

# JASAE セミナー

第24回JASAE/ETセミナー  
自動車等組込みシステムのセキュリティ技術

## 組込みシステムの セキュリティへの取組みガイド

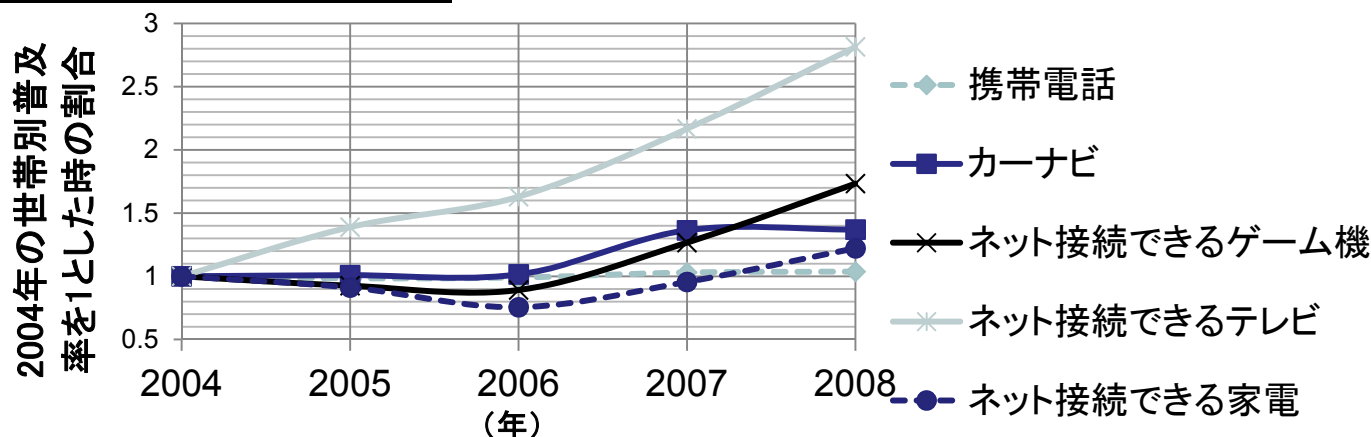
2010年10月15日  
独立行政法人 情報処理推進機構  
セキュリティセンター  
情報セキュリティ技術ラボラトリー 研究員  
萱島 信 (博士(工学))

組込みシステムは、日本では重要な産業※1

- 組込みシステム関連企業従事者数は475万人(全産業比率8.1%,製造業比率47.9%)、国内総生産は約66.7兆円(国内生産比率13.1%)

日本での組込みシステムをとりまく現状※2

- 組込みシステムの普及率は年々上がっており、会社、家庭など様々な場所で使われるようになった。
- 近年、組込みシステムの機能やサービスの向上が著しく、ネットワークに接続される製品が増えている。



ネット接続できる組込みシステムの世帯別普及率

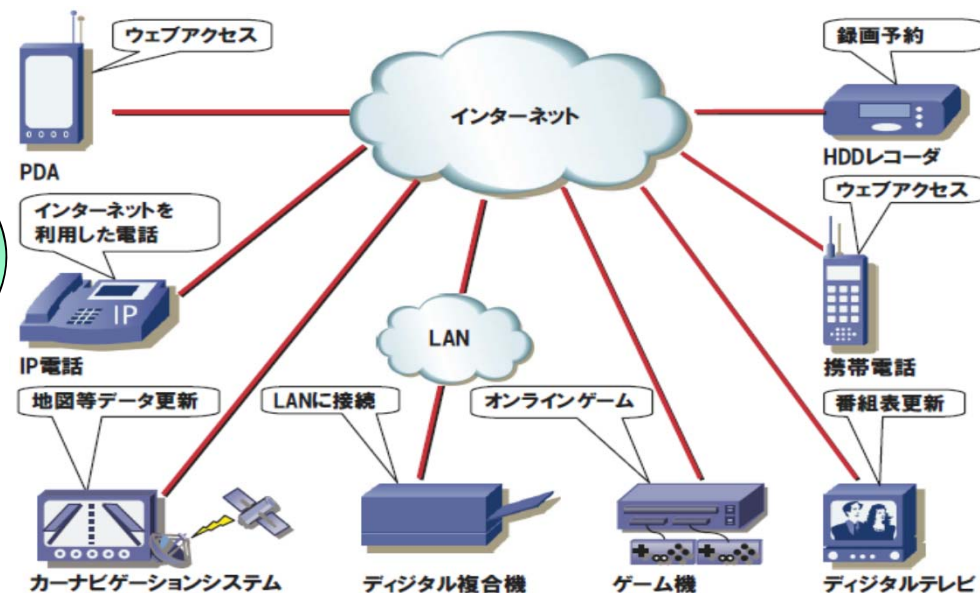
※1経済産業省「2008年度組込みソフトウェア産業実態調査」  
※2総務省「平成20年度通信利用動向調査」

# 組み込みシステムセキュリティの必要性

## なぜ今、組み込みシステムセキュリティを考えるのか？

- 旧来はスタンドアロンであった組み込みシステムがネットワークに繋がってきたことによって、ネットワークを介した脅威にさらされる様になった。
- PCの場合であればアンチウイルスソフトの導入やファイアウォールの利用などで防がれていた脅威が、組み込みシステムでは十分な対策がなされないままに利用されている。

