



組込みシステムセキュリティへの取組み ～自動車の情報セキュリティ～

2010年12月
独立行政法人 情報処理推進機構
セキュリティセンター

脅威の現状

インターネットの環境は大きく変化している
攻撃(悪意)の動機も変化している

<初めの頃は>



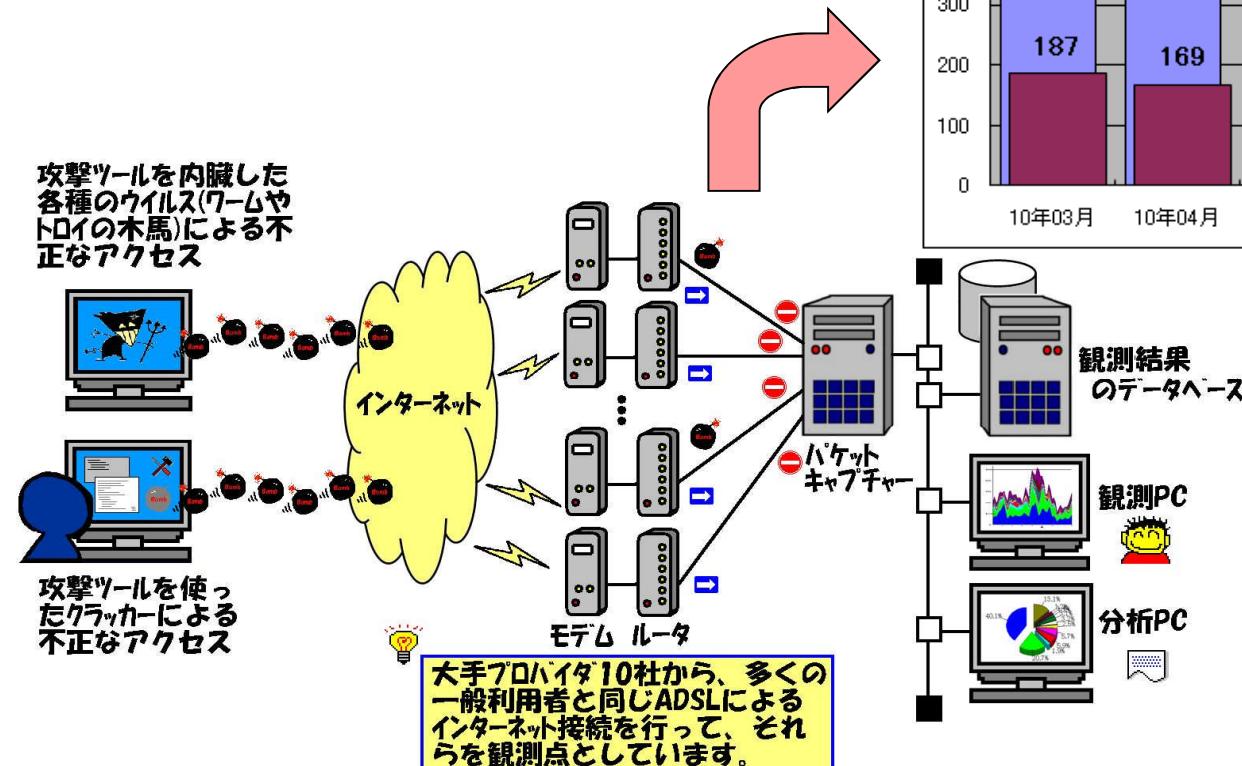
いたずら



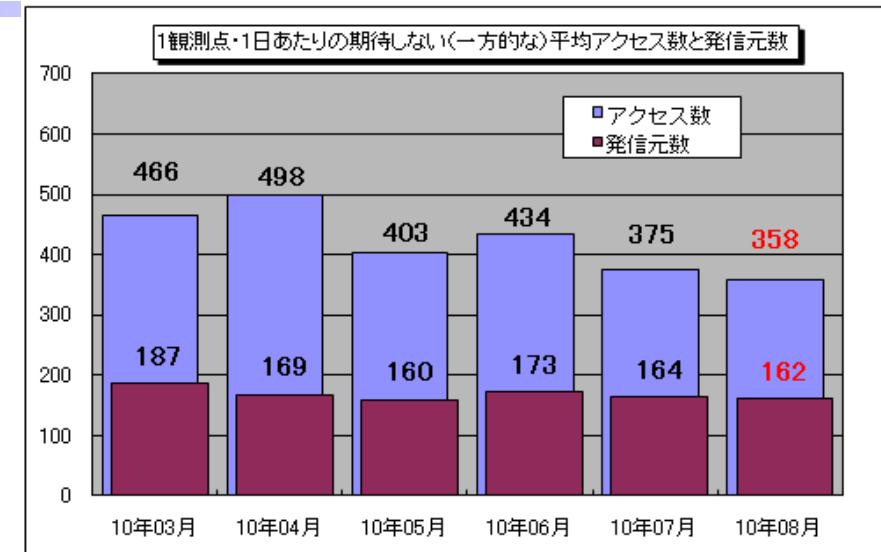
金銭・犯罪・テロ・情報戦

期待しないアクセス

**2010年8月の期待しないアクセスは、
1日あたり162の発信元から358件の
アクセスがあった**



1日あたりの期待しないアクセス数及び発信元数



**約4分ごとに
誰かがあなたの
パソコンを
のぞいている。**

インターネット定点観測TALOT2の仕組み

多様化する脅威



「不安解消」、「安心・安全の確保」に対する社会的ニーズ増大

サイバー攻撃の変容

IPA®

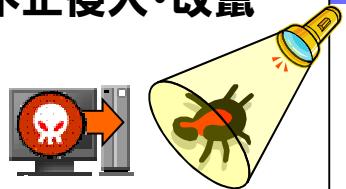
2000

2004~

2006~

2009~

