脆弱性対処に向けた
製品開発者向けガイド

独立行政法人情報処理推進機構
セキュリティセンター

2020 年 8 月

目次

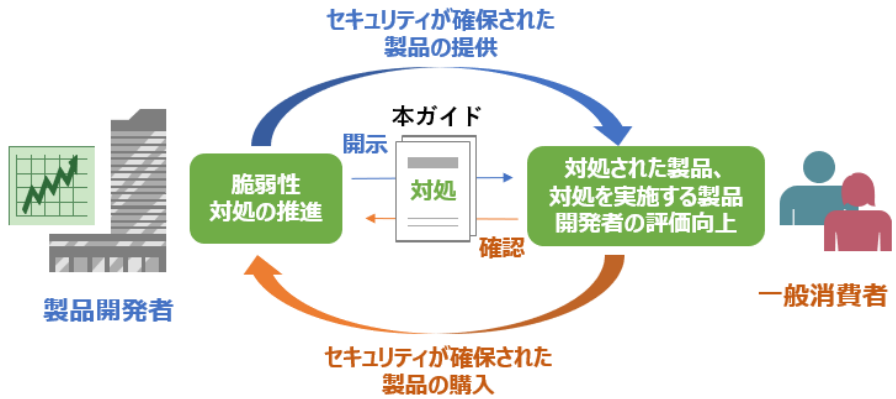
エクゼクティブサマリ

近年、ネットワーク家電等、様々な機器がネットワークに接続され、様々な情報が活用できる環境が実現されていますが、このような環境では、ネットワークを通じて製品の脆弱性が悪用され、個人情報や重要情報の流出といったインシデントが発生する可能性もあります。

脆弱性への対処（以降、脆弱性対処）については実施事項が多く、特に**リソースに限りのある製品開発者にとってはどれから着手してよいのかの判断に迷う**という課題があります。本ガイドでは、製品開発者が実施すべき対処について文献調査をもとに**重要と思われる 12 項目**をまとめました。**実施すべき対処について段階的に示して**いますので、可能なところから実施することができます。

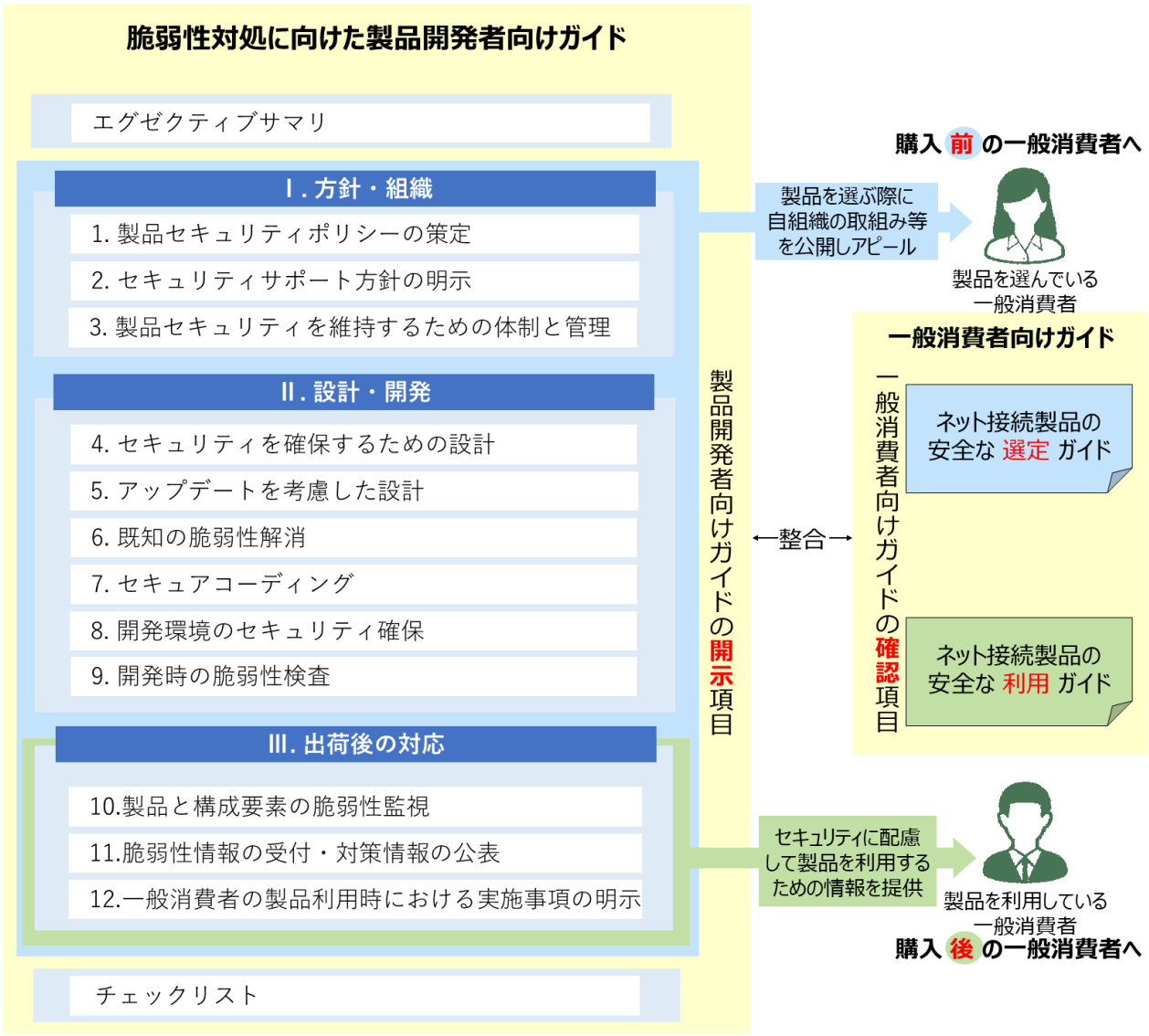
また、製品開発者が実施する**脆弱性対処は製品開発者が脆弱性対策にどのように取り組んでいるかが一般消費者からは分からないため、一般消費者からの製品評価向上、製品選定の優位性（顧客獲得及び売上等）になりづらい**状況です。本ガイドでは、製品開発者が実施している脆弱性対処を一般消費者に伝えるため、実施内容の開示方法も併せて掲載しています。「製品開発者が実施・開示すべきとした項目」と、同時に開示している一般消費者向けのガイドで「一般消費者が確認・実施すべきとした項目」は整合性を取っており、**本ガイドに沿って製品開発者が実施した対処を開示することで、一般消費者が対処状況を容易に確認することが可能**となります。

これにより、顧客の安全に考慮している製品の評価の向上、製品開発者への信頼につながり、**セキュリティが確保された製品も市場原理として適い、普及することを期待**します。



図：脆弱性対処状況の開示と確認による
セキュリティが確保された製品の普及

本ガイドを参考に、組織の脆弱性対処を検討及び推進してください。



図：本ガイドの構成

概要

背景

近年、ネットワーク家電等、様々な機器がネットワークに接続され、様々な情報が活用できる環境が実現されています。このような環境は、一般消費者にとって便利である一方、ネットワークを通じて製品の脆弱性が悪用され、個人情報や重要情報の流出といったインシデントが発生する可能性もあります。

ネットワークに接続する製品に関して、製品開発者が脆弱性対処を実施していたとしても、その組織努力は一般消費者からは見えないため、一般消費者からの製品評価向上、製品選定の優位性（顧客獲得及び売上等）になりづらい状況です。このため、製品開発者が実施している脆弱性対処を積極的に開示しアピールすることで、顧客の安全に考慮していない製品開発者及び製品との差別化を実現し、ひいては顧客の安全に考慮している製品の評価の向上、製品開発者への信頼につながる仕組みを構築することで、市場原理としてセキュリティが確保された製品が普及することを期待します。

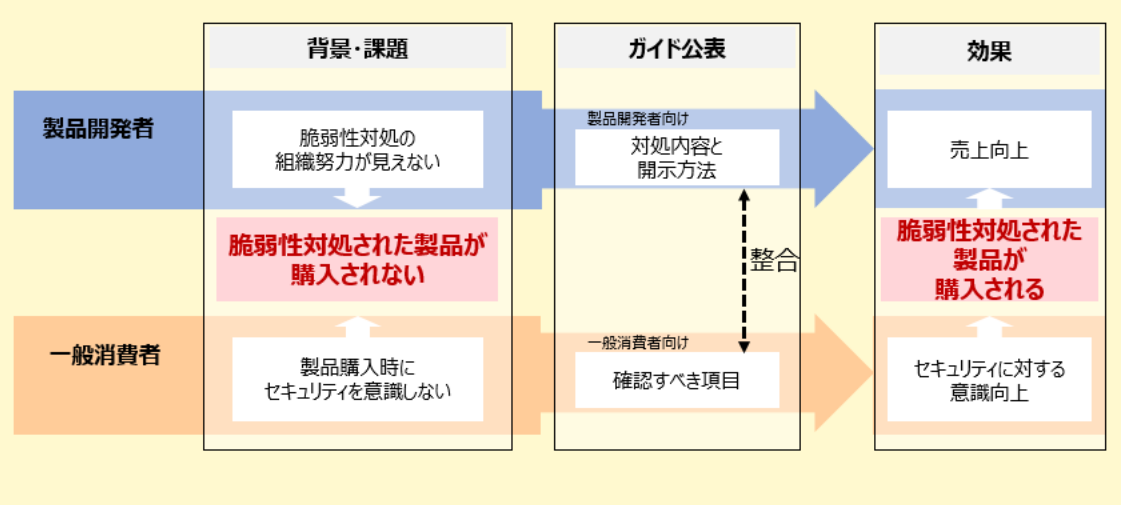
本ガイドについて

本ガイドでは、**製品開発者において実施すべき脆弱性対処と、その開示方法を掲載**しています。**実施すべき対処は段階的に示して**いるため、リソースに限りのある製品開発者においても、可能なところから実施できるように構成しています。

なお、本ガイドに合わせて、一般消費者に対して、製品開発者が開示した対処を踏まえて安全な製品を選定し、さらに購入後も適切に利用されることを目的として、以下 2 つのガイドを開示しています。

- 一般消費者が安全な製品を選定するためのガイド
  「ネット接続製品の安全な選定ガイド」
- 一般消費者が購入した製品を安全に利用するためのガイド
  「ネット接続製品の安全な利用ガイド」

本ガイドにおいて製品開発者が実施・開示すべきとした項目と、一般消費者向けのガイドで確認・実施すべきとした項目は整合性を取っており、本ガイドに沿って製品開発者が実施した対処を開示することで、一般消費者が対処状況を容易に確認することが可能となります。開示によって対策を実施していることを示すことは、組織を守ることにもつながることに加え、一般消費者に対して、製品開発者によって開示された情報の確認を促すことで、以下に示したような効果が得られると期待できます。