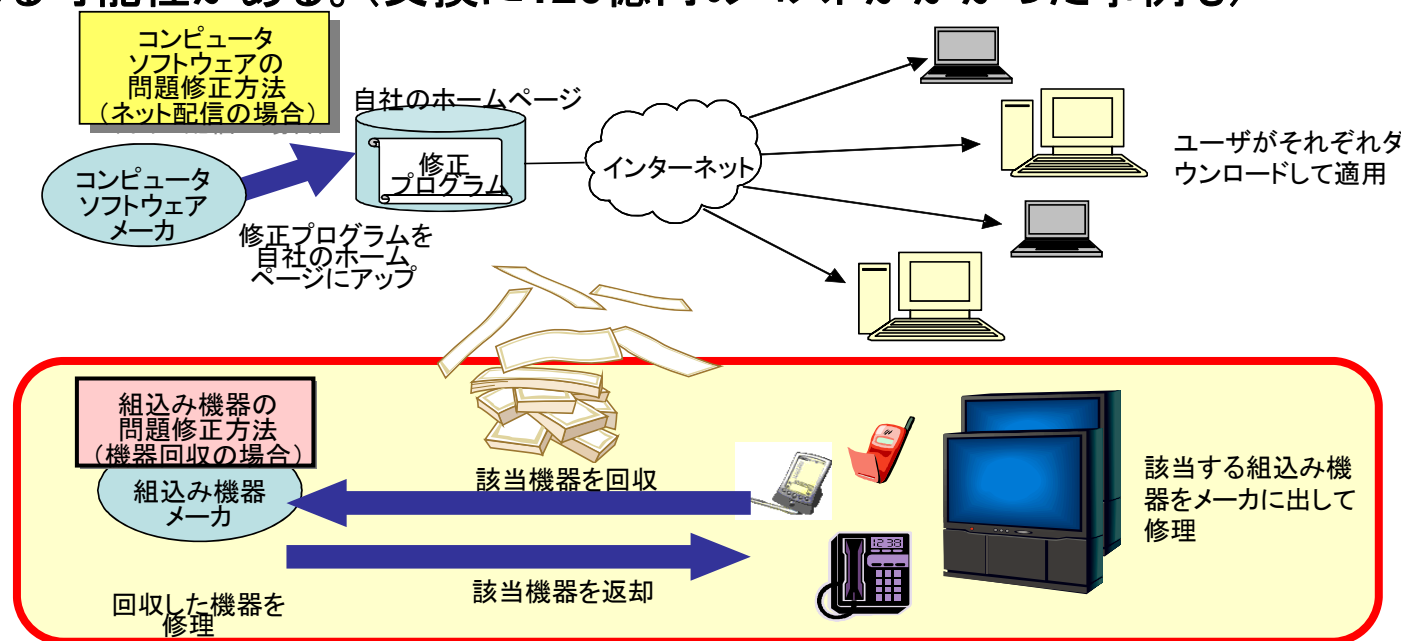
・コスト優先の現状ではなかなかセキュリティにリソースをさけない  
・開発者のセキュリティ教育を実施するのも困難



開発者の声

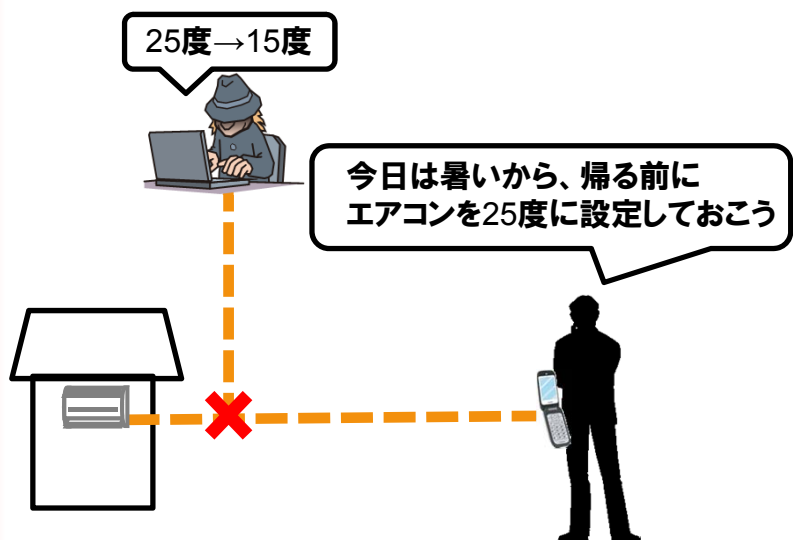
# 組み込みシステム特有の課題(1/2)

- 製品回収が必要になる可能性がある
  - 組み込みシステムはソフトウェアとハードウェアが一体化されて開発されている。そのため、セキュリティ上の課題としてソフトウェアとハードウェアの関係がより密接になった。
  - この結果、セキュリティ上の弱点の解決に修正パッチのみで対応できるとは限らなくなり、製品回収が必要になる可能性もでてきた。
  - 組み込みシステムメーカーはセキュリティ対策を怠ると、多大なコストを背負うことになる可能性がある。(交換に120億円のコストがかかった事例も)



## 組み込みシステム特有の課題(2/2)

- パソコンに比べ、人体に対する被害が発生する可能性がある
  - 組み込みシステムはパソコンと違って多種多様な機能を持つ。人間が快適に生活するためのものや、人の命を預かるものもある。
  - そのため、セキュリティ上の弱点を突かれると、深刻な事故が起こる可能性がある。
  - パソコンのセキュリティインシデントは情報漏洩や金銭にまつわるものが大半だが、組み込みシステムの場合は人体に被害が及ぶ可能性が高い。



