製品利用者向けガイド

IPA 独立行政法人情報処理推進機構
セキュリティセンター

2026年3月

目次

はじめに

経営者の皆様へ

近年、企業において、自社が利用する基幹系システムや情報系システム、または社外の顧客向けに提供または公開しているシステムやサービスにソフトウェアを導入し、運用することで、便利で多様なシステム・サービスが実現されています。

このため、ソフトウェアを利用することは、事業活動を営むうえで、システムやサービスの利用・構築・提供など、絶対に必要なことであり、むしろソフトウェアの利用をなくては立ちいかぬものとなっていると考えられます。

一方でソフトウェアを利用することにはリスクも伴い、ネットワークを通じて、ソフトウェアの脆弱性が悪用され、自社のシステム・サービスから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。

経営者は、脆弱性リスクを適切に管理するための人材・プロセス・技術を整備し、セキュアなシステム・サービスを構築するための方針・体制や、脆弱性対処やインシデント対応を円滑に実施するための方針・体制を定め、システム・サービスのライフサイクルに応じた脆弱性管理を推進することが求められます。

システム・サービスにおける脆弱性への対処（以降、脆弱性対処）については実施事項が多く、**ソフトウェア等を含めて構築されるシステム・サービスを利用している組織（以降、製品利用者）がどのように考え、適切な対処を実施してよいのか判断に迷う**という課題があります。

他方、リスクを軽減してセキュアに事業活動を営む上で、単純にセキュリティ修正プログラムを適用する等、製品開発者の指示に従えば十分ということではなく、以下のシステム・サービスのライフサイクルの段階ごとに総合的かつ戦略的にセキュアな製品利用を行う必要があります。

I. 計画・要件定義

II. 調達

III. 導入

IV. 運用

V. 廃棄

本ガイドでは、製品利用者が実施すべき脆弱性対処について、文献調査の結果や、脆弱性対処を実施している企業へのアンケート調査結果およびヒアリング調査結果をもとに、**重要と思われる内容をシステム・サービスのライフサイクルのフェーズごとにまとめました。**実施すべき脆弱性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。

これにより、企業が利用するシステム・サービスにおけるセキュリティの向上、製品利用者への信頼につながり、**製品利用者自身がセキュアなソフトウェアを選び、適切に利用することで、市場全体のセキュリティ向上に寄与することを期待**します。

本ガイドの概要

本ガイドについて

本ガイドでは、製品利用者において実施すべき脆弱性対処を掲載しています。脆弱性対処のうち、人材・プロセス・技術の整備や、方針・体制については、組織のリソースに応じて実施できるよう段階的に示しており、可能なところから着手できるよう構成しています。

本来、脆弱性対処はシステム・サービスのライフサイクル全体を通じた網羅的な実施が望ましいですが、最初からすべてを行うのはハードルが高い場合もあります。まずは自組織の状況に合わせて「どこから始められるか」を検討し、脆弱性対処の第一歩を踏み出すための参考にしてください。

なお、本ガイドは、製品利用者が主体的に実施すべき脆弱性対処の内容を必ずしも網羅的ではありませんが、幅広く整理したものです。記載された内容は、製品開発者と製品利用者間における契約上の責任範囲や役割分担（責任分界点）を規定・定義するものではありません。実際の対処にあたっては、製品開発者側のサポート範囲や、使用するソフトウェアの契約内容や SLA（サービスレベル合意書）を確認した上で、適切な役割分担のもと実施してください。

対象製品

本ガイドの対象となる製品は、以下のような製品を想定しています。

- ソフトウェア・パッケージソフトウェア
- ソフトウェアを組み込んだ機器
- 上記を含めて構築されるシステム・サービス（自社開発・委託開発を含む）

想定読者

本ガイドの読者は、ソフトウェアやソフトウェアを含めて構築されるシステム・サービスを利用している組織のうち、比較的中規模から大規模の組織における CSIRT、IT・セキュリティ部門の脆弱性担当者、情報システム部門のセキュリティ担当者等を想定しています。

本ガイドの構成

「Ⅰ．計画・要件定義」、「Ⅱ．調達」、「Ⅲ．導入」、「Ⅳ．運用」、「Ⅴ．廃棄」という５つの大項目に分類し、製品利用者が実施すべき望ましい脆弱性対処を示しました。

各項目の内容は以下のように「構築・調達形態に応じた利用方法」、「意義」、「実施内容」の構成となっています。

■ 構築・調達形態に応じた利用方法

製品利用者におけるシステム・サービスの構築や、ソフトウェアの調達形態ごとに、以降の内容をどのような目的で確認すべきかを記載しています。各形態については後述する「システム・サービスの構築、ソフトウェアの調達形態に応じたアプローチ」を確認してください。

■ 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

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システム・サービス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。自社のシステム・サービスの機能や性質、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。

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。

- 製品利用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
- 委託先に求めるセキュリティ対策として要求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
- 取引先やビジネスパートナーに対し、自組織の取組み状況をアピールするために必要な事項を把握できる

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。

- 組織の脆弱性対処担当者が現状と課題を把握し、上長に報告
- ソフトウェアを外部から調達する際、調達におけるセキュリティ要件や、契約内容を確認するために活用
- システム・サービスの構築や運用を外部に委託する際、委託における遵守事項や、契約内容を確認するために活用
- 委託先の脆弱性対処の状況確認に活用

脆弱性管理の全体像と基本的な考え方

本ガイドの読み方

本章では、ガイドの内容に入る前に、製品利用者が脆弱性対処に取り組む際の全体像と、組織として備えておくべき基本的な考え方を示します。

システム・サービスのライフサイクルに応じた脆弱性管理

脆弱性対処は、自組織にシステム・サービスを導入した後に始まるものではありません。「計画・要件定義」から「廃棄」に至るまで、システム・サービスのライフサイクル全体に組み込まれるべきプロセスです。

このため、本ガイドもシステム・サービスのライフサイクル全体における脆弱性管理という観点から構成されています。各段階で行うべき主な実施事項は以下の通りです。また括弧書きで、実施事項に対応するガイドの章番号を記載しています。

段階	主な実施事項
Ⅰ．計画・要件定義	脆弱性リスクを適切に管理するための人材・プロセス・技術の整備（1章）
	セキュアなシステム・サービスを構築するための方針・体制（2章）
	脆弱性対処やインシデント対応を円滑に実施するための方針・体制（3章）
Ⅱ．調達	セキュリティを確保するための調達（4章）
Ⅲ．導入	ソフトウェアを導入するための IT 資産管理（5章）
	ソフトウェアを導入する際における脆弱性対処（6章）
Ⅳ．運用	ソフトウェアの運用時における脆弱性対処（7章）
	ソフトウェアの運用時にインシデントが発生した場合の対応（8章）
Ⅴ．廃棄	ソフトウェアの廃棄時における脆弱性対処（9章）

