IPA

IoT製品・サービス脆弱性対応ガイド

安全安心なIoT製品・サービスを提供するために

～ 経営者・管理者向け：企業が実施すべきIoT脆弱性対策のポイント ～

本資料の目的と想定する読者

本資料の目的

本資料は、IoT製品※・サービスの提供における、セキュリティ対応に対する企業の責任の考え方や、脆弱性対策が必要な理由等を解説し、セキュリティ対応に企業として取り組んでいただくことを目的としています。

本資料が対象とする読者

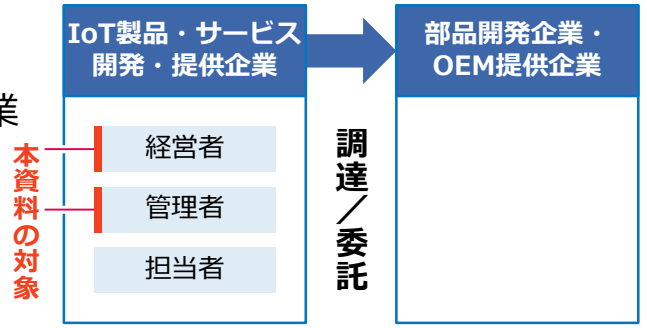
本資料は、次の方にお読みいただくことを想定しています。

対象企業

- IoT製品を開発・提供されている企業
- IoTサービスを開発・提供されている企業

対象者

- 経営者
- 管理者



本資料の使い方

経営者や管理者の方には、本資料により脆弱性対策の**必要性を理解いただいた**後、**担当者にお渡しいただく**ことで、本資料をより広く活用いただくことを期待しています。

また、IoTサービス開発・提供者が製品開発者に調達/委託する際にも本資料をご活用ください。

担当者の方が対策を検討する際には、具体的な対策を示した参考資料等もご参照ください。（参考資料参照）

※ 本資料においてIoT製品とは通信機能を有し、ネットワークに接続される製品全般を指します。

エグゼクティブ・サマリ ～経営者の皆様へ～

背景

- IoT技術の進展に伴い、利用者の生活がより便利になる一方、脆弱性を起因とした攻撃により、**利用者への被害が発生するリスク**も高まっています。

IoT製品・サービスに対する攻撃や事故

- 利用者に被害が発生すると、開発企業において**レピュテーションの低下**や、製品回収や損害賠償等による**企業経営への影響**が発生します。

IoT製品・サービスの脆弱性対応の必要性

- IoTの脆弱性対応は、**利用者を守るため**、そして**自社への信頼を高めるため**に必要です。
- 経営者は、安全安心なIoT製品・サービスを提供するために、**率先して脆弱性への対応方針を策定**し、**対外的に示す**ことが必要です。
- **セキュリティ対策を「コスト」ではなく、将来の事業活動・成長への「投資」**と捉え、**セキュリティ対策予算の確保と体制の整備**を行うことが必要です。
- IoTでは、**モノの提供からサービスの提供へビジネスモデルが転換**していきます。
  継続的にサービスを提供する中で、脆弱性対応を維持管理の一環として考えることが有効です。

目 次

資料中に引用したアンケート調査結果については、四捨五入しているため、構成比の合計が必ずしも100%とはならない場合があります。

1. IoTに潜むリスク

1.1. セキュリティ対策を行わないと・・・

利用者への影響

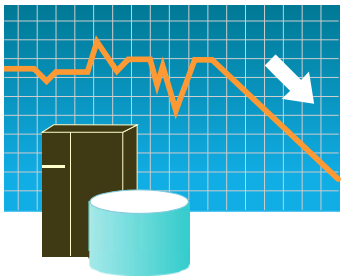
セキュリティ対策が不完全なIoT製品・サービスは以下のような被害を利用者にもたらす恐れがあります。

- 情報流出・改ざん
- IoT製品の不正操作・障害、それに伴う生命・身体に対する影響

企業経営への影響

利用者に被害が出た場合、当該製品・サービスを提供した企業の経営へ悪影響が発生すると考えられます。

- 他社製品への乗り換えによる売上の低下、マーケットシェアの低下
- 製品回収コストの発生、損害賠償による損害
- ブランドの毀損
- 社員モチベーションの低下、人材の流出・採用への影響



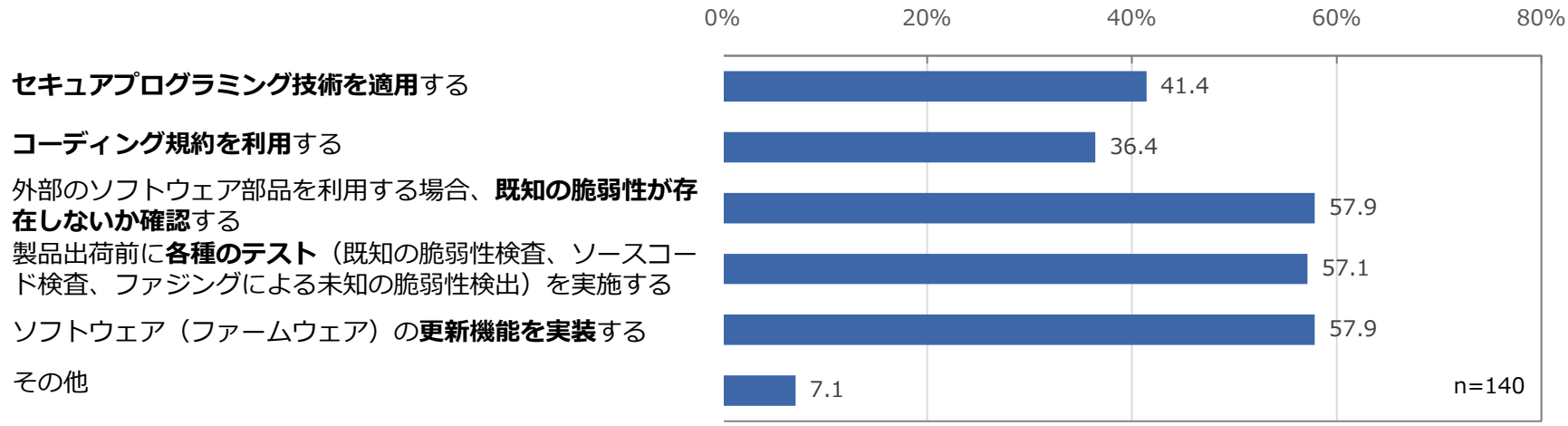
社会への影響

DDoS攻撃の踏み台となり、IoT製品利用者が他者への攻撃に加担させられる可能性があります。
それによって、インターネットの障害等、社会的な混乱も引き起こされます。

脆弱性へのトータルな対応はまだまだ進んでいない

2017年度にIPAにおいて、日本国内のIoT製品・サービスを開発している企業205社に対し、アンケート調査※を実施したところ、脆弱性対策を考慮している企業は約7割という結果が出ています。ただし、更新機能の実装等の**脆弱性対策を行う企業はまだ少ない**のが現状で、特に、セキュアプログラミング技術の適用やコーディング規約の利用等の製品設計段階における脆弱性対策を行う企業は約4割でした。

IoT製品・サービスの開発段階で脆弱性対策を考慮している企業の状況



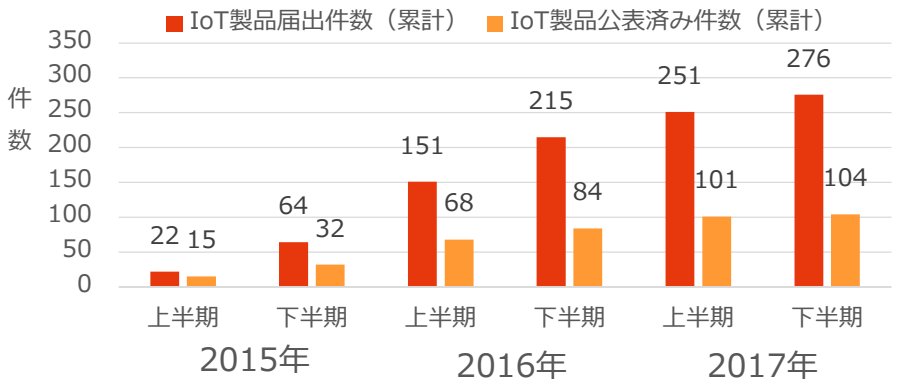
※ IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）

