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

JASA 安全性向上委員会
情報セキュリティWG

製品開発におけるセキュリティ

2017/11/15

Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

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

設計編

Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

1. 概要

□組込み開発現場におけるセキュリティの課題

1. 時間・コストが割けない。
2. 体系化された手順がない。
3. 情報は沢山あるが、どれが良いか判断できない。

□このような状況から、セキュリティ設計について、考えた内容と課題について共有します。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

2. 開発現場におけるセキュリティとは…

- セキュリティ評価、業務依頼内容から、開発現場でのセキュリティに対する現状は…

1. セキュリティ部分は、後付け
   - 開発ドメイン(金融など)によっては、優先されるが…
   - セキュリティ設計の作業自体が見積りされていない。
   - そもそもセキュリティを知らないので、触れたくないものになっている？
   - セキュアコーディングや脆弱性のチェックはされるが…
   - 顧客の要望は、変わってきているが…
     - 大抵、要望に答えるだけの方法論や体系がない…
     - 開発基準にセキュリティの項目があっても詳細がない…
2. システム特性、機能を考慮して設計されていない
   - 特定の製品を導入することがセキュリティ設計？
3. 複数のスキルセットを持つエンジニアがいない
   - セキュリティエンジニアの多くは、システム設計、脅威分析、セキュリティ設計など、複数のスキルセットを合わせて持っていない。
   - スキルセット自体が、特定製品、ソリューション導入、セキュリティ監視、脆弱性診断に偏っている。

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

3. 参考にしたもの

□ 参考書籍

- □ Microsoftの書籍
  - □ The Security Development Lifesycle

□ 参考文献

- □ IPA
  - □ IoT開発におけるセキュリティ設計の手引き
  - □ 情報セキュリティーの10大脅威総合編
    - □ https://www.ipa.go.jp/security/iot/iotguide.html
  - □ つながる世界の開発指針
    - □ https://www.ipa.go.jp/sec/reports/20160324.html
  - □ CC評価を理解する為の開発者向け説明会
    - □ https://www.ipa.go.jp/security/jisec/seminar/documents/cc_eval_20120625.pdf
- □ その他
  - □ OWASP Internet of Things(IoT) Project
    - □ https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
  - □ OTA IoT Trust Framework
    - □ https://otalliance.org/initiatives/internet-things

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

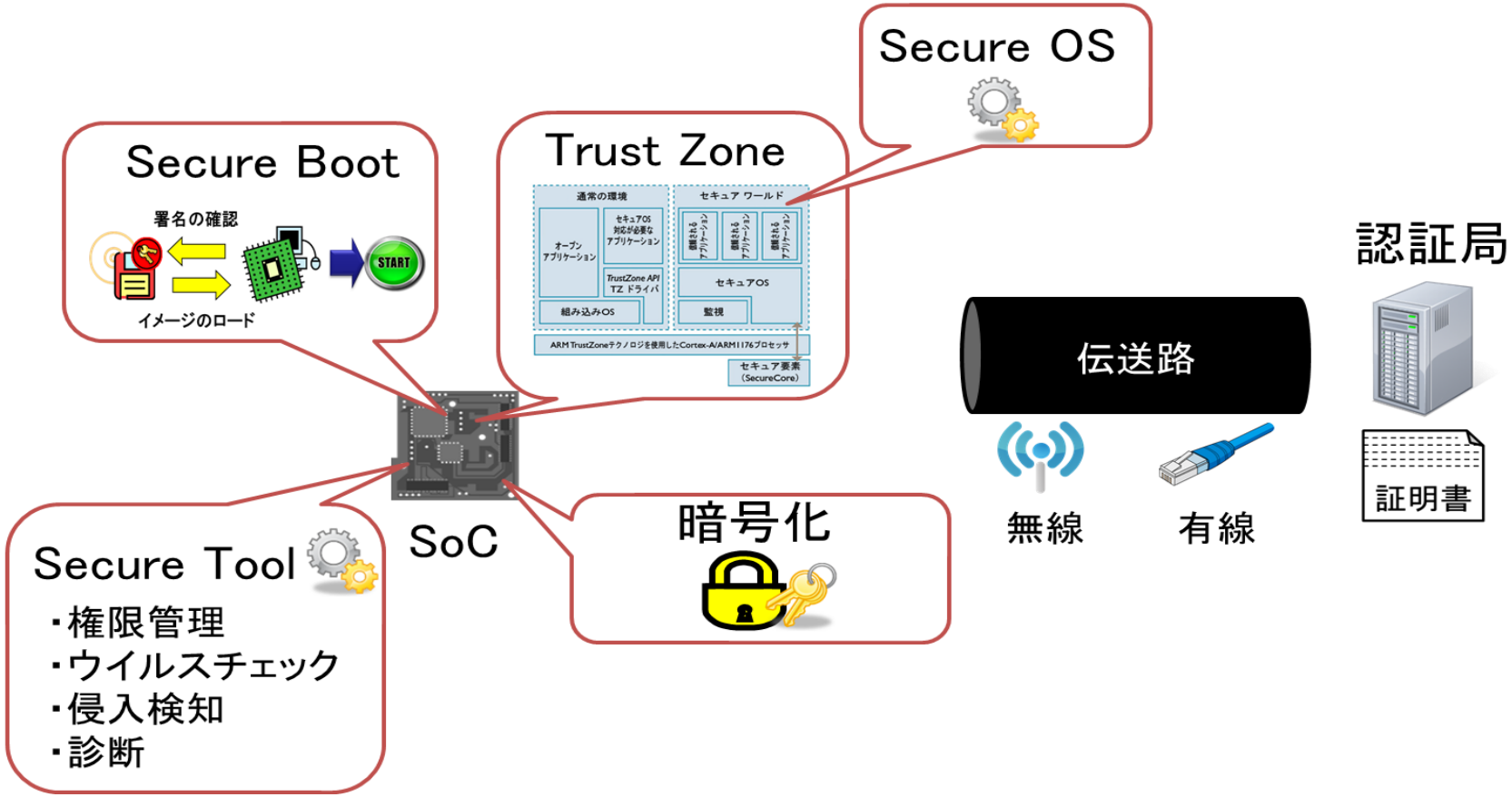
4. 参考にしたものを読んでみて…

- 参考書籍
  - 考え方や分析方法、キーワードを覚えるには良いが、そのまま使うのは難しい…
- 参考文献
  - ガイド文書に基づいて実施することは望ましいが…
    - セキュリティ設計業務の体系化まで手が回らない。
      - 設計の流れを検討するための参考にする。
  - 成果物のイメージを決めるために使えるか…
    - 何を検討し、何を対策していくか？の設計書のイメージに使う。
    - 記載されている内容を要素ごとに分けて整理するのに使う。
    - セキュリティ対策の評価方法に使う。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

