関係各部署　御中

表示	PROTECTED 関係者外秘	原紙保管	M/Y：1/2032
		コピー保管	M/Y：1/2032

サプライヤ SIRT 要件書	制御電子プラットフォーム開発部 制御ネットワーク・アーキ開発室			
	No. SEC-ePF-VCL-SIRT-REQ-SPEC-a00-00-b			
	承認 河井	調査 平林	作成 三澤 日昔	2022/1/25
	電子承認取得			

適用範囲	全ての電子 PF に搭載される ECU に適用する
変更内容	新規作成
説明	【目的】 ✧　サイバーセキュリティ法規要求を満たすために必要となる サプライヤ SIRT 活動に関わる要件を示す。 【入手方法】 ✧　本文書は、iSpirit からダウンロード可能 [Folder] Repository/Electronics_Spec/Cybersecurity[サイバ゛-セキュリティ]/Standard[標準]/SPEC[仕様書]/SIRT[セキュリティインシデント対応チーム] 社外開示：海外事業体/ボデーメーカー/協業先 OEM/サプライヤ/委託先には、目的（外設申/RFQ 等）に沿った機密保持に係る契約を締結している場合のみ展開可 【問合せ】 ✧　問合せ窓口 制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室 http://team-adsp.kitora.toyota.co.jp/sites/cybersecurity/SitePages/Sec_Contact2.aspx

変更履歴

Version	発行日	変更箇所	備考	変更者
a00-00-a	2020-05-15	新規発行		46F3G 加藤
a00-00-b	2022-01-25	表紙 【入手方法】 ・入手先更新(BBS→iSpirit) ・開示範囲追加 ・問合せ先変更(メール→Web QA フォーム)		46F3G 日昔

目次

1　はじめに

1.1 背景

近年、自動車は単なる移動手段にとどまらず、自動運転やインターネット接続など、制御の高度化と利便性の向上が図られている。その一方で、新たな課題も増えており、サイバー攻撃の脅威もその一つといえる。

自動車は、サイバー攻撃により走る・曲がる・止まる等の基本機能が不正に操作された場合にその影響が人命にまで及ぶ可能性があるという点で、IT 製品等とは異なる。これらの基本機能を攻撃するには、攻撃者が車両内に乗り込んで攻撃用の機器を物理的に接続する必要があると、以前は考えられていた。ところが最近では、携帯電話通信や Bluetooth、Wi-Fi 等の無線インターフェイスを有するシステムの脆弱性を突かれ、車載ネットワークに侵入され、遠隔から車両基本機能に影響を及ぼされてしまうのではないか、といった脅威の想定が必要となっている。

また、脆弱性は悪用されない限り影響が表れず、攻撃されて初めて影響が出るという点で、一般的なソフトウェアバグや仕様不具合とは異なる。それ故に、既知の脆弱性を開発の中で修正した後に、新たな脆弱性が発見されることは少なくない。いかに注意深く開発したとしても、このような「新規脆弱性」のすべてを開発中に顕在化させることは困難である。

よって、開発中から開発後にわたり、脆弱性や脅威等のサイバーセキュリティ(CS)関連情報を監視し、発見した情報のアセスメントを実施し、影響ある場合はインシデント対応・脆弱性対応することが必要である。その活動にあたっては、サプライチェーンの構成者が互いに協力し、長期にわたり継続的に行えるような新たな仕組みを自動車業界全体で構築する必要がある。

また、近年は国連 WP29 の車両 CS 法規化が進み、2022 年には欧州はじめとする全世界で CS プロセス認証・車両型式認証が行われる予定となっている。この法規認証においては、各社の CS プロセスが ISO21434 に準拠していること、また、各車両がその CS プロセスに従い開発・生産・運用・廃棄されていることが求められる見込みである。よって、トヨタとそのサプライチェーンは、ISO21434 に準拠した CS プロセスの確立と、その CS プロセスに従った製品開発・生産・運用・廃棄を確実に行う必要がある。

1.2 本書の目的

CS 法規要求を満たすために必要となる、サプライヤ SIRT 活動に関わる要件を示す。

1.3 本書の読み方

本書が示す要件は以下の方法で分類を行う。

1.3.1 要件の分類

本書が示す要件には以下の 2 種類がある。

【必須】： 必須として満たすことを求める要件。

【任意】： サプライヤ判断で実施可否を決定できる要件。

1.4 用語説明

本書で使用する用語、略語については、以下の文書を参照のこと。

文書名：車両サイバーセキュリティ及びプライバシー用語定義書

文書 ID：SEC-ePF-TRM-GUD-PROC-***-**-*

(***-**-*はバージョンを表す)

1.5 関連文書

本書の関連文書を表 1 に示す。

表 1 関連文書一覧

文書名	発行元
ISO21434	ISO

2　SIRT 活動にあたっての前提説明

本章では、SIRT 活動にあたっての前提となる考え方を説明する。

まず 2.1 章では車両ライフサイクルのどこで SIRT 活動するかの考え方を示す。

次に 2.2 章では SIRT 活動の基本フローである監視、アセスメント、対応の考え方を示す。

最後に 2.3 章では監視、アセスメント、対応におけるトヨタとサプライヤの役割分担の考え方を示す。

2.1 車両ライフサイクルにおける SIRT 活動のスコープ

車両ライフサイクルは一般的に、開発・生産・運用・廃棄の各フェーズに分けられる。開発フェーズで既に公開されていた、公知となっていた、あるいは発見されていた脆弱性は、開発の中で修正するのが基本である。しかし最終仕様 FIX（原則は CV だが、変動する場合がある）の間際になって以降は、仕様変更する必要が生じた場合には、システム的には他部品あるいは車両全体に影響を与えるリスクを判断し、対応を決定しなければならない。これらのフェーズ遷移と脆弱性対応の考え方を図 1 に示す。原則として、出荷判断後に発覚した脆弱性に対しては SIRT の枠組みで対応する。

