EdgeTech+2022講演

製品ライフサイクルにおける サイバーセキュリティ対応

～サイバーセキュリティ動向と組込み開発に求められるスキルセット～

2022年11月16日

組込みシステムセキュリティ委員会

副委員長 牧野進二

mailto:buildlab.koha9ru108@gmail.com

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

コネクティッドな世界

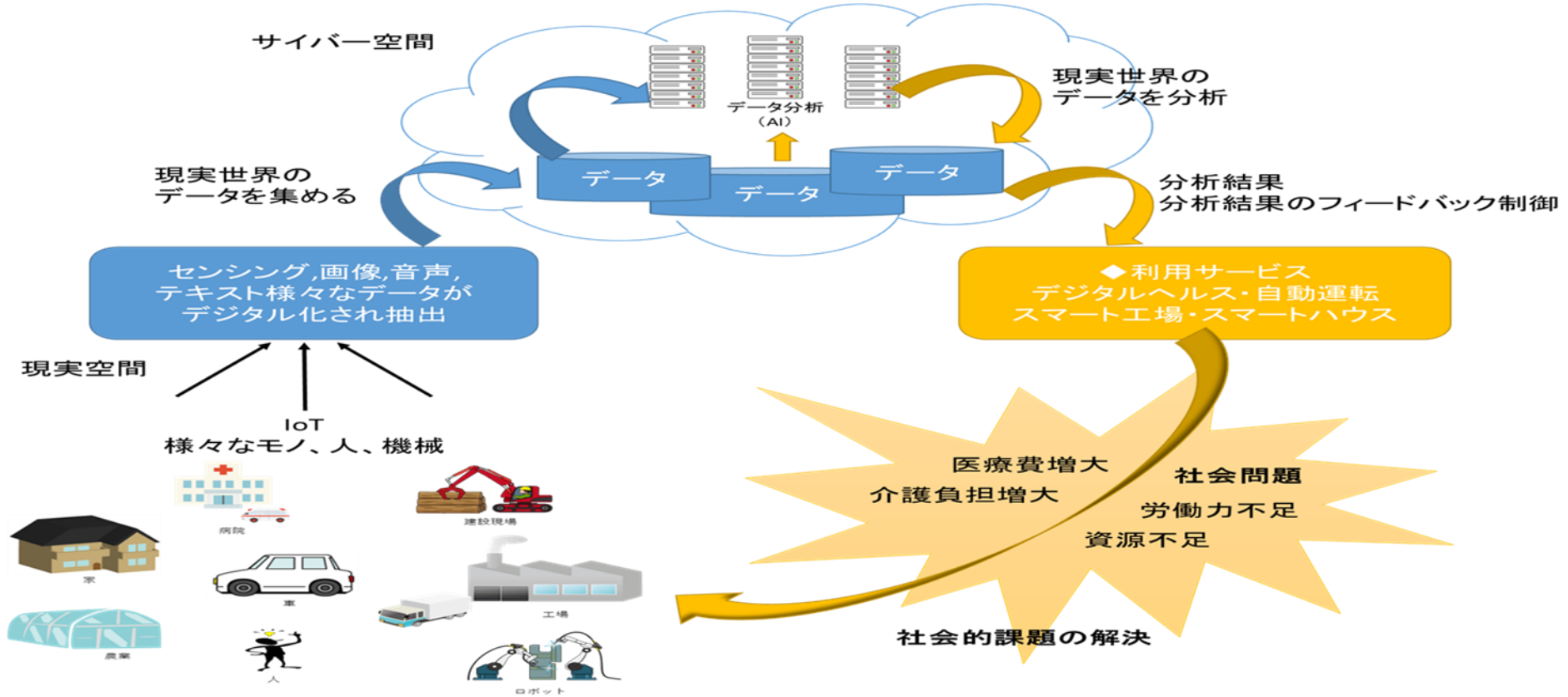
IoT機器の活用

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

1．コネクティッドな世界

■ 代表的な利用例：Society5.0(日本)

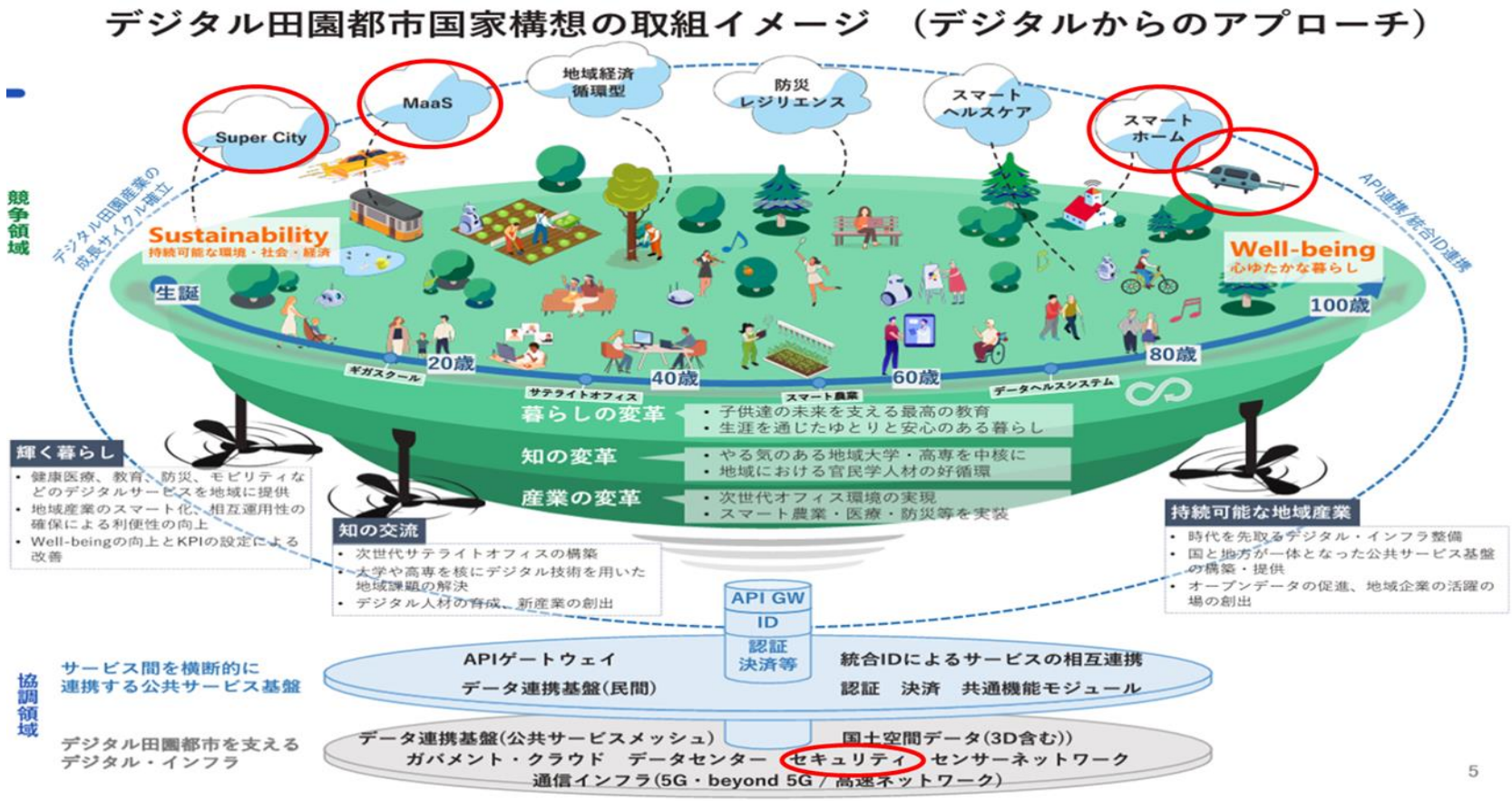
- Connected Industriesの社会



1．コネクティッドな世界

■ 代表的な例：デジタル田園都市国家構想

- スマートホームなど、様々なサービスの連携



出展：内閣官房 第1回デジタル田園都市国家構想実現会議

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

1．コネクティッドな世界

■ 代表的な例：MaaS(Mobility as a Service)

- 新規事業開発
- オープンイノベーション
- クロスインダストリー
- スマートシティ
- スーパーシティ
- Society5.0

Beyond MaaS

異業種との連携、まちづくりや社会課題の解決

主な提供先

- 住宅、不動産
- 観光
- 医療、介護、ヘルスケア
- 小売り
- 電力、エネルギー
- フィナンテック、金融
- 広告、プロモーション
- ゲーム、イベント
- シェアオフィス
- 働き方改革
- 物流
- 災害、防災
- まちづくり
- 行政課題

- 鉄道、バス、タクシー連携
- 快適性の向上、付加価値の創出
- 地域交通のマネジメント効率化
- コスト削減、経営効率化
- 交通の持続可能性、交通弱者対策

Deep MaaS

交通分野でのサービス深化や効率化、価値創造

主な実現手段

- 交通事業者の経営改革
- MaaSコントローラ
- マッチング技術の応用(ユーザ、モビリティ)
- 遊休資産の活用
- 新モビリティの追加(自動運転、オンデマンドモビリティなど)
- サブスクリプション、ダイナミックプライシングなど
- AI、IoTなど先端技術の活用

MaaS基本機能

利用者接点を作る出発点

MaaSコントローラ
①データ収集・分析・予測 ②モビリティ連携機能 ③MaaSアプリ連携

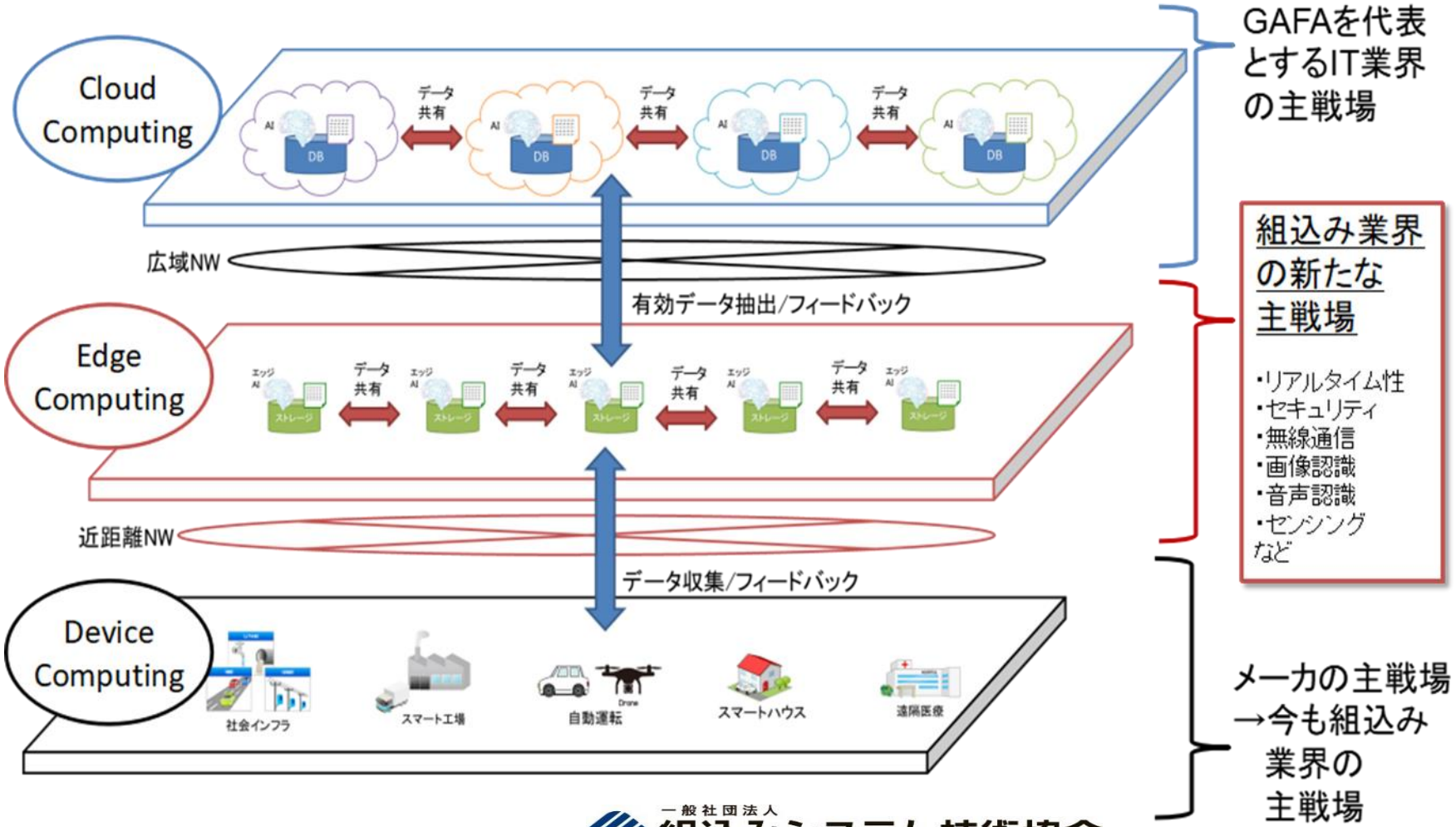
主な機能

- ナビゲーション(地図、経路探索、運賃、所要時間など)
- 予約、決済、通知、ガイドなど

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

1．IoTとは？

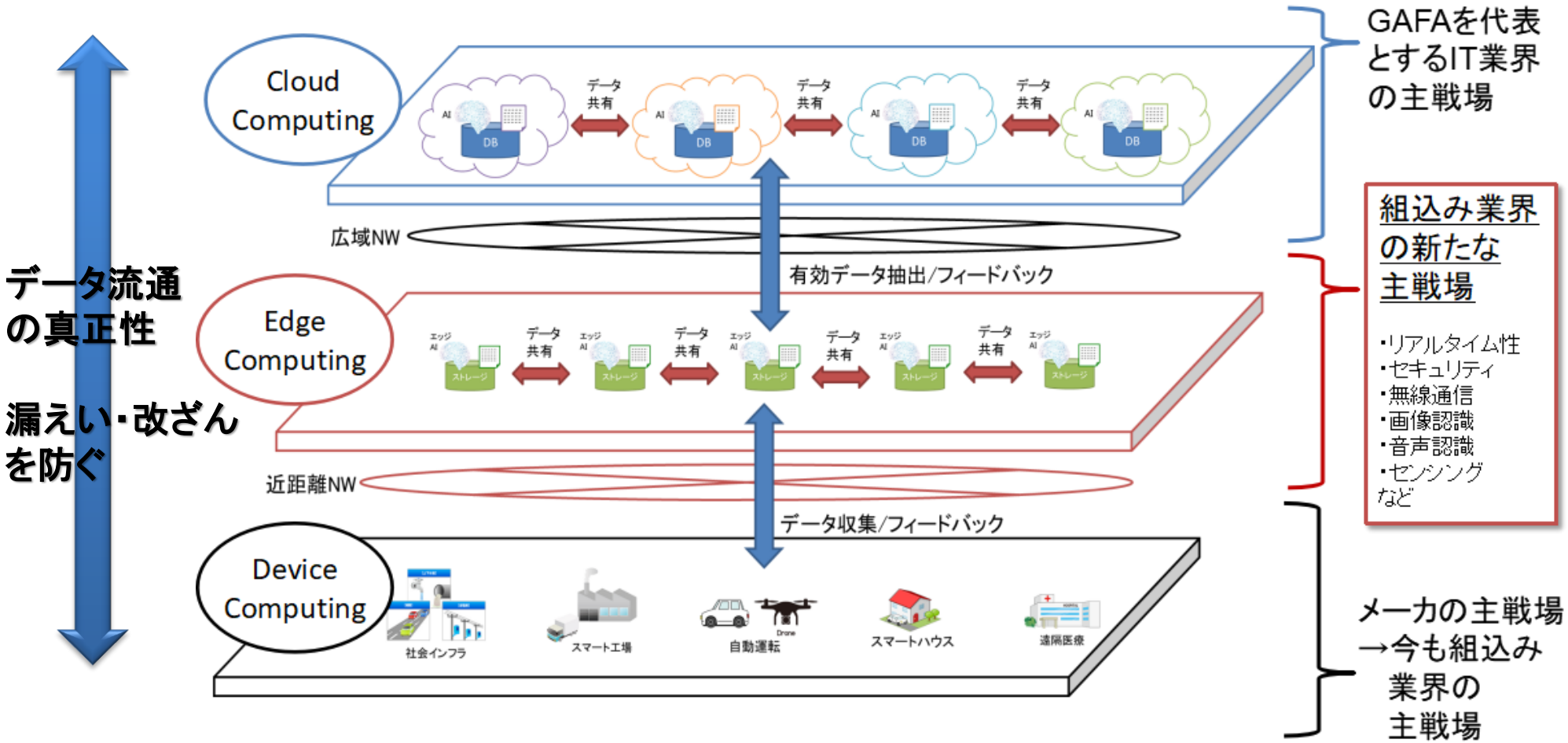
■ データ活用の基盤例：DX(Digital Transformation)



