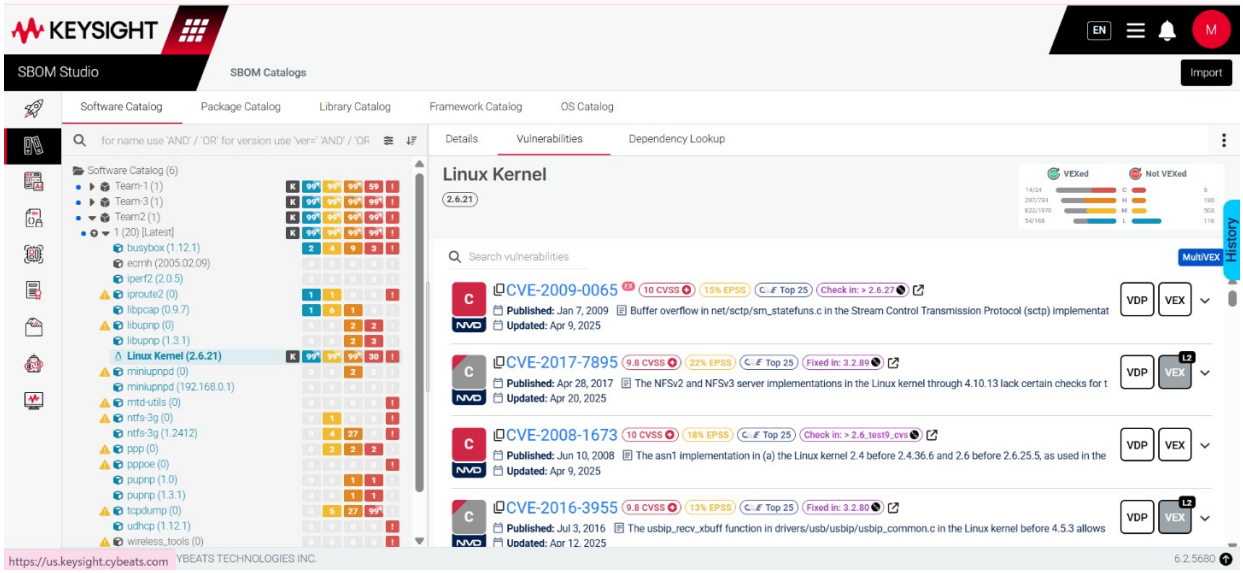
SBOM Manager

IoT機器のSBOM生成・管理一体型ソリューション

近年、IoT機器にサードパーティ製のソフトウェアが組み込まれるケースが増えており、セキュリティ対策の一環としてSBOM（Software Bill of Materials）への注目が高まっています。SBOMとは、機器に含まれるソフトウェアを構成するコンポーネント、およびそれらの依存関係やライセンス情報、バージョン情報などをリスト化した、いわばソフトウェアの部品表です。

SBOM Managerは、SBOMの作成から継続的な管理、運用まで実施可能なKeysight社のソフトウェア製品です。セキュリティテスタの開発を得意とするKeysight社と、SBOMを専門として北米や欧州の医療・産業大手からの厚い信頼を受けるCybeats社との連携により、バイナリデータからの高精度なSBOM生成機能、生成済みSBOMの管理・監視機能の双方を兼ね備えた、SBOM周りの環境すべてを包括的にカバーするソリューションとしてご利用いただけます。



特長

■ **SBOMの品質をスコア化し、情報を強化して再構築**

当製品は、作成・取込したSBOMをただ蓄積するだけではなく、そのSBOMの品質を評価し不足した情報を補完します。各コンポーネントを脆弱性データベース、脅威インテリジェンスフィード、そしてコードリポジトリ上の年数・メンテナンス状況・EOL/EOS情報と照合して情報を強化します。規制要件に対応する為だけに作成された“提出物として”のSBOMではなく、製品品質を示し迅速な脆弱性対応を可能にする“有用なデータとして”のSBOMを作成、管理することができます。

