Open RAN推進分科会 第４回

Fujitsu's Open RAN Activities

Naoto Sato
Head of Mobile Solution Business Div.
Fujitsu Limited

December 12, 2022

FUJITSU

1. **Advancement of network operation and management**
   - Responding to increasing network complexity and power consumption
2. **Security Initiatives**
   - SBOM Management

Obstacles… in front of ORAN market

FUJITSU

Obstacles to accelerating ORAN adoption ： Operation

Complexity, difficulty, expertise, diversity of stakeholders, etc.

- **Minimal resource control for QoS/QoE & UX/CX satisfaction**
- **Flexible control of resources following changes in service and content characteristics**
- **Cloud native-oriented security technology for virtualization, software and openness**
- **Integration ： Enhanced system availability and resiliency**

1. Advancement of network operation and management

- Responding to increasing network complexity and power consumption

01

2. Security Initiatives

- SBOM Management

02

Network Operations Management Challenges in 5G

FUJITSU

Responding to the growing complexity of operational management due to the diversification of network usage patterns

Dynamic movement of NW resources for sudden events is often difficult to deal with manually

Dynamic control of resources over small time periods is difficult with human hands

Increasing power consumption of 5G NW is a major issue from the viewpoint of reducing greenhouse gas emissions

The installation of many radio equipment is required, and the power consumption increases. NW's global power consumption is projected to increase to 490 TWh in 2018 and 2,400 TWh in 2030 [1]

1. Japan Science and Technology Agency https://www.jst.go.jp/lcs/pdf/fy2020-pp-04.pdf

Advanced RAN operation and management at Fujitsu

FUJITSU

Proactive, automated RAN optimization addresses the growing complexity of network operations management and power consumption

QoE: Quality of Experience

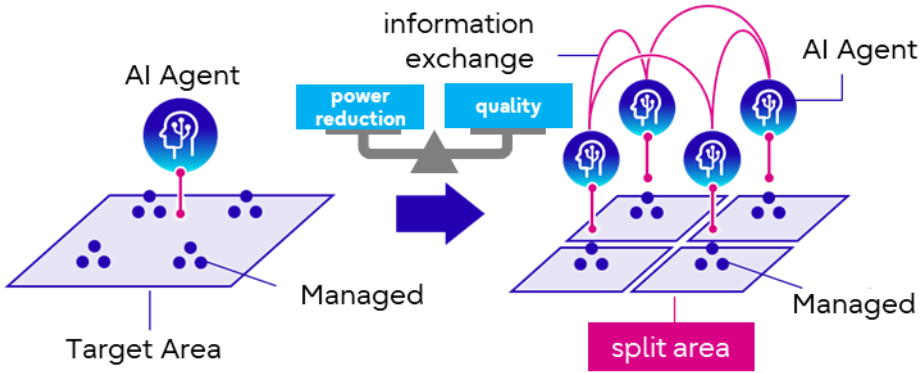
- Predict Quality of Service (QoS) degradation in networks that are difficult for humans to detect
- Automate analysis and remediation of quality degradation causes

- Response to quality degradation felt by users that could not be detected by QoS indicators
- Assign resources to other services that are used for excessive quality that users cannot perceive.

