研究室紹介
IoT松井研究室

情報セキュリティ大学院大学　教授
松井　俊浩

自己紹介

小中学校　将来はプログラマになりたいとの作文を書く、電子工作少年

1976年 大学2年、マイクロコンピュータに魅せられる

1980年 東京大学計数工学科卒業

1982年 東京大学大学院情報工学修士修了

1982年 電子技術総合研究所入所　ロボットのソフトウェアの研究

1991年 東京大学大学院　工学博士

1991~99年　スタンフォード大学ロボット工学研究所、マサチューセッツ工科大学AIラボ、オーストラリア国立大学などの客員研究員等

2001-03年 産総研企画本部総括企画主幹、ビルを建てる

2003-07年 デジタルヒューマン研究センター副センター長　岩波DH本を書く

2008-12年 情報通信エレクトロニクス分野、副研究統括

2012-14年 セキュアシステム研究部門長　セキュリティの研究

2015- NEDO技術戦略研究センター　IT技術開発戦略の策定

2016- 情報セキュリティ大学院大学

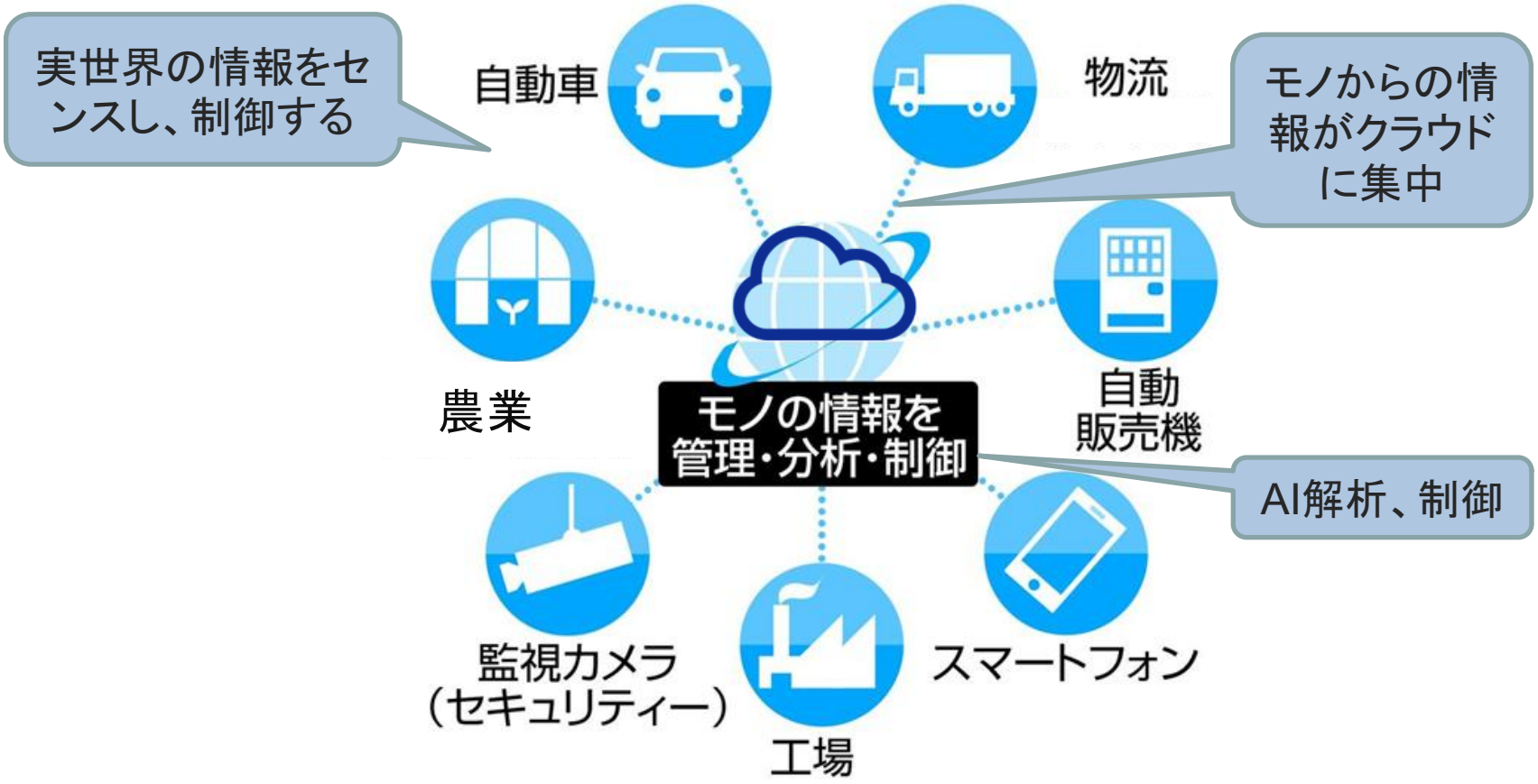
- 日本ロボット学会フェロー
- 情報セキュリティスペシャリスト、エンベッディッドシステムスペシャリスト
- 産総研名誉リサーチャ

