Online Trust Alliance
an Internet Society initiative

IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® は、出荷時及び全体のライフサイクルにおいて、IOTデバイスとそのデータを安全に保つ為の一連の戦略的原則を含んでいます。 コンセンサス主導のマルチステークホルダープロセスを経て、接続型家庭用、オフィス、そして玩具、活動量計、またフィットネスデバイスを含むウェアラブルテクノロジー向けの基準が定められました。 フレームワークは、製品購入前の包括的開示の必要性、データ収集、データ使用、そしてデータ共有に関する方針、また保証期間後のセキュリティパッチの諸条件の概要を述べています。セキュリティアップデートは、脆弱性があわらになり攻撃が進化する際に、IoTデバイスの保護を最大化する為に不可欠です。 さらに、フレームワークはデバイスのアップデート機能と広範囲にわたるデータプライバシー関連問題について、製造業者への提言を行い、透明性とコミュニケーションを高めます。

固有のセキュリティリスクとプライバシー問題に対する取り組みの中核にあるものは、デバイスソリューションあるいは工コシステム全体へその原則を適用することです。 これらには、デバイスやセンサー、サポートするアプリケーション、そしてバックエンドあるいはクラウドサービスが含まれています。 多くの販売されている製品は、サードパーティーあるいはオープンソースのコンポーネントやソフトウェアに頼っているため、これらの原則の適用と、サプライチェーンセキュリティとプライバシーリスクアセスメントの実施は、開発者の義務になります。

開発者、購入者、そして小売業者の為のリスクアセスメントガイドとして、フレームワークは将来のIoT認証プログラムの基盤となっています。 OTAは、これらの基準を満たしているデバイスを紹介し、消費者、また公共および民間部門が、十分な情報を得た上で購入判断を下せるようにすることを目的としています。 フレームワークと関連のリソースはhttps://otalliance.org/IoTで御覧になれます。

フレームワークは4つの主要エリアに分類されます：

- **セキュリティの原則**(1-12) – あらゆるデバイスまたはセンサー、そして全てのアプリケーションとバックエンドクラウドサービスに適用されます。これらは、 綿密なソフトウェア開発セキュリティプロセスの適用から、データセキュリティの原則に忠実に従ったデバイスによるデータ保存および送受信、サプライチェーン管理、侵入テスト、そして脆弱性報告プログラムにまで及びます。さらには、ライフサイクルを通じてセキュリティパッチを行う必須要件の概要を述べています。
- **ユーザーアクセスとクレデンシャル**(13-17) – 全てのパスワードとユーザー名の暗号化が必須であること、デバイスにユニークなパスワードを設定して出荷、一般的に受け入れられているパスワード再設定プロセスの実行、そして「ブルートフォース」ログインの防御を可能にする機能の統合。
- **プライバシー、開示そして透明性**(18-33) – 必須条件は一般的に受け入れられているプライバシー原

則からなり、パッケージング、店頭あるいはオンライン、またはその両方においてはっきりと開示されていること、ユーザーがデバイスを工場出荷時設定にリセットできる機能があること、EU一般データ保護規則（EU GDPR）や児童プライバシー規則などの適用する規制上の要件へ準拠すること、が含まれます。 また、接続が無効の場合の製品の特徴や機能への影響を開示するよう述べています。

- **通知と関連するベストプラクティス**(34-40) – デバイスのセキュリティを維持する秘訣は、脅威や必要な行動をユーザーに速やかに知らせるメカニズムとプロセスがあることです。セキュリティ通知には電子メール認証が必要であり、メッセージは全ての読解力レベルのユーザーが理解できるものでなければなりません。さらには、不正開封防止包装とアクセスがしやすいことが必須であると強調しています。