システム・サービスの構築、ソフトウェアの調達形態に応じたアプローチ

製品利用者の形態によって、注力すべきポイントが異なります。

なお、本ガイドは「自社で利用するシステム・サービス」や「当該システム・サービスに含まれるソフトウェア・ソフトウェアを組み込んだ機器」を対象としており、不特定または多数への販売を目的としたソフトウェアそのものの開発プロセス（製品開発者としての活動）は対象外としています。製品開発者としての活動における脆弱性対処は「製品開発者ガイド」を確認してください。

製品利用者におけるシステム・サービスの構築や、ソフトウェアの調達形態は様々なパターンが考えられますが、本ガイドでは主要な形態として以下の４つを想定しています。それぞれの形態によって、本ガイドで特に留意すべき点が異なるため、自組織が脆弱性対処を行うシステム・サービスに関連する形態ごとの特徴を確認し、当てはまる形態において特に留意すべき点を重点的に確認してください。また括弧書きで、留意すべき点に対応するガイドの章番号を記載しています。

形態	特徴	本ガイドで特に留意すべき点
外部ソフトウェア製品の調達	ソフトウェア製品、パッケージ製品、ソフトウェアを組み込んだ機器を外部から調達し、自組織で利用する	● 適切なセキュリティ要件を備えた製品の選定（４章） ● 製品開発者が提供する情報の監視とパッチ適用（７章） ● ソフトウェアのサポート・利用終了に伴う廃棄（９章）
クラウド（SaaS）利用	サービスとして外部のクラウド（SaaS）と契約し、利用する	● 設定不備の排除（６章） ● 利用クラウド（SaaS）における障害発生時等の事業者への確認（７章） ● クラウド（SaaS）利用終了時のデータ消去（９章）
外部委託によるシステム・サービスの構築	外部事業者にシステム・サービスの構築を委託し、その範囲内でソフトウェアを利用する	● 委託先との契約への脆弱性対処の明記（４章） ● 導入時のテストの実施（６章）
自社によるシステム・サービスの構築	自社でシステム・サービスの構築を行い、その範囲内でソフトウェアを利用する	● 企画・設計段階からのセキュリティ要件定義（４章） ● 自組織の開発部隊による脆弱性の監視（７章）

ポリシーを軸としたガバナンス

組織として一貫した脆弱性対処を行うため、組織としてのセキュリティの方針・考え方を表明する「セキュリティポリシー」に則った、システム・サービスの「構築・調達ポリシー」を中核に据えます。セキュリティポリシーおよび構築・調達ポリシーの策定にあたっては、２章のセキュアなシステム・サービスを構築するための方針・体制の実施内容を確認ください。

構築・調達ポリシーは、本ガイドの考え方と同様に、脆弱性対処をシステム・サービスのライフサイクル全体に組み込むため、本ガイドが記載するライフサイクルのフェーズごとの実施事項をすべて含めることを推奨します。

I. 計画・要件定義

1 脆弱性リスクを適切に管理するための人材・プロセス・技術の整備

構築・調達形態に応じた利用方法

製品利用者における構築・調達形態のすべての形態に共通して、本項目の内容は必須となります。

構築・調達形態に関わらず、組織としての脆弱性に対処するための基盤となる人材、プロセス、技術の整備を行うために、本ガイドの内容を確認し、実装してください。

意義

脆弱性リスクを適切に管理することができる組織は、早期段階において自社のシステム・サービスにおける脆弱性リスクを特定し、必要に応じた対処を行うことで、脆弱性が放置されることにより生じるサイバー攻撃による被害や、組織としての信用を失うリスクを回避することができます。

実施内容

脆弱性リスクの管理に関与する組織内外の関係者が、脆弱性リスクに対処するために必要な役割と責務を定義し、それらを実践できるよう、人材、プロセス、技術を整備します。

またその中で、組織外の関係者に求めるべき役割と責務や、実践のための必要なプロセスは、外部委託の活用や組織間の連携強化を通じて、その実践の確実性、継続性を担保します。

組織における適切な脆弱性リスクの管理では、関係する組織内外の関係者の役割と責務を明確にしつつ、円滑に実施するためのポリシーや規程類の策定によるプロセスを整備することが重要です。またそれらを効率的に実現するために、外部への委託や連携も望まれます。

実施手順
① **人材・プロセス・技術の整備** システム・サービスにおける脆弱性リスクの管理全体が網羅されるよう、組織内外の関係者を洗い出すとともに、それぞれの関係者に求められる役割と責務を明確化し定義します。関係者には、情報システム部門、IT・セキュリティ部門、CSIRT、および組織内のセキュリティに関する責任者である CISO 等が挙げられます。 組織内外の関係者に求めるべき役割と責務を実践していくために必要なプロセスを整理し、それぞれの関係者が確実に実践できるようにポリシーや規程類を策定します。組織としての基本的なセキュリティの目的や基本方針は不可欠です。他に整備すべきポリシーや規程類の例は以下の通りです。 ● 脆弱性リスクの管理に係る社内の人員体制や連携方法を示す組織的なポリシー ● 脆弱性リスクの管理対象や手順を示す運用面のポリシー ● 対処すべき脆弱性の優先順位の考え方や基準を示すトリアージガイドライン

- インシデント対策ポリシーやインシデント対応手順　　等

定義された役割と責務や、実践のための必要なプロセスについては、適切に維持されていることを定期的に確認し、必要に応じて更新します。

定義された役割と責務や、策定されたポリシーや規程類は、組織内外の関係者に周知を行います。周知は、これらの内容が更新された場合にも実施します。また、脆弱性リスクの管理に携わる組織内のすべての担当者に対して、定期的な教育・研修を実施します。

② 経営層のコミットメント

脆弱性リスクの管理に関与する組織内外の関係者がセキュリティへの感度を高め、組織レベルで脆弱性リスクの管理を行うことが事業継続性の観点からも重要であることを正しく理解することが必要となります。経営層が脆弱性の管理やその後の対処に強く関与することで、組織の脆弱性リスクの管理をはじめとするセキュリティ人員の確保や、セキュリティ対策への投資の実現につながります。

加えて、組織としての基本的なセキュリティの目的や基本方針に基づく、経営目標やセキュリティに関する指標を公表することも効果的です。

③ 外部委託の活用

脆弱性リスクの管理対象となるシステム・サービスのリスクや影響範囲が大きい場合（例：365 日 24 時間稼働することが求められるようなシステム・サービス等）や、組織内のリソースが限られている場合は、外部委託または組織間の連携強化を活用して、確実かつ継続的に実施される体制を構築します。

