# JPCERT/CCから見た IoTをめぐる脅威の現状

2017年11月30日

JPCERTコーディネーションセンター
早期警戒グループ
阿部 真吾

# JPCERT/CCとは

- **一般社団法人 JPCERT コーディネーションセンター**
  **Japan Computer Emergency Response Team / Coordination Center**
  - コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応など**国内の「セキュリティ向上を推進する活動」**を実施
  - **サービス対象: 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）**
  - インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**日本の窓口となる「CSIRT」**
    ※各国に同様の窓口となるCSIRTが存在する
    (例、米国のUS-CERT, CERT/CC, 中国のCNCERT, 韓国のKrCERT/CC)
- 経済産業省からの委託事業として、**サイバー攻撃等国際連携対応調整事業を実施**

「JPCERT/CCをご存知ですか？」

# JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

## 脆弱性情報ハンドリング

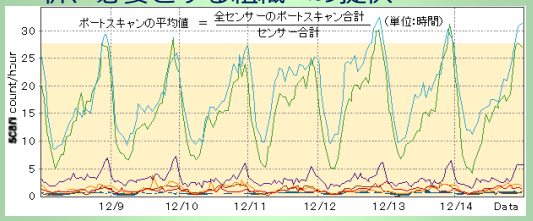
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

## 情報収集・分析・発信

**定点観測（TSUBAME）**

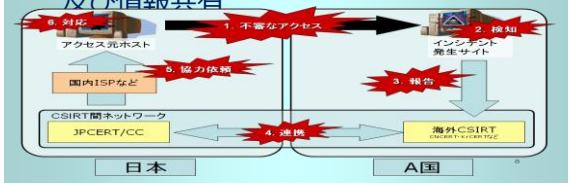
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供




