資料38－4

# IoT機器のセキュリティ対策への取組みについて

**平成30年4月27日**

**一般社団法人 電子情報技術産業協会**

# 一般社団法人 電子情報技術産業協会（JEITA）の概要

- ◆ JEITAは国内外で約36兆円の規模を持つIT・エレクトロニクス産業を担うわが国最大級の業界団体
- ◆ 設　立：2000年11月1日(EIAJとJEIDAが統合)
- ◆ 会員数：394社(正会員291社　賛助会員103社　2018年3月14日現在)
- ◆ 会　長：長榮　周作　パナソニック株式会社　取締役会長
- ◆ 目　的：電子機器、電子部品の健全な生産、貿易及び消費の増進を図ることにより、電子情報技術産業の総合的な発展に資し、わが国経済の発展と文化の興隆に寄与する
- ◆ 領　域：電子機器、電子部品/材料、電子デバイス、ITソリューション・サービス等

## ◆ 基本方針 *Society 5.0*の推進

高度な情報活用による世界に先駆けた「超スマート社会」の実現（*Society 5.0*）に向け、異業種、ベンチャー、海外等とも連携し、成長分野に関わる課題の検討や政府への提言など、会員の新たな取組みを促進するための活動にスピード感を持って取り組む。

また、会員の競争力強化のため、規制・制度改革や税制改正要望等の事業環境整備に着実に取り組んでいく。これらの事業を推進することにより、IT・エレクトロニクス産業ならびにわが国の経済・社会の発展に貢献していく。

