標準「ネットワークセキュリティ技術ソフトウェア部品表データフォーマット」（意見募集案） 作成要領

I. 作業の概要

1.1 権限の源

国家標準化管理委員会が 2023 年に公布した標準要求により、「サイバーセキュリティ技術ソフトウェア部品表データ形式」は水資源部情報センターが担当している。この標準は国家ネットワークセキュリティ標準化技術委員会の管理下にある。

1.2 背景

ソフトウェアサプライチェーンの複雑化、オープンソースソフトウェアの利用の増加、ソフトウェアアップグレードやパッチに対する保護措置が不十分であることが、ソフトウェアサプライチェーンにおけるセキュリティリスクの増加や監督を困難にしている主な原因である。ソフトウエアサプライチェーンの複雑化、膨大な数のソフトウエア入れ子式参照コンポーネント、中国におけるソフトウエア部品表構築のための統一仕様の欠如を考慮すると、ソフトウエア部品表（SBOM）の形式に関する仕様を策定し、ソフトウエアコンポーネントとその依存関係を識別し、ソフトウエアのライフサイクル全体の可視性と透明性を向上させ、ソフトウエアサプライチェーンのセキュリティ管理能力を強化する必要がある。SBOM は、ソフトウェアサプライチェーンの供給者、需要者、規制者が、ソフトウェアのセキュリティ脆弱性と知的財産権のリスクを発見することを支援することができる。

1.3 ドラフト作成プロセス

(1) 標準プロジェクトの宣言

2023 年 7 月から 2023 年 8 月にかけて、標準準備グループが設立され、数回の議論を行い、ソフトウェア部品表関連政策、標準仕様、技術実装に関する調査を行い、標準「サイバーセキュリティ技術のためのソフトウェア部品表データフォーマット」の予備草案を形成した。2023 年国家標準プロジェクト宣言の要件に従い、国家標準開発プロジェクト申請書を提出した。

(2) ドラフト段階

2023 年 8 月、WG7 作業部会の第 2 回全体会合でプロジェクト宣言の初期レビューを報告し、レビュアーのコメントに基づいて標準草案を改良する。

2023 年 9 月、サイバーセキュリティ標準委員会の国家標準制定専門家審査会議で、

2023 年サイバーセキュリティ国家標準第 2 陣が報告され、審査専門家のコメントに従って標準案が改善された。

2023 年 10 月～2024 年 2 月、まず水資源省と南部電力網の情報センターでパイロット・バリデーションを実施し、バリデーションの実践活動に基づく正式なパイロット・バリデーション・プログラムを策定し、グループ内でパイロット・バリデーション・ユニットの募集を実施する。

2024 年 2 月、「ネットワークセキュリティに関する 17 の国家標準プロジェクトの設立に関する国家ネットワークセキュリティ標準化技術委員会通知」（Net Security [2024] No.2）通知により、本標準はネットワークセキュリティ標準設定プロジェクトとして正式に承認された。

2024 年 3 月 13 日、WG7 ワーキンググループの専門家レビュー会議において報告がなされ、専門家の意見に基づき、データモデル図や標準フィールド記述の修正・改善に重点を置いた議論が行われた。

削除: （2）征求意见阶段

(2) 相談段階

3 月 27 日から 2024 年 4 月 1 日にかけて、WG7 はメンバーによる標準規格の回し投票を組織し、メンバーは標準規格を公開草案に変更することに投票した。

2024 年 4 月 11 日、TC260 専門家レビュー会議にて報告され、専門家の意見により、規格の枠組み図をさらに修正・改善し、要素の分類を整理したこと、規格のモデル図を改善し、モジュール内の文章をスリム化し、イラストなどの情報を追加したこと、規格の序文、用語などをさらに改善・補足したこと、構成要素の重要性に関する関連情報を補足したことが報告された。

2024 年 4 月 21 日、水資源省は専門家質問会を開催し、参加した専門家に標準の内容を報告し、専門家の意見に従って、標準の序文を修正し、リストの構成と記述の論理構造を修正し、略語の定義を増やし、表現の文脈で内容の一部を統一し、一部の分野の定義をさらに明確にした。

