



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「組み込みシステムのセキュリティへの取り組みガイド」のご紹介

独立行政法人情報処理推進機構 (IPA)

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

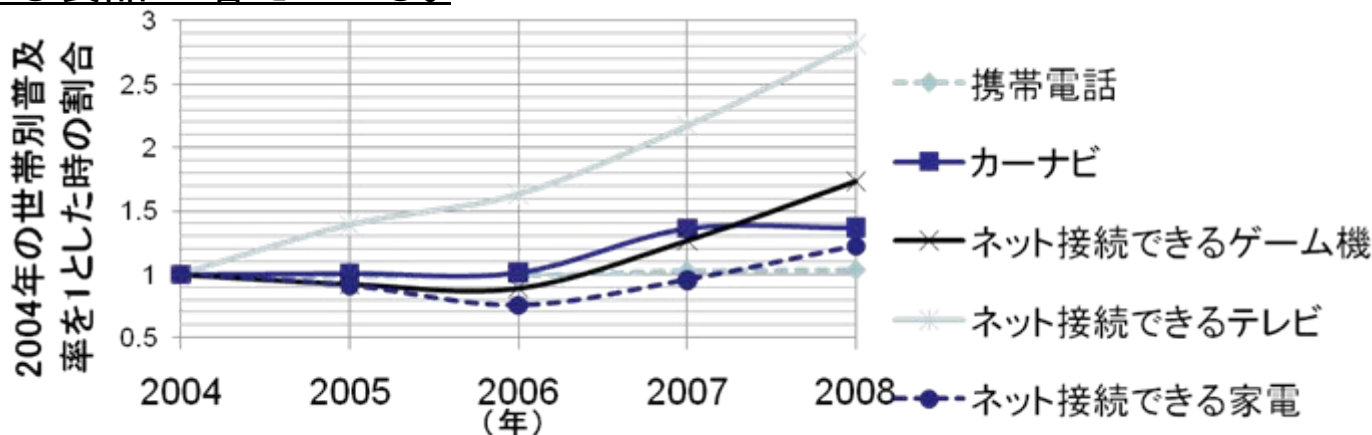
背景

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

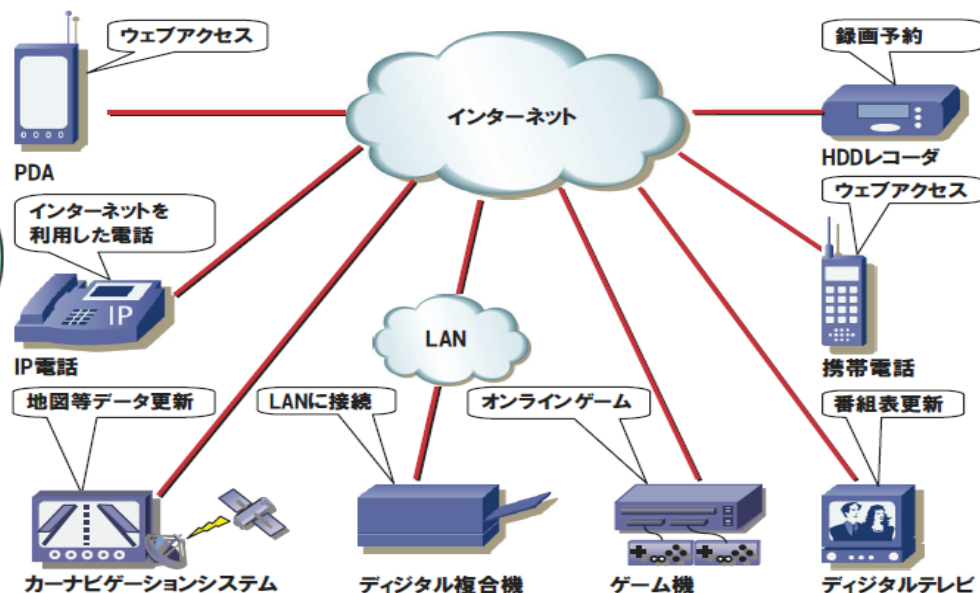
※1経済産業省「2008年度組込みソフトウェア産業実態調査」
 ※2総務省「平成20年度通信利用動向調査」

