OT側の脆弱性管理への新しいアプローチ方法！

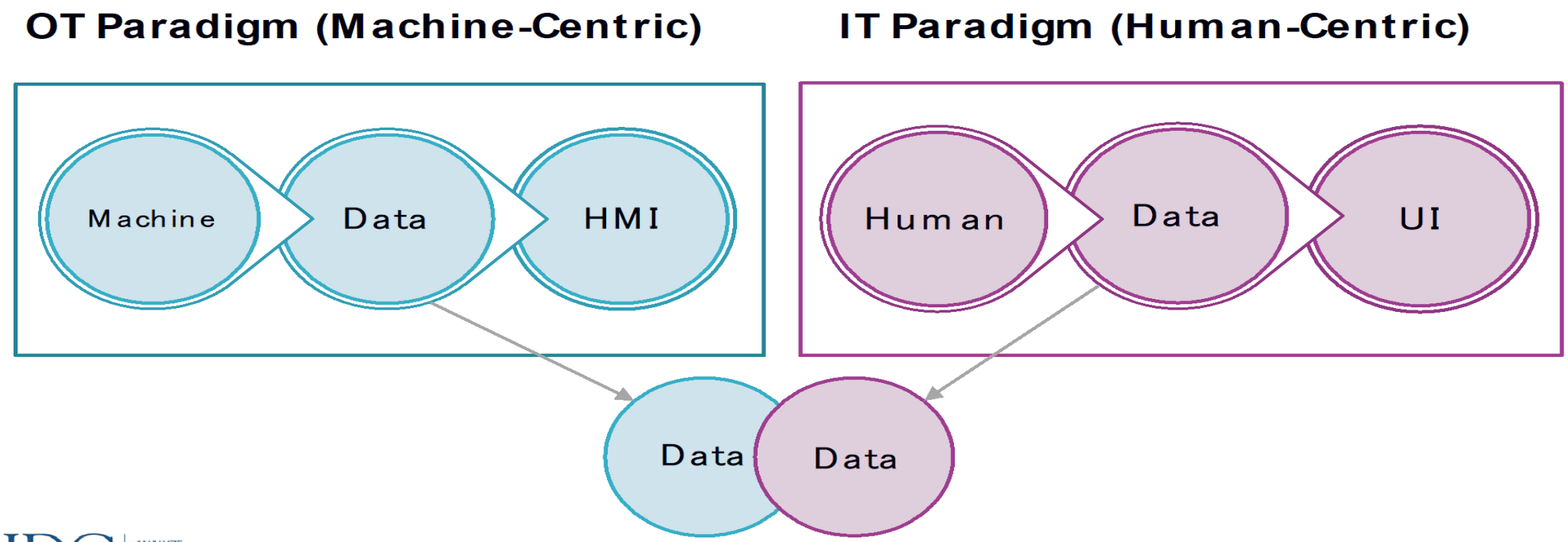
Gabe Authier

データはOT&ITの共通事実

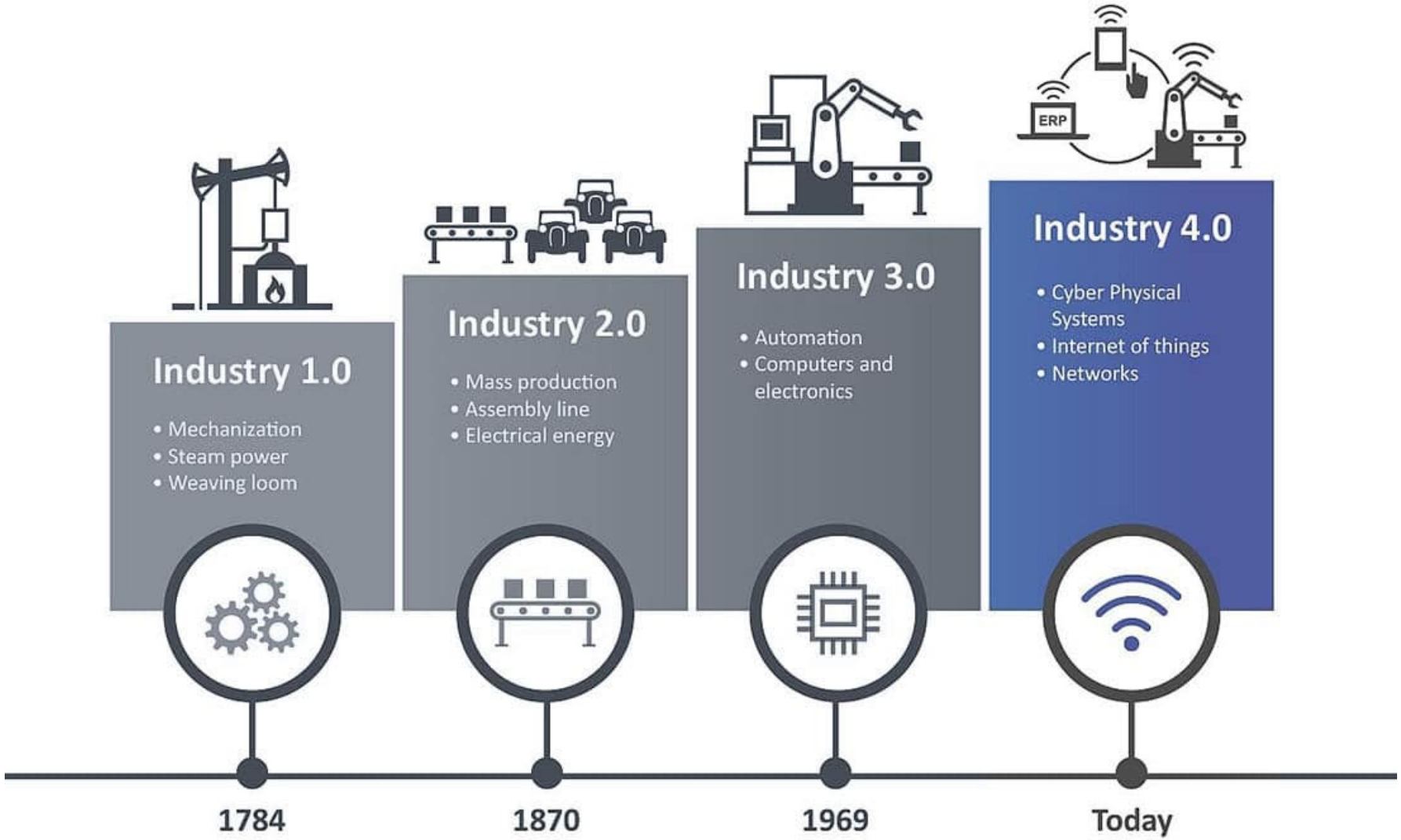
OTとIT両方の世界のデータが結合したときIIoTの魔法が起きる