一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

1．IoTとは？

■ DFFT（Data Free with Trust）



IoTの課題

データ活用における３つの課題

2．IoTの課題

■ データ活用における３つの課題

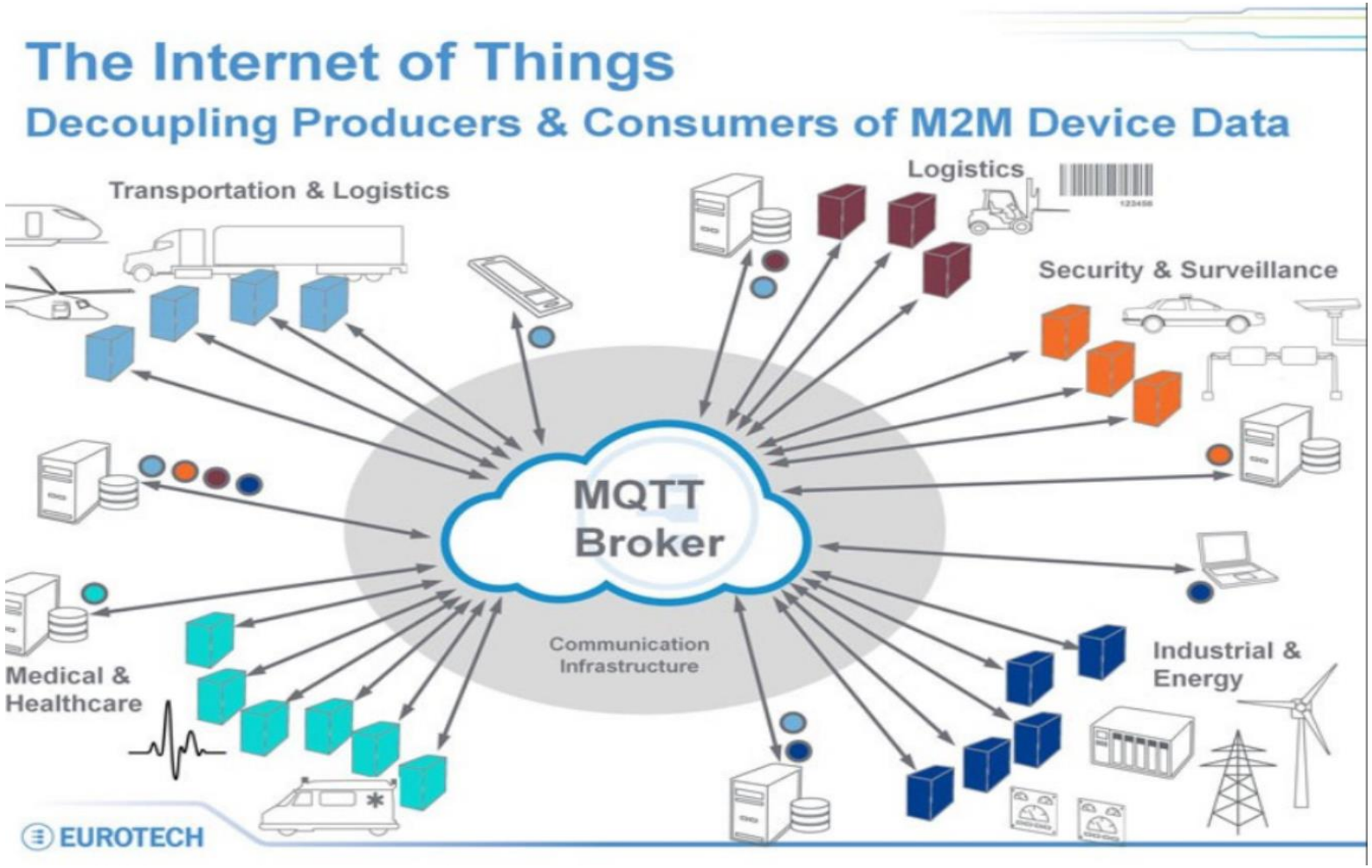
1. データのプライバシーの課題
2. データの使用権の課題
3. データの責任所在の課題

2．IoTの課題

■ MQTTプロトコルの情報漏えい例

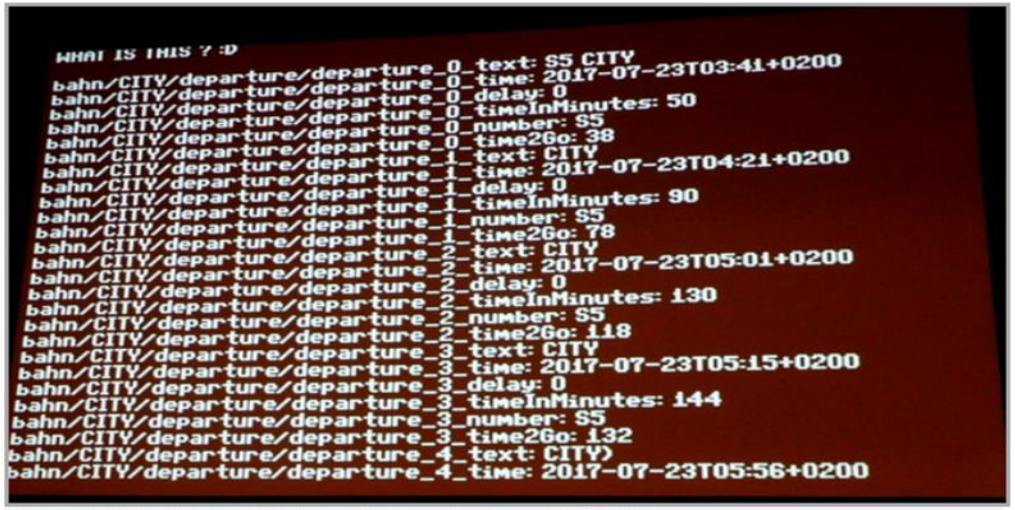
平文で通信できてしまう

DDoS攻撃に悪用される。
平文での情報やりとりのため
攻撃対象を見つけやすい。
JSONのTopic処理に様々な
問題（脆弱性）が発見され
ている。

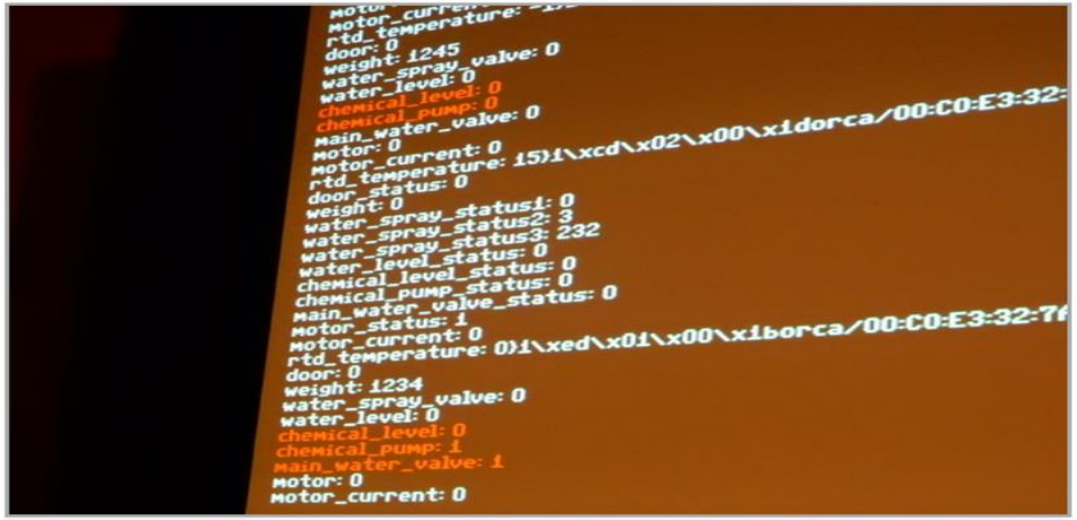


参考URL：https://www.trendmicro.com/jp/iot-security/news/3591
https://japan.zdnet.com/article/35129893/

2．IoTの課題



ドイツ鉄道の路線の運行状況に関するメッセージが丸見え



原子力発電所から流れてきたメッセージには、冷却装置やモーターの状況などが分かる

位置情報を継続的に取得すれば行動パターンがわかってしまう

★MQTTが利用される場合の課題

①大量のIoTデバイスとのコネクション
②再送への対応
③IoTデバイスへのプッシュ通知
④使用できるネットワーク帯域、
　バッテリー制限があるIoTデバイス

参考URL：https://ascii.jp/elem/000/001/538/1538505/#eid1538498
https://blogs.akamai.com/jp/2019/06/iot---iot-egge-connect--.html

2．IoTの課題

■ 監視カメラの脆弱性

- http://www.insecam.org/の例

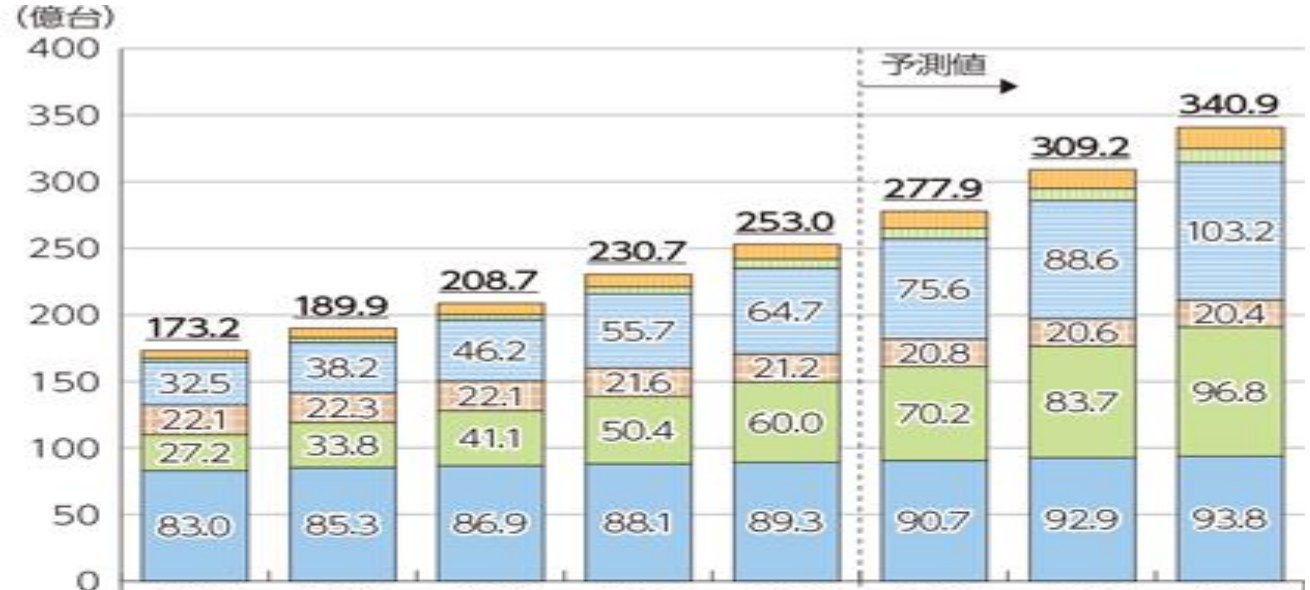
参考資料：IPA IoTセキュリティ教材 IoTのビジョンより引用

IoT機器のセキュリティ課題

現状の状況

3．IoT機器のセキュリティ課題

■ 世界のIoT機器の推移および予測



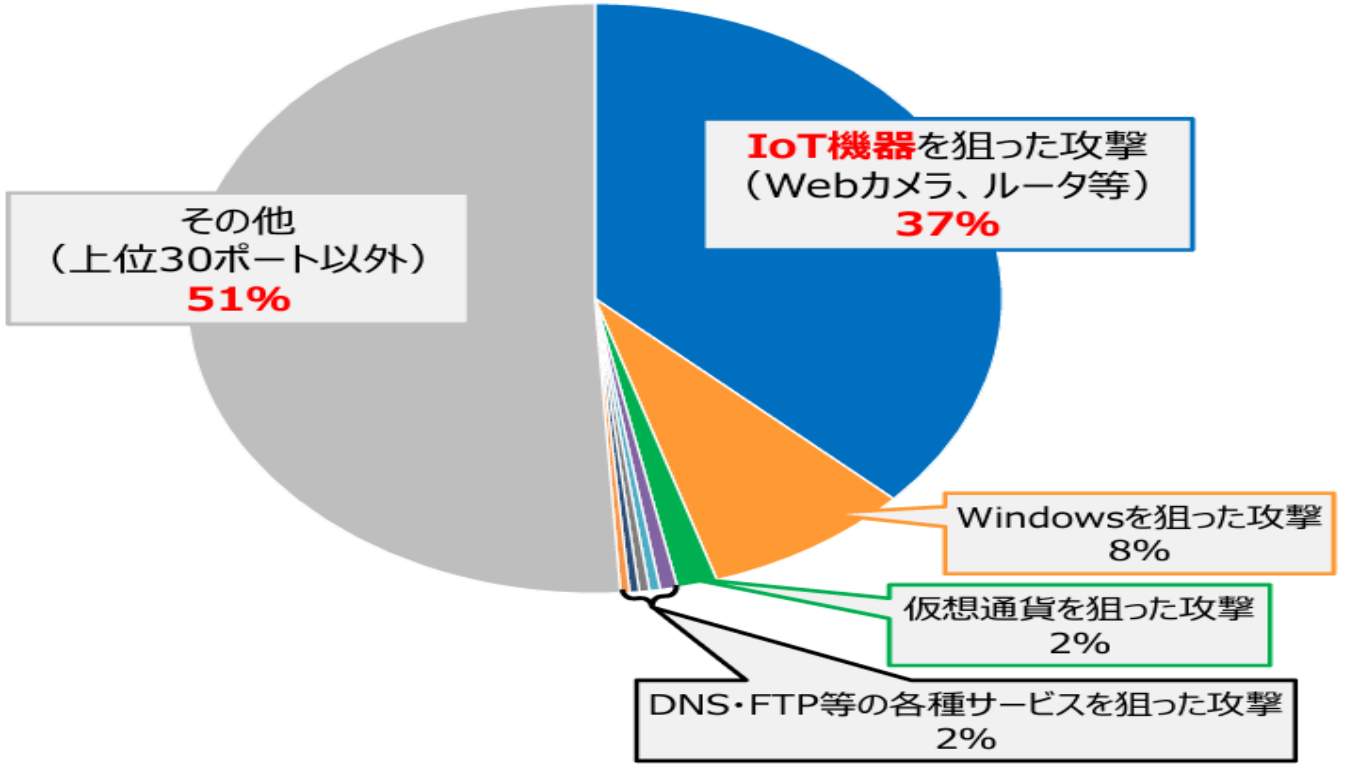
	2016	2017	2018	2019	2020	2021	2022	2023
合計	173.2	189.9	208.7	230.7	253.0	277.9	309.2	340.9
自動車・宇宙航空	5.7	7.1	8.5	9.8	11.3	12.7	14.2	15.7
医療	2.6	3.3	4.0	5.1	6.5	7.8	9.2	10.9
産業用途	32.5	38.2	46.2	55.7	64.7	75.6	88.6	103.2
コンピューター	22.1	22.3	22.1	21.6	21.2	20.8	20.6	20.4
コンシューマー	27.2	33.8	41.1	50.4	60.0	70.2	83.7	96.8
通信	83.0	85.3	86.9	88.1	89.3	90.7	92.9	93.8

参考URL：総務省 情報通信白書ポイント

3．IoT機器のセキュリティ課題

■ NICT NICTERによる統計結果

✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が年々多様化**



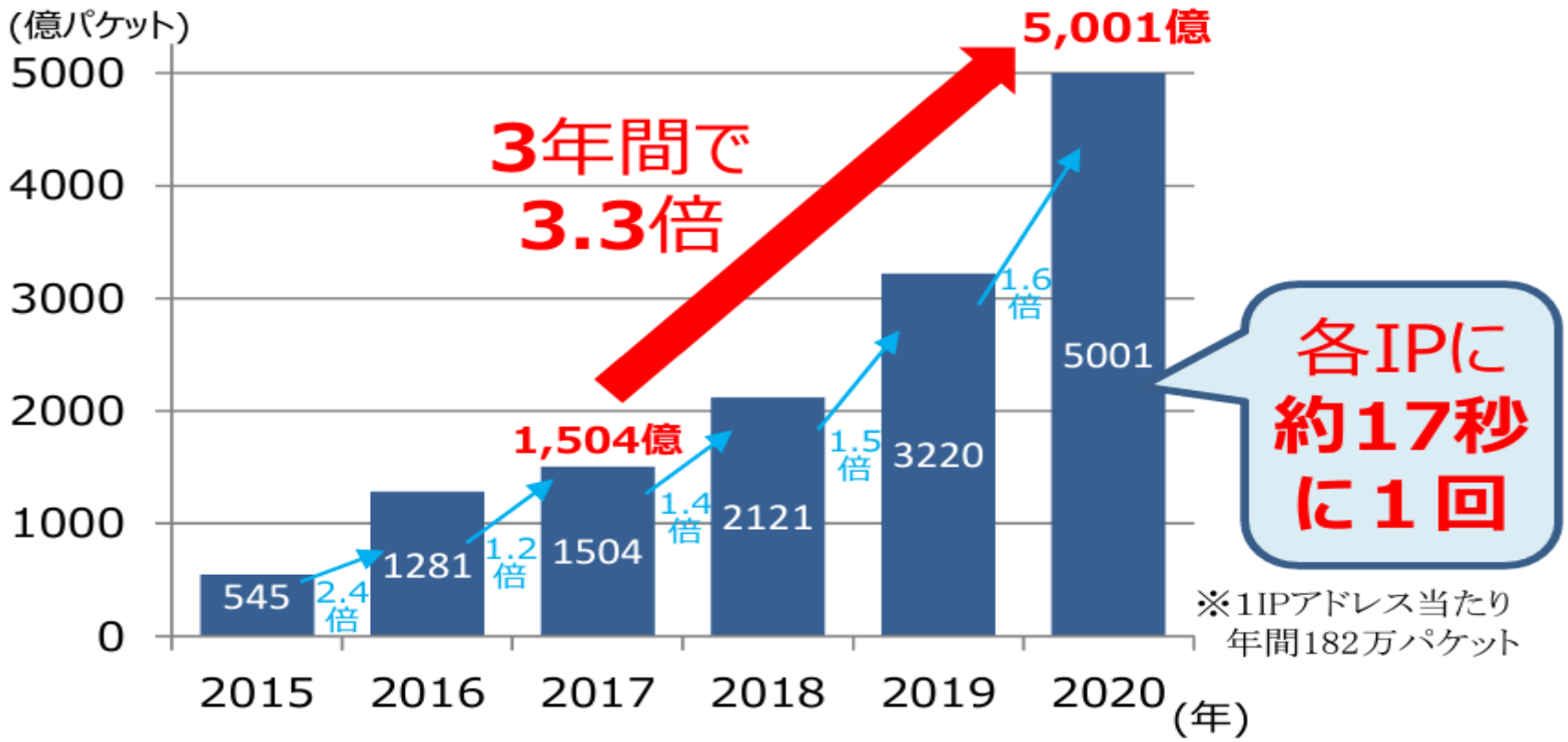
※ NICTERで2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析したもの。なお、IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