組込みシステムセキュリティの必要性

なぜ今、組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。

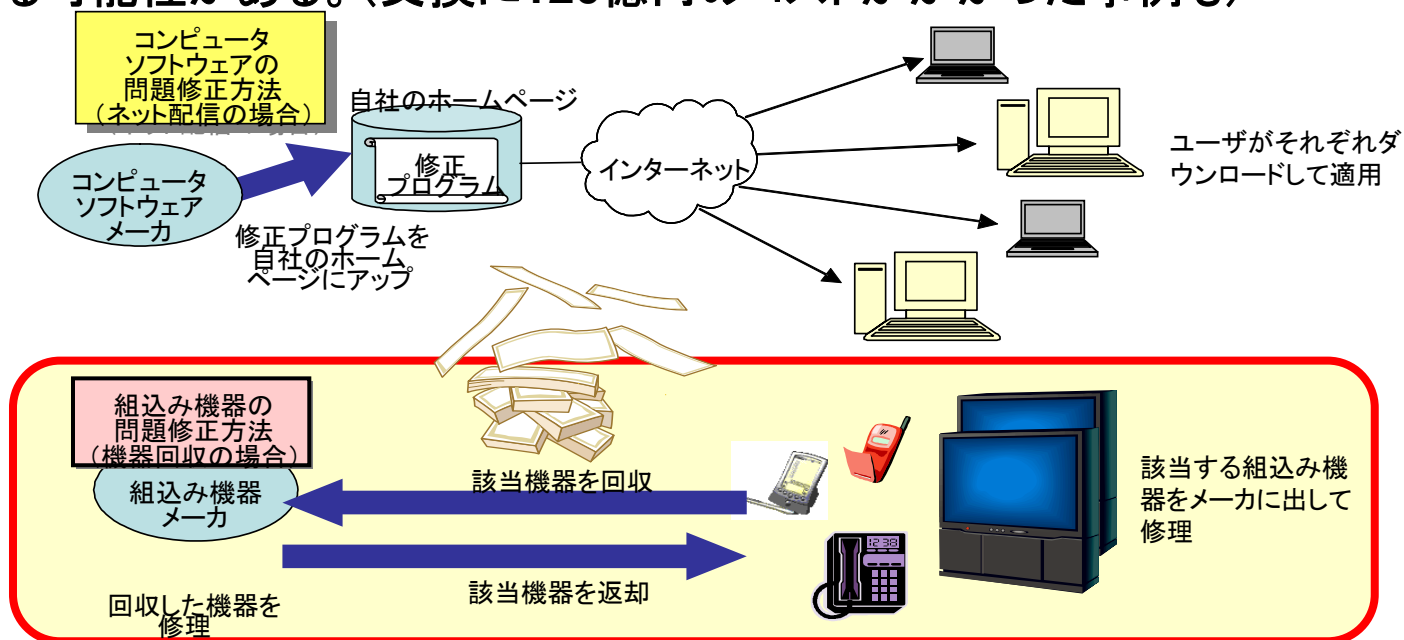
・コスト優先の現状ではなかなかセキュリティにリソースをさけない
・開発者のセキュリティ教育を実施するのも困難



開発者の声

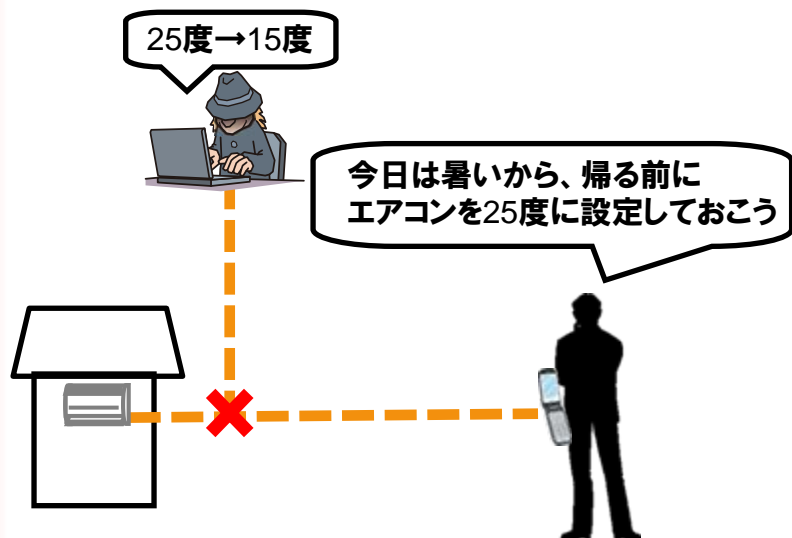
組み込みシステム特有の課題(1/2)

