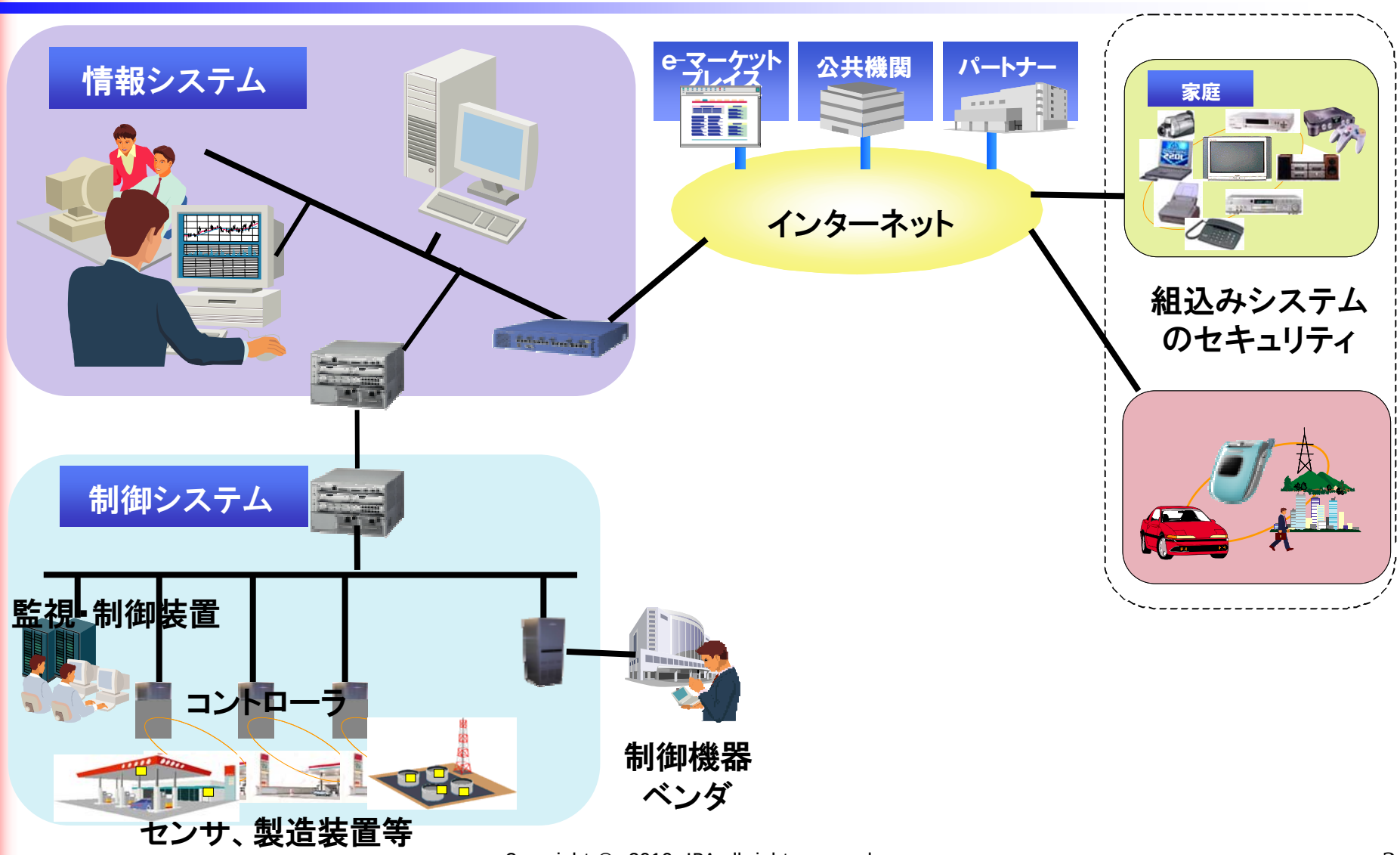
IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

