Hanwha Vision

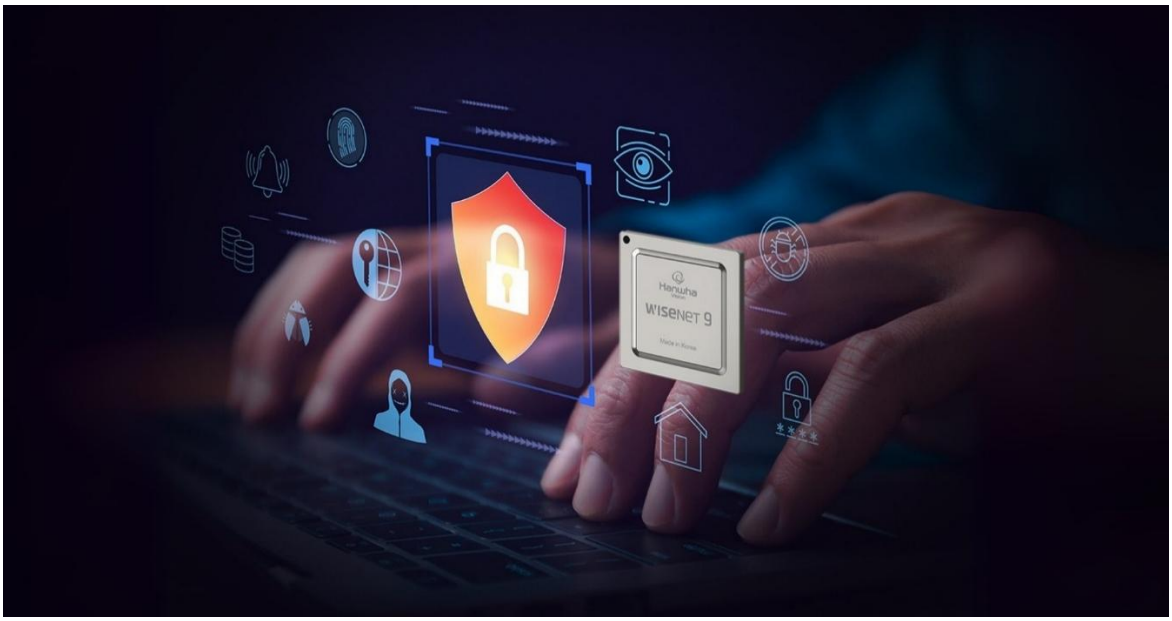
White Paper

Wisenet 9 ベース製品の 次世代サイバーセキュリティ

2025年 8月

1. はじめに

ハンファビジョンWisenetSoC（System on a Chip）は製品セキュリティ強化のために着実に新技術を融合して発展してきた。特に最新のWisenet9SoCが搭載されたカメラは、製品、開発プロセス、データ、サプライチェーンに対するセキュリティにさらに重点を置いて、ハンファビジョン映像セキュリティソリューションに対する顧客信頼をさらに高めている。



製品セキュリティを強化するためには、強固なセキュリティ標準とプロセスに基づく先制的な取り組みが必要である。Hanwha Visionは、業界で認められた数多くのグローバル標準の中から、IoT（モノのインターネット）デバイス向けのセキュリティ規格である ETSI EN 303 645 を戦略的に採用した。これは、当社のセキュリティ認証について独立した第三者による検証を可能にするものである。

Hanwha Visionは、長年にわたりアップグレードを続けてきた開発プロセスにおけるセキュリティについて、公式な検証を確保することも目指した。そのため、すでに ISO/IEC 27001 情報セキュリティ認証 を保有しているにもかかわらず、セキュリティ機能の設計・開発・テスト・保守方法に関するガイドラインを提供する ISA/IEC 62443-4-1 認証 を新たに取得した。

機密性の高いデータ保護は、保護すべき資産やデータを体系的に特定することから始まり、それを守るための技術的ソリューションの開発へとつながる。Hanwha Visionは、追加の防御層を提供するため、FIPS 140-3 認証を取得したセキュアエレメント（Secure Element） を採用し、RoT（Root of Trust）に基づくセキュアストレージを実現している。