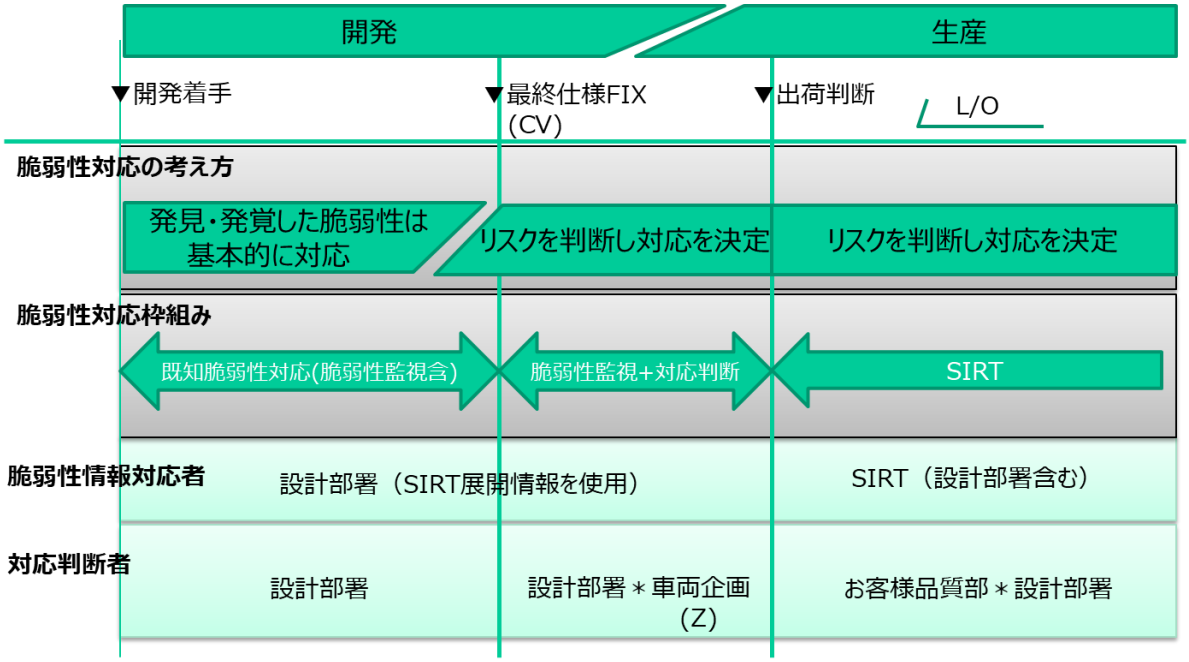

図 1　開発～生産のフェーズ遷移と脆弱性への対応イメージ

2.2 SIRT 活動の基本フロー

本節では、SIRT 活動の基本フローである監視、アセスメント、対応の考え方を示す。(具体的なサプライヤ SIRT 要件については 3 章で示す)

図 2 に示すように、脆弱性情報に対応する SIRT 活動の基本フローは、監視、アセスメント、対応の 3 段階に分けられる。脆弱性情報はトリアージによってイベントへエスカレーションされ、アセスメントによってリスクレベルが高いと判断されたイベントはインシデントへエスカレーションされる。インシデント対応プロセスは、トヨタお客様品質部が主導する従来の市場対応の仕組みを用いる。

また、脆弱性対応には、現在進行中の車両／部品開発への情報展開、次期開発での反映や量産仕様変更(R/C)に同期しての改善等を含む。

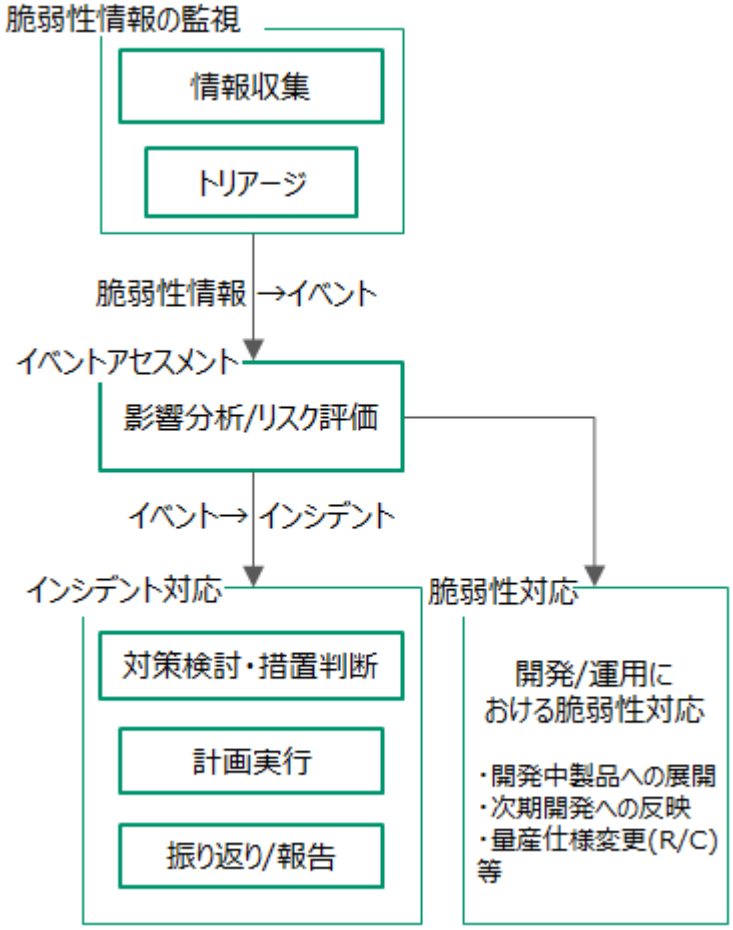

図 2　SIRT 活動の基本フロー（監視、アセスメント、対応）

図 2 は トヨタ やサプライヤの区別なく描かれているが、脆弱性情報の監視は双方が実施し、イベントアセスメント以降のプロセスは内容によって、一方が、または双方で協調して実施することになる。(トヨタとサプライヤ連携の詳細については 3 章にて説明)

