組込みシステムセキュリティ委員会
取組み紹介

組込みシステムセキュリティ委員会
副委員長 牧野 進二

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

JASA活動実績
IoTセキュリティの国際安全基準適合の認証支援

セキュアIoTプログラム(認証支援)

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

1．セキュアIoTプログラム(認証支援)

ガイドライン等の実効性の強化

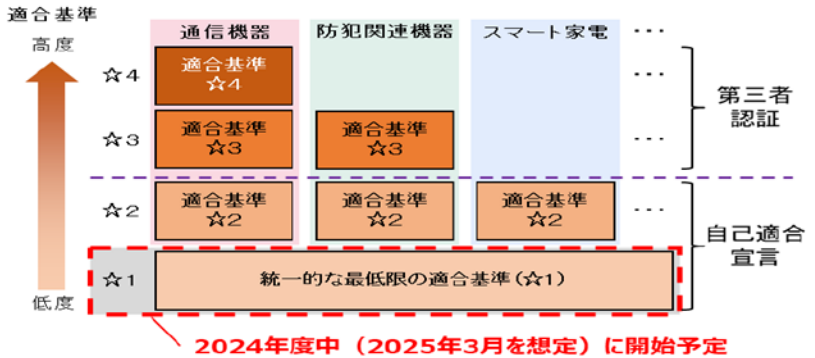
実効性強化

（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

- セキュリティ対策レベルを評価し、それを可視化する取組の**先行例として、IoTセキュリティ適合性評価制度を検討中**。**米欧等の諸外国との制度調和を図るための議論も継続中**。
- また、**SBOM（ソフトウェア部品構成表）**導入時の課題検証のための実証や企業向けの手引書を策定。
- IoTセキュリティ適合性評価制度の実効性強化やSBOMの導入促進に向けては、**産業界との連携のほか、政府調達等の要件化等に向けて関係省庁と議論も開始**。
- さらに、米国が策定し、我が国政府も共同署名をしたセキュア・バイ・デザインのガイダンスも踏まえ、**ソフトウェア開発者が行うべき取組整理**や**安全なソフトウェアの自己適合宣言の仕組みの検討**を行っていく。

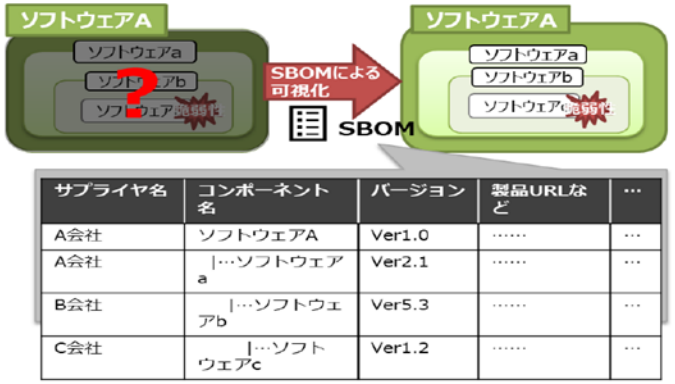
IoTセキュリティ適合性評価制度

- 幅広い**IoT製品を対象**として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、**2024年度中に一部運用を開始**予定。



SBOMのイメージ

- **SBOM（ソフトウェア部品構成表）**がソフトウェアのセキュリティの脆弱性を管理する手法の一つとして着目。



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

セキュアバイデザイン・セキュアバイデフォルト

- **セキュア・バイ・デザイン**：IT製品（ソフトウェア等）が、設計段階から安全性を確保されていること。
- **セキュア・バイ・デフォルト**：ユーザーが、追加の手間をかけることなく、購入後すぐにIT製品（ソフトウェア等）を安全に利用できること。

（出典：国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」）（2023年10月28日署名）

1．セキュアIoTプログラム(認証支援)

- 「脆弱性検査およびIoTセキュリティ検査」とIoTシステムに求められるセキュリティ要件を以下の点に絞り込み、国際標準への適合性を確認する「セキュアIoT認定」を組合わせたIoT機器のセキュリティ適合性評価基準を満たすプログラム
- 産業用システム、業務システム、コンシューマ機器における最終的なIoT機器だけではなく、IoT機器を構成する部品やソフトウェア、システムも認定対象（対象となる機器に求められるセキュリティレベルにより、１～４までのクラスを設定）
- セキュアIoTプラットフォーム協議会が発行する[IoTセキュリティ手引書」を認定基準(IEC62443、SP-800シリーズなどセキュリティ国際安全基準/ガイドラインの参照し策定）として検査
- JASA / SIOTP協議会が運営事務局,認定機関となり、登録指定検査事業者により、申請された事業者のIoT機器の検査実施、結果を[セキュアIoT認定」として認定

