

# コンテナセキュリティって必要なの？ ～コンテナセキュリティベストプラクティスご紹介～

ソフトバンク コマース&サービス株式会社

ICT事業本部 MD本部

テクニカルマーケティングセンター ビジネス開発課

竹石 渡, CISSP

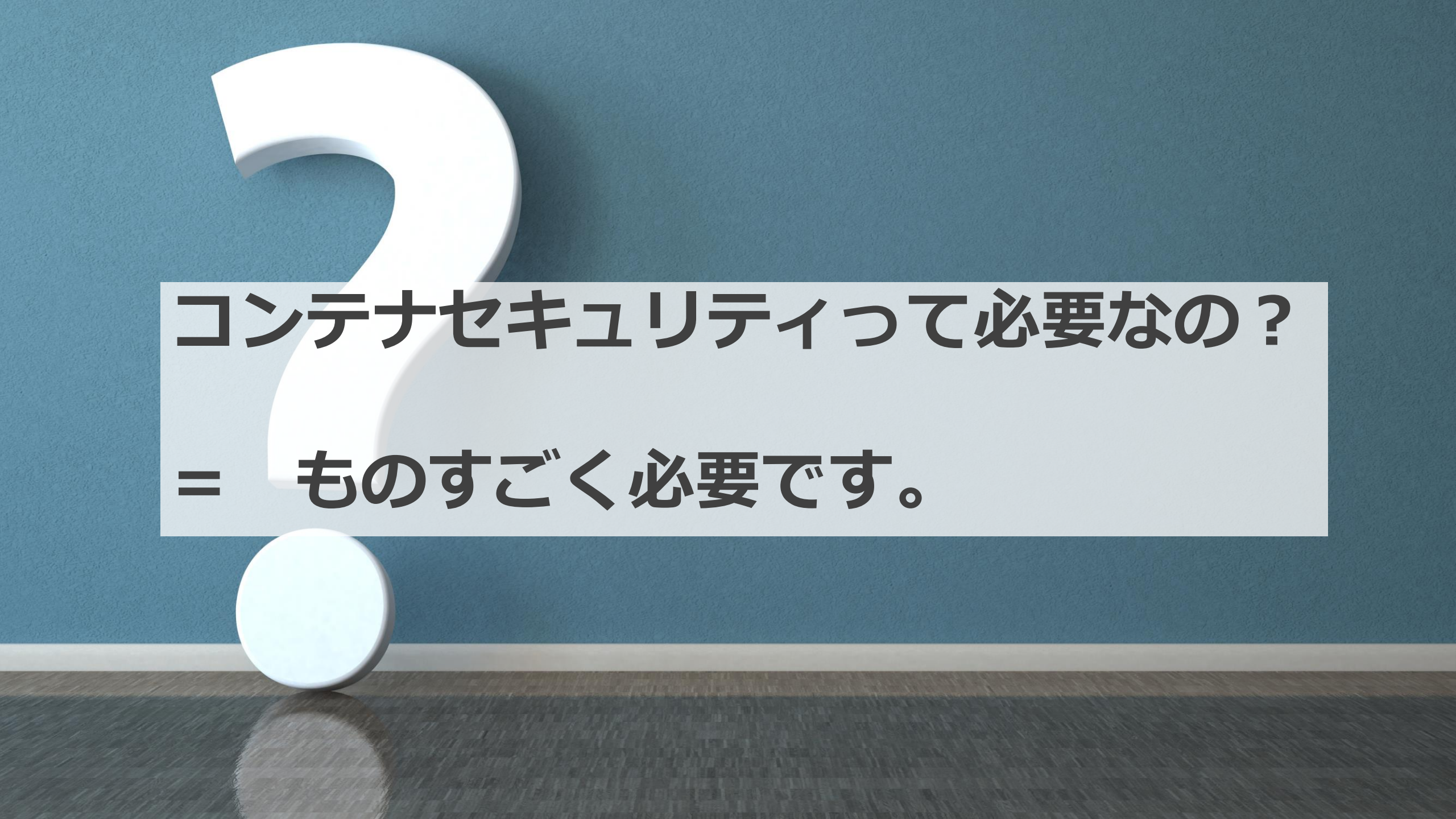


# ソフトバンク コマース&サービス

セキュリティ製品のプリセールス  
→ビジネス開発