担当講義　(2017年度予定)

- 情報デバイス技術　(大久保先生と共担)
  - 論理回路、メモリ、LSI
  - マイクロプロセッサ、並列計算機
  - マイクロコントローラ、DSP、GPU、FPGA、組込システム
  - デバイスインタフェース、デバイスドライバ、センサー、周辺機器
- 情報システム構成論　(後藤先生と共担)
  - システム工学、プログラミングシステム、システムファンクション
  - 並列処理、分散システム
  - 人工知能、ロボット、実時間処理
- IoTセキュリティ特論
  - 組み込みシステム演習
  - IoTデバイスへのタンパー攻撃
  - フィールドネットワーク（車載ネットワーク）への侵入

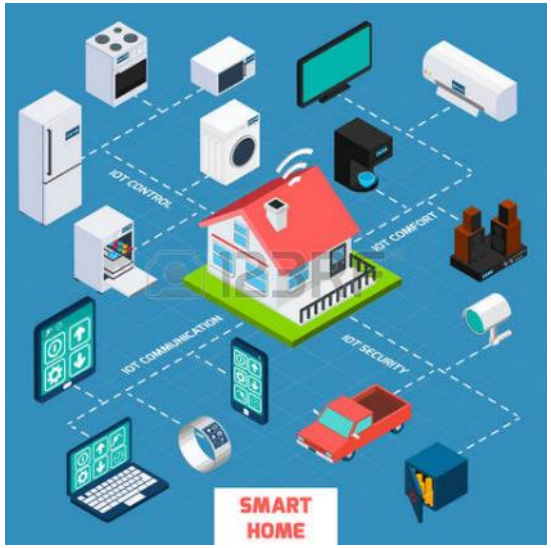
IoT (Internet of Things)

- MITのKevin Ashton が、RF-IDの普及を指して初めて言った(1999)
- A network of networks of uniquely identifiable endpoints (or “things”) that communicate without human interaction using IP connectivity. （IDC)
- 中央集権的コントローラがいない
- M2M通信を行う



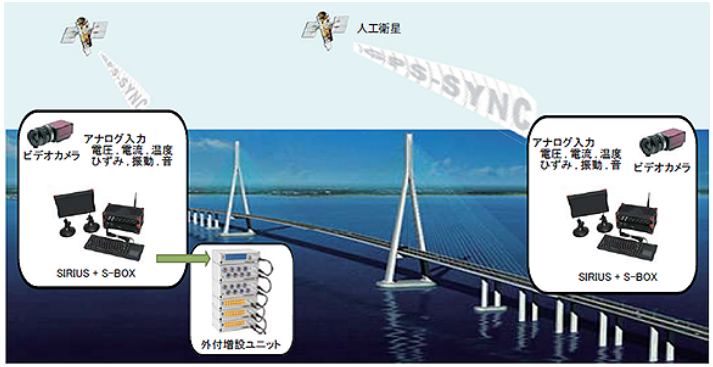
IoTの事例

ヘルスケア用ウェアラブル機器



スマートホーム

産業機器の情報収集やメインテナンス



インフラ保守用の
センサーネットワーク

制御システムネットワークのセキュリティ

インターネット

保守／サービス、関連工場と連携、セールス

ファイアウォール
(防火壁)