セキュアIoTプログラム

IoTセキュリティ検査

●検査項目：ライフサイクル管理
- ・真正性の担保 (鍵管理、ROT)
- ・認証と識別
- ・セキュアアップデート (OTA)

✓ 対象となるIoTシステムに求められるセキュリティ強度によりclass1～4の基準を選択し、適合する検査を実施 *

脆弱性検査

- ・ソースコード解析
- ・ファームウェア解析
- ・ネットワークスキャン
- ・既知脆弱性診断　など

セキュアIoT認定

●認定基準

✓ 一定基準の「脆弱性検査」をクリア
- ・Bronze: 80%以上
- ・Silver: 90%以上
- ・Gold: 95%以上

✓ 加えてGoldの場合は、該当するclassの「IoTセキュリティ検査」要件クリア

セキュアIoT認定

認定有効期間: 5年間
発行物: 認定証書、認定マーク

＊ 認定対象の利用用途や目的によって適切なclassを認定機関が決定します。

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

1．セキュアIoTプログラム(認証支援)

Secure IoT Platform Consortium

IoT機器適合性評価事業「セキュアIoTプログラム」における共同運営

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

IEC62443をはじめとする国際標準やSP800シリーズなどのセキュリティ規格が定められ、調達基準としても採用され始めているが、取得のためには莫大の費用と長期の検証期間がかかるため適合できるのが一部の大手企業に限定されるのが現状である。

「IoTセキュリティ手引書」をベースに「脆弱性検査およびIoTセキュリティ検査」とIoTシステムに求められるセキュリティ要件を以下の点に絞り込み、国際標準(IEC62443)への適合性を確認する「セキュアIoT認定」を組合わせたプログラムを発表。

【検証ポイント】

- **ライフサイクル管理**
  - **真正性の担保 (鍵管理、ROT：Root Of Trust)**
  - **認証と識別 (設計・製造、利用、廃棄、リサイクル)**
  - **セキュアアップデート (OTA：Over The Air)**

