経済産業省

資料３－４

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和６年１０月８日

経済産業省

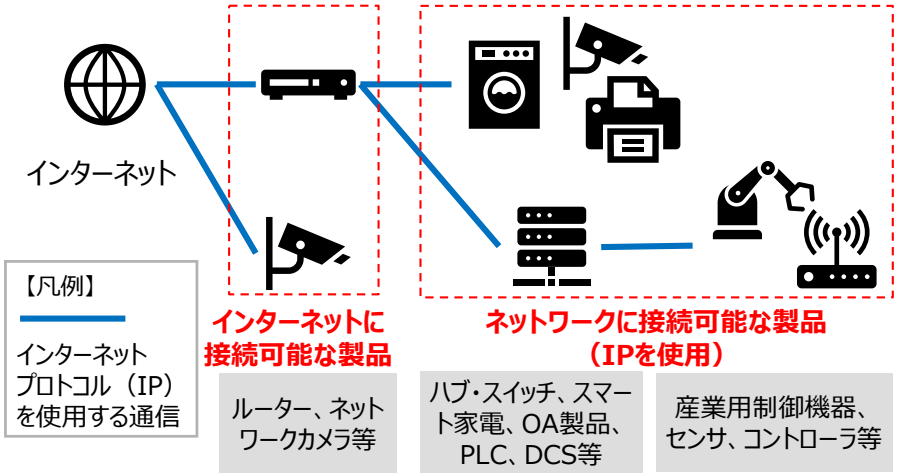
１．「IoT製品に対するセキュリティ適合性評価制度構築方針」の公表

２．「ソフトウェア管理に向けたSBOMの導入に関する手引きver2.0」の公表

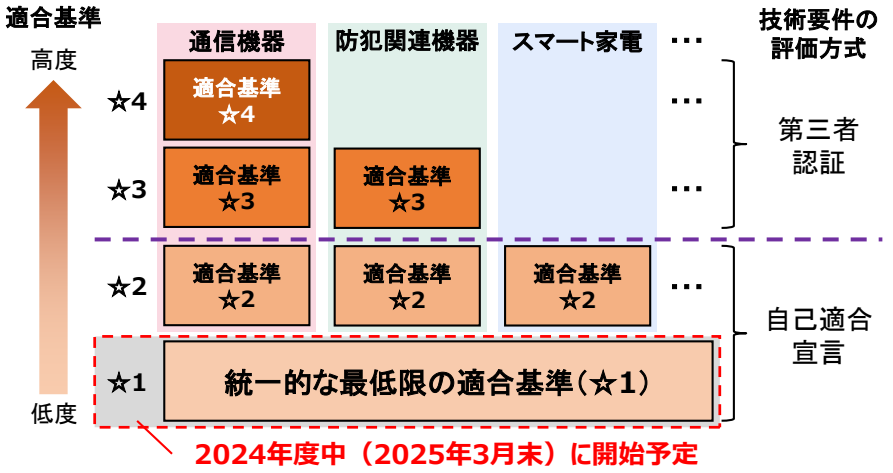
IoTセキュリティ適合性評価制度の概要

- IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省にてIoTセキュリティ適合性評価制度(※1)を構築中。2024年3月～４月にパブリック・コメントを実施し、その結果を踏まえた**制度構築方針(※2)を8月23日に公表**。9月末にIPAから制度開始の案内を実施。
- インターネットに直接的又は間接的に接続されるIoT製品を対象とし、複数のレベル（☆1～4）を用いた任意制度。**全ての対象製品の統一的な最低限の基準（☆１）について、2024年度末（2025年3月末頃）に受付を開始**予定。IoT製品類型ごとの特徴に応じた基準（☆2～☆4）については、順次策定予定。
- G7各国を中心に、諸外国においても同様のIoT製品の適合性評価制度の検討が進んでいる。IoT製品ベンダーの負担を抑えるため、**米・EU当局と相互承認に向けた議論を実施中**。

対象製品の概要(※3)



適合性評価レベル（☆1～☆4）のイメージ

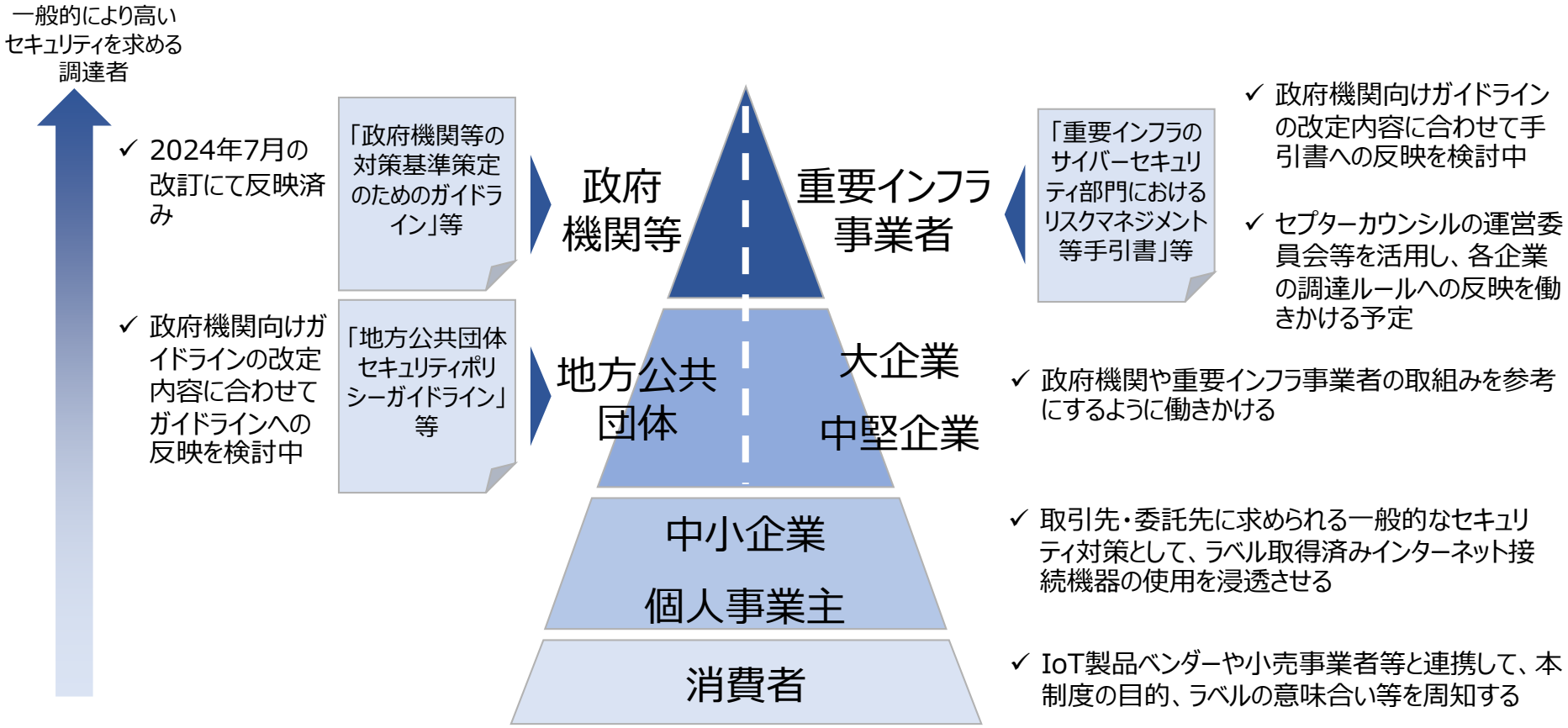


レベル	位置付け	適合基準	評価方式
☆3以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆2	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型別	自己適合宣言
☆1	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	自己適合宣言

