IPA Better Life with IT

消費者のための

ネット接続製品の安全な選定・利用ガイド

-詳細版-

昨今、パソコンやスマートフォンだけではなく、エアコンや冷蔵庫などの家電製品や玩具など、色々なものがネットにつながるようになりました。その分、消費者がサイバー攻撃を受けるリスクも高まっています。

このため、製品メーカーは開発する製品に対してセキュリティを確保するための機能を搭載するなどの対応を行っています。消費者の皆様はセキュリティを確保する機能を備えた製品を選び、正しくその機能を理解して利用していますか。

このガイドでは以下の 2 点を達成する為のポイントをまとめています。

- 安全なネット接続製品を選ぶ
- 購入したネット接続製品を安全に利用する

このガイドは、確認のポイントや場所、実施しなかった場合の影響や対策などを解説した **詳細版** です。消費者の皆様が親しみ易いように、絵で分かり易くポイントだけ記載した小冊子版も提供しています。

「デザインや性能、価格だけで選んでいませんか？」

より安全なネット接続製品を選ぶためのガイドです。
家電量販店や EC サイトなどでネットに接続する製品を購入する際に安全な製品を選ぶための確認ポイント、およびその確認方法を 7 項目にまとめています。

「購入した製品を、そのままの状態で使い続けていませんか？」

ネットに接続する製品を安全に利用するためのガイドです。
購入した製品を安全に利用するためのポイント、および対応方法を 7 項目にまとめています。

上記の小冊子、および「ネット接続製品の安全な選定・利用ガイド –詳細版-」はこちらの QR コードからアクセス可能です。

ガイドの使い方

「デザインや性能、価格だけで選んでいませんか？」

購入を検討している製品について、「購入①～購入⑦」に従って、製品メーカーのセキュリティに関する対応状況や、製品に搭載されているセキュリティ機能を確認してください。
確認箇所は各ポイントの「主に確認できる場所」にチェックがあるものを参照してください。

「購入した製品を、そのままの状態で使い続けていませんか？」

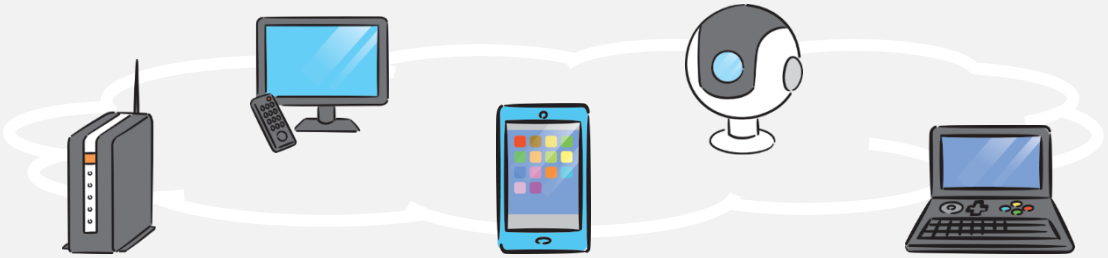
購入した製品や現在利用している製品について、「利用①～利用⑦」に記載されていることを消費者の皆様が対応できているか確認してください。
対応方法は各ポイントの「主に確認できる場所」にチェックがあるものを参照してください。

- ✓ このガイドには、末尾に「用語について」という項目があり、用語の説明を記載しています。ガイド本編を確認する際には、併せてご参照ください。
- ✓ 「主に確認できる場所」は、製品メーカーや製品によって異なるため、チェックのついたものを見ても情報を確認できない場合は製品メーカーか量販店へ問い合わせてください。
- ✓ 「主に確認できる場所」として「パッケージ」にチェックがついていたとしても、EC サイトで購入する場合などは事前にパッケージを確認できない場合があります。このような場合はウェブサイトを確認してください。