オフィスネットワーク

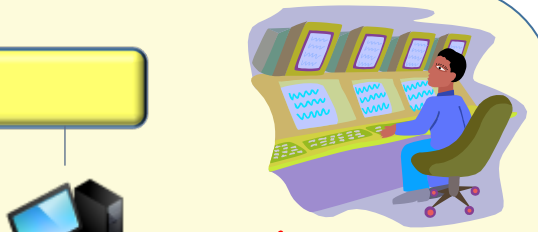
制御システムネットワーク

(工場、ビル、浄水場、発電・変電所、ガスタンク、防災センター、etc)

DCS

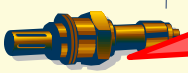
PLC

バルブの開閉
温度や圧力の制御
ロボットへの指令



監視室(SCADA)

エンジニアリングPC



2010年、Stuxnetによるイラン各施設へのサイバー攻撃

DCS: Distributed Control System
PLC: Programmable Logic Controller

SCADA: Supervisory Control And Data Acquisition

6

家電
アイロン

BBC News - Russia: Hidden chips 'launch spam attacks from irons'
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337

BBC News Sport Weather Capital Culture Autos TV Radio More... Search

NEWS NEWS FROM ELSEWHERE

Home | UK | Africa | Asia | Europe | Latin America | Mid East | US & Canada | Business | Health | Sci/Environment | Tech | Entertainment | Video

28 October 2013 Last updated at 12:02 GMT

Russia: Hidden chips 'launch spam attacks from irons'

News from Elsewhere...
...as found by BBC Monitoring

How Russian TV covered the story about the chips, shown inset

Cyber criminals are planting chips in electric irons and kettles to launch spam attacks, reports in Russia suggest.

About #NewsfromElsewhere
A collection of stories being reported by media around the world, as found by BBC Monitoring and curated by Andy McFarlane. Find out more.

More from BBC Monitoring
BBC MONITORING
About BBC Monitoring
Reports and analysis from TV, radio, web and print media around the world
Country Profiles
An instant guide to the history, politics and economics of countries and territories

NEWS MAGAZINE
More from the Magazine

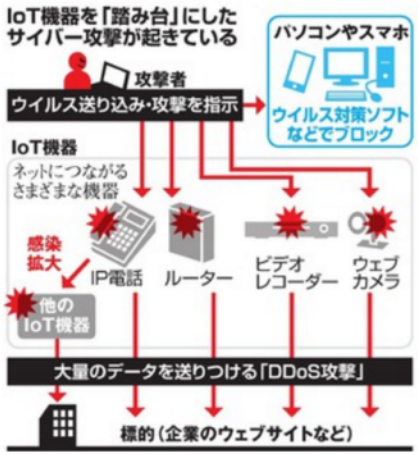
中国から輸入された電気式アイロンに隠されていたのは小さなチップ。このチップは半径200m以内で暗号キーなしで接続できるWi-Fiを利用しているPCに侵入し、ウイルスをまき散らすように設計されていたとのこと。

似たようなチップが中国製の携帯電話や自動車、カメラからも発見されており、専門家は「電化製品や自動車に隠されていたチップは、会社のネットワークに侵入しスパムメールを送信することに使用されていたものでしょう」と話しています。

- 2013年10月22日　英国BBC
- **電気ケトル、偽iPhoneからも発見された。**
- WiFi**経由でPCをマルウェアに感染させる。**
- **仕様上の重量とわずかな差があったことから発覚した。**

サイバー攻撃、家庭のIoT機器悪用　ルーター販売停止

編集委員・須藤龍也　2016年11月3日05時03分



IoT機器を「踏み台」にしたサイバー攻撃が起きている

ネットにつながる家電など「IoT機器」を経由する新手のサイバー攻撃に悪用される恐れがあるとして、パソコン周辺機器大手のアイ・オー・データ機器（金沢市）は2日、一部製品の販売停止を決めた。パソコンなどに比べセキュリティーが弱いIoT機器を狙ったウイルスに感染するリスクがあるという。

