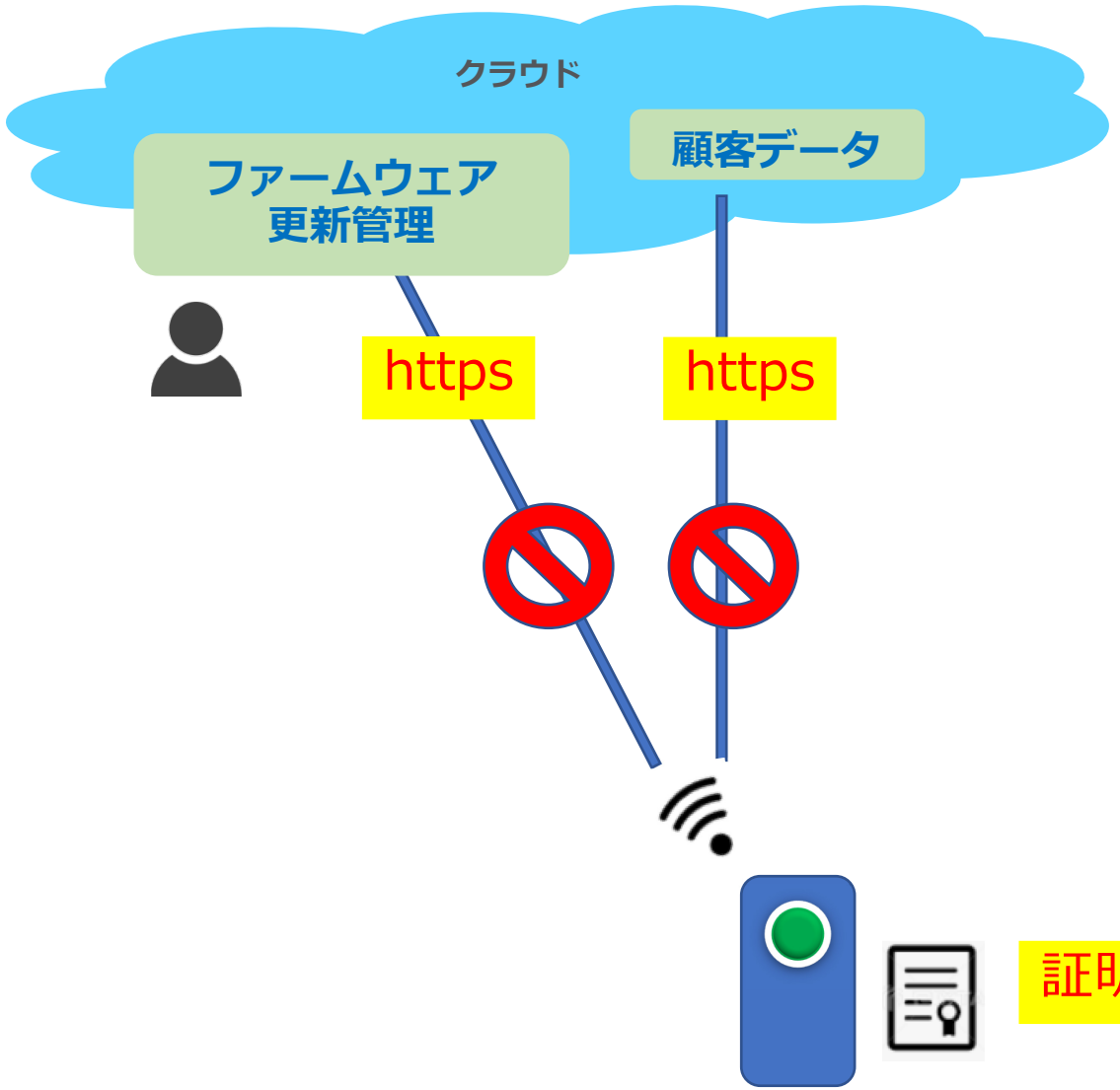
DX推進に必要なセキュリティ人材とは？

情報処理推進機構産業サイバーセキュリティセンター サイバー技術研究室 専門委員
(フォーティネット ジャパン株式会社　OTビジネス開発部　部長)
佐々木　弘志

消費者向けIoTデバイスに起きた悲劇…

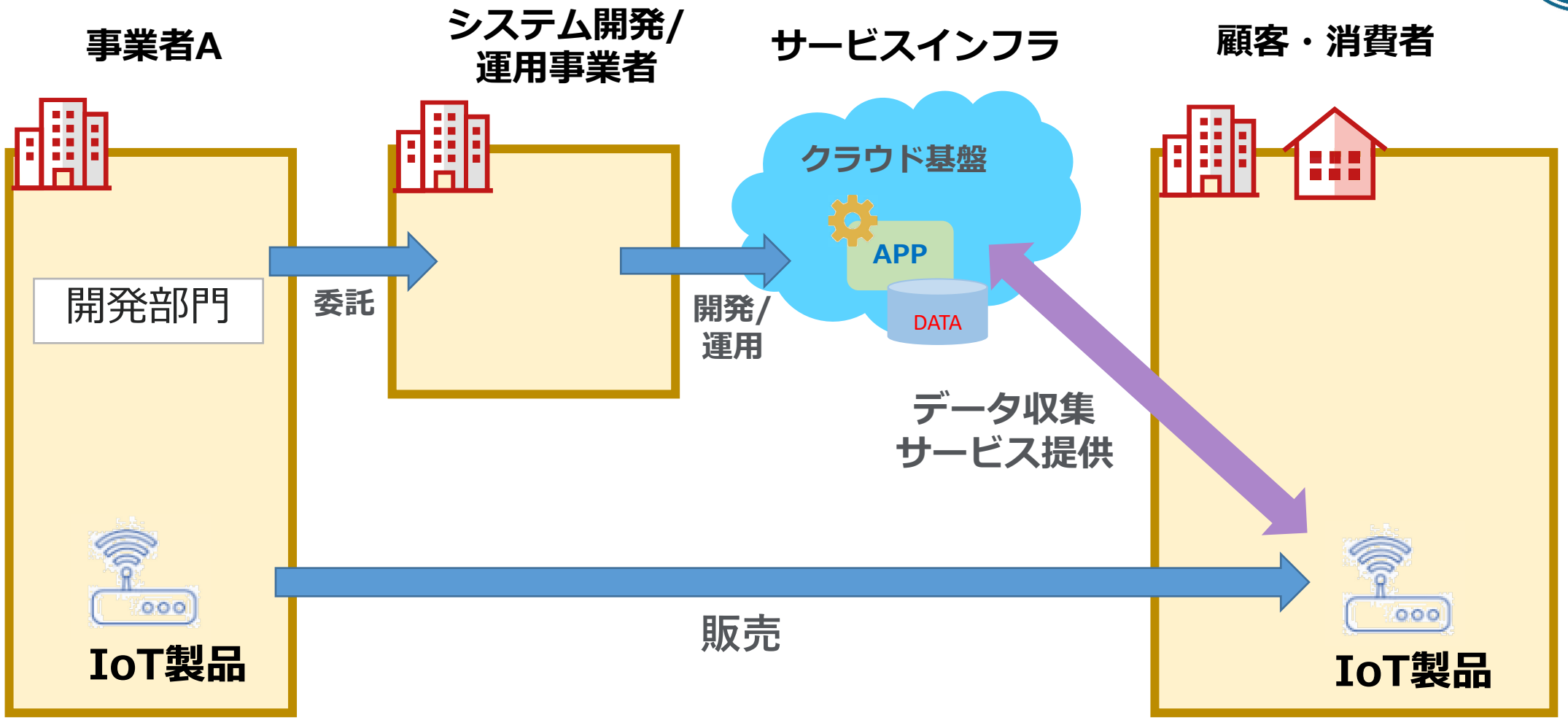


うんこボタンはHTTPSでサーバと通信しているのだが、サーバ証明書がミスにより期限切れになってしまった。サーバ証明書の変更に合わせてデバイスのファームウェアを定期的に書き換えるはずなのだが、そのOTA（Over The Air）アップデートもまた、HTTPSを用いるため、「**詰んでしまった**」という。