- 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。

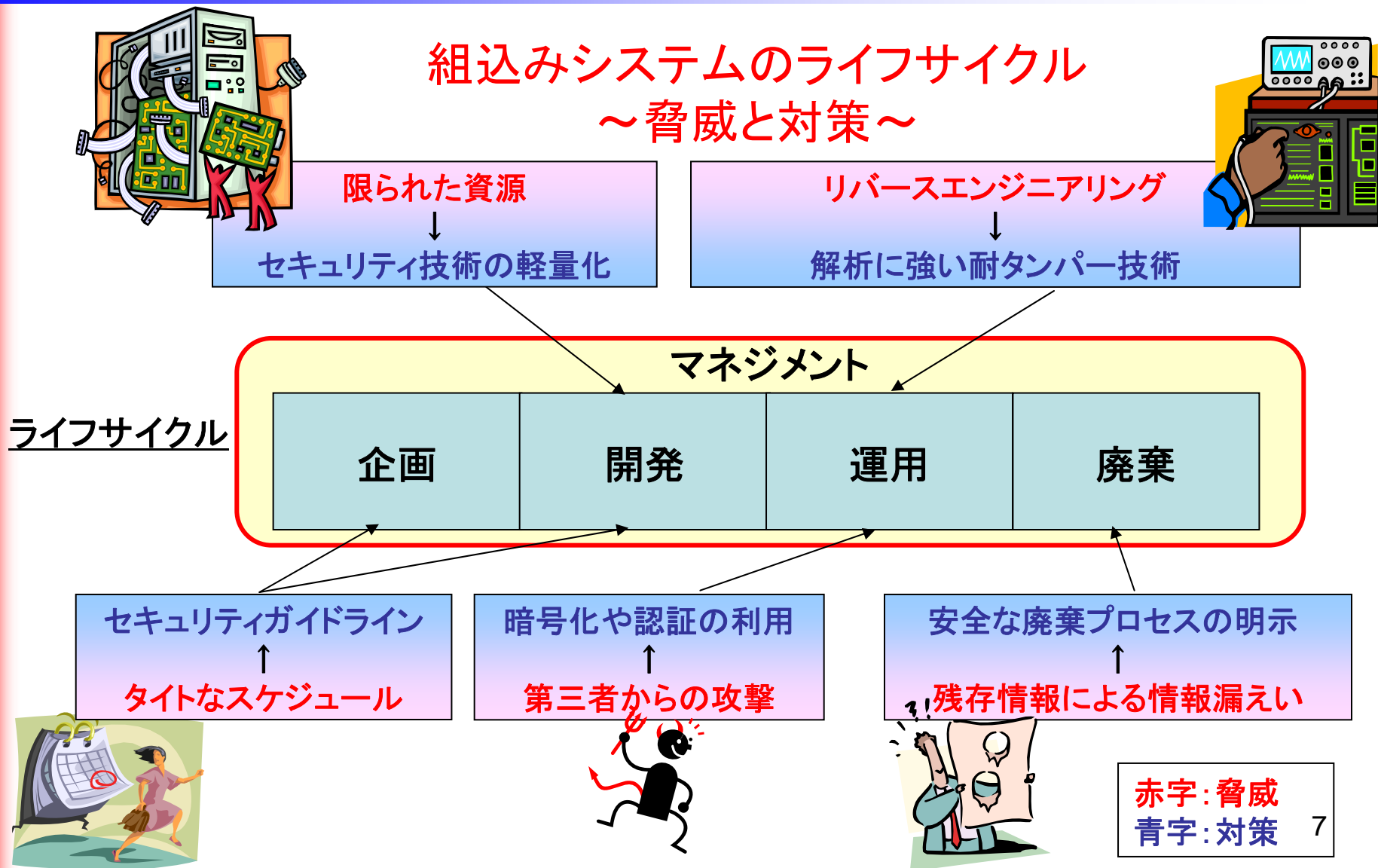
課題を受けて

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、どのような事に取り組めば良いかという指針を示す。**
 - － 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、**具体的な15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。**

