2017年11月30日（木）
第22回日本インターネットガバナンス会議（IGCJ22)
ヒューリックホール＆ヒューリックカンファレンス

ICT-ISACにおける
IoTセキュリティの取組みについて

一般社団法人ICT-ISAC
IoTセキュリティWG　主査
NTTコミュニケーションズ株式会社　則武　智

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

一般社団法人ICT-ISAC

- 通信事業者、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者などから構成
- 安全なICT社会の形成に寄与することを目的として設立

名称　　：一般社団法人ICT-ISAC
発足　　：2016年3月9日
所在地　　：東京都港区虎ノ門2-5-5 櫻ビル8階
HPのURL　：https://www.ict-isac.jp/public/about.html

【活動内容】

1．情報セキュリティに関する情報収集・調査・分析
ICTに関わる情報セキュリティ対策に資する情報（インシデント情報を含む。）を収集、調査、分析する活動

2．情報共有の推進（情報共有）
情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ会員企業間で相互協調する仕組みを整備し、それを促進する活動

3．セキュリティ人材の育成、セキュリティ啓発（普及啓発・人材育成）
会員企業のセキュリティ人材育成を促進する活動およびユーザが安全にICTを利用するための普及啓発活動

4．セキュリティガイドライン等の整備に関する活動
会員各社がセキュリティ対策を円滑に行う上で必要となるガイドラインの検討および法制度に関する政府研究会等への参画活動

ICT-ISACのメンバー構成とWG活動

ICT-ISAC JAPAN

メンバー構成

通信系	SIベンダ系	放送系	セキュリティベンダ系
- ISP - 通信キャリア - 携帯キャリア	- ルータベンダ - FW/NATベンダ - 通信機器メーカ - SIer - IoTベンダ - 家電メーカ	- 放送事業者 - CATV事業者	- アンチウイルス事業者 - セキュリティコンサル

WG活動

業界特化系

通信系	SIベンダ系	放送系	セキュリティベンダ系
経路情報共有-WG	デバイス脆弱性ハンドリング検討-WG	放送設備サイバー攻撃対策-WG	セキュリティベンダ課題検討WG
ACCESS-WG			
SoNAR-WG			
DoS攻撃即応-WG			

業界横断系

- 情報共有-WG
- 人材育成WG
- 脆弱性保有ネットワークデバイス調査WG
- IoTセキュリティの取組み
- DNS運用者連絡会
- サイバー攻撃対応演習-WG
- IoT調査-WG
- ACTIVE業務推進-WG
- サイバー攻撃への適正対処検討のためのWG
- WiFiリテラシー向上WG
- IoTセキュリティ-WG

ICT-ISACがIoTセキュリティに取組むべき背景

脆弱なIoT機器を狙った攻撃が深刻度を増す中、ICT-ISACとして取組むべき方向性について議論が必要となった。

ICT-ISACを取り巻く状況（2016年）

- IoTを踏み台とした大規模のDDoS攻撃が発生（Mirai botnetなど）
- ICT-ISAC会員企業が提供するIoT機器やサービスなどがサイバー攻撃の対象となるリスクの増加(対策が必要となる)
- IoTセキュリティに関してはこれまでのPCを中心としたセキュリティと異なり対策手法は未整理