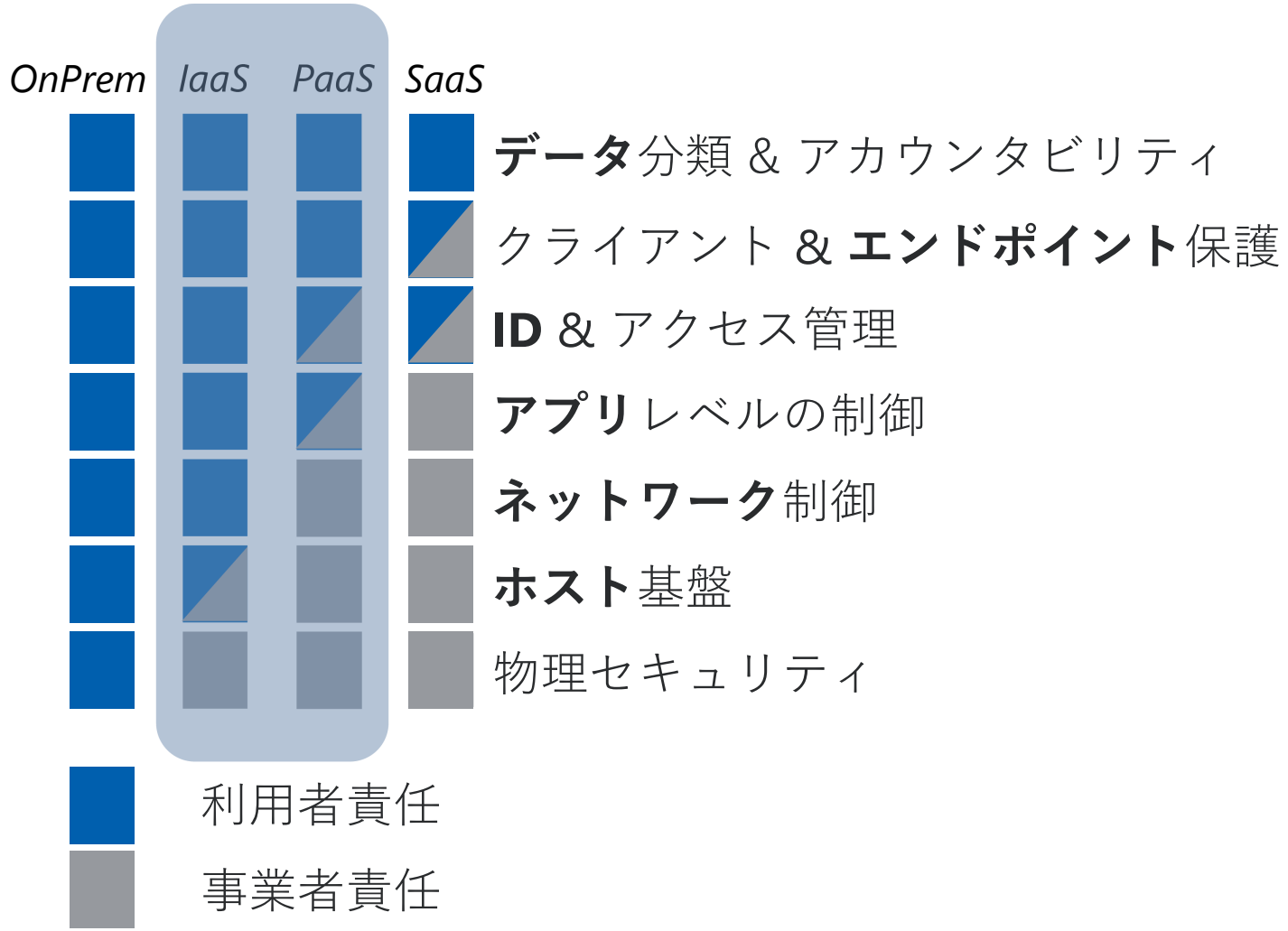
セキュリティ機能導入の際に
設計が不十分だとむしろ害悪になる例

https://www.itmedia.co.jp/news/articles/1811/28/news077.html

「モノ」売りから「コト」売りへ⇒クラウド基盤の活用へ



クラウド利用の責任共有モデル



ローカルのアプリケーション

パソコン/サーバー

アプリケーション（App）

データ

OS

ハードウェア

CPU　メモリ　HDD

外部I/F（通信等）

App&データ管理の複雑化

クラウド上のアプリケーション（コンテナ）

