ETSI EN 303 645 V2.1.1 (2020-06)

CYBER;
Cyber Security for Consumer Internet of Things: Baseline Requirements

ETSI EN 303 645 V2.1.1 (2020-06)

欧州電気通信標準化協会（ETSI）
サイバーセキュリティ技術委員会（CYBER）；
民生用 IoT 機器のサイバーセキュリティ: ベースライン要件

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Reference

REN/CYBER-0048

Keywords

cybersecurity, IoT, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

参照

REN/CYBER-0048

キーワード

サイバーセキュリティ、IoT、プライバシー

***ETSI*（欧州電気通信標準化協会）**
650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

留意事項

本文書は下記よりダウンロード可能:
http://www.etsi.org/standards-search

本文書は、電子版及び／又は印刷版として利用可能である。本文書の電子版及び／又は印刷版の内容は、ETSI の書面による事前の許可なくして変更してはならない。そのようなバージョン及び／又は印刷版の間に、内容の相違がある、又は相違が認められる場合、www.etsi.org/deliver で PDF 形式で入手可能なものが、ETSI の成果物の現行バージョンである。

本文書の利用者は、本文書に改訂又は変更の可能性があることを認識しておくことが望ましい。本文書及びその他の ETSI 文書のステータスに関する情報は、https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx で入手できる。
本文書の内容に誤りを見つけた場合は、以下のいずれかのサービスまでコメントを送信されたい。:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

目次

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER).

National transposition dates	
Date of adoption of this EN:	19 June 2020
Date of latest announcement of this EN (doa):	30 September 2020
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2021
Date of withdrawal of any conflicting National Standard (dow):	31 March 2021

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

As more devices in the home connect to the Internet, the cyber security of the Internet of Things (IoT) becomes a growing concern. People entrust their personal data to an increasing number of online devices and services. Products and appliances that have traditionally been offline are now connected and need to be designed to withstand cyber threats.

The present document brings together widely considered good practice in security for Internet-connected consumer devices in a set of high-level outcome-focused provisions. The objective of the present document is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products.

知的財産権

必須特許

規範的な成果物に必須、又は潜在的に必須である知的財産権が ETSI に宣言されている場合がある。これらの必須の知的財産権に関する情報がある場合は、ETSI のメンバー及び非メンバーに対して公開されており、ETSI 事務局から入手可能な「ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*」に記載されている。最新のアップデートは、ETSI の Web サーバ（https://ipr.etsi.org/) から入手可能である。

ETSI の知的財産権ポリシーに基づき、ETSI は知的財産権の調査を含むいかなる調査も行っていない。ETSI SR 000 314 (又は ETSI Web サーバ上のアップデート) で言及されていない、本文書にとって必須、又は必須となる可能性のある他の知的財産権の存在については、保証されるものではない。

商標

本文書には、所有者が主張又は登録した商標及び／又は商号が含まれる場合がある。ETSI は、ETSI の所有物であると示されているものを除き、これらの所有権を主張しておらず、いかなる商標や商号を使用又は複製する権利も譲渡しない。本文書におけるこれらの商標の言及は、これらの商標に関連する製品、サービス、組織を ETSI が推奨することを意味するものではない。

序文

この欧州規格 (EN) は、ETSI サイバーセキュリティ技術委員会 (CYBER)が作成したものである。

国内規格への移管日	
本欧州規格の採択日：	2020 年 6 月 19 日
本欧州規格の最新発表日 (doa)：	2020 年 9 月 30 日
新国内規格の最新公表日又は本欧州規格の承認日 (dop/e)：	2021 年 3 月 31 日
矛盾する国内規格の廃止日 (dow)：	2021 年 3 月 31 日

法助動詞の用語

本文書では **"shall"**、**"shall not"**、**"should"**、**"should not"**、**"may"**、**"need not"**、**"will"**、**"will not"**、**"can"**、**"cannot"** は ETSI Drafting Rules (Verbal forms for the expression of provisions)の 3.2 項で述べられているように解釈するものとする。

ETSI の成果物では、直接引用する場合を除き、**"must"** 及び **"must not"** の**使用は禁じられている**。

はじめに

家庭でインターネットに接続する機器が増えるにつれて、モノのインターネット（IoT）のサイバーセキュリティに関する懸念が高まっている。人々は、ますます多くのオンラインの機器やサービスに自分の個人データを預けるようになっている。従来はオフラインであった製品や家電がインターネットに接続されるようになり、サイバー脅威に耐えられるような設計が必要となっている。

本文書は、インターネットに接続された民生用機器のセキュリティについて、広く考えられているグッドプラクティスを、成果に焦点を当てた一連の高レベルな規定としてまとめている。本文書の目的は、民生用 IoT 機器の開発・製造に関わるすべての関係者に、製品をセキュアにするガイダンスを提供することである。

The provisions are primarily outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products.

The present document is not intended to solve all security challenges associated with consumer IoT. It also does not focus on protecting against attacks that are prolonged/sophisticated or that require sustained physical access to the device. Rather, the focus is on the technical controls and organizational policies that matter most in addressing the most significant and widespread security shortcomings. Overall, a baseline level of security is considered; this is intended to protect against elementary attacks on fundamental design weaknesses (such as the use of easily guessable passwords).

The present document provides a set of baseline provisions applicable to all consumer IoT devices. It is intended to be complemented by other standards defining more specific provisions and fully testable and/or verifiable requirements for specific devices which, together with the present document, will facilitate the development of assurance schemes.

Many consumer IoT devices and their associated services process and store personal data, the present document can help in ensuring that these are compliant with the General Data Protection Regulation (GDPR) [i.7]. Security by design is an important principle that is endorsed by the present document.

ETSI TS 103 701 [i.19] provides guidance on how to assess and assure IoT products against provisions within the present document.

The provisions in the present document have been developed following a review of published standards, recommendations and guidance on IoT security and privacy, including: ETSI TR 103 305-3 [i.1], ETSI TR 103 309 [i.2], ENISA Baseline Security Recommendations [i.8], UK Department for Digital, Culture, Media and Sport (DCMS) Secure by Design Report [i.9], IoT Security Foundation Compliance Framework [i.10], GSMA IoT Security Guidelines and Assessment [i.11], ETSI TR 103 533 [i.12], DIN SPEC 27072 [i.20] and OWASP Internet of Things [i.23].

NOTE: Mappings of the landscape of IoT security standards, recommendations and guidance are available in ENISA Baseline Security Recommendations for IoT - Interactive Tool [i.15] and in Copper Horse Mapping Security & Privacy in the Internet of Things [i.14].

As consumer IoT products become increasingly secure, it is envisioned that future revisions of the present document will mandate provisions that are currently recommendations in the present document.

規定は、規範的なものではなく、主に成果に焦点を当てたものであり、組織が自社製品に適したセキュリティソリューションを採用し、実装する柔軟性を提供するものである。

本文書は、民生用 IoT 機器に関連するすべてのセキュリティ課題を解決することを目的としていない。また、長期的／高度な攻撃や、機器への継続的な物理アクセスを必要とする攻撃からの保護にも焦点を当てていない。むしろ、最も重要で広範なセキュリティの欠点に対処する上で、最も重要な技術的管理策と組織的ポリシーに焦点を当てている。全般的に見れば、セキュリティの基本的なレベルが考慮されている。これは、基本的な設計上の弱点（簡単に推測できるパスワードの使用など）に対する初歩的な攻撃から保護することを目的としている。

本文書は、すべての民生用 IoT 機器に適用される一連の基本的な規定を提供する。本文書は、本文書とともに保証スキームの開発を促進することになる、より具体的な規定及び特定の機器に対する十分にテスト可能及び／又は検証可能な要件を定義した他の標準類によって補完されることを意図している。

多くの民生用 IoT 機器とその関連サービスは、個人データを処理及び保存する。本文書は、これらが EU 一般データ保護規則（GDPR）[i.7]に準拠していることを保証するのに役立つ。セキュリティ・バイ・デザインは、本文書で承認されている重要な原則である。

ETSI TS 103 701 [i.19]は、本文書内の規定に対する IoT 製品の評価と保証の方法に関するガイドラインを提供している。

本文書の規定は、IoT のセキュリティとプライバシーに関する公開された標準類、勧告、ガイダンスのレビューを経て策定されたもので、それらには以下のものが含まれる。

ETSI TR 103 305-3 [i.1]、ETSI TR 103 309 [i.2]、ENISA Baseline Security Recommendations [i.8]、UK Department for Digital, Culture, Media and Sport (DCMS) Secure by Design Report [i.9]、IoT Security Foundation Compliance Framework [i.10]、 GSMA IoT Security Guidelines and Assessment [i.11]、ETSI TR 103 533 [i.12]、DIN SPEC 27072 [i.20]、OWASP Internet of Things [i.23]

注： IoT セキュリティの標準類、勧告、ガイダンスのマッピングは、ENISA Baseline Security Recommendations for IoT - Interactive Tool [i.15] 及び Copper Horse Mapping Security & Privacy in the Internet of Things [i.14]で入手できる。

民生用 IoT 製品がますますセキュアになるにつれて、将来の改訂で、現在本文書で推奨されている規定が義務化されることが想定される。

1 Scope

The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. A non-exhaustive list of examples of consumer IoT devices includes:

- connected children's toys and baby monitors;
- connected smoke detectors, door locks and window sensors;
- IoT gateways, base stations and hubs to which multiple devices connect;
- smart cameras, TVs and speakers;
- wearable health trackers;
- connected home automation and alarm systems, especially their gateways and hubs;
- connected appliances, such as washing machines and fridges; and
- smart home assistants.

Moreover, the present document addresses security considerations specific to constrained devices.

EXAMPLE: Window contact sensors, flood sensors and energy switches are typically constrained devices.

The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table B.1 provides a schema for the reader to give information about the implementation of the provisions.

Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document.

The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.

Annex A (informative) of the present document has been included to provide context to clauses 4, 5 and 6 (normative). Annex A contains examples of device and reference architectures and an example model of device states including data storage for each state.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

適用範囲

本文書は、ネットワークインフラ（インターネットやホームネットワークなど）に接続される民生用 IoT 機器と、その関連サービスとのやりとりに関する高レベルのセキュリティ及びデータ保護規定を規定している。関連サービスについては適用範囲外である。民生用 IoT 機器の例の非網羅的なリストには、以下が含まれる。

- 接続された子供のおもちゃ及びベビーモニタ；
- 接続された煙探知機、ドアロック、及び窓センサ；
- 複数の機器が接続する IoT ゲートウェイ、基地局、及びハブ；
- スマートカメラ、スマートテレビ、及びスマートスピーカー；
- ウェアラブル健康トラッカー；
- 接続されたホームオートメーションシステム及びアラームシステム、特にそのゲートウェイ及びハブ；
- 洗濯機や冷蔵庫などの接続された電化製品；
- スマートホームアシスタント

さらに、本文書では、制約のある機器に特有のセキュリティの考慮事項も扱っている。

例：窓の接触センサ、洪水センサ、及びエネルギースイッチは、典型的な制約を受ける機器である。

本文書は、民生用 IoT の開発及び製造に携わる組織が、これらの規定をどのように実施するかについて、例と説明文を通じて、基本的なガイダンスを提供する。表 B.1 は、読者に規定の実施に関する情報を提供するためのスキーマを提供する。

民生用 IoT 機器ではない機器、例えば、製造業、医療、又はその他の産業用途での使用を主目的とする機器は、本文書の適用範囲外である。

本文書は、主に消費者の保護を支援するために作成されたが、民生用 IoT の他のユーザも、ここに記載されている規定の実装によって、同様の恩恵を受ける。

本文書の附録 A（参考）は、4 項 、 5 項、及び 6 項（引用）の背景を提供するために含まれている。附録 A には、機器及び参照アーキテクチャの例と、各状態でのデータ記憶装置を含む機器の状態のモデル例が含まれている。

参照

2.1 引用規格

参照には、特定のもの（発効日及び／又は版番号又はバージョン番号で識別される）と特定していないものがある。特定の参照については、引用されたバージョンのみ適用される。特定していない参照については、参照された文書の最新版（すべての改訂を含む）が適用される。

期待される場所で一般に入手できない参照文献は、https://docbox.etsi.org/Reference/ にあるかもしれない。

注：本項に含まれている URL は、公開時には有効であったが、ETSI はその長期的な有効性を保証するものではない。

本文書の適用には、以下の参考文書が必要である。

該当なし。

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations".

[i.2] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.3] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[i.4] ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".

NOTE: Available at https://www.iso.org/standard/45170.html.

[i.5] OASIS: "CSAF Common Vulnerability Reporting Framework (CVRF)".

NOTE: Available at http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html.

[i.6] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.8] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

NOTE: Available at https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a50601aa75ed71a1/language-en/format-PDF/source-117211901.

[i.9] UK Department for Digital, Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report", March 2018.

NOTE: Available at https://www.gov.uk/government/collections/secure-by-design.

[i.10] IoT Security Foundation: "IoT Security Compliance Framework", Release 2 December 2018.

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-SecurityCompliance-Framework-Release-2.0-December-2018.pdf.

[i.11] GSMA: "GSMA IoT Security Guidelines and Assessment".

NOTE: Available at https://www.gsma.com/iot/iot-security/iot-security-guidelines/.

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] Commission Notice: The "Blue Guide" on the implementation of EU products rules 2016 (Text with EEA relevance), 2016/C 272/01.

NOTE: Available in the Official Journal of the European Union, https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=OJ:C:2016:272:TOC.

[i.14] Copper Horse: "Mapping Security & Privacy in the Internet of Things".

NOTE: Available at https://iotsecuritymapping.uk/.

2.2 参照文献

参照には、特定のもの（発効日及び／又は版番号又はバージョン番号で識別される）と特定していないものがある。特定の参照については、引用されたバージョンのみ適用される。特定していない参照については、参照された最新版（すべての改訂を含む）が適用される。

注：本項に含まれている URL は、公開時には有効であったが、ETSI はその長期的な有効性を保証するものではない。

以下の参照文献は、本文書の適用に必要なものではないが、特定の主題の領域について、ユーザを支援するものである。

[i.1] ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations".

[i.2] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.3] NIST Special Publication 800-63B: "Digital Identity Guidelines - Authentication and Lifecycle Management".
注：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf で入手できる。

[i.4] ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".
注：https://www.iso.org/standard/45170.html で入手できる。

[i.5] OASIS: "CSAF Common Vulnerability Reporting Framework (CVRF)".
注：http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html で入手できる。

[i.6] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.8] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, ISBN: 978-92-9204-236-3, doi: 10.2824/03228.
注：https://op.europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a50601aa75ed71a1/language-en/format-PDF/source-117211901 で入手できる。

[i.9] UK Department for Digital, Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report", March 2018.
注：https://www.gov.uk/government/collections/secure-by-design で入手できる。

[i.10] IoT Security Foundation: "IoT Security Compliance Framework", Release 2 December 2018.
注：https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-SecurityCompliance-Framework-Release-2.0-December-2018.pdf で入手できる。

[i.11] GSMA: "GSMA IoT Security Guidelines and Assessment".
注：https://www.gsma.com/iot/iot-security/iot-security-guidelines/ で入手できる。

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] Commission Notice: The "Blue Guide" on the implementation of EU products rules 2016 (Text with EEA relevance), 2016/C 272/01.
注：欧州連合（EU）の官報 https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=OJ:C:2016:272:TOC で入手できる。

[i.14] Copper Horse: "Mapping Security & Privacy in the Internet of Things".
注：https://iotsecuritymapping.uk/ で入手できる。

[i.15] ENISA: "Baseline Security Recommendations for IoT - Interactive Tool".

NOTE: Available at https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-securityrecommendations-for-iot-interactive-tool.

[i.16] IoT Security Foundation: "Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies".

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/VulnerabilityDisclosure-Design-v4.pdf.

[i.17] F-Secure: "IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks".

NOTE: Available at https://blog.f-secure.com/iot-threats/.

[i.18] W3C: "Web of Things at W3C".

NOTE: Available at https://www.w3.org/WoT/.

[i.19] ETSI TS 103 701: "CYBER; Cybersecurity assessment for consumer IoT products".

NOTE: It is under development.

[i.20] DIN SPEC 27072: "Information Technology - IoT capable devices - Minimum requirements for Information security".

[i.21] GSMA: "Coordinated Vulnerability Disclosure (CVD) Programme".

NOTE: Available at https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/.

[i.22] IoT Security Foundation: "Vulnerability Disclosure - Best Practice Guidelines".

NOTE: Available at https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/VulnerabilityDisclosure_WG4_2017.pdf.

[i.23] OWASP Internet of Things (IoT) Top 10 2018.

NOTE: Available at https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.

[i.24] IEEE 802.15.4™-2015: "IEEE Standard for Low-Rate Wireless Networks".

NOTE: Available at https://standards.ieee.org/content/ieee-standards/en/standard/802_15_4-2015.html.

[i.25] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[i.26] GSMA: "SGP.22 Technical Specification v2.2.1".

[i.27] ISO/IEC 27005:2018: "Information technology - Security techniques - Information security risk management".

NOTE: Available at https://www.iso.org/standard/75281.html.

[i.28] Microsoft® Corporation: "The STRIDE Threat Model".

NOTE: Available at https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx.

[i.29] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.15] ENISA: "Baseline Security Recommendations for IoT - Interactive Tool".
注：https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-securityrecommendations-for-iot-interactive-tool で入手できる。

[i.16] IoT Security Foundation: "Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies".
注：https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/VulnerabilityDisclosure-Design-v4.pdf で入手できる。

[i.17] F-Secure: "IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks".
注：https://blog.f-secure.com/iot-threats/ で入手できる。

[i.18] W3C: "Web of Things at W3C".
注：https://www.w3.org/WoT/ で入手できる。

[i.19] ETSI TS 103 701: "CYBER; Cybersecurity assessment for consumer IoT products".
注：現在、策定中。

[i.20] DIN SPEC 27072: "Information Technology - IoT capable devices - Minimum requirements for Information security".

[i.21] GSMA: "Coordinated Vulnerability Disclosure (CVD) Programme".
注：https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/ で入手できる。

[i.22] IoT Security Foundation: "Vulnerability Disclosure - Best Practice Guidelines".
注：https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/VulnerabilityDisclosure_WG4_2017.pdf で入手できる。

[i.23] OWASP Internet of Things (IoT) Top 10 2018.
注：https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 で入手できる。

[i.24] IEEE 802.15.4™-2015: "IEEE Standard for Low-Rate Wireless Networks".
注：https://standards.ieee.org/content/ieee-standards/en/standard/802_15_4-2015.html で入手できる。

[i.25] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[i.26] GSMA: "SGP.22 Technical Specification v2.2.1".

[i.27] ISO/IEC 27005:2018: "Information technology - Security techniques - Information security risk management".
注：https://www.iso.org/standard/75281.html で入手できる。

[i.28] Microsoft® Corporation: "The STRIDE Threat Model".
注：https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx で入手できる。

[i.29] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

administrator: user who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality

associated services: digital services that, together with the device, are part of the overall consumer IoT product and that are typically required to provide the product's intended functionality

EXAMPLE 1: Associated services can include mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs).

EXAMPLE 2: A device transmits telemetry data to a third-party service chosen by the device manufacturer. This service is an associated service.

authentication mechanism: method used to prove the authenticity of an entity

NOTE: An "entity" can be either a user or machine.

EXAMPLE: An authentication mechanism can be the requesting of a password, scanning a QR code, or use of a biometric fingerprint scanner.

authentication value: individual value of an attribute used by an authentication mechanism

EXAMPLE: When the authentication mechanism is to request a password, the authentication value can be a character string. When the authentication mechanism is a biometric fingerprint recognition, the authentication value can be the index fingerprint of the left hand.

best practice cryptography: cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques

NOTE 1: This does not refer only to the cryptographic primitives used, but also implementation, key generation and handling of keys.

NOTE 2: Multiple organizations, such as SDOs and public authorities, maintain guides and catalogues of cryptographic methods that can be used.