Maintaining Quality of Service and Conserving Energy

Fujitsu's Advanced AI Technology Supports RAN Operations

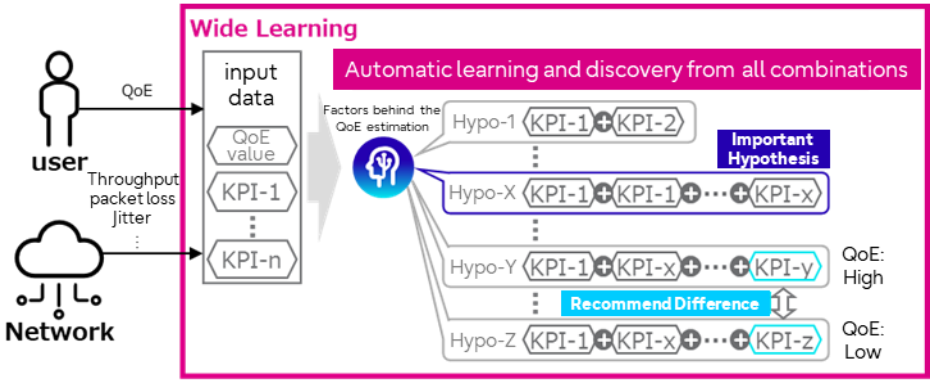
PeACE-RL*



- Achieve multiple KPIs simultaneously while reducing coordination and validation effort
- By dividing the area, the processing amount per area is reduced and the speed is increased.
- The agents in each area work together to optimize the entire system.

* Performance-level Assured Cooperative and Efficient Reinforcement Learning

Wide Learning™



- It is possible to derive important hypotheses that influence QoE estimation and to construct a highly explanatory model
- If the QoE estimation results fluctuate, recommend the combination of input data of the hypothesis that caused the difference as a hint for solution.

Creating New Value for the Network

Network × AI → Creating New Value

Network

- Evolution from 5G to 6G
- Openness
- Environmental considerations

Creation of new network value

AI

- Extensive examples of real-world applications
- Utilization of all kinds of data

Diversification of network usage patterns

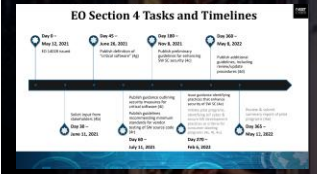
1. Advancement of network operation and management
   - Responding to increasing network complexity and power consumption

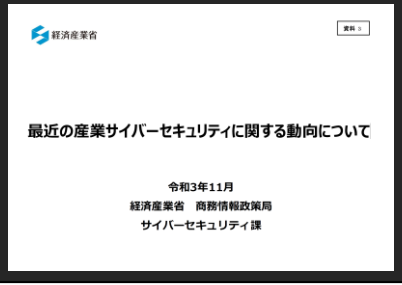
01

2. Security Initiatives
   - SBOM Management

02

Executive Order 14028




経済産業省

最近の産業サイバーセキュリティに関する動向について

令和3年11月
経済産業省　商務情報政策局
サイバーセキュリティ課

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

1 官民の脅威情報共有における障害の除去 (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにした上で、特定のインシデント情報の共有を義務づける。
2 連邦政府におけるより強力な標準の近代化と導入 (Section 3)	● FedRAMP改定等を通じて、**連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援**し、多要素認証と暗号化の導入を義務づける。
3 ソフトウェア・サプライチェーンのセキュリティ向上 (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づける**。 ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。
4 サイバー安全審査委員会の創設 (Section 5)	● 国土安全保障省は、**重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置**し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 インシデント対応のための標準プレイブックの策定 (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 調査及び修復能力の向上 (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

（出典）各種公開情報より作成

6

【米国】ソフトウェア検証の最低基準に関するガイドラインの公表

- 大統領令を受け、NISTは、**ソフトウェア検証の最低基準に関するガイドラインを7月9日に公開**した。
- ガイドラインでは、**ベンダーや開発者によるソフトウェア検証の際に推奨される、11の最低基準**が示されている。
- 最低基準は、実行可能なコンピュータプログラムすべてに推奨され、**将来的には、ソフトウェアベンダーや開発者に対する強制基準の基礎となりうる**ことが明記されている。

