# IoTの「リスク評価」を考える

## CSAジャパン IoT WGの活動紹介

IoT WG リーダー（アルテア・セキュリティ・コンサルティング）

二木真明

# IoT WGの概要

- IoT クラウドサービスWGから改称
  - もともと、（CSAなので）サービスサイドからIoTを考えようという発想で立ち上げ
  - でも、グローバルIoT WG（米国本部がデバイス側も含めてアウトプットを出し始めた）（暴走？？）
  - なので、「サービスにフォーカス」しつつも、全体をカバーする方向に
- 独自のアウトプット（リスク評価やサービス側についてのコンテンツ）を模索しつつ、グローバルとも連携する活動を行っている
  - IoTインシデントの影響評価に関する考察（5月リリース）
  - IoTに関する脅威シナリオ集（現在とりまとめ作業中：年内目途に第一弾を完成させる予定）
  - グローバルコンテンツのレビューへの参加と翻訳活動
    - IoT早期導入者のためのセキュリティガイダンス
      - Security Guidance for Early Adopters of the Internet of Things (IoT)
    - IoTにおけるID/アクセス管理　要点ガイダンス
      - Identity and Access Management for the Internet of Things – Summary Guidance
    - 翻訳作業中（2月頃リリース予定）
      - Future Proofing The Connected World (13 Steps To Developing Secure IoT Products)
  - 書籍、記事の共同執筆
    - 日経BP社　IoTセキュリティ　～インシデントから開発の実際まで～
      - IoT早期導入者のためのセキュリティガイダンス解説等の寄稿
  - IoTに関連する政府パブコメ等への意見提出

メンバー　10名　（2016/11時点）

# IoT関連のインシデント

公開日:2016/11/04 最終更新日:2016/11/04

JVNTA#95530271
Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威

概要
近年、IoT 機器を使用した大規模なボットネットが構築され、分散型サービス運用妨害(DDoS)攻撃に使用されています。システムやネットワークの保護のために、IoT 機器および接続されているハードウェアを保護することが重要です。

影響を受けるシステム

- プリンタ、ルータ、ビデオカメラ、スマート TV など、インターネット経由でデータの送受信を行う IoT 機器

詳細情報
2016年9月20日、Krebs on Security が最大で 620Gbps を超える大規模な DDoS 攻撃を受けました。この DDoS 攻撃は、Mirai と呼ばれるマルウェアに感染した IoT 機器によって構築されたボットネットから行われました。Mirai は、脆弱な IoT 機器を定期的にスキャンして感染し、ボットネットに取り込みます。Mirai は初期設定で使われることの多いユーザ名・パスワードの組み合わせ 62組からなるリストを使用して、脆弱な機器をスキャンします。多くの IoT 機器は保護が全くされていない、または不十分なため、この短いリストでも数十万の機器へのアクセスが可能になります。Mirai の作者を名乗る人物によると、38万を超える IoT 機器が Mirai に感染し、Krebs on Security に対する攻撃に使用されたとのことです。

9月下旬には、フランスのウェブホスト OVH に対して、Mirai を使用した最大で 1.5Tbps にもなる DDoS 攻撃が行われました。

Mirai の影響を受けた IoT 機器は主に、家庭用ルータ、ネットワークカメラ、デジタルビデオレコーダでした。9月末には Mirai のソースコードが公開されたため、他の DDoS 攻撃に広く使用される可能性があります。

JVN
HOME
JVNとは
脆弱性レポートの読み方
脆弱性レポート一覧
VN-JP
VN-JP(連絡不能)
VN-VU
TA
TRnotes
JVN iPedia 脆弱性対策情報データベース
MyJVN
JVNJS/RSS
ベンダ情報一覧
連絡不能開発者一覧
脆弱性情報の届出
お問合せ先

*Ｗｅｂカメラ、ルーター等に感染するマルウエアの大流行と、それによるDDoS攻撃の発生　（620Gbps超!!）*

# 制御システム関連のインシデント

Jeep ハッキングと大規模リコール

IoTと呼ぶかどうかは別として
単独で深刻な影響をもたらすものも・・


ウクライナ発電所へのサイバー攻撃
(CNN.co.jpより）

# IoTブームの危うさ

- 簡単に「繋がる」環境
  - IoT機器は簡単に作れる
    - 安価なH/Wとオープンソースのプラットホーム
- 異業種の参入
  - ネット利用とは無縁だった業界、業種、部門の参入
    - 「常識」の欠落・・・・
    - （企業全体としてはノウハウがあっても）部門の壁が高い
- 利用者にとっての“uncontrollable”
  - できることは、買わないかネットに繋がないことだけ
    - 製品価値の多くがネットから提供されているから、購入が無意味になる可能性が高い・・・