セキュアIoT認定

セキュアIoTプログラム

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

JASA活動実績
IoTセキュリティ教育事業の展開

JASA版 IoTセキュリティ教材

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

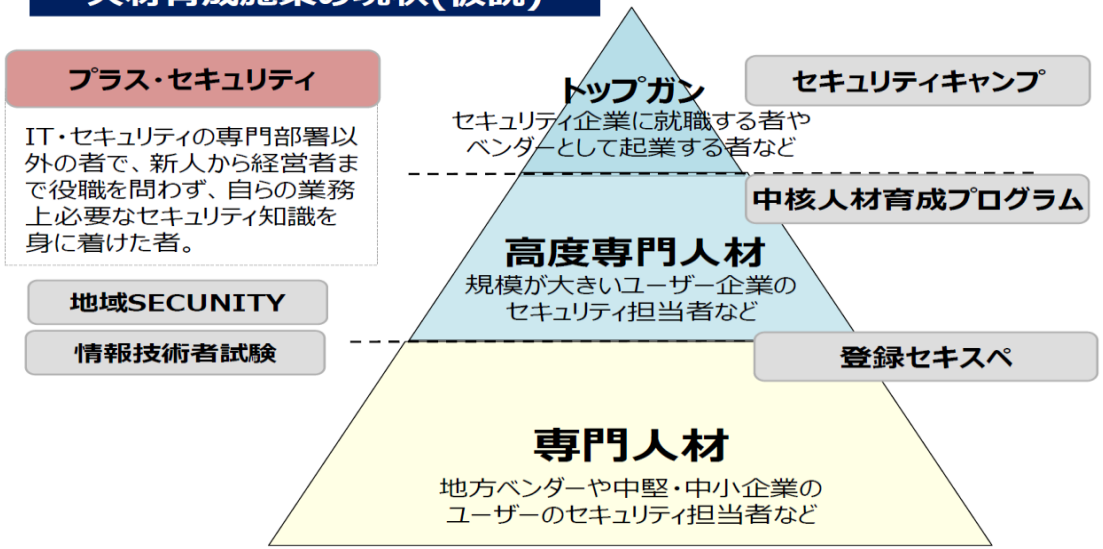
2．JASA版 IoTセキュリティ教材

サイバーセキュリティ人材の育成・確保に向けた取組の方向性

供給力強化

- セキュリティ市場の拡大に向けたエコシステムを構築するためには、産業・技術基盤の維持・発展を支える供給側、セキュリティ対策を実装する需要側、**双方の基盤となる人材の育成・確保が重要**。
- しかし、NRIセキュアの調査（※1）によると、日本においては、従業員規模に関わらず**９割の企業でセキュリティ人材が不足していると回答**。またISC2の調査（※２）によると国内のサイバーセキュリティ人材は現在約48万人存在しているが、**11万人不足**。
- セキュリティ人材施策として、セキュリティキャンプや中核人材育成PG、情報処理安全確保支援士試験を通じた**高度専門人材の育成**、地域SECUNITY活動等を通じた**プラス・セキュリティの普及**等を進めてきているが、**需給ギャップを解消するためには、セキュリティ人材の裾野を更に拡大するための施策の検討が必要**。
- また、NISC改組後の「新たな組織」を含む**政府機関等において十分なセキュリティ人材を確保する**ことにより、政府全体でのサイバー安全保障分野での対応能力を向上につなげることも重要。こうしたセキュリティ人材が、産業界に留まることなく、**政府と民間との間でより活発に行き来できるようにする**ことも必要ではないか。

人材育成施策の現状(仮説)



現状の課題

- これまで、トップガンや高度専門人材の育成は進めてきたものの、1年間に育成できる人数が限定的。
- 登録セキスペは、首都圏のベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- これまで施策では、地方ベンダーや中堅・中小企業のユーザーのセキュリティ担当者などにアプローチできない。

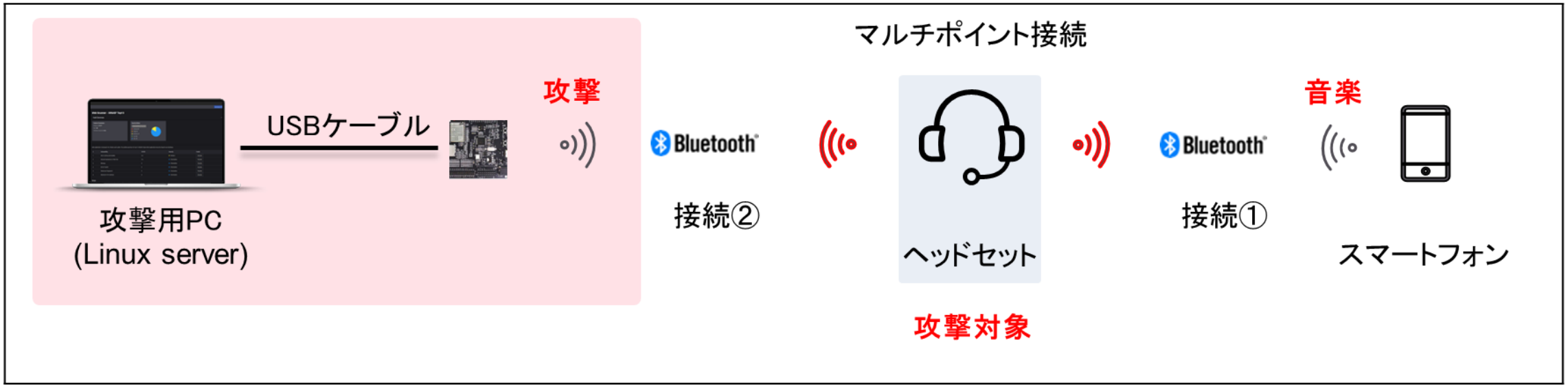
今後の方向性

- トップガンの発掘・育成及び事業化促進に向けてセキュリティキャンプの拡張及び未踏事業との連携を検討。
- ユーザー企業における登録セキスペの活用を促進（中小企業等とのマッチング実証事業、DX促進施策との連動等）するとともに、制度の見直しも検討。これらを通じて、**登録人数**（2024年４月現在、約2.3万人）**を2030年までに５万人まで増加を目指す**。
- 専門人材の育成に関する課題整理を行うとともに、基礎知識・スキル習得できるような環境整備に関する検討を実施。