参考URL：総務省 ICTサイバーセキュリティ総合対策2021

3．IoT機器のセキュリティ課題

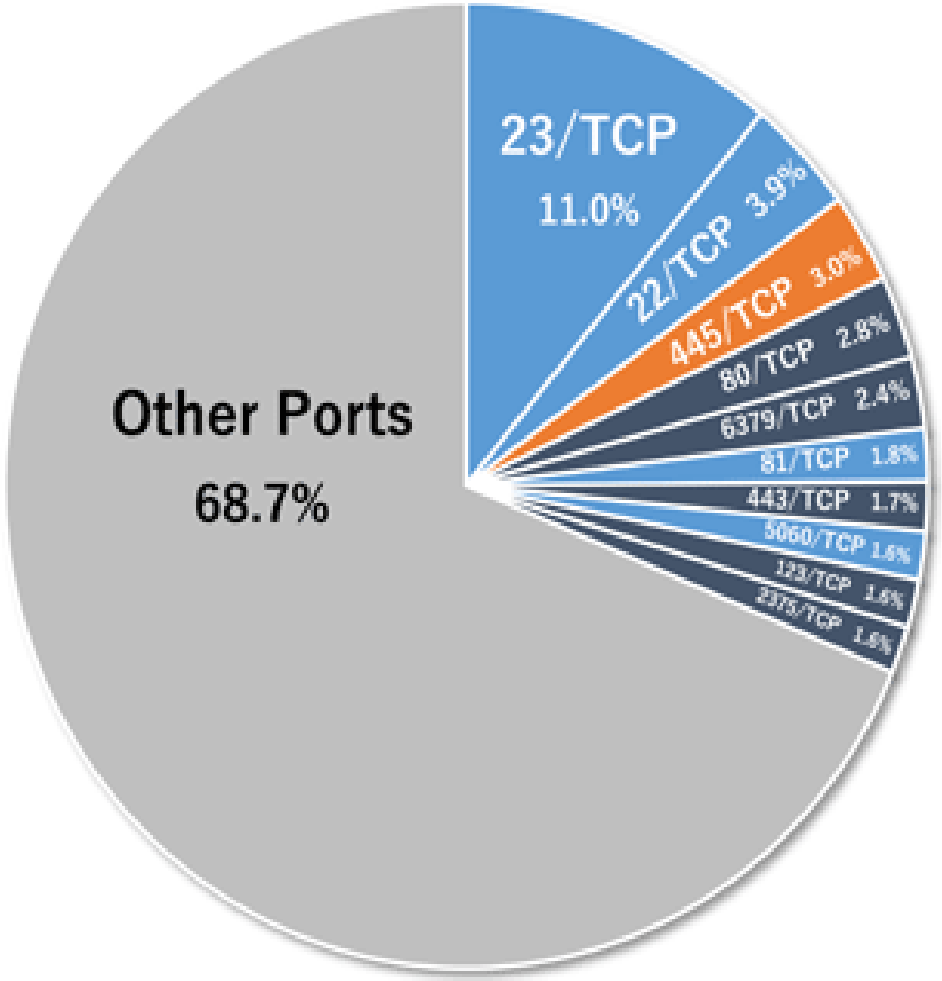
■ NICT NICTERによる統計結果

図１　IoT 機器を狙った攻撃の増加
（NICTER により１年間に観測されたサイバー攻撃回数）



参考URL：総務省 ICTサイバーセキュリティ総合対策2021

3．IoT機器のセキュリティ課題



ポート番号	攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
445/TCP	Microsoft-DS（SMB, Samba等）
80/TCP	HTTP（Web管理画面）
6379/TCP	Redis
81/TCP	HTTP（ホームルータ等）
443/TCP	HTTPS (Webサーバ)
5060/UDP	SIP (PBX, ルータ等)
123/UDP	NTP
2375/TCP	Docker REST API

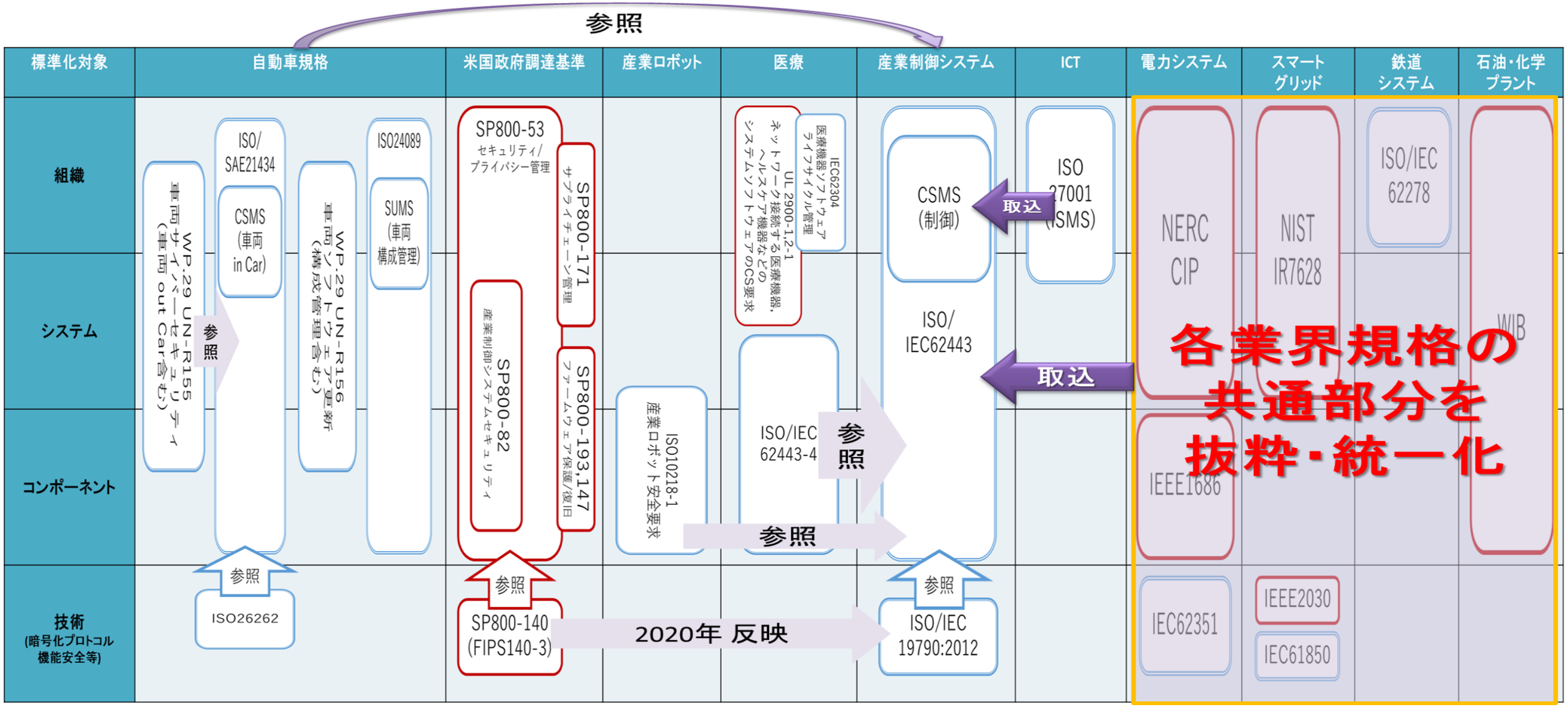
宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

参考URL：情報通信研究機構 NICTER観測レポート2021

国際規格の動向

分野別のセキュリティ国際規格

4．国際規格の動向



4．国際規格の動向

■ 法律、国際規格以外にも、コンシューマ用途のIoT機器に対するガイドラインや認定制度もでてきている。

NIST IR8259

IoT機器製造業者向けの基礎的サイバーセキュリティ活動と呼ばれるもので、医療のIoT機器も含む、医療機器製造業者のサイバーセキュリティ活動を「市販前」と「市販後」の2フェーズに分け、全6つの活動において考慮すべき事項