(※1)IoTセキュリティ適合性評価制度の概要は、2024年2月の第36回重要インフラ専門調査会にて説明済み
(※2)経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針」 https://www.meti.go.jp/shingikai/mono_info_service/Sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
(※3)国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外

調達者への制度展開戦略

- 今年度、政府機関等、重要インフラ事業者、地方公共団体向けの各ガイドライン類に本制度のラベル付与製品の調達に関する方針を盛り込むよう協議を進める。
- 2024年7月に改訂された政府統一基準群のガイドラインには、本制度の活用方針が反映された。その内容も踏まえて、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」等への反映を検討する予定。
- 併せて、IoT製品ベンダー・団体等にラベル取得を働きかけ、および民間企業・消費者に本制度の目的やラベルの意義等の周知を行い、ラベル取得製品の調達・購入を浸透させていく。



政府統一基準群のガイドラインへの反映

- 2024年7月に公開された政府統一基準群のガイドラインの「4.3 機器等の調達」の解説に、今後の本制度活用を反映済み。

「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」（抜粋）

4.3　機器等の調達

4.3.1　機器等の調達

（解説）

- **基本対策事項 4.3.1(1)-2「必要なセキュリティ機能が適切に実装されていること」について**

必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT 機器等に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。

- 容易に推測可能な初期パスワードの設定禁止
- 主体認証のネットワークを介した総当たり攻撃対策
- 容易に行えるソフトウェアの脆弱性対策（アップデート等）
- 機器内のセキュリティパラメータの保護
- 安全な通信の確保
- 利用者が作成したデータの容易な消去
- 利用しない機能や通信ポートの無効化

本制度☆１適合基準相当の内容

機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、次の「IoT 製品のセキュリティ適合性評価制度」の活用が考えられる。

本制度の活用方針

IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるものである。☆１の取得を確認することで、上記に記載しているセキュリティ機能の実装状況の確認の代用とすることができる。

また同制度では、製品種別毎により高度なセキュリティ適合基準に対する評価を行う☆２（自己適合宣言）、☆３以上（第三者認証）が順次整備される予定である。制度整備の状況を踏まえつつ、2025 年度中に同制度の☆１以上を取得していることを機器等の選定基準に含めるとともに、以降も、☆２、☆３以上の対象機器の拡充に応じて選定基準への反映を順次行っていく予定である。

情報システムの重要度に応じて「重要度：低」は☆１以上、「重要度：高～中」は少なくとも☆３以上の IoT 機器等を各機関等の選定基準に含めることの追加を検討している。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針である。

参考：経済産業省「IoT 製品のセキュリティ適合性評価制度構築方針」
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html）

（出典）NISC「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」 https://www.nisc.go.jp/pdf/policy/general/guider6.pdf

（参考）目的と位置付け

制度構築方針
2.1～2.3

- IoT製品に対する適合性評価制度を国内で構築し、広く普及させ、そして社会に浸透させるためには、まずは**調達者が自身を守るために、求めるセキュリティ水準のラベルが付与された製品を優先的に選択するようになること**が必要不可欠である。そのうえで、IoT製品ベンダーの積極的なラベル取得を促すため、以下の三つを主目的として制度を構築する。

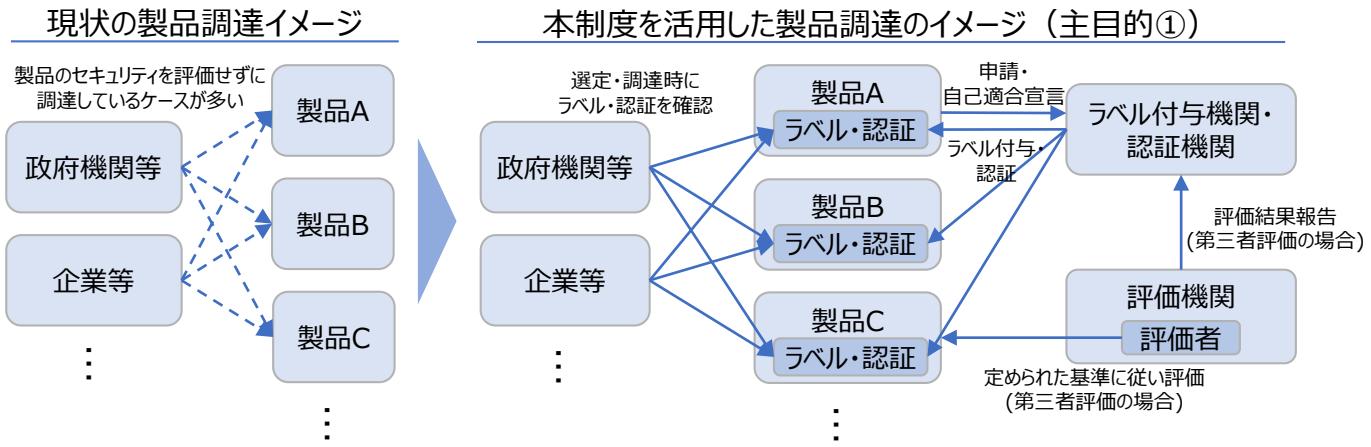
  ① **政府機関や企業等で調達する製品について、共通的な物差しでIoT製品のセキュリティを評価・可視化**できるようにすることで、各組織の求めるセキュリティ水準を満たしたIoT製品の選定・調達を容易にする。

  ② 特定分野のシステムに組み込まれて調達・利用されるIoT製品に求められるセキュリティ要件を定め、必要な認証・ラベルを各業界団体等で指定できるようにすることで、当該**特定分野において求められるセキュリティが確保されたIoT製品のみが採用される**ようにする。

  ③ **諸外国の制度と協調的な制度を構築し、相互承認を図る**ことで、IoT製品を海外に輸出する際に求められる適合性評価にかかるIoT製品ベンダーの負担を軽減する。