Data is a Common Factor Between OT & IT

The magic of IIoT happens when we combine the data from these two worlds



インダストリー4.0



出典：Dzone.com

現代のOTネットワーク

出典：Dzone.com

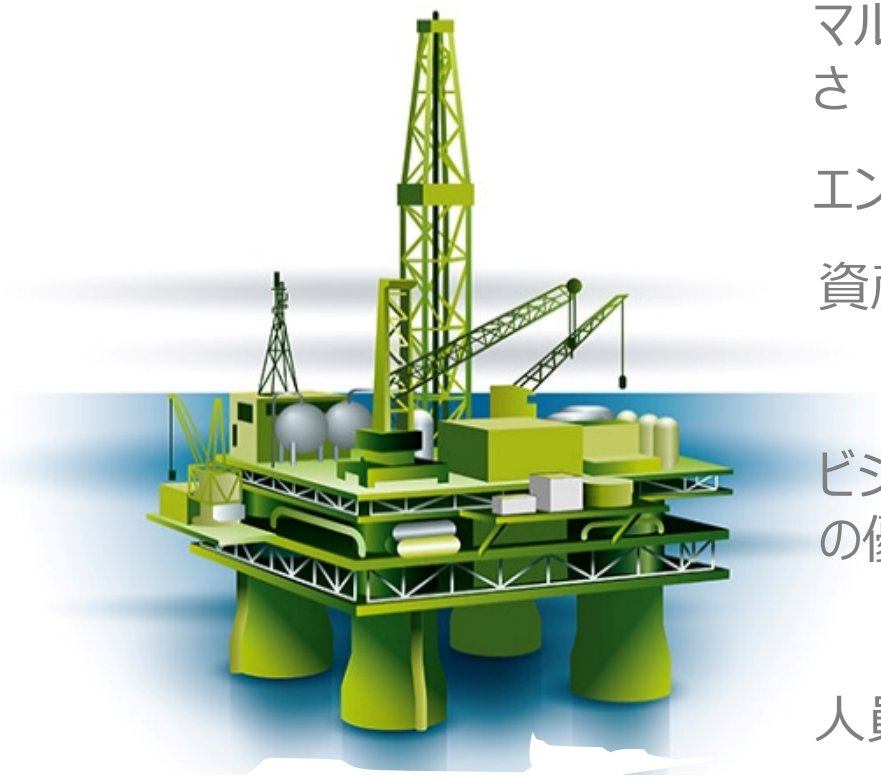