ETSI 103 645
Baseline Requirements

ETSI 303 645
Baseline Requirements

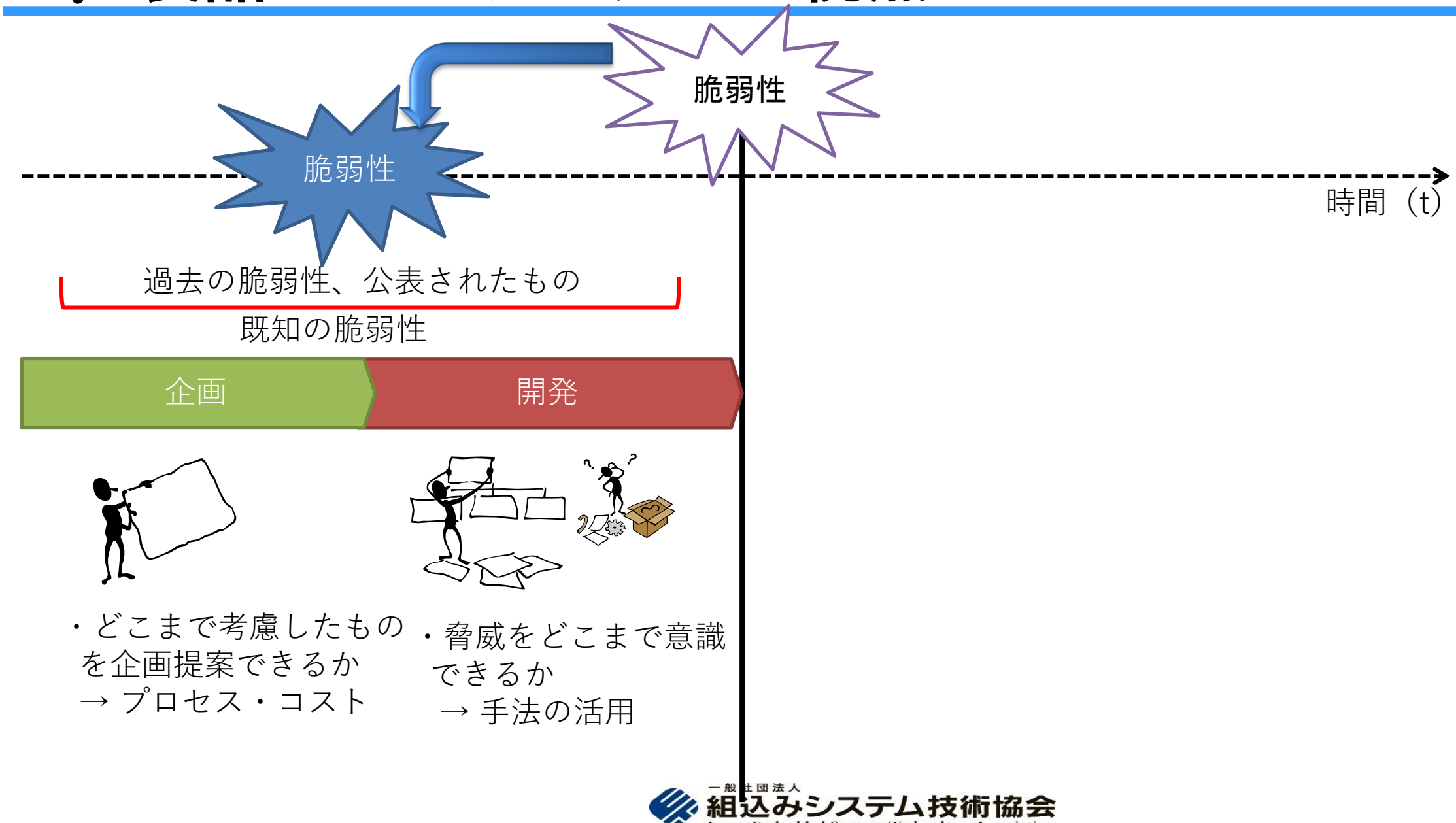
消費者向けIoT機器のセキュリティ・データ保護規定

IoT SF
自己認証開始

製品ライフサイクルの視点

企画段階～開発までのセキュリティ対策

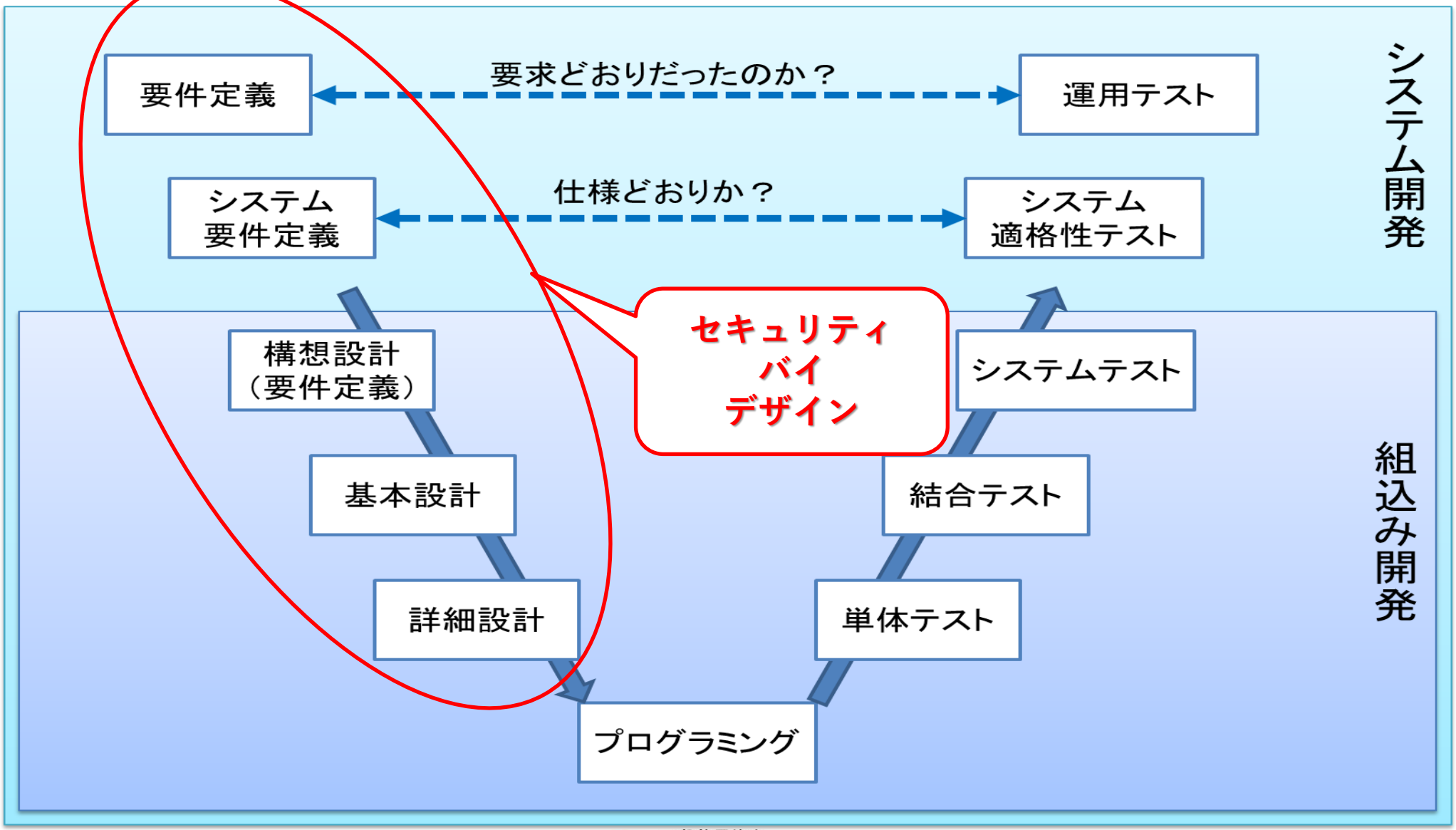
5．製品ライフサイクルの視点



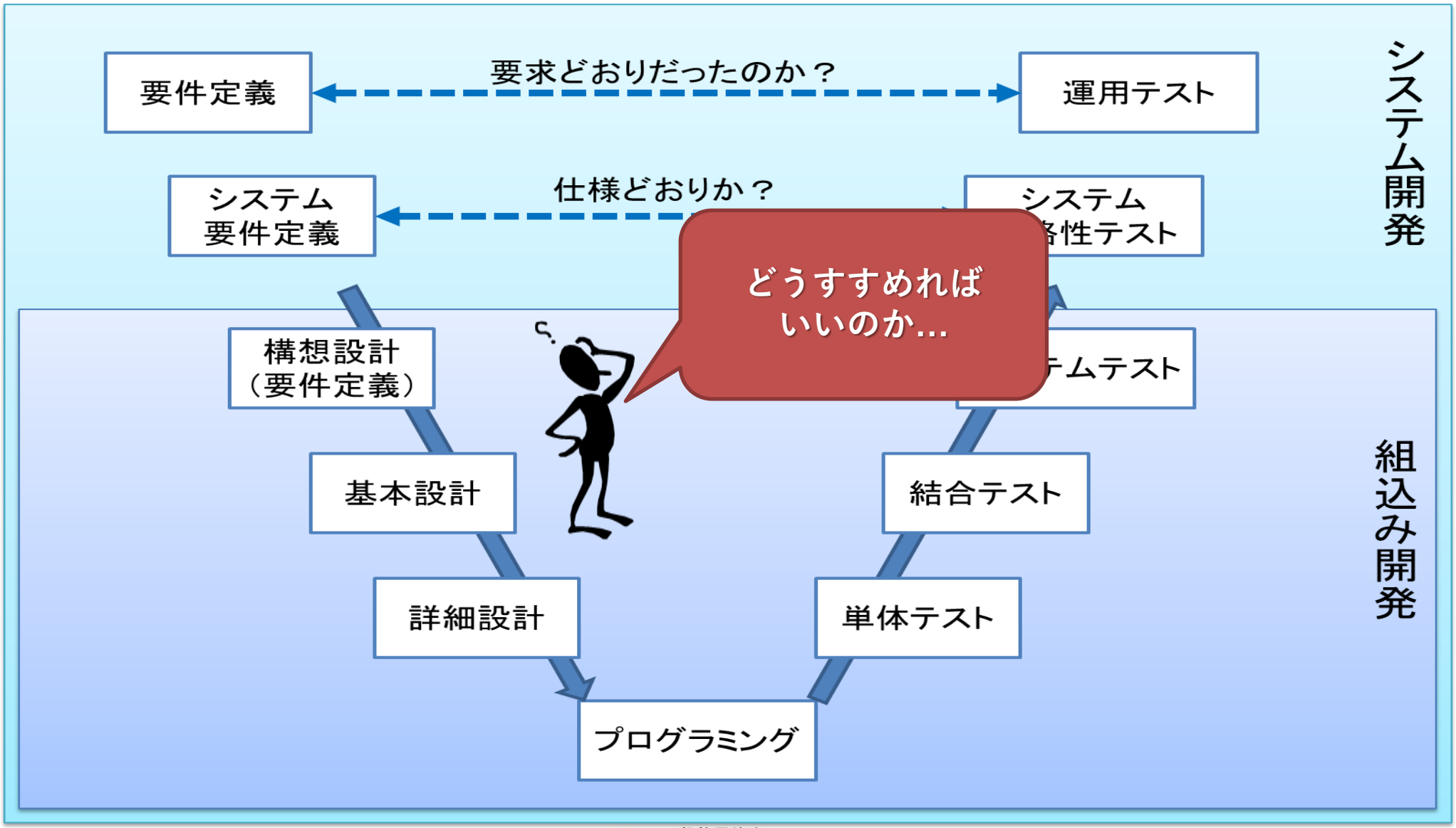
セキュリティ設計入門

SbD（Security by Design）

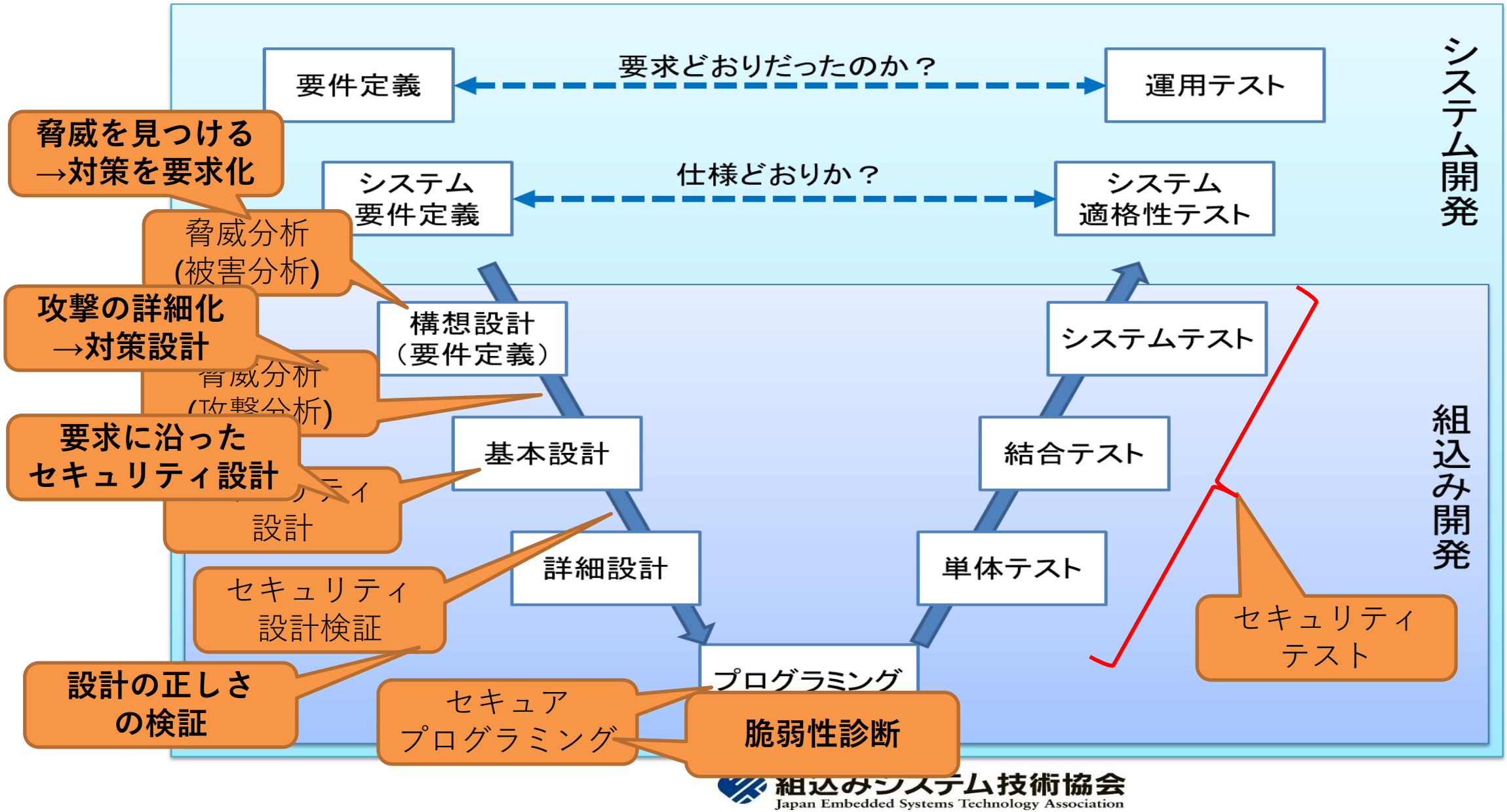
6．セキュリティ設計



6．セキュリティ設計



6．セキュリティ設計

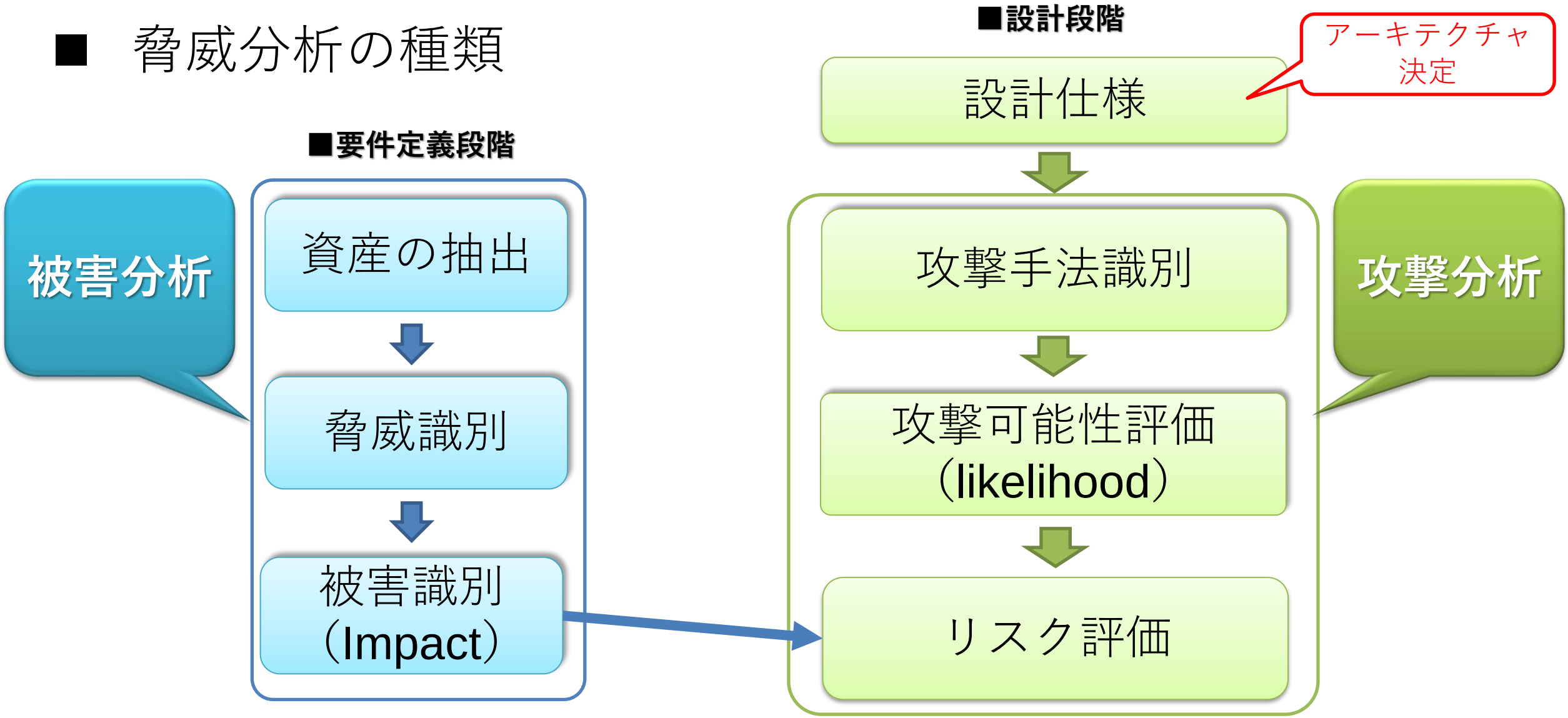


脅威分析入門

脅威分析とは？

7．脅威分析入門

■　脅威分析の種類



4．脅威分析とは？

被害分析

改ざんされたら？

盗まれたら二次被害は？
etc...

魅力的な資産？
個人情報、安全機能
etc...

資産分析

攻撃者(人)

脅威

攻撃

脆弱性

資産

一緒に考えることが
重要

攻撃分析

破壊・改ざん

盗聴・搾取
マルウェアの送り込み
etc...

脆弱性対策

セキュアブート、暗号化、
侵入検知
etc...

攻撃経路分析

ネットワーク、CAN、
デバックポート
etc...

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

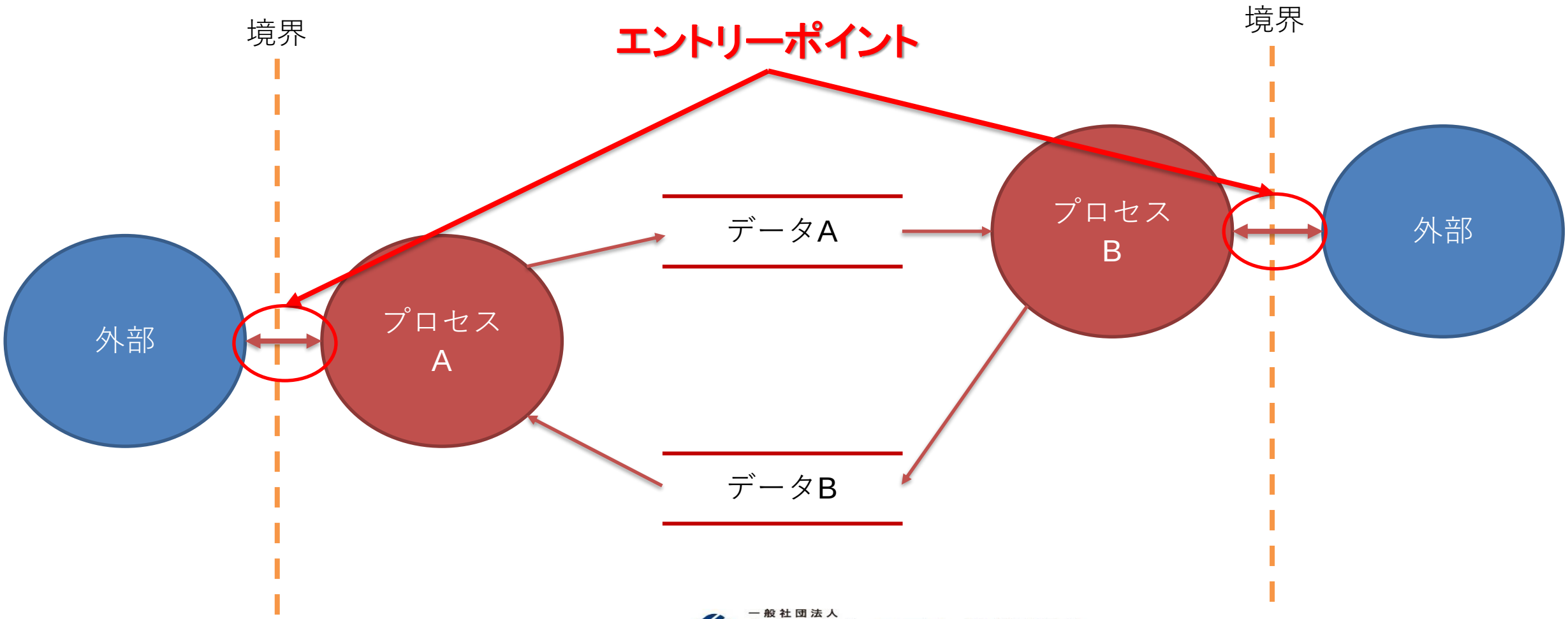
7．脅威分析入門

■ 脅威分析まとめ

- 対象システムのアーキテクチャ構造に対して、脅威を識別し、影響を評価し、対策を策定をする分析を指します。
- 「脅威」は、要求策定者、利害関係者(ステークホルダー)ではなく、「攻撃者(第三者)」の悪意にもとづいているため、分析が難しいと言われています。
  - 分析対象が「人」となるため分析が難しい。

7．脅威分析入門

■ DFD(Data Flow Diagram)利用



7．脅威分析入門

攻撃者

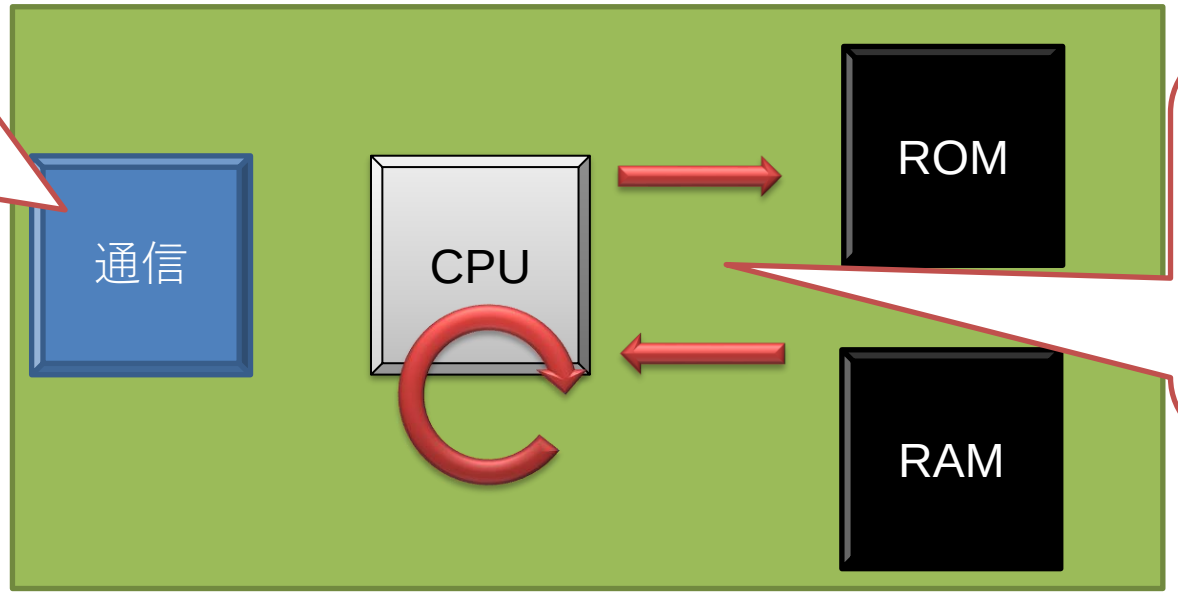
調査フェーズ（情報収集）	攻撃準備フェーズ（攻撃の準備）	攻撃フェーズ（攻撃実行）	事象発生
ポートスキャン 盗聴 分解(プログラム解析)	パスワード辞書 マルウェア 攻撃用スクリプト BOFツール	パスワードクラック BOFツール 攻撃スクリプト バックドア マルウェア	遠隔操作 情報搾取 改ざん 事象の公開