5. 世の中の動向

- IoTのキーワードから、世の中でもセキュリティ製品が多く、組込みの中にも出回ってきた。

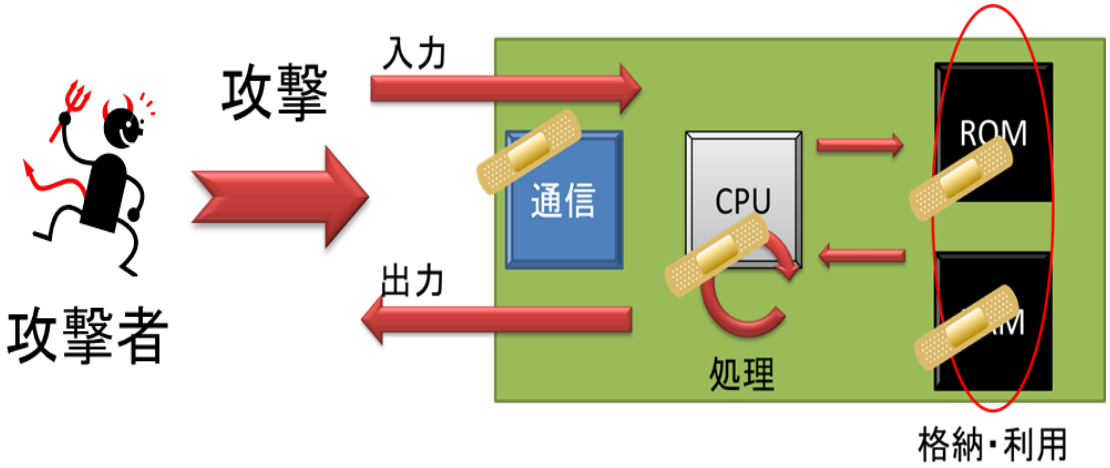


図参考：http://www.arm.com/ja/products/processors/technologies/trustzone.php

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

6. 世の中の動向を踏まえて…

- 製品・サービスは、いろいろあるが…
  - 利用するもの（手段）でしかないが…どう利用するか？
  - 良いところだけを聞いて、利用してしまうと…守れてるか心配？
    - 張りぼてで、穴だらけになりそう. . .
  - 利用するのは良いが、コストが…どの程度掛ければ良いか？



Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

7. 裁判での判決

- 「SQLインジェクション」に代表される攻撃によって、被害があった判例での判決で、経済産業省、IPAなどが注意喚起していた事を怠ったなど、重過失として理由となった事例が多くなってきている。

  - 参考1：
    - https://www.softic.or.jp/semi/2014/5_141113/rep.pdf
  - 参考2：
    - https://www.softic.or.jp/semi/2014/5_141113/op.pdf
  - 参考3：
    - https://www.softic.or.jp/semi/2014/5_141113/rep2.pdf

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

8. 調査まとめ

- いろいろ情報や製品やらと多種多様…
  - 本当に有効なのか？を確信するには…
- きちんと、セキュリティ設計（分析）をしよう！！
  - 明確になれば、安心できる。
- 判例もあるので、IPAからの情報発信には留意する！！

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

セキュリティ設計（分析）とは？

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

1. セキュリティ設計のときに意識しなくてはならないもの…

□そもそも、セキュリティ設計って何？

□簡単にまとめると、以下。

項番	意識しなければならないこと	考えなければならないこと
1	システムに対する脅威とは何か	システムってそもそも何？
		何が起きると脅威と言える？
		脅威の種類はどの程度？
2	脅威は対象システムの何処にあるのか？	そもそも対象システムは何を目的にしているか？
		情報の変換点は何処？
		情報の変換点に対して発生する処理は？
3	脅威はどの程度の影響があるか？	脅威に対する重み付けをする。 （すべての脅威に対処することはできないかも）
4	脅威へどのような対策をするか？	脅威対策方針の検討をする。 （対策方針を実装する手段は複数あるかも）
5	脅威対策の実装はどうするか？	実装手法/手段の選択 （自社で対応するか？製品を導入するか？）

脅威分析

セキュリティ設計

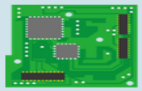
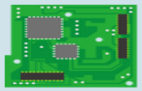
セキュリティ設計（広義）

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

□システムとは？どう定義するのか…

□一般的には、情報(データ)を入力→処理→出力する機能を持っているものと定義できる。

システムモデル

概念図	人 or 機器 	入力	処理	出力	人 or 機器 
機能 提供機能 提供機器		・入力デバイス ・伝送路	・プログラム ・OS ・ハードウェア	・出力デバイス ・伝送路	

情報(データ)の変換点

情報(データ)の変換点	入力		伝送	変換/処理	伝送	出力	
例	人 (利用者)	機器	LAN 専用バス	・CPU ・GPU ・FPGA	LAN 専用バス	機器	人 (利用者)

Confidential

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

ISO/IEC 27000の定義を再確認

特性名	内容	イメージ
機密性（Confidentiality）	ある資産へのアクセスを許可と許可されていないものを明確に区分し、許可された範囲内で動作（読込み・書込み・一覧表示・実行など）をできるようにする特性	見せたくない情報（データ）は見せないこと
完全性（Integrity）	あるデータが発生してから処理されるまでに行う工程（入力・編集・保存・読取り・削除など）で、欠落や重複，改ざんなどが発生せずデータの正当性・正確性・網羅性・一貫性を維持する特性	意図せずにかわっていないこと
可用性（Availability）	頻繁にシステムダウンや恒常的にレスポンスが遅い、1つの処理に何分も待たされたりなどの事象がなく、いつでも正常なサービスを提供できる状態を維持する特性	利用・使用したいときに使えること