# IoTの「リスク」

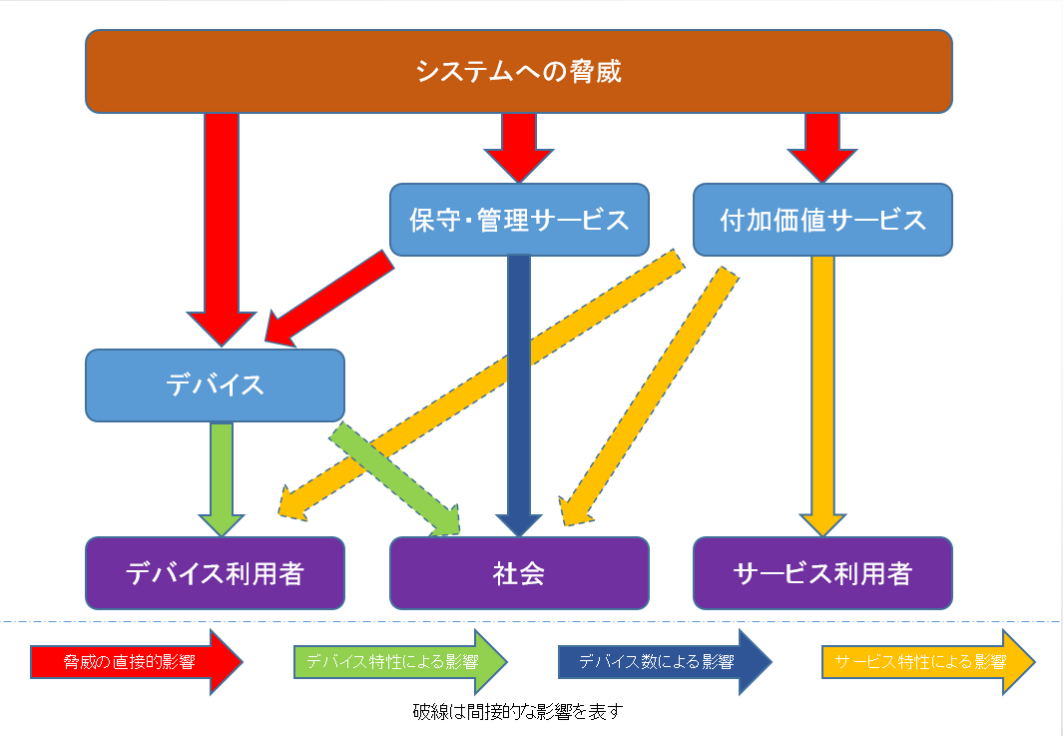
- 作る側のリスク
  - サイバー攻撃、マルウエアの標的となることで、利用者や第三者に被害を与える可能性（企業責任の問題）
  - 機器やサービスの機能停止等による損害、改修、リコール等に多くの労力と費用が発生する可能性
- 使う側のリスク
  - サイバー攻撃、マルウエアの標的になることで、直接的な被害（物理的被害、情報漏洩などの被害）を受ける可能性
  - 機器が機能しなくなることによる利便性や安全性の低下の可能性
  - （知らない間に）機器が悪用され、他者に被害を与える可能性
- 社会的なリスク
  - 社会インフラや重要サービスに対して直接、間接に悪影響を与える可能性
  - 社会的混乱や社会不安を発生する可能性

# 作る側の大きな「誤解」

- 人が死んだり怪我をしたりしないから・・・・
  - 直接的には影響しなくても間接的には？
    - たとえば、車のスピーカーから突如として大音響が出たら何が起きるか・・・といった考察は必要（車載機器でなくても、GPSや位置、速度検出機能があれば、車に乗っていることを認識することは可能）
    - 誤った情報が与えられることで、人の行動に影響する可能性も検討が必要
- 機能や能力が限定されているから、これを攻撃してもメリットはないだろう・・・
  - 大規模なデバイスネットワーク全体を乗っ取られるリスクも検討が必要
    - サービスサイトが乗っ取られたら？
    - ファームウエア更新サーバが乗っ取られて、改ざんされたファームウエアが一斉配布されたら？
    - mirai worm 感染デバイスのように、ネットワークインフラに破壊的な影響を与える可能性も