セキュリティを考慮すべき15項目 …の前に

組み込みシステムのライフサイクル ～脅威と対策～



セキュリティを考慮すべき15項目

このライフサイクルに基づき、セキュリティを考慮すべき15項目を選定し、それをもとに自分の現状を把握できるようにしました。

マネジメント

セキュリティ関連商品の開発中でなくても、メーカーとして常に行っていなければならないことです。

- 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をしたり、システムの開発を行うフェーズです。

- 予算、設計、開発プラットフォーム選定、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

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ているフェーズです。

- 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

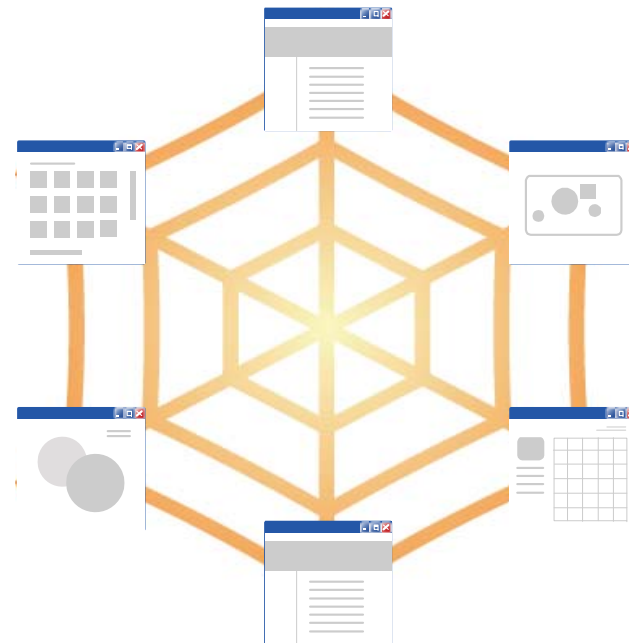
買い替え、故障などで組込みシステムが廃棄、リサイクルされるフェーズです。

- 機器廃棄方法の周知

これらの15項目の内、いくつかをピックアップして説明します。

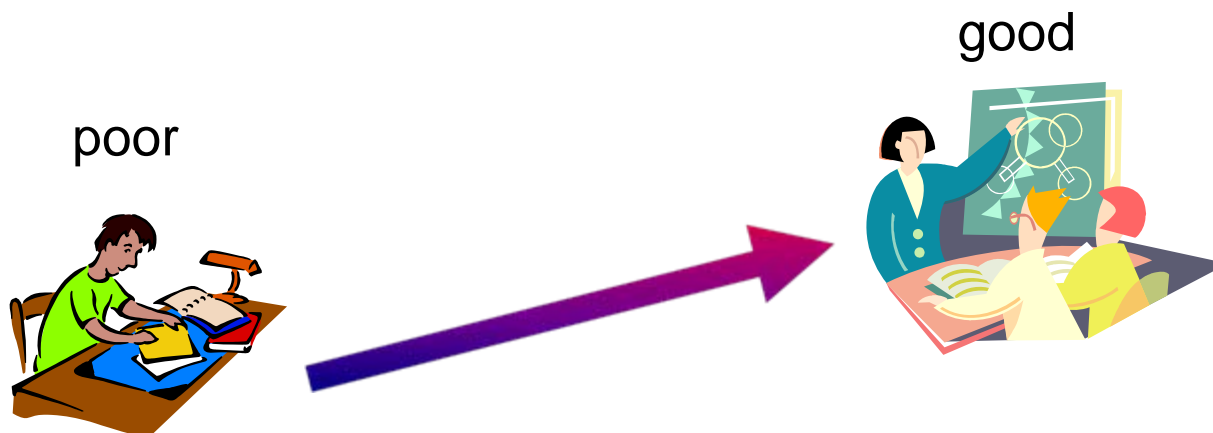
15項目の取組みの説明 ～マネジメントフェーズ～

- 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



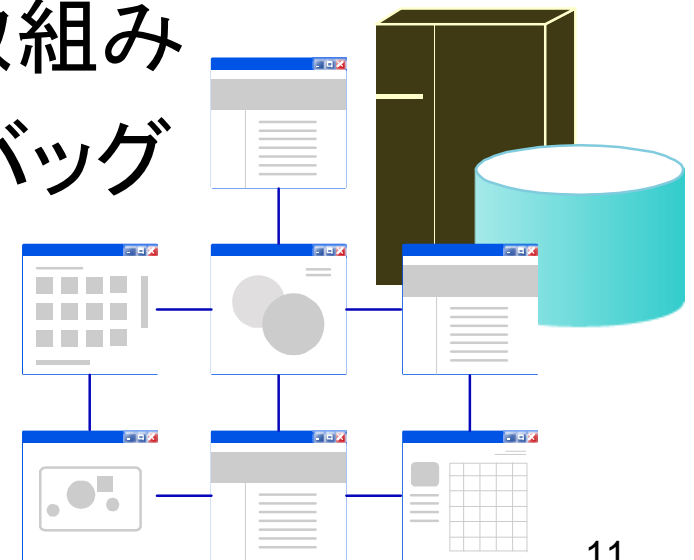
セキュリティ教育

- 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
- 特に、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です。



15項目の取組みの説明 ～企画・開発フェーズ～

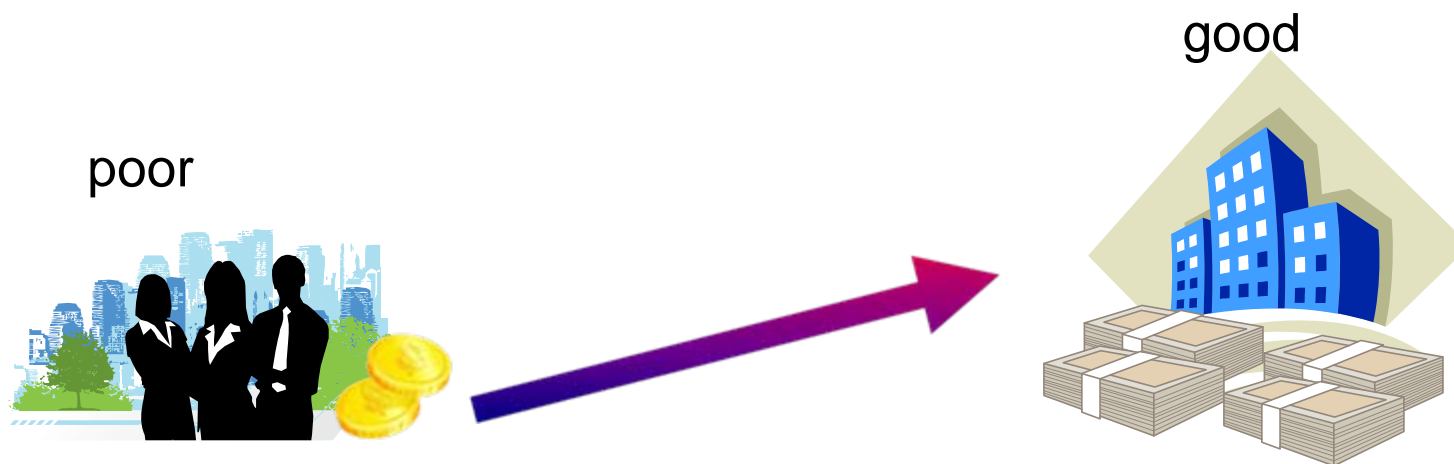
- 予算
- 設計
- 開発プラットフォーム選定
- ソフトウェア実装
- 開発の外部委託における取組み
- セキュリティ評価テスト・デバッグ
- ユーザガイド
- 工場生産管理