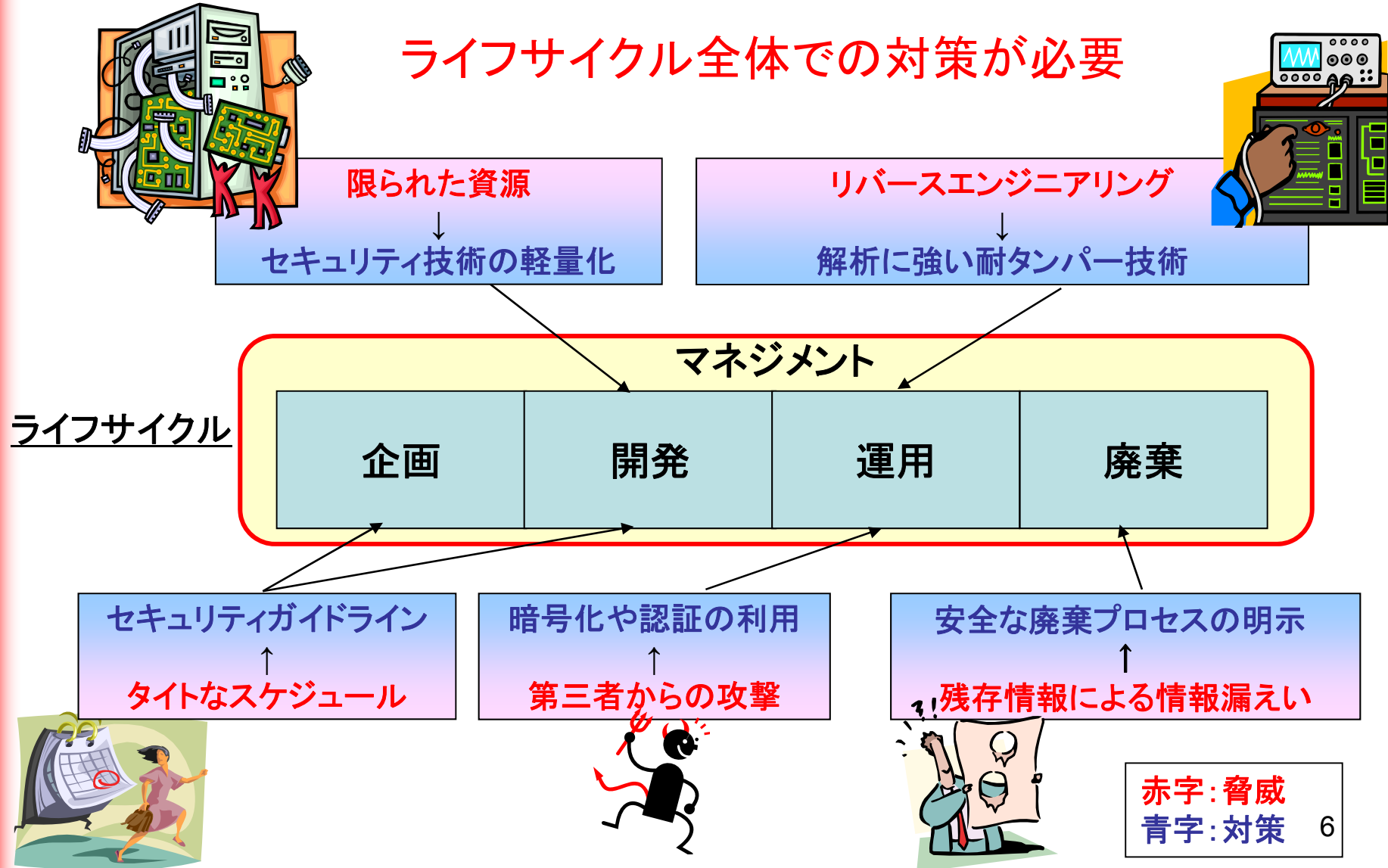
エアコンの設定温度を極端な温度に変えてしまう。  
その部屋の住人が体調を崩す可能性がある。



カーナビに対して、行き止まりなのに行き止まりではないと間違った情報を流す。  
運転者を混乱させ、事故につながる可能性がある。

# 製品に対するセキュリティ対策の基本

ライフサイクル全体での対策が必要



# セキュリティへの取組みアプローチ

セキュリティ上の問題により、被害や損失が発生する前に  
**まずは**組込みシステムのセキュリティを意識することが重要

- 今回のアプローチで目指したのは・・・
  - 組込みシステムの開発に関わる、経営者、開発者を対象として、**セキュアな組込みシステムの開発を行うために、システムのライフサイクル全体で取り組むべき指針**を示す。
  - 自組織のセキュリティへの取組みのレベルを把握できるように、**ライフサイクルにおける16の項目と4つのレベル**を策定する。
  - これによって**経営者、開発者のセキュリティ意識向上**を目指す。

# 「セキュリティへの取組み」のレベル

	マネジメント方針	企画方針	開発方針	運用方針	廃棄方針
レベル4	セキュリティへの取組みに対して、組織としての方針策定および実施に加え、監査のプロセスを有する	組織の方針に基づき、客観的評価を想定したセキュリティルールが策定および運用される		組織の方針として脆弱性対策方針を定めると共に、一般への公開を行う	客観的な基準に基づいたセキュリティリスクの軽減方法が用意される
レベル3	セキュリティへの取組みに対して、組織としての方針策定および実施する	組織の方針に基づいてセキュリティルールが策定および運用される		組織の方針として、脆弱性対策方針を定めている	廃棄時のセキュリティリスクの軽減方法が用意される
レベル2	セキュリティへの取組みを開発責任者や開発者に一任し、問題を案件ごとに個別に対応する	セキュリティルールが開発責任者や開発者主導で策定および運用される		脆弱性対策方針を製品ごとに定めている	廃棄方法が仕様書等に明記される
レベル1	セキュリティへの取組みを行っていない	セキュリティルールは定めていない		脆弱性に対する保証基準を設けていない	廃棄方法が考慮されていない

# セキュリティを考慮すべき16項目

マネジメント(セキュリティ関連商品でなくても、メーカーとして常に行うべき事柄)

- セキュリティルール、セキュリティ教育、セキュリティ情報の収集

企画・開発(ライフサイクル全体の計画および、システムの開発を行うフェーズ)

- 予算、開発プラットフォーム選定
- 設計、ソフトウェア実装、開発の外部委託における取組み、セキュリティ評価テスト・デバッグ、ユーザガイド、工場生産管理、新技術への対応

運用(組込みシステムがユーザの手に渡った後、製品として利用されるフェーズ)

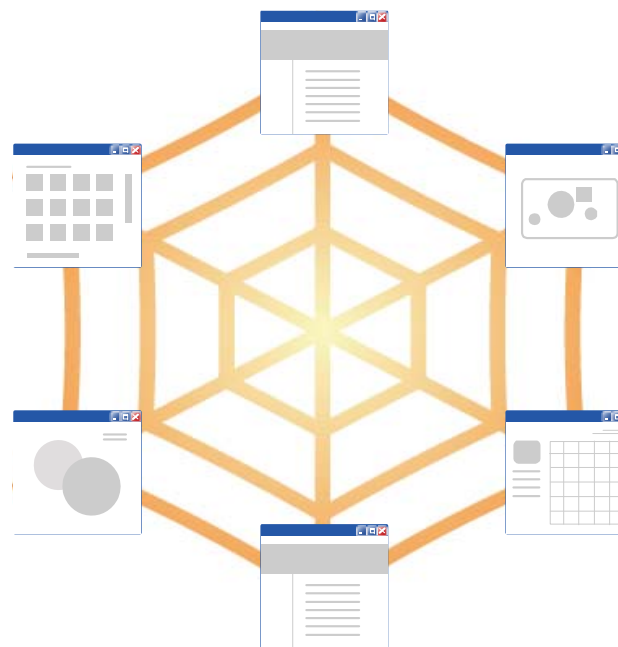
- セキュリティ上の問題への対応、ユーザへの通知方法と対策方法、脆弱性関連情報の活用

廃棄(買い替え、故障などで組込みシステムが廃棄、リサイクルされるフェーズ)