クラウド/データセンター

アプリケーション（App）

データ

仮想コンピューティング/NW/ストレージ

オーケストレーションツール（ミドルウェア）

コンテナ

VM（仮想マシン）　VM　VM

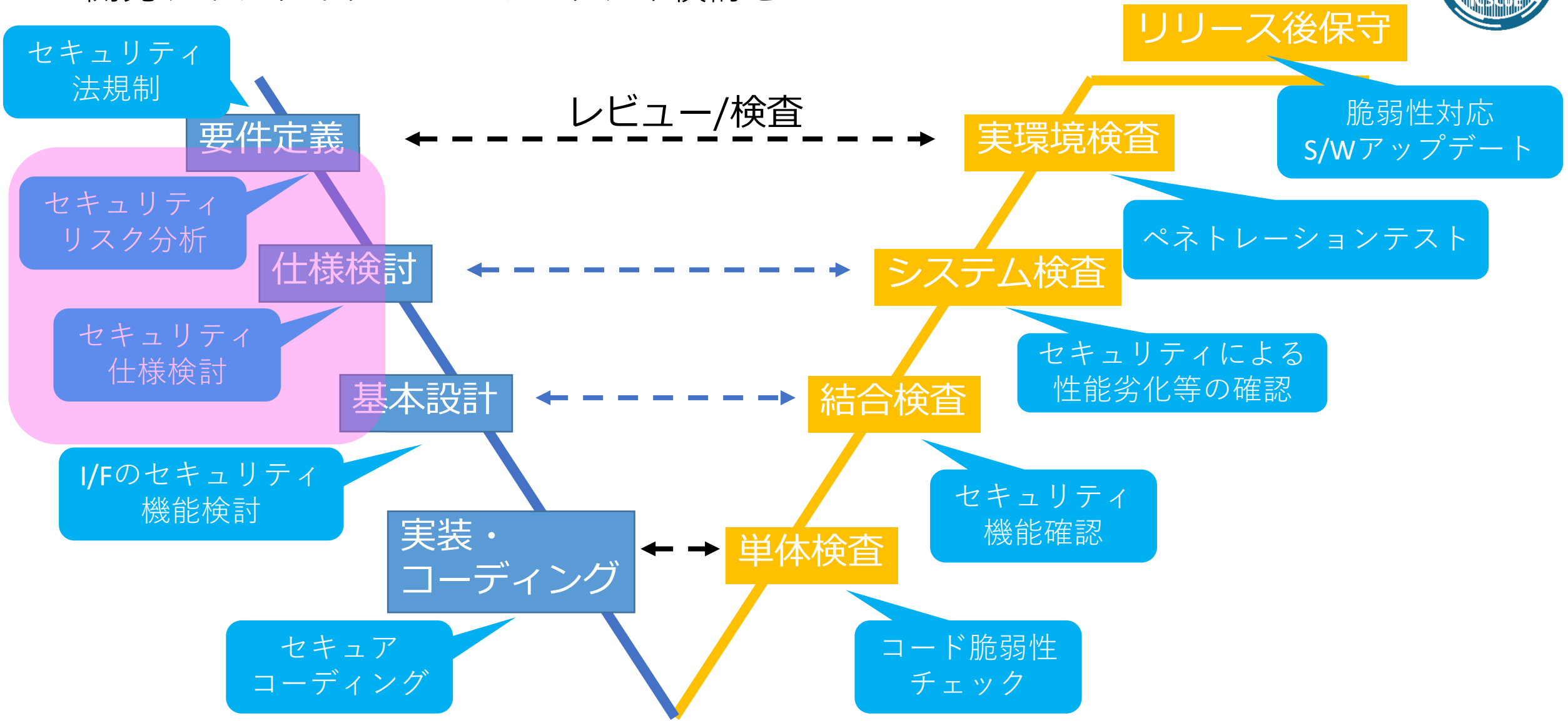
コンテナRT　コンテナRT　コンテナRT

OS　OS　OS

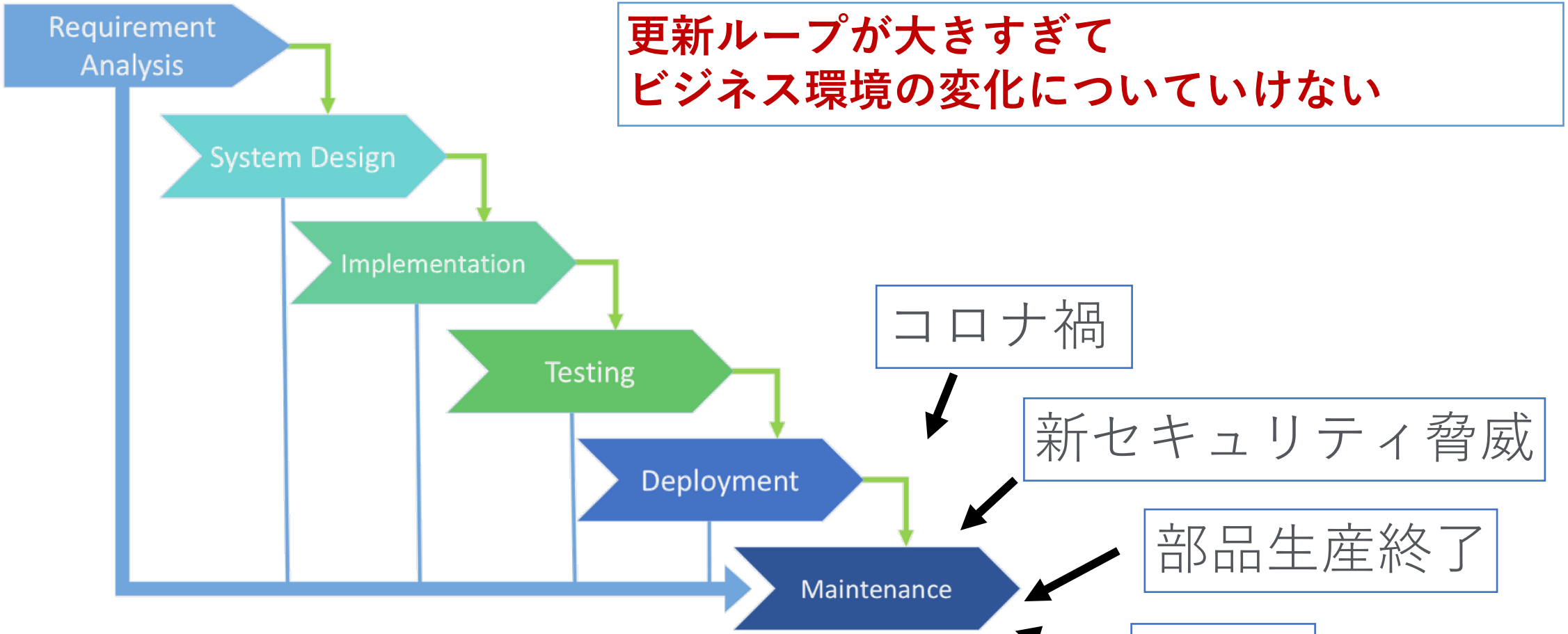
ハードウェア　ハードウェア　ハードウェア

セキュリティ・バイ・デザイン

開発ライフサイクルにセキュリティ検討を“BUILT-IN”