EXAMPLE: The device manufacturer uses a communication protocol and cryptographic library provided with the IoT platform and where that library and protocol have been assessed against feasible attacks, such as replay.

constrained device: device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use

NOTE 1: Physical limitations can be due to power supply, battery life, processing power, physical access, limited functionality, limited memory or limited network bandwidth. These limitations can require a constrained device to be supported by another device, such as a base station or companion device.

EXAMPLE 1: A window sensor's battery cannot be charged or changed by the user; this is a constrained device.

EXAMPLE 2: The device cannot have its software updated due to storage limitations, resulting in hardware replacement or network isolation being the only options to manage a security vulnerability.

EXAMPLE 3: A low-powered device uses a battery to enable it to be deployed in a range of locations.

Performing high power cryptographic operations would quickly reduce the battery life, so it relies

on a base station or hub to perform validations on updates.

EXAMPLE 4: The device has no display screen to validate binding codes for Bluetooth pairing.

EXAMPLE 5: The device has no ability to input, such as via a keyboard, authentication information.

3 用語、記号、略語の定義

3.1 用語

本文書では、以下の用語が適用される：

管理者： 機器のユーザに対して可能な最高の特権レベルを持つユーザ。これは、意図された機能に関連する設定を変更できることを意味する。

関連サービス： 機器と共に民生用 IoT 製品全体の一部であり、通常は製品の意図された機能を提供するために必要なデジタルサービス。

例 1： 関連サービスには、モバイルアプリケーション、クラウドコンピューティング／ストレージ、及びサードパーティのアプリケーションプログラミングインタフェース（API）を含めることができる。

例 2： ある機器は、機器の製造業者によって選択されたサードパーティのサービスにテレメトリデータを送信する。このサービスは関連サービスである。

認証メカニズム： エンティティの真正性を証明するために使用される方法。

注： 「エンティティ」は、ユーザ又はマシンのいずれかである。

例： 認証メカニズムには、パスワードの要求、QR コードのスキャン、又は生体認証用指紋スキャナの使用がある。

認証値： 認証メカニズムで使用される属性の個別値。

例： 認証メカニズムがパスワードの要求である場合、認証値は文字列とすることができる。認証メカニズムが生体指紋認証である場合、認証値は左手の人差し指の指紋とすることができる。

ベストプラクティスの暗号技術： 対応するユースケースに適した暗号技術で、現在すぐに利用でき、実行可能な攻撃の兆候がない技術。

注 1： これは、使用される基本的な暗号だけでなく、実装、鍵生成、及び鍵の取り扱いについても当てはまる。

注 2： 標準開発機関や公的機関など複数の組織が、使用可能な暗号化手法のガイドとカタログを保持している。

例： 機器の製造業者は、IoT プラットフォームと共に提供される通信プロトコルと暗号化ライブラリを使用し、そのライブラリとプロトコルは、リプレイ攻撃などの実現可能な攻撃に対して評価されている。

制約のある機器： データを処理する機能、データを通信する機能、データを保存する機能、又はユーザと対話する機能のいずれかにおいて、意図された使用から生じる制約のために物理的な制約がある機器。

注 1： 物理的な制約は、電源、バッテリ寿命、処理能力、物理アクセス、機能の制限、メモリの制限、又はネットワーク帯域幅の制限による場合がある。これらの制約により、制約のある機器は、基地局やコンパニオンデバイスなどの別の機器によってサポートされることが必要となる場合がある。

例 1： 窓センサのバッテリは充電又は交換できない；これは制約のある機器である。.

例 2： ストレージの制限により、機器のソフトウェアをアップデートすることができないため、セキュリティの脆弱性を管理するためには、ハードウェアの交換又はネットワークの分離しか選択肢がない。

例 3： 低電力機器は、様々な場所に配置できるようにバッテリを使用している。
高電力な暗号化処理を実行するとバッテリの寿命が急速に短くなるため、アップデートの検証は基地局又はハブに頼っている。

例 4： 機器に、Bluetooth ペアリングのためのバインドコードを検証するための表示画面がない。

例 5： 機器に、キーボードなどの認証情報の入力機能がない。

NOTE 2: A device that has a wired power supply and can support IP-based protocols and the cryptographic primitives used by those protocols is not constrained.

EXAMPLE 6: A device is mains powered and communicates primarily using TLS (Transport Layer Security).

consumer: natural person who is acting for purposes that are outside her/his trade, business, craft or profession

NOTE: Organizations, including businesses of any size, use consumer IoT. For example, Smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses.

consumer IoT device: network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables

NOTE 1: Consumer IoT devices are commonly also used in business contexts. These devices remain classified as consumer IoT devices.

NOTE 2: Consumer IoT devices are often available for the consumer to purchase in retail environments. Consumer IoT devices can also be commissioned and/or installed professionally.

critical security parameter: security-related secret information whose disclosure or modification can compromise the security of a security module

EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.

debug interface: physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality

EXAMPLE: Test points, UART, SWD, JTAG.

defined support period: minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates

NOTE: This definition focuses on security aspects and not other aspects related to product support such as warranty.

device manufacturer: entity that creates an assembled final consumer IoT product, which is likely to contain the products and components of many other suppliers

factory default: state of the device after factory reset or after final production/assembly

NOTE: This includes the physical device and software (including firmware) that is present on it after assembly.

initialization: process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access

initialized state: state of the device after initialization

IoT product: consumer IoT device and its associated services

isolable: able to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured

EXAMPLE: A Smart Fridge has a touchscreen-based interface that is network-connected. This interface can be removed without stopping the fridge from keeping the contents chilled.

logical interface: software implementation that utilizes a network interface to communicate over the network via channels or ports

注 2： 有線接続された電源を有し、IP ベースのプロトコル及びそのプロトコルで使用される暗号プリミティブをサポートできる機器は、制約のある機器ではない。

例 6： 機器はコンセントを使って給電され、主に TLS（トランスポート層セキュリティ）を使用して通信を行う。

消費者： 自己の商取引、ビジネス、工芸、専門的職業以外の目的のために行動している自然人。

注： あらゆる規模の企業を含む組織が、民生用 IoT を利用している。例えば、スマートテレビは会議室に頻繁に導入されているし、ホームセキュリティキットは小規模企業の敷地を保護することができる。

民生用 IoT 機器： ネットワークに接続された（及びネットワークに接続可能な）機器で、関連サービスとの関係を持ち、通常は家庭内で、又は装着可能な電子機器として消費者に使用される。

注 1： 民生用 IoT 機器は、一般的にビジネスの環境においても使用される。これらの機器は、引き続き民生用 IoT 機器として分類される。

注 2： 民生用 IoT 機器は、多くの場合、消費者が小売り環境で購入することができる。民生用 IoT 機器は、専門的に委託及び／又は設置することもできる。

重要なセキュリティパラメータ： 曝露又は改ざんによってセキュリティモジュールのセキュリティが侵害される可能性がある、セキュリティ関連の秘密情報。

例： 秘密の暗号鍵、パスワードなどの認証値、PIN、証明書のプライベート要素。

デバッグインタフェース： 製造業者が開発中に機器と通信するため、又は機器の問題のトリアージを実行するために使用し、消費者向けの機能の一部としては使用されない物理インタフェース。

例： テストポイント、UART、SWD、JTAG。

定義されたサポート期間： 製造業者がセキュリティアップデートを提供する期間又は終了日付で表される最小期間。

注： この定義は、セキュリティの側面に焦点を当てており、保証などの製品サポートに関連する他の側面には焦点を当てていない。

機器の製造業者： 他の多くのサプライヤの製品及びコンポーネントを含む可能性がある、組み立てられた最終民生用 IoT 製品を作るエンティティ。

工場出荷時のデフォルト： 工場出荷時の状態にリセットした後の状態、又は最終的な製造／組み立て後の機器の状態。

注： これには、物理的な機器と、組み立て後にその機器に存在するソフトウェア（ファームウェアを含む）が含まれる。

初期化： 操作のために機器のネットワーク接続を有効化し、オプションとしてユーザ又はネットワークアクセスのための認証機能を設定するプロセス。

初期化状態： 初期化後の機器の状態。

IoT 製品： 民生用 IoT 機器とその関連サービス。

分離可能： 接続されているネットワークから取り外すことができ、生じた機能損失は、その接続性だけに関連し、その主な機能には関係しない。その代わりに、その環境内の機器の完全性が確実である場合に限り、他の機器と共に自己完結型の環境に置くことができる。

例： スマート冷蔵庫は、ネットワークに接続されたタッチスクリーンベースのインタフェースを備えている。このインタフェースは、冷蔵庫の中身の冷却を止めることなく取り外すことができる。

論理インタフェース： ネットワークインタフェースを利用し、チャネル又はポートを介してネットワーク上で通信するソフトウェア実装。

manufacturer: relevant economic operator in the supply chain (including the device manufacturer)

NOTE: This definition acknowledges the variety of actors involved in the consumer IoT ecosystem and the complex ways by which they can share responsibilities. Beyond the device manufacturer, such entities can also be, for example and depending on a specific case at hand: importers, distributors, integrators, component and platform providers, software providers, IT and telecommunications service providers, managed service providers and providers of associated services.

network interface: physical interface that can be used to access the functionality of consumer IoT via a network

owner: user who owns or who purchased the device

personal data: any information relating to an identified or identifiable natural person

NOTE: This term is used to align with well-known terminology but has no legal meaning within the present document.

physical interface: physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer

EXAMPLE: Radios, ethernet ports, serial interfaces such as USB, and those used for debugging.

public security parameter: security related public information whose modification can compromise the security of a security module

EXAMPLE 1: A public key to verify the authenticity/integrity of software updates.

EXAMPLE 2: Public components of certificates.

remotely accessible: intended to be accessible from outside the local network

security module: set of hardware, software, and/or firmware that implements security functions

EXAMPLE: A device contains a hardware root of trust, a cryptographic software library that operates within a trusted execution environment, and software within the operating system that enforces security such as user separation and the update mechanism. These all make up the security module.

security update: software update that addresses security vulnerabilities either discovered by or reported to the manufacturer

NOTE: Software updates can be purely security updates if the severity of the vulnerability requires a higher priority fix.

sensitive security parameters: critical security parameters and public security parameters

software service: software component of a device that is used to support functionality

EXAMPLE: A runtime for the programming language used within the device software or a daemon that exposes an API used by the device software, e.g. a cryptographic module's API.

telemetry: data from a device that can provide information to help the manufacturer identify issues or information related to device usage

EXAMPLE: A consumer IoT device reports software malfunctions to the manufacturer enabling them to identify and remedy the cause.

unique per device: unique for each individual device of a given product class or type

user: natural person or organization

3.2 Symbols

Void.

製造業者： サプライチェーン内の関連事業者（機器の製造業者を含む）。

注： この定義は、 民生用 IoT 機器エコシステムに関与する多様な主体及びそれらの主体が責任を共有する複雑な方法を認めている。機器の製造業者以外にも、例えば目前の特定のケースに応じて、輸入業者、販売業者、インテグレータ、コンポーネント及びプラットフォームプロバイダ、ソフトウェアプロバイダ、IT 及び電気通信サービスプロバイダ、マネージドサービスプロバイダ及び関連サービスのプロバイダなどがある。

ネットワークインタフェース： ネットワークを介して民生用 IoT の機能にアクセスするために使用できる物理的インタフェース。

所有者： 機器を所有するユーザ、又は購入したユーザ。

個人データ： 識別された、又は識別可能な自然人に関するあらゆる情報。

注： この用語は、周知の用語と整合させるために使用されているが、本文書内では法的意味を持たない。

物理インタフェース： 物理層で機器と通信するために使用する物理ポート又はエアインタフェース（無線、オーディオ、光など）

例： 無線、イーサネットポート、USB などのシリアルインタフェース、及びデバッグに使用されるもの。

公開セキュリティパラメータ： セキュリティ関連の公開情報で、改ざんされるとセキュリティモジュールのセキュリティが侵害される可能性があるもの。

例 1： ソフトウェアアップデートの真正性／完全性を検証するための公開鍵。

例 2： 証明書の公開要素。

リモートアクセス可能： ローカルネットワークの外部からアクセスできるよう意図されている。

セキュリティモジュール： セキュリティ機能を実装する、ハードウェア、ソフトウェア、及び/又はファームウェアのセット。

例： 機器には、ハードウェアの信頼の基点、信頼できる実行環境内で動作する暗号化ソフトウェアライブラリ、及びユーザの分離やアップデートメカニズムなどのセキュリティを強化する OS 内のソフトウェアが含まれている。これらすべてが、セキュリティモジュールを構成している。

セキュリティアップデート： 製造業者が発見した、又は製造業者に報告されたセキュリティの脆弱性に対処するためのソフトウェアアップデート。

注： 脆弱性の深刻度が、より高い優先度の修正を必要とする場合、ソフトウェアアップデートは純粋なセキュリティアップデートになり得る。

機密のセキュリティパラメータ： 重要なセキュリティパラメータ及び公開セキュリティパラメータ。

ソフトウェアサービス： 機能をサポートするために使用される機器のソフトウェアコンポーネント。

例： 機器のソフトウェア内で使用されるプログラミング言語のランタイム、又は機器のソフトウェアで使用される API を公開するデーモン（暗号化モジュールの API など）

テレメトリ：機器の使用に関する問題や情報を製造業者が特定するのに役立つ情報を提供することができる機器からのデータ。

例： 民生用 IoT 機器は、ソフトウェアの不具合を製造業者に報告し、製造業者が原因を特定して修正できるようにする。

デバイスごとに固有： 所定の製品クラス又はタイプの個々の機器毎に固有。

ユーザ： 自然人又は組織。

3.2 記号

無効

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
ASLR	Address Space Layout Randomization
CVD	Coordinated Vulnerability Disclosure
CVRF	Common Vulnerability Reporting Framework
DDoS	Distributed Denial of Service
DSC	Dedicated Security Components
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
GSM	Global System for Mobile communications
GSMA	GSM Association
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
LAN	Local Area Network
LoRaWAN	Long Range Wide Area Network
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NX	No execute
OTP	One-Time Password
QR	Quick Response
SBOM	Software Bill of Materials
SDO	Standards Development Organization
SE	Secure Elements
SSID	Service Set IDentifier
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
SWD	Serial Wire Debug
TEE	Trusted Execution Environment
TS	Technical Specification
UART	Universal Asynchronous Receiver-Transmitter
UI	User Interface
UK	United Kingdom
USB	Universal Serial Bus
WAN	Wide Area Network

4 Reporting implementation

The implementation of provisions in the present document is informed by risk assessment and threat modelling (such as ISO/IEC 27005:2018 [i.27] and STRIDE Threat Model [i.28]); this is performed by the device manufacturer and/or other relevant entities and is out of scope of the present document. For certain use cases and following risk assessment, it can be appropriate to apply additional provisions as well as those contained within the present document.

The present document sets a security baseline; however, due to the broad landscape of consumer IoT it is recognized that the applicability of provisions is dependent on each device. The present document provides a degree of flexibility through the use of non-mandatory "should" provisions (recommendations).

Provision 4-1 A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.

Table B.1 provides a schema to record these justifications in a structured manner. This is to allow other stakeholders (e.g. assurance assessors, members of the supply chain, security researchers or retailers) to determine whether provisions have been applied correctly and appropriately.

3.3 略語

本文書では、以下の略語を使用する。

API	Application Programming Interface アプリケーション・プログラム・インタフェース
ASLR	Address Space Layout Randomization アドレス空間配置のランダム化
CVD	Coordinated Vulnerability Disclosure 協調的脆弱性開示
CVRF	Common Vulnerability Reporting Framework 脆弱性情報の標準記述形式
DDoS	Distributed Denial of Service 分散型サービス拒否
DSC	Dedicated Security Components 専用のセキュリティ・コンポーネント
ENISA	European Union Agency for Network and Information Security 欧州ネットワーク・情報セキュリティ機関
EU	European Union 欧州連合
GDPR	General Data Protection Regulation EU 一般データ保護規則
GSM	Global System for Mobile communications 汎欧州デジタル移動体通信システム
GSMA	GSM Association GSM アソシエーション
IEEE	Institute of Electrical and Electronics Engineers 米国電気電子学会
IoT	Internet of Things モノのインターネット
IP	Internet Protocol インターネット・プロトコル
ISO	International Organization for Standardization 国際標準化機構
JTAG	Joint Test Action Group IEEE 1149.1　ジョイントテストアクショングループ IEEE1149.1
LAN	Local Area Network ローカルエリアネットワーク
LoRaWAN	Long Range Wide Area Network 長距離広域通信網
MAC	Media Access Control 媒体アクセス制御
NIST	National Institute of Standards and Technology 米国国立標準技術研究所
NX	No execute 実行不可
OTP	One-Time Password ワンタイムパスワード
QR	Quick Response クイック・レスポンス
SBOM	Software Bill of Materials ソフトウェア部品表
SDO	Standards Development Organization ソフトウェア開発団体［組織］
SE	Secure Elements セキュアエレメント
SSID	Service Set IDentifier サービスセット識別子
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege なりすまし（ID 偽装）、改ざん、否認、情報漏洩、サービス拒否、権限昇格
SWD	Serial Wire Debug シリアルワイヤデバッグ
TEE	Trusted Execution Environment 信頼できる実行環境
TS	Technical Specification 技術仕様書
UART	Universal Asynchronous Receiver-Transmitter 汎用非同期送受信回路
UI	User Interface ユーザインタフェース
UK	United Kingdom 英国
USB	Universal Serial Bus ユニバーサル・シリアル・バス
WAN	Wide Area Network ワイドエリアネットワーク

4 報告の実施

本文書の規定の実装は、リスクアセスメント及び脅威モデリング（ISO/IEC 27005:2018 [i.27] 及び STRIDE Threat Model [i.28]など）によって与えられる；これは、機器製造業者及び／又は他の関連するエンティティによって実施され、本文書の適用範囲外である。特定のユースケース及びその後のリスクアセスメントについては、本文書に含まれる規定だけでなく、追加の規定を適用することが適切な場合がある。

本文書はセキュリティのベースラインを設定しているが、民生用 IoT の広範な状況により、規定の適用可能性は各機器に依存することが認識されている。本文書は、非強制的な「することが望ましい（should）」規定（推奨事項）を使用することで、ある程度の柔軟性を提供している。

規定 4-1　民生用 IoT 機器に適用されない、又は実行されないと見なされる本文書の各推奨事項について、理由が記録されなければならない。

表 B.1 は、これらの正当性を構造化された方法で記録するためのスキーマを提供する。これは、他のステークホルダー（例えば、保証評価者、サプライチェーンのメンバー、セキュリティ研究者又は小売業者）が、規定が正しく適切に適用されているかを判断できるようにするためである。

EXAMPLE 1: The manufacturer publishes a completed version of table B.1 alongside the product description on their website.

EXAMPLE 2: The manufacturer completes table B.1 for internal record keeping. Sometime later, an external assurance organization assesses a product against the present document and requests information relating to the product's security design. The manufacturer can easily provide this information as it is contained within table B.1.

Cases where a provision is not applicable or not fulfilled by the consumer IoT device can include:

- when a device is a constrained device in such a way that implementation of certain security measures is not possible or not appropriate to the identified risk (security or privacy);
- where the functionality described in the provision is not included (e.g. a device that only presents data without requiring authentication).

EXAMPLE 3: A window sensor with a limited battery life sends alerts via a remote associated service when triggered and is controlled via a hub. Due to its limited battery life and processing power compared to other consumer IoT devices, it is a constrained device. In addition, because the user controls the device via a hub, the user does not need to use passwords, or other authentication mechanisms, to directly authenticate to the device.

5 Cyber security provisions for consumer IoT

5.1 No universal default passwords

Provision 5.1-1 Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

NOTE: There are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged according to NIST Special Publication 800-63B [i.3]. Using passwords for machine to machine authentication is generally not appropriate.

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

EXAMPLE 1: During initialization a device generates certificates that are used to authenticate a user to the device via an associated service like a mobile application.

To increase security, multi-factor authentication, such as use of a password plus OTP procedure, can be used to better protect the device or an associated service. Device security can further be strengthened by having unique and immutable identities.