II.標準作成の原則、その主な内容、決定の根拠

2.1 標準化の原則

(1) 普遍性の原則

データ分野は、需要側のソフトウェアサプライチェーンリスク管理、供給側のソフトウェア部品表管理、規制側の業界およびマルチレベルの規制要件など、供給、需要、規制のステークホルダーのニーズを満たすように選択される。

(2) コンプライアンスの原則

本標準は、ソフトウェアサプライチェーンセキュリティに関する関連法規の規定に準拠し、標準条項の内容は、中国の法規及び関連政策の要求事項に沿ったものである。

(3) 一貫性の原則

この標準は、国内外の関連技術標準と調和しており、中国のソフトウェアサプライチェーンセキュリティの関連標準と矛盾するものではない。

(4) 互換性の原則

既存標準との互換性が高く、既存標準の必要な分野をカバーし、国際標準フォーマットの変換に関するガイダンスを提供する。

(5) 操作性：標準は、インベントリを作成し交換する自動化された手段をサポートできる。

2.2 主要要素とその識別の根拠

この標準は、ソフトウェア部品表の構成、リストファイル形式の要件、ソフトウェア部品表の要素を含む、共通のソフトウェア部品表データ交換フォーマットを規定する。ソフトウェア部品表の構成ソフトウェア部品表には、どのような要素が含まれているか、また要素の意味と内容が含まれている。ソフトウェア部品表文書のリストファイル形式の要件は、フォーマット仕様に準拠する必要がある。ソフトウェア部品表の要素は、フィールドとフィールドの値の形式のソフトウェア部品表の要素を提供し、各フィールドの説明の意味を与える。

標準は、以下の基準に基づいて策定されている：

a）標準フォーマットは GB/T 1.1-2020 の要求に従って作成されている。

b）この標準は、以下の政策文書や国家標準を参考に策定されている：

中華人民共和国ネットワーク・セキュリティ法

重要情報インフラのセキュリティ保護に関する規則

第 14 次 5 カ年計画における国家情報化計画

サイバーセキュリティ審査スキーム

GB/T 24420-2009 サプライチェーンリスクマネジメント

GB/T 25069-2022 情報セキュリティ専門用語集

GB/T 36637-2018 情報セキュリティ技術 ICT サプライチェーンセキュリティリスク管理ガイドライン

情報セキュリティ技術ソフトウェアサプライチェーンセキュリティ要件（承認案）

ソフトウェア部品表構成では、リストが基本情報、ソフトウェア構成情報、外部依存情報、セキュリティ情報、拡張情報、署名情報の 6 カテゴリー17 要素から構成されることを規定し、リストの基本機能をサポートする最小限の要素セットを規定している。

テキストファイルまたはファイルのグループの情報を運ぶためにソフトウェア部品表のためのソフトウェア部品表のファイル形式の要件をリスト、ファイルの形式、特定の要件を命名する。

ソフトウェア部品表要素（Software Bill of Materials element）は、要素のフィールドとフィールド値のフォーマットの仕様を提供する。概要、基本情報カテゴリ、ソフトウェア構成情報カテゴリ、外部依存情報カテゴリ、セキュリティ情報カテゴリ、拡張情報カテゴリ、署名情報カテゴリの 7 章からなる。本章のソフトウェア部品表の概要部分では、フィールド記述の統一的な仕様を提案しており、フィールド名、フィールド記述、フィールドタイプ、フィールドの必要性を含むべきである。基本情報カテゴリには、ソフトウェア情報とインベントリ情報の 2 つの章があり、ソフトウェア情報には、ロゴ、サプライヤ、ソース、認証、完全性、その他の情報に関わるソフトウェアが含まれ、インベントリ情報には、バージョン、ロゴ、作成、アクセス、その他の情報に関わるソフトウェア部品表が含まれる。ソフトウェア構成情報のカテゴリには、コンポーネント情報、ファイル情報、コード断片情報、内部依存情報の 4 つの章がある。 コンポーネント情報は、ソフトウェアに含まれるすべてのコンポーネントのリストを提供し、各コンポーネントには、コンポーネントの識別、サプライヤ、ライセンス契約、整合性チェックなどのコンポーネント情報が含まれる。ファイル情報は、ソフトウェアの最初のレイヤで解凍およびミラーリングされた製品ファイルのリストを記述し、ファイル名、パス、使用状況、整合性チェックなどの情報が含まれる。コード・スニペット情報（Code Snippet Information） 自身が開発したソースコードに含まれる、コミュニティやフォーラムなど他のソースか らのソースコード・スニペットのリストを記述するもので、スニペットの識別子、場所、ソース、ライセ ンスなどの情報が含まれる。内部依存情報： コンポーネント、ファイル、コード・スニペット間の依存関係を記述する。