図：ガイド活用により期待される効果

対象製品

本ガイドの対象製品は、主に一般消費者が利用するようなインターネットやホームネットワーク等のネットワークに接続する以下のような機器を想定しています。

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

ただし、工場・プラント等で利用されるような制御機器（PLC（Programmable Logic Controller）、シーケンサ等）については対象外とします。

想定読者

対象製品の開発を行う事業者（主に中小規模）を対象とします。

本ガイドの構成

「Ⅰ.方針・組織」、「Ⅱ.設計・開発」、「Ⅲ.出荷後の対応」という 3 つの大項目に分類し、製品開発者が実施すべき望ましい脆弱性対処の 12 項目を示しました。

各項目の内容は以下のように「意義」「実施内容」「開示方法」の構成となっています。

■ 意義

対策を実施する必要性やメリット、実施しない場合に想定される影響等を記載しています。

■ 実施内容

具体的な実施内容について記述しています。項目によっては実施内容を最大 3 段階にレベル分けしているため、組織の状況に合わせて可能なレベルから実施し、徐々にレベルを高めることができます。「実施することが理想的な事項」をレベル 3 としており、その実施が困難な場合はレベル 2 を、それも難しい場合はレベル 1 の記載事項を参照してください。

レベル 1　　：最低限実施すべき事項
レベル 2　　：実施することが望ましい事項
レベル 3(※)：実施することが理想的な事項
（※）「7 セキュアコーディング」の「実施することが理想的な事項」はレベル 2

レベル分けしていない事項は、「実施することが望ましい事項」、あるいは実施対象となる製品の性質や機能に応じて内容を取捨選択する必要があるものです。自組織の製品の機能や性質、自組織のリソースを考慮し、実施内容を選択してください。

■ 開示方法

組織の脆弱性対処の取組み状況を一般消費者に理解してもらうために、開示する情報とその例について説明しています。

一般消費者が製品を選ぶ際に必要な情報は、購入前も確認できるようパッケージ及びウェブサイト等の容易に確認できる場所に記載します。

記載内容によっては、インシデント等が発生した場合に責任を問われる等のリスクもあるため、開示内容や記載内容については、広報や法務など組織内の関連部門とも相談してください。全ての内容を開示することが必須ではありません。

なお、本ガイドに記載した脆弱性関連情報に関する取扱いについては「情報セキュリティ早期警戒パートナーシップガイドライン」に則っています。

【情報セキュリティ早期警戒パートナーシップ】
「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）の告示を踏まえ、国内におけるソフトウェア製品等の脆弱性関連情報を適切に流通させるために作られている枠組み

活用方法

本ガイドの活用方法としては、例えば以下のように活用方法があります。

- 製品開発者がセキュリティ対策として実施すべき項目を把握できる
- 実施する対処を徐々にレベルアップできる
- 一般消費者に自組織の取組み状況をアピールするため、すべきことを把握できる

また、本ガイドの最後に対処状況を確認するためのチェックリストを付けています。チェックリストは、例えば以下のように活用できます。

- 組織の製品開発プロジェクトマネージャーが現状と課題を把握し、上長に報告
- 部品メーカー等に発注する際、発注する部品のセキュリティレベルを確認・把握するために活用
- 委託先の脆弱性対処の状況確認に活用

Ⅰ. 方針・組織

1 製品セキュリティポリシーの策定

意義

製品セキュリティを確保するための組織の取り組み姿勢や実施事項について内外に理解を促すために、製品セキュリティポリシーを策定し、開示します。組織の製品セキュリティポリシーを策定しない場合は、組織内でのセキュリティに関する意識が高まらず、守るべき事項や対策を明確にしないことで対策が統一的に実施されない恐れがあります。その場合、脆弱性対処に取り組んだ成果が出ていたとしても、統一的に実施されないことで作り込まれた脆弱性により、組織として許容できないインシデントなどのリスクが生じかねません。また、製品セキュリティに対する組織の姿勢を対外的に示すことで、社会的評価を高めることが期待できます。

実施内容

製品セキュリティポリシーは組織の取り組み姿勢や実施事項を表すため、経営層の意向や自組織の製品の特性を踏まえて策定し、経営層の承認を得て組織内に周知するとともに組織外に開示します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順
① **組織として製品セキュリティポリシー策定の意思決定** 組織として製品セキュリティポリシーを策定するにあたっては、まず経営層も含めた意思決定、製品セキュリティポリシー策定の体制作り、予算確保等を行います。製品セキュリティポリシーは組織としての製品セキュリティの方針・考え方を表明するものであるため、策定にあたっては経営層の意向を確認します。 ② **製品セキュリティポリシー案の作成** 経営層の意向や法令、ガイド等を踏まえて、組織面、技術面でのセキュリティ対策等を盛り込んだポリシー案を作成します。また、製品セキュリティとして製品の利用環境等で考慮すべき点がある場合は、それも含めて作成します。 なお、製品セキュリティポリシーは組織外に開示するため、法務部門や広報部門等、対外的な対応を行う部門の確認を得ることも重要です。 ③ **経営層による承認** 経営層に作成した製品セキュリティポリシーの承認を得ます。

④ **組織内への周知、組織外への開示**

承認された製品セキュリティポリシーに沿った統一的な対策が組織内で実施されるように、具体的な製品セキュリティの実施事項も作成します。

その後、組織内のセキュリティに関する意識を高めるとともに、策定した製品セキュリティポリシーに沿った活動が行われるように、教育等により組織内への周知を図ります。また、組織外に策定した製品セキュリティポリシーを開示します。開示については、「開示方法」を参照してください。

製品セキュリティポリシーは策定するだけでなく、決められたことが適切に実行されているかを確認し、実行されない場合は是正していくことが重要です。また、製品セキュリティポリシーに関係する法令やガイド等の改定や製品セキュリティへの社会的な要求事項の変化等があった場合、製品セキュリティポリシーを見直すことも必要です。

上記の実施内容はレベル 3 をベースにしています。これらの項目の対応が難しい場合は、以下に記載している他のレベルの実施内容を参照し対応を検討してください。

レベル	実施内容
1	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定します。
2	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定し、外部に開示します。
3	製品セキュリティに関する方針・考え方に加え、実施事項を含めて製品セキュリティポリシーとして策定し、外部に開示します。

開示方法

- 製品セキュリティポリシーを定め、一般消費者に対してウェブサイトのポリシーページで開示します。
  - 実際の開示事例での開示場所は、CSR のように組織の社会的責任の説明項目の一環として開示する場合や、品質・調達等の方針と共に開示する場合等、様々な場所があります。また、開示する文書にはポリシーだけではなく、ガイドラインや指針など様々な形態があり得ます。
- 各項目の開示内容は抽象的でも、より具体的でも構いません。具体的に記載する場合は、ホワイトペーパー等に記載する方法もあります。

具体的な製品セキュリティポリシーの例を以下に示します。示した開示例は「ひな型」ではないので、組織の実施状況等を踏まえた内容を記載ください。

【開示例（レベル 3）】

製品セキュリティポリシー

当社は、製品セキュリティレベル維持及び改善を含めた活動を継続的に実施し、お客様に安全性の高い製品を提供します。

(1)組織的対策

当社では、全社的な方針の下、製品セキュリティを確保する体制を整備し、セキュリティ対策を実施します。また、国内外のガイド等に基づいた製品セキュリティ対策基準を策定し、これに基づいた製品のセキュリティ設計・開発を行います。

(2)技術的対策

当社では、製品の出荷前に脆弱性検査を実施し、製品に脆弱性が含まれないように努めます。また、出荷後も、自社製品の脆弱性に関する情報を収集し、発見された脆弱性が、お客様への被害や製品性能に影響を及ぼす可能性があると判断した場合には、アップデートや対策ソフトウェアの提供等、当社が必要と判断した対応策等、適切な情報を提供します。

(3)情報の提供

セキュリティレベルの維持は、適切なセキュリティ対策を行った当社製品をお客様が適切に利用することで実現できます。当社は、セキュリティに関する注意喚起やセキュリティを確保した上で製品を利用するための情報等を提供します。

【開示例（レベル 2 の場合の例）】

製品セキュリティに関する方針

当社では、以下の方針の下、製品セキュリティの確保に取り組みます。

1. 製品セキュリティを確保するための体制を整備します。
2. セキュリティを考慮した設計・開発を行い、製品出荷前は、脆弱性検査により脆弱性の解消に努めます。
3. 製品出荷後も脆弱性情報を広く収集し、リスクがあると判断した場合は迅速に対応を行います。
4. セキュリティに関する情報や対策方法を利用者の皆様に提供します。

2 セキュリティサポート方針の明示

意義

いつまで新規に発見された脆弱性のサポートをするのかを一般消費者に伝えるため、製品ごとにセキュリティサポート方針を定め、開示します。セキュリティサポート方針を示さないと、出荷した製品に対して一般消費者が長期のセキュリティサポートを期待することになります。その結果、製品提供期間や体制等の理由から脆弱性に対応できずインシデント等が発生した場合、一般消費者から苦情を受け、ひいては社会的責任を問われることになりかねません。セキュリティサポート方針を示すことで、一般消費者に対しサポート期間中は安心して製品を利用できることを示せるとともに、サポート終了のタイミングに合わせて後継製品に切り替えることを促す等の対応ができます。

実施内容

製品出荷後の脆弱性対処を考慮し、セキュリティサポート方針を定め、必要な体制を整備します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

① セキュリティサポート方針策定の意思決定

セキュリティサポート方針は製品セキュリティサポートへの対応方針やサポート期間を示すため、策定にあたっては、経営層も含めた意思決定を行います。

② セキュリティサポート方針案の作成

セキュリティサポート方針案は、以下の点に留意して作成します。また、セキュリティサポート方針は組織外に開示するため、法務部門や広報部門等、対外的な対応を行う部門の確認を得ることも重要です。

- 製品の構成要素(コンポーネント、ライブラリ等)や OS 等のサポート期間も影響するため、サプライチェーンを含めた製品のサポート期間を考慮します。
- 製品の企画や設計段階から検討します。
- ソフトウェア製品の場合、セキュリティサポート終了後は、使用中止や後継製品への移行を一般消費者に呼びかけます（ハードウェア製品の場合は、ネットワークに接続せずに使用する等の利用も可能です）。