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

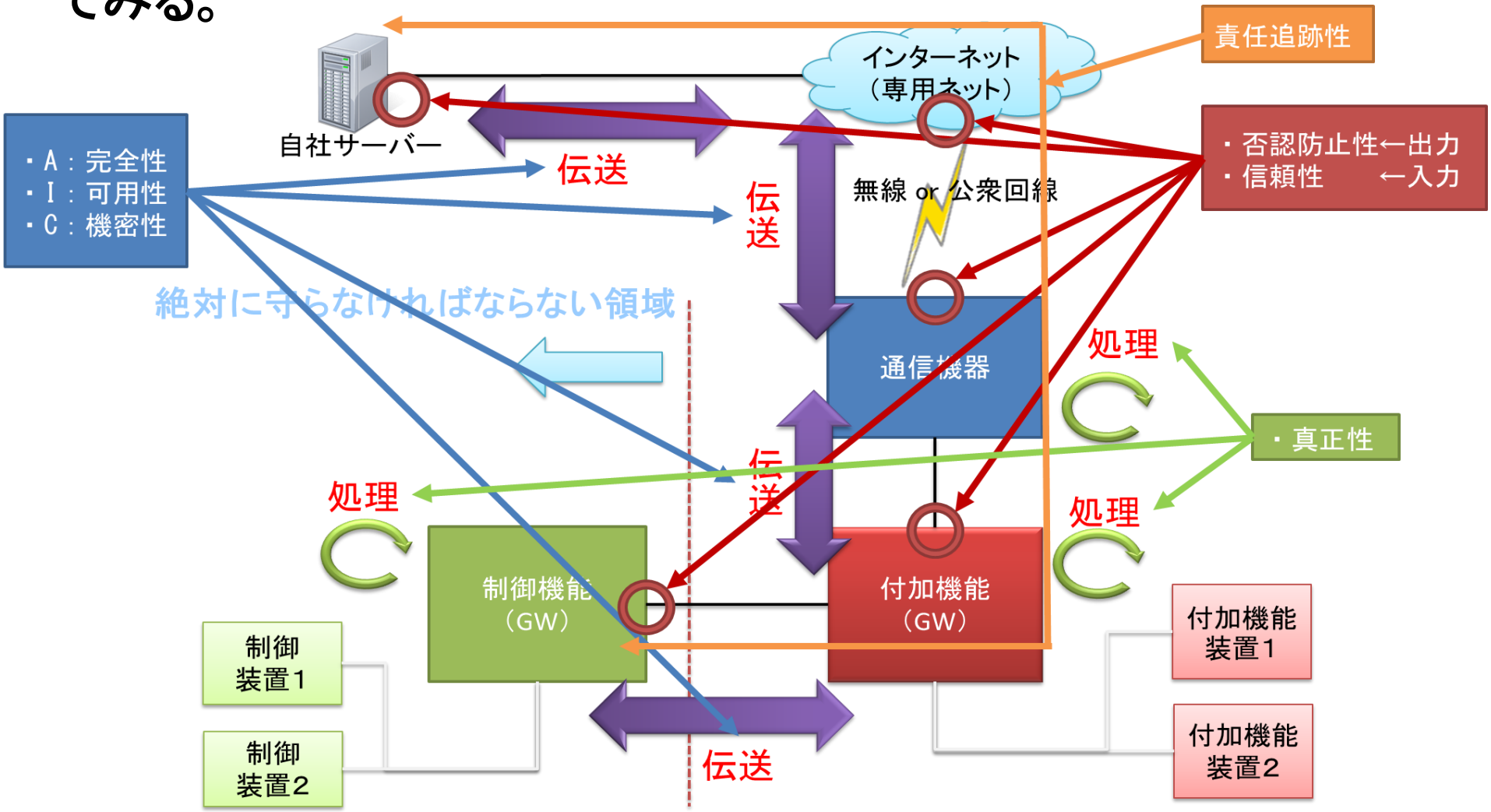
□ISO/IEC 27000の定義を再確認

特性名	内容	イメージ
真正性（authenticity）	プロセス、システム、データ及び操作者が、確実に認証・識別できる特性です。人間を対象とした場合には、権限のなりすましによる情報資産へのアクセスを防止する技術を利用します。	Aさん（入力物）が正しくAさん（入力物）であること。
責任追跡性（accountability）	操作者、プロセス、システムの動作内容を一意に追跡できることを確実にする特性です。入退館やシステム操作に対する証跡・ログを確実に取得する仕組みを策定します。	誰（処理）がやったか分かること。
否認防止（non-repudiation）	ある事象が発生した後で、否認されないように証明する特性です。ディジタル署名やタイムスタンプは否認防止に有効な技術です。	やった事（処理）を否定できないこと。
信頼性（reliability）	実行した操作や処理結果に矛盾が発生しないことを確実にする特性です。定期保守やテスト強化でバグを排除することで対策します。	依頼（入力）した事が正しい結果（出力）に処理されていること。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

4. 脅威ってどういうこと？

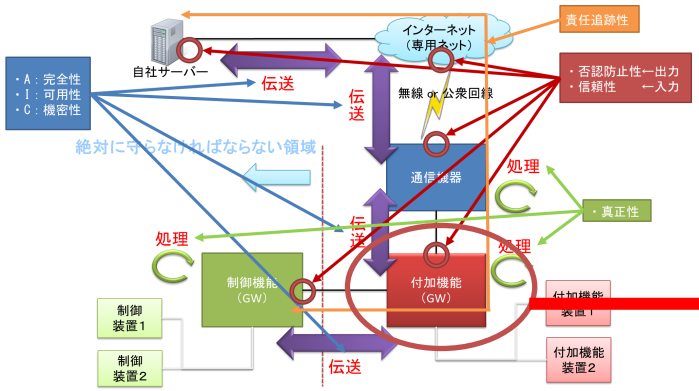
- 全体システムを実際に、ISO/IEC27000 情報セキュリティ要素と比べてみる。

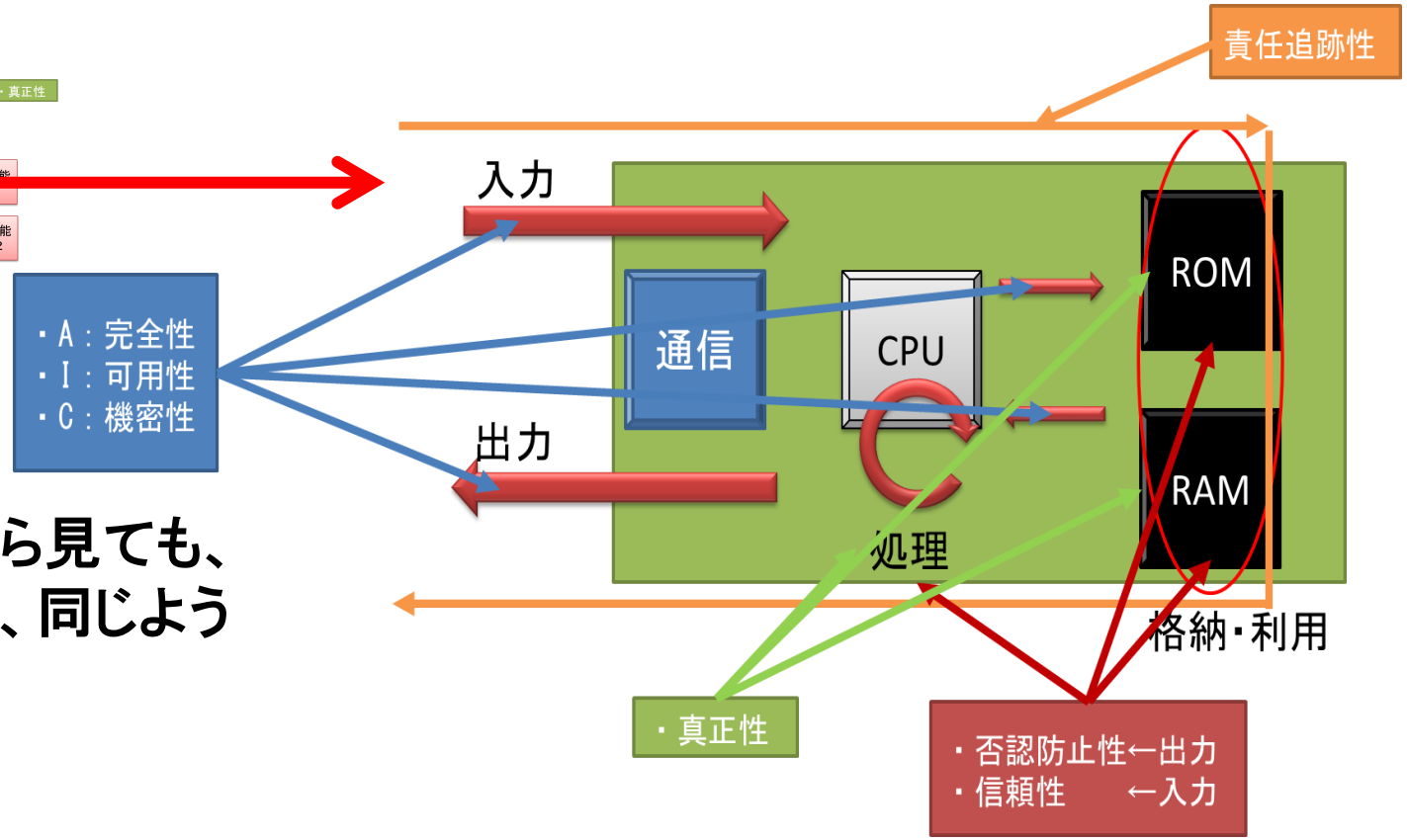


Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

5. 担当システム部分でも同じ事をやってみる。

□ 対象システムを元に検討してみる。





全体システム構成から見ても、自身の担当部分でも、同じような定義ができる。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

6. 脅威を定義しよう。

- そもそも、脅威って何だっけ？…定義してみる。
  - 脅威は、「情報（データ）が、入力→伝送→処理（変換）→出力」となる流れにおいて、ISO/IEC 27000に定義されているセキュリティ要素が、守れないこと。
  - 具体的な脅威はどんなことがあるか？検討してみる。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