2.3 基本フローにおける役割分担

本項では、SIRT 活動の基本フローである監視、アセスメント、対応の各段階におけるトヨタとサプライヤ間の役割分担を示す。

監視、アセスメント、対応の各段階について、トヨタ／サプライヤの各専門領域とその製品の選択の観点から次のように分類し、RASCI 形式で役割を示す。

- サプライヤ専門領域の製品でトヨタからサプライヤに供給するもの
- サプライヤ専門領域の製品でサプライヤ自身が選択しているもの
- トヨタ専門領域としての自動車やシステムなど

また、インシデントになった場合は従来の品質の枠組みで対応する。

RASCI 形式中の記号が表す役割は表 2 のとおりである。

表 2　RASCI 役割

記号	役割
R（responsible）	実行責任者　タスクについて責任を負う者
A（accountable）	説明責任者 承認者
S（support）	サポート　実行責任者の配下に割り当てられた人員
C（consulted）	協業先 相談を受ける者
I（informed）	報告先 報告を受ける者

2.3.1　脆弱性情報の監視

脆弱性情報の監視とは、日々公開・更新される、あるいは発見される脆弱性情報を収集し、自製品に対してトリアージを実施してイベントを抽出することである。この一連のプロセスにおけるトヨタとサプライヤの役割分担の考え方を以下に示す。

原則として、トヨタ、Tier1 サプライヤ、Tier2 サプライヤ等が各対象製品（ソフトウェア含む）の開発領域を監視する。それぞれの目線で監視することで、車両全体で抜けなく脆弱性情報が監視されていることが理想である。そのためには、Tier1 は Tier2 以下と監視の役割分担について合意しておく必要がある。Tier2 以下のサプライヤが何らかの理由により監視できない場合は、Tier1 と Tier2 以下で協議して管理方法や対応を決める必要がある。

対象製品の監視における役割分担を表 3　に示す。

表 3　監視における役割分担

分類		役割分担	
		トヨタ	サプライヤ
サプライヤ開発領域（ECU・SW など）	サプライヤ選択	I	R,A
	トヨタ指定	R,A	S,C
トヨタ開発領域（自動車・システムなど）		R,A	S,C

2.3.2　イベントのアセスメント

脆弱性情報の影響分析では、自製品に対して脆弱性当該機能の使用有無、攻撃手法公開状況や発生可能性、実際の攻撃リスク、影響有無、影響範囲、被害想定、および対策要否を詳細に調査する。これをイベントのアセスメントという。この一連のプロセスにおいてトヨタとサプライヤの役割分担の考え方を以下に示す。

原則として、トヨタ、Tier1 サプライヤ、Tier2 サプライヤ等が各対象製品（ソフトウェア含む）の専門領域でアセスメントを実施する。それぞれの目線でアセスメントすることで、車両全体で抜けなくアセスメントできていることが理想である。そのためには、Tier1 は Tier2 以下とアセスメントの役割分担について合意しておく必要がある。Tier2 以下のサプライヤが何らかの理由によりアセスメントできない場合は、Tier1 と Tier2 以下で協議して対応を決める必要がある。

対象製品のアセスメントにおける役割分担を表 4 に示す。

表 4　アセスメントにおける役割分担

分類		役割分担	
		トヨタ	サプライヤ
サプライヤ開発領域（ECU・SW など）	サプライヤ選択	I	R,A
	トヨタ指定	R,A	S,C
トヨタ開発領域（自動車・システムなど）		R,A	S,C

2.3.3　インシデント対応と脆弱性対応

インシデント対応、脆弱性対応において市場対応や設計変更することになった場合は、以下の考え方で対応する。

- 役割分担： 原則として、トヨタとサプライヤが各対象製品にインシデント対応、脆弱性対応を実施する。
- トヨタが市場対応必要と判断した場合、従来の品質対応の仕組みを用いてインシデント対応を実施する。
- トヨタが市場対応不要と判断した脆弱性情報については、トヨタが立案した計画に従い、トヨタとサプライヤが各対象製品に脆弱性対策を実施する。

3　SIRT 活動に関わる要件

本章では、トヨタとサプライヤの SIRT が連携して実施すべき手順と、サプライヤ SIRT に関わる要件を示す。

3.1 章では、トヨタ SIRT とサプライヤ SIRT が連携するための全体的な基本手順を説明する。

3.2 章では、サプライヤ SIRT 体制の構築に関わる要件を示す。

3.3 章では、サプライヤ SIRT 手順に関わる要件を示す。

3.4 章では、サプライヤ SIRT 体制の運用に関わる要件を示す。

3.1　基本手順の説明

2.2 で示した SIRT 活動の基本フローである監視、アセスメント、対応を通したトヨタ(OEM) SIRT とサプライヤ SIRT の一連の連携手順を、図 3 に示す。この基本フローに従い、トヨタとサプライヤはお互いに情報共有することで問題の早期解決を図る。

