令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第８編　具体的な構築・運用の実践　【レベル３】

第21章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

章の目的
第 21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明します。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を理解することを目的とします。

主な達成目標
◘ 実施例から工程を理解することで、中小企業が主体的に関与するポイントを理解すること ◘ 情報システムを導入する工程で、作成すべきドキュメントを理解すること ◘ 情報システムを導入する工程の中で、セキュリティ機能を実装、運用するポイントを理解すること

21-1. EC サイトの構築とセキュリティ機能の実装と運用

「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する方法と、セキュリティ機能を実装する方法について説明します。具体的に説明するために、EC サイトの導入を例にとって説明します。

EC サイト導入における全体概要は以下の通りです。

サービス・業務企画
EC サイトの事業目的と提供するサービスの具体的な方向性を定めるフェーズです。 ・ サービスの利用者の種類やニーズを特定します。（ペルソナ分析など） ・ 現状の業務フローを分析し、サービスの改善点を明確にします。
要件定義
サービスの実現に必要な機能と非機能の要件を定義します。 ・ 業務要件と機能要件を定義します。 ・ Fit＆Gap 分析を実施します。
調達
EC サイト開発に必要なリソースや外部業者を調達します。 ・ 調達仕様書を作成します。 ・ 適正価格で最適な業者を選定します。
設計・開発
プロジェクトの計画立案とその管理を行います。 ・ 設計・開発実施計画書を作成します。 ・ テストを管理し、また自社で品質を確認するために受入テストを実施します。
サービス・業務の運営と改善
サービスを運営しながら、必要に応じて改善を行います。 ・ EC サイト運営における業務マニュアルを作成します。 ・ 研修教育資料（業務マニュアルなど）を用いて、従業員に対して教育を実施します。
運用および保守
システムの安定稼動を維持しつつ、継続的な改善を行います。 ・ 運用・保守の詳細な作業内容や実施方法などを検討します。 ・ 運用・保守の改善を継続的に実施していきます。

セキュリティに関する要件は、適用宣言書をもとにして行います。セキュリティに関する要件を決める流れは以下の通りです。

1. **情報システムで取扱う情報資産に対して、リスクアセスメントを実施する。**
2. **リスクアセスメントの結果をもとに、必要な管理策を決定する。（適用宣言書の作成）**
3. **適用宣言書の内容を満たすように、非機能要件などでセキュリティ要件を決定する。**

※セキュリティ要件の詳細は「21-1-2.要件定義」で説明します。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

21-1-1. サービス・業務企画

本工程は、規模に関わらずすべての企業にとって重要です。顧客ニーズを理解し、現状の業務を分析した上で、新しいサービスや業務プロセスを計画することは、中小企業の成長と効率化に直結します。

利用者視点でのニーズ把握

サービスを検討するための大前提として、利用者の立場でサービスを受けることを想像し、利用者のニーズがどこにあるかを考えることが大切です。しかし、サービスを提供する側は、どうしても「提供者側の視点」に立ちがちになります。さまざまな利用者のそれぞれの立場でニーズを把握するための手法の１つとして、「ペルソナ分析」があります。

ペルソナ分析

「ペルソナ」とは、サービスの典型的な利用者の、目的、意識、行動などのパターンを構造化し、利用対象者を仮想の人物として定義するものです。例えばサービスのターゲットを「会社員」と抽象的に定義すると、検討チームのメンバーそれぞれが思い描く「会社員」の姿が異なるため、チームとして判断する際にブレが生じてしまいます。ペルソナ分析ではもっと具体的に「氏名、年齢、性別、家族構成、勤務先、仕事内容、そのほかの詳細条件」などを設定します。このような具体的な利用者像をイメージしながら検討を行うことで、利用者が抱える課題や問題を浮き彫りにし、具体性の高いアイデアを創出しやすくなります。

ペルソナの作り方

以下の企業を想定としたペルソナ作成の例を紹介します。

- 地方の特産品を扱う中小企業を想定
- 実店舗がある。

- EC サイトは現在なく、これから構築しようと検討している。
- 実店舗に加えて、販売窓口を増やしたいと考えている。

1.ターゲットとなる利用者に関する情報を収集する

- インタビュー・アンケート
  実店舗の来店者に対して、購入動機、どのような商品をオンラインで購入したいか、どのような購入体験を期待しているかを尋ねる。実店舗での顧客に対して、購入理由、購入頻度、地域とのつながりなどをアンケートにより収集する。

- Web 検索や公開調査データ
  EC サイトを利用する層（地域外の顧客や新規顧客）について、公開されている市場調査データを収集。

- 店舗の観察・ヒアリング
  店舗スタッフからのヒアリングにより、どのような顧客層が頻繁に訪れているのかを確認。

2.収集した情報を分析し、グルーピングする

- 地域住民か観光客か
  地域に住んでいるリピーター、観光目的で訪れた一見の顧客。

- 年齢層
  若年層、中年層、高齢層

- 購入動機
  日常の食材としての購入、贈答品としての購入、観光の記念品としての購入。

- 利用方法
  実店舗での対面購入、電話注文、リピーターによる定期購入。

3.グルーピングした情報から利用者像を具現化、ペルソナを作成

ペルソナの例:「地域住民のリピーター」	
名前	山田 花子（45 歳）
職業	地元の学校で働くパートタイムスタッフ
居住地	店舗のある地方都市

家族構成	夫と高校生の娘１人
趣味	地元のイベントや料理教室に参加すること
価値観	地元の発展に貢献することを大切にしており、地元産品の購入を積極的に行う。安全で新鮮な食品を求めるため、実店舗で直接商品を見て購入することに安心感を得ている。
利用動機	日常の食材として地元の特産品を購入。特に週末に家族で食事を楽しむため、実店舗で定期的に訪れて新しい商品を見つけるのを楽しみにしている。
購入経路	現在は実店舗での対面購入を利用。EC サイトが構築されれば、忙しいときでもオンラインで注文し、自宅での受け取りや店舗での受け取りができることに興味を持っている。

ペルソナの案を作成後、ターゲットとなる利用者と直に接している人などに、実際の利用者像とかけ離れたところがないか、ターゲットたる利用者としてふさわしいかを確認してもらいます。実際の利用者像と作成したペルソナにかい離が見られた場合は、随時内容を修正してください。

業務の現状把握

業務を観察した結果は、多くのドキュメントとしてまとめられることがあり、分析に関わった人は内容を理解できますが、初めて読む人にはポイントを把握することが難しいことがあります。プロジェクト内部の従業員や外部の関係者、システム開発事業者など、多様な立場の人が内容を確認する必要があるため、業務の状況を誰にでもわかりやすく伝えるために、業務フローなどを用いた視覚的にわかりやすい資料を作成することが重要です。

業務フローの作成

業務フローは、現在行っている業務を「誰が（どの組織が）」「いつ」「何を」「どの順番で」実施しているか、「どの範囲が情報システム化されているか」を可視化するものです。対策の検討や企画後の業務内容の変化箇所を特定するためにも有効です。

業務フローには、現行（AsIs）と将来（ToBe）があります。はじめに作成するのは、現行の業務フローです。業務フローの書き方については、さまざまな表記方法があります。基本的に、関係者にとってわかりやすい表記であれば、どのような表記方法でも問題ないです。縦に流れるフローでも、横に流れるフローでも、どちらでも構いません。

例：お客様が実店舗で商品を購入するフロー

- 地方の特産品を扱う中小企業を想定
- 実店舗での商品購入フロー

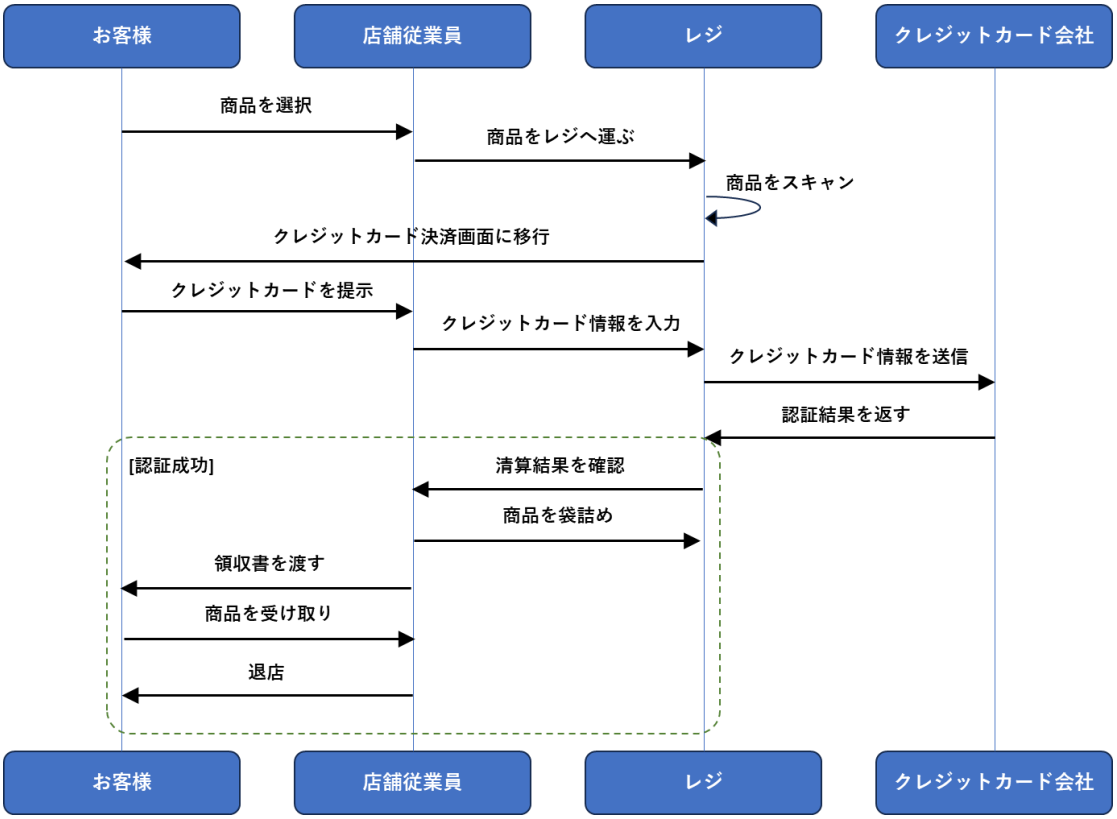

図 83. 実店舗で商品を購入するフロー例

サービス・業務企画内容の検討

現状把握が終わった後は、企画案を練り上げます。企画案の方向性がある程度決まったら、プロジェクト内外の関係者にわかりやすく説明し、改善点のフィードバックを受け取るために、将来（ToBe）の業務フローを活用します。現行（AsIs）の業務フローをもとに、将来どこがどのように変わるのかを明確に示し、変更点とその効果を具体的に示します。関係者と目指す姿を共有できるようにするために、業務フローに吹き出しを付けることは効果的です。

例：お客様が EC サイトで商品を購入するフロー

- 地方の特産品を扱う中小企業を想定
- 実店舗での商品購入フローをもとに、EC サイトでの購入フローを作成

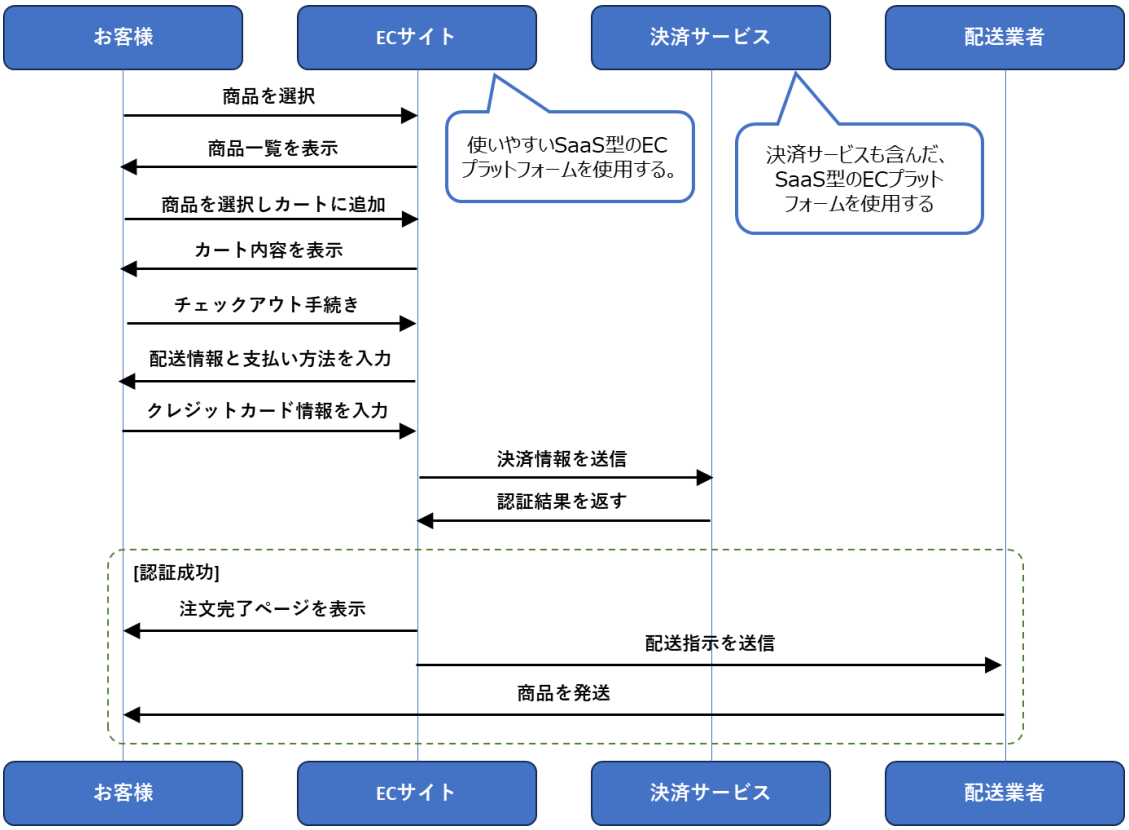

図 84. EC サイトで商品を購入するフロー例

21-1-2. 要件定義

RFI や事業者からの情報収集といった活動を通して、市場にあるサービスや他社の事例などを把握します。その上で、情報システムを導入する際、明確な要件を定義することは中小企業にとっても非常に重要です。必要な機能を確実に実装し、パフォーマンスや信頼性などの非機能要件も満たすことができます。

セキュリティに関する要件については、適用宣言書に基づいて決定することが重要です。

一貫性を持った要件定義書の作成

要件定義の内容を記した文書は、プロジェクト管理を行うチームや担当者と事業者がサービス・業務や情報システムの目指すべき姿を共有するとともに、事業者との契約上の合意文書となる重要なものであるため、誤った定義や曖昧な定義が行われると、後続の工程に重大な影響を与えます。

そのため、要件定義の内容は次に示す点を参考に、正確で一貫性のある記載となるようにし、受託業者の解釈によりブレない内容とすることが重要です。

- 曖昧な用語や一般的な意味と異なる使い方をしている用語などは、プロジェクト関係者間での認識の齟齬を防止するため、用語の定義および機能を定義する粒度や深さについて統一す

る。

- 要件定義書の「業務要件定義」のインプットであるサービス・業務企画の内容とも整合の取れた区分、順番で機能を記載する。業務の単位ごとに記載する場合も、共通処理機能を識別できるように整理するなど、機能数を把握できるように記載する。
- 機能の説明は、箇条書きなどにして簡潔に記載する。既存のサービス・業務や情報システムの変更を行う際の要件定義では、追加・変更となる要件が明確になるよう、変更箇所の記載ルールを定めて記載を統一する。

機能要件の定義

機能要件として定義しないといけない内容は５つです。

- 機能
- 画面
- 帳票
- データ
- 外部インターフェース

要件定義の対象となる情報システムによっては、このうちの一部を定義しない場合もあります。例えば、他の情報システムと連携しない Web サイトであれば外部インターフェースの定義は不要となります。

機能に関する事項

「機能」とは、情報システムが外部に価値を提供する一連の動作のまとまりのことです。基本的に「入力」・「演算（処理）」・「出力」で構成されます。ボタンを押したら画面に情報が表示されるのも、夜間にバッチ処理で帳票が大量に印刷されるのも、それぞれ 1 つの機能です。情報システムが提供する形はさまざまですが、それらを「機能」としてリスト化して整理するために用いるものが、「情報システム機能一覧」と呼ばれるドキュメントです。

情報システム機能一覧（例）

NO	機能 ID	機能分類	機能名	機能概要			処理方式	利用者区分	現状の機能との差異
				入力	処理	出力			
1	XXX	新規ユーザー登録	新規ユーザー登録機能	記載事項の入力	・・・	・・・	オンライン	新規登録申込者	・・・
2	XXX	新規ユー	新規ユー	出力方式	・・・	新規登録	オンラ	新規登	・・・

		ザー出力	ザー出力機能	の選択		申込書の出力	イン	録申込者	

画面に関する事項

情報システムの画面は、利用者が業務の流れの中で情報システムとやり取りを行う窓口となるため、画面上で取扱う情報の種類、画面を構成する要素の配置は、利用者の業務効率や満足度に大きな影響を与えます。