Provision 5.1-2 Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.

EXAMPLE 2: Pre-installed passwords are sufficiently randomized.

As a counter-example, passwords with incremental counters (such as "password1", "password2" and so on) are easily guessable. Further, using a password that is related in an obvious way to public information (sent over the air or within a network), such as MAC address or Wi-Fi® SSID, can allow for password retrieval using automated means.

Provision 5.1-3 Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

例 1： 製造業者が、表 B.1 の完成版を製品説明と一緒にウェブサイトで公開する。

例 2： 製造業者が、内部記録保管のために表 B.1 を完成させる。その後、外部の保証組織が本文書に照らして製品を評価し、製品のセキュリティ設計に関する情報を要求する。この情報は表 B.1 に記載されているので、製造業者は容易に提供できる。

民生用 IoT 機器によって規定が適用されない、又は実行されないケースには、以下を含むことができる：

- 特定されたリスク（セキュリティ又はプライバシー）に対して、あるセキュリティ対策の実施が不可能であるか、適切でないような制約のある機器である場合；
- 規定に記載された機能が含まれていない場合（例えば、認証を必要とせずにデータのみを提示する機器）

例 3： バッテリの寿命が限られている窓センサは、センサが感知するとリモート関連サービス経由でアラートを送信し、ハブ経由で制御される。他の民生用 IoT 機器と比較して、バッテリの寿命や処理能力が限られているため、窓センサは制約のある機器である。また、ユーザはハブを介して機器を制御するため、ユーザはパスワードやその他の認証メカニズムを使用して機器を直接認証する必要はない。

5 民生用 IoT のためのサイバーセキュリティ規定

5.1 汎用のデフォルトパスワードを使用しない

規定 5.1-1 パスワードが使用され、工場出荷時のデフォルト以外の状態にある場合、すべての民生用 IoT 機器のパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。

注： 認証を行うために使用されるメカニズムは多数あり、 パスワードはユーザを機器に認証するための唯一のメカニズムではない。しかし、パスワードを使用する場合は、NIST Special Publication 800-63B [i.3] に準じて、パスワードのベストプラクティスに従うことが推奨される。一般に、マシン間認証にパスワードを使用することは適切ではない。

多くの民生用 IoT 機器は、ユーザインタフェースからネットワークプロトコルまで、汎用のデフォルトのユーザ名とパスワード（”admin、admin”など）で販売されている。汎用のデフォルト値の継続的な使用は、IoT における多くのセキュリティ問題の原因となっており [i.17]、この慣習はやめる必要がある。上記の規定は、機器ごとに固有のプリインストールされたパスワードを使用することによって、及び／又は初期化の一部としてベストプラクティスに従っているパスワードを選択するようにユーザに要求することによって、又はパスワードを使用しない他の方法によって達成することができる。

例 1 ： 初期化中に、機器はモバイルアプリケーションなどの関連サービスを介して、ユーザを機器に認証するために使用する証明書を生成する。

セキュリティを強化するために、パスワードとワンタイムパスワード（OTP）手順を使用するなどの多要素認証を使用することで、機器又は関連サービスをより良く保護することができる。機器のセキュリティは、固有で変更不可能な ID を持つことで、さらに強化することができる。

規定 5.1-2 プリインストールされた、機器毎に固有のパスワードを使用する場合、パスワードは機器のクラス又はタイプに対する自動化された攻撃のリスクを軽減するメカニズムで生成されなければならない。

例 2： プリインストールされたパスワードが、十分にランダム化されている。

逆の例として、増加するカウンタによるパスワード（"password1"、"password2"など）は、容易に推測可能である。また、明らかに MAC アドレスや Wi-Fi® SSID などの（無線又はネットワーク内で送信される）公開情報に関連するパスワードを使用すると、自動化された手段を使用して、パスワードを検索することが可能となる。

規定 5.1-3 機器に対してユーザを認証するために使用される認証メカニズムは、技術、リスク、及び用途の特性に適したベストプラクティスの暗号技術を使用していなければならない。

Provision 5.1-4 Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.

EXAMPLE 3: For biometric authentication values the device manufacturer allows this change in authentication value through retraining against a new biometric.
EXAMPLE 4: A parent in a household creates an account on the device for their child and selects and manages the PIN or password that the child uses. The parent is an administrator on the device and can restrict the child from changing the PIN or password.
EXAMPLE 5: To make it simple for the user to change a password, the manufacturer designs the password change process in a way that it requires a minimal number of steps. The manufacturer explains the process in a user manual and in a video tutorial.

An authentication mechanism used for authenticating users, whether it be a fingerprint, password or other token, needs to have its value changeable. This is easier when this mechanism is part of the normal usage flow of the device.

Provision 5.1-5 When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.

EXAMPLE 6: A device has a limitation on the number of authentication attempts within a certain time interval. It also uses increasing time intervals between attempts.

EXAMPLE 7: The client application is able to lock an account or to delay additional authentication attempts after a limited number of failed authentication attempts.

This provision addresses attacks that perform "credential stuffing" or exhaust an entire key-space. It is important that these types of attacks are detected by the consumer IoT device and defended against, whilst guarding against a related threat of "resource exhaustion" and denial of service attacks.

5.2 Implement a means to manage reports of vulnerabilities

Provision 5.2-1 The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:

- contact information for the reporting of issues; and
- information on timelines for:
  1) initial acknowledgement of receipt; and
  2) status updates until the resolution of the reported issues.

A vulnerability disclosure policy clearly specifies the process through which security researchers and others are able to report issues. Such policy can be updated as necessary to further ensure transparency and clarity in the dealings of the manufacturer with security researchers, and vice versa.

Coordinated Vulnerability Disclosure (CVD) is a set of processes for dealing with disclosures about potential security vulnerabilities and to support the remediation of these vulnerabilities. CVD is standardized by the International Organization for Standardization (ISO) in the ISO/IEC 29147 [i.4] on vulnerability disclosure and has been proven to be successful in some large software companies around the world.

In the IoT industry, CVD is currently not well-established [i.16] as some companies are reticent about dealing with security researchers. Here, CVD provides companies a framework to manage this process. This gives security researchers an avenue to inform companies of security issues, puts companies ahead of the threat of malicious exploitation and gives companies an opportunity to respond to and resolve vulnerabilities in advance of a public disclosure.

Provision 5.2-2 Disclosed vulnerabilities should be acted on in a timely manner.

A "timely manner" for acting on vulnerabilities varies considerably and is incident-specific; however, conventionally, the vulnerability process is completed within 90 days for a software solution, including availability of patches and notification of the issue. A hardware fix can take considerably longer to address than a software fix. Additionally, a fix that has to be deployed to devices can take time to roll out compared with a server software fix.

規定 5.1-4 ユーザが機器に対して認証できる場合、機器は、使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。

例 3： 生体認証値の場合、機器の製造業者は、新しい生体認証に対する再トレーニングを通じて、認証値を変更することを許可する。

例 4： 家庭内の保護者が、機器で子供のためのアカウントを作成し、子供が使用する PIN 及びパスワードを選択し、管理する。 保護者は機器の管理者であり、子供が PIN 又はパスワードを変更することを制限できる。

例 5： ユーザが簡単にパスワードを変更できるように、製造業者は必要な手順が最小限になるようにパスワード変更プロセスを設計する。製造業者は、ユーザマニュアルとチュートリアル動画でその手順を説明する。

ユーザの認証に使用される認証メカニズムは、指紋、パスワード、又はその他のトークンであるかどうかにかかわらず、その値を変更できる必要がある。このメカニズムが機器の通常の使用フローの一部であれば、これは容易である。

規定 5.1-5 機器が制約のある機器ではない場合、ネットワークインタフェースを介したブルートフォース攻撃を実行不可能にするメカニズムを持たなければならない。

例 6： 機器には、特定の時間間隔内での認証試行回数に制限がある。また、試行間の時間間隔を長くしている。

例 7： クライアントアプリケーションは、制限された回数の認証の試行に失敗した後、アカウントをロックしたり、追加の認証試行を遅らせたりすることができる。

この規定は、“クレデンシャルスタッフィング攻撃”や鍵空間全体を使い果たしたりする攻撃に対処している。これらの種類の攻撃が、民生用 IoT 機器で検出され、防御されると同時に、“リソースの枯渇”や DoS 攻撃に関連する脅威から保護されることが重要である。

5.2 脆弱性の報告を管理するための手段を導入する

規定 5.2-1 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない：

- 問題を報告するための連絡先情報；
- 以下のタイムラインに関する情報：
  1) 最初の受領確認；
  2) 報告された問題が解決されるまでの状況の更新。

情報開示ポリシーは、セキュリティ研究者やその他の人々が問題を報告できるプロセスをはっきりと明記する。このようなポリシーは、製造業者とセキュリティ研究者との関係において透明性と明瞭性を一層確実にするために、必要に応じてアップデートすることができ、またその逆も可能である。

協調的脆弱性開示（CVD）は潜在的なセキュリティの脆弱性に関する開示に対処し、これらの脆弱性の是正を支援するための一連のプロセスである。CVD は国際標準化機構（ISO）によって脆弱性の開示に関する ISO/IEC 29147 [i.4] で標準化されており、世界中のいくつかの大規模ソフトウェア企業で成功が実証されている。

IoT 業界では、セキュリティ研究者との関係に消極的な企業もあるため、現在 CVD は十分に確立されていない [i.16] 。ここで、CVD はこのプロセスを管理するためのフレームワークを提供する。これにより、セキュリティ研究者は企業にセキュリティ問題を知らせることができ、企業は悪意のある悪用の脅威を先取りし、脆弱性が公開される前に対応して解決する機会が与えられる。

規定 5.2-2 開示された脆弱性には、タイムリーな方法で対処することが望ましい。

脆弱性に対処するための「タイムリーな方法」は、かなり多様であり、インシデントに固有である。しかし、従来、脆弱性の対処プロセスは、パッチの利用可能性と問題の通知を含め、ソフトウェアソリューションの場合は 90 日以内に完了することになっている。ハードウェアの修正は、ソフトウェアの修正に比べ、かなり長い時間を要することがある。さらに、機器に展開する必要がある修正は、サーバのソフトウェア修正と比較して、展開に時間がかかる場合がある。

Provision 5.2-3 Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.

NOTE 1: Manufacturers are expected to exercise due care for all software and hardware components used in the product, this includes due care related to the selected third parties that provide associated services to support the functions of the product.

Software solutions often contain open source and third party software components. Creating and maintaining list of all software components and their sub-components is a pre-requisite to be able to monitor for product vulnerabilities. Various tools exist to scan source code and binaries and build a so-called Software Bill of Materials (SBOM), which identifies third party components and the versions used in the product. This information is then used to monitor for the associated security and licensing risks of each identified software component.

Vulnerabilities are expected to be reported directly to the affected stakeholders in the first instance. If that is not possible, vulnerabilities can be reported to national authorities. Manufacturers are also encouraged to share information with competent industry bodies, such as the GSMA [i.21] and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation [i.22] which references ISO/IEC 29147 [i.4].

This is expected to be performed for devices within their defined support period. However, manufacturers can continue this outside that period and release security updates to rectify vulnerabilities.

Manufacturers that provide IoT products have a duty of care to consumers and third parties who can be harmed by their failure to have a CVD programme in place. Additionally, companies that share this information through industry bodies can assist others who can be suffering from the same problem.

Disclosures can comprise different approaches depending on the circumstances:

- Vulnerabilities related to single products or services: the problem is expected to be reported directly to the affected stakeholder (usually the device manufacturer, IoT service provider or mobile application developer). The source of these reports can be security researchers or industry peers.

- Systemic vulnerabilities: a stakeholder, such as a device manufacturer, can discover a problem that is potentially systemic. Whilst fixing it in the device manufacturer's own product is crucial, there is significant benefit to industry and consumers from sharing this information. Similarly, security researchers can also seek to report such systemic vulnerabilities. For systemic vulnerabilities, a relevant competent industry body can coordinate a wider scale response.

NOTE 2: The Common Vulnerability Reporting Framework (CVRF) [i.5] can also be useful to exchange information on security vulnerabilities.

Cyber security threat information sharing can support organizations in developing and producing secure products according to ETSI TR 103 331 [i.6].

5.3 Keep software updated

Developing and deploying security updates in a timely manner is one of the most important actions a manufacturer can take to protect its customers and the wider technical ecosystem. It is good practice that all software is kept updated and well maintained.

Each provision from 5.3-3 to 5.3-12 is dependent upon an update mechanism being implemented, as per provision 5.3-1 or 5.3-2.

Provision 5.3-1 All software components in consumer IoT devices should be securely updateable.

NOTE 1: Managing software updates successfully generally relies on communication of version information for software components between the device and the manufacturer.

Not all software on a device will be updateable.

EXAMPLE 1: The first stage boot loader on a device is written once to device storage and from then on is immutable.

EXAMPLE 2: On devices with several microcontrollers (e.g. one for communication and one for the application) some of them might not be updateable.

規定 5.2-3 製造業者は、定められたサポート期間中、販売、製造された製品及び運用するサービス内のセキュリティ脆弱性を継続的に監視し、特定し、修正することが望ましい。

注 1： 製造業者製造業者は、製品に使用されるすべてのソフトウェア及びハードウェアの構成要素に対して当然払うべき注意を払うことが期待されており、これには製品の機能をサポートするために関連サービスを提供する選択されたサードパーティに関する当然払うべき注意も含まれる。

ソフトウェアソリューションには、多くの場合、オープンソース及びサードパーティのソフトウェアコンポーネントが含まれている。すべてのソフトウェアコンポーネントとそのサブコンポーネントのリストを作成して管理する事は、製品の脆弱性を監視できるための前提条件である。ソースコードとバイナリをスキャンし、製品で使用されているサードパーティのコンポーネントとバージョンを識別する、いわゆるソフトウェア部品表 (SBOM) を作成するためのさまざまなツールがある。この情報は、識別された各ソフトウェアコンポーネントに関連するセキュリティ及びライセンスのリスクを監視するために使用される。

脆弱性は、最初に影響を受けるステークホルダーに直接報告されることが期待される。それが不可能な場合、脆弱性は国の当局に報告することができる。また製造業者は、GSMA [i.21] や IoT Security Foundation などの所轄の業界団体と情報を共有することも推奨される。ISO/IEC 29147 [i.4]を参照している IoT Security Foundation [i.22] から、Guidance on Coordinated Vulnerability Disclosure（協調的脆弱性開示に関するガイダンス）が入手可能である。

これは、定められたサポート期間内の機器に対して行われることが期待されている。ただし、製造業者はその期間外でもこれを継続し、脆弱性を修正するためのセキュリティアップデートをリリースすることができる。

IoT 製品を提供する製造業者は、CVD プログラムを導入していないことで損害を受ける可能性のある消費者や第三者に対して注意義務を負っている。さらに、業界団体を通じてこの情報を共有する企業は、同じ問題に苦しむ可能性のある他の企業を支援することができる。

開示は、状況に応じて様々なアプローチで構成できる：

- 単一の製品又はサービスに関連する脆弱性：問題は、影響を受けるステークホルダー（通常はデバイスメーカー、IoT サービスプロバイダ、モバイルアプリケーション開発者）に直接報告されることが期待される。これらの報告元は、セキュリティ研究者や業界の同業者である可能性がある。
- システム的な脆弱性：機器製造業者などのステークホルダーは、システム的な可能性を持つ問題を発見することができる。機器製造業者の製品で修正することが重要だが、この情報を共有することは、業界と消費者に大きな恩恵をもたらす。同様に、セキュリティ研究者も、そのようなシステム的な脆弱性の報告しようとすることができる。システム的な脆弱性については、関連する管轄の業界団体がより大規模な対応を調整することができる。

注 2： 脆弱性情報の標準記述形式（CVRF） [i.5] も、セキュリティ脆弱性に関する情報交換に有用である。

サイバーセキュリティ脅威情報の共有は、ETSI TR 103 331 [i.6]に従って、セキュアな製品を開発・生産する組織を支援することができる。

5.3 ソフトウェアを最新の状態に保つ

セキュリティアップデートをタイムリーな方法で開発して展開することは、製造業者が顧客及び、より広範な技術エコシステムを保護するために実行できる最も重要な行動の一つである。すべてのソフトウェアがアップデートされ、適切に維持されていることは、グッドプラクティスである。

5.3-3 から 5.3-12 までの各規定は、規定 5.3-1 又は 5.3-2 に従って実装されるアップデートメカニズムに依存する。

規定 5.3-1 民生用 IoT 機器に含まれるすべてのソフトウェアコンポーネントは、セキュアにアップデート可能であることが望ましい。

注 1： ソフトウェアのアップデートを正常に管理することは、一般に、機器と製造業者間のソフトウェアコンポーネントのバージョン情報の通信に依存する。

機器上のすべてのソフトウェアがアップデート可能となるわけではない。

例 1： 機器上の第一段階のブートローダは、機器のストレージ上に一度だけ書き込まれ、それ以降は不変である。

例 2： 複数のマイクロコントローラ（例えば 1 つは通信用、もう 1 つはアプリケーション用）を搭載した機器では、その一部がアップデートできない場合がある。

Provision 5.3-2 When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.

NOTE 2: There are cases where provision 5.3-1 applies even where 5.3-2 does not.

"Securely updateable" and "secure installation" means that there are adequate measures to prevent an attacker misusing the update mechanism.

EXAMPLE 3: Measures can include the use of authentic software update servers, integrity protected communications channels, verifying the authenticity and integrity of software updates. It is recognized that there are great variances in software update mechanisms and what constitutes "installation".

EXAMPLE 4: An anti-rollback policy based on version checking can be used to prevent downgrade attacks.

Update mechanisms can range from the device downloading the update directly from a remote server, transmitted from a mobile application or transferred over a USB or other physical interface. If an attacker compromises this mechanism, it allows for a malicious version of the software to be installed on the device.

Provision 5.3-3 An update shall be simple for the user to apply.

The degree of simplicity depends on the design and intended usage of the device. An update that is simple to apply will be automatically applied, initiated using an associated service (such as a mobile application), or via a web interface on the device. If an update is difficult to apply, then that increases the chance that a user will repeatedly defer updating the device, leaving it in a vulnerable state.

Provision 5.3-4 Automatic mechanisms should be used for software updates.

If an automatic update fails, then a user can, in some circumstances, no longer be able to use a device. Detection mechanisms such as watchdogs and the use of dual-bank flash or recovery partitions can ensure that the device returns to either a known good version or the factory state.

Security updates can be provided for devices in a preventative manner, as part of automatic updates, which can remove security vulnerabilities before they are exploited. Managing this can be complex, especially if there are parallel associated service updates, device updates and other service updates to deal with. Therefore, a clear management and deployment plan is beneficial to the manufacturer, as is transparency to consumers about the current state of update support.

In many cases, publishing software updates involves multiple dependencies on other organizations such as manufacturers that produce sub-components; however, this is not a reason to withhold updates. It can be useful for the manufacturer to consider the entire software supply chain in the development and deployment of security updates.

It is often advisable not to bundle security updates with more complex software updates, such as feature updates. A feature update that introduces new functionality can trigger additional requirements and delay delivery of the update to devices.

EXAMPLE 5: Under the EU Product Legislation, a feature update could change the intended use of a device and thus turn it into a new product, requiring a new conformity assessment to be conducted. However, a software update with limited impact could be considered a maintenance update which would not require a new conformity assessment. More information on the impact of software updates in the context of the EU Product Legislation can be found in the Blue Guide [i.13].

Provision 5.3-5 The device should check after initialization, and then periodically, whether security updates are available.

EXAMPLE 6: The user could be shown the existence of updates via the interface with which the device is initialized.

EXAMPLE 7: A device checks for available updates daily at a randomized time.

For some products, it can be more appropriate for the associated service, rather than the device, to perform such checks.

Provision 5.3-6 If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.

