Panasonic

2018年1月23日

IoTセキュリティ
～その技術体系と実践～

パナソニック株式会社

全社CTO室

梶本 一夫

Panasonic

パナソニックの
Internet of Things取組み事例

技術10年ビジョン　－　IoT/ロボティクス領域　－

人工知能、センシング、UI/UXの技術を深化、出口戦略に基づき顧客価値提供

AI ロボティクス家電

家事からの解放
- くらしデータ解析
- 感情推定
- レコメンデーション
- 自動清掃/収納

店舗・接客ソリューション

接客品質の向上
- 多言語音声翻訳
- 対話
- 行動予測
- 自動棚卸／補充

自動運転・コミュータ

事故・渋滞ゼロ
- 障害物検知
- 外界認識
- 行動計画
- 人状態認識

次世代物流・搬送

労働不足の解消
- 対象物認識
- 不定形ピッキング
- 人協調作業
- 自律移動

出典　http://www.panasonic.com/jp/corporate/technology-design/10years-vision.html

Panasonic

IoTセーフティ＆セキュリティでの新たな懸念

WebからIoTへの移行
⇒情報漏洩から直接的に生命・財産が侵されるリスクへ
（火事、健康被害、盗難、・・・）

垂直統合型から自動車と住宅連携など水平分業・組合せの多様化
⇒一社だけではセーフティ＆セキュリティが保証できない世界へ

B2CからB2B2C（ODM）の多用（サプライチェーンの多様化）
⇒進入経路の多種多様化（中国内陸部メーカでのウィルス混入等）

OSSの主流化、SoCの固定化
⇒お客様を限定しないB2C商品の改造手法の流通の恐れ

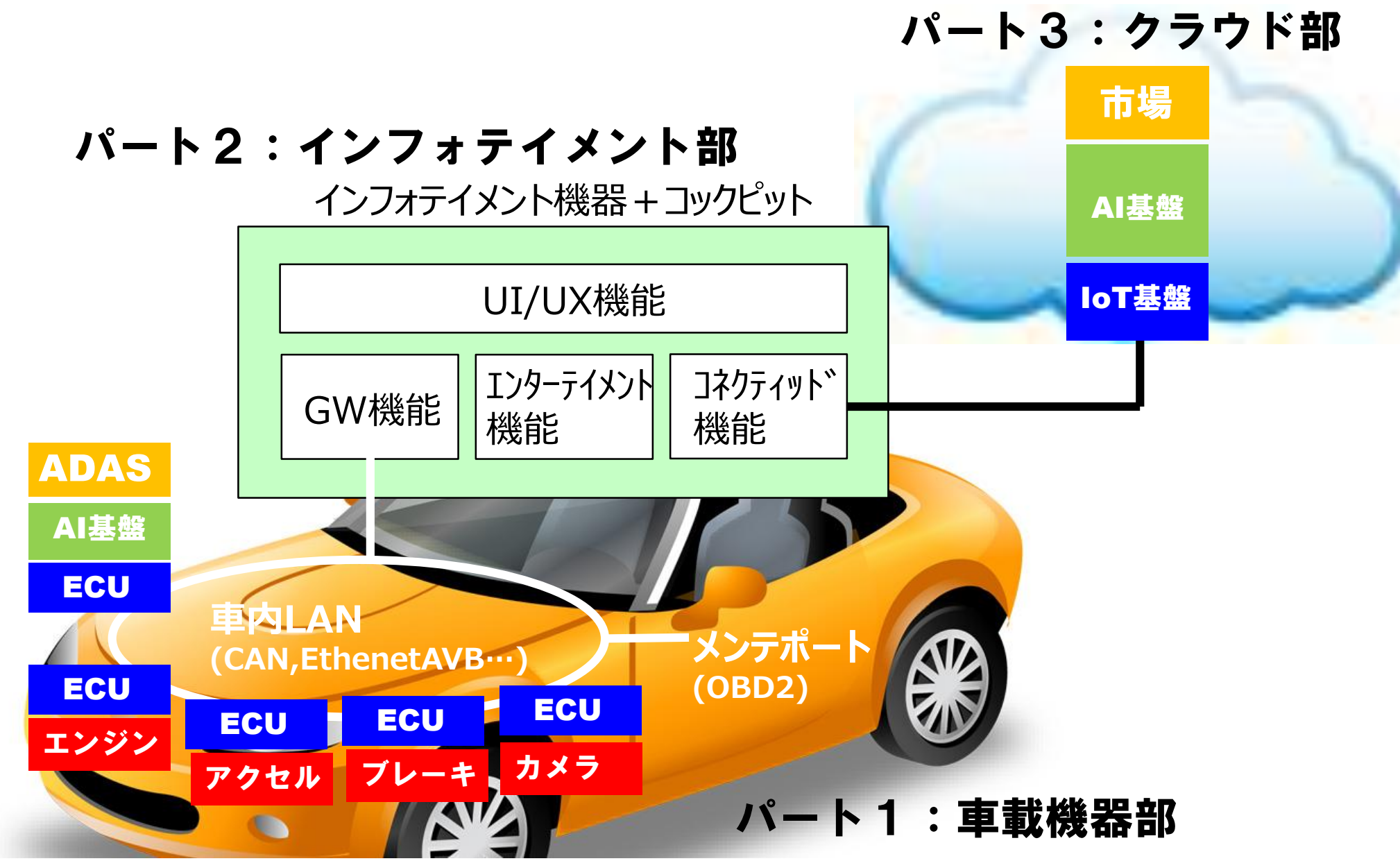
BCP（事業継続性）のリスク
⇒セーフティ＆セキュリティ対応投資とビジネス収益の関係（相場感）
無限責任の回避（言い訳の科学的証明）