また、2.3 で示したトヨタとサプライヤの役割分担の考え方に従い、双方が責任を持って監視、アセスメント、対応を行う。

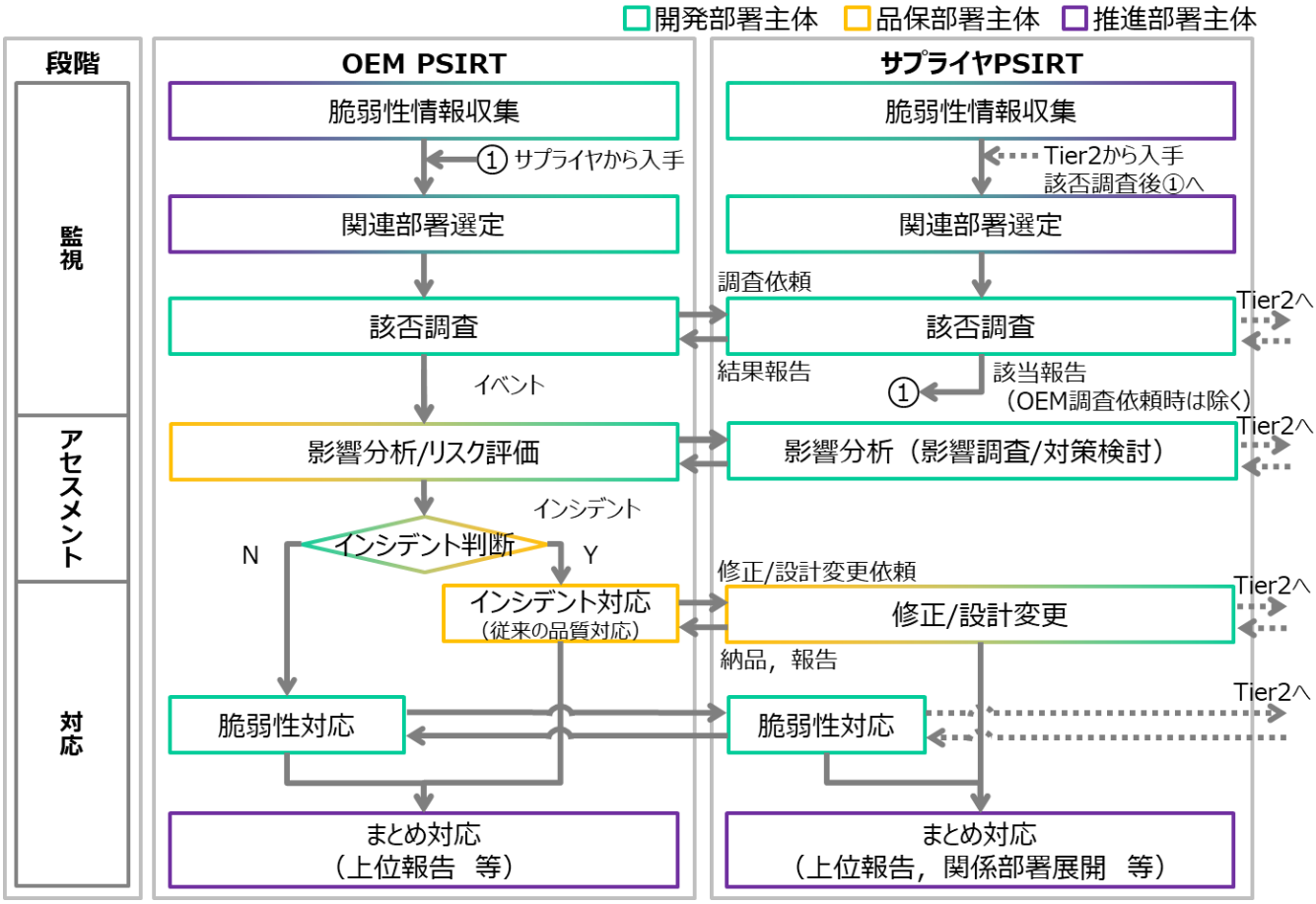

図 3　OEM・サプライヤ連携基本フロー

3.1.1 脆弱性情報収集

脆弱性情報の監視はトヨタとサプライヤ双方が実施する。

監視対象とすべき情報源（例：Auto-ISAC、脆弱性 DB 等）を定期的に巡回し、自社の製品またはサービスに関連する脆弱性情報が新たに発生していないか監視する。

3.1.2 関連部署選定

収集した脆弱性情報に対して、一般的な深刻度評価や車両影響有無により重要度を判定し、関連する開発部署（例：脆弱性が Linux に関するものだった場合、Linux を搭載する ECU の開発部署）を選定する。

3.1.3 該否調査

選定された開発部署は、収集した脆弱性情報が自社製品に該当するか否かの調査を行う。トヨタは必要に応じて Tier1 サプライヤに該否調査を依頼する。同様に、Tier1 サプライヤは必要に応じて Tier2 サプライヤに該否調査を依頼する。以上の結果、製品に該当する脆弱性が見つかった場合はイベントとして抽出し、影響分析を行う。

3.1.4 影響分析／リスク評価、インシデント判断

イベントアセスメント以降のプロセスは内容によって、一方が、または双方で協調して実施する。

イベントアセスメントにおいては、影響分析/リスク評価を行い、インシデントか否かを判定する。その際、トヨタは必要に応じて Tier1 サプライヤに影響分析を依頼する。同様に、Tier1 サプライヤは必要に応じて Tier2 サプライヤに影響分析を依頼する。

3.1.5 インシデント対応

影響分析/リスク評価の結果からインシデントと判定された場合、トヨタお客様品質部が主導する従来の品質対応の枠組みで対応する。

3.1.6 脆弱性対応

インシデントと判定されなかった場合、トヨタが脆弱性対応計画を立案し、サプライヤと設計改善を実施する。その後、トヨタとサプライヤそれぞれの推進部署がまとめ対応として振り返り・再発防止展開や必要な上位報告を行って完了とする。（推進部署がない場合は開発部署や品質保証部署が対応する）

3.2 サプライヤ側 SIRT 体制に関わる要件

サプライヤ SIRT 体制の構築・運用準備に関わる要件を示す。

3.2.1 推進部署の明確化

【必須】

3.2.1.1 サプライヤ内で全社統括的に SIRT 活動を推進する、推進部署を置くこと。
※ただし専門の部署を置くか否かはサプライヤの判断に委ねる。
例えば対象となる ECU 数が 1 件の場合、その開発部署が推進部署を兼ねてもよい。