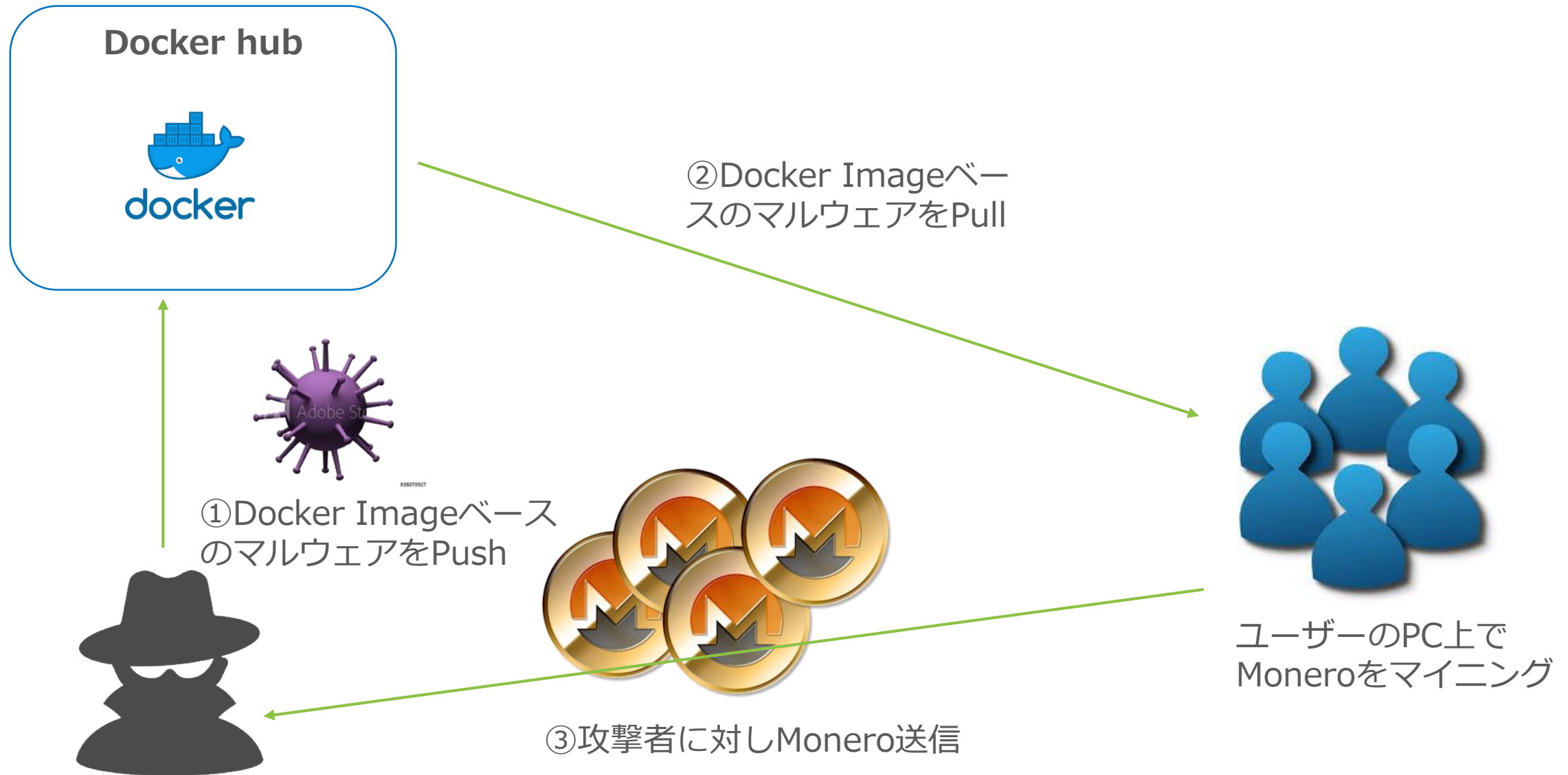
竹石 渡



コンテナセキュリティって必要なの？

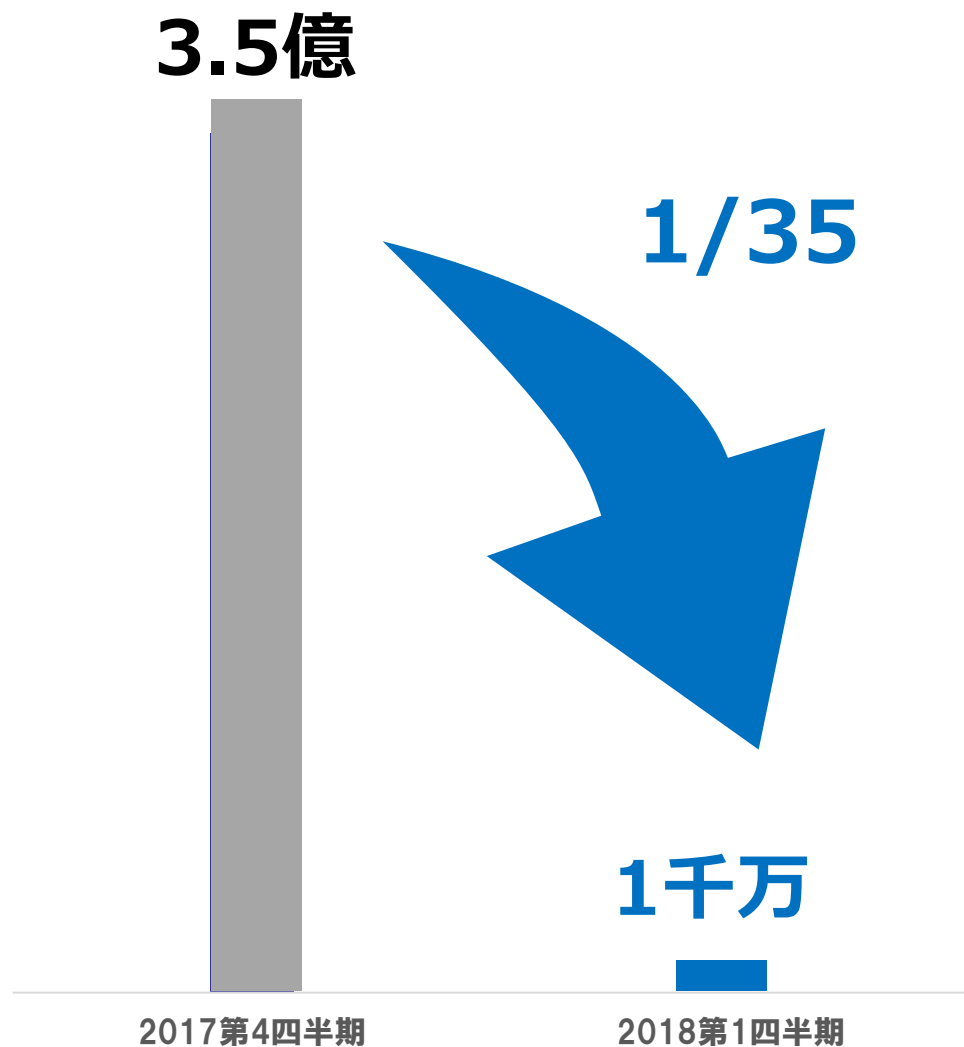
= ものすごく必要です。

# 悪意を持った Docker Image

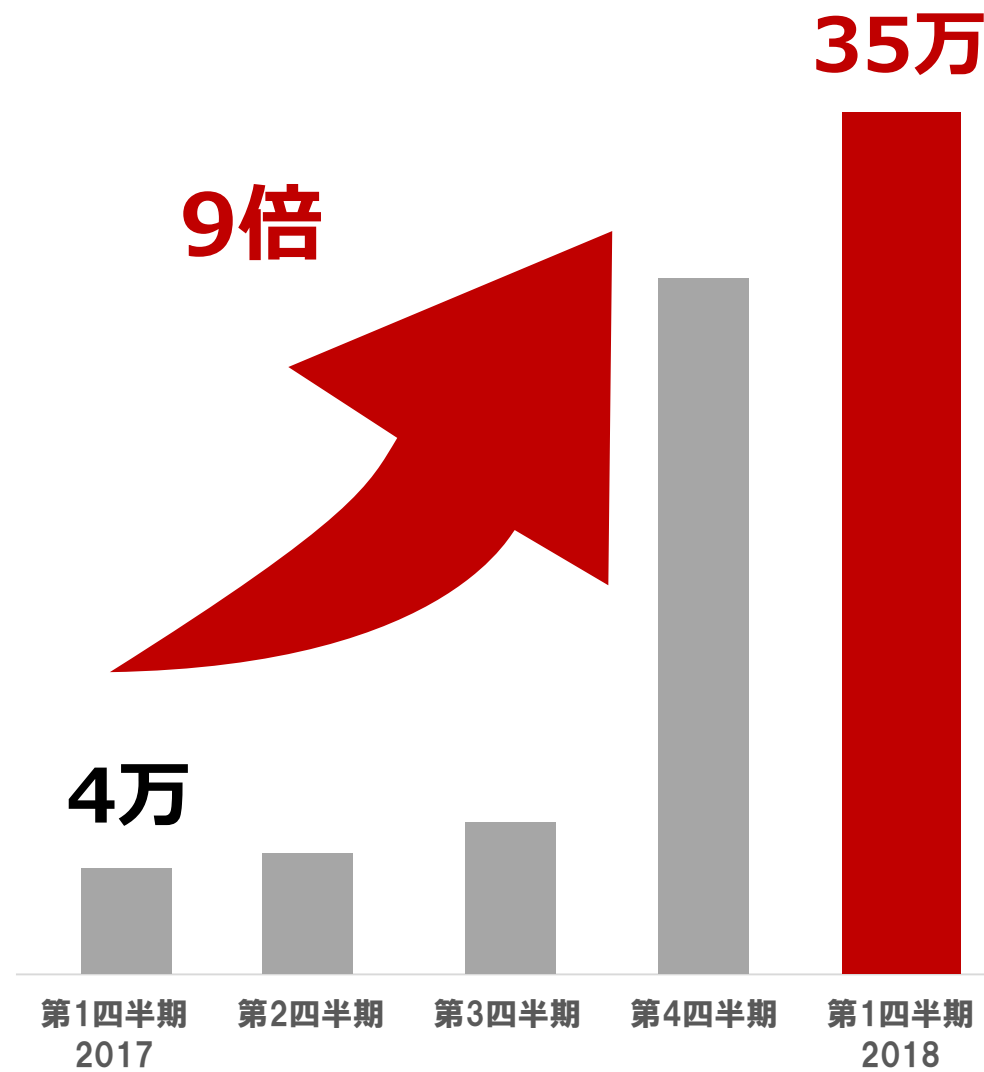


