pwc | Japan

# IoT活用企業におけるプライバシー保護に関する考慮事項とは

2019-09-03

2019年6月27日にアメリカ国立標準技術研究所（National Institute of Standards and Technology: NIST）から「IoTに関するサイバーセキュリティとプライバシーリスクの考慮点（原題：NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks）」（以下、NISTIR 8228）（※1）が公表されました。IoTをセキュアに利活用することについては、比較的、サイバーセキュリティに軸足を置いた議論が従前より行われてきました。しかしながらNISTIR 8228では、タイトルで明示的に「プライバシーリスク」と掲げており、これは今後、企業がIoTを利活用する際には、サイバーセキュリティに留まらず、個人のプライバシーを侵害するリスクを十分に認識し、必要となるコントロールを整備する必要性を強調しているものと考えられます。

このような背景のもとで、本コラムでは、NISTIR 8228の中でも特にプライバシーに関する内容を取り上げながら、企業がIoTを活用したビジネスを展開するために必要となる、個人のプライバシー保護に関する考慮点について解説します。

また、コラムにおいて「プライバシーデータ」という言葉を用いていますが、個人PCのIPアドレスやCookie情報等のオンライン識別子等も含めた、広義の意味での個人のプライバシーに係るデータ全般をこの言葉で表現しています。

なお、本コラムにおける意見・判断に関する記述は筆者の私見であり、所属組織の見解とは関係のない点をあらかじめお断りしておきます。

# IoTとは何か

IoTの定義についてはさまざまな国の標準団体等が公表していますが、わが国では、2018年に総務省が公表した『平成30年版情報通信白書』において、以下のように定義しています。

> IoTとは、「Internet of Things」の略で、「モノのインターネット」と訳されることが多い。
> 電車やクルマ、工場やビル、製造機械や飛行機のエンジン、冷蔵庫や洗濯機、農地や牧場の牛など、あらゆるものをネットワークに接続することで、それぞれの最新状態を示すデータを集め、その分析から、より最適な状態に導くようにフィードバックを返すという、一連の流れを指している。

出典：総務省, 2018.『平成30年版情報通信白書』より（※2）

ネットワークに接続できるIoT機器は、世界中で加速度的に普及しています。この機器は今や、インターネットを介してさまざまにつながり、フィジカル空間から収集した多くの情報をもとに、AI等の先端技術と連携することで、新たな価値を創造しています。具体的には、下記のような産業を中心に、今後もさらなる利用の拡大が見込まれています。

| 産業 | IoT機器の例 |
|---|---|
| スマートシティ | ウェアラブル（情報・映像）、デジタルサイネージ、監視カメラ、生体情報システム |
| ヘルスケア | ウェアラブル（スポーツ・フィットネス）、コンシューマヘルスケア機器、X線、超音波 |
| スマート工場 | 産業用ロボット、マシンビジョン、プログラマブルロジックコントローラ |
| コネクテッドカー | 自動車向けセンサーモジュール（車載器） |
| スマートエネルギー | スマートメータ、スマート照明機器 |

出典：総務省, 2019.『IoT国際競争力指標（2017年実績）』を参考にPwC作成（※3）

# IoTにおけるプライバシーデータ保護の必要性

IoT機器が収集するデータの中には、プライバシーデータと見なされる可能性が高いものが多く含まれています。これらのデータは、他のデータと紐付けることで特定の個人を識別することが可能になるものもあります。IoTを用いたサービスを提供している企業の中には、自社のIoT機器からデータを収集、分析し、自社のビジネスに活用しているものもあります。

例えば、自動車に搭載された車載器からデータを取得することで、車両のメンテナンス時期の提案を行うサービスや、製品の潜在的欠陥を予測し、不具合を事前に検知するサービスが既にあります。また、車両の走行記録を多数収集すれば、交通状況の予測に役立てることも可能になります。さらに、これらのデータを組み合わせ、個人のライフスタイルを特定し、マーケティング目的で他社にデータを提供することも可能となります。このように、IoTによるデータの活用は、企業にとって大きなビジネスチャンスとなっています。