ICT-ISACとして取組むべき「IoTセキュリティ対策」に関する議論が必要

ICT-ISAC SC運営委員を中心とした検討会を開催（2016年8月～9月）

IoTセキュリティを検討するWGを設置（2016年9月）

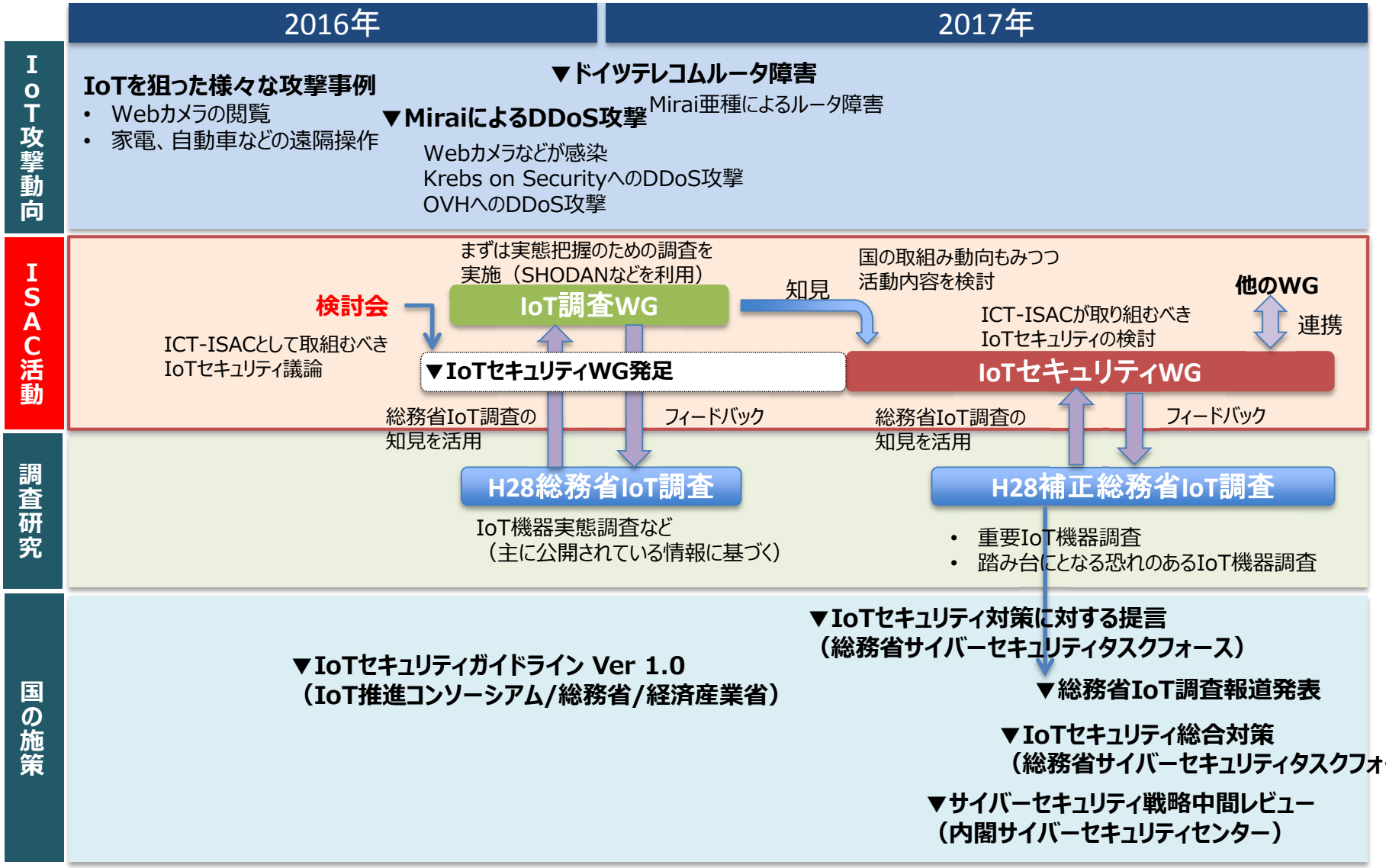
IoTセキュリティに関する２つのWG

IoTセキュリティWG（2016年9月～現在）
IoTセキュリティに関する対策の推進

IoT調査WG（2016年12月～2017年3月）
- ICT-ISACが取組むべき方向性を検討するため、脆弱なIoT機器の実態調査を実施
- 実態調査に特化した期間限定のWG

ICT-ISACが取組むべきIoTセキュリティについて
実態調査、対策検討、ICT-ISAC他WGとの連携、国の施策との連携を通して推進する

IoTセキュリティの動向とICT-ISACの取組み



ICT-ISACにおける活動の特徴と活動

IoTセキュリティWG（IoT調査WG含む）の特徴

- ISPの運用技術者やセキュリティ企業の技術者、研究者などの専門家から構成される
- 各社の運用上の課題をタイムリーに議論し、各社に持ち帰ることができる
- ICT-ISACが進める総務省IoT調査の知見を活用し、議論できる
- 関連する他のWGとの連携も視野に入れている

現在までの活動

IoT調査WG（2016年度）

- 日本国内に設置されたサイバー攻撃の踏み台となる恐れのある特定ポート（23/tcp,80/tcpなど）がインターネットに公開されている機器を主にIoT機器検索サービス(SHODAN,Censys)を用いて調査
- その他ネットワークスキャンの実施やサイバー攻撃事例の共有など