組織における適切な脆弱性リスクの管理では、関係する組織内外の関係者の役割と責務を明確にしつつ、円滑に実施するためのポリシーや規程類の策定によるプロセスを整備することが重要です。またそれらを効率的に実現するために、外部への委託や連携も望まれます。

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	CISO 等の経営層を含めた組織内の関係者が、適切な脆弱性リスクの管理を実現するために必要な役割と責務を定義します。
2	適切な脆弱性リスクの管理が組織内のシステム・サービス全体に網羅されるよう、CISO 等の経営層を含めた組織内の関係者が、必要な役割と責務を定義し、それらを実践できるよう、人材、プロセス、技術を整備します。
3	脆弱性リスクの管理対象となるシステム・サービスのリスクや影響範囲に応じて、外部委託の活用や組織間の連携強化を図りつつ、適切な脆弱性リスクの管理が組織内のシステム・サービス全体に網羅されるよう、CISO 等の経営層を含めた組織内の

	関係者が、必要な役割と責務を定義し、それらを実践できるよう、人材、プロセス、技術を整備します。

2 セキュアなシステム・サービスを構築するための方針・体制

構築・調達形態に応じた利用方法

製品利用者における構築･調達形態のうち､外部ソフトウェア製品の調達､クラウド（SaaS）利用、外部委託によるシステム・サービスの構築、自社によるシステム・サービスの構築のすべての形態において、本項目の内容は必須となります。

特に外部ソフトウェア製品の調達、およびクラウド（SaaS）利用においては、外部事業者からの調達、もしくは外部事業者のサービス利用に向け、脆弱な製品・サービスの利用を未然に防ぐため、本ガイドの内容を確認し、実装してください。

また、外部委託によるシステム・サービスの構築、および自社によるシステム・サービスの構築においては、構築が開始する前に、委託先や自組織の構築チームに本ガイドで定めるポリシーを提示し､構築中に遵守させるため､本ガイドの内容を確認し､活用してください。

意義

セキュアなシステム･サービスの構築に資する組織の体制､取組みを整備することにより、組織内での脆弱性対処をはじめとするセキュリティ確保に関する意識を高めるとともに、社会的な評価を高めることが重要です。

利用するソフトウェアおよびソフトウェアを導入したシステム・サービスに対して、セキュリティを担保するための方針を定めることにより、ソフトウェアやシステム・サービスのライフサイクル全体にわたってセキュリティを考慮・維持するというガバナンスを効かせることが必要です。

実施内容

法令の順守や、サプライチェーン強化などの社会的な要求事項に対応して、組織がセキュアなソフトウェアまたはソフトウェアを導入したシステム・サービスの利用を推進していく際の取組姿勢やセキュリティ対処の基本方針・ルールを、セキュリティポリシーとして策定します。

あわせて、セキュリティポリシーに基づいたソフトウェアの調達や、システム・サービスの構築ができるよう、構築・調達ポリシーとして策定します。

利用するソフトウェアやソフトウェアを導入したシステム・サービスが、セキュリティポリシーや構築・調達ポリシーを遵守していることを定期的に確認できるようにするため、ガバナンスの確立が求められます。

セキュリティポリシーおよび構築・調達ポリシーは策定するだけではなく、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、セキュリティポリシーおよび構築・調達ポリシーに関係する法令やガイド等の改定や社会的な要求事項の変化等があった場合、セキュリティポリシーおよび構築・調達ポリシーを見直すことも必要です。

実施手順

① **システム・サービス構築チームの構築**

ソフトウェアまたはソフトウェアを導入したシステム・サービスの利用におけるセキュリティ上の問題に対処できるようにするため、システム・サービス構築チームを構築します。チームには、責任者だけではなく、情報システム部門、IT・セキュリティ部門、CSIRT、法務部門、調達部門等を含めます。チームに参加する担当者には、近年の法令やセキュリティ動向を踏まえ、ソフトウェアや製品開発者におけるセキュリティに関する実績を評価できるスキルや、部門間のコミュニケーションを円滑に行うスキルが望まれます。

責任者は、構築チームの担当者に対し、近年の関連する法令や社会的な要求事項、セキュリティに関する最新動向の把握を求めることが望まれます。

② **計画・ポリシー・手順の策定**

経営者の意向や、法令の遵守、サプライチェーンの強化などの社会的な要求事項を踏まえて、組織がセキュアなソフトウェアまたはソフトウェアを導入したシステム・サービスの利用を推進していく際の取組姿勢やセキュリティ対処の基本方針・ルール等を盛り込んだセキュリティポリシーを策定し、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受けた後、外部に開示します。

下記(1)～(4)の手順に従い、セキュリティポリシーを策定します。

(1) 組織としてセキュリティポリシー策定の意思決定

組織として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、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。セキュリティポリシーは組織としての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) 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、利用するソフトウェアや構築するシステム・サービスについても、自組織のセキュリティポリシーを遵守できるものを調達できるよう、システム・サービスの構築・調達ポリシーもあわせて作成します。

なお、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。

システム・サービスの構築・調達ポリシーは、脆弱性対処をシステム・サービスのライフサイクル全体に組み込むため、本ガイドで示しているような以下の観点を網羅する内容とすることが望まれます。

構築・調達ポリシーに含まれるべき内容

- セキュリティを確保するための設計が検討され、実装されていること
- ソフトウェアを導入するための IT 資産管理が検討され、実装されていること
- ソフトウェアを導入する際における脆弱性対処が検討され、実装されていること
- ソフトウェアの運用時における脆弱性対処が検討され、実装されていること

- ソフトウェアの運用時にインシデントが発生した場合の対応が検討され、実装されていること
- ソフトウェアの廃棄時における脆弱性対処が検討され、実装されていること

(3) 経営層による承認

経営層に作成したセキュリティポリシーおよび構築・調達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

承認されたセキュリティポリシーおよび構築・調達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、策定したセキュリティポリシーおよび構築・調達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、組織外に策定したセキュリティポリシーおよび構築・調達ポリシーを開示します。

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	セキュリティポリシーおよび構築・調達ポリシーを策定します。
2	セキュリティポリシーおよび構築・調達ポリシーを策定し、利用するソフトウェアやソフトウェアを導入したシステム・サービスが同ポリシーを遵守していることを確認します。
3	セキュリティポリシーおよび構築・調達ポリシーを策定し、利用するソフトウェアやソフトウェアを導入したシステム・サービスが同ポリシーを遵守していることを確認し、ソフトウェアやシステム・サービスのライフサイクル全体にわたってセキュリティが確保されていることを定期的に確認します。