不正侵入・改竄



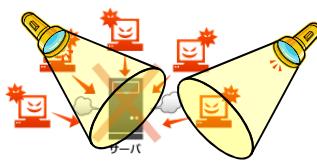
1脆弱性=1攻撃の時代

PCとホームページ改竄がターゲット

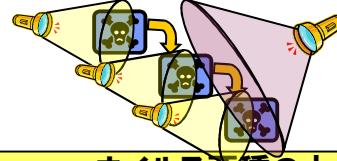


攻撃者ひとり

体系化(Botnet)



多段化
(Botnet技術基盤利用)



正規サービスの
攻撃基盤利用

正規サイト・サービス利用

ウイルス亜種の大量出現
シーケンシャルマルウェア(多段型攻撃)
0-Day脆弱性利用
toolによるウイルス生産
情報システムがターゲット

攻撃組織間連携



戦術的攻撃

多様な意図性(情報搾取攻撃)

PCの破壊・HP改竄

対象:PC、サーバ

影響(業務インパクト)の変化

情報搾取等

e-マーケットビジネス、決済等への影響
決済関連情報搾取等、サプライチェーン
危機管理

対象:情報システム(組織・ビジネス)

セキュリティ製品でカバー(製品の出現)
製品を置く設計思想

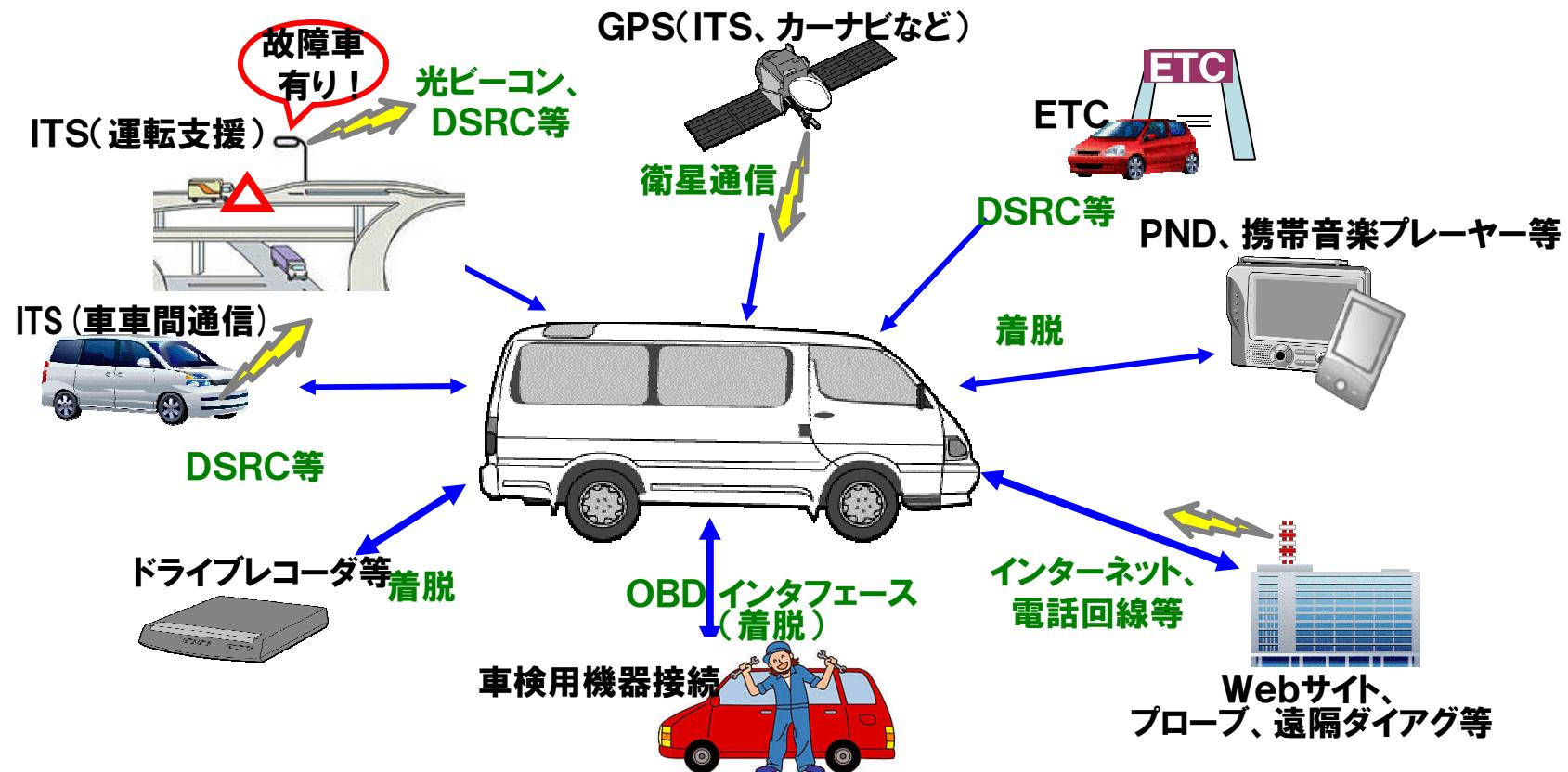
出展:亀山社中

?
設計思想を変
化させないと...