増加するIoT製品の脆弱性届出

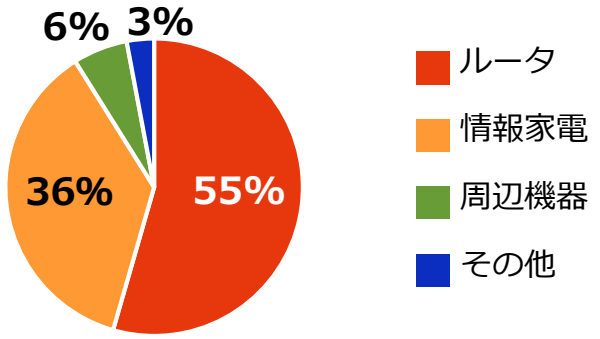
IoT技術の進展に伴い、利用者の生活がより便利になる一方、IoT製品が身近になることで、脆弱性を原因とした利用者への被害が発生するリスクも高まっています。

IPAが運用する「脆弱性関連情報の届出受付制度」に届け出られたIoT製品の脆弱性は、2015年～2017年において276件に上りました。また、対策が完了し公表された脆弱性は届出の38%にとどまります。公表された脆弱性の多くは、ルーターまたは情報家電の脆弱性でした。

2015年～2017年における、IoT製品届出件数と公表件数



2015年～2017年における、IoT製品の公表件数の種類別内訳



IoT製品・サービスの脆弱性対策は十分ではなく、
対策が完了していない脆弱性も多いのが現状です。

2. IoTが攻撃されたら

2.1. 利用者へ影響する事例（1）

IoT製品における通信の盗聴・傍受、それに伴うプライバシーに対する侵害

IoT製品の脆弱性によって、個人のプライバシーが侵害される場合があります。

事例 1 カメラの覗き見サイト

2016年1月：米国・日本・各国

- ロシアのウェブサイトにより覗き見できる監視カメラが世界中に多数存在していることが露呈された。しかもその数が膨大で、映像を閲覧できる件数は、**米国の監視カメラは5,000件以上**、**日本の監視カメラは1,800件以上**（2017年11月時点）であった。

事例 2 通信の傍受・改ざん

2017年10月：日本・各国

- セキュリティ専門家は、WPA2の脆弱性を利用し、**通信を傍受・改ざんする実演内容をYouTubeで公開した。**それに対し、NISC（内閣サイバーセキュリティセンター）とIPAが注意喚起を行い、関連する製品の開発企業はパッチを作成し、リリースした。

2.1. 利用者へ影響する事例（2）

IoT製品の不正操作・障害、それに伴う生命・身体に対する影響

IoT製品の脆弱性によって、生命・身体に危険をもたらす場合があります。

事例 3 自動車の不正操作

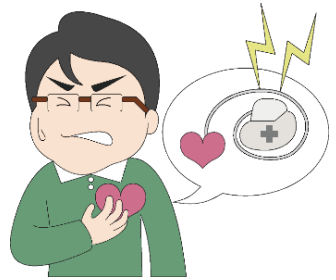
2015年7月：米国

- セキュリティの専門家が、専用無線回線を通じて、**外部から自動車のエンジンを切ったり、ワイパーを動かしたり**する実験を成功させたため、開発企業は**約140万台のリコールを実施した。**今回、利用者への実害はなかったが、実験により脆弱性が発見できなければ、人命に影響した可能性があった。

事例 4 医療機器の不正操作・障害

2017年8月：米国

- ネットワーク経由の攻撃により、**ペースメーカーのバッテリ寿命を消耗させたり、心拍数及び心拍リズムを変更したりすることができる**脆弱性が発見され、開発企業はパッチの作成で対応した。



2.2. 企業経営へ影響する事例

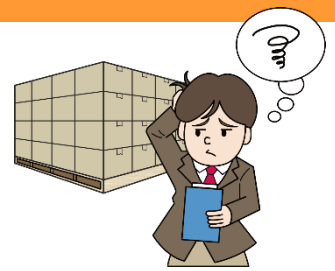
製品回収や販売停止

IoT製品に脆弱性が発見された場合、想定される被害の大きさ次第では、レピュテーションの低下にとどまらず、製品回収や販売停止等を行わざるを得ない可能性があり、IoT製品の開発企業の経営に大きな影響も及ぼしかねません。

事例 5 ポケットルータの店頭在庫回収

2016年10月末：日本

- 第三者による遠隔操作が可能となる脆弱性が発見され、開発企業は**店頭の在庫を回収**し、HPで情報を公開した。11月下旬に脆弱性を対処済みの製品の出荷を再開した。



事例 6 モバイルストレージの出荷停止

2016年12月：日本

- サイバー攻撃に悪用される可能性のある脆弱性がモバイルストレージに確認され、開発企業は**出荷を停止**した。翌年の9月に脆弱性を対処済みの製品の出荷を再開した。

2.3. 社会へ影響する事例（1）

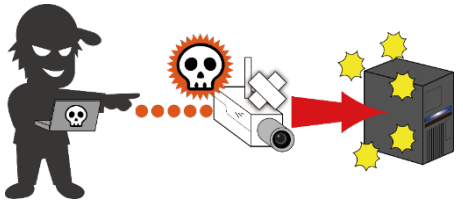
攻撃の踏み台

IoT製品が脆弱性によって乗っ取られ、他者の機器への攻撃の踏み台として使われることで、利用者が攻撃に加担させられ、社会に大きな影響を与える可能性があります。

事例 7 ネットワークカメラが乗っ取られる可能性

2016年12月：日本

- ネットワークカメラに複数の脆弱性があることが発見された。この脆弱性は、条件が整えば、当該機器を**乗っ取り、任意で操作したり、踏み台として攻撃に加担させられたり**する可能性がある。開発企業は情報をHPで公開し、その後パッチのリリース等で対応した。



狙われるネットワークカメラ

- ネットワークカメラの普及に伴い、DDoSの踏み台として狙われる可能性が高まっています。
- 2017年7月19日、米国のニュースサイトThreatpostはネットワークカメラに関する脆弱性の影響範囲の広さを示す研究を報道しました。当該研究では、ある開発企業が提供している251のモデルのうちに249のモデルが同じ脆弱性を有し、また34社以上のソフトウェアベンダ等にも影響があると指摘しました。

2.3. 社会へ影響する事例（2）

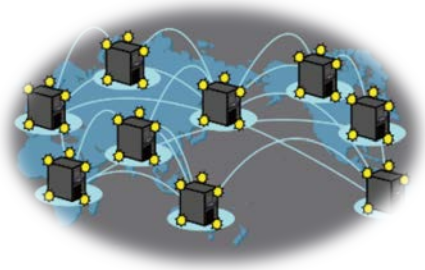
IoT製品の脆弱性やパスワード設定不備等によって起こるDDoS攻撃

脆弱性だけではなく、パスワードの設定不備によっても、IoT製品が攻撃の踏み台になってしまう場合があります。

事例 8 IoT製品を踏み台にした大規模DDoS攻撃の多発

2016年10月：各国

- 不正プログラム「Mirai」に感染した**10万台**を越えるIoT製品によって、以下のITサービスを中心にDDoS攻撃を受け、**世界的にITサービスが停止した。**
  - フランスホスティング事業者「OVH」
  - セキュリティブログ「KrebsOnSecurity」
  - DNSサービスプロバイダ「Dyn」
    よってTwitter、SoundCloud、Spotify、Redditといった企業のウェブサイトが影響を受けた。