# 攻撃のトレンド

## ランサムウェア



## コインマイナー



# Build and Ship any Application Anywhere

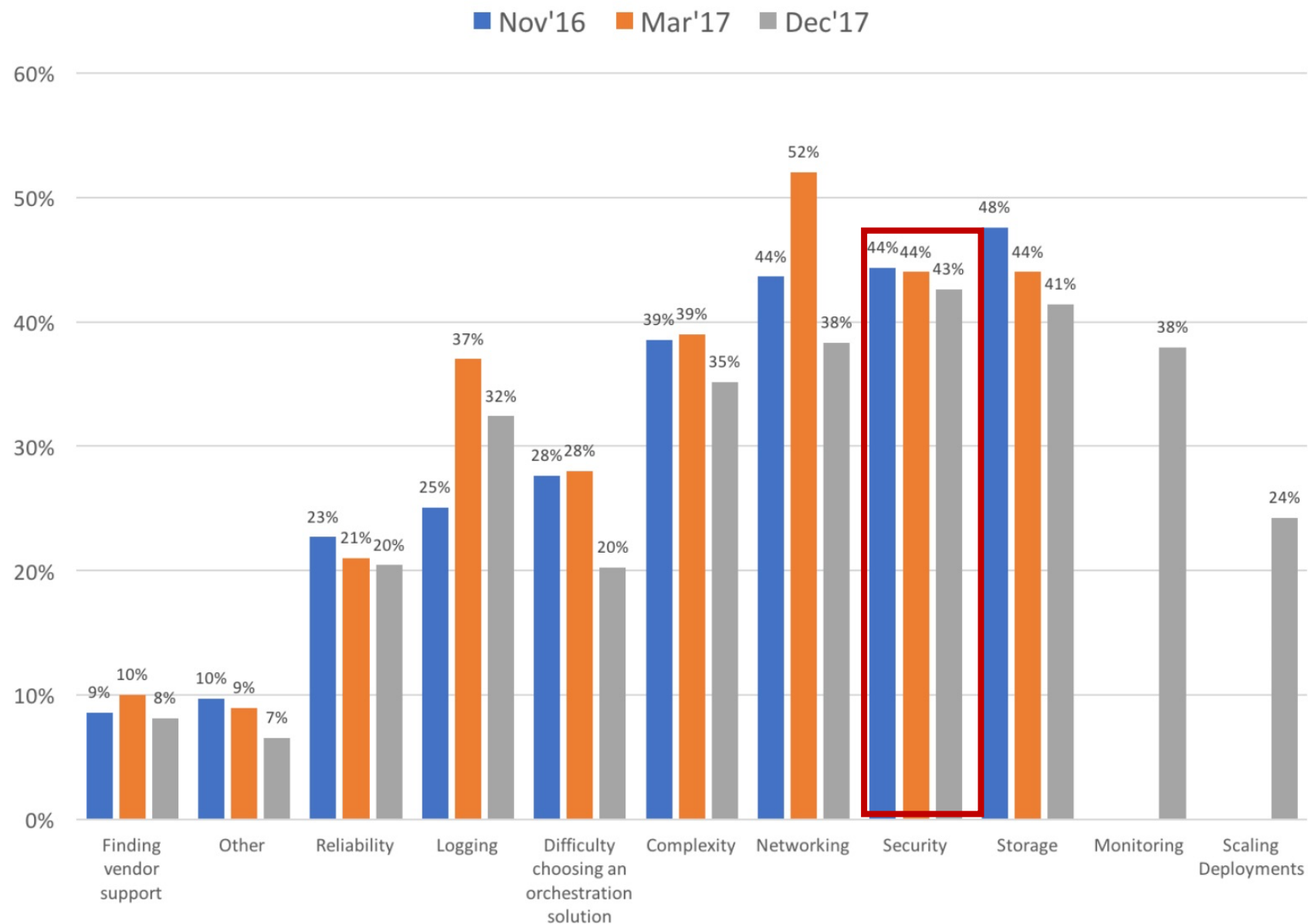
Docker Hub is the world's easiest way to create, manage,  
and deliver your teams' container applications.