この画面に関する要件を取りまとめるドキュメントは、一般的に画面一覧、画面イメージ（画面モックアップ）、画面遷移図、画面設計方針書（画面設計ポリシー）と呼ばれるもので構成されています。

画面一覧（例）

NO	画面ID	画面分類	画面名	画面概要	画面入出力要件	画面設計要件	該当機能	利用者区分
1	XXXX	新規ユーザー登録画面	新規ユーザー登録作成	新規ユーザー登録の作成画面	表示方法：… 入力操作概要：…	Web ブラウザで表示可能であること。	機能ID：XXXX	新規ユーザー登録者
2	XXXX		新規ユーザー登録確認	新規ユーザー登録の作成確認画面	表示方法：… 入力操作概要：…	…	機能ID：XXXX	新規ユーザー登録者

帳票に関する事項

情報システムの帳票とは、サービス・業務で使用するために情報システムから出力した紙や PDF 形式などの電子帳票を指します。帳票は、利用者が業務上意識して用いられるものであるため、業務の内容やきっかけと結びついた重要な情報を持ちます。帳票に関する要件を取りまとめるドキュメントは、一般的に帳票一覧、帳票イメージ、帳票設計方針書（帳票設計ポリシー）と呼ばれるもので構成されています。

帳票一覧の例

NO	帳票ID	帳票名	帳票概要	入出力の区分	帳票入出力要件	帳票設計要件	入出力形式	該当機能	利用者区分
1	XX	○○申込書	○○申込	出力	モノクロ印刷	用紙サイズ：A4	紙	機能 ID：XX	○○申込者
2	XX	△△申込書	△△申込	出力	カラー印刷	用紙サイズ：A4	PDF	機能 ID：XX	△△申込者

データに関する事項

情報システムで取扱うデータに関して機密性レベル別に分類し、その管理方法を定義しておく必要があります。システム内に存在することになるデータに関して、その機密性を認識し、分類し、またその管理方法を「データ要件」として記述することにより、その後の設計・開発作業に確実につなげていくことができます。データに関する要件を取りまとめる際には、データモデル、データ一覧、データ定義などのドキュメントを整備することが重要です。

データ要件を取りまとめる際に整備するドキュメント（例）

NO	ドキュメント名	説明
1	データモデル	・ 画面や帳票などに含まれる情報を抜き出して、意味のある単位（識別キー）ごとにまとめた情報の集合体である「データ」と、他のデータとの関連を 1 枚に表現した図で、ER（Entity Relationship）図という表記法で記述します。 ・ 基本的に 1 つのデータ項目は、必ずどこか 1 ヶ所のデータのみに属するようにデータを定義します（これを「正規化」といいます）。
2	データ一覧	・ データがどのようなまとまりの単位になっているかを一覧形式で示す表で、データモデルやデータ定義の目次として利用されます。 ・ マスターデータとマスターデータ以外に分け、データの用途や保存期間、データ件数などを定義します。
3	データ定義	・ データ一覧にあるデータのまとまり単位にそれぞれに含まれるデータ項目の内容・説明を示す表です。

外部インターフェースに関する事項

情報システムの外部インターフェースとは、サービス・業務の内容を実現するために、自分の情報システムが他の情報システムと連携して情報を受け渡す仕組みです。情報連携の内容や形式・仕

組みにはさまざまなものがあり、明確に定義する必要がありますが、連携先である他の情報システムの都合もあるため、双方の要件を出し合い、すり合わせることが必要となります。この外部インターフェースに関する要件を取りまとめるドキュメントは、一般的に外部インターフェース一覧と呼ばれます。

外部インターフェース一覧（例）

NO	外部インターフェース ID	外部インターフェース名	外部インターフェース概要	相手システム	送受信区分	実装方式	送受信データ	送受信タイミング	送受信の条件
1	XXXX	申込者情報連携	申込の審査に関わる申請者の情報を○○システムから日次で取得する	○○システム	受信	API	申込者情報	リアルタイム	日次
2	XXXX	申込結果連携	承認された申込情報を○○システムに日次で提供する。	○○システム	送信	ファイル共有	承認済み申込者情報	リアルタイム	日次

非機能要件の定義

非機能要件として定義しないといけない内容は次に挙げる 17 の事項です。
非機能要件は、安定的なサービスの継続に重要です。

- 情報セキュリティに関する事項
- ユーザビリティおよびアクセシビリティに関する事項
- システム方式に関する事項
- 規模に関する事項
- 性能に関する事項
- 信頼性に関する事項
- 拡張性に関する事項
- 上位互換性に関する事項
- 中立性に関する事項
- 継続性に関する事項
- 情報システム稼動環境に関する事項

- テストに関する事項
- 移行に関する事項
- 引継ぎに関する事項
- 教育に関する事項
- 運用に関する事項
- 保守に関する事項

機能要件の場合は、内容の一部を定義せず、調達時の事業者の提案に委ねることもあります。しかし、非機能要件の場合は基本的にすべての項目を定義します。情報システムやプロジェクトの特性によって、定義すべき内容の量は異なります。

情報セキュリティに関する事項

セキュリティに関する要件の決定は、適用宣言書をもとにして行います。セキュリティ要件を決める流れは以下の通りです。

1. 情報システムで取扱う情報資産に対して、リスクアセスメントを実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。（適用宣言書の作成）
3. 適用宣言書の内容を満たすように、セキュリティ要件を決定する。

※リスクアセスメントの実施方法の詳細については、「12-2.リスクマネジメント：リスクアセスメント」を参照してください。

EC サイトにおいて、セキュリティ要件を決める例

1.リスクアセスメントの実施

ステップ 1:情報資産の特定

EC サイトで取扱う主な情報資産は以下の通りです。

情報資産名	内容
顧客情報	氏名、住所、電話番号、メールアドレス、クレジットカード情報など
注文情報	商品名、購入日、購入金額など
在庫情報	商品の在庫数、入荷予定など
支払い情報	クレジットカード情報、銀行口座情報など

ステップ 2:リスク特定

各情報資産に対する脅威と脆弱性を特定します。

情報資産名	脅威	脆弱性
顧客情報	データの漏えい、フィッシング攻撃	弱いパスワード、暗号化されていないデータ通信
注文情報	改ざん、不正アクセス	セキュリティパッチの未適用、不適切なアクセス権限管理
在庫情報	データの改ざん、誤った更新	適切な監査ログがない、アクセス制御の欠如
支払い情報	クレジットカード情報の盗難、不正取引	PCI DSS に準拠していないサービスの利用、暗号化されていないストレージ

ステップ 3:リスク分析

脅威と脆弱性がもたらすリスクを評価し、リスクレベルを「高」「中」「低」に分類します。

情報資産名	リスクレベル
顧客情報の漏えい	高
注文情報の改ざん	中
在庫情報の誤った更新	中
支払い情報の盗難	高

ステップ 4:リスク評価

リスク分析の結果をもとに、リスクの優先順位を決定し、それに対する対応策（リスク軽減、リスク回避、リスク受容など）を検討します。

2.適用宣言書の作成

リスクアセスメントの結果に基づいて、管理策を導入する適用宣言書を作成します。

※管理策は、ISMS の管理策だけでなく CSF2.0 の管理策も参考にできます。CSF2.0 の管理策については、「付録：CSF2.0」を参照してください。

情報資産	リスク内容	リスクレベル	適用する管理策
顧客情報（氏名、住所、電話番号、メールアドレス、クレジ	不正アクセスによる個人情報の漏えい	高	情報セキュリティのための方針群（5.1） 個人情報の取扱いに関する方針を策定し、従業員に周知。 アクセス制御（5.15）

ットカード情報）			顧客情報へのアクセス権を最小限に制限。 暗号の利用（8.24） 顧客情報を保存時・転送時に暗号化。
注文情報（商品名、購入日、購入金額など）	不正なデータ改ざんや漏えい	中	アクセス制御（5.15） 注文情報へのアクセスを業務上必要な従業員に限定。 情報セキュリティインシデント管理の計画策定および準備（5.24） 注文情報の改ざんや漏えいが発生した場合の対応手順を整備。
在庫情報（商品在庫数、入荷予定など）	内部関係者による不正なアクセス	中	情報セキュリティの意識向上、教育および訓練（6.3） 従業員に対するセキュリティ教育を実施し、在庫情報の取扱いに関するリスクを軽減。 アクセス制御（5.15） 在庫情報システムへのアクセスを制限。
支払い情報（クレジットカード情報、銀行口座情報）	クレジットカード情報や銀行口座情報の盗難・不正利用	高	暗号の利用（8.24） 支払い情報は保存時および転送時に暗号化。 アクセス制御（5.15） 支払い情報へのアクセスを厳格に制限。 ログ取得（8.15） 支払い情報に関する操作の記録を保護し、監視を実施。

3.セキュリティ要件の定義

適用宣言書を満たすためのセキュリティ要件を定義します。

セキュリティに関する要件定義の例
1.セキュリティ要件 1.1 顧客情報の保護 要件 1.1.1:顧客情報（氏名、住所、電話番号、メールアドレス、クレジットカード情報）は、すべて暗号化技術を用いて保存および転送すること。 要件 1.1.2:顧客情報へのアクセスは、役割ベースで制限し、必要な従業員のみに許可すること。アクセス権は定期的にレビューし、不要な権限は削除すること。

要件 1.1.3:顧客情報の取扱いに関するセキュリティポリシーを文書化し、全従業員に周知すること。ポリシーの順守状況を定期的に監査すること。

1.2 注文情報の保護
要件 1.2.1:注文情報（商品名、購入日、購入金額）は、適切なアクセス制御により保護し、業務上必要な従業員のみがアクセスできること。
要件 1.2.2:注文情報の改ざんや漏えいが発生した場合のインシデント対応手順を整備し、インシデントの発生時には即座に対応できる体制を構築すること。

1.3 在庫情報の保護
要件 1.3.1:在庫情報（商品在庫数、入荷予定など）へのアクセスは、必要最低限の従業員のみに制限すること。アクセス制御リストは定期的に見直し、不要なアクセス権は削除すること。
要件 1.3.2:在庫情報に関するセキュリティ教育を実施し、従業員が適切に情報を取扱うようにすること。教育内容には、在庫情報の重要性とリスクについても含めること。

1.4 支払い情報の保護
要件 1.4.1:支払い情報（クレジットカード情報、銀行口座情報）は、保存時および転送時に暗号化技術を用いて保護すること。
要件 1.4.2:支払い情報へのアクセスは、業務上必要な従業員に限定し、アクセス権は厳格に管理すること。アクセスログは定期的にレビューすること。
要件 1.4.3:支払い情報に関する操作ログを記録し、改ざんや削除を防ぐための保護を施すこと。ログの保管には、セキュアなストレージを使用し、バックアップを定期的に取得すること。

2.可用性要件
2.1 システムの高可用性
要件 2.1.1:システムは 24 時間 365 日稼動し続けること。メンテナンスやアップグレード時には、事前に計画を立て、影響を最小限に抑えること。
要件 2.1.2:システム障害発生時の迅速な復旧を支援するために、定期的なバックアップを実施し、災害復旧計画を策定すること。

3.パフォーマンス要件
3.1 応答時間
要件 3.1.1:ユーザーからの要求に対する応答時間は、システムの種類に応じて以下の基準を満たすこと。

Web ページの表示:3 秒以内
データベースクエリの実行:2 秒以内

4.コンプライアンス要件

4.1 法令順守

要件 4.1.1:個人情報保護法、クレジットカード業界の規制、電子商取引に関する規制など、関連する法令や規制を順守するためのプロセスを確立し、定期的な監査を実施すること。

EC サイトの構築時におけるセキュリティ対策要件

IPA が公開している「EC サイト構築・運用セキュリティガイドライン」では、EC サイトの構築時におけるセキュリティ対策要件を示しています。要件ごとに求められるセキュリティの水準に応じて、「必須」、「必要」、「推奨」を定め、それぞれ表中の区分に表記しています。

「必須」は、EC サイト運営事業者が EC サイトのセキュリティを確保する上で早急かつ確実な対策実施が求められるものであり、実装が必須として求められる内容と定義しています。

「必要」は、事業の重要度、対策費用、対策までの期間、対策を実施しないことによる影響度など、または他の代替策を実施するなどを考慮して導入時期を検討した上で実装が求められる内容と定義しています。

「推奨」は、EC サイト運営事業者がサイバー被害を受けるリスクの低減、被害範囲の拡大防止、EC サイトを復旧する場合において、対策実施が求められるものであり、事業の重要度、影響度などを考慮した上で、EC サイト運営事業者が各自の責任において、その実装を検討すべき内容と定義しています。

「必須」の要件については必ず実装することが重要ですが、「必要」、「推奨」の要件ついては、自社の適用宣言書に基づき、実装を検討することが大切です。

NO	セキュリティ対策要件（構築時）	区分
要件 1	「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」に準拠して、EC サイトを構築する。	必須
要件 2	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須
要件 3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須
要件 4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須
要件 5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須
要件 6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セ	必須

	キュリティガイドライン」を順守する。	
要件 7	サイト利用者情報の登録時およびパスワード入力時における、不正ログイン対策を実施する。	必須
要件 8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須
要件 9	ドメイン名の正当性証明と TLS の利用を行う。	必須
要件 10	サイト利用者のログイン時における二要素認証を導入する。	必要
要件 11	サイト利用者のパスワードの初期化および変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要
要件 12	Web サーバや Web アプリケーションなどのログや、取引データなどのバックアップデータを保管する。	必要
要件 13	保管するログやバックアップデータを保護する。	推奨
要件 14	サーバおよび管理端末において、セキュリティ対策を実施する。	推奨

EC サイトの構築時におけるセキュリティ対策要件一覧
（出典）IPA「EC サイト構築・運用セキュリティガイドライン」をもとに作成

要件 1.「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」に準拠して、EC サイトを構築する。

「詳細理解のため参考となる文献（参考文献）」に掲げた「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」では、「ウェブアプリケーションのセキュリティ実装」として、「脆弱性関連情報の届出制度」で届出の多かったものや攻撃による影響度が大きい脆弱性である、SQL インジェクション、OS コマンド・インジェクションやクロスサイト・スクリプティングなど 11 種類の脆弱性を取り上げています。それぞれの脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴などを解説し、脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を期待できる対策を示しています。

また、「ウェブサイトの安全性向上のための取組」として、ウェブサーバのセキュリティ対策やフィッシング詐欺を助長しないための対策など 7 つの項目を取り上げています。主に運用面からウェブサイト全体の安全性を向上させるための方策を示していますので、IPA の「EC サイト構築・運用セキュリティガイドライン」を参考にして EC サイトを構築してください。

なお、EC サイトの構築を委託する場合は、外部委託先事業者にガイドラインを参考にして構築することを依頼してください。

詳細理解のため参考となる文献（参考文献）	
安全なウェブサイトの作り方	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf
セキュリティ実装チェックリスト	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

要件 2.サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。

EC サイトを構築する場合、次のように利用しているソフトウェアへの脆弱性対策を実施することが重要です。

- 脆弱性情報などセキュリティに関連する情報を公表している EC サイト構築プログラムを選定してください。
- EC サイトを構成するソフトウェア（サーバと管理端末の OS、ミドルウェアとライブラリ、または、Web アプリケーションなど）を確認の上、一覧にまとめ、それぞれのソフトウェアに関する脆弱性情報などセキュリティに関連する情報を収集して管理し、それらの情報の内容を把握してください。
- EC サイトの構築時に利用しているサーバおよび管理端末の OS、ミドルウェアおよびライブラリ、または、Web アプリケーションや OSS などのソフトウェアについては、その時点の最新バージョンを使用してください。
- 利用しているソフトウェアなどについて、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は公開までにセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響がないことを確認（動作検証）してください。それ以外の脆弱性については、セキュリティパッチの適用や最新版へのバージョンアップを行うか否かを、脆弱性によるシステムへの影響などを考慮して判断してください。

要件 3.EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する

EC サイトを新規に構築した際は、EC サイトを公開するまでに脆弱性対策を実施する期間を確保して、次のような第三者による EC サイトへの脆弱性診断を実施して、EC サイトに脆弱性がないかを確認し、発見された危険度「高」、「中」の脆弱性への対策を行った上で公開してください。

- 脆弱性診断は、原則、第三者（外部委託先事業者、自社以外の第三者）による脆弱性診断を実施し、実施する脆弱性診断は、プラットフォーム診断、Web アプリケーション診断の 2 種類を実施してください。

- Web アプリケーション診断の実施範囲は、最低でも以下の画面について脆弱性診断を実施してください。
    - ログイン画面
    - サイト利用者情報登録/変更画面
    - 商品検索画面

・　注文・決済画面など

- 脆弱性診断を第三者に依頼する場合は、IPA が公開している「情報セキュリティサービス基準適合サービスリスト」にある「脆弱性診断サービス」に記載されている事業者を選定することを推奨します。

- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、「中」、「低」の 3 段階で分類されており、危険度「高」、「中」については、対策を行った上で EC サイトを公開してください。