OTA IoT Trust Framework® v2.5（2017年10月14日更新）

このバージョンは、ウェアラブルテクノロジーを含む、家庭用及び企業用の「消費者向け」デバイスおよびサービスに重点を置いています。

IoT Trust Framework ● 必須（義務） ○ 推奨 （提案）	
セキュリティ – デバイス、アプリ、そしてクラウドサービス	
1. デバイスにセキュリティ関連のアップデートを受信する機能があるかどうかを開示し、もしある場合は、デバイスがセキュリティアップデートを自動的に受信できるかどうか、デバイスが正しく、そして適時にアップデートを受信しているか確認する為にユーザーがとるべき行動は何かを開示する。	●
2. デバイスと関連アプリケーションが現在一般的に受け入れられているセキュリティと暗号プロトコル、そしてベストプラクティスをサポートしているか確証する。送受信、また保存されている全ての個人を特定できるデータは、現在一般的に受け入れられているセキュリティ基準を使用して暗号化されなければならない。これには有線、Wi-Fi、そしてブルートゥース接続が含まれるが、これらに制限されているわけではない。	●
3. すべてのIoTサポートウェブサイトはデバイスとバックエンドサービス間のユーザーセッションを完全に暗号化しなければならない。 現在のベストプラクティスは、AOSSLまたは常時SSLとして知られているHTTPSとHTTP Strict Transport Security (HSTS) が、デフォルトで設定されている。 デバイスはバックエンドサービスとサポートしているアプリケーションを確実に認証するメカニズムを含んでいるべきである。[1]	●
4. 脆弱性の影響を容認できるレベルに減少させる為に、IoTサポートサイトは定期的なモニタリングと継続的なサイトセキュリティとサーバー設定の改善を行わなければならない。 少なくとも年に2回は侵入テストを行う	●
5. 第三者からの対外的脆弱性レポートを受け、追跡、そして速やかに対応するプロセスとシステムを含む脆弱性開示を取りまとめ、確立する。第三者は顧客、消費者、学界と研究コミュニティを含むが、それらに制限するものではない。製品リリース後のデザイン脆弱性や脅威は、公的に責任ある態度で、リモートアップデート、消費者への実行可能な通知、またはその両方、あるいはそのほかの効果的なメカニズムによって修正する。開発者は脆弱性を明らかにするた為に、「バグ発見報奨金」プログラム、およびクラウドソーシング方法を考慮すべきである。	●
6. ソフトウェア、ファームウェア、またはその両方のアップデート、パッチそして修正を提供する為に、自動化された安全かつ確実な方法を用いたメカニズムがあることを確証する。このようなアップデートには署名、信頼された発行元であることを認証、あるいはその両方が必要である。署名や整合性チェックが含まれるが、これらに制限されるわけではない。	●
7. アップデートとパッチはユーザーが設定したプリファランス、セキュリティ、プライバシー設定、またはこれら全てをユーザーに通知することなしに変更してはならない。デバイスファームウェアあるいはソフトウェアが上書きされた場合、その後最初に使用する際に、ユーザーはプライバシー設定をレビューし、選択できるようにしなければならない。	●