## ◆主な事業活動

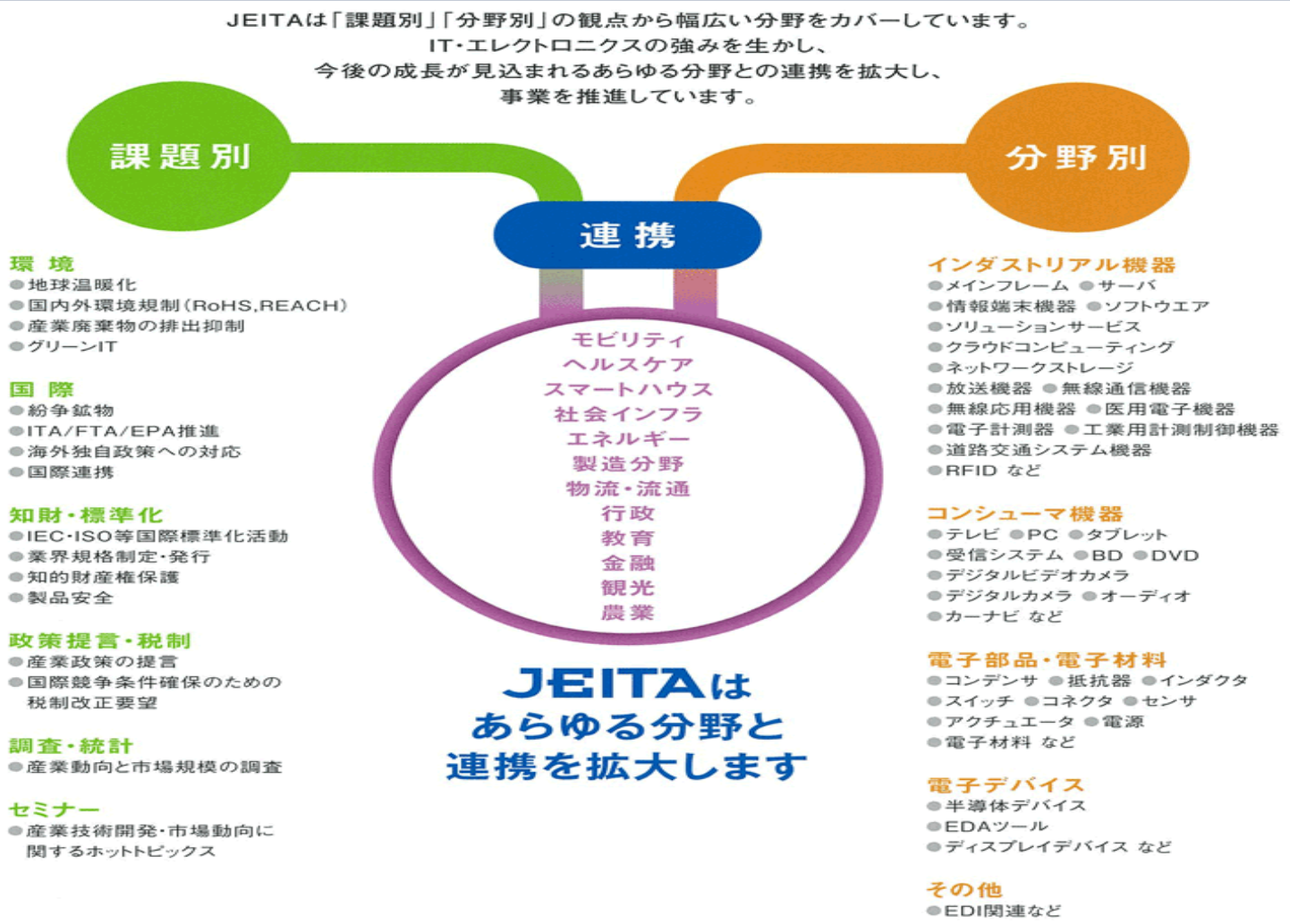
**政策提言**：CPS/IoTの推進
税制改正/規制改革

**調査統計**：幅広い製品分野の動向把握

**課題解決**：社会的要請や業界共通課題解決に向けた取組み

**市場創出**：共創と競争によるイノベーションを促し、新たな市場創出のための事業。「CPS/IoTの総合展」CEATEC JAPAN開催など

# JEITAの主な対象分野




- ◆ 対象分野:電子機器(産業/民生)～部品・材料、デバイス等多岐。
- ◆ モビリティ、ヘルスケア等様々な分野で利用
- ◆ IoT時代にネットに繋がり製品は多数

# 実世界とサイバー空間が相互連携した社会

家、社会、車、街中で・・・様々なシーンでIoT機器・システムが新たなサービス実現に貢献！


今後の考えられるIoT製品(例)

・家庭内で使われる照明やエアコン、冷蔵庫、洗濯機、電子レンジ、炊飯器などの白物家電。

・センサーデバイス。
自動運転カーと交通インフラを共有する可能性のある移動体（自転車やバイク、場合によっては歩行者）

・スマートホームで利用される玄関の鍵、等々

出展：JEITA webより：https://www.jeita.or.jp/cps/about/to2020/

# １．JEITAのサイバーセキュリティ対策

## ■JEITAとしての取組み

IoT技術によるデータ連携により、技術革新が急激に進展し、新たなサービス創出が期待されている。一方で、各対象分野共通で、機器/サービスの信頼性確保上、サイバーセキュリティ対策は最も重要な課題と認識し、以下の活動を行っている。

① パブコメを通じた、業界意見の提出
② サイバーセキュリティ関連ガイドラインの周知
③ CEATEC等を活用し、有識者等のセミナー主催、サイバーセキュリティ対策重要性の周知
④ 海外の関連団体とも連携した諸外国におけるサイバーセキュリィ関連動向把握、ルール整備への対応
⑤ 「サイバーセキュリティ対策検討WG」及び「セキュリティ対策室」の設置により自主的な取り組みの推進を図っていく。
＜主な活動案＞
- 対象機器に対するサイバーセキュリティ対策の検討
- 業界（各社）のサイバーセキュリティ対策の周知

# 1．JEITAのサイバーセキュリティ対策

## ■IoT機器のサイバーセキュリティに対する考え方

1. IoTのセキュリティ対策は、ネットワーク全体、個々の対象機器、運用等、極めて幅広く影響が及ぶが、一律的な対策を避け、重要度や各機器の特性に応じたメリハリある対策を講じるべき。

2. 国境を越えるサイバー空間において、サイバー攻撃はグローバルに展開されるため、サイバーセキュリティ確保のためには、国際連携が不可欠である。
   また、市場のグローバル展開が加速しているなか、日本独自の施策、対応は市場の成長を損なう。国際的な基準や諸外国の制度とのすり合わせ、連携などによる取が必要である。