脅威全貌とポイントが見えにくい時代
一定の情報運用で守る時代(情報連携)
皮を切られても肉まで切られない発想設計
システム・ネットワークトポロジ設計で防御

ネットワークで広がる自動車の世界

- 自動車の全体像が分からない
 - 何がつながるか、どのような情報が来るか、それらは信頼できるか
 - どのような情報が出て行くか、どのように利用されるか

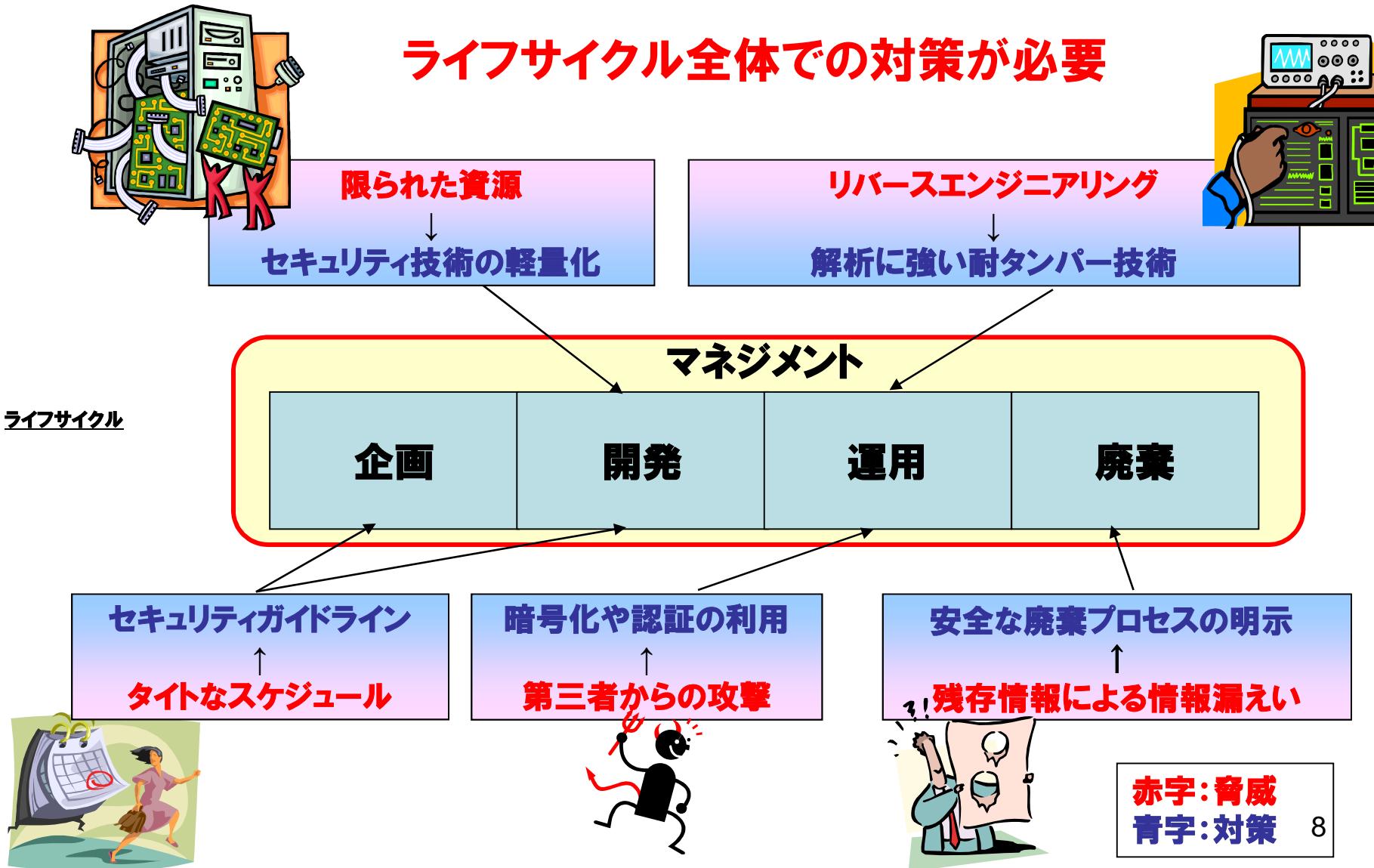


組込みシステムセキュリティの特殊性

- 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
- もしパソコンにセキュリティ対策をしていなかつたら…
 - 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

組込みシステムにおいては、開発環境や製品の特徴等の違いから、PCと同じような対策を実施するのは困難。

製品に対するセキュリティ対策の基本



事例から見る自動車の情報セキュリティ



自動車に対する実験的なセキュリティ分析

論文: Experimental Security Analysis of a Modern Automobile
<http://www.autosec.org/publications.html>

実験環境

2台の車を購入といくつかのECU購入

- A ベンチマークテスト
- B 静止した車への実験
- C 路上実験

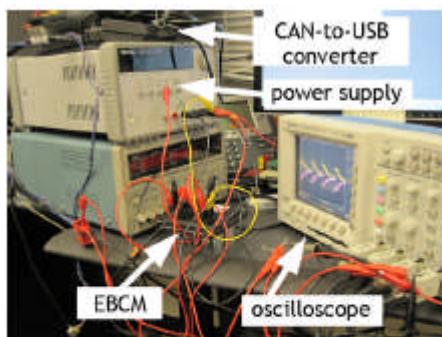


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (EBCM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.