※１　NRI Secure Insight 2023
※２　ISC2 Cybersecurity Workforce Study 2023

2．JASA版 IoTセキュリティ教材

■ 演習教材の開発、公開



Bluetooth機器を使ったセキュリティ演習教材

申し込み用のQRコード

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

2．JASA版 IoTセキュリティ教材

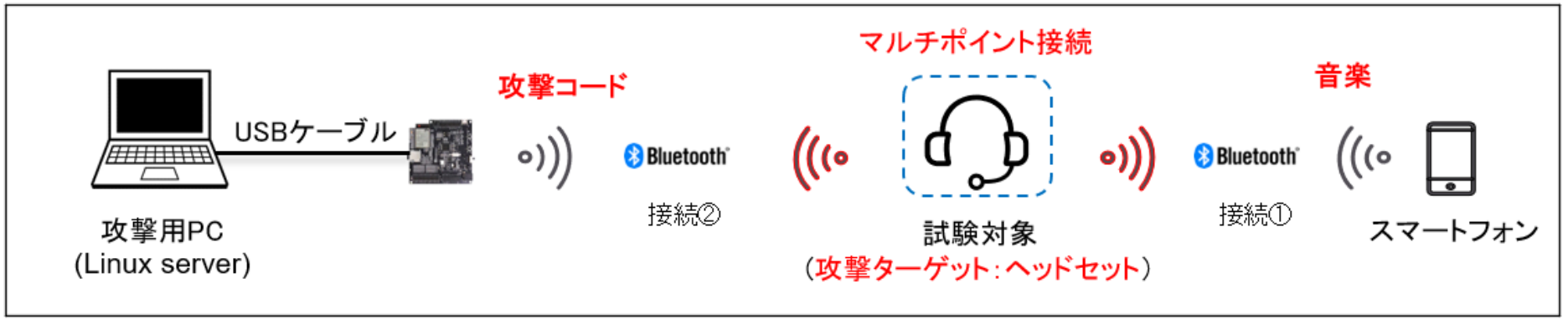
演習3　チーム毎に攻撃ターゲットを実際に検証してみよう②

3-1.ヘッドセットのマルチポイント接続機能を使ってみましょう

3-2.ヘッドセットのデバイス名から、既知の脆弱性があるか検索して攻撃コード（Exploit）を特定しましょう

3-3.攻撃コード（Exploit）を実行し、どのような被害が生じるのか確認してみましょう

3-4.実施の結果、試験レポートからどのような情報が取得できるか確認しましょう



申し込み用のQRコード

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

サイバーセキュリティ動向 SBOMの活用

～委員会の取組みとSBOM動向の紹介～

2024/11/22

キーサイト・テクノロジー株式会社

千徳 仁

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

Application Security Testing（AST）

✓SAST（Static Application Security Testing：静的解析）

・ソースコード解析

・バイナリ解析

・**ソフトウェアコンポジション解析（SCA）**　☞SBOM（Software Bill of Materials：ソフトウェア部品表）

・ソースコードを利用した手法

・バイナリデータを利用した手法

☞本日は主に、組み込み機器に対するファームウェアのSBOMについてお話します（バイナリ解析）

✓DAST（Dynamic Application Security Testing:動的解析）

・ファジング

・脆弱性スキャン

★SASTとDASTの結果を悪用した「ペネトレーションテスト」

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

SBOMとは何か？

✓Software Bill of Material（SBOM）は、ソフトウェア製品や
アプリケーションで使用されるすべてのコンポーネント
（オープンソース商用の両方）の詳細なリストまたは在庫表です。

✓SBOMの各項目には、コンポーネントのバージョン、
ライセンス、出所、既知の脆弱性などの詳細が含まれています。

✓SBOMは、ソフトウェアのサプライチェーン全体を理解し、
セキュリティとコンプライアンスを確保するために不可欠です。

なぜSBOMは重要か？

セキュリティ: ソフトウェアのコンポーネントを把握することで、脆弱性を迅速に特定することができます。

コンプライアンス: 各コンポーネントのライセンス条件を把握することで、法的義務の管理に役立ちます。

リスク管理: 各コンポーネントがシステム全体に与えるリスクを評価するのに役立ち、特にセキュリティ侵害が発生した場合に有効です。

サプライチェーンの透明性: ソフトウェアのサプライチェーンへの可視性を向上させ、不正な改ざんや悪意のあるコンポーネントの検出を容易にします。

SBOM 標準

	SPDX	CycloneDX	SWID
主な焦点	ライセンス、コンプライアンス	セキュリティ、脆弱性管理	ソフトウェア資産の追跡
対象者	法務チーム、コンプライアンス担当者	セキュリティ専門家	IT資産管理者 ソフトウェアベンダー
フォーマット	JSON、XML、YAML、RDF、タグ値	JSON、 XML	XML
採用者	オープンソース、法務部門	セキュリティチーム、DevSecOps	ソフトウェアベンダー 資産管理チーム
ユースケース	ライセンスコンプライアンス	脆弱性追跡、依存関係管理	ソフトウェアインストールの追跡
国際標準	ISO/IEC 5962:2021	ISO認証未取得 広く採用されている	ISO/IEC 19770-2:2015