3. 今後、産業界としてもサイバーセキュリティ対策を自主的に推進することが重要と考える。また政府も、官民による検討の場を設けるなどして、政府として一本化した体制で、サプライチェーン全体、国際的な動きを見据えた合理的な施策を検討頂きたい。

# １．JEITAのサイバーセキュリティ対策

## ■IoT機器のサイバーセキュリティに関する自主的取組みについて

産業構造や社会構造が大きく変わりつつあるなか、当協会は、高度な情報活用による世界に先駆けた「超スマート社会」の実現（Society 5.0）に向け、異業種、ベンチャー、海外等とも連携し、新たなビジネスの創出に取り組んでいる。

IoTが社会のあらゆる分野に浸透し、これまで接続されていなかった機器が、インターネットに接続され、DDoSのようなサイバー攻撃等、新たな脅威が発生している。

セキュリティ対策が産業界共通の重要課題と認識しており、IoT推進コンソーシアム、総務省、経済産業省策定の「IoTセキュリティガイドライン」等に沿い、IoT機器のセキュリティ対策に取り組んでいる。

今後、ユーザーにセキュリティの確保された製品を提供するために、当協会は所管するIoT機器について、取り組みの可視化も含めて具体的な自主的対応策を検討する。

# 2．JEITAでの検討にあたっての考え方

「IoT機器のセキュリティ対策」の検討については、各社からの意見に基づき、下記のような項目を十分に勘案して、対策を進めて行きたい。

＜製造業者の責任＞

個々の機器に必要なサイバーセキュリティ対策を行うことは、製造メーカーの基本的な責務と考える。既に、会員各社は各社独自にセキュリティ確保に取り組んでいる。

＜日々替わるセキュリティ対策＞

しかしながら、サイバー攻撃は年々増加し、かつ複雑かつ巧妙化している。脅威は日々変化し、当然、対策も日々変化せざるをえない。

＜運用等を含んだ総合的な対策の中での機器の対応＞

また、セキュリティ対策は、機器独自の対策だけでなく、ネットワークやシステム全体の運用も含むセキュリティ対策と組み合わせた総合的な対策が必要であり、複数の種類のIoT機器に一律の対策を行うことは難しく、その有効性を慎重に検討する必要がある。

＜セキュリティ対策コスト＞

セキュリティ対策に必要なコストも上記の総合的な対策の中で検討されるべきであり、その機器が使われる用途・環境を十分に加味しないといたずらに不必要なコストアップにつながる懸念がある。

＜セキュリティ対策の見える化＞

セキュリティ対策の顧客・消費者への見える化は重要であるが、その見える化が何を担保するのか誤解を生まないよう慎重な運用が必要。

＜グローバル市場に対する対応＞

多くの機器の市場はグローバルであり、セキュリティ対策は、国際標準化や国際的な規格との親和性があることが望ましい。

# 3．JEITAの検討体制

- 理事会
  - 総合政策部会
    - 総合政策委員会
      - サイバーセキュリティ対策検討WG
  - スマートホーム部会
    - スマートホームサイバーセキュリティWG

※経産省産業サイバーセキュリティ研究会WG1　スマートライフ分野SWGとして機能
※検討項目

Step1. スマートホームサプライチェーンで活用できる「サイバー・フィジカル・セキュリティ対策フレームワークの策定
Step2. 各事業者が実際のセキュリティ対策オペレーションレベルの活用のための実効的な施策検討
Step3. スマートホームからスマートライフ分野に対応したセキュリティ対策について検討