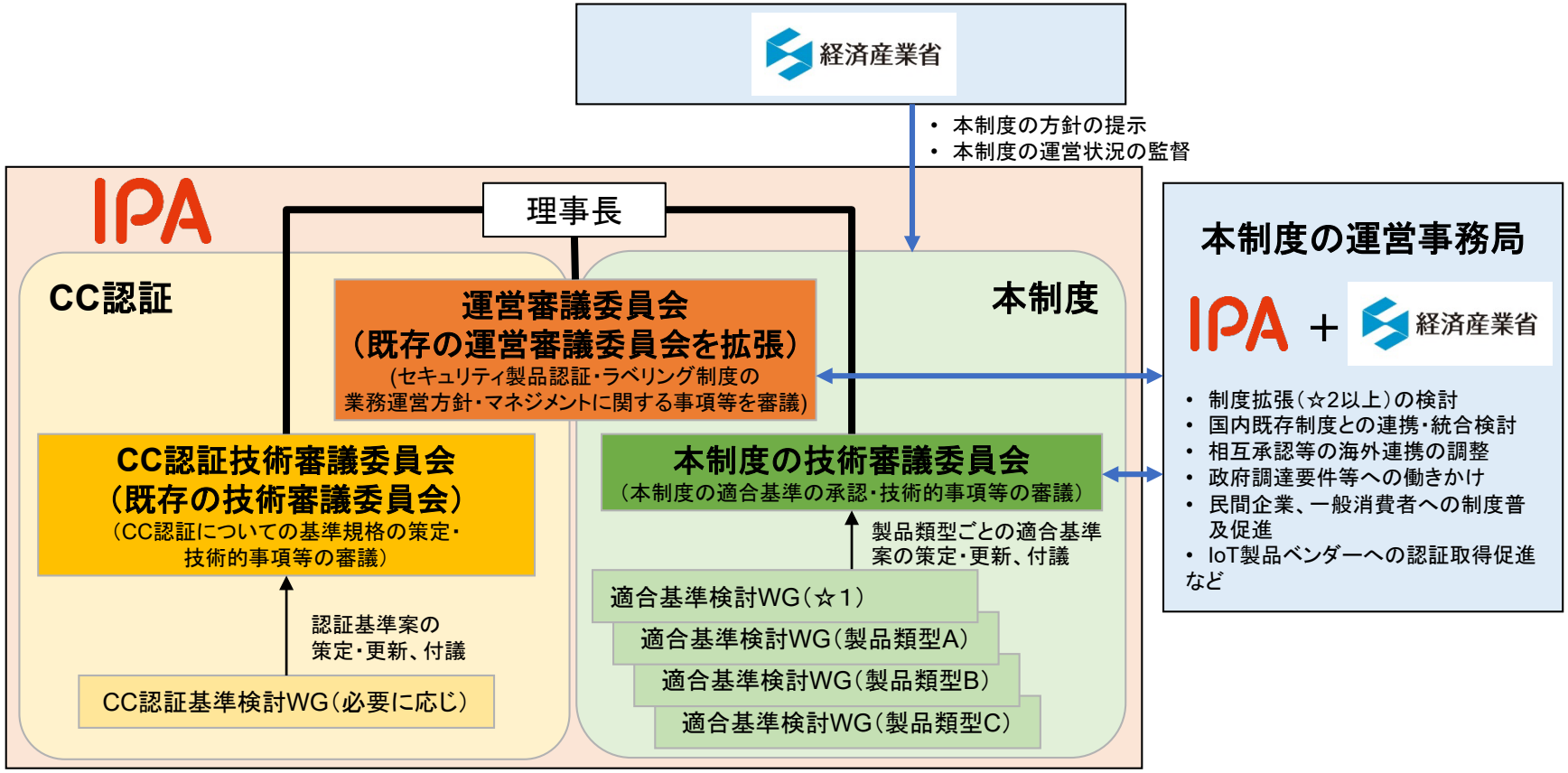
- 本制度は、国内の既存制度と将来的な統合や棲み分け・連携の方針を合意しながら、**任意制度**として構築する。適合性評価を受けた製品に対してセキュリティ要件に応じたラベルを付与することで、製品の付加価値向上に繋げる。

- 主目的①に関して、**まずは政府機関等、重要インフラ事業者、地方公共団体等にラベル付与製品の選定を調達要件に含める**ことを働きかけ、それらのIoT製品ベンダーに本制度のラベルを取得することを促していき、制度が着実に広まる中で、民間の大企業の調達要件での活用、中小企業や消費者への普及を図る



（参考）運用体制

- 経済産業省の示す基本方針に従い、同省の監督のもと、本制度を構築し、運営する**スキームオーナーをIPA**とする。IPAが運営するJISEC制度を、CC認証のみの対象から本制度を含む形に拡張させる枠組みとする。（現行の運営審議委員会を拡張）
- 本制度の**技術審議委員会**は、プレ委員会を引き継ぐ形で**新設**し、本制度についての**適合基準の承認・技術的事項等を審議**する。
- ☆1および☆2以上の各製品類型ごとの適合基準案の策定は、本制度の技術審議委員会の配下に設置する適合基準検討WGにて行う。**各WGは、当該製品類型のIoT製品ベンダーや主な調達組織、それらの関連機関・団体を中心に構成**する想定である。
- **経済産業省も運営事務局に加わり**、制度の拡張・普及や海外との相互承認・連携等について推進する。



制度構築方針
3.4

（参考）セキュリティ要件・適合基準・評価手順（3/3）

- ☆1で考慮する脅威は、☆1で主に想定する守るべき資産、アタックサーフェスを踏まえ、プレ委員会で整理したものである。
- 想定脅威に対して、☆1で必要なセキュリティ要件を全体のリストから抽出し、国内外の基準を参照して**☆1の適合基準（評価手順としては16項目に集約）を作成**している。

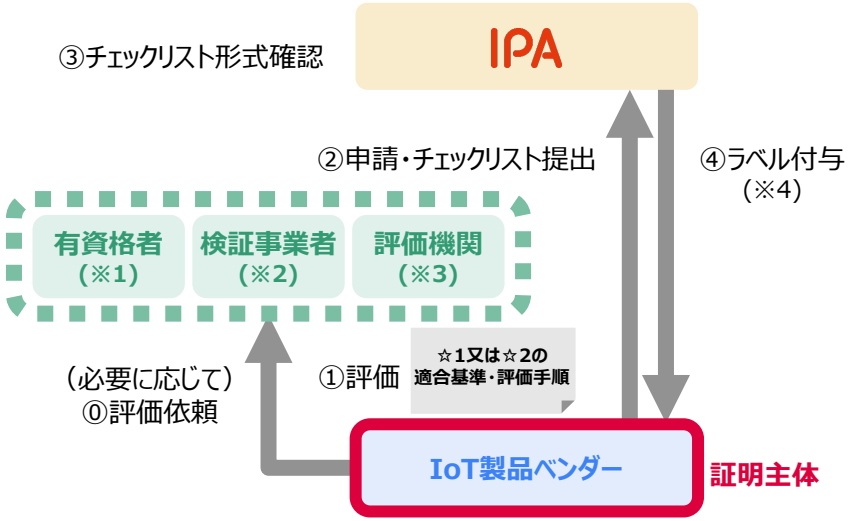
☆1で考慮する主な脅威			脅威に対抗するために☆1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**[1-5]	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)[17-12,17-3,17-5,17-8,17-10]
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能[3-1,3-2] (7)**容易かつ分かりやすいアップデート手順**[3-3] (8)アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10)ユーザが型式番号を認識可能とする記載・機能[3-16]	情報・問い合わせの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開**[2-1] (9)セキュリティアップデートの優先度決定方針の文書化[3-8]
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)[6-1]	–	–
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、匿名化**等)[4-1]	–	–
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)[5-1,5-7]	–	–
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**[11-1]	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)[9-1]	–	–

※「適合基準の概要」欄の先頭の"(N)"は対応する☆1評価項目番号を、末尾の"[N-N]"は対応するセキュリティ要件の番号(複数の場合、代表的な要件を先頭に記載)を示す。
※ 複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。