[Sign up for Docker Hub](#)[Browse Popular Images](#)

# 24%

脆弱性のあるDocker hub上のイメージの割合

# コンテナの導入時に企業が直面している最大の課題



# コンテナセキュリティベストプラクティス

## **NIST SP800-190**

### **Application Container Security Guide**

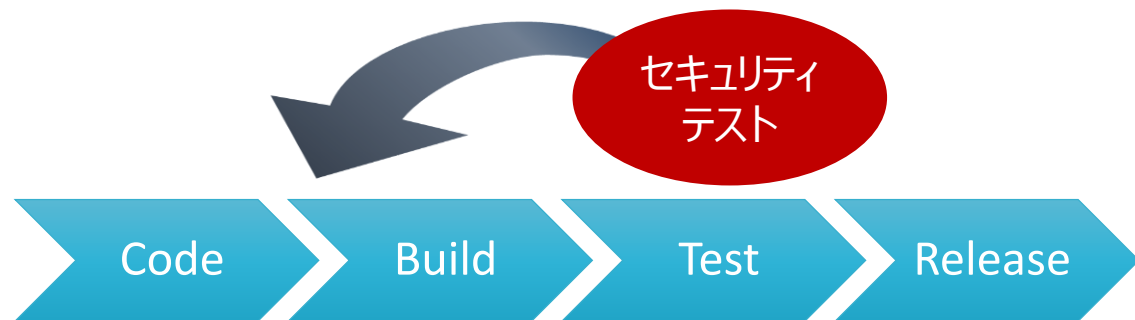
- Image countermeasures
- Redistry countermeasures
- Orchestrator countermeasures
- Container countermeasures
- Host OS countermeasures

# NIST SP-800 190詳細

| リスク      |                                                           | 主な対策                                 |
|----------|-----------------------------------------------------------|--------------------------------------|
| イメージ     | 脆弱性、マルウェア<br>アクセス制御など設定の不備<br>平文シークレット情報の保持<br>信頼されないイメージ | コンテナに特化したイメージのスキャン<br>信頼されたイメージのみを許可 |
| レジストリ    | 不正アクセス<br>古く脆弱性の残ったイメージ                                   | レジストリ通信は暗号化<br>古いイメージを削除、タグ付けし区別     |
| オーケストレータ | 無制限の特権アクセス<br>異なる機密度レベルのワークロードの混在                         | 必要性に応じた権限付与<br>機密度レベルに応じてグルーピング      |
| コンテナ     | ランタイムの脆弱性<br>無制限なネットワークアクセス<br>野良コンテナ<br>Appの脆弱性          | 脆弱性スキャン<br>Appの挙動のホワイトリスティング         |
| ホストOS    | カーネルを共有するリスク<br>OSコンポーネントの脆弱性                             | コンテナ特化のHost OSの利用<br>ホストOSセキュリティ     |

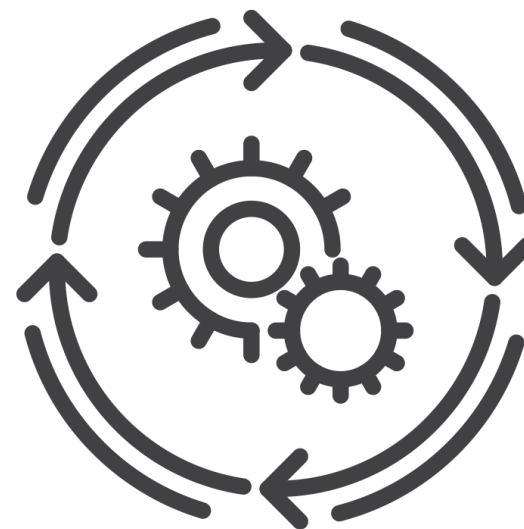
# アジリティとセキュリティの両立

## シフトレフト



開発初期段階でセキュリティテストを実施

## セキュリティテストの自動化



CIツールなどと連携

# コンテナセキュリティ製品を選ぶポイント

## ・ DevOpsツールチェーンとの連携

- コンテナの目的は開発ライフサイクル改善、セキュリティが足かせになってはいけない
- DevOpsツールと連携し**テストの自動化**と**シフトレフト**が重要

## ・ 様々なプラットフォームをサポート

- コンテナは可搬性が高い
- OS、オンプレ/クラウド問わずサポートしていることが重要

## ・ コンテナの特性に対応している

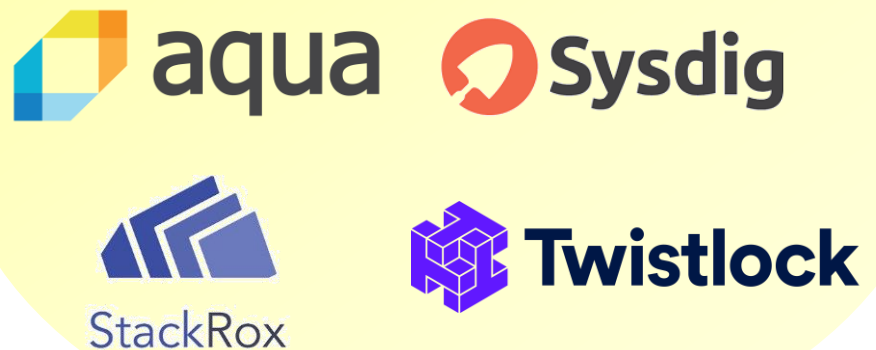
- ライフサイクルが早い、レイヤー構造などの特性がある
- レガシーなスキャナでは対応できない可能性あり