3.2.2 SIRT 体制・プロセス

【必須】

3.2.2.1 推進部署は、SIRT の体制やプロセスについてトヨタと合意すること。

3.2.2.2 合意内容には以下の内容を含むこと。

a) SIRT 体制（組織体制図、連絡先窓口リスト）
b) フィールド監視プロセス（脆弱性情報の監視先、監視頻度、トリアージ基準含む）
c) インシデント対応プロセス
d) 脆弱性対応プロセス
e) 設計へのフィードバックプロセス

【任意】

3.2.2.3 SIRT 体制構築にあたっては、米国 Auto-ISAC の Best Practice ”Incident Response” を参考にすること。

3.3 サプライヤ側 SIRT 手順に関わる要件

トヨタとサプライヤが連携する SIRT フローにおける、サプライヤ側手順に関わる要件を示す。
監視からアセスメント、対応に至る基本フローの考え方は、2.2 で示した考え方に従う。
また、トヨタとサプライヤの役割分担の考え方は、2.3 で示した考え方に従う。

3.3.1 脆弱性情報収集

【必須】

3.3.1.1 推進部署あるいは開発部署は、日々公開・更新される、あるいは発見される、脆弱性情報を定期的に監視すること。

3.3.1.2 推進部署あるいは開発部署は、脆弱性情報を入手した場合、自社製品に該当するかどうかの一次的な照合調査を行うこと。

3.3.1.3 推進部署あるいは開発部署は、Tier2 以下とそれぞれの監視対象等を具体的に合意しておくこと。

3.3.1.4 推進部署あるいは開発部署は、Tier2 より脆弱性情報を入手した場合、その Tier2 供給部品以外にも該当する部品がないか一次的な照合調査を行うこと。(ただしその Tier2 が情報開示を許諾した場合に限る)

3.3.1.5 推進部署あるいは開発部署は、自社製品の開発段階（脆弱性分析・脆弱性評価）において発見された脆弱性情報を社内で入手し、既に市場にある他の自社製品に該当するかどうかの照合調査を行うこと。

【任意】

3.3.1.6 脆弱性情報の監視／確認対象は、以下から入手可能な、自製品の機能・性能等に影響のあるものとする。

① 公開 DB（JVN(JVN と JVNiPedia)、NVD）に公開されたもの
② 自製品の構成部品のサプライヤやベンダ等が web ページ等で公開したもの
③ サプライチェーンより直接入手した／通知された情報*1
④ 業界団体（Auto-ISAC 等）の情報*2 にあるもの
⑤ 脆弱性開示プログラムにより入手した情報、研究者等から知らされた情報
⑥ トヨタの要求仕様書等に記載があるデータベース

*1) 例：トヨタからの情報、購入ソフトウェアや導入パッケージの提供元からのサポート情報、Tier2 以下から該当したとして挙がってきた情報

*2) Auto-ISAC 情報によっては開示先が制限されている情報もあるので、メンバー資格やアクセス可能範囲には注意・配慮が必要である。

3.3.1.7 脅威情報の監視／確認対象は、以下から入手可能な、自製品の機能・性能等にとって脅威となるものとする。

① 公開 DB（JVN(JVN と JVNiPedia)、NVD）に公開されたもの
② 自製品の構成部品のサプライヤやベンダ等が web ページ等で公開したもの
③ サプライチェーンより直接入手した／通知された情報*1
④ 業界団体（Auto-ISAC 等）の情報*2 にあるもの
⑤ 脆弱性開示プログラムにより入手した情報、研究者等から知らされた情報
⑥ トヨタの要求仕様書等に記載があるデータベース

*1) 例：トヨタからの情報、購入ソフトウェアや導入パッケージの提供元からのサポート情報、Tier2 以下から該当したとして挙がってきた情報

*2) Auto-ISAC 情報によっては開示先が制限されている情報もあるので、メンバー資格やアクセス可能範囲には注意・配慮が必要である。

3.3.2 関連部署選定

【必須】

3.3.2.1 推進部署あるいは開発部署は、当該脆弱性を含む可能性がある部品の担当部署を漏れなく選定し、確実に該否調査依頼をすること。

3.3.3 該否調査

【必須】

3.3.3.1 調査責任部署として選定された開発部署は、自社製品に当該脆弱性が該当するか否かの調査を下記観点で実施すること。

a）当該脆弱性を含むハードウェア／ソフトウェア搭載製品の有無
b）当該脆弱性を含む機能の使用有無

3.3.3.2 開発部署は、必要に応じて設計を委託している外部関係先（Tier2 サプライヤ・開発ベンダ等）に該否調査を依頼すること。

3.3.3.3 開発部署は、該否調査の結果から製品が当該脆弱性を含む（イベントである）と判断した場合、速やかにトヨタの開発部署に報告すること。

※トヨタから調査依頼を受けた場合と、自社や Tier2 以下で発見した場合も同様。

3.3.4 影響分析（影響調査／対策検討）

【必須】

3.3.4.1 開発部署は、トヨタから影響分析の依頼を受けた場合、自社製品に当該脆弱性が与える影響の分析を下記観点で実施すること。

a) 当該脆弱性を攻撃されたときの想定される被害／影響の大きさと及ぶ範囲（リスク想定）
b) 脆弱性攻撃のメカニズム（サプライヤとして可能な攻撃経路分析、攻撃情報詳細）
c) 当該脆弱性が以前に検討済みのものかどうか（例えば脅威分析フェーズにて）
d) 対策内容と対策の可否
e) 対策計画案

3.3.4.2 開発部署は、必要に応じて設計を委託している外部関係先（Tier2 サプライヤ・開発ベンダ等）に影響分析を依頼すること。

3.3.4.3 開発部署は、自製品への影響分析結果だけでなく、可能な範囲での他の関連製品や関連システム等への影響なども分析し、リスクレベルの許容可否や対策要否を判断すること。