ガイドの対象製品

インターネットやホームネットワークにつながる以下のような製品

- ネットワーク家電
  （ブルーレイレコーダー、テレビ、エアコン、ロボット掃除機等）
- プリンタ
- ルータ
- ネットワークカメラ
- 玩具、ゲーム機
- スマートフォンやパソコンのアプリケーション など



「デザインや性能、価格だけで選んでいませんか？」

記載のポイント全てを確認できることが望ましいですが、全てが確認できない場合、より多くのポイントが確認できる製品の購入を検討してください。

購入① アップデート機能がありますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
✓	✓	✓*

*製品情報ウェブサイト

確認しないとどうなる？

アップデート機能がないと、製品購入後にセキュリティ上の問題が発生した際に、問題をなおすことができません。製品を最新ではない状態で使い続けることで、ネットを通じて製品に不正に侵入され、製品から情報※が盗まれたり、製品に不正な指示を送られて不具合を発生させられる恐れがあります。

※　氏名や住所、クレジットカード番号などの情報が狙われます。

＜確認方法＞
製品のパッケージやウェブサイト等に、製品がアップデートを行う旨や、アップデート方法が掲載されているかを確認ください。

購入② 製品のセキュリティに関する最新情報がウェブサイトに掲載されていますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
ー	ー	✓*

*製品サポートウェブサイト

確認しないとどうなる？

製品の最新情報が得られないと、製品のセキュリティに関する不具合があったときに、その内容や影響、対応方法を知ることができません。さらに、利用者はアップデートのためのファイルを入手できず、アップデートを実施できない場合があります。製品の出荷前にセキュリティ対策を実施していたとしても、時間の経過により製品出荷後にセキュリティ上の問題が発覚する場合があります。これは珍しいことではありません。

セキュリティ上の問題を修正したときに、問題の内容と対策方法をきちんと一般消費者へ公表している製品メーカーの製品が望ましいです。

＜確認方法＞
製品のウェブサイトに、アップデートによる製品の設定や機能の変更・改善点が継続的に掲載されているか確認してください。

購入③ 問い合わせ先がありますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
✓	✓	✓

確認しないとどうなる？

製品メーカーの問い合わせ先を把握できないと、製品に不具合が発生したときに、製品メーカーの対応状況の確認や、利用者における不具合への対応方法を確認することができず、製品が利用できなくなる場合があります。

＜確認方法＞
製品のパッケージ等に、お客様窓口や製品サポート窓口等、製品メーカーの問合せ先が掲載されているかを確認ください。

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	−	✓

購入④ 製品のセキュリティ方針について記載がありますか？

確認しないとどうなる？

製品に関するセキュリティ方針が策定・開示されていないと、製品メーカーがセキュリティ対策を組織として責任を持って実施しているか確認できません。製品メーカーがセキュリティ方針を策定していない場合、製品のセキュリティが保たれなかったり、事故が起こった場合に誠意ある対応を期待できない場合があります。

＜確認方法＞

製品メーカーのウェブサイト等に、「製品セキュリティポリシー」「製品セキュリティ方針」等、製品のセキュリティを確保するための、企業としての方針・考え方・宣言等について掲載されているかを確認ください。

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	✓	✓*

*製品情報ウェブサイト

購入⑤ 製品のセキュリティ機能や設定※について具体的な記載がありますか？

確認しないとどうなる？

製品のセキュリティ機能や設定に関する具体的な記載がないと、利用する際に正しく設定できず、セキュリティ機能や設定が十分に機能しないことで、セキュリティを脅かされる恐れがあります。

※ ここでの「セキュリティ機能や設定」とは、IDやパスワードを変更する機能や、製品に対する不具合を改善するためのアップデート機能などを示しています。

＜確認方法＞

本項での「セキュリティ機能や設定」は、主に下記のような機能を指します。
下記はネット接続についての一般例です。製品によって必要となる機能は異なるため、これ以外にも存在する場合があります。どのような機能が備わっているべきかは、複数の同種製品について機能比較をすることで確認ください。