Panasonic

IoTセーフティ・セキュリティ
～自動車の場合～

Panasonic

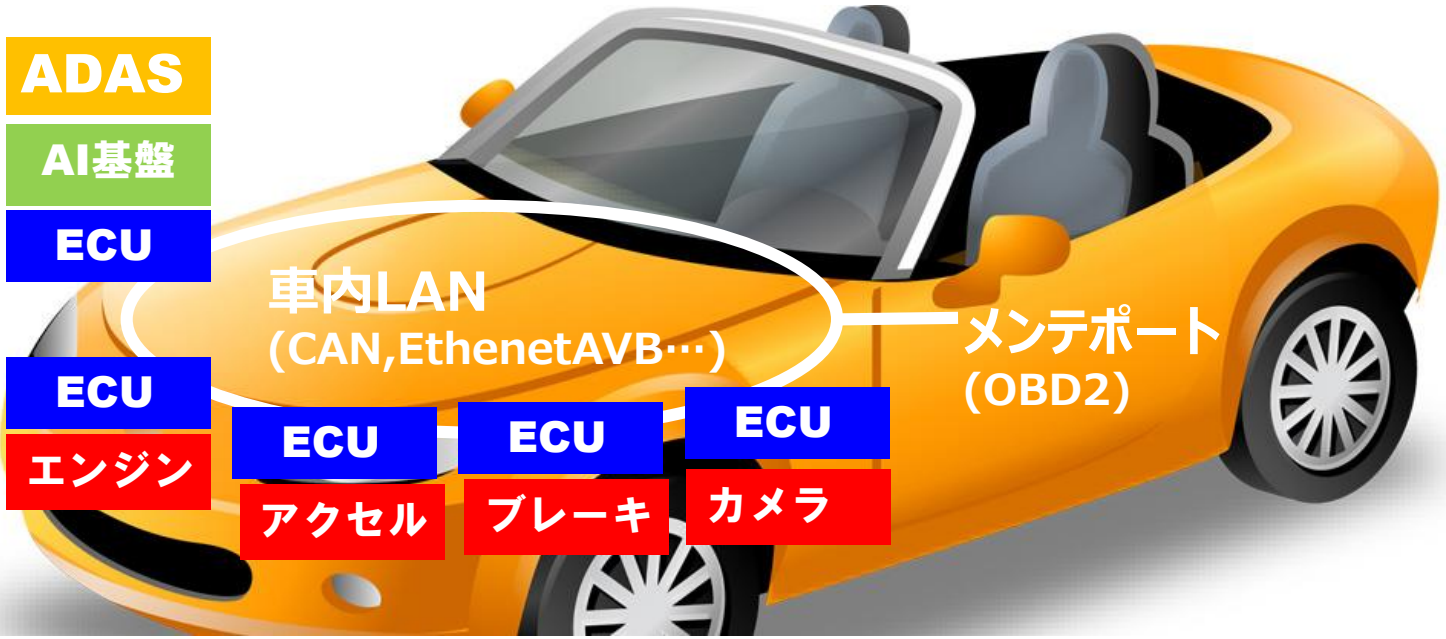
自動車システムの全体アーキテクチャ



Panasonic

パート1：車載機器部

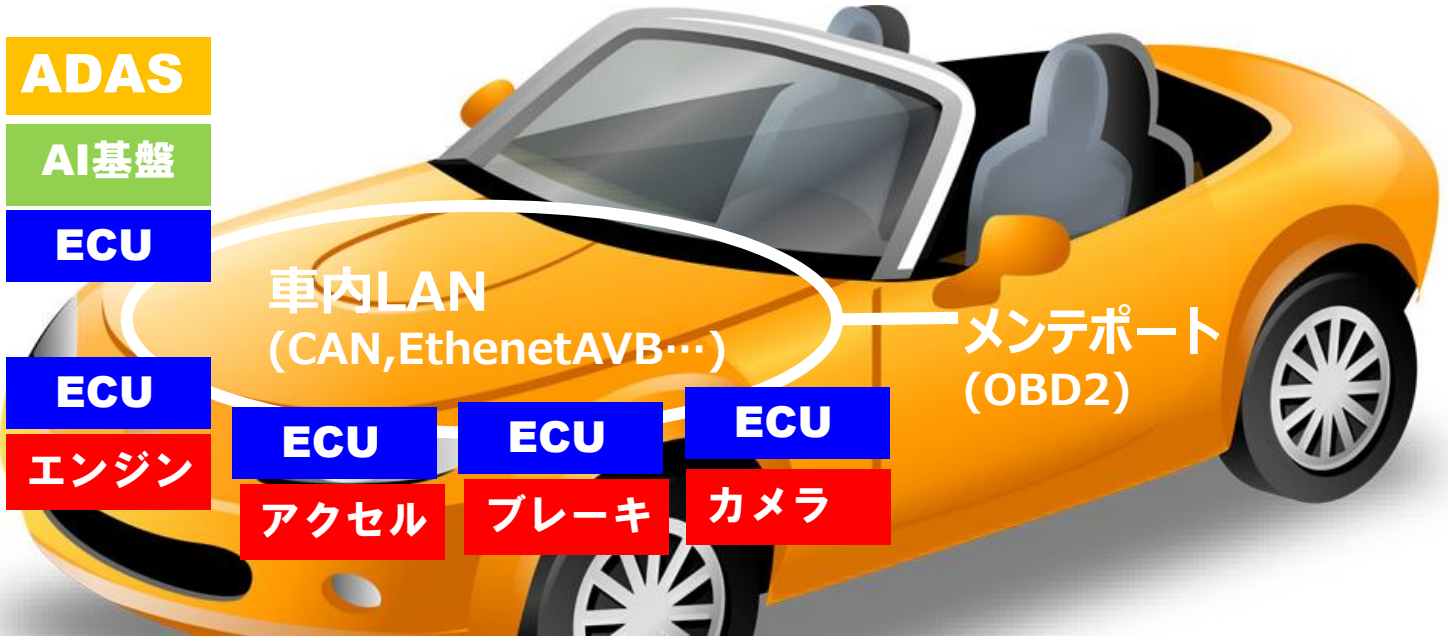
・走る・曲がる・止まるに関連するパート
・車載LANでECUが結ばれ各ECUがソフトウェアで制御
・ECU間で通信が発生し複合した連携動作を実現
・機能安全面でASILに応じた実装要請（ハード、ソフト、プロセス、ツール…）
・ADASや自動運転は即時制御必須のため、車内LAN直結で実装
（認識技術で深層学習が最近は使われる）



Panasonic

パート1：車載機器部のセキュリティリスク

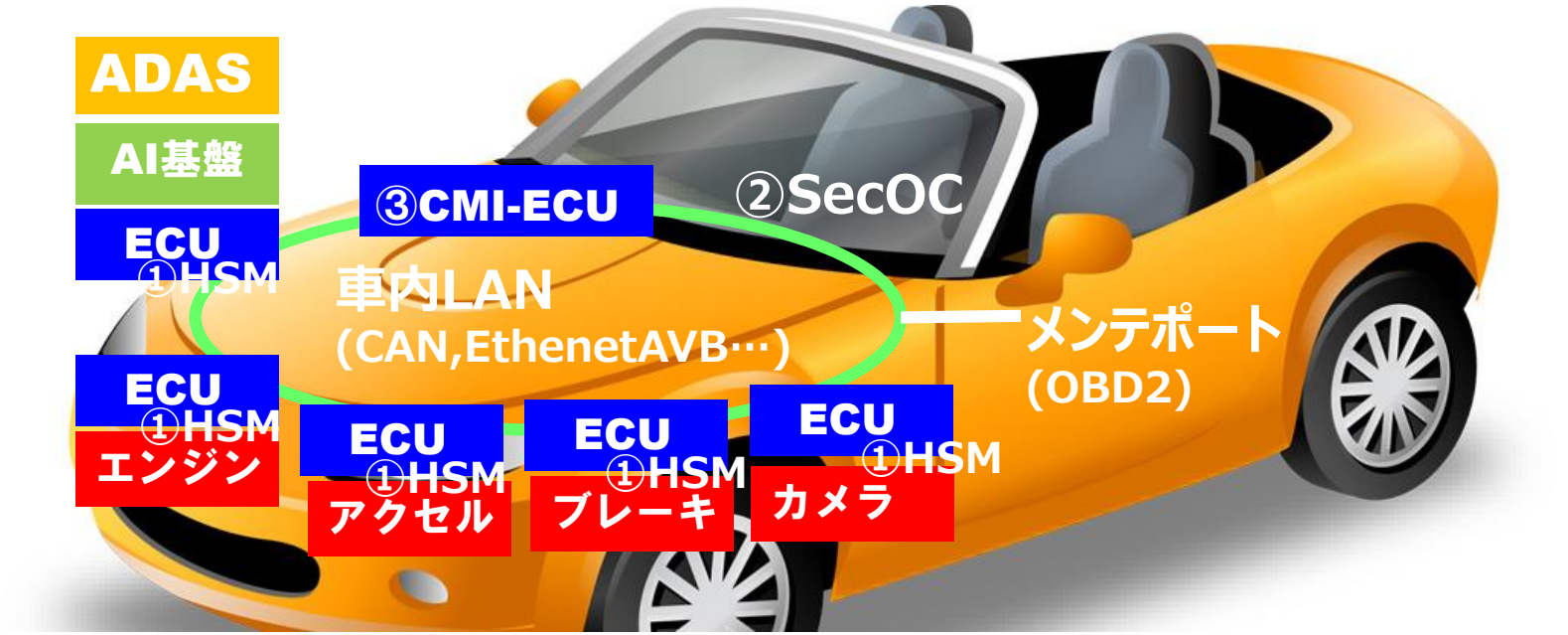
・CANが暗号化されておらず、OBD2ポートより車内コマンド解析され公開済み
・OBD2からCANコマンドを送り込むことで制御や表示データ改ざんが可能
・ECUの実装によってはファームウェアを読み出すコマンドをサポートしており、
ファームウェア解析後、セキュリティホールを具備するようアップデートされるリスク