環境情報は、データベース管理システム、ウェブアプリケーションフレームワーク、ミドルウェア、オペレーティングシステム、BIOS など、ソフトウェアの運用をサポートする基本的な動作環境のリストであり、基本環境の名称、バージョン、代替可能性、供給

元などの情報を含む。

セキュリティ情報」には、「ネットワークサービスインタフェース情報」、 「パッチ情報」、「ライセンス情報」、「セキュリティ脆弱性」、「設定リスク」、 「ライフサイクル保守中断リスク」の 6 つのセクションがある。ネットワークサービスインタフェース情報」には、ソフトウェアが提供するネットワークサービスインタフェースのうち、アクセスまたは呼び出すことができるインタフェースのリスト（インタフェースの説明、プロトコル、アドレス、リクエストメソッド、その他の情報を含む）を記述する。「パッチ情報」には、ソフトウェアのリリースから部品表が作成されるまでの間に、問題や抜け穴を修正し、性能を最適化するために発行されたパッチのリスト（パッチの名称、元の製造者のロゴ、その使用に関する説明を含む）を記述する。ライセンス情報には、ライセンスの名称、内容、リスク及びその他の情報を含む、ソフトウェア及びそのコンポーネントとコードフラグメントの使用におけるライセンスリストが記述される ;セキュリティ脆弱性には、脆弱性の名称、関連する番号、オブジェクトの影響、状況の修復及びその他の情報を含む、セキュリティ脆弱性リストの生成前に修復されたコンポーネントのリストが記述される ;構成リスクには、ソフトウェアのリリースから、ソフトウェアの発見時の部品表の生成までのソフトウェアが、既知の構成のソフトウェアリスクのデフォルト構成に存在する可能性があることが記述される。構成リスクは、ソフトウェアのリリースから部品表作成までの間に発見されたソフトウェアのデフォルト構成項目に存在する可能性のある既知の構成リスクを記述する。ライフサイクル保守中断リスク（Lifecycle maintenance interruption risk） ソフトウェアのライフサイクル中に発生する可能性のある保守サービ ス終了リスクのリストを、中断の種類、説明、中断が予想される時間、廃棄、 その他の情報を含めて記述する。

拡張情報（Extended Information） 本文書で定義されていないその他のソフトウェア材料情報のリストで、拡張情報の 属性名と属性値を含む。

署名情報のリストを記述する電子証明書および署名ファイル情報は、国または業界の規制に準拠する組織 が発行した電子証明書を使用しなければならない。

2.3 改定前後の技術的内容の比較【標準規格改定プロジェクトに限る

関係ない。

III.試験検証、技術的・経済的正当性、期待される経済的・社会的・生態学的便益に関する分析と統合報告書

3.1 実験的検証分析

標準の作成過程において、ソフトウェア部品表の基本概念、応用価値及び関連する国

際標準について包括的な調査を実施し、ソフトウェア製品の調達又はカスタマイズ開発に関わる関連部門に対して多くの調査を実施し、調査報告書を作成し、予備的な検証計画を策定し、水利及びエネルギー産業における 38 のシステム/サブシステムについてパイロット検証を実施し、実現可能性及び安全上の利点を検証した。水利業界とエネルギー業界において、38 のシステム/サブシステムのパイロット・バリデーションが実施され、実現可能性、安全上の利点が検証され、いくつかの標準条項の実施可能性が実証された。