- アップデート機能： 利用者に被害が生じないように、セキュリティ上の不具合を改善する機能
- 初期化機能： 製品破棄時に情報が漏洩しないように、購入時の状態に戻す機能
- 暗号通信機能： 通信が他の人から読み取られることで情報漏えいしないように、通信を暗号化する機能
- ID/パスワードが必要な場合、設定が変更できる機能

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
✓	−	✓*

*製品情報ウェブサイト

購入⑥ サポート情報について記載がありますか？

確認しないとどうなる？

製品のサポート期限がわからないまま使い続けていると、サポート終了後に最新のセキュリティに関する情報や最新のソフトウェアを入手することができず、セキュリティを脅かされたまま製品を使わなければなりません。

＜確認ポイント＞

製品購入時点で、予めサポート期間（サポート終了時期）が掲載されている製品を選ぶことが望ましいです。

購入⑦ 製品を廃棄するとき購入時の状態に戻せますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
✓	✓	✓*

*製品情報ウェブサイト

確認しないとどうなる？

製品に保存された情報は、購入時の状態に戻す（初期化）等をしないと完全に削除ができません。完全に削除しないままに廃棄すると、製品に保存された情報が漏洩し、プライバシーが侵害されたり、盗まれた情報を悪用される恐れがあります。

※ ここでの「購入時の状態」とは、製品に保存した連絡先、写真、メモといった情報、製品を使用するために設定した情報やインストールしたアプリ等を全て削除して、製品が工場出荷時の状態になっていることを指します。

「購入した製品を、そのままの状態で使い続けていませんか？」

利用①

アカウント設定がある製品は

購入したらすぐにパスワードの変更など セキュリティの設定を実施していますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
–	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

初期設定のパスワードが「推測されやすいもの」や公開されている「取扱説明書等に記載されているもの」だった場合、そのパスワードは他人から容易に推測されたり、取扱説明書等によって他人に知られてしまったりする恐れがあります。それによってネットを通じて製品に不正に侵入され、製品から情報が盗まれたり、製品に不正な指示を送られて不具合を発生させられる恐れがあります。

対策できないときは？

セキュリティ設定としてどのような設定項目があるかわからない場合や設定方法がわからない場合は、製品メーカーに尋ねてください。利用者がセキュリティ設定をしなくても安全に使えるよう設計されている製品であれば問題ありませんが、セキュリティに配慮がなく、セキュリティ設定を実施できない製品の場合は、できるだけ早期に設定可能な製品に買い替えてください。

利用②

製品メーカーのウェブサイトを確認して アップデートしていますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
–	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

アップデートを行わないと、製品メーカーが提供する更新されたセキュリティ機能を製品に適用できません。セキュリティ機能が最新ではない状態が続くことで、ネットを通じて製品に不正に侵入され、製品から情報が盗まれたり、製品に不正な指示を送られて不具合を発生させられる恐れがあります。

対策できないときは？

アップデートの状況や実施方法がわからない場合は、製品メーカーに尋ねてください。アップデートできない場合は、製品メーカーが提示している問題の回避策を適用するか、ネットから切り離して利用するなどします。回避策がなく、ネットへ接続する必要がある場合は、買い替えてください。もともとアップデートができない製品である場合は、買い替え時期が来たら、アップデート機能を持つ製品に買い替えてください。

利用③

セキュリティのサポートが終了した製品を 利用していませんか？

利用をやめるか、買い替えましょう

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
–	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

製品のサポートが終了すると、製品に最新のセキュリティ機能が提供されなくなったり、不具合が起こった時に対処されなくなったりする場合があります。セキュリティ機能が最新ではない状態で製品を利用し続けることで、サイバー攻撃を受けるリスクが高まります。

対策できないときは？

サポート終了後に速やかに製品の利用を中止できない場合は、製品メーカーに連絡し、どのような対応が適切か確認してください。サポートしている後継製品がある場合は、後継製品へ乗り換えてください。後継製品がない場合は、同じような機能を有する製品を製品メーカーに尋ねて買い替えてください。