- 機器廃棄方法の周知

# 16項目の取組みの説明 ～マネジメント～

- セキュリティルール
- セキュリティ教育
- セキュリティ情報の収集



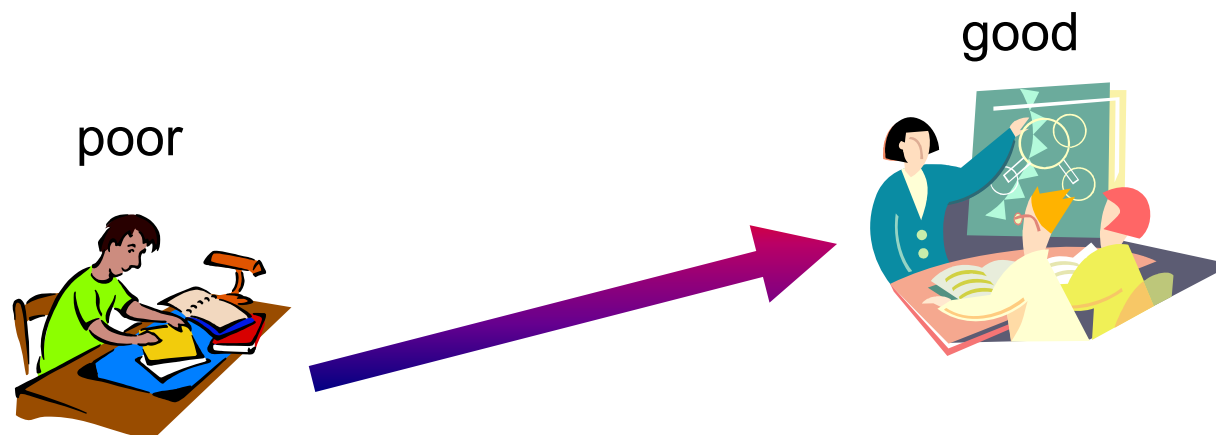
# セキュリティルール

- 取組みを場当たりのにしないための、実施すべき項目/禁止項目を明確にする
- 組織の取組みとしては、ISMSが参考になる
  - 情報セキュリティ基本方針
  - 組織全体に関する情報セキュリティ管理規則
  - 人的リソースに関する規則
  - 開発体制・環境に関する規則
  - 設計に関する規則
  - 調達に関する規則
  - 運用に関する規則
  - 廃棄品として回収した機器に関する規則

# セキュリティ教育

- 脆弱性を作り込まないためには、情報セキュリティに関する知識が必要です。例えば以下のようなものです。
  - ー現時点で知られている脆弱性に関する知識
  - ーセキュア・プログラミングに関する知識
  - ーセキュリティテストに関する知識

セキュリティ教育を個人や一部のグループの自主的な活動にまかせるのではなく、組織としての教育システムをつくるのが理想的



# セキュリティ情報の収集

- オープンソースソフトウェアは、開発元による積極的なセキュリティ情報の収集が必要
  - 脆弱性に関する情報 → IPAのWebサイト
  - 暗号技術に関する規格動向 → CRYPTRECのWebサイト



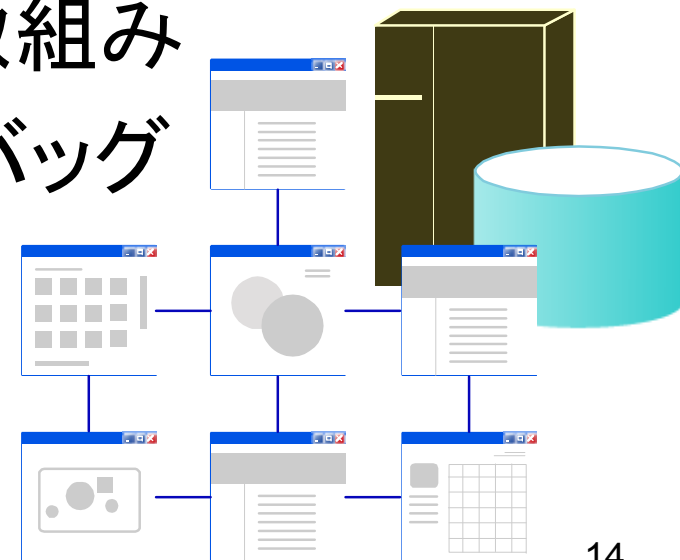
JVN iPedia



MyJVN

# 16項目の取組みの説明 ～企画・開発フェーズ～

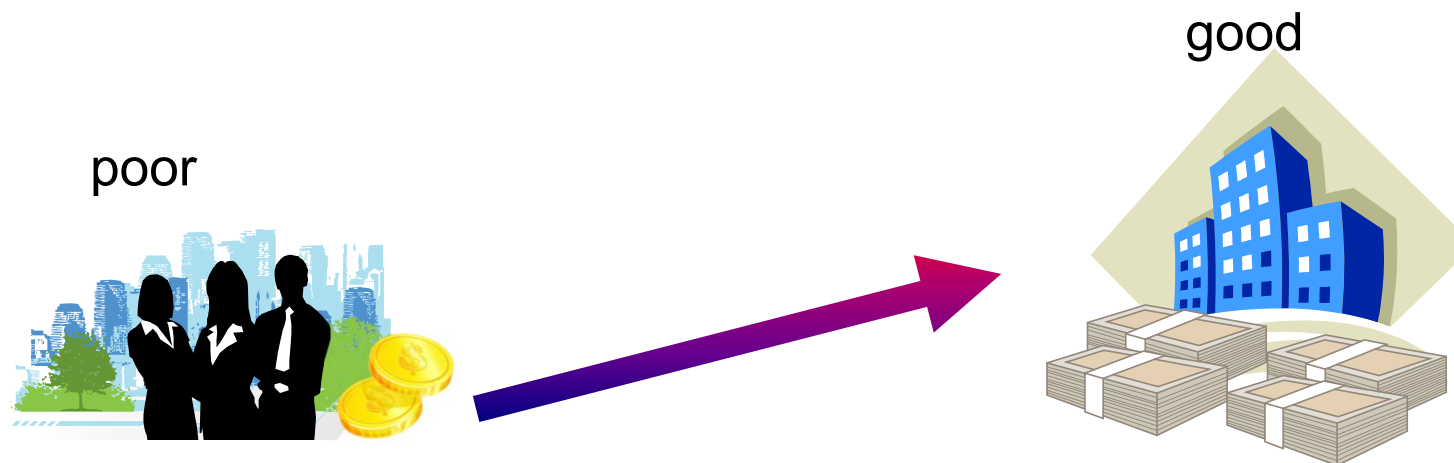
- 予算
- 開発プラットフォーム選定
- 設計
- ソフトウェア実装
- 開発の外部委託における取組み
- セキュリティ評価テスト・デバッグ
- ユーザガイド
- 工場生産管理
- 新技術への対応