SBOM関連の規制および標準～欧州～

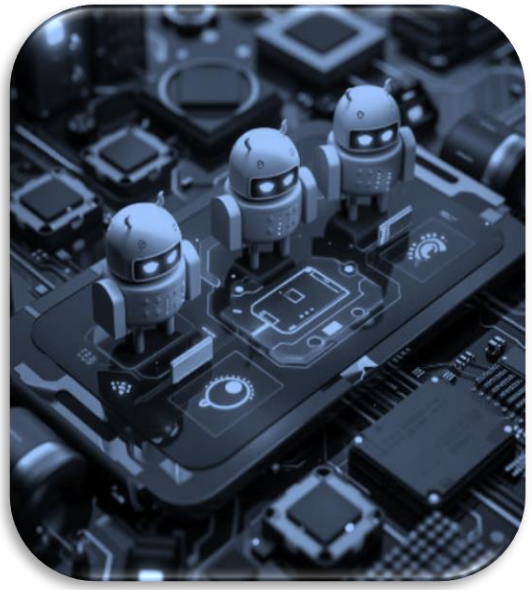
規制/標準	地域/範囲	SBOM 要件/焦点
U.S. Executive Order 14028	アメリカ合衆国	政府および重要なソフトウェアに必要
NIST SP 800-218 (SSDF)	アメリカ合衆国	安全なソフトウェア開発のためのベストプラクティス
EU Cyber Resilience Act	欧州連合（審議中）	デジタル製品向けのSBOM要件（提案）
FDA Medical Device Guidelines	アメリカ合衆国（医療）	医療機器の市場前承認のためのSBOM
HSCC Practice Guide	アメリカ合衆国（医療）	医療および医療機器向けに推奨
CISA Guidance for Critical Infrastructure	アメリカ合衆国	重要インフラ分野向けに推奨
ISO/SAE 21434	国際	車両向けに推奨
DOE SBOM Pilot Program	アメリカ合衆国（エネルギー）	ユーティリティおよびグリッドソフトウェア向けのパイロットプログラム
OpenChain ISO/IEC 5230	国際	オープンソースライセンスコンプライアンスのためのSBOMを推奨

SBOM関連の規制および標準～APAC～

国/地域	規制/フレームワーク	SBOM 関連性
シンガポール	Cybersecurity Labelling Scheme (CLS)	高いコンプライアンスレベルでIoTセキュリティ向けにSBOMを推奨
日本	Cyber/Physical Security Framework (CPSF)	重要分野のサプライチェーンセキュリティ向けにSBOMを推奨
オーストラリア	Critical Infrastructure Act, Cybersecurity Strategy	重要インフラセキュリティ向けにSBOMを推奨する可能性
インド	Data Protection Bill, CERT-In Guidelines	重要および規制分野でSBOMの推奨が増加
中国	Cybersecurity Law, Multi-Level Protection Scheme (MLPS) 2.0	SBOM原則に沿ったサプライチェーンの透明性を推奨
韓国	Software Supply Chain Security Guidelines 1.0	高リスク分野（金融、医療）でのSBOM導入が予想される