セキュリティサポート期間は、以下の点を考慮して定めます。

- 製品出荷後の機能拡張・機能追加に関する計画の方針や期間
- 製品の販売期間とその後のサポート方針（サポートするか否か、する場合でも無償か有償か等）
- 開発部門及び品質管理部門等の関係部門が動作確認や脆弱性検査、対策策定が可能な期間
- 開発環境や言語もしくは外部から組み込んだソフトウェア/製品に関する脆弱性監視（サポート状況の監視を含む）が可能な期間

・ 外部から組み込んだソフトウェア/製品のサポート期間
  - 外部に委託して開発した、もしくは有償のコンポーネント・ライブラリ等
  - サポート期間や対応が予め明確でない製品のサポート終了時もしくはセキュリティ修正対応がされない製品（継続利用するか否か。継続利用する場合は、発見された脆弱性へ対処する必要があります）

③ 経営層による承認

経営層に作成したセキュリティサポート方針の承認を得ます。あわせて、セキュリティサポートに取り組むために必要な予算の確保、体制や人材の整備を行います。

④ 組織外への開示

一般消費者が製品の利用停止や後継製品への買い替え等の判断ができるように、策定したセキュリティサポート方針を開示します。開示については、「開示方法」を参照してください。

セキュリティサポート方針は、継続的な状況把握や見直しを行うことも必要です。また、製品販売を委託する代理店等との調整が必要になることもあります。

上記の実施内容はレベル 3 をベースにしています。これらの項目の対応が難しい場合は、以下に記載している他のレベルの実施内容を参照し対応を検討してください。

レベル	実施内容
1	製品出荷後に、サポートできなくなったタイミングでサポート終了としてその旨を開示します。
2	組織内で企画・設計段階からサポート期間を定め、遅くともサポート終了時までにサポート終了を開示します。
3	組織内で企画・設計段階からサポート期間を定め、セキュリティサポート方針として出荷時に開示します。

開示方法

- 一般消費者にサポートが可能な期間を伝えるため、セキュリティサポート方針として製品セキュリティサポート期間について製品情報を掲載しているウェブサイト等で開示します。
  - 実際の開示事例では、セキュリティサポート方針として開示している場合や、製品の（セキュリティに限らない一般的な）サポート方針と共にセキュリティサポート方針を記載している場合があります。
- セキュリティサポート終了後は、一般消費者に対し、製品の使用中止や後継製品への移行を促す旨も記載します。

【開示例（レベル 3）】

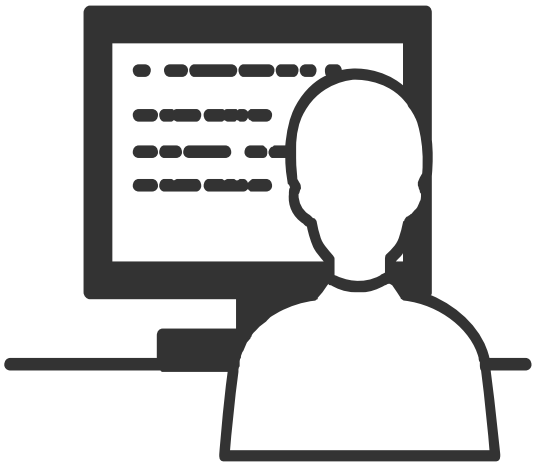
セキュリティサポート期間

弊社が提供する製品のセキュリティサポート期間は以下のとおりです。

バージョン	セキュリティサポート状況	セキュリティサポート期間		留意事項
		リリース日	終了日	
V3.0、3.1	サポート中	2019.x.x	V4 リリース日	–
V2.0	サポート終了	2015.x.x	2020.x.x	最新バージョンにバージョンアップしてください。バージョンアップ方法は[こちら]
V1.0	サポート終了	2010.x.x	2015.x.x	

メジャーバージョンアップのリリース計画

V4 は 2022.x.x にリリース予定



3 製品セキュリティを維持するための体制と管理

意義

製品セキュリティを維持するために、組織内の様々な部門間だけでなくサプライチェーンや脆弱性情報の提供組織等の外部組織も含め、連携した体制を構築し、製品セキュリティを管理する必要があります。製品セキュリティを維持する体制が整備できない場合は、製品セキュリティポリシーで定めた守るべき事項や対処が適切に実施できない、必要な情報が外部組織から入手できない等、製品セキュリティを維持することが困難になります。製品セキュリティを維持する体制を構築し、設計・開発段階から製品出荷後までセキュリティを管理することで、セキュリティが確保された製品を出荷することが可能となり、製品出荷後に発見された脆弱性やインシデントに迅速に対応することができます。

実施内容

製品セキュリティポリシーに基づき組織として実施すると定めたセキュリティ対処について、必要な体制を整備します。体制には、自組織内の部門はもちろん、外部組織も含みます。また、「方針決定」「設計開発」「出荷後の対応」に必要な『平時の体制』だけでなく、外部から脆弱性報告の受領時や未修正の脆弱性が開示もしくは悪用された場合などの『緊急時の体制』についても、製品セキュリティポリシーを策定した際に整備しておく必要があります。なお、製品に関する緊急時の体制のことを PSIRT（Product Security Incident Response Team）[1]と言います。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順
① 関係者の洗い出し 製品セキュリティポリシーに規定したセキュリティ対処を実施するために必要な関係者（自組織の関係部門及び外部関係者）を洗い出します。自組織で実施が難しいセキュリティ対処項目は、委託することも検討してください 。自組織の関係部門は下記の図を参照してください。 **② 役割の明確化・手順書策定** 自組織の部門及び外部組織の役割を明確化します。自組織の部門が確実にその役割を実施できるように手順書を策定します。

[1] PSIRT Services Framework 1.0 日本語版（一般社団法人コンピュータソフトウェア協会、JPCERT/CC）
https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.0_jp.pdf

③ 周知・教育・訓練

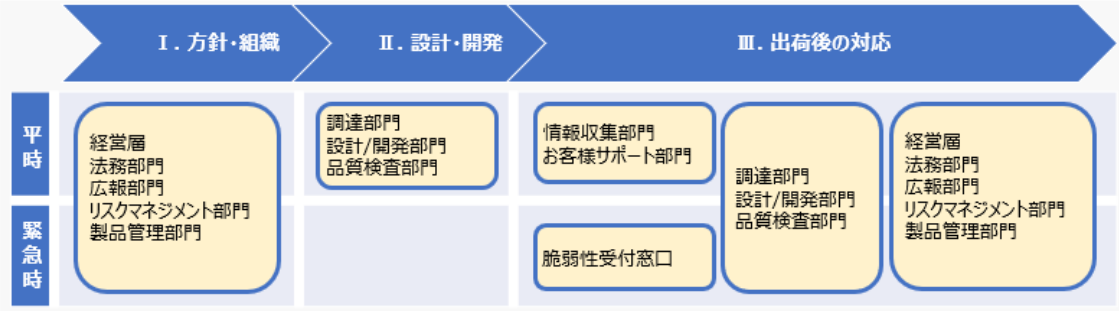
策定した製品セキュリティポリシー及び手順書は関連する自組織の部門に周知・教育を行います。周知・教育は、策定時だけでなく変更時も実施します。また、緊急時には迅速な対応が実施できるように、定期的に訓練を実施することが望まれます。

なお、セキュリティの問合せに対する誤った回答は利用者が被害を受けるだけでなく、組織や製品に対する評価低下や信頼喪失に繋がる恐れがあるため、窓口担当者だけで対応せず開発部門等に事前に確認・相談のうえ回答するように周知することが重要です。

④ 監査・見直し

手順書に則り実施されていることを定期的に監査します。また、ポリシーや手順書の内容は定期的に見直しを行います。

体制整備には、様々な部門の理解と協力及びこの体制を確保するための予算が必要です。このため、経営層による強いリーダーシップ及び支援が必要不可欠です。



図：自組織の関連部門

外部関係者も含め、連携が必要となる関係者と役割については、「附属 主要な関係者・役割表」を参照してください。

開示方法

- 外部からの問合せや脆弱性報告を受け付けるために、一般消費者及び脆弱性発見者からの問合せ窓口を設置し、ウェブなどで告知しておきます。一般消費者向けの問合せ窓口（電話、メールアドレス等）は、製品を開封しなくてもわかるウェブサイトの製品ページや製品パッケージ等、容易に確認可能な場所に記載します。
- 製品セキュリティを維持するための体制を構築していることを製品セキュリティポリシーに含め開示します。

- 脆弱性情報の受付など、積極的に脆弱性対処を実施していることを関係者にアピールするため、緊急時の体制(PSIRT)に関する説明や体制図等を自組織のウェブサイト等で開示する場合もあります。

【開示例（問合せ窓口）】

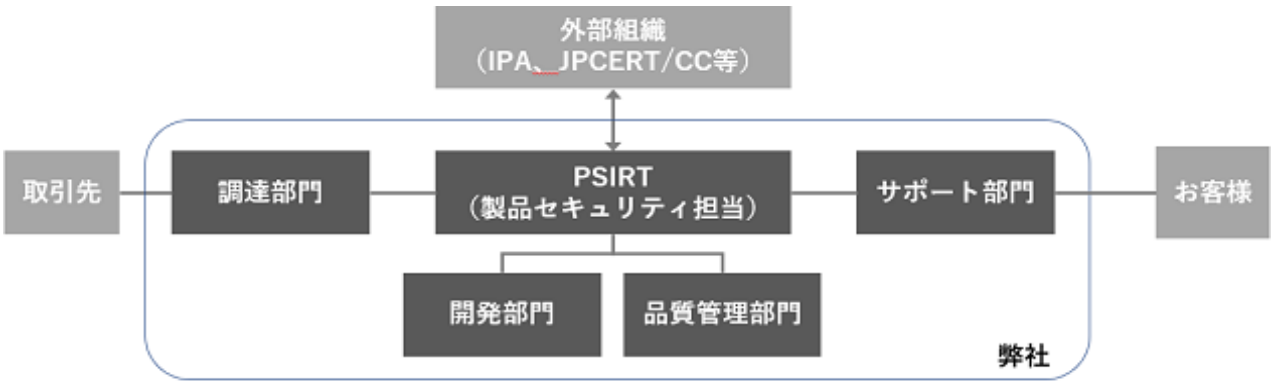
サポートに関するお問合せ

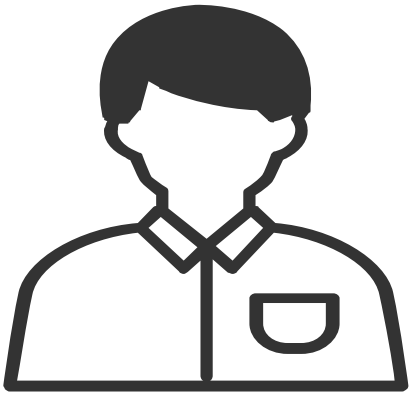
電話：0120-XXX-XXX　**メールでのお問合せ** 

（9:00-18:00　平日）　**（フォームが開きます）**

【開示例（体制）】

製品セキュリティ体制





II. 設計・開発

4 セキュリティを確保するための設計

意義

製品自体にセキュリティ機能を搭載するためには、設計段階からセキュリティ機能を検討する必要があります。設計段階から製品のセキュリティ機能を考慮しておかないと、後工程で機能追加ができない場合、製品利用時の脅威が残存してしまうことになります。また、追加できたとしてもコストが増え、開発スケジュールが遅延する等の問題が発生することになります。機能搭載の検討にあたっては、製品の利用用途等を想定したリスク分析の結果を踏まえる必要があります。この分析をしないと、必要な機能が漏れる可能性があります。設計段階からセキュリティ機能を搭載することで、製品の開発工程全体のコストを抑える効果があります。

