

PSIRTを支援するSBOM管理ソリューション

Cyber Regulation Platform(PSIRTモジュール)

開発、製造、PSIRTが連携して製造物責任を果たす取り組みを始めよう

サイバーフィジカルシステムやIoTの時代になり、メーカーは製造物責任（PL法）を果たすためにセーフティに加えてセキュリティ対策が必須となっており、セーフティと同様に以下の説明責任が求められています。

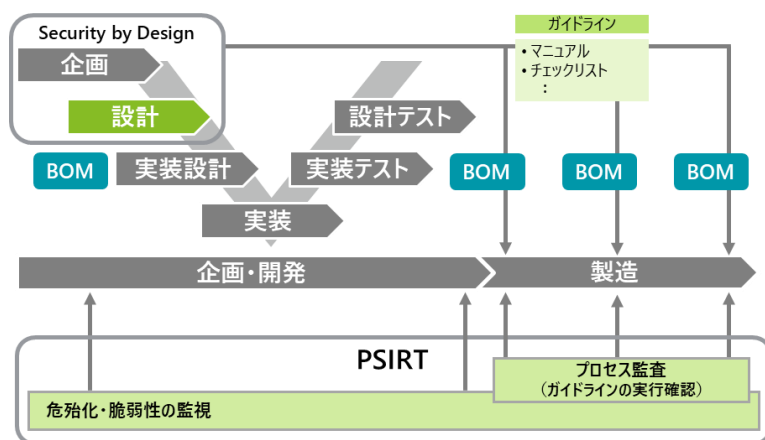
- ① 開発・設計の責任 ～部品表で証明～
ー 攻撃を受けても製品が安全に使えることを証明
- ② 製造の責任 ～ガイドラインで証明～
ー 攻撃を受けても正しく製造できていることを証明
- ③ 指示（告知）の責任

さらにPL法は、販売後も10年間は安全であることを求めています。セキュリティではセーフティと違って脆弱性や危殆化が課題となり得るため、上記①、②に対して継続的に以下の活動が求められます。

- 部品の脆弱性や危殆化の有無をチェックして、必要に応じて対策を実施
- ガイドラインどおりに実施されていることを確認

このように、脆弱性や危殆化の監視およびプロセス監査を継続的に実施することがPSIRTの活動です。

近年、ソフトウェアを部品として管理するソフトウェアBOMの法制化が各国で進んでいますが、IoT製品ではソフトウェアBOMに加えてハードウェア対策やプロセス監査の情報を含めて管理しなければ、製造物責任を果たすことができません。このように、製造物責任の要求事項に合わせて作成する部品表のことをセキュアBOMと呼称します。



セキュアBOM管理における課題

しかし、セキュアBOMを継続的に管理するには、主に4つの課題があります。この4つの課題を効果的に解決するために、デロイト・トーマツではSBOM管理ソリューションであるCyber Regulation Platform(PSIRTモジュール)を提供しています。