低消費電力化する組込み機器

The
2 Firmware Types



Operating System-based Firmware

✓Linux、Android、FreeRTOS上に構築
✓複雑なIoTデバイスに適している

Bare Metal Firmware

✓OSなしでハードウェア上で直接動作する
✓シンプルなデバイスに最適

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

進化するソフトウェアの開発環境と配布

✓サーバーレスコンピューティング

・クラウド上でビルドプロセスや依存関係の解決が自動化され、ブラックボックス化されやすい

・最終的なバイナリには、ビルドプロセス中に導入された変更が含まれる可能性がある

Binary Analysis

✓コンテナ化

・開発効率の向上を目指し、再ビルド不要なコンテナイメージの利用が増加

✓プリコンパイル済みライブラリ

・開発効率の向上を目指し、サードパーティ製のライブラリの利用が増加

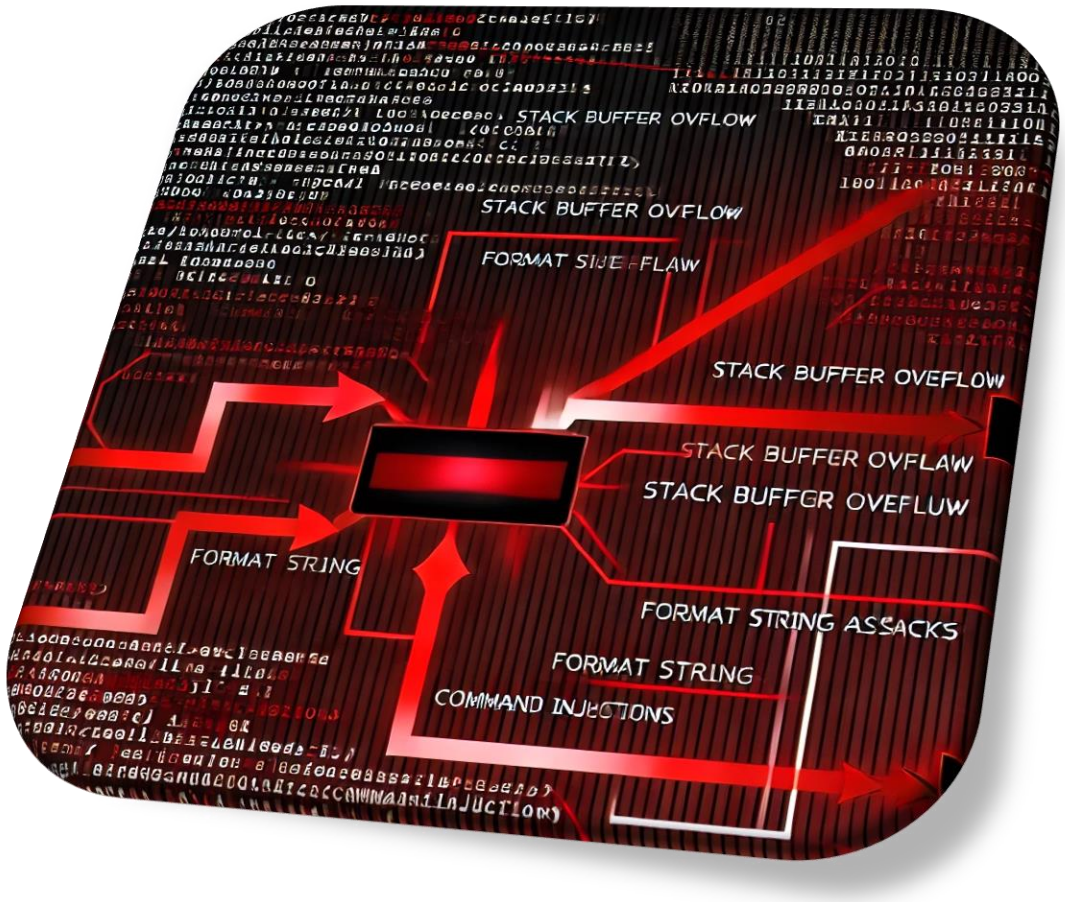
バイナリ解析とは

✓**ソースコードは不要**: バイナリ解析は、元のソースコードに依存しないため、ソースコードが利用できない場合（サードパーティのライブラリやプロプライエタリソフトウェアなど）にも有用です。