One Point

脆弱性診断を実施する上で参考にしていただきたいこと

【脆弱性診断の目的】

脆弱性診断は、EC サイトがサイバー攻撃を受けて被害をまねく元となる脆弱性が存在していないかを調べるために行う、とても重要で必要な工程です。もし脆弱性が見つかった場合、脆弱性による EC サイトへの影響度を確認する必要があります。見つかった脆弱性の危険度および、脆弱性による EC サイトへの影響度により、対応の要否を判断して、対応をすることが重要です。

【脆弱性診断の種類】

脆弱性診断は、診断対象、診断方法によって、以下のものがあります。

＜診断対象＞

・　プラットフォーム診断：サーバやネットワーク機器などの OS やミドルウェアを診断します。
・　Web アプリケーション診断：Web サーバ上で動作するアプリケーションを診断します。

＜診断方法＞

・　ツールによる診断：ツールにより自動で診断します。ツールによって診断できる範囲が異なります。（ツールには無償のものと有償のものがあります。）
・　手動による診断：人手により診断します。
・　ハイブリッド診断：ツールでの診断が難しい箇所（人による判断が必要な場合）を人手で行うといった両者を組み合わせて診断します。

※手動による診断は、ツールによる診断に比べて費用が高額となります。手動による診断は、ツールでは見つけられない脆弱性を発見でき、ツールによる診断と組み合わせることで結果として精度の高い診断が可能です。

【脆弱性診断の実施者】
ツールで自動的に診断できる部分があるとはいえ、ツールの使用や診断結果を判断するため、脆弱性診断を行う人はそれなりのスキルが必要になります。自社に脆弱性診断を実施する技術者がいない場合は、脆弱性診断サービスの利用を検討することが重要です。

要件 4.管理者画面や管理用ソフトウェアへ接続する端末を制限する。

管理者画面や管理用ソフトウェアにアクセスするための ID・パスワードが攻撃者に漏えいすると、サイト利用者の顧客情報や、注文・取引データなどが大量に漏えいすることにつながるおそれがあるため、次のように厳重に管理することが重要です。

- 管理者画面や管理用ソフトウェアにアクセスするための ID・パスワードが不正に取得された場合に備えて、アクセスできる端末を制限するための IP アドレス接続制限や、アクセスできる利用者を制限するために、二要素認証（ID とパスワードによる認証後に SMS（ショートメッセージサービス）などでの認証を行う方法）を導入してください。

要件 5.管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。

管理者画面や管理用ソフトウェアへのアクセスに用いる端末がマルウェアに感染すると、端末内部および、当該端末がアクセス可能なサーバなどに保管しているサイト利用者の顧客情報や、注文・取引データなどが外部に送信されるおそれがあります。アクセスする端末に対して、マルウェア対策ソフトウェアを導入し、リアルタイム検知の実施および、定義ファイルの更新、端末のフルスキャンなどの定期的（1 回/日を推奨）な実施や、USB メモリなど外部記憶媒体の利用制限を通じて、マルウェア感染防止対策を行うことが重要です。

要件 6.クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を順守する。

クレジットカード決済を提供する場合には、割賦販売法におけるセキュリティ要求事項を反映した、クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」（カード情報の非保持化、カード決済の EMV 3D セキュアの導入など）を順守するとともに、契約するクレジットカード会社および決済代行会社（PSP）とコミュニケーションを取り、常に最新のセキュリティ対策の実施を検討してください。

要件 7.サイト利用者情報の登録時およびパスワード入力時における、不正ログイン対策を実施する。

サイト利用者のパスワードが攻撃者に漏えいすると、サイト利用者の個人情報や、注文・取引データなどの漏えいにつながるおそれがあるため、次のような不正ログイン対策を実施することが重

要です。

- サイト利用者がパスワードを登録する際に 10 文字以上、英大文字と小文字、数字、記号を組み合わせて、推測困難なパスワードを登録するようにしてください。また、推測されやすいパスワードは登録できないようにすることが重要です。
- ログイン用の ID とパスワードのすべてのパターンを機械的に繰り返し入力し、EC サイト利用者の ID とパスワードを盗み出すという総当たり攻撃に備えて、パスワードなどの入力間違いの回数が一定数（10 回以下を推奨）を超えた場合はアカウントをロックするようにしてください。

要件 8.サイト利用者の個人情報に対して安全管理措置を講じる。

個人情報保護法第二十三条（安全管理措置）に基づき、EC サイトの運用を通じて取扱う個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のために必要かつ適切な措置（個人データの取扱規定の整備、個人データを保存するシステム、機器および電子媒体の盗難、漏えいの防止、システム、機器へのアクセス制御、不正アクセス防止など）を講じる必要があります。

要件 9.ドメイン名の正当性証明と TLS の利用を行う。

EC サイト利用者が ID とパスワードを不正に窃取するフィッシングサイトではないこと（正規のサイトであること）を確認できるようにするためには、TLS/SSL 証明書などを導入し正当性証明を行うこと、および TLS（Transport Layer Security）の利用により通信を暗号化することが重要です。

要件 10.サイト利用者のログイン時における二要素認証を導入する。

なりすましなどによる不正ログインが行われる可能性が高い（ある）と判断した場合には、ID とパスワードを用いたサイト利用者の認証に加えて、安全性を高められる二要素認証（ID とパスワードによる認証後に SMS などでの認証を行う方法）を導入します。

要件 11.サイト利用者のパスワードの初期化および変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。

正規サイトを装ったフィッシングサイトや、パスワードの変更などを行うように不正に誘導するフィッシングメールにだまされて、サイト利用者が気づかないうちに ID とパスワードを盗まれることがあります。そのため、なりすまされて登録情報を変更されたことにサイト利用者が気づくことができるようにするために、EC サイト利用者のメールアドレスの登録および変更、パスワードの初期化および変更、アカウントの登録および削除、決済処理時といった重要な処理を実行した際に、メールや SMS などを用いて、サイト利用者への通知を行うようにします。

要件 12.Web サーバや Web アプリケーションなどのログや、取引データなどのバックアップデータを保管する。

顧客情報の漏えい事故を発生させてしまった場合には、事故の原因究明のためにフォレンジック調査会社に依頼します。フォレンジック調査で原因究明を徹底的に行うためには、調査に必要なデータが十分に揃っていることが必要となるため、Web サーバや Web アプリケーションのログや、取引データなどのバックアップデータ（該当サーバ以外の外部ストレージサービスや、自社管理のサーバへの保管など）を過去 1 年間分以上保管しておくようにしましょう。

フォレンジック調査の依頼先は、IPA が公開している「情報セキュリティサービス基準適合サービスリスト」にある、「デジタルフォレンジックサービス」に記載されている事業者を参考にすると良いでしょう。

また、レンタルサーバ事業者を利用する場合は、Web サーバのアクセスログなどの保管および提供が可能な事業者を選ぶようにしましょう。

要件 13.保管するログやバックアップデータを保護する。

Web サーバのログおよび Web アプリケーションのログ、取引データなどのバックアップデータを過去 1 年間分以上保管していても、保管ログおよびデータへの不正アクセスがあれば、前述したフォレンジック調査による原因究明に支障が生じ、誤った結果が導かれるおそれがあります。このため、ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないような対策を実施する必要があります。

要件 14.サーバおよび管理端末において、セキュリティ対策を実施する。

サーバおよび管理端末自体がマルウェアに感染すると、サーバや管理端末内部に保管しているサイト利用者の顧客情報や、注文・取引データなどが外部に送信されるおそれがあるため、マルウェア対策ソフトウェアを導入し、リアルタイム検知の実施および、定義ファイルの更新、ファイル・メモリのスキャンなどの定期的（1 回/日を推奨）な実施や、USB メモリなど外部記憶媒体の利用制限を通じて、マルウェア感染防止対策を行うことが必要です。

EC サイトの構築時に有効な CSF2.0 の管理策（例）

セキュリティ対策の要件を決める際は、CSF2.0 の管理策を参考にすることも有効です。

有効な管理策の例
パッチ適用に関する管理策 ● GV.SC-09:サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリスク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイクル全体を通じて監視される。 ● ID.RA-01:資産の脆弱性を特定、検証、記録する。

- PR.AT-01:要員は、サイバーセキュリティリスクを念頭において一般的な業務を遂行するための知識と技能を有するよう、意識向上とトレーニングを受ける。
- PR.PS-02:ソフトウェアはリスクに見合った保守、交換、削除が行われる。

など

認証に関する管理策

- PR.AA-01:許可されたユーザー、サービス、およびハードウェアの ID とクレデンシャルが組織によって管理される。
- PR.AA-03：ユーザー、サービス、ハードウェアを認証する。

など

バックアップに関する管理策

- PR.DS-11:データのバックアップが作成、保護、維持、およびテストされる。
- RC.RP-03:バックアップやそのほかのリストア資産をリストアに使用する前に、その完全性を検証する。

など

※各管理策の詳細は、「付録：CSF2.0」を参照してください。

詳細理解のため参考となる文献（参考文献）	
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html
情報セキュリティサービス基準適合サービスリスト	https://www.ipa.go.jp/security/service_list.html
脆弱性診断サービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20240611_2.pdf
デジタルフォレンジックサービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20240611_3.pdf

ユーザビリティおよびアクセシビリティに関する事項

ユーザビリティとは、利用者がサービス・業務を利用して実施したいことを、ミスなく効率的に行うために必要となる事項であり、アクセシビリティは、目的の情報へのたどり着きやすさを指します。どちらも利用者の年齢、身体的制約、利用環境などの違いによる配慮が必要です。

EC サイト構築におけるユーザビリティの要件（例）

NO	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成 （直観・シンプル）	・ 利用者が何をすれば良いか直感的に理解できるデザインにすること。 ・ 無駄な情報、凝ったデザイン、不要な機能を排したシンプルでわかりやすい画面にすること。

2	画面の構成 （フォントおよび文字サイズ）	・ 十分な視認性のあるフォントおよび文字サイズを使用すること。 ・ 画面サイズや位置を変更できること。 ・ 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成 （マルチデバイス対応）	・ スマートフォン、タブレット端末により本サービスを利用する利用者を想定し、これら端末の特性を考慮した画面にすること。 ・ レスポンシブ Web デザインにより、PC、タブレット端末、スマートフォンなどの利用環境を問わず、同一の情報をグリッドレイアウトなどの適切なレイアウトにより表示できるようにすること。
4	画面遷移	・ 利用者が次の処理を想像しやすい画面遷移とすること。 ・ 無駄な画面遷移を排除し、シンプルな操作とすること。

EC サイト構築におけるアクセシビリティの要件（例）

No	アクセシビリティ分類	アクセシビリティ要件
1	言語対応	本情報システムでは、日本語のほか、XX 語で記載されたコンテンツに対応すること

システム方式に関する事項

「システム方式」では、定義された業務要件のうち、情報システムが処理・実行する範囲について、情報システムとして動作するために必要となる「道具」の具体的な実現方法を明確にします。

EC サイト構築におけるシステム方式に関する事項（例）

No	全体方針の分類	全体方針
1	システムアーキテクチャ	本情報システムのシステムアーキテクチャは、【メインフレーム型／クライアントサーバ型／Web サーバ型／外部サービス利用型／スタンドアロン型】とする
2	アプリケーションプログラムの設計方針	情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする
3	ソフトウェア製品の活用方針	広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する アプリケーションプログラムの動作、性能などに支障をき

		たさない範囲において、可能な限りオープンソースソフトウェア（ＯＳＳ）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらのＯＳＳ製品のサポートが確実に継続されていることを確認しなければならない
4	システム基盤の方針	クラウドサービス提供者が提供するサービス・機能を最大限活用した構成とする

規模に関する事項

「規模」とは、情報システムを使うユーザーの数や取扱う情報量を指します。利用者が多ければ単位時間当たりで多くのリクエストを処理できる能力が必要となりますし、情報量が多ければ、より大容量のデータベースなどが必要になります。要件定義では「利用者は最大 100 人、平日は常時 80 人、土日は基本的に休みのため 10 人未満」といった要件を定量的に示します。

EC サイト構築における利用者数に関する事項（例）

NO	ユーザー区分	ユーザー数
1	想定ユーザー（アクティブユーザー）	5000（人）

EC サイト構築における情報量に関する事項（例）

NO	項目	処理件数	補足
1	業務処理件数（ピーク時）	300（件／分）	1 月 1 日から 1 月 3 日ごろまで、初売りセールのため処理が集中する
2	業務処理件数（通常時）	120（件／分）	平日は 80（件／分）、土日祝日は 100（件／分）

性能に関する事項

「性能」とは、情報システムの能力を指します。能力を測る指標には、応答性能やスループット（処理性能）などがあります。ネットショッピングで例えると、商品を検索し検索結果のリストが表示され、特定の商品を選択すると詳細情報が表示される、という一連の流れが一般的ですが、検索ボタンや選択ボタンを押してから、次の画面が表示されるまでの時間が応答性能です。スループットは、一度にどれだけの量を処理できるかという性能で、通常時でも大量に注文が発生するバーゲンセール開催中でも、定義した応答性能が担保されるということを表します

EC サイト構築における応答性能の事項（例）

NO	指標名	目標値	補足
1	参照系処理	3 秒	画面の読み込み、情報の表示に関する処理
2	更新系処理	5 秒	情報の登録、更新、削除に関する処理

EC サイト構築における処理性能に関する事項（例）

NO	設定対象	指標名	目標値	応答時間達成率
1	○○処理	レスポンスタイム	定常時：X 秒以内 ピーク時：X 秒以内	90%
2		ターンアラウンドタイム	定常時：X 秒以内 ピーク時：X 秒以内	90%
3		サーバ処理時間	定常時：X 秒以内 ピーク時：X 秒以内	平均値

信頼性に関する事項

「信頼性」とは、情報システムが持つ故障への耐性の度合いのことを指します。一般的には平均故障間隔（分または時間）で評価します。平均故障間隔の値が小さければ小さいほど信頼性は高いといえます。

EC サイト構築における信頼性に関する事項（例）

NO	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ・ 接続回線の計画停止時間 ・ 大規模災害などの天災地変に起因する停止時間 ・ 連携するサービスまたはクラウドサービスまたはスマートフォン端末の通信キャリアの障害・計画停止・緊急メンテナンスなどに起因する停止時間 ・ 本サービスのメンテナンスによる計画停止時間
2	稼動率	99.9%以上	本サービスにおける稼動率を以下の計算式により定義する。 稼動率＝年間実稼動時間／年間予定稼動時間 x100 当該計算式において、年間実稼動時間は「利用者がサービスを利用可能な時間の合計」、年間予定稼動時間は「年間稼動時間（24 時間 365 日）から計画停止時間および大規模災害

			による停止・縮退時間を除いた時間の合計」とする。

拡張性に関する事項

「拡張性」とは、利用率の増加、データ量の増加などにより、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うことです。また、将来の制度改正などにより機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うことも指します。

EC サイト構築における拡張性に関する事項（例）

基本方針
本システムの利用率の増加、データ量の増加などにより、規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正などにより機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。
マネージドサービスなどの活用
本サービスはクラウドサービスを利用する想定としている。本サービスの構築に当たっては、当該クラウドサービスをマネージドサービスなど可能な限り活用することにより、処理能力などの動的調整を実現することにし、業務量および処理能力の拡張性については特段の拡張性要件を定義しない。
機能の追加
機能の追加や、新たな機能開発の必要が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。 本サービスは、連携業務アプリケーションとの一層の連携など、拡張性を備えたシステム・サービスであることが求められる。連携機能などの拡張が必要になった際に拡張が容易となるような構成を取ること。

上位互換性に関する事項

「上位互換性」とは、主にソフトウェア製品において、新しいバージョンの製品で古いバージョンの製品が利用できることを指します。代表的な製品は上位互換性がありますが、バージョンアップに伴い、レイアウトが崩れたり、ブラウザの場合画面のレイアウトや特定のボタンが動作しなくなったりといった、一部の機能に限り上位互換性がないこともあります。

EC サイト構築における上位互換性に関する事項（例）

クラウドサービスのバージョンアップ
システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョン

アップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。
OS などへの依存
原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェアなどの特定バージョンに依存する場合は、その利用を最低限とすること。
クライアント端末の更新
クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

中立性に関する事項

「中立性」とは、情報システムを構成する要素が、特定の技術や製品に特化しないことを指します。例えば、新規に情報システムを構築する際に、ある事業者が開発・販売している製品を利用しなければ運用・保守ができない構成にしたとします。その後、運用・保守業務を一般競争入札で調達しようとしても他の事業者ではその製品を入手できないなどの理由により、その製品を導入した事業者による一者応札となってしまいます。このような状態になることを防ぐために、特定の事業者の技術に依存せず、多くの事業者が扱える製品を採用するなど、中立性への配慮が必要です。

EC サイト構築における中立性に関する事項（例）

データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

- 情報システム内のデータについては、原則として XML や CSV などの標準的な形式で取り出すことができるものとすること。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）を文書化すること。文書については、情報システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当文書の内容に変更が生じる場合は継続して改定を行い最新化できること。
- 移行データに関する文字コードなどは以下に従うこと。
    - 取扱う日本語文字集合の範囲：JIS X 0213
    - 文字コード：ISO/IEC 10646
    - 文字の符号化形式：UTF-8

継続性に関する事項

「継続性」では、当該情報システムを構成する要素（サブシステム、サービスなど）に分解し、情報システム全体での目標復旧時間を踏まえて、各要素の継続性に係る指標や目標値を要件として示します。

