



# サプライチェーン全体にわたって機器の透明性を確保します

## 概要

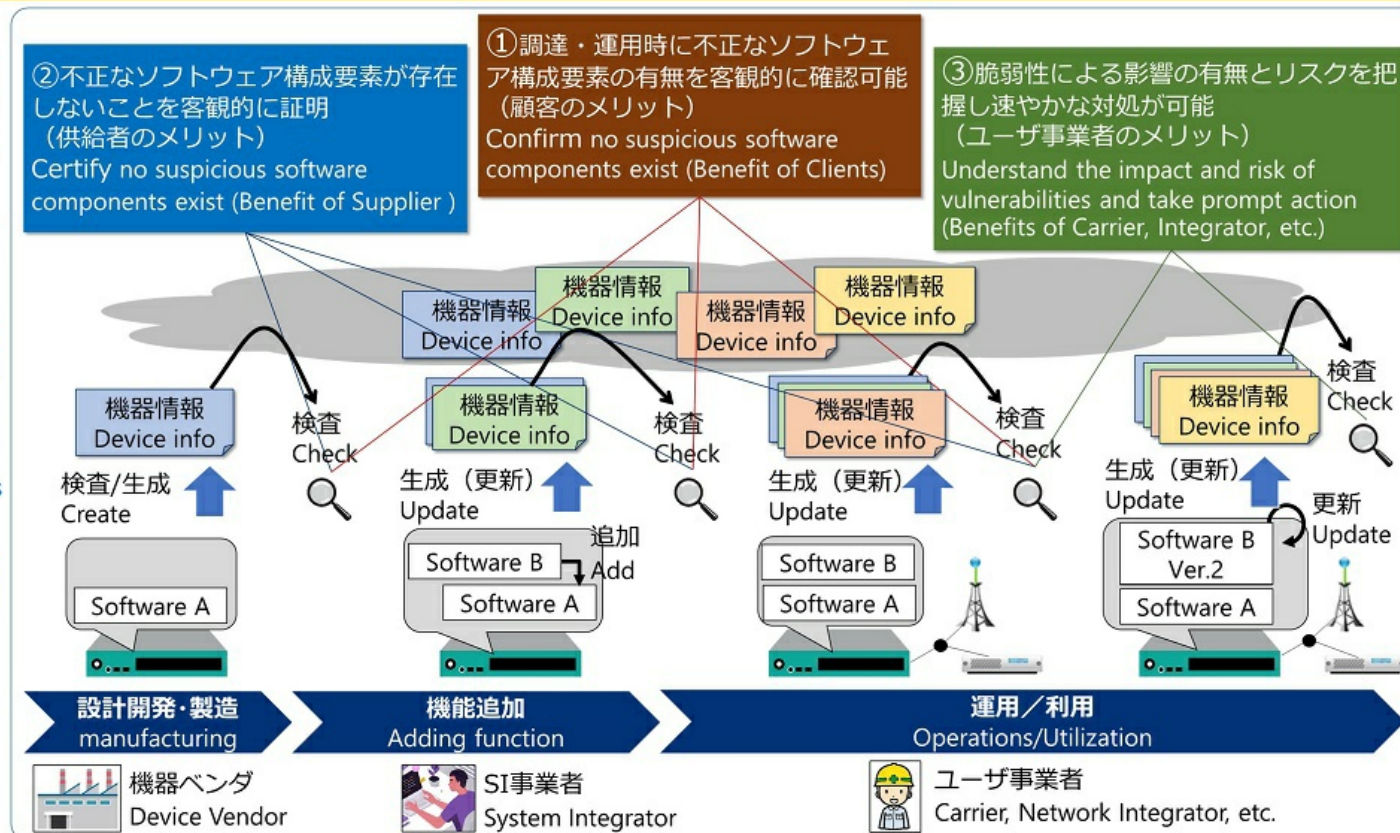
通信機器におけるOSS利用の普及や高機能化に伴い、サプライチェーンリスクが顕在化しています。本技術は、機器の構成やリスクの可視化による透明性の確保と分析により、漏れがなく効率的なセキュリティ管理を実現します。これにより、5G、6G、IOWNなどのネットワークを誰もが安心して利用できる世界をめざします。

### STT : Security Transparency assurance Technology (セキュリティトランスペアレンシー確保技術)

通信機器の「構成」「リスク」を可視化した機器情報を生成し、サプライチェーン全体にわたる共有により抜本的にセキュリティ向上を図る技術  
STT radically improve security by generating device info that visualizes the "configuration" and "risks" and sharing it throughout the supply chain.

#### 従来の問題点 Problems

- ① 調達や構築の依頼者は、機器内の不正なソフトウェア構成要素の有無の確認が困難なため、採用可否を企業のブランドや信用に依存している  
It is difficult for Clients to check for suspicious software on the devices, so they make a purchase decision based on corporate brand or trust.
- ② 供給者は機器の安全性を証明することが難しく、事業者として信用がなければ機器を調達してもらえない  
It is difficult for Suppliers to prove the safety of devices and devices they manufactured are not purchased unless they are trusted.
- ③ ユーザ事業者は、脆弱性が発見された際に速やかに気づき、その内容に応じて適切に対処を行うことが難しい  
It is difficult for Carriers and Network integrators to become aware of the impact of newly discovered vulnerabilities on their devices and to take appropriate action based on risk.



## 特徴

- 機器の製造から運用までの各フェーズで機器情報を生成し、機器の構成やリスクを可視化
- 機器情報を用いることで、正確かつ漏れのないリスク分析を実行可能

## 利用シーン

- 機器の調達時に不正なソフトウェア構成要素の有無を確認する
- 新たに発見された脆弱性による影響を確認し素早い対処を行う

## 今後の展開

- ローカル5G設備などにおける試験運用を通してセキュリティトランスペアレンシー確保技術の有効性を確認し、コンソーシアムを立ち上げ、技術仕様の普及を図っていきます。

## コラボレーションパートナー

- 日本電気株式会社

## 出展社

- 日本電信電話株式会社

問い合わせ先 : rdforum-sv-ml@hco.ntt.co.jp