Figure 3. To test ECU behavior in a controlled environment, we immobilized the car on jack stands while mounting attacks.



Figure 7. Road testing on a closed course (a de-commissioned airport runway). The experimented-on car, with our driver wearing a helmet, is in the background; the chase car is in the foreground. Photo courtesy of Mike Haslip.

自動車内無線ネットワークのセキュリティとプライバシー脆弱性 タイヤ空気圧警報システムTire Pressure Monitoring Systemのケーススタディー

IPA®

Security and Privacy Vulnerabilities of In-Car Wireless Networks

: A Tire Pressure Monitoring System Case Study

<http://www.privacylives.com/wp-content/uploads/2010/08/rfid-tire-pressure-2010-002-tpms.pdf>

ノースカロライナ大学のコンピュータ・サイエンス・エンジニアリング部と、Rutgear大学のWINLABの9人の研究者

TPMS概要と目標

各タイヤのバブル裏手にセンサー、
アンテナ、ECU、受信装置、
ダッシュボードTPM警告ライト、

TPMセンサーは定期的に、ID付で圧力と温度
データをブロードキャスト。

2000年フォード社が使用していたファイアーストーンのタイヤ事件をきっかけ。米国や欧州で搭載が義務付けられたタイヤ・プレッシャー・モニタリング(TPMS)。車載が義務付けられたワイヤレスネットワーク。

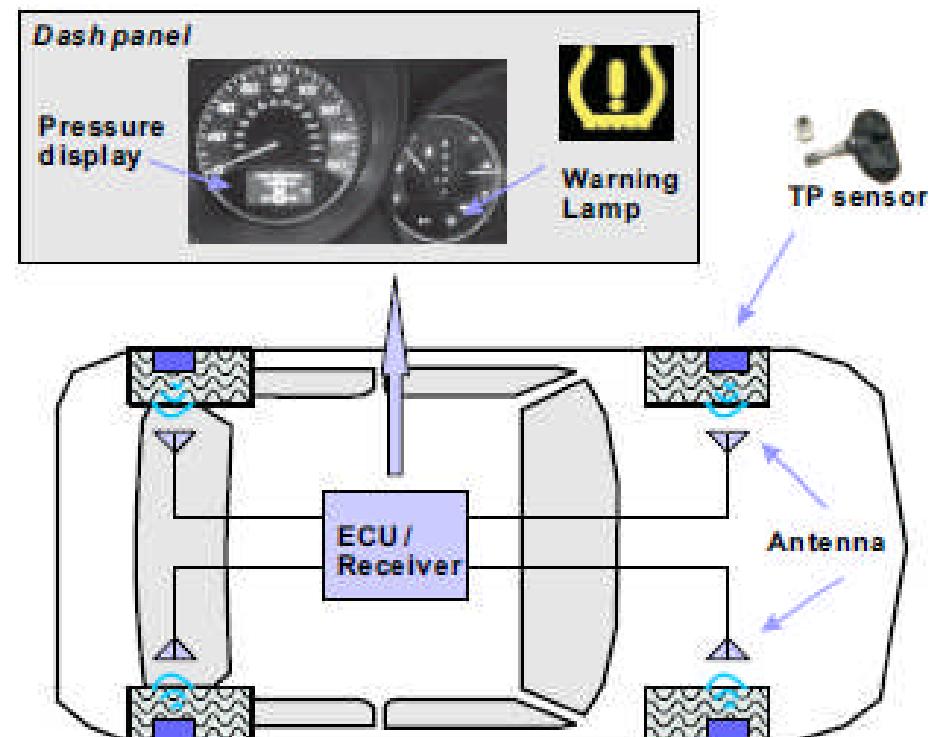


Figure 1: TPMS architecture with four antennas.

自動車内無線ネットワークのセキュリティとプライバシー脆弱性 タイヤ空気圧警報システムTire Pressure Monitoring Systemのケーススタディー

SCAN DISPATCH :走行中の車載ネットワークへのリモート攻撃に成功 2010年09月30日

記事抜粋

https://www.netsecurity.ne.jp/2_16051.html

車内ワイヤレスネットワークの特徴。

- 1) TPMとECU間のワイヤレス通信は、315 MHz か 433 MHz HF (UHF) の ASK(Amplitude Shift Keying)あるいはFSK (Frequency Shift Keying) モジュレーションを使用。
独自のプロトコル用いているが、ワイヤレスシグナルはインプットバリデーションや暗号化がされておらず、GNUラジオとUniversal Software Radio Peripheral (USRP)を使用すれば簡単に傍受できる。
- 2) コミュニケーション可能範囲が広い。TPMSの場合、ローノイズ・アンプを使用すれば40m先までシグナルを受信できることがわかった。
そのため、対象となる車の横を走行している自動車から簡単にハッキングができてしまう。
実際に研究者たちは時速45キロで並走している車から、対象となる車へのリモート攻撃を行っている。
- 3) タイヤ内部のセンサーは、それぞれのセンサー独自の32ビットのアイデンティファイアーを送信している。
このアイデンティファイアーを一度読み込めば、対象となる車の位置を特定することができ、個人のプライバシーの問題にもなってくる。