規定 5.3-2 制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。

注 2： 規定 5.3-2 が適用されない場合でも、規定 5.3-1 が適用される場合がある。

「セキュアにアップデート可能」及び「セキュアにインストールする」とは、攻撃者がアップデートメカニズムを悪用することを防止するための適切な対策があることを意味する。

例 3： 対策には、信頼のおけるソフトウェアアップデートサーバの使用、完全性が保護された通信チャネル、ソフトウェアアップデートの真正性と完全性の検証を含めることができる。ソフトウェアアップデートのメカニズムや「インストール」を構成するものには、大きな差異があることが認識されている。

例 4： バージョンチェックに基づくアンチロールバックポリシーは、ダウングレード攻撃を防止するために使用することができる。

アップデートメカニズムには、機器がリモートサーバから直接アップデートをダウンロードするもの、モバイルアプリケーションから転送されるもの、USB 又はその他の物理インタフェースで転送されるものがある。攻撃者がこのメカニズムを侵害した場合、悪意のあるバージョンのソフトウェアを機器にインストールすることが可能となる。

規定 5.3-3 アップデートは、ユーザが簡単に適用できるものでなければならない。

簡単であることの程度は、機器の設計と意図された使用方法によって異なる。簡単に適用できるアップデートは、自動的に適用されるか、関連サービス（モバイルアプリケーションなど）を使用して開始されるか、又は機器のウェブインタフェースを介して適用される。アップデートの適用が困難な場合、ユーザが機器のアップデートを繰り返し延期し、機器が脆弱な状態になる可能性が高くなる。

規定 5.3-4 ソフトウェアのアップデートには、自動化メカニズムを使用しなければならない。

自動アップデートに失敗すると、状況によっては、ユーザは機器を使用できなくなる。ウォッチドッグやデュアルバンクフラッシュ又はリカバリパーティションの使用などの検出メカニズムによって、機器を既知の正常なバージョン又は工場出荷時の状態に戻す事を確実にできる。

セキュリティアップデートは、自動アップデートの一部として、悪用される前にセキュリティ脆弱性を除去することができる予防的な方法で機器に提供される。特に関連サービスのアップデート、機器のアップデート、その他のサービスのアップデートが並行して行われる場合、その管理は複雑になる可能性がある。したがって、明確な管理と展開の計画は製造業者にとって有益であり、アップデートサポートの現状に関する消費者への透明性も同様に有益である。

多くの場合、ソフトウェアアップデートの公開は、サブコンポーネントを製造する製造業者など、他の組織への複数の依存関係が伴う。ただし、これはアップデートを保留する理由にはならない。製造業者がセキュリティアップデートを開発、展開する際に、ソフトウェアのサプライチェーン全体を考慮することは有益である。

セキュリティアップデートを、機能アップデートなどの、より複雑なソフトウェアアップデートと一緒にしないことが望ましい場合が多い。新しい機能を導入する機能アップデートは、追加の要件をもたらし、機器へのアップデートの配信を遅らせる可能性がある。

例 5： EU 製品法（EU Product Legislation）では、機能アップデートは機器の使用目的を変更する可能性があるため、新製品とみなされ、新たな適合性評価の実施が必要となる。しかし、影響が限定的なソフトウェアアップデートは、新たな適合性評価を必要としないメンテナンスアップデートとみなされる可能性がある、EU 製品法の文脈におけるソフトウェアアップデートの影響に関する詳細は、Blue Guide [i.13]に記載されている。

規定 5.3-5 機器は初期化後、定期的にセキュリティアップデートが利用可能かどうかを確認することが望ましい。

例 6：機器が初期化されるインタフェースを介して、ユーザにアップデートの存在を示すことができる。

例 7：機器は、毎日ランダムな時間に利用可能なアップデートを確認する。

製品によっては、機器ではなく、関連サービスがこのような確認を行うことがより適切である場合がある。

規定 5.3-6： 機器が自動アップデート及び／又はアップデート通知をサポートする場合、これらは初期化された状態で有効であり、ユーザがセキュリティアップデート及び／又はアップデート通知のインストールを有効、無効、又は延期できるように設定可能であることが望ましい。

It is important from a consumer rights and ownership perspective that the user is in control of whether or not they receive updates. There are good reasons why a user may choose not to update, including security. In addition, if an update is deployed and subsequently found to cause issues, manufacturers can ask users to not upgrade their software in order that those devices are not affected.

Provision 5.3-7 The device shall use best practice cryptography to facilitate secure update mechanisms.

Provision 5.3-8 Security updates shall be timely.

"Timely" in the context of security updates can vary, depending on the particular issue and fix, as well as other factors such as the ability to reach a device or constrained device considerations. It is important that a security update that fixes a critical vulnerability (i.e. one with potentially adverse effects of a large scale) is handled with appropriate priority by the manufacturer. Due to the complex structure of modern software and the ubiquity of communication platforms, multiple stakeholders can be involved in a security update.

EXAMPLE 8: A particular software update involves a third party vendor of software libraries, an IoT device manufacturer, and an IoT service platform operator. Collaboration between these stakeholders ensures appropriate timeliness of the software update.

Provision 5.3-9 The device should verify the authenticity and integrity of software updates.

A common approach for confirming that an update is valid is to verify its integrity and authenticity. This can be done on the device; however, constrained devices can have power limitations that make performing cryptographic operations costly. In such cases, verification can be performed by another device that is trusted to perform this verification. The verified update would then be sent over a secure channel to the device. Performing verification of updates at a hub and then on the device, can reduce the risk of compromise.

It is good practice for a device to act upon the detection of an invalid and potentially malicious update. Beyond rejecting the update, and without limitation, it can report the incident to an appropriate service and/or inform the user. In addition, mitigating controls can be put in place to prevent an attacker from bypassing or misusing an update mechanism. Giving the attacker as little information as possible as part of the update mechanism reduces their ability to exploit it.

EXAMPLE 9: When a device detects that an update could not be delivered or applied successfully (by failing integrity or authentication checks), the device can mitigate information leakage by not providing any information about the failure to the initiator of the update process. However, the device can generate a log entry and deliver notification of the log entry to a trusted peer (e.g. a device administrator) over a secure channel, so that the occurrence of the incident is known and the owner or administrator of the device can make an appropriate response.

Provision 5.3-10 Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

NOTE 3: Valid trust relationships include: authenticated communication channels, presence on a network that requires the device to possess a critical security parameter or password to join, digital signature based verification of the update, or confirmation by the user.

NOTE 4: The validation of the trust relationship is essential to ensure that a non-authorized entity (e.g. device management platform or device) cannot install malicious code.

Provision 5.3-11 The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.

EXAMPLE 10: The manufacturer informs the user that an update is required via a notification on the user interface or via an email.

Provision 5.3-12 The device should notify the user when the application of a software update will disrupt the basic functioning of the device.

NOTE 5: This is not necessary if a notification is made by an associated service.

This notification can include extra detail, such as the approximate expected duration for which the device will be offline.

EXAMPLE 11: A notification includes information about the urgency and approximate expected duration of downtime.

消費者の権利と所有権の観点から、ユーザがアップデートを受け入れるかどうかの主導権を握っていることが重要である。ユーザがアップデートしないことを選択するのには、セキュリティを含む正当な理由がある。また、アップデートが展開され、その後問題が発生することが判明した場合、製造業者は、それらの機器が影響を受けないようにするために、ソフトウェアのアップグレードを行わないようユーザに要請することができる。

規定 5.3-7 機器は、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。

規定 5.3-8 セキュリティアップデートは、適時でなければならない。

セキュリティアップデートの文脈における「適時」は、特定の問題や修正に加え、機器に到達する能力や制約のある機器の考慮事項などの他の要因によって異なる場合がある。重要な脆弱性（大規模な悪影響を及ぼす可能性のある脆弱性）を修正するセキュリティアップデートは、製造業者が適切な優先順位で処理することが重要である。現代のソフトウェアは複雑な構造を持ち、通信プラットフォームが偏在しているため、セキュリティアップデートに複数のステークホルダーが関与する可能性がある。

例 8： ある特定のソフトウェアアップデートには、ソフトウェアライブラリのサードパーティベンダ、IoT 機器製造業者、IoT サービスプラットフォーム運用者が関与している。これらのステークホルダー間の協力により、ソフトウェアアップデートの適時性が確実となる。

規定 5.3-9 機器は、ソフトウェアアップデートの真正性と完全性を検証することが望ましい。

アップデートが有効であることを確認するための一般的なアプローチは、その完全性と真正性を検証することである。これは機器上で実行することができるが、制約のある機器では、電力の制限によって暗号化操作の実行にコストがかかる場合がある。このような場合、信頼されている別の機器で検証を実施することができる。検証されたアップデートは、その後、セキュアなチャネルを介して機器に送信される。アップデートの検証をハブで実施し、その後、機器上で実施することで、侵害のリスクを低減することができる。

無効及び悪意のある可能性のあるアップデートを検出した時点で対処することが、機器にとってのベストプラクティスである。機器は、アップデートを拒否するだけでなく、制限なく、適切なサービスにインシデントを報告すること及び／又はユーザに通知することもできる。さらに、攻撃者がアップデートメカニズムを回避したり悪用したりするのを防ぐために、緩和策を講じることもできる。アップデートメカニズムの一部として、攻撃者にできるだけ少ない情報を与えることで、攻撃者がそれを悪用する能力を低下させることができる。

例 9： 機器が、アップデートを正常に配信又は適用できなかったことを検出（完全性又は認証のチェックに失敗）した場合、機器は失敗に関するいかなる情報もアップデートプロセスの開始プログラムに提供しないことによって、情報漏洩を軽減することができる。ただし、機器は、インシデントの発生を把握し、機器の所有者又は管理者が適切な対応を取れるようにすることを可能にするために、ログエントリを生成し、セキュアなチャネルを介してそのログエントリの通知を信頼できるピア（機器管理者など）に配信することができる。

規定 5.3-10 アップデートがネットワークインタフェースを介して配信される場合、機器は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。

注 3： 有効な信頼関係には、認証された通信チャネル、参加するために重要なセキュリティパラメータ又はパスワードを所有することを機器に要求するネットワーク上の存在、アップデートのデジタル署名に基づく検証、又はユーザによる確認が含まれる。

注 4： 信頼関係の検証は、権限のないエンティティ（機器管理プラットフォーム又は機器など）が悪意あるコードをインストールできないようにするために不可欠である。

規定 5.3-11 製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知することが望ましい。

例 10： 製造業者は、ユーザインタフェース上の通知又は電子メールを介して、アップデートが必要であることをユーザに通知する。

規定.3-12 ソフトウェアアップデートの適用により、機器の基本的な機能が阻害される場合には、機器からユーザに通知することが望ましい。

注 5： 関連サービスによって通知が行われる場合には、この必要はない。

この通知には、機器がオフラインになるおおよその予想期間など、追加の詳細を含めることができる。

例 11： 通知には、緊急性とダウンタイムのおおよその予想期間についての情報が含まれる。

It can be critical for users that a device continues to operate during an update. This is why the provision above recommends to notify the user when an update will disrupt functionality where possible. Particularly, devices that fulfil a safety-relevant function are expected not to turn completely off in the case of an update; some minimal system functional capability is expected. Disruption to functionality can become a critical safety issue for some types of devices and systems if not considered or managed correctly.

EXAMPLE 12: During an update, a watch will continue to display the time, a home thermostat will continue to maintain a reasonable temperature and a Smart Lock will continue to lock and unlock a door.

Provision 5.3-13 The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.

When purchasing a product, the consumer expects this period of software update support to be made clear.

Provision 5.3-14 For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.

Provision 5.3-15 For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.

There are some situations where devices cannot be patched. For constrained devices a replacement plan needs to be in place and be clearly communicated to the consumer. This plan would typically detail a schedule for when technologies will need to be replaced and, where applicable, when support for hardware and software ends.

Provision 5.3-16 The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.

This is often performed by communicating with a device over a logical interface, however it can also be part of a UI.

EXAMPLE 13: A device has a HTTP (or HTTPS when appropriate) API that reports the model designation (after user authentication).

Knowledge of the specific designation of the device is often required to check the defined support period of software updates or the availability of software updates.

5.4 Securely store sensitive security parameters

Provision 5.4-1 Sensitive security parameters in persistent storage shall be stored securely by the device.

Secure storage mechanisms can be used to secure sensitive security parameters. Appropriate mechanisms include those provided by a Trusted Execution Environment (TEE), encrypted storage associated with the hardware, Secure Elements (SE) or Dedicated Security Components (DSC), and processing capabilities of software running on a UICC, according to ETSI TR 121 905 [i.29], ETSI TS 102 221 [i.25]/embedded UICC according to GSMA SGP.22 Technical Specification v2.2.1 [i.26].

NOTE: This provision applies to persistent storage, but manufacturers can also implement similar approaches for sensitive security parameters in memory.

EXAMPLE 1: The root keys involved in authorization and access to licensed radio frequencies (e.g. LTE-m cellular access) are stored in a UICC.

EXAMPLE 2: A remote controlled door-lock using a Trusted Execution Environment (TEE) to store and access the sensitive security parameters.

EXAMPLE 3: A wireless thermostat stores the credentials for the wireless network in a tamper protected microcontroller rather than in external flash storage.

Provision 5.4-2 Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.

EXAMPLE 4: A master key used for network access that is unique to the device is stored in UICC which is compliant to relevant ETSI standards (see, for example ETSI TS 102 221 [i.25]).

ユーザにとって、アップデート中も機器が動作し続けることは非常に重要である。このため、上記の規定では、アップデートによって機能が中断される場合は、可能な限りユーザに通知することを推奨している。特に、セーフティ関連の機能を果たす機器は、アップデートの際に完全に電源が切れることはなく、最低限のシステム機能が期待される。機能の中断は、正しく考慮又は管理されていない場合、ある種の機器やシステムにとって重大なセーフティ上の問題となる可能性がある。

例 12： アップデート中、時計は時刻を表示し続け、サーモスタットは適切な温度を維持し続け、スマートロックはドアのロック／アンロックをし続けることができる。

規定 5.3-13 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。

製品を購入する際、消費者はこのソフトウェアアップデートのサポート期間が明確となっていることを求めている。

規定 5.3-14 ソフトウェアアップデートできない制約のある機器については、製造業者は、ソフトウェアアップデートができない根拠、ハードウェア交換のサポート期間と方法、及び定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表することが望ましい。

規定 5.3-15 ソフトウェアアップデートできない制約のある機器については、製品は分離可能で、ハードウェアは交換可能であることが望ましい。

機器にパッチを適用できない状況もある。制約のある機器については、交換の計画を定め、消費者に明確に伝える必要がある。この計画には、通常、技術のリプレースが必要となる時期、及び適用可能な場合には、ハードウェアとソフトウェアのサポートが終了する時期についてスケジュールを詳述する。

規定 5.3-16 民生用 IoT 機器のモデル名称は、機器上のラベル又は物理的インタフェースを介して、明確に認識可能でなければならない。

これは多くの場合、論理インタフェースを介して機器と通信することによって実施されるが、ユーザインタフェース（UI）の一部であることも可能である。

例 13： 機器には（ユーザ認証後に）モデル名称を報告する HTTP（又は適切であれば HTTPS）API がある。

ソフトウェアアップデートの定められたサポート期間又はソフトウェアアップデートの可用性を確認するために、機器の具体的な名称に関する知識がしばしば必要となる。

5.4 機密セキュリティパラメータをセキュアに保存する

規定 5.4-1 永続ストレージにある機密セキュリティパラメータは、機器によってセキュアに保存されなければならない。

機密セキュリティパラメータをセキュアにするために、セキュアなストレージ・メカニズムを使用することができる。適切なメカニズムには、ETSI TR 121 905 [i.29], ETSI TS 102 221 [i.25]による信頼できる実行環境（TEE）、ハードウェアに関連付けられた暗号化されたストレージ、セキュアエレメント (SE) 又は専用のセキュリティ・コンポーネント (DSC)、及び GSMA SGP.22 Technical Specification v2.2.1 [i.26]による UICC で実行されるソフトウェアの処理機能が含まれる。

注： この規定は永続ストレージに適用されるが、製造業者はメモリ内の機密セキュリティパラメータに同様のアプローチを実装することも可能である。

例 1： 認可された無線周波数（例：LTE-m 携帯アクセス）への認可及びアクセスに関連するルートキーは、UICC に保存される。

例 2： 信頼できる実行環境（TEE）を使用して機密セキュリティパラメータを保存し、アクセスするリモート制御ドアロック。

例 3： ワイヤレスサーモスタットは、無線ネットワークの認証情報を、外部のフラッシュストレージではなく、改ざん防止されたマイクロコントローラに保存する。

規定 5.4-2 ハードコードされた機器ごとの固有の ID がセキュリティ目的で機器で使用される場合、物理的、電気的、又はソフトウェアなどの手段による改ざんに耐えられるように実装しなければならない。

例 4： 機器に固有のネットワークアクセスに使用されるマスターキーは、関連する ETSI 規格（例えば、 ETSI TS 102 221 [i.25])に準拠した UICC に保存される。

Provision 5.4-3 Hard-coded critical security parameters in device software source code shall not be used.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. These credentials can also be API keys that allow usage of security-sensitive functions in a remote service, or private keys used in the security of protocols that the device uses to communicate. Such credentials will often be found within source-code, which is well-known bad practice. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken.

Provision 5.4-4 Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

EXAMPLE 5: A different symmetric key is deployed on every device of the same product class for generating and verifying message authentication codes for software updates.

EXAMPLE 6: The device uses the manufacturer's public key to verify a software update. This is not a critical security parameter and does not need to be unique per device.

Provisioning a device with unique critical security parameters helps to protect the integrity and authenticity of software updates as well as the communication of the device with associated services. If global critical security parameters are used, their disclosure can enable wide-scale attacks on other IoT devices such as to enable the creation of botnets.

5.5 Communicate securely

Provision 5.5-1 The consumer IoT device shall use best practice cryptography to communicate securely.

Appropriateness of security controls and the use of best practice cryptography is dependent on many factors including the usage context. As security is ever-evolving it is difficult to give prescriptive advice about cryptography or other security measures without the risk of such advice quickly becoming obsolete.

Provision 5.5-2 The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.

Reviews and evaluations can involve an independent internal or external entity.

EXAMPLE 1: Distributed software libraries within the development and test community, certified software modules, and hardware equipment crypto-service providers (such as the Secure Element and Trust Execution Environment) are all reviewed or evaluated.

Provision 5.5-3 Cryptographic algorithms and primitives should be updateable.

NOTE 1: This is also known as "cryptoagility".

For devices that cannot be updated, it is important that the intended lifetime of the device does not exceed the recommended usage lifetime of cryptographic algorithms used by the device (including key sizes).

Provision 5.5-4 Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.

NOTE 2: Functionality can vary significantly on the use case and can encompass a range of things, including access to personal data and device actuators.

There are devices that provide public, open data for example in the Web of Things [i.18]. These devices are accessible without authentication to provide open access to all.

The device can be compromised via vulnerabilities in network services. A suitable authentication mechanism can protect against unauthorized access and can contribute to defence-in-depth in the device.

Provision 5.5-5 Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.

NOTE 3: Protocols that are an exception include ARP, DHCP, DNS, ICMP, and NTP.

