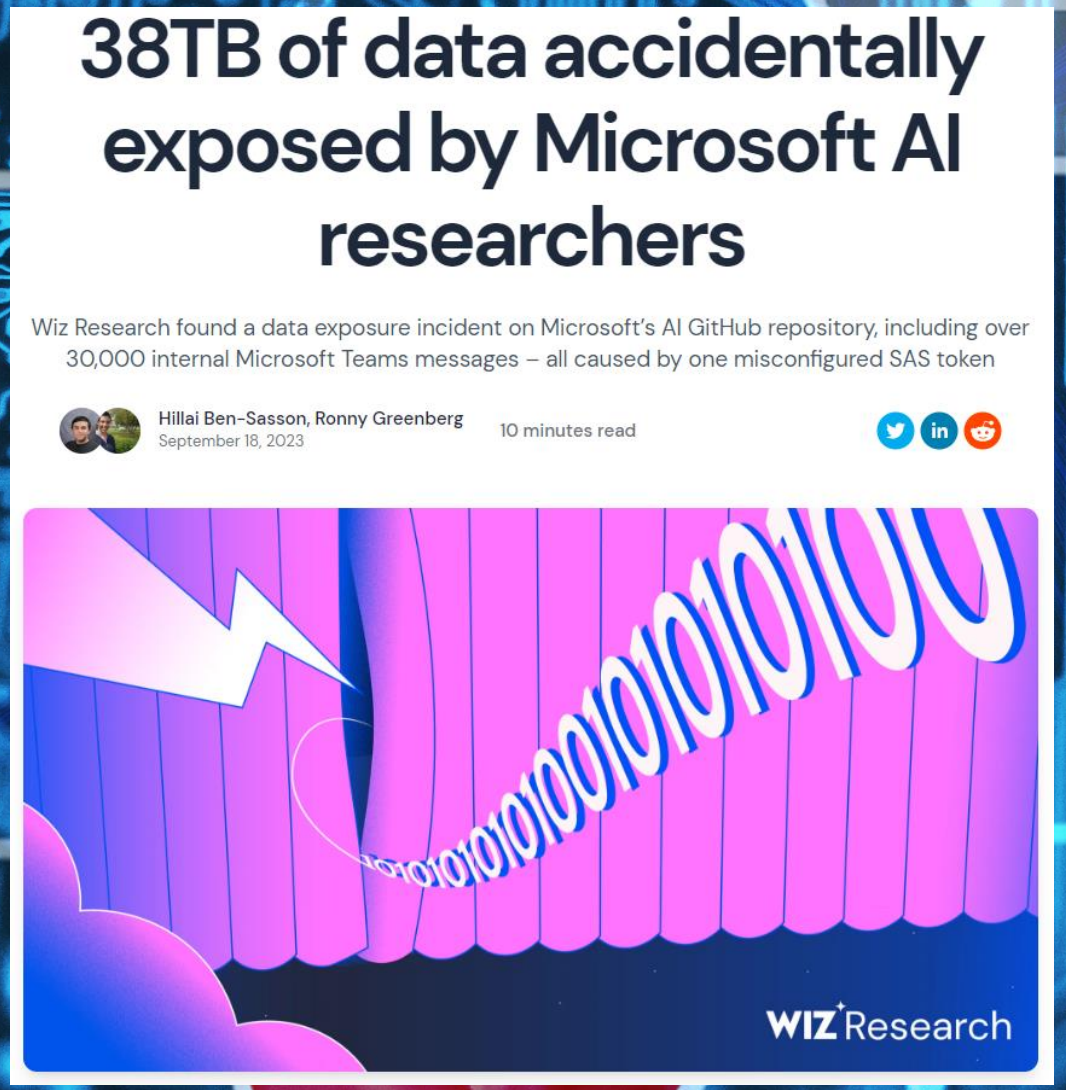
などなど……

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
- ✓ アクセスキーの漏洩
- ✓ 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