Panasonic

パート1：車載機器部のセキュリティリスク対策

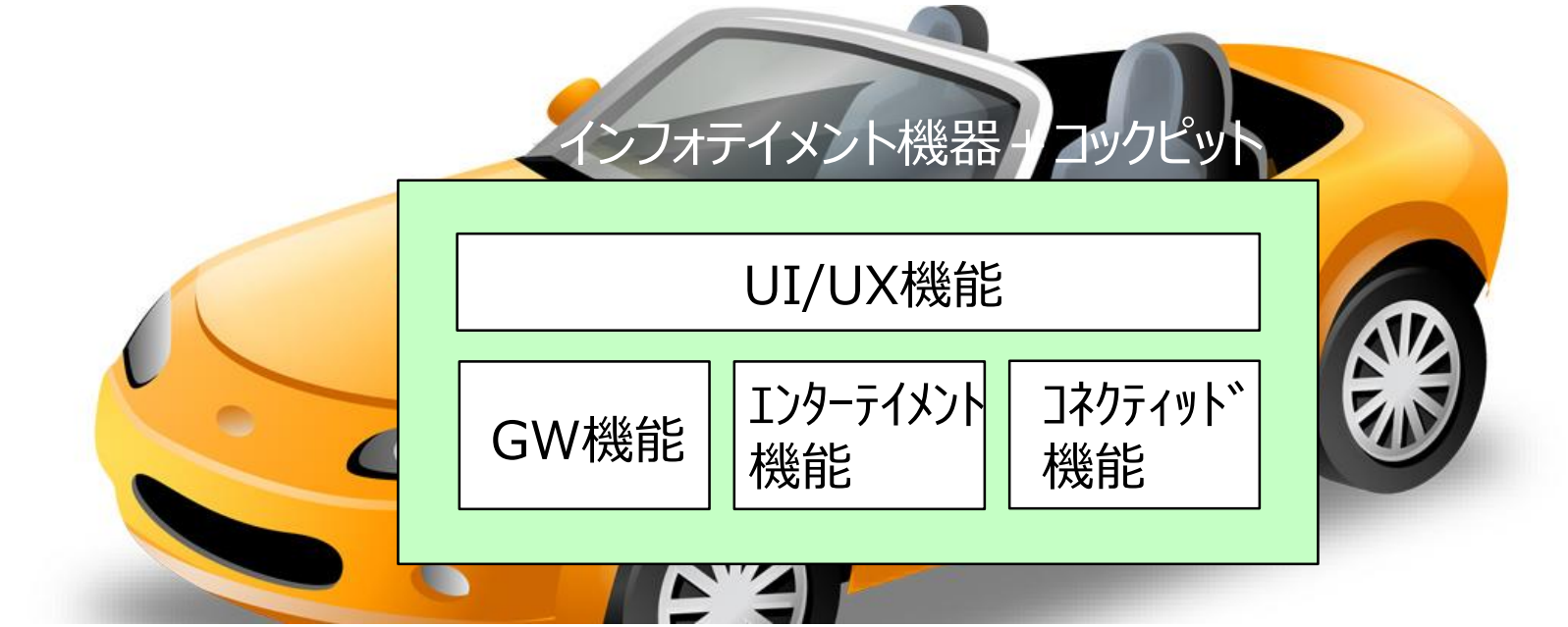
①個々のECUが改ざん検知、暗復号エンジンなどHSM(Hardware Security Module)を搭載(EVITA:E-safety Vehicle Intrusion proTected Applications等)→長期解
②車内LANの暗号化(AutosarのSecOC:Secure on Board Communication等)→長期解
③車内LAN信号を観測し異常な動きのパケットを無効化する→中期解
(ESCAR Europe2015でのPanasonicのCMI-ECU(Centralized Monitoring and Interceptor ECU)等)



Panasonic

パート2：インフォテイメント部

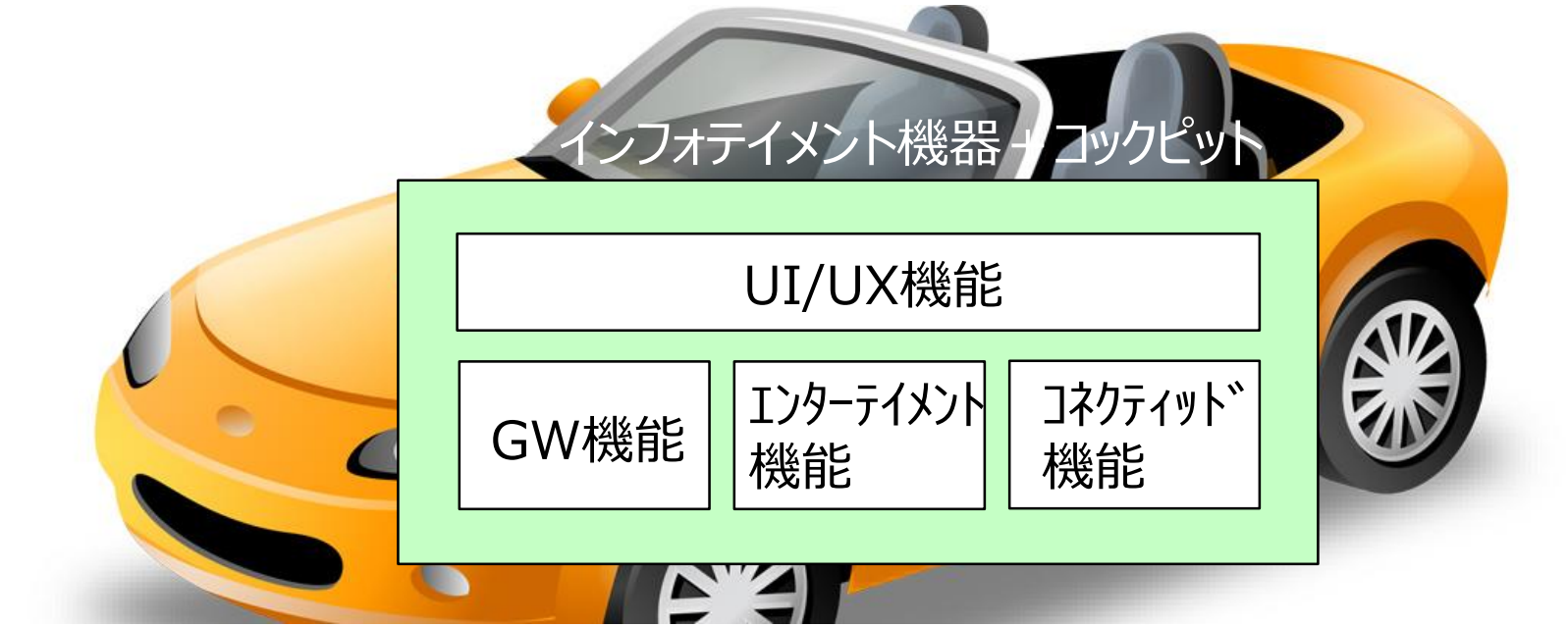
・スピードメータ、ナビなどドライバ、同乗者と情報のインターフェースとなる部分
・車内では比較的リッチなハードリソースが利用可能
・OSはAGL, Android Auto, CarPlayの３つに収斂（保安部品部を除く）
・車載機器部とはGW機能を介して結ばれ、3D地図の勾配情報によるシフトダウン、ヒヤリハット地域での速度制限などの車載機器動作への介入や、各ECUのソフトアップデートなどが実施される
・コネクティッド機能を介してクラウドサービスと通信を行いデータのやりとりを実施