実施内容

リスク分析などを行い、分析結果をもとに必要となるセキュリティ機能を搭載します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順
① 保護すべき機能と情報の特定 自組織の製品において守るべき対象を洗い出します。コンテンツやデータ、制御機能の動作や通信も保護対象です。 **② 脅威の特定** 上記①で保護すべき機能や情報に対するサイバー攻撃による脅威を想定します。以下の表「主な脅威と対応するセキュリティ機能例」を参考にしてください。 **③ リスクアセスメント** 想定した脅威の発生頻度や想定被害から保護すべき機能や情報に対するリスクを算定し、受容するか対策が必要かを評価します。 **④ 搭載するセキュリティ機能の検討** 上記③の結果、受容できない脅威があればセキュリティ対策技術を検討します。適用可能な技術（製品に搭載する機能）は複数あるため、コストや効果、導入難易度などを考慮して選定します。

上記実施内容については、「IoT 開発におけるセキュリティ設計の手引き[2]」を参照ください。

[2] IoT 開発におけるセキュリティ設計の手引き（IPA）https://www.ipa.go.jp/security/iot/iotguide.html

要件定義や設計の段階において、上記の分析・評価を実施し、セキュリティを確保する機能を検討します。リスク分析の結果を踏まえ、搭載する機能を選択してください。

表：主な脅威と対応するセキュリティ機能例

対応する主な脅威	セキュリティ機能
機器に保存されるデータや設定情報の漏えい	初期化機能
通信データの傍受や改ざん	暗号通信機能
機器に対する不正アクセス	インシデント検知機能、ログ出力機能
機器のマルウェア感染等によるデータ消失	バックアップ機能
運用段階で検出された脆弱性	アップデート機能

上記機能の詳細については、「IoT 開発におけるセキュリティ設計の手引き」を参照ください。

セキュリティ機能を搭載する際に、初期設定値（デフォルト値）が安全な設定になっているよう配慮しておくことも重要です。

なお、悪意のある第三者による製品への不正侵入、不正操作等により製品が誤動作をした場合に、誤動作によって製品利用者に危害を及ぼさないため、安全に製品を停止させる機能も考慮する必要があります。具体的な設計の考え方等については「IoT セキュリティガイドライン ver1.0 [3]」「つながる世界の開発指針 第 2 版[4]」を参照ください。

開示方法

- セキュリティを確保するための設計に関する取り組みを製品セキュリティポリシーに含め開示します。
- 一般消費者がセキュリティ機能を正しく利用できるように、製品に搭載しているセキュリティ機能の利用方法や設定内容については、取扱説明書や製品情報を掲載しているウェブサイト等に記載します。
- 一般消費者が製品を選ぶ際に、搭載しているセキュリティ機能（アップデート機能、初期化機能等）を、製品を開封しなくても確認できるよう、パッケージや製品情報を掲載しているウェブサイト等に記載します。EC サイトなど販売形態によってはパッケージの記載を確認できない場合が想定されるため、複数個所に記載することが望ましいです。

[3] IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省）
http://www.iotac.jp/wp-content/uploads/2016/01/03-IoT セキュリティガイドライン ver1.0 別紙 1 .pdf

[4] つながる世界の開発指針 第 2 版（IPA）https://www.ipa.go.jp/files/000060387.pdf

5 アップデートを考慮した設計

意義

製品出荷後に脆弱性が発見された場合に製品セキュリティを維持するため、脆弱性に対処したソフトウェアにアップデートできる機能を搭載する必要があります。製品にアップデート機能がなければ、発見された脆弱性に対処したソフトウェアが提供されたとしても適用することができません。対策がされていない脆弱性が悪用され、攻撃が発生した場合には、製品や製品開発者に対する一般消費者からの信頼を失うことになりかねません。また、修正のため製品回収が必要になった場合、想定外のコストが発生します。アップデート可能な仕様にしておくことで、製品が安全でない状態を放置せずに済みます。

実施内容

出荷後にも製品をアップデートできるよう、アップデート機能を設計します。アップデートは、製品への機能の搭載だけでなく、出荷後にもアップデートファイルを作成・頒布し、適用させるまでの仕組みを維持・運用することも重要です。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

下記①～②の検討を踏まえて、アップデート機能を設計します。

① 設計するアップデート方法の選定

対象機器におけるアップデートの提供方法を検討します。アップデート方法の種類及び対象例については、表「アップデートの種類」にまとめています。例えば、一般消費者が意識せずに自動的にアップデートされる仕様の場合、常に製品が最新の状態に保たれることが期待できます。一方で、アップデートすることで製品の動作が一時的に中断し、それによって製品の利用に影響が生じる場合には、アップデートのタイミングを一般消費者に選択させる設計を検討することも必要です。

アップデートの提供方法を検討する際には、以下の点を考慮します。

- 製品が提供する機能や想定する利用環境
- 利用者によるアップデートに係る作業負荷（容易性）
- 製品のネットワークへの接続頻度
- セキュリティ対応以外を目的としたアップデートの想定頻度
- アップデート機能搭載の費用対効果

また、アップデート方法に応じてメモリなどハードウェアの増強が必要になったり、オンラインでのアップデートであれば、アップデート配信用のサーバの構築及び運用管理も必要になったりします。アップデート方法を検討する際は、設計にともなう部品や設備等へのコストが発生する事も配慮して選定します。

② アップデート機能実装により発生する影響への対応

アップデート実施に関する処理の負荷や製品機能の停止時間などの影響を低減させる必要がある場合はその方法を検討します。例えば、アップデートによる帯域不足が生じる場合には、使用する帯域幅を制限した仕様とすれば未使用の帯域を確保できます。また、オンラインでのアップデート機能を採用する場合には、アップデートファイルの改ざんによるマルウェアの混入などを防ぐため、安全なアップデート方法を設計することが望まれます。具体的な内容は表「アップデート機能実装により発生する影響への対応」を参照してください。

アップデートの種類
■ 1. 製品が自動的に実施するアップデート オンラインの自動アップデート機能の提供を指します。一般消費者の負担にならず、アップデートの実施率を上げられるため、製品セキュリティの確保が容易です。一方、利用者がアップデートのタイミングを選べないため、アップデートによる製品動作への影響がある場合には、利用者が、自動でアップデートするか自身の判断でアップデートする（以下 2.）かを、設定等で選択できるようにすることが望まれます。 対象例 常時ネットワークに接続して利用する製品、更新が頻繁である製品
■ 2. 利用者が実施時期を選択するアップデート オンラインのアップデート機能の提供を指します。ユーザインタフェース上に、ポップアップや通知ランプの点滅等でアップデートがあることを通知し、適用を促します。 対象例 常時ネットワークに接続して利用する製品、利用者自身が更新適用の時期を判断する必要がある製品
■ 3. 利用者による手動のアップデート インターネット経由のアップデートファイル（パッチ・ファームウェア）の提供を指します。利用者がそれをダウンロードしアップデートを適用します。アップデート時に利用者が製品を操作する必要があるため、アップデートファイルの入手方法やその適用手順を利用者へわかりやすく説明、開示する必要があります。 対象例 利用時のネットワーク接続が頻繁ではない製品、ネットワークに接続していない状態でも製品の利用が可能な製品
■ 4. オフラインでのアップデート 製品開発者が製品設置場所に訪問する、または、利用者が製品を製品開発者に発送するなどして、ネットワークを経由しない方法で、製品開発者が製品を直接アップデートする方法を指します。訪問によるアップデートの場合は、USB メモリなどの外部記憶媒体を介してアップデートファイルを製品に適用します。オフラインでのアップデートの場合、来訪の対応や発送手続きなど利用者に作業が生じます。そのため、利用者が行う作業については予め周知する必要があります。また、利用者の作業負担があるため、アップデートの適用率が他の手法より低くなる可能性があります。 対象例 インターネットに常時接続していない製品、更新が頻繁ではない製品、アップデート機能の搭載コストが製品価格に見合わない製品

アップデートの種類を比較すると、オンラインのアップデート機能を製品へ実装することはオフラインでのアップデートよりもコストがかかるように見えます。しかし、オフラインでのアップデートの場合、配送費や訪問費が発生するため、長期的にはオフラインでのアップデートの方がかえってコストがかかります。また、一般消費者による適用率を上げるという観点でも、適用が容易なオンラインによるアップデートを採用することが望まれます。

表：アップデート機能実装による影響への対応

影響への対応手段	目的・効果
アップデート日時の設定や帯域制御を可能とする	アップデート中の性能低下・ネットワーク帯域不足の防止
自動的にアップデート前のバージョンに戻すことを可能とする（特に自動アップデートの場合）	アップデート後に動作しなくなる可能性の低減
通信の暗号化	アップデートファイルの改ざん防止
アップデートファイルのコード署名	
アップデートの状況確認機能	・アップデート状況・バージョン情報の確認を確認可能にする ・アップデート忘れの防止
製品の異常動作検知	不正な更新が行われた場合の検知
ウイルスチェック（特にオフラインでのアップデートの場合）	USB メモリなどを経由したアップデート時のウイルス混入（感染）防止

開示方法

- 一般消費者が製品を選ぶ際に、製品を開封しなくても容易に確認できるようアップデートの種類は、パッケージや製品情報を掲載しているウェブサイト等に開示します。
- 利用者がアップデートを正しく実施するために、アップデート方法を、取扱説明書や製品情報を掲載しているウェブサイト等で掲示します。
- ソフトウェア製品に対してアップデート機能を実装していることを製品セキュリティポリシー等に含め開示します。