クラウドのリスクマネジメントで「把握」すべき6つの事項

Connect 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

- 機密データの流出
- 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

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！

マルチクラウド・マルチアカウント問わず、すべてのリソースや資産の管理ができる

クラウド特有のリスクを把握し、すべての環境で最新のリスクに対する分析ができる

クラウドの利用状況に関わらず、自動で資産管理とリスク分析が実現される

把握すべきチームだけがリスクを理解し、迅速に修復に取り掛かれる

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……

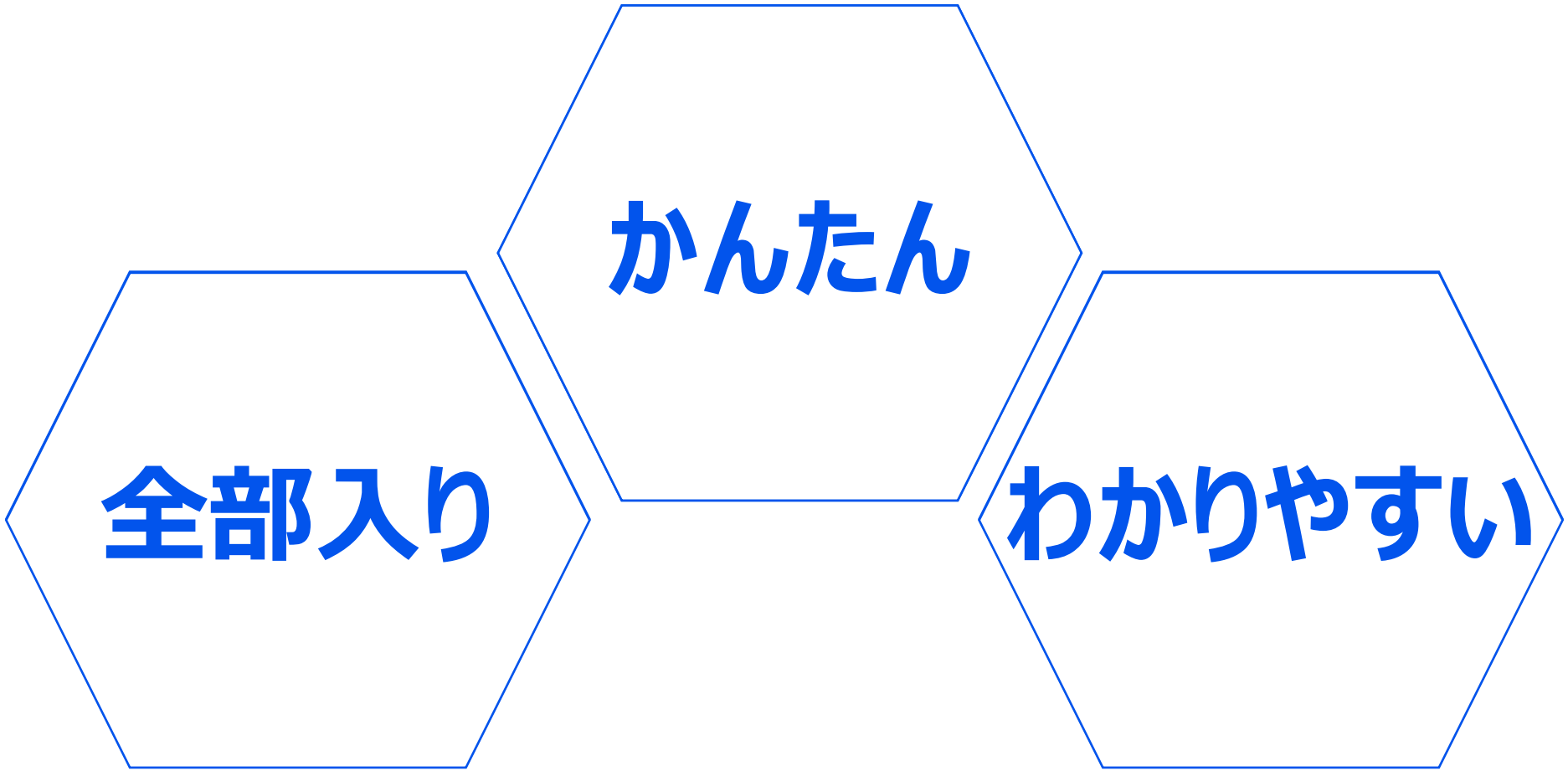
です

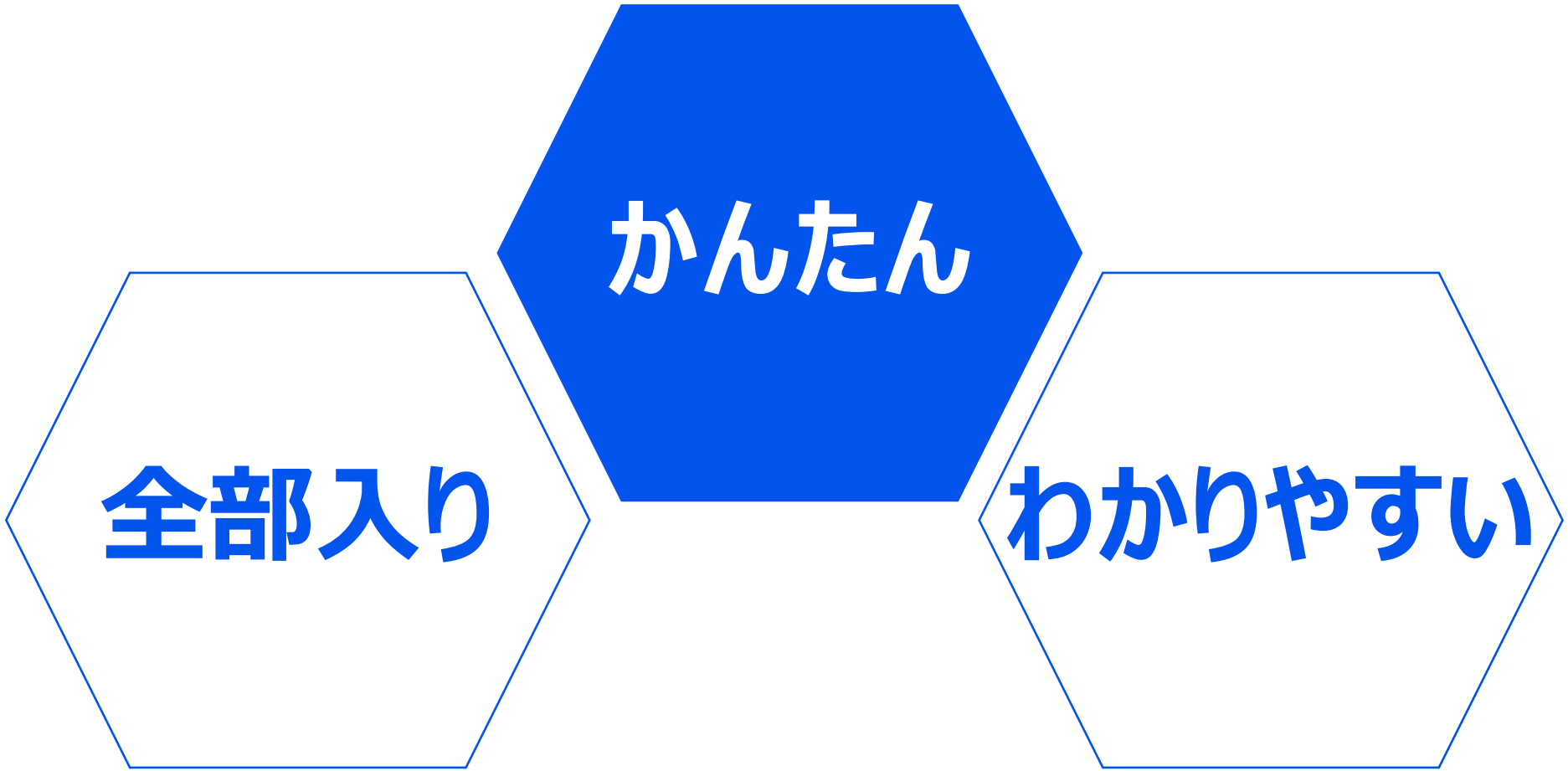