Panasonic

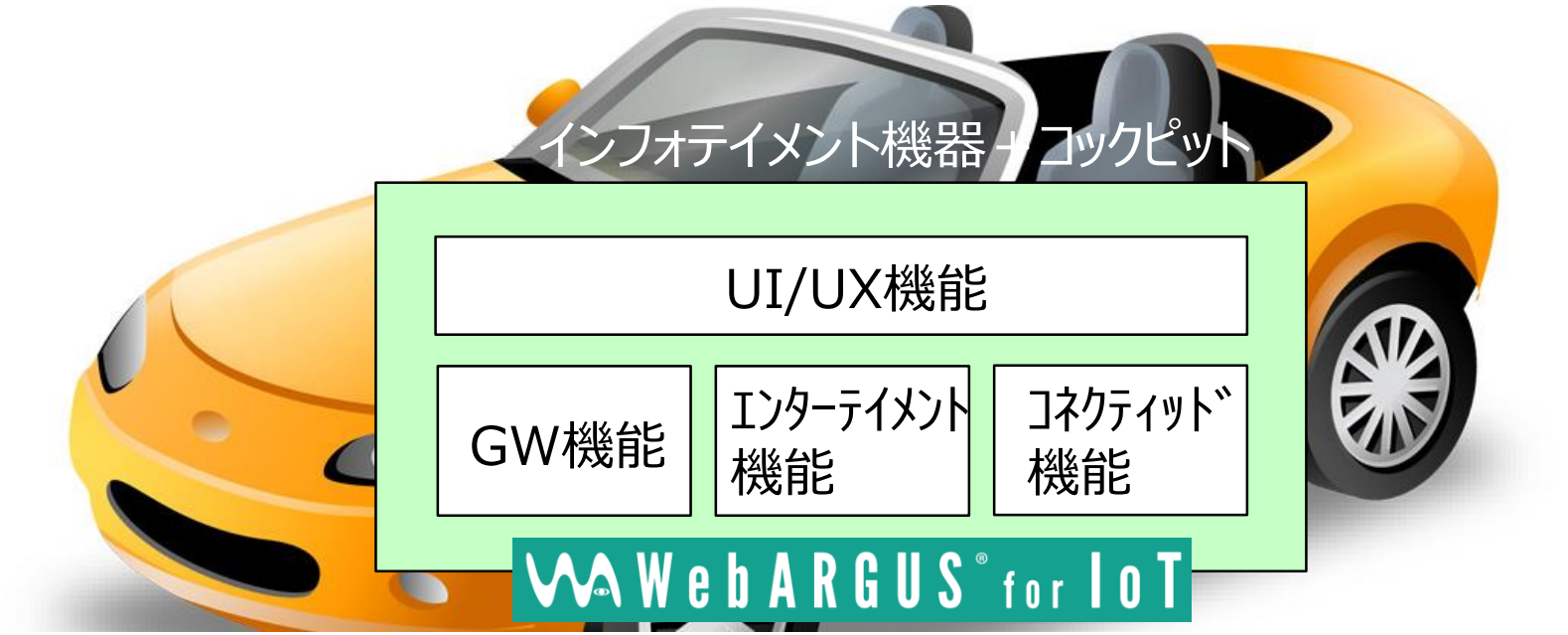
パート2：インフォテイメント部のセキュリティリスク

- 正規オーナがインフォテイメント機器を分解しソフトのオフライン解析のリスク
- USBやBLE通信で外部からマルウェア感染等を仕掛けられるリスク
- 自身が汚染されるとGWを介し車載機器部のソフトウェア不正アップデートや不正規CANコマンドの送信などを行うリスク
- 自身が汚染されるとスピードメータなど運転に必要な情報が正常に表示できなくなるリスク
- コネクティッド機能を介しクラウドサービス側からマルウェア等を仕込まれるリスク



パート2：インフォテイメント部のセキュリティリスク対策

①オフライン解析を避けるため必要に応じソフト難読化など耐タンパ化対応
②USBやBLE通信におけるファイヤーウォール
③車載機器部との通信におけるフィルタの徹底実施、ファイヤーウォール化
④車載機器部とのGW/スピードメータ等運転に必須部分、ナビ、コネクイティッド機能の各々を仮想化によりOSごとアイソレートを可能にする安心実装
⑤コネクティッド機能側がファイヤーウォールとしてクラウド側をフィルタリング
⑥それでも侵入、改ざんされた際の改ざん検知と即時書き戻し(WebARGUS for IoT)



Panasonic

パート3：クラウド部

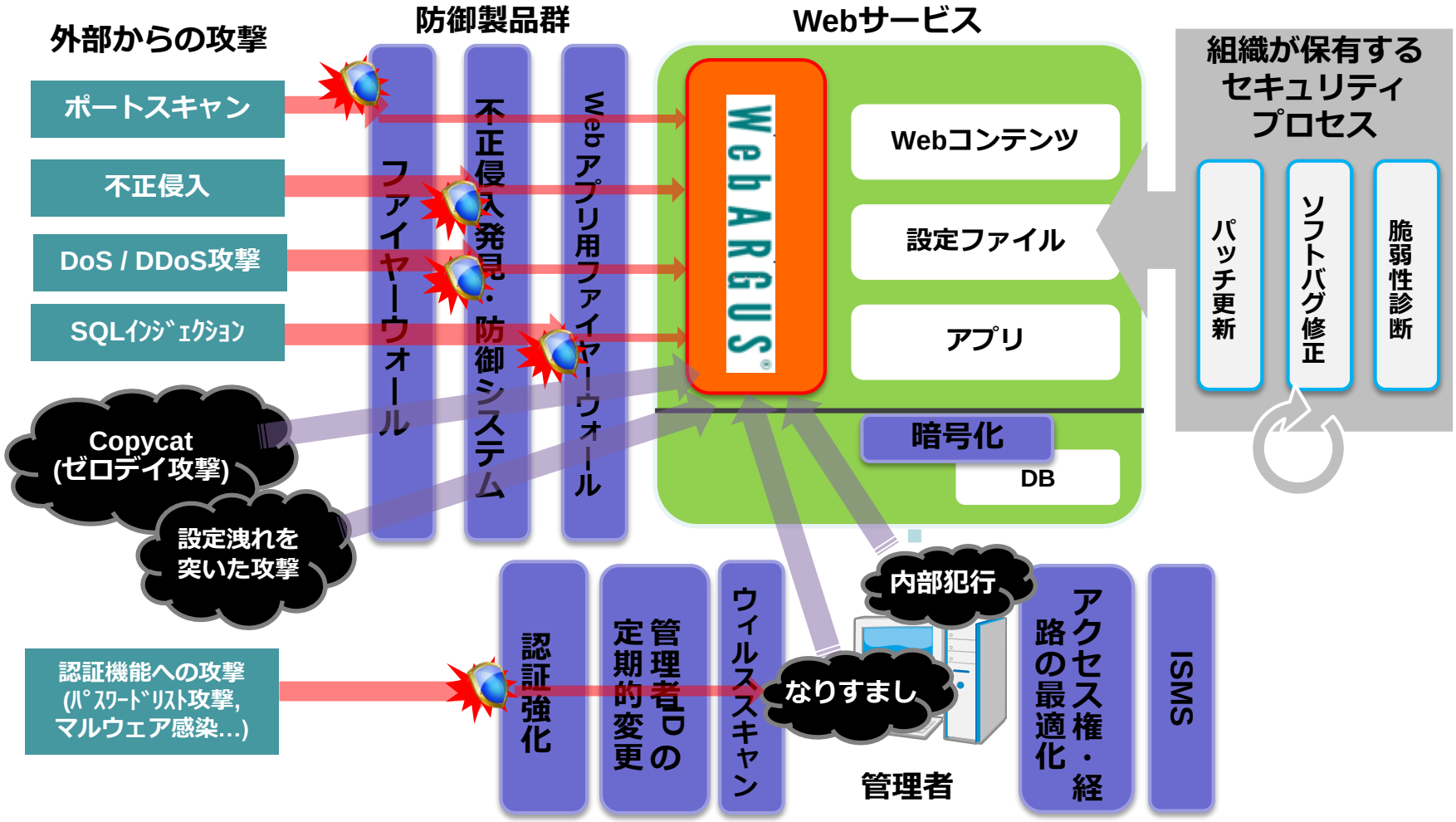
・現在地と関連したレストラン等のレコメンドを実施
・個人ごとにカスタマイズされた嗜好を保持
・人間系のオペレータへの接続も支援
・渋滞等でルート変更を提案
・インフォテイメント部、車載機器部のMDM
(Mobile Device Management)