2017年11月：南米・北アフリカ・各国

- 「Mirai」の亜種は、南米、北アフリカをはじめ、各国にあるネットワークカメラ、デジタルビデオレコーダー等の**IoT製品を踏み台にし、約380万回以上の攻撃を実行した。**

セキュリティ対策が不十分なIoT製品が、大規模なDDoS攻撃を引き起こしました。

3. IoTの脆弱性対策とは

脆弱性対応は、お客様を守り、自社の信頼を高め、社会的要請に対応すること

IoTの脆弱性対応により高いセキュリティ品質を実現することは、企業価値や競争力の源泉となります。

1. お客様を守るため	多くの利用者は、使っている製品やサービスの脆弱性に気づけません。利用者が危険な状況から脱し、リスクを低減するためには、製品開発者による脆弱性対応が不可欠です。
2. 自社への信頼を高めるため	脆弱性対応は、企業が世に出した製品やサービスの品質を保つ取組です。脆弱性情報やパッチの提供等の対応について公表し、品質を維持していることを利用者に示すことは、説明責任を果たすとともに、自社の信頼を高めることになります。
3.社会的要請に対応するため	脆弱性によりサイバー攻撃の踏み台となり、意図せず攻撃に加担してしまうことにより、社会全体に重大な影響を及ぼすことがあります。社会の一員として脆弱性対応に取り組むことは、企業の社会的責任(CSR)の1つです。

経営者は、セキュリティの責任を持ち、方針を示すことが必要

IoTのリスクには利用者への影響や企業経営・存続に関わる影響をもたらす可能性があります。
経営者が責任を持ち、率先して脆弱性への対応方針を策定し、対外的に示すことが必要です。

実施事項

IoT製品・サービスのセキュリティに取り組む予算の確保、体制の整備を行うこと

- IoTセキュリティに関する基本方針の策定、社内への周知
- 継続的な実現状況把握、見直し
- セキュリティに必要な予算の確保、体制・人材の整備

サプライチェーンに対するセキュリティ対策を行うこと

- 系列企業等のビジネスパートナーを含めたセキュリティ対策

平時及び緊急時のいずれにおいてもステークホルダーとコミュニケーションを行い、信頼醸成を図ること

- 利用者へセキュリティ対策に関する適切な情報開示
- 社外からの報告・問い合わせ窓口の設置
- 緊急時に備えた社内の体制・ルールの整備（緊急時対応計画の施策・危機管理広報体制の整備等）

管理者は、脆弱性に対処した製品を選定することが必要

IoT製品の調達時に脆弱性に対処した製品を選定することが必要です。

実施事項 製品・サービス開発者 サービス提供者

契約において脆弱性対処の項目を含めること

- 調達時の要求仕様及び運用・保守契約における脆弱性対処の明示

管理者は、脆弱性を作り込まず、対処可能とすることが必要

できるだけ脆弱性を作り込まないこと、見つかった脆弱性を適切に修正することの両方が重要です。

実施事項 製品・サービス開発者

脆弱性を作り込まないこと

- セキュリティ設計への考慮、脆弱性を作り込まない開発

見つかった脆弱性に対処可能とすること

- 脆弱性を適切に修正可能な機構の作り込み

管理者は、脅威の抑制と脆弱性対応を行うことが必要

運用/保守時には、脅威（被害の原因）の抑制と脆弱性対応の両方に取り組む必要があります。

実施事項　製品・サービス開発者　サービス提供者

継続的にシステムの状態を把握し、脆弱性対策を行うこと

- IoT継続的な脆弱性対策情報の収集
- 脆弱性対策情報（更新ソフトウェアを含む）の作成
- 更新ソフトウェアの製品への適用

利用者に対し、脆弱性の存在を公表し、回避策を提示すること

- 脆弱性が存在することを説明し、更新を促進
- 更新版がなく対策の適用が困難な場合には、当該製品・サービスの使用を避けるよう説明

関係者（部品開発企業等）との協力関係を築くこと

- 自社だけではできない脆弱性への対応

4. IoTによくある課題と対応

4.1. セキュリティ対策コスト

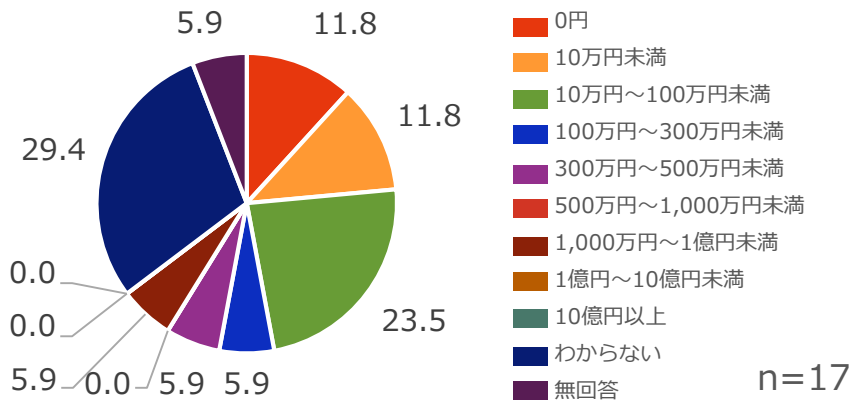
課 題

- レピュテーションや企業の社会的な責任が重視されています。
- しかし、IoTは安価な製品・サービスも多く、**セキュリティ対策のコストを販売価格に転嫁することが困難**な場合もあります。

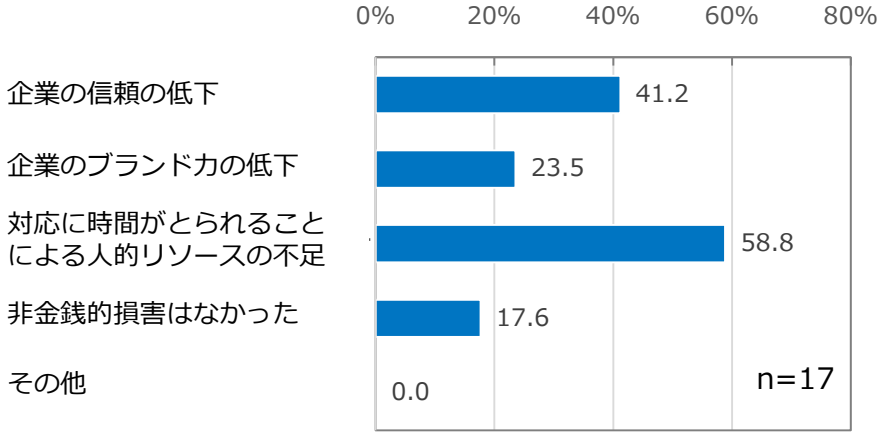
対 応

- 事故発生時の対応コストを考慮すると、**事前に対策を講じていた方が、総合的にはコストの低減**につながります。
- 顧客から安心・安全を理由に製品・サービスを選定されるようにすることで、セキュリティ対策コストは**リターンを生む投資につながる**ものと位置づけて予算を検討してください。

脆弱性事故による金銭的被害※



事故による非金銭的な損害※



※ IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）

4.2. セキュリティ人材の不足

課 題

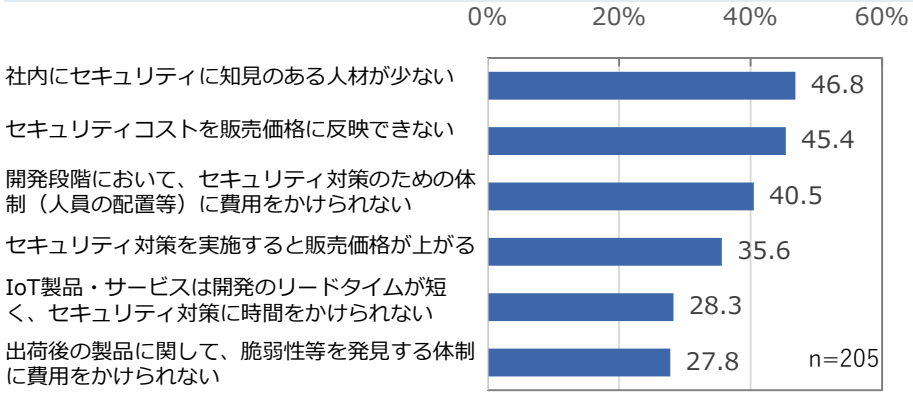
- IoTのセキュリティに関する専門知識を持った人材が社内にいない場合があります。
- IPAの調査※1によると、5割近くの会社が、**社内にセキュリティに知見のある人材が少ない**ことが、IoT製品のセキュリティ対策の阻害要因になっています。
- 国全体でも、**今後高度セキュリティ人材が不足**するとの調査結果※2もあります。