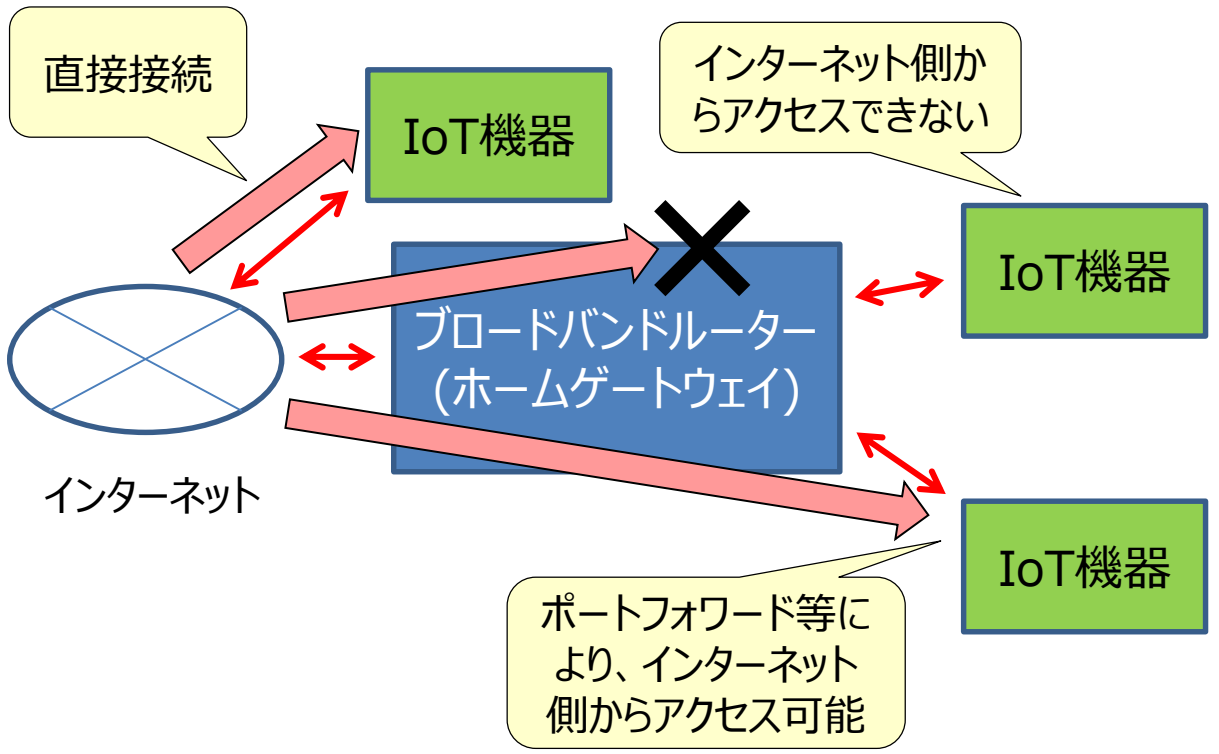
# ４．セキュリティ対策が必要と考えられる製品

セキュリティ対策が必要と考えられる機器について、サイバーセキュリティ検討WGメンバー各社による例示（JEITA関連製品以外も含む）

| 機　器　名 | 理由(一部のみ) |
|---|---|
| ネットワーク(監視）カメラ | ・乗っ取られた場合、踏み台となり、DDoS攻撃に利用される。重大情報（個人情報、プライバシー映像）を取得・保持する可能性があるため |
| 上記付属の映像レコーダー(DVR) | |
| ルーター（ホームゲートウェイ等） | グローバルネットワークからの家庭内ネットワークの入り口となるため，家電製品のセキュリティ対策としてその対策強化は最も重要 |
| スマートスピーカー | 個人のプライバシーが音声情報を通じて漏洩する可能性がある。また、家庭内のIoT機器を制御する機能をもつなど、乗っ取られた場合の影響が大きい |
| テレビ・レコーダー・STB等宅内機器 | 昨今のMirai事案の攻撃対象となりうる |
| 医療用機器 | 人命に関わる製品であるため |
| 複合機（MFP） | DDos攻撃などにより「つながる相手に迷惑をかけない」という視点（IoTセキュリティガイドライン　要点９）から |
| 車載ゲートウェイ・自動運転制御系機器 | 車載へのリモート攻撃の事例が報告されており、車の基本的な機能（走る、曲がる、止まる）の誤動作は直接人命にかかわる可能性がある |
| 家庭用ゲーム機器 | 多く台数が出回っていると共に、高い演算機能を備えていることから、DDoS攻撃の踏み台として利用されることが懸念される |
| スマートメーター | 金銭に関わる製品であるため |
| NFC関連 | 金銭に関わる製品であるため |