3 脆弱性対処やインシデント対応を円滑に実施するための方針・体制

構築・調達形態に応じた利用方法

製品利用者における構築･調達形態のうち､外部ソフトウェア製品の調達､クラウド(SaaS)利用、外部委託によるシステム・サービスの構築、自社によるシステム・サービスの構築のすべての形態において、本項目の内容は必須となります。

特にクラウド（SaaS）利用においては、インシデント発生時に、クラウドサービス提供側の SIRT との連携・協力体制を強化するため、本ガイドの内容を確認し、実装してください。

また、自社によるシステム・サービスの構築においては、自組織内の CSIRT と構築チーム間との連携・協力体制を強化するため、本ガイドの内容を確認し、実装してください。

意義

組織内の脆弱性対処やインシデント対応を適切に行うために、組織内の様々な部門間だけでなく公的機関等の外部組織やソフトウェアの製品開発者も含め、連携した体制を構築する必要があります。この体制が整備できない場合は、対処すべき脆弱性情報を十分に把握することができない、インシデントが発生した際に適切な対応をとることができない等、ソフトウェアやシステム・サービスのセキュアな利用を維持することが困難になります。

実施内容

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、ソフトウェアやシステム・サービスの利用に必要な『平時の体制』だけでなく、外部から脆弱性報告を受け付けた場合などの『緊急時の体制』についても、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、自組織内のセキュリティに関する緊急時の体制のことを CSIRT（Computer Security Incident Response Team） と言います。

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。

実施手順
① **CSIRT の構築・維持** セキュリティポリシーに従ってセキュリティ対処を実施する CSIRT を構築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。 CSIRT のスタッフとなる自組織の関連部門及び CSIRT と連携を図る外部組織を特定し、それぞれ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 CSIRT のスタッフには、昨今の脆弱性等の脅威の状況やサイバー攻撃の傾向を把握するため、最新動向の調査・研究や、セキュリティスキルの習得・研修の機会を設け、最新のセキュリティ分野の知識を獲得することが求められます。加えて、自組織の円滑なセキュ

リティ対策を推進する上で必要なコミュニケーション能力や、情報収集能力・解析能力が求められます。

② **CSIRT が提供する機能の検討**

CSIRT の組織において、セキュリティポリシーに従ってセキュリティ対処を実施するために配置すべき必要な機能を検討します。必要な機能を検討する上で考慮すべき機能は以下の通りです。

インシデントの予防・未然防止のために考慮すべき機能

- 体制整備：セキュリティポリシーの策定、脆弱性情報の受付窓口、監視システムの維持
- 情報収集：脆弱性情報や攻撃予告情報の収集
- 情報分析：脆弱性情報の分析、トリアージ、対策検討
- 脆弱性対処：セキュリティ修正プログラムの適用、脆弱性対処に係る組織内外との連携
- 教育・啓発：社員へのセキュリティ教育プログラムの実施、実践的なトレーニング

インシデント発生時の対応のために考慮すべき機能

- 検出・調査：攻撃の特定、被害範囲の調査、原因の分析
- 封じ込め・復旧：被害拡大の防止（ネットワーク切断等）とシステム正常化
- 報告・連携：経営層、法務、警察、顧客など社内外への報告・情報共有

インシデント対応の振り返りのために考慮すべき機能

- 再発防止：インシデント発生の経緯を振り返り、対応フローの改善

③ **計画・ポリシー・手順の策定**

CSIRT が提供する機能に応じ、自組織が利用するソフトウェアやシステム・サービスに脆弱性が発見された場合に速やかに対処するための方針や、インシデント対応に関するプロセスを明確にするための方針を定め、実施するための手順を示す規程類を策定します。CSIRT が適切に活動するために必要となる規程類の例は以下の通りです。

- ソフトウェアの管理手順
- 定期的な脆弱性スキャンの方針等を示す脆弱性管理に関する規程類
- 外部からの攻撃やマルウェアの検知等に関する規程類
- インシデントの予防・検知・対応・再発防止等に関する規程類

④ **ステークホルダー間の関係強化**

自組織が利用するソフトウェアやシステム・サービスにおける脆弱性対処やインシデント対応を円滑に行うために、CSIRT と外部組織との間の情報連携・協力体制を強化します。

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。

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。

なお、本ガイドでは、ソフトウェアやサービス、システムにおける技術上の脆弱性に関する対応を中心に記載していますが、一般的に、CSIRT は、脆弱性への対応だけを目的しているわけではありません。脆弱性を起因とするもの以外のインシデント対応や、フォレンジック分析、通信監視など、組織に応じて様々な役割が設定されます。

そのような CISRT の構築・運用全般については「セキュリティ対応組織の教科書」[1] が参考となります。

レベル	実施内容
1	CSIRT を構築・維持し、セキュリティポリシーに従って、CSIRT がセキュリティ対処を実施するために必要な機能を定義します。
2	セキュリティポリシーを策定し、具体的な脆弱性対処やインシデント対応に係る規程類を策定し、CSIRT の活動上必要となる体制やプロセスを整備します。
3	CSIRT を構築・維持し、CSIRT がセキュリティポリシーに従ってセキュリティ対処を実施するために必要な機能を定義するとともに、脆弱性対処計画の策定やステークホルダー間の関係強化を通じて、CSIRT の活動上実効性のある体制やプロセスを整備します。

[1] セキュリティ対応組織の教科書（ISOG-J） https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html

II. 調達

4 セキュリティを確保するための調達

構築・調達形態に応じた利用方法

製品利用者における構築・調達形態のうち、外部ソフトウェア製品の調達、およびクラウド（SaaS）利用においては、本ガイドで定めた内容を、製品・サービスの選定時の要件や、比較の観点として活用してください。

外部委託によるシステム・サービスの構築においては、本ガイドで定めたセキュリティ要件を各種契約書に盛り込み、システム・サービスの構築プロセスに確実に実装されるようにしてください。

また自社によるシステム・サービスの構築においても同様に、本ガイドで定めたセキュリティ要件を組織内の構築チームに要求し、システム・サービスの構築プロセスに確実に実装してください。

外部の構築、自社の構築に関わらず、構築が完了するまで、本ガイドのセキュリティ要件が遵守され、定期的に確認することが必要です。

意義

セキュアにソフトウェアおよびソフトウェアを導入したシステム・サービスを利用するためには、設計段階からセキュリティ要件を検討する必要があります。設計段階からソフトウェアやシステム・サービスのセキュリティ要件を考慮しておかないと、運用後にセキュリティ製品等の導入をはじめとする追加投資が必要になり、コストがかかります。セキュリティ要件の検討にあたっては、ソフトウェアやシステム・サービスにおいて想定される脅威や被害から保護すべき機能や情報を踏まえたリスク分析の結果を踏まえる必要があります。