クラウドサービスとオンプレミスは継続方法の確保方法が異なります。クラウドサービスを利用する場合には、オンプレミスのように別途保管する必要はなく、クラウドサービス提供者が提供するバックアップサービスを利用すれば良いと考えられます。ただし、バックアップサービスにはさまざまな種類が存在することに鑑み、選択する手法が妥当なものであることを確認しておきましょう。

EC サイト構築における継続性に関する事項（例）

データバックアップ
・ バックアップ対象 データバックアップに当たっては、本サービスの稼動に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグなどに起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。 ・ バックアップ頻度 バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR：Point In Time Recovery/Restore を保存するなどの対応を行うこと。 ・ 保存期間 万一の障害発生に備え本サービスの稼動に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

情報システム稼動環境に関する事項

「情報システム稼動環境」とは、当該情報システムに係る、クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件などを明らかにすることを指します。稼動環境には、運用、保守、研修、検証などに必要な環境も含めます。

EC サイト構築における情報システム稼動環境に関する事項（例）

動作保証対象とする利用端末			
NO	端末	OS	バージョン
1	PC	～	Ver○○
…	…	…	…

動作保証の対象とするブラウザ
● PC の場合：○○ブラウザの最新バージョン ● スマートフォンの場合：□□ブラウザの最新バージョン ● タブレット端末の場合：△△ブラウザの最新バージョン

※動作保証の対象とする OS やブラウザは、想定される利用者に合わせて決定する必要があります。動作保証対象とする OS やブラウザの種類を絞りすぎると、アクセスできない利用者から不満が出る可能性があります。想定される利用者をできるだけ広くカバーできるように動作保証対象を設定することが重要です。

テストに関する事項

情報システムのテストには、ソフトウェアの設計に基づいて事業者が行うテストと、発注者および情報システムの利用者の視点で行うテストが存在します。テストに関する要件には、実施するテストの内容や方法、環境などを示します。

EC サイト構築におけるテストに関する事項（例）

NO	テスト工程	テストの目的・内容	テスト環境	テストデータ	テスト実施主体
1	単体テスト	アプリケーションを構成する最小の単位で実施するテストであり、主に機能単位で設計通りに動作するかを事業者（プログラマ）が確認する。	開発環境	テスト用に作成したデータ	事業主
2	結合テスト	複数の機能を連携させて動作を確認するテストであり、主にユースケース単位で設計通りに動作するかをテスト担当者が確認する。	検証環境	テスト用に作成したデータ	
3	総合テスト	システム全体が設計の通りに	検証環境	テスト用に作成	

		動作することを確認するテストであり、ユースケースを組み合わせた一連の業務が行えることを機能面や非機能面の観点からテスト担当者が確認する。		したデータ、または本番データから作成した疑似データ	
4	受入テスト	納品されるシステムが要件通りに動作することを確認するテストであり、発注者が主体となり、事業者と協力して確認する。	検証または本番環境	本番データ、または本番データから作成した疑似データ	

移行に関する事項

移行には、データ移行、システム移行および業務運用移行の 3 つの要素があります。業務の安定的な継続が最重要課題であるため、移行の各ステップにおいて状況を評価し、最悪の場合でも既存の情報システムへ切り戻せるような計画と、プロセスの準備を要求しておくことが必要です。

移行に向けた作業手順および役割分担（例）

No	作業名	主管部	工程管理支援業者	現行システム運用保守事業者	次期システム設計開発事業者
1	移行計画の作成	■	●	△	◎
2	移行データ準備・提供	◎・■	●	◎	△
3	移行データ分析	■	●	△	◎
4	移行設計	■	●		◎
5	データ移行サーバ・ツール開発	■	●		◎
6	移行リハーサル	■	●	△	◎
7	移行判定	◎・■	●		◎
8	本番移行	■	●	△	◎
9	稼動判定	◎・■	●		◎

◎：主体者、●：確認者、■：承認者、△：支援者

EC サイト構築における移行対象データ（例）

NO	移行元	移行対象業務	件数	提供方法

1	商品情報	商品テーブル	XX	CSV 形式での提供
2		新規登録ファイル	XX	CSV 形式での提供
3		商品情報	XX	CSV 形式での提供

引継ぎに関する事項

情報システムの構築およびテストが完了し本番運用に移行する際、または年度の節目などで事業者や要員が交代する場合、円滑な業務運営を維持するためには、あらかじめ引継ぎ項目を整理し、想定しておくことが重要です。現在その作業を担当している事業者を「引継ぎ元」と定義し、その事業者が担当している作業を「引継ぎ内容」として明らかにします。基本的には事業者ごとに作業・成果物などを定義した契約が存在しているため、その内容をもとに整理すると効率的です。引継ぎ期間は 1 ヶ月程度を設定することが一般的ですが、十分ではないケースが多く見られます。引継ぎ期間が十分でない場合には、他の事業者が参入できなかったり、その後の業務運営に支障が生じたりするおそれがあるため、十分な期間を確保することが重要です。

EC サイト構築における引継ぎ事項（例）

NO	引継ぎ期間	引継ぎ先	引継ぎ内容	引継ぎ手順
1	令和〇年〇月〇日 ～ 令和〇年〇日〇月	運用・保守事業者（令和 X 年度後半に調達予定）	● ソースコード（テスト・構成管理・環境構築などに利用するコード含む）開発環境に必要となる各種ツール ● 各種設計書・ドキュメント類 ● 運用課題（管理簿） ● 仕様課題（管理簿） ● インシデント状況（管理簿） ● 連携業務 AP 対応状況（管理簿） ● ヘルプデスク作業 ● 各種運用・保守作業 ● そのほか納品物一式 ● （クラウドサービスの管理に必要なアカウントや鍵情報、また Infrastructure as Code に基づくシステム構築・管理に係る構成管理ファ	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。

			イルなど情報を漏れなく含む)	
2	令和〇年〇月〇日 ～ 令和〇年〇日〇月	連携先システムである●●システムのアプリケーション保守事業者	必要となる知識など	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。

One Point

事業者がソフトウェアライセンスを保有している場合の引継ぎ

事業者が情報システムを構成するソフトウェアのライセンスを保有している場合、事業者が交代する際にソフトウェアライセンスを引継ぎ先の事業者へ譲渡することが必要になります。ソフトウェアライセンスの契約条件によっては譲渡に制約が生じ、引継ぎ先の事業者による運用・保守作業に支障が生じる場合があります。そのため、譲渡可能なソフトウェアライセンスを調達する旨とソフトウェアライセンスの譲渡に関する制約がある場合はその情報を開示する旨を、要件定義書に記載しましょう。落札後、ソフトウェアライセンスの契約条件を発注者・事業者間で合意した上で、ソフトウェアライセンスを調達しましょう。

教育に関する事項

「教育」とは、情報システムの利用者が、その情報システムの機能を理解し、効率的に運用していくために必要となる、利用者に対する操作研修などを指します。

業務要件定義で作成した業務フロー図などを参考に、教育対象者の範囲を定めます。基本的には業務フロー図に表現されているすべてのアクター（役割）が、教育対象者の候補となりますが、対象者の役割、所属する組織、場所などを考慮し、教育効果や費用を考慮して教育内容や用いる教材などについて要件として示します。

EC サイト構築における教育対象者（例）

NO	教育対象者	教育内容	教育対象者数
1	システム部門従業員	運用業務の全体概要、システム部門従業員の業務手順など	XXX
2	業務部門従業員	従業員の業務に関する本システムの操作手順、画面遷移、UI 表示仕様、エラー発生時の対応など	XXX
3	運用・保守事業者	運用・保守業務の全体概要、運用・保守事業者の業務手順、運用・保守要員の業務内容など	XXX

EC サイト構築における教育資料の概要（例）

NO	教材	教材の概要	対象者	補足
1	システム概要資料	情報システムや関連業務の概要を取りまとめた資料	システム部門従業員 業務部門従業員 運用・保守事業者	対象者ごとに教材を作成
2	操作動画	情報システムの操作方法について動画に取りまとめたもの	業務部門従業員	XXX
3	FAQ	よくある質問や回答を取りまとめた資料	システム部門従業員 業務部門従業員 運用・保守事業者	対象者ごとに教材を作成

運用に関する事項

情報システムの運用とは、稼動状態をあらかじめ定めた品質基準に基づき維持することであり、今ある環境を正常な状態に保ち続ける活動ともいえます。詳細な内容は情報システムの運用設計において検討しますが、運用要件の内容によって、情報システムの機能要件および非機能要件に求める事項が異なることもあるため、基本的な要件はここで定義しておきます。

EC サイトの運用時におけるセキュリティ対策要件

IPA の「EC サイト構築・運用セキュリティガイドライン」には、EC サイト運用時におけるセキュリティ対策要件が記載されています。「必須」、「必要」、「推奨」という区分や定義については、「21-1-2.要件定義」で前述したものと同じです。「必須」の要件については、必ず実装することが重要ですが、「必要」、「推奨」の要件ついては、自社の適用宣言書に基づいて実装するようにしましょう。

No	セキュリティ対策要件（運用時）	区分
要件 1	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須
要件 2	EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須
要件 3	Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須
要件 4	システムの定期的なバックアップの取得およびアクセスログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。	必須

要件 5	重要な情報はバックアップを取得する。	必須
要件 6	WAF（Web Application Firewall）を導入する。	推奨
要件 7	サイバー保険に加入する。	推奨

EC サイトの運用時におけるセキュリティ対策要件一覧
（出典）IPA「EC サイト構築・運用セキュリティガイドライン」をもとに作成

要件 1.サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。

ソフトウェアを安全な状態で利用するためには、その前提として、脆弱性情報に関する常日頃の情報収集が大切です。すでに攻撃方法が見つかっていたり、被害の存在が広く知られていたりするなど、危険度の高い脆弱性に関しては、セキュリティパッチの適用や最新版へのバージョンアップによるアップデートを迅速に行うことが重要です。それ以外の脆弱性に関しては、セキュリティパッチの適用や最新版へのバージョンアップを行うか否かを、脆弱性によるシステムへの影響などを考慮して判断してください。

- EC サイトの構築時に利用している Web サーバなどの OS・ミドルウェア、プラグインおよびライブラリや、Web アプリケーションや OSS のソフトウェアについては、運用時点の最新版を使用してください。

- 利用しているソフトウェアなどについては、EC サイト運営事業者や外部委託先において最新の脆弱性情報を収集することが大切です。セキュリティ情報サイトでの定期的な情報収集をするとともに、ソフトウェアを提供している企業から脆弱性に関する情報収集方法が用意されている場合は必ず登録するようにしてください。

- 利用しているソフトウェアなどで脆弱性が発見された場合、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は、3 ヶ月程度を目途にセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響がないことを確認（動作検証）してください。

要件 2.EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する。

EC サイトを構築後、新たな脆弱性が発見される・新たな脆弱性を作り込む可能性があるため、定期的およびカスタマイズを行った際に脆弱性診断を実施します。

- 新機能の開発・追加やシステム改修などのカスタマイズを行ったときには、その都度 Web アプリケーション診断を実施することが重要です。なお、診断箇所は、最低でも新機能の開発や追加やシステム改修などを行った箇所を対象とした診断を実施してください。

- 上記のような新機能の開発・追加やシステム改修などのカスタマイズを行っていない場合でも、OS やミドルウェアなどの脆弱性は継続的に発見されているため、四半期に 1 回の頻度でプラットフォーム診断を実施することが望まれます。

- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、「中」、「低」の 3 段階で分類されており、危険度「高」の脆弱性については、迅速に対策を行うことを推奨しています。また、危険度「中」は、3 ヶ月程度を目途に対策を行うことが推奨されています。

要件 3.Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。

不正アクセスやマルウェア感染により、Web サーバ内部に保管しているサイト利用者の顧客情報や、注文・取引データなどを外部に送信する不正なプログラムが、Web サーバの公開ディレクトリ配下などに仕掛けられた場合でも、それを検知できるように、定期的な差分チェック（ファイル整合性監視）や、Web サイト改ざん検知ツールを利用した監視を行うようにしましょう。

要件 4.システムの定期的なバックアップの取得およびアクセスログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。

不正アクセスやマルウェア感染により、システムを改ざん、破壊された場合、EC サイトでの事業の継続ができなくなる可能性があるため、システムのバックアップを最低 1 回/月取得するようにします。また、EC サイトへの不審なログインの試行が増えたり、システム上で対応されていない不正な注文ができたりするという不正アクセスの予兆が発生している場合もあります。このため、Web サーバのアクセスログを定期的に確認し、確認した結果、不正なアクセス（特定の IP アドレスからの大量のアクセスなど）があれば、ファイアウォールなどのネットワーク機器の設定でアクセスの制限をかけるなどの対策を実施しましょう。

Web サーバのアクセスログの定期的な確認は、IPA が提供する「ウェブサイトの攻撃兆候検出ツール iLogScanner」を利用して確認可能です。

詳細理解のため参考となる文献（参考文献）	
ウェブサイトの攻撃兆候検出ツール iLogScanner	https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

要件 5.重要な情報はバックアップを取得する。

サイト利用者の顧客情報や仕入先情報、売上情報などの重要な情報がランサムウェアによって暗号化されると、EC サイトでの事業の継続ができなくなる可能性があるため、重要な情報は 1 回/日にバックアップを取得（ネットワークに接続されていないオフライン環境へ保管）します。

要件 6.WAF（Web Application Firewall）を導入する。

すでに見つかっている脆弱性に対して対応するまでに期間が必要な場合や、必要となるセキュリティ対策を実装するまでに期間が必要な場合が想定されます。対策をするまでの期間内にサイバー攻撃を受けることがないよう、応急処置として、WAF（Web Application Firewall）を導入すると良いでしょう。

要件 7.サイバー保険に加入する。

万が一、EC サイトまたは、自社システムがサイバー攻撃による被害を受けた場合に備えて、サイバー保険に加入しておきましょう。サイバー保険については、IPA 調査でも顧客情報の漏えい事故を発生させてしまった EC サイトの多くが、被害後に加入していますが、損害賠償や事故対応費用の負担、収益の減少を補う効果が認められることから、被害が発生していない場合でも被害発生に備えて加入することが推奨されます。

EC サイトの運用時に有効な CSF2.0 の管理策（例）

セキュリティ対策の要件を決める際は、CSF2.0 の管理策を参考にすることも有効です。

有効な管理策の例

パッチ適用に関する管理策

- GV.SC-09:サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリスク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイクル全体を通じて監視される。
- ID.RA-01:資産の脆弱性を特定、検証、記録する。
- PR.AT-01:要員は、サイバーセキュリティリスクを念頭において一般的な業務を遂行するための知識と技能を有するよう、意識向上とトレーニングを受ける。
- PR.PS-02:ソフトウェアはリスクに見合った保守、交換、削除が行われる。

など

脆弱性情報に関する管理策

- ID.RA-08:脆弱性の開示を受領、分析、対応するためのプロセスを確立している。

など

ログに関する管理策

- PR.PS-04:ログ記録を作成し、継続的なモニタリングに利用できるようにする。
- DE.CM-02:潜在的に有害な事象を発見するために、物理的環境をモニターする。
- DE.CM-03:潜在的な有害事象を発見するため、従業員の活動および技術利用を監視する。
- DE.AE-02:潜在的有害事象を分析し、関連する活動をよりよく理解する。
- DE.AE-03:情報は複数の情報源から関連付けられている。
- DE.AE-06:有害事象に関する情報は、権限を与えられたスタッフおよびツールに提供される。

など

バックアップに関する管理策

- PR.DS-11:データのバックアップが作成、保護、維持、およびテストされる。
- RC.RP-03:バックアップやそのほかのリストア資産をリストアに使用する前に、その完全性を検証する。

など

※各管理策の詳細は、「付録：CSF2.0」を参照してください。

EC サイト構築における運用計画書の記載（例）

NO	項目	補足
1	作業概要	監視・運用・保守作業の対象範囲、管理対象、作業概要を記載する。
2	作業体制に関する事項	運用・保守業務を実施するための体制について、管理体制図、本件受託者の要因（責任者、作業者、役割分担）、連絡手段などについて記載し、全体的な運用管理体制を明確にする。
3	管理対象	受託者は本業務で開発する XXX システムおよびドキュメントについて保守を行うこと。
4	サービスレベル	運用・保守業務で達成目標とするサービスレベル項目およびサービスレベルを主管課が協議の上、決定すること。

主な運用作業例

NO	運用作業の分類	主な運用作業の内容
1	パッチ適用	保守におけるパッチ適用要否の判断結果に基づき、パッチを

		適用の上、適用後の稼動確認を行う。
2	ログ管理業務	● 操作ログやアクセスログなどのシステムログ、例外事象の発生に関するログを取得すること。 ● ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ● 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。
3	システム監視	● サービスの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性などで分類した上で、メールなどにより自動で通知する仕組みを構築すること。 監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）、外形監視（当該システムを利用するユーザーと同じ方法でアクセスし正常に動作しているか監視する方式）など ● 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直しなどが必要な場合は、主管課の承認を得た上でこれに係る設計を行い、対応を実施すること。 ※システムサイジングについても定期的に分析を行い、主管課の承認を得た上で見直すこと。
4	問題管理	● 本サービスに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度および優先度を定め、根本原因の調査および解決策の立案を行うこと。
5	ヘルプデスク業務	● 本サービスの利用方法に関する問い合わせの受け付けからクローズまでを一元管理するヘルプデスクを設け、本サービス利用者からの問い合わせを受け付けること。