規定 5.4-3 機器のソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータを使用してはならない。

機器やアプリケーションのリバースエンジニアリングによって、ソフトウェアにハードコードされたユーザ名やパスワードなどの認証情報を容易に発見することができる。これらの認証情報は、リモートサービスのセキュリティの影響を受ける機能の使用を許可する API 鍵、又は機器が通信に使用するプロトコルのセキュリティに使用される秘密鍵である可能性もある。このような認証情報は、しばしばソースコード内で見つかることがあるが、これはよく知られたバッドプラクティスである。このようなハードコードされた情報を隠したり暗号化したりするために使用される単純な難読化手法は、簡単に破られる可能性がある。

規定 5.4-4 ソフトウェアアップデートの完全性及び真正性チェック、及び機器のソフトウェアにおける関連サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、機器のクラスに対する自動化された攻撃のリスクを低減するメカニズムで生成されるものとしなければならない。

例 5： ソフトウェアアップデートのためのメッセージ認証コードを生成し検証するために、同じ製品クラスのすべての機器に異なる対称鍵が配備される。

例 6： 機器は、ソフトウェアアップデートを検証するために製造業者の公開鍵を使用する。これは重要なセキュリティパラメータではないので、機器ごとに固有である必要はない。

固有の重要なセキュリティパラメータを使用して機器をプロビジョニングすると、ソフトウェアアップデートの完全性と真正性、及び機器と関連サービスの通信の保護に役立つ。グローバルな重要なセキュリティパラメータが使用されている場合、その開示により、ボットネットの作成を可能にするなど、他の IoT 機器に対する広範な攻撃が可能となる。

5.5 セキュアに通信する

規定 5.5-1 民生用 IoT 機器は、ベストプラクティスの暗号技術を使用してセキュアに通信しなければならない。

セキュリティ管理策及びベストプラクティスの暗号技術の使用の妥当性は、使用状況を含む多くの要因に依存する。セキュリティは絶えず進化しているため、暗号技術やその他のセキュリティ対策についての規範的なアドバイスの提供は、そのアドバイスがすぐに時代遅れとなるというリスクを冒さずに行うことは困難である。

規定 5.5-2 民生用 IoT 機器は、ネットワーク及びセキュリティ機能、特に暗号技術の分野においてレビュー又は評価された実装を使用することが望ましい。

レビュー及び評価には、独立した内部又は外部のエンティティが関与することができる。

例 1： 開発及びテストコミュニティ内の提供されたソフトウェアライブラリ、認定されたソフトウェアモジュール、及びハードウェア機器の暗号サービスプロバイダ（セキュアエレメントや 信頼できる実行環境（TEE））は、すべてレビュー又は評価されている。

規定 5.5-3 暗号アルゴリズムとプリミティブは、アップデート可能であることが望ましい。

注 1： これは「クリプトアジリティ(cryptoagility)」とも呼ばれる。

アップデートできない機器については、機器の意図されたライフタイムが、機器が使用する暗号アルゴリズム（鍵サイズを含む）の推奨使用ライフタイムを超えないことが重要である。

規定 5.5-4 初期化された状態のネットワークインタフェースを経由した機器の機能へのアクセスは、そのインタフェースでの認証後にのみ可能であることが望ましい。

注 2： 機能はユースケースによって大きく異なり、個人データや機器のアクチュエータへのアクセスなど、様々なものが含まれる可能性がある。

例えばウェブオブシングス(Web of Things)[i.18]のように、公開されたオープンデータを提供する機器がある。これらの機器は、すべての人にオープンなアクセスを提供するために、認証なしでアクセスできる。

機器は、ネットワークサービスの脆弱性によって侵害される可能性がある。適切な認証メカニズムは、不正なアクセスから保護し、機器の多層防御（defence-in-depth ）に貢献することができる。

規定 5.5-5 ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする機器の機能は、認証後にのみアクセス可能でなければならない。ただし、機器が依存するネットワークサービスプロトコルで、機器の動作に必要な設定を製造業者が保証できない場合は、例外とする。

注 3： 例外となるプロトコルには、ARP、DHCP、DNS、ICMP、NTP が含まれる。

EXAMPLE 2: Security-relevant changes include permission management, configuration of network keys and password changes.

Provision 5.5-6 Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.

Provision 5.5-7 The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

Many different methods exist for enrolment and authentication. Some authentication values are provided by out-of-band authentication mechanisms, such as a QR code, and some are human-readable, such as a password.

Where an authentication mechanism uses unique values per authentication attempt (e.g. in a challenge-response mechanism or when using one time passwords as a second factor), the response is not the authentication value itself. However, it is still good practice to apply confidentiality protection to those values.

Confidentiality protection can be achieved using an encrypted communication channel or payload encryption. This is often done using protocols or algorithms at least as strong as the key material transmitted, however other mitigations, such as the need for close proximity, are available.

Provision 5.5-8 The manufacturer shall follow secure management processes for critical security parameters that relate to the device.

The use of open, peer-reviewed standards for critical security parameters (commonly referred to as "key management") is strongly encouraged.

5.6 Minimize exposed attack surfaces

The "principle of least privilege" is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Provision 5.6-1 All unused network and logical interfaces shall be disabled.

EXAMPLE 1: An administrative UI that is supposed to be accessed from the LAN is not accessible from the WAN by default.

EXAMPLE 2: A Direct Firmware Update (DFU) service exposed over Bluetooth® Low Energy is used for development but not expected to be used in production. It is disabled in the final product.

Provision 5.6-2 In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.

Security-relevant information can be exposed over a network interface as part of the initialization process. When security-relevant information is shared by a device when establishing a connection, it can be used by attackers to identify vulnerable devices.

EXAMPLE 3: When finding vulnerable devices throughout the whole IP address space, security-relevant information could be information about the device configuration, kernel version or software version.

Provision 5.6-3 Device hardware should not unnecessarily expose physical interfaces to attack.

Physical interfaces can be used by an attacker to compromise firmware or memory on a device. "Unnecessarily" refers to the manufacturer's assessment of the benefits of an open interface, used for user functionality or for debugging purposes.

EXAMPLE 4: A micro-USB port meant to be used to power the device only is physically configured so as not to also allow command or debug operations.

Provision 5.6-4 Where a debug interface is physically accessible, it shall be disabled in software.

EXAMPLE 5: A UART serial interface is disabled through the bootloader software on the device. No logon prompt and no interactive menu is available due to this disabling.

例 2： セキュリティ関連の変更には、許可管理、ネットワーク鍵の設定、パスワードの変更が含まれる。

規定 5.5-6 重要なセキュリティパラメータは、転送中は暗号化されることが望ましく、その暗号化は技術の特性、リスク及び用途に適切なものであることが望ましい。

規定 5.5-7 民生用 IoT 機器は、リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。

登録と認証には、多くの異なる方法が存在する。認証値には、QR コードのような帯域外（OOB）認証メカニズムによって提供されるものもあれば、パスワードのように人間が判読できるものもある。

認証メカニズムが認証の試行ごとに一意の値を使用する場合（例えば、チャレンジ・レスポンス・メカニズムで使用する場合や、第 2 因子としてワンタイムパスワードを使用する場合）、その応答は認証値そのものではない。しかし、これらの値に対して機密性保護を適用することは、それでもやはり良いプラクティスである。

機密性保護は、暗号化された通信チャネル又はペイロードの暗号化を使用して実現できる。これは、少なくとも送信されるキーマテリアルと同程度の強度のプロトコル又はアルゴリズムを使用して行われることが多いが、近接の必要性など、他の緩和策も利用可能である。

規定 5.5-8 製造業者は、機器に関連する重要なセキュリティパラメータについて、セキュアな管理プロセスに従わなければならない。

重要なセキュリティパラメータ（一般に「鍵管理」と呼ばれる）については、オープンで専門家の審査を受けた標準の使用が強く推奨される。

5.6 露出した攻撃面を最小化する

「最小権限の原則」は、優れたセキュリティエンジニアリングの基礎であり、他の応用分野と同様に IoT にも適用できる。

規定 5.6-1 すべての未使用のネットワークインタフェース及び論理インタフェースは無効化しなければならない。

例 1： LAN からアクセスすることが想定されている管理用 UI は、デフォルトでは WAN からアクセスできない。

例 2： Bluetooth® Low Energy 経由で露出されるファームウェアの直接更新(Direct Firmware Update：DFU) サービスは、開発には使用されるが、生産では使用されない。最終製品では、無効化される

規定 5.6-2 初期化状態において、機器のネットワークインタフェースは、認証されていないセキュリティ関連情報の開示を最小化しなければならない。

セキュリティ関連情報は、初期化プロセスの一部としてネットワークインタフェース上で露出されることがある。接続を確立する際にセキュリティ関連情報が機器によって共有されると、攻撃者が脆弱な機器を特定するためにそれを使用することができる。

例 3： IP アドレス空間全体から脆弱な機器を見つける場合、セキュリティ関連情報は、機器の構成、カーネルのバージョン、ソフトウェアのバージョンに関する情報である可能性がある。

規定 5.6-3 機器のハードウェアは、物理インタフェースを不必要に攻撃にさらすことは望ましくない。

物理インタフェースは、攻撃者が機器上のファームウェアやメモリを侵害するために使用することができる。「不必要に」とは、ユーザ機能又はデバッグのために使用されるオープンインタフェースの利点を製造業者が評価することを指している。

例 4： 機器への電力供給のみに使用される予定のマイクロ USB ポートが、コマンド又はデバッグ操作も許可しないように物理的に構成されている。

規定 5.6-4 物理的にアクセス可能なデバッグインタフェースは、ソフトウェアで無効化しなければならない。

例 5： UART シリアルインタフェースは、機器上のブートローダソフトウェアを通じて無効化される。この無効化により、ログオンプロンプトや対話型メニューは利用できない。

Provision 5.6-5 The manufacturer should only enable software services that are used or required for the intended use or operation of the device.

EXAMPLE 6: The manufacturer does not provision the device with any background processes, kernel extensions, commands, programs or tools that are not required for the intended use.

Provision 5.6-6 Code should be minimized to the functionality necessary for the service/device to operate.

EXAMPLE 7: "Dead" or unused code is removed and not considered to be benign.

Provision 5.6-7 Software should run with least necessary privileges, taking account of both security and functionality.

EXAMPLE 8: Minimal daemons/processes run with "root" privileges. In particular the processes that use network interfaces require unprivileged users rather than requiring a "root" user.

EXAMPLE 9: Applications running on a device that includes a multi-user operating system (e.g. Linux®) use different users for each component or service.

Software attacks on devices that aim to corrupt memory can be mitigated through mechanisms such as stack canaries, Address Space Layout Randomization (ASLR). The manufacturer can use platform security features where they are available to help further reduce the risk. Reducing privileges that they run at and minimizing code also helps to mitigate this risk.

Provision 5.6-8 The device should include a hardware-level access control mechanism for memory.

Software exploits often use the lack of access control in memory to execute malicious code. Access control mechanisms limit whether data in memory on the device can be executed. Suitable mechanisms include technologies such as MMUs or MPUs, executable space protection (e.g. NX bits), memory tagging, and trusted execution environments.

Provision 5.6-9 The manufacturer should follow secure development processes for software deployed on the device.

Secure development processes, including using version control, or enabling security-related compiler options (e.g. stack protection) can help ensure software artefacts are more secure. Manufacturers can use these options when using toolchains that support them.

5.7 Ensure software integrity

Provision 5.7-1 The consumer IoT device should verify its software using secure boot mechanisms.

A hardware root of trust is one way to provide strong attestation as part of a secure boot mechanism. A hardware root of trust is a component of a system from which all other components derive their "trust" - i.e. the source of cryptographic trust within that system. To fulfil its function, the hardware root of trust is reliable and resistant to both physical and logical tampering, as there is no mechanism to determine that the component has failed or been altered. By utilizing a hardware root of trust, a device can have confidence in results of cryptographic functions, such as those utilized for secure boot. A hardware root of trust can be either backed by mechanisms used for secure storage of credentials or other alternatives providing baseline levels of security assurance proportionate to the required level of security for a given device.

Provision 5.7-2 If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.

The ability to recover remotely from unauthorized changes can rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.

If a consumer IoT device detects an unauthorized change to its software, it will be able to inform the right stakeholder. In some cases, devices can have the ability to be in administration mode.

EXAMPLE: A thermostat in a room can have a user mode; this mode prevents changing of other settings. If an unauthorized change to software is detected, an alert to the administrator is appropriate, as the administrator has the ability to act on the alert (whereas a user does not).

規定 5.6-5 製造業者は、意図された機器の用途又は操作に使用される、又は必要とされるソフトウェアサービスのみを有効にすることが望ましい。

例 6： 製造業者は、意図された用途に必要とされないバックグラウンドプロセス、カーネル拡張、コマンド、プログラム又はツールを機器にセットアップしない。

規定 5.6-6 コードは、サービス／機器の操作に必要な機能に最小化されることが望ましい。

例 7: デッドコード又は未使用のコードは削除され、無害であると見なさない。

規定 5.6-7 ソフトウェアは、セキュリティと機能の両方を考慮し、必要最小限の権限で実行することが望ましい。

例 8：「root」権限で実行される最小限のデーモン／プロセス。特に、ネットワークインタフェースを使用するプロセスには、「root」ユーザではく、非特権ユーザを必要とする。

例 9： マルチユーザオペレーティングシステム（例： Linux®))を含む機器上で動作するアプリケーションは、コンポーネントやサービスごとに異なるユーザを使用する。

メモリ破壊を目的とした機器へのソフトウェア攻撃は、スタック保護（スタックカナリア）やアドレス空間配置のランダム化（ASLR）などのメカニズムによって軽減することができる。製造業者は、プラットフォームのセキュリティ機能を利用することで、リスクをさらに軽減することができる。また、実行する特権を減らし、コードを最小限に抑えることも、このリスクを軽減するのに役立つ。

規定 5.6-8 機器には、メモリに対するハードウェアレベルのアクセス制御メカニズムを含めることが望ましい。

ソフトウェアの悪用では、しばしば、メモリのアクセス制御の欠如を利用して悪意のあるコードを実行する。アクセス制御メカニズムは、機器上のメモリにあるデータが実行可能かどうかを制御する。適切なメカニズムには、MMU 又は MPU、実行保護（例：NX ビット）、メモリタギング、及び信頼できる実行環境などの技術が含まれる。

規定 5.6-9 製造業者は、機器に展開されるソフトウェアについて、セキュアな開発プロセスに従うことが望ましい。

バージョン管理の使用、又はセキュリティ関連のコンパイラオプション（例：スタック保護）の有効化を含むセキュアな開発プロセスは、ソフトウェア成果物がよりセキュアであることを確実にするのに役立つ。製造業者は、これらのオプションをサポートするツールチェーンを使用する場合に、これらのオプションを使用することができる。

5.7 ソフトウェアの完全性を確実にする

規定 5.7-1 民生用 IoT 機器は、セキュアブートメカニズムを使用してそのソフトウェアを検証することが望ましい。

ハードウェアの信頼の基点は、セキュアブートメカニズムの一部として強力な認証を提供する一つの方法である。ハードウェアの信頼の基点は、他のすべてのコンポーネントがその「信頼」を得るシステムのコンポーネント、すなわちそのシステム内の暗号化の信頼の源である。その機能を果たすために、ハードウェアの信頼の基点は信頼性が高く、物理的及び論理的な改ざんに対して耐性がある。これは、コンポーネントが故障したか、又は変更されたかを判断するメカニズムがないためである。ハードウェアの信頼の基点を利用することで、機器はセキュアブートに利用されるような暗号関数の結果を信頼することができる。ハードウェアの信頼の基点は、認証情報をセキュアな保存に使用されるメカニズム、又は所与の機器に必要なセキュリティのレベルに相応したベースラインレベルのセキュリティ保証を提供するその他の代替手段によって裏付けられる。

規定 5.7-2 ソフトウェアに不正な変更が検出された場合、機器はユーザ及び／又は管理者に問題を警告することが望ましく、警告機能を実行するために必要なネットワークよりも広いネットワークに接続することは望ましくない。

不正な変更からリモートで回復する能力は、機器の安全な回復とアップデートを可能にするために既知の正常なバージョンをローカルに保存するなど、既知の正常な状態を頼りにすることが出来る。これにより、サービス拒否や費用のかかるリコールやメンテナンス訪問を回避できるとともに、アップデートやその他のネットワーク通信メカニズムを悪用する攻撃者によって機器が乗っ取られる可能性があるリスクに対処できる

民生用 IoT 機器が、そのソフトウェアに対する不正な変更を検出した場合、適切なステークホルダーに通知できるようになる。場合によっては、機器を管理モードにすることができる。

例： 部屋のサーモスタットには、ユーザモードを設定できる。このモードでは、他の設定を変更できない。ソフトウェアへの不正な変更が検出された場合、管理者には警告に応じて行動する能力がある（一方、ユーザはそうではない）ので、管理者に警告するのが適切である。

NOTE: An attack that forces a device to revert to a known good state can introduce a DoS risk if the device is unable to successfully perform this or if the attacker is able to repeatedly cause this effect.

5.8 Ensure that personal data is secure

Provision 5.8-1 The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.

Provision 5.8-2 The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.

NOTE 1: In the context of this provision, "sensitive personal data" is data whose disclosure has a high potential to cause harm to the individual. What is to be treated as "sensitive personal data" varies across products and use cases, but examples are: video stream of a home security camera, payment information, content of communication data and timestamped location data. Carrying out security and data protection impact assessments can help the manufacturer make appropriate choices.

NOTE 2: Associated services in this context are typically cloud services. Moreover these services are controlled or can be influenced by the manufacturer. These services typically are not operated by the user.

NOTE 3: Confidentiality protection often includes integrity protection according to best practice cryptography.

Provision 5.8-3 All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.

EXAMPLE: An external sensing capability can be an optic or acoustic sensor.

Clause 6 of the present document contains provisions specific to protecting personal data.

5.9 Make systems resilient to outages

The aim of the provisions in the present clause is to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases, including in functions that are relevant to personal safety. It is important to note that safety-related regulations can apply, but the key is to avoid making outages the cause of impact on the user and to design products and services that provide a level of resilience to these challenges.

Provision 5.9-1 Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.

Provision 5.9-2 Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.

NOTE: "Recovering cleanly" normally involves resuming connectivity and functionality in the same or improved state.

Provision 5.9-3 The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.

EXAMPLE 1: A Smart Home loses connection to the internet following a power outage. When the network connection is restored, the devices in the home reconnect after a randomized delay to minimize network utilization.

EXAMPLE 2: After making an update available, the manufacturer notifies devices in batches to prevent them all simultaneously downloading the update.

IoT systems and devices are relied upon by consumers for increasingly important use cases that can be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures can include building redundancy into associated services as well as mitigations against Distributed Denial of Service (DDoS) attacks or signalling storms, which can be caused by mass-reconnections of devices following an outage. It is expected that the level of resilience necessary is proportionate and determined by usage, with consideration given to others that rely on the system, service or device given that an outage can have a wider impact than expected.

注： 機器を既知の正常な状態に強制的に戻す攻撃は、機器がこれを正常に実行できない場合、又は攻撃者がこの効果を繰り返し引き起こすことができる場合、DoS リスクをもたらす可能性がある。

5.8 個人データがセキュアであることを確実にする

規定 5.8-1 機器とサービス（特に関連サービス）間で通信される個人データの機密性は、ベストプラクティスの暗号技術を使用して保護されることが望ましい。

規定 5.8-2 機器と関連サービス間で通信される機密の個人データの機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。

注 1： この規定の文脈において「機密の個人データ」とは、その開示が個人に害を及ぼす可能性が高いデータである。「機密の個人データ」として扱われるものは、製品やユースケースによって異なるが、例えば、家庭用セキュリティカメラのビデオストリーム、支払い情報、通信データの内容、タイムスタンプ付きの位置データなどがある。セキュリティとデータ保護の影響評価を実施することは、製造業者が適切な選択を行うのに役立つ。

注 2： この規定の文脈における関連サービスとは、一般的にクラウドサービスのことである。さらに、これらのサービスは、製造業者によって制御されるか、又は影響を受ける可能性がある。これらのサービスは、通常、ユーザによって操作されることはない。

注 3： 機密保護には、しばしばベストプラクティスの暗号技術に従った完全性保護が含まれる。

規定 5.8-3 機器のすべての外部感知機能は、ユーザにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。

例： 外部感知能力は、光学センサ又は音響センサである場合がある。

本文書の第 6 項には、個人データ保護に特化した規定が含まれている。

5.9 停止に対してレジリエントなシステムにする

本節の規定の目的は、消費者の生活のあらゆる場面で IoT 機器の導入が増加するにつれて、個人の安全に関連する機能を含め、IoT サービスが稼働し続けることを確実にすることである。安全関連の規制が適用されることもあるが、重要なのは、停止がユーザへの影響の原因となることを避け、これらの課題に対応するレベルのレジリエンスを提供する製品やサービスを設計することである。

規定 5.9-1 データネットワークと電源の停止の可能性を考慮して、レジリエンスを民生用 IoT 機器とサービスに組み込むことが望ましい。

規定 5.9-2 民生用 IoT 機器は、ネットワークアクセスが失われた場合にも動作を維持し、ローカルで機能し続けることが望ましく、電源損失が回復した場合にも正常に回復することが望ましい。

注：「正常に回復する」には、通常、接続と機能を同じ状態又は改善された状態で再開することが含まれる。

規定 5.9-3 民生用 IoT 機器は、インフラの能力を考慮し、期待された、運用可能な安定した状態で、秩序ある方法でネットワークに接続することが望ましい。

例 1： スマートホームが、停電によりインターネットへの接続を失う。ネットワーク接続が回復すると、ネットワーク使用を最小限に抑えるために、ランダムな遅延の後にスマートホーム内の機器が再接続される。

例 2： アップデートを利用可能にした後、製造業者は、すべての機器が同時にアップデートをダウンロードするのを防ぐために、バッチで機器に通知する。

IoT のシステムや機器は、安全に関わる、又は生命に影響を与える可能性のある、ますます重要となるユースケースで消費者から頼りにされている。ネットワークが失われた場合にサービスをローカルで稼働させ続けることは、レジリエンスを高めるためにできる対策の一つである。その他の対策としては、関連サービスに冗長性を持たせることや、停止後に機器の大規模な再接続によって引き起こされる可能性がある分散型サービス拒否（DDoS）攻撃やシグナルストームに対する緩和策などがある。停止が予想以上に大きな影響を及ぼす可能性があるため、必要なレジリエンスのレベルは、システム、サービス、又は機器に依存する他のユーザへの配慮をした上で、使用状況に応じて決定されることが期待される。

Orderly reconnection means in a manner that takes explicit steps to avoid simultaneous requests, such as for software updates or reconnections, from a large number of IoT devices. Such explicit steps can include the introduction of a random delay before a reconnection attempt according to an incremental back-off mechanism.