# 予算

- 組み込みシステムのライフサイクル全てのフェーズにおいて予算の確保が必要
- セキュリティの問題は事前予測が困難
- リスク回避の観点から全社的かつ継続的なセキュリティ予算を確保

プロジェクトリーダーから要求があった場合に限り予算確保が容認されるのではなく、開発プロセスの一つとしてセキュリティ予算が割り振られていたり、組織にセキュリティ部門を設置することが望ましい。



# 開発プラットフォーム選定

- ハードウェアの選定
  - 基板のデータバス上に機密情報が流れる場合、攻撃者による読み取りを困難なものを選定
  - 機密情報を扱うチップは、端子からプローブされないものを選定
- ソフトウェア(ファームウェア)の選定
  - 組込みソフトウェアパッケージを導入する場合には販売元の脆弱性対策に関するサポート状況を事前確認すること

# 設計

- 該当の組込みシステムが考慮すべきセキュリティ要件を抽出し、各セキュリティ要件に対し、どのような対策を実施するかを検証する必要があります。

## セキュリティ要件の例:

機密情報の保護、障害復旧、サービス機能の保護、ハードウェアへの直接的な攻撃の対策、踏み台攻撃への対策、アラート機能/ロギング機能/廃棄機能の付加 など

設計段階のセキュリティ対策は開発担当者に一任されているのではなく、組織として設計段階で行うべきルールを規定すべき。



# ソフトウェア実装

- 攻撃者はソフトウェア自身の振る舞いを解析する可能性がある  
→ ソフトウェア耐タンパ性の確保
- 攻撃者は想定外のデータをソフトウェアに送り込んで誤動作を引き起こさせる可能性がある  
→ セキュアコーディングと、ツールを用いたソースコードレビューの実施



# 開発の外部委託における取組み

- システムの大規模化と開発コストを抑制するため、システムの一部を外部委託するケースが増加
- 委託先にまったく同じ取組みを求めることは困難
- セキュリティルールを策定して委託することが重要
  - 土台部分の設計を委託する場合、設計ルールや選定基準を明示
  - 取組みが行われていることを確認する手段を設ける
  - セキュリティ対策に関連する研修条件を設定
  - 委託先とのコミュニケーションを密にし、実態に即したセキュリティルールの運用に配慮
  - 問題発生時の責任範囲を契約上で明確化

# セキュリティ評価テスト・デバッグ

- 組み込みシステムに対する代表的な攻撃の対策が行われているか検証すること
  - インジェクション攻撃
  - フォーマット攻撃
  - バッファオーバーフロー
  - DoS攻撃
    - セキュアプログラミングの観点からソースをチェック
  - リバースエンジニアリング
  - サービス用ポート等の悪用
  - サイドチャネル攻撃
    - ハードウェア的な防護が行われているかチェック

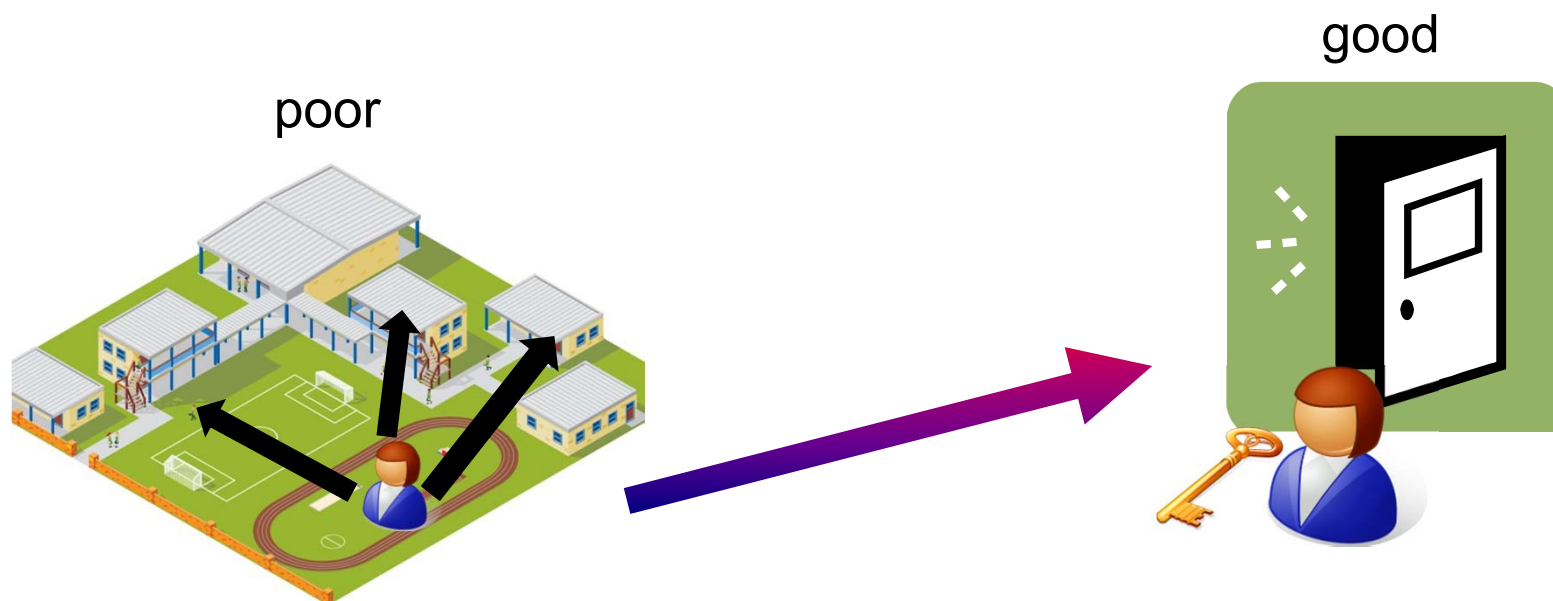
# ユーザガイド

- 脆弱性は運用フェーズに入ってからでも発見される
- 対策に必要な情報はユーザガイドに明記すべき
  - システムをセキュアに使用するためのガイド
    - パスワード設定の手段などと、その手順を実施しなかった場合の問題についての説明など
  - トラブル対応手順
    - セキュリティ問題がおきたときの対処法（電源オフ、リブートなど）
  - 法的な免責事項
  - 対応しているセキュリティ規格
    - 暗号、認証等で採用したセキュリティ規格名