8. セキュリティアップデートプロセスが自動化されている場合は（自動的に対して）、開示しなければならない。 自動化されたアップデートでは、ユーザーはアップデートを承認、許可、そして拒否することができるようにする。 どのように、またいつアップデートするかをユーザー自身が決定できる機能もつける。データ消費とモバイルキャリアあるいはISP接続を介しての接続を含むが、これらに制限するわけではない。 逆に、自動的なアップデートは、ユーザーとの対話なしに、途切れることなくデバイスへプッシュし、ユーザーへの通知が必ずしもあるわけではない。	●
9. 全てのIoTデバイスと関連ソフトウェアが、ユニット、システム、承認、そしてレグレッションテスト、また脅威モデリングを含む、綿密で標準化されたソフトウェア開発サイクルテストに従っていることを確証する。あらゆるサードパーティーまたはオープンソースのコード、コンポーネント、またはそれら両方のソースコードも維持すべきである。 広範囲にわたる典型的なユースケースシナリオにおいて、一般的に受け入れられているコードとシステムのハードニング技術を使用する。デバイス、アプリ、そしてクラウドサービス間のデータ漏洩防止を含む。 安全なソフトウェア開発の為には、プロジェクト開始から実装、テスト、そしてデプロイメントを通じて、セキュリティを考慮に入れる必要がある。 デバイスはすでにわかっている重大な脆弱性に対応する為に、最新のソフトウェアをインストールして出荷、最初の立ち上げ時に自動的にアップデートをプッシュ、あるいはその両方が行われるべきである。	●
10. 全てのサービスおよびクラウドプロバイダーに対して、セキュリティおよびコンプライアンスリスクアセスメントを行う。 IoTリソースガイド https://otalliance.org/IoTを参照。	●
11. ソフトウェア、ファームウェア、ハードウェア、そしてサードパーティーソフトウェアのライブラリ（オープンソースモジュールとプラグインを含む）を含んだ「部品表」を作成し、維持する。これはデバイス、モバイル、クラウドサービスに適用され、報告された脆弱性を迅速に修正 する手助けになる。	◘
12. 操作の必要最低条件に対してデバイスを設計する。 例えば、USBポートあるいはメモリーカードスロットはデバイスの操作とインテナンスに必要な場合にのみ含まれるべきである。 不使用のポートとサービスは無効にすべきである。	●
ユーザーアクセスとクレデンシャル	
13. strong authenticationをデフォルト設定とし、ユニークな、システム作成の、あるいは使い捨てパスワードを提供する。あるいは代わりにSSL認証クレデンシャルを使用。 必要に応じて、管理者アクセスの為にユニークなパスワードの使用を必要とし、デバイスとサービス、またエ場出荷時設定へのリセットのそれぞれの影響を分けています。	●
14. IoTアプリケーションとサポートパスワード、ユーザーのパスワードが存在しない場合に多要素検証および認証（電子メールと電話等）を用いたクレデンシャルのリセットメカニズム、またはその両方の為に一般的に受け入れられているリカバリーのメカニズムを提供。	●
15.「ブルートフォース」、その他の悪意のあるログイン（自動化したログインボット等）、あるいはその両方から保護する為の策を講じ、相当な数のログインの失敗があった場合には、ユーザーとデバイスのサポートアカウントをロックあるいは無効にする。	●
16. ユーザーにパスワードリセットあるいは変更の通知をおくり、安全な認証、帯域外通知、あるいはその両方を使用する。	●

17. 認証クレデンシャルはユーザーパスワードを含むが（それだけに制限されない）、ソルト、ハッシュ、暗号化、あるいはそれら全てを採用するものとする。全ての保存されたクレデンシャルに適用され、不正アクセスやブルートフォース攻撃の防御に役つ。	●
プライバシー、開示と透明性	
18. 購入、アクティブ化、ダウンロード、あるいは加入の前に、プライバシー、セキュリティ、そしてサポートポリシーが容易に見つけることができ、明確であり、レビューの為にすぐに入手できることを確証する。製品パッケージングとウェブサイトの目立つ場所に配置することに付け加え、企業がQRコード、わかりやすく短いURL、そして店舗での他の似たような方法を利用することを推奨。	●
18. セキュリティとパッチサポートの存続期間と終了を開示する。（製品保証期間を過ぎたもの。）従来の保証期間とは違って、サポートは2025年1月1日などの日没日に終了、あるいは購入日から特定の期間で終了する可能性がある。理想的にはそのような開示はデバイスの期待寿命に基づいているべきであり、購入前に消費者に知らせるべきである。 ***（IoTデバイスは無期限に安全、またはパッチを当てられるものではないと認識されている。使用可能な日を超過したデバイス使用のリスク、警告を無視、あるいはデバイスの使用をやめない場合の他人への影響とリスクを伝えることを検討する。）*** ユーザーによる料金支払いや年間サポート契約申し込みが必要な場合、購入前に開示すべきである。	●
20. 個人を特定できる、慎重に扱うべきデータのどのタイプと属性が収集され、どのように使用されるのかをはっきりと開示し、収集されたデータの機能と目的に合理的に役立つデータに限定して収集する。他の目的の為のオプトインを消費者に開示し提供する。	●
21. 接続性あるいはバックエンドサービスが無効、あるいは停止した場合に、どの機能がどのように機能しなくなるのかを開示する。物理的なセキュリティへの潜在的な影響を含むが、それだけに制限されるわけではない。デバイスがセキュリティアップデートを受信しなくなったとき、あるいはユーザーがデバイスのアップデートを失敗した場合に何がおこるのかも含む。*（潜在的な脅威を軽減する為に、接続性を無効にする、あるいはポートを無効にする機能を構築することを検討する。一方で、デバイスの使用を基に製品のコアの機能を維持し、潜在的な寿命あるいは安全問題のバランスを保つ。）*	●
22. データリテンションポリシーと個人を特定できる情報の保存期間を開示する。	●
23. IoTデバイスは、最初にペアリング、オンボーディング、他のデバイス、プラットフォームあるいはサービスと接続する、またはそれら全てを行うとき、通知、ユーザー確認のリクエスト、またはその両方を行わなければならない。	●
24. IoTデバイス、製品あるいはサービスのオーナーシップとデータがトランスファーされる可能性がある場合は、その旨を開示し、どのように行うのかも開示する。（例：接続型家庭があたらしい所有者に売却される、あるいはフィットネストラッカーの販売。）	●
25. 消費者の積極的同意なしで消費者の個人データを第三者と共有してはいけない。製品の特徴の使用あるいはサービス運用に必要で、それらに限定した場合を除く。サードパーティーサービスプロバイダーも同じポリシーに従う。それらのデータへの守秘義務、いかなるデータ損失または漏洩インシデント、不正アクセス、またはその全てを含む。	●
26. コントロール、ドキュメンテーション、またはその両方を提供し、消費者が「工場出荷時設定」にリセットできる機能を含むIoTデバイスのプライバシープリファランスをレビュー、または編集できるようにする。	●