■ **サプライチェーンの透明性確保**

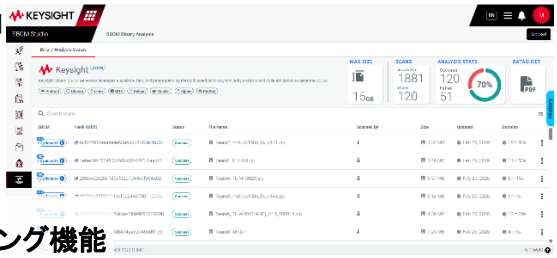
当製品は、以下に示す幅広いプラットフォームに対応しております。最終製品に対するバイナリ解析により、サプライヤー提供のSBOMや独自コンポーネント等を含めて検証・照合を行いサプライチェーン全体の透明性を確保することが可能です。

- ✓ 組込み向けファームウェア対応（モノリシック・ベアメタル）
- ✓ オープンソース、RTOS、商用・独自コンポーネント、動的・静的リンクされたコンポーネント
- ✓ OS対応：Android, Ubuntu, Linux, Debian, Docker, QNX, Windows
- ✓ フォーマット対応：SPDX, CycloneDX, VEX CycloneDX

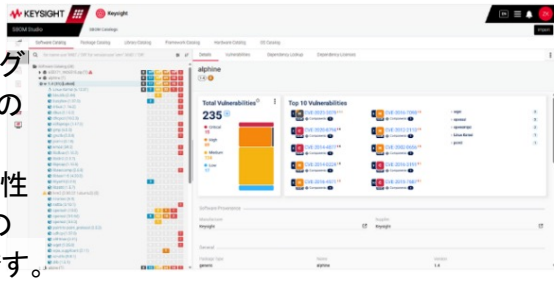
SBOM Manager

機能

当製品は、生成から継続管理、モニタリングに至るまでの包括的なSBOM対策・検証機能を有しています。



- **バイナリデータに基づく高精度のSBOM生成機能**
- **生成・取込したSBOMの対象機器別・バージョン別管理機能**
- **フォーマットを指定したSBOM出力／フォーマット変換機能**
- **EUVD・NVD・CISA KEV・OSV等を用いた脆弱性自動チェック・モニタリング機能**
- **EU CRA・FDA・NTIA・METI等の各国ガイドラインに準拠した検証機能**



生成したSBOMは、脆弱性情報との結び付けを行い、継続的にモニタリングすることで初めて、脆弱性へのマネジメントに大きく寄与するデータとしての効力を発揮します。
当製品は、SBOMの生成と継続管理により、更新時の差分や最新の脆弱性への攻撃動向を踏まえた対応優先度の判断、新たに報告された脆弱性の影響範囲絞り込みを迅速化する、唯一無二の統合SBOMソリューションです。

SBOMの必要性

IoT機器のソフトウェア部品表として注目されているSBOMは、近年世界的に活用の流れが広まってきています。既に米国やヨーロッパなどではSBOMへの対応義務を定めた規制や標準も成立しており(※1)、特にEU CRA(欧州サイバーレジリエンス法)では、製品に影響を及ぼす可能性のある、実際に悪用されている脆弱性や重大なインシデントについて、製造業者に対して段階的な報告義務が求められます。例えば、悪用されている脆弱性については、初期通知を24時間以内に行い、その後72時間以内に脆弱性の概要や影響、対策状況などを追加報告し、さらに必要に応じて詳細な情報を報告する流れとなります。そのため、製品に使用されているソフトウェアを一元的に把握し、脆弱性情報が追加・更新された時点で、自社製品への影響有無を速やかに確認できる体制が不可欠です。特に、過去に出荷したレガシー製品も対象となる可能性があるため、SBOMと脆弱性管理プロセスの整備が急がれています。
今後日本を含む他国もSBOMを用いた制度策定の取り組みに追従し、さらにSBOM活用の流れが拡大していくことが予想されます。SBOM Managerは、SBOMの作成のみならず継続的な更新・管理・モニタリング機能を備えEU CRAをはじめとする各種規制要件・ガイドラインにも準拠しております。本製品の導入により、SBOM対応が求められる情勢にいち早く対応し、セキュアな運用を強化する環境の整備をいち早く進めることが可能です。