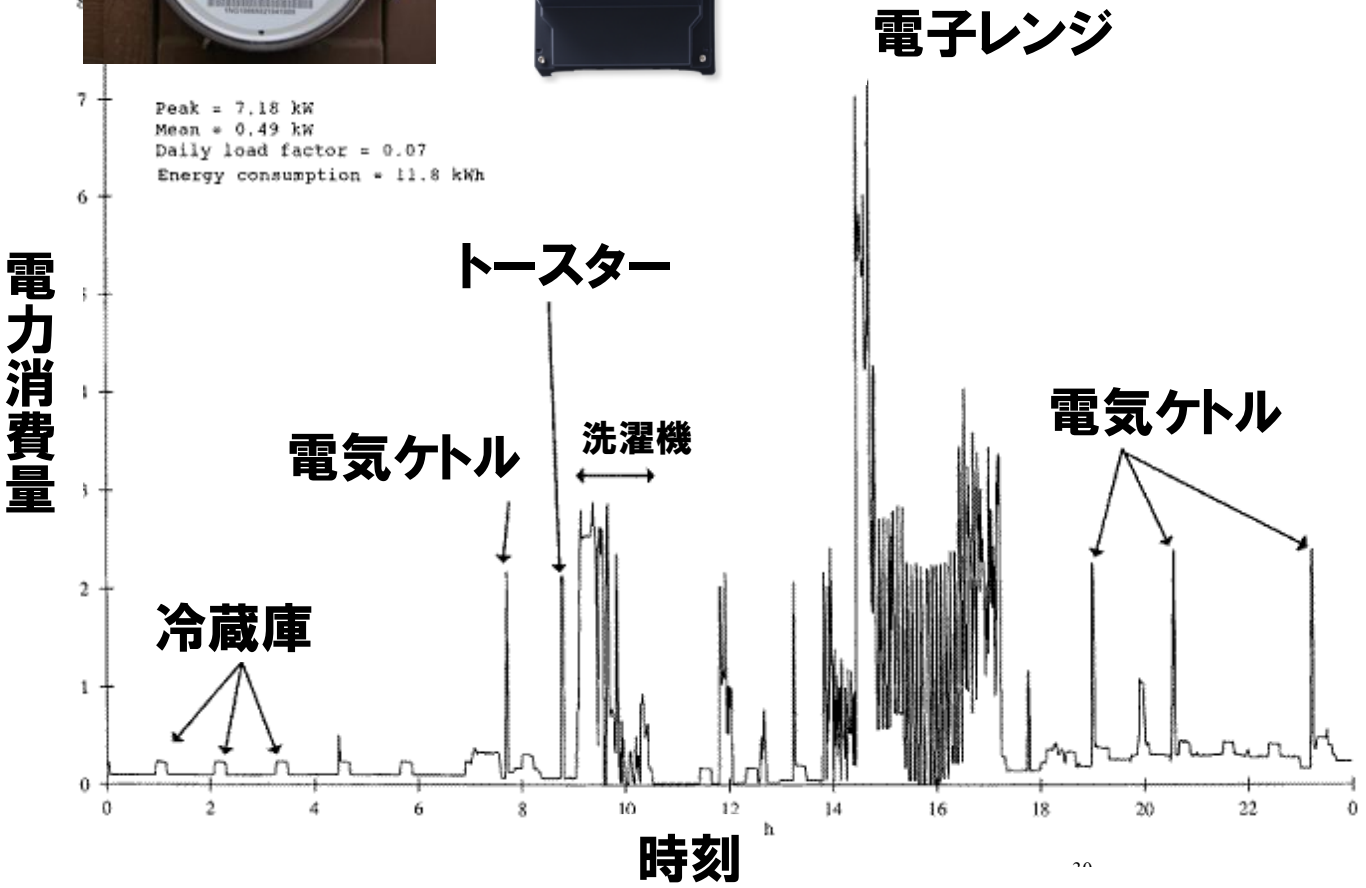
大手製造ルーター、販売停止　サイバー攻撃に悪用の恐れ →

販売を停止する製品は「Wi—Fiストレージ ポケドラ」。無線LANの電波を出すルーター機能や、スマホのデータ保存機能を持つ機器だ。2013年9月に発売され、国内全体で2万2800台出荷されているという。機器に保存した情報を抜き取られる可能性もあり、店頭から商品の回収を始めている。