3.3.4.4 開発部署は、影響分析が必要となった際に再現検討等が実施できるよう体制を準備しておくこと。

3.3.4.5 開発部署は、トヨタと合意した期限内に、トヨタのカウンターパート開発部署（影響分析依頼の発信部署）に影響分析した結果を報告すること。

3.3.5 修正／設計変更

【必須】

3.3.5.1 品保部署あるいは開発部署は、トヨタが市場対応必要と判断した場合は、トヨタお客様品質部が主導する従来の品質対応と同じ考え方・仕組みで自社製品の修正／設計変更を実施すること。

3.3.5.2 品保部署あるいは開発部署は、自社製品の修正／設計変更を行う際には、必要に応じて設計を委託している外部関係先（Tier2 サプライヤ・開発ベンダ等）に修正／設計変更の対応を依頼すること。

3.3.6 脆弱性対応

【必須】

3.3.6.1 開発部署は、トヨタがインシデント対応不要と判断し、脆弱性対応を行う場合、トヨタの指示に従い脆弱性対応を実施すること。

3.3.6.2 開発部署は、脆弱性対応を行う際に必要に応じて設計を委託している外部関係先（Tier2 サプライヤ・開発ベンダ等）に修正／設計変更の対応を依頼すること。

3.3.6.3 開発部署は、脆弱性対応を行った結果をトヨタの開発部署に報告すること。

3.3.6.4 開発部署は、残存させると判断した脆弱性については、その判断時にリスク評価の見直しタイミングと役割をトヨタと合意すること。

【任意】

3.3.6.5 開発部署は、サプライヤとして脆弱性対応が必要と判断した場合、トヨタの開発部署に報

告の上、脆弱性対応を行うこと。

3.3.7 まとめ対応（行動記録、再発防止、報告　等）

【必須】

3.3.7.1 推進部署は、脆弱性情報入手から対応完了までの一連の行動を記録すること。

3.3.7.2 推進部署は、インシデント対応、脆弱性対応をした結果をノウハウ・過去事例として管理し、その後の開発に反映すること。

3.3.7.3 推進部署は、インシデント対応、脆弱性対応をした結果を、上位組織、経営層および必要と判断した関係部署に報告すること。

【任意】

3.3.7.4 推進部署は、社外にインシデント情報、脆弱性情報を提供する際には、機密保持契約を締結すること。

※トヨタ-サプライヤ間には部品取引基本契約内の機密保持条項が存在する。

3.4 サプライヤ側 SIRT 運用に関わる要件

サプライヤ SIRT の運用に関わる要件を以下に示す。

3.4.1 定期的な活動

【必須】

3.4.1.1 推進部署あるいは開発部署は、3.3.6.4 で残存させると判断した脆弱性については、定期的にリスク評価の見直しを行うこと。

3.4.1.2 推進部署は、規定したプロセスを定期的に評価し、継続的に改善を図ること。

3.4.1.3 推進部署は、トヨタによる脆弱性情報監視・アセスメント状況の監査に対応すること。

3.4.1.4 推進部署あるいは開発部署は、SIRT 活動の成果物を作成・保管し、対外的に説明できる状態にしておくこと。

※トヨタは、サプライチェーン全体を通じて SIRT による監視・アセスメントが適切に実施されていることを対外的に保証するために、以下を実施する場合がある。

- サプライヤの監視・アセスメントの実施状況を監査
- サプライヤの監視実施状況の報告書提出を要求

報告書内容 例）

① 監視対象とした情報源
② 情報の入手日と判断日
③ 判断者・承認者
④ トリアージ結果とその理由
⑤ 分析／評価対象とした脆弱性情報
⑥ 分析／評価の実施日
⑦ 分析／評価の実施者、結果の承認者
⑧ 影響無の場合は、その判断理由
⑨ 影響有の場合

a) 影響範囲（該当部品番号、S/N、製造期間など）
b) 想定される発生事象（サプライヤ担当部品に閉じた事象でも可）
c) 推奨対策案（複数の場合は各々の長所・短所。サプライヤ担当部品に閉じた対策でも可）

3.4.1.5 推進部署は、SIRT 体制における組織体制図、連絡先窓口リストおよび情報伝達の方法を定期的に見直し最新化すること。

4　OSS 採用時の留意点

サプライヤは、OSS を採用する際には下記課題への対応も考慮した上で、採用するか否かを判断すること。ただし、トヨタが開発・使用指示したものを除く。

【OSS 固有の課題】

＜セキュリティサポートの継続性＞

・OSS のセキュリティサポートを開発元に強制することができない

・採用した OSS へのセキュリティサポートが打ち切られる可能性がある

・セキュリティサポートが打ち切られることで、脆弱性への対応が困難となる可能性がある

＜セキュリティアップデートの影響拡大＞

・ある OSS のセキュリティアップデートを反映させるために、その OSS が動作する OS（カーネル）のアップデートも同時に必要になる場合があるなど、セキュリティアップデートがソフトウェア全体に影響を及ぼす可能性がある

APPENDIX A

A.1 トヨタ側 SIRT 手順

3章で示したトヨタとサプライヤが連携するSIRTフローにおけるトヨタ側の手順を参考として示す。

A.1.1 脆弱性情報収集

推進部署は、監視対象とすべき情報源（例：Auto-ISAC、脆弱性 DB 等）を定期的に巡回し、自社の製品またはサービスに関連する脆弱性情報が新たに発生していないか監視する。