対 応

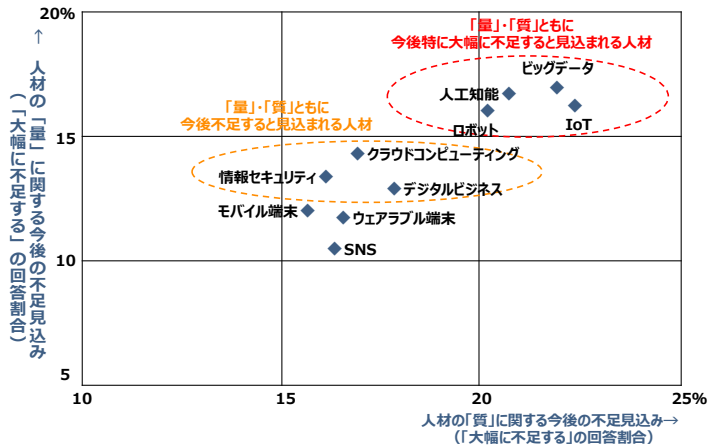
- 以下のような外部リソースで、セキュリティ人材不足の緩和を検討しましょう。

1. 公的ガイドライン等の**評価が確立された知見**の活用
2. **セキュリティを考慮**した開発・運用委託
3. **セキュリティが考慮されたミドルウエア・製品・サービス**の活用
4. **外部専門家**の活用
5. 中長期的にはセキュリティ人材を社内で育成し、評価する仕組を整えましょう。

セキュリティ対策の課題（上位6項目）※1



今後不足する先端IT人材※2



※1 IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）
※2 経済産業省「IT人材の最新動向と将来推計に関する調査結果」（2016年）

4.3. 長期間に渡る保守・運用

IPA

課 題

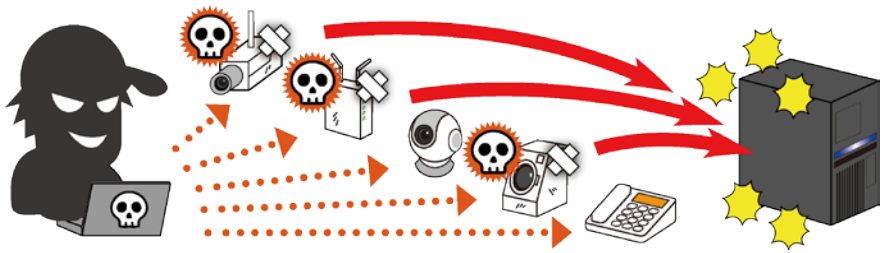
- IoTは、何十年も使われ続ける場合も想定しなければなりません※1。
- しかし、販売終了した製品・サービスについて、**脆弱性対応の体制を維持し続けることは困難**です。
- 旧製品の開発チームの解散等により、パッチを開発することも難しくなります。

対 応

- 製品・サービスについては、**販売後のセキュリティサポート※2方針を設定**し、利用者には事前に周知することが重要です。
- セキュリティサポート終了後に脆弱性が発見された場合、**回避策の提示**や**使用中止を呼びかけたり**、**後継製品への移行**を呼びかけたりする等の配慮が必要となります。

保守・管理されなくなったIoT製品の課題

- 保守・管理されなくなったIoT製品は、「サイバーデブリ」「野良IoT」等と呼ばれ、攻撃の踏み台として利用されることで社会への影響を引き起こす等、インターネット環境における一種のゴミ問題となる可能性が指摘されています。



※1 PCとIoTの耐用年数の違い（法定耐用年数）：建物の設備としてのIoT＝15年、PC＝4年～5年。 ※2 セキュリティサポートとは「脆弱性対策を含むセキュリティ対応」を示します。

4.4. 外部委託の活用

IPA

課 題

- 自社だけでIoT製品・サービスを開発提供することは難しくなっています。海外製品を利用したり、海外に開発・製造を委託したり等海外依存も高まっています。
- しかし、**海外等の外部委託先の管理は難しい**場合があります。
- ソフトウェア開発を外部委託する場合、出荷後に脆弱性が発覚すると、パッチの作成等が困難になる場合があります。

対 応

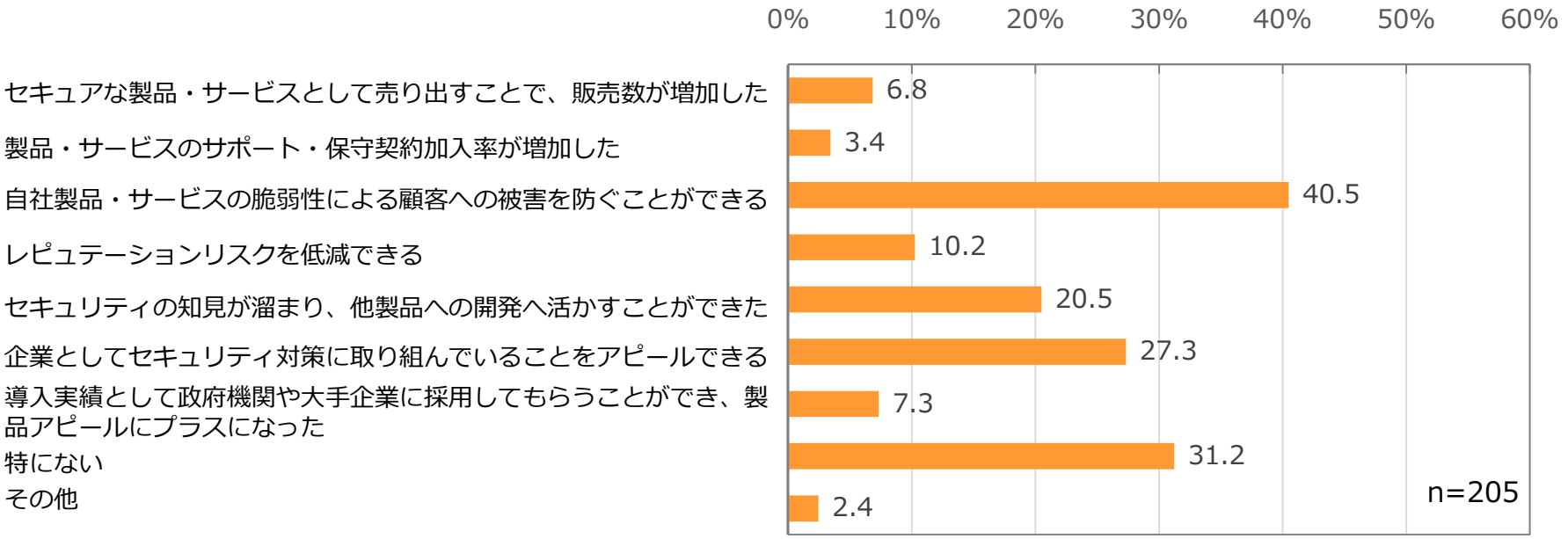
- 自社の製品・サービスの品質維持のため、**委託先との契約**に運用時の対応や責任の明示、委託先が対応できない場合の**代替策**の検討等が必要です。OEM製品も、同様の考慮が必要です。
- IoTの場合、開発時のコストだけを考えるのではなく、**製品ライフサイクルを通じた開発・運用コストを考慮**し、自社で実施するか外部委託するか検討してください。