【課題1：危殆化の監視】

公開情報から危殆化情報を読み取るには、煩雑で高い専門性が求められる

【課題2：脆弱性の監視】

頻繁に更新される脆弱性情報から該当する脆弱性を手作業で抽出するのは、煩雑な作業が必要となる

【課題3：製造のプロセス監査】

経年で定期的にプロセス監査を実施し、記録を正しく残していく必要がある

【課題4：関連部門の連携】

セキュアSBOMは、開発やPSIRTなど複数部門が横断的に管理・運用する必要がある

【解消ポイント1】

専門家が危殆化情報をチェックし、セキュアBOMに該当する危殆化情報を通知します

【解消ポイント2】

公開情報から自動取得した脆弱性情報とセキュアBOMを突合し、該当する脆弱性情報を通知します

【解消ポイント3】

実施結果を記録に残し、ダッシュボードで実施状況や記録を管理します

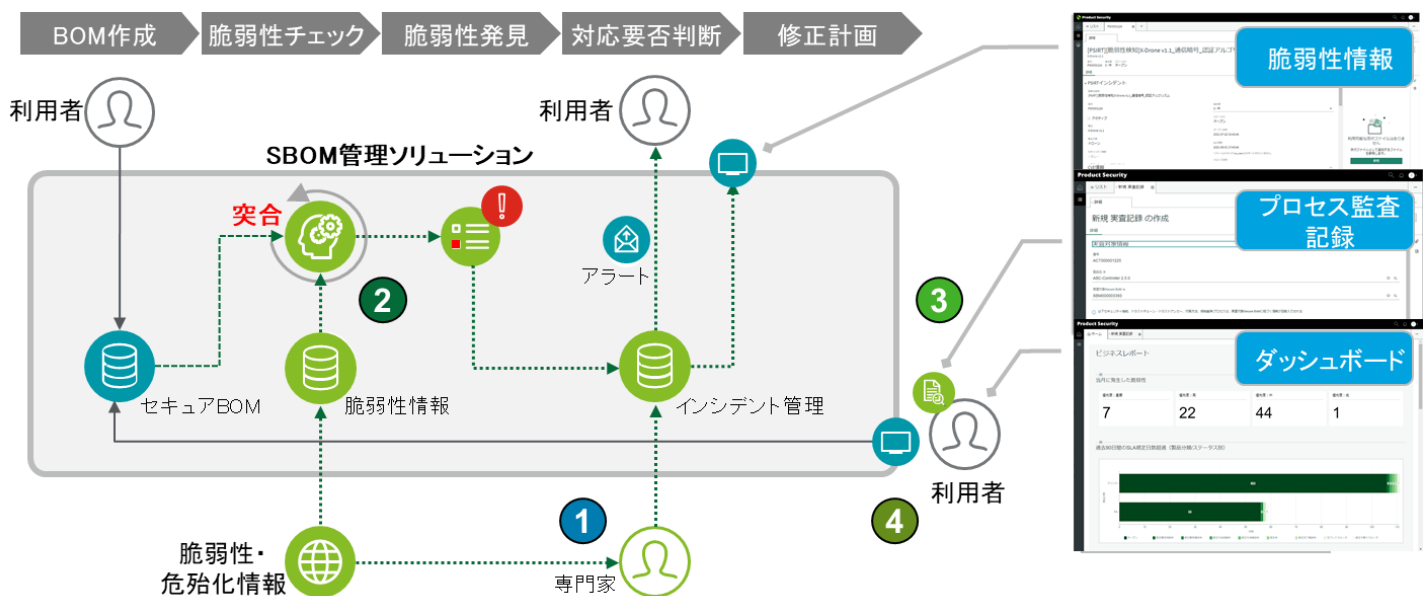
【解消ポイント4】

ダッシュボードやワークフローを活用し、関連部門が連携してセキュアBOMを管理・運用します

Cyber Regulation Platformとは

Cyber Regulation Platformとは、デジタル時代における企業のサイバー規制・準拠を支えるデロイトのプラットフォームです。サービスの1つとしてPSIRTの運用において必要となる機能をSBOM管理ソリューションとして提供しています。

SBOM管理ソリューションの概要



SBOM管理ソリューションの特徴

ソフトウェアBOMに加え、PL法に合わせてハードウェア対策やプロセス監査の情報をセキュアBOMとして管理します

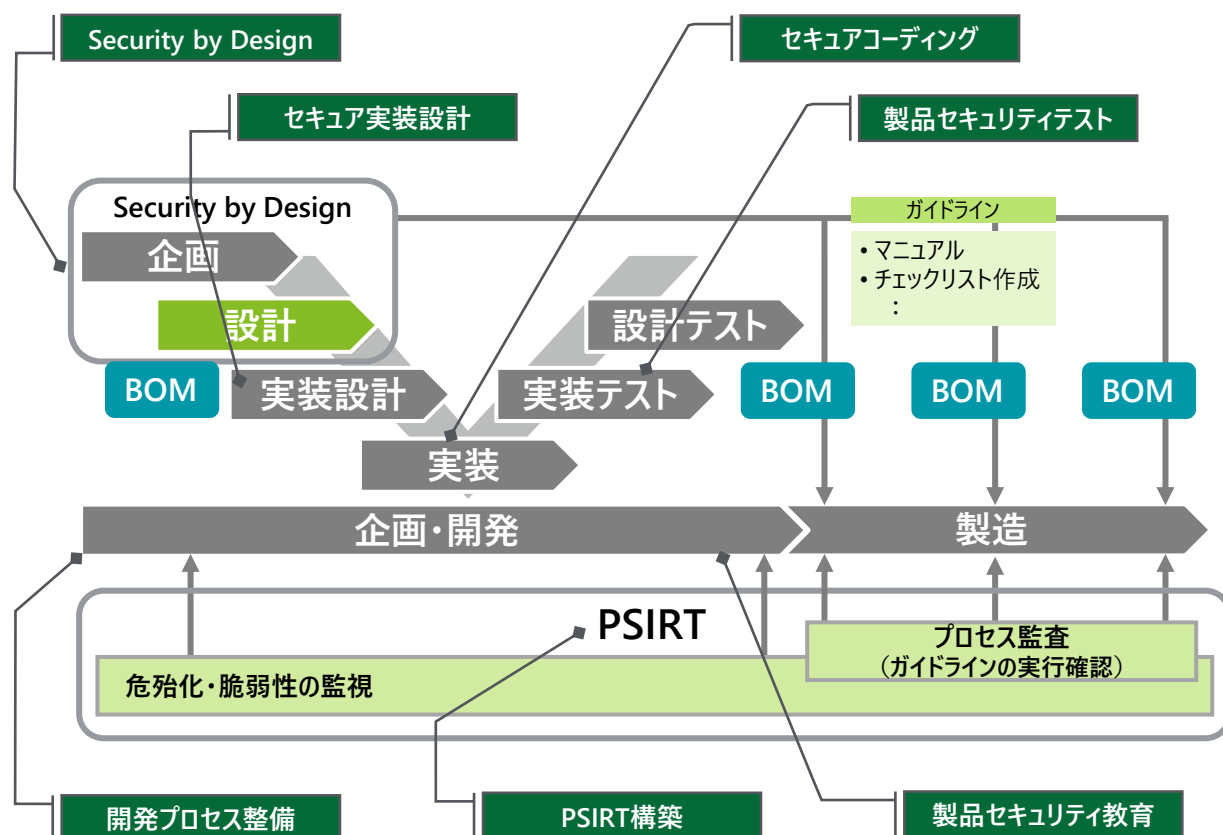
デロイト・トーマツの専門家が危殆化情報を定期的にチェックし、該当する部品に対してアラートを通知します