自動車内無線ネットワークのセキュリティとプライバシー脆弱性 タイヤ空気圧警報システムTire Pressure Monitoring Systemのケーススタディー

SCAN DISPATCH :走行中の車載ネットワークへのリモート攻撃に成功 2010年09月30日

記事抜粋

https://www.netsecurity.ne.jp/2_16051.html

これまで、自動車間、自動車とインフラ間通信のセキュリティは各種研究が行われているが、TPMSのような自動車内部のワイヤレスネットワークは遅れていた。それは、

- a)車の金属ボディーがワイヤレスシグナルを遮断する
- b)ワイヤレスシグナルを受信できる範囲が非常に狭い

と想定されていたためだ。しかし、今回の研究では、この前提が覆されることになる。

研究者らはTPMとECU間のプロトコルをリバースエンジニアリングして突き止めている。
それによれば、「大学の研究者レベルのエンジニアなら2~3日」で、
「大学院レベルでも2~3週間」あればリバースエンジニアすることができたとしている。
また、これに使用された機器は総額1,500ドル程度だったそうだ。技術的にもコスト的にも簡単な攻撃と指摘されている。

今回の研究では、こうした脆弱性を悪用した攻撃が、TPMのシグナルをスプーフィングして偽の空気圧の値をECUに送信する程度にとどまっているが、初のリモートからの攻撃実証は、今後、車載搭載PCシステムへのリモートからの攻撃の増加を予測するものと言えよう。

未来の自動車ソフトウェアの脅威？

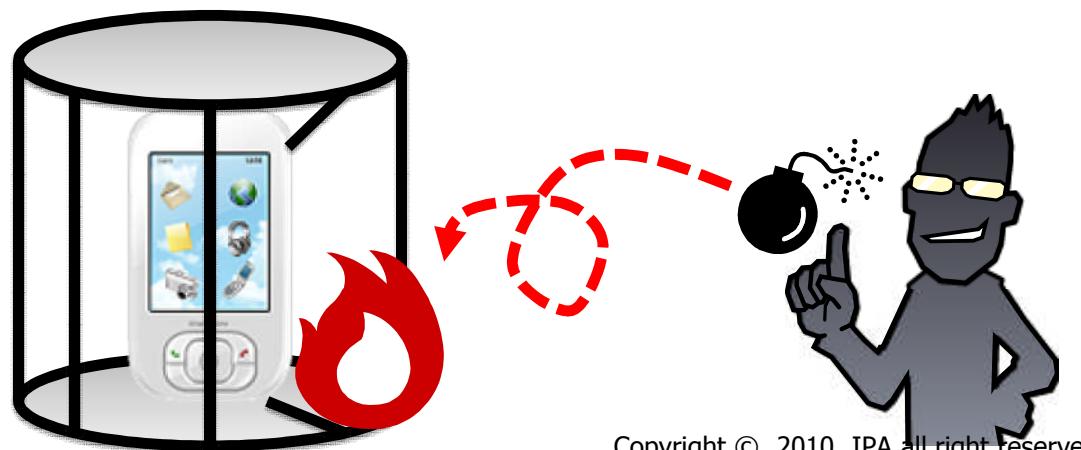
- スマートフォン(iPhone, Androidなど)上のアプリは普通、**制限された環境(檻、Jail)**の中で動作する
- 安全のため、次のようなことはできない：
 - 勝手に電話をかける/メールを発信する
 - 勝手にモノを購入する
 - 勝手にGPS情報を取得する
 - スマートフォン自体を使用不能にする
 - スマートフォン自体や他のアプリの動作を変える



- より便利に使いたいと、**利用者自身が檻を破って(脱獄、Jailbreak)**スマートフォンを使うことがある
 - メーカー不認可のアプリを使いたい
 - テザリング(PC用のモデムとして使用)したい
- 檻の中にいた時より、安全性は低下
 - 身に覚えのない請求が来るかも
 - コンピュータウイルスに感染するかも
- 法的な位置づけは揺れている

脆弱性による Jailbreak の発生

- 脆弱性があれば、**利用者の意志と無関係に檻を破られることがある**
- 2010年8月、**iPhone/iPad** に**脆弱性**があり、攻撃により Jailbreak され得る状態だった
 - <http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001892.html>
- その結果、様々な被害が起き得た**
 - 勝手に電話を使用される
 - プライバシー情報を窃取される
- 実証サイト JailbreakMe** (<http://jailbreakme.com/>)
- LAC注意喚起** (<http://www.lac.co.jp/info/alert/alert20100812.html>)



Copyright © 2010, IPA all right reserved.