OTの世界を複雑化する技術上の問題

未知の脆弱性

レガシー機器

侵害の特定・対応が取られているかが不確実

変化する規制への準拠



マルチナショナル向けレポートの複雑さ

エンドポイントの数の増加

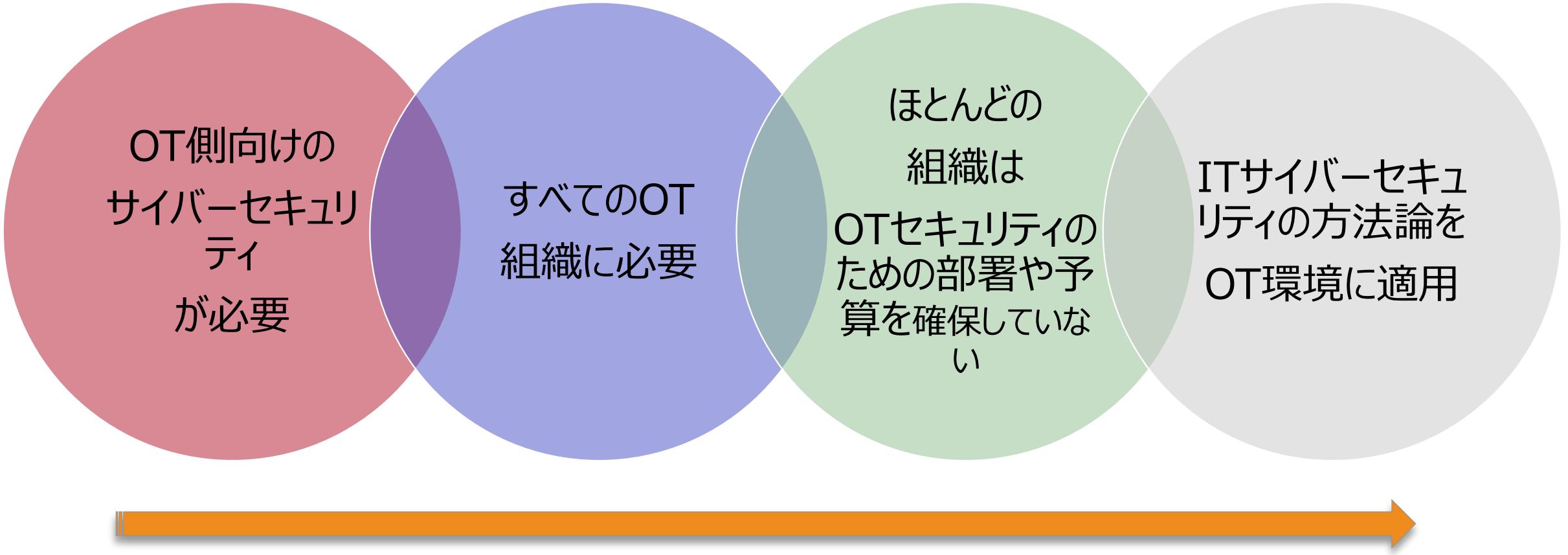
資産の不十分な可視性

ビジネス上の関連性に基づいた脅威の優先順位付けが困難