ウォーターフォール型ソフトウェア開発ライフサイクル（Software Development Life Cycle: SLDC）



DXを実現するための考え方や仕組み

DevOps

組織の文化の変革

- 相互信頼・尊重・協力
- ビジネスの持続的推進

CI/CD

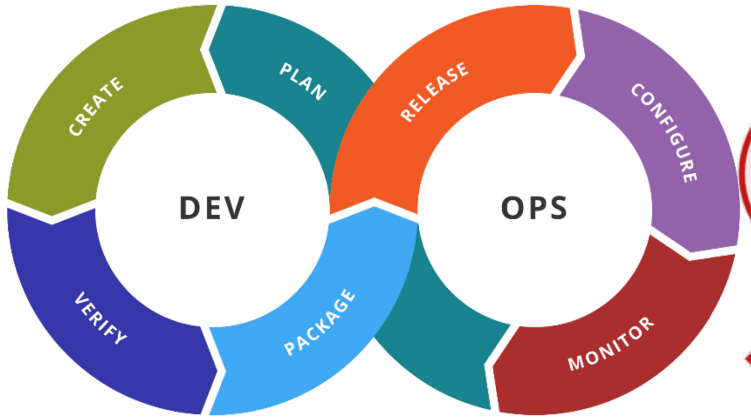
ソフトウェアエンジニアリングのプラクティス

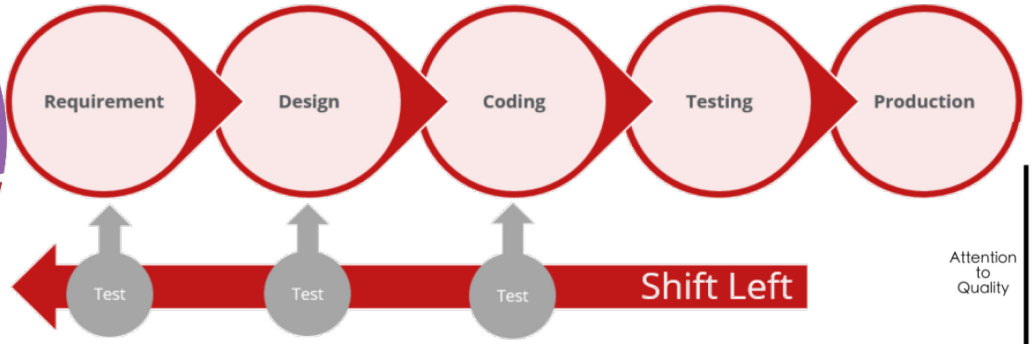
- 構築と統合の自動化
- テストの自動化

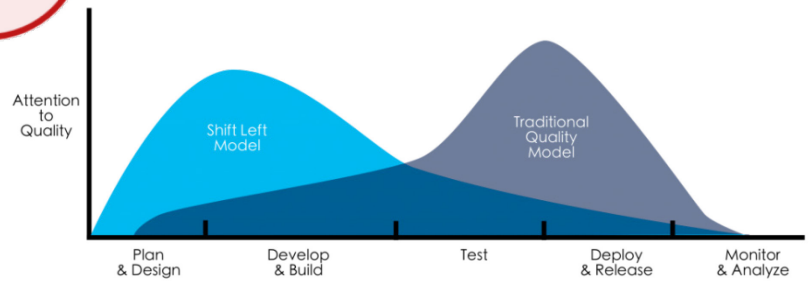
ShiftLeft

テストの前倒しによるバグ・脆弱性の修正

- コスト削減
- クオリティ向上

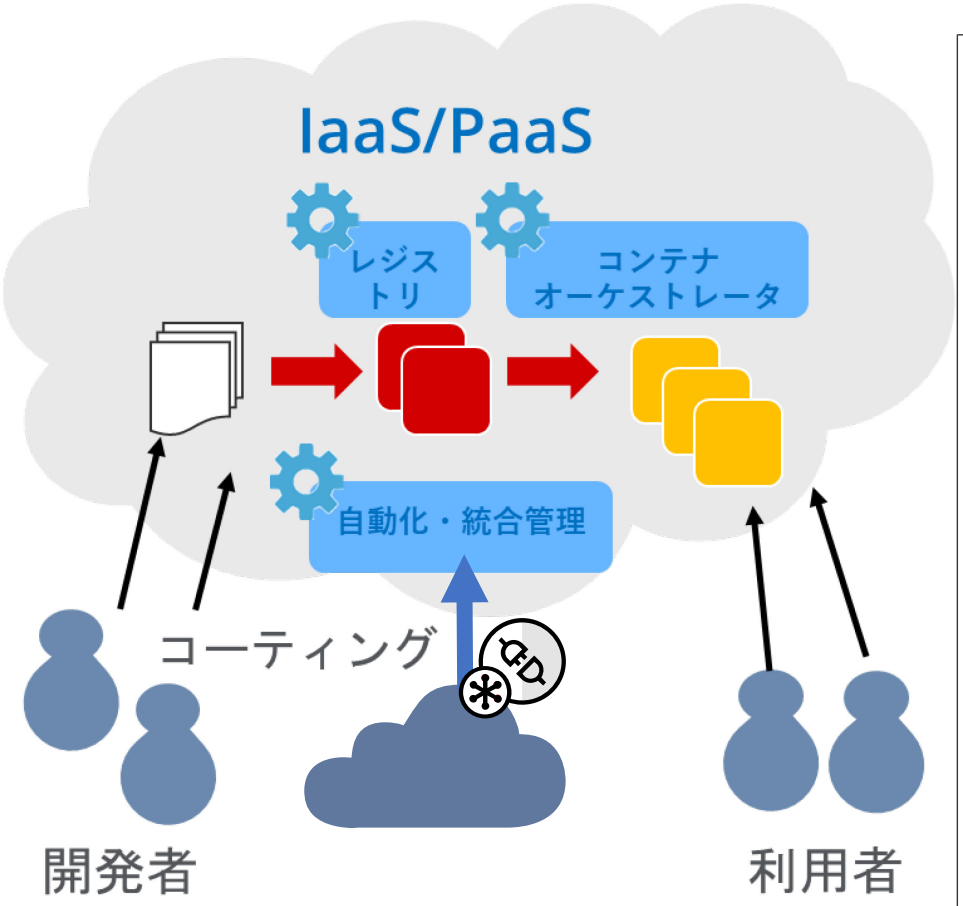






CI/CD: Continuous Integration/ Continuous Delivery

コンテナアプリケーション開発の流れ



1. 開発者用システム（イメージを生成し、テストや認定へ送る）
2. テスト/認定システム（イメージの内容の妥当性確認・検証、イメージへの署名、レジストリへのイメージの送付）
3. レジストリ（イメージを保存し、要求に応じてオーケストレータに配布する）
4. オーケストレータ（イメージをコンテナに変換し、コンテナをホストにデプロイする）
5. ホスト（オーケストレータの指示通りに、コンテナを実行したり停止したりする）