「想像力」の欠落とも言える

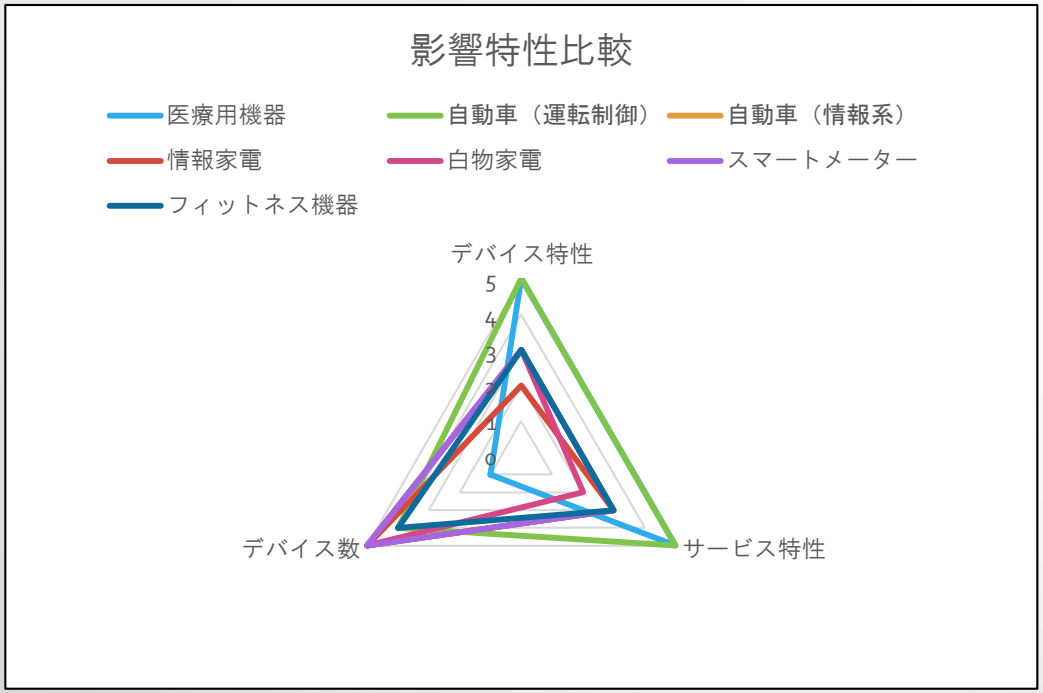
# まずは「影響評価」から




脅威は様々な切り口から攻撃を仕掛けてくる

IoT全体を「システム」として捉えて、脅威の影響を見極める必要がある。

# 影響要素




| システム例 | デバイス特性 | サービス特性 | デバイス数 | I | i |
|---|---|---|---|---|---|
| 医療用機器 | 5 | 5 | 1 | 26 | 4.3 |
| 自動車（運転制御） | 5 | 5 | 4 | 29 | 4.8 |
| 自動車（情報系） | 3 | 3 | 5 | 20 | 3.3 |
| 情報家電 | 2 | 3 | 5 | 17 | 2.8 |
| 白物家電 | 3 | 2 | 5 | 18 | 3.0 |
| スマートメーター | 3 | 3 | 5 | 20 | 3.3 |
| フィットネス機器 | 3 | 3 | 4 | 19 | 3.2 |

「IoTインシデントの影響評価に関する考察」　から抜粋

脅威はその目的によって
最も効率の良い影響要素
を狙ってくる

デバイスの特性
・デバイスが直接、間接に
　周囲に与える影響

サービス特性
・サービスがその利用者や
　接続されているデバイス
　を介して周囲に与える影響

デバイス数
・機器が多数同時に制御を
　奪われた場合に、社会や
　利用者全体に与える影響

特性を見極めて対処すること
が必要

# まずは対策の「ベースライン」を決める

- 開発しようとするシステムの「影響要素」を分析
  - デバイス特性、サービス特性、デバイス数の3軸で影響度を評価し、それに応じた基本的な対策レベルを決めて、設計に活かす
  - 詳細な脅威分析の前に、平均的な影響度を見極め、それを対策の最低ライン（ベースライン）として、各種のガイダンス等を参考に必要なセキュリティ対策を選択する

| システム例 | デバイス特性 | サービス特性 | デバイス数 | I | i |
|---|---|---|---|---|---|
| 医療用機器 | 5 | 5 | 1 | 26 | 4.3 |
| 自動車（運転制御） | 5 | 5 | 4 | 29 | 4.8 |
| 自動車（情報系） | 3 | 3 | 5 | 20 | 3.3 |
| 情報家電 | 2 | 3 | 5 | 17 | 2.8 |
| 白物家電 | 3 | 2 | 5 | 18 | 3.0 |
| スマートメーター | 3 | 3 | 5 | 20 | 3.3 |
| フィットネス機器 | 3 | 3 | 4 | 19 | 3.2 |