予算

- 組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です。
- セキュリティの問題は事前予測が困難です。そのため、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の確保が望まれます。

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といえます。



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:

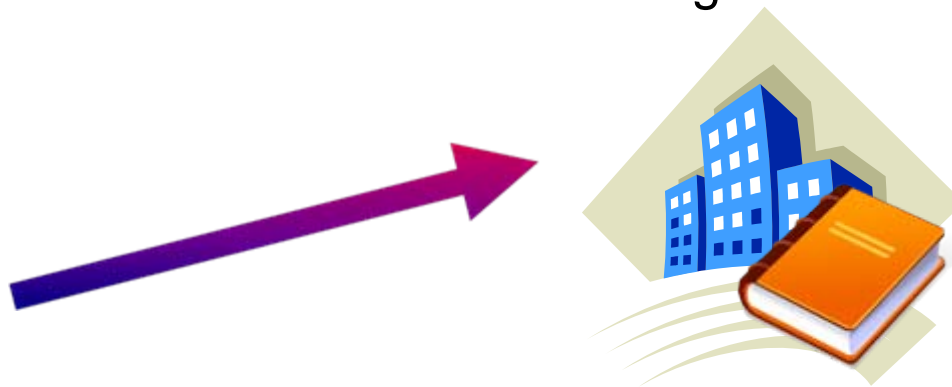
機密情報の流出防止、障害復旧、踏み台攻撃への対策、
アラート機能、ロギング機能、サービス機能 など

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が規定されているのが望ましいと言えます。

poor



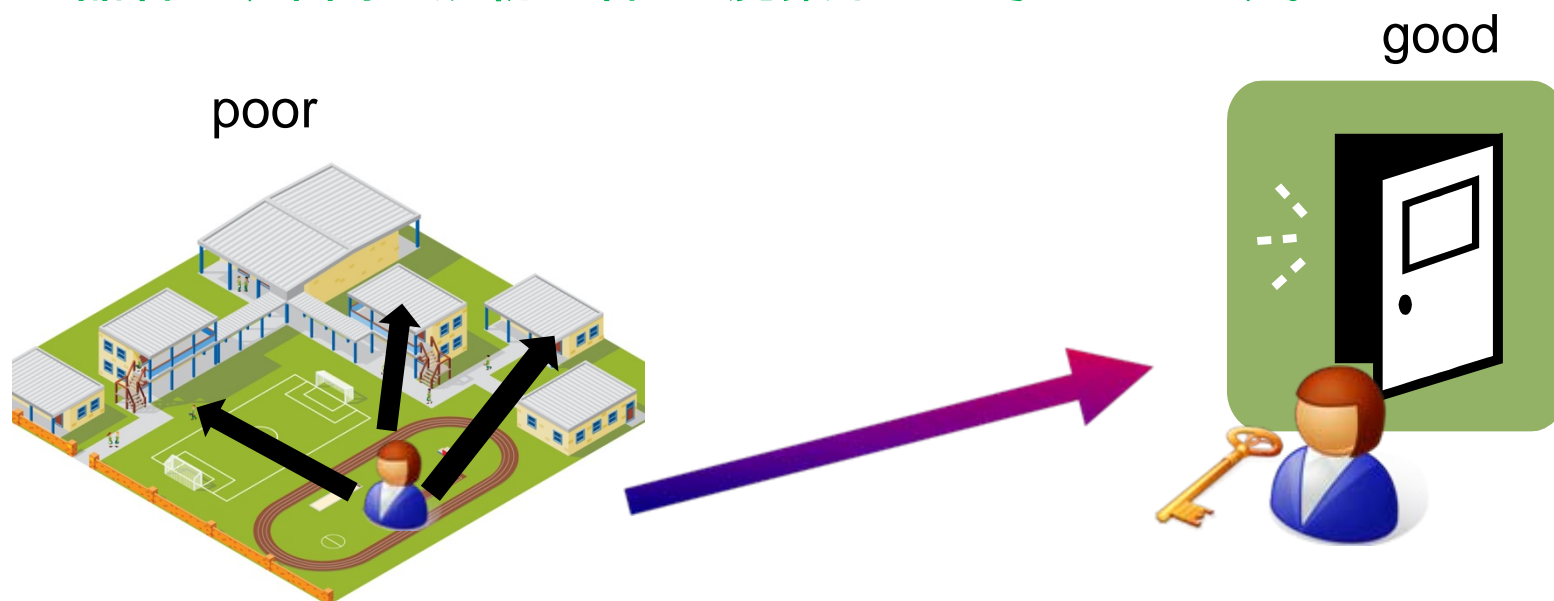
good



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が行われます。組立て工程において、情報漏えいやウィルス混入が発生しないための管理を行う必要があります。