今日のソフトウェア開発・配布環境においては、ソフトウェアサプライチェーンのセキュリティと透明性がますます重要となっている。ソフトウェア構成要素を明確に文書化・管理する SBOM（Software Bill of Materials） は、セキュリティ脆弱性の解決、運用効率の維持、オープンソースライセンスの遵守保証、ソフトウェアサプライチェーン攻撃の防止において重要な役割を果たす。

本ホワイトペーパーでは、Hanwha Vision Wisenet 9 ベースのカメラにおけるセキュリティ強化のために適用された主要な戦略と技術について詳しく解説する。特に、ETSI EN 303 645 および IEC 62443-4-1 標準への準拠プロセス、FIPS 140-3 認証セキュアエレメントによるデータ保護戦略、そして SBOMの効果的活用によるソフトウェアサプライチェーンセキュリティの強化 に焦点を当てて説明する。

2. ETSI EN 303 645規格に準拠

ハンファビジョンは、Wisenet9ベースの製品にETSI EN 303 645規格の要件を実装しました。欧州電気通信標準化機構（ETSI）が開発したこの国際的なセキュリティ規格は、IoTデバイスのサイバーセキュリティを強化するように設計されています。Wisenet9ベースのカメラがこの規格に準拠することにより、顧客はハンファビジョンプラットフォームのサイバーセキュリティを信頼できます。

2.1. ETSI EN 303 645の概要

ETSI EN 303 645規格は欧州連合（EU）で最初に制定され、ドイツ（BSI/ITセキュリティラベル）、イギリス（PSTI法）、シンガポール（サイバーセキュリティラベリングシステムTier1および2）を含むヨーロッパおよびアジア諸国でIoTデバイスのセキュリティ要件として広く採用されています。また、日本（JC-STAR1）、EU（サイバー復元力法）などのような他の地域でも採択を検討している。

ETSI EN 303 645規格は、ステークホルダーがセキュリティ要件を理解して実装するのを支援するために、3つの文書を提供しています。

- Security Baseline Requirements : ETSI EN 303 645 V3.1.3(2024-09)
- Conformance Assessment Methodology : ETSI TS 103 701 V2.1.1(2025-05)
- Guidance on Implementation : ETSI TR 103 621 V2.1.1(2025-07)

ハンファビジョンは、Wisenet7製品に米国ベースのネットワーク接続製品ソフトウェアサイバーセキュリティ認証であるUL2900-2-3標準を適用した経験がある。この規格はアメリカ標準協会（American National Standards Institute、ANSI）とカナダの国家標準（National Standard of Canada、NSC）が採用したもので、主に脆弱性、ソフトウェアの弱点、マルウェアの有無、アーキテクチャおよび設計内のセキュリティリスク制御の有無のテストに重点を置いて製品に対する侵入テストの実施も要求する。

一方、ETSI EN 303 645規格は、顧客の個人データ保護に大きな比重を与えます。この規格は、製造業者が製品およびサービスを使用する顧客に個人データの選択を提供することを要求します。これには、データ収集の同意オプションの提供、常時の同意の撤回の許可、データ収集の目的の説明などが含まれます。（リファレンスを参照）

これらの違いにもかかわらず、どちらの標準も共通して、脆弱性の開示方針、継続的な脆弱性の監視、識別および解決活動、セキュリティ認証と承認、セキュリティ通信、セキュリティブート、セキュリティアップデート、外部インターフェイスおよびサービスに対する保護メカニズムなど、さまざまな要件が含まれています。

2.2. ETSI EN 303 645主な要件

- **基本パスワードの削除**：セキュリティカメラには、ハッキングを容易にするために事前設定された共通パスワードがあってはなりません。

- **セキュア通信**：カメラが画像やデータ転送にセキュア通信プロトコルを使用することで、不正な傍受やデータ操作を防ぐ必要があります。
- **脆弱性管理**：製造業者は、カメラで発見された脆弱性を解決し報告するプロセスを備えなければならない。
- **データプライバシー**：カメラは不正アクセス、誤用、漏洩から個人および機密データを安全に保護する機能を備えなければならない。さらに、データが明確に削除されたことをユーザーに知らせ、それを確認するための手順を提供する必要があります。
- **定期的なソフトウェアアップデート**：製造業者は、デバイスのライフサイクル中に新しい脆弱性から保護するために定期的なソフトウェアアップデートを提供しなければならない。
- **セキュリティストレージ**：メーカーは暗号鍵、ユーザーパスワード、固有のデバイスIDなどの重要な情報を安全に保存するための手段を提供する必要があります。

