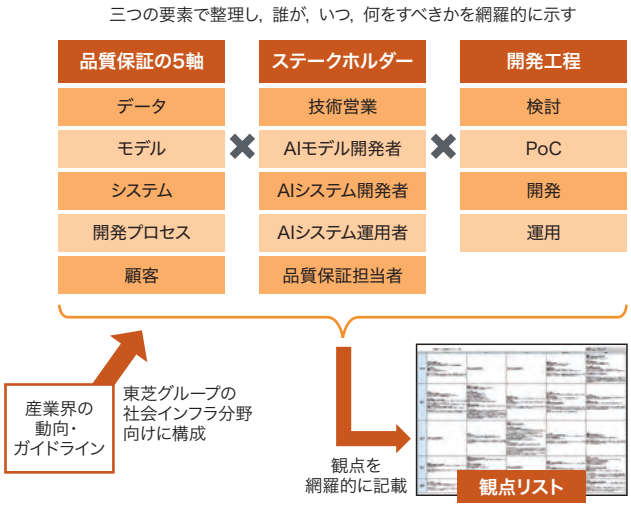
AI搭載システムの品質保証ガイドライン



PoC：Proof of Concept（概念実証）

AI搭載システムの品質保証の考え方
Toshiba Group's approaches to quality assurance for artificial intelligence (AI) systems

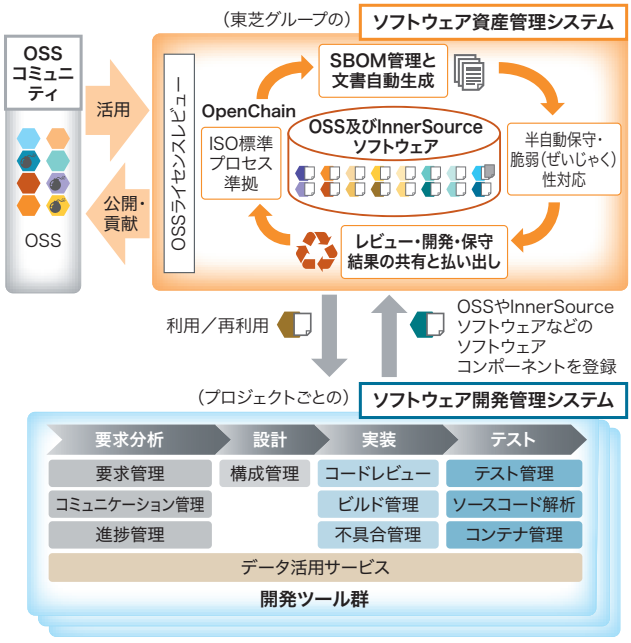
近年，AIを搭載したシステムが増えているが，AIを組み込んだ場合の品質保証方法はいまだ十分には確立していない。大量のデータを元にモデルを構築するAIでは，動作を明確に定義して説明することは容易ではない。このような特徴を持つAIを搭載したシステムに対して，AIプロダクト品質保証コンソーシアムなどの産業界の動向も参考にしつつ，どのように品質保証を行うかを検討し，東芝グループの社会インフラ分野に適合した“AI搭載システム品質保証ガイドライン”を策定した。

このガイドラインでは，評価の対象を示す“品質保証の５軸”，担当者である“ステークホルダー”，及び開発ライフサイクルの時点を示す“開発工程”の三つの要素を整理し，品質保証に必要な観点をリストとしてまとめた。誰が，いつ，何をすべきかを網羅的に示すことで，抜け漏れのない観点で品質保証が可能となった。

今後，このガイドラインを製品開発に適用し，AIを搭載したシステムの品質を向上させる取り組みを進めていく。

ソフトウェア技術センター

ソフトウェアコンポーネントの管理と再利用を促進する共創ソフトウェア開発プラットフォーム



SBOM：Software Bill of Materials

共創ソフトウェア開発プラットフォームのコンセプト
Concept of Toshiba Group's collaborative software development platform

東芝グループのソフトウェア開発効率を向上させるため，次の二つで構成される共創開発プラットフォームを開発した。

(1) ソフトウェア資産管理システム　　共創手段としてオープンソーススタイルによる組織内の開発手法であるInnerSourceの導入を支援し，ソフトウェアコンポーネントカタログとしても機能する。オープンソースコンプライアンスプロセスの国際標準であるISO/IEC 5230:2020（国際標準化機構／国際電気標準会議規格5230:2020）OpenChain Specification(注)に備えたオープンソースソフトウェア（OSS）の管理共有や分析支援が可能となる。

(2) ソフトウェア開発管理システム　　ソフトウェアの開発と運用を連携させたDevOpsの導入を支援する。ウォーターフォールやアジャイルなどの開発プロセスに対応し，開発工程や成果物などを管理できる。