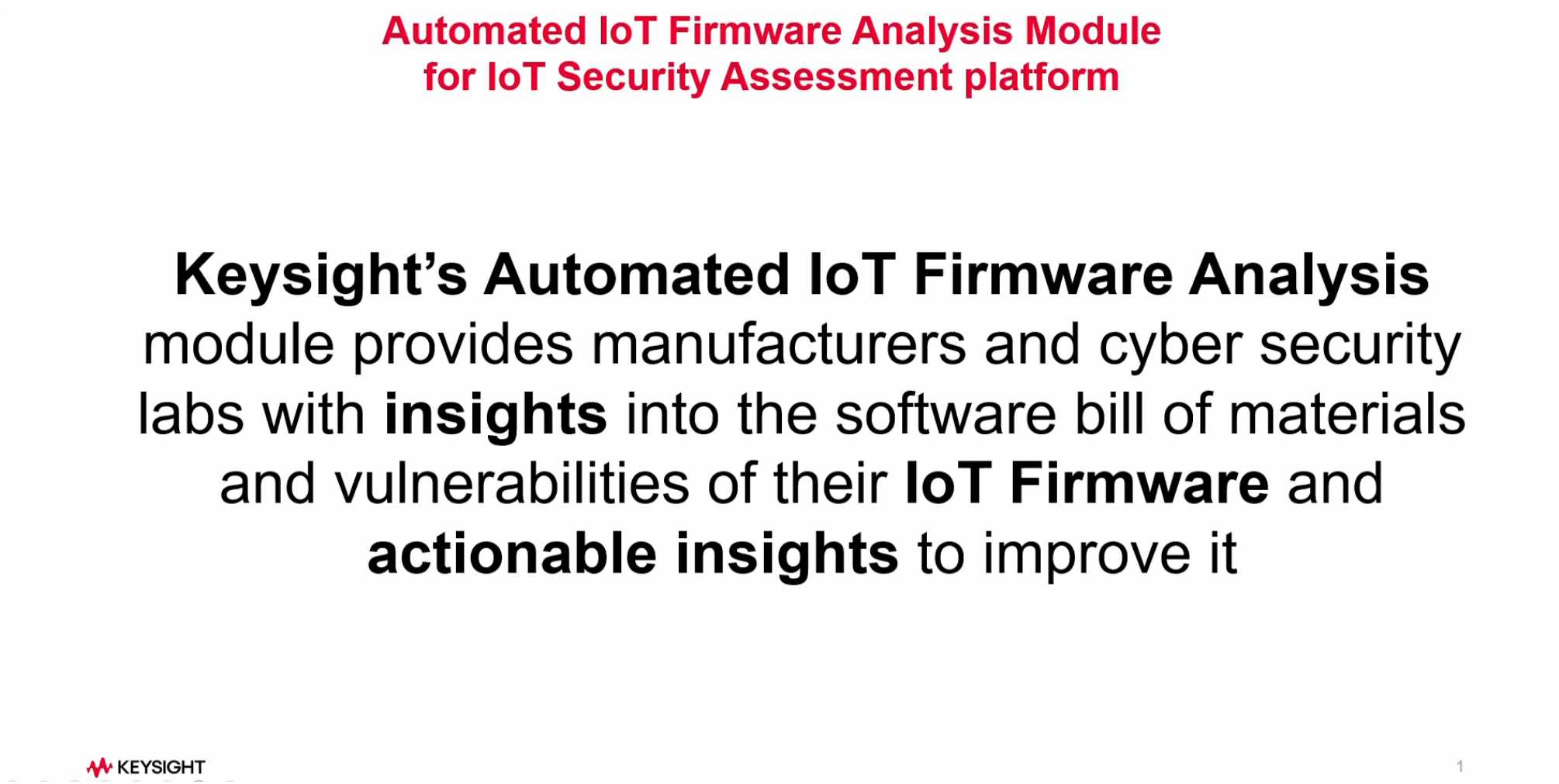
✓**コンパイル済みバイナリの解析**: この解析は、コンパイルされたバイナリに直接作用し、リバースエンジニアリングによってコードの動作を理解します。

✓**潜在的な脆弱性の特定**: バイナリの構造、制御フロー、データフローを調べることで、バイナリ解析ツールは脆弱性の存在を示唆するパターンや異常を検出することができます。

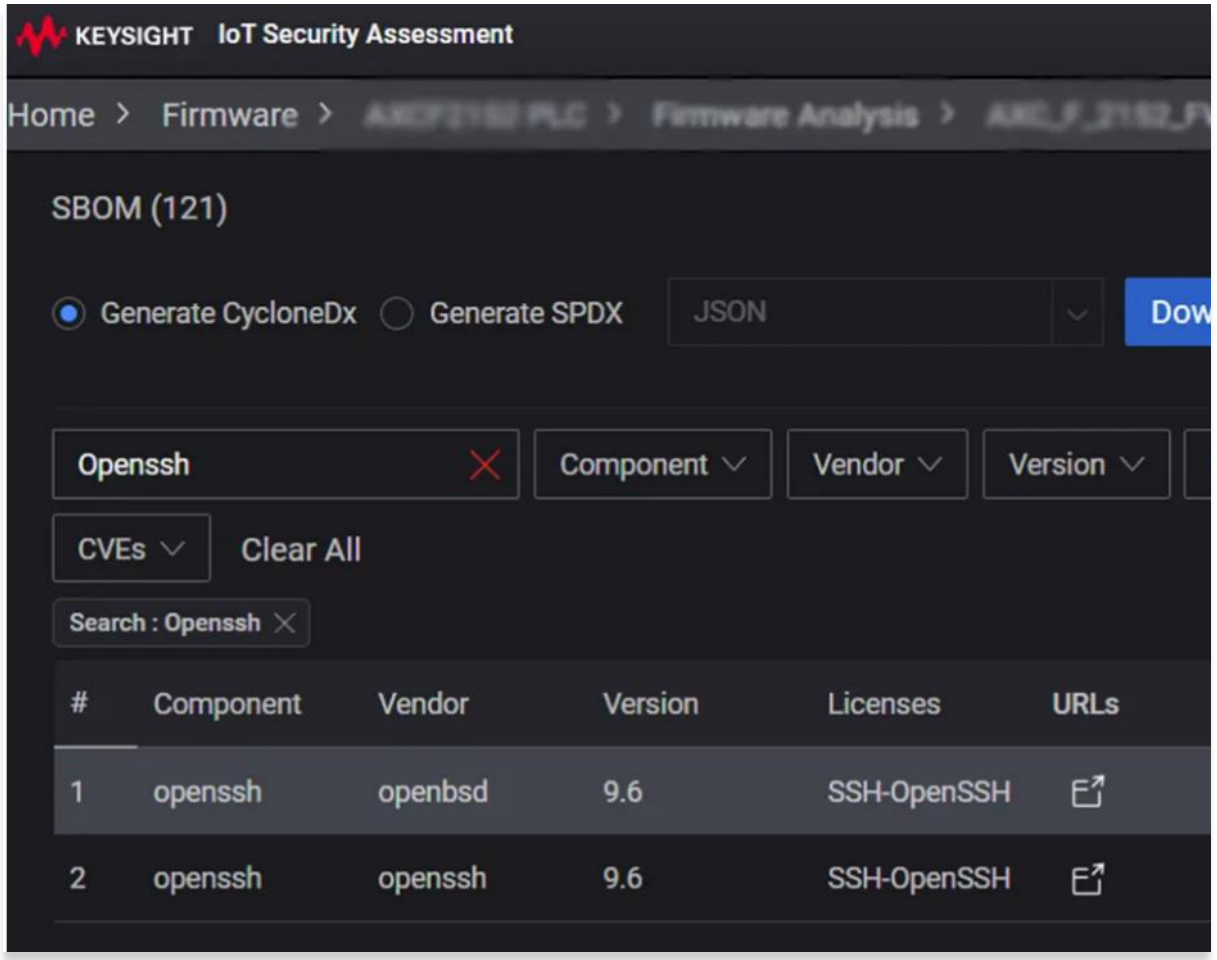
✓**実行を必要としない**: バイナリを実行しないため、解析はIoTデバイスへのアクセスがなくても実施可能です。また、悪意のあるコードや有害なコードを実行するリスクを回避できるため安全です。