(※1)SBOM関連の規制・標準

欧州サイバーレジリエンス法(EU CRA)
適用時期:報告義務は2026年9月、主要な義務は2027年12月より
EU市場で提供されるデジタル要素を含む製品を対象に、セキュアな設計・開発・製造、脆弱性対応、SBOMを含む技術文書の整備などを求める規制。実際に悪用されている脆弱性や重大なインシデントについては、24時間以内の初期通知、72時間以内の詳細通知、必要に応じた最終報告など、段階的な報告義務が課される。

FDA医療機器ガイドライン
適用時期:2023年10月より本格適用
米国で新たに発売申請されるサイバー機能を有する医療機器を対象に、サイバーセキュリティ対策に関する情報の提出を求める要件。申請資料には、医療機器に含まれるソフトウェアコンポーネントを把握するためのSBOM情報も含まれる。

BSI TR-03183
位置付け:EU CRA対応を支援する技術ガイドライン
ドイツ連邦情報セキュリティ庁(BSI)が公開している技術ガイドライン。製造業者がEU CRAに対応するための参考情報として、製品のサイバーレジリエンス要件やSBOMに関する考え方を整理している。

お問い合わせ
ComWorth
株式会社コムワース 通信機器事業部
TEL: 03-3777-0888 FAX: 03-3772-8497
Web: https://www.comworth.co.jp
Mail: info2@comworth.co.jp

IoT Security Assessment

無線IoT機器の脆弱性検証・管理製品

IoT機器は、インターネット上に存在するシステムやWebサイトなどと同様に、悪意あるものから脆弱性を突いた攻撃を受ける危険性があります。しかし、特に無線を搭載するIoT機器については、機器に潜む脆弱性の検査や可視化を行う手段が乏しく、近年のIoT化の流れに対して脆弱性対策や検証の手段が十分ではないことが課題となっています。
IoT Security Assessmentは、無線IoT機器に対してIPv4やBluetoothなどの外部通信を用いた脆弱性の検出、ファームウェア解析による内部構造上にある脆弱性の検出、各種セキュリティ規制で求められるセキュリティ試験を行います。
また行った試験結果を可視化することができ、管理体制の簡素化や効率化も実現可能です。

特長

■ IoT機器に対する脆弱性試験と結果の一元管理
当製品は、IoT機器を対象として様々なベクトルから脆弱性を検証する試験を実施可能です。また実施した試験結果の可視化や継続的な管理も行えます。セキュアなIoT機器を実現するための対策が、複数の製品やサービスにわたることなく当製品のみで完結するため、無線IoT機器のセキュリティ管理体制を簡素化することが可能です。

■ 必要機能の選択的な導入
IoT Security Assessmentは、IoT機器に対して実施可能な検査ごとに下記のようなモジュールが用意されており、要件に応じて以下を選択することが可能です。

- ✓ IPv4通信を用いた脆弱性検証
- ✓ WLAN通信を用いた脆弱性検証
- ✓ Bluetooth通信を用いた脆弱性検証
- ✓ ファームウェア解析（SBOM生成機能を含む）