【利用者の対策】

- アプリや OS を最新に保つ
- 信用できないアプリを導入しない

【アプリ開発者の対策】

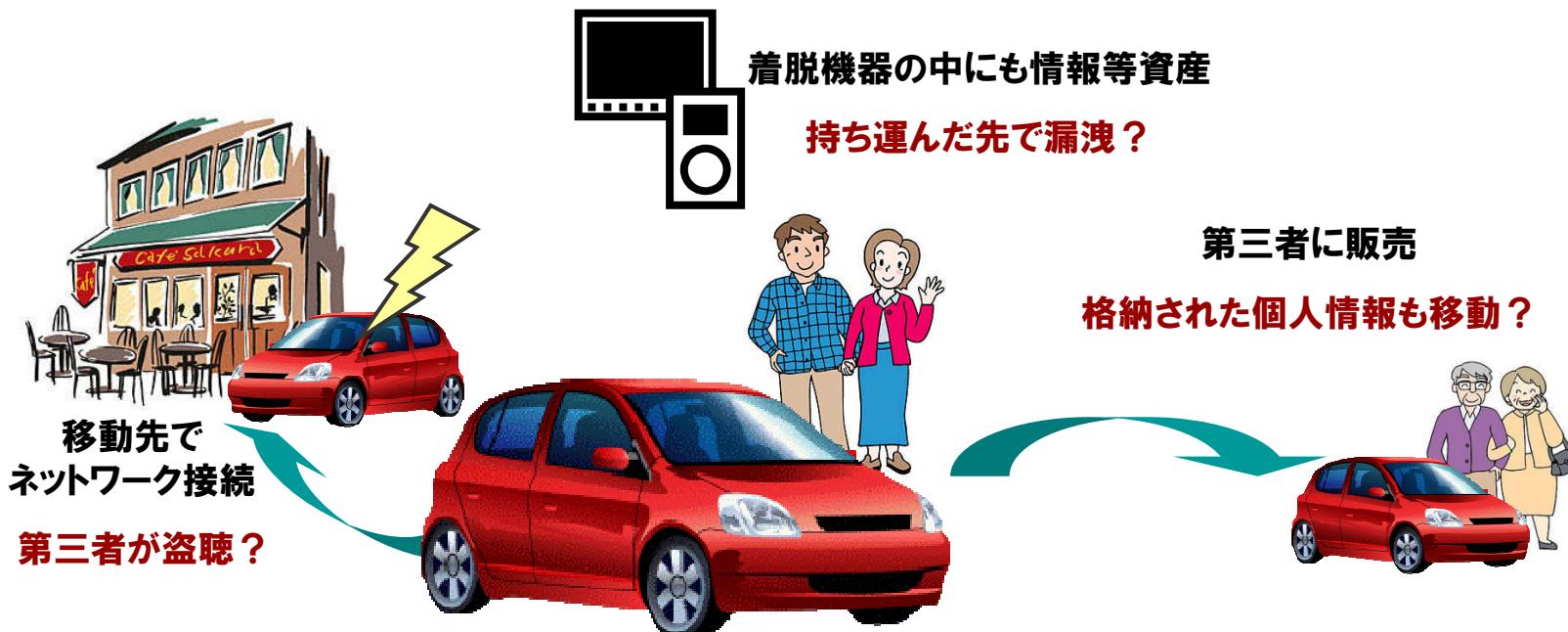
- Jail に頼らないセキュアコーディング



自動車の情報セキュリティ対策の方向性

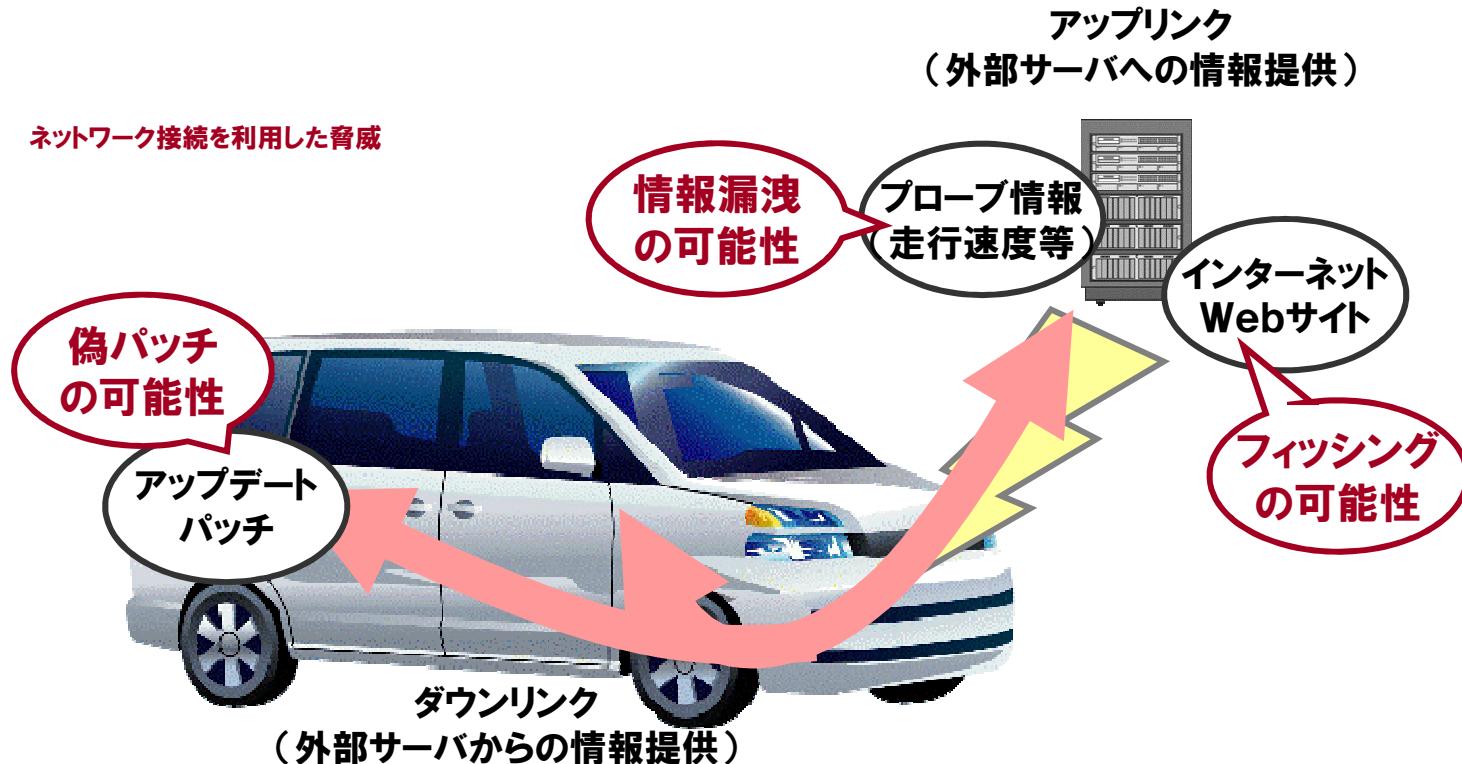
自動車における脅威の特徴(1)