評価法は「IoTインシデントの影響評価に関する考察」を参照

# 個別のリスク（脅威）評価

| システム例 | デバイス特性 | サービス特性 | デバイス数 | I | i |
|---|---|---|---|---|---|
| 医療用機器 | 5 | 5 | 1 | 26 | 4.3 |
| 自動車（運転制御） | 5 | 5 | 4 | 29 | 4.8 |
| 自動車（情報系） | 3 | 3 | 5 | 20 | 3.3 |
| 情報家電 | 2 | 3 | 5 | 17 | 2.8 |
| 白物家電 | 3 | 2 | 5 | 18 | 3.0 |
| スマートメーター | 3 | 3 | 5 | 20 | 3.3 |
| フィットネス機器 | 3 | 3 | 4 | 19 | 3.2 |

個々の影響要素でベース値を超える要素は、個別のリスク評価を脅威シナリオベースで行って、それに応じた対策項目を追加する

# 脅威シナリオベースの評価

脅威の選択（システムが攻撃対象となる可能性があるもの）

↓

シナリオの選択（攻撃の目的に応じたシナリオの選択：複数）

↓

手段の抽出（シナリオから用いられる手段を抽出：複数）

↓

可能性の評価と対策の検討（複合的な対策）

# 脅威シナリオ集

現在 IoT WGでとりまとめ中

▪A1. 家電製品の乗っ取りによる DDoS 攻撃

ある国際的なスポーツイベント当日、イベントの Web 情報サイトや、メディアセンターの
インターネット回線が使えなくなる障害が発生した。調べてみると
の IP アドレスから、DDoS 攻撃が発生し、ISP の回線すら飽和させ
発生していた。また、攻撃の一部は DNS を標的としており、DNS
上のサービスのアクセス不能、メールの不達などの影響も出た。攻
は、国内の主要な ISP の加入者に対し動的に割り当てられたもの
いるため、個別対処が困難となった。発生から数時間の後、ISP は
なく全加入者の利用を一時的に停止させたが、これによる社会的影
もたたず、インターネットが生命線の ISP とビジネスユーザに多
すことになった。後日、調査の結果、家庭内にある複数のインター
攻撃の発信元と判明した。

【原因】

家電製品へのマルウエア感染、ファームウエア改ざんなど複数の原

①家電製品の解析により、ファームウエアの動作とメーカーサー
を把握し、その脆弱性を把握。脆弱性を利用してメーカーサイトに
ームウエアを一斉配布した。この方法で改ざんされたデバイスは、
らのソフトウエア更新などは一切できなくなってしまった。

②一部の製品は、UPnP を使用したサービスに脆弱性があり、家庭
から攻撃可能な状態にあった。これらの製品は、外部から攻撃を受
ト実行させられてしまった。

③一部の家庭では、スパムメールに添付されたマルウエアに PC が
トワーク内の家電製品を探して、脆弱性を攻撃した。不要なサービ
かつそのサービスに脆弱性があった機器は、かなりの部分が進入を
を埋め込まれた。スパムメールは家電メーカーを騙った物で、複数
された。それぞれに、そのメーカーの家電製品攻撃に特化したマル

【対応策】

①製品とサービスの安全対策

・家電製品におけるファームウエアのリバースエンジニアリング抑止。たとえば、ファームウエアの難読化などによる解析作業の困難化。
・ファームウエア改ざんの防止。たとえば、パッケージへの電子署名と製品内のチップに保存された公開鍵による検証など。
・サービスサイトのセキュリティ強化。多数の製品を統括、管理するサイトは、高度な攻撃を受ける可能性が高く、リスクレベルは非常に高いという認識が必要。防御しきれない前提で、侵害の発見と対応を念頭においた対策が重要。