## インシデントハンドリング

**（インシデント対応調整支援）**

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



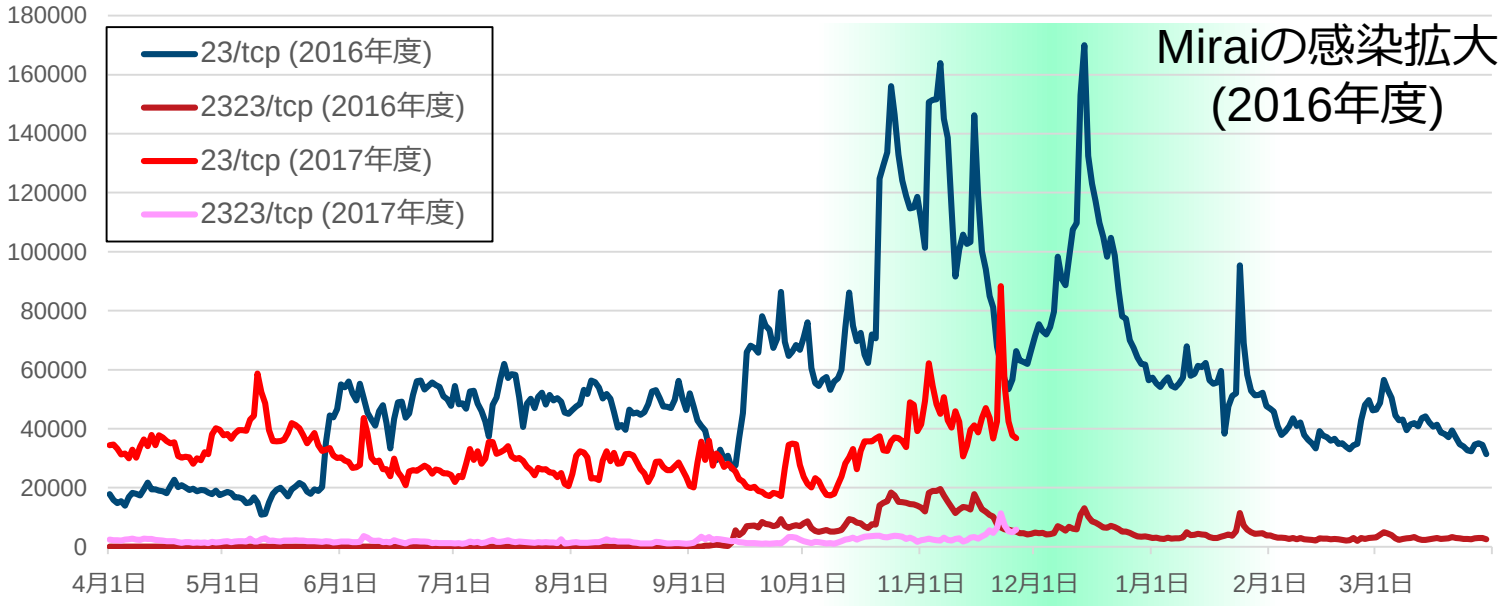

| | |
|---|---|
| **早期警戒情報** | 重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信 |
| **CSIRT構築支援** | 海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援 |
| **制御システムセキュリティ** | 制御システムに関するインシデントハンドリング/情報収集,分析発信 |
| **アーティファクト分析** | マルウエア（不正プログラム）等の攻撃手法の分析、解析 |
| **国内外関係者との連携** | 日本シーサート協議会、フィッシング対策協議会の事務局運営等 |
| **国際連携** | 各種業務を円滑に行うための海外関係機関との連携 |

# IOT関連のセキュリティ事例

# IoT botnetの問題は継続して発生

- 2017年の脅威予測として昨年末・年始に多く取り上げられていた問題
  - IoT botnetによるDDoS攻撃の活発化

- 23/tcp 及び 2323/tcp へのスキャン観測状況




**2017年度は、~1Tbpsという巨大なDDoSは観測されていないが、IoT botnetの問題は継続している**

# 最近の感染事例

- **Mirai 亜種**
  - 特定の機器にハードコードされたパスワードを悪用して感染
  - 多くの感染元はアルゼンチンだが、日本でも感染が確認されている

  (参考) http://blog.netlab.360.com/early-warning-a-new-mirai-variant-is-spreading-quickly-on-port-23-and-2323-en/

- **IoTroop Botnet (IoT_reaper)**
  - 脆弱なパスワードを悪用するのではなく、**機器の既知の脆弱性を悪用**し感染を拡大
    - D-Link, Netgear, Vacron, Linksys, AVTECHなどの製品の脆弱性が挙げられている
    - DDoS攻撃実行機能(DNS amp攻撃)が確認されている

  (参考) https://research.checkpoint.com/iotroop-botnet-full-investigation/

# IoTにおいて考えたい脆弱性の問題 ~2017年~

- **2017年はモバイル端末を含め広く影響を与える問題が複数指摘された**
  - “Broadpwn” Broadcom WiFi SoCにおける問題
  - “BlueBorne” の脆弱性
  - “KRACK Attacks” WPA2における問題

- **仕様・実装の問題や、製品の特徴を捉えた指摘**
  - コンソールを悪用される問題や、Web管理画面の脆弱性などではなく、プロトコルや実装の本質に議論が及ぶ
  - 脆弱性を現実に悪用するには、条件などの環境上の問題は残っているが、実証コードも公開される

# “BlueBorne”に関するさまざまなデモ

- Armisによるデモ
  - Google Pixelをリモートから操作するデモ
    - 任意のコードが実行される
  - Windowsからの PAN接続時の通信を摂取し、フォームの入力情報を取得するデモ
    - 中間者攻撃により情報を摂取される
  - “SmartWatch” への攻撃デモ
    - マイクで拾った音声が盗聴される