開発部署は、サプライヤより自社製品に関する脆弱性情報を入手した場合、推進部署が関連部署に情報を迅速に展開できるようにするため直ちにその内容を推進部署に連絡する。

推進部署は、脆弱性情報を入手した際にその情報の内容を確認する。自動車に関連する脆弱性情報については引き続き関連部署選定に移行する。

A.1.2 関連部署選定

推進部署は、収集した脆弱性情報から関連する開発部署（例：脆弱性が Linux に関するものだった場合、Linux を搭載する ECU の開発部署）を選定する。

推進部署は、自社車両への影響有無を迅速かつ簡易的に把握するため、開発部署に該否調査を依頼する。その際に推進部署は、車両への影響とその大きさ（例：車両オーナー自身の被害だけでなく、交通システムの混乱などの社会的な影響、風評による顧客の不安など）から調査の優先度を決定し、調査完了期日などを一意に設定する。

A.1.3 該否調査

開発部署は、以下の観点で調査を実施する。

- 脆弱性が特定されている場合、当該脆弱性を含むハードウェア／ソフトウェアを使用しているか
- 影響範囲（大まかな*車種、システム年代等）

*該否調査は詳細な影響分析へ移行するトリガであり、詳細な調査よりも該否判定のスピードが求められるため。

開発部署は、必要に応じてサプライヤ等の外部関係先に調査を依頼する。

開発部署は、該否調査結果を推進部署に報告する。

推進部署は、社内の関係者と脆弱性情報の影響を共有するため、該否調査結果を必要に応じて他の関連部署（例：品質、生産、広報等）に報告する。

A.1.4 影響分析／リスク評価、インシデント判断

推進部署は、自社車両への影響をより詳細に把握するため、開発部署に以下の観点で調査を依頼する。

- 影響を受ける車種、仕向け、年式、仕様またはモデル（型式）、台数等
- 脆弱性の影響、メカニズム
- 対策計画案（R/C、定期機能アップデート、次の設計タイミングでの改善等）

開発部署は、必要に応じてサプライヤ等の外部関係先に調査を依頼する。

開発部署は、詳細調査結果を、推進部署に報告する。

開発部署と推進部署は、脆弱性情報が市場の自社製品またはサービスに与えるリスクレベルが高いと判断した場合（インシデントであると判断した場合)、品質保証部署に報告する。品質保証部署は、開発部署からの市場影響可能性の報告を受け、市場対応の必要性を判断する。必要と判断した場合、従来の品質対応の仕組みを用いてインシデント対応に移行する。

市場の自社製品またはサービスに与えるリスクレベルが低いと判断した場合（インシデントでないと判断した場合)、推進部署と開発部署は、脆弱性への今後の対策計画案（R/C、定期機能アップデート、次の設計タイミングでの改善等）を立案し、脆弱性対応に移行する。実施したアセスメントの結果については、少なくとも下記のような情報を文書化し記録する。

① 分析・評価対象となった情報の入手先
② サプライチェーン関係者からの入手情報の記録と分析／評価の日時
③ 最終的な分析／評価の実行者・承認者
④ 車両レベルでの影響範囲（製造台数や期間、該当車両）
⑤ 判断結果とその理由

A.1.5 インシデント対応

市場対応が必要と判断した場合、開発部署と品質保証部署が従来の品質対応の仕組みを用いてインシデント対応を実施する。

開発部署は、対策計画をまとめ、推進部署に報告する。推進部署は全体状況を把握するため、開発部署からの報告を受ける。

A.1.6 脆弱性対応

開発部署は、市場対応不要と判断した脆弱性情報について、今後どう対策するかの対策計画を立案し、実行する。

開発部署は、可能な限り速やかに、以下の内容を含む脆弱性対策計画を立案する。

- 脆弱性対策を行う車両・システムの頭出し時期
- 改善の方法（R/C、定期機能アップデート、次の設計タイミングでの改善等）

開発部署は、推進部署に、脆弱性対策計画を報告する。

開発部署は、脆弱性対策計画に従い、従来の品質対応の仕組みを用いてサプライヤへの修正指示等を行う。

推進部署は、開発部署が立案した脆弱性対策計画が実行されているかフォローする。また、必要に応じて技術的なフォローを行う。

A.1.7 まとめ対応（上位報告　等）

推進部署は、脆弱性情報対応の結果を文書にまとめ、社内の上位・関連部署や、社外の関係者に報告を行う。

推進部署は、脆弱性の要因分析と対策立案から得られたノウハウを、過去のトラブル事例として管理し、開発部署が今後の設計を行う際に参照できるようにする。

A.2 脆弱性情報取り扱い時の注意点

A.2.1 収集時の注意点

監視段階における情報の入手先には、日々一般公開されている情報（脆弱性情報データベース）、団体などの会員のみに共有される限定公開情報、自社製品の評価時に発見される情報、販売店や関係会社から知らされる情報、外部ベンダやサイバーセキュリティの研究者等からの通報による情報などがある。

これら多岐にわたる脆弱性情報を監視するために、情報量が多くかつまとまっている脆弱性情報データベースから定期的に収集する手段をとるのが良い。脆弱性情報データベースの例※を以下に示す。これらは脆弱性情報データベースが多数公開されている中で、確実な情報が充実しているという点で推奨される。

- NVD（National Vulnerability Database）
  NVD:NIST (National Institute of Standards and Technology) が運営、管理する脆弱性データベース。
  https://nvd.nist.gov/

- JVN（Japan Vulnerability Notes）
  JVN:JPCERT/CC と IPA が共同で運営している脆弱性対策情報ポータルサイト。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的として構築された。
  https://jvn.jp/

- JVN iPedia
  JVN iPedia:IPA が運営する脆弱性対策情報データベース。JVN に掲載される脆弱性対策情報の他、国内外問わず日々公開される脆弱性対策情報を収集、蓄積することを目的として構築された。
  http://jvndb.jvn.jp/