設定したセキュリティ要件は自組織が遵守するだけではなく、外部から調達するソフトウェアがある場合においては、調達要件に含めることや、システム・サービスの構築・運用を外部に委託する場合においては、委託契約に含めることが重要です。

実施内容

リスク分析などを行い、分析結果をもとにソフトウェアやシステム・サービスに求めるセキュリティ要件を検討します。定められたセキュリティ要件に基づき、ソフトウェア・ソフトウェアパッケージや、ソフトウェアを組み込んだ機器を調達することや、ソフトウェアを導入したシステム・サービスを構築することを遵守します。

実施手順
① 保護すべき IT 資産の特定 自組織において守るべき対象を洗い出します。組織によっては、対象となる IT 資産の稼働状況や残存状況が把握できない場合や、各部門が独自に取得した未知の IT 資産が存

在する可能性があるため、IT 資産の台帳等を作成し、継続的に IT 資産の管理を行うことが望まれます。この時、組織の IT 資産の数に応じて、IT 資産の管理を網羅的に行うため、ソフトウェア部品票（SBOM）を活用して可視化を図ることも検討します。

② 脅威の特定

上記①で保護すべき IT 資産について、関連する脅威を洗い出します。脅威は近年の脆弱性情報や脆弱性を悪用する攻撃動向等が挙げられます。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[2] を利用できます。脆弱性の深刻度については、共通脆弱性評価システム（CVSS）[3] や脅威指標等を参考にしてください。これらの情報を確認し、組織の IT 資産に関係する脅威を整理します。

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 セキュリティ要件の定義

リスク評価結果を踏まえた上で、セキュリティ要件を定義します。この時、リスク評価結果を十分に踏まえ、構築するシステム・サービスのセキュリティレベルを十分に担保できるセキュリティ要件を抜け漏れなく設定し、その内容について、構築チームで合意を得ることが望まれます。

セキュリティ要件を検討する際、考慮すべき観点の例は以下の通りです。

- ソフトウェアの製品開発者における組織・体制面
  - 関係者の役割・責務の定義、および人材・プロセスの整備状況
  - 製品セキュリティ方針（セキュア・バイ・デザイン等）の策定状況
  - 脆弱性やインシデントに対応する PSIRT の構築・維持　　等
- ソフトウェアの開発・製造面
  - 既知の脆弱性の解消および、セキュアコーディング規約の遵守
  - 開発・ビルド・検査環境におけるセキュリティ確保
  - 出荷前の脆弱性検査（ツールによる自動診断や手動テスト）の実施　　等
- ソフトウェアの運用・サポート面：
  - 出荷後の脆弱性情報の収集および、利用者への迅速な情報提供
  - 脆弱性受付窓口（VDP）の設置と、適切にトリアージする仕組み
  - 利用者がセキュアに利用するための設定ガイドやリスク情報の提供

等

⑤ セキュリティ要件に基づく契約

定めたセキュリティ要件を実効性のあるものにするため、ソフトウェア製品の調達時や運用・保守の委託時における契約に、セキュリティ要件を明確に盛り込みます。製品開発

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

[3] 共通脆弱性評価システム CVSS v3 概説（IPA） https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

者や運用・保守に関する委託先との間で、セキュリティ品質や対応プロセスに関する合意形成（SLA 等）を行い、契約書や仕様書に明記することで、組織が求めるセキュリティレベルを担保します。

自社によるシステム・サービスの構築において、契約行為は発生しませんが、定めたセキュリティ要件を組織内の構築チームに要求し、システム・サービスの構築プロセスに確実に実装することを要求します。

III. 導入

5 ソフトウェアを導入するための IT 資産管理

構築・調達形態に応じた利用方法

製品利用者における構築・調達形態のうち、外部ソフトウェア製品の調達、およびクラウド（SaaS）利用においては、本ガイドで定めた通り、購入したライセンスや利用サービスについてもれなく台帳登録し、管理責任者を割り当ててください。

一方、外部委託によるシステム・サービスの構築、および自社によるシステム・サービスの構築においては、本ガイドで定めた通り、システム・サービスを構成するミドルウェアや OSS ライブラリ等について、もれなく台帳登録し、管理責任者を割り当ててください。

意義

脆弱性対処の第一歩は、自組織が管理すべき対象を正確に把握することです。ハードウェア、ソフトウェア、ライセンス、SaaS 等の IT 資産が未管理の状態で放置されると、脆弱性の修正漏れや攻撃の足がかりとなるリスクが急増します。

導入するソフトウェア等を含め、自組織の IT 資産を網羅的に可視化・管理することで、脆弱性が生じ得る範囲を把握し、その後の脆弱性対処を円滑にします。

実施内容

関連する IT 資産を網羅的に整理する管理台帳を定常的に更新します。

実施手順
① ソフトウェア等の IT 資産の台帳への追加 ソフトウェア・パッケージソフトウェアや、ソフトウェアを組み込んだ機器を導入する場合、自組織の IT 資産の台帳等に、導入するソフトウェア等を追加します。 **② 台帳の更新** 作成した台帳に基づき、IT 資産のうちソフトウェアのアップデートや設定変更が行われた際には速やかに台帳を更新します。また定期的なネットワークスキャンや棚卸しを実施することで、利用停止や廃棄された IT 資産が台帳に残っていないかを確認します。

6 ソフトウェアを導入する際における脆弱性対処

構築・調達形態に応じた利用方法

製品利用者における構築・調達形態に関わらず、導入に際してはソフトウェア本体だけでなく、付帯する文書（利用規約、マニュアル、契約書等）の確認が前提となります。

特に外部ソフトウェア製品の調達、およびクラウド（SaaS）利用においては、調達や契約が完了した後、デフォルトの状態のまま導入してしまいがちになるため、利用条件の精査と、導入時の製品・サービスの設定確認が重要になります。

一方、外部委託によるシステム・サービスの構築、および自組織によるシステム・サービスの構築においては、構築されたシステム・サービスのテスト結果が、自組織が定めたセキュリティ要件をもれなく満たしているか、再度確認することが重要になります。

意義

ソフトウェアには、製品開発者が想定する利用環境や使用上の制約が存在します。利用規約やマニュアルを確認せず、製品開発者の想定しない方法や環境で利用した場合、予期せぬ動作や脆弱性を引き起こす原因となり得ます。

また、セキュアバイデフォルトに未対応のソフトウェアは適切に設定を変更しない場合、攻撃者にとって攻撃しやすい状態が維持されることになります。加えて、ソフトウェアのテストを実施しない場合、自組織のセキュリティ要件が適切に運用されないリスクが生じます。このため、ソフトウェア導入の際には、正しい利用範囲を理解して設定を行うだけでなく、潜在的な脆弱性や設定不備が存在しないかを確認するための脆弱性診断を実施し、セキュリティが担保されているかを確認することが重要です。