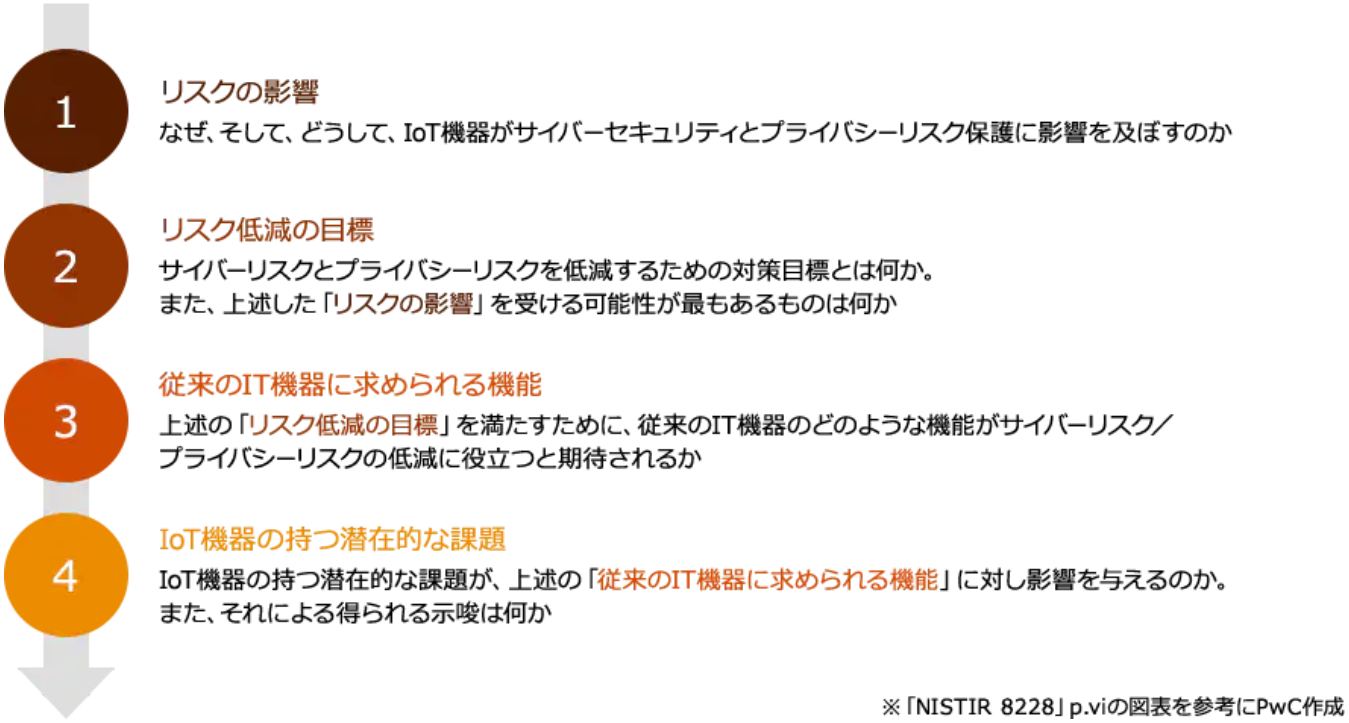
一方で、消費者や海外の規制当局は、企業におけるプライバシーデータの処理方法、および流通を厳しく監視しています。例えば、プライバシーデータの漏洩といった何らかのセキュリティインシデントの発生によって、消費者がひ

とたび不信感を持てば、サービスは敬遠され、データ流通は規制され、企業の成長も阻害される可能性が考えられます。このため、企業はIoT機器から得られたデータにプライバシーデータが含まれているリスクを認識し、これらのデータを適切に保護し、プライバシーの侵害を防ぐ必要があります。

## NISTIR 8228から理解できること

NISTIR 8228では、まず、IoT機器がどんなサイバーリスク／プライバシーリスクの保護に影響を及ぼすのかを解説し、そのリスクを低減するための対策目標を掲げています。そして、その目標を満たすために、従来のIT機器に求められる機能とIoT機器の持つ機能を比較し、IoT機器が抱える潜在的な課題を整理する構成となっています。