# 工場生産管理

- 組込みシステムは、多くの場合工場で組立てを行う際にソフトウェアの書き込みを実施
- 組立て工程において、情報漏えいやウィルス混入を発生させないための管理が必要

例えば個人情報や機密情報を扱うような場所には、何らかの障壁を設けることが望ましい。具体的には、物理的・ネットワーク障壁、ログ管理、物品管理、中間生成物の管理・廃棄などが考えられる。

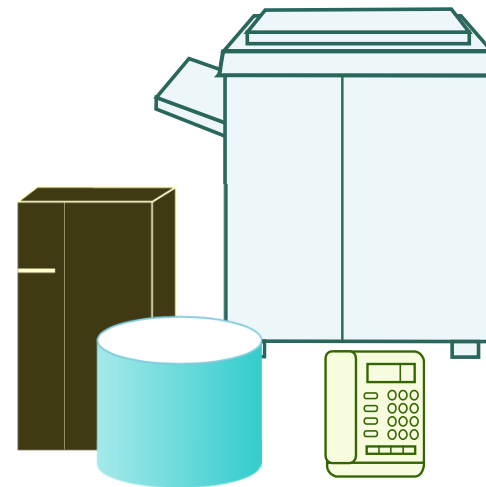


# 新技術への対応

- IPv6やWeb技術などの新技術が取り入れられつつあり、セキュリティに対する備えも必要
  - IPv6
    - グローバルなIPアドレスに対する保護
      - 攻撃に直接さらされる可能性
    - IPv6に特有のアドレス付与方式につけこむ攻撃の対策
      - IPアドレス=ユーザ、MACアドレスが判別可能に
  - Web技術
    - 内蔵Webサーバを用いた設定インタフェース
      - 攻撃者による各種インジェクション攻撃の対策
    - ブラウザ内蔵組み込み機器
      - 接続先URLの表示、ポップアップ抑止、脆弱暗号の利用抑止

# 16項目の取組みの説明 ～運用フェーズ～

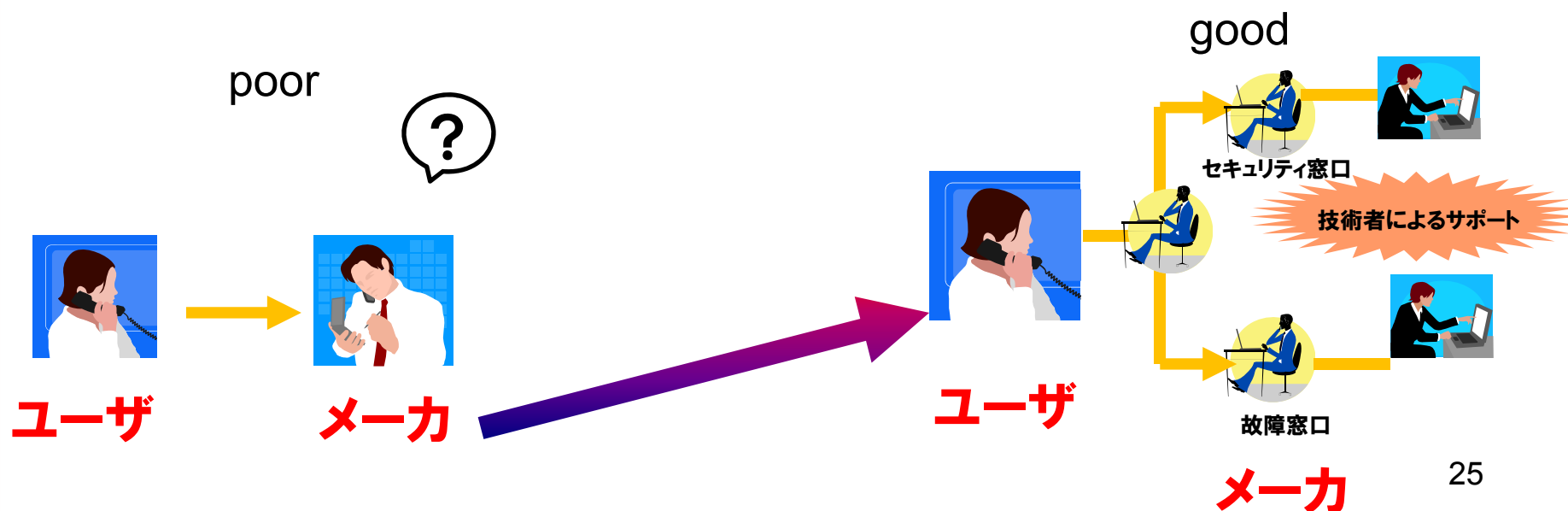
- セキュリティ上の問題への対応
- ユーザへの通知方法と対策方法
- 脆弱性関連情報の活用