6 既知の脆弱性解消

意義

製品の構成要素（コンポーネント、ライブラリ等）に存在する既知の脆弱性に対しては、攻撃手法や攻撃ツール等が開示されている場合があり、サイバー攻撃を受ける可能性が高いことから、既知の脆弱性は可能な限り解消する必要があります。製品に残存した既知の脆弱性の悪用により一般消費者がサイバー攻撃の被害を受けると、対処に多くの費用が必要となることに加え、攻撃された製品がサイバー攻撃の踏み台となり、利用者に限らず社会へ影響が拡大すれば、かかる費用も比例する可能性があります。大規模な被害となった場合、たとえ外部組織が開発した構成要素が原因でも、製品や製品開発者に対する評価の低下を引き起こすことにもなりかねません。製品の設計・開発時から、構成要素の脆弱性の有無を可能な限り確認、対応することで、出荷後に脆弱性による問題が発生するリスクを低減することが可能となります。

なお、製品の設計・開発時だけではなく、出荷後も脆弱性の監視を行う必要があります。出荷後の実施事項の詳細は、本ガイドの「10. 出荷後の脆弱性情報の収集と対応」を参照ください。

実施内容

構成管理を実施し、構成要素に含まれる脆弱性に関する情報収集を行い、必要な対処の判断と適用を実施します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

① 構成管理

すべての構成要素に関し構成管理を実施します。構成管理として記録すべき情報は、製品名、製品開発者名、バージョン情報等です。特に、バージョン情報がないと、脆弱性情報に対して該当製品か否かを判断できません。その結果、対処が遅れる可能性等があるため留意が必要です。構成管理を行う上でのポイントは以下の通りです。

- 委託開発したソフトウェアについては、そのソフトウェアの構成要素の情報を納品物に含むよう契約に明記します。
- 設計・開発工程（要件定義、設計、テスト）で製品に組み込む製品（コンポーネント）に変更が生じた場合は、随時記録します。また、製品リリース時に最新情報を運用部門へ展開できるようにします。

② 脆弱性に関する情報収集

構成要素毎に関連する製品開発者、公的機関及びセキュリティコミュニティ等から脆弱性情報（対策情報含む）を収集します。

脆弱性情報の収集・対応は、設計・開発フェーズの初期段階だけではなく、出荷直前まで定期的に実施します。

脆弱性情報及びその深刻度等の情報収集には、脆弱性対策情報のデータベースである JVN iPedia[5] を利用できます。

③ 必要な対処の判断と適用

脆弱性によって生じる被害とその大きさ、及びその発生の可能性からリスクを分析し、リスクの大きさにあわせて対応を検討し、対処します。

上記の実施内容は、レベル３をベースにしています。これらの項目の対応が難しい場合は、以下に記載している他のレベルの実施内容を参照し対応を検討してください。

レベル	実施内容
1	可能な範囲で構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、深刻度の高い脆弱性から対処を行います。深刻度については、共通脆弱性評価システム（CVSS）[6] や脅威指標等を参考にしてください。
2	すべての構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、深刻度の高い脆弱性から対処を行います。深刻度については、共通脆弱性評価システム（CVSS）や脅威指標等を参考にしてください。
3	すべての構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、製品に関連した脆弱性情報に関するリスク分析結果に応じて対処を行います。

脆弱性情報の収集と対処については「脆弱性対策の効果的な進め方（実践編）第 2 版 [7]」を参照ください。

開示方法

- 既知の脆弱性を解消する取り組みを製品セキュリティポリシー等に含め開示します。

[5] JVN iPedia https://jvndb.jvn.jp/

[6] 共通脆弱性評価システム CVSS v3 概説（IPA） https://www.ipa.go.jp/security/vuln/CVSSv3.html

[7] 脆弱性対策の効果的な進め方（実践編）第 2 版（IPA）https://www.ipa.go.jp/files/000071660.pdf

7 セキュアコーディング

意義

開発時に弱性を作り込まないようにするために、セキュリティに配慮したコーディング規約をもとに開発を行う必要があります。それを行わない場合、プログラムへのセキュリティ実装が開発者のスキルに依存することになり、組織あるいは製品のセキュリティレベルが安定しません。その結果、保守しづらくなるだけでなく、脆弱性が作り込まれる可能性が高まり、製品利用時の脅威が残存する可能性も高まります。

セキュリティに配慮したコーディング規約をもとにした開発を実施することで、プログラムの品質や保守性だけでなく、セキュリティを高めることが期待できます。

実施内容

セキュリティに考慮したコーディング規約を策定し、規約に則った実装が行われていることを確認します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

① **セキュアコーディング規約の策定**

セキュリティに配慮したコーディング規約を定めることが重要です。公表されているコーディング規約等[8] [9] [10] [11]を参照しつつ、組織に適したコーディング規約を定めます。コーディング規約には、例えば、重要情報（特定の動作環境等のリソース、例えばパスワードや IP アドレス、暗号化鍵等）をソースコードに埋め込むことを避け、重要情報をハードコーディングしないこと等も記載します。

② **教育**

策定したセキュアコーディング規約をプログラマに周知し、定期的に教育を実施します。

③ **実装**

策定したセキュアコーディング規約に則りコーディングを行います。

[8] セキュア・プログラミング講座（IPA）
https://www.ipa.go.jp/security/awareness/vendor/programming/index.html

[9] 安全なウェブサイトの作り方（IPA）https://www.ipa.go.jp/security/vuln/websecurity.html

[10] セキュアコーディング（JPCERT/CC）https://www.jpcert.or.jp/securecoding/

[11] SEC BOOKS: ESCR Ver.3.0:組込みソフトウェア開発向けコーディング作法ガイド［C 言語版］ESCR Ver.3.0（IPA）
https://www.ipa.go.jp/sec/publish/tn18-004.html

④ **レビュー担当者によるレビュー**

開発者本人がソースコードを見直すだけでなく、別の担当者が第三者の視点でレビューを行います。開発者本人がソースコードを見直すだけでなく、複数でレビューすることで、規約に則っていないコーディングの発見やコーディング規約についての認識のずれ等を解消でき、これにより脆弱性の作り込みの低減を期待できます。

⑤ **コーディング規約の更新**

新たな攻撃手法に対応するため、定期的に更新します。

上記の実施内容は、レベル 2 をベースにしています。これらの項目の対応が難しい場合は、レベル 1 の実施内容を参照し対応を検討してください。

レベル	実施内容
1	組織のコーディング規約を定めて、コーディングを実施します。
2	組織のコーディング規約を定めて、コーディングを実施し、別に定めたレビュー担当者がレビューします。

なお、開発時にオープンソースなどを利用すると、ソースコードが開示されているため開発にかかる時間が短縮されるメリットがあります。しかし、ソースコードが開示されているという特性上、脆弱性が存在した場合に攻撃者にそれを発見、特定されやすいです。よって、オープンソースなどを利用する場合にも、策定したセキュアコーディング規約にそったコーディングがされているかを確認し、対処する必要があります。

開示方法

- セキュリティを配慮したコーディング規約を策定し開発を行っている点を製品セキュリティポリシー等に含め開示します。
- 具体的に記載する場合は、ホワイトペーパー等に記載する方法もあります。

8 開発環境のセキュリティ確保

意義

開発にあたっては、ソフトウェア製品のセキュリティだけではなく、開発するための施設や環境、開発するために使うソフトウェアのセキュリティを確保することが重要です。開発環境に不正にアクセスされてしまうと、開発中のソフトウェア製品の情報が窃取、改ざんされる可能性があります。製品の開発に使うソフトウェアが改ざんされてしまうと、作成するソフトウェア製品にも脆弱性が作りこまれてしまうことが考えられます。また、開発時に使用していたテスト用の機能やアカウントの情報などが製品に残存していた場合、これらの情報が悪用される可能性があります。

安全にソフトウェアを開発するには、開発環境全体のセキュリティ確保が必要です。

実施内容

ソフトウェア製品の開発に関する情報を情報資産ととらえ、開発するための施設や環境へのセキュリティ対策を実施します。また、開発に使用するソフトウェア製品については、セキュリティが確保されているものを利用します。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

① 開発に使う施設・設備のセキュリティの確保

自組織の情報セキュリティポリシーや製品セキュリティポリシーに基づいて、開発に使用する施設・設備のセキュリティを確保します。開発に使用する施設・設備は、自組織で使う一般的な情報システムとは物理的にも論理的にも分離させておくことが望まれます。物理的な分離方法としては、執務フロア内にセキュリティ区画を設けて入退室管理を実施する方法があります。また論理的なものとしては、開発で使用するネットワークや開発用端末のアカウントや IP アドレスなどをもとにアクセス制限を実施する方法があります。また、開発に使用する端末では、マルウェアの感染による情報漏えいや改ざんを防止するため、業務目的での日常的なメールやインターネットブラウザの使用を制限することも検討します。

② 開発中のソフトウェア製品のソースコードや仕様書等のセキュリティの確保

開発中のソフトウェア製品のソースコードや仕様書などのソフトウェア製品に関連するドキュメントは、情報資産として、適切なアクセス制御のもと管理します。ソースコードは、改ざんの防止機能をもつバージョン管理システムやリポジトリを使うことで効率的に管理することができます。

また、テスト用に設けた特別な機能やアカウントの情報が記載されたドキュメントは、漏えいすると、攻撃が容易になる可能性があり、十分に注意する必要があります。

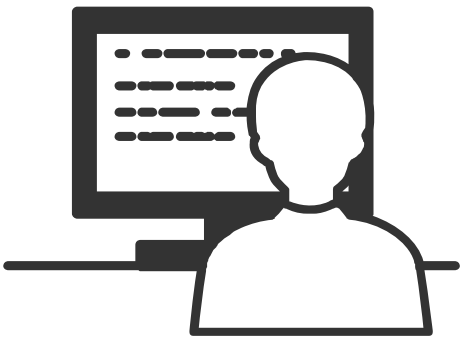
③ 開発に使用するソフトウェア製品セキュリティの確保

コンパイラやユーティリティソフトウェアにセキュリティ上の問題がある場合、それらのソフトウェア製品を使って開発したソフトウェア製品にも、脆弱性が作りこまれてしまう可能性があります。開発に使用するソフトウェア製品は、最新のバージョンを利用することを検討します。

近年、ソフトウェア開発において、インターネット上でソースコードの管理を行えるウェブサービスが利用されることがあります。そのようなウェブサービスにおいて、テスト用の機能やアカウント情報などの機密情報を誤って開示してしまうと、攻撃に悪用される可能性もあり、情報へのアクセス権限の設定には注意が必要です。

開示方法

- 開発環境のセキュリティを確保していることについて、製品セキュリティポリシー等に記載します。
- 具体的に記載する場合は、ホワイトペーパー等に記載する方法もあります。