図1




※「NISTIR 8228」p.viの図表を参考にPwC作成

IoT機器が抱える潜在的な課題として、例えばIT機器には通常備わっているログ取得機能がIoT機器には実装されて

いない場合が多いことが取り上げられています。このことから、企業が情報漏洩等のセキュリティインシデントの検知や原因分析ができない可能性が考えられるため、企業がIoTを利活用する上で考慮すべきリスクの一つとして挙げられています。

多種多様なIoT機器が世の中に存在する中で、IoT機器にどのようなリスクがあるのか、企業がIoTに係るビジネスを展開する上で、どのような点に気を付ければよいのかを従来のIT機器との比較のもとで体系的に理解できるという意味でも、NISTIR 8228は有益であると考えられます。

## 個人のプライバシーを守る視点からIoT機器に欠けている機能

NISTIR 8228では、IoTにおけるセキュリティに関して「IoT機器そのものを守ること」「データセキュリティを守ること」「個人のプライバシーを守ること」の3点をリスク低減の目標として掲げており、それぞれの目標を満たす上で、IoT機器が従来のIT機器に比べて欠けている機能を取り上げています。本コラムでは、上記3点のうち、「個人のプライバシーを守ること」にフォーカスを当て、整理します。

以下に、NISTIR 8228のコンテンツのうち、個人のプライバシーを保護する上でIoT機器に欠けている機能と潜在的なリスクを取り上げ、コントロールする上での考え方を参考までに記載しました。コントロールについては、企業が展開するビジネスや、企業の組織体制、ガバナンス構造、制定している方針や手続き等に大きく依存するため、必ずしもこの限りではありません。

1) 利用者と意思疎通を図るための機能が不足している

| 考えられるリスクの一例 | コントロールの考え方 |
| --- | --- |
| IoT機器においては、個人のプライバシーの取り扱いに対する利用者の意思決定の結果を反映できない。<br>– 利用者が、企業のプライバシーポリシーを閲覧できない<br>– 利用者が、プライバシーデータの処理に対する明確な同意を与えることができない | GDPRに代表されるように、企業がプライバシーデータを取り扱うにあたっては、対象者の明示的な同意を要求している法令が整備されています。<br>このため、企業はIoT機器だけではなく、従来のIT機器の機能、対面または書面での確認手続きを複合的に利用する等、さまざまな手段を用いて利用者とコミュニケーションを取る方法を確立しておく必要があります。 |

2) 中央制御するための機能が不足している

| 考えられるリスクの一例 | コントロールの考え方 |
| --- | --- |
| 個人のプライバシー保護に関するポリシーや法規制の要求事項を十分に適用できない。<br>– 企業が定めたポリシーをIoT機器の隅々まで適用できず、意図に反する形でプライバシーデータを収集、解析、転送してしまう<br>– ポリシーや法規制の要求事項が変更された場合、それに対応するコントロールとしての機能をIoT機器に柔軟に実装できない | 企業は、IoT機器が持つこのような特性を考慮し、要求事項を満たすIoT機器の選定や開発を行う必要があります。<br>また、収集するプライバシーデータを明確にした上で、必要に応じて収集内容の制限を行う必要があります。 |

3) プライバシーデータの処理フローに関連した機能が不足している

| 考えられるリスクの一例 | コントロールの考え方 |
| --- | --- |
| IoT機器には、プライバシーデータの処理フローに関連する機能が不足している場合がある。<br>– IoT機器の中には、通信の可視化、制御を行うための機能が不足しており、意図しないサーバー等にプライバシーデータを送信してしまう<br>– 暗号化機能が適切に実装されておらず、第三者が解読可能な形で、プライバシーデータを保管、通信してしまう<br>– ログ出力の機能が実装されておらず、インシデントの迅速な検知や事後の原因分析が阻害される | 上記2）で記載したコントロールの考え方に加え、IoTによる処理を全て自動化するのではなく、何らかのチェックポイントを設定し、そこで問題点を検知する仕組み（モニタリング機能）を実装することが考えられます。 |

# 個人のプライバシー侵害に伴うビジネス上のリスク

ここからは、万が一、IoT機器を利用することで個人のプライバシー侵害が発生した場合、どのようなビジネス上のリスクにつながるかを解説します。

ビジネス上のリスクにはさまざまな捉え方と整理の仕方がありますが、このコラムでは、プライバシーデータの漏洩が発生した場合のリスクを、実リスクとコンプライアンスリスクという観点で整理します。