5.10 Examine system telemetry data

Provision 5.10-1 If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.

EXAMPLE 1: Security anomalies can be represented by a deviation from normal behaviour of the device, as expressed by the monitored indicators, for example an abnormal increase of failed login attempts.

EXAMPLE 2: Telemetry from multiple devices allows a manufacturer to notice that updates are failing due to invalid software update authenticity checks.

Examining telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimizing security risk and allowing quick mitigation of problems.

Clause 6 of the present document contains provisions specific to protecting personal data when telemetry data is collected.

5.11 Make it easy for users to delete user data

Provision 5.11-1 The user shall be provided with functionality such that user data can be erased from the device in a simple manner.

NOTE 1: User data in this context means all individual data which is stored on the IoT device including personal data, user configuration and cryptographic material such as user passwords or keys.

Provision 5.11-2 The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.

Such functionality is intended for situations when there is a transfer of ownership, when the consumer wishes to delete personal data, when the consumer wishes to remove a service from the device and/or when the consumer wishes to dispose of the device. It is expected that such functionality is compliant to applicable data protection law, including the GDPR [i.7].

Removing personal data "easily" means that minimal steps are required to complete that action that each involve minimal complexity.

Such functionality can potentially present an attack vector.

Provision 5.11-3 Users should be given clear instructions on how to delete their personal data.

Provision 5.11-4 Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.

Consumer IoT devices often change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications. When a consumer wishes to completely remove their personal data, they also expect retrospective deletion of backup copies.

Deleting personal data from a device or service is often not simply achieved by resetting a device back to its factory default state. There are many use cases where the consumer is not the owner of a device, but wishes to delete their own personal data from the device and all associated services such as cloud services or mobile applications.

EXAMPLE: A user can have temporary usage of consumer IoT products within a rented apartment. Carrying out a factory reset of the product can remove configuration settings or disable the device to the detriment of the apartment owner and a future user. A factory reset, deleting all data from the IoT device, would not be an appropriate way to delete the personal data of a single user in a shared use context such as this.

NOTE 2: Annex A of the present document contains an example model of device states including data storage for each state.

秩序立った再接続とは、多数の IoT 機器からのソフトウェアアップデート又は再接続などの同時リクエストを回避するための明確な手順を踏む方法を意味する。このような明確な手順には、増分バックオフメカニズムによる再接続試行前のランダム遅延の導入が含まれる場合がある。

5.10 システムのテレメトリデータを調べる

規定 5.10-1 民生用 IoT 機器やサービスから使用状況や計測データなどのテレメトリデータが収集される場合、セキュリティ上の異常がないかどうかを調べることが望ましい。

例 1： セキュリティ上の異常は、監視されたインジケータによって表される、機器の通常の動作からの逸脱、例えばログイン試行失敗の異常な増加によって表すことができる。

例 2： 複数の機器からのテレメトリにより、製造業者は、ソフトウェアアップデートの真正性チェックが無効であることが原因によるアップデートの失敗に気付くことができる。

ログデータを含むテレメトリを調べることは、セキュリティ評価に役立ち、異常な状況を早期に特定して対処することでセキュリティリスクを最小限に抑え、問題を迅速に軽減することができる。

第 6 節には、テレメトリデータを収集する際の個人データの保護に特化した規定がある。

5.11 ユーザが簡単にユーザデータを消去できるようにする

規定 5.11-1 ユーザは、簡単な方法で機器からユーザデータを消去できるような機能を提供されなければならない。

注 1： この文脈でのユーザデータとは、個人データ、ユーザ設定、ユーザパスワードや鍵などの暗号マテリアルを含む、IoT 機器に保存されるすべての個人データを意味する。

規定 5.11-2 消費者は、簡単な方法で個人データを関連サービスから削除できるような、機器上の機能を提供されることが望ましい。

このような機能は、所有権の移転がある場合、消費者が個人データを削除したい場合、消費者が機器からサービスを削除したい場合、及び／又は消費者が機器を廃棄したい場合を対象としている。このような機能は、GDPR [i.7]を含む、適用されるデータ保護法に準拠していることが期待される。

個人データを「簡単に」削除することは、その操作を完了するために必要な手順が最小限で済み、それぞれの操作の複雑さも最小限であることを意味する。

このような機能は、潜在的に攻撃ベクトルを提示する可能性がある。

規定 5.11-3 ユーザは、個人データを削除する方法について、明確な指示が与えられることが望ましい。

規定 5.11-4 ユーザは、サービス、機器、及びアプリケーションから個人データが削除されたことを示す明確な確認を提供されることが望ましい。

民生用 IoT 機器は所有者が変わることが多く、最終的にはリサイクルされるか廃棄される。消費者がコントロールを維持し、サービス、機器及びアプリケーションから個人データを削除することを可能にするメカニズムが提供される。消費者が個人データの完全な削除を希望する場合、バックアップコピーを過去にさかのぼって削除することも求められる。

機器やサービスからの個人データの削除は、多くの場合、機器をリセットして工場出荷時のデフォルト状態に戻すだけでは達成されない。消費者が機器の所有者ではないが、機器及びクラウドサービスやモバイルアプリケーションなどのすべての関連サービスから自分の個人データを削除したい場合、多くのユースケースが存在する。

例： ユーザは、賃貸アパートで民生用 IoT 機器を一時的に使用することができる。製品の工場出荷時の状態へのリセットを実行すると、アパートの所有者と将来のユーザに不利益となるように構成設定を削除したり、機器を無効にしたりすることができる。IoT 機器からすべてのデータを削除する工場出荷時の状態へのリセットは、このような共同使用の文脈における単一ユーザの個人データを削除する適切な方法ではない。

注 2： 附録 A には、各状態のデータストレージを含む機器の状態のモデル例が含まれている。

5.12 Make installation and maintenance of devices easy

Provision 5.12-1 Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.

EXAMPLE: The user uses a wizard to setup the device where a subset of configuration options is presented with the common defaults already specified and with appropriate security options already turned on by default.

Provision 5.12-2 The manufacturer should provide users with guidance on how to securely set up their device.

However, the ideal is for a process that involves the minimum of human intervention and which achieves a secure configuration automatically.

Provision 5.12-3 The manufacturer should provide users with guidance on how to check whether their device is securely set up.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

In the general case, the average overhead of securely setting up a device is higher than the average overhead of checking whether a device is securely setup. The check of a secure setup, from a process standpoint, can be undertaken in large part by the manufacturer through an automated process that communicates with the device remotely. Part of such an automated process could include validation of the device's capacity to establish a secure communication channel.

5.13 Validate input data

Provision 5.13-1 The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools such as fuzzers can be used by attackers or testers to exploit potential gaps and weaknesses that emerge as a result of not validating data.

EXAMPLE 1: The device receives data that is not of the expected type, for example executable code rather than user inputted text. The software on the device has been written so that the input is parameterized or "escaped", preventing this code from being run.

EXAMPLE 2: Out of range data is received by a temperature sensor, rather than trying to process this input it identifies that it is outside of the possible bounds and is discarded and the event is captured in telemetry.

6 Data protection provisions for consumer IoT

Many consumer IoT devices process personal data. It is expected that manufacturers provide features within consumer IoT devices that support the protection of such personal data. In addition, there exist laws and regulations that relate to the protection of personal data in consumer IoT devices (for example the GDPR [i.7]). The present document intends to help manufacturers of consumer IoT devices provide a number of features for the protection of personal data from a strictly technical perspective.

Provision 6-1 The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

Provision 6-2 Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.

Obtaining consent "in a valid way" normally involves giving consumers a free, obvious and explicit opt-in choice of whether their personal data can be used for a specified purpose.

5.12 機器の設置及びメンテナンスを容易にする

規定 5.12-1 民生用 IoT 機器の設置及び保守は、ユーザによる決定を最小限にすることが望ましく、ユーザビリティに関するセキュリティのベストプラクティスに従うことが望ましい。

例： ユーザはウィザードを使用して機器をセットアップする。ここでは、共通のデフォルトが既に指定され、適切なセキュリティオプションがデフォルトで既に有効にされた設定オプションのサブセットが提示される。

規定 5.12-2 製造業者は、機器をセキュアにセットアップする方法について、ユーザにガイダンスを提供することが望ましい。

ただし、人の介在を最小限にとどめ、セキュアな設定を自動的に実現するプロセスが理想的である。

規定 5.12-3 製造業者は、使用する機器がセキュアにセットアップされているかどうかを確認する方法について、ユーザにガイダンスを提供することが望ましい。

消費者の混乱や設定ミスに起因するセキュリティの問題は、ユーザインタフェースの複雑さやデザインの悪さに適切に対処することで軽減でき、時には解消されることもある。また、機器をセキュアに設定する方法についてユーザに明確なガイダンスを提供することで、脅威にさらされる機会を減らすことができる。

一般的なケースでは、機器をセキュアにセットアップするための平均オーバーヘッドは、機器がセキュアに設定されているかどうかをチェックするための平均オーバーヘッドよりも高くなる。プロセスの観点から、セキュアなセットアップのチェックは、機器とリモートで通信する自動化されたプロセスを通じで、製造業者が大部分を行うことができる。このような自動化されたプロセスの一部には、セキュアな通信チャネルを確立するための機器の能力の検証が含まれる可能性がある。

5.13 入力データの妥当性を確認する

規定 5.13-1 民生用 IoT 機器のソフトウェアは、ユーザインタフェース経由、アプリケーションプログラミングインタフェース（API）経由、又はサービスと機器のネットワーク間で転送されるデータの入力の妥当性を確認しなければならない。

システムは、異なるタイプのインタフェースを介して転送される不正確にフォーマットされたデータ又はコードによって破壊される可能性がある。ファザー（fuzzer）などの自動化されたツールは、攻撃者やテスターによって、データの妥当性確認をしないことで生じる潜在的なギャップや弱点を突くために使用されることがある。

例 1： 機器は、ユーザが入力したテキストではなく、例えば実行可能コードのような、期待されるタイプではないデータを受信する。機器上のソフトウェアは、それらの入力がパラメータ化又は「エスケープ」されるように記述されているため、このコードは実行されない。

例 2： 範囲外のデータが温度センサによって受信され、この入力を処理しようとするのでなく、可能な範囲外であることを識別して破棄し、そのイベントをテレメトリにキャプチャする。

6 民生用 IoT のためのデータ保護規定

多くの民生用 IoT 機器は、個人データを処理する。製造業者は、そのような個人データの保護をサポートする機能を民生用 IoT 機器内に提供することが期待される。さらに、民生用 IoT 機器における個人データの保護に関する法律及び規制が存在する（例えば GDPR [i.7]）。本文書は、厳密な技術的観点から、個人データ保護のための多くの機能を提供する民生用 IoT 機器の製造業者を支援することを目的としている。

規定 6-1 製造業者は、消費者に対し、機器及びサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供しなければならない。これは、広告主を含む、関与する可能性のある第三者にも適用される。

規定 6-2 個人データが消費者の同意に基づいて処理される場合、この同意は妥当な方法で取得されなければならない。

「妥当な方法」による同意の取得には、通常、自分の個人データを特定の目的に使用できるかどうかについて、自由で明白かつ明示的なオプトインの選択肢を消費者に与えることが含まれる。

Provision 6-3 Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.

Consumers expect to be able to preserve their privacy by configuring IoT device and service functionality appropriately.

Provision 6-4 If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.

Provision 6-5 If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.

規定 6-3 個人データの取得に同意した消費者は、いつでもそれを撤回できなければならない。

消費者は、IoT 機器やサービスの機能を適切に設定することで、自分のプライバシーを保護できることを期待する。

規定 6-4 消費者の民生用 IoT 機器及びサービスからテレメトリデータが収集される場合、個人データの処理は、意図された機能にとって必要最小限のものにとどめることが望ましい。

規定 6-5 消費者の民生用 IoT 機器及びサービスからテレメトリデータが収集される場合、どのようなテレメトリデータが収集され、それが誰によって、どのような目的で使用されているかについての情報が消費者に提供されなければならない。

Annex A (informative): Basic concepts and models

A.1 Architecture

A consumer IoT device is a collection of hardware and software components, generally with physical interfaces which can also be network interfaces. A general example and a specific "Smart Speaker" sophisticated example are shown below in figure A.1. These architectures are informative and it is not expected that a device would have all or some of the components pictured.

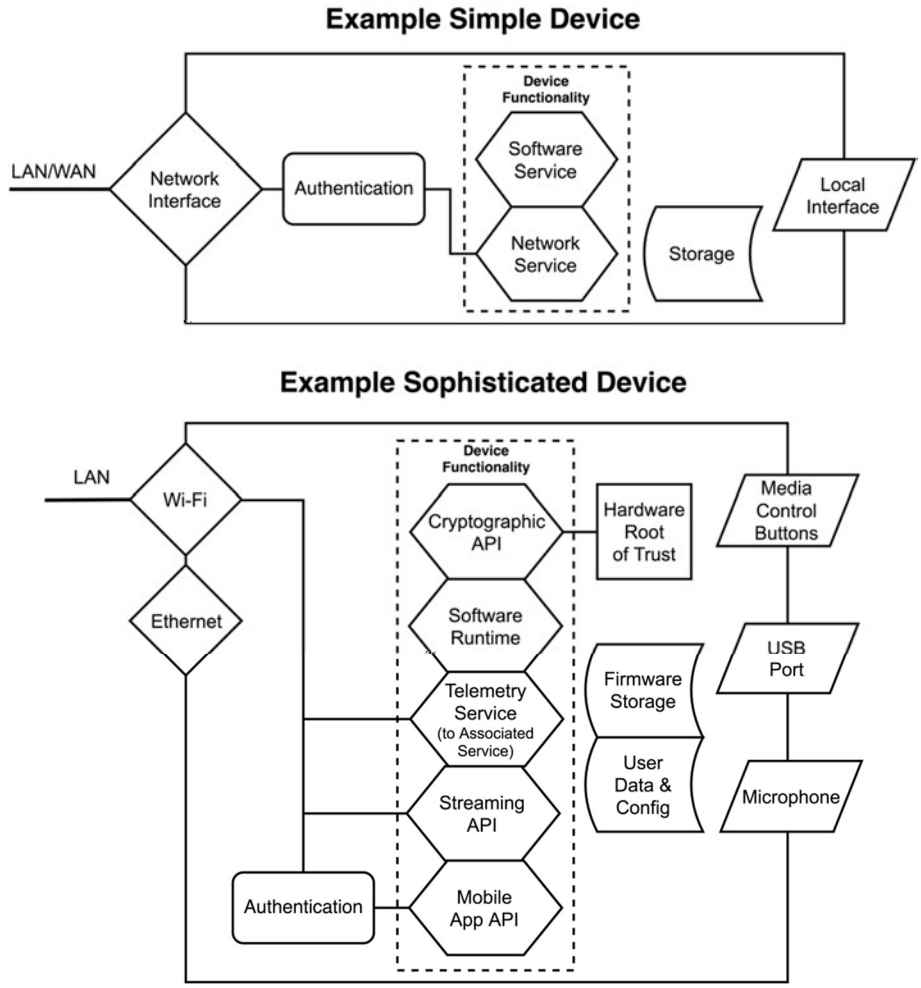

Figure A.1: Examples of a general architecture of a device and of an architecture for a Smart Speaker

Consumer IoT deployed in the home will often consist of a variety of both constrained and non-constrained devices that will be connected to the LAN, either directly through IP connectivity, such as over Ethernet or Wi-Fi®, or indirectly via a gateway or hub. This indirect connection to the LAN will generally use non-IP connectivity (e.g. protocols based on IEEE 802.15.4 [i.24]). A router will then connect the LAN to the WAN (i.e. the Internet). In some cases, however, a device within the home can connect directly to the WAN over other non-IP or IP connections (such as GSM or LoRaWAN).