所有者には、感染を防ぐ修正プログラムを配布する予定で、それまではルーター機能を使わないよう呼びかけている。同社は「重大な事態と認識しており、商品のチェックが甘かった」としている。

http://www.asahi.com/articles/ASJC16J7BJC1UUPI002.html

スマートメータのプライバシ問題



グラフは以下より:
NISTIR 7628, Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

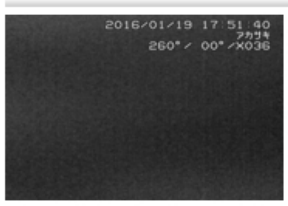
【ヤバすぎ】監視カメラの映像が丸ごと流出して業界騒然！セブンは2500人の社員が手分けして確認作業！パスワード強化などを呼び掛け

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... 1164

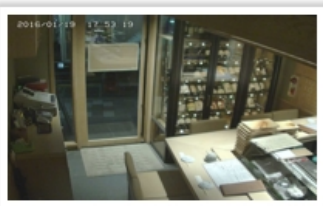
'atch PanasonicHD camera in
Japan
Osaka

Watch PanasonicHD camera in
Japan
Tokyo

Watch PanasonicHD camer
Japan
Musashino



/atch PanasonicHD camera in
Japan
Tokyo



Watch PanasonicHD camera in
Japan
Musashino

Watch PanasonicHD camer
Japan
Muko

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | ... 1164

☆肉まん買う客の姿もくっきり　防犯カメラ映像丸見え「全く想定外の状況だ」セブン社員2500人が奔走
URL　http://headlines.yahoo.co.jp/hl?a=20160123-00000005-withnews-soci
引用：
世界中の防犯カメラの映像が見られるとうたうインターネットサイトが話題になっています。パスワードがきちんと設定されていない監視カメラの映像が、世界中で2万5000カ所以上、日本だけで約6000カ所登録されています。
～省略～

http://www.insecam.org/

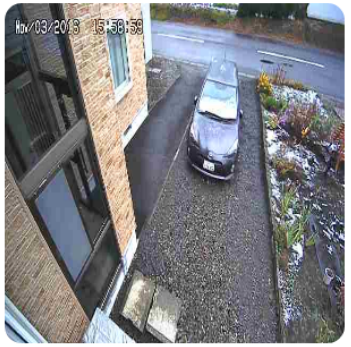
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IP cameras: Japan

« 1 ... 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 ... 223 »