6. 脅威を定義しよう。

□ISO/IEC 27000に則って、定義をしてみる。

項番	セキュリティ要素	脅威の概要	脅威例	考えられる攻撃シナリオ例
1	機密性（Confidentiality）	情報（データ）のやり取りが盗聴される。	盗聴など	対象機器が送受する情報（データ）が窃取され、機器の情報（データ）が盗まれ、新たな攻撃（不正操作など）に使われる。
2	完全性（Integrity）	情報（データ）のやり取りが改ざんされる。	改ざんなど	対象機器が送受する情報（データ）が改ざんされ、関連機器に正確な情報（データ）が伝えられなくなる。
3	可用性（Availability）	処理の提供が妨害される。	DoSなど	対象機器に大量のデータが送られ、対象機器が停止して、関連機器に処理が提供できなくなる。

Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

6. 脅威を定義しよう。

□ISO/IEC 27000に則って、定義をしてみる。

項番	セキュリティ要素	脅威の概要	脅威例	考えられる攻撃シナリオ
1	真正性（Authenticity）	受信者になりすまされる	関連機器のなりすまし	攻撃者が対象とする機器になりすますことで、関連機器の情報（データ）を盗聴したり、改ざんしたりする。
2	責任追跡性（Accountability）	情報・処理の結果が記録されない	追跡の防止	攻撃者が行ったことや、処理結果の記録が改ざん、削除されることで、不正な操作がされたことが突き止めることができなくなる。
3	否認防止（Non-repudiation）	送信者になりすまされる。	関連機器のなりすまし	攻撃者が対象とする機器になりすますことで、関連機器の情報（データ）を盗聴したり、改ざんしたりする。
4	信頼性（reliability）	意図しない処理が実行される。	不正操作	機器に侵入し、意図しない処理を実行することで、関連機器の情報（データ）を改ざん、窃取したり、システムダウンを起こすなどの処理を実行する。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

7. 脅威からの分析

- なるほど、定義するのは簡単にできる。
  - ざっくり定義はできるけど、何か足りないような気がする…
  - 脅威を定義したが、本当に攻撃される恐れがあるのかな…
  - 組込み機器なんだけど、エンタープライズみたいな攻撃が想定されるのかな…
  - そもそも、脅威を考えるときに、エンタープライズ系の情報を真似ていて良いのかな…
- などなど…疑問が出てくる。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

7. 脅威からの分析

- 脅威はあることは、理解できた。何故そもそも、攻撃対象となるのか？を更に分析してみる。
  - ISO/IEC 27000の定義を使って分析して見た結果、解ったこととしては、攻撃者は、情報(データ)に着目しているように見える。
  - そもそも、攻撃目的がはっきりしていないことには、何を守るか？が見えないような気がする。
  - そもそも、情報(データ)に資産価値があるのか？が見えていないのに、脅威に対する脆弱性を対策しなければならないとは思えないような気がする。

- 重要なのは、システム/対象機器で扱う情報(データ)がどんな種類や資産価値を明確にすることが重要！！

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

7. 脅威からの分析

- CC（Common Criteria：コモンクライテリア）からの分析
  - ISO/IEC 15408のベースとなった共通基準

- CC Part 1からすると…（要約）
  - 「脅威は、資産に対する脅威エージェントの有害なアクションから構成される。」
  - 「有害なアクションとは、資産価値を生じる資産の1つ以上の特性に影響を与える。」（特性：CIA）
  - 「脅威エージェントの例には、ハッカー、利用者、コンピュータのプロセスや、事故などが想定される。」