**“IoT” ならではの攻撃シナリオとなっている**

# セキュリティに関する対応を行う上での課題

# IoT全般の課題｜1

## IoT機器の課題

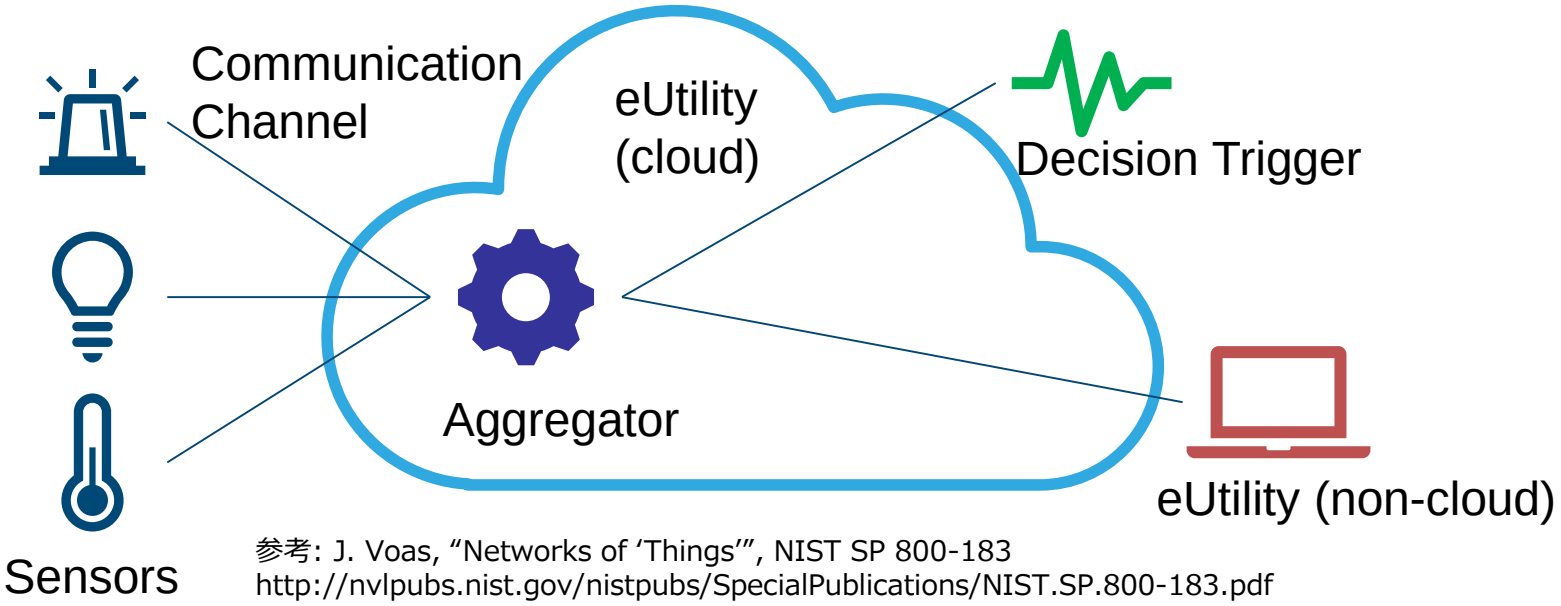
- 性能・機能の向上により“スマートな”機器に対する脅威はPCとほぼ変わらない
- 設置された後、適切にメンテナンスされない可能性も考慮する必要がある

## Internet of Threatsに関する課題

- IoTには、何かしらの“モノへの制御機能”が備わる
- モノのスケールが大きくなると Cyber-Physical Threatな問題に発展する可能性がある
- インターネットに“モノ”を直接接続することでセーフティに影響が及ばないかを考える必要がある
  - セーフティとセキュリティの両方の観点を考慮する必要がある

# IoT全般の課題｜2

- **IoTという言葉で認識する対象範囲の違いによる課題**
  - IoTの問題は機器だけでなく、クラウド、サーバ、ネットワークなどシステム全体の問題である
  - 開発者はそれぞれの立場で自分と繋がる“何か”を意識し、影響を考慮する必要がある
  - 開発者 (ベンダ) 、利用者 (ユーザ) 双方がシステム全体の特徴を知る必要がある