ソフトウェア検証において推奨される11の最低基準

1. 脅威分析 ソフトウェア開発の早期に脅威分析を実施し、設計段階でのセキュリティ問題を特定する。	**5. チェック機能・保護機能を用いたプログラム実行** 開発中や完成後のソフトウェアに対して、プログラム言語のビルトインチェック機能や保護機能を用いてプログラムを実行する。	**9. ファジングテスト** 入力値を自動で大量生成するツール（ファザー）を使用して、ファジングテストを実行する。
2. 自動化ツールの使用 静的解析及び動的解析の一部の検証において、自動化ツールを活用する。	**6. ブラックボックステスト** セキュリティで重要とされている範囲を包括的にカバーしたテストケースに基づき、ブラックボックステストを実施する。	**10. Webアプリケーションのスキャン** ソフトウェアがWebサービスを提供する場合は、Webアプリケーションをスキャンする動的解析ツールやIASTツール※を使用して脆弱性を検出する。
3. ソースコードに対する静的解析 静的解析ツールを使用してソースコードの解析を行い、様々な種類の脆弱性を検出する。解析は、ソースコード作成直後に行う。	**7. コードベーステスト（ホワイトボックステスト）** ソースコードの仕様に基づいたホワイトボックステストを行う。ほとんどのコードに対して、単体テストの時点で実行する必要がある。	**11. コンポーネントの監視** ソフトウェアに含まれているコンポーネント（OSS等の外部ソース含む）は、脆弱性データベース等を活用して、その脆弱性を継続的に監視する必要がある。
4.ハードコードされたクレデンシャル情報の確認 ハードコードされたパスワードや暗号鍵等がないかを確認するために、静的解析ツールや手動レビューにより確認する。	**8. 回帰テスト** 以前にテストしたソフトウェアが、変更後もまだ動作するかどうかを、再度実行して確認する。	■ 脅威分析に関する基準　■ 静的解析に関する基準 ■ 静的解析・動的解析の両方に関する基準　■ 動的解析に関する基準 ■ コンポーネントの脆弱性に関する基準

※：Interactive Application Security Testingの略で、実際に動作しているアプリケーションのデータフローを解析し、脆弱性の検出を行うテスト手法のこと。

出所）NIST, "Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

8

Ministry of Economy, Trade and Industry
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/003_03_00.pdf

Security Initiatives SBOM 1/2

【米国】SBOMの「最小要素」の定義

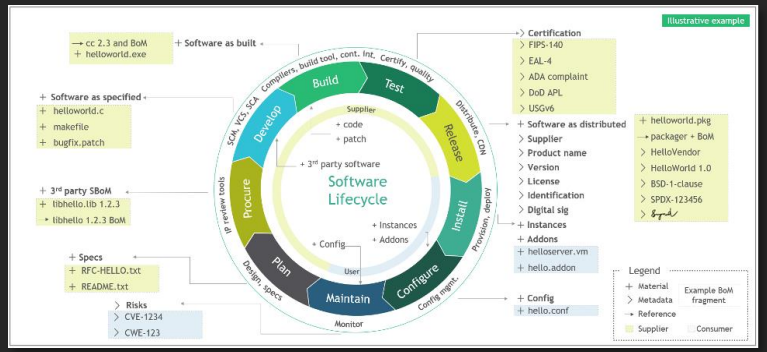
- 大統領令を受け、NTIAは当該定義に関するパブリックコメントを実施。**ソフトウェア関連の企業や専門家からの意見を踏まえ、SBOMの「最小要素」の定義を7月12日に公開**した。
- SBOMの「最小要素」には、**「データフィールド」、「自動化サポート」、「プラクティスとプロセス」**の3つのカテゴリが含まれ、**コンポーネントを一覧化した部品表に含まれる情報だけでなく、SBOMの利用者が実施すべき事項**も規定されている。
- 定義された「最小要素」に基づき、**ソフトウェア購入者へのSBOM提供に関するガイダンスが整備**されるほか、将来的には、**各省庁のソフトウェアに関する取組が本定義に基づき実施される**ことが明記されている。

3つのカテゴリ	「最小要素」の概要	「最小要素」の具体的な定義
データフィールド (Data Fields)	各コンポーネントに関する基本情報を明確化すること	以下の情報をSBOMに含めること。 • サプライヤー名 • 依存関係 • コンポーネント名 • SBOMの作成者 • コンポーネントのバージョン • タイムスタンプ • その他の一意な識別子
自動化サポート (Automation Support)	SBOMの自動生成や可読性などの自動化をサポートすること	SBOMデータは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWIDタグを用いること。
プラクティスとプロセス (Practices and Processes)	SBOMの要求、生成、利用に関する運用方法を定義すること	SBOMを利用する組織は、以下の項目に関する運用方法を定めること。 • SBOMの作成頻度 • SBOMの共有 • SBOMの深さ • アクセス管理 • 既知の未知 • 誤りの許容