		● 問い合わせの要件は以下に示す。 ・ 平均処理時間：6 分 ・ 平均応答速度：20 秒 ・ 一日の問い合わせ想定量：30 件 ● ヘルプデスク担当者のスケジューリングなどの運営を適切に行うこと。 ● ヘルプデスク担当者による対応手順、サービスレベルなどを統一するため、ヘルプデスク運用マニュアルを作成し、主管課の承認を得ること。 ● ヘルプデスク運営の中で FAQ は適宜追加、更新など、メンテナンスを行うこと。 ● 受け付けた問い合わせは、質問、インシデント、サービス要求、作業依頼などに分類した上で、対応日時、問い合わせ元、内容、回答状況などとともに記録すること。なお、具体的な運用方法については、本サービスの設計開始以降に改めて検討する。 ● 問い合わせ記録は受け付け件数、問い合わせ者情報、問い合わせ内容、回率、回答に要した期間、回答内容などを適切な粒度で整理した上で、定期的に問題発生状況を分析し、必要な対応を行うこと。 運用･保守の計画および実施状況について、主管課の定める報告様式に従って取りまとめ、主管課に報告を行うこと。（原則、月次での報告）

保守に関する事項

「保守」とは機能要件に変更を加えずにプログラム修正のみを行うことです。「機能要件を変えずにプログラム修正する」という特徴があるため、現状の各種ドキュメントを正しく管理することが重要です。運用・保守計画書および運用・保守実施要領に基づき作業をします。

EC サイト構築における保守に関する事項（例）

保守業務の実施
● 受け付けた問い合わせをインシデントとして管理し、クローズまで、対応を継続すること。 ● 障害について対応したときは、障害報告書を作成し、主管課に報告すること。

保守設計

- **役割分担の整理**

・ 保守業務の設計に際し、受託者の責任範囲およびクラウドサービスを含めた関連事業者間の役割分担を整理すること。

・ 新システムがクラウドサービス上で稼動することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。

アプリケーションの保守

- **インシデント管理**

・ 運用管理・監視など作業におけるインシデント管理と適切な連携を図ること。

- **是正保守**

・ アプリケーションに起因した障害発生時、監査指摘事項への対応時など、アプリケーションの是正が必要な場合に、是正保守を行うこと。

- **適応保守**

・ OS、ブラウザ、ミドルウェアなどのバージョンアップ対応など、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。

- **予防保守**

・ アプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合または新たに脆弱性が報告された場合に、予防保守を行うこと。

- **改善措置**

・ アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性などの改善が必要な場合に、対処を行うこと。

- **根本原因の分析**

・ 是正保守および予防保守の実施に当たり、障害、監査指摘、潜在する問題などに係る根本原因の分析を行うこと。

- **検証**

・ 修正したアプリケーションを本番環境へ展開（デプロイ）する前に、修正が適切に実施されているか否かについて検証環境において検証すること。

- **文章の修正**

・ アプリケーション保守に伴い、ドキュメント（設計書、マニュアルなど）の修正を要する場合は、速やかに修正を行うこと。

SaaS 型サービスの選定基準と利用時に必要となる対策

EC サイトの形態の選定において、SaaS 型サービスを選定した場合、以下のセキュリティ対策の実施状況について確認する必要があります。

【SaaS 型サービスの選定基準】

- 選定したサービスがクレジットカードを扱う場合には PCI DSS に準拠していることを確認してください。（当該サービスの運営事業者のホームページやパンフレットなどに情報が公表されていない場合は、サービスの営業窓口に問い合わせて確認してください）

- CSF2.0 の管理策（ID.RA-09: ハードウェアとソフトウェアの真正性と完全性は、取得および使用前に評価される。）を参考にすることも有効です。ソフトウェアが信頼できるものであるか、セキュリティに問題がないかを導入前に確認することが大切です。

SaaS 型サービスを選択した場合も、セキュリティ対策は必要です。例えば、セキュリティ対策を行わなかった場合、サービスの管理画面を乗っ取られ、EC サイトに不正ログインされる可能性があります。また、カスタマイズした部分（SaaS 型サービス利用で独自の処理を追加したホームページを作成している場合）に関しては、自社構築サイトと同等レベルのセキュリティ対策を行う必要があります。EC サイト運営事業者は、上記を理解した上で以下のセキュリティ対策を必ず実施することが重要です。

【SaaS 型サービス利用時に注意すべきセキュリティ対策】

- 管理画面の乗っ取りを未然に防ぐため、SaaS 型サービスの管理画面や管理用ソフトウェアへアクセスする管理端末を利用する従業員を極力最低限に限定し、管理端末からのアクセス時は二要素認証と IP アドレスや端末 ID による接続制限の導入などを必須にします。

- 管理端末のサイバー攻撃者からの乗っ取りを防ぐために、セキュリティ対策（マルウェア対策ソフトウェアの導入、USB メモリなど外部記憶媒体の利用制限、OS、ソフトウェアの最新版へのアップデートなど）を実施します。

Fit&Gap 分析

Fit&Gap 分析は、SaaS やパッケージソフトを導入する際に非常に重要なプロセスです。Fit&Gap 分析によって、RFI などの情報収集活動によって選定した SaaS やパッケージソフトと、自社の業務要件との適合性を評価します。

Fit＆Gap 分析にはさまざまなやり方がありますが、一般的な実施手順の例を紹介します。

Fit＆Gap 分析の実施方法（例）

Fit＆Gap 分析の一般的な実施手順（例）

1. 現状分析
2. SaaS、パッケージソフトウェアの機能調査
3. 比較分析
4. ギャップへの対応策検討
5. 費用対効果の分析
6. 実施計画の策定

「3.比較分析」は Fit＆Gap 分析の中核をなす重要なステップのため、手順を詳細に説明します。

比較分析の一般的な実施手順（例）

1. 比較項目の設定
2. 評価基準の設定
3. 比較表の作成
4. 詳細比較
5. ギャップの特定と分類
6. フィットの評価
7. 結果の文書化
8. 視覚化（必要があれば実施する）
9. 要件の再検討
10. ステークホルダーレビュー

上記の手順をもとに、実際に Fit＆Gap 分析の例を紹介します。

前提条件

企業名:地方の特産品を扱う中小企業「A 社」

現状:

- 実店舗は運営しているが、EC サイトはまだ存在しない。
- 主要な売上は観光客や地元の顧客による実店舗での購入。
- オンラインでの販売に関する経験がない。
- 自社には IT やセキュリティの専門家がいない。

目標:

パッケージソフトや SaaS を利用し、商品の購入から配送までを管理できる EC サイトを構築する。

1.現状分析

現在のビジネスプロセスを詳細に文書化します。また、組織の要件を明確にします。

現状分析の例

- 商品仕入れと在庫管理
  地元の生産者から商品を仕入れ、表計算ソフトで手動管理している。商品ごとの在庫情報は店舗ごとに管理されている。

- 店舗販売
  実店舗での販売が主体で、一般的なレジを使用し、クレジットカード決済は外部の決済端末を利用している。

- 配送対応
  電話やメールで受けた注文に対して手動で配送手配を行っている。オンライン販売は行っていない。

ビジネスプロセスをもとに、組織の要件を明確にします。

組織の要件を明確にする例

- EC サイトを構築し、実店舗外の顧客にもアプローチできるようにする。
- 在庫管理、注文管理、配送管理を一元化する。
- EC サイトにはクレジットカード決済機能も追加し、オンラインでも安全な決済を行えるようにする。
- セキュリティ対策を確実に実施する。（PCI-DSS 準拠）

2.パッケージソフト・SaaS の機能調査

パッケージソフトや SaaS が提供する機能を詳細に調査します。また、各機能の仕様や制限を理解します。

EC サイト構築のために適したパッケージソフトや SaaS を調査する例

SaaS サービス A

- 世界的に使用されている EC サイト構築プラットフォーム。多言語対応、国際配送、複数の決済オプションをサポートしている。
- PCI-DSS に準拠しており、セキュリティ面で強固な対策が施されている。

SaaS サービス B

- 日本市場向けに特化した EC 構築サービス。豊富なカスタマイズ機能を提供している。
- クレジットカード決済機能が統合されており、在庫管理機能も充実している。

パッケージソフト C:

- 中小規模のビジネス向けに使いやすいプラットフォーム。簡単に EC サイトを開設でき、決済機能も搭載している。
- セキュリティ面での拡張性は限定的で、標準機能では PCI-DSS に準拠していない。

3.比較分析

組織の要件とパッケージソフト・SaaS の機能を比較します。また、適合する部分（フィット）と不一致の部分（ギャップ）を特定します。「比較分析」は、Fit＆Gap 分析の中核をなす重要なステップです。

3-1.比較項目の設定

要件定義の結果を踏まえて、業務プロセス、機能要件、非機能要件、法規制対応など、比較すべき項目を事前に定義します。これらの項目を具体的かつ測定可能な形で記述します。

比較項目の設定例

- 業務プロセス
  商品の仕入れ、在庫管理、オンライン販売、決済、配送の各フローを統合して管理できること。

- 機能要件
  EC サイト構築、クレジットカード決済の統合、在庫管理、顧客管理、配送管理の機能が含まれていること。

- 非機能要件
  システムの稼動率が 99%以上であること、セキュリティ（PCI-DSS 準拠）、ユーザビリティ（初心者でも使いやすい操作画面が備わっていること。）

- 法規制対応
  個人情報保護法、特定商取引法、PCI-DSS 対応などの法規制に準拠していること。

3-2.評価基準の設定

各項目に対する評価基準を設定します（例：完全一致、部分一致、不一致）。必要に応じて重要度や優先度を設定します。

評価基準の設定例

- 完全一致：要件がそのまま満たされている場合に該当します。
- 部分一致：要件の大部分が満たされているが、一部の設定やカスタマイズが必要な場合に該当します。
- 不一致：要件を満たしていない場合に該当します。

3-3.比較表の作成

候補となるパッケージソフトや SaaS が複数ある場合は、縦軸に組織の要件、横軸にパッケージソフトや SaaS の機能を配置した比較表を作成します。次に「2.評価基準の設定」で決定した評価基準をもとに、各パッケージソフト・SaaS が組織の要件を満たしているか評価します。これにより、組織の要件とパッケージソフト・SaaS の機能との対応関係を視覚化します。

比較表の例

要件	SaaS サービス A	SaaS サービス B	パッケージソフト C
EC サイト構築	完全一致	完全一致	完全一致
クレジットカード決済の統合	完全一致	完全一致	部分一致
在庫管理	部分一致	完全一致	部分一致
配送管理	完全一致	完全一致	部分一致
顧客管理	完全一致	完全一致	部分一致
稼動率（99%以上）	完全一致	完全一致	完全一致
セキュリティ（PCI-DSS 準拠）	完全一致	完全一致	不一致
法規制対応	完全一致	完全一致	部分一致
操作画面の使いやすさ	完全一致	部分一致	完全一致

3-4.詳細比較

各要件に対して、パッケージソフトや SaaS が対応する機能を詳細に比較します。機能の有無だけでなく、その実現方法や操作性なども考慮します。

SaaS サービス A をもとに機能を詳細化する例を示します。他のパッケージソフトや SaaS も同様に詳細化し、比較を行います。

SaaS サービス A における詳細比較の例

- EC サイト構築
  SaaS サービス A は EC サイト構築において、豊富なテンプレートとカスタマイズ機能を提供しています。操作画面もシンプルで直感的に使えるため、初心者でも容易に利用できます。多言語対応もあり、国際展開を視野に入れている企業にとっては非常に有利です。標準機能でほぼすべての要件に対応しており、カスタマイズの必要がほとんどありません。

・ クレジットカード決済の統合
SaaS サービス A は、主要な決済サービスに対応しており、クレジットカード決済の統合がシンプルに行えます。PCI-DSS 準拠の決済システムが組み込まれているため、セキュリティ面も非常に強固です。操作も自動化されており、管理の手間がかかりません。

・ 在庫管理
SaaS サービス A には基本的な在庫管理機能があり、在庫数の自動追跡や通知が可能です。実店舗とオンライン店舗の在庫を一元管理できますが、複雑な在庫管理には追加のカスタマイズが必要です。

・ 配送管理
SaaS サービス A は主要な配送サービスと連携し、発送手続きや追跡をオンラインで一元管理できます。配送ラベルの自動生成やステータス通知により、手動管理の手間が減少します。操作画面もシンプルで使いやすいです。

・ 顧客管理
SaaS サービス A には顧客の購入履歴や連絡先を自動管理する基本的な顧客管理機能があり、リピート顧客向けのプロモーションも可能です。ただし、詳細なデータ分析を行う場合は、追加のカスタマイズが必要です。

・ 稼動率
SaaS サービス A はクラウドベースで、99.99%以上の稼動率を提供しており、システムが停止するリスクが非常に低いです。多くのアクセスが集中しても、安定してサイトが動作するため、安心して運用できます。

・ セキュリティ（PCI-DSS 準拠）
SaaS サービス A は PCI-DSS に準拠しています。クレジットカード情報が安全に取扱われ、すべての決済データが暗号化されます。また、定期的にセキュリティパッチが更新され、最新の脅威に対応できます。

・ 法規制対応
SaaS サービス A は日本の法規制に対応しており、個人情報保護法や特定商取引法の要件に応じたプライバシーポリシーや利用規約の設定が可能です。

・ 操作画面の使いやすさ
SaaS サービス A の操作画面は非常に直感的で、初心者でも迷うことなく利用できます。基本的な設定は数クリックで完了し、EC サイト運営の初心者にとって使いやすい設計となっています。

3-5.ギャップの特定と分類

不一致（ギャップ）を見つけたら、その性質を分類します。（例：機能欠如、プロセスの相違、法規制への非対応など）ギャップの影響度や重要度を評価します。

ギャップの特定と分類例

SaaS サービス A のギャップ：在庫管理機能の不足

・ 性質:機能欠如
SaaS サービス A は高度な在庫管理（多店舗連携や自動補充）に対応していないため、外部プラグインやカスタマイズが必要です。
・ 影響度:
在庫管理はビジネス運営において重要な部分を占めます。標準機能では不足するため、プラグインやカスタマイズが必要ですが、比較的容易に対応できるため業務に大きな影響は与えないと考えられます。

SaaS サービス B のギャップ：操作画面の複雑さ

・ 性質:プロセスの相違
SaaS サービス B は操作がやや複雑で、初心者にとっては学習コストが発生しますが、導入初期の対応で解決可能です。
・ 影響度:
操作画面の複雑さは導入初期の学習コストを増加させますが、時間と研修によって解消できます。長期的には業務に大きな支障をきたさないため、影響度は低いと考えられます。

パッケージソフト C のギャップ：セキュリティ対応の不足

・ 性質:法規制への非対応
パッケージソフト C は PCI-DSS 準拠のセキュリティ対策が不足しており、クレジットカード決済に対する対策が別途必要です。
・ 影響度:
セキュリティ対応の不足は、顧客情報の漏えいや法的な問題につながる可能性があるため、ビジネス全体に強い影響を与える可能性があると考えられます。

3-6.フィットの評価

一致している部分（フィット）についても、適合度を評価します。単なる機能の有無だけでなく、使いやすさや効率性も考慮します。

フィットの評価例

SaaS サービス A のフィット評価

・ クレジットカード決済の統合
SaaS サービス A は PCI-DSS 準拠であり、セキュリティ面での信頼性が高いです。クレジットカード決済の統合もスムーズで、安全かつ使いやすいシステムを提供しています。

・ 稼動率
SaaS サービス A は 99%以上の稼動率を誇り、安定した運用が可能です。ビジネスが途切れることなく継続できます。

・ 操作画面の使いやすさ
操作画面は非常に直感的で、初心者でも簡単に利用可能です。これにより、迅速な導入と運用が可能となります。

SaaS サービス B のフィット評価

・ 在庫管理
SaaS サービス B は強力な在庫管理機能を持っており、大量の商品を扱う際に効率的な管理が可能です。この機能は、標準で十分なレベルに達しています。

・ クレジットカード決済の統合
SaaS サービス B も PCI-DSS に準拠しており、決済機能が安全に統合されています。法規制対応も含め、安心して利用できる環境が整っています。

・ 稼動率
99%以上の稼動率を持っており、ビジネスの安定運用が確保されています。システムの信頼性が高く、長期的な運用に適しています。

パッケージソフト C のフィット評価

・ EC サイト構築
パッケージソフト C はシンプルで使いやすいインターフェースを提供しており、短期間でのサイト構築が可能です。特に中小企業に向いており、導入コストが低いのも魅力です。