7．脅威分析入門

攻撃者

①ネットワーク系のI/F
- Ethernet
- Wi-Fi
- Bluetooth

②シリアル系のI/F
- USB
- CAN



③専用バスのI/F
- I2C
- SPI

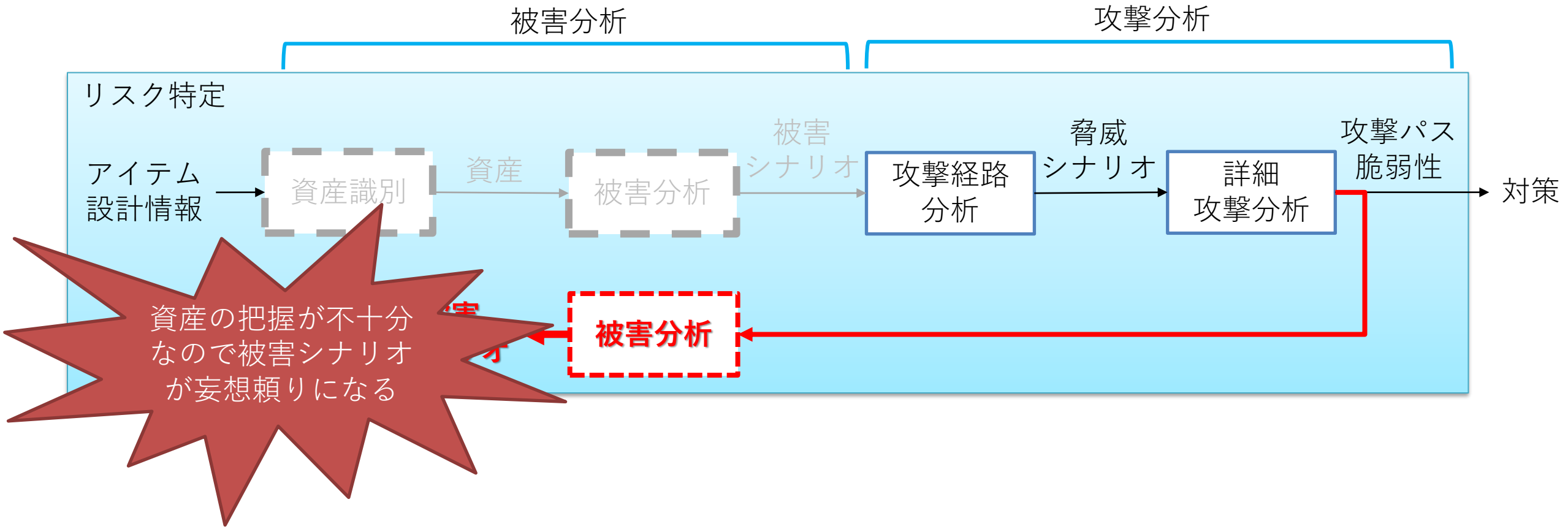
④デバッグ系のI/F
- Serial
- JTAG

7．脅威分析入門

■ STRIDE

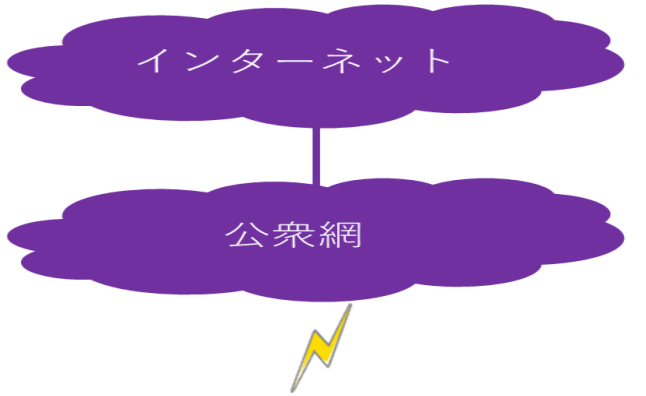
Spoofing（なりすまし）
Tampering（改ざん）
Repudiation（否認）
Information Disclosure（情報漏えい）
Denial of Service（サービス拒否）
Elevation of Privilege（特権の昇格）

7．脅威分析入門



7．脅威分析入門

■ 製品開発する担当によっては、脅威分析のやり方が変わってくる可能性がある。



システム構成 A

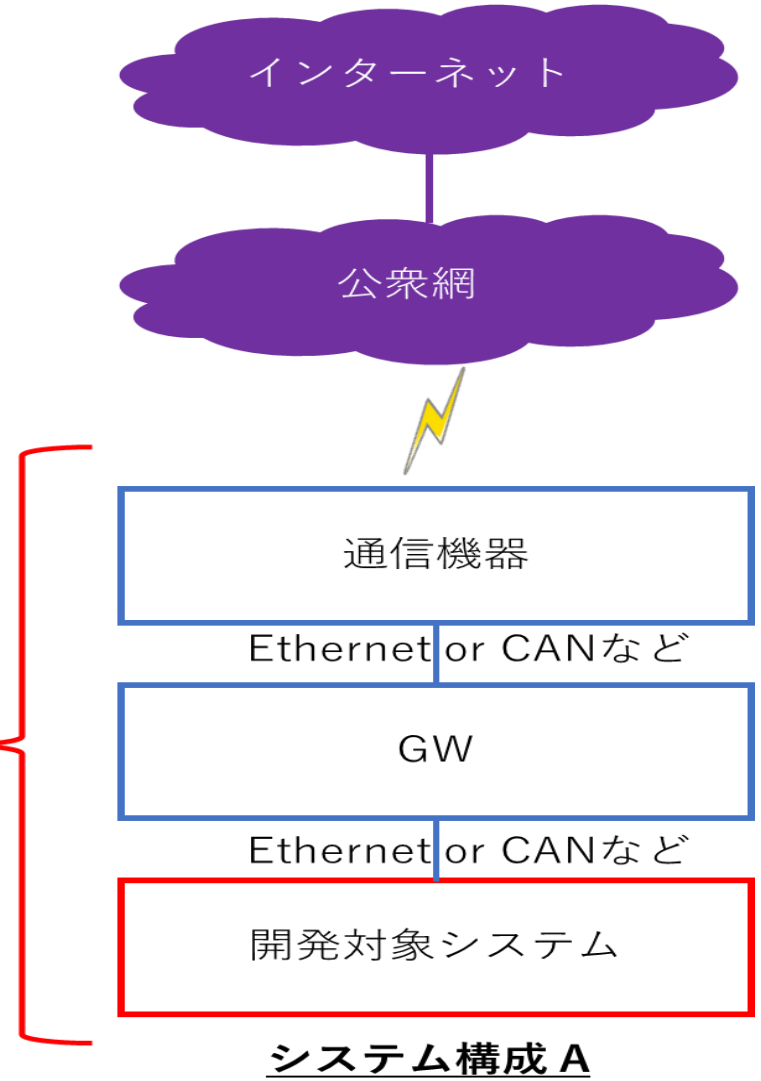
システム構成 B

7．脅威分析入門

■ 受託開発の場合

- 発注先との責任分担が必要

発注先がサイバーセキュリティ対応として、コンセプトを決め、**脅威分析を実施している場合**、**サイバーセキュリティ要求**として必要な機能を明示してくる場合は、**脅威分析のやり方を工夫**する必要が出てくる。

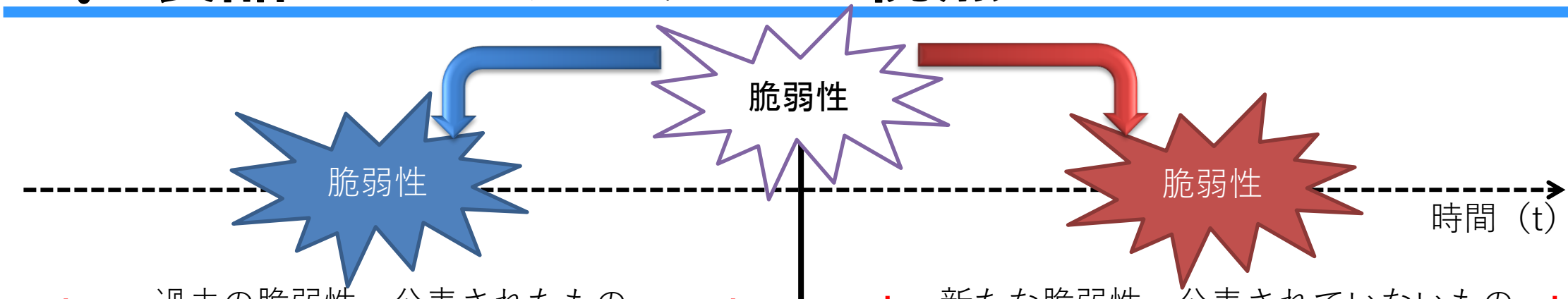


システム構成 A

製品ライフサイクルの視点

運用～廃棄までのセキュリティ対策

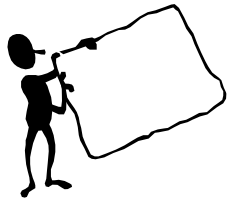
8．製品ライフサイクルの視点



過去の脆弱性、公表されたもの
既知の脆弱性

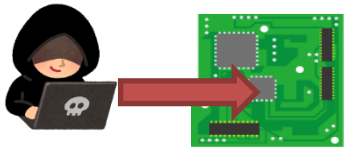
新たな脆弱性、公表されていないもの
未知の脆弱性

企画 | 開発 | 運用 | 破棄

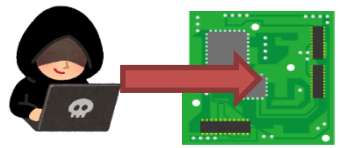


・どこまで考慮したものを企画提案できるか
→ プロセス・コスト

・脅威をどこまで意識できるか
→ 手法の活用



・ネットワークなどからの脅威
・製品分解での脅威



・製品分解での脅威

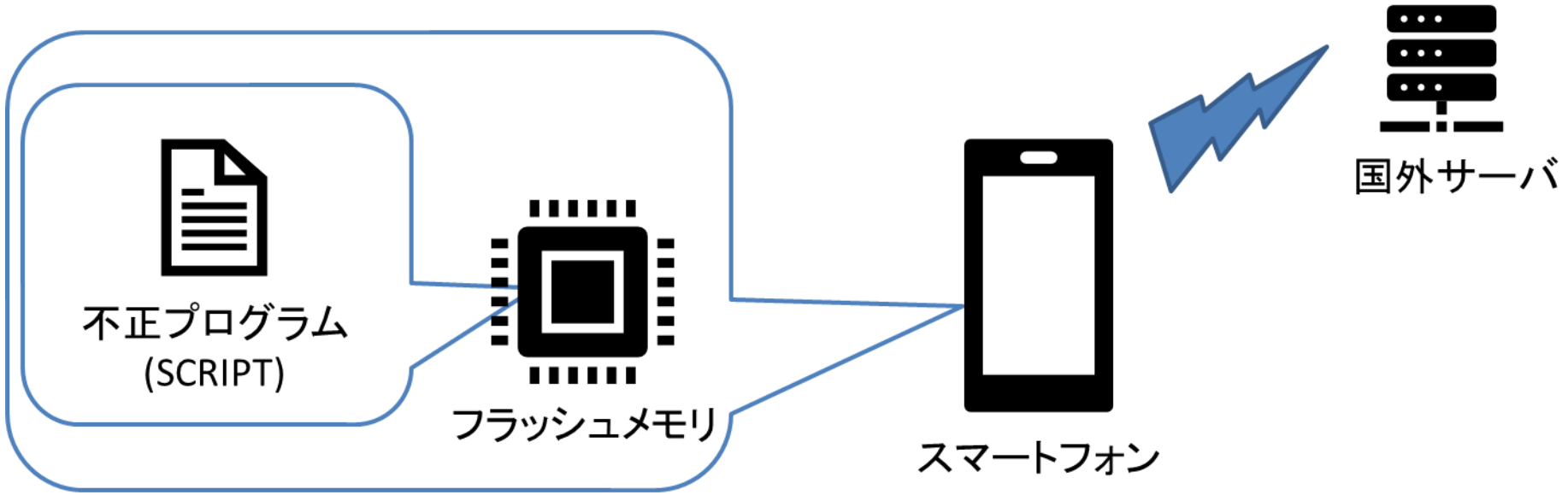
一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