出所）NTIA, "The Minimum Elements For a Software Bill of Materials (SBOM)"
https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

9

Ministry of Economy, Trade and Industry
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/003_03_00.pdf



NTIA Illustrative Example of
Software Life Cycle and Bill of Materials Assembly Line

5G CHALLENGE

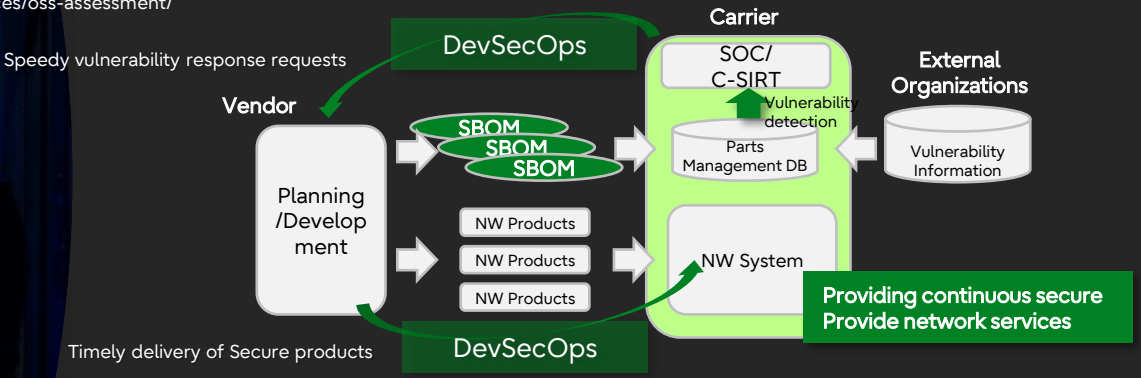
https://www.ntia.doc.gov/5g-challenge

Security Initiatives SBOM 2/2

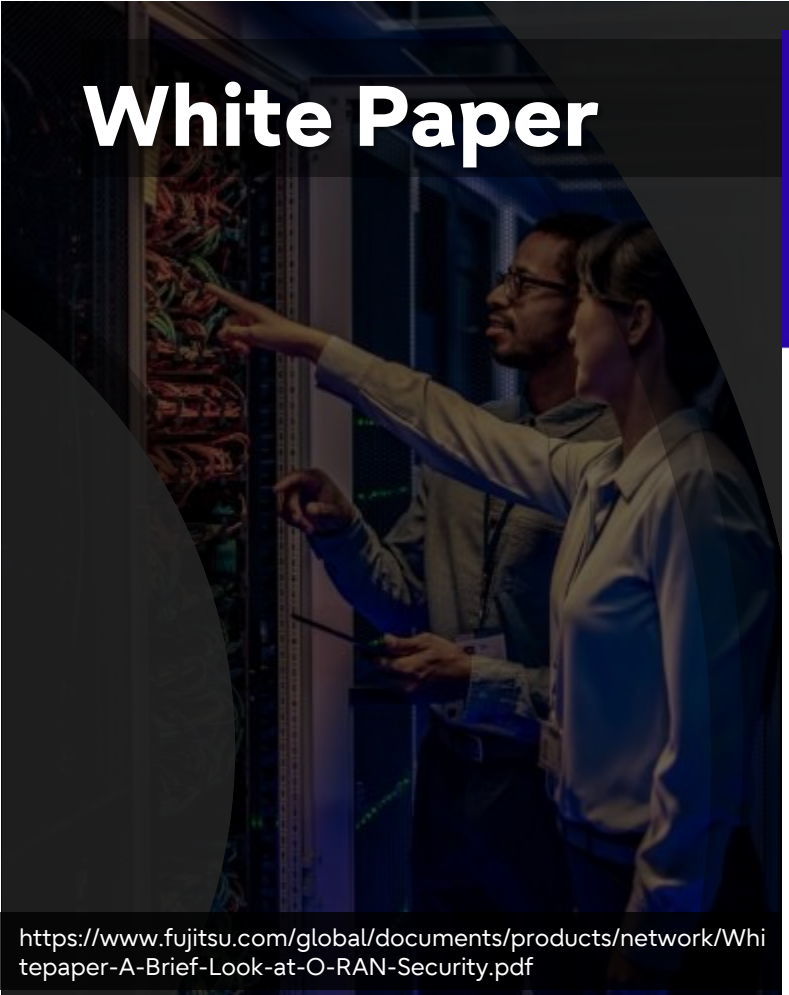
OSS Assessment Support Services

Classification	List	Outline of Support
SBOM operational support	SBOM Creation	In accordance with the customer's OSS utilization policy, we will create a policy regarding the fulfillment of license obligations and support license clarification and SBOM creation with a license scanner.
	SBOM management system construction	Based on the customer's development environment and other factors, we will support the creation of a DevSecOps environment according to the customer's needs with a set of tools necessary for vulnerability monitoring
	Virtual Security Operation Center (vSOC) construction	We will monitor vulnerability information related to SBOM's OSS, determine whether or not the information is relevant, and support the analysis and preparation of a response plan using the client's contracted vulnerability monitoring tool.

https://www.fujitsu.com/jp/products/software/os/linux/products-services/oss-assessment/



White Paper



https://www.fujitsu.com/global/documents/products/network/Whitepaper-A-Brief-Look-at-O-RAN-Security.pdf

A Brief Look at O-RAN Security
White Paper

FUJITSU

Executive Summary

The paper presents a brief history of O-RAN alliance and outlines its goals and vision [1]. Then O-RAN security working group and its specifications are introduced, and its objectives and approach are reviewed. Architectural component of O-RAN and security solution for each component is addressed in some detail. Next a few key security features of the O-RAN architecture are highlighted. Security testing objectives, types and procedures are also described. Lastly, Fujitsu's viewpoint on security is described. The presentation showcases how the use of technology, processes and best practices result in a secure solution for 5G networks.