従来のネットワーク・ベースおよびホスト・ベースのセキュリティ・ソリューションは、コンテナを認識できない

-Gartner

# 商用コンテナセキュリティ製品プレイヤー

## 新興系コンテナ特化



## 脆弱性スキャン



## エンドポイントAV



# Aqua Security Softwareについて

- 事業：コンテナ向けセキュリティ製品を提供
- 設立：2015年
- 本社：イスラエル Ramat Gan
- 社員数：100名
- マネージメントチーム：



# aqua



Dror Davidoff  
Co-Founder and CEO  
元Mcafee



Amir Jerbi  
Co-Founder and CTO  
元CA Technologies



Michael Cherny  
Chief Architect  
元Imperva



Liz Rice  
Technology Evangelist

# Aqua Security Softwareについて

## 組織

出身企業は多岐に渡る



## 戦略的パートナーシップ



## 出資関係

Microsoft Ventures | Lightspeed | Shlomo Kramer | TLV Partners

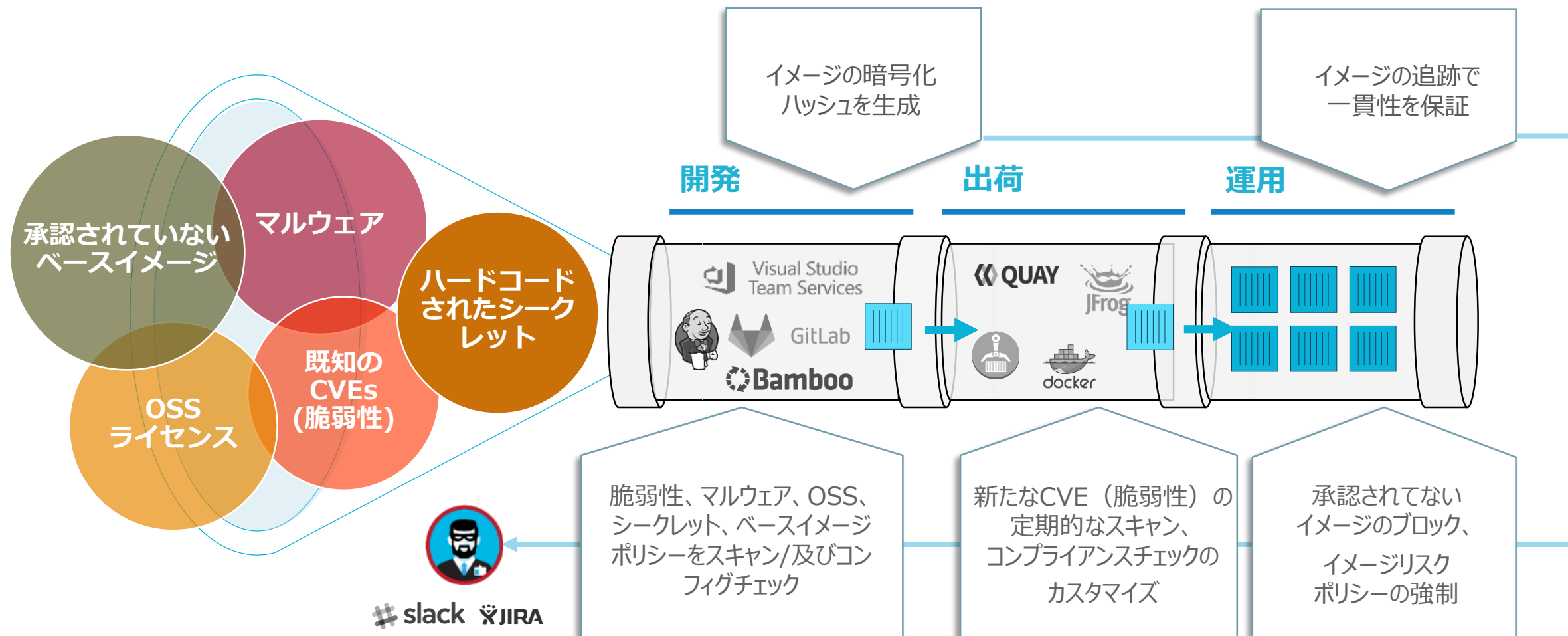
📍 Boston

📍 San Francisco

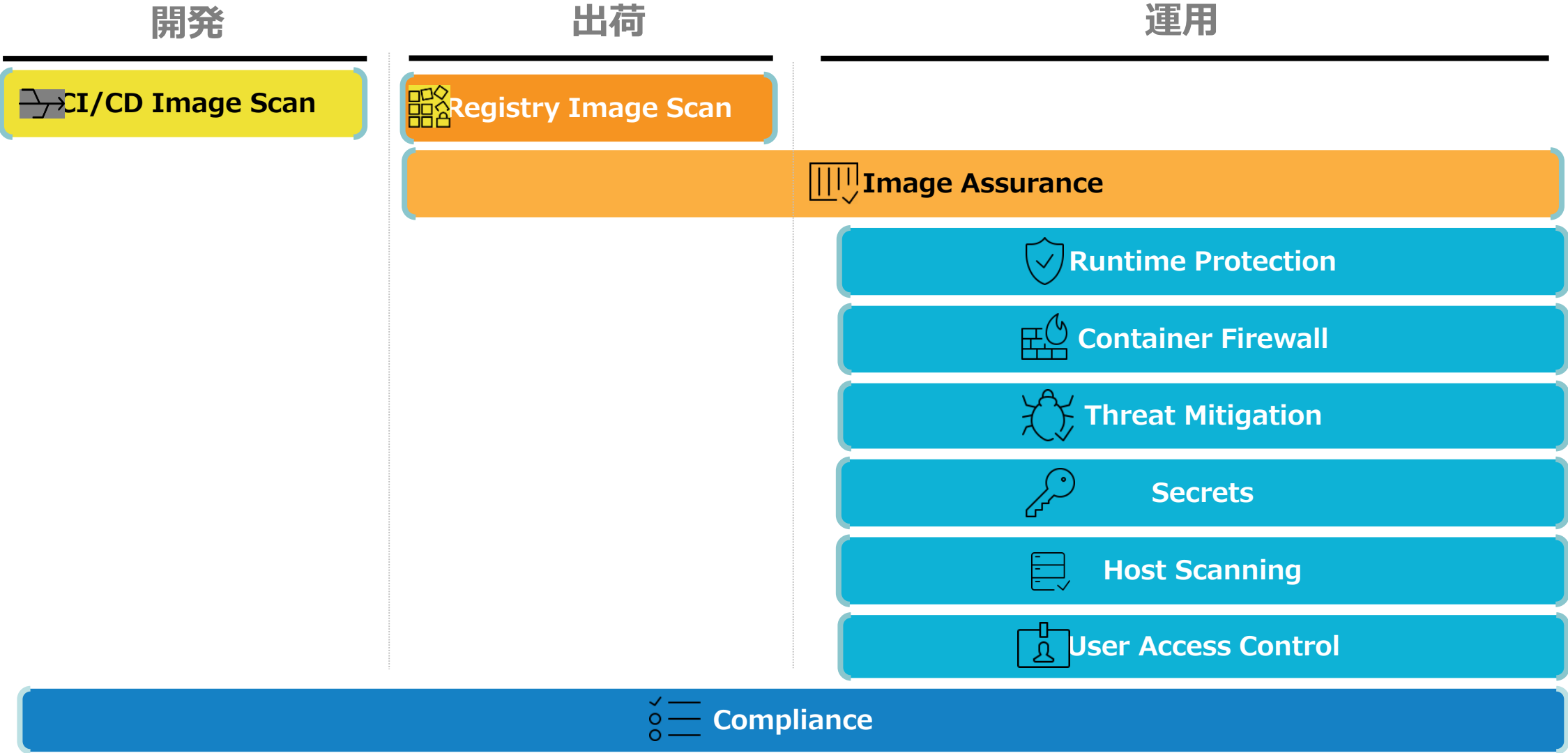
📍 Tel Aviv

# DevSecOpsの実現

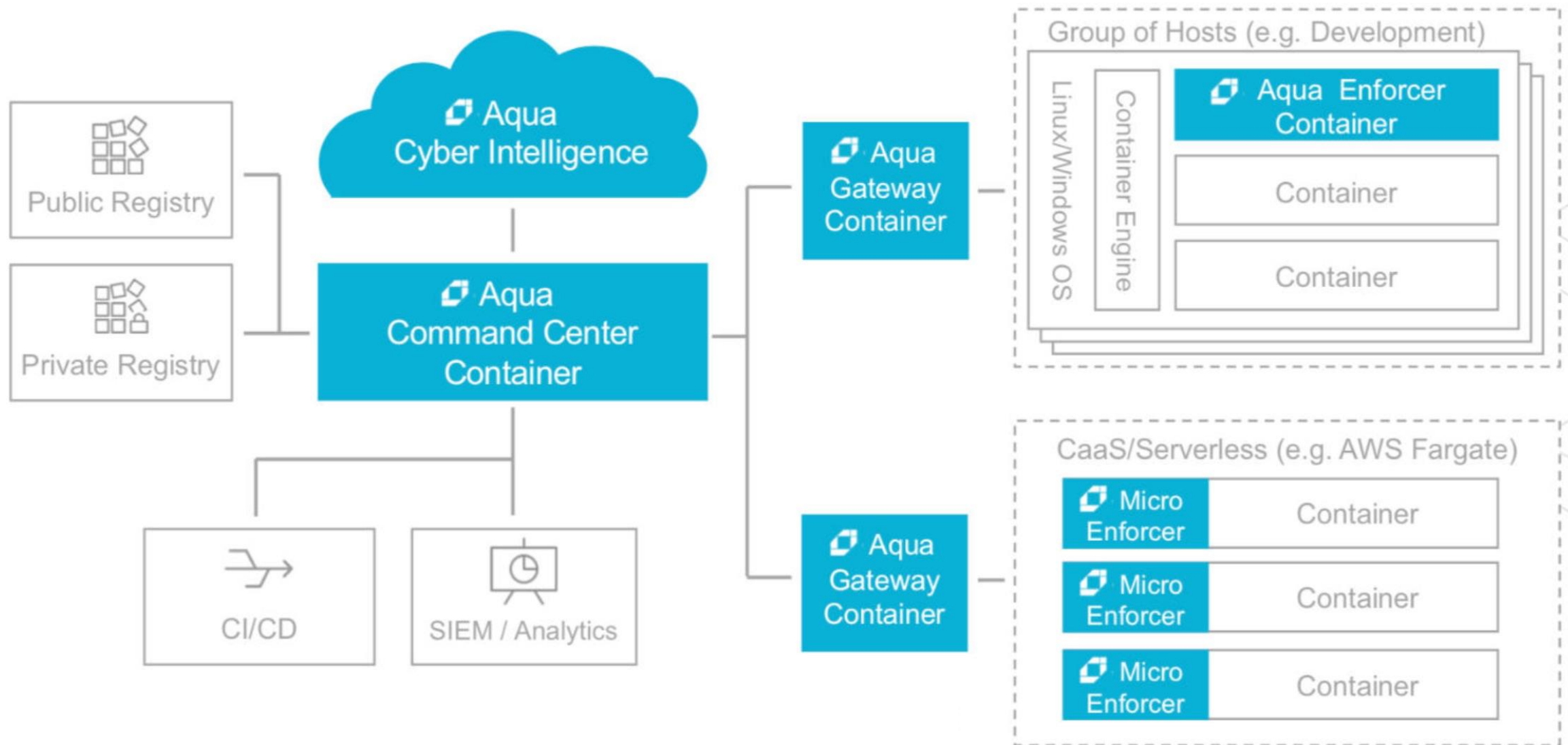
セキュリティチェックの自動化とイメージの探知を開発初期段階で実施（シフトレフト）