実リスクとは、個人のプライバシーに関するセキュリティインシデント（例：情報漏洩）が発生した場合の、事態の収束から業務の回復に至るまでに企業が被るリソース（人的、金銭的、時間的等）等、負の影響を指します。下記が実リスクの一例として挙げられます。

| 実リスクの一例 | 説明 |
|---|---|
| 対応コストの発生 | 事態を収拾させるまでに必要となる、直接および間接的に発生する対応コストを指します。ここでいう直接コストは「外部組織の支援を受けるための費用」、間接コストは「社内の人員稼働に関する内部人件費や時間的リソース」を指します。以下は対応コストの一例です。<br>– セキュリティベンダー（フォレンジックの実施等）への依頼<br>– コールセンター業者への依頼<br>– 法的助言を得るための弁護士事務所への相談費用<br>– 顧客への通知にかかる対応費用<br>– 謝罪広告の掲載費用、損害賠償に関する訴訟費用<br>– 外部のコンサルティングファームへの再発防止策の立案支援依頼費用<br>– インシデントの原因分析（社内組織による稼働および外部組織の支援を含む）<br>– 緊急対策チームの組成と管理<br>– 経営陣や取締役会等における緊急協議<br>– 規制当局への報告<br>– 緊急の社員研修や点検の実施を含む再発防止策の検討と実施 等 |
| レピュテーション（風評）低下による機会損失 | 企業の評判が悪化することで損失を被るリスクを指します。例えば、顧客の流出、顧客からの評価の低下、業務上の信用の失墜、顧客開拓業務の負担増に加えて、株価の低下、競争優位性の低下、これに伴う企業価値の低下等が挙げられます。<br>これに加えて、失墜した信頼を回復するためのさまざまな取り組みが継続的に必要となるため、これが業務に与える影響も考慮する必要があります。 |

企業は、このような実リスクに加え、コンプライアンスリスクについても留意しなければなりません。コンプライアンスリスクとは、法令違反によって当局から制裁金や行政処分等の罰則を被る可能性を指します。近年、さまざまな国や地域で個人のプライバシー保護に対する法規制が制定されており（以下表を参照）、これに違反した場合は多額の制裁金を含む厳しいペナルティが課されています。

主要国におけるプライバシーデータ保護に関する法規制（2019年7月時点）

| 国・地域 | 法規制名称 | 備考 |
|---|---|---|
| 日本 | プライバシーデータ保護法 | 2017年の改正では、社会的身分・病歴等が含まれるプライバシーデータを「要配慮プライバシーデータ」として定義し、より慎重に取り扱うことを定めています。 |
| 米国 | 包括的なプライバシーデータ保護の規制は連邦レベルのものは無し | CCPA（California Consumer Privacy Act）等といった州レベル、および、CoPPA（Children's Online Privacy Protection Act）、HIPPA（Health Insurance Portability and Accountability Act）等の業界レベルでの規制が存在します。 |
| EU | EU一般データ保護規則（GDPR） | プライバシーデータの域外移転制限、データ侵害時の72時間以内のデータ保護当局への通知、違反時の高額な罰金等、従前のEUデータ保護指令と比べて厳格化されています。 |
| 中国 | 包括的な個人情報保護の法規制は無い | 中国サイバーセキュリティ法等にプライバシーデータ保護の法規制が散在しています。 |
| 韓国 | プライバシーデータ保護法（PIPA） | 最大1億ウォンと禁固刑10年を含む罰則が定められています。 |
| シンガポール | プライバシーデータ保護法（PDPA） | プライバシーデータの収集、使用および開示に先立ち同意を取得するよう義務付け、データの国外移転先について条件が明記されています。 |

下記は、2019年上半期で科された制裁の一例です。IoT機器で収集したプライバシーデータの侵害に係る例示のみではありませんが、グローバルでビジネスを展開しようとしている企業にとっては、各国で収集したプライバシーデータを適切に扱わなければ、このような巨額な制裁金を課されてしまうリスクがあることを念頭に置いておく必要があります。