調査から見えてきた問題点

IoT検索サービスを用いた調査手法では、ある程度脆弱なIoT機器の状態はわかるが、実態把握には不十分

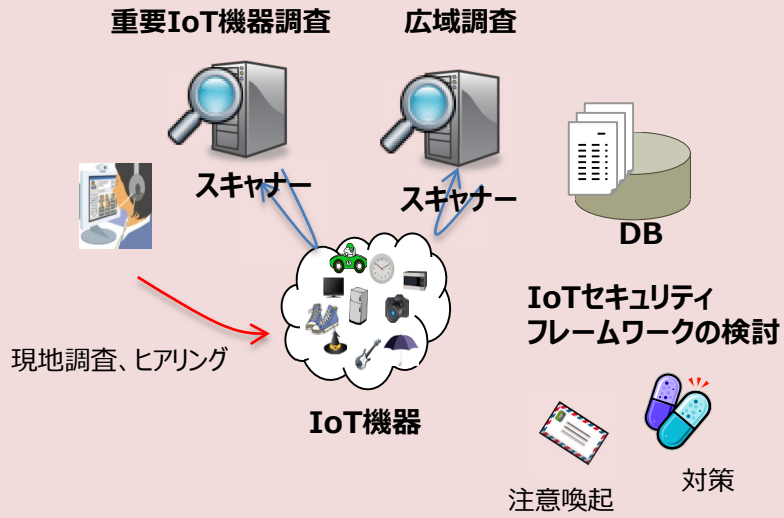
- IoT検索サービスの信頼性
- IoT機器名特定の困難性
- 検出された機器の脆弱性評価
（ポートが開いていたら脆弱か？）

課題

- 調査手法についての検討と更なる調査
- 対策すべき対象機器と対策手法、ステークホルダーの整理

IoTセキュリティWG【2017年度）

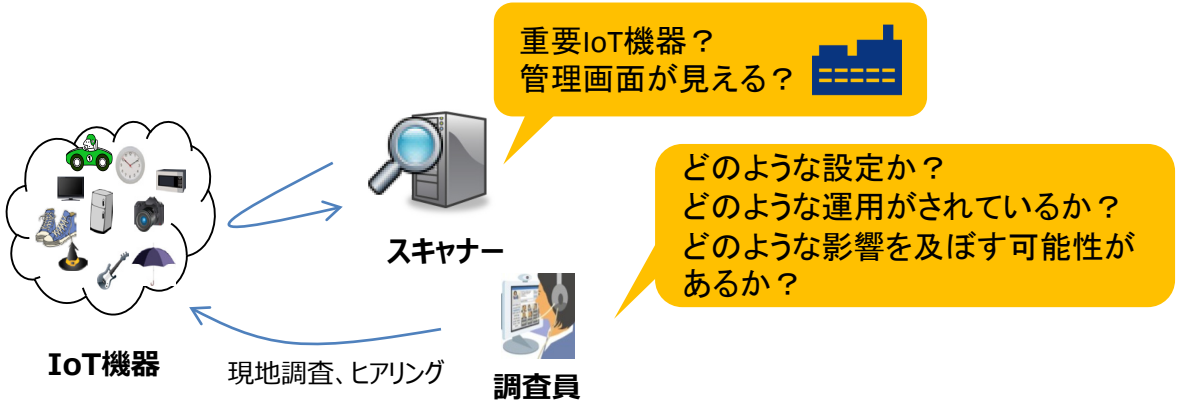
- サイバー攻撃により社会に大きな影響を及ぼす可能性のある日本国内重要IoT機器の調査
- 日本国内に設置されたサイバー攻撃の踏み台となる恐れのあるIoT機器のスキャン調査（広域調査）
- IoTセキュリティフレームワーク(対策）の検討



総務省IoT調査の概要

重要IoT機器のセキュリティ対策に関する調査（重要IoT機器調査）

サイバー攻撃により社会に大きな影響を及ぼす恐れのあるIoT機器を検出し、現地調査を含めた実態調査を実施



サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがあるIoT機器のセキュリティ対策に関する調査（広域調査）

日本国内にある特定ポート（80/tcp、23/tcpなど）がオープンであるIoT機器の調査と対策を検討

（参考）総務省報道発表

ICT-ISACは
横浜国立大学と連携し、
IoT機器に関する
脆弱性調査等を実施

平成29年9月5日

IoT機器に関する脆弱性調査等の実施

総務省は、一般社団法人ICT-ISAC、国立大学法人横浜国立大学等と連携して、重要IoT機器を中心にIoT機器の実態調査を行い、脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。