人員・スキル不足

無関心なマネジメント層

OT側向け脆弱性管理

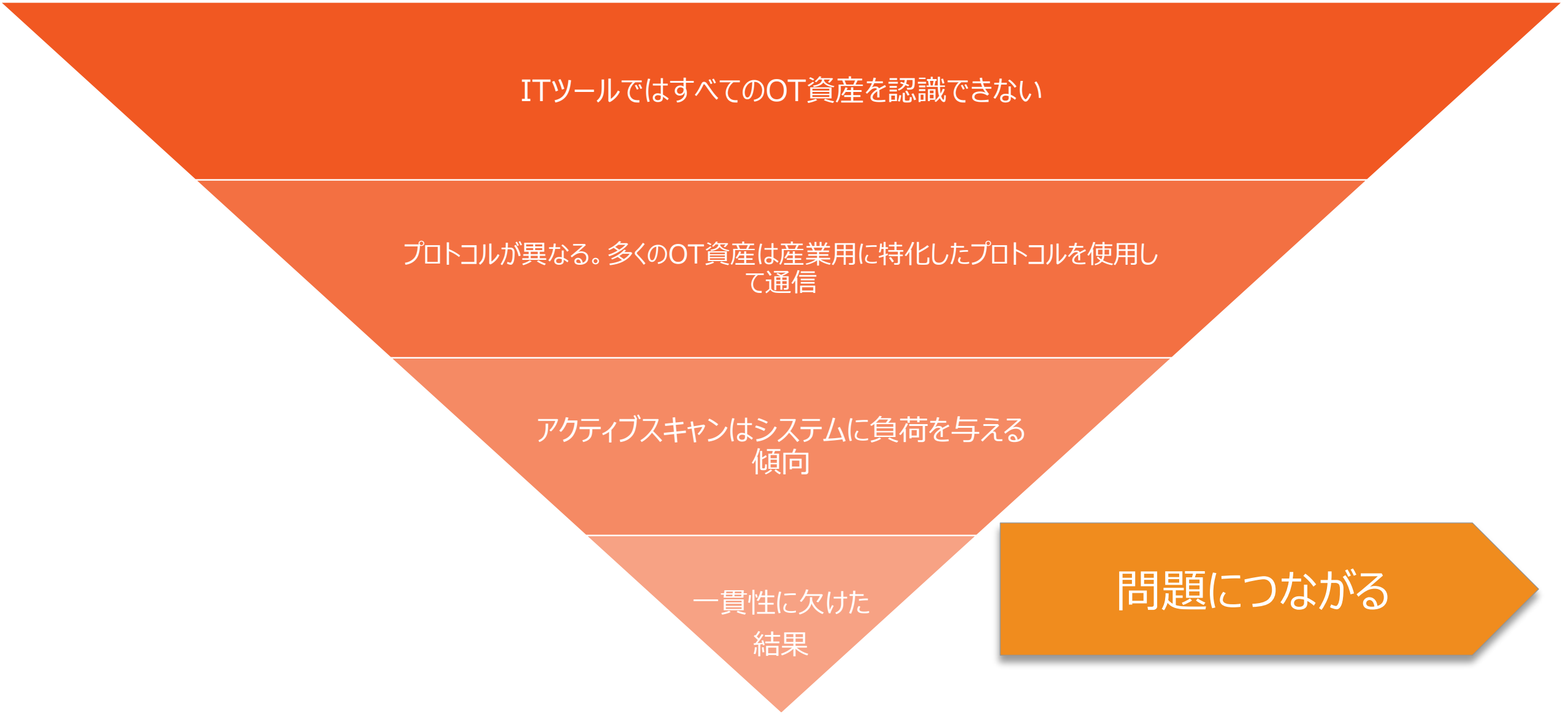

OT側向けの
サイバーセキュリティ
が必要
すべてのOT
組織に必要
ほとんどの
組織は
OTセキュリティの
ための部署や予
算を確保していな
い
ITサイバーセキュ
リティの方法論を
OT環境に適用