※出典：IPA（独立行政法人情報処理推進機構）の web ページ
http://www.ipa.go.jp/

これらデータベースから得た脆弱性情報は、構成情報との照合でイベントを抽出するために活用する。

A.2.2 照合時の注意点

入手した脆弱性情報と製品の構成情報との照合にあたっては、以下の情報などを活用する。特に上記データベースから入手した脆弱性情報のソフトウェア名、ベンダ名、バージョン番号（以下 Ver.）を確認することで照合精度を高めるのが良い。

- CVE 番号
- 情報更新日
- ソフトウェア名
- ベンダ名
- Ver.（バージョン番号）
- 脆弱性内容
- 影響・不具合情報

脆弱性情報を製品の構成情報と照合する際、照合する脆弱性情報のソフトウェア名やVer.の記載方法が統一されていないために、単純に一致しないものが多くある。例えば、Linux kernel の Ver.が以下のような cpe 表記※によって記述される場合などである。

- NVD データベース（cpe 表記）の例

  cpe:2.3:o:linux:linux_kernel:4.8.10:*:*:*:*:*:*:* and previous versions

  cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
  +versions up to (including) 4.13.11

このような自然文を含む表記になっている場合は機械的な照合が難しく、目視による確認作業が発生する。この例では、推進部署が照合する場合、Ver.範囲が構成情報の Ver.とおおよそ一致している、あるいは範囲内であるなどの判断をしてから、開発部署に具体的な調査を依頼する必要がある。

※cpe 表記：ハードウェア、オペレーティングシステム、アプリケーションなどのプラットフォームを識別するための名称で、製品種別、ベンダ名、製品名を連結した表記（IPA の web ページ http://www.ipa.go.jp/ より）

監視からアセスメントは、開発後も設計者自身が実施していく必要がある。しかし膨大な脆弱性情報から自製品に影響のある脆弱性を探すのは多大な工数を要するため、組織として監視作業の効率化を図ることが望ましい。

例えば推進部署等が専門チームを組織して監視作業を実施する方法がある。設計者が専門チームに構成情報を提供し、照合作業を専門化することで監視の作業を効率化できる。設計者は専門チームが照合し絞り込んだ情報のみを影響分析すればよく、作業負荷軽減に繋がる。

また、脆弱性の深刻さ（深刻度）を一つの基準とし、深刻な情報に絞り込んで対応することも推奨できる方法である。深刻度を定量的に比較する一つの指標として CVSS 値がある。CVSS 値は 0.0～10.0 までのスコア値で脆弱性を評価する。このスコア値が大きいほど攻撃が容易であったり、攻撃の影響が大きかったりする。例えば CVSS 7.0 以上の深刻度「重要・緊急」に相当する情報を調査対象とするなどの閾値を作り、重点的に調査する対象を絞り込むことができる。

A.2.3　該否調査、影響分析時の注意点

該否調査においては、トヨタ～サプライヤ間の重複調査を避けるために、開発完了時にトヨタ～サプライヤ間で以下の情報を共有しておくと、役に立つことがある。

- マイコン種別／型番
- 使用 OS
- 外部 IF
- 主要スタック
- 使用 OSS リスト

該否調査や影響分析では攻撃情報の分析や攻撃されたときのリスク分析を行うが、これら観点における攻撃されたときの具体的な影響は以下の点を考慮しておくのが良い。

- クルマの基本性能（走・曲・止）への影響
- 便利機能等への影響
- ソフトウェアの改ざん

- お客様の資産への影響
- お客様のプライバシー情報漏洩
- センター、インフラへの影響

また、該否調査や影響分析は、開発した設計者あるいは設計内容をよく理解している者が実施する必要がある。当該製品の設計を具体的に理解していなければ、分析や対策に時間を要したり不適切な対策で二次不具合を誘発したりする可能性があるからである。そのため、開発終了後に設計チームを解散するなどの組織変更時には、実際にインシデント発生した時に誰も設計内容を把握できないという問題が起きる可能性に十分注意する必要がある。したがって、必要に応じて設計を委託している外部関係先（サプライヤ・開発ベンダ等）や時には外部専門家に該否調査や影響分析を依頼するのが良い。

A.2.4 インシデント対応、修正／設計変更時の注意点

インシデント対応は、トヨタがインシデントの市場への影響を取り除き、平常に戻すための市場対応を実施することである。トヨタがインシデント対応を実施する場合に、実際に開発を担当したサプライヤに具体的な修正／設計変更を依頼することがある。その場合、サプライヤの開発部署は、インシデント判断をしたトヨタから依頼を受けて、修正／設計変更として対策品の設計（パッチ開発）を行う。

開発したパッチの品質評価や出荷判断は、対策品として開発したパッチの評価・テストだけでなく、確認できる範囲でパッチ適用による他の関連製品や関連システム等への影響評価も実施したうえで行う必要がある。

パッチを作成した後、適用による他の関連システム等への影響が大きく、トヨタとサプライヤで相談の上パッチを適用しない判断をすることがある。その場合、機能の一部停止、暗号化などのセキュリティ強化、攻撃に対する監視強化、代替システムの提案などのバックアップ案で対応することもある。

インシデントによっては攻撃手法等が推定できず、パッチ開発が困難で、適用できない場合がある。その場合、外部関係先（サプライヤ・開発ベンダ等）を含む開発部署だけでなく、関係機関やセキュリティの専門家にも相談し、脆弱性の影響緩和措置や回避措置で対応することもある。

また、インシデント対応、修正／設計変更時の計画立案にあたって、脆弱性は悪意ある攻撃を受けることで、短期間で広範囲に問題が顕在化する可能性があるため、サイバーセキュリティ対策の計画は、従来の品質対応（故障や問題の特定操作による不具合等）より短期間での対応が要求されることを考慮する必要がある。

以上のような手順で監視、アセスメント、対応のプロセスを実行することが、第三者の攻撃に対するリスクを減らし、自動車業界におけるサイバーセキュリティの品質を高めることに繋がる。