1 経緯等

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や社会経済活動確保の観点から重要な課題となっています。

IoT機器については、その性質から、サイバー攻撃の対象になりやすく、IoT機器を狙ったサイバー攻撃は年々増加傾向にあります。また、諸外国においても、深刻な被害が発生しています。

このような状況を踏まえ、「IoTセキュリティ対策に関する取組方針ver1.0」（平成29年4月12日サイバーセキュリティタスクフォース提言）及び「2020年及びその後を見据えたサイバーセキュリティの在り方について」（平成29年7月13日サイバーセキュリティ戦略本部決定）において、IoT機器に関するセキュリティ対策が取りまとめられたところです。

2 実施概要

上記を踏まえ、総務省は、一般社団法人ICT-ISAC、国立大学法人横浜国立大学等と連携し、サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を行います。サイバー攻撃の対象になりやすい脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。また、必要に応じ製造事業者等に対し脆弱性に関する技術的な情報提供を行います。

・（概要：別紙参照）

【関係報道資料等】
・「IoTセキュリティ対策に関する取組方針ver1.0」（平成29年4月12日公表）
http://www.soumu.go.jp/main_content/000478813.pdf
・「2020年及びその後を見据えたサイバーセキュリティの在り方について」
（平成29年7月13日 内閣サイバーセキュリティセンター公表）
http://www.nisc.go.jp/active/kihon/pdf/csway2017.pdf

http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html

（参考）ICT-ISAC報道発表

ICT-ISACは
横浜国立大学と連携し、
IoT機器に関する
脆弱性調査等を実施

2017年9月6日
一般社団法人ICT-ISAC

脆弱なIoT機器の調査及び注意喚起について

一般社団法人 ICT-ISAC（アイシーティ・アイザック）【所在地：東京都港区、 理事長：齊藤忠夫、 以下、ICT-ISAC Japan】は、国内のISPを含む通信事業者に加え、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者等、幅広い分野の会員と連携し、サイバーセキュリティの観点から、安全な情報通信技術（ICT）社会の形成に寄与する活動を推進しております。

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や、社会経済活動確保の観点から重要な課題となっています。
IoT機器については、その性質から、サイバー攻撃の対象になりやすく、IoT機器を狙ったサイバー攻撃は年々増加傾向にあります。また、諸外国においても、深刻な被害が発生しています。

このような状況を踏まえ、ICT-ISAC Japanでは、総務省、国立大学法人横浜国立大学等と連携し、サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を行います。サイバー攻撃の対象になりやすい脆弱なIoT機器およびその所有者等を特定した場合には、所有者等に対し注意喚起を行います。また、必要に応じ製造事業者等に対し情報提供を行います。

○関連情報
・総務省
IoT機器に関する脆弱性調査等の実施
http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html

https://www.ict-isac.jp/news/news20170906.html

IoTセキュリティWGの進め方

インプット

- サイバー攻撃動向
- サイバー攻撃対策技術
- 総務省IoT機器調査
  - 重要IoT機器調査
  - 踏み台となる恐れのあるIoT機器調査
- 国内外の政策動向など
- メンバーからの情報共有