・ 稼動率

パッケージソフト C も 99%以上の稼動率を誇りますが、大規模運用には適さない場合があります。小規模運用には十分な安定性があります。

・ 操作画面の使いやすさ
パッケージソフト C は非常にシンプルな操作画面を提供しており、初心者でも簡単に利用できます。低コストで迅速な運用が可能です。

3-7.結果の文書化

比較結果を詳細に文書化します。フィットとギャップの両方について、具体的な説明を記載します。

結果の文書化例

SaaS サービス A の結果

・ フィット：SaaS サービス A は、重要度の高い要件であるクレジットカード決済の統合、セキュリティ（PCI-DSS 準拠）、法規制対応、そして稼動率 99%以上をすべて満たしています。また、操作画面の使いやすさも完全一致しており、操作に慣れていないスタッフでも扱いやすいです。
・ ギャップ：在庫管理機能については一部カスタマイズが必要であり、標準機能では自社の要件を完全に満たしません。カスタマイズにより、初期導入コストやシステム設定に追加の手間がかかる可能性があります。

SaaS サービス B の結果

・ フィット：SaaS サービス B は、在庫管理、顧客管理、配送管理の各プロセスにおいて高い適合度を示しており、特に中小企業の実務に即した機能が充実しています。重要度の高いセキュリティや法規制対応も完全一致しており、安心して導入できます。稼動率も高く、パフォーマンス面でも良好です。
・ ギャップ:操作画面の使いやすさについては、初心者にとってはやや複雑で、導入時にトレーニングが必要となります。ただし、業務に大きな支障はないと考えられます。

パッケージソフト C の結果

・ フィット：パッケージソフト C は、導入コストが非常に低く、簡単に EC サイトを構築できるため、迅速にオンライン販売を開始したい企業には適しています。操作画面の使いやすさにおいても高い評価を受けており、特に IT に不慣れなスタッフでも容易に操作できます。
・ ギャップ:大きなギャップは、セキュリティ要件が不十分な点です。特に、PCI-DSS 準拠が不足しているため、クレジットカード決済を安全に運用するためには追加のセキュリティ

対策が必須となります。また、配送管理や在庫管理の一部機能が標準では不足しており、カスタマイズが必要です。初期の導入コストが低い反面、長期的には追加コストが発生するリスクがあります。

3-8.視覚化（必要があれば実施する）

必要に応じて結果をグラフや図表で表現し、全体像を把握しやすくします。例えば、ヒートマップやレーダーチャートなどを使用します。

3-9.要件の再検討

分析結果に基づき、組織の要件自体の妥当性を再検討します。場合によっては、要件の修正や優先順位の変更を行います。

要件の再検討例

要件 1：EC サイトを構築し、実店舗外の顧客にもアプローチできるようにする。
分析結果の確認：SaaS サービス A、SaaS サービス B、パッケージソフト C すべてが EC サイト構築要件に対して完全一致しており、特に問題がないことが確認できます。
再検討の必要性:なし

要件 2:在庫管理、注文管理、配送管理を一元化する
分析結果の確認：SaaS サービス A とパッケージソフト C は在庫管理や配送管理が部分一致であり、一部カスタマイズや追加機能が必要です。SaaS サービス B は完全に一致しています。
再検討の必要性：在庫管理や配送管理の重要度は高いため、SaaS サービス A やパッケージソフト C を選ぶ場合にはカスタマイズや追加機能導入の検討が必要です。要件自体は妥当ですが、システム選定時にはこれらの要件の優先順位を高く維持するべきです。

要件 3:EC サイトにはクレジットカード決済機能を追加し、オンラインでも安全な決済を行えるようにする
分析結果の確認：SaaS サービス A と SaaS サービス B はクレジットカード決済に完全一致していますが、パッケージソフト C を選択する場合には追加のセキュリティ対策が必要となります。
再検討の必要性：SaaS サービス A と SaaS サービス B は必要ありません。パッケージソフト C を選択する場合は追加のセキュリティコストを考慮する必要があります。

要件 4:セキュリティ対策を確実に実施する（PCI-DSS 準拠）
分析結果の確認：SaaS サービス A と SaaS サービス B は PCI-DSS に完全に準拠していますが、パッケージソフト C はこの要件に不一致であり、セキュリティ対策を強化しなければなり

ません。
再検討の必要性：パッケージソフト C を選択する場合には、外部セキュリティ対策を追加するコストを考慮しなければなりません。セキュリティは最も重要な要件の一つであり、特にクレジットカード決済においては必須です。

3-10.ステークホルダーレビュー

分析結果を関係者に共有し、フィードバックを得ます。必要に応じて追加の調査や分析を行います。

「1.比較項目の設定」から「10.ステークホルダーレビュー」までの詳細な比較分析により、パッケージソフト・SaaS と組織の要件との適合性を正確に評価し、導入に向けた的確な判断や計画立案が可能になります。

※比較分析の作業において業者に協力を求める場合、当該作業の内容と責任の所在を明確にする必要があります。また、複数の業者からの提案書および Fit&Gap 分析の評価を求める場合は、書式の統一、用語の定義などに配慮し、誤解が生じないようにすることが信頼性の確保につながります。

4.ギャップへの対応策検討

カスタマイズ、ビジネスプロセスの変更、代替ソリューションを検討します。
（可能な限りカスタマイズは避けた方がよく、ビジネスプロセスを変更することで対応することが推奨されます。）

SaaS サービス A を例にとり、説明します。

SaaS サービス A のギャップへの対応策例

ギャップの概要

SaaS サービス A の在庫管理機能が標準では自社の要件に完全には対応していないため、カスタマイズやビジネスプロセスの調整が必要です。

対応策:

- ビジネスプロセスの変更：在庫管理の運用をシンプルにし、SaaS サービス A が標準で提供している在庫管理機能に適合するようにプロセスを調整できるか検討します。例えば、在庫の更新頻度を増やす、複雑な商品区分を簡略化するなど、システム側に合わせたプロセスの変更で対応可能な部分があるかを確認します。
- カスタマイズ：ビジネスプロセスの変更が難しい場合、在庫管理の不足部分に対して追加のプラグイン導入といったカスタマイズを行います。この際、必要最小限のカスタマイズに留めることが重要です。

5.費用対効果の分析

ギャップへの対応策実施にかかるコストと得られるメリットを評価します。

SaaS サービス A を例にとり、説明します。

費用対効果の分析例

ギャップの概要

SaaS サービス A の在庫管理機能が標準では自社の要件に完全には対応していないため、カスタマイズやビジネスプロセスの調整が必要です。

対応策 1：ビジネスプロセスの変更

コスト

- 初期費用：なし（社内でプロセスを調整）
- 運用費用：低コスト（社内のスタッフによる在庫管理の簡略化）

メリット

- SaaS サービス A の既存の在庫管理機能に合わせてプロセスを調整することで、カスタマイズ不要のため初期費用がかかりません。
- 社内運用のみで対応できるため、カスタマイズのコストが不要です。
- シンプルな運用による管理の効率化が見込まれます。

対応策 2:カスタマイズ（プラグイン導入）

コスト

- 初期費用：中程度（プラグインの導入コストや設定費用がかかる）
- 運用費用：月額 5000 円～10000 円（在庫管理用のプラグイン利用料）

メリット

- カスタマイズにより、標準機能では対応できない在庫管理機能を補完できるため、自社の業務フローに完全に対応することが可能です。
- システム全体の効率性が向上し、在庫管理の自動化やリアルタイムでの在庫情報管理が可能です。

6.実施計画の策定

分析結果に基づいて、具体的な導入計画を立案します。

例では SaaS サービス A の導入を推奨とし、その導入プロセスを具体的に示します。

導入計画の例

1.契約と初期設定（1 週間）
SaaS サービス A の契約を締結し、サイトの基本レイアウトを設定します。

2.商品データと在庫管理（2～3 週間）
商品情報を登録し、在庫管理のカスタマイズを実施します。

3.クレジットカード決済とセキュリティ設定（1～2 週間）
クレジットカード決済機能を設定し、セキュリティ対策を強化します。

4.配送システムの設定（1～2 週間）
配送オプションを設定し、配送業者との連携を行います。

5.テスト運用（1～2 週間）
商品購入から配送までのプロセスをテストし、問題がないか確認します。

6.スタッフトレーニング（1 週間）
SaaS サービス A の操作方法をスタッフに対してトレーニングします。

7.公開とマーケティング（1 週間）
EC サイトを公開し、プロモーションを実施します。

8.運用とメンテナンス
定期的にセキュリティチェックとシステムのメンテナンスを行います。

全体の期間:約 8～10 週間で EC サイトを構築し、運用を開始します。

サービス・パッケージ候補とのギャップを解消するポイント

RFI により提示した要件と提案されたサービス、パッケージ候補とのギャップを、委託候補企業の言いなりにならず、主体的に解消することが重要です。

- 要件の変更
  Gap が大きすぎる場合は、最も適合性の高いサービスに合わせて、既存の業務プロセスやシステム要件を見直すことが望ましい。

- サービスのカスタマイズを利用

Gap が小さい場合は、サービス内のカスタマイズを利用することで Gap を埋める方法があります。しかし、セキュリティの観点からから安易なカスタマイズは避け、できる限り業務プロセスをパッケージや SaaS に合わせることが望ましい。

- 補完的なサービスを利用
  特定の機能のみが不足している場合は、別のパッケージや SaaS を組み合わせることで補完する方法があります。別のシステムを利用することにより専門的な機能の利用や、迅速な導入ができるので、初期投資が低く抑えられます。

独自カスタマイズのリスクについて

GAP を埋めるために、あらかじめ用意されているパッケージソフトや SaaS サービス内のカスタマイズではなく、独自のカスタマイズを行う場合、以下のようなリスクがあります。

・ コストの増加
  カスタマイズには追加の開発費用がかかります。予算を超える可能性があり、コスト管理が難しくなることがあります。

・ 時間の遅延
  カスタマイズ作業が予想以上に時間がかかることがあり、プロジェクト全体のスケジュールに影響を与える可能性があります。

・ メンテナンスの複雑化
  カスタマイズされたシステムは、カスタマイズのないシステムに比べてメンテナンスが難しくなります。将来的なアップデートやバグ修正が困難になる可能性があります。

・ 互換性の問題
  カスタマイズにより、他のシステムやソフトウェアとの互換性が損なわれる可能性があります。これにより、システム全体のパフォーマンスや安定性に影響を与える可能性があります。

・ サポートの制限
  カスタマイズされた部分については、ベンダーからのサポートが受けられない場合があります。これにより、問題が発生した際の対応が遅れる可能性があります。

・ 品質やセキュリティレベルの低下
  カスタマイズが不十分な場合、システムのセキュリティや品質が低下するリスクがあります。

これにより、ユーザーの満足度が低下するだけでなく、セキュリティインシデントの発生可能性も高まる可能性があります。

- 将来のアップグレード問題
  カスタマイズされたシステムは、将来的なバージョンアップや新機能の追加が難しくなることがあります。最新の技術や機能を利用できなくなるというリスクがあります。

カスタマイズには多くのリスクがあるため、カスタマイズの必要性は慎重に検討し、業務プロセスなどをシステムにあわせて変更することが推奨されます。

どうしても機能などを追加する場合は、本体のシステムに与える影響の少ないアドオン（外側に機能を追加する方法）で対処することが推奨されます。

21-1-3. 調達

調達仕様書の作成方法

要件定義書を含めた調達仕様書の作成方法を説明します。

調達仕様書とは、プロジェクトの目的の達成に必要な製品の入手や、必要となる役務を実施する外部事業者を選定するために示す、発注者側の条件を集めたドキュメントです。

調達仕様書には、発注者側の要望（要件）に加えて、制約となる条件を記載します。実現したいことに加えて、実現を図っていく過程で守るべき前提条件や制約条件を合わせて記載することで、調達仕様書としての完成度を高められます。

調達仕様書の全体像（例）

目次	主要な記載内容
調達案件の概要	背景、目的、効果、業務・情報システムの概要
調達案件および関連調達案件の調達単位、調達の方式など	調達内容、関連する調達案件、方式、時期
情報システムに求める要件	要件定義の内容
作業の実施内容に求める要件	作業の内容、成果物の範囲、納品期日
作業の実施体制・方法に関する事項	作業実施体制、資格要件、管理の要領
作業の実施に当たっての順守事項	機密保持、資料の取扱い、順守する法令
成果物に関する事項	知的財産権の帰属、契約不適合責任、検収
見積り依頼をする業者の選定に関する事項	業者選定要件
再委託に関する事項	再委託の制限、条件、承認手続き

パッケージソフト、クラウドサービスの選定、利用に関するセキュリティ関連事項（要機密情報を取扱う場合）	パッケージソフト、クラウドサービスの選定・利用に関する共通セキュリティ要件、成果物の取扱い
そのほか特記事項	機器などのセキュリティ確保、制約条件
附属文書	要件定義書など

調達仕様書を作成するときに、特に注意が必要なポイントについて説明します。項目の詳細な説明は、ひな型を参照してください。

調達仕様書を作成するときに、特に注意が必要なポイント

調達の意図や目的を正しく伝える

外部業者からプロジェクトにとって有用な提案をもらうためには、以下の点をしっかり伝える必要があります。

- プロジェクトの背景と目的
  このプロジェクトがなぜ必要なのか、達成したい目標を明確に説明します。業者がプロジェクトの意図を理解しやすくなります。

- 調達の経緯と期待する効果
  なぜこの調達が必要になったのか、どんな成果や効果を期待しているのかを詳しく説明します。業者が具体的な提案を考えやすくなります。

- プロジェクトの全体像とスケジュール
  プロジェクトの全体的な流れやスケジュールを示すことで、業者がプロジェクトの全体像を把握しやすくなります。

これらの情報は、調達仕様書の「調達案件の概要」に記載し、プロジェクト全体のスケジュールも含めることで、業者がより適切で有用な提案をしやすくなります。

作業内容・納品物を関連付けて網羅的に記載する

調達仕様書では、外部事業者の作業内容、納品物をそれぞれ漏れなく定める必要があります。しかし、設計・開発などの調達では多種多様な作業や納品物があるため、漏れなく記載するのは困難です。これらを定義する際は、作業内容、納品物を関連付けて定義していくことで、効果的に抜け漏れを確認していくことができます。作業の実施内容と納品物を関連付けて一覧としてまとめておくと、工程完了時の納品物のチェックにも活用でき、検収時の確認負荷を減らせます。

外部事業者の具体的な作業内容を明確にする

外部事業者が実際に何を実施する必要があるのか理解できるように、作業内容を明確に記載することが重要です。

例えば、「支援」という言葉は人によって解釈が大きく異なります。「マニュアル作成支援」という作業項目があった際、2 つの役割分担が考えられます。1 つ目は、従業員がもととなる原案や素材を用意した上で事業者が体裁を整えるという役割分担です。2 つ目は、事業者がマニュアルの原案自体を作成して従業員が内容を確認するという役割分担です。このような役割分担の違いによって、事業者が実施する作業範囲や必要工数は大きく変わります。実際に実施する内容が事業者に正確に伝わらない場合、上記の事態をまねくおそれがあるため、事業者に実施を求める内容は正確に記述することが重要です。

作業内容が曖昧な場合に懸念される事態

- 必要な人員のスキルや数について、外部事業者の想定と発注者側の希望や想定がミスマッチとなる場合、契約した後に業務を完遂できない。
- 作業を終えることができても、成果物の品質（機能性、信頼性、使用性、効率性、保守性、移植性）が著しく低下する。
- 契約した外部事業者からの問い合わせや協議などが増加し、発注者側に想定していた以上の作業が発生する。

作業の実施体制を明確にする

調達案件を通じてプロジェクトの活動を円滑に進めていくためには、発注者側であるプロジェクト管理を行うチームや担当者や関係する従業員が、体制や役割分担、責任範囲を明確にし、外部事業者と一緒に協働していくことが大切です。調達仕様書や要件定義書をしっかり記載し、適切な外部事業者を選定することが仮にできたとしても、望んだ情報システムを必ずしも手に入れられるわけではありません。プロジェクトを進めていくと、要件の内容を設計として具体化・詳細化していく中で発注者側が決定しなければならないこと、他の関係者と調整しなければならないことは多く発生します。また、進捗上の課題や問題が発生した場合に発注者側の判断を要する場合もあります。

サービス・業務の企画や要件定義のように新しいサービス・業務や情報システムの内容を決定するような活動においては、特に注意が必要です。意思決定の責任は発注者にあることを認識した上で、プロジェクト管理を行うチームや担当者以外の関係者も含めて、適切な判断ができる体制を組成して調達仕様書に明示することが重要です。

成果物の取扱いに注意する（知的財産権）

知的財産権の取扱いについては、設計・開発した文書やアプリケーションプログラムの知的財産権が誰に帰属するかを明確にしておくことが重要です。

- パッケージ製品
  全く改変せず採用した場合、その知的財産権は提供もとに帰属します。

- 蓄積データ
  パッケージ製品を利用して蓄積されたデータの帰属については、発注者が所有することが一般的です。

- 機能拡張やクラウド設定
  発注者の要望に基づいて拡張した機能や設定の知的財産権については、契約内容により帰属先が変わります。

再委託に関する事項を定める

情報システム整備プロジェクトでは、規模が大きくなると多くの専門的役割が必要となり、特定分野の外部事業者を活用することが増えます。これらの事業者が再委託を行う場合、委託元が再委託先の作業を管理する責任がありますが、再委託に関するトラブルも少なくありません。