1 O-RAN Alliance

O-RAN was formed by the merger of the C-RAN Alliance and the XRAN Forum in 2018. The C-RAN alliance consisted of China Mobile and many other Chinese vendors, while the XRAN Forum was formed by US, European, Japanese, and South Korean vendors and operators. The founding operators of the O-RAN Alliance were AT&T, China Mobile, Deutsche Telekom, NTT Docomo and Orange. Since then, many other operators, vendors, integrators, and academic institutions have joined the alliance. Today ORAN Alliance eco system consists of over 340 companies and institutions across the world. The Alliance's vision is to enable open, virtual, intelligent and interoperable radio access networks resulting in faster innovation cycles, efficient mobile networks and competitive supplier eco system which benefits both customers and mobile operators [1].

O-RAN alliance develops access O-RAN specifications, releases open-source code in conjunction with Linux foundation and supports companies in testing and integration of their O-RAN implementations. There are currently a total of 11 technical working groups developing through the entire system. O-RAN addresses the security for every component of the system such as individual interfaces and functions. Above and beyond that, security for the entire end-to-end system as the information flows into and out of the system is investigated as well. It is noteworthy that O-RAN benefits from 5G advanced security features as it is built on 3 GPP's architecture. In the remainder of this section, security measures for various components of O-RAN are addressed.

2.1 Near-RT RIC

The Near-Real Time RAN Intelligent Controller (Near-RT RIC) is a virtual function introduced by O-RAN which adds programmability to radio access networks and is designed to enable optimization and control of radio access network elements by utilizing AI/ML schemes. The three interfaces associated with it are E2 interface as well as A1 and O1 open interfaces. xApp micro service-based applications consisting of one or more micro services run on Near-RT RIC. Association between xApp and RAN functionality is made through E2 interface. The security issues related to

Thank you