（参考）適合性評価の主体

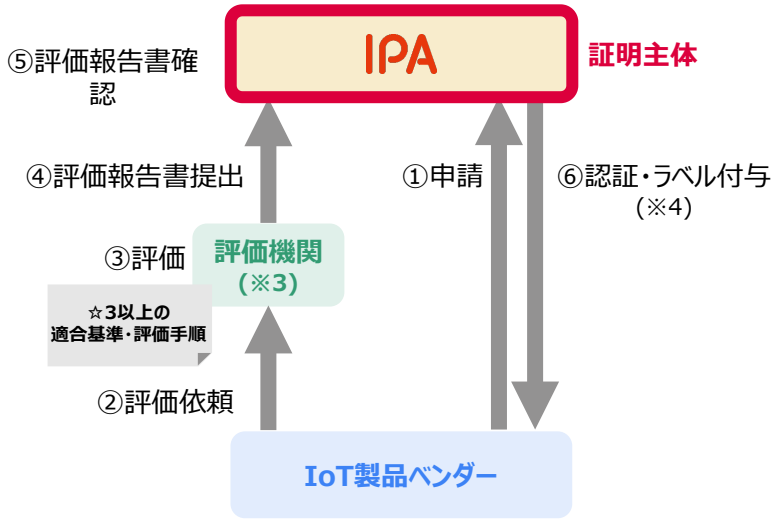
- 制度を広く普及させるため**☆1、☆2は自己適合宣言によるラベル付与**とし、高い信頼性が求められる**☆3以上は独立した第三者による評価を受ける第三者認証**とする。
- ☆1、☆2では、IoT製品ベンダーの自己評価に加え、**有資格者(※1)や検証事業者(※2)、評価機関等への評価の委託も可能**である。
- ☆3以上では、**ISO/IEC17025に基づく本制度の評価機関認定(※3)を受けた評価機関による評価**を求める。

☆1、☆2（自己適合宣言）



① IoT製品ベンダーは、☆1又は☆2の適合基準・評価手順を用いて評価を実施し、チェックリストを作成する。
なお、有資格者や検証事業者、評価機関等に評価を委託してもよい。
※ ☆2において有資格者や検証事業者、評価機関による評価実施を求めるかは別途検討
② IoT製品ベンダーは、IPAに申請を行い、チェックリストを提出する。
③ IPAは、チェックリストの形式確認を行う。
④ IPAは、申請されたIoT製品に対し、ラベルを付与する。

☆3以上（第三者認証）



① IoT製品ベンダーは、IPAに申請を行う。
② IoT製品ベンダーは、評価機関に対して、評価依頼を行う。
③ 評価機関は、☆3以上の適合基準・評価手順を用いて評価を実施する。
④ 評価機関は、評価報告書をIPAに提出する。
⑤ IPAは、認証機関として、評価報告書の内容に問題がないか確認する。
⑥ IPAは、申請されたIoT製品に対し、認証・ラベルを付与する。

(※1)指定資格の保有者（情報処理安全確保支援士等）が、IoTセキュリティ評価に関する研修受講完了又は評価ガイドラインを理解していることの宣誓したうえで、評価又は評価結果の確認を実施した場合に「有資格者」による評価とする。
(※2)情報セキュリティサービス基準への適合性について審査及び登録する情報セキュリティサービス基準審査登録制度の機器検証サービス（2023年9月より募集開始）にサービスが登録されている事業者を「検証事業者」とする。
(※3)製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度(ASNITE)の中に、本制度の☆3以上の評価を行える事業者についてISO/IEC17025に基づく評価機関認定制度を設け（2024年度以降、別途検討）、適切な能力及び体制を整備した事業者を「評価機関」として認定する。
(※4) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

制度構築方針案
3.6～3.7

（参考）ラベルの意味合いと信頼性確保の仕組み

- 本制度の**ラベルは、あくまで定められた適合基準への適合を示すもの**であり、ラベルが付与されているからといって、IoT製品のセキュリティが完全に確保されていることを保証するものではない。
- 本制度は任意制度であるため、**ラベルの表示義務は設けない**。製品本体、パッケージ、マニュアル、パンフレット、Webサイト等に掲載する場合は、**本制度のロゴ**及びラベル付与製品毎の**情報提供ページのURLを埋め込んだQRコードを掲載**する。
- 自己適合宣言の有効期限は**ラベル取得日を起点として最大2年間**とし、その後ラベルを継続する場合は**自己適合宣言**を再度行う。
- **スキームオーナーはラベル付与製品に対して検査やサーベイランスを行える権利を有する**。☆1では、コストの観点から定期的なサーベイランスは行わず、**基準への適合に疑義が生じた場合に、必要に応じ、証跡提出の要求やサーベイランス**の実施を行う。

各評価レベルにおけるラベルの意味合い

評価レベル	ラベルの意味合い
☆1、☆2 （自己適合宣言）	ラベル取得時点において定められた適合基準へ適合していることについて、IoT製品ベンダー自らが宣言したことを示すもの。（証明主体はIoT製品ベンダー自身） IPAはラベル付与機関として評価結果を記載したチェックリストの形式確認は行うが、IoT製品のセキュリティ適合性等を、IPAが認証するものではない。
☆3以上 （第三者認証）	ラベル取得時点（再評定時を含む）において定められた適合基準へ適合していることについて、認証機関となるIPAが認証したことを示すもの。（証明主体はIPA） IPAは、独立した第三者である評価機関が本制度の定める適合基準及び評価手順に従い評価した結果を確認したうえで、当該基準への適合に対する認証を行う。ただし、IPAは、評価機関による評価の結果を適切に確認する責任を負う一方、ラベルを取得した当該IoT製品に対して、明示あるいは黙示を問わず、いかなる保証も行わない。