パブリッククラウド向けセキュリティソリューション

東京エレクトロン デバイス

WIZ

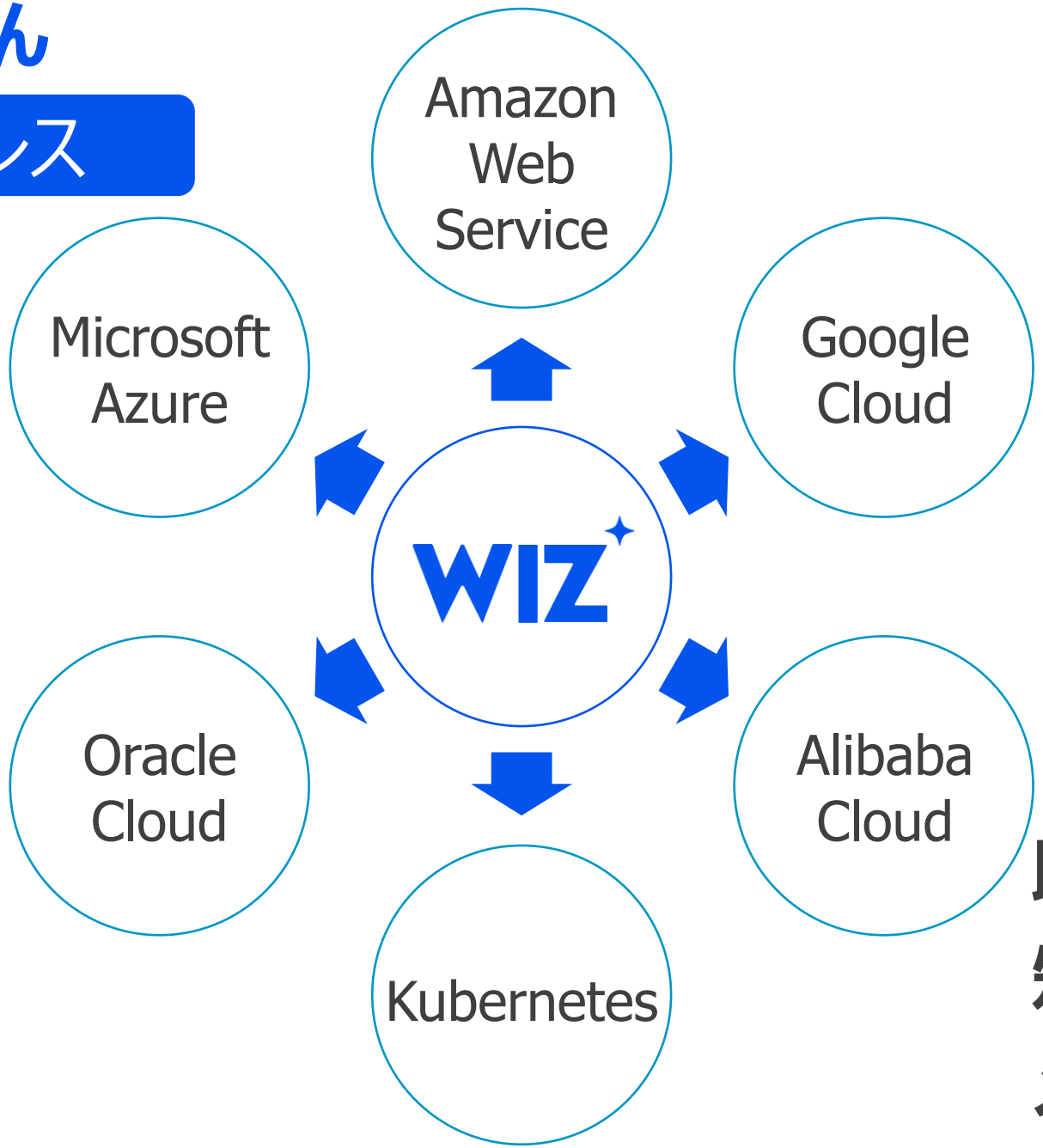
3つの特徴





特徴1: かんたん

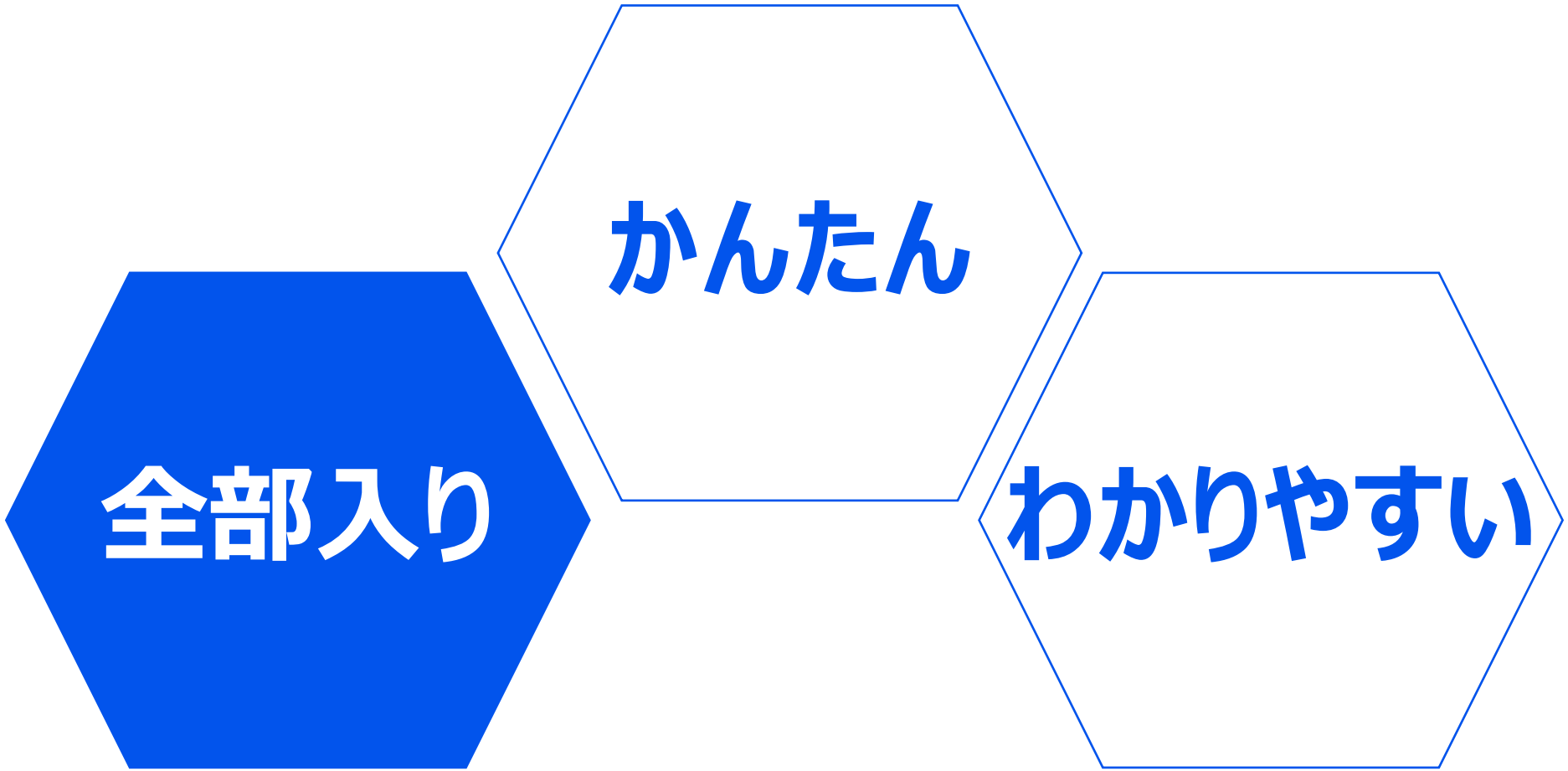
エージェントレス



既存環境に影響なし

短期導入

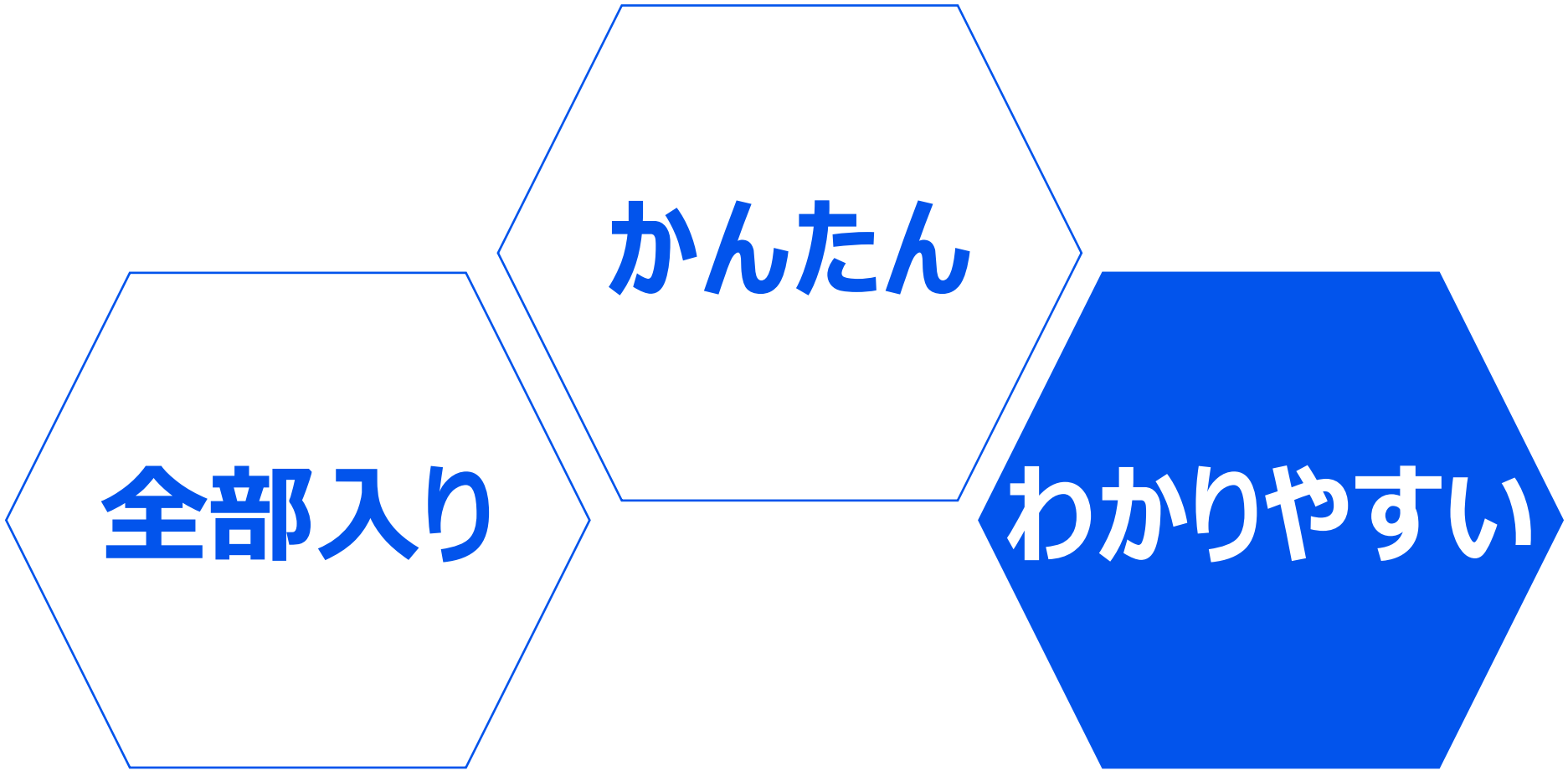
メンテナンス不要



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