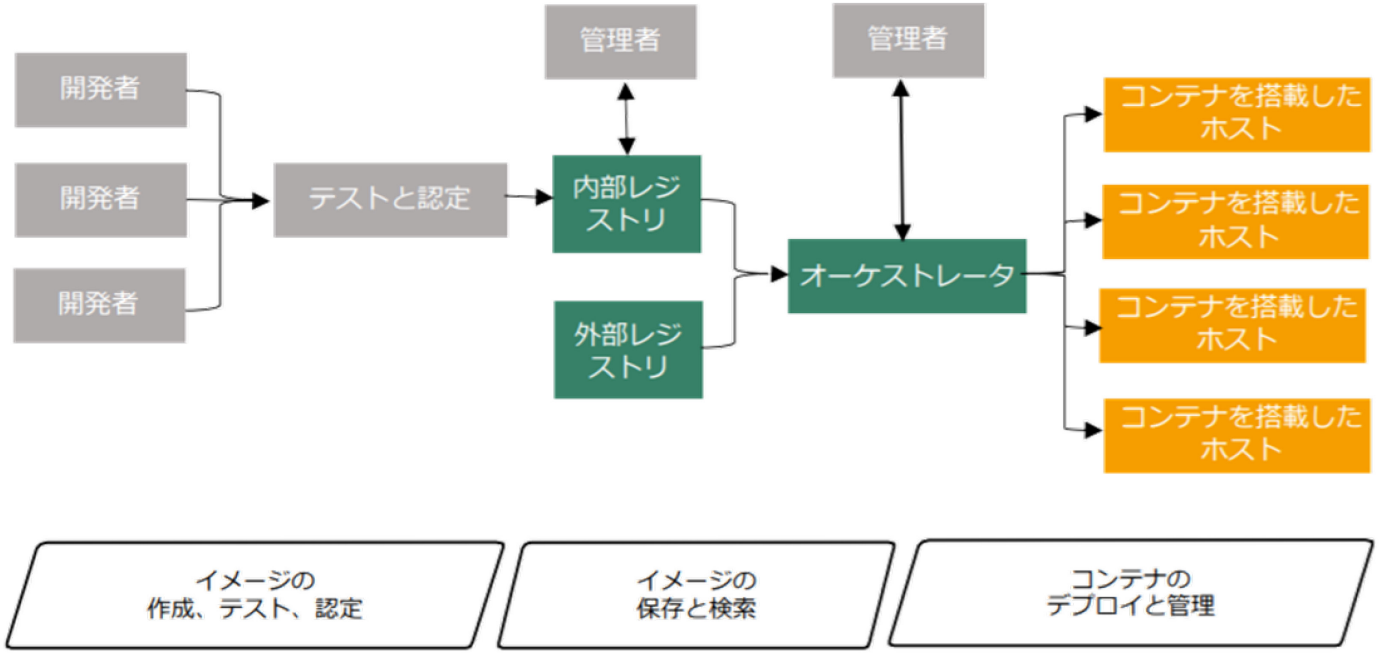
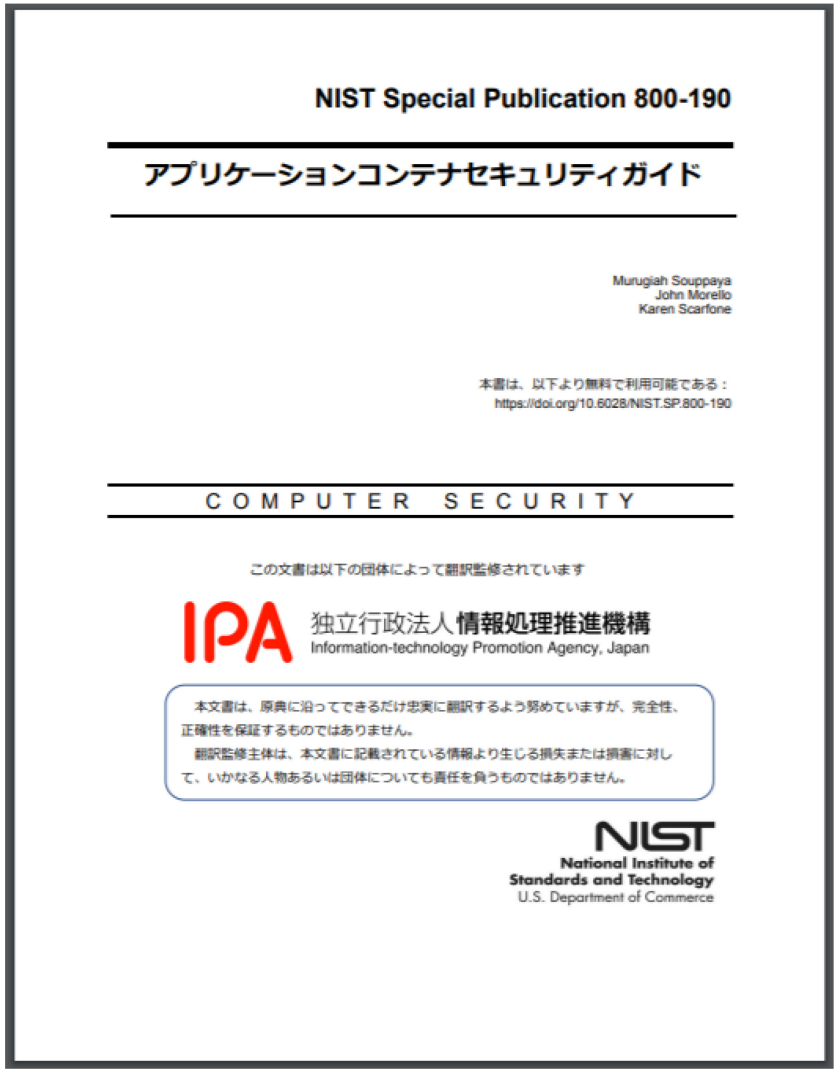


図 3：コンテナ技術アーキテクチャの階層、コンポーネント、およびライフサイクルフェーズ

https://www.ipa.go.jp/files/000085279.pdf

米国政府システムセキュリティ基準　NIST SP800-190
～コンテナセキュリティガイド～


NIST Special Publication 800-190

アプリケーションコンテナセキュリティガイド

Murugiah Souppaya
John Morello