IoTのセキュリティ対策による効果

コラム

- 2017年度のIPAの調査※によると、IoTのセキュリティ対策による効果として、「自社製品・サービスの脆弱性による顧客への被害を防ぐことができる」ことに加え、「企業としてセキュリティ対策に取り組んでいることをアピールできる」が約3割挙げられました。
- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要です。

セキュリティ対策による効果※



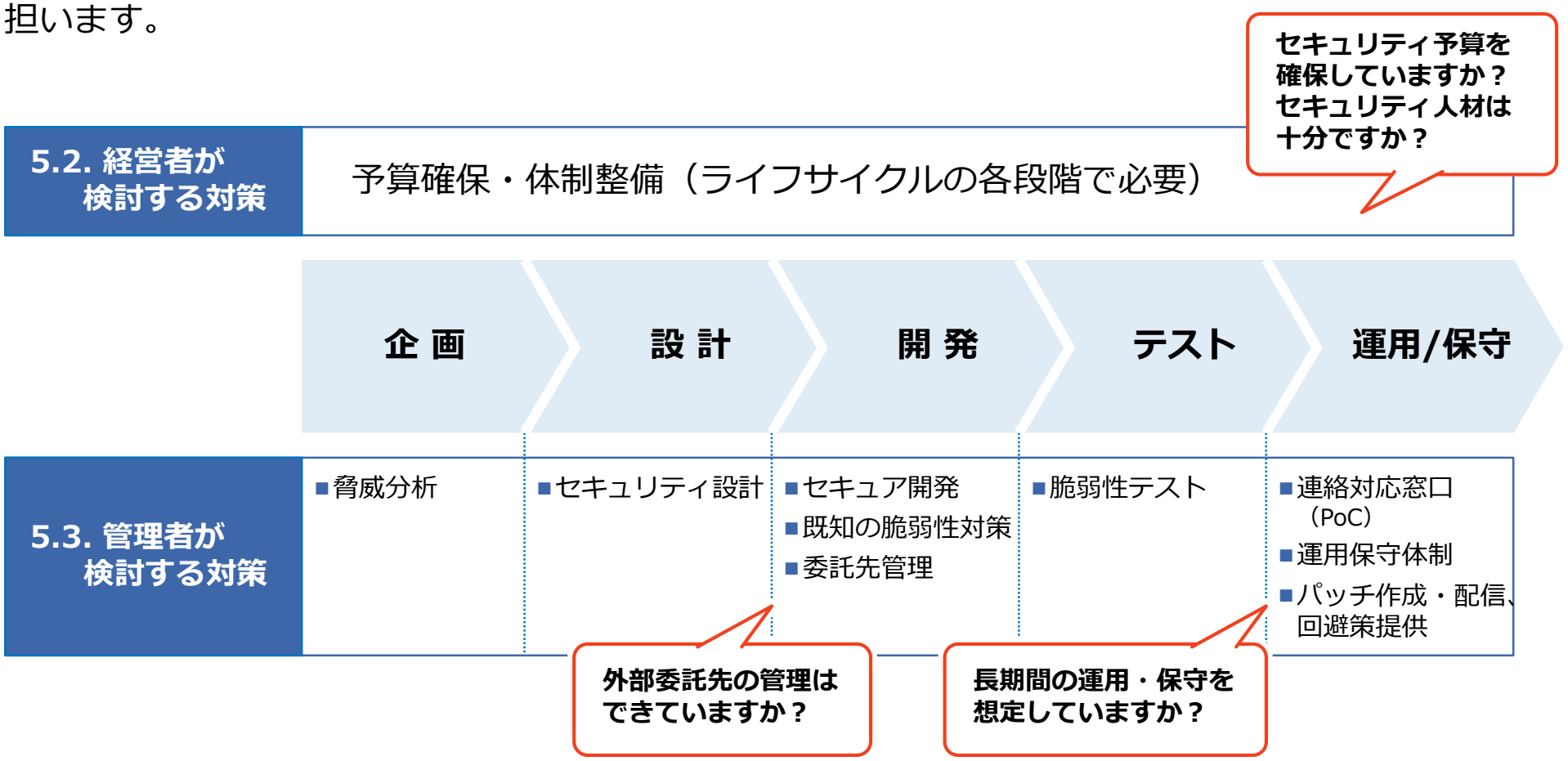
※ IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）

5. IoT製品・サービスの対策ポイント

5.1. 対策の全体像

安全安心なIoT製品・サービスの提供は自社を守るだけではなく、社会全体のリスクを低下させるためにも重要です。

安全安心なIoT製品・サービスの提供には、**開発部門だけではなく経営者と管理者も重要な役割**を担います。



※ 5.1から5.3で示した対策やその他の対策については、参考資料に示した関連ガイドライン等を参照ください。

5.2. 経営者が検討する対策

安全安心なIoT製品・サービスを提供するために、経営者は以下の点を考慮する必要があります。

ポイント1：セキュリティ対策予算を確保する

- セキュリティ対策は費用と考えられる傾向がありますが、事前にセキュリティ対策を実施していないと、事故が発生した際に事前対策費用以上の費用が発生する可能性があります。
- そこで、セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉え、予算を確保する必要があります。

ポイント2：体制を整備する

- 安全安心なIoT製品・サービスを提供するためには、セキュリティ詳しい人材を開発・運用体制に含めることが重要となります。
- しかし、セキュリティ人材は日本全体でも不足しており、確保は困難な可能性があります。
- 中長期的な視点に立ったセキュリティ人材の育成や、以下のような外部リソースの活用も検討し、セキュリティを確保できる体制を整備しましょう。

- 公的ガイドライン等の評価が確立された知見の活用
- セキュリティが考慮された、ミドルウエア・製品・サービスの活用
- 開発・運用委託時におけるセキュリティの配慮
- 外部専門家の活用

※ 5.1から5.3で示した対策やその他の対策については、参考資料に示した関連ガイドライン等を参照ください。

5.3. 管理者が検討する対策（1）企画・設計

IoT製品・サービスの企画・設計段階では、以下の項目を参考にセキュリティ対策を実施する必要があります。

ポイント1：脅威分析を実施しライフサイクルを考慮したセキュリティ設計を行う

- 安全安心なIoT製品・サービスを提供するためには、企画・設計段階での脅威分析とライフサイクルを考慮したセキュリティ設計を実施する必要があります。
- 脅威分析では、提供するIoT製品･サービスで守るべきIoT機能や情報を洗い出す必要があります。脅威分析の観点としては以下のようなものがあります。
  - 自社製品・サービス以外とつながることによるリスク
  - 不正操作や製品への物理的な攻撃によるリスク　等

ポイント2：セキュリティサポート方針※を明確にする

- IoT製品・サービスの販売後のセキュリティサポート方針を企画・設計段階から検討する必要があります。
- セキュリティサポート期間終了後にIoT製品・サービスに脆弱性が発見された場合の対応についても検討することが望ましいです。対応方針には以下のようなものがあります。
  - 回避策の提供
  - 後継製品の利用推奨　等

※ セキュリティサポートとは「脆弱性対策を含むセキュリティ対応」を示します。※ 5.1から5.3で示した対策の詳細やその他の対策については、参考資料に示した関連ガイドライン等を参照ください。

5.3. 管理者が検討する対策（2）開発・テスト

IoT製品・サービスの開発・テスト段階では、以下の項目を参考にセキュリティ対策を実施する必要があります。

ポイント3：脆弱性を作り込まない開発をする

- IoT製品・サービスを開発する際にはセキュリティに考慮した開発を行う必要があります。
- 脆弱性を作り込まないよう、既知の脆弱性については、JVN（参考資料3参照）等を参照して開発を進める必要があります。
- IoT製品・サービスの開発にあたって、国内外の開発・製造委託先を活用する際は、委託先のセキュリティ対策も考慮する必要があります。委託契約等で委託先にセキュリティ対策の実施を求めることを検討することが必要です。
- IoT製品・サービスをリリースする前には、脆弱性検査等を実施し脆弱性がないか検査することが望ましいです。