# Aquaのフルライフサイクル

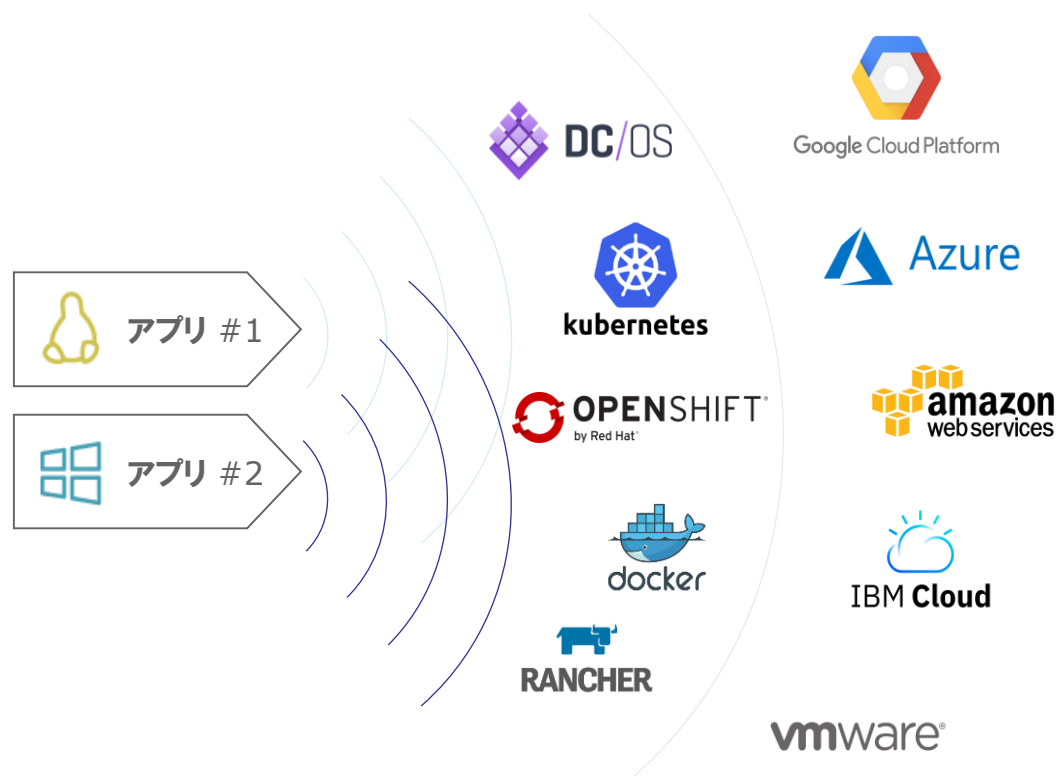


# Aqua コンポーネント



# すべての環境でアプリを守る

Aquaのソリューション：一度の導入で、あらゆるプラットフォームに対応  
-セキュリティはアプリと共にインフラを移動



- ✓ Linux と Windows コンテナ
- ✓ 全てのオーケストレータ：Kubernetes, OpenShift, DC/OS, Docker Swarm
- ✓ クラウド or オンプレ：AWS, Azure, GCP, IBM cloud, VM環境
- ✓ CaaS：AWS Fargate と Azure ACI
- ✓ マルチテナント管理
- ✓ Coming Soon…：  
*Pivotal Cloud Foundry*対応

# Aqua社の3つのアプローチ

## DevSecOps の自動化



- CI/CD パイプライン全体を守る
- セキュリティの“シフトレフト”、問題は早い段階で発見、対処
- セキュリティの自動化でアプリのデリバリーを早める

## コンテナ全般への 次世代のセキュリティ



- 不変性の維持  
：パッチを一切行わない
- ホワइटリストによる制御、異常な挙動を検知
- マイクロサービスへのファイアウォール適応によるアクセス制御
- 状況の可視化とコンプライアンス対応