Karen Scarfone

本書は、以下より無料で利用可能である：
https://doi.org/10.6028/NIST.SP.800-190

COMPUTER SECURITY

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

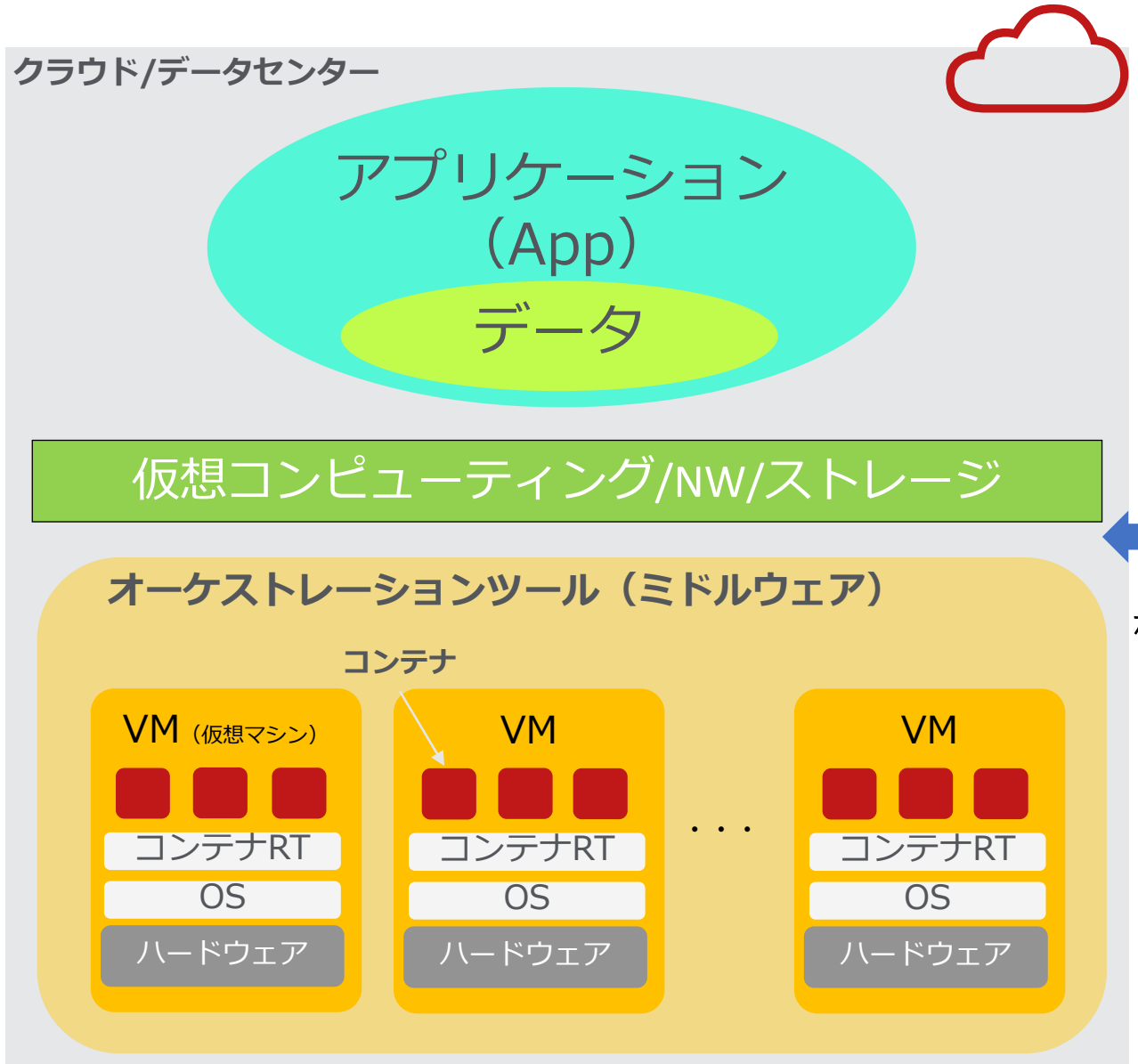
本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。
翻訳監修主体は、本文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。