検証から管理までを一元的に行える製品であると同時に、必要とする機能のみを選択、拡張することが可能なスケーラビリティも持った製品です。

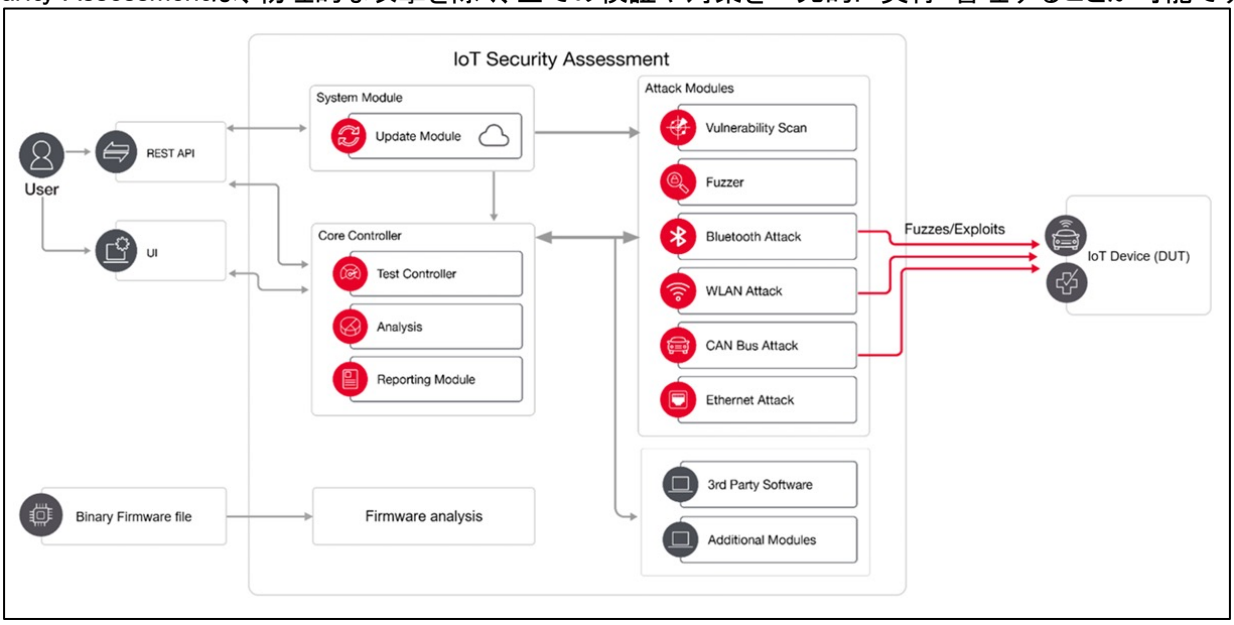
IoT Security Assessment

検証内容

IoT機器に対しては、悪意あるユーザーによって攻撃被害に遭うことを防ぐため、下記に代表される様々な側面からセキュリティの検証と対策を行うことが求められています。

- **チップセットやハードウェアのセキュリティ**
  →サイドチャネル攻撃や情報の改ざんといった物理的な脆弱性による被害の防止
- **ファームウェアのセキュリティ**
  →アップデートが安全に実行されるか、組み込みソフトウェアに脆弱性が含まれていないか、など
- **ネットワークプロトコルのセキュリティ**
  →保護されていないネットワークトラフィックがないか、プロトコルに未知の脆弱性がないか（ファジング試験）、など
- **アプリケーションソフトウェアのセキュリティ**
  →認証機構に脆弱性がないか、Webベースの攻撃に対しての露出がされていないか、など

IoT Security Assessmentは、物理的な攻撃を除く、全ての検証や対策を一元的に実行・管理することが可能です。



SBOMへの対応

近年、IoT機器にサードパーティ製のソフトウェアが組み込まれるケースが増えています。このような機器の構成が十分に把握できていない場合、脆弱性が発見された際の原因特定や修正に多くの時間を要します。
上記問題点への対策として、SBOM（Software Bill of Materials）への注目が高まっています。SBOMとは、機器に含まれるソフトウェアを構成するコンポーネント、およびそれらの依存関係やライセンス情報、バージョン情報などをリスト化した、いわばソフトウェアの部品表です。
SBOM活用の流れは世界的にも広まってきており、既に米国やヨーロッパなどではSBOMへの対応義務を定めた規制や標準も成立しています（※1）。そのため、今後日本を含む他国もSBOMを用いた制度策定の取り組みに追従し、さらにSBOM活用の流れが拡大していくことが予想されます。
IoT Security Assessmentは、SBOMの作成を行うモジュールも用意されています。本製品の導入により、SBOM対応が求められる情勢にいち早く対応し、セキュアな運用を強化する環境の整備が可能です。

（※1）SBOM関連の規制・標準

欧州サイバーレジリエンス法（EU CRA）
発効：2027年12月（EU圏）
EU圏内のデジタル製品に対するSBOM要件を提案

FDA医療機器ガイドライン
発効：2023年10月（米国）
発売する医療機器の承認取得のために必要となるSBOMを規定

BSI TR-03183
発効：2027年12月（ドイツ）
上記“EU CRA”に準拠するためのSBOM要件について記述

お問い合わせ
ComWorth
株式会社コムワース 通信機器事業部
TEL: 03-3777-0888 FAX: 03-3772-8497
Web: https://www.comworth.co.jp
Mail: info2@comworth.co.jp