※ 5.1から5.3で示した対策やその他の対策については、参考資料に示した関連ガイドライン等を参照ください。

5.3. 管理者が検討する対策（3）運用/保守段階

IoT製品・サービス提供後（運用/保守）も以下の項目を参考にセキュリティ対策を実施する必要があります。

ポイント4：連絡窓口（PoC（Point of Contact））を設置する

- IoT製品・サービス提供後も、自社で脆弱性情報等を収集し、社外からの自社製品・サービスの脆弱性等について連絡を受け付ける連絡窓口（PoC）を設置する必要があります。

ポイント5：運用・保守体制を整備・維持する

- IoT製品・サービスの中には提供者が想定している以上に、利用者が長期間利用する可能性があります。
- そこで、IoT製品・サービス提供後も脆弱性等が発見された場合に備え、製品・サービスの運用・保守体制を整備し、セキュリティサポートを提供する必要があります。
- セキュリティサポート方針の利用者への周知や、セキュリティサポート終了後に脆弱性が発見された場合は、使用中止や後継製品への移行を利用者にお願いすることが望ましいです。

ポイント6：脆弱性が発見されたときは適切に対応する

- 自社のIoT製品・サービスに脆弱性が発見されたときは、脆弱性を修正し、パッチの適用を利用者に依頼・周知する必要があります。
- 脆弱性の修正が困難な場合は、回避策の提供や最新製品の利用等の代替策を提供する方法もあります。

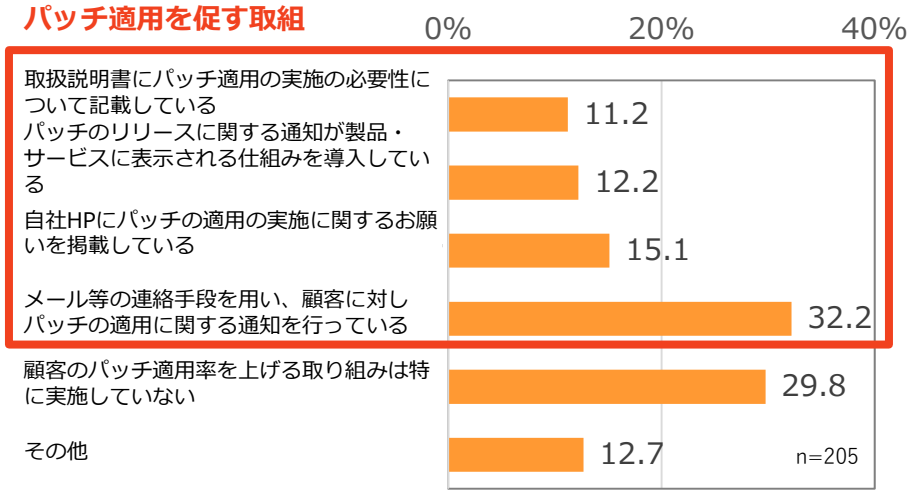
※ 5.1から5.3で示した対策やその他の対策については、参考資料に示した関連ガイドライン等を参照ください。

IoT製品・サービスの脆弱性対策と対策促進の取組

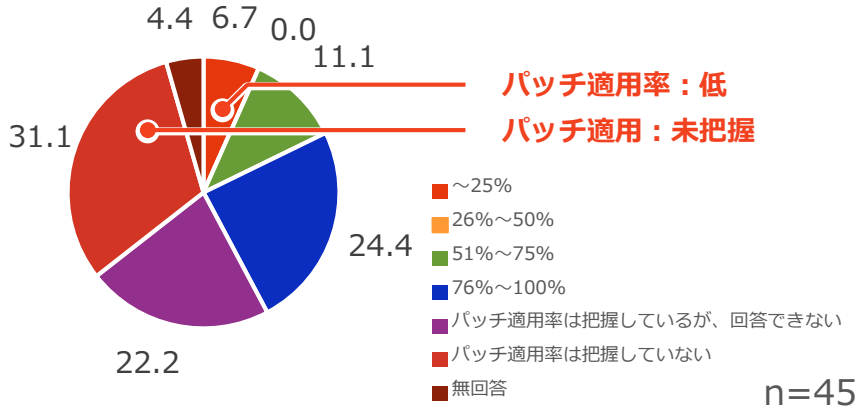
コラム

- 自社のIoT製品・サービスに脆弱性が発見された場合、パッチを配信することがあります。
- 企業では、利用者のパッチ適用を促すための取組が進められていますが、利用者がパッチ適用を必ず実施するとは限りません。
- 利用者に安心して製品・サービスを利用してもらうためにも、**利用者にパッチ適用を促すさらなる取組が企業に求められます。**

利用者のパッチ適用率を上げるための企業の取組※



利用者の1年以内のパッチ適用状況※



注：脆弱性が発見され、利用者に対してパッチ配信を実施した企業のみ回答

企業は利用者のパッチ適用率を上げる取組を実施していますが、
利用者のパッチ適用率は必ずしも高くなく、パッチ適用状況も把握できていません。

※ IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）

IoT製品・サービスの脆弱性対応から得られた教訓

コラム ヒアリングや公開記事から得られた、企業における脆弱性対応の知見・ノウハウを以下に示します。

脆弱性対応から得られた教訓

利用実態が想定と違う場合がある：

- 製品をLAN内で使う想定でいたため、インターネット接続製品より緩い基準としていたが、インターネットにつなげて使われることがあった。利用者の使い方を決めつけないことが必要。（公開記事）

回避策を先に公開することが重要である：

- ファームウエアによる対策に時間がかかりそうである場合、回避策を先に公開することが有効。（公開記事）

複数製品が該当する脆弱性へは早めに対応方針を公表する：

- 脆弱性の存在が公表された場合、「自社製品に該当するものがあるため、調査中であること」を発表するのが重要。（公開記事）

古い製品の脆弱性へは利用停止を案内する：

- 脆弱性が発見された古い製品にファームウエアによる対策はすでにできない状態だったため、製品そのものの利用停止をお願いする案内を実施。（公開記事）

脆弱性の深刻度と世の中での影響度が異なる場合がある：

- 深刻度が高くない脆弱性に対して、深刻度に応じた社内対応を実施していたが、世の中で大きく騒がれてしまい、対外対応が必要となることがある。深刻度が高くなくても、現場で対応を判断せず、脆弱性対応の責任者に情報を集約して企業としての判断と対応が必要。（ヒアリング※）

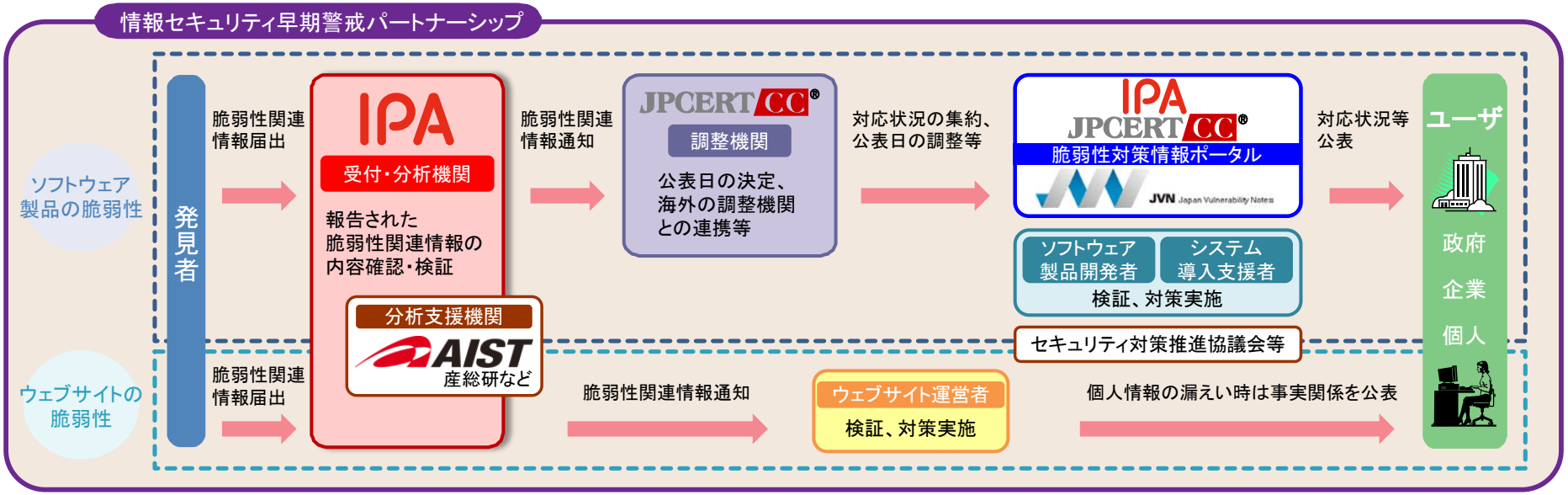
※ IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」（2018年）