NIST National Institute of Standards and Technology U.S. Department of Commerce

https://www.ipa.go.jp/files/000085279.pdf

対象	リスク	主な対策（抜粋）
イメージ	脆弱性、設定不備、埋め込みマルウェア＆平文秘密、信頼できないイメージ使用	コンテナ技術に特化した脆弱性管理ツール、信頼できるイメージとレジストリのセットを維持
レジストリ	セキュアでない接続、古いイメージ、認証・認可の制限不良	暗号化されたチャネル、認証制限強化
オーケストレータ	管理者アクセス制限不良、不正アクセス、NWトラフィックの不十分な分離、WLの機密性レベルの混合、ノードの信頼	最小権限のアクセスモデル、多要素認証、機微性のレベルでのホスト分けたデプロイ
コンテナ	ランタイムソフトウェア内の脆弱性、無制限のNWアクセス、セキュアでないランタイム設定、アプリ脆弱性、未承認コンテナ	脆弱性モニタリング、コンテナの外部通信制限、ランタイム設定の標準準拠自動化
ホストOS	大きなアタックサーフェス、共有カーネル、OSコンポーネント脆弱性、ユーザアクセス権、OSファイルシステム改ざん	コンテナ専用OS使用、コンポーネントバージョン管理ツール、認証ログ、重要ディレクトリ監視

IaaS/PaaS基盤の総合的なセキュリティ保護



セキュリティソリューション

データとAppの保護とリスク管理

DLP（情報漏えい）対策
マルウェア対策
アプリとデータのリスクの優先順位付け

CWPP (VM/コンテナ保護)

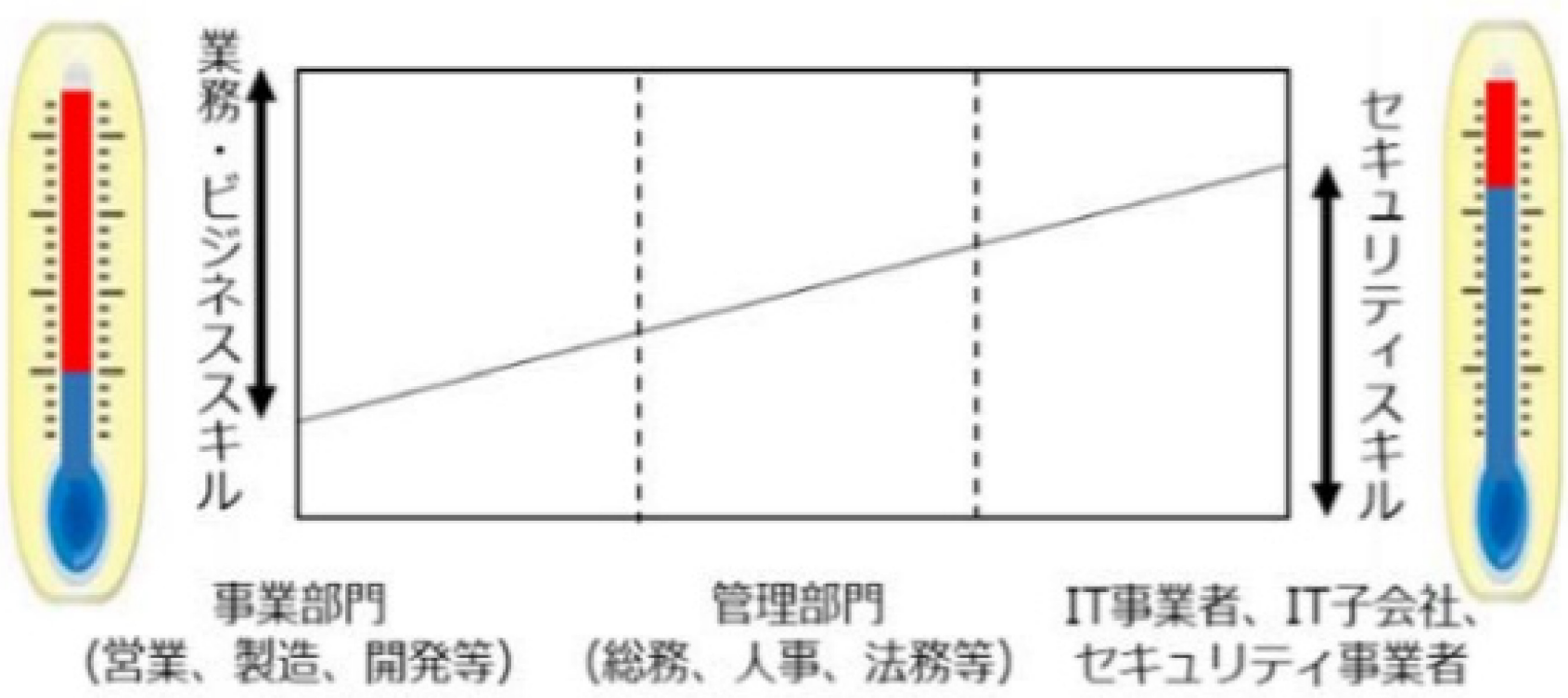
脆弱性診断と脅威検知
全てのVMとアプリケーションの発見
アプリケーション制御とセグメンテーション
ネットワーク監視（コンテナ間含む）