サプライチェーンにおける課題

外部調達におけるセキュリティ課題

9．サプライチェーンにおける課題

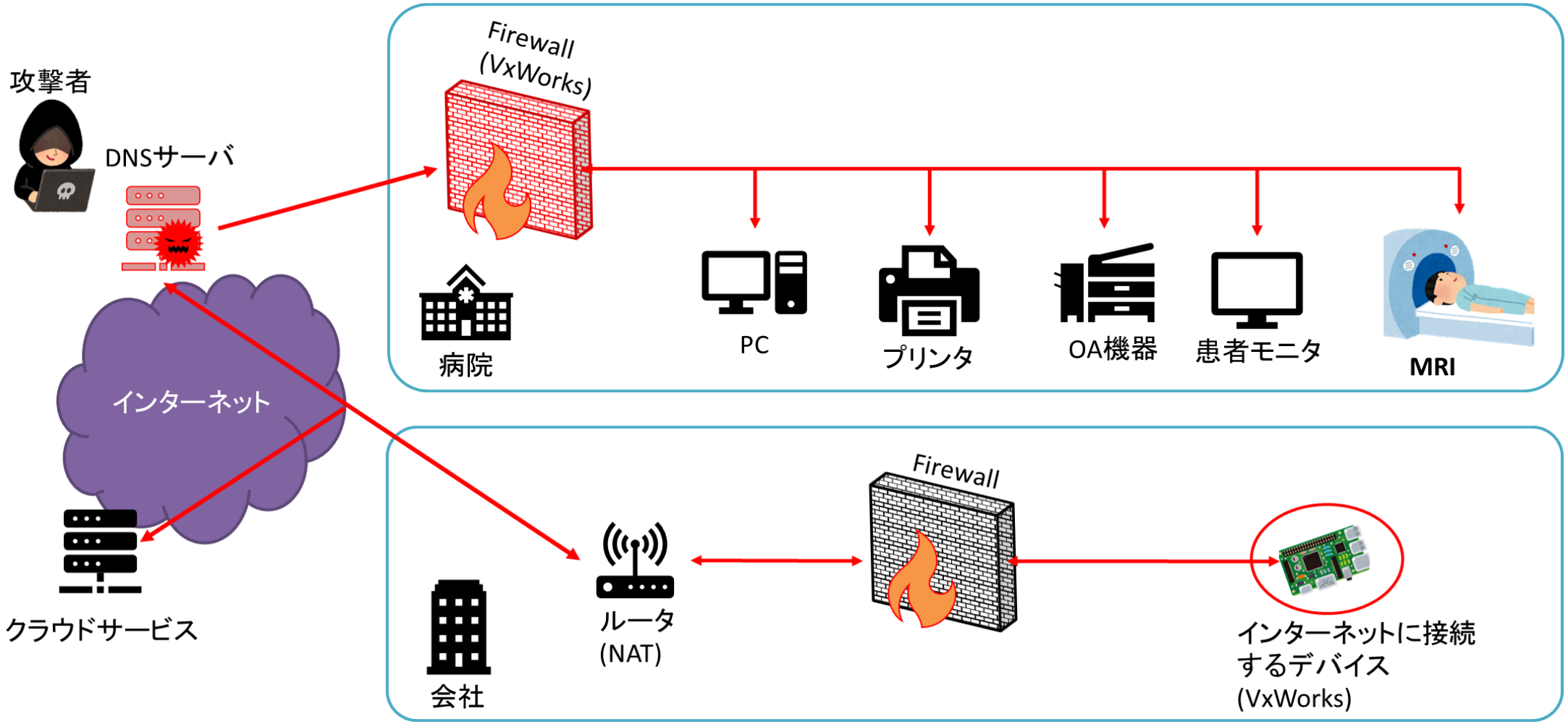
■ 2016年の米国における携帯電話からの情報漏えい



参考文献：経済産業省:サイバー・フィジカル・セキュリティ対策フレームワーク

9．サプライチェーンにおける課題

■ 2019年 商用RTOSにおける脆弱性「URGENT/11」

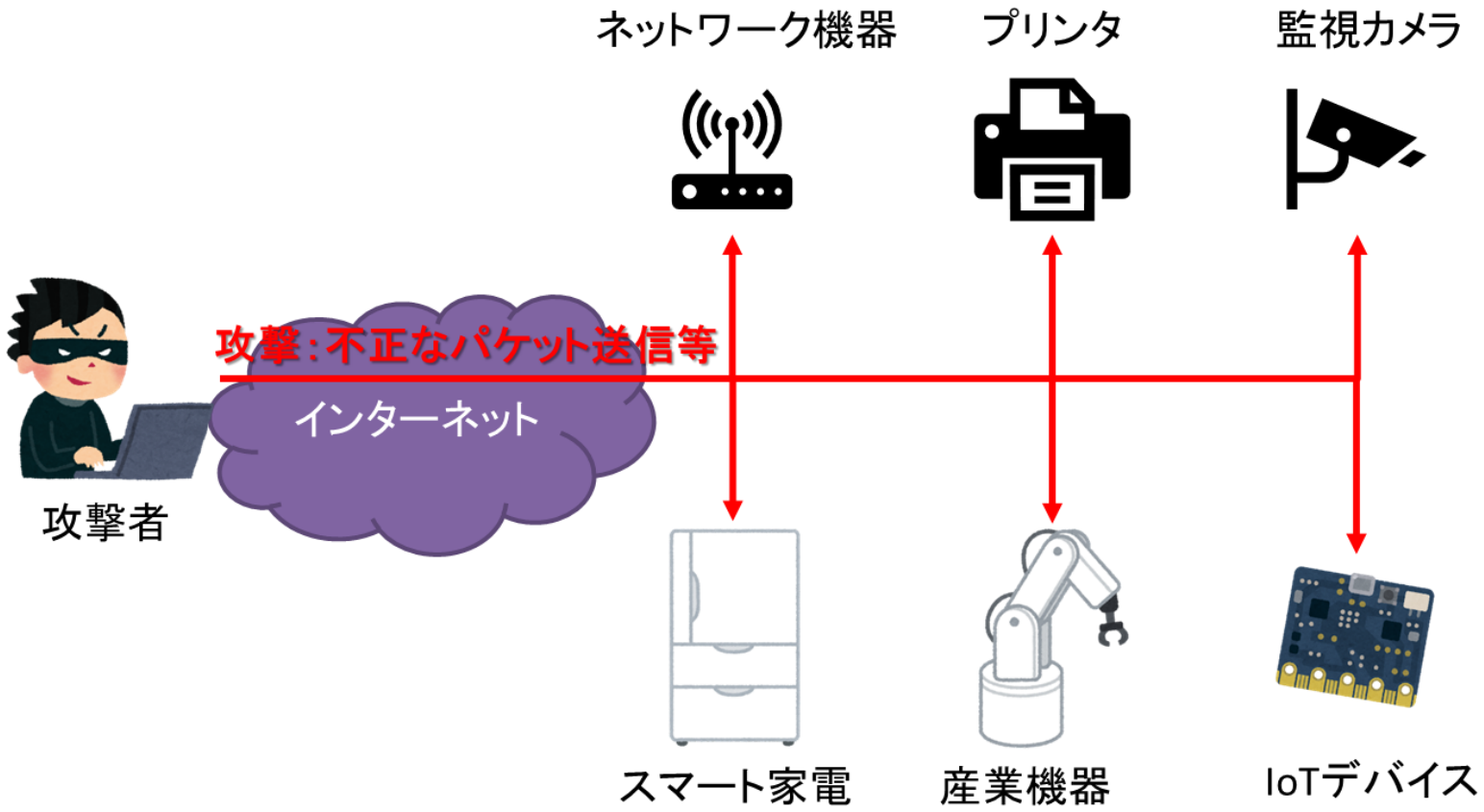


一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

参考URL：ARMIS社 URENT/11

9．サプライチェーンにおける課題

■ 2020年 プロトコルスタックの脆弱性 「Ripple20」



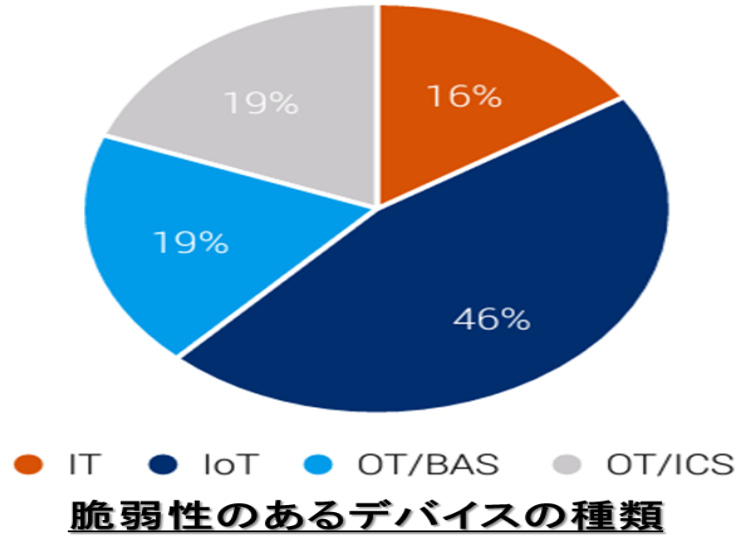
想定被害：任意コード実行、情報漏えい、DoS攻撃

- ✓ Treck社 TCP/IP Stackは、HP社、Schneider Electric社、Intel社、Rockwell Automation社、Caterpillar社、Baxter社党の製品が採用
- ✓ 同様の脆弱性が、関連する他のTCP/IPスタックにも存在することが報告されている。

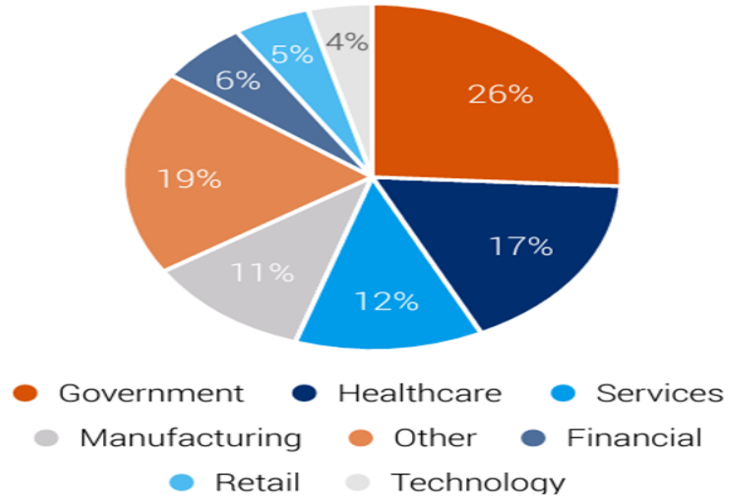
参考URL：JSOF社 Ripple20

9．サプライチェーンにおける課題

■ 2020年 プロトコルスタックの脆弱性「AMNESIA:33」



脆弱性のあるデバイスの種類



脆弱性のあるデバイスが使われている分野

影響範囲
以下のTCP/IPスタックを使用しているデバイス ✓ uIP、Contiki OS、Contiki-NG ✓ Nut/Net ✓ FNET ✓ picoTCP、pico TCP-NG

脆弱性「NAME:WRECK」の影響範囲
以下のTCP/IPスタックを使用しているデバイス ✓ Free BSD ✓ IPnet ✓ Nucleus NET ✓ NetXzz

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

参考URL：FORESOUT社 AMNESIA:33

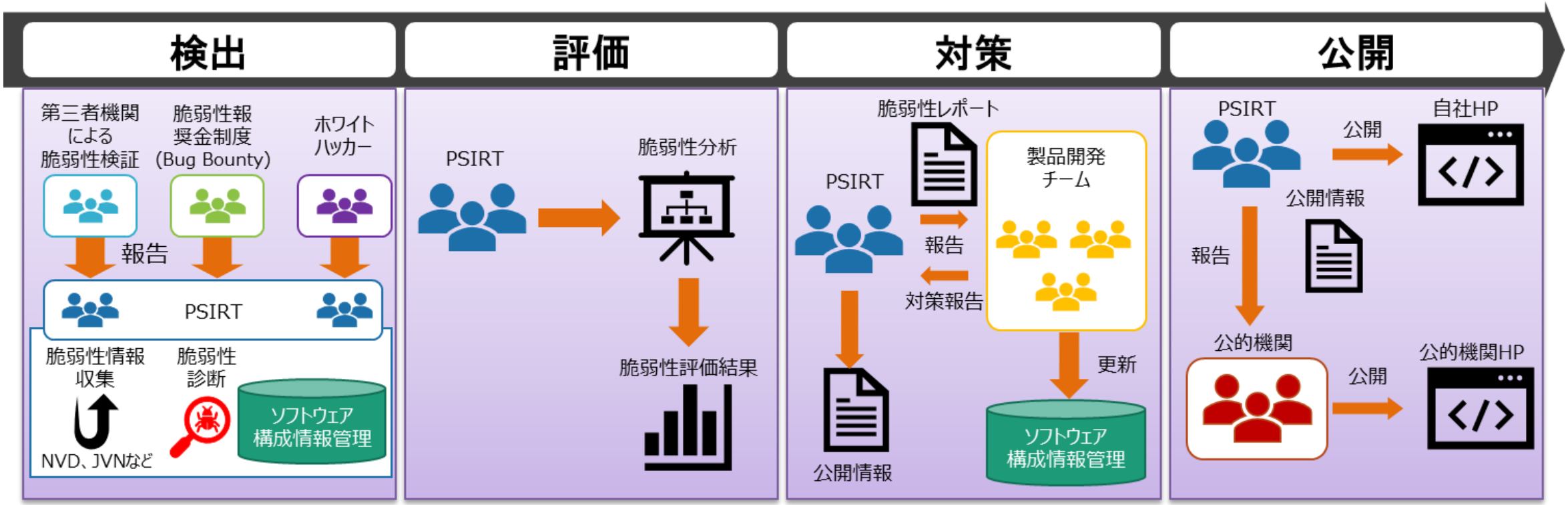
インシデント対応の事例紹介

CVE情報から対策までのフロー

10. インシデント対応の事例紹介

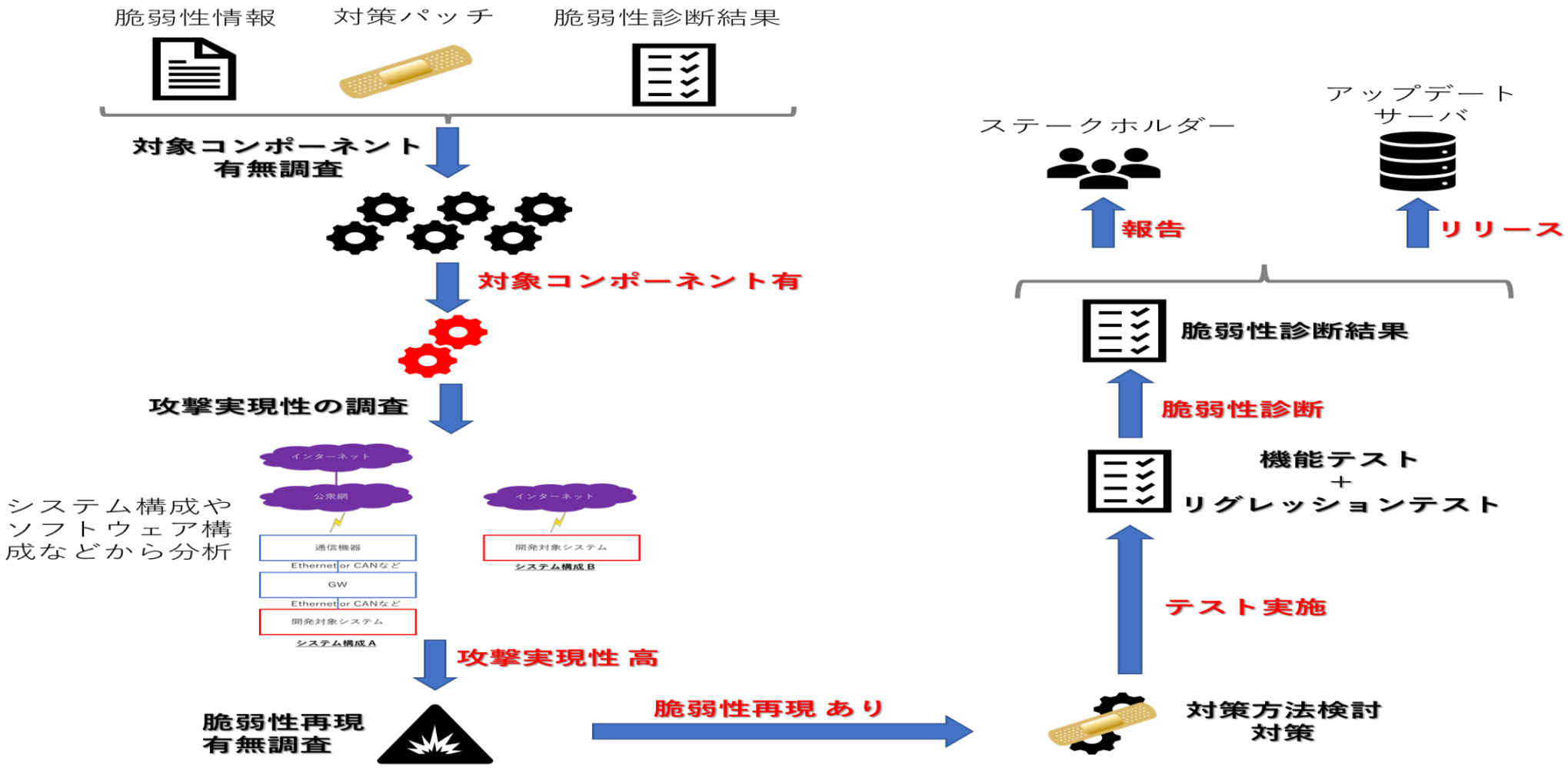
■ 脆弱性対策は、検出～公開までの運用フローがある。

- 日々、脆弱性の監視を行いながら、脆弱性が発見された場合には対策、公開までの対応が必要になる。



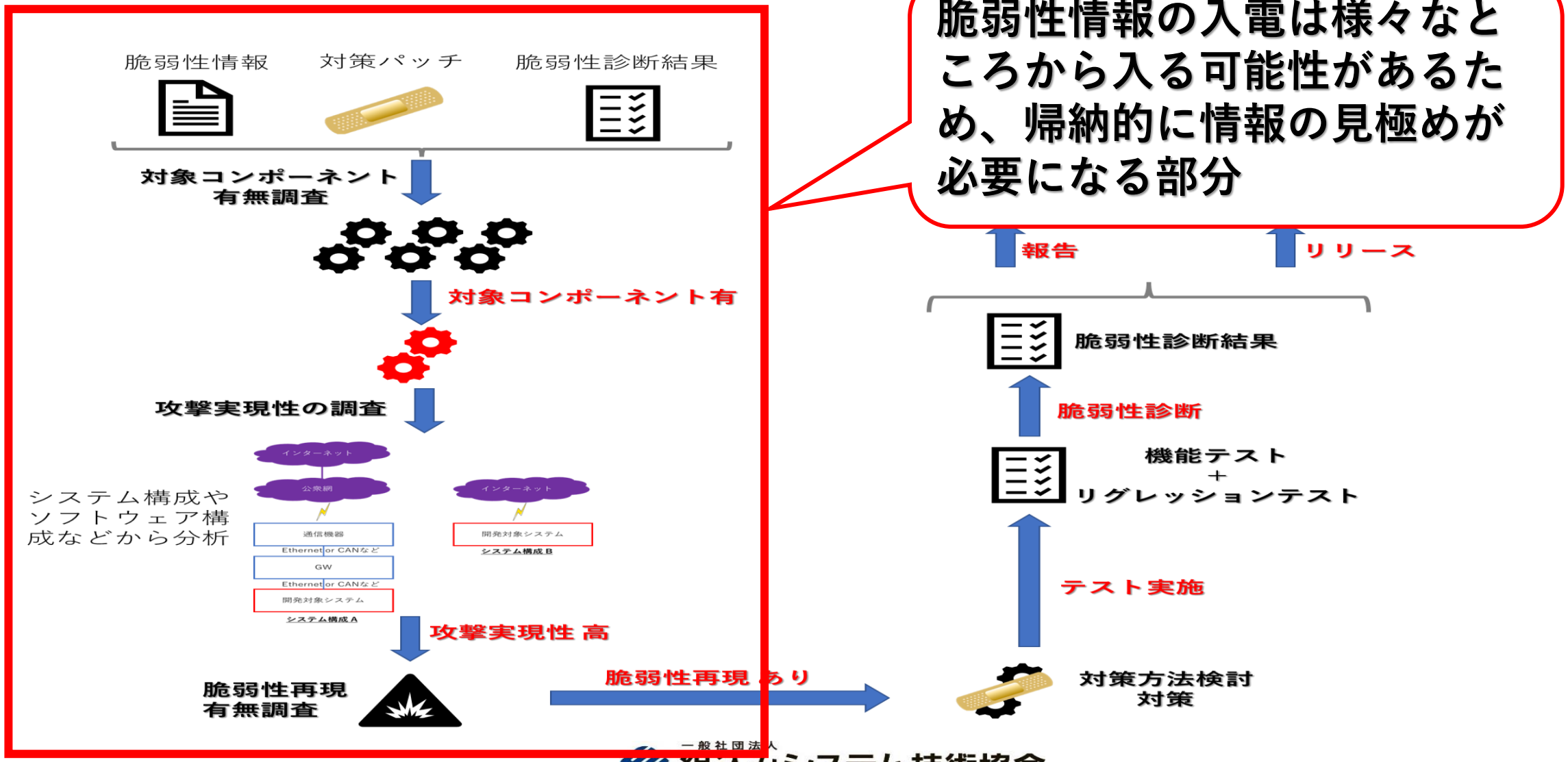
10. インシデント対応の事例紹介

■ 例：対応時のフロー



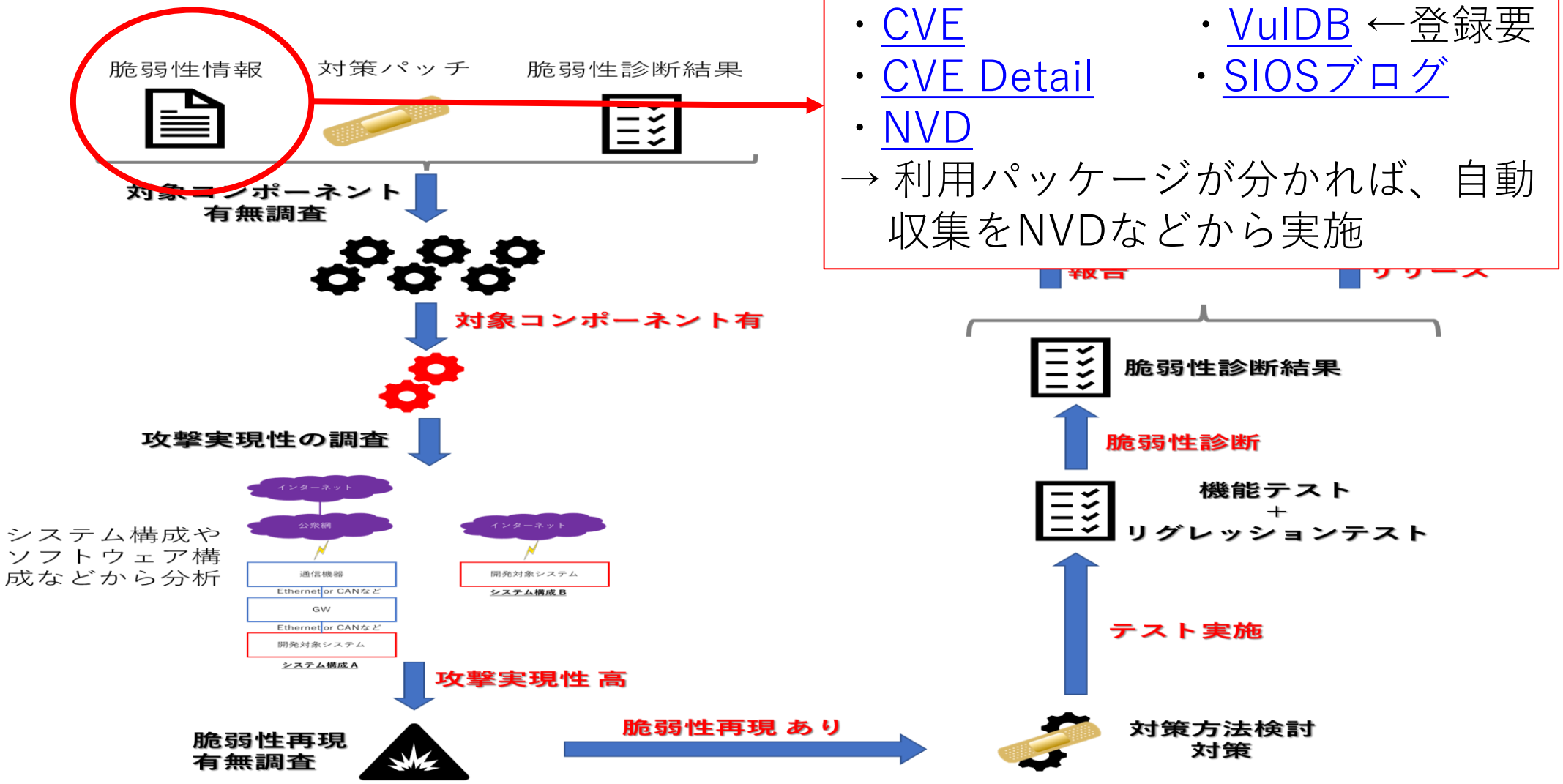
一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