- 脅威を考える場合は、「誰が」、「どの資産に」「どんな有害なアクションをする？」を明記することも必要になってくる！！

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

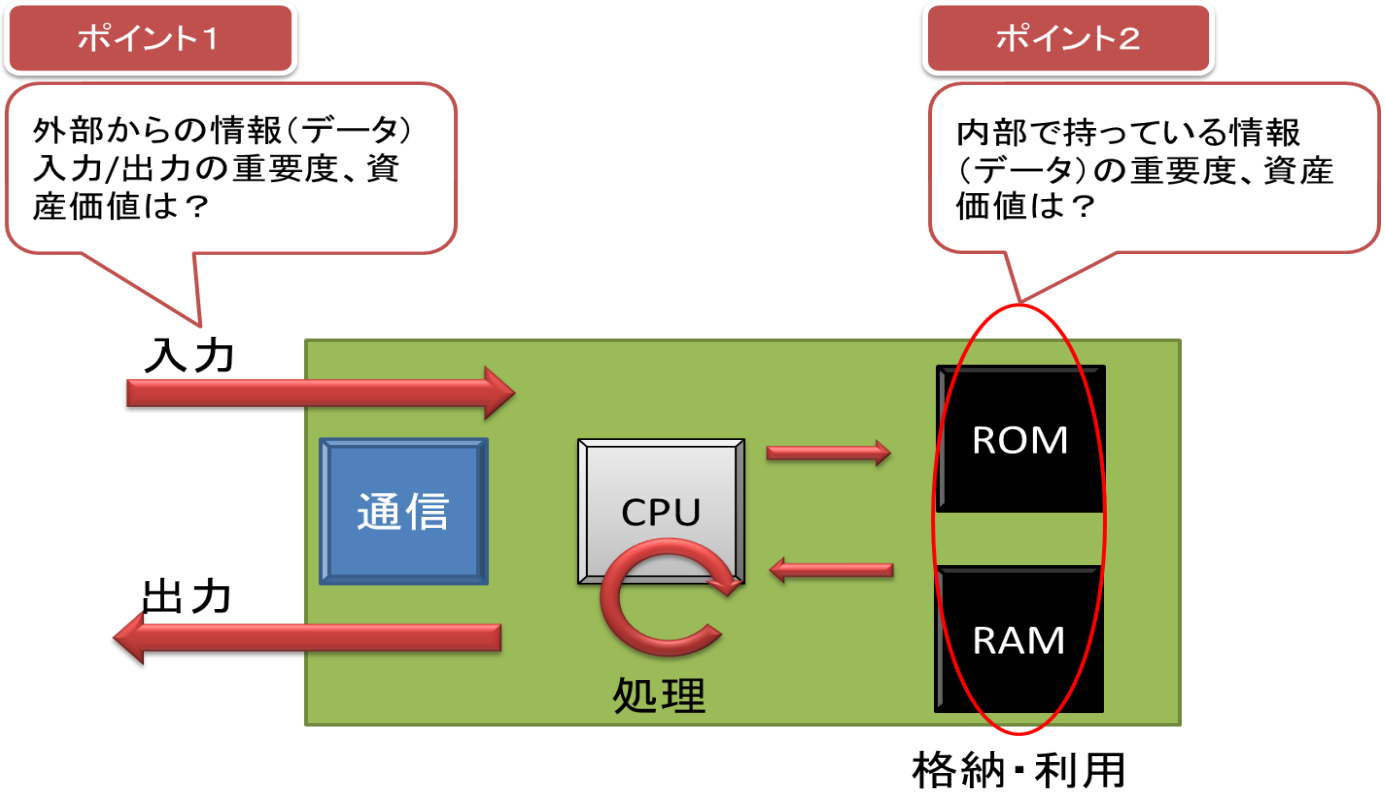
□ 脅威目的を分類して、目的を把握しよう。

攻撃手法	主な目的、実行可能な内容など									
	侵入のための情報収集	機密情報の取得	不正なサイトへの誘導	ネットワークへの不正接続	ホストへの侵入	管理者権限の奪取	セッションの乗っ取り	不正な処理・機能の実行	システムやデータの破壊・改ざん	サービス妨害・迷惑行為
アドレススキャン（pingスイープ）	○									
ポートスキャン	○									
スタックフィンガープリンディング	○									
パケット盗聴	○	○								
DNSサーバーからの情報収集（不正なゾーン転送要求）	○									
ソーシャルエンジニアリング	○	○								
フィッシング（Phishing）		○	○							
DNSキャッシュポイズニング攻撃		○	○				○			
ウォードドライビング（無線LANへの不正接続）				○						
パスワードクラック				○	○	○				
セッションハイジャック		○		○	○		○			
ARPスプーフィング				○			○			
セッションフィクセーション		○		○	○		○			
バッファオーバーフロー（BOF）攻撃		○			○	○		○	○	○
クロスサイトスクリプティング（XSS）		○	○				○	○	○	
SQLインジェクション		○	○					○	○	○
OSコマンドインジェクション		○			○	○		○	○	○
HTTPヘッダインジェクション		○	○				○	○	○	
メールヘッダインジェクション			○					○		
ディレクトリトラバーサル攻撃		○								
クロスリクエストフォージェリ（CSRF）							○	○		○
DoS攻撃									○	○
スパムメール			○							○
マルウェア（ウィルス、ワーム、ランサムウェア、ボットなど）	○	○	○	○	○	○	○	○	○	○
クリックジャッキング攻撃			○					○		
標的型攻撃		○	○					○		
SEOポイズニング			○					○		

Confidential

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

- システム/対象機器で取り扱う情報(データ)の重要度、資産価値を分析し、本当に脅威が存在するのか？を整理して、脆弱性の対策する。



Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

7. 脅威からの分析

- など、気をつけるべきものを明確にしていく作業が必要。

- 分析には、適切な手法を適用して、明確化していくことが必要になってくる。
  - 代表例
    - STRIDE
    - Attack Tree
    - FT法+5W法
    - STAMP/STAP-SEC

  - 適用しやすそうな手法と記述を使って、明確にしていくことが必要です。
  - 専門家や、IPAなどの情報を使っていくことをお勧めします。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

8. 組込み機器で考えなければならいこと

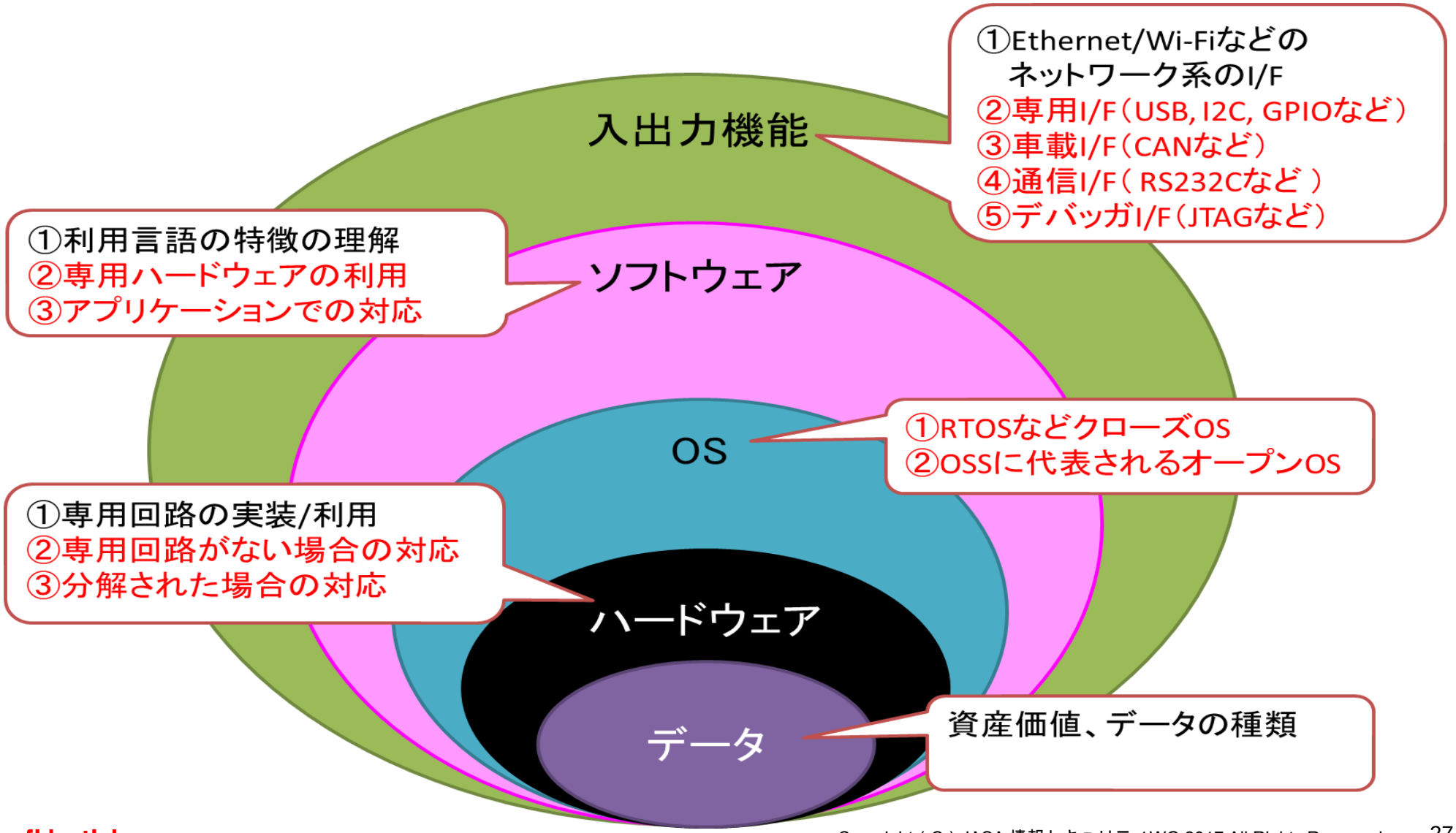
- 一般的に語られている事柄は、対象がネットワークと繋がった場合の事柄が多い。（IoTなどネットワークとの融合など）

  - ネットワークを利用し、製品価値を上げるためのサービスを提供する流れはある。
    - エンタープライズでの経験値を活用して、対策検討する部分

  - しかし、組込み機器特有となると、ネットワークを利用していないものもあるので、ネットワーク意外の部分も対象とする必要があるのではないか？と思われる。
    - 一体どうやって考えるのか…