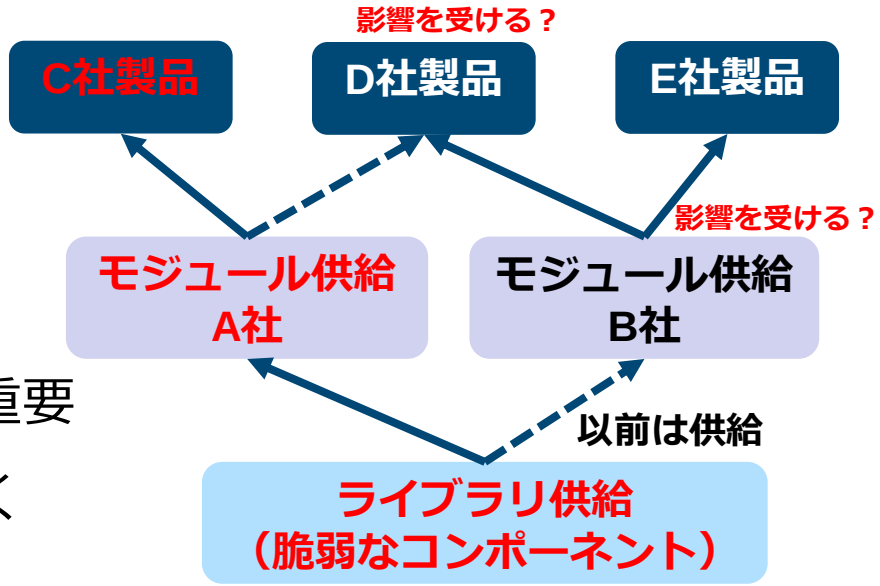



参考: J. Voas, “Networks of ‘Things’”, NIST SP 800-183
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

# 脆弱性に対する製品の管理における課題

- **ファームウエアや、サードパーティのライブラリなどでの脆弱性をどう考えるか？**
  - アップデートに対する製造者にかかる責任/負担
  - 最終的な製品がどの脆弱性の影響を受けるのか、影響範囲がどこまでなのかといった脆弱性の管理が必要
  - 開発が大規模になればなるほど、既知の脆弱性対策の反映が困難
    - 脆弱性情報の収集と取り纏め
    - 外部委託先での管理

- **IoT では、影響が広い範囲に及ぶケースも考えられる**
  - 製品に脆弱性が発見された場合、ユーザに不安を与えず、冷静に対処してもらうことも重要
  - 業界全体で対応を検討していくことも必要