組込みシステムセキュリティの概要

2010年7月22日（木）

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

様々な組込みシステム



身近な組込みシステム

流通を支える組込みシステム

RFID

識別・認証

カーライフを支える組込みシステム

通信サービス

カーナビ・ETC

安心・便利を支える組込みシステム

携帯電話

モバイルを支える
組込みシステム

ICカード

消費を支える組込みシステム

金融端末

情報家電

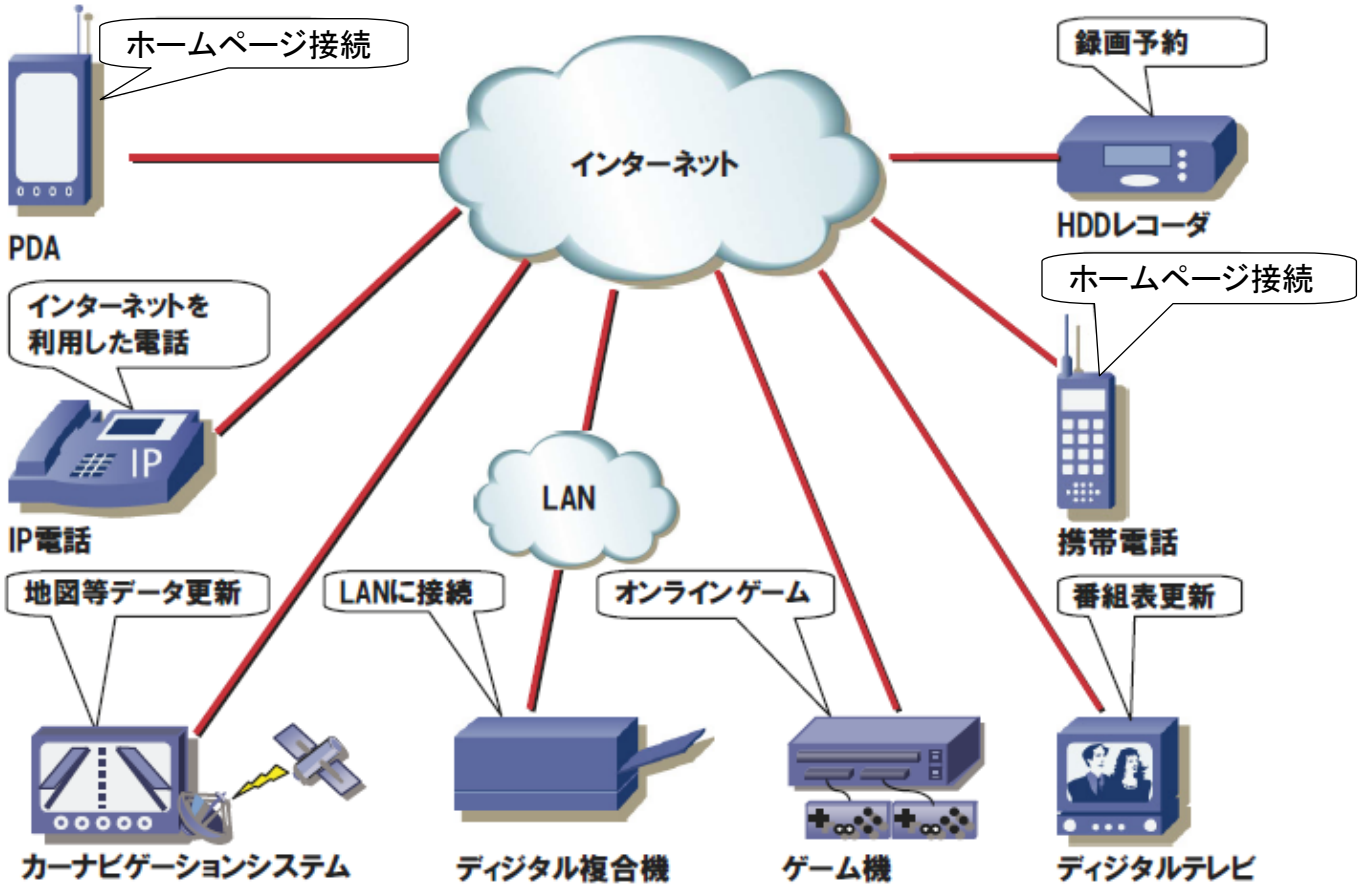
生活を支える組込みシステム