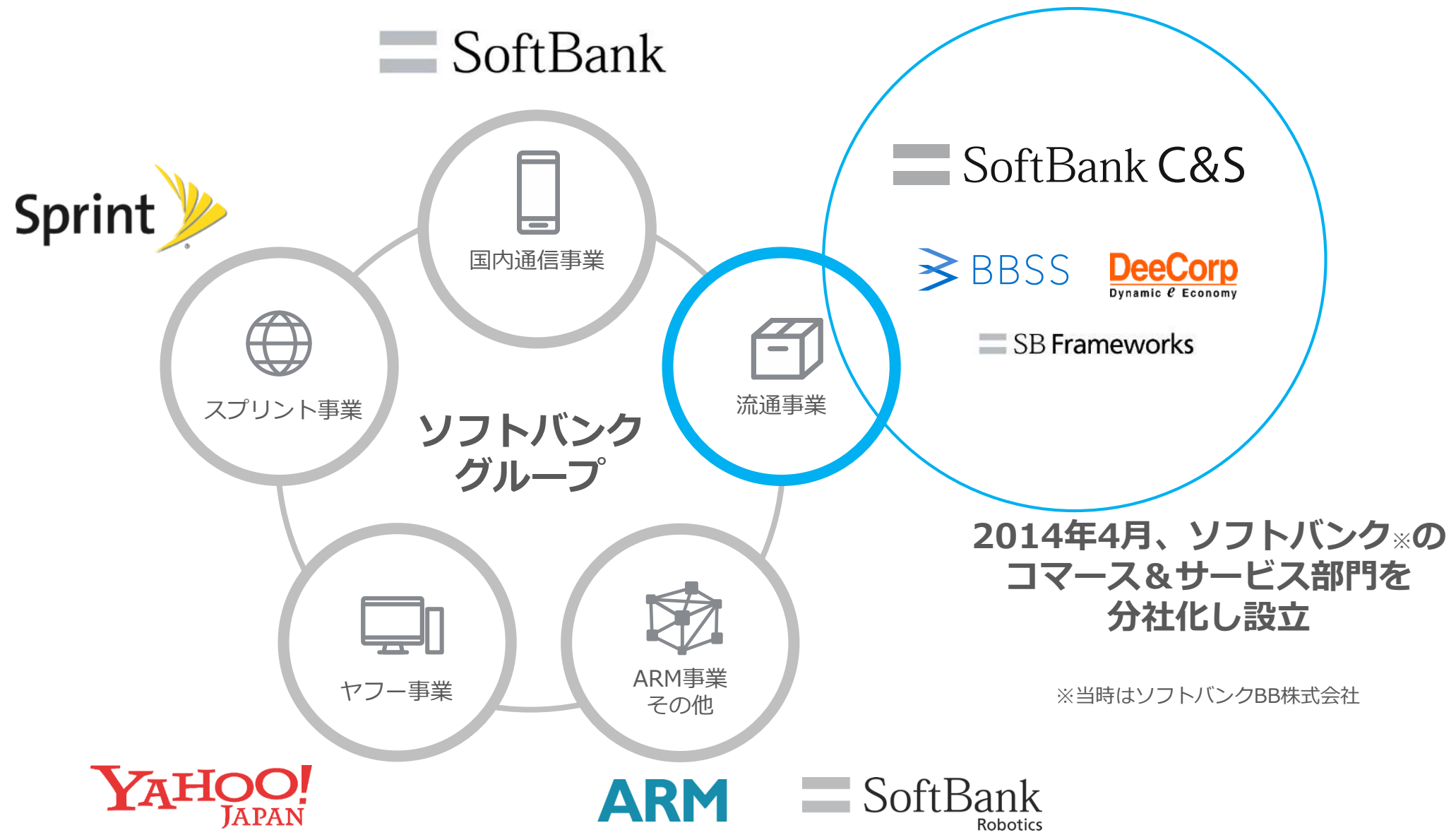
## 一度の導入で、あらゆる プラットフォームに対応



- プラットホーム、クラウド、OSに関わらずアプリを守る
- ハイブリッドクラウドやクラウド移行が可能
- クラウドロックインを防止

# ソフトバンクコマース&サービスについて

# ソフトバンクC&Sの位置づけ



幅広い商品と長年の実績で、ICT流通を支える



販売パートナー 全国

**10,000** 社

**40,000** 拠点



取り扱いメーカー

**4,000** 社



取り扱い商材

**400,000** 点以上

# コンテナの盛り上がりとC&Sの取り組み

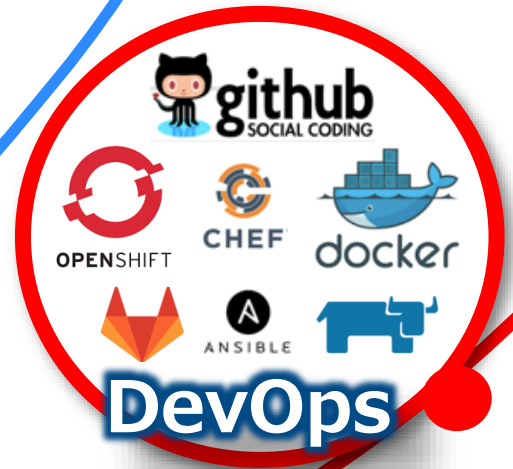
コンテナ化されたアプリの数  
**500億・90万種類**

爆発的な利用者の増加  
**156,000%**  
(2014年比)

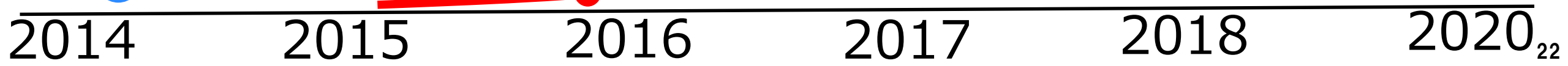
コンテナが広く  
利用され始める

北米での技術調査、  
ソリューション検討開始

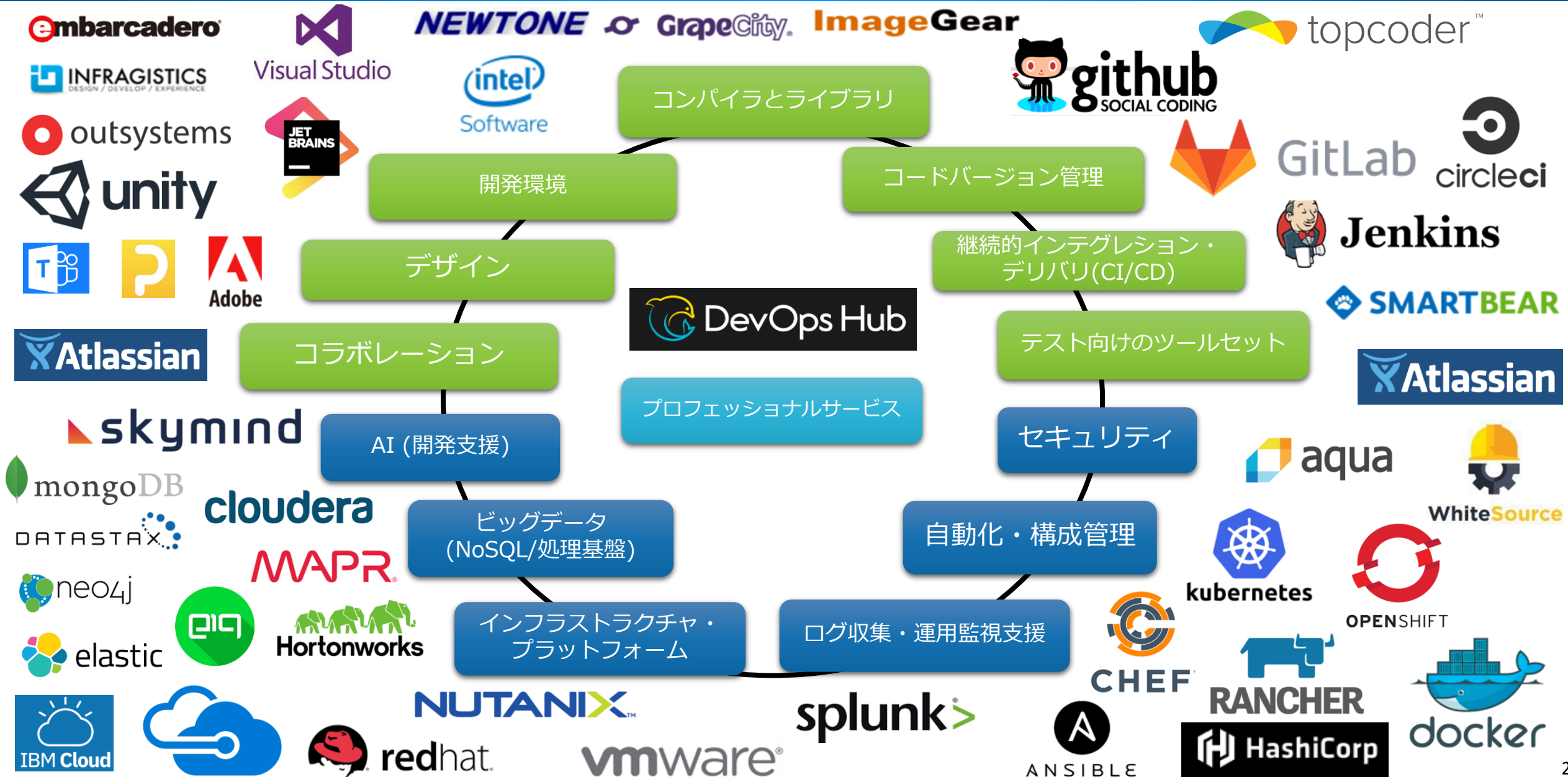
幅広いニーズに答える  
新しいDevOps製品を検討中



コンテナ製品を含むDevOps  
ソリューションとして販売開始



# SBC&S DevOps 製品ポートフォリオ

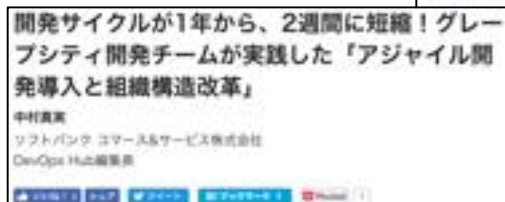




# DevOps Hub

<https://licensecounter.jp/devops-hub/>

- DevOps専用のオウンドメディア
- 有識者の情報発信 + 事例公開



製品購入やサービスに関するお問い合わせは、  
担当営業もしくは、以下窓口までお願いいたします。



DevOps相談窓口

[SBCASGRP-  
DevOps@g.softbank.co.jp](mailto:SBCASGRP-DevOps@g.softbank.co.jp)

 SoftBank C&S