再委託の制限や条件、承認手続き、再委託先の契約違反に関する規定を調達仕様書に記載し、責任の所在を明確にすることが重要です。また、プロジェクト遂行中の体制変更も、発注者と協議しながら進める必要があります。再委託に関しては、情報セキュリティポリシーの規定も確認する必要があります。

納品後に不具合が発覚したときの責任を明確にする（契約不適合責任）

2020 年 4 月に施行された改正民法により、「瑕疵担保責任」が廃止され、代わりに「契約不適合責任」が導入されました。これは、システム納品後の不具合に対する責任を、契約で定められた種類、品質、数量に適合しているか否かに基づいて判断するものです。この改正は、取引の実情に合わせたものであり、特に請負契約において次のような相違点が重要です。

- 救済手段の多様化
  契約不適合責任では、契約の解除、損害賠償請求に加えて、修補や代替物の引渡し、報酬減額請求など、多様な救済手段が追加されました。

- 権利行使期間の変更
  瑕疵担保責任では瑕疵を知ってから 1 年以内に権利行使をする必要がありましたが、契約不適合責任では不適合を知ったときから 1 年以内に通知すれば救済が可能になりました。

- 「隠れた瑕疵」の要件の廃止
  瑕疵担保責任では、発注者が瑕疵の存在について善意無過失であったこと（瑕疵が「隠れた瑕疵」であったこと）が要件とされていましたが、契約不適合責任ではこの要件はなくなり、「隠れた瑕疵」でなくても業者の責任を問うことができるようになりました。

適正な価格で最適な業者の選定

中小企業が適正な価格で最適な業者を選定し、不利益を被らないような、実施可能な手続きについて説明します。

調達仕様書の明確化

中小企業にとって、調達仕様書が曖昧だと、不要な追加コストが発生するリスクが高まります。具体的な要求内容、納品スケジュール、品質基準などを明確に記載し、業者が正確な見積りを行えるようにすることが重要です。また、調達仕様書を適切に作成することで、業者の作業内容を厳密に管理し、不適切な追加請求を防げます。

透明性と公平性の維持

調達プロセス全体において透明性と公平性を確保することは、中小企業が不利益を被らないために不可欠です。提案依頼書や契約書の内容を整合性のあるものにし、期待する成果が正確に伝わるようにすることで、業者との間に不必要な誤解が生じるリスクを軽減します。

複数の見積り取得

中小企業が適正な価格を確保するためには、必ず複数の業者から見積りを取得し、比較検討することが必要です。三点見積りを活用することで、極端な価格設定による影響を排除し、より適正な予算を設定できます。また、特定の業者に依存するリスクを避けるため、依頼する業者を増やす工夫が大切です。

EC サイト構築における、3 点見積りの実施例

中小企業が SaaS やパッケージソフトを用いて EC サイトを構築する際、セキュリティ対策や運用・保守コストを含めた三点見積りを実施する例を説明します。

平均見積りの計算式

$$\text{平均見積り} = \frac{\text{楽観値} + 4 \times \text{最頻値} + \text{悲観値}}{6}$$

楽観値	最も良い条件が揃った場合の最低コスト。追加コストやリスクが発生せず、プロジェクトが順調に進むことを想定した見積りです。
最頻値	一般的な条件で進行した場合の予測コスト。通常のリスクや変動を含めた、最も現実的な見積りです。
悲観値	最悪の状況が発生した場合の最高コスト。予期しない問題や追加のコストが発生する場合を考慮した見積りです。

この式では最可能値に重きを置き、楽観値と悲観値を考慮してより現実的な平均を算出します。

SaaS 型サービス A（標準プラン）
サービス内容:クラウドベースの EC プラットフォーム。テンプレートを使って簡単にサイトを作成可能。基本的なセキュリティ機能を提供し、月額利用料で運用可能。
楽観値:60 万円（基本プランと最低限のセキュリティ対策） 最頻値:75 万円（追加のカスタマイズと標準的なセキュリティ対策） 悲観値:120 万円（高度なカスタマイズと強化されたセキュリティ対策） **平均見積り:80 万円**

パッケージソフト B
サービス内容:自社サーバにインストール可能なソフトウェア。高度なカスタマイズが可能で、独自の機能を追加可能。セキュリティや保守管理が必要。
楽観値:80 万円（シンプルな設定と標準的なセキュリティ対策） 最頻値:100 万円（通常のカスタマイズと強化されたセキュリティ対策） 悲観値:130 万円（広範なカスタマイズと最強のセキュリティ対策） **平均見積り:約 102 万円**

SaaS 型サービス C（上位プラン）
サービス内容:上位の SaaS プランで、より多くの機能や強化されたセキュリティ（WAF、不正利用検知など）を提供。追加のカスタマイズが可能。
楽観値:70 万円（標準プランと基本的なセキュリティ対策） 最頻値:90 万円（カスタマイズ対応と追加セキュリティ機能） 悲観値:170 万円（最上位プランと強化されたセキュリティ対策） **平均見積り:100 万円**

三点見積りで比較した結果

SaaS 型サービス A（標準プラン）が、導入コストが最も低く、基本的なセキュリティ対策も標準装備されているため、コストパフォーマンスが最も高い選択肢です。

パッケージソフト B は、カスタマイズ性が高く、独自の機能を追加したい企業に最適ですが、セキュリティや運用にかかる費用が増えるため、予算に余裕がある場合に適しています。

SaaS 型サービス C（上位プラン）は、SaaS の利便性を維持しつつ、セキュリティ機能や機能拡張が必要な場合に選ぶと良いですが、標準プランに比べて費用が増します。

セキュリティやコストバランスを考慮すると、SaaS 型サービス A（標準プラン）が最もバランスが良いと考えられます。

21-1-4. 設計・開発

中小企業でも、プロジェクトの計画立案とその管理は重要です。規模は小さくても、体系的なアプローチを取ることで、効率的な開発と品質の確保が可能になります。

設計・開発の計画

設計・開発事業者が決まれば、最初に行うことは計画を立てることです。設計・開発は実態が見えにくい活動になるため、問題の発覚が遅れて大惨事になることがあるため、しっかりと作成することが重要です。

設計・開発実施要領

プロジェクト・業務・情報システムの概要で、実施されるに当たり知っておくべき内容を記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	コミュニケーション管理	設計・開発事業者が参加すべき会議、開催頻度、議事録などの管理
3	体制管理	作業体制の管理手法
4	工程管理	設計、開発の作業、工程の管理手法
5	品質管理	品質基準、品質管理方法
6	リスク管理	リスクを提示する際の手順や報告様式
7	課題管理	課題を提示する際の手順や報告様式
8	システム構成管理	ハードウェアやソフトウェア製品、ネットワークなどの各資産における管理項目
9	変更管理	管理対象、変更手順、管理手法
10	情報セキュリティ管理	情報セキュリティ確保に必要な対策

設計・開発実施計画書

プロジェクト・業務・情報システムの概要や実施するに当たり手順や内容をまとめたものを記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	設計・開発の対象範囲、作業概要
3	作業体制に関する事項	作業内容および関係者間の関係性、役割分担、責務
4	スケジュールに関する事項	作業内容およびスケジュール、マイルストーン
5	成果物に関する事項	成果物、品質基準、担当者、納入期限、納入方法、納入部数、構成、内容
6	開発形態、開発手法 開発環境、開発ツールなど	開発形態、開発手法、開発環境、開発ツール
7	そのほか	設計・開発の実施の事情に応じて必要な事項

実施計画書のスケジュールに関する事項で作成するスケジュール例を紹介します。

【マイルストーン】

No.	アクティビティの記述	プロジェクトのスケジュール期間				
		5月	7月	9月	11月	1月
1	キックオフ	◆				
2	仕様凍結		◆			
3	連携テスト開始				◆	
4	受入テスト開始					◆
5	リリース					◆

【スケジュール（概略）】

No.	アクティビティの記述	プロジェクトのスケジュール期間				
		5月	7月	9月	11月	1月
1	設計	■				
2	実装		■			
3	結合テスト			■		
4	総合テスト				■	
5	受入テスト					■

設計・開発・テストの管理

設計・開発の大部分の作業は事業者が行いますが、発注者が適切に関わらないと品質が落ちる可

能性が高くなります。テストには、「単体テスト」、「結合テスト」、「総合テスト」などがあります。

ここでは、「受入テスト」例を紹介します。受入テストは、システムの妥当性を検証（ユーザーの要件や期待に合致しているか否か、システムが正しく機能するか）、バグや不具合の検出、ユーザーの満足度向上（ユーザーがシステムを実際に操作することによって、使いやすさや機能性に関するフィードバックを得る）のために実施します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	テスト体制	体制、役割、責任範囲
3	テスト環境	実施場所、環境、ツール、前提条件
4	作業内容	テスト対象、実施手順、確認・検証事項
5	作業スケジュール	全体スケジュール、各工程の作業スケジュール
6	テストシナリオ	確認・検証事項、テスト結果の予測
7	合否判定基準	品質基準、合否判定基準

21-1-5. サービス・業務の運営と改善

新しいシステムや業務プロセスを導入した後、それを定着させ、継続的に改善していくことは、中小企業の競争力維持に不可欠です。

業務の定着と次の備え

情報システムの設計・開発のリリースが近づいたところで、研修教育資料（業務マニュアルなど）を用いて、実業務を担当する従業員に対して教育を実施します。

EC サイト運営における業務マニュアル作成例と、作成に当たっての注意点を解説します。

EC サイトの運営業務は、大きく「フロントエンド業務」と「バックエンド業務」の 2 つに分けられます。

フロントエンド業務

商品の企画や仕入れ、マーケティング、EC サイトの制作など、主に「集客や商品の売上につながる業務」のことを指します。

フロントエンド業務の例

- 商品管理
  商品の情報を EC サイトに登録し、在庫数と公開設定を行います。
- 注文処理

受注管理画面で注文を確認し、出荷準備を行い、配送状況を更新します。

- 顧客対応
  顧客からの問い合わせや返品・交換リクエストに対応します。
- プロモーション管理
  割引キャンペーンや特別オファーを設定し、広告バナーを作成して配置します。
- コンテンツ更新
  ブログやニュースの投稿を行い、サイトデザインの変更を実施します。

バックエンド業務

商品情報の登録や受注管理、出荷、アフターサポートなど、「販売を支え、お客様の満足度を高める業務」のことを指します。

バックエンド業務の例

- 受注処理
  顧客からの注文内容を確認し、在庫や決済状況をチェックした上で、注文ステータスを更新します。
- 在庫管理
  在庫状況を定期的に確認し、補充や棚卸しし、新入荷商品のシステム登録を行います。
- 出荷作業
  出荷リストに基づいて商品を梱包し、発送準備を整えて集荷を依頼します。
- 配送作業
  商品の配送状況を追跡し、問題が発生した場合には配送業者と連絡を取り、顧客に対応します。
- アフターサービス
  返品や交換、顧客クレームに迅速に対応し、顧客満足度を維持します。

バックエンド業務のマニュアル例を紹介します。

バックエンド業務マニュアル（例）

1.目的

このマニュアルは、EC サイトのバックエンド業務に関する標準手順を提供し、業務の効率化と品質向上を目的とします。

2.業務の流れ

2.1 受注処理

目的:顧客からの注文を迅速かつ正確に処理します。

1.注文確認:

- 毎日午前 10 時と午後 3 時にシステム内の「注文管理」画面を確認し、すべての新しい注文をリスト化します。
- 各注文の内容（商品名、数量、配送先）を確認し、備考欄に特記事項があればそれに従います。

2.決済確認:

- 決済状況を確認し、「支払い済み」ステータスでない場合は、決済プロセスをチェックします。
- 決済エラーが発生した場合、顧客に連絡し、再決済や別の支払い方法を提案します。

3.在庫確認:

- 各注文の商品の在庫数をシステム上で確認し、在庫切れが発生していないかを確認します。
- 在庫が不足している場合、直ちに仕入れ担当者に連絡し、在庫補充を手配します。

4.ステータス更新:

注文ステータスを「処理中」に変更し、システムに自動的に反映されるよう設定します。

2.2 在庫管理

目的:適切な在庫管理を行い、欠品を防ぎます。

1.在庫確認:

- 毎週月曜日の午前にシステムで在庫状況を確認します。特に在庫が少ない商品に対しては自動アラートを設定し、タイムリーに補充が行えるようにします。
- 在庫が特定の数値以下になった場合は、即時に仕入れ担当に通知され、発注が行われます。

2.棚卸し:

- 月末に物理的な在庫とシステム上の在庫を照合し、差異がないか確認します。
- 差異が発見された場合は、原因を特定し、システム上で修正します。

3.新入荷処理:

- 新しく入荷した商品が届いた場合、納品書と実際の在庫数を確認し、商品の状態をチェックします。
- 問題がなければ、システムに入荷処理を行い、在庫数を更新します。

2.3 出荷作業

目的:顧客に正確かつ迅速に商品を届けます。

1.出荷指示:

- システムの「出荷準備」画面から、当日の出荷リストを取得します。

- 各商品を倉庫から取り出し、ピッキングリストに従って確認します。

2.梱包:

- 商品が破損しないよう、適切なサイズの梱包材を使用して商品を梱包します。
- 伝票（納品書や配送伝票）を正しく同梱し、配送業者のステッカーを貼り付けます。

3.発送準備:

発送業者に集荷依頼を出し、翌日集荷の確認が取れたら、システムで発送ステータスを「発送済み」に更新します。

2.4 配送作業

目的:配送状況を確認し、顧客に確実に商品を届けます。

1.配送確認:

- 発送業者の追跡システムで、すべての配送中の商品のステータスを確認します。
- 配送中に問題が発生した場合は、業者に連絡し、問題解決を図ります。

2.追跡番号連絡:

配送後、システム上で自動生成された追跡番号を、顧客にメールで通知します。

3.問題対応:

配送トラブルが発生した場合は、迅速に配送業者と連絡を取り、顧客に問題が解決する見通しを通知します。

2.5 アフターサービス

目的:顧客満足度を向上させ、リピーターを増やします。

1.返品対応:

- 顧客から返品リクエストがあった場合、商品の状態を確認し、返品の可否を決定します。
- 返品が承認された場合、システム上で返金処理を行い、顧客に返金確認メールを送ります。

2.交換手続き:

不良品や誤配送が発生した場合、代替商品の発送手配を行い、顧客に交換手続きの詳細を案内します。

3.クレーム対応:

- 顧客からのクレームがあった場合、可能な限り迅速に対応し、問題解決を目指します。
- 必要に応じて、社内での対応策を共有し、再発防止策を講じます。

業務マニュアル作成時の注意点

- 業務マニュアルは、同じ業務に携わる担当者が共通の理解を持つために有効ですが、組織や取扱う情報の種類によっては、同じ業務でも異なるルールが存在する場合があります。いわ

ゆる、ローカルルールと呼ばれるものです。これをすべて業務マニュアルに記載しようとすると、膨大な量となり、マニュアルの更新が追いつかず、現場とのかい離が発生するおそれがあります。同じ業務内で共通化するものと、組織ごとに個別に定めるものとで分けて業務マニュアルを作成することで、その後の保守性を向上させることができます。

- 業務マニュアルは、そのまま従業員向けの教育資料の一部とすることができます。そのことを念頭に、業務マニュアルの内容・構成を検討してください。

- 業務マニュアルには、具体的なシステムの操作手順にとらわれず、業務の流れや手順を中心に記述してください。その流れの説明において、情報システムのどの機能を使うのか、がわかれば、使いやすいものになります。情報システムの操作手順や画面説明の詳細はシステム用のマニュアルに任せることで、マニュアルの品質を上げることができます。

- 業務マニュアルは業務全体の業務フローを理解している従業員が作成、またはレビューすることが重要です。マニュアル上の業務説明が途中で途切れたり、内容の重要性に偏りが出たりすることが防げます。マニュアルができ上がったら、業務に初めて携わる従業員がそのマニュアルを読んで業務が行えるか、という観点でチェックすることが重要です。

業務の改善

サービス・業務を運営していく中で発生するさまざまな情報を集め、改善に向けた取組につなげていきます。情報システムの見直しが必要なものは「サービス・業務企画」に立ち戻り、運用保守の見直しが必要なものは「運用および保守」に立ち戻ります。これらに該当しないものは、日常的な改善として対応していく必要があります。具体的には次のようなものに該当します。

日常的に実施する改善事項の例

- 業務の見直し
  情報システムに影響を与えない範囲であれば、日常的に実施が可能です。定期的な改善を検討し、その結果は業務手順書などに反映させることが大切です。

- 教育・訓練の見直し
  具体的には教育資料の改訂やカリキュラムの改訂に相当します。現状の分析結果を踏まえて、より従業員に遡及できるような教育内容に作り替えていくことが大切です。

- モニタリングの見直し
  日常的に把握すべき指標とその仕組みの見直しに相当します。KPI で取るべき指標値は、業

務の状況に応じて変更しても構いませんので、それに応じて値の取得方法や内容を見直し、現状を正確に把握できるようにすることが大切です。

そのほか、利用者からの問い合わせが多い機能や操作などについては、マニュアルの改善や FAQ に情報を追加・更新することで改善が図れるため、適宜改善を検討することが大切です。