標準には現在、27 の必須フィールドと 97 の非必須フィールドがある。この予備テスト検証では、27 の必須フィールド、水利業界における 23 の自動アクセスフィールド（自動化率 85%）、エネルギー業界における 24 の自動アクセスフィールド（自動化率 89%）をカバーしている。

その後、この標準は、金融、運輸、政府、通信など、さまざまな業界の標準作成に携わったユニットによって積極的にテストされ、適用される。

正式なパイロット検証プログラムが策定され、当初は以下のレベルで計画されている：

1.標準の実現可能性を検証する：

(1)標準的なフィールド採集の実現可能性と、それが技術的または非技術的な手段によって得られるかどうか；

(2)標準フィールドへのアクセスのしやすさ、および技術キャプチャの自動化能力；

(3) 捕捉された標準フィールドの信頼性；

(4)ソフトウェアライフサイクルの各段階において、どの分野をどのような手段で取得するかという取得プロセスの検証；

2.安全性の検証

(1)標準分野がどのような問題に焦点を当てることができるか、例えば、脆弱性修復への有用性、緊急対応への有用性などである；

3.互換性の検証

(1)国際標準との互換性、2 つのフォーマットを相互に変換できるかどうか；

3.2 技術経済的正当性

国際標準と関連組織はソフトウェア部品表の標準フォーマットに関するコンセンサスを徐々に確立し、Intel、Microsoft、Siemens、Sony、Synopsys、VMware、WindRiver を含む多くの企業はすでにソフトウェア部品表を使用して、自社のポリシーやツールでソ

フトウェア部品表情報を伝達しており、中国の主要なソフトウェア部品分析システムのほとんどは、国際標準に基づいてソフトウェア部品表の生成と検証などの機能を実装している。中国の主要なソフトウェア部品分析システムのほとんどは、国際標準に基づいてソフトウェア部品表の生成と検証の機能を実装している。ソフトウェア部品表生成は主に 2 つのステップから構成され、1 つは部品表データの取得、もう 1 つは部品表ファイルの生成である。前者はソフトウェア部品分析、セキュリティ管理プラットフォーム、3 者間データ共有などの技術的手段に依存し、後者はフォーマット変換エンジンを使用することで実現できる。国内外の現在の管理及び製品実務の分析から、標準フォーマットに基づくソフトウェア部品表は技術的な実現可能性があり、ソフトウェア部品表の実施原理の分析から、技術的な実施の難易度は大きくないが、より高い自動化レベルを実現し、国内のソフトウェアサプライチェーンセキュリティ管理の実際のニーズに沿ったデータリストの取得を実現するためには、技術的及び経済的な実証と検証をさらに進め、国内のソフトウェアサプライチェーンセキュリティ管理のために、技術的に実現可能で経済的に合理的な技術的解決策を選択する必要がある。技術的に実現可能で、経済的に合理的な技術プログラムを選択し、標準内容の設定に科学的根拠を提供する必要がある。

3.3 期待される経済的・社会的便益

本標準の制定は、ソフトウェア部品表の分野における中国の国家標準のギャップを埋め、供給側、需要側、規制当局間のソフトウェア部品表情報の生成、共有、標準化の利用のためのソフトウェアサプライチェーンを促進し、ソフトウェアサプライチェーン関連の規制政策と規則の実施を支援し、中国のソフトウェアサプライチェーンセキュリティ管理システムの段階的な改善を促進し、重要な情報インフラがゲームの「首」の問題を解決するのを助け、中国経済の高品質な発展を保護し、社会の安定と国家の安全を維持する。重要な情報インフラが大国のゲームにおける「首」の問題を解決するのを助け、中国経済の質の高い発展を保証し、社会の安定と国家の安全を維持する。ソフトウェア部品表の形式を標準化することで、形式の変換、エラーの修正など、形式の不一致による追加コストを削減することができ、ソフトウェア開発全体のコストを削減することができる。ソフトウェア部品表の標準化を推進・適用することで、ソフトウェアサプライチェーンの透明性が効果的に向上し、ソフトウェア部品のトレーサビリティ、ソフトウェア製品の依存関係の突合せ、既知の脆弱性の影響範囲の判断、マルウェア侵入のタイムリーな発見などが大幅に容易になり、ソフトウェア部品表の管理コストを効果的に削減し、脆弱性の修復コストを削減し、サイバーセキュリティインシデントによる経済的損失を削減し、企業の経済的利益を増大させることができる。