# セキュリティ上の問題への対応

- 組込みシステムにセキュリティ上の問題が発見された場合、迅速かつ適切に対応する必要がある

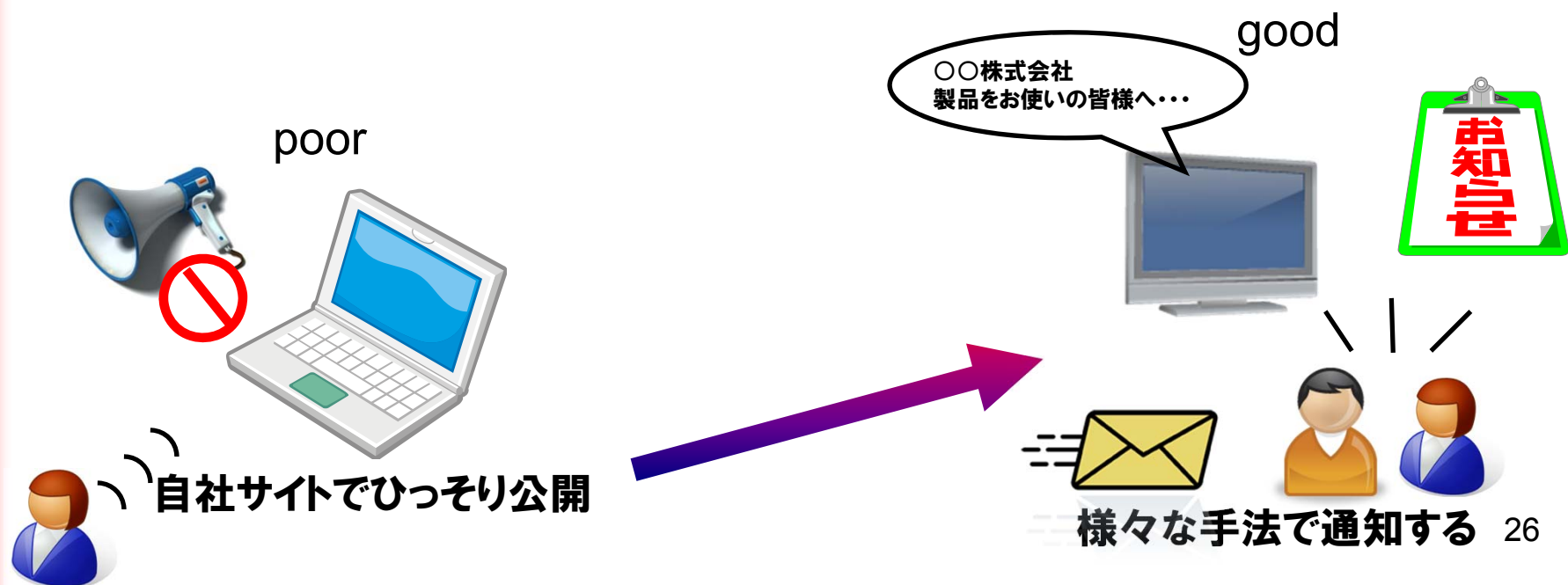
故障が起きた時と同様に、セキュリティ問題へも対応できる窓口の設置が必要  
流通している組込みシステムにセキュリティ問題が発生した時の対応フローや  
関連諸組織との連絡方法を確認すべき。



# ユーザへの通知方法と対策方法

- 脆弱性が発見された場合、脆弱性の程度に応じて、修正プログラムやアップデートの適用・回収・修理が必要になる
- ユーザに通知する方法としては、郵送・電子メール、自社のWebページ・脆弱性対策情報データベース(JVN)などがある

製品の特性を踏まえて、より確実にユーザのもとに届くような方法で通知を行う必要がある。

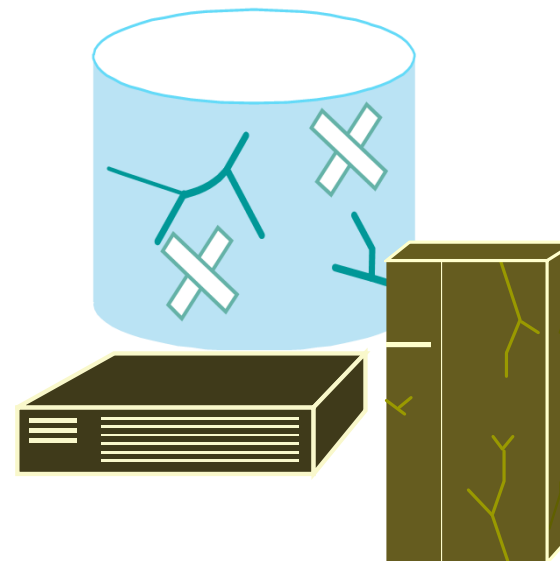


## 脆弱性関連情報の活用

- セキュリティ問題を絶対に起こさせないようにすることは不可能(非現実的)
- 脆弱性関連情報の活用で自社および製品のブランド価値毀損を防止
  - 類似する他社製品での事例より、自社製品の問題を早期に把握
  - 自社での過去事例の対応を教訓とし、次の事故に備える

# 16項目の取組みの説明 ～廃棄フェーズ～

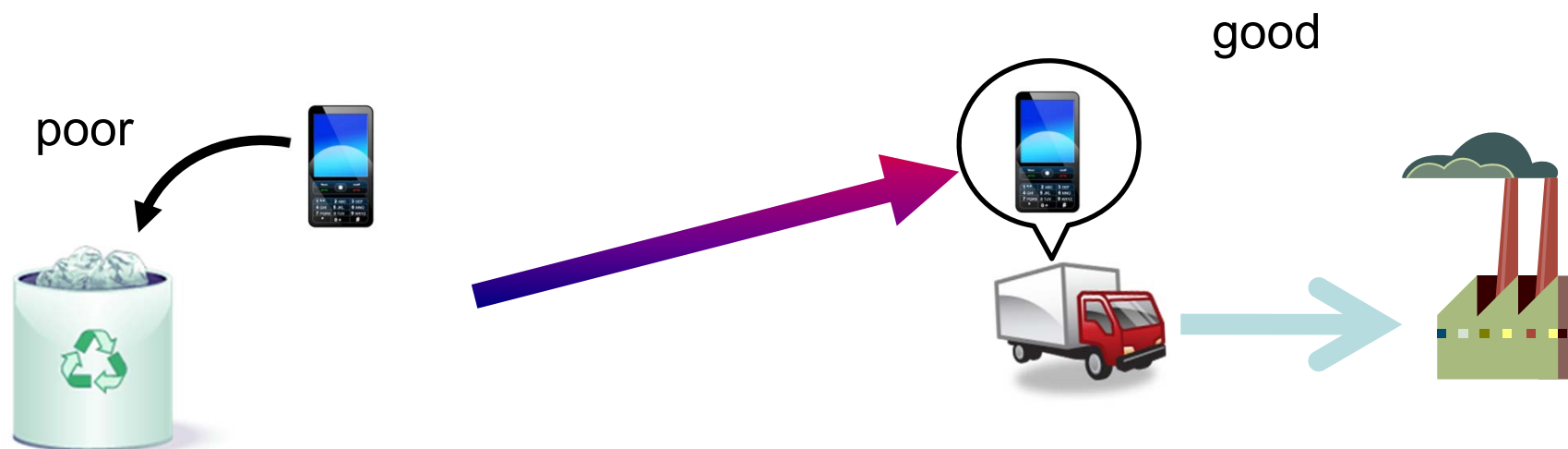
- 機器廃棄方法の周知



# 機器廃棄方法の周知

- 組込み機器は、ユーザが使用することによって個人情報などの機密情報がどんどん蓄積されていきます。廃棄された組込み機器から個人情報等が漏えいしないための仕組みが必要です。

機密情報を守るためには、ユーザが組込み機器を手放す際に簡単にこれらの機密情報を消去できるようにすることが必要。必要に応じて、製品の回収・廃棄には組織的に対応し、活動のための投資を行う必要がある。