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
  - 機密データの特定
  - など

CNAPP

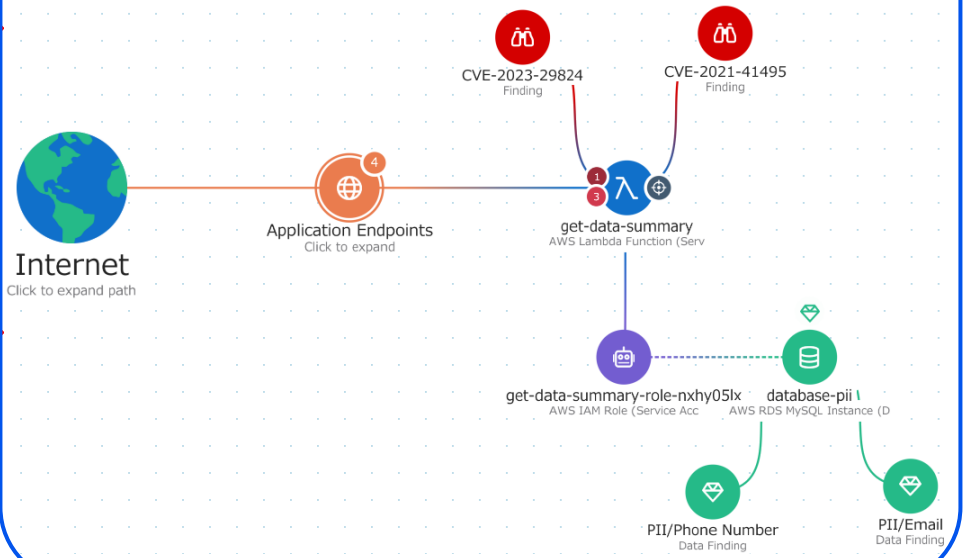
アラート
アラート
アラート
アラート
アラート
アラート

Wizのコンテキスト化

自動でアラートを相関付け、トリアージ

攻撃経路
重大度
修復方法

がひと目でわかる



東京エレクトロン デバイス

急成長するWiz

設立**18**ヵ月で売上(ARR) **$100M**(¥145億)到達

設立**3**年で評価額**$10B**(¥1.45兆)超の**デカコーン**

Fortune 100の**40%**が採用

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**。
複数チーム体制に対応できる**柔軟な権限管理やリソース管理が魅力**。

○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