9 開発時の脆弱性検査

意義

脆弱性が残ったままで製品を出荷しないために、脆弱性検査を実施することが必要です。製品の出荷後に脆弱性が発覚すると、アップデートファイルの開発・適用や一般消費者に対する説明等に対応コストが発生します。脆弱性の内容によってはアップデートができず、製品を回収する必要が生じる恐れもあります。開発時の脆弱性検査は、出荷後に発見された脆弱性に対処するためのコスト及び脆弱性を悪用した致命的なインシデントへの対処コスト削減することが期待できます。

実施内容

設計・開発の各段階で脆弱性検査を実施し、検知された脆弱性の対応を行います。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

① テスト方針・計画の策定

企画（要件定義）の段階で、テストの目的や範囲、必要なテスト環境やその体制、スケジュール、テスト完了基準などを明確にし、テスト計画書として文書化します。

脆弱性検査に関する要員のスキル等によっては、セキュリティベンダへの脆弱性検査の依頼を検討しておきます。

テスト計画の記載内容を組織内で合意をしておきます。テスト計画にもとづき、必要な予算や体制を確保します。

② セキュリティテストケース作成

企画（要件定義）時に作成したセキュリティ要件にもとづき、設計の段階でセキュリティテストケースを作成します。

セキュリティ要件通り実装できているのか、また、一般的な既知の脆弱性（SQL インジェクションなど）を作りこんでいないかの確認を行います。

テストケースは、「機能にもとづくテストケース」のみでなく、「セキュアコーディング規約にもとづくテストケース」、「一般的な脆弱性（SQL インジェクションなど）に関する汎用的なテストケース」、「実装言語にもとづくテストケース」なども含めるようにします。

③ 脆弱性検査実施

作成したセキュリティテストケースに従い、脆弱性検査を実施します。各テスト工程（単体テスト、結合テスト、システムテスト）に応じ、必要な脆弱性検査を実施することが望まれます。

また、脆弱性検査には様々な手法があり、発見できる脆弱性の種類も異なります。主な検査名は、下表のとおりです。各検査の詳細については、「脆弱性検査と脆弱性対策に関するレポート[12]」、「ファジング活用の手引き[13]」を参照してください。

検査名	概要	特徴
ソースコードセキュリティ検査	・ソースコードに作り込んでしまった脆弱性を検出する検査。 ・ソースコードの中の脆弱性を引き起こしやすい関数を見つけたり、構文解析を実施したりします。	・実装の段階で生じる脆弱性を対象に検査することが主です。よって、設計で入り込んでしまう脆弱性や未知の脆弱性は検証できません。
ウェブアプリケーションセキュリティ検査	・文字列を送付したり、ページの遷移を確認したりして、ウェブアプリケーションに特化した脆弱性の存在を検出する検査。	・深刻な被害をもたらすSQLインジェクション等の脆弱性を見つけることができる。 ・実装の段階で作り込まれる脆弱性の発見に向いている。
システムセキュリティ検査	・組み込み構成要素（コンポーネント）等に脆弱性がないか確認するためのリクエストや、バージョンを確認するためのリクエストを送付し、既知の脆弱性が残っていないか、セキュティ上問題のある設定が行われていないか等を検出する検査。	・基本的に既知の脆弱性を見つけることを目的としている。
ファジングによる検査	・脆弱性を発現させやすいデータやファイルを送り込み、脆弱性を検出する検査。	・他の検査では見つけづらい脆弱性が見つけられる。
ペネトレーションテスト	・攻撃者が実際に侵入できるかどうかという点に着目した検査。	・攻撃者がどこまで侵入できるのか、何をされてしまうのか、の検証に着目していることが特徴。 ・ソフトウェアの脆弱性だけではなく、ネットワーク上の不適切な運用についても見つけることができる。

④ 検知された脆弱性の管理と対応

脆弱性などの検知された問題については、対応要否を確認し適切に修正を行います。その際、問題の詳細・修正内容を記録し管理します。

原因や修正内容は関係者で共有し、発見された箇所以外にも、同様の問題がないか確認し、対応を行います。

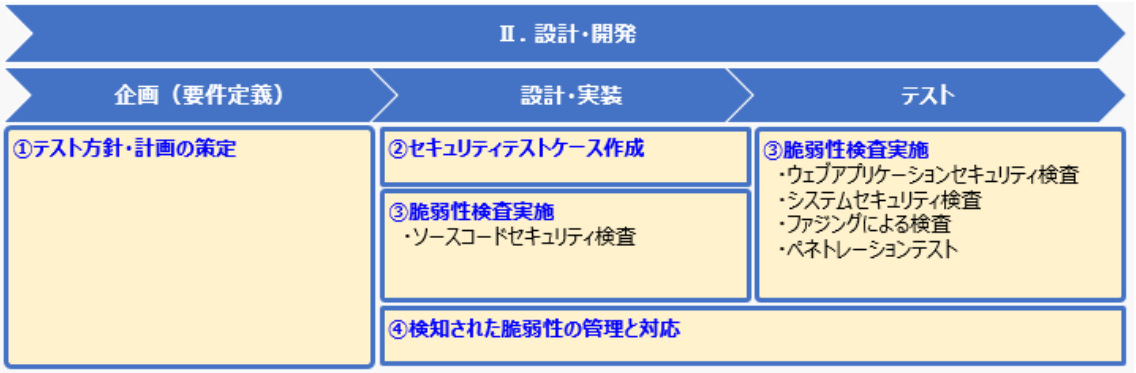
設計の変更を伴うような修正を行うなどした場合は、リグレッションテストを行い、修正以外の箇所に新たな脆弱性を生み出していないかも検証する必要があります。

[12] 脆弱性検査と脆弱性対策に関するレポート（IPA）https://www.ipa.go.jp/files/000032929.pdf

[13] ファジング活用の手引き（IPA）https://www.ipa.go.jp/security/vuln/fuzzing.html

なお、脆弱性検査ツールで全ての脆弱性パターンについて調査することは不可能であることや、発見できない脆弱性もあることを認識し、不足するパターンについては、手動テストで補うことが必要です。

また、脆弱性検証を行う担当者は、脆弱性検査に関する知識・経験を備えた専門家であることが望まれます。自組織内で要員の確保が難しい場合は、必要に応じて、セキュリティベンダへ検証を依頼することも検討します。



図：開発時の脆弱性検査実施の流れ

脆弱性検査を計画・実施する際には、以下の資料も参照してください。

- 「IoT セキュリティ評価検証ガイドライン Rev1.0[14]」
- 「OWASP SAMM[15]」

開示方法

- 開発時に脆弱性検査を実施している点を製品セキュリティポリシー等に含め開示します。

[14] IoT セキュリティ評価検証ガイドライン_r1.0（CCDS）https://www.ccds.or.jp/public_document/#Verification_guidelines1.0

[15] OWASP SAMM（JPCERT/CC）https://www.jpcert.or.jp/research/2010/SAMM_20100407.pdf

Ⅲ. 出荷後の対応

10 製品と構成要素の脆弱性監視

意義

出荷後に発見された脆弱性を早期に対処するためには、組織の製品及び構成要素（コンポーネント、ライブラリ等）に関する脆弱性情報を収集することが重要です。脆弱性は日々発見されています。出荷後の製品の脆弱性の対処が後手に回ることの無いように、日々の情報収集が必要です。遅れれば、脆弱性を悪用したサイバー攻撃を受けるリスクが高まります。積極的に脆弱性情報を収集することで、より迅速に脆弱性に対処し、被害を最小限に抑えることができます。

実施内容

出荷後の製品について、関連する脆弱性情報の収集を行います。収集した情報から脆弱性の存在が判明した場合には、対策の策定、対策の開示を行います。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順

① 脆弱性に関する情報収集

出荷した製品と、製品に組み込んだ構成要素に関する脆弱性情報を収集します。

出荷した製品の脆弱性情報は、セキュリティに関連する組織やコミュニティによって開示されることがあります。またソーシャルメディアなどで開示されることもあります。構成管理の情報をもとにして、製品や組織の体力に応じて定期的なパブリックモニタリングをすることが有用です。

また、利用者からの不具合に関する問い合わせの中には、原因が脆弱性であると判明する場合もあります。利用者からの問い合わせも情報源として扱います。

構成要素については「6 既知の脆弱性解消」において作成した構成管理の資料をもとに、製品出荷後も継続して脆弱性情報を収集します。詳細については、「6 既知の脆弱性解消」を参照してください。

第三者から自社の製品に関する脆弱性情報の連絡があった場合については、「11 脆弱性報告の受付・対策情報の公表」を参照してください。

② 脆弱性検証

上記①で収集した情報について、再現するかどうかを確認します。再現しない場合には、可能な範囲で、脆弱性情報の提供元に確認を行います。

③ 対策策定

脆弱性が存在する場合、脆弱性によって生じる被害とその大きさ及び発生の可能性からリスクを分析し、リスクの大きさにあわせて対応を検討し、対処します（詳しくは「6 既知の脆弱性解消」を参照ください）。このフェーズでは製品の出荷後の対応であり、利用者や第三者など脆弱性による被害を受ける相手が現に存在しているため、可能な限り早急な対応が望まれます。

また、脆弱性の修正が困難な場合は、回避策や代替策で脆弱性の悪用を防げる場合があります。もし回避策や代替策がない場合は、利用者に対して使用停止を促すことを検討します。

④ 対策情報の公表

策定した対策を利用者に適用してもらうため、脆弱性対策情報を製品サポートのページ等で公表します。対策情報の公表方法については「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル[16] 」を参照してください。

⑤ 構成管理資料の更新

脆弱性対策を適用した状態の製品の構成情報を、構成管理の資料に反映します。製品の構成は、脆弱性対策だけでなく、機能強化などによっても変更になることがあるため、製品のアップデートごとに構成情報を資料に反映します。

開示方法

- 出荷後に脆弱性情報を収集し対処している点を製品セキュリティポリシー等に含め開示します。
- 製品に関する脆弱性情報とその対策について、利用者に対して製品サポートのウェブページ等で開示します。

[16] ソフトウエア製品開発者による 脆弱性対策情報の公表マニュアル（IPA）
https://www.ipa.go.jp/files/000081019.pdf

11 脆弱性報告の受付・対策情報の公表

意義

第三者によって発見された脆弱性は、組織として適切に報告を受付・対処し、対策情報を公表する必要があります。

第三者からの脆弱性報告を受け付ける窓口を設置し、それを判りやすく公開しないと、第三者は脆弱性を発見しても報告できません。脆弱性が放置された結果、悪用されてしまうかもしれません。また、脆弱性対策を作成してもその対策情報が適切に公表されない場合、製品の利用者が対策の必要性を認識できず、対策を適用しないと被害に遭う恐れがあります。その結果、製品や製品開発者への信頼低下に繋がりかねません。