Panasonic

パート3：クラウド部のセキュリティリスク

・通常のクラウド、Webサービス同様、DoS攻撃などのリスク
・オーナのなりすまし、プライバシー情報の流出
・アップデートの実行、マルウェア感染
・MDM乗っ取りによる全対象車の乗っ取りリスク

パート3：クラウド部のセキュリティリスク対策=Webセキュリティ対策



https://webargus-jp.ditproducts.com/

デジタルインフォメーションテクノロジー社様資料より引用

サイバー攻撃はITで防ぐ、早期復旧はOTで→早期復旧もIT+OTで行う

Jeep事案

Panasonic

組織による
IoTセーフティ＆セキュリティ対応

Panasonic

IoTセキュリティでの注意点(１)

１）B2C, B2B2Cで製品が一般消費者に渡る場合は、オフラインでのハッキング対策に注意

２）購入時以外に、譲渡、廃棄など製品の全ライフサイクルに渡るリスク分析が必要

３）ネットワークの常識は通じない。製品だけ販売するケースでは、ファイヤーウォールがある前提に立ってはいけない。またデフォルトのパスワードはワンタイム化する、パスワード忘れ対応では多要素認証を行うなどする必要あり

４）製品認証xユーザ認証の徹底により、野良化（管理者不在）の機器が接続に来るのを防ぐ

５）アーキテクチャ全体像は複雑だが、全体像を把握した上で対策を実施

Panasonic

IoTセキュリティでの注意点（２）

６）業界分野ごとに過去からのしがらみ（CANの平文通信など）があり、それを熟知した上でプロセスアプローチ・アーキテクチャアプローチ双方で対策を実施

７）セーフティが冒されるケースを重視したセキュリティ対策が必要。しかし、対策結果がかえってセーフティリスクを高めることはあってはならない
（例えば、自動車がハッキングされたことを検知し、運転中に急ブレーキで止める対策は危険なケースもある）

８）製品の組込みソフトウェアにOSSを利用する場合は、ライセンス条件を見て、消費者保護の観点を優先

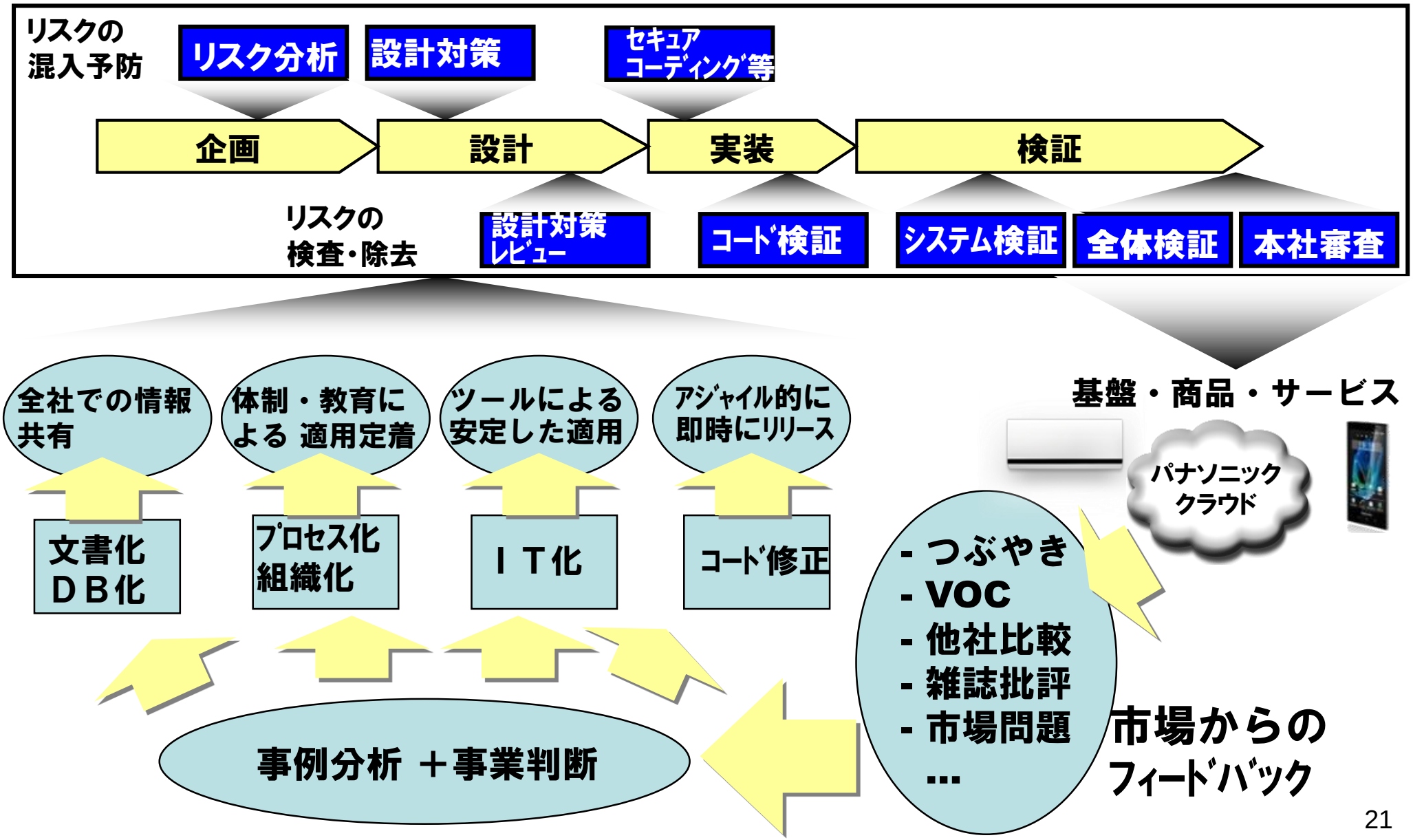
Panasonic

IoTセキュリティ対応17の指針（IPA）

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する
		指針2 安全安心のための体制・人材を見直す
		指針3 内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する
		指針5 つながることによるリスクを想定する
		指針6 つながりで波及するリスクを想定する
		指針7 物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする
		指針9 つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 つながることによるリスクを一般利用者に知ってもらう