10. インシデント対応の事例紹介



一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

10. インシデント対応の事例紹介



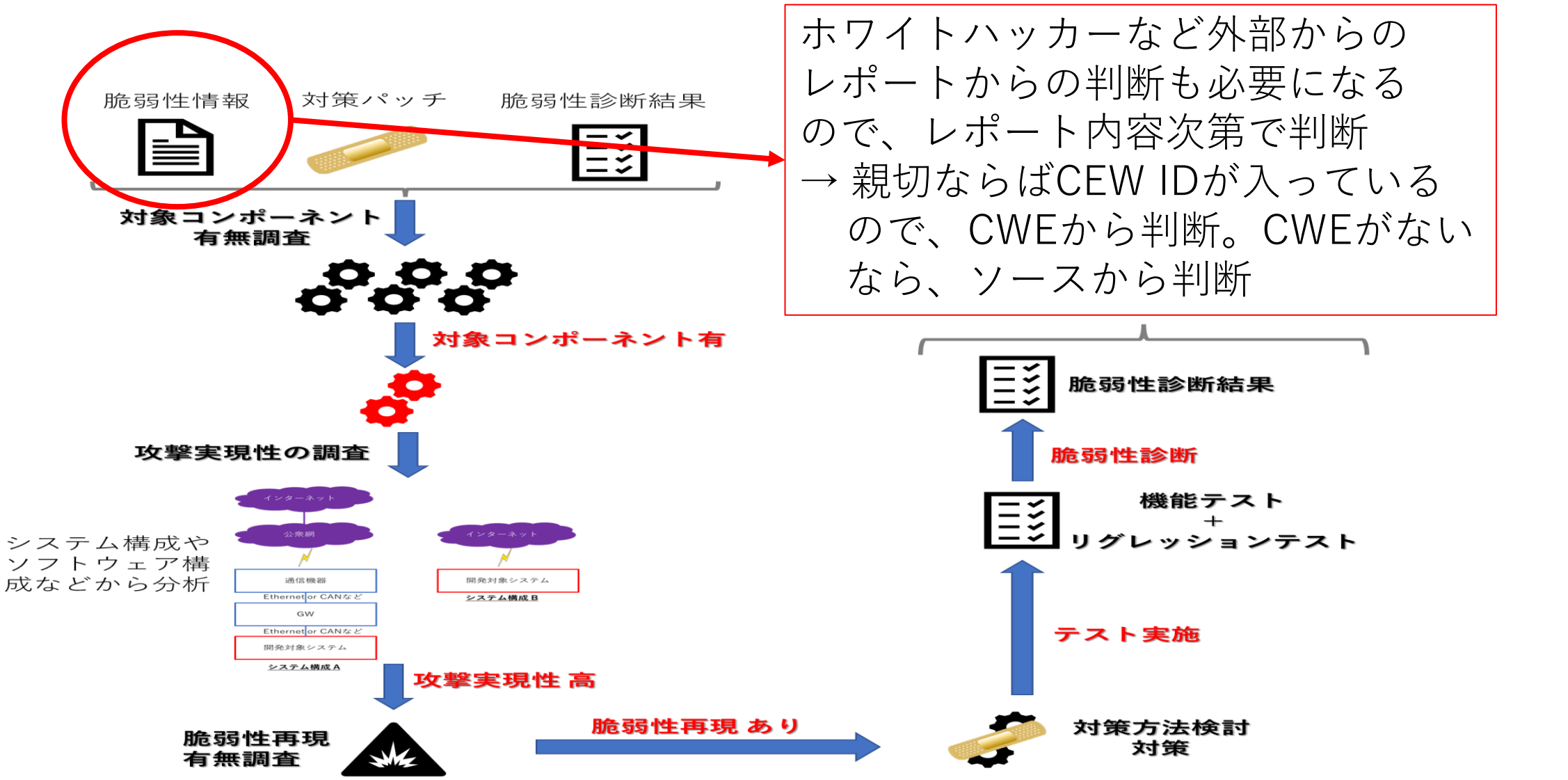
情報収集サイト

- CVE
- CVE Detail
- NVD
- VulDB ←登録要
- SIOSブログ

→ 利用パッケージが分かれば、自動収集をNVDなどから実施

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

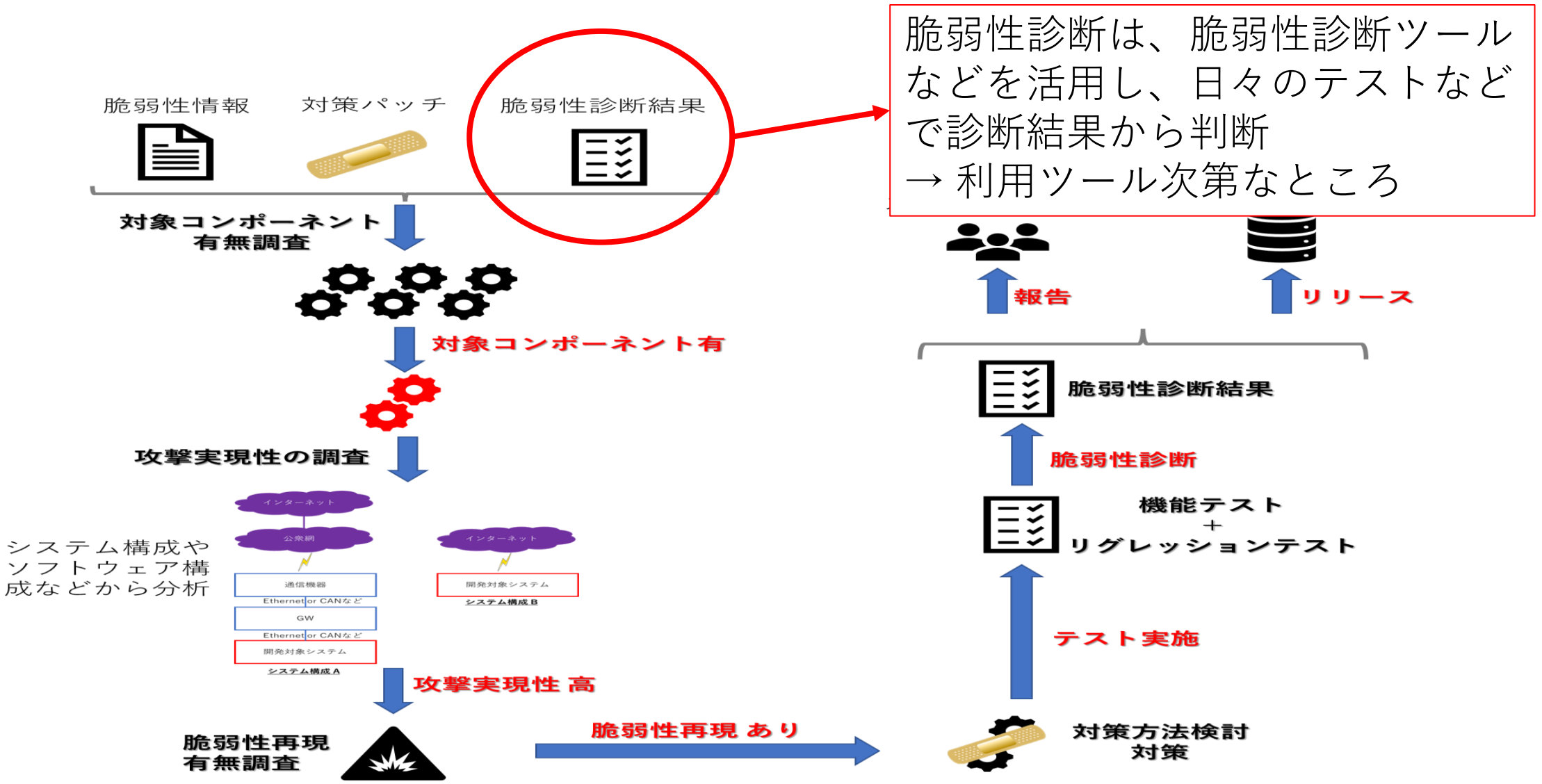
10. インシデント対応の事例紹介



ホワイトハッカーなど外部からのレポートからの判断も必要になるので、レポート内容次第で判断
→ 親切ならばCEW IDが入っているので、CWEから判断。CWEがないなら、ソースから判断

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

10. インシデント対応の事例紹介

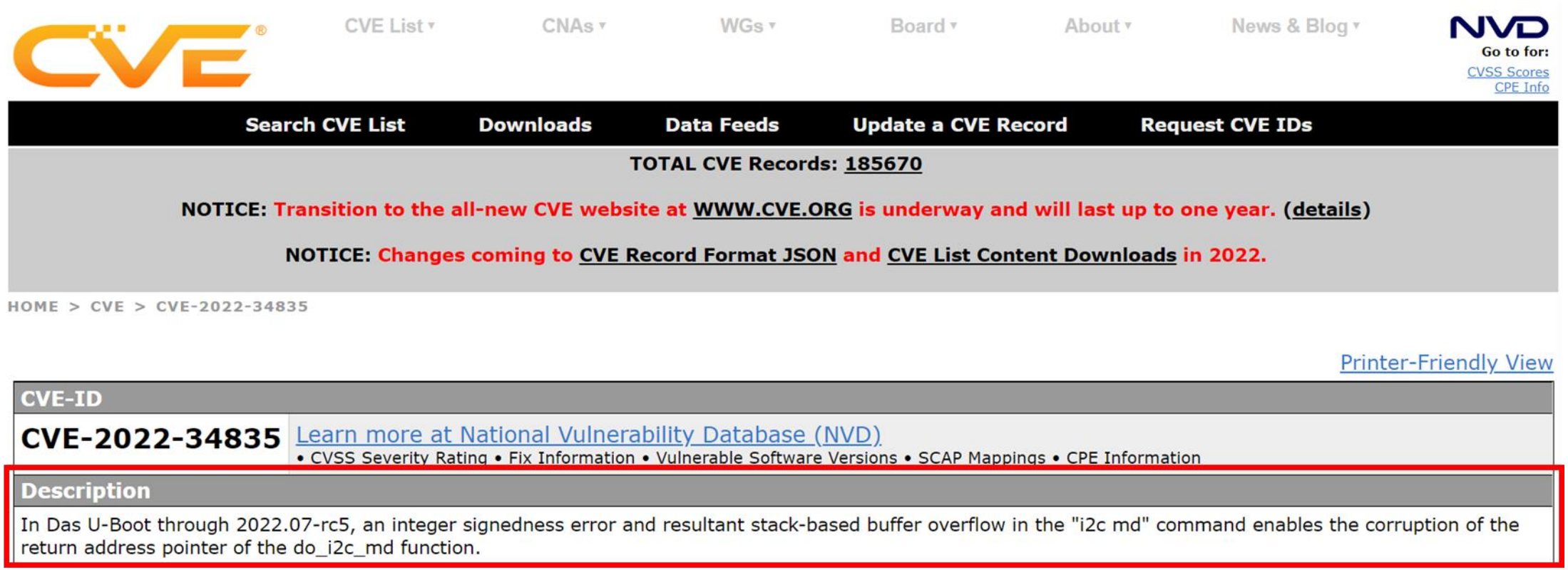


一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

インシデント対応の事例紹介

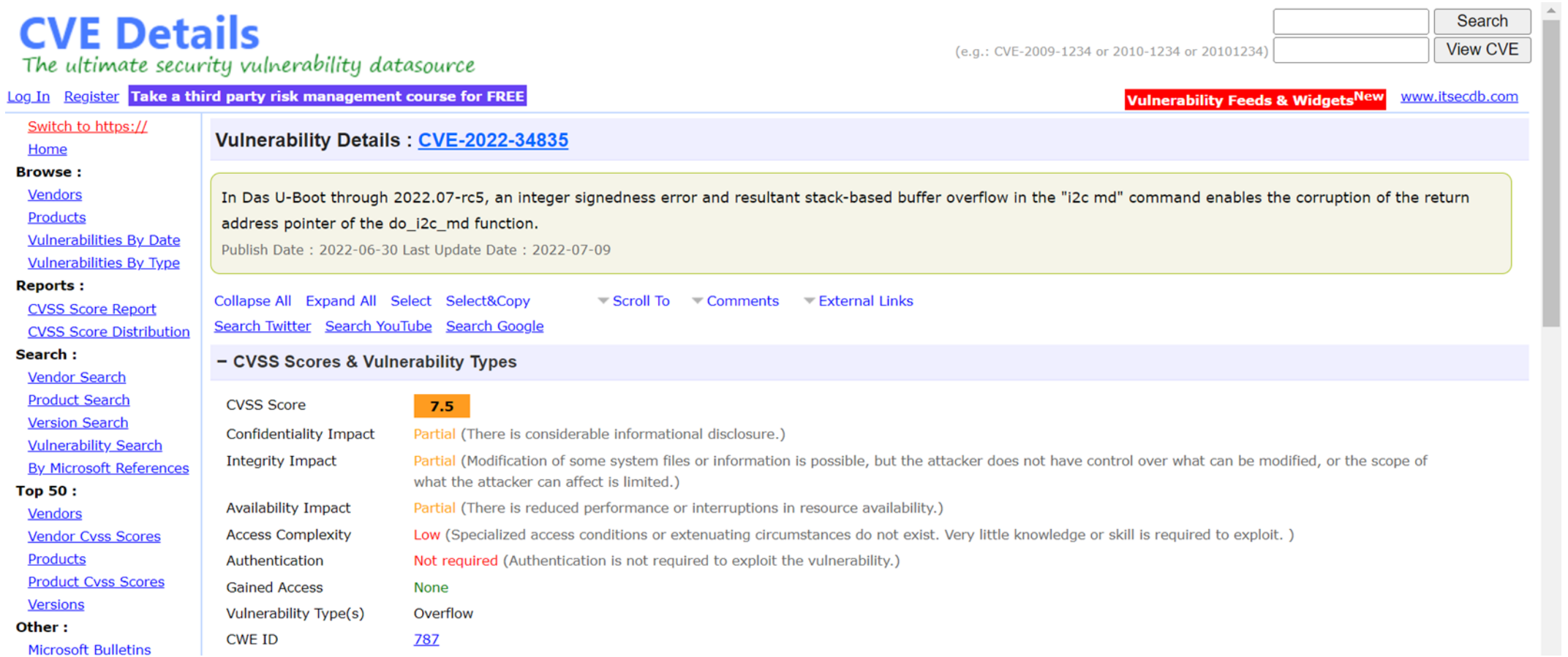
CVE-2022-34835の対応例

10. インシデント対応の事例紹介



Descriptionから、概要を判断する。

10. インシデント対応の事例紹介



CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search / View CVE

Log In Register **Take a third party risk management course for FREE**

Vulnerability Feeds & Widgets[New] www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins

Vulnerability Details : CVE-2022-34835

In Das U-Boot through 2022.07-rc5, an integer signedness error and resultant stack-based buffer overflow in the "i2c md" command enables the corruption of the return address pointer of the do_i2c_md function.