2.3. 標準コンプライアンスによる製品信頼の確保

Wisenet9ベースの製品は、さまざまなセキュリティ要件、顧客ニーズ、業界標準を満たし、蓄積してきました会社の専門知識に基づいて開発されました。ハンファビジョンは市場動向を継続的に監視し、顧客ニーズを予測し、業界最高レベルのセキュリティ基準を維持します。市場に優秀で安全な製品を提供するよう努めています。

3. IEC 62443-4-1規格に準拠

ハンファビジョンは、Wisenet9ベースのカメラを含む製品のセキュリティ開発プロセス全体にわたってIEC 62443-4-1標準要件に準拠しています。この認証取得により、ハンファビジョンは顧客に会社のコンプライアンス活動を透明に知らせることができる。

3.1. IEC 62443-4-1の概要

IEC 62443-4-1は、産業自動化および制御システム（Industrial Automation and Control Systems、IACS）のセキュリティ開発ライフサイクル（SDL）要件を定義した国際規格です。ヨーロッパの船舶、流通、鉄道などの安全なカメラ分野の顧客の間で、この規格に準拠する要求が徐々に増加するにつれて、関連する認証の必要性も高まっています。この規格は、ハードウェア、ソフトウェア、ファームウェアなどの製品開発の全過程にセキュリティを体系的に反映させるようにし、開発組織は製品が設計段階からセキュリティを内在するようにプロセスを実装することを要求する。

3.2. IEC 62443-4-1の主な要件

IEC 62443-4-1規格の要件は、合計47の要件を含む8つの主要なプロセス領域で構成されています。各プロセス領域と主な要件は次のとおりです。

[表1]IEC 62443-4-1要件の要約

プロセス領域	主な要件
セキュリティ管理	セキュリティポリシーと手順の確立、セキュリティロールと責任の定義、セキュリティトレーニングと認識プログラムの運用、セキュリティ要件とリスク管理
セキュリティ要件の指定	セキュリティ要件の識別、文書化、レビュー、承認、追跡
セキュリティ設計	セキュリティ設計原則の適用とセキュリティアーキテクチャ設計、セキュリティ設計のレビュー、検証、追跡、およびリスク分析の実行
セキュリティの実装	セキュリティコーディング標準の適用とコードレビュー、静的分析ツールの使用
セキュリティ検証と検証テスト	セキュリティ要件、脅威の軽減、脆弱性、侵入などのテスト
セキュリティ問題の管理	セキュリティ問題の報告、レビュー、評価、解決、開示、セキュリティ欠陥管理慣行の定期的なレビュー
セキュリティアップデートの管理	セキュリティアップデートとドキュメント提供
セキュリティガイドライン	製品の保護とセキュリティ強化（廃棄/運用）ガイドの提供

3.3. セキュリティ認証による製品開発信頼の確保

ハンファビジョンは、IEC 62443-4-1規格の遵守を通じて、この国際規格を満たすSDLプロセスを備えた製品開発組織として公式に認証された。

この認証はハンファビジョン製品の開発信頼性を保証する。また、要件の識別からセキュリティ機能の設計と実装、セキュリティ問題のレビューと管理、問題解決のためのファームウェアと文書の配布まで、堅牢なセキュリティプロセスがあります。

ハンファビジョンは今後も製品ライフサイクル全体にわたってセキュリティ管理を継続的に強化し、顧客との信頼と責任に対する約束を果たし、グローバル市場で優れたサービスを提供する。

4. セキュアストレージを実装するためのセキュアエレメントの活用

セキュアストレージ（Secure Storage）は、機密データを安全に保存し、不正アクセスや漏洩からデータを保護するための必須技術です。

ハンファビジョンはWisenet7からHTPM（Hanwha Trusted Platform Module）を開発し、SoCと独立したハードウェアTPMモジュールを通じてハイエンド製品にセキュアストレージを実装した。この広範な経験に基づいて、ハンファビジョンはWisenet9ベースの製品で最新のFIPS 140-3レベル3標準認証を取得したハードウェアセキュアエレメント（Secure Element）を適用した。セキュアエレメントを通じて、Hanhwa Vision IPカメラは機密データを保存するための安全なストレージを提供します。