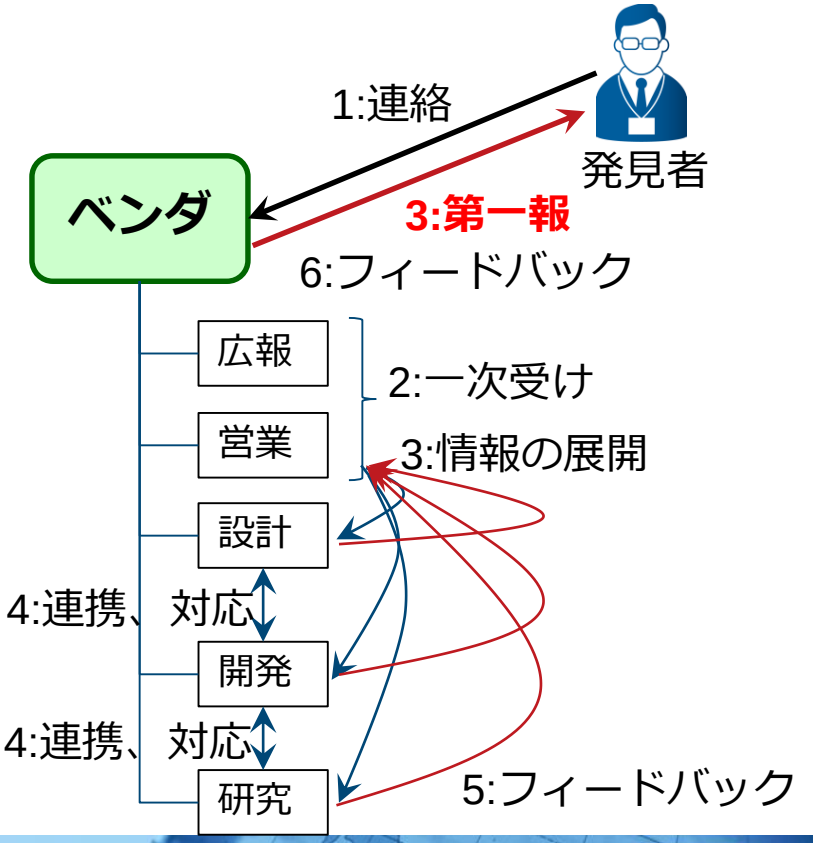



**サイバー攻撃を受けることを前提とした対策の検討が肝要**

# 組織内での部門連携の問題

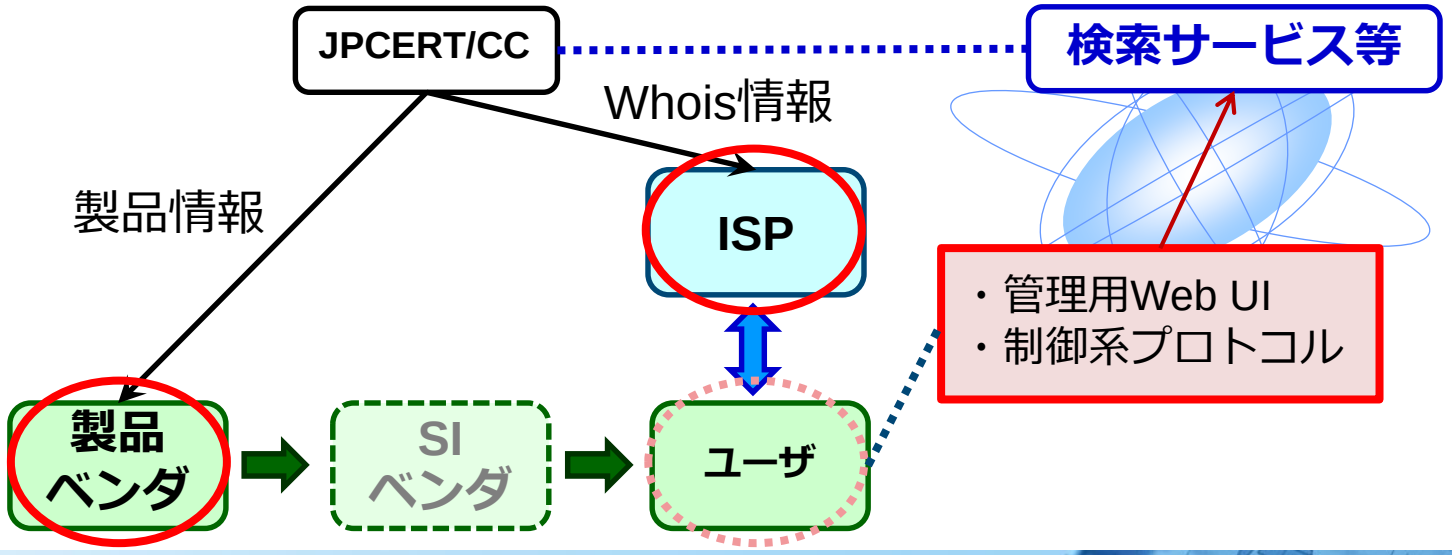
- セキュリティに関する情報が外部から届いたら・・・
  - セキュリティ担当者が直接外部からの情報を受け取るケースは少ない
  - 情報を受け取った人が適切な部署に情報を展開する必要がある
    - 情報のトリアージ
  - さらに内容によって組織内の様々な部門との連携が必要
    - 設計の見直し
    - コード修正、パッチ作成
    - テスト、リリース
    - 発見者への報告