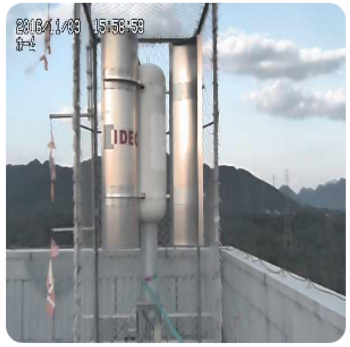
Watch Axis camera in Japan,Osaka

Panasonic camera in Japan,Tokyo



Watch PanasonicHD camera in Japan,Sapporo

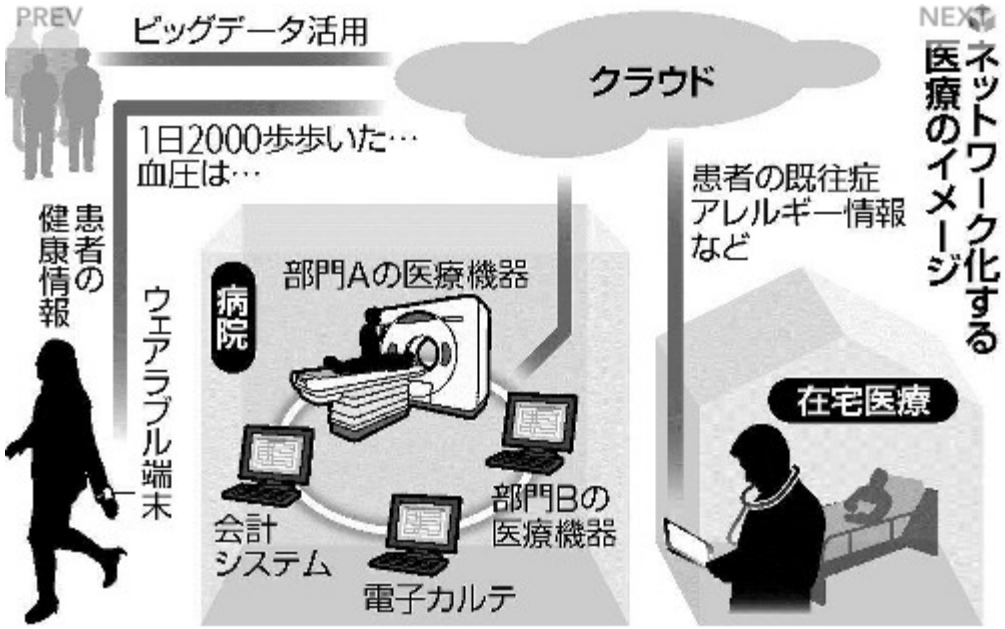
Watch PanasonicHD camera in Japan,Nagoya



Watch PanasonicHD camera in Japan,Tokyo

Watch Panasonic camera in Japan,Toyama

医療機器



医療機器などを巡る主な問題点

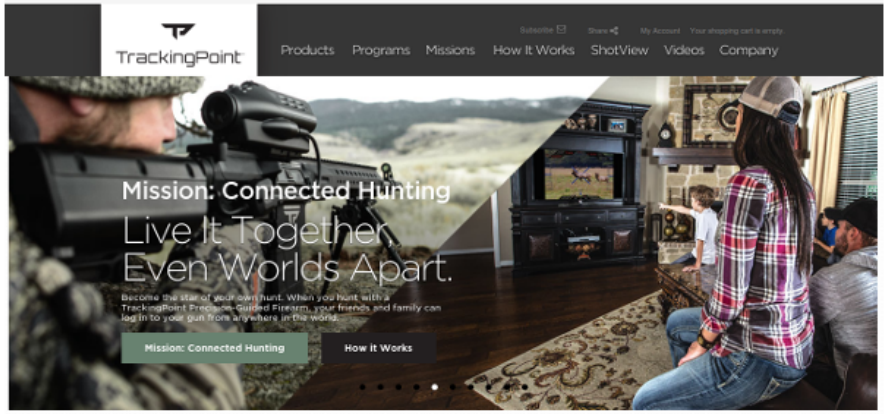
2008年	アメリカの学会で「ペースメーカーをハッキングし、電流を流したり機器を止めたりすることが可能」という研究成果が発表される
2009	米国のMRI装置がウイルス感染で、外部から操作されていたことが発覚。同様の医療機器の感染が世界で約300台見つかる
2011	糖尿病患者用のインスリンポンプへのハッキングがセキュリティー会議で実演される。投与量を外部から操作できることを証明
2012	遺伝子検査製品に使われるソフトウェアなど複数の医療機器の脆弱性がみつかり、FDAがリコール公表
2013	手術用機器や人工呼吸器など300機器のパスワードに問題があり、遠隔操作される危険があるとしてICS-CERTが対策呼びかけ

http://www.yomiuri.co.jp/science/feature/CO017291/20150626-OYT8T50053.html

2015年08月18日 21時00分00秒

Linux搭載のライフル銃がWi-Fiハッキングで乗っ取られる脆弱性が発覚

なんとハンティングしているスコープの映像を自宅の家族に共有できるんだとか。

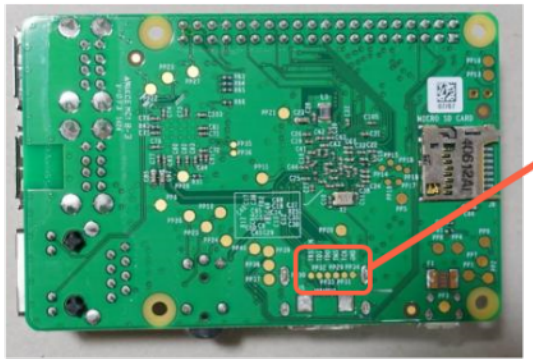


標的を狙うスコープにLinuxを搭載したコンピューターを内蔵し、驚異の命中率を誇るというTrackingPointの「スマートライフル」にシステムが乗っ取られるという脆弱性が判明しました。この脆弱性が悪用されると設定していた標的が知らないうちに別のものに置き替えられ、本来とは異なる標的を撃ち抜いてしまう危険性があります。