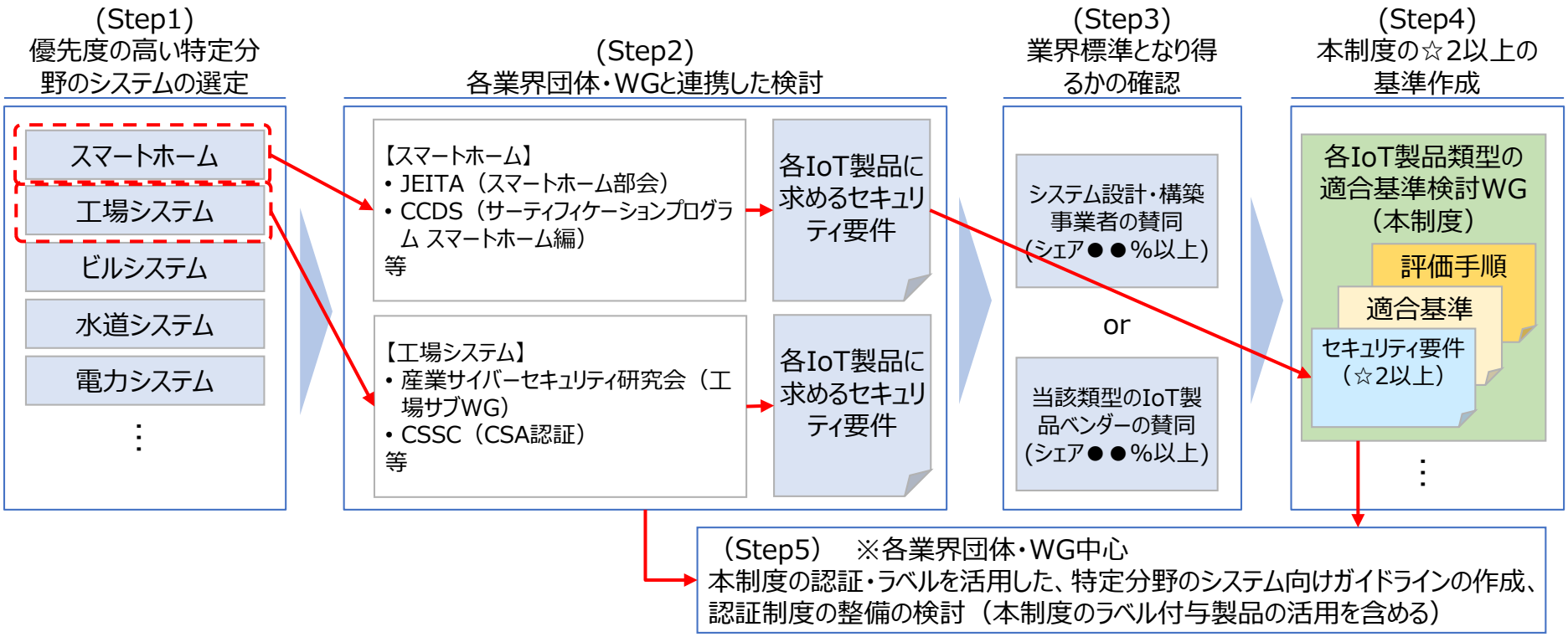
情報提供ページの掲載情報案

掲載情報	掲載内容
本制度の概要	• 本制度の概要及び詳細説明HPのURL
製品情報	• 製品名 • 型式番号 • IoT製品の製造業者名　※公開/非公開は任意 • 製造国又は地域　※公開/非公開は任意 • 製品概要 • 製品WebサイトのURL • 製品の問い合わせ先 • 他認証の認証番号等
ラベル情報	• ラベル識別番号 • 当該製品の適合性評価レベル（☆1～☆4） • 当該製品の製品類型の名称　※☆2～☆4の場合 • 評価された適合基準のバージョン • 適合評価結果（チェックリスト又は評価報告書等） • ラベルステータス情報 • ラベル発行・更新日 • ラベルの有効期限 • 申請者名 • 評価者区分
安全情報	• 当該製品に関わる脆弱性情報 • 脆弱性の報告窓口のURL
その他セキュリティ関連情報	• 必要があれば、IoT製品ベンダーから調達者に向けたセキュリティ関連情報

制度構築方針
3.8.2

（参考） 特定分野のシステムに関する業界団体・WGとの連携

- 製品単体で比較されず、特定分野のシステムに組み込まれて調達されるIoT製品について、以下の観点で**検討優先度の高い特定分野のシステムを選定**し、各システム全体のセキュリティを考えている業界団体やワーキンググループと連携し、各システムに組み込まれるIoT製品に求めるセキュリティ要件や☆**2以上の適合基準をその必要性も含めて検討**を検討する。
  - 意識しないまま**セキュリティ対策が十分でないIoT製品を利用している中小企業や消費者が多い**と考えられる分野のシステム
  - インシデント発生時の社会的な影響が大きい**重要インフラ分野**のシステム
- 各分野において、IoT機器を選定する立場の事業者又は当該IoT製品を製造するベンダーから、認証・ラベル制度の整備とその活用について一定割合以上の賛同が得られる場合（**業界標準となり得ると判断される場合**）、本制度として☆2以上の整備を進める。
- 各特定分野の**システム全体のセキュリティガイドラインの作成や認証制度等の整備は、各業界団体やワーキンググループで検討**し、本制度はオブザーバーの立場で連携する。



制度構築方針
3.8.3

（参考） 諸外国制度との連携

- 諸外国においても同様のIoT製品の適合性評価制度の検討が進んでいる。国内IoT製品ベンダーの負担を抑えるため、主要国制度の基準も参考にしながら本制度の基準を検討し、**相互承認の調整**を図る。
- ☆1開始の正式案内時に制度が既に導入されている**シンガポールと英国とは、案内時に相互承認の方向性を提示**する予定。正式案内時に制度設計途中の見込みである**欧米については、順次方向性を公表**する。

国・地域	日本	シンガポール	英国	米国	EU
制度名	検討中	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI法)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) ※欧州委員会草案の内容
開始時期	• ☆1：2024年度下期(2025年3月)開始予定 • ☆2以上：2025年度以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定	未定（報告義務を除き2027年開始想定）
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者向け無線IoT機器	デジタル製品
適合基準	☆1：ETSI EN 303 645及びCLSの記載内容を中心に検討（ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討）	• ＊1：ETSI EN 303 645の基準の一部(※1) • ＊2：＊2の基準に加え、ETSI EN 303 645の基準の一部(※2) • ＊3及び＊4：＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	• 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意済。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定。
評価方法	• ☆1、☆2：自己適合宣言 • ☆3以上：第三者	• ＊1及び＊2：自己適合宣言 • ＊3及び＊4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	• 「重要なデジタル製品」以外の製品：自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（リスクが低い製品）でEUCCやEN規格の対象外の製品及びクラスⅡ（リスクが高い製品）の製品：第三者認証

(※1) ETSI EN 303 645のサイバーセキュリティ規定5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16
(※2) ETSI EN 303 645のサイバーセキュリティ規定5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1及びデータ保護規定6.1、6.2、6.3、6.5

１．「IoT製品に対するセキュリティ適合性評価制度構築方針」の公表

２．「ソフトウェア管理に向けたSBOMの導入に関する手引きver2.0」の公表

「ソフトウェア管理に向けたSBOMの導入に関する手引」の改訂概要

- セキュアなソフトウェアの流通を促進するため、経済産業省では、**ソフトウェアの部品構成表であるSBOM（Software Bill of Materials）の企業による活用を推進**。
- 2023年7月28日、企業が**SBOMを導入するメリットや実際に導入するにあたって実施すべきポイント**をまとめた手引書を「**ソフトウェア管理に向けたSBOMの導入に関する手引ver1.0**」として公表。
- 今般、中小企業も含め、あらゆる企業にとって**SBOMをより効率的に活用できる方法等を検討**し、その内容を盛り込む形で、**「導入手引」を改訂。**

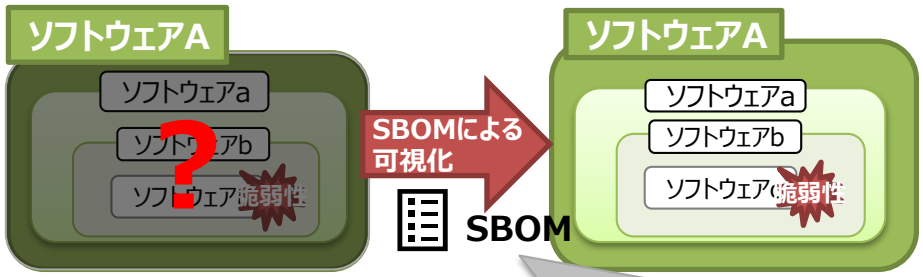
【主な改訂のポイント】

- ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方をまとめた「**脆弱性管理プロセスの具体化**」
- SBOM導入の効果及びコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワークである「**SBOM対応モデル**」
- 委託先との契約等においてSBOMに関して規定すべき事項（要求事項、責任、コスト負担、権利等）を示した「**SBOM取引モデル**」