附録 A (参考): 基本コンセプトとモデル

A.1 アーキテクチャ

民生用 IoT 機器は、ハードウェアとソフトウェアのコンポーネントの集合体であり、通常はネットワークインタフェースでもある物理インタフェースを備えている。一般的な例と、「スマートスピーカー」の高度な例を図 A.1 に示す。これらのアーキテクチャは参考であり、機器が図に示されているコンポーネントのすべて又は一部を備えていることは求められていない。

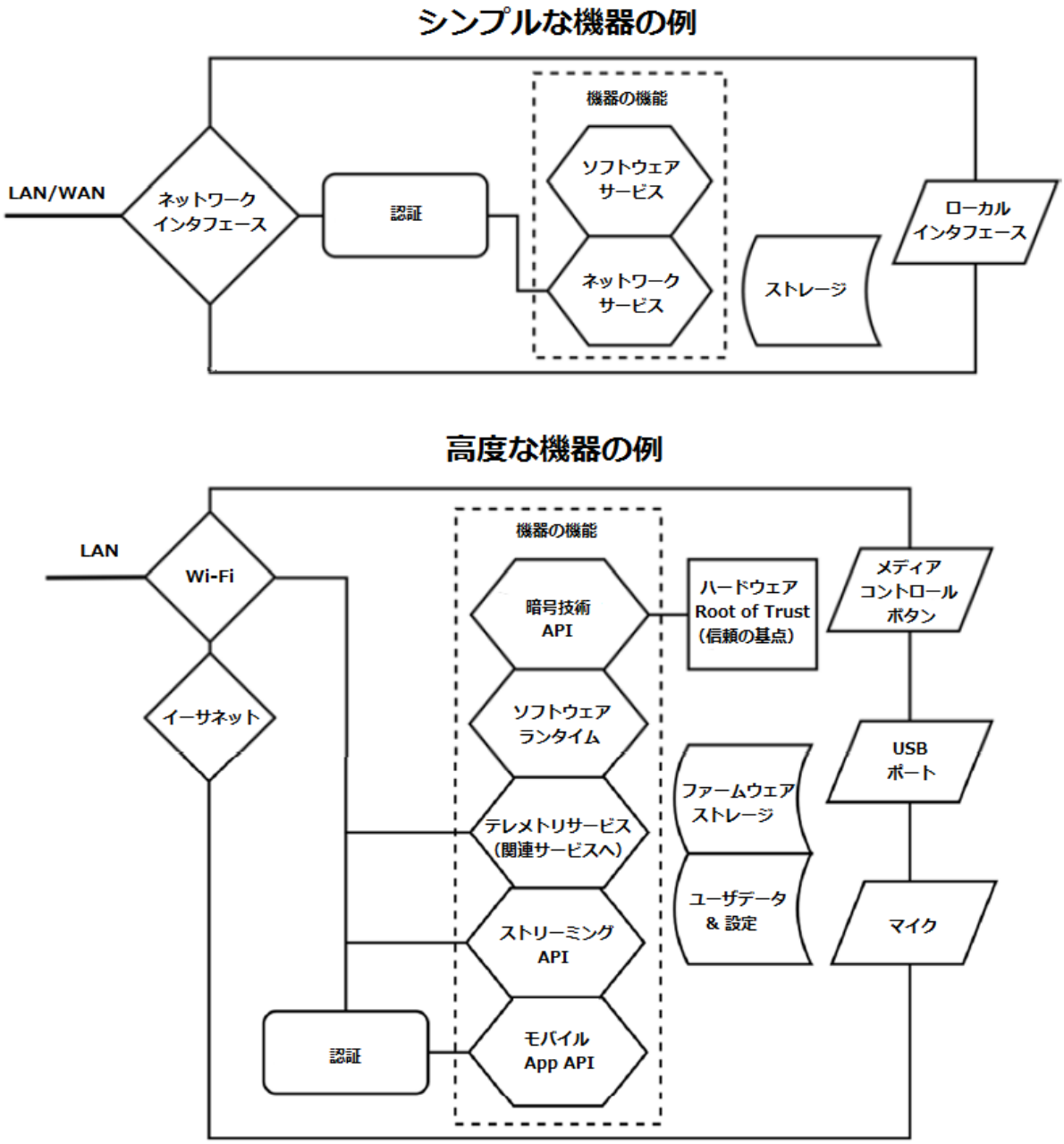

図 A.1: 機器の一般的なアーキテクチャの例とスマートスピーカーのアーキテクチャの例

家庭内に導入される民生用 IoT は、多くの場合、制約のある機器と制約のない機器の両方で構成され、イーサネットや Wi-Fi®などの IP 接続を介して直接又はゲートウェイやハブを介して間接的に LAN に接続される。この LAN への間接接続では、通常、非 IP 接続（IEEE 802.15.4 [i.24]に基づくプロトコルなど)が使用される。その後、ルータが LAN を WAN（すなわちインターネット）に接続する。ただし、場合によっては、家庭内の機器が他の非 IP 又は IP 接続（GSM 又は LoRaWAN など）を介して WAN に直接接続できる。

Consumer IoT devices in the home will often connect outwards to (or be connected into by) online or local services. In the present document those that are included by the manufacturer (for example telemetry, or a companion mobile application) or that have to be installed as part of the initialization are classed as associated services - in cases where the user chooses to install a service, or access external content then these would not count as associated services. For example, some scenarios:

- websites accessed via a device's browser are likely to not be associated services as the user is deciding to access them, not the developer of the device software;
- software applications (such as an "app" that might be installed on a Smart TV) that run on a device; if they are installed by default, then they would generally be classified as associated services. If, however, they are installed through a store at the choice of the user, then they would not be associated;
- connecting to a telemetry platform would be an associated service as this is usually pre-configured by the device manufacturer.

Figure A.2 provides an example of an architecture for this model of deployment. The "home" boundary represents the approximate extent of the scope defined for the present document - including communication to associated services.

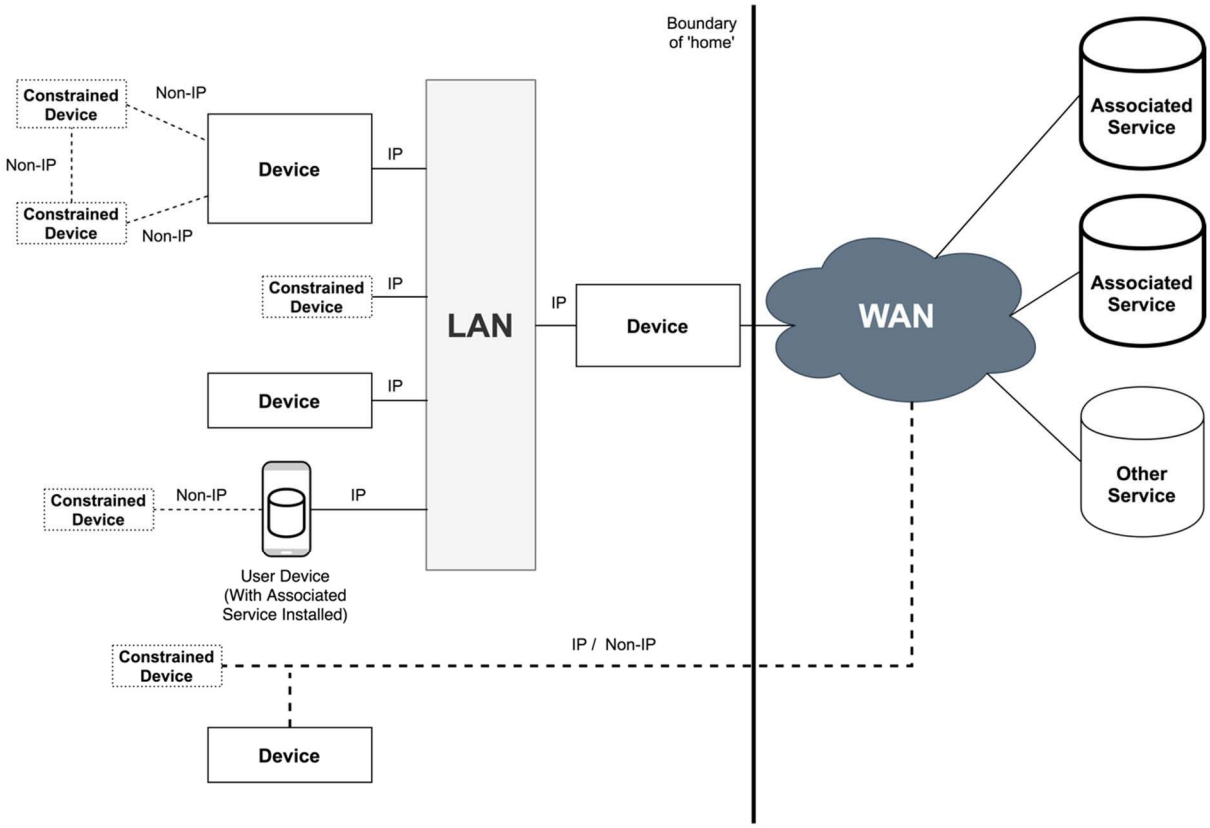

Figure A.2: Example of a reference architecture for consumer IoT deployment in a home environment

Figure A.3 shows an example, realistic, deployment of consumer IoT within a home. The following use-cases illustrate how this setup would be used and clarify what would and would not be covered under definitions:

- The Smart TV communicates with two external services. The first is the Device Telemetry Service (an associated service); this captures, with user permission, information from the TV such as crash logs and data on usage to enable the developers to fix software defects and prioritize development of new functionality. The Smart TV also connects to a Video Sharing Service through an application downloaded by the user after initialization. This Video Sharing Service enables a user to watch entertainment via a third-party application, which is installable within the operating system used by the TV. This streaming service would not be an associated service.
- The Gateway provides access to a variety of constrained devices, including an IEEE 802.15.4 [i.24] mesh network and a Light Sensor, used to monitor and manage the home. It connects to a Cloud Access Service that enables the user to control their Smart Lock remotely and see data from sensors. This is an associated service.

家庭内の民生用 IoT 機器は、多くの場合、オンライン又はローカルサービスに外部接続する（又はそれらによって外部から接続される）。本文書では、製造業者によって含まれるもの（例えばテレメトリ、又はモバイルコンパニオンアプリ）、又は初期化の一部としてインストールされる必要があるものは、関連サービスとして分類される。ユーザがサービスのインストールや外部コンテンツへのアクセスを選択した場合、これらは関連サービスとは見なされない。例えば、以下のようなシナリオがある：

- 機器のブラウザ経由でアクセスするウェブサイトは、機器のソフトウェアの開発者ではなく、ユーザがアクセスを決定しているため、関連サービスではない可能性がある；
- 機器上で実行されるソフトウェアアプリケーション（スマートテレビにインストールされる「アプリ」など）；それらがデフォルトでインストールされている場合、通常、関連サービスに分類される。ただし、ユーザが選択したストアを介してインストールされている場合は、関連サービスに該当しない；
- テレメトリプラットフォームへの接続は、通常、機器の製造業者によって事前に構成されているため、関連サービスとなる。

図 A.2 は、この展開のモデルのためのアーキテクチャの例を示している。「家庭」の境界は、関連サービスへの通信を含む、本文書で定義された範囲のおおよその範囲を表している。

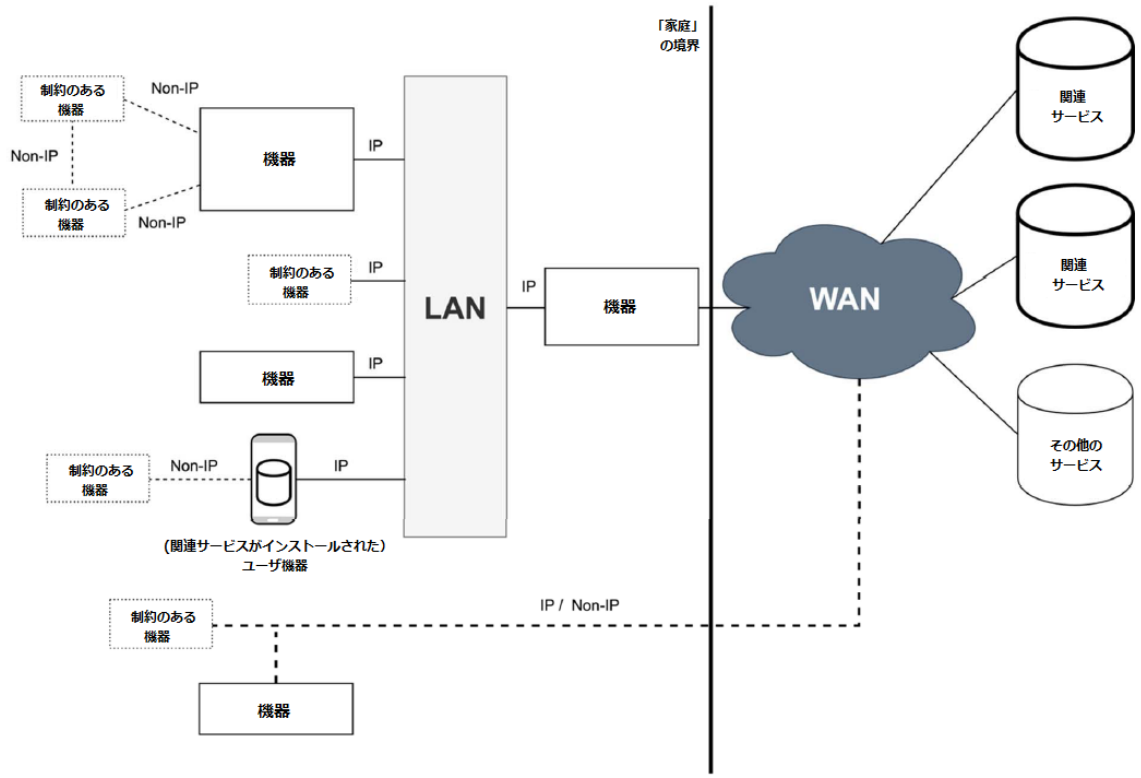

図 A.2：家庭環境における民生用 IoT の展開のための参照アーキテクチャの例

図 A.3 は、家庭内での民生用 IoT の現実的な展開の例を示している。以下のユースケースでは、このセットアップがどのように使用されるかを示し、定義で何がカバーされ、何がカバーされないかを明確にする：

- スマートテレビは、2 つの外部サービスと通信する。1 つは、機器のテレメトリサービス（関連サービス）；これはユーザの許可を得て、テレビからクラッシュログや使用状況のデータなどの情報を取得し、開発者がソフトウェアの不具合を修正したり、新機能の開発に優先順位をつけたりできるようにするためのものである。また、スマートテレビは、初期設定後にユーザがダウンロードするアプリケーションを通じて、ビデオ共有サービスに接続する。このビデオ共有サービスは、テレビが使用する OS 内にインストール可能なサードパーティアプリケーションを介して、ユーザがエンターテインメントを視聴することを可能にする。このストリーミングサービスは、関連サービスではない。
- ゲートウェイは、IEEE 802.15.4 [i.24]メッシュネットワークや光センサなど、様々な制約のある機器へのアクセスを提供し、家庭を監視及び管理するために使用される。ユーザはクラウドアクセスサービスに接続して、スマートロックをリモートで制御したり、センサのデータを確認したりできる。これは関連サービスである。

- The Smart Fridge has a web browser installed; this allows the user to view headlines from a news website while nearby. The news website would not be an associated service.

- The Weather Sensor is used by the user to check the temperature outside their home. As it is physically remote from the home itself it is unable to connect to the LAN. Instead it communicates via GSM directly to the WAN. The service the Weather Sensor connects to is an associated service.

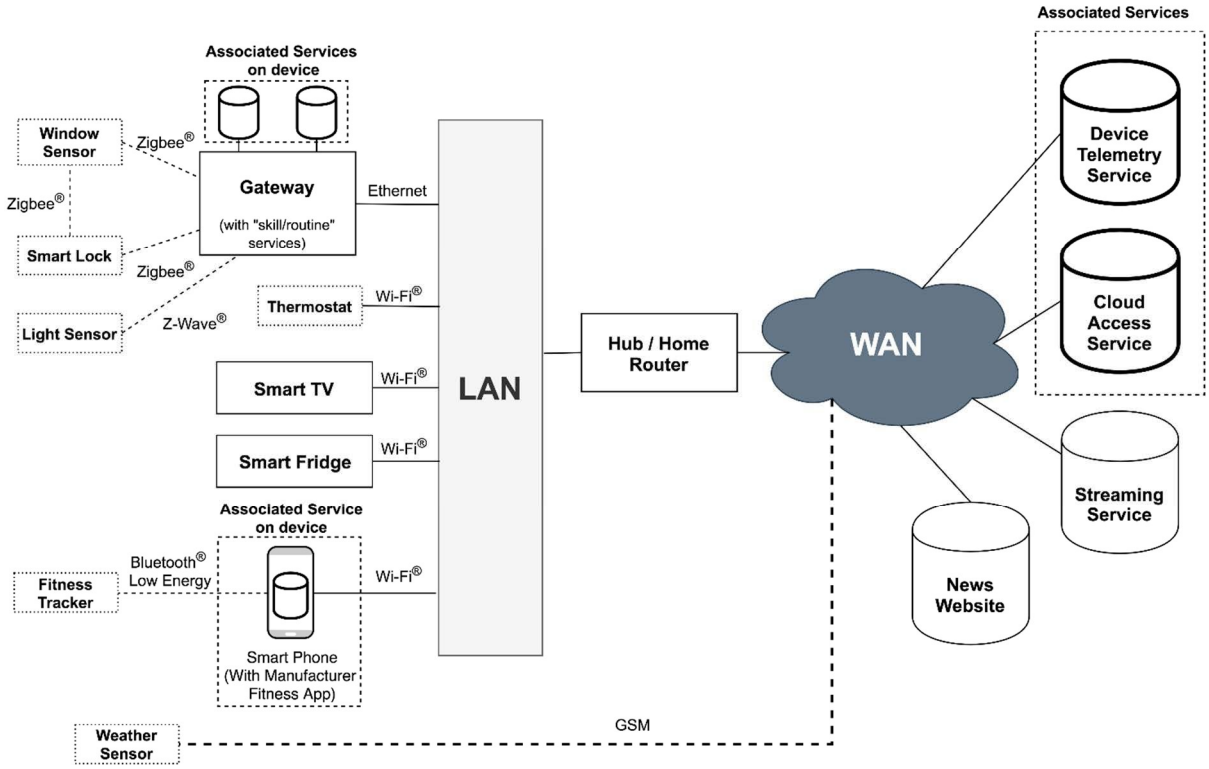

Figure A.3: Example architecture of a consumer IoT deployment

A.2 Device states

Decommissioning devices is out of scope of the present document. A decommissioned device is in a state where sensitive data is not present. A device (from manufacturing to decommissioning) will transition between several states. These transitions are illustrated in figure A.4, to make clear how the defined states could be used in a device. In this model, a decommissioned device would be in the Factory Default state, as the Factory Reset process is likely to be the process used to remove all user data and configuration.

EXAMPLE: When decommissioned, a device can be recycled, resold or destroyed.

- スマート冷蔵庫にはウェブブラウザがインストールされている；これにより、ユーザは冷蔵庫の近くにいながらニュースウェブサイトのヘッドラインを閲覧することができる。ニュースウェブサイトは関連サービスではない。
- 天気センサは、ユーザが自宅の外の気温を確認するために使用する。自宅から物理的に離れているため、LAN に接続できない。代わりに、GSM を介して WAN と直接通信する。天気センサが接続するサービスは、関連サービスである。

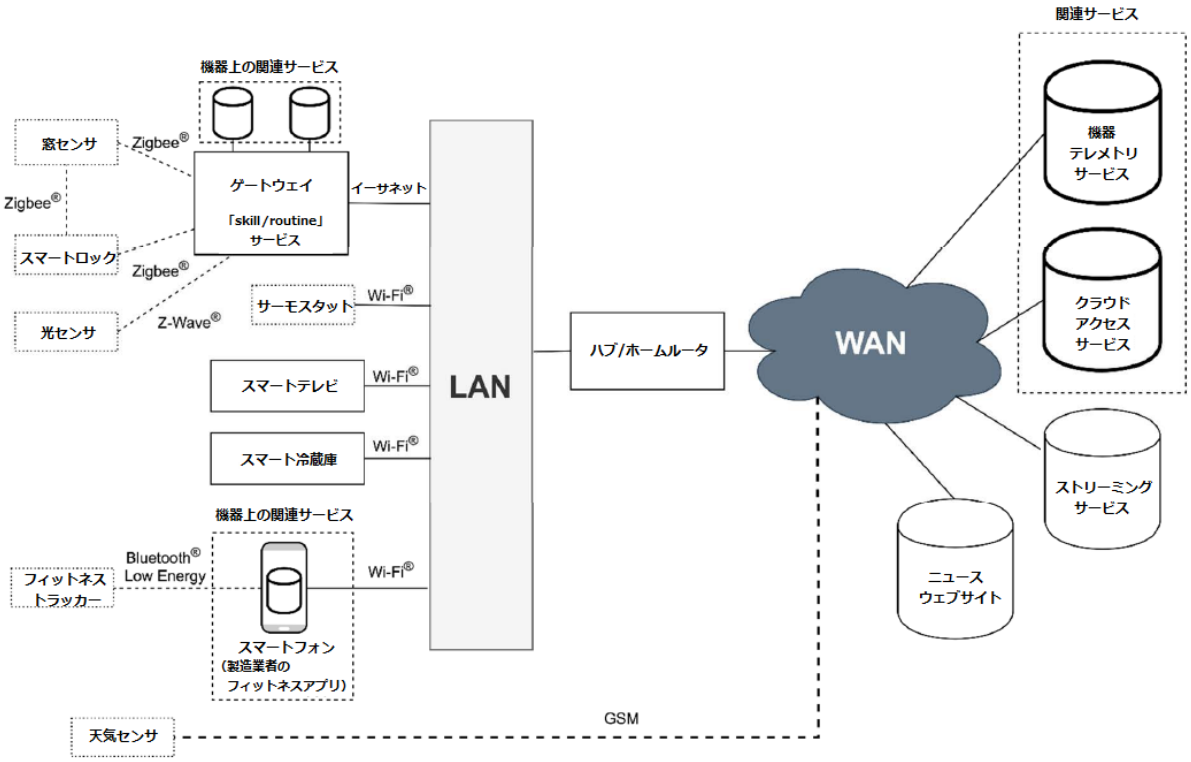

図 A.3：民生用 IoT の展開のアーキテクチャ例

A.2 機器の状態

機器の廃止は、本文書の範囲外である。廃止された機器は、機密データが存在しない状態である。機器は（製造から廃止まで）いくつかの状態の間を遷移する。これらの遷移を図 A.4 に示し、定義された状態が機器でどのように使用されるかを明確にしている。このモデルでは、工場出荷時の状態へのリセットプロセスがすべてのユーザデータと構成を削除するために使用するプロセスである可能性が高いため、廃止された機器は工場出荷時のデフォルト状態であるだろう。