- 自動車の脅威が拡大する可能性
 - 情報等資産の多種多様化、範囲拡大の可能性
 - オークションやレンタルによる情報の漏洩等の可能性
 - セキュリティレベルが低い組込み機器が混在する可能性
 - 移動先で何が繋がり、誰が利用しているか分からない可能性



自動車における脅威の特徴(2)

- ネットワーク経由による脅威の可能性
 - 着脱機器やプローブによる情報等資産の拡散の可能性
 - 偽のダウンロードパッチを受け入れてしまう可能性
 - カーナビ経由でインターネットの不正サイトにアクセスしてしまう可能性

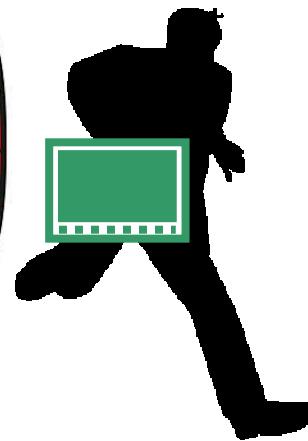


自動車における脅威の特徴(3)

- 直接的な攻撃の可能性
 - h) 駐車場等での第三者による不正な改造の可能性
 - i) メーカ点検員になりました第三者による不正な改造の可能性
 - j) 利用者自身による改造の可能性



窓を割ってPNDを盗む



ECUを不正書き換え、
不正なECUを追加



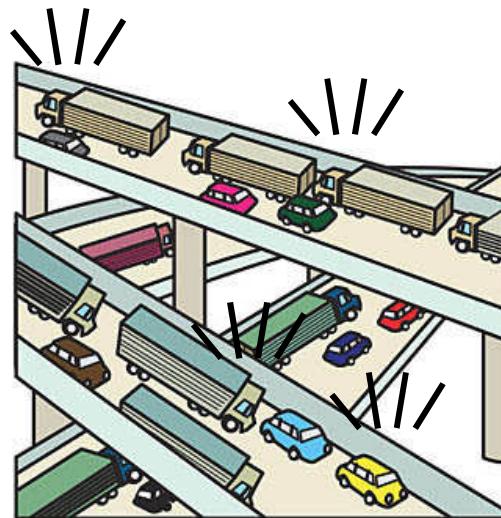
屋外に置かれていると攻撃しやすい

自動車における脅威の特徴(4)