## 16項目に対する取組みのレベル

組込みシステムメーカーがセキュリティに取り組むために、セキュリティへの意識、組織内のセキュリティルールの有無、組織の体制などを基準に1～4にレベル分けした。

レベル1: セキュリティ対策は行われていない

レベル2: セキュリティ対策は担当者主導のもと行われる

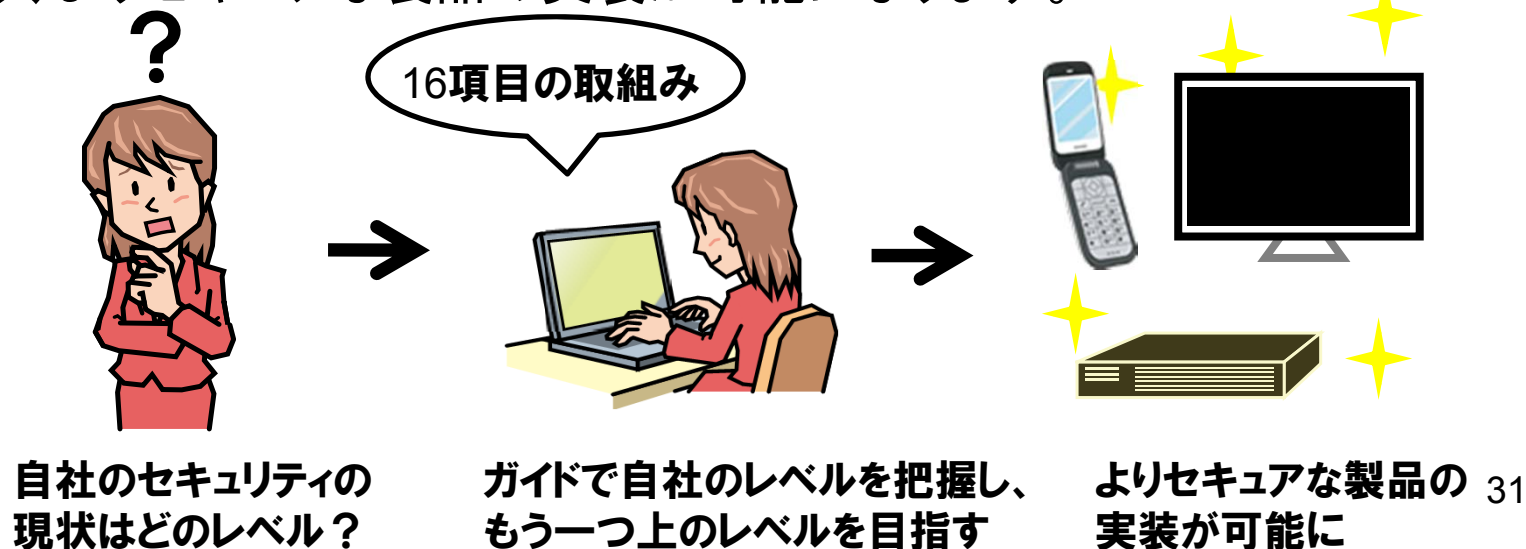
レベル3: 組織としてセキュリティ対策に取り組んでいる

レベル4: 組織としてセキュリティに取り組む、外部からの監査システムがある

# 本アプローチの活用法

私たちは、本アプローチを以下のように使ってほしいと考えています。

- **自組織の把握**: 自組織の「セキュリティへの取組み」と、本アプローチで定義したレベルとを見比べ、現在の自組織のレベルを把握します。
- **上位を目指す**: 今自分がいるレベルから、さらに上位のレベルを目指します。上位のレベルになるほど、より組織的にセキュリティに取り組んでいることになります。
- **よりセキュアな製品**: 組織の「セキュリティへの取組み」のレベルが上がることで、その組織の製品の組込みシステムのセキュリティのレベルも上がり、よりセキュアな製品の実装が可能になります。



# 今後の方向性

IPAは今後・・・

- この成果をさらに多くの方に活用していただけるような取組みを行います
  - 組込みシステムのベンダへのヒアリング等をもとに内容のブラッシュアップを図っていきます
  - セキュリティ対策のためのツールや様々な事例を紹介するなど、組込みシステムのセキュリティレベル向上のための、より具体的な提案をしていきます
- 今後も組込みシステムに関して、関係団体等と協力の下、利用者やメーカー、サービス事業者のセキュリティ対策の向上に向けた活動を行なっていきます。

# 組込みセキュリティに対するIPAの活動

2007年5月10日公開

組込みシステムの脅威と対策に関する  
セキュリティ技術マップの調査研究

2008年1月29日公開

複数の組込み機器の組み合わせに  
関するセキュリティ調査研究

2009年3月10日公開

自動車と情報家電の組込みシステムの  
セキュリティに関する調査研究

2010年4月15日公開

国内外の自動車の情報セキュリティ動向と  
意識向上策に関する調査研究

**組込みシステムセキュリティへの取組み**

2009年6月24日公開、2010年9月7日改訂版公開  
組込みシステムのセキュリティへの取組みガイド

組込みシステムの  
ライフサイクル

企画

開発

運用

廃棄

2006年5月19日公開

現場技術者向け「40のポイント集」  
経営者向け「組込みセキュリティ資料」

報告書(第四版)、検証ツール: 2009年1月8日公開

TCP/IPに係る既知の脆弱性検証ツール

報告書、検証ツール: 2009年4月23日公開

SIPに係る既知の脆弱性検証ツール

2007年4月25日公開

組込みシステムを含んだソフトウェアの  
脆弱性関連情報の受付・蓄積・公開

2007年9月26日公開

セキュア・プログラミング講座

ご清聴ありがとうございました！



本成果はIPAのWebサイトでダウンロードすることができます。

<http://www.ipa.go.jp/security/index.html>

Contact:

独立行政法人 情報処理推進機構

セキュリティセンター

情報セキュリティ技術ラボラトリー

TEL 03(5978)7527

FAX 03(5978)7518

電子メール [vuln-inq@ipa.go.jp](mailto:vuln-inq@ipa.go.jp)

(担当:小林・中野・長谷川)

組込みシステムの  
セキュリティへの取組み  
ガイド(2010年度改訂版)

16個の具体的なチェック項目により、  
自組織のセキュリティレベルを明確にする



2010年9月  
IPA® 独立行政法人 情報処理推進機構  
セキュリティセンター