# 5．想定する接続形態例

■機器の利用において想定する接続形態例
（同じ機器でも、利用形態により接続形態が異なる）

| 機　器　名 | 接 続 形 態 |
|---|---|
| ネットワーク(監視）カメラ、<br>または<br>ネットワーク(監視）カメラ<br>＋　上記付属の映像レコーダー(DVR) |  |
| ルーター（ホームゲートウェイ等） | |
| スマートスピーカー | |
| テレビ・レコーダー・STB等宅内機器 | |
| 医療用機器 | |
| 複合機（MFP） | |
| 車載ゲートウェイ・自動運転制御系機器 | |
| 家庭用ゲーム機器 | |
| スマートメーター | |
| NFC関連 | |



※左記機器の全てを網羅した調査に基づくものではない。

# 6．対策例

## ■攻撃対象としてリスクの高いネットワークカメラについての脅威・対策の例

| 機 器 名 | 脅威（例） | 資産への侵害 | | | 対策（例）（会員企業事例） |
|---|---|---|---|---|---|
| | | C | I | A | |
| ネットワーク(監視）カメラ、<br>または<br>ネットワーク(監視）カメラ<br>＋上記付属の映像レコーダー(DVR) | 画像/映像が詐取される | ✓ | | | ＜セキュリティ確保の取組み（例）＞<br>企画段階での脅威分析、セキュアコーディング、独立部門による脆弱性診断（ポートスキャンやパスワード脆弱性チェック等、機器の特性や脅威を考慮し様々な観点から診断）等<br><br>＜機能/設定（例）＞<br>・不要なTCP/UDPポートを閉じて出荷<br>・ID/パスワードによる認証機能。パスワード変更機能。初回立ち上げ時パスワード強制入力必要(8文字以上, 大文字・小文字を区別、英字・数字・記号のうち2種類以上使用）<br>※ビジネス用途等、より高いセキュリティが求められる高価格帯機種については、カメラへデバイス証明書を組み込むことによりSSL通信を行うなど高度な対策を実施。<br><br>(注)上記は一例であり会員企業それぞれにおいて、機器の利用用途、お客様要求等に応じ、機種やシステムごとに様々な対策を講じている。 |
| | 画像/映像が改ざんされる | | ✓ | | |
| | カメラやDVRが不正に設定、制御される | | | ✓ | |
| | 踏み台にされる | | | ✓ | |

対策は接続形態や脅威毎に示したものではない

C: Confidentiality(機密性), I: Integrity(完全性), A: Availability(可用性)

# 7．セキュリティ対策規定に関する課題

■IoT機器のサイバーセキュリティに関する取組みを行っていく上で、対策が講じられている（セキュリティ機能が実現されている）こととして規定する場合の課題

1. 情報の機密性、完全性、可用性を確保するために、さまざまな対策が考えられる。
   製品の特性や、使われる環境によりセキュリティの脅威やリスクは異なる。インターネットに直接つながる場合もあれば、セキュアなルーターを介する場合もあり、接続や認証の形態も一律ではない。広い範囲の機器や環境に対して、何らかの条件定義を行わず、一律の対策として規定するのは難しいと考える。

2. 対策が必要となる諸条件の絞り込み等が不十分なまま一律の対策を規定した場合、本来対策の必要がない機器や別の対策で対応している機器においては、不必要な機能追加や設計変更等が発生する可能性がある。
   諸条件等の定義は、さまざまな要因を考慮し、最大限慎重に検討しなければならないと考える。

3. 既に販売・設置もされている機器への対応を検討する必要である。
   極めて対応が難しいと考えるが、ファームウェアのアップデートなどにより対応が可能な場合もある。その場合も、対策がされているかどうかを明示するのか、明示するとしたならば、どのように行うのかなど課題も多い。

以上のように、対策を規定する場合は慎重な検討が必要である。

# ８．今後の取組みについて

1. JEITA関連製品での取組み
「対策」を一律に規定することによる実効性や実現性については、まだまだ多くの課題があり、ネットワークカメラを含むJEITA関連製品の対策の在り方については、政府での関連の検討の状況も踏まえつつ、検討する。

2. 関連した検討の場への参画
対策（技術要件）、評価要件等の検討の場に参画し、JEITAの関連していない製品やネットワークとの調和を考慮し、JEITA関連製品対応について取組みを行っていく。

ご静聴ありがとうございました。

JEITA