例： 廃止されると、機器はリサイクル、再販又は破壊することができる。

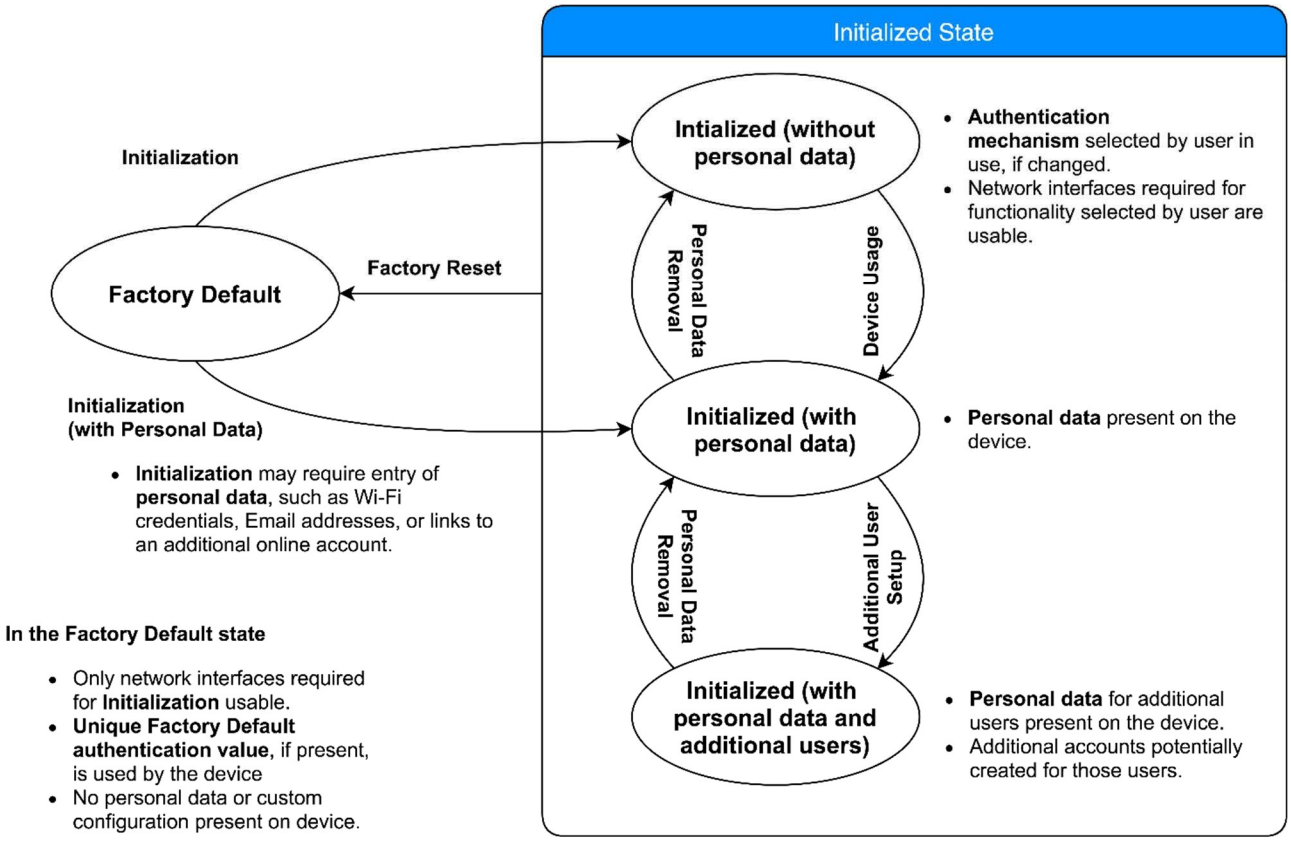

Figure A.4: State diagram for consumer IoT device states

Within these states, figure A.5 shows an example model for what data would be stored within an arbitrary device. It is not expected that this would be the same for every case.

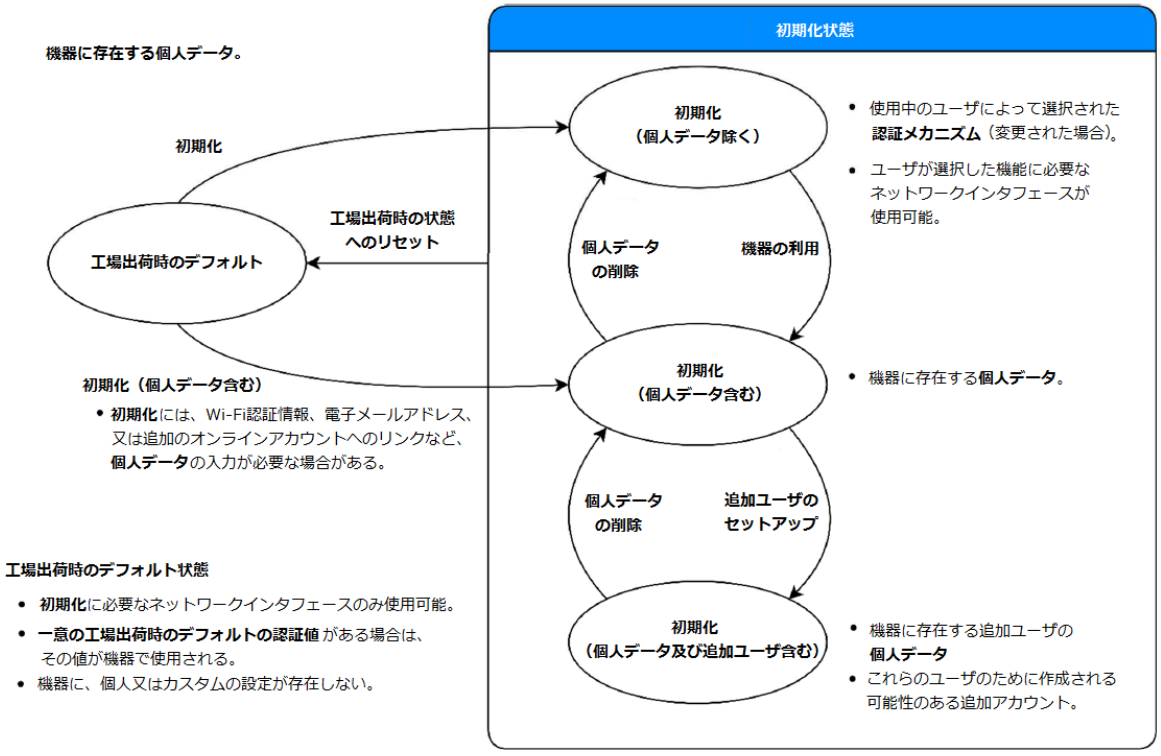

図 A.4：民生用 IoT 機器の状態の状態図

これらの状態の中で、図 A.5 は、任意の機器内にどのようなデータが保存されるかのモデル例を示している。これがすべてのケースで同じであるとは想定されていない。

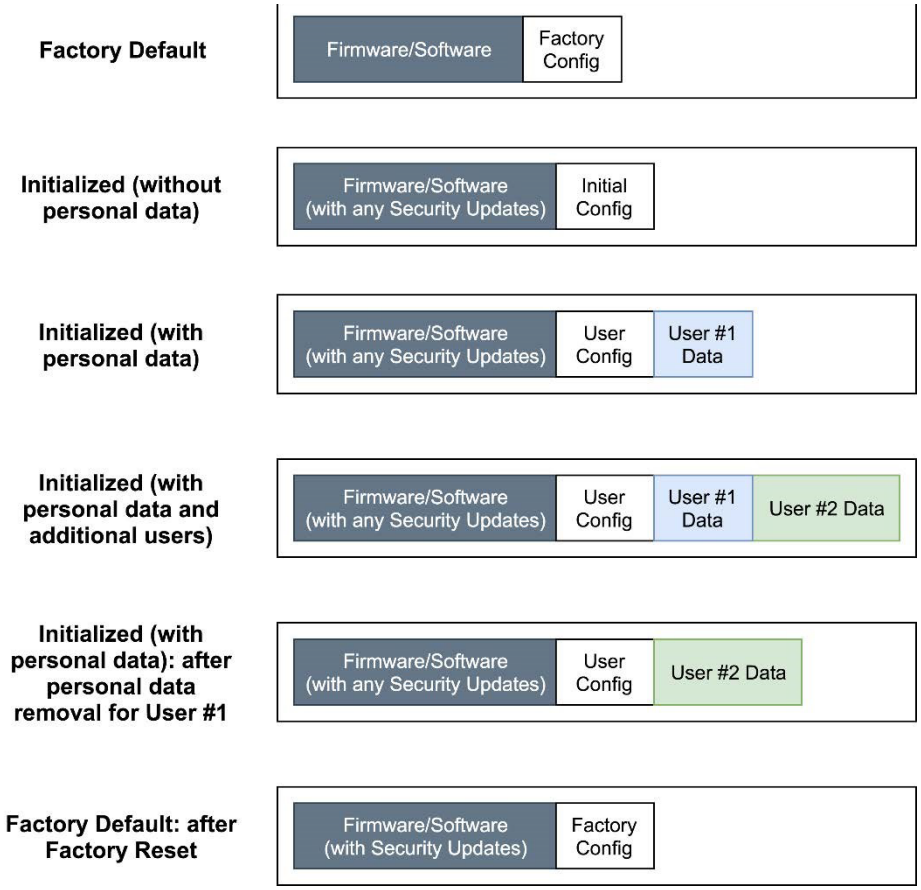

Figure A.5: Model of example device storage in states

図 A.5：状態における機器のストレージの例のモデル

Annex B (informative): Implementation conformance statement pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document can freely reproduce the pro forma in the present annex so that it can be used for its intended purposes and can further publish the completed annex including table B.1.

Table B.1 can provide a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of consumer IoT) to give information about the implementation of the provisions within the present document.

The reference column gives reference to the provisions in the present document.

The status column indicates the status of a provision. The following notations are used:

M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional

NOTE: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

Y	supported by the implementation
N	not supported by the implementation
N/A	the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

The detail column can be filled in by the user of the present document:

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.
- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.
- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

附録 B (参考)：実装適合性宣言の形式

本文書の本文に関する著作権条項の規定にかかわらず、ETSI は、本文書の利用者が、意図した目的に使用できるように本附録の形式を自由に複製し、さらに表 B.1 を含む完成した附録を公開できることを許諾する。

表 B.1 は、本文書のユーザ（民生用 IoT 機器の開発又は製造に関わるエンティティであることが期待される）が、本文書内の規定の実施に関する情報を提供するためのメカニズムを提供することができる。

「参照」列は、本文書内の規定への参照を示す。

「ステータス」列は、規定のステータスを示す。以下の表記が使用される：

M 規定は必須要件である。

R 規定は勧告である

M C 規定は必須要件であり、かつ条件付きである。

R C 規定は勧告であり、条件付きである。

注： 条件付き表記が使用されている場合、これは規定の本文に基づく条件である。条件を明確にするために、関連する規定の参考文献を表の下に記載している。

「サポート」列は、本文書のユーザが記入することができる。以下の表記が使用される：

Y 実装によってサポートされている。

N 実装によってサポートされていない。

N/A 規定は適用されない（「ステータス」列で示されるように規定が条件付きであり、当該製品にその条件が適用されないと判断される場合にのみ許可される）

「詳細」列は、本文書のユーザが記入することができる。

- 規定が実装によってサポートされている場合、「詳細」列のエントリには、サポートを実現するために実装された措置に関する情報を記入する。
- 規定が実装によってサポートされていない場合、「詳細」列には実装が不可能又は適切でない理由についての情報を記入する。
- 規定が適用されない場合、「詳細」列にその判断の根拠を記入する。

Table B.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.1 No universal default passwords			
Provision 5.1-1	M C (1)		
Provision 5.1-2	M C (2)		
Provision 5.1-3	M		
Provision 5.1-4	M C (8)		
Provision 5.1-5	M C (5)		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		
Provision 5.2-2	R		
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R		
Provision 5.3-2	M C (5)		
Provision 5.3-3	M C (12)		
Provision 5.3-4	R C (12)		
Provision 5.3-5	R C (12)		
Provision 5.3-6	R C (9, 12)		
Provision 5.3-7	M C (12)		
Provision 5.3-8	M C (12)		
Provision 5.3-9	R C (12)		
Provision 5.3-10	M (11, 12)		
Provision 5.3-11	R C (12)		
Provision 5.3-12	R C (12)		
Provision 5.3-13	M		
Provision 5.3-14	R C (3, 4)		
Provision 5.3-15	R C (3, 4)		
Provision 5.3-16	M		
5.4 Securely store sensitive security parameters			
Provision 5.4-1	M		
Provision 5.4-2	M C (10)		
Provision 5.4-3	M		
Provision 5.4-4	M		
5.5 Communicate securely			
Provision 5.5-1	M		
Provision 5.5-2	R		
Provision 5.5-3	R		
Provision 5.5-4	R		
Provision 5.5-5	M		
Provision 5.5-6	R		
Provision 5.5-7	M		
Provision 5.5-8	M		
5.6 Minimize exposed attack surfaces			
Provision 5.6-1	M		
Provision 5.6-2	M		
Provision 5.6-3	R		
Provision 5.6-4	M C (13)		

表 B.1：民生用 IoT のセキュリティに関する規定の実施

項番号及びタイトル			
参照	**ステータス**	**サポート**	**詳細**
5.1 汎用のデフォルトパスワードを使用しない			
規定 5.1-1	M C (1)		
規定 5.1-2	M C (2)		
規定 5.1-3	M		
規定 5.1-4	M C (8)		
規定 5.1-5	M C (5)		
5.2 脆弱性の報告を管理するための手段を導入する			
規定 5.2-1	M		
規定 5.2-2	R		
規定 5.2-3	R		
5.3 ソフトウェアを最新の状態に保つ			
規定 5.3-1	R		
規定 5.3-2	M C (5)		
規定 5.3-3	M C (12)		
規定 5.3-4	R C (12)		
規定 5.3-5	R C (12)		
規定 5.3-6	R C (9, 12)		
規定 5.3-7	M C (12)		
規定 5.3-8	M C (12)		
規定 5.3-9	R C (12)		
規定 5.3-10	M (11, 12)		
規定 5.3-11	R C (12)		
規定 5.3-12	R C (12)		
規定 5.3-13	M		
規定 5.3-14	R C (3, 4)		
規定 5.3-15	R C (3, 4)		
規定 5.3-16	M		
5.4 機密セキュリティパラメータをセキュアに保存する			
規定 5.4-1	M		
規定 5.4-2	M C (10)		
規定 5.4-3	M		
規定 5.4-4	M		
5.5 セキュアに通信する			
規定 5.5-1	M		
規定 5.5-2	R		
規定 5.5-3	R		
規定 5.5-4	R		
規定 5.5-5	M		
規定 5.5-6	R		
規定 5.5-7	M		
規定 5.5-8	M		
5.6 露出した攻撃面を最小化する			
規定 5.6-1	M		
規定 5.6-2	M		
規定 5.6-3	R		
規定 5.6-4	M C (13)		

Clause number and title			
Provision 5.6-5	R		
Provision 5.6-6	R		
Provision 5.6-7	R		
Provision 5.6-8	R		
Provision 5.6-9	R		
5.7 Ensure software integrity			
Provision 5.7-1	R		
Provision 5.7-2	R		
5.8 Ensure that personal data is secure			
Provision 5.8-1	R		
Provision 5.8-2	M		
Provision 5.8-3	M		
Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.9 Make systems resilient to outages			
Provision 5.9-1	R		
Provision 5.9-2	R		
Provision 5.9-3	R		
5.10 Examine system telemetry data			
Provision 5.10-1	R C (6)		
5.11 Make it easy for users to delete user data			
Provision 5.11-1	M		
Provision 5.11-2	R		
Provision 5.11-3	R		
Provision 5.11-4	R		
5.12 Make installation and maintenance of devices easy			
Provision 5.12-1	R		
Provision 5.12-2	R		
Provision 5.12-3	R		
5.13 Validate input data			
Provision 5.13-1	M		
6 Data protection provisions for consumer IoT			
Provision 6.1	M		
Provision 6.2	M C (7)		
Provision 6.3	M		
Provision 6.4	R C (6)		
Provision 6.5	M C (6)		

Conditions
1) passwords are used;
2) pre-installed passwords are used;
3) software components are not updateable;
4) the device is constrained;
5) the device is not constrained;
6) telemetry data being collected;
7) personal data is processed on the basis of consumers' consent;
8) the device allowing user authentication;
9) the device supports automatic updates and/or update notifications;
10) a hard-coded unique per device identity is used for security purposes;
11) updates are delivered over a network interface; 12) an update mechanism is implemented;
13) a debug interface is physically accessible.

項番号及びタイトル			
規定 5.6-5	R		
規定 5.6-6	R		
規定 5.6-7	R		
規定 5.6-8	R		
規定 5.6-9	R		
5.7 ソフトウェアの完全性を確実にする			
規定 5.7-1	R		
規定 5.7-2	R		
5.8 個人データがセキュアであることを確実にする			
規定 5.8-1	R		
規定 5.8-2	M		
規定 5.8-3	M		
項番号及びタイトル			
参照	**ステータス**	**サポート**	**詳細**
5.9 停止に対してレジリエントなシステムにする			
規定 5.9-1	R		
規定 5.9-2	R		
規定 5.9-3	R		
5.10 システムのテレメトリデータを調べる			
規定 5.10-1	R C (6)		
5.11 ユーザが簡単にユーザデータを消去できるようにする			
規定 5.11-1	M		
規定 5.11-2	R		
規定 5.11-3	R		
規定 5.11-4	R		
5.12 機器の設置及びメンテナンスを容易にする			
規定 5.12-1	R		
規定 5.12-2	R		
規定 5.12-3	R		
5.13 入力データの妥当性を確認する			
規定 5.13-1	M		
6 民生用 IoT のためのデータ保護規定			
規定 6.1	M		
規定 6.2	M C (7)		
規定 6.3	M		
規定 6.4	R C (6)		
規定 6.5	M C (6)		

条件

1) パスワードを使用している；
2) プリインストールされているパスワードを使用している；
3) ソフトウェアコンポーネントがアップデート可能ではない；
4) 機器に制約がある；
5) 機器に制約がない；
6) テレメトリデータが収集されている；
7) 消費者の同意に基づいて個人データが処理されている；
8) ユーザ認証を許可する機器；
9) 機器が、自動化されたアップデート及び／又はアップデート通知をサポートしている；
10) ハードコードされた機器ごとの一意の ID が、セキュリティ目的のために使用されている；
11) アップデートがネットワークインタフェースを介して配信される；
12) アップデートメカニズムが実装されている；
13) デバッグインタフェースが物理的にアクセス可能である。

History

Document history			
V1.1.1	February 2019	Publication as ETSI TS 103 645	
V2.0.0	November 2019	EN Approval Procedure	AP 20200224: 2019-11-26 to 2020-02-24
V2.1.0	April 2020	Vote	V 20200619: 2020-04-20 to 2020-06-19
V2.1.1	June 2020	Publication	

履歴

ドキュメント履歴			
V1.1.1	2019 年 2 月	ETSI TS 103 645 として公開	
V2.0.0	2019 年 11 月	EN 承認手続	AP 20200224: 2019-11-26 to 2020-02-24
V2.1.0	2020 年 4 月	投票	V 20200619: 2020-04-20 to 2020-06-19
V2.1.1	2020 年 6 月	公開	