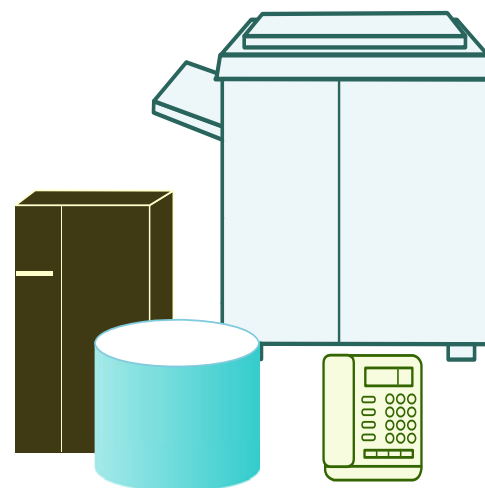
例えば個人情報や機密情報を扱うような場所には、何らかの障壁を設けることが望ましいといえます。具体的には、物理的・ネットワーク障壁、ログ管理、物品管理、中間生成物の管理・廃棄などが考えられます。



15項目の取組みの説明

～運用フェーズ～

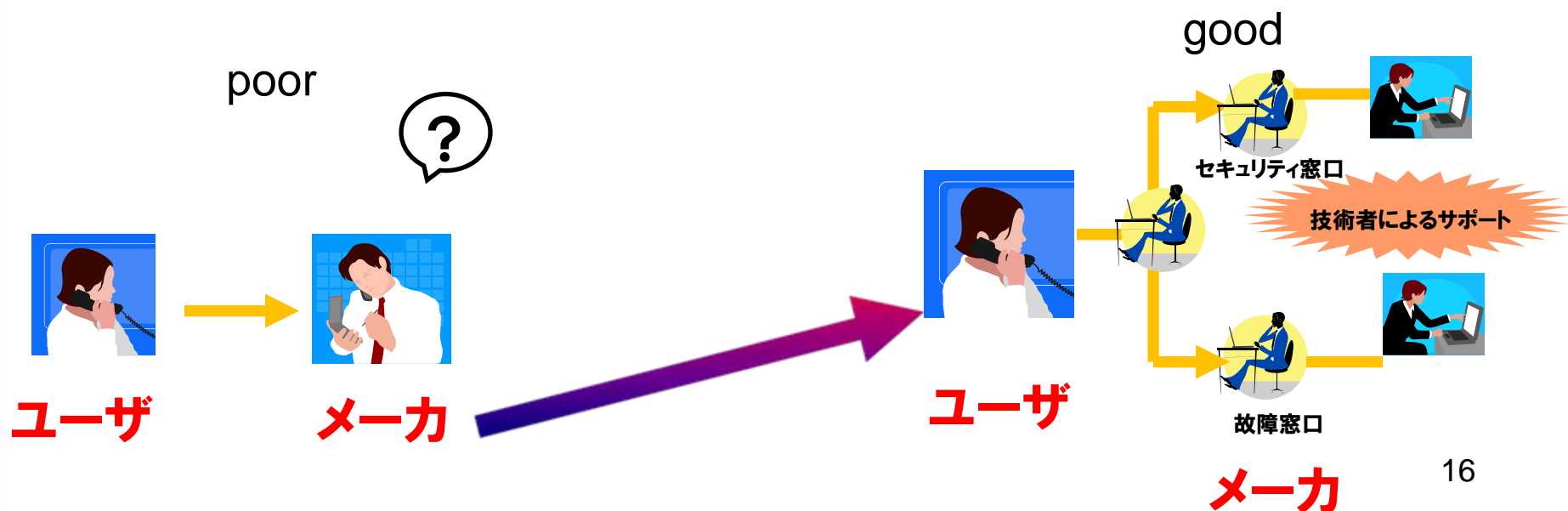
- セキュリティ上の問題への対応
- ユーザへの通知方法と対策方法
- 脆弱性関連情報の活用