Hacking a computer-aided sniper rifle
http://www.usatoday.com/story/tech/2015/08/06/computer-controlled-rifle-black-hat-trackingpoint/31239637/

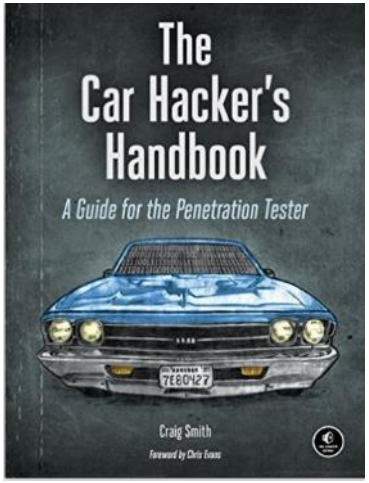
Black Hat USA 2015 | Briefings
https://www.blackhat.com/us-15/briefings.html#when-iot-attacks-hacking-a-linux-powered-rifle

組込機器へのタンパー攻撃



組込システムの開発・保守ポート
組込学習ボードRaspberry Piのボード裏面にあるテストパッド。TRST, TDI, TDOなどは、JTAGの信号名。

- JTAGなどのテストピンから侵入
- Bluetoothからデバッグポートに入れるモノがある
- デバッグポートから内部メモリの読み出しが可能
  - プログラムを解析して、脆弱性を発見される
- 内部メモリ(フラッシュ）に書き込みが可能
  - プログラムを改編してバックドアを付加
- 整備、補修用のポートは保護しにくい



IoTセキュリティガイドライン

総務省と経済産業省

① 脅威の影響範囲/影響度合いが大きいこと
- グローバルなインターネット、数が多い

② IoT機器のライフサイクルが長いこと、長寿命性
- 長期の機器保守に使われる、対象機器より長寿命

③ IoT機器に対する監視が行き届きにくいこと
- 小さくて多数、設置を忘れられる、監視機器の監視はしない

④ IoT機器側とネットワーク側の環境や特性の相互理解が不十分
- 専門家でなくても、誰でも使える

⑤ IoT機器の機能/性能が限られていること
- 最も安価なハードウェアを使用、暗号や認証が限定的

⑥ 開発者が想定していなかった接続が行われる可能性があること
- 動的社会、継続的な機能拡張

ARMやシマンテックら、IoTセキュリティのための新プロトコル「OTrP」で連携

Danny Palmer （ZDNet.com） 翻訳校正： 編集部 2016年07月21日 13時27分

http://japan.zdnet.com/article/35086192/

モノのインターネット（Internet of Things：IoT）とコネクテッドデバイスに関しては、統合的なサイバーセキュリティ規格が存在せず、そのことが原因で、産業用ネットワークや企業ネットワーク、ホームネットワークに甚大な被害をもたらす可能性のあるセキュリティ侵害が発生するおそれがある。

センサから自動車、医療用機器まで、膨大な数の各種デバイスが既にインターネットに接続されている。Gartnerの試算によると、毎日550万台の新しい「モノ」がインターネットに接続されているという。現在50億台以上のデバイスが接続されており、その数は2020年までに200億台に達する見通しだ。

研究課題

- 従来のPCやWebサーバーや業務システムに対する脅威から、コンピュータが組み込まれた数百億台の機器に脅威が広がる
- 情報漏洩よりも、制御やサービスを止める可用性への攻撃、ハードウェアを置き換えるような完全性への攻撃が増える
- ネットワークからの侵入もあるが、駐車場や公共の場所など攻撃者の手の届く場所に機器があることから、物理的攻撃の脅威が増大

IoTデバイスやIoTネットワークを保護するセキュリティ技術の研究

- IoTデバイス、組込ソフトウェアのセキュア設計
- コンテクスト型機器認証によるシステム保護
- ハードウェアの耐タンパー性
- 人工知能による異常検知

実施中の研究課題

- WebアクセスログをRNN（Recurrent Neural Network)で解析することによる詐欺行為の発見
- Wireless Sensor Networkにおけるソースロケーションプライバシ保護
- 自動車組込みデバイス（車載ネットワークやECU)のセキュリティ
- 半導体の偽造防止PUFの安全性評価
- ハニーポットを使った攻撃の挙動解析

本格IoTの前に先回り対策を!