実施内容

導入するソフトウェアについて、利用規約・マニュアル等の文書確認、デフォルト設定の確認と適切な変更、および脆弱性診断を含む各種セキュリティテストを実施し、これらの内容を関係者に周知します。

実施手順
① ソフトウェアに関する規約・マニュアル・契約内容の確認 実際に利用を開始する前に、製品開発者から提供される利用規約、ユーザーマニュアルや、製品開発者と締結した契約内容等を確認します。製品開発者が保証する利用環境（OS、ネットワーク構成等）や、禁止事項（用途制限等）を確認し、製品開発者が想定しない誤った使い方にならないよう、自組織での利用方法との整合性を確認します。 **② ソフトウェアの設定確認** デフォルト設定を確認し、自組織のセキュリティポリシーを満たすように適宜設定を変更し、攻撃者に狙われる可能性がある設定を排除・変更します。確認すべき設定の例は以下の通りです。

- 不要な機能・サービスが無効化されているか
- ソフトウェアの権限は最小化されているか
- ログの保存期間は十分か

③ 脆弱性診断およびセキュリティテストの実施

実際に導入・本番移行へ進む前に、脆弱性診断を中心としたセキュリティ状況の確認と各種テストを行います。

(1) 脆弱性診断と適切な設定の確認

導入予定のソフトウェアやシステム・サービス全体に対して、脆弱性診断（脆弱性診断ツールによる自動スキャンや、専門家によるペネトレーションテスト等）を実施し、既知の脆弱性が存在しないかを確認します。またこの診断工程の中で、②で行った設定変更が正しく反映され、意図した通りに適切な設定状態が維持されているかについても確認します。

(2) 機能・統合テストの実施

製品やサービスのセキュリティ機能が、自組織の要件を満たし正しく動作するかを検証します。その後、自組織のシステム・サービスと統合した際に、セキュリティ機能が阻害されず、かつシステム・サービス全体として問題なく稼働するかを検証する統合テストを行います。

(3) 脆弱性診断・テスト結果の反映

脆弱性診断や統合テストの結果を踏まえ、脆弱性や設定不備が判明した場合には、本番移行前にセキュリティ修正プログラムの適用や、再度適切なソフトウェアの設定変更を実施し、リスクを排除します。

④ 関係者への周知

ソフトウェアに関する規約・マニュアル・契約の内容や、導入時の設定内容、脆弱性診断・テストの結果は、導入時の考慮事項として関係者で共有します。これによりソフトウェアが運用される上で、推奨されていない設定の変更や適切ではない使い方がされないように、関係者間でソフトウェアに対する理解を深めた上で、実際の運用に進みます。

IV. 運用

7 ソフトウェアの運用時における脆弱性対処

構築・調達形態に応じた利用方法

製品利用者における構築・調達形態に関わらず、運用時の脆弱性対処は必須の内容となるため、本ガイドの内容を確認し、実装してください。

特に、外部ソフトウェア製品の調達においてはソフトウェア製品の製品開発者が提供する情報を確認し、求められる対処を適切に実施すること、クラウド（SaaS）利用においてはサービス提供者が提供する情報を確認し、求められる対処を適切に実施することが重要になります。

また、自組織によるシステム・サービスの構築の場合、自組織の主体的な脆弱性対処が必要となるため、本ガイドの内容を確認・実装する上で、外部機関との連携は維持しつつ、自組織自らが脆弱性を発見するために定期的な脆弱性検査を定常業務に組み込むことも求められます。

意義

ソフトウェアの運用開始後に発見された脆弱性に素早く対処するには、脆弱性情報を収集する必要があります。脆弱性は日々発見されており、対処が後手に回らないように、定常的な情報収集が必要です。積極的に脆弱性情報を収集することで、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。

脆弱性が発見された際は、当該脆弱性が特定のソフトウェアに起因するものか、複数のソフトウェアまたは自組織のシステム・サービス全体に関わるものかを調査・検証します。その上で、発見された脆弱性についてリスク評価を行い、自組織への影響を踏まえ、優先順位づけを行った上で、セキュリティ修正プログラムの適用をはじめとする脆弱性の修正対策を、業務影響等を考慮しながら実施します。

脆弱性への適切な対処には、関係者への周知・教育が不可欠です。脆弱性への対処が遅れるとインシデントにつながる可能性もあります。その結果、自組織の顧客等のステークホルダーからの信頼低下に繋がりかねません。

実施内容

ソフトウェアについて、関連する脆弱性情報の収集、組織内外において発見された脆弱性の報告受付、新しい脆弱性を発見するための脆弱性検査を行います。

報告された脆弱性情報について、影響範囲を明らかにし、脆弱性の認定を行います。認定後は、トリアージに基づき、脆弱性の修正対策としてセキュリティ修正プログラムの適用等を行います。

脆弱性への対処が必要な場合には、修正対策の実施と関係者への周知を行います。

実施手順

① 製品と構成要素の脆弱性の監視

ソフトウェアとソフトウェアに組み込まれた構成要素に関する脆弱性情報を収集します。

ソフトウェアの脆弱性情報は、ソフトウェアの製品開発者や、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、自組織で運営しているサービス（ウェブサイトやウェブサービス）の場合、そのサービスの利用者からの不具合に関する問い合わせから、脆弱性が判明する場合もあります。これらの問い合わせも情報源として扱います。

② 脆弱性報告の受付

下記(1)～(2)の方法により、組織内外で発見された脆弱性について、組織として適切に報告を受付・対処します。

(1) 受付窓口の設置

組織内外に対し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。情報システム部門、IT・セキュリティ部門、CSIRT 等のセキュリティ関連部門が設けている問い合わせ窓口以外の窓口（広報部門や IR 部門）に脆弱性情報が報告される場合もあるため、そのような別目的の窓口に脆弱性の報告があった場合の対応を定め、周知します。

(2) 脆弱性情報の判断、連携

窓口に脆弱性情報の報告があった場合、当該脆弱性が特定のソフトウェアに起因するものか、複数のソフトウェアまたは自組織のシステム・サービス全体に関わるものかを検証します。検証結果を踏まえ、(1)で決めた報告ルートに従い、ソフトウェアの製品開発者や自組織内の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について、発見者に連絡するとともに、組織内外の関係者にも情報共有します。