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

□製品機器を概念的に考える。

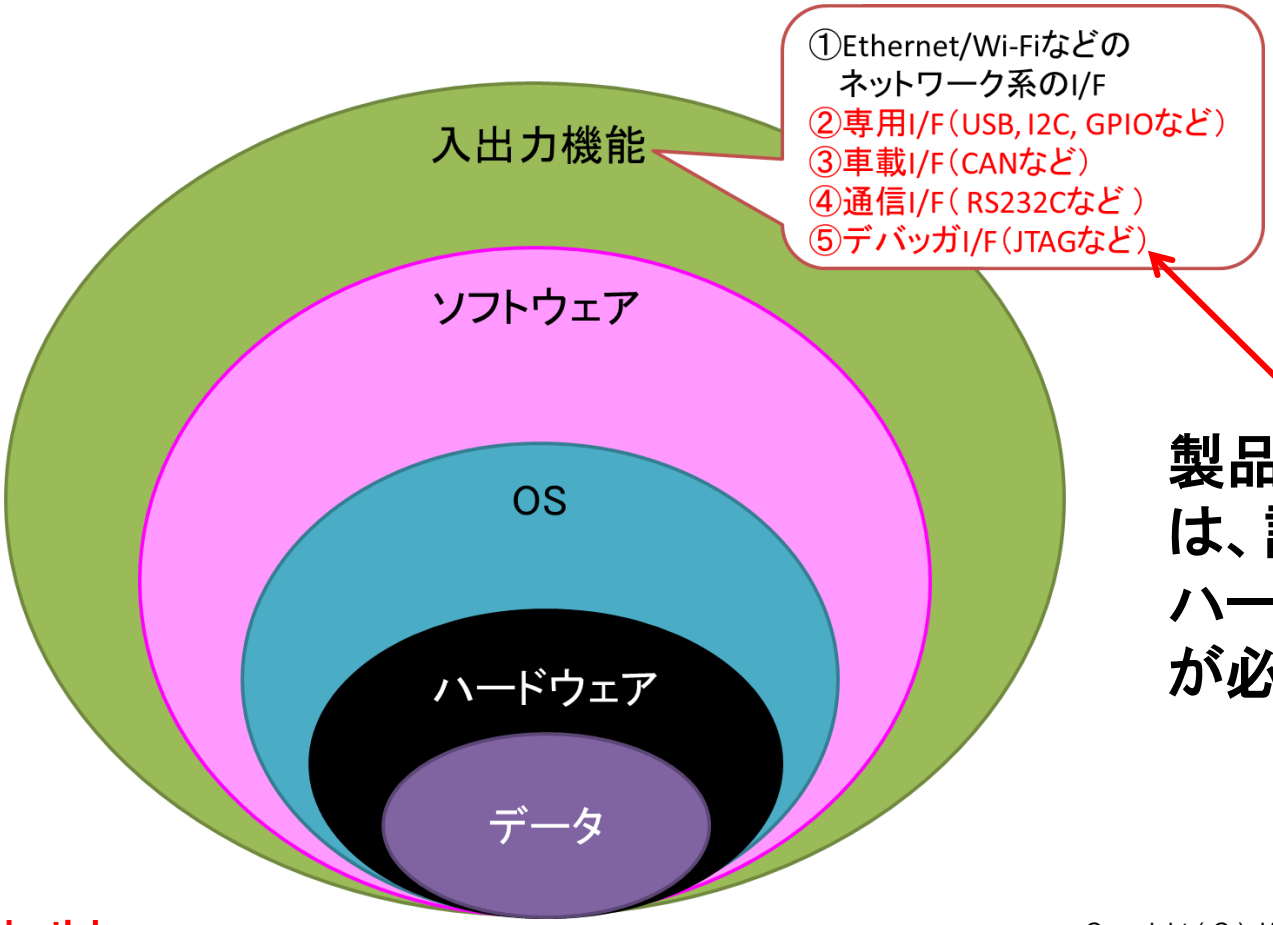


Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

□入出力機能

□機器に侵入できるI/Fがある点。侵入や情報(データ)を窃取される恐れがある。



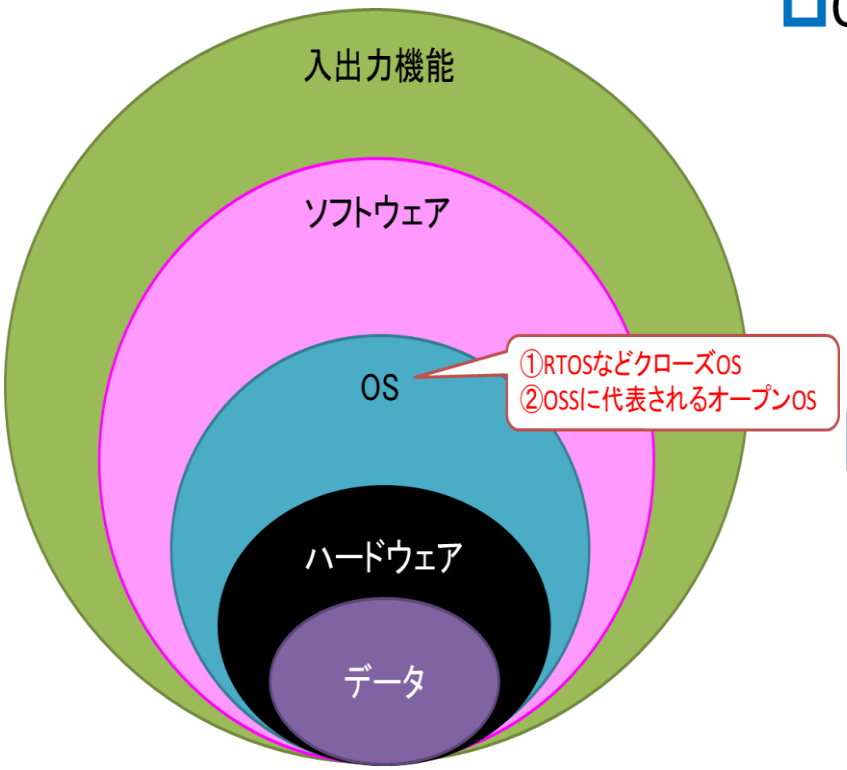
製品上のリスクとなる部分は、設計時に抑えること。ハードウェア技術者との協力が必要。

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

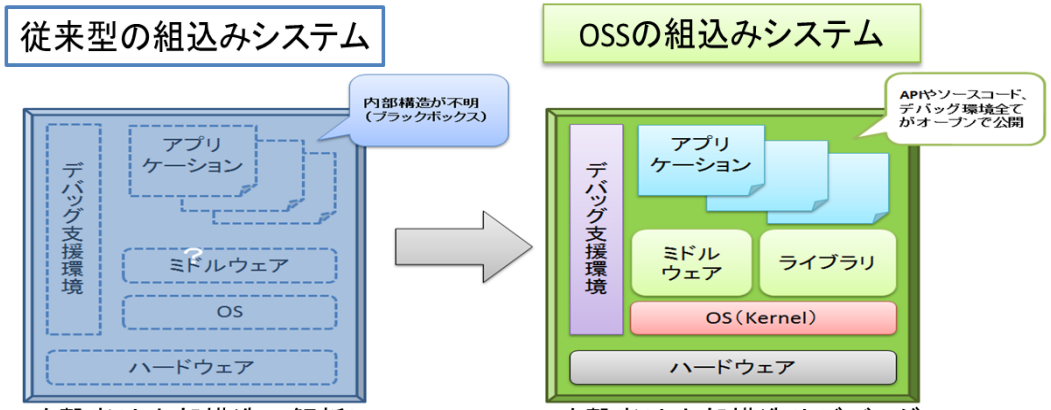
8. 組込み機器で考えなければならいこと

□OS部分

- □専用OS/オープンOSが使われる。専用OSの場合は、OSベンダーの協力が必須。



- □OSSを採用するデメリット
  - □広く公開されているOSSを採用すると開発が簡易化するが、ハッキングなど攻撃を受けるリスクがある。
    - □内部構造は容易に推測し易い。
    - □設計情報・思想ソースコードから推測し易い。
    - □デバッグ環境が簡単に利用できる。