4.1. FIPS 140-3認証

FIPS 140-3は、セキュリティストレージなどの暗号モジュールのセキュリティを評価するための国際標準であり、グローバル市場での信頼性を保証します。FIPS140-2と比較して、FIPS 140-3は次のようにさまざまな分野で重要な改善と強化されたセキュリティ要件を必要とします。

- **ISO/IEC 19790およびISO/IEC24759統合：**FIPS 140-3は、ISO/IEC19790（暗号化モジュールのセキュリティ要件）およびISO/IEC24759（暗号化モジュールのテスト要件）規格に基づいています。これにより、国際標準との適合性がさらに高まった。
- **モジュールタイプ分類：**暗号化モジュールをハードウェア、ソフトウェア、ファームウェア、ハイブリッドモジュールタイプに精密に分類し、評価基準を細分化した。
- **ソフトウェア/ファームウェアセキュリティ：**ソフトウェアとファームウェアの整合性検証方法の明確な定義を含みます。特に、レベル2はデジタル署名ベースとメッセージ認証コードベースの整合性の両方を認識し、レベル3はデジタル署名ベースの整合性のみを認識するという違いがあります。
- **セルフテスト：**暗号化モジュールは操作前に事前操作セルフテストを実行し、特定の機能を提供するときは条件付きセルフテストを実行する必要があります。
- **ライフサイクル保証：**設計、開発、配布から廃棄に至る暗号化モジュールの完全なライフサイクルをカバーするセキュリティ要件が強化されました。

4.2. FIPS 140-3セキュリティレベル

FIPS 140-3は暗号化モジュールを4つの段階的なレベルに分類し、各レベルに応じてセキュリティ要件の厳格性が高まります。ハンファビジョンが使用するセキュア要素はレベル3を達成するように設計されています。このレベルは、次の主要領域でレベル2と比較してセキュリティが向上します。

- 役割（ロール）/サービス（サービス）/認証
- ソフトウェア/ファームウェアセキュリティ
- 物理セキュリティ

- 非侵害セキュリティ（非インバシブセキュリティ）
- セキュリティパラメータ管理(Security Parameter Management)
- 寿命サイクル保証

[表2]FIPS 140-3の概要[1]

Requirement Area		Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification		Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces		Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication		Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security		Approved integrity technique, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test	
Operational Environment		Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security		Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security		Module is designed to mitigate against non-invasive attacks specified in Annex "F".			
		Documentation and effectiveness of mitigation techniques specified in Annex "F"		Mitigation testing	Mitigation testing
Security Parameter Management		Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
		Automated SSP transport or SSP agreement using approved methods			
		Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests		Pre-operational: software/firmware integrity, bypass, and critical functions test			
		Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance	Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
	Design	Module designed to allow testing of all provided security related services			
	FSM	Finite State Model			
	Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
	Testing	Functional testing		Low-level testing	
	Delivery & Operation	Initialization procedures	Delivery procedures		Operator authentication using vendor provided authentication information
	Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks		Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

各レベル別のセキュリティ要件をまとめると、次のようになります。

[1] 注： https://lightshipsec.com/fips-140-3-is-here/

- **レベル1：**最低セキュリティレベルで、基本的な暗号化と鍵管理機能を必要とし、ソフトウェア専用モジュールに適しています。
- **レベル2：**不正アクセスを防止し、物理的変調を検出するための物理的セキュリティ対策（ロック、改ざん防止ステッカーなど）と役割ベースの認証が必要です。
- **レベル3（ハンファビジョンセキュア要素に適用）：**より高いレベルの物理的セキュリティを必要とする。物理侵入の試みを検知する改ざん防止抵抗、アイデンティティベースの認証、温度および電圧変動を含む環境攻撃に対する保護が必要です。
- **レベル4：**最高のセキュリティレベルで、非常に洗練された攻撃を防ぐことに焦点を当てます。改ざん防止機能、多重認証、環境攻撃、またはエラー注入検出時に機密データを削除する機能が含まれます。