ソフトウェア・セキュリティ確保手段としてのSBOM

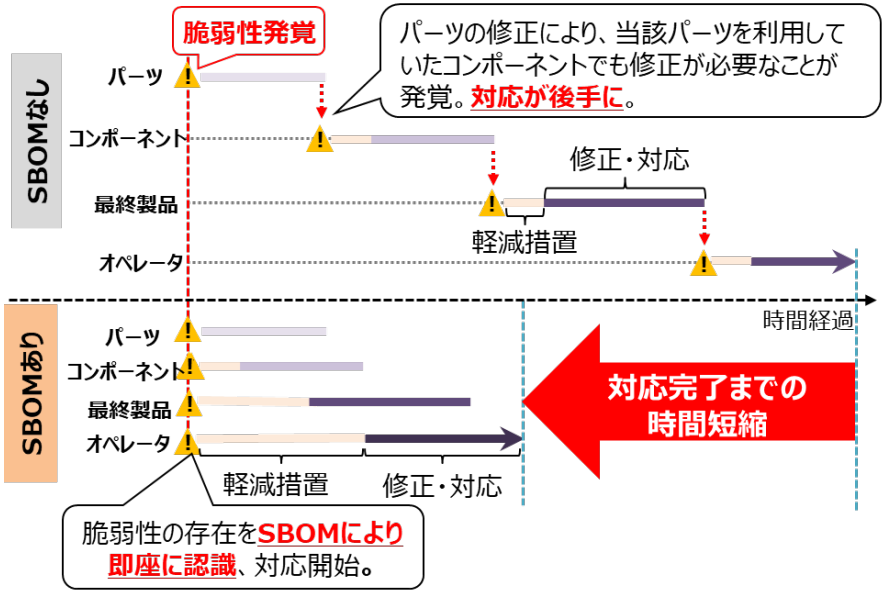
- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。ソフトウェアを構成する**各部品（コンポーネント）を誰が作り、何が含まれ、どのような構成となっているか**等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができるため、脆弱性情報の即時の特定が可能であり、**脆弱性対応などへの活用が期待**できる一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、**「ソフトウェア管理に向けたSBOMの導入手引ver1.0」を公表**。SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示す。

＜SBOMイメージ＞



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	……	…

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェアの利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOM活用の効果が確認できた。一方、SBOM導入・活用に際しては様々な課題(例：脆弱性管理の効率化、分野や用途に応じたSBOMの適切な範囲、ソフトウェアの調達者と供給者の立場間の取り決め）が存在することが明らかとなった。
- 本手引では、**SBOMに関する「基本的な情報」や「誤解と事実」を提供し、**企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び認識しておくべきポイント**を示す。(ver1.0)
- 加えて、ソフトウェアの脆弱性を管理する一連プロセスにおいて**SBOMを効果的に活用するための具体的な手順と考え方**、SBOM導入の効果及びコストを勘案して**SBOMを導入することが妥当な範囲を検討するためのフレームワーク**、ソフトウェアの受発注において、**調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考例**を示す。(ver2.0)

対象読者

- 主にパッケージソフトウェアや組込みソフトウェアに関する **ソフトウェアサプライヤー**
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス(ver1.0)

フェーズ1 環境構築・体制整備
- 1-1. SBOM適用範囲の明確化
- 1-2. SBOMツールの選定
- 1-3. SBOMツールの導入・設定
- 1-4. SBOMツールに関する学習

フェーズ2 SBOM作成・共有
- 2-1. コンポーネントの解析
- 2-2. SBOMの作成
- 2-3. SBOMの共有

フェーズ3 SBOM運用・管理
- 3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施
- 3-2. SBOM情報の管理

脆弱性管理プロセスの具体化(ver2.0)

- SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、**SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要。**
- 脆弱性管理の一連プロセスにおいてSBOMを効果的に活用するための**具体的手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報**を提供。

SBOMを活用した脆弱性管理プロセス

フェーズ1 脆弱性特定
- マッチング手法区分選択
- 利用可能なSBOMデータ特定
- 脆弱性DBの選択
- マッチング手法の選択・作成

フェーズ2 脆弱性対応優先度付
- 予備フィルタリング
- 優先度付情報の選択・取得
- 判断ツリーに基づくカテゴリ判定
- 優先度スコア評価

フェーズ3 情報共有
- 共有情報と共有相手の特定
- 共有方法の特定と実施

フェーズ4 脆弱性対応
- 脆弱性の暫定対応
- 脆弱性の根本対応

SBOM対応モデル(ver2.0)

- SBOM導入の効果及びコストを勘案してSBOMを導入することが**妥当な範囲を検討するためのフレームワーク(5W1Hを網羅するよう体系化)**。
- 実証を通じて、**医療機器、自動車、ソフトウェア製品等の分野**において、コスト・効果を考慮して妥当な対応範囲の参考例を提示。
- 当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できる。

SBOM取引モデル(ver2.0)

- ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して**契約に規定すべき事項（要求事項、責任、コスト負担、権利等）**について参考となる例を示す。
- 既存のソフトウェアに関するモデル契約書と組合せることで、**SBOMに対応した契約書を作成する際の項目案を提示**するもの。

ver1.0の内容

（参考）ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。
- ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOMを活用することで効率的なソフトウェア管理を実施できることが確認できた一方で、実際のSBOM導入に際しては様々なハードルが存在することが明らかとなった。
- 本手引では、**SBOMに関する基本的な情報やSBOMに関する誤解と事実を提供**するとともに、企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び導入にあたって認識しておくべきポイント**を示す。

対象読者

- 主に、パッケージソフトウェアや組込みソフトウェアに関するソフトウェアサプライヤー※
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

※ このうち、以下に示すようなSBOM初級者を特に対象としている。

- ソフトウェアにおける脆弱性管理に課題を抱えている組織
- SBOMという用語は聞いたことがあるが具体的な内容やメリットは把握できていない組織
- SBOMの必要性は理解しているが、導入に向けた取組内容が認識できていない組織　など

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス

フェーズ1　環境構築・体制整備フェーズ

- **1-1. SBOM適用範囲の明確化**
  - ✓ SBOMを作成する対象ソフトウェアに関する情報（言語、開発ツール、構成図、契約形態・取引慣行、規制要求事項、SBOM導入に関する組織内の制約等）を整理する。
  - ✓ 整理した情報を踏まえて、SBOM適用範囲を明確化する。
- **1-2. SBOMツールの選定**
  - ✓ SBOMツールの選定の観点を整理し、当該観点に基づきSBOMツールを評価・選定する。
    （選定観点の例：機能、性能、解析可能な情報・データ形式、コスト、対応フォーマット、解析方法、サポート体制、他ツールとの連携、ユーザーインタフェース、対応する言語、日本語対応等）
- **1-3. SBOMツールの導入・設定**
  - ✓ SBOMツールが導入可能な環境の要件を確認し、整備する。
  - ✓ 取扱説明書等を確認して、SBOMツールの導入・設定を行う。
- **1-4. SBOMツールに関する学習**
  - ✓ 取扱説明書等を確認して、SBOMツールの使い方を習得する。
  - ✓ ツールの使い方に関するノウハウや各機能の概要は記録し、組織内で共有する。