参考資料

参考1. 情報セキュリティ早期警戒パートナーシップ
参考2. パートナーシップからIoT製品の脆弱性情報が届けられた際の対応方法や注意点
参考3. 脆弱性対策情報データベース：JVN iPedia
参考4. IPA「つながる世界の開発指針」
参考5. IPA「IoT開発におけるセキュリティ設計の手引き」
参考6. IPA「つながる世界のセーフティ＆セキュリティ設計入門」
参考7. IoT推進コンソーシアム・総務省・経済産業省「IoTセキュリティガイドラインver1.0」
参考8. IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

（参考1）　情報セキュリティ早期警戒パートナーシップ

- IPAでは、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（経済産業省告示第19号） を踏まえ、国内で利用されているソフトウエア製品や、主に日本国内からのアクセスが想定されるサイトで稼動するウェブアプリケーションの脆弱性に関する届出を受け付けています。
- IPAでは、脆弱性に関する届出を受け付けた場合、JPCERT/CCに連絡し、JPCERT/CCから当該製品の開発者にその旨を連絡し、脆弱性対策の実施を促します。
- 同制度ではIoT製品の脆弱性についても扱っています。



※IPA:独立行政法人情報処理推進機構, JPCERT/CC:一般社団法人　JPCERTコーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

(URL)　https://www.ipa.go.jp/security/ciadr/partnership_guide.html

（参考2）パートナーシップからIoT製品の脆弱性情報が届けられた際の対応方法や注意点

IPA

- 製品開発者は、自社のIoT製品の脆弱性を通知された場合、その内容を検証すること、さらに当該脆弱性が存在した場合には、利用者へ対策方法を周知することが望まれます。
- また、JPCERT/CCから脆弱性関連情報に係わる技術的事項および進捗状況について問合せを受けた場合には、ご協力ください。

窓口の設置	■ 脆弱性関連情報を受け付ける窓口を設置し、JPCERT/CCに連絡してください。 ■ 窓口の変更があれば速やかにJPCERT/CCにご連絡ください。
脆弱性の検証	■ 製品開発者は、JPCERT/CCから脆弱性関連情報を受け取ったら、製品への影響を調査し、脆弱性検証を行って、その結果をJPCERT/CCにご報告ください。 ■ 脆弱性関連情報を第三者に漏えい・開示しないように管理してください。
公表日程の調整 **対策の作成**	■ 検証の結果、脆弱性が存在することを確認した場合には、対策方法の作成や外部機関との調整に要する期間、当該脆弱性情報流出に係わるリスクを考慮しつつ、脆弱性情報の公表に関するスケジュール※についてJPCERT/CCとご相談ください。 ■ 製品開発者は、脆弱性情報の公表日までに対応状況をJPCERT/CCに連絡するとともに、対策方法を作成するよう努めてください。
一般への公表	■ 製品開発者は、脆弱性情報の公表日以降、対策方法を製品利用者に周知してください。

※ 公表日は脆弱性の起算日から45日を目安としますが、さらに時間がかかる場合はJPCERT/CCとご相談ください。なお、起算日から1年間以上経過した届出について、発見者はIPAに情報非開示依頼の取り下げを求め、当該脆弱性情報を公表する可能性があります。

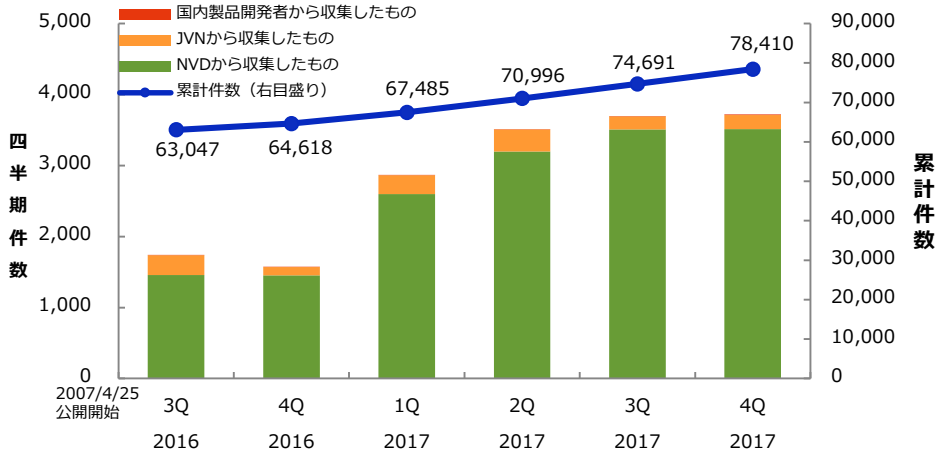
（参考3）脆弱性対策情報データベース：JVN iPedia

- JVN iPediaではソフトウェア製品（IoT製品などの組み込みソフトウェアも含む）の脆弱性が登録・公開されています。

  - 脆弱性対策情報データベース「JVN iPedia」国内外で使用されているソフトウェアの脆弱性対策情報を収集・公開し、様々な検索や活用をするための機能を備えています。
  - IoT製品を含む、組み込みソフトウェアの脆弱性も約1,305件登録されており、IoT製品の開発にあたって、利用するソフトウェア部品の既知の脆弱性の確認、対策に活用できます。

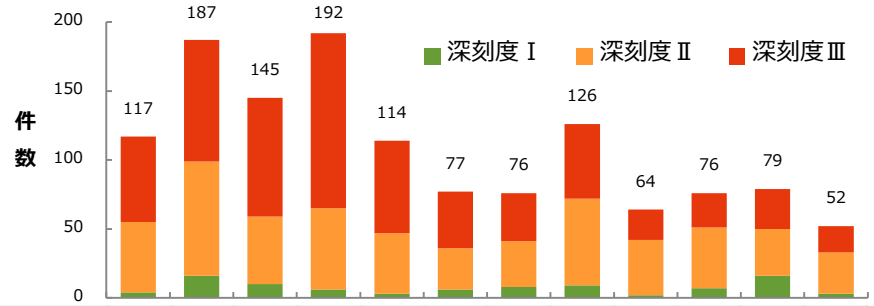
脆弱性対策情報の登録件数（2017年第4四半期）

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	10件	196件
	JVN	213件	7,864件
	NVD	3,496件	70,350件
	計	3,719件	78,410件
英語版	国内製品開発者	8件	194件
	JVN	31件	1,642件
	計	39件	1,836件



JVN iPediaの登録件数の四半期別推移

IoT製品を含む、組み込みソフトウェアの脆弱性対策情報 公開年別推移



	～2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
深刻度Ⅰ	4	16	10	6	3	6	8	9	2	7	16	3
深刻度Ⅱ	51	83	49	59	44	30	33	63	40	44	34	30
深刻度Ⅲ	62	88	86	127	67	41	35	54	22	25	29	19
組込みソフトウェア合計	117	187	145	192	114	77	76	126	64	76	79	52

JVN: Japan Vulnerability Notes、JPCERT/CC及びIPAの脆弱性対策情報ポータルサイト。
NVD: National Vulnerability Database、米国国立標準技術研究所NISTの脆弱性データベース。