RFID（Radio Frequency IDentification）
ETC（Electronic Toll Collection System）

組込みソフトウェアを用いた機器の現状

ネットワーク機能を備えた組込み機器の例

背景 ： あらゆるものが、ネットワークにつながる



PDA（Personal Digital Assistants）
HDD（Hard Disk Drive）

組込みシステムセキュリティの必要性

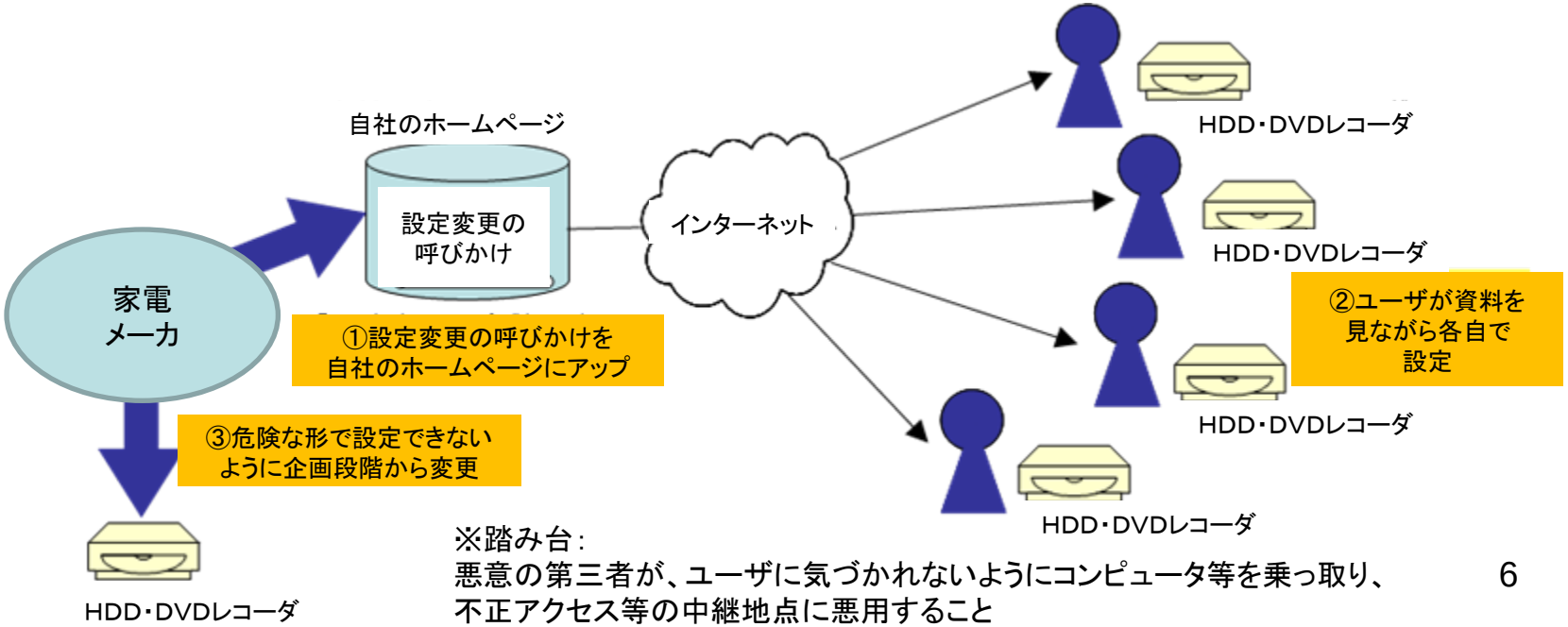
- もしパソコンにセキュリティ対策をしていなかったら・・・
  - ウィルス等のマルウェアへの感染
  - 悪意あるユーザの攻撃による被害