CSPM(クラウド基盤の設定監査)

コンプライアンス監査
全てのIaaS/PaaSサービス資産の発見
カスタムポリシーによる修復
CI/CDツールとの統合

製品・サービスに関わる全てのステークホルダーにセキュリティ知識が必要!

プラス・セキュリティとは？



図表７　所属企業・部門におけるセキュリティスキルと業務ビジネススキルとの関係イメージ

出典：JCIC 作成

業務に関わる「セキュリティ知識」の必要性の高まり

https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf

CSIRTがプラス・セキュリティ人材育成を主導

ITセキュリティ部門（CSIRT）

プラス・セキュリティ人材育成の取り組み管理
- 教育プログラム検討
- 教育プログラム作成
- 外部サービス紹介

など

開発部門	OT部門	調達部門	顧客対応部門	法務部門
ソフトウェア脆弱性管理	サプライヤに要求するセキュリティ要件（ISMS等）		ソフトウェア脆弱性管理	セキュリティに関する契約条項（賠償・免責）
Security by Design 開発	OTセキュリティリスク評価手法	サプライヤに要求するセキュリティ要件（ISMS等）	顧客に関するセキュリティ規制・ガイドライン	サプライヤに要求するセキュリティ要件（ISMS等）
自社製品・サービスに関する脅威	OTシステム一般脅威	製品・サービス一般脅威	製品・サービス一般脅威	顧客に関するセキュリティ規制・ガイドライン
製品・サービス一般脅威				セキュリティ関連裁判の判例

情報セキュリティ基礎知識　(従来)

業務知識

産業サイバーセキュリティセンター（ICSCoE）

IT/OT両方のサイバーセキュリティの最先端技術を学ぶことで「DX推進」においても活躍できる人材となる

- 2017年4月、IPAに産業サイバーセキュリティセンターを設置
- 中核人材育成プログラムの第１期（平成29年7月～平成30年6月）では、電力、ガス、鉄鋼、石油、化学、自動車、鉄道、ビル、空港、放送、通信、住宅等の各業界60社以上から76名の研修生を受け入れ、実践的な演習・対策立案等のトレーニングを行った。第5期生が受講中。

責任者・実務者向けプログラム

業界別サイバーレジリエンス強化演習（CyberREX）

第2回 令和2年10月23～24日(東京開催)　第3回 11月27～28日(大阪開催)

本演習は、部署・部門のサイバーセキュリティに関する対応力・回復力の強化、業界特性を意識した企業組織全体の強靭化を目的としています。
業界別に仮想企業を想定した、シナリオによる実践的演習の形式を中心としたトレーニングとなっていることが特徴です。また、海外子会社、系列企業、サプライチェーン等のビジネスパートナーが直面するサイバーセキュリティ規制やガイドライン等の解説に関する集中講義を行います。
対象業界：電力、鉄道、ビル・物流などの「インフラ系」業界および自動車（製造）、ファクトリーオートメーションなどの「産業系」業界

サイバー危機対応机上演習（CyberCREST）

令和3年1月27～29日

本演習では、高度化するサイバー脅威から制御システムを有する企業を守るための戦略として、アメリカの先進的なサイバーセキュリティ戦略「コレクティブ・ディフェンス」を学習します。この戦略は、サイバー脅威から、政府・同業他社と情報共有を図りながら企業を守る考え方です。
米国サイバーコマンド出身の専門家やCISO、セキュリティアーキテクトの専門家が自身の経験を共有するとともに、ロールプレイング演習を交えながら、この戦略を企業に適用する方法をご紹介します。

戦略マネジメント系セミナー

事業のデジタル化（デジタルトランスフォーメーション）が進む中、企業にとって「サイバーセキュリティは経営課題」であることを正しく認識する必要性がますます高まっています。
本演習では、方針立案やリスク管理を含むセキュリティ対策を担う方を対象に、事業継続の観点からセキュリティ対策に必要な組織と機能について、講義を行います。

制御システム向けサイバーセキュリティ演習

第1回 令和2年12月15～16日

本演習では、模擬プロセス制御ネットワークを使用して、機器の不正な制御に使用されるサイバー攻撃や対応策による防御を体験いただきます。制御システムのセキュリティについてより深く理解いただける実践的な内容となっています。
ITと制御システムのアーキテクチャ、セキュリティ脆弱性、および制御システムに固有の対策など、産業用制御システムのセキュリティを習得いただけます。

IPA 独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター

2020.9.30

- 中核人材育成プログラム　1年間フルタイム・プログラム
- 責任者・実務者向けプログラム
  （CyberREX, CyberCREST, 戦略マネジメント系セミナーなど）

- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成
業界横断の情報共有の輪の醸成

秋葉原オリエンテーションにおける模擬システム説明会の模様

https://www.ipa.go.jp/files/000069940.pdf