③ 内部テストによる脆弱性の発見

脆弱性情報の収集や、組織内外からの脆弱性報告では発見されない新しい脆弱性を発見するため、定期的な脆弱性検査等を実施します。

④ 脆弱性の認定

脆弱性が発見された際、当該脆弱性のリスクを評価した上で、自組織への影響を検討します。検討の結果、自組織において対処が必要な脆弱性であると判断された場合、対処すべき脆弱性として認定します。

発見された脆弱性が複数にわたる場合や、発見された脆弱性が自組織の複数のシステム・サービスに影響がある場合、どこから対処を行うかの優先順位を検討します。優先順位の検討は、影響が及ぶ範囲や、事業への影響等を考慮して行います。

⑤ 修正対策の実施

発見された脆弱性への対策においては、脆弱性が発見されたソフトウェアの製品開発者や自組織内の構築チーム、外部委託先にセキュリティ修正プログラムの提供や、提供されるまでの暫定措置について依頼します。

セキュリティ修正プログラムが提供された後、自組織に展開する前に、検証環境においてセキュリティ修正プログラムを適用した上での動作確認を行い、既存のシステム・サービスの正常運用に影響しないかなどを確認します。また、こうした対策がもたらす業務への影響についても事前に考慮しておく必要があります。

また、セキュリティ修正プログラムを適用したことにより、システム・サービスに影響があった場合に備え、事前にバックアップを整備することも有効です。

一方で、セキュリティ修正プログラムを適用するためには、前述した通りシステム・サービスの一時停止などを伴う場合もあり、業務上の影響が予想されます。そのため、自組織内の関係者内でセキュリティ修正プログラムの適用範囲やスケジュールについて協議のうえ、合意を得ながら進める必要があります。

脆弱性へ修正対策を実施した後は、IT 資産およびソフトウェアの構成情報の変更を行い、資産台帳を更新します。

8 ソフトウェアの運用時にインシデントが発生した場合の対応

構築・調達形態に応じた利用方法

製品利用者における構築･調達形態のうち､外部ソフトウェア製品の調達､クラウド（SaaS）利用、外部委託によるシステム・サービスの構築、自社によるシステム・サービスの構築のすべての形態において、本項目の内容は必須となります。

構築・調達形態に関わらず、適切にインシデントに対応するために、本ガイドの内容を確認し、実装してください。

意義

ソフトウェアの脆弱性に起因したインシデントでは、自組織の機密情報への不正アクセスやマルウェア感染等による情報の漏えいや改ざん、破壊・消失、システム・サービスの機能停止など、さまざまな事象が起こり得ます。このような事象が及ぼす被害によって組織の経営や事業に重大な影響がもたらされる可能性があります。

ソフトウェアの脆弱性に対して、迅速にセキュリティ修正プログラムを適用することにより、インシデント発生による被害とその影響範囲を最小限に抑えられるようにすることが重要です。

実施内容

インシデント発生時には、「検知・初動対応」、「報告・公表」、「再発防止」の 3 つの段階における対応を実施します。

実施手順
① 検知・初動対応 下記(1)～(3)の方法により、インシデントを早期把握し、迅速に対応することで、インシデント発生による被害とその影響範囲を最小限に抑えます。 (1) 検知と連絡受付 社内でインシデントが疑われる兆候や実際の発生を発見した場合は、CSIRT に報告します。 第三者から通報を受け付けた場合は、通報者の連絡先等を控えます。 (2) 対応体制の構築 CSIRT は、対応すべきインシデントであると判断した場合に、速やかに経営者に報告します。 経営者は、速やかにインシデント対応のための体制（情報セキュリティ委員会や緊急対策会議等）を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確にします。 (3) 初動対応

初動対応として、外部からの問い合わせを受け付ける際の対応窓口を設置します。インシデントによる被害を受けた自組織の部門に対して、要員を派遣し、必要となる情報収集や、原因調査の支援を行います。

ただし、原因調査の支援では、対象機器の電源を切る等、不用意な操作により保全されるべき証拠が失われないようにします。

原因調査の結果、特定のソフトウェアの脆弱性に起因している可能性が判明した場合には、当該ソフトウェアの製品開発者の PSIRT の協力を得て、脆弱性の修正対策を進めることとなります。また、PSIRT から、関連する脅威指標の特定や、侵害されたか否かを判断するためのログの調査方法などの特定に協力を依頼されることがありますので、自組織の関係者間で対応を協議・検討するようにしてください。

② 報告・公表

インシデントの発生状況および被害拡大防止のための対策について、周知・報告を行います。

組織内の関係者には、社内メールや社内ポータルサイトを通じて、顧客などの社外関係者には自組織のウェブサイトや、営業担当者等を通じて連絡することが一案です。

③ 再発防止

インシデントを再発させないために根本原因を分析し、新たな対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討し、実施します。

インシデントが、製品開発者が既に修正対策を提供している既知の脆弱性に起因するものだった場合には、当該既知の脆弱性の修正対策情報を把握していたかどうか、把握していたけれども修正を適用できていなかったのか等を確認し、今後の類似事案の再発防止に努めてください。

V. 廃棄

9 ソフトウェアの廃棄時における脆弱性対処

構築・調達形態に応じた利用方法

製品利用者における構築･調達形態のうち､外部ソフトウェア製品の調達､クラウド(SaaS)利用、外部委託によるシステム・サービスの構築、自社によるシステム・サービスの構築のすべての形態において、本項目の内容は必須となります。

構築・調達形態に関わらず、廃棄前に適切な脆弱性対処を行い、リスクが残存することがないよう、本ガイドの内容を確認し、実装してください。また構築・調達形態に関わらず、自組織でセキュアな廃棄を行うことが困難な場合、専門の事業者にセキュアな廃棄を委託してください。

意義

ソフトウェアの製品開発者がソフトウェアのサポート終了を決定した場合や、自組織においてソフトウェアの利用終了を決定した場合には、当該ソフトウェアが不正アクセス等により保存された重要なデータが不正に窃取されることがないよう、速やかにセキュアな方法で廃棄を行うことが重要です。ソフトウェアが適用された機器・システムを廃棄する場合を含め、廃棄予定のソフトウェアが残置されている場合、時間の経過に伴って管理が行き届かなくなり、サイバー攻撃により被害を受けるリスクが高まります。

実施内容

ソフトウェアのセキュアな廃棄について、契約時に自組織とソフトウェアの製品開発者の間でサポート終了時期の事前通知や、自組織が行うべき対応事項等に関する取り決めを行います。