機能安全・セキュリティ・コンプライアンスの全体プロセス

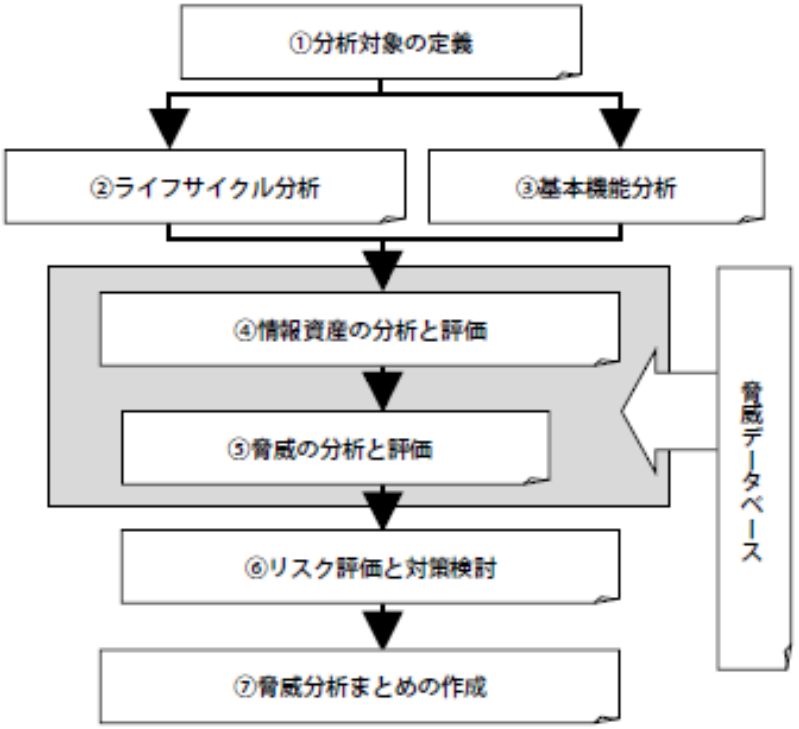
機能安全・セキュリティ・コンプライアンスの全体プロセス



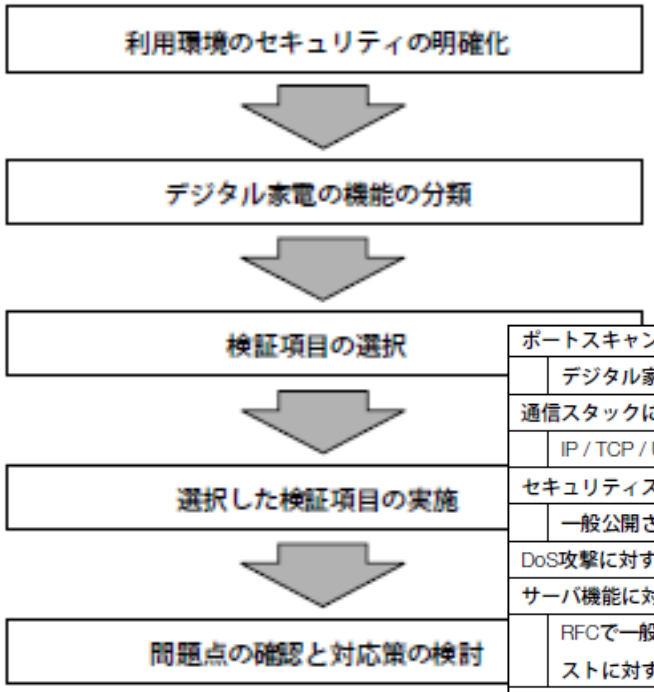
Panasonic

セーフティ＆セキュリティでの取組み（１）

社内の製品セキュリティセンターにて、ホワイトハッカーによるセキュリティ検証サービスを実施



脅威分析のフロー例



ポートスキャン
デジタル家電上で起動している通信サービスの検出
通信スタックに対する実装の確認
IP / TCP / UDP / ICMP
セキュリティスキャナ
一般公開されている脆弱性の検出
DoS攻撃に対する耐性の確認
サーバ機能に対する実装の確認
RFCで一般公開されているプロトコル，主に異常なリクエストに対する耐性の確認
クライアント機能に対する実装の確認
RFCで一般公開されているプロトコル，主に不正なサーバからの応答に対する耐性の確認
ファームウェアに関する確認
独自ユーザー認証に対する実装の確認
認証のバイパスや再送攻撃に対する確認
独自通信プロトコルに対する実装の確認

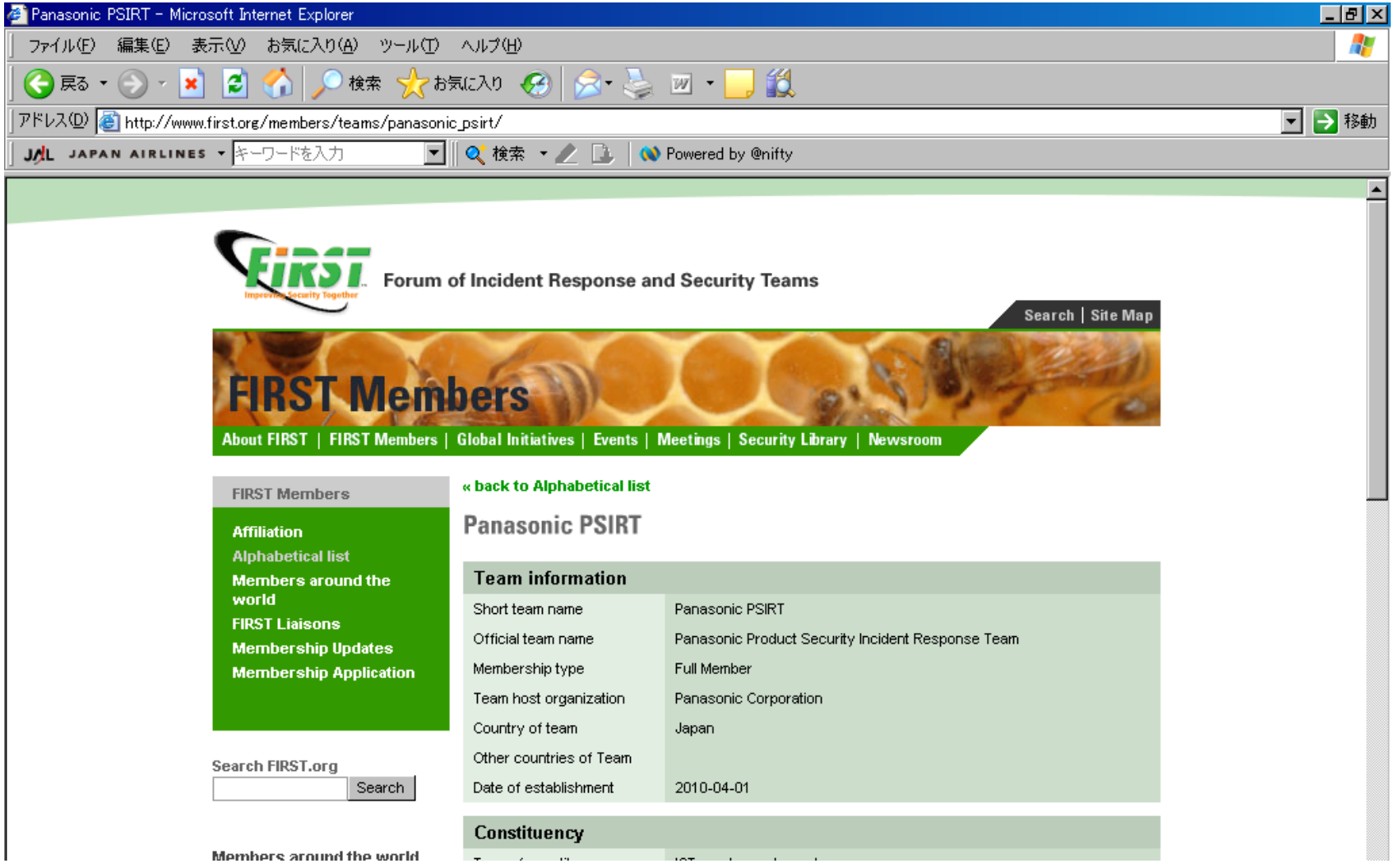
IP : Internet Protocol　TCP : Transmission Control Protocol
UDP : User Datagram Protocol
ICMP : Internet Control Message Protocol　DoS : Denial Of Services
RFC : Request For Comments