2019年上半期で科された制裁の実例

| 制裁対象 | 制裁金 | 制裁事由 |
|---|---|---|
| インターネット関連サービス大手 | 約62億円 | プライバシーデータを収集する際に取得すべき利用者との合意のメカニズムに不備がありました。 |
| ホテル業界大手 | 約135億円※ | 大規模な顧客情報の流出を引き起こしました。 |
| 航空業界大手 | 約250億円※ | 大規模な顧客情報の流出を引き起こしました。 |
| インターネット関連サービス大手 | 約5,400億円※ | 収集したプライバシーデータを不正に取り扱っていました。 |

※2019年7月時点で係争中であり、制裁金の金額は未確定

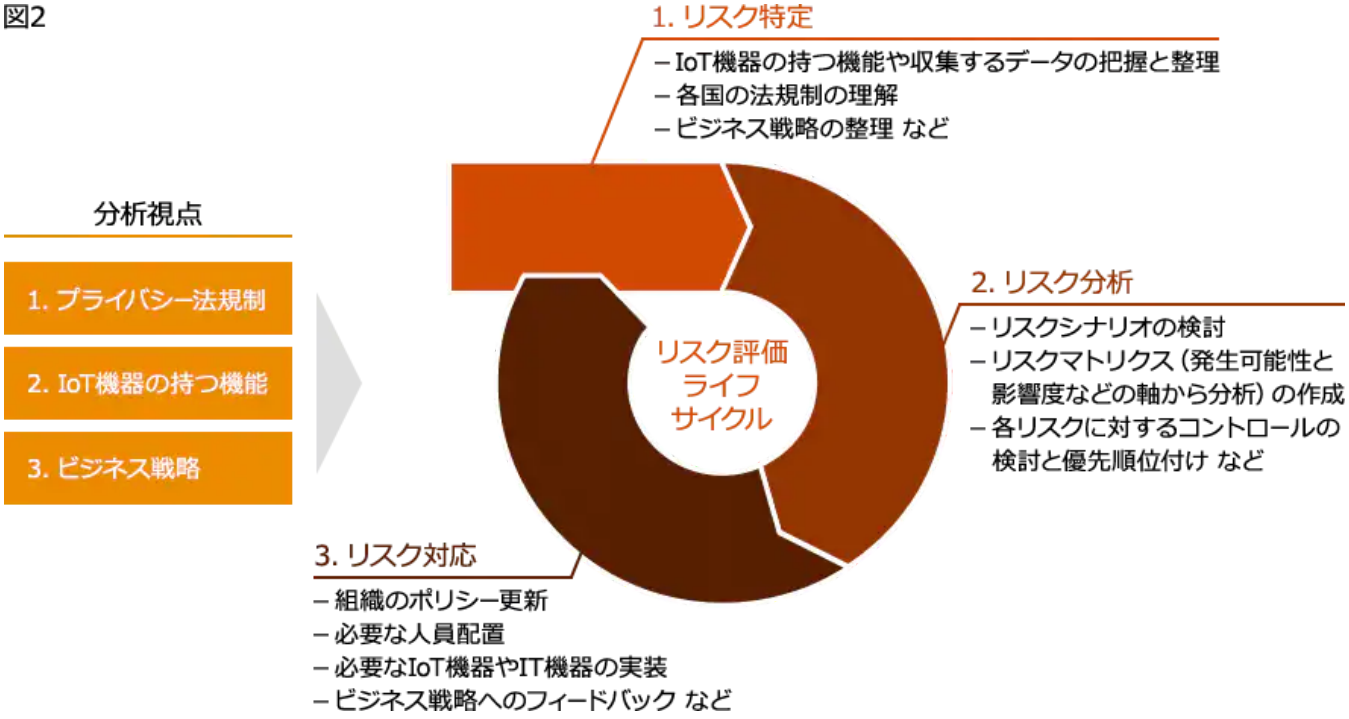
# 企業の対応策

ここまで、個人のプライバシーを守る視点からIoT機器に欠けている機能を整理し、企業が個人のプライバシー保護を怠った際に発生し得るビジネス上のリスクについて説明してきました。ここからは、このようなリスクを顕在化させないために、企業が講じるべき対応策について解説します。