実施手順
① 製品開発者がソフトウェアのサポートを終了する際の対応 製品開発者がソフトウェアのサポート終了を決定した場合には、製品開発者に対し、契約時に取り決めた期日まで、サポート終了時期等を事前通知するとともに、当該ソフトウェアのセキュアな廃棄に必要な情報を継続的に利用できるように依頼します。 **② 自組織がソフトウェアの利用を終了する際の対応** 自組織がソフトウェアの使用終了を決定した場合には、ソフトウェアの利用規約や契約時の取り決めに従い、当該ソフトウェアに登録・保存されているデータの消去を適切に行います。 なお、データの消去はデータの機密性のレベルやデータが保存されている環境に応じた適切な消去方法を選択し、消去を確実に履行します。このような消去方法としては、下記(1)～(2)の方法について考慮します。 (1) ソフトウェアが適用された機器の記憶媒体に保存されているデータを消去する場合

高いレベルの機密性が求められるデータについては、記憶媒体の分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元不可能とします。また、そのような破壊を委託事業者に依頼する場合は、当該破壊の完了証明書により、消去が確実に履行されたことを確認します。それ以外のデータについては、ソフトウェアからアクセス可能なすべてのストレージ領域をデータ消去ソフトウェア等を用いて上書きして消去する上書き消去や、磁気的な消去、ブロック消去のうち、いずれかの消去を行い、確実に復元不可能とします。

(2) ソフトウェアと連携するクラウド環境に保存されているデータを消去する場合

共用を前提とするクラウド環境に保存されているデータについては、記録媒体の物理的な破壊や磁気的な消去ができないため、データを暗号化し、暗号化したデータを消去するとともに、データの復号を不可能とするため、鍵自体を消去する暗号化消去を行い、確実に復元不可能とします。

用語集

CISO

Chief Information Security Officer の略称であり、組織における情報セキュリティ対策の統括と、経営層としての意思決定を行う責任者。

CSIRT

Computer Security Incident Response Team の略称であり、情報セキュリティインシデントが発生した際、または発生の兆候を検知した際に、迅速に対応・解決するためのチーム。

CVSS

Common Vulnerability Scoring System の略称であり、情報システムの脆弱性に対する深刻度を、同一の基準で定量的に評価・スコアリングするためのオープンで汎用的な枠組み。

JVN iPedia

日本国内で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供するポータルサイト、およびデータベース。

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。本ガイドでは、製品開発者側において脆弱性対応を行う組織を指す。

SaaS

Software as a Service の略称であり、ソフトウェアの機能を、製品利用者の端末にインストールするのではなく、ネットワーク経由でクラウドサービスとして利用する提供形態。

SBOM

Software Bill of Materials の略称であり、特定のソフトウェアを構成するコンポーネント（OSS 等のライブラリ）やそのバージョン、依存関係などの情報をリスト化したソフトウェア部品表。

SLA

Service Level Agreement の略称であり、サービス提供者と製品利用者の間で、提供されるサービスの品質や役割分担について合意した文章。

インシデント（情報セキュリティインシデント）

ソフトウェアの脆弱性悪用等による、情報の漏えいや改ざん、破壊・消失、システム・サービスの機能停止など、組織の事業継続やセキュリティを脅かす事象。

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。

■ 脆弱性診断

システムやソフトウェアに対し、ツールによる自動スキャンや専門家の手動操作によって、既知の脆弱性や設定の不備が潜んでいないかを確認するテスト。

■ セキュリティ修正プログラム

ソフトウェアに発見された脆弱性や不具合を修正・解消するために、製品開発者から提供される追加のプログラムデータ。

■ 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。

■ トリアージ

新たに発見・報告された脆弱性に対して、リスクの大きさや事業への影響度を評価し、どの順序で対処を行うか優先順位を決定するプロセス。

■ 製品開発者

ソフトウェア、機器、クラウドサービス等を開発・構築し、市場や製品利用者に提供する組織。

■ 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。

別紙：製品利用者向けガイド チェックリスト

製品利用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	/9	実施済 レベルなし	/6	実施済 （レベル 1）	/3	実施済 （レベル 2）	/3	実施済 （レベル 3）	/3

カテゴリ	No	項目			チェック	備考
Ⅰ．計画・要件定義	1	脆弱性リスクを適切に管理するための人材・プロセス・技術の整備	レベル 1	CISO 等の経営層を含めた組織内の関係者が、適切な脆弱性リスクの管理を実現するために必要な役割と責務を定義します。		
			レベル 2	適切な脆弱性リスクの管理が組織内のシステム・サービス全体に網羅されるよう、CISO 等の経営層を含めた組織内の関係者が、必要な役割と責務を定義し、それらを実践できるよう、人材、プロセス、技術を整備します。		
			レベル 3	脆弱性リスクの管理対象となるシステム・サービスのリスクや影響範囲に応じて、外部委託の活用や組織間の連携強化を図りつつ、適切な脆弱性リスクの管理が組織内のシステム・サービス全体に網羅されるよう、CISO 等の経営層を含めた組織内の関係者が、必要な役割と責務を定義し、それらを実践できるよう、人材、プロセス、技術を整備します。		
	2	セキュアなシステム・サービスを構築するための方針・体制	レベル 1	セキュリティポリシーおよび構築・調達ポリシーを策定します。		
			レベル 2	セキュリティポリシーおよび構築・調達ポリシーを策定し、利用するソフトウェアやソフトウェアを導入したシステム・サービスが同ポリシーを遵守していることを確認します。		
			レベル 3	セキュリティポリシーおよび構築・調達ポリシーを策定し、利用するソフトウェアやソフトウェアを導入したシステム・サービスが同ポリシーを遵守しているこ		

				とを確認し、ソフトウェアやシステム・サービスのライフサイクル全体にわたってセキュリティが確保されていることを定期的に確認します。		
	3	脆弱性対処やインシデント対応を円滑に実施するための方針・体制	レベル 1	CSIRT を構築・維持し、セキュリティポリシーに従って、CSIRT がセキュリティ対処を実施するために必要な機能を定義します。		
			レベル 2	セキュリティポリシーを策定し、具体的な脆弱性対処やインシデント対応に係る規程類を策定し、CSIRT の活動上必要となる体制やプロセスを整備します。		
			レベル 3	CSIRT を構築・維持し、CSIRT がセキュリティポリシーに従ってセキュリティ対処を実施するために必要な機能を定義するとともに、脆弱性対処計画の策定やステークホルダー間の関係強化を通じて、CSIRT の活動上実効性のある体制やプロセスを整備します。		
II. 調達	4	セキュリティを確保するための調達	–			
III. 導入	5	ソフトウェアを導入するための IT 資産管理	–			
	6	ソフトウェアを導入する際における脆弱性対処	–			
IV. 運用	7	ソフトウェアの運用時における脆弱性対処	–			

	8	ソフトウェアの運用時にインシデントが発生した場合の対応	–		
V．廃棄	9	ソフトウェアの廃棄時における脆弱性対処	–		

製品利用者向けガイド

2026 年 3 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