- PCの場合の対策例
  - アンチウィルスソフトウェアの導入
  - セキュリティファイアウォールの利用
  - セキュリティパッチのダウンロード・適用

組込みシステムにおいて同じような対策は出来ているでしょうか？

情報家電分野のインシデント事例

- **踏み台※にされる可能性のあった、ハードディスクレコーダ**
  - インターネット対応のハードディスクDVDレコーダをインターネット上に接続すると、anonymous proxyとして動作してしまう脆弱性が発覚
  - メーカ側では、想定した利用環境以外でのネットワーク利用を想定できていなかった
  - 対策として、修正版へのソフト更新（バージョンアップ）もしくはセキュリティ設定の変更を行うよう、当該機器のユーザに呼びかけた



※踏み台：
悪意の第三者が、ユーザに気づかれないようにコンピュータ等を乗っ取り、不正アクセス等の中継地点に悪用すること

自動車分野のインシデント事例（1/2）

車載システムへの攻撃で自動車が制御不能に、研究者がセキュリティ問題を指摘

攻撃者が自動車の電子制御システムに侵入すれば、ブレーキを効かなくさせたり、逆にブレーキを強制して車を急停止させたりすることができてしまう。

2010年05月19日 08時13分 更新　[ITmedia]

停車中にもかかわらず速度計に偽の速度と任意のメッセージを表示できてしまったという（出典:「Experimental Security Analysis of a Modern Automobile」）

例えばシステムに悪質なコードを仕込むといった手口で自動車の電子制御ユニット（ECU）に侵入すれば、さまざまな安全システムの動作を妨害し、ブレーキを効かなくさせたり、エンジンを停止させたりできる。攻撃者が自動制御機能を操って運転手が車を停められないようにしたり、逆にブレーキを強制して車を急停止させることができてしまうことを実証したという。

自動車分野のインシデント事例(2/2)

ディーラーのシステムへ不正侵入、車100台を動けなくした元従業員を逮捕

これはパスワードのセキュリティの大切さを物語る事件であり、企業にとって学ぶべき教訓は多いとSophos研究者が指摘する。

2010年03月19日 08時54分 更新　[ITmedia]

米テキサス州で2月に解雇された20歳の自動車ディーラー元従業員がコンピュータシステムに侵入し、遠隔操作で100台以上の車を動けなくしたとして警察に逮捕された。顧客のローン支払いが滞った場合に使われるWebベースシステム「WebTeck Plus」に侵入した疑いがかけられている。このシステムはディーラーが販売した車に小さなボックスを取り付けて、遠隔操作でエンジンに点火できなくしたり、警笛を鳴らしたりできる仕組みになっていた。2月下旬の5日間で100人以上の顧客が被害に遭い、エンジンがかからなくなってけん引車を呼んだり、バッテリーを取り外したりする羽目になったとされる。ディーラーはこの男が解雇された時点でユーザーネームとパスワードを無効にしていたが、男は別の従業員のアカウントを使ってシステムにアクセスしていたとみられる。

制御システム分野のインシデント事例(1/2)

- ワームによる自動車工場の操業停止
  - 2005年8月18日、ダイムラー・クライスラー（現ダイムラー）の米国にある13の自動車工場が単純なインターネットワームによって操業停止。情報ネットワークと制御ネットワークの間にはファイアウォールが設置されていたにも関わらず、プラント中に広まった。

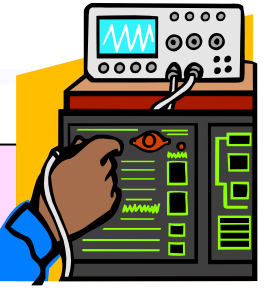
    ＃外部から持ち込まれ、制御システムに接続されたノートPC経由で＃感染したという可能性も。。。
  - 50,000人の労働者の作業が中断され、自動車生産が50分間停止した後、システムにパッチをあてることで生産を再開したが、周囲への感染に対する懸念も生じ、およそ1,400万＄の損害が発生。

制御システム分野のインシデント事例(2/2)

- ワームによる自動車工場の操業停止
  - 2003年1月、オハイオ州の原子力発電所でマイクロソフトのSQLサーバを狙ったSlammerワームがVPN接続を介して侵入・感染し、SCADAシステムを約5時間にわたって停止させた。
  - 発電所のサーバはファイアウォールで外部ネットワークと遮断されていたが、ファイアウォール内部のネットワークに接続した、発電所のコンサルタント会社の端末が感染源となった。
  - Slammerワームに対するパッチは、インシデント発生時点で公開されていたが、発電所のシステムには当該パッチがあてられていなかった。