27. 買収側のプライバシーポリシーにより諸条件に重 大な 変更が生じないという条件のもと、最初にデータを収集したコアの事業の売却あるいは清算の従属部分でない限り、いかなる身元が確認できる消費者データを売却あるいは譲渡しないことを誓う。 さもなければ、通知を入手し、承諾を得なければならない。	●
28. 操作の前に提示されたプライバシーの慣行をレビューした後に消費者が製品を無償で返品できるようにする。そのような諸条件が購入前にはっきりと開示されなかった場合のみとする。 返品期間（日数）は小売業者の現在の、あるいは前もって特定された交換ポリシーと一致しなければならない。	●
29. いかなるポリシーを拒否する、あるいは参加しない機会を提示するときはいつでも、それによる影響を明確に、また客観的に説明しなければならない。これは製品の特徴あるいは機能へのすべての影響を含む。参加によるエンドユーザーへの有用性、データの共有、またはその両方をエンドユーザーに伝えることが望ましい。	●
30. 適用される規制に準拠する。これには児童オンラインプライバシー保護法（COPPA）、国際プライバシー、セキュリティ、そしてデータ転送法的規制が含まれるが、これらに制限されるわけではない。[3] [4]	●
31. 重大なプライバシーに関する通知の変更の履歴は、最低2年間は公的に提示する。 ベストプラクティスにはデータサンプリング、変更箇所への印、そして変更による影響の概要が含まれる。	●
32. デバイスの使用中止、紛失あるいは売却において、企業のサーバーに保存されている個人あるいは慎重に扱うべきデータ（購入履歴を除く）を、ユーザーまたは代理人が、削除あるいは匿名にすることができるようにする。	o
33. デバイスとアプリケーションを工場出荷時設定にリセットできるようにする。譲渡、レンタル、紛失あるいは売却の場合にユーザーデータを消去するようにもする。	o
通知と関連するベストプラクティス	
34. エンドユーザーのコミュニケーションには電子メールおよびSMSが含まれるが（これらに制限されるわけではない）、スピアフィッシングやスプーフィングを防ぐ為に、認証プロトコルを導入しなければならない。ドメインは全てのセキュリティ、プライバシー関連のコミュニケーション、そして通知、またパークドメインと電子メールを送信しないドメインも同様に、SPF、DKIMおよびDMARCを実装すべきである。[5]	●
35. 電子メールでのコミュニケーションにおいて、DMARCポリシーをパブリッシュした180日以内に、リジェクトあるいは隔離ポリシーを実行する。これによりISPと受信側ネットワークが電子メー認証検証チェックを通らなかった電子メールを拒絶することができる。[6]	o
36. 電子メールでのコミュニケーションを利用するIoTベンダーはトランスポートレベルの機密性を採用すべきである。安全なコミュニケーションと、メッセージのプライバシーとインテグリティの強化に役立つ一般的に受け入れられているセキュリティ技術を含む（「Opportunistic TLS」とも呼ばれている）。[7]	o
37. デバイスのいかなる物理的改ざんを防ぐ、あるいはそれがはっきりとわかるようにする方法を実行する。 このような方法は、インストー ル後に悪質な目的にさらされ、または変更されることを防ぎ、あるいは危殆化した状態で小売業者へ返却されることを防ぐために役立つ。	o