IV.同種の国際標準および外国標準との技術内容の比較

ソフトウェア部品表の研究では、外国は先に開始され、SBOM の研究では、米国は、

ソフトウェアのサプライチェーンのセキュリティ研究の焦点となっている完璧な知識と標準を形成している、エネルギー、医療、製造業、実用的な経験の形成のアプリケーションのための他の産業では、米国は SBOM の国内でのコンセンサスを形成しており、広く使用される。

ソフトウェア部品表に関連する海外の標準には、ISO/IEC 19770-2:2015 "Information Technology.ソフトウェア資産管理。Part 2: Software identification labelling" や ISO/IEC 5962:2021 "Information technology - SPDX specification V2.2.1" などがある。

ISO/IEC 19770-2:2015 は、ソフトウェア製品を記述するための構造化メタデータフォーマット SWID を規定している。 SWID フォーマット仕様では、ラベル ID、ソフトウェア名、関連組織名と役割、関連リンクといったいくつかの必須フィールドを除き、その他の要素や属性はすべて任意であり、コンポーネントだけでなくソフトウェアが依存する三者構成要素に関する情報も含まれていない。ソフトウェアが依存する三者間コンポーネントや、コンポーネント間の依存関係に関する情報が含まれていない。 ユーザーにとっては柔軟性が高いが、インベントリ情報の網羅性を確保するための標準化が不十分であり、システム運用者や監督部門の管理ニーズを満たすことができない。

ISO/IEC 5962:2021 は、パッケージ情報、ファイル情報、コードスニペット情報、依存関係情報、その他のソフトウェア構成情報を含む、パッケージ関連コンポーネントとメタデータ情報を転送するための標準データフォーマットSPDXを定義している。SPDX フォーマット仕様では、ソフトウェア開発とビルドプロセスを管理するために使用されるサードパーティサービス情報、ツール、システム情報は含まれていない。SPDX フォーマット仕様では、開発ツールやサードパーティサービスプロバイダなどのソフトウェア関連情報が含まれていない。これらは、攻撃者の主要な標的であり、いくつかの主要なソフトウェアサプライチェーンセキュリティ攻撃に密接に関連しているため、ソフトウェア部品表にこのような情報を含めることは、ソフトウェアサプライチェーンセキュリティリスクへの効率的な緊急対応にとって極めて重要である。

中国は、「情報セキュリティ技術ソフトウェアサプライチェーンセキュリティ要求事項」、「情報セキュリティ技術オープンソースコードのソフトウェア製品セキュリティ評価方法」など、ソフトウェアサプライチェーンセキュリティに関する関連標準の策定を開始した。前者は、ソフトウェアサプライチェーンのセキュリティ目標を定め、ソフトウェアサプライチェーンのセキュリティリスク管理要求事項を規定し、供給側と需要側の組織管理と供給活動管理のセキュリティ要求事項を規定しており、ソフトウェアサプライチェーンの供給側と需要側がリスク管理と供給活動管理を実施する際の指針となる。前者は、ソフトウェアサプライチェーンのセキュリティリスク管理要求事項を制定し、需給側の組織

管理及び供給活動管理のセキュリティ要求事項を規定し、ソフトウェアサプライチェーンの需給側がリスク管理、組織管理及び供給活動管理を実施する際の指針となる。

現在、国内外で正式に発表されている標準の中には、最新のソフトウェアサプライチェーン攻撃のシナリオをカバーし、システム運用者や監督部門の管理ニーズを満たすソフトウェア部品表フォーマット標準が存在しないため、本標準の策定は、中国のソフトウェア部品表フォーマット関連標準の空白を埋め、私の情報技術分野の標準および仕様体系を改善することになる。