**対応完了前に発見者がセキュリティに関する情報(脆弱性の詳細やPoCコードなど)を公開してしまう場合もあるので慎重な対応が求められる**



# JPCERT/CCがインシデント未然防止活動を行う上での課題

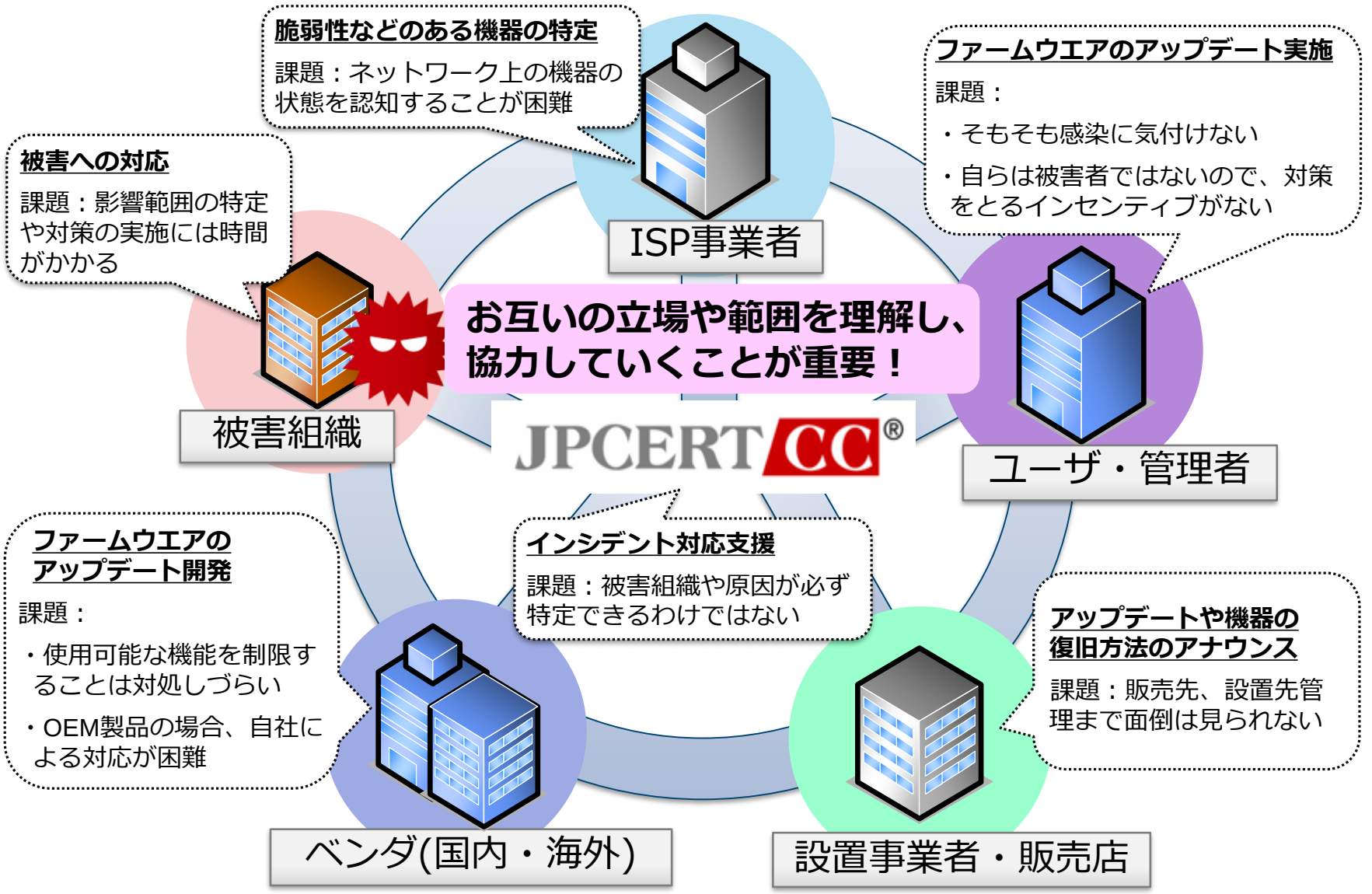
- 機器のIPアドレスから調査したWhois情報は多くの場合、ISPまでしか特定できない
  - 法律上の問題（通信の秘密）によってインシデント発生前にユーザ（アセットオーナ）を特定することが難しい
- 製品を特定し製品ベンダに連絡したとしても対応が限られる
  - ユーザ（アセットオーナ）の特定、（製品の範囲での）対策の実施が難しい