攻撃者は内部構造の解析に時間が掛かる

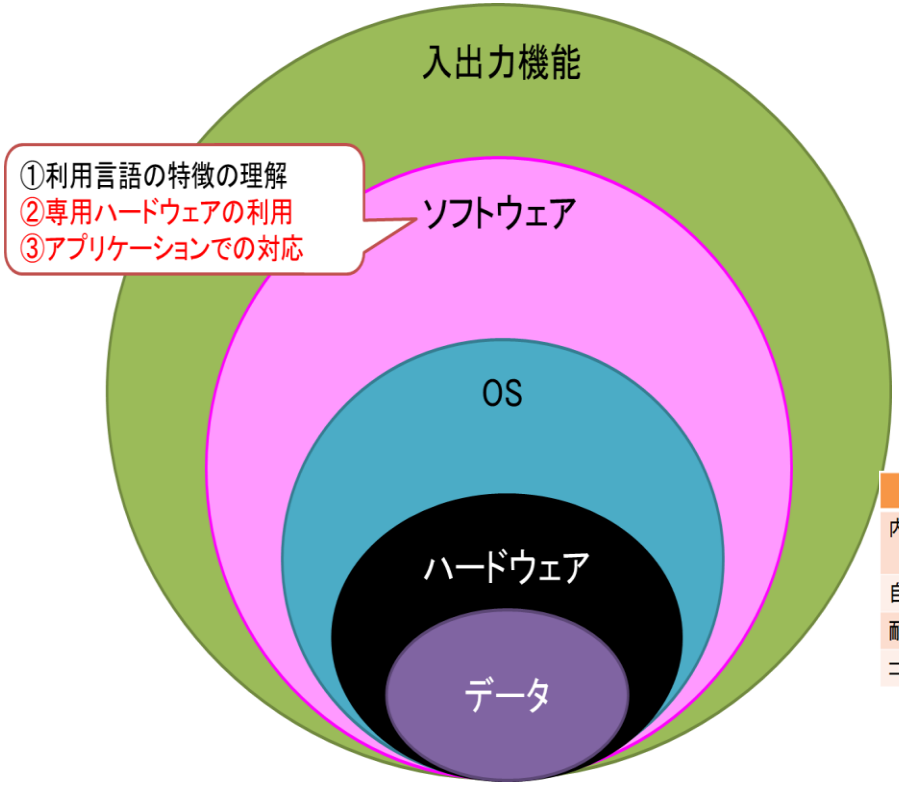
攻撃者は内部構造やデバッグ方法を知った上で攻撃可能

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

8. 組込み機器で考えなければならいこと

□ソフトウェア部分

- □利用言語の特徴を抑える必要がある。
- □ハードウェア機能/システム構成によって対策が異なってくる。



□対策（防御）の分類 例

- □セキュリティ対策の基本は、機器側で各種アルゴリズム、暗号鍵を解析されないようにすること。仮に解析されても被害を最小限にすること。
  - □以下にポイントを示す。

各種アルゴリズムや暗号鍵が解析されないようにする

	ソフトウェア	ハードウェア
内容	ソフトウェアロジックを工夫して守る	セキュリティ支援機構を利用して守る
自由度	○	×
耐タンパ性	×	○
コスト	○	×

各種アルゴリズムや暗号鍵が漏れても被害を最小限にする

	機器	サーバ
内容	機器のストレージを主として暗号鍵を持つ。	サーバ側のストレージを主として暗号鍵を持つ。
メリット	システム構築が容易	秘密が漏洩した場合の被害が少ない
デメリット	漏洩した場合の被害が大きい	運用コストが大きい

- □機器側のハードウェア支援機構を使ってサーバ側のストレージを主とする方が堅牢製は高いがコストも高くなる。

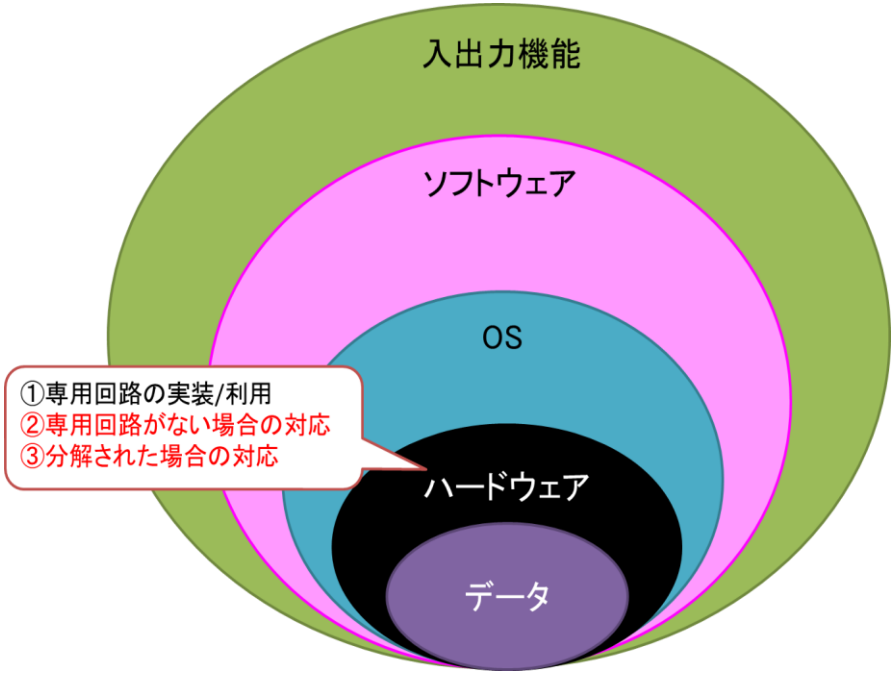
Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

8. 組込み機器で考えなければならいこと

□ハードウェア部分

- □資産価値を持っている情報(データ)が入っている部分。特に分解された場合の対応などを考えておく、必要がある。



フラッシュメモリーは「電線の直結」でハッキングし、情報を抜き取れる——米研究グループが発見

デジタルデヴァイスに搭載されたフラッシュメモリーのデータを簡単にハッキングする手法を、研究者グループが発見した。必要なものは5本の電線とSDカードリーダー、はんだ付けの技術だけ。その具体的な手法と、メーカーが講じるべき対策とは。

TEXT BY LILY HAY NEWMAN
TRANSLATION BY TAKU SATO/GALILEO

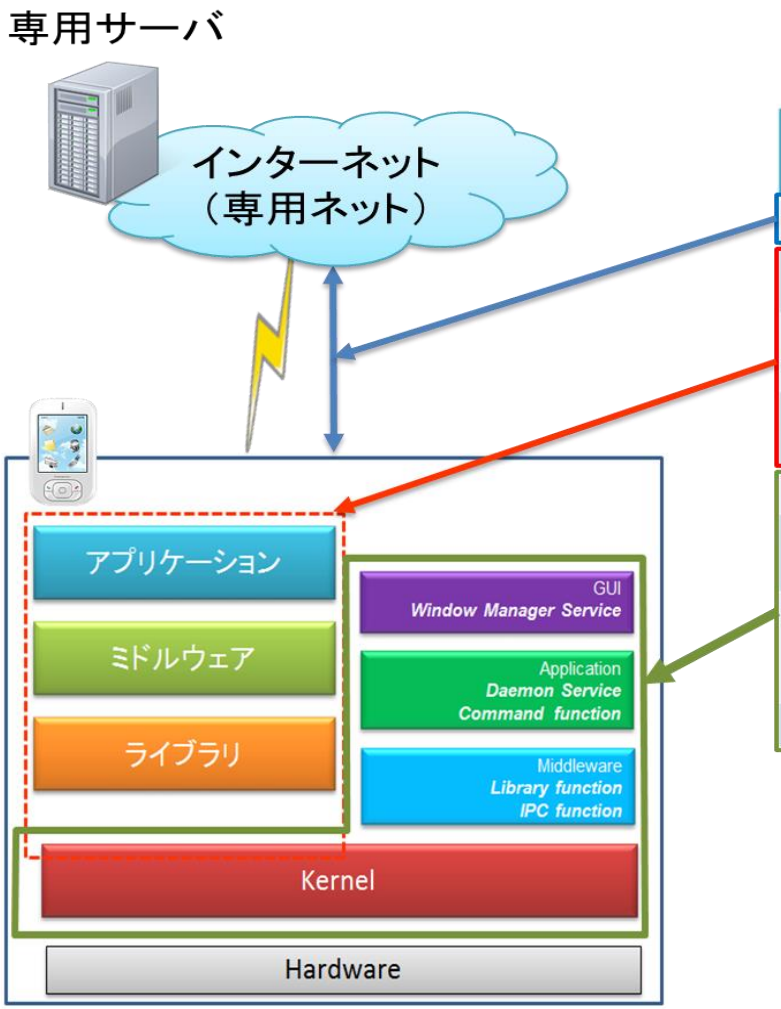
WIRED(US)