第三者からの脆弱性報告を適切に受付・対処することは、脆弱性の放置を未然に防ぐことにつながります。また、適切に脆弱性情報を公表すれば、利用者へ脆弱性対策を促すとともに、脆弱性への対応を怠っていない企業の姿勢を一般消費者に訴求でき、信頼や製品満足度の向上につながります。

実施内容

第三者によって発見された脆弱性の報告受付、分析と対策策定、情報開示を行います。連携が必要となる関係者とその役割については、「附属 主要な関係者・役割表」を参照してください。

実施手順
① 受付窓口の設置 脆弱性情報の受付窓口を設置し、脆弱性の発見者から情報を受け付けられるようにします。なお、受付窓口は脆弱性情報専用である必要はありませんが、脆弱性情報を受け付けていることが分かるように明示します。 また、脆弱性情報の報告があった場合に適切な対応が取れるように、組織内での報告ルートや対応方法を事前に組織内に周知します。一般的な問い合わせ窓口へ脆弱性情報が報告される場合もあるため、脆弱性の報告があった場合の対応を定め、周知します。 **② 脆弱性情報の受付** 窓口に脆弱性情報の報告があった場合、①で決めた報告ルートに従い、適切な部門に連絡します。脆弱性情報を受領した旨や対応状況を報告者へ連絡します。 **③ 脆弱性検証** 脆弱性情報が送られてきた担当部門では、報告された脆弱性情報が再現するかを確認します。再現しない等、報告内容に不明点がある場合は、報告者に確認等を行います。

④ 対策策定

脆弱性であると確認がとれた場合、脆弱性によって生じる被害とその大きさ及び発生の可能性からリスクを分析し、リスクの大きさにあわせて対応を検討し、対処します（詳しくは「6 既知の脆弱性解消」を参照ください）。このフェーズは製品の出荷後であり、脆弱性による被害を受ける利用者や第三者が現に存在しているため、可能な限り早急な対応が望まれます。

また、脆弱性の修正が困難な場合は、回避策や代替策で問題の発生を防げる場合があります。もし回避策や代替策がない場合は、利用者に対して使用停止を促すことを検討します。

⑤ 対策情報の公表

策定した対策を利用者に適用してもらうため、脆弱性対策情報を製品サポートのページ等で公表します。対策情報の公表方法については「ソフトウエア製品開発者による脆弱性対策情報の公表マニュアル 」を参照してください。

⑥ 構成管理資料の更新

脆弱性対策を適用した状態の製品の構成情報を、構成管理の資料に反映します。製品の構成は、脆弱性対策だけでなく、機能強化などによっても変更になることがあるため、製品のアップデートごとに構成情報を資料に反映します。

脆弱性を発見した第三者が、IPA と JPCERT/CC が運営する「情報セキュリティ早期警戒パートナーシップ」に報告[17]する場合があります。その場合の製品開発者への脆弱性情報の報告は JPCERT/CC から来ることになり、直接の報告よりも時間を要します。そのため、開発者は脆弱性情報を迅速に入手できるよう、JPCERT/CC の製品開発者リストに予め登録しておいてください。パートナーシップの詳細は「情報セキュリティ早期警戒パートナーシップガイドライン[18]」を参照してください。

開示方法

- 脆弱性の発見者が報告をするために、脆弱性の受付窓口をウェブサイト等でわかりやすく掲示します。
- 利用者が迅速に対策を適用できるよう、報告された脆弱性情報とその対策について、製品サポートのウェブページ等で公表します。

[17] 脆弱性関連情報の届出受付業務における取扱いプロセス（IPA）
https://www.ipa.go.jp/security/vuln/report/process.html

[18] 情報セキュリティ早期警戒パートナーシップガイドライン（IPA）https://www.ipa.go.jp/files/000073901.pdf

- 脆弱性の報告受付・対応・情報提供を行っていることについて、製品セキュリティポリシーに含め開示します。
- 報告された脆弱性がどのように取り扱われるかを脆弱性の発見者が理解できように、脆弱性の報告受付・対応・情報提供に関して、対応フローや判断基準の詳細をウェブサイトに開示する場合もあります。

【開示例（対策情報の例）】

☆☆☆☆株式会社 ＞ セキュリティ脆弱性情報 ＞ ○○○○製品

緊急

○○○○製品における××××の脆弱性

公開日 20XX 年 12 月 4 日
最終更新日 20XX 年 12 月 9 日

■概要

○○○○のバージョン△△以前に××××の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、○○○○が動作しているコンピュータ上で□□□□が実行されてしまう危険性があります。

この問題の影響を受ける○○○○のバージョンを以下に示しますので、以下の修正プログラムを適用してください。

該当製品をご利用の場合、今後被害が拡大するおそれがあるため、至急、修正プログラムをインストールしてください。

■該当製品の確認方法

影響を受ける製品は以下の製品です。

製品名称　○○○○
該当バージョン
1.5.4 (Windows 版)　以前の全てのバージョン
1.5.4 (Linux 版)　以前の全てのバージョン

使用しているバージョン番号の確認方法は以下の通りです。
1, ○○○○を起動し、「ヘルプ」メニューから「バージョン情報」を選択する。
2. 現れたウィンドウの下記の部分が起動している○○○○のバージョン番号です。

バージョン表示ウィンドウの図　（省略）

■脆弱性の説明

○○○○製品は、ファイルの■■■■のために▽▽▽▽の機能を搭載しています。◎◎◎◎データの一部として提供され▲▲▲▲で配布された▽▽▽▽の機能に、××××の脆弱性が存在するため、外部の第三者からインターネット越しに□□□□を実行される脆弱性が存在します。

※その他の設定および条件

▽▽▽▽の機能が搭載されていないバージョン 1.5.4 以前（Windows 版） を利用している場合、または、この機能が無効化されている場合には、外部の第三者からインターネット越しに□□□□を実行されることはありません。
・CWE-20　不適切な入力確認

■脆弱性がもたらす脅威

システム管理者権限でログインして本ソフトウエアを利用している場合、攻撃が成功すると、悪意のある第三者によってコンピュータを完全に制御されてしまう可能性があります。これにより、悪意のある第三者は、不正プログラムのインストール、データの変更や削除など、システム管理者の権限でコンピュータを任意に操作する可能性があります。
・CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/BS9.8　緊急
・〇〇製品における技術詳細情報

■対策方法

バージョン 1.5.4.より前の製品を利用されているお客様は、一度製品をアンインストールしてから対策版製品をインストールしてください。バージョン 1.1 以降の製品を利用されているお客様は、修正プログラムをインストールしてください。
各プログラムのインストール方法に関しては同梱の readme.txt を参照してください。

対象製品名称　〇〇〇〇
修正プログラムのダウンロード
1.5.5 patch.zip (Windows 版) 20XX.12.4
1.5.5 patch.tgz (Linux 版) 20XX.12.4

・修正プログラムによって置き換えられる設定ファイル
xxxxx.cfg、yyyyy.dif

■回避策

この脆弱性は、次の手順で影響を緩和できる場合があります。
〇〇〇〇で使用する管理用ポート番号宛ての通信を、信頼できる IP アドレスのみに限定するよう、ルータ等にてフィルタリング設定を行うことで、攻撃元の範囲を限定することができます。

■関連情報

CVE-20XX-12345678
JVN#12345678 〇〇〇〇製品における××××の脆弱性

■謝辞

□□□の□□□氏よりこの問題をご報告いただき（略）

■更新履歴

20XX.12.4　この脆弱性情報ページを公開しました。
20XX.12.9　脆弱性がもたらす脅威に、システム管理者の権限でコンピュータを任意に操作する際の技術詳細情報を追加しました。

■連絡先

本件に関するお問い合わせはこちら
脆弱性連絡窓口
電話　：03-xxxxx-xxxx (平日 10:00 – 17:00)
メール：example@example.co.jp

12 一般消費者の製品利用時における実施事項の明示

意義

製品セキュリティを維持するためには、製品開発者が脆弱性対処を実施することに加え、利用者に対し、セキュリティを確保するための設定やセキュリティ機能の利用方法等を説明し、正しく利用するよう促すことが重要です。利用者がセキュリティ機能を正しく利用できない場合、セキュリティが維持されていない状態で製品を利用し続けることになり、サイバー攻撃により被害を受けるリスクが高まります。利用者が実施するべき事項と実施しない場合にどんな問題が起こるかを明示することで、利用者がセキュリティ確保の必要性を認識することが期待できます。

実施内容

製品の利用開始時、利用中及び利用終了時に利用者によって実施すべき事項をまとめ、利用者に開示します。また、実施しない場合のリスクも明示します。

利用者の実施事項
■ **利用開始前に実施することの明示** ➢ パスワード設定・ネットワーク接続設定等の初期設定を正しく実施すること ➢ 利用開始時に工場出荷時の製品共通のアカウント・パスワードを変更すること ■ **利用中に実施することの明示** ➢ 製品のアップデート情報や脆弱性対策情報を確認し、必要な対策を実施すること ➢ 製品が提供するセキュリティ機能を利用すること ➢ バックアップや設定内容の記録を行うこと ➢ セキュリティサポートが終了した製品の利用は中止するか、サポート対応中の製品に変更すること ■ **利用終了時に実施することの明示** ➢ 製品を利用しない場合は、ネットワークから切り離すこと ➢ 製品を廃棄する際に保存されているデータを消去すること（初期化等）

上記記載の実施依頼事項を実施しない場合の、利用者が受けるリスクも併せて明示してください。

開示方法

- 利用者がセキュリティ機能を正しく利用できるように、利用者自身が実施すること及び実施しなかった場合に発生しうる被害等のリスクについて、製品の取扱説明書や製品情報を掲載しているウェブサイト等で開示します。

IV. 一般消費者に向けて実施すべきこと

一般消費者へ開示すべきこと

本ガイドで示した一般消費者に開示すべき項目一覧は以下の「脆弱性対処に向けた製品開発者ガイド」の列に記載しているとおりです。本一覧を活用し、一般消費者が確認するのに十分な情報が正しく開示されていることを確認してください。また、開示する情報が、一般消費者にとって理解できる内容、わかりやすい表現となるように留意してください。IPA では、一般消費者向けにも「ネット接続製品の安全な選定ガイド」「ネット接続製品の安全な利用ガイド」を開示しています。２つのガイドでは、「一般消費者」の列に記載しているとおり製品開発者が開示した情報を確認するよう促しています。