- 重大かつ広範囲の被害の可能性
 - 重大な被害の可能性
 - 社会的混乱を招く可能性



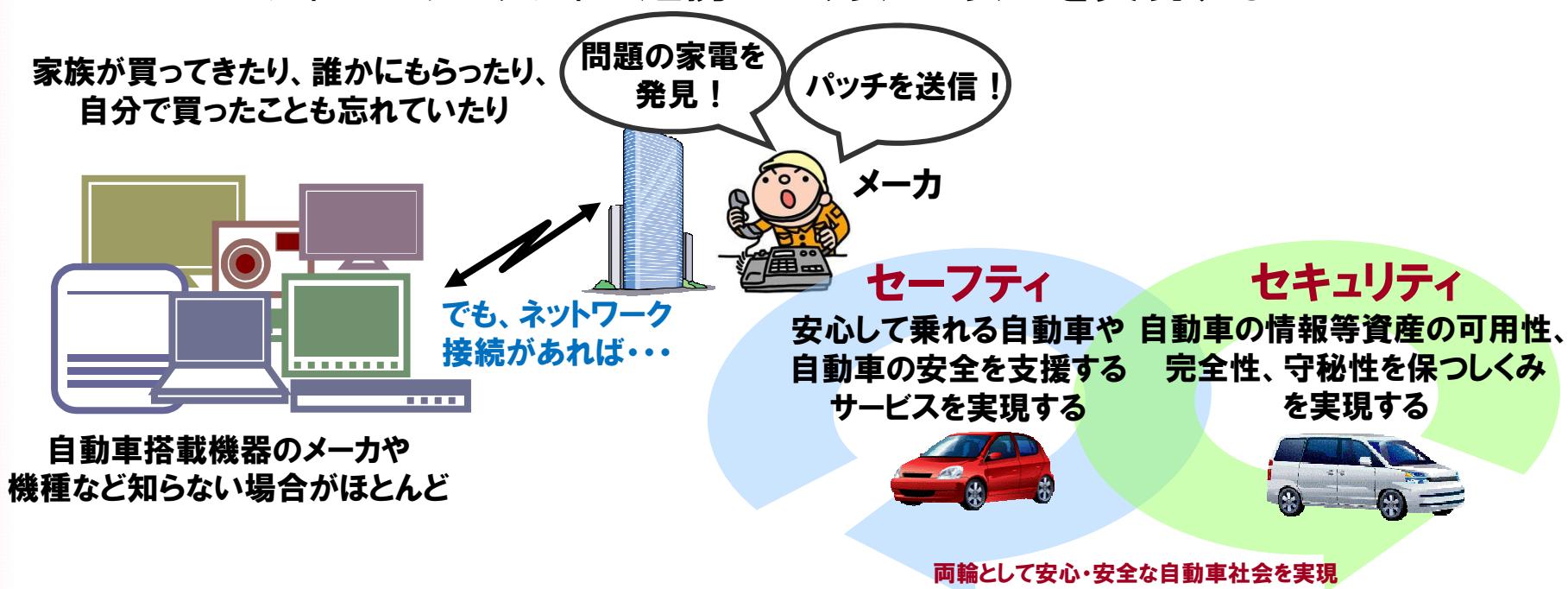
身体への被害の可能性も



偽の情報で日本中が大渋滞
(「地震が来る」等のデマなど)

自動車の情報セキュリティ対策の方向性

1. 利用者にセキュリティ対策を施す意識、被害に気づく知識をもたせる
2. 利用者側にセキュリティ対策にコストをかける文化を醸成する
3. メーカやサービス提供企業に充分なセキュリティ対策を働きかける
4. 自動車のセキュリティ対策に関連した制度やしくみを充実する
5. 何が繋がっているか、誰が利用しているかを明らかにする
6. セーフティとセキュリティの連携により安全・安心を実現する



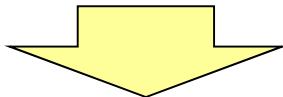


まとめ

似た課題を抱える分野

組込みシステムセキュリティの課題の一歩先の事例としての制御システムセキュリティ

	制御システム	組込みシステム
課題1	オープン化に伴う脆弱性リスクの混入 ・汎用製品、標準プロトコル採用により、脆弱性リスク、ワームなどのウィルス進入、機密情報朗読の恐れ	○同じ課題が当てはまる ・ウィルス進入や個人情報漏洩の脅威は昨年指摘されている
課題2	製品長期利用に伴うセキュリティ対策陳腐化 ・制御システムは通常 10-20年使用。セキュリティ対策も最新ではない可能性	○同じ課題が当てはまる ・自動車のライフサイクルは、およそ 10年前後。常に最新の対策を施しておくことは困難な可能性
課題3	可用性重視に伴うセキュリティ機能絞込み ・可用性重視の観点から、一般的にシステム上の負荷となるウィルス監視やチェックプログラムの自動更新せず	○同じ課題が当てはまる ・機能安全性(可用性、完全性)と低成本重視の観点から、ウィルス監視機能などは搭載機能順位が低くなる



制御システムのセキュリティ課題と類似性は高い。
制御システムにおけるセキュリティ対策の取り組みは、
組込みシステム業界での取り組みの参考になると考える

セキュリティに関する取り組み状況の比較



- 自動車等の組込みセキュリティに関する取組みはこれから

	オフィスの 情報機器	自動車	情報家電
セキュリティや セーフティを 保つための 仕組みや制度	セキュリティポリシーや 社内規則に基づき、情 報システム部門の管理 担当者が、チェック。	車検(道路運送車両法) 等で定期的な検査が 義務付けられている。	特になし。 ただし2009年4月よ り「長期使用製品安 全点検制度」が施行。
セキュリティや セーフティに料 金を支払う慣習	情報システム管理や、 セキュリティ・ソフトウェア にコストが必要であるこ とは一般的。	車検、点検等に費用が かかることは、自動車の 所有者には認知されて いる。	特になし。
利用者教育の 仕組み	社員は業務の一環とし てセキュリティ対策に必 要な知識を学習するこ とが一般的。	運転免許取得時に、 知識および技術の習得 が義務付けられている (道路交通法)。	特になし。
個人的な 改造に対する 制限	会社の物品であり、個 的な改造は許可され ないことが一般的。	合格基準を満たさない 改造を行うと、車検は 通らない。	所有物については自 由(保証を受けられな くなる場合はある)

今後の検討課題

- 利用者、メーカー、サービス事業者等の情報リテラシー向上
 - 利用者の情報セキュリティのリテラシー向上、対策コストの必要性の理解促進。
 - リテラシー向上が難しい利用者を誰がどのように保護するかの方策検討。
 - 自動車等の組込みシステムセキュリティが必須となる関係企業に対するガイドライン、利用者向け説明資料の整備、配布。
- ライフサイクルを通じた検討
 - 設計段階からのセキュリティ検討、廃棄時の個人情報やセキュリティ機能の適切な消去などライフサイクルを通じた検討。
- 協力および提言の場の確立
 - 利用者、メーカー、サービス事業者、セキュリティ技術者が協力し、セキュリティ対策を検討するとともに、法制度の整備について国に提言していく場の設置。
- ネットワークの両側でのセキュリティ対策の実施
 - 機器側(メーカー側)とサービス側(サービス提供企業側)の双方でのセキュリティ対策による、より確実な脅威の解消。

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

2010年9月7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
(2010年度改訂版)

2009年11月25日公開
上水道分野用の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

2010年5月31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5版)、検証ツール:2010年11月25日公開
TCP/IPに係る既知の脆弱性検証ツール
報告書(第2版)、検証ツール:2010年11月30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)