議論

IoTセキュリティWG

- 脆弱なIoT機器の実態把握
- 対策の検討
- 情報発信

連携

ICT-ISAC内関連WGとの連携

知見の共有と対策などの検討

- ACTIVE業務推進-WG（マルウェア対策など）
- SoNAR-WG（ABUSE対応など）
- その他の関連WG

アウトプット

ICT-ISACが取組むべきIoTセキュリティ

- 関連組織との情報共有
- 対策推進への取組み

（参考）IoT調査WGにおける議論の例

WGメンバーなどからのインプット

IoT機器検索サービスを用いた実態調査

動的IPアドレスにおける脆弱なIoT機器スキャン調査報告

脆弱なブロードバンドルータとIoT機器のスキャン調査報告

ドイツテレコムルータ障害（2016年11月）に関する情報共有

最新IoTセキュリティ（Miraiその他の状況など）報告

インプット

IoT調査WG

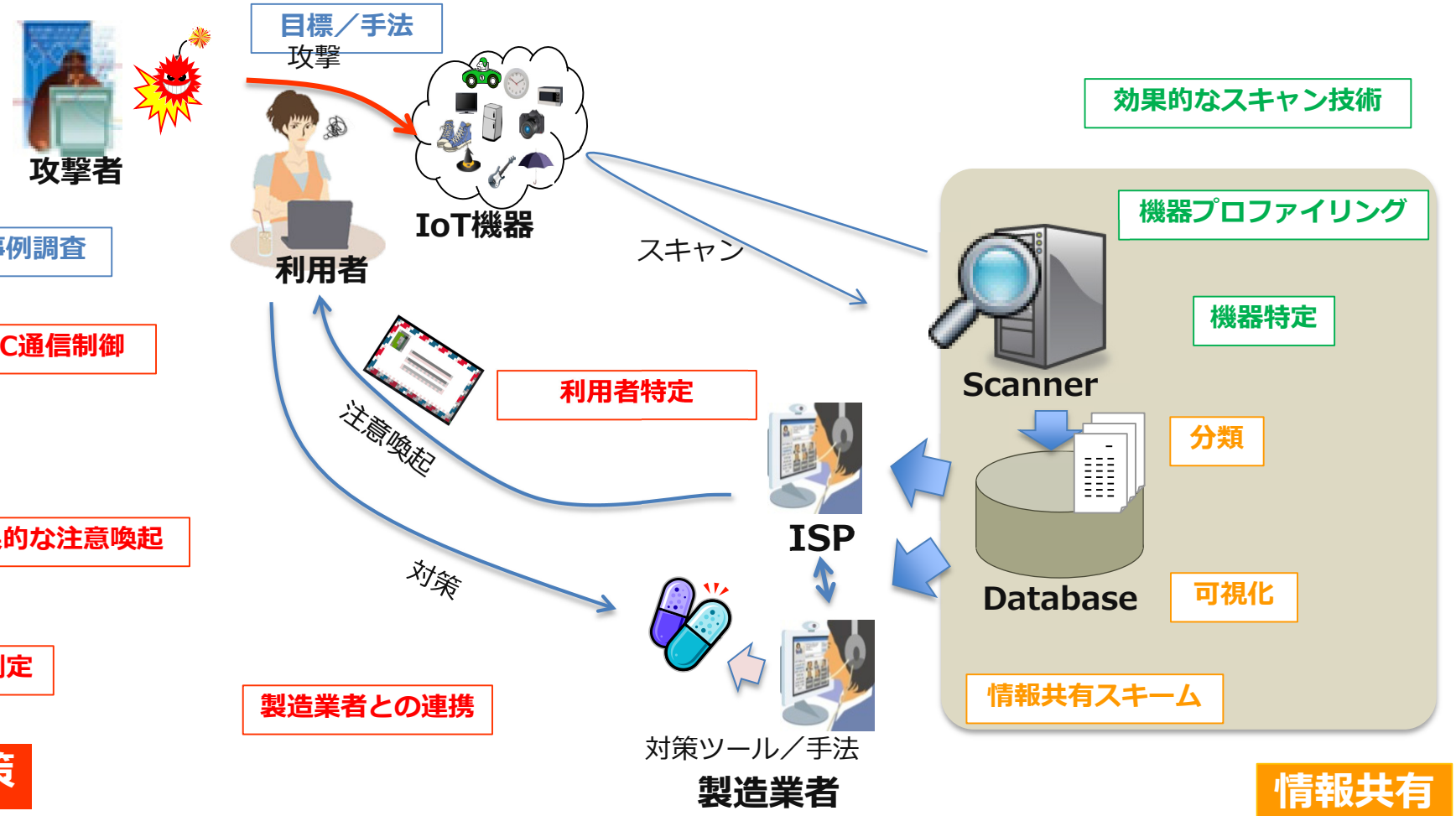
脆弱なIoT機器の実態把握とICT-ISACの取るべき方向性に関する議論

（参考）IoTセキュリティフレームワークのアイデア

IoTセキュリティフレームワークを検討する上でのキーワード
IoTセキュリティWGで意識していく取組み

サイバー攻撃動向の把握

検知



今後の課題

既に世の中に出回っている脆弱なIoT機器の実態を把握し、**安心・安全なインターネット社会**を目指していくために考えること

- 様々なステークホルダーとどのように連携していくか？
- 対策の必要性を誰にどのように伝えていくか？
- 対策はだれの責任で進めるべきか？コストはどうするか？