セキュリティ検証のフローと検証項目例

セーフティ＆セキュリティでの取組み（２）

製品やサービスのネットワークセキュリティ課題発生時の対応体制（PSIRT:　Panasonic Product Security Incident Response Team）

2010/4/1より運用中



Panasonic

IoTセーフティ・セキュリティを支える技術体系

Panasonic

技術分類（1）

数学的技術

内容	キーワード
数学理論により裏付けられる技術	暗号（安全性）、ビットコイン（希少性）、暗号計算（安全な統計処理）、秘密分散

ビットコインを支えるブロックチェーン
http://sssslide.com/speakerdeck.com/ks91/blockchain-overview

秘匿検索・秘密計算
http://www.nstac.go.jp/services/pdf/121116_6-1.pdf

秘密分散の効能
http://www.panasonic.com/jp/business/its/cloud_backup/lp.html

秘密分散の原理
https://www.panasonic.com/jp/corporate/technology-design/ptj/pdf/v5902/p0107.pdf

アナログ要素技術

内容	キーワード
アナログ信号を使った解読など、デジタル情報を支える物理信号に関連する技術	真正乱数（熱雑音の利用）、サイドチャネルアタック（電力量や不要輻射の変化から暗号鍵を解読）

インテルの真性乱数生成器
（エントロピー・ソース）
https://www.isus.jp/security/drng-guide/

立命館大学　藤野研究室
（サイドチャネルアタック対抗の根本対策技術）
http://www.ritsumei.ac.jp/se/re/fujinolab/

技術分類（2）

人間行動解析技術

内容	キーワード
人間の行動解析からリスク検知を行う技術	BIOCATCH Less Friction·Less Fraud 人のタッチパネル等の操作の癖から個人認証。人のふりをするマルウェアの検知 http://www.biocatch.com/ FORTSCALE INTELLIGENT CYBER INSIGHT 人事DBと重要情報DBを元に社内人員のアクセスパターンと組合わせて不正行為のリスクが高い人を発見 https://fortscale.com/ Terrogence Ltd. SNSやYouTube等からテキスト、写真などを分析し、自爆テロ、サイバーテロなどの不法行為の時間や場所、ターゲットを予測 https://www.terrogence.com/

Panasonic

技術分類（3）

生体認証技術

内容	キーワード
人間の個人認証を指紋等で確実に行う技術	指紋認証、虹彩認証、顔認証、音声認証など

IPA生体認証運用の手引き
https://www.ipa.go.jp/files/000024404.pdf

耐タンパ化技術

内容	キーワード
処理を見破られないように実装する技術	難読化（ソースコードを結果は同じだがロジックを追えない複雑な計算に変更）、破壊（ハードの分解を試みると回路、LSIが破壊され中身を見れなくなる）など

ICカードリーダの耐タンパ紹介
http://sol.panasonic.biz/ic/jt-r400_r230.html

.NETのSoftware Obfuscation解説
https://msdn.microsoft.com/ja-jp/library/ms227295.aspx

三菱電機TURBOMISTY
http://www.mitsubishielectric.co.jp/corporate/giho/2002/04/pdf/0204109.pdf
http://itpro.nikkeibp.co.jp/members/NIT/ITARTICLE/20020712/1/zu1.html

Panasonic

技術分類（4）

静的解析・セキュアコーディング技術

内容	キーワード
ソースコードを解析し、脆弱性の存在を指摘。代替手段でのソース改善方法の提示などを行う。	スタックオーバーフローやSQLインジェクションにつながるソースコードを排除

ソースコード静的解析CHECKMARX社
https://www.checkmarx.com/
ソースコードを静的解析し、関数の呼び出し関係も考慮した上で、最も効率的な改善点をピンポイントで提示

ソースコード静的解析FOSSID社
https://fossid.com/
OSS由来のコードを静的解析により見つけ出し、旧バージョンであれば、それが持つ脆弱性を指摘、脆弱性対策がなされた新バージョンへの置換を促す

バイナリーコード静的解析INSIGNARY社
https://www.insignary.com/
FOSSID同様だがバイナリーでも対応可能に特徴

セキュアコーディングSONY DNA社
https://www.sonydna.com/sdna/solution/scc.html
Secure Coding Checkerを提供し、プログラミングがJSSECセキュアコーディングガイドに従っているかを都度検証（http://www.jssec.org/dl/android_securecoding.pdf）

技術分類（5）

仮想化技術

内容	キーワード
ハイパーバイザーで処理を孤立化	redbend, GreenHills等が組込み向けにも提供

redbend社の仮想化技術を利用したP-04D(スマホ)のパーソナルプロテクト
http://153.127.246.254/pdf/2013-08-01/122161.pdf

セキュアハード技術

内容	キーワード
ハードウェアとして特殊なモードでしかアクセスできないモードを設けるなど、セキュリティを考慮したつくりを提供	暗復号エンジン、TrustZone(ARM)、TPM(Trusted Platform Module)による改ざん検出の保証、バススクランブラ、デバッガー認証ROM化時のバックドア封止　etc

ARM社TrustZone技術解説
https://www.arm.com/products/security-on-arm/trustzone

Let’s Note(PC)におけるTPM等の解説
http://askpc.panasonic.co.jp/beginner/topics/security04.html

技術分類（6）

フォールトトレランス技術

内容	キーワード
回路など多重化することにより、一系統が停止しても、もう一系統で動作を継続	ftServer（Stratus社）、複数データセンターによる多重化、データの多重格納　etc.

Stratus社のftServer
http://www.stratus.com/solutions/platforms/ftserver/

Amazon Web Serviceでの冗長実装紹介
https://aws.amazon.com/jp/cdp/cdp-floating/

レジリエンス技術

内容	キーワード
システムはダウンすることを前提に対応する技術	避難訓練に伴う退避・復旧を常に行うことで、予測できないシステムダウンからも常に復旧できる

産総研のレジリエンスOS MiRK
（エルイーテック社の技術を引継ぎ）
http://www.itri.aist.go.jp/events/IoTSecSymp16/pdf/20160307poster_ysato.pdf

Netflix Chaos Monkey
https://github.com/netflix/chaosmonkey

技術分類（7）

枯れた技術

内容	キーワード
古くから実用化され、挙動、寿命などの特性が良くわかっている技術を採用する	衛星打ち上げロケットや人工衛星では、できるだけ安定化した技術の採用とともに、別会社が同じ仕様で別の実装を納入し、それで二重化するなどが実施されている

京都大学 磯部准教授の講座資料より
http://www.kwasan.kyoto-u.ac.jp/~isobe/etc/seika13/file/Seika-20130618.pptx.pdf