脆弱性対処に向けた製品開発者ガイド			一般消費者	
項目	開示項目	場所	選定	利用
1. 製品セキュリティポリシーの策定	製品セキュリティポリシー (項目 2～12 を掲載)	ウェブサイト	○	-
2. セキュリティサポート方針の明示	セキュリティサポート期間	製品情報ウェブサイト	○	○
3. 製品セキュリティを維持するための体制と管理	製品サポート窓口	ウェブサイト 製品パッケージ	○	-
	緊急時(PSIRT)体制	ウェブサイト	○	
4. セキュリティを確保するための設計	製品廃棄時の初期化機能	製品パッケージ 製品情報ウェブサイト	○	-
	セキュリティ機能や設定	取扱説明書 製品情報ウェブサイト	○	○
5. アップデートを考慮した設計	アップデートの種類	製品パッケージ 製品情報ウェブサイト	○	-
	アップデートの方法	取扱説明書 製品情報ウェブサイト	-	○
10. 製品と構成要素の脆弱性監視	脆弱性情報と対策情報	製品サポートウェブサイト	○	○
11. 脆弱性報告の受付・対策情報の公表	脆弱性情報と対策情報	製品サポートウェブサイト	○	○
	脆弱性の受付窓口	ウェブサイト	○	-
	対応フローや判断基準の詳細	ウェブサイト	○	-
12. 一般消費者の製品利用時における実施事項の明示	パスワード変更	取扱説明書 製品情報ウェブサイト	-	○
	セキュリティ機能の利用方法		-	○
	バックアップ方法		-	○
	利用終了時のネットワーク切離し		-	○
	廃棄時の初期状態実施		-	○
	実施しない場合のリスク		-	○

用語集

■ CSR

Corporate Social Responsibility の略称であり、企業が社会に与える影響について責任を持ち、社会の持続的発展のために貢献すべきとする考え方。また、そのような考え方に基づいて実践される諸活動。

■ PSIRT

Product Security Incident Response Team の略称であり、組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能。

■ 脅威指標

脆弱性対策情報を提供している製品開発者が独自で定め公表している脅威に関する指標。

■ サプライチェーン

複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れ。

■ 脆弱性

ソフトウェア製品やウェブアプリケーション等におけるセキュリティ上の問題箇所。コンピュータへの不正アクセスやコンピュータウイルス等により、この問題の箇所が攻撃されることで、そのソフトウェア製品やウェブアプリケーションの本来の機能や性能を損なう原因となり得るもの。

■ セキュリティポリシー

トップマネジメントによって正式に表明された組織のセキュリティに係る意図や方向付け及びそのような意図や方向付けに基づいてセキュリティ対策を行うために組織が定めた規定。

■ ハードコーディング

ソフトウェア開発の際に、特定の動作環境を確定し、その環境を前提とした処理やデータをソースコードの中に直に記述すること。

■ パブリックモニタリング

ソフトウェアの脆弱性や攻撃手法等に関して、公開情報から継続的に情報収集すること。

■ リスク分析

リスクの特質を理解し、リスクレベル（ある事象の結果とその起こりやすさとの組合せとして表現される、リスクの大きさ）を決定するプロセス。

附属：主要な関係者・役割表

凡例	説明
○	当該部門/関係者の関与が必須の場合
△	当該部門/関係者の関与が状況次第の場合

部門/組織		方針			設計・開発						製品出荷後						役割の説明
		組織									平時			緊急時			
		1	2	3	4	5	6	7	8	9	10	11	12	10	11	12	
自組織の関連部門	経営層	○	○	○							△	△		△	○		・製品セキュリティポリシー、製品サポート方針、緊急時の対応方針に関して、策定時・変更時の承認・決定を行う。 ・必要な予算の確保、及び、体制構築のため各部門へ指示を行う。 ・脆弱性対策情報の公表は、製品ブランドイメージや販売計画に影響を及ぼす場合があるため、公表内容の承認を行う場合がある。 ・外部から脆弱性の報告を受付した場合は、不適切な対応をすると未修正の脆弱性情報が公開されるなどのインシデントに繋がるため、脆弱性の対処状況の把握する。
	法務部門	○	○												△		・製品セキュリティポリシー、製品サポート方針、緊急時の対応方針に関して、策定時・変更時の内容確認を行う。 ・脆弱性が悪用され世の中に被害を及ぼした場合、製品ブランドイメージや販売計画に影響を及ぼす場合があるため、脆弱性対策情報の公表内容の確認を行う場合がある。 ・セキュリティ対処をアウトソースしている場合、契約締結時に契約内容の内容確認を行う。 ・自社の脆弱性対応や外部組織の対応に関して、契約内容との齟齬が発生した場合に、確認や折衝を行う場合がある。
	広報部門	○	○								○	○	○	○	○		・対外的に情報を開示、公表を行う場合には内容の確認を行う。 特に製品セキュリティポリシー、製品サポート方針、脆弱性対策情報の公表内容など
	リスクマネジメント部門	○	○	○							△	△	△	△	○		・製品セキュリティポリシー、製品サポート方針、緊急時の対応方針の策定時・変更時に際に、リスクマネジメントの観点で確認を行う。 ・関係部門において手順書に則った対応が実施されているか定期的な監査を行う。 ・脆弱性が悪用され世の中に被害を及ぼした場合、製品ブランドイメージや販売計画に影響を及ぼす場合があるため、脆弱性対策情報の公表内容の確認を行う。
	製品管理部門	○	○	○	○	○	○	○	○	○	○	○	○	○	○		・製品管理部門は、全工程において状況を把握、管理を行う。 ・製品セキュリティポリシー、製品サポート方針、緊急時の対応方針および手順書の策定を行う。 ・手順書の周知・教育・訓練を主導する。 ・セキュリティ対処をアウトソースする場合、セキュリティベンダの選定基準の策定を行う。 ・外部の情報共有組織との連携や所轄官庁への報告を行う。
	調達部門				○		○		○		△	△		△	△		・設計/開発時に、構成要素(コンポーネントやライブラリ等)の比較検討や調達を行い、構成要素に関する脆弱性情報の収集と構成管理表の管理を行う。 ・セキュリティ対処をアウトソースする場合、セキュリティベンダ等との調整や管理を行う。 ・製品出荷後に、構成要素(コンポーネントやライブラリ等)に脆弱性が発覚した際に、製品サプライヤへ問い合わせや調整を実施する場合がある。
	設計/開発部門				○	○	○	○	○	△	○	○		○	○		・製品の設計/開発を行う。 ・脆弱性検査の結果、脆弱性が検出された場合は、修正を行う。 ・製品出荷後に脆弱性の改修を行う。
	品質検査部門									○	○	○		○	○		開発時の脆弱性検査、製品出荷後に機能改修や脆弱性修正パッチ公開前に脆弱性検査等を行う。
	情報収集部門										○			○			・出荷した製品の脆弱性情報が開示されてないかSNSやセキュリティコミュニティを監視する。 ・調達部門から構成管理表を引き継ぎ、構成要素の脆弱性監視を行う。
	製品サポート窓口										○	○		○	○		・製品出荷後、製品利用者からの問い合わせ受付を行う。脆弱性に関する報告を受付ける場合もある。 ・自社製品の脆弱性対策情報を公開する際、代理店などへ事前に説明などを行う場合がある。 ・自社製品の脆弱性対策情報を公開後、一般利用者から対策適用に関して問い合わせ受付を行う。
	脆弱性受付窓口														○		脆弱性報告を受付、及び、報告者とのコミュニケーションを行う。

外部関係者	製品サプライヤ				△	△	○				○			○			構成要素(コンポーネントやライブラリ)の供給元。
	セキュリティベンダ				△	△	△	△	△	△	△			△			脆弱性検査など高い専門性が求められる対処をアウトソースする場合がある。
	情報共有組織																日本シーサート協議会(NCA)、ソフトウェアISACなどに加盟することで、製品セキュリティに関する組織体制やセキュリティ対処に関する情報共有や意見交換を行う。
	脆弱性情報の報告者														○		脆弱性の報告は、IPAおよびJPCERT/CCからされる場合がある。
	代理店		△									○	○		○		量販店など製品開発者に代わり販売やサポートを行う場合がある。
	一般消費者															○	一般消費者が購入した製品に対して、セキュリティ設定やセキュリティ機能の利用を行う。

別紙：製品開発者向けガイド チェックリスト

製品開発者向けガイドの項目に沿って作成したチェックリストです。

未実施	/12	実施済 レベルなし	/8	実施済 （レベル 1）	/4	実施済 （レベル 2）	/4	実施済 （レベル 3）	/3

カテゴリ	No	項目			チェック	備考
I.方針・組織	1	製品セキュリティポリシーの策定	レベル 1	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定します。		
			レベル 2	製品セキュリティに関する方針・考え方を、製品セキュリティポリシーとして策定し、外部に開示します。		
			レベル 3	製品セキュリティに関する方針・考え方に加え、実施事項を含めて製品セキュリティポリシーとして策定し、外部に開示します。		
	2	セキュリティサポート方針の明示	レベル 1	製品出荷後に、サポートできなくなったタイミングでサポート終了としてその旨を開示します。		
			レベル 2	組織内で企画・設計段階からサポート期間を定め、遅くともサポート終了時までにサポート終了を開示します。		
			レベル 3	組織内で企画・設計段階からサポート期間を定め、セキュリティサポート方針として出荷時に開示します。		
	3	製品セキュリティを維持するための体制と管理	–			

II. 設計・開発	4	セキュリティを確保するための設計	–			
	5	アップデートを考慮した設計	–			
	6	既知の脆弱性解消	レベル 1	可能な範囲で構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、深刻度の高い脆弱性から対処を行います。深刻度については、共通脆弱性評価システム（CVSS）や脅威指標 等を参考にしてください。		
			レベル 2	すべての構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、深刻度の高い脆弱性から対処を行います。深刻度については、共通脆弱性評価システム（CVSS）や脅威指標等を参考にしてください。		
			レベル 3	すべての構成管理を実施します。製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、製品に関連した脆弱性情報に関するリスク分析結果に応じて対処を行います。		
	7	セキュアコーディング	レベル 1	組織のコーディング規約を定めて、コーディングを実施します。		
			レベル 2	組織のコーディング規約を定めて、コーディングを実施し、別に定めたレビュー担当者がレビューします。		
	8	開発環境のセキュリティ確保	–			
	9	開発時の脆弱性検査	–			

III. 出荷後の対応	10	製品と構成要素の脆弱性監視	–		
	11	脆弱性報告の受付・対策情報の公表			
	12	一般消費者の製品利用時における実施事項の明示	–		

脆弱性対処に向けた
製品開発者向けガイド

2020 年 8 月 第 1 版発行

独立行政法人情報処理推進機構

〒113-6591

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

URL　https://www.ipa.go.jp/security/

電話　03-5978-7527　　FAX　03-5978-7552