# IoT・製品を取り巻くエコシステムにおける課題｜1

- **想定外の利用によって発生しうるセキュリティ上の問題をどのように対応するのか**
  - 共通コンポーネント、ライブラリ、OSなど、共通するフレームワークに脆弱性があった場合、複数の製品など広い範囲に影響が出る可能性がある
    そのときに・・・
    - 誰がコストを負担するのか
    - 関係者に誰が説明するのか
    - 運用中のシステムに適用できるのか

# IoT・製品を取り巻くエコシステムにおける課題｜2



# 業界や関係者で情報共有を行うことの重要性

- **対策を進める上で、PSIRT の構築や、情報共有 (PSIRT間、同業他社、コミュニティ) がカギ**
  - 情報セキュリティの分野では、ISAC (Information Sharing and Analysis Center) による脅威情報の共有が進められている
  - 特に、脅威や影響などに関して共通の話題がある場合には情報共有は進みやすい

- **コミュニティでの取り組み例**
  - コンシューマ向けIoTセキュリティガイド
    http://www.jnsa.org/result/iot/
    - JNSA IoT セキュリティ WG にてとりまとめ (2016年)
    - 業界を横断して横のつながりで情報を整理
      - セキュリティベンダ、メーカ、その他

**コミュニティでの活動がIoTセキュリティにとって大きな役割を担ってくると考えられる**

# まとめ

# 2017年におけるIoTセキュリティの動向

## インシデントに関する問題

- IoT botnetの問題は継続中
  脆弱なパスワードの悪用だけでなく、製品の脆弱性を悪用するケース (IoT reaper) も観測されている
- botnet だけでなくフィッシングサイトやサイバー攻撃の踏み台にされている事例も観測されている

## 脆弱性に関する問題

- 仕様や実装の問題や特徴がよく考えられた指摘が続いた
- 現在はまだ、Web管理インターフェースにある脆弱性が悪用されているものが多いが、今後はより攻撃が複雑になっていく可能性がある

# おわりに

- **インターネットに接続されたモノに対する脅威は増加している**
  - 脆弱性の問題の悪用にも注意
  - 脆弱性への対策は、製品の運用時だけでなく、製品を作る際においても考慮が不可欠
- **実際の攻撃では一瞬のスキを突かれてしまう**
  - アップデートまでの時間差
  - 仕様上の問題、実装上の問題
  - 共通ライブラリにおける脆弱性などの問題
- **IoT・製品を取り巻くエコシステムに対する課題**
  - インシデントを防止、軽減するためにも同業他社、業界を超えた協力が不可欠

**セキュリティに関して何かございましたら、JPCERT/CCまでご一報ください！**

# お問合せ、インシデント対応のご依頼は

**JPCERTコーディネーションセンター**

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

**インシデント報告**

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

**制御システムインシデントの報告**

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form

# ご静聴ありがとうございました