今日のOTネットワークにおける脆弱性管理の効果は

OT&IT：違う世界

	オペレーショナルテクノロジー	情報テクノロジー
定義	オペレーションの制御と自動化を促進するための技術、システム、プロセス、イベントの連携（物理的には必ずしもそうなるとは限らない）	データの処理と配信を行うためのコンピューターシステム、ソフトウェア、ネットワークの開発、保守、使用に関連する技術
一般的なシステム	産業制御システム向けの技術が主にOT環境内で使用される	IT環境内のインフラストラクチャー（コンピューティング、ネットワーク、ストレージ用）とその上で動作するアプリケーション
一般的なプロトコル	独自仕様の機器が多いため、膨大な種類のネットワークプロトコルを考慮する必要がある	中核的なコンピューティングアーキテクチャーと通信プロトコルの大部分が標準化されている
デプロイメントモデル	オンプレミス	各種デプロイメントモデルの混合。ただしクラウド指向型が増加中
優先順位	生産のスループットと資産の可用性	従業員の生産性、リスクの低減

アクティブスキャンがうまくいかない理由



問題につながる

アクティブスキャンの問題

Subtitle

アクティブスキャンの方法に起因するサービスの停止ITスタイルの非常に軽量な検出・スキャン機能でさえサービス停止の原因となり得る

予測不能な挙動

資産の可視化が不十分、狭いカバー範囲

不完全な脆弱性評価

デバイスの故障「産業用デバイスを攪乱させる」

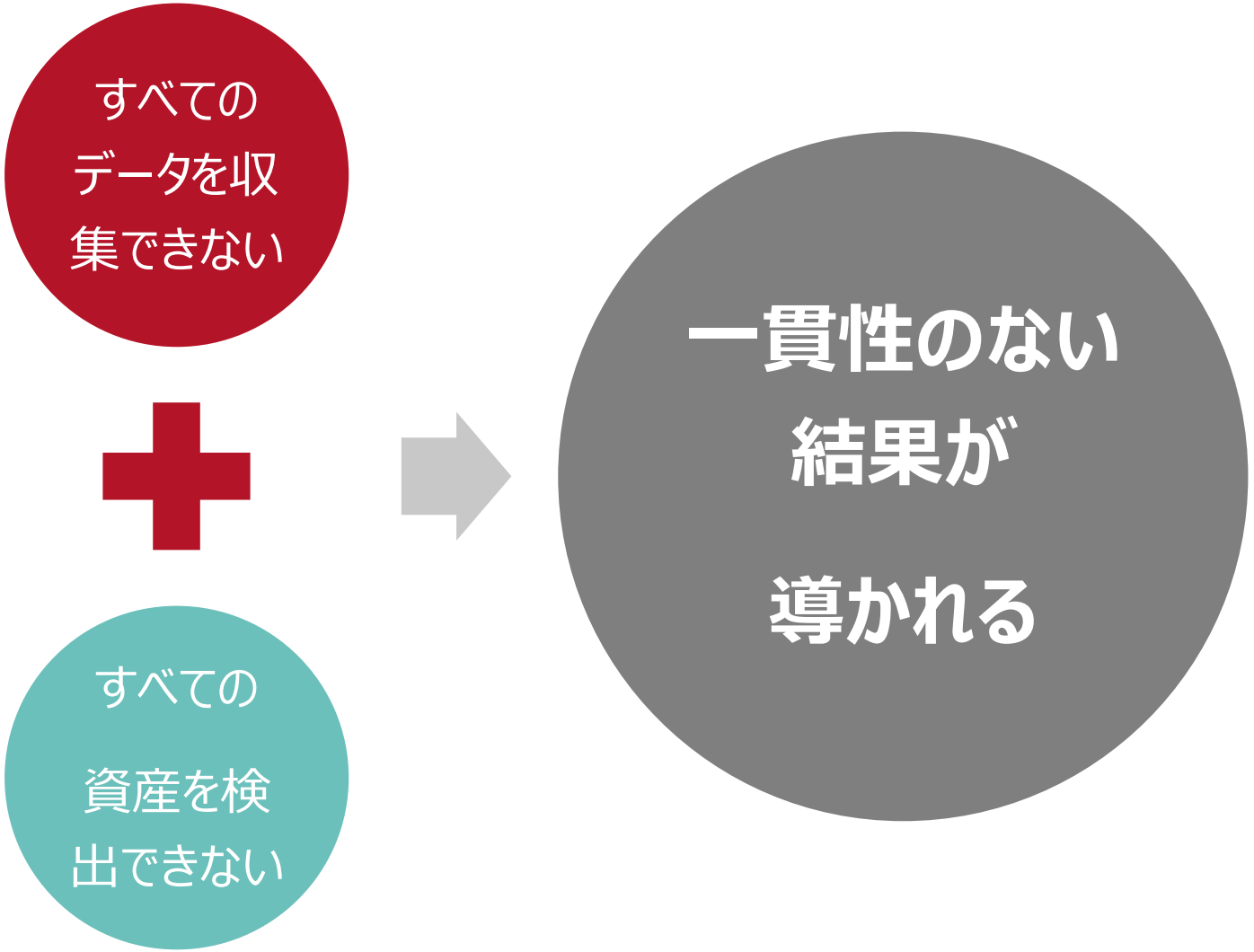
機能停止 – ネットワークおよびデバイスレベル

産業用資産が予期しないリクエスト/方法にうまく対処できない

資産の検出が不完全

検出漏れや誤検出につながる

パッシブ型モニタリングも選択肢としてあるが、同様の問題がある



効果的なアプローチ：アクティブ型/パッシブ型/ハイブリッド型のソリューションを統合

アクティブ

- デバイスとアクティブなインタラクションを行う
  - ポーリング、すなわち：