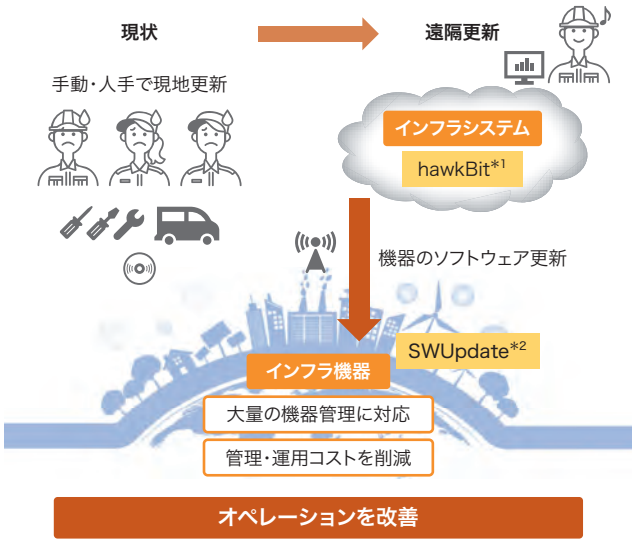
これらにより，ソフトウェアコンポーネントの再利用性の向上と合わせて，コンプライアンスプロセスの効率化が期待できる。

（注）OSSコンプライアンスの一貫した実現を目的とするオープンソースプロジェクト。

関係論文：東芝レビュー，2020，75，5，p.23–26.

ソフトウェア技術センター

Linux® ベースのIoTシステムにおける遠隔ソフトウェア更新技術



＊1：大量の更新対象機器を登録し，ソフトウェア更新を管理制御するOSS
＊2：更新対象機器側でソフトウェアを更新するためのデータ認証・保存・再起動・テストを行うOSS

インフラ機器の遠隔ソフトウェア更新による現地作業の改善
Improvement of on-site work by updating remote software of infrastructure equipment

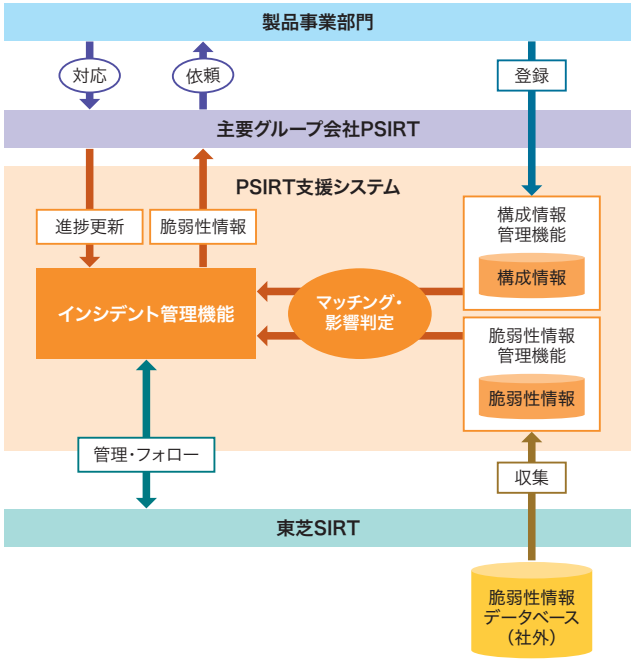
IoT（Internet of Things）システムにおける組み込み機器のソフトウェアは，機能の拡張や脆弱（ぜいじゃく）性への対応のための更新が必要となる。そこで，Linux® をOS（基本ソフトウェア）として用いる組み込み機器の遠隔ソフトウェア更新技術を開発した。

遠隔からのソフトウェア更新を実現するシステムでは，組み込み機器側に，ソフトウェア更新イベントを検知して更新データの取得と認証，更新データでの再起動と起動テスト，及び起動失敗時の復旧処理を自動的に行うソフトウェアを導入する。また，更新ソフトウェアを供給する管理サーバー側には，大量の更新対象機器を管理し，更新データの配布と状態を記録するソフトウェアを導入する。開発した技術により，従来は保守作業員が現地で対応していたソフトウェア更新作業の工数・リソースが削減され，社会インフラにおけるIoTシステムの運用コストの低減とタイムリーなシステムのアップデートが期待される。また，この技術はOSSで実現し，概念実証（PoC：Proof of Concept）を実施した。今後，東芝グループ内のインフラ機器向け遠隔監視システム上での実用化を進めていく。

関係論文：東芝レビュー．2020，75，6，p.68–69.

ソフトウェア技術センター

PSIRT支援システムによる製品セキュリティー対応強化



SIRT：Security Incident Response Team

PSIRT支援システムによる脆弱性対応の自動化・省力化の概要
Overview of automated processes for labor saving to address vulnerabilities in products achieved by product security incident response team (PSIRT) assistance system

東芝グループの製品を使用している顧客のセキュリティーに関する事業リスクを低減するため，製品の脆弱性に迅速かつ確実に対応することが求められる。東芝グループは，近年急増している脆弱性情報に対応するため，PSIRT（Product Security Incident Response Team）支援システムを開発して，運用している。

PSIRT支援システムは，脆弱性対応を自動化・省力化するシステムである。このシステムに製品の構成情報を登録しておくと，脆弱性対策情報データベースJVN iPediaなどで公表された脆弱性情報に該当する製品を自動抽出し，当該製品の担当者に通知される。通知を受けた担当者は，PSIRT担当者と連携を取りながら，脆弱性の製品への影響調査や，対策の実施，公表などの脆弱性対応フローを実施する。各脆弱性への対応状況は，このシステムで一元管理され，ダッシュボードで確認することができる。

東芝グループは開発したPSIRT支援システムを活用して，製品の脆弱性に迅速かつ確実に対応していく。

サイバーセキュリティセンター