4.3. セキュアエレメント活用事例とシナリオ

エンドユーザーがデバイスに組み込まれたセキュアエレメントの詳細な活用方式や具体的な役割を知る必要はない。製品全体で強力なサイバーセキュリティを確保することは、完全に製造業者の責任です。そのため、セキュリティ機能は、複雑さや不快感を招くことなくユーザーを保護するように設計する必要があります。

ハンファビジョンは責任あるメーカーで、暗号鍵、ユーザー設定パスワードなどを通じて保護が必要な機密データを先制的に識別してきた。以下の表3は、これらのデータカテゴリを詳細に示しています。

機密データを保護するための最も効果的な方法の1つは、デバイスにデータが保存されたときに暗号化することです。しかし、暗号鍵自体も安全に保護されなければならない。これを解決するための最も効果的なソリューションは、デバイスに組み込まれたセキュアエレメントを活用して機密データを保存して管理するのだ。

[表3]機密データ型

カテゴリー	機密データ
ユーザー設定 パスワード	デバイスにアクセスするためのログイン
	SMTP/FTP/NASサーバーアクセス
ユーザー設定 暗号鍵	802.1xアクセス用の秘密鍵/証明書
	HTTPS/TLSのための秘密鍵/証明書
	802.1x認証サーバーの真偽を確認するためのCA証明書
メーカー設定 暗号鍵	HTTPS/TLS、デバイス認証のための秘密鍵/証明書
	セキュアブート/署名付きファームウェア検証用の公開鍵
	オープンプラットフォームアプリの真偽を確認するためのCA証明書
	相互認証の真偽を確認するためのCA証明書
	バックアップ/回復のための秘密鍵

ハンファビジョンセキュア要素は製造中に生成される固有の対称キーを使用しますデバイスごとに機密データを暗号化します。このキーはFIPS 140-3レベル3認証を受けたセキュア要素によって保護されるため、露出する可能性が非常に低いです。1つに流出しても、特定のデバイスにのみ影響を与えます。この隔離は潜在的なセキュリティ事故の影響を大幅に制限し、全体的なリスクを最小限に抑えます。

5. ソフトウェアサプライチェーンセキュリティの強化

ハンファビジョンはWisenet9ファミリを皮切りに、ソフトウェアプラットフォームへのSoftware Bill of Materials（SBOM）の展開を開始した。

5.1. SBOMについて

SBOMは、ソフトウェア製品を構成するすべてのソフトウェアコンポーネント、特にすべてのオープンソースライブラリとサードパーティライブラリを明確に識別する詳細なリストです。そのようなコンポーネントは、さまざまなソースから開発リポジトリに侵入する可能性があり、このプロセスで既知のオープンソースの脆弱性が意図せずに製品に含まれる可能性があります。

このため、オープンソースの脆弱性管理はソフトウェアサプライチェーンセキュリティの重要な部分となり、SBOMは効果的な管理を可能にするために重要な役割を果たしています。SBOMを管理し維持することで、ソフトウェアサプライチェーンの透明性とセキュリティが向上し、次のような利点があります。

- **ソフトウェアの透明性と信頼性の向上：最新の**ソフトウェアは、オープンソースとサードパーティのライブラリに大きく依存しています。SBOMはソフトウェアに含まれるすべてのコンポーネントを明確にリストし、セキュリティの脆弱性やマルウェアを含むコンポーネントを迅速に識別できるようにします。これはソフトウェアサプライチェーンの信頼性を高め、顧客とユーザーに大きな透明性を提供します。

  例：Log4jの脆弱性（Log4Shell、2021）などのセキュリティ上の問題が発生した場合、SBOMを利用すると、そのライブラリを含むソフトウェアをすばやく識別して対応できます。

- **規制遵守と業界標準を満たす**：多くの国で規制遵守のためにSBOMを使用する必要があります。

  例：米国行政命令14028（2021）によれば、連邦政府と契約するソフトウェアベンダーはSBOMを提供しなければならない。さらに、SBOMを使用して標準に準拠していることを確認すると、ソフトウェアライセンス違反に関する法的問題を防ぐことができます。

  例：SBOMは、業界標準ISO/IEC5230[Linux Foundation Open Chain Specification ベースのオープンソースソフトウェアライセンス準拠規格]の重要な要素です。