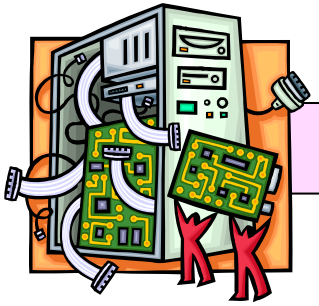
このような事が発生しないように、また発生した場合においても速やかな対応が出来るように、組込みシステムにおける課題を認識しておくことが必要。

具体的なセキュリティ課題



利用者(ユーザ)が攻撃者になる

リバースエンジニアリング



リソースの制約

情報資産の改竄・漏洩

組込みシステムのライフサイクル

企画 | 開発 | 運用 | 廃棄

セキュリティ課題の混在

脆(ぜい)弱性の作りこみ

個人情報の漏洩

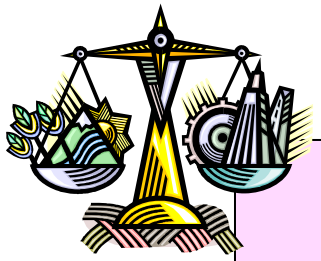
企画書の漏洩

情報漏えいのようなインシデントの発生

リバースエンジニアリング:
機械を分解したり、ソフトウェアを解析するなどして、製品の構造を分析し、そこから製造方法や動作原理、ソースコードなどを調査する事

具体的なセキュリティ対策

耐タンパー性付与等の
システム解析(攻撃)への耐性強化



低リソースで利用できる
セキュリティ技術の普及

暗号・認証の利用

組込みシステムの
ライフサイクル

企画	開発	運用	廃棄

セキュリティ対策
ガイドラインの策定

セキュアプログラミング
セキュリティ検証

廃棄方法の周知

一環したセキュリティ対策

インシデント対応方法体制の確立

組込みシステム特有の課題

- 背景
  - ICカード、携帯電話、情報家電、自動車関連機器など、組込みシステムの利用者は多岐にわたり、PCの利用者と同様のリテラシーが期待できない。また、PCに比べて長期間利用される傾向のものが多い。
    - 中長期的な視点から、組込みシステムにおける情報セキュリティ対策の検討及び情報セキュリティ対策の作りこみに資する情報提供が必要。
  - 組込みソフトウエアの情報セキュリティ事象が、製造物の問題となる可能性が考えられる。しかし、組込みシステム開発者の情報セキュリティに対する意識は必ずしも十分とはいえない状況にある。
    - パソコンにおける常識と組込みシステムにおける常識に差がある可能性も。
    - 組込みシステムの技術者に対する情報セキュリティ対策の底上げに資する総合的な情報提供が重要。

安全な組込みシステム社会にむけて

- 課題解決に向けた提案
  - 組込みシステムの特徴（省電力、低リソース、等）を考慮した上で、従来の情報システムのセキュリティインシデントやその対策についてのセキュリティに関する考察
  - 組込みシステム間の相互接続や融合時の複合的な環境でのセキュリティに関する考察
  - 利用者の個人情報、金銭被害に繋がる情報、さらに人命に繋がる情報等、取扱う情報資源の特徴の観点を考慮に入れた考察
  - 組込みシステム開発者・技術者のセキュリティを含めた意識共有の為の活動

様々な観点から課題を検討し、組込み開発者やユーザ、事業者、セキュリティ研究者といった組込みシステムに係る方々の連携で、課題の解決に向けて取り組む必要がある。

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
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
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
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

2009年6月24日公開
組込みシステムのセキュリティへの取組みガイド
2009年11月25日公開
上下水道分野用のSCADAセキュリティ グッド・プラクティス

2009年3月30日公開
重要インフラの制御システムセキュリティと
ITサービス継続に関する調査
2009年3月30日公開
制御システムセキュリティの信頼性と
推進施策に関する調査

**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事ができます。
http://www.ipa.go.jp/security/index.html

Contact：
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
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）