ツイート シェア G+ B!ブックマーク 13

出展協力:https://wired.jp/2017/09/30/sd-card-hack/
https://www.exploitee.rs/
https://www.defcon.org/

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

□通信端末の例



対策	説明	対策者	
		機器側	サーバ側
通信の暗号化	独自暗号でサーバと通信	アプリ	アプリ
デバッガ検知	デバッガを検知すると動作をとめる	ドライバ/アプリ	–
アプリケーション暗号化	インストールした以外の機器で動作していることを検知すると動作を止める	アプリ	–
暗号ロジックと暗号鍵の頻繁な変更	攻撃者に対して解析に十分な時間を与えない	アプリ	アプリ
パッチの迅速な適用	特権に昇格できるような脆弱性を塞ぐ	全般	–
Root化の検知	Root化を検知するとシステムロックをかける	全般	–
JTAGの無効化	秘密鍵を知らないとJTAGを利用できなくする。若しくは、JTAGを物理的に使えなくする	全般（ハード）	–
ストレージの暗号化	別の機器につないでも解析できない	全般	–

Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

8. 組込み機器で考えなければならいこと

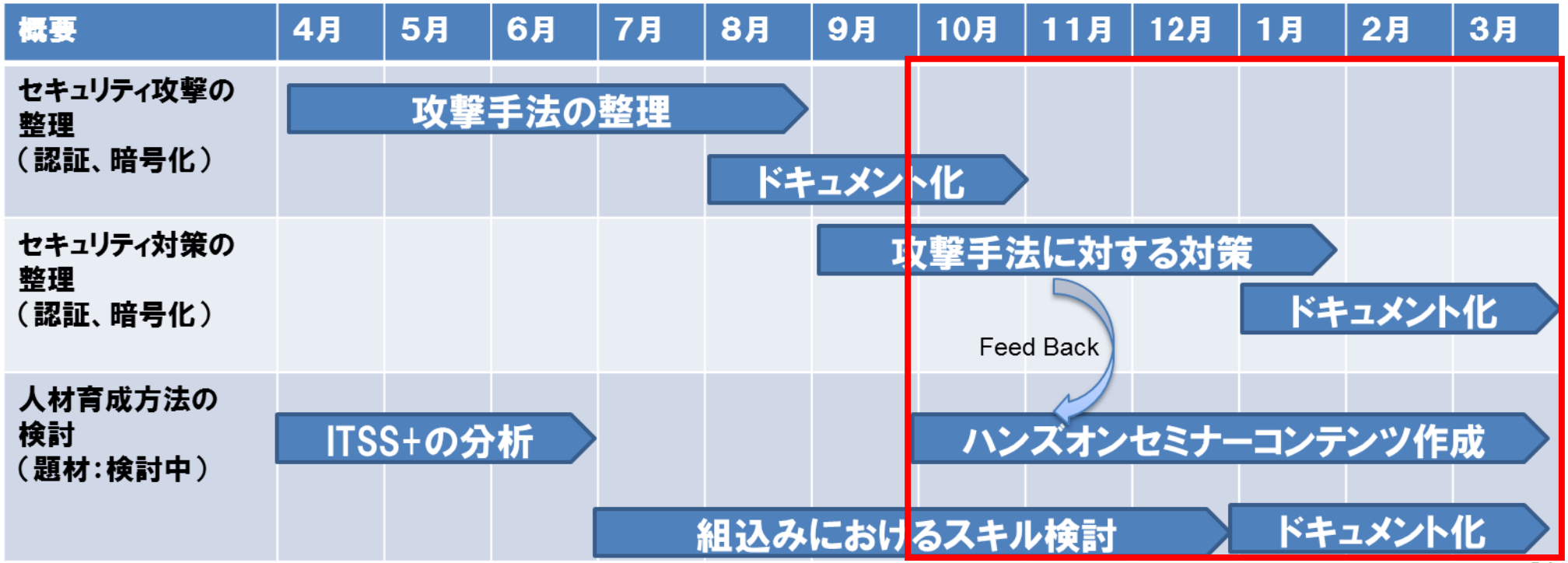
- 実装時は、脆弱性を作り込まないため、ルールを作っておくことが大切です。
  - IPA殿が展開している「セキュア・プログラミング講座」を参考にしたコーディング、レビュールールなどの定義をする。
  - 参考出展：
    https://www.ipa.go.jp/security/awareness/vendor/programmingv2/cc01.html
- ルール化することで、脆弱性がどのように作り込まれるか？の参考にもなります。

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

9. まとめ

□JASA 情報セキュリティWGの取り組み

- □17年度の取り組みは、実例や体験をメインに活動を実施中
- □組込み技術者に参考にできる資料を纏め、展開予定
- □ハンズオンは、都立産業技術研究所様と協力して対応予定
- □組織のセキュリティは、別途協議しながら推進中



Confidential

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

9. まとめ

- まとめ
  - セキュリティには、多くの情報と設計時の分析・検討作業に多く時間を費やす必要がある。
  - 脅威があるからと言って、安易な対策を採るのではなく、脅威分析をする。
  - 扱っている情報(データ)の価値を知ろう。知って、無駄な対策をしないようにする。
  - 組込みの場合、システム構成やハードウェア構成によっての対策が変わってくる。
  - ハードウェア技術者にも意識させないといけない。
  - 利用ソフトウェアが自社以外のものであったら、セキュリティ責任の範囲を明確にする。
- などと多くの課題があるので、みなさんからの意見・要望をお待ちしています。

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

9. まとめ

- セキュリティは、日々の確認からです。
- 脅威は、身近に存在しています。人が最も脅威かもしれません。

- 現状把握をする事が大切です。

- **まずは開発製品の自己診断を実施しましょう！！**

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

A. 情報セキュリティWGについて

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

- 産業技術研究センター（産技研）・組込みシステム協会（JASA）での共同運営 2015年4月再発足
  - WG 指針 “中小組織の情報セキュリティ能力向上”、“組込み開発におけるセキュリティ能力向上”
    - 情報セキュリティに関する事故事例の収集、対策調査
      - IPA様との共同調査
    - ツール・マニュアルの開発・普及
      - セキュリティ監査ツール：CMSiS
      - 脆弱性診断ツール（都技研様）
      - 製品のSecurity検討手引きマニュアル
    - 製品開発におけるセキュリティ検討
      - 分析手法の研究

Copyright（C）JASA 情報セキュリティWG 2017 All Rights Reserved.

A. 情報セキュリティWGについて

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

- 会員資格は、指針に賛同頂ければ、参加可能です。
  - 会費無料
  - 現在会員20社、30名程度
    - 常時参加者は、10名程度
  - 開催日時：月1回 原則第二木曜日 15:00～17:00
  - 開催場所：都立産業技術センター 2階会議室
- 情報セキュリティに関する相談には、何でも応じます。疑問・調査事項あれば、以下のMLに投稿ください。
  - 情報セキュリティWG ML： jesec-wg@jasa.or.jp

Copyright (C) JASA 情報セキュリティWG 2017 All Rights Reserved.

END