対応策の一例として「各国のプライバシー法規制」「IoT機器が持つ機能」「ビジネスの今後の展望」という3つの分析観点から、リスク評価の仕組みを整備することが挙げられます。各国のプライバシー法規制も、IoT機器の機能もダイナミックに変化しており、これに対応するために自社のビジネスにも、変化が常に求められています。このため、収集したプライバシーデータを適切に保護し、プライバシー侵害を防ぐために、これらの変化を適時適切に捉え、それについて自社に与える影響を分析し、ポリシーやプロセス、ビジネスの今後の展望等にフィードバックするというサイクルを構築することが肝要です。

以下は、このサイクルを図示したものです。リスク評価にあたっては、まずIoT機器がどのようなデータを収集するかを正確に特定することが肝心です。この作業はビジネスの内容によっては、膨大な労力と時間を要する場合もありますが、プライバシーデータを保護するための根幹をなす重要なタスクですので、着実に取り組むことが望まれます。

図2




グローバルでビジネスを展開している、またはこれから展開を検討している企業は、どの国や地域を対象として、どのような情報を取得・処理し、ビジネスに活用するのかという戦略を、現行あるいは今後に制定される予定の法規制を正確に理解しつつ、企業内のポリシーやプロセスを必要に応じて見直す必要があります。その際には、ビジネス推進部門は法務部やリスク管理部等の社内の関連部門、および必要に応じて適切な知識と経験を持った外部専門家と連携しながら、ビジネスの早期段階から検討を始めることが望まれます。

IoTに代表されるような最先端技術をビジネスで利活用する際は、利益や結果の追求、いわゆるビジネス上の「攻め」の部分で活用し、傾倒する企業が多いように思われます。しかし同時に、それらのプライバシーデータをどのようなポリシー・プロセスに基づき保護していくかといった、足元の「守り」を固めることも重要です。このような姿勢が欠如すると、情報漏洩等の思わぬインシデントが発生し、巨額の賠償金や制裁金の発生、または事業停止といったビジネス上の危機にもつながる可能性があります。企

業には「攻め」だけでなく「守り」の意識も忘れずに、プライバシーデータを利活用するビジネスの設計・展開に取り組むことが求められているのです。

## <リファレンス>

※1 National Institute of Standards and Technology, 2019. **NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks**

※2 総務省，2018. 『**平成30年版情報通信白書**』

※3 総務省，2019. 『**IoT国際競争力指標（2017年実績）**』

## 執筆者

綾部 泰二

パートナー, PwCあらた有限責任監査法人

由良 修平

シニアアソシエイト, PwCあらた有限責任監査法人

※法人名、役職、コラムの内容などは掲載当時のものです。

お問い合わせ

採用情報

イベント／セミナー

ニュースルーム

情報提供ホットライン

サービス

**監査およびアシュアランス**

**コンサルティング**

**ディールアドバイザリー**

**税務**

**法務**

**日本企業の海外事業支援**

Today's issues

業種別サービス

**自動車**

**重工業・産業機械**

**化学**

**エネルギー・資源・鉱業**

**建設**

**運輸・物流**

**消費財・小売・流通**

**テクノロジー**

**情報通信**

**エンタテイメント&メディア**

**ホスピタリティ&レジャー**

**総合商社**

**金融サービス**

**銀行・証券**

**資産運用**

**保険**

**不動産**

**プライベート・エクイティ**

**都市・インフラストラクチャー**

**官公庁・公的機関**

**農業**

**医薬・ライフサイエンス**

**ヘルスケア**

**人材サービス**

ナレッジ

**調査／レポート**

**会計基準や税制、法令等に関するニュース**

**広報誌**

**トピック解説／コラム／対談**

**イベント／セミナーレポート**

**各種ガイドブック**

**書籍**

**寄稿記事**

**動画**

**ケーススタディ／事例紹介**

PwC Japanグループ

**PwCあらた有限責任監査法人**

**PwC京都監査法人**

**PwCコンサルティング合同会社**

**PwCアドバイザリー合同会社**

**PwC税理士法人**

**PwC弁護士法人**

**PwC総合研究所合同会社**

**PwCサステナビリティ合同会社**

**PwCビジネスアシュアランス合同会社**

**PwCビジネスソリューション合同会社**

**PwCアセットアドバイザリー合同会社**

**一般財団法人PwC財団**

Alumni