（URL） https://jvndb.jvn.jp/

（参考4）IPA「つながる世界の開発指針」

IPA「つながる世界の開発指針」における各指針と本資料の対応は以下の通りです。

開発指針一覧（「つながる世界の開発指針」）及び本資料との対応関係

	指 針	経営者 （本資料5.2）	管理者 （本資料5.3）
方針の策定	指針1：安心安全の基本方針を策定する	ポイント1,2	
	指針2：安心安全のための体制・人材を見直す	ポイント1,2	
	指針3：内部不正やミスに備える	ポイント1,2	
リスク分析の実施	指針4：守るべきものを特定する		ポイント1
	指針5：つながることによるリスクを想定する		ポイント1
	指針6：つながりで波及するリスクを想定する		ポイント1
	指針7：物理的なリスクを認識する		ポイント1
設計段階の対策	指針8：個々でも全体でも守れる設計をする		ポイント1,3
	指針9：つながる相手に迷惑をかけない設計をする		ポイント1
	指針10：安全安心を実現する設計の整合性をとる		ポイント1
	指針11：不特定の相手とつなげられても安全安心を確保できる設計をする		ポイント1
	指針12：安全安心を実現する設計の検証・評価を行う		ポイント1,3
運用保守段階の対策	指針13：自身がどのような状態かを把握し、記録する機能を設ける		ポイント1
	指針14：時間が経っても安全安心を維持する機能を設ける		ポイント1
	指針15：出荷後もIoTリスクを把握し、情報発信する		ポイント2,4,5,6
	指針16：出荷後の関係事業者に守ってもらいたいことを伝える		ポイント2,4,5,6
	指針17：つながることによるリスクを一般利用者に知ってもらう		ポイント2,4,5,6

（URL） https://www.jpa.ga.jp/files/000060387.pdf

（参考5）IPA「IoT開発におけるセキュリティ設計の手引き」

- IPA「IoT開発におけるセキュリティ設計の手引き」では、IoT製品やサービスのセキュリティ設計を行う場合の手順として、以下が紹介されています。

	Step 1	対象とするIoT製品やサービスのシステム全体構成を明確化する。
	Step 2	システムにおいて、保護すべき情報・機能・資産を明確化する。
Phase1:脅威分析	Step 3	保護すべき情報・機能・資産に対して、想定される脅威を明確化する。
Phase2:対策検討	Step 4	脅威に対抗する対策の候補（ベストプラクティス）を明確化する。
	Step 5	どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定する。

- また、セキュリティ対策の一つとして必要不可欠な脆弱性への対応詳細として、以下が紹介されています。

	脆弱性への対応内容
開発段階での対応	(1) 新たに脆弱性を作り込まないこと
	(2) 既知の脆弱性を解消すること
	(3) 残留している脆弱性を検出・解消すること
	(4) 製品出荷後の脆弱性の新たな発見に備えること。
運用段階での対応	(1) 継続的な脆弱性対策情報の収集
	(2) 脆弱性対策情報（更新ソフトウェアを含む）の作成
	(3) 脆弱性対策情報の利用者への通知
	(4) 更新ソフトウェアの製品への適用

(URL)　https://www.ipa.go.jp/files/000052459.pdf

（参考6）IPA「つながる世界のセーフティ＆セキュリティ設計入門」

- 機器やシステムの安全・安心を実現するためのセーフティとセキュリティの設計手法、ソフトウェアの再利用や流通において第三者に論理的に説明できる設計品質の見える化手法等について解説した入門書です。
- 事故やインシデント事例、セーフティ・セキュリティの観点からの開発等について解説しています。

つながる世界のセーフティ＆セキュリティ設計入門の概要

章	概 要
第1章　つながるシステムのセーフティとセキュリティ	■ 的確なリスク対応、セーフティとセキュリティの設計、見える化による設計情報の共有の重要性について解説
第2章　事故及びインシデント事例	■ ソフトウェアの品質／脆弱性により発生した事故およびインシデント事例を、原因と対策のヒントとともに紹介
第3章　セーフティとセキュリティのための開発プロセス	■ 開発プロセスにおけるセーフティとセキュリティの必要性や具体的なプロセスについて解説するとともに、その課題と対応例を紹介
第4章　ソフトウェア技術者のためのセーフティ設計	■ セーフティ対応のプロセスにおけるハザードの特定、リスク評価およびセーフティ設計について解説
第5章　ソフトウェア技術者のためのセキュリティ設計	■ セキュリティ対応のプロセスの前段となる脅威の特定、リスク評価およびセキュリティ設計について解説
第6章　ロジカルな設計品質の説明	■ 設計品質の見える化の一手法である「アシュアランスケース」について解説するとともに、その具体例も紹介

（URL）　https://www.ipa.go.jp/files/000055007.pdf

（参考7）IoT推進コンソーシアム・総務省・経済産業省「IoTセキュリティガイドラインver1.0」

IPA

- IoT製品・サービスに提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針や一般利用者がIoT機器等を利用する際のルールを説明したガイドラインです。
- セキュリティ確保の観点から求められる基本的な取組について、セキュリティ・バイ・デザインを基本原則として解説しています。

IoTセキュリティガイドラインver1.0 の概要

指針		主な要点
方 針	**IoTの性質を考慮した基本方針を定める**	■経営者がIoTセキュリティにコミットする ■内部不正やミスに備える
分 析	**IoTのリスクを認識する**	■守るべきものを特定する ■つながることによるリスクを想定する
設 計	**守るべきものを守る設計を考える**	■つながる相手に迷惑をかけない設計をする ■不特定の相手とつなげられても安全安心を確保できる設計をする ■安全安心を実現する設計の評価・検証を行う
構築・接続	**ネットワーク上での対策を考える**	■機能及び用途に応じて適切にネットワーク接続する ■初期設定に留意する ■認証機能を導入する
運用・保守	**安全安心な状態を維持し、情報発信・共有を行う**	■出荷・リリース後も安全安心な状態を維持する ■出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える ■IoTシステム・サービスにおける関係者の役割を認識する ■脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		■問合せ窓口やサポートがない機器やサービスの購入・利用を控える ■初期設定に気をつける ■使用しなくなった機器については電源を切る ■機器を手放す時はデータを消す

(URL) http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

（参考8）IPA「IoT製品・サービス開発者における セキュリティ対策の現状と意識に関する報告書」

- 2017年度、IPAではIoT製品開発者における脆弱性対策の現状認識と課題等を明らかにするための調査を実施しました。
- 調査は①IoT製品の脆弱性に起因する問題事例に関する調査、②IoT製品開発者を対象とした郵送でのアンケート調査、③ヒアリング調査、に分かれています。
- アンケート調査は、日本国内のIoT製品・サービスを開発している企業205社を対象としました。

アンケート調査の概要

調査対象	■国内に拠点を置くIoT製品・サービス開発者（企業） 回答部門 IoT製品・サービスのセキュリティ確保に責任を持つ部門（第一優先） IoT製品・サービスのアフターサービスに責任を持つ部門（第二優先）
有効回答数	205件（なお、同一企業内で複数のIoT製品・サービスを開発している場合、１製品・サービスを1件とする）
調査項目数	42項目
調査項目	■IoT製品・サービスにおけるセキュリティ対策の状況 ■IoT製品・サービスにおけるセキュリティの事件・事故 ■IoT製品・サービスにおける脆弱性対策の手段 ■IoT製品・サービスにおける脆弱性対策を妨げる要因や問題点　等
調査手法	郵送調査
調査期間	2017年11月～12月
発送数	発送数：1,500件　（うち120社に複数枚の調査票を送付）

【 IoT製品・サービス脆弱性対応ガイド 】

安全安心なIoT製品・サービスを提供するために

～ 経営者・管理者向け：企業が実施すべきIoT脆弱性対策のポイント ～

2018年3月 第1版発行

独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込２丁目２８番８号　文京グリーンコードセンターオフィス１６階

URL　https://www.ipa.go.jp/security/

電話　03-5978-7527　　FAX　03-5978-7552