    1) ネイティブICSプロトコル
    2) SNMP
  - コマンドラインインターフェイス
  - Webユーザーインターフェイス
  - ソフトウェアエージェント
- 直接的なインタラクション

パッシブ

- ネットワークトラフィックのコピーをパッシブに調査・分析する
  - スイッチポートアナライザー（SPAN）
  - ミラーポート
  - タップ
- 傍受

ハイブリッド

- 既にデータを保持している、あるいはデータ収集のためのドライバーを持つアプリケーションとインタラクションを行う。すなわち：
  - Rockwell FactoryTalk AssetCentre
  - MDT Autosave
  - Kepware
  - Project Files
- サードパーティ製品を使用

このアプローチの利点

より広いカバー範囲

ほとんどの脆弱性の検知が可能

低い誤検出率

サービス中断が発生しない

まとめ

- 100%アクティブ型、100%パッシブ型、100%ハイブリッド型のいずれのソリューションでも包括的な産業用VMは実現できない
- あらゆる脆弱性に対応するには、それら3つを組み合わせることが最も効果的なアプローチとなる
- デジタルツイン、AIあるいはIoTセンサーなどの最新技術を使用することがOTネットワークに非常に有利に働く
- 産業用VMプログラムの成功には、柔軟なVMソリューションの採用が鍵となる

ご清聴ありがとうございました

導入のご相談はお気軽に

弊社製品、ソリューションに関するお問い合わせは下記にてお受けいたします

トリップワイヤ・ジャパン株式会社　営業本部

TW-Sales-Japan@tripwire.com

03-6848-6350

〒103-0027 東京都中央区日本橋1-12-8　第二柳屋ビル2階

30日間お試しいただけます

Tripwire IP360を30日間フル機能にてお試しいただけます

トリップワイヤ・ジャパン 評価版お申し込みページ

https://www.tripwire.co.jp/download/