フェーズ2　SBOM作成・共有フェーズ

- **2-1. コンポーネントの解析**
  - ✓ SBOMツールを用いて対象ソフトウェアのスキャンを行い、コンポーネントの情報を解析するとともに、コンポーネントの解析結果について、コンポーネントの誤検出や検出漏れが無いかを確認する。
  - ✓ SBOMツールを用いることで、手動の場合と比較して効率的にコンポーネントの解析及びSBOMの作成を行うことができる。
  - ✓ パッケージマネージャーを用いることで、SBOMツールでは特定できない粒度の細かいコンポーネントを特定できる場合がある。
- **2-2. SBOMの作成**
  - ✓ 作成するSBOMの項目、フォーマット、出力ファイル形式等のSBOMに関する要件を決定し、当該要件を満足するSBOMを作成する。
- **2-3. SBOMの共有**
  - ✓ 対象ソフトウェアの利用者及びサプライヤーに対するSBOMの共有方法を検討した上で、当該方法に基づきSBOMを共有する。

フェーズ3　SBOM運用・管理フェーズ

- **3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施**
  - ✓ 脆弱性に関するSBOMツールの出力結果を踏まえ、深刻度の評価、影響度の評価、脆弱性の修正、残存リスクの確認、関係機関への情報提供等の脆弱性対応を行う。
  - ✓ ライセンスに関するSBOMツールの出力結果を踏まえ、OSSのライセンス違反が発生していないかを確認する。
- **3-2. SBOM情報の管理**
  - ✓ SBOMに含まれる情報やSBOM自体を適切に管理する。
    ※ SBOMの管理は、組織内のPSIRTに相当する部門が対応することが効果的
  - ✓ 自動で脆弱性情報が更新・通知されるSBOMツールを用いることで、新たな脆弱性に関する情報を即座に把握することができる。ツールを用いた自動管理ができない場合、担当者を別途設置するなど運用面でカバーする。

ver2.0追加内容

（参考）脆弱性管理プロセスの具体化

背景・目的

- SBOMを活用した脆弱性管理の方法と手順についてプロセスに基づく具体例を示す。
- SBOMを活用した脆弱性管理においては、**現状では未解決の課題**が存在し、それらの課題を十分に解決するためには、新たな**技術開発、標準化、ツール環境整備**などが必要になる。
- 本章では、それらの課題も含めて、SBOM利用者側の運用によって課題を回避するための考え方や現状で可能なベストプラクティスについて示す。

主な課題と解決アプローチ・ノウハウ等

課題	解決アプローチ・ノウハウ
部品IDが併存し、脆弱性DBとの突合に障害	Purl2cpeなどID変換ツールの利用やAPIを用いたID部分照合
多様な脆弱性DBの網羅性の確保	リスクとコストの低減効果に基づく脆弱性DBの選択方法の提示
脆弱性対応の優先付けによる迅速対応と効率化	SSVCをベースとした判断ツリーによる優先付けカテゴリ判定法の提示
サプライチェーンを通じた情報共有と役割分担	情報共有のステップと開発者・ユーザによる実施項目の提示
脆弱性対応の役割分担	暫定対応・本格対応における開発者・ユーザによる実施項目の提示

SBOMを活用した脆弱性管理プロセス（概要）

フェーズ1 脆弱性特定

1. **マッチング手法区分の選択**
   組織の目的、技術力、利用環境に応じて、SBOM既成ツール、APIスクリプト利用、WebUIの３手法から選択する。
2. **利用可能なSBOMデータの特定**
   サプライヤーからのSBOM提供、ツールを用いたSBOM作成など、利用可能なSBOMデータを特定する。
3. **脆弱性DBの選択**
   脆弱性情報のカバレッジ拡大、自動化・効率化、優先付けの精度向上など、リスク低減、コスト低減などの目的に応じて重要度の高いDBを選択する。
4. **マッチング手法の選択・作成**
   以上の選択肢を総合して、脆弱性特定手法を決定する。

フェーズ2 脆弱性対応優先付け

1. **予備的フィルタリング**
   外部情報を活用した優先付けの前に、既知の情報から対応が必要な脆弱性情報を絞り込む。
2. **優先付け情報の選択・取得**
   リスクの構成要素に基づき、インシデントの有無、Exploitコードの流通状況、CVSS、VEX情報など自社のポリシーに従い必要な情報を選択・取得する。
3. **判断ツリーに基づくカテゴリ判定**
   SSVCに基づき整理した判断ツリーに従い、（開発者、ユーザ組織）×（技術力の高・低）応じて優先付けカテゴリ判定を行う。
4. **優先度スコア評価**
   1から３のステップと並行して、必要に応じて、必要に応じて定量的なスコアリングによりカテゴリ内の優先付けを行うことで詳細な優先付けを行う。

フェーズ3 情報共有

1. **共有情報と共有相手の特定**
   ・共有情報の特定：脆弱性情報、負荷情報、優先付け判定結果など共有情報を特定する。
   ・共有相手の特定：社会組織、社外（ユーザ、ベンダー、サプライヤー―）などの共有相手、順序を特定する。
   ・共有認知・トリガー：プッシュ型、プル型など共有のトリガーを特定する。
2. **共有方法の特定と実施**
   ・共有方法の特定：ファイル送受信、SaaSなど共有方法を特定。
   ・アクセス権限の特定：機密性に応じて、非公開、開示範囲、権限などを特定。
   ・共有実施：決定した共有方法、アクセス権限に基づき共有を行う。

フェーズ4 脆弱性対応

1. **脆弱性暫定対応**
   ・暫定策の検討：利用中断、縮退、回避策など暫定策の検討
   ・暫定策の適用：決定した暫定策について、ステークホルダーに周知し適用する。
2. **脆弱性根本対応**
   ・根本対応の実施：脆弱性に関わるソフトウェアの開発者を特定し、開発者が脆弱性を修正する
   ・SBOM/VEX更新：脆弱性修正に伴い、SBOM、VEX情報を更新する。
   ・SBOM/VEXの共有：供給先に更新したSBOM/VEXを提供し、必要に応じてSBOM履歴管理を行う。

ver2.0追加内容

（参考）SBOM対応モデルの概要

SBOM対応モデルの構成要素

- SBOMの作成・活用に関する選択肢について、コストと効果への影響の大きい項目について5W1Hを網羅するように体系化。実証および有識者委員会の意見を反映してSBOM対応項目を整理。
- 実証を通じて、医療機器、自動車、ソフトウェア製品等の分野において、コスト・効果を考慮して妥当な対応範囲の参考例を提示