外部委託先におけるセキュリティ対策の実施状況の定期的確認

外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先に委託する自社のセキュリティ対策を、選定時には実施可能かを確認するとともに、運用時においても継続的に実施状況を確認してください。確認すべきセキュリティ対策は以下の通りです。

- セキュリティ対策要件（運用時）の要件 1～5 の実施状況を定期的に確認してください。

- 確認頻度の目安としては、以下を参考にしてください。
  - （要件 1 の確認頻度）随時
  - （要件 2 の確認頻度）プラットフォーム診断は、少なくとも四半期に 1 回程度
    Web アプリケーション診断は、新機能の開発や追加やシステム改修などを行ったタイミングで実施
  - （要件 3 の確認頻度）少なくとも週に 1 回程度
  - （要件 4 の確認頻度）少なくとも週に 1 回程度
  - （要件 5 の確認頻度）少なくとも週に 1 回程度

NO	セキュリティ対策要件（運用時）	区分	自社で対応可能な要件	外部委託の活用で対応すべき要件
要件 1	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須		
要件 2	EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須		
要件 3	Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須		
要件 4	システムの定期的なバックアップの取得およびアクセ	必		

	スログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。	須		
要件 5	重要な情報はバックアップを取得する。	必須		
要件 6	WAF を導入する。	推奨		
要件 7	サイバー保険に加入する。	推奨		

21-1-6. 運用および保守

システムの安定稼動と継続的な改善は、中小企業にとっても重要です。適切な運用・保守計画を立て、定期的に見直すことで、長期的なコスト削減と効率化が図れます。

運用・保守の計画

運用・保守を担当する事業者が決まったら、事業者とともに調達仕様書で示した内容から、運用・保守の詳細な作業内容や実施方法などを検討し、計画書と実施要領として明文化します。運用・保守の作業はこの計画に基づいて実施することになるため、作業が漏れたり不十分だったりすると後々問題を引き起こすこともあるため、注意が必要です。

運用計画書の作成

運用計画書には、以下のような内容を記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	運用作業の対象範囲、作業概要
3	作業体制に関する事項	定常時およびインシデント発生時の体制
4	スケジュールに関する事項	運用業務の年次、四半期ごと、月次、週次、日次などのスケジュール
5	成果物に関する事項	成果物、担当者、納入期限、納入方法、納入部数、納入場所など
6	運用形態、運用環境など	運用において採用する運用形態（オンサイト、リモートなど）、定常時および障害発生時における運用環境（本番環境、検証環境、研修環境などの有無）など
7	そのほか	運用を行う上で留意すべき前提条件、運用の時間や予算、

		品質などに関する制約条件

保守計画書の作成

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	保守作業の対象範囲、作業概要
3	作業体制に関する事項	定常時およびインシデント発生時の体制
4	スケジュールに関する事項	提案書などの内容、保守事業者からの情報提供などを踏まえた保守業務のスケジュール
5	成果物に関する事項	成果物、担当者、納入期限、納入方法、納入部数、納入場所など
6	保守形態、保守環境など	保守において採用する保守形態（オンサイト、リモートなど）、アップデートファイル（セキュリティパッチなど）の適用前テストなどを行う検証環境など
7	そのほか	保守を行う上で留意すべき前提条件、保守の時間や予算または品質などに関する制約条件

運用・保守の改善と業務の引継ぎ

運用・保守の改善は、継続的に実施していきます。改善の内容には定常的な作業の範囲内で実施できるものもあれば、契約更新や事業者の交代、ライセンスの切れ目やハードウェアの交換でしか対応ができないものなど、さまざまなものがあります。これらは、対応できるタイミングが同一にはなりませんので、以下の点に留意して、確実に改善につなげるようにします。

改善を管理するポイント

- 運用・保守の定常的な作業内で解決が難しい課題は、「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の第 8 章「サービス・業務の運営と改善」内の問題管理として、どのタイミングで対応するかを明確に管理する。

- 現行の運用・保守契約期間では対応することが難しい大規模の改善については次回の契約において対応せざるを得ないものもあるので、改善のための予算規模やスケジュールなどについて計画を立て、関係者と事前調整を行うなど、早期から準備を進めておくことが重要である。

EC サイトを運営中の場合において実行すべき取組

EC サイトを運営中の場合においては、いつサイバー被害に遭ってもおかしくない状況を回避または、改善することが必要です。

取組 1.過去を振り返って、これまでのセキュリティ対策が不十分ではないか自己点検する。

IPA が公開している「安全なウェブサイトの作り方」や、「EC サイト構築・運用セキュリティガイドライン」の付録にある EC サイトの構築時や運用時における講じるべきセキュリティ対策要件をまとめたチェックシートを活用して、自社の EC サイトにおけるセキュリティ対策の自己点検を行ってください。

取組 2.セキュリティ対策が不十分であることがわかり、対策までに時間がかかる場合、対策までのサイバー被害リスクを減らすため、応急処置を行う。

セキュリティ対策が不十分であることがわかり、対策実施には時間がかかる場合、その間の攻撃リスクを減らすため、応急処置（例：WAF 実装、サイバー保険への加入）を実施してください。

なお、サイバー保険については、さまざまな種類・プランがあり、万が一の際の補償内容・金額やカバーされる脅威の範囲はもとより、事業性（売上高など）やセキュリティ対策状況、過去のインシデント被害経験などにより保険料が決まるため、詳細は保険会社にご確認ください。

取組 3.セキュリティ対策の不十分な箇所を対策する。

セキュリティ対策の不十分な箇所を対策し、あわせて、長期的（EC サイトの運用を継続する期間）なトータルコストを評価し、SaaS 型サービスやモール型サービスの利用も検討してください。

要員の交代で情報が欠落しないようにする

事業者が交代すると知識やドキュメント化されていない情報が抜け落ちてしまうことで作業効率が下がるリスクがあります。場合によっては、事業者が情報を持ち逃げするリスクもあり、持ち逃げされた情報を取り戻すために費用が発生するような場合もあります。このような事態を避けるためにも、従業員や運用・保守事業者の交代時には、以下の点に注意して、情報が抜け落ちてしまうことを防ぐことが重要です。

従業員や事業者の交代の際に気を付ける点

- 計画時点で作業に対する成果物を明確化する。作業を実施する場合は、基本的に作業手順書を作成し提出するよう、合意する。
- 中間成果物となるようなドキュメント・コンテンツは、維持が必要なもの、維持が必要ないものを明確にしていく。
- 運用・保守作業に関係する事項は、従業員や事業者の特定の担当者が抱え込むことなく、必

ずその作業を担当する事業者が管理するドキュメントに記載し管理する。

編集後記

本節では、はじめに「デジタル・ガバメント推進標準ガイドライン」の全体像を説明しました。次に EC サイトを具体例として取り上げ、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する際の流れと、セキュリティ対策の実装および運用のポイントを解説しました。

企画から要件定義、調達、設計・開発、運用保守などの各段階で、中小企業においても役に立つ部分を「デジタル・ガバメント推進標準ガイドライン」からピックアップして紹介しました。特に要件定義におけるセキュリティ要件は、組織で作成した適用宣言書をもとに決定することが重要です。情報資産におけるリスクを考慮して適切なセキュリティ要件を決めることで、情報システムのセキュリティ対策強化につながります。

「デジタル・ガバメント推進標準ガイドライン」は、政府や地方自治体の情報システム構築を前提としていますが、中小企業でも活用できる重要な部分が数多く記載されています。情報システムを導入する際は、本ガイドラインを参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能です。

引用文献

EC サイト構築・運用セキュリティガイドライン
https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

参考文献

DS-100 デジタル・ガバメント推進標準ガイドライン
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf
セキュリティ実装チェックリスト
https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx
EC サイト構築・運用セキュリティガイドライン
https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf
情報セキュリティサービス基準適合サービスリスト
https://www.ipa.go.jp/security/service_list.html
脆弱性診断サービス
https://www.ipa.go.jp/security/ug65p90000019fc0-att/20240611_2.pdf
デジタルフォレンジックサービス
https://www.ipa.go.jp/security/ug65p90000019fc0-att/20240611_3.pdf
ウェブサイトの攻撃兆候検出ツール iLogScanner
https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

■AI

Artificial Intelligence の略。

「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第 4 次 AI ブームに入ったとの見方もある）。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画

■CSIRT（シーサート）

Computer Security Incident Response Team の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■DFFT

Data Free Flow with Trust の略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

■EDR

Endpoint Detection and Response の略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政法人情報処理推進機構（IPA）内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence、ICSCoE）

が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■ICT

Information and Communication Technology の略。IT（情報技術）に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常な通信をブロックする機能はない

■IoT（アイ・オー・ティー）

Internet of Things の略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

■IPS

Intrusion Prevention System の略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。現在主に使用されているこれら 4 つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6 では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携の取り組み推進を図る組織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取組。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる

■ISP

個人や企業などに対してインターネットに接続するため

のサービスを提供する事業者のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる

■IT リテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる

■JVN

Japan Vulnerability Notes の略。日本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対策情報を提供する、脆弱性対策情報ポータルサイトのこと

■KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの。

■LockBit2.0

「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される

■MAC アドレス

Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

■NISC

National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

■NIST サイバーセキュリティフレームワーク（CSF）

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

■NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

■PII

Personally Identifiable Information の略。「個人を特

定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号だけでなく、氏名、生年月日、住所、勤務先などの情報も PII に含まれる

■PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管理を行うチームや担当者を指す

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

■PMO

Project Management Office の略。（企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。）組織全体のプロジェクトを横断的に管理する体制を指す

政府ガイドラインでの PMO は、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う（例：計画、予算、執行管理、PJMO 支援など）

■RFI

Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること

■SASE（サシー）

Secure Access Service Edge の略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の 1 つで、IT 環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

■SBOM（エスボム）

Software Bill of Materials の略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOM は、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOM は、ソフトウェアのリスクを把握・管理するのに役立つ

■SDP

Software-Defined Perimeter の略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPN は、ネットワーク接続前に一度だけ認証を行うのに対し、SDP は、ユーザーの情報（デバイス、場所、OS など）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

■Society5.0

日本が目指すべき未来社会の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなってきている。しかし、歴史的経緯で SSL の用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する

■SWG

Secure Web Gateway の略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■WAF（ワフ）

Web Application Firewall の略。従来のファイアウォールが、IP アドレスとポート番号で通信を制御していたことに対して、Web アプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者に依頼する必要がある

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することにより、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口や ATM に出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェアがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真つきの手配書のようなもの

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

■完全性

参照する情報が改ざんされていなく、正確である特性

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている

■供給者

組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PC やサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている

■コーディング

プログラミング言語でソースコードを書くこと

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまでさまざまである。デジタル社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022

では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される

■情報セキュリティの 3 要素「CIA」

情報セキュリティの 3 つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

■スクリーンセーバ

離席時に PC の画面の内容を盗み見されることを防ぐ機能のこと。PC に対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した 22 歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、独立行政法人情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載することが一般的

■ゼロデイ攻撃

OS やソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開の Web サイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2

つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである

■デジタル情報

0、1、2 のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の 2 進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO27001 の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある。

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Em

ail Compromise とも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンの OS に付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

■ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバー

セキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

■ブラックマーケット

広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するインターネット上の市場（闇市）

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Web サーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施することができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

■ミラサポコネクト

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェア

のこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

■無線 LAN

LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線 LAN を通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

■無停電電源装置

UPS とも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

■リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかのセキュリティ対策を講じる必要がある

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス

■リモートデスクトップ接続

パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法

CSF2.0 の管理策と実装例

機能	カテゴリ	サブカテゴリ	実装例
ガバナンス（GV）:組織のサイバーセキュリティリスク管理戦略、期待、ポリシーが確立され、伝達され、監視されている。	組織の状況（GV.OC）:組織のサイバーセキュリティリスクマネジメントの意思決定を取り巻く状況（ミッション、利害関係者の期待、依存関係、法律、規制、契約上の要件）が理解されている。	GV.OC-01:組織のミッションが理解され、サイバーセキュリティリスク管理に反映されている。	例 1:組織の使命を（ビジョンや行動指針、マーケティング、サービス戦略などを通じて）共有し、その使命を阻害する可能性のあるリスクを特定するための根拠を事前に提供する。
		GV.OC-02:社内外の利害関係者が理解され、サイバーセキュリティリスク管理に関する彼らのニーズと期待が理解、考慮される。	例 1:関連する社内の利害関係者と、彼らのサイバーセキュリティに関連する期待を特定する（例えば、役員、取締役、顧問に対する実績とリスクに関する予測、従業員に対する文化的な期待）。
			例 2:関連する社外の利害関係者と、彼らのサイバーセキュリティに関する期待を特定する（例えば、顧客のプライバシー、ビジネスパートナーの事業、規制当局のコンプライアンス、社会倫理などへの予測について）。
		GV.OC-03:サイバーセキュリティに関する法的、規制的、契約上の要件（プライバシーおよび市民的自由の義務を含む）が理解・管理される。 ※市民的自由:思想・言論・行動の自由など、権利章典によって保証されている自由のこと。	例 1:個人情報の保護について法的・規制要件を追跡・管理プロセスを決定する（医療保険の相互運用性と説明責任に関する法律、カリフォルニア州消費者プライバシー法、一般データ保護規則など）。
			例 2:サプライヤー、顧客、パートナーの情報についてサイバーセキュリティ管理に関する契約要件を追跡し管理するプロセスを決定する。
			例 3:組織のサイバーセキュリティ戦略を、法的・規制的・契約的要件と整合させる。
		GV.OC-04:ステークホルダーが組織に依存または期待する重要な目的、能力、サービスを理解し、伝達する。	例 1:社内外のステークホルダーから見た能力とサービスの重要性を判断する基準を確立する。
			例 2:ミッション目標の達成に不可欠な資産および事業活動と、そのような業務の損失（または部分的な損失）による潜在的な影響を判断する（例えば、ビジネスインパクト分析から）。
			例 3:さまざまな運用状態（例:攻撃時、回復時、通常運用時）において、重要な能力とサービスを提供するための回復

			目標（例:回復時間目標）を設定し、伝達する。
		GV.OC-05:組織が依存する成果、能力、サービスが理解、伝達されている。	例 1:組織の外部リソースへの依存度（例:施設、クラウドベースのホスティングプロバイダー）と、組織の資産およびビジネス機能との関係の目録を作成する。
			例 2:組織の重要な機能およびサービスにとって潜在的な障害となる外部依存関係を特定、文書化し、その情報を適切な要員と共有する。
	リスクマネジメント戦略（GV.RM）:組織の優先事項、制約事項、リスクの許容と選好度、前提が設定・伝達され、オペレーショナルリスクの意思決定を支援するために使用される。	GV.RM-01:リスクマネジメントの目標が設定され、組織の利害関係者によって決定・合意される。	例 1:年次戦略計画の一環として、また大きな変更が発生したときに、短期的および長期的なサイバーセキュリティリスク管理目標を更新する。
			例 2:サイバーセキュリティリスク管理のための測定可能な目標を設定する（例:ユーザートレーニングの質を管理する、産業用制御システムの適切なリスク保護を確保する）。
			例 3:シニアリーダーがサイバーセキュリティの目標に合意し、リスクとパフォーマンスの測定・管理に活用している。
		GV.RM-02:リスク選好度およびリスク許容度が設定され、伝達され、維持されている。	例 1:組織にとっての適切なリスクレベルについての期待を伝えるリスク選好度に関する声明を決定し、伝達する。
			例 2:リスク選好度を、具体的かつ測定可能で、広く理解可能なリスク許容度に変換する。
			例 3:既知と残存リスクに基づいて、組織目標とリスク選好度を定期的に見直す。
		GV.RM-03:サイバーセキュリティリスクマネジメントの活動と成果が、企業のリスクマネジメントプロセスに含まれる。	例 1:他の企業リスク（例:コンプライアンス、財務、業務、規制、風評、安全性）とともに、サイバーセキュリティリスクを集約し、管理する。
			例 2:企業のリスク管理計画にサイバーセキュリティリスクマネージャーを含める。
			例 3:企業のリスク管理におけるサイバーセキュリティリスクのエスカレーション基準を設定する。
		GV.RM-04:適切なリスク対応の選択肢を示す戦略的方策を確立し、伝達する。	例 1:さまざまな分類のデータについて、サイバーセキュリティ上のリスクについて受容および回避の基準を明示する。
			例 2:サイバーセキュリティ保険に加入するか否かの判断をする。
			例 3:責任共有モデルが許容される条件を文書化する（例:特定のサイバーセキュリティ機能のアウトソーシング、サード

			パーティが組織に代わって金融取引を実行する、パブリッククラウドベースのサービスを使用する)。
		GV.RM-05:サプライヤーやそのほかの第三者からのリスクも含め、サイバーセキュリティリスクに関する組織横断的なコミュニケーションラインを確立する。	例 1:上級管理職、取締役、および経営幹部が、組織のサイバーセキュリティ体制について、合意された間隔で更新する方法を決定する。
			例 2:経営陣、業務担当者、内部監査員、法務担当者、買収担当者、物理セキュリティ担当者、人事担当者など、組織全体にまたがるすべての部門が、サイバーセキュリティリスクについてどのように互いにコミュニケーションを図るかを明らかにする。
		GV.RM-06:サイバーセキュリティリスクの算出、文書化、分類、優先順