- 管理**とセキュリティ事故の対応：**ソフトウェアコンポーネントのバージョン情報を含めることで、SBOMは顧客が一般的な脆弱性インデックスと比較してセキュリティ脆弱性を迅速に識別できるようにします。セキュリティ事故が発生した場合、SBOMは顧客が影響を受けるソフトウェアを即座に識別して対応するのに役立ちます。

- **効率的なソフトウェアメンテナンス：**SBOMは、顧客とメーカーの両方がソフトウェアコンポーネントに関する情報を体系的に管理するのに役立ち、古いコンポーネントを更新したり、廃止されたコンポーネントを削除したりするなどのメンテナンス作業を容易にします。

- **オープンソースライセンスの遵守：**SBOMは、製品に含まれるオープンソースライブラリと関連ライセンスを明確に文書化し、ライセンスコンプライアンスを保証します。これは、製造元がGPL、Apache、MITなどのライセンスの要件を満たすのに役立ちます。

- **ソフトウェアサプライチェーン攻撃の防止：**最近のソフトウェアサプライチェーン攻撃（SolarWinds、Log 4j、Kaseyaイベントなど）が増加するにつれて、SBOMはサプライチェーン全体の脆弱性を特定し防止する上で重要な役割を果たしています。これは、ソフトウェアコンポーネントのソースを追跡し、信頼できないコンポーネントを削除するのに役立ちます。

5.2. ハンファビジョンSBOMの特徴

ハンファビジョンは、顧客が必要な情報に簡単にアクセスして管理できるようにSBOMを公開した。これには、オープンソースソフトウェアコンポーネントの名前とバージョン、ソース、機能説明、ライセンス、著作権者、Common Platform Enumeration（CPE）、パッケージURL（purl）、脆弱性パッチの詳細などが含まれます。

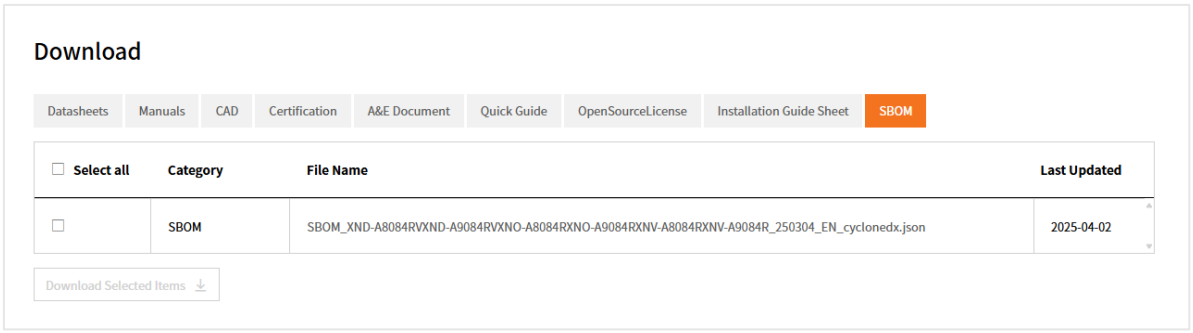


図1.ハンファビジョンウェブサイトに公開されたXNV-A9084RSBOM

ハンファビジョンは、単にSBOMの提供を超えて、各製品の長期ファームウェアサポートポリシーに従って定期的なファームウェアアップデートを通じて既知のオープンソースの脆弱性を先制的に解決することに専念しています。

- ハンファビジョンSBOMはOWASP(Open Web Application Security Project, https://owasp.org/)が主導する標準であるCycloneDX形式を使用し、.JSONファイルで提供される。
- SBOMユーティリティまたはビューアを使用してコンテンツを簡単に確認して検索できます。

5.3. ハンファビジョンSBOM活用法

顧客はハンファビジョンSBOMを効果的に活用してセキュリティを強化し、ソフトウェアコンポーネント管理を簡素化することができる。

1. **影響評価**：特定のオープンソースソフトウェアで既知のCommon Vulnerabilities and Exposures（CVE）が発生した場合、顧客はサプライヤが提供する製品固有のSBOMを参照して、その製品が影響を受けていることを確認できます。これにより、どのオープンソースソフトウェアとバージョンが影響を受けたかをすばやく把握できます。
2. **パッチの確認**：影響を受けるバージョンが特定された場合、顧客はSBOMで利用可能な脆弱性パッチ情報を確認する必要があります。場合によっては、CVEのセキュリティパッチが以前のバージョンにバックポートされる可能性があるため、使用している特定のバージョンが実際には脆弱ではない可能性があります。