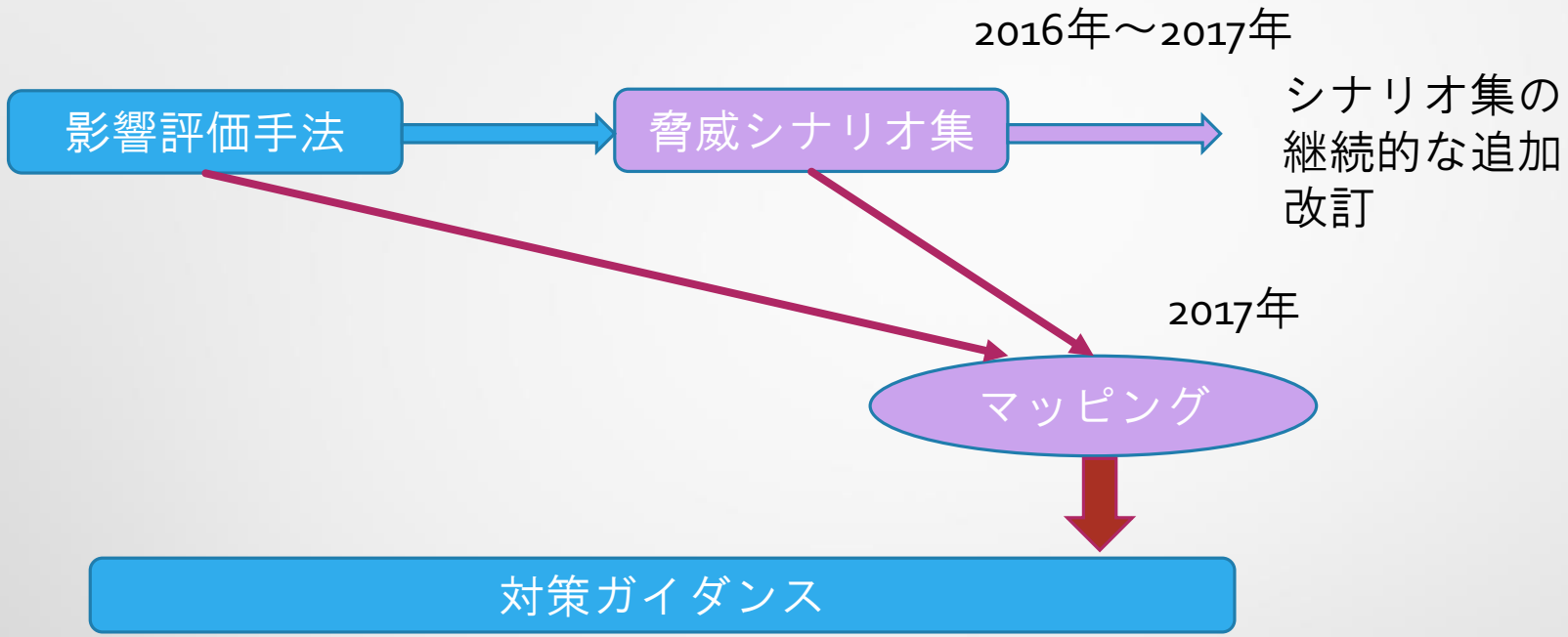
②UPnP を含む外部接続のセキュリティ強化

・UPnP 実装の脆弱性対策。発見された脆弱性が早期に修正されるような更新方法の実装。
・サービスポート開放の是非の再検討。安易に外部からのアクセスを受け付けるのではなく、内部側からのアクセスでサービスを行う方法を採用すること。

③PC 等のマルウエアからの攻撃対策

・DLNA 機能へのアクセス制御の強化。PC などネットワーク上のコンピュータからのアクセスは利用者が明示的に許可するまで禁止すること
・機器のシステムに汎用 OS を使用する場合、必要なサービス以外を確実に停止させ、かつファイアウォール機能を有効にして、外部からの不要なアクセスを、すべて遮断すること
・機器のファームウエアの脆弱性、とりわけ汎用ソフトウエアに含まれる脆弱性を確実に修正できるようなアップデート手段を実装すること

# Roadmap




IoT早期導入者のためのセキュリティガイダンス（日本語版）
Future Proofing The Connected World　（2017/01日本語化予定）

# 是非、WGに参加を

- 企業会員、個人会員メンバー募集中
- コラボレーション、意見交換先も募集中

**IoTで「明るい未来」を創造するために**

http://www.cloudsecurityalliance.jp/IoT_WG.html