脆弱性や危殆化情報に加えて、関連する脅威情報など有益な情報を提供します（簡易版）

【ご参考】デロイト トーマツ サイバーが提供する製品セキュリティサービスメニュー

デロイト トーマツ サイバーは、SBOMを効率的に管理するSBOM管理ソリューション以外にも、製品の企画・設計から構築・テスト、運用まで、製品セキュリティ関連のサービスを提供しています。

製品セキュリティのサービスメニュー



サービス		概要
企画 開発	Security by Design	お客様の製品を取り巻くシステムにおいて、PL法を順守するためのリスク分析を網羅的に行い、規格やベストプラクティスに基づいた対策案を立案します
	セキュア実装設計	Security by Designで立案した対策を具現化するための製品内部の実装設計を防御、検知、対応・復旧に体系立てて設計します
	セキュアコーディング	製品内部に脆弱性やバックドアを作りこまないためのセキュアコーディングについて、静的解析ツール等を使用して助言を行います
	製品セキュリティテスト	Security by Design及びセキュア実装設計の設計思想に基づき、Validation / Verificationを行うための各種セキュリティテストを計画します
	開発プロセス整備	現状の組織体制や文書体系を確認した上で、品質としてセキュリティを組み込むためのプロセスや文書を作成します
運用 保守	PSIRT構築	セキュリティ技術の危殆化や製品の脆弱性に備え、被害を最小限に抑えるために平時からPSIRTによるモニタリング活動をするための態勢を整備します
製品セキュリティ教育		製品にセキュリティを組み込むために必要な設計・実装・テスト等について、お客様向けにカスタマイズした教材で、弊社講師による教育を提供します

デロイト トーマツ サイバー合同会社

Mail ra_info@tohmatsumatsu.co.jp

URL www.deloitte.com/jp/dtcy

【国内ネットワーク】東京・名古屋・福岡・前橋

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス 内容がご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ コーポレート ソリューション 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスク アドバイザリー、コンサルティング、ファイナンシャル アドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万5千名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバル ネットワーク 組織を構成するメンバー フォーム およびそれらの関係 法人（総称して“デロイト ネットワーク”）のひとつまたは複数の指しします。DTTL（または“Deloitte Global”）ならびに各メンバー フォーム および関係 法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバー フォーム ならびに関係 法人は、自らの作為および不作為についてのみ責任を負い、互いに他のフォーム または関係 法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行います。詳細は www.deloitte.com/jp/about をご覧ください。デロイト アジア パシフィック リミテッドはDTTLのメンバー フォーム であり、保証 有限責任 会社です。デロイト アジア パシフィック リミテッドのメンバー およびそれらの関係 法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャル アドバイザリー、リスク アドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500® の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をバース（存在理由）として標榜するデロイトの約345,000名のプロフェッショナルの活動の詳細については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバル ネットワーク 組織を構成するメンバー フォーム およびそれらの関係 法人（総称して“デロイト ネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家に相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバー フォーム、関係 法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接または間接に発生したいかなる損失および損害に対して責任を負いません。DTTLならびに各メンバー フォーム およびそれらの関係 法人はそれぞれ法的に独立した別個の組織体です。

Member of
Deloitte Touche Tohmatsu Limited

© 2022. For information, contact Deloitte Touche Tohmatsu LLC.,
2022.09_0382



IS 669126 / ISO 27001