3. **影響の未確認時の製造元への問い合わせ**：SBOMに脆弱性パッチが指定されていない場合、これはビルド時にコンパイラによって脆弱なコードが含まれていないか、その脆弱性が外部に公開されていないことを意味する可能性があります。そのような場合、顧客は製造元に連絡して製品が実際に影響を受けていることを確認する必要があります。
4. **ソフトウェア更新要求**：実際の影響が確認されたら、顧客は製造元に影響を受けたオープンソースソフトウェアの更新またはパッチを要求することができます。廃止されたモデルの場合、サポートは長期ファームウェアサポートポリシーの適用可能性と期間によって異なります。

詳細については、Long-Term Firmware Support Policyのドキュメントを参照してください。

6. 結論

製品セキュリティは、単に製品の脆弱性を防ぐことを超えています。これには、ソフトウェアコンポーネントのサプライチェーンセキュリティ管理、開発環境、および人材のセキュリティ、製品内に保存および処理されるデータの保護など、包括的に含まれます。

セキュリティの脆弱性がどのように発生するのかを理解することで、なぜ包括的な保護措置が不可欠なのかを明確にすることができます。脆弱性は、製品の計画および設計段階から実装、流通、さらには運営に至るあらゆる段階で流入する可能性があります。もちろん、コスト削減のためにこれらの脆弱性を先制的に排除するのが理想的ですが、現実的には困難な場合が多いです。そのため、新しい脆弱性が発見されたときに迅速に対応できる開発および脆弱性対応プロセスを備えることが非常に重要です。グローバルセキュリティ標準はこれらの統制を義務付けており、ハンファビジョンは優れたソリューションを提供するためにこれらの要件を製品および開発プロセスに継続的に統合しています。

ハンファビジョンは、製品の脆弱性を識別するための侵入テストを実施し、開発者のための内部バグバウンティプログラム（Bug Bounty Program）運営、徹底したセキュリティレビューなど、先制的なセキュリティ努力を続けている。また、CVE Numbering Authority（CNA）として脆弱性の識別と開示の役割を忠実に実施しています。ハンファビジョンは信頼できるサプライチェーンとサイバーセキュリティに対するしっかりとした集中を通じて、世界レベルの映像セキュリティソリューションプロバイダーとして先頭を固めている。

7. リファレンス

- [5.11-1]ユーザー情報を簡単に削除できる機能を提供します。
  ※ユーザー情報：パスワード、キー、環境設定情報、個人情報など
- [5.11-2]関連サービスに保存されている個人情報を簡単に削除できる機能の提供
  ※デバイスに接続されたクラウドサービスにユーザーの個人情報（アカウント情報、動画など）が保存されている場合のみ
- [5.11-3]個人情報の削除方法に関する簡潔で正確なユーザードキュメントを提供します。
  ※個人情報が保存されている場合に限ります。
- [5.11-4]すべての削除機能において、個人情報が削除されたことを明確に確認し、正常に完了したことを示すメッセージを提供します。
  ※個人情報が保存されている場合に限ります。
- [6-1]個人情報の処理に関する透明な情報提供。
  ※個人情報のリスト、利用目的・方法・主体など。
  ※個人データを処理する場合に限る。
- [6-2]個人情報の取り扱いに関する
  お客様の同意の取得。※有効な方法により
  お客様の同意を得る必要があります。※お客様の同意に基づいて個人情報を処理する場合のみ該当します。
- [6-3]お客様にいつでも個人情報処理に対する同意を撤回する権利を提供します。
  ※お客様の同意に基づいて個人情報を処理する場合に限ります。
- [6-4]個人情報の取り扱いは、目的達成に必要な最小限の範囲にとどめること。
  ※テレメトリデータを収集する場合に限る。
- [6-5]お客様へのテレメトリデータに関する情報提供。
  ※テレメトリデータの一覧、利用目的・方法・対象等。
  ※テレメトリデータを収集している場合に限る。

Hanwha Vision
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
www.HanwhaVision.com