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ります。

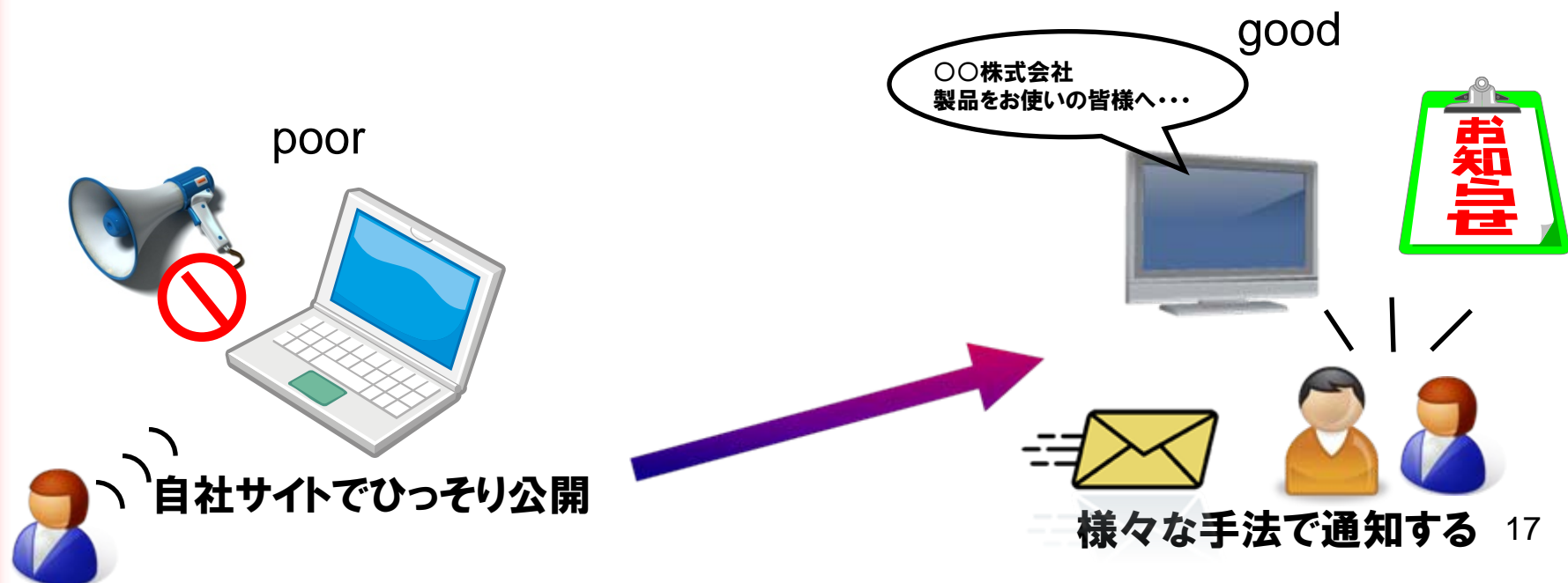
故障が起きた時と同様に、セキュリティ問題へも対応できる窓口の設置が必要です。流通している組込みシステムにセキュリティ問題が発生した時の対応フローや関連諸組織との連絡方法を確認しておきましょう。



ユーザへの通知方法と対策方法

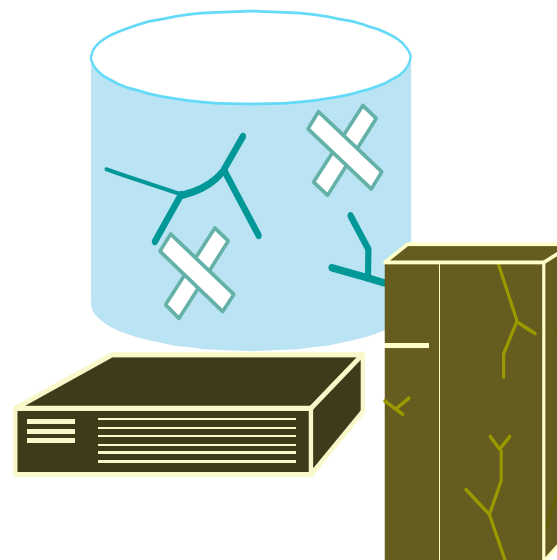
- 脆弱性が発見された場合、脆弱性の程度に応じて、修正プログラムやアップデートの適用・回収・修理が必要になります。
- ユーザに通知する方法としては、郵送・電子メール、自社のWebページ・脆弱性対策情報データベース(JVN)などがあります。

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ります。



15項目の取組みの説明 ～廃棄フェーズ～

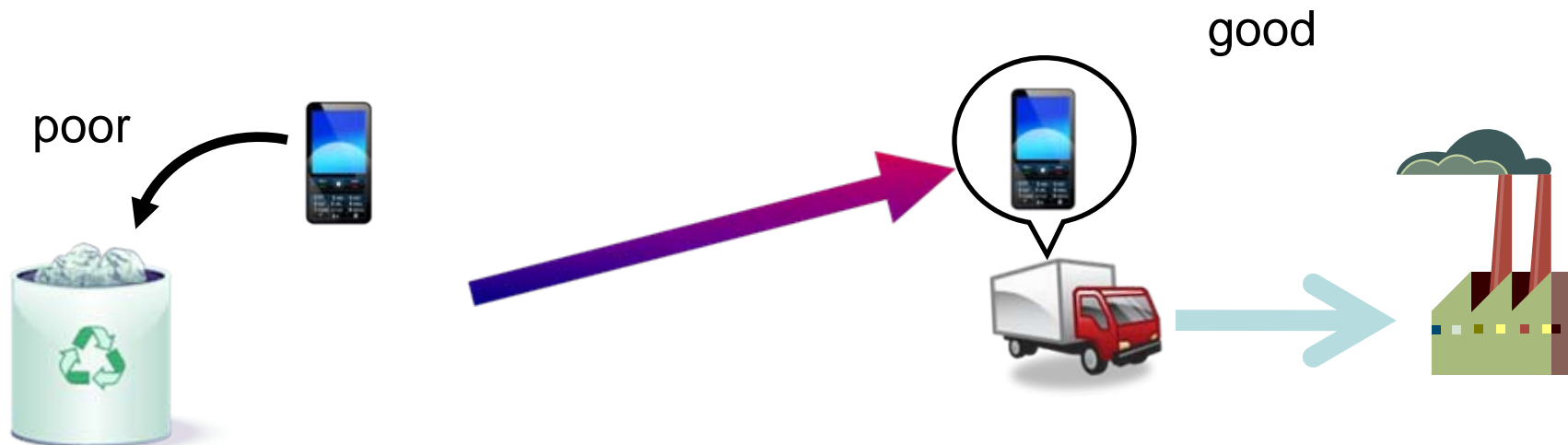
- 機器廃棄方法の周知



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です。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ります。