SBOM対応項目の選択肢

	適用区分	主な適用項目（選択肢）	コスト	主な実施内容とコスト要素
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社	小	自社開発で直接利用する部品を構成ファイルなどから特定し、SBOMを生成する。コード改変部品を含む。
		(a2)サプライヤ（開発委託先）取引契約あり	中	取引契約のある開発委託先のソフトウェアで利用する部品のSBOMを生成する。
		(a3)サプライヤ（サードパーティ）取引契約なし	大	取引契約によるSBOMの要件化できないOSSや既成部品ベンダーがSBOMを作成する。(b2)(c2)
	(b)部品範囲 (What, Where)	(b1)直接利用部品※1	小	開発者が直接利用する部品を構成ファイルなどから特定し、ツールなどでSBOMを生成する。
		(b2)間接利用部品※2	大	サードパーティ部品について、再帰的に利用される部品に対してSBOMを生成する。
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成	小	直接利用する部品情報を構成ファイルなどを用いて作成する。
		(c2)ツールで特定・生成・誤検知精査なし	中	ツールを用いてSBOMを生成し、精査は省略する。ツールの利用は再帰部品のSBOM生成を主に想定するため商用ツールの利用を想定する。
		(c3)ツールで特定・生成・誤検知精査あり	大	商用ツールを用いてSBOMを生成し、ソースコードレビューを行い、誤検知、検出漏れの精査を行う。（再帰利用部品を含む）
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査	大	開発委託元が、開発委託先の作成したSBOMを受け入れる際に、ツールなどで独立してSBOMを作成するなどして信頼性を検査する。
	(c')生成手段（部品検出手法）	依存関係解析	中	パッケージマネージャ等の構成情報を静的に解析する。
		ファイル照合	中	ハッシュ値当を用いてソースコードのファイル単位の一致を検出する。OSSのライブラリの検出なども含む。
		スニペット解析	大	ソースコードの部分的な文字列一致や類似性により検出する。
		バイナリ解析	大	バイナリファイルのビットパターンなどをもと類似性を検出する。
		実行形式内部の再帰的な依存解析	大	実行形式内にリンク済みのライブラリについて、そのライブラリをビルドする際の依存解析を再帰的に行う。
		上記に対応しない。	小	予め認識している部品をSBOMに変換する。
	(c'')生成手段（対象ソフト種別）	開発時に確定する部品	小	スタティックライブラリ、アプリケーション
		実行時に確定する部品	中	ランタイムライブラリ、サービス（ローカル、外部クラウド）、OS、ミドルウェア、実行環境（コンテナ、VM、APサーバ）
		周辺ツール環境	大	開発運用で使用するツール（インストーラ、アップデータ、配布パッケージ、開発環境、ツールチェーン、SBOMツール）
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）	中	SPDXなどの標準フォーマットで作成する。
		(d2)大統領令におけるデータフィールドの最小要素を含む	中	大統領令におけるデータフィールドの最小要素を含むSBOMを作成する。
		(d3)上記を満たさない要素	小	独自の最小限の要素を作成する。
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定	小	NVD, JVN等のDBを対象として脆弱性の検索・特定を行う。
		(e2)脆弱性の深刻度評価	中	CVSS値をベースとした深刻度を評価し、脆弱性対応の優先度を設定する。
		(e3)脆弱性の悪用可能性等の評価と対処	中	VEX情報等を用いて悪用可能性、脆弱性対処の必要性を評価する。必要に応じて対処策等のアドバイザリを発行する。
		(e4)ライセンス特定	中	ライセンスの特定と規約の取得を行う。
	(f)活用主体 (Who)	(f1)製品利用者	小	脆弱性が特定された場合、利用を中断し、ベンダーによる修正を待つ。業務中断コストも考慮すれば損害は大きい。
		(f2)最終製品ベンダー	中	利用者に脆弱性を通知するとともに、開発者への修正依頼、修正後のビルド・利用者への提供を行う。必要に応じて当局、ISAC等に報告する。
		(f3)各部品の開発者	大	開発者は、脆弱性の監視と修正を行い、調達者に修正版を提供する。必要に応じて当局、ISAC等に報告する。

ver2.0追加内容

（参考）SBOM取引モデルの概要

SBOM取引モデルの主な構成要素（契約で規定することが期待される事項）

- 契約で規定すべき事項として、SBOMに関する要求事項、責任、コスト負担、権利などの区分で整理される。業界の取引慣行、タスクフォース意見を網羅するように整理。脆弱性管理、ソフトウェア品質保証に重要な要件を言語化。主に要件定義後の請負契約が対象と想定。

区分		規定すべき事項	レベル
SBOM要求事項	フォーマット・標準	**（SBOMフォーマット）※1** 採用するSBOM標準フォーマットについて規定する。（SPDX, CycloneDX, SWID等の標準とバージョンを規定）	基礎
		（ID標準）※1 採用する部品ID標準を規定する。（CPE, PURL, SWD, 独自形式等）	基礎
		（SBOM最小要素）※1 採用するSBOMフォーマットの要素項目のうち最小要素を規定する。NTIAのSBOM最小要素を参考にする。	基礎
	品質・信頼性 （SBOM対応モデルに該当）	**（対象サプライヤ契約形態）** SBOM作成範囲として、委託開発契約、サードパーティ利用規約（商用既製品、OSS）の契約形態による範囲を規定する。	基礎
		（再帰的利用部品）※1 SBOM作成範囲として、直接利用部品か再帰的な間接利用部品までとするか規定する。	発展
		（構成解析手法の適用範囲）※1 間接利用部品について、部品を特定する際に利用する構成解析手法の適用範囲を規定する。（依存関係解析、ファイル照合、スニペット解析等）	発展
		（部品精査の要否）※1 ツールによる部品特定の結果に対して、手動による誤検知・検出漏れの精査の要否を規定する。	発展
		（部品の対象フェーズ）※1 部品情報の範囲としてビルド時、ランタイム、クラウドサービス等の範囲を規定する。	発展
		（サードパーティ部品の事前合意） サードパーティ部品（商用部品、OSS）を利用する場合、事前の申告と合意の要否について規定する。	基礎
	保守・運用	**（共有方法）※1** SBOMファイルによる授受またはSaaS等によるリアルタイム共有について規定する。	基礎
		（VEX対応）※1 SBOMに関連する脆弱性情報について悪用可能性に基づくVEX情報の提供を行うか規定する。	発展
		（SBOM更新）※1 ソフトウェアのアップデート、SBOM不具合修正等に応じて、SBOMを更新する期限や頻度を規定する。	基礎
		（脆弱性監視・通知） ソフトウェアの運用フェーズにおいて、脆弱性を監視し、脆弱性が発見された場合に、調達者に通知の期限を規定する。	発展
		（脆弱性対応・優先付け）※1 脆弱性が発見された際に、脆弱性対応の要否、優先付け（トリアージ）について調達者に情報提供を行うか規定する。	発展
		（EOL・EOS） サードパーティ部品および委託開発部品のEOL、EOSやその期限変更に対する通知について規定する。	発展
責任と保証		**（エビデンス提出）** SBOM要求事項について適合していることを証明するエビデンス、第三者証明の提出の要否について規定する。	発展
		（契約不適合責任） SBOM要求事項に対する不適合が見つかった場合には、SBOM修正等の瑕疵対応の要否について規定する。	基礎
		（損害賠償）※2 SBOM要求事項の不適合が原因で事故が発生した場合、損害賠償額上限等について規定する。ライセンス違反の損害賠償を含む。	基礎
		（免責） SBOM要求事項への適合性エビデンスを提出している場合について、技術的制約（ツールの誤検知など）に帰する理由で、損害が発生した場合について損害賠償の制限、免責について規定する。	発展
コスト負担		**（見積）※2** SBOM要求事項、責任・保証に基づき見積の作成し、その合意金額に基づき対価支払について規定する。	基礎
権利・機密保持		**（知的財産権の帰属）** 作成したSBOMの知的財産権、使用権の帰属、第三者への提供可否について規定する。	発展
		（機密保持） SBOMの機密保持・管理およびSBOMを用いたリバースエンジニアリングの禁止について規定する。	発展

凡例：基礎 分野共通で最低限期待される事項
発展 特定分野、要求レベルの高い分野で期待される事項

※1　発注仕様書に記載することも想定される。
※2　ソフトウェア開発一般の請負契約と共通化することが想定される。