松井研究室

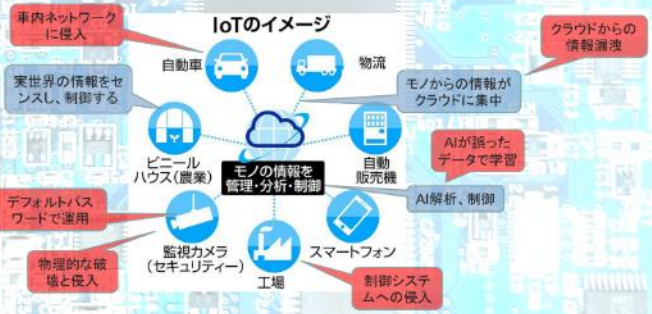
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoTのセキュリティをAIで守る

身の回りのさまざまなモノがインテリジェントになり、情報を集めてクラウドに送るIoT社会が広がりつつあります。監視カメラ、自動車エレクトロニクス、家電、また、工場やオフィスのロボットや医療機器などがインターネット接続を持つようになります。もともとは個々独立した使用を想定していた機器がインターネットにつながると、多数のセキュリティリスクが生じます。PCやスマフォより危険なのは、これらのIoTデバイスは、M2M（機器間通信）で動作し、必ずしも人間と対話しないため、ユーザーによる監視が行き届きにくいことです。また、インターネット接続だけを心配すればよいのではなく、PCもUSBメモリから侵入されることがあるように、物理的な攻撃にもさらされます。たとえば、PCは家の中にあって守られていますが、自動車は駐車場に放置されていたりします。

さて、これらの新しい脅威にどのように対処していくのでしょうか。ネットワークに接続されることによって生じる脅威は、実は、PC、スマフォ、制御システムによって経験済みなのです。すなわち、不正アクセスの検知、マルウェアの検出、ログの分析、仮想マシンでの監視など、まだまだ研究の余地はたくさんあるものの、さまざまな方法が検討されています。私たちは、IoT独自の脅威とは、物理的攻撃やパスワード認証の困難さなどにあるのではないかと考えています。両方とも、IoTはM2Mであるがために、人が関われないことが本質です。ユーザーがいくら注意していても、見えないところで事件が起きます。人が入れないならどうするか？人に代わる知性を注入したらどうでしょうか。つまりAIです。AIが人に代わってIoTのセキュリティを守る技術が必要になります。



研究室所属学生：博士課程2名（1名はベトナムからの留学生）、修士課程5名

研究テーマ例

- Webアクセスログを RNN（Recurrent Neural Network)で解析することによる詐欺行為の発見
- Wireless Sensor Networkにおけるソースロケーションプライバシ保護
- 自動車組込みデバイスのセキュリティ
- 半導体の偽造防止PUFの安全性評価

教授紹介　松井俊浩：　1982年から、工業技術院電子技術総合研究所において、ロボットの動作計画、オブジェクト指向を用いたロボットプログラミング、オフィス内移動サービスロボットJijo2などの研究。1990年代に、スタンフォード大学、マサチューセッツ工科大学（MIT)、オーストラリア国立大学などの客員研究員。2003-2007年、産総研デジタルヒューマン研究センターにおいてヒューマノイドロボットの実時間制御、身体バイタルサインから心理状態の推測の研究。2012年から産総研セキュアシステム研究部門長、2015-2017年、NEDOにおいてIT技術開発戦略の策定、2016年より本学教授。授業では、情報デバイス技術、情報システム構成論、IoTセキュリティ特論を担当。

ご清聴ありがとうございました。