15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み、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。



自社のセキュリティの現状はどのレベル？



ガイドで自社のレベルを把握し、もう一つ上のレベルを目指す



よりセキュアな製品の実装が可能に 21

今後の方向性

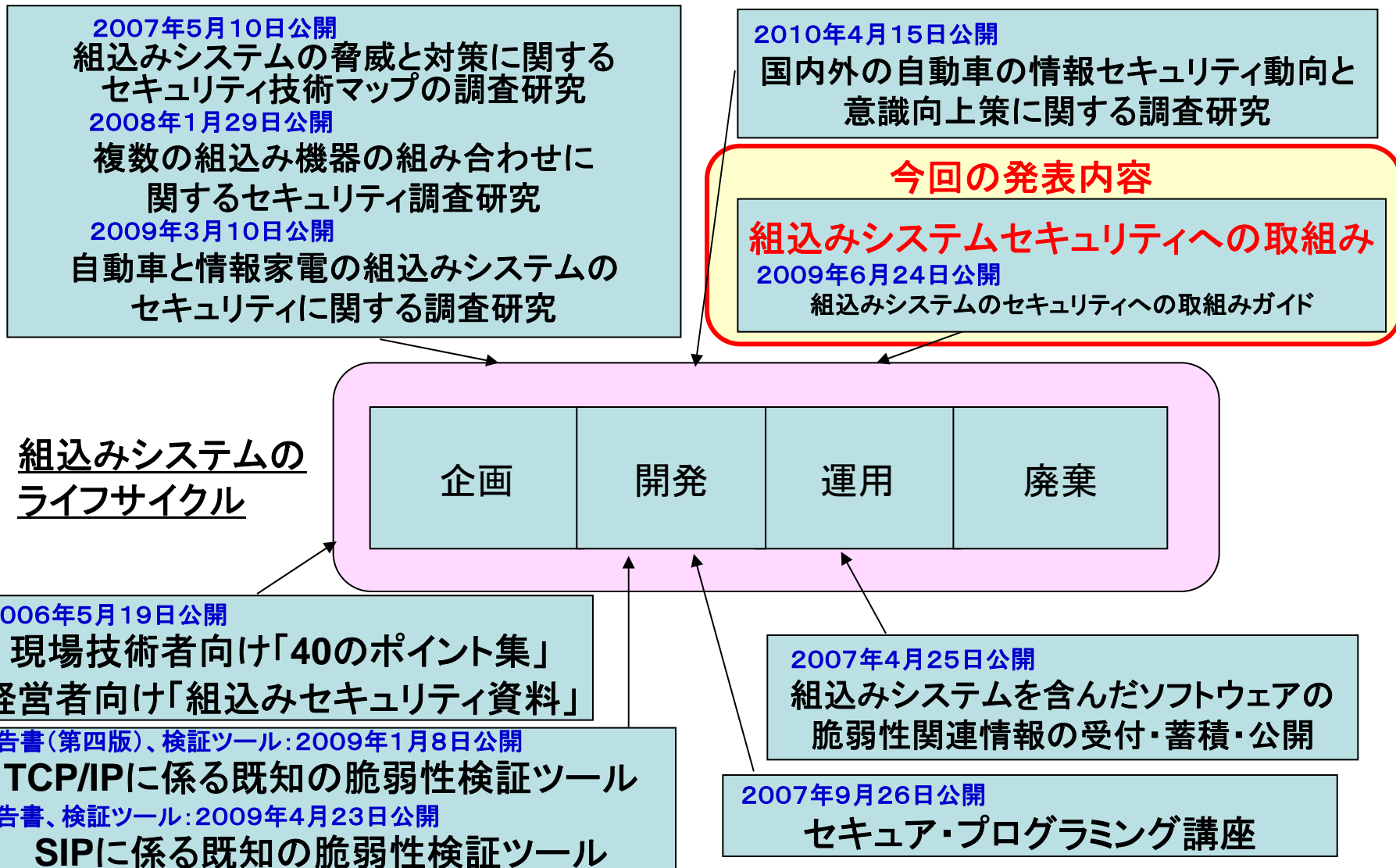
IPAは今後・・・

- 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

2010年夏頃には本内容を更に充実させたガイドの改訂版も発行予定

- 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。

組み込みセキュリティに対するIPAの活動



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>

組込みシステムの セキュリティへの取り組み ガイド

15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



2009年6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

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

(担当: 小林・萱島・中野・長谷川)