V. 国際標準に基づく起草、国際標準および外国標準の引用または準拠の有無、国際標準を採用しない理由。

いない。

VI.関連法規、行政法規、関連標準との関係

現在、ソフトウェア・サプライチェーンのセキュリティに関連する中国の既存の法律には、「中華人民共和国サイバーセキュリティ法」、「重要情報インフラのセキュリティ保護に関する規則」、「サイバーセキュリティ審査弁法」などがある。サイバーセキュリティ審査弁法」は、重要情報インフラが調達する製品やサービスについて、サイバーセキュリティ審査を受けることを義務付けており、サイバーセキュリティ審査では、供給途絶などのサプライチェーンリスクを識別できる必要がある。重要情報インフラ保護規則では、事業者は安全で信頼できるネットワーク製品やサービスを調達することが求められているため、事業者は安全で信頼できるネットワーク製品の評価・選定戦略を確立する必要がある。業界レベルでは、金融業界は「金融業界におけるオープンソース技術の応用と開発の規制に関する意見」を発表し、金融機関にオープンソース技術応用口座の設立を求め、金融機関がオープンソース技術のサプライチェーン管理を強化することを支援している。

2018 年、中国はサプライチェーンセキュリティ管理の国家標準である「情報セキュリティ技術 ICT サプライチェーンセキュリティリスク管理ガイドライン」を導入し、サプライチェーンの完全性、機密性、可用性、管理可能性というセキュリティ目標を達成するため、リスク評価の考え方を採用し、製品ライフサイクル全体の観点からリスク分析と管理を実施している。中国は、既に、「情報セキュリティ技術ソフトウェアサプライチェーンセキュリティ要求事項（案）」、「情報セキュリティ技術ソフトウェア製品オープンソースコードセキュリティ評価方法（案）」等、ソフトウェアサプライチェーンセキュリティに関する関連標準の策定を開始している。前者は、ソフトウェアサプライチェーンのセキュリティ目標を確立し、ソフトウェアサプライチェーンのセキュリティリスク管理要求事項を規定し、供給側と需要側の組織管理、供給側と需要側のセキュリティ要求事項、供給活動の管理について規定している。前者は、ソフトウェアサプライチェーンのセキュリ

ティリスク管理要求事項及び需給双方の組織管理及び供給活動管理のセキュリティ要求事項を制定し、ソフトウェアサプライチェーンにおける需給双方のリスク管理、組織管理及び供給活動管理の指針を提供することができ、後者は、ソフトウェア製品に含まれるオープンソースコードのセキュリティ評価目的、評価指標体系及び評価方法を示し、ソフトウェア製品に含まれるオープンソースコードのセキュリティ評価に適用することができる。要約すると、本標準と現行の法律、規制、国家標準との間に矛盾や齟齬はない。

VII. 主な意見の相違の歴史と根拠

現時点ではいない。

特許に関する関連事項

関係ない。

IX.標準の実施要件，並びに組織的措置，技術的措置，移行期間及び実施時期に関する提案などの措置の提案

国家安全保障に影響するソフトウェアシステムは、この標準に基づいて、ソフトウェア部品表を制定し、内容の範囲、生成、生成頻度、生成の深さ、更新チェックの仕組みなどを明確にし、配信プロセス、配信方法、配信プロセスのセキュリティ対策などの配信を含むソフトウェア部品表の生成を明確にし、ソフトウェア資産管理、ソフトウェア脆弱性管理、セキュリティインシデント対応などの内部シナリオの組織内での実際の使用シナリオを明確にする。ソフトウェア資産管理、ソフトウェア脆弱性管理、セキュリティインシデント対応など、組織内におけるソフトウェア部品表の実際の使用シナリオを明確にする必要がある。ソフトウェア部品表管理ツールプラットフォームを構築し、技術的手段によってソフトウェア部品表の統一管理を実現する。

X. その他明確にすべき事項

いない。

ネットワークセキュリティ技術ソフトウェア部品表データフォーマット標準準備グループ

2024 年 4 月 26 日付