38. 視覚障害、聴覚障害、運動障害、またはそのすべてをもつユーザーの為に、全ての物理的機能へのアクセスを最大化するアクセス要件に対応する方法を考慮する。	o
39. あらゆる潜在的セキュリティまたはプライバシー問題、生産終了通知、そして製品リコールの可能性に関するユーザー認識を最大化する為のコミュニケーションプロセスを開発する。アプリ内通知も含む。コミュニケーションは一般ユーザーの読解力レベルにおいて理解を最大にするために文書でおこなわれるべきである。 多国語でのコミュニケーションを考慮し、英語はユーザーにとって「第二言語」の可能性があることを認識する（セキュリティとメッセージインテグリティの関連原則を参照）。	●
40. 侵害とサイバーの対応と消費者通知計画を定め、少なくとも年に1回、あるいは重大な内部システム、技術的、または操作上の変更が合った後、またはその両方で、再評価、テスト、あるいはアップデートを行う。	●

リソースとアップデートはhttps://otalliance.org/IoTで御覧になれます。

用語、定義、そして説明

1. スコープ -「ウェアラブルテクノロジーを含む、家庭用及び企業用の「消費者向け」デバイスおよびサービス」に重点を置いています。 自律自動車、自動運転車、または医療デバイスとHIPPAデータを含む、スマートカー[8]はフレームワークのスコープ外である一方で、基準の大部分は適用されるとみなされている。 それぞれが幹線道路交通安全局（NHTSA）と食品医薬品局（FDA）の規制的監視下にある。[9]
2. デバイス製造業者、ベンダー、アプリケーション開発者、サービスプロバイダーおよびプラットフォームオペレータの用語は全て「企業」と表示されている。
3. 企業は法執行機関とデータを共有する場合は開示し、法的に許された、適用する透明性レポートに言及することを期待されている。
4. スマートデバイスとはネットワークにつながっており、一方向のコミュニケーションのみの場合があるデバイス（そしてセンサー）のことである。

[1] https://otalliance.org/resources/always-ssl-aossl

[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures

[3] 企業、製品、そしてサービスは個人的で慎重に扱うべき情報の収集と扱いを統治する管轄のあらゆる法律と規制に準拠しなければならない。これはEU-US Privacy Shield Framework www.commerce.gov/privacyshield 、EU一般データ保護規則 (GDPR) www.eugdpr.org 、またはその両方に従うことを含むが、それらに制限はされるわけではない。遵守を怠った場合はこのフレームワークにも準拠していないことになる可能性がある。

[4] 児童オンラインプライバシー保護法（COPPA） https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[5] 電子メール認証 - https://otalliance.org/eauth

[6] DMARC -https://otalliance.org/resources/dmarc

[7] 電子メールのTLS暗号化 - https://otalliance.org/best-practices/transport-layered-security-tls-email

[8] U.S. 米連邦厚生省, Health Information Privacy http://www.hhs.gov/hipaa/index.html

[9] http://www.nhtsa.gov/Vehicle+Safety と http://www.fda.gov/MedicalDevices/default.htm

---

OTAは Internet Society (ISOC)内のイニシアチブ、501c3（IRSコード）の 慈善非営利団体で、世界中の全ての人々が恩恵を受ける為に、オープンな開発、進化、そしてインターネットの使用の促進を目的としています。 OTAの目的はオンラインへの信頼、ユーザーへの権限委譲、マルチステークホルダーのイニシアチブを集結したイノベーションの向上であり、ベストプラクティスを開発また奨励し、プライバシー慣行とデータの監督と報告の責務を担うことです。 さらに詳しい情報は https://otalliance.org を https://www.internetsociety.orgを御覧ください。

R1014