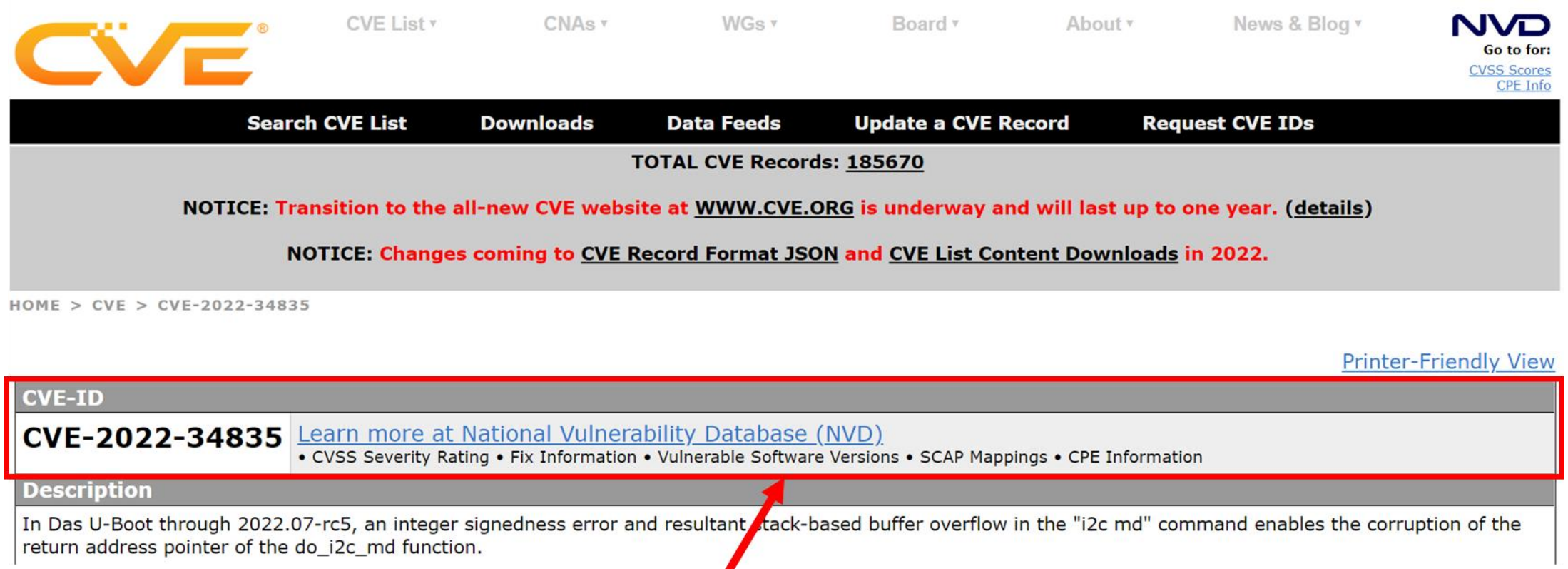
Publish Date : 2022-06-30 Last Update Date : 2022-07-09

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Overflow
CWE ID	787

10. インシデント対応の事例紹介



詳細は、NVDを利用する。

10. インシデント対応の事例紹介

■ CPE情報から、対象パッケージの確認

- 対象パッケージが開発製品に含まれるか調査

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:denx:u-boot:*:*:*:*:*:*:*:*	Up to (excluding)
Show Matching CPE(s)	2022.07
cpe:2.3:a:denx:u-boot:2022.07:rc1:*:*:*:*:*:*	
Show Matching CPE(s)	
cpe:2.3:a:denx:u-boot:2022.07:rc2:*:*:*:*:*:*	
Show Matching CPE(s)	
cpe:2.3:a:denx:u-boot:2022.07:rc3:*:*:*:*:*:*	
Show Matching CPE(s)	
cpe:2.3:a:denx:u-boot:2022.07:rc4:*:*:*:*:*:*	
Show Matching CPE(s)	
cpe:2.3:a:denx:u-boot:2022.07:rc5:*:*:*:*:*:*	
Show Matching CPE(s)	

10. インシデント対応の事例紹介

■ CVSSスコアで対策の緊急度を確認

Analysis Description

In Das U-Boot through 2022.07-rc5, an integer signedness error and resultant stack-based buffer overflow in the "i2c md" command enables the corruption of the return address pointer of the do_i2c_md function.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 9.8 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

10. インシデント対応の事例紹介

- VuIDBの情報からエクスプロイト価格なども対策可否判断に利用
  - 閲覧には、アカウント作成が必要

10. インシデント対応の事例紹介

■ 対策パッチの有無の調査

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://github.com/u-boot/u-boot/commit/8f8c04bf1ebbd2f72f1643e7ad9617dafa6e5409	Exploit Patch Third Party Advisory
https://lists.denx.de/pipermail/u-boot/2022-June/486113.html	Exploit Patch Vendor Advisory
https://source.denx.de/u-boot/u-boot/-/commit/8f8c04bf1ebbd2f72f1643e7ad9617dafa6e5409	Patch Vendor Advisory

10. インシデント対応の事例紹介

■ 対策パッチがない場合、CWE IDから推測

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-787	Out-of-bounds Write	NIST

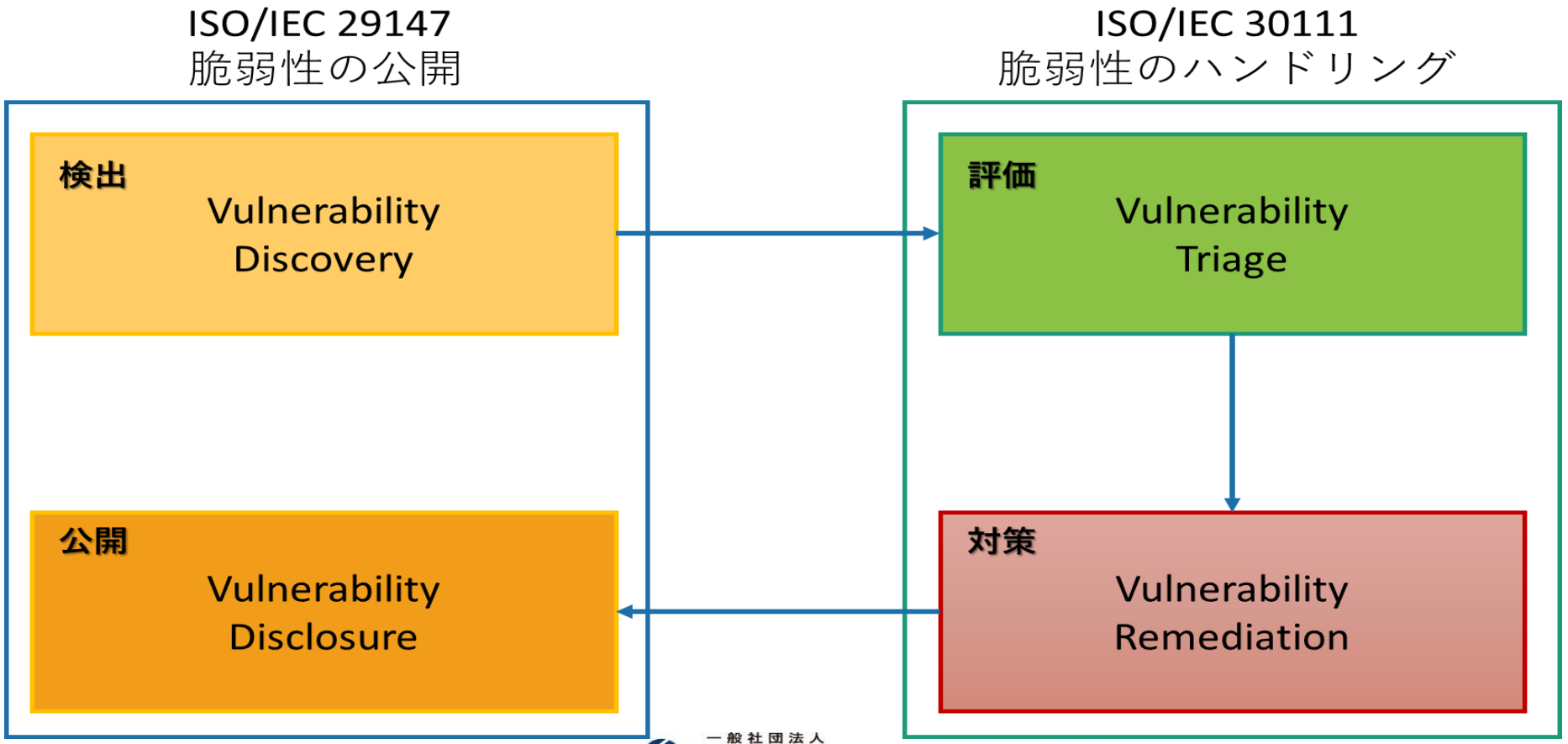
PSIRT活動

運用～廃棄までのサイバーセキュリティ対策

11. PSIRT活動

■ 脆弱性対応にあたっての国際規格

- ISO/IEC29147、ISO/IEC30111の活用



参考URL：https://www.ipa.go.jp/files/000037395.pdf

11. PSIRT活動

■ サービス、分野によってSIRTの種類がある。

- 各SIRTで「対象」「守るべきもの」が変わってくる。

xSIRT	設置部署	対象	守るべきもの	活動
CSIRT (Company SIRT)	ガバナンス部門 IT部門	全般	自社で取り扱う機密情報 個人情報	セキュリティ活動全般 各xSIRT活動の支援 組織間のハブ・ファシリテータ
PSIRT (Product SIRT)	製品開発部門 品質保証部門	製品	自社製品を利用する顧客の 安全・機密情報	製品開発ライフサイクルにおける 脆弱性リスクマネジメント
FSIRT (Factory SIRT)	生産管理部門	工場 生産ライン	生産ラインの安定稼働	サイバー攻撃から工場設備の保護 活動
DSIRT (Digital service SRIT) SSIRT (Service SRIT)	サービス開発部門 品質保証部門	サービス	自社サービスを利用する顧客の 安全・機密情報 自社サービスの継続的な提供	サービス開発ライフサイクルに おけるリスクマネジメント

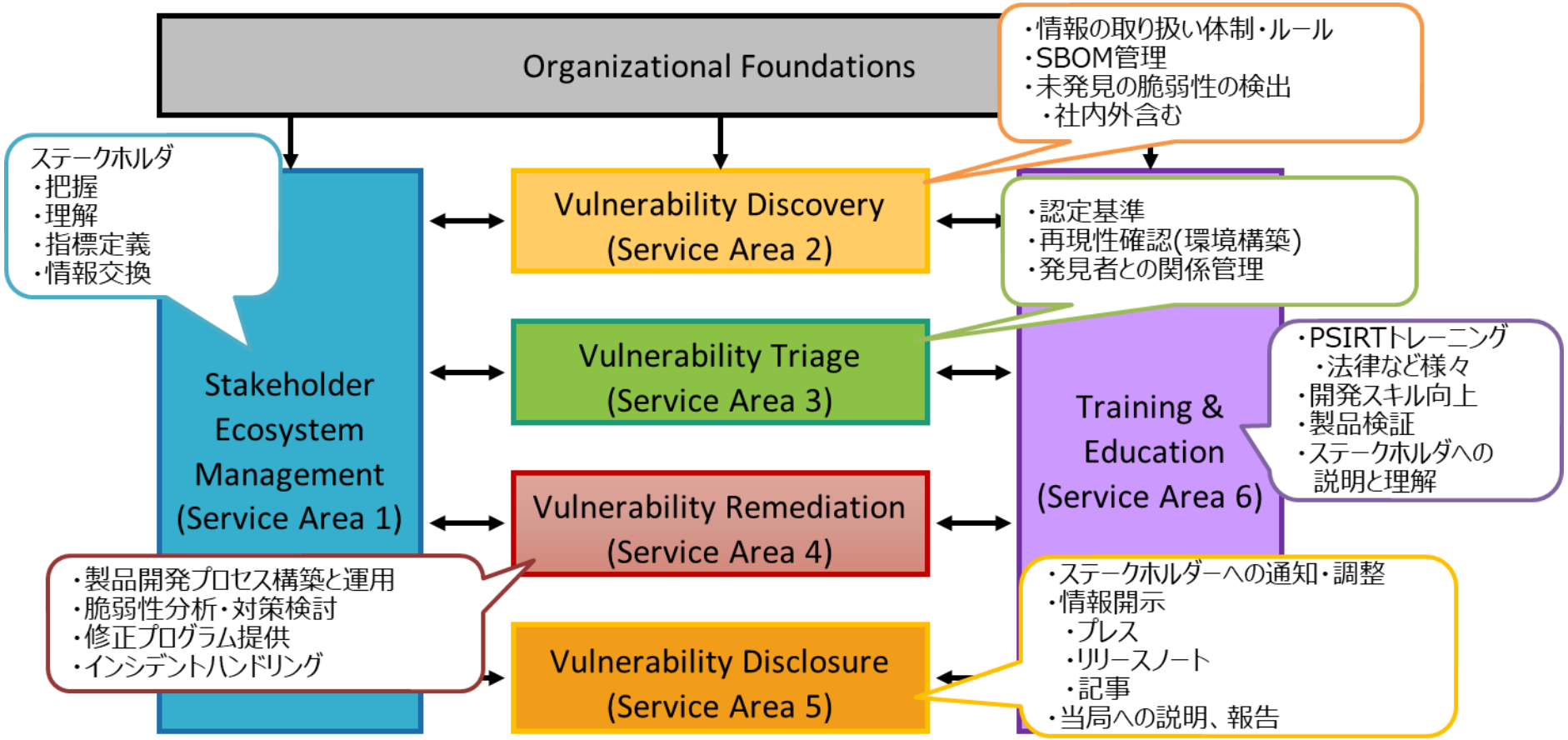
11. PSIRT活動

■ 例：CSIRTとPSIRTの比較

	CSIRT (Computer SIRT)	PSIRT (製品SIRT)
①インシデント 情報の検知	高確率でサイバー攻撃と判断できるので、判定プロセスが不要 → すぐに対処に移れる。	製品の不具合である可能性もあるため、サイバー攻撃による事象の判断が必要になる。
②対処方法	暫定的な対処が可能 → 機能制限、ネットワーク遮断など	機能によって暫定対処は可能 機能がミッションクリティカルな機能、安全に関わる機能場合は対処方法を検討する必要がある
③対外報告	報告フローによって報告	インシデントの重大性によって報告する内容やフローが変わる

11. PSIRT活動

■ 参考：PSIRT Services Framework Ver1.0



参考URL：PSIRT Services Framework Ver1.0

JASAのセキュリティ教材のご紹介

2023年１月以降の公開(予定)

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

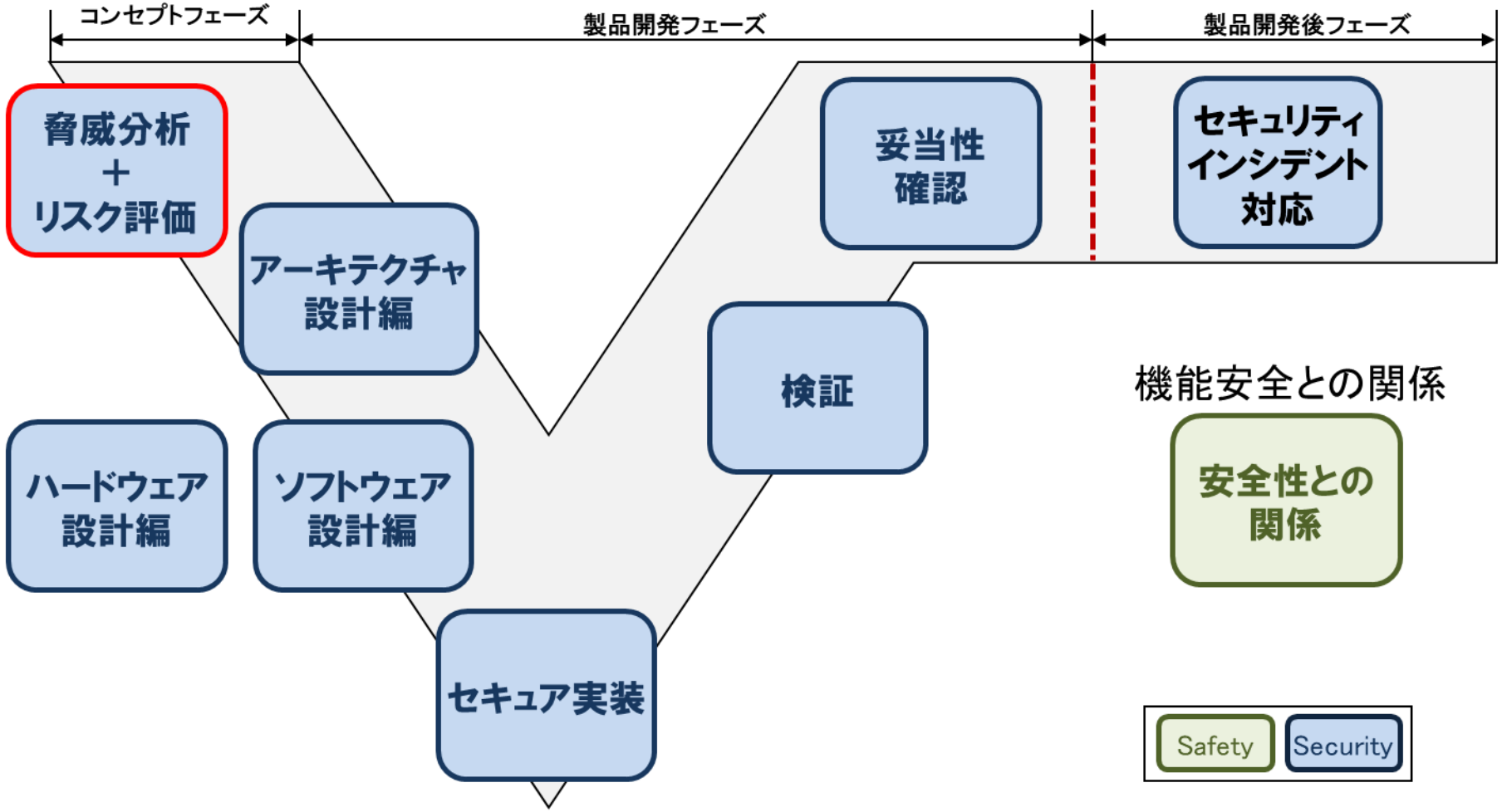
11. JASA セキュリティ教材のご紹介

事前に知っておくべき
知識体系を整理

要素技術
＋
専門用語

サイバーセキュリティ
動向

動向、法規
＋
規格、ガイド



機能安全との関係

安全性との
関係

Safety Security

開発済み

「製品ライフサイクルにおけるサイバーセキュリティ対応」

2022/11/16 発行

発行者　一般社団法人 組込みシステム技術協会
東京都 中央区 入船 1-5-11 弘報ビル5階
TEL: 03(6372)0211 FAX: 03(6372)0212
URL: https://www.jasa.or.jp/