バイナリ解析によるSBOM自動生成の例



最近話題となった「regreSSHion」の検証例



✓OpenSSHのサーバーにおける認証されていない
リモートコード実行を許す脆弱性で、完全なrootアクセスを
許可する。

✓デフォルト設定に影響し、ユーザーの操作を必要とせず
重大な悪用リスクを伴う。

✓OpenSSHのバージョン4.4以前および8.5以降9.8未満が
影響を受ける。

バイナリ解析によって検出される脆弱性のタイプ

- Stack Buffer Overflow
- Format String Vulnerabilities
- Command Injection

Stack Buffer Overflow

✓プログラミングにおいて、プログラムが実行されると、
関数の呼び出しパラメータやローカル変数、戻り先アドレスなどの
一時的なデータを保存するために「スタック」と呼ばれるメモリ
領域を使用します。

✓バッファは、スタック内の小さく固定サイズの記憶コンテナ
（「バックパック」のようなもの）です。

✓問題は、プログラムがバッファに設計された容量以上のデータを
誤って格納してしまうと発生します。この場合、バッファが
「オーバーフロー」し、スタック上の他の重要なデータを上書きして
しまいます。

✓これにより、予期しない動作が発生することがあり、クラッシュを
引き起こすこともあります。最悪の場合、攻撃者がオーバーフロー
した領域に悪意のあるコードを注入することで、プログラムを
制御される危険性もあります。

Stack Buffer Overflowの例

```c
#include <stdio.h>
#include <string.h>

void vulnerable_function(char *input) {
    char buffer[10]; // buffer can only hold 10 characters
    strcpy(buffer, input); // copy input into buffer
    printf("You entered: %s\n", buffer);
}

int main() {
    char user_input[100];
    printf("Enter your name: ");
    gets(user_input); // gets() is unsafe and allows large inputs
    vulnerable_function(user_input);
    return 0;
}
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

IoT Security Assessmentのご紹介

JASA公式ホームページへ！

出典：一般社団法人 組込みシステム技術協会ホームページ
https://www.jasa.or.jp/lists/bluetooth2024

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

まとめ

✓ソフトウェアコンポジション解析（SCA解析）ツールでSBOMを自動生成する

✓SBOM生成には、ソースコード解析とバイナリ解析の2種類の手法がある

✓組込み機器のファームウェアには、主にOSベースとベアメタルの2種類が存在する

✓SBOM生成だけでなく、最終的に実装されるファームウェアの潜在的な
脆弱性を確認することも重要

「サイバーセキュリティ動向 SBOMの活用」

2024/11/22 発行

発行者　一般社団法人 組込みシステム技術協会
東京都 中央区 入船 1-5-11 弘報ビル5階
TEL: 03(6372)0211 FAX: 03(6372)0212
URL: https://www.jasa.or.jp/