プロセス技術

内容	キーワード
手順、権限をはっきりさせ、リスク分析・脅威分析から設計、実装、検証の各内容・結果の相互関係のトレーサビリティを保証する（トップダウンアプローチ）	脅威分析等の手順ごとに従来は手法の実施において、ExelやWordなどのドキュメントに手作業で書いていたが、ツールチェーンで全体をサポートする方法が、徐々に採用されつつある

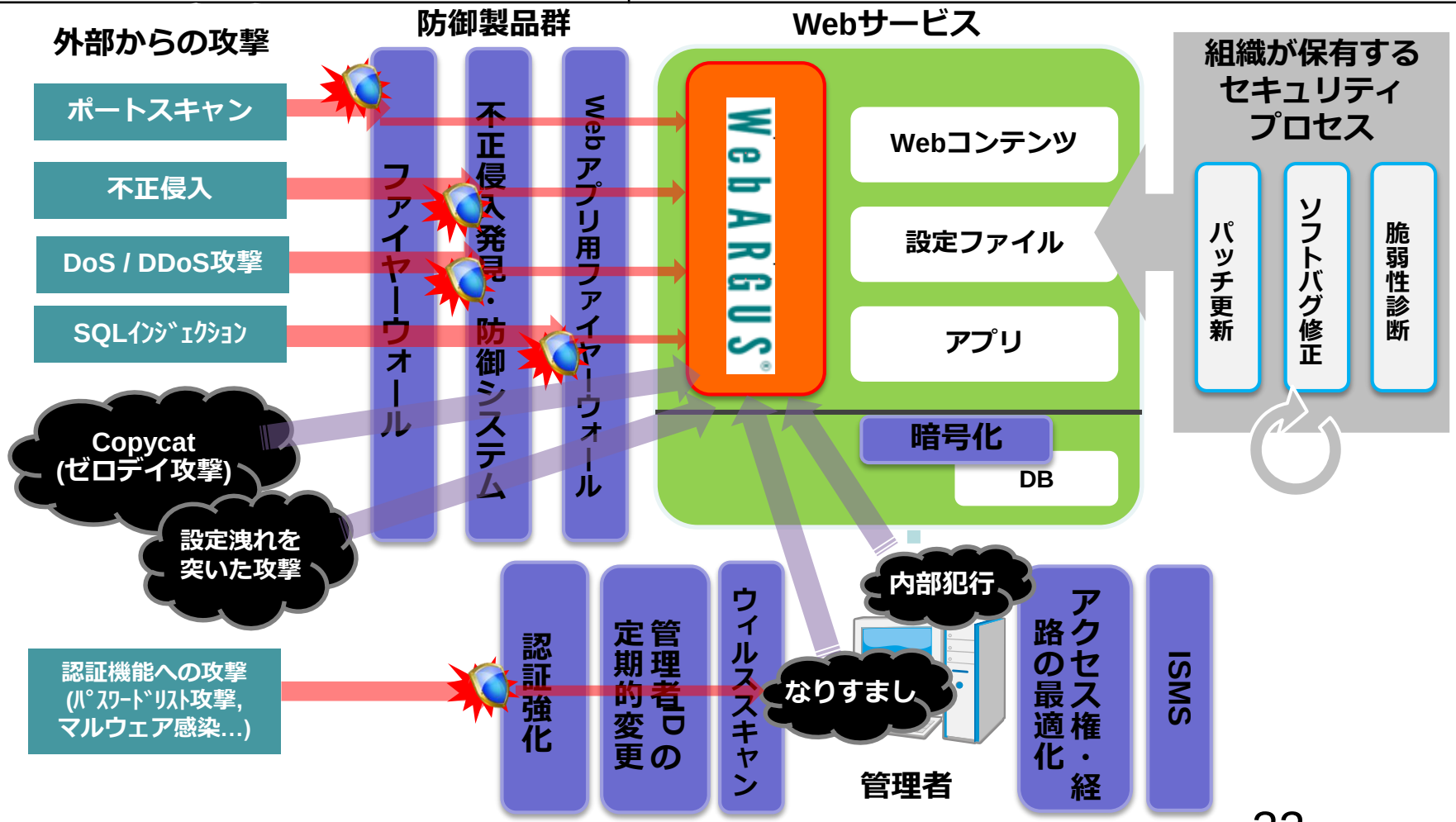
フランスCEA LISTのPapyrusプロジェクト説明
http://www-list.cea.fr/en/184-media/list-tv/embedded-systems/195-papyrus
https://www.youtube.com/watch?v=cUmysH--J7I

Panasonic

技術分類(8)

ネットワーク・Web技術

内容	キーワード
ネットワークやWebの特性に由来する脆弱性を防ぐ技術	ポートスキャン対応、Firewall、証明書による改ざん検知、改ざん監視・復旧など



https://webargus-jp.ditproducts.com/

技術分類（9）

AI技術

内容	キーワード
過去事例や新規のZero Dayアタック対処法の発表から対策と診断手順を学習、自システムを都度、自動診断し、リスクのアラートや、場合により自己修復を実施	2017/7現在、対応する製品はないが、ITシステムにおいて、過去事例と診断手順を学習し、システムトラブル発生時の課題切分けと対策提案、事故状況によっては自動修復まで行うツールはある

Ipsoft社のIPCenter（AIによるシステムダウン時の自動修復ツール）
http://www.ipsoft.com/ipcenter/

法的対策

内容	キーワード
法制化、法律適用によりセキュリティ問題発生の抑止力とする	リスクの高いままでの製品やサービスの発売抑制、セキュリティ犯罪者の処罰など

B-CASカード社サイトより（刑事罰の明記）
https://www.b-cas.co.jp/law/

Panasonic

脅威分析・リスク分析のイメージ

リスク・脅威	対策	対策の分類
第三者によるハードディスク換装での個人情報不正コピー	ハードディスクの勝手感想は保証外とする	方針による対策
ログイン時、背後からパスワードを盗み見られる	パスワード入力時、画面上は＊の表示にする	仕様による対策
不正規なサイトに誘導される	ユーザにURL入力をさせず、特定サイト固定とする	仕様による対策
DoS攻撃中、録画が止まってしまう	録画やデコードに関連するプロセス、スレッドの優先度を上げる（優先度設計）	SW設計による対策
	プロセス間通信のドメインを外部解放型のinetから内部権限型のunixドメインに変更する（データ通信設計）	SW設計による対策
不正規なJPEGファイルでハングアップや例外で別コード起動を誘発される	データ領域のメモリ内容を命令コードと解釈しないよう実行コードの難読化とHW内部での自動復号実行	HW設計による対策
	JPEGファイルの解釈を厳密化（配列パラメータチェックの厳密化でバッファオーバーラン防止）	セキュアコーディング技法・静的解析技法
TCP Optionに不正規なデータを入れられてハングアップする	TCP解釈部の文字列チェックを厳密化（Linuxカーネルのデバッグ）	セキュアコーディング技法・静的解析技法
APIを不正規に呼び出され、想定外の入力値で誤動作を誘発される	設計時より関数をUML記述。入力値範囲を全件自動生成させ、ツール上で自動検証を実施。全ケース正常動作を保証。	開発手法による対策

パナソニックにおける「ことづくり」と「エコシステム」

綱領

産業人タル本分ニ徹シ
社會生活ノ改善ト向上ヲ圖リ
世界文化ノ進展ニ
寄與センコトヲ期ス

共存共栄

松下幸之助

創業者 松下幸之助

（当社資料）

Panasonic

A Better Life,
A Better World

IoTビジネスモデル、OSS、IoTセキュリティ等の個別相談・疑問などあれば
kajimo7126@gmail.comまでご連絡ください