※ ここでのサポートはセキュリティサポートを意味しており、セキュリティサポート終了後も、ネットに接続せずに製品を利用できることがあります。

利用④ パスワード以外に、提供されたセキュリティ機能を使用していますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	✓	✓

対策しないとどうなる？

製品のセキュリティ機能を使っていなかったり、取扱説明書などの記載を基に正しく設定していなかったりすると、製品のセキュリティ機能が十分に動作せず、その結果セキュリティを脅かされる恐れがあります。

対策できないときは？

セキュリティ機能や設定について具体的にどのような機能があるかわからない場合や設定方法がわからない場合は、製品メーカーに尋ねてください。

利用⑤ 不慮の事故に備えて、バックアップや設定内容の記録を取っていますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

バックアップや設定内容の記録を取っていないと、事故が発生した時や、製品に保存された情報が他人に暗号化されたり、全て消去されたりした場合に、復元できなくなるなどの恐れがあります。その結果、製品が二度と利用できなくなったり、機器の状態を元に戻すのが大変になる、あるいは元に戻せなくなったりすることもあります。

対策できないときは？

バックアップの方法や設定内容の記録方法がわからない場合は、製品メーカーに尋ねてください。

利用⑥ 使わなくなった製品はネットから切り離していますか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

使わなくなった製品は、製品メーカーが不具合を改善するアップデートを提供しても、適用されることはありません。そのため、製品にセキュリティ上の不具合が発見された場合、アップデートが適用されないままネットに繋がり続けることになります。その結果、ネットを通じて製品に不正に侵入され、製品から情報が盗まれたり、製品に不正な指示を送られて不具合を発生させられる恐れがあります。

対策できないときは？

ネットからの切り離し方がわからない場合は、製品メーカーに尋ねるか、あるいは製品の電源を切って他人がネットを通じて製品にアクセスできないようにしてください。

利用⑦ 製品を廃棄する場合には購入時の状態に戻しましたか？

主に確認できる場所

パッケージ	取扱説明書	ウェブサイト
−	✓	✓*

*製品情報ウェブサイト

対策しないとどうなる？

購入時の状態（初期化された状態）に戻さずに製品を廃棄した場合、製品に残っている情報が盗み取られる恐れがあり、その結果、漏洩し、プライバシーが侵害されたり、盗まれた情報を悪用される恐れがあります。

※ ここでの「購入時の状態」とは、製品に保存した連絡先、写真、メモといった情報、製品を使用するために設定した情報やインストールしたアプリ等を全て削除して、製品が工場出荷時の状態になっていることを指します。

対策できないときは？

製品購入時の状態に戻す方法がわからない場合は、製品メーカーに尋ねてください。製品購入時に戻すことができない製品の場合は、手動でデータを消去して廃棄する、物理的に破壊する等して、再利用できないようにします。また、今後は、購入時の状態に戻せる製品を買うようにしてください。

用語について

● アカウント	スマートフォンやパソコン等の製品・端末、ネットワーク、ネットワークを通じたサービス等を利用する際の権利。通常は、利用者に割り当てられるIDのこと。 IDとパスワードを合わせて「アカウント」と呼ぶこともあります。
● アップデート	ソフトウェアを更新し、最新の状態にすること。
● サイバー攻撃	ネットワークやパソコン等を利用して行われる攻撃のこと。 近年は、家電やネットワークカメラなど、様々なものがインターネットに接続しているため、サイバー攻撃の対象となります。
● セキュリティ	スマートフォンやパソコン等の製品・端末、ネットワーク、ネットワークを通じたサービス、その上でやりとりされるデータ・情報等を、サイバー攻撃・災害等から保護すること。

本ガイドに関するお問合せ先

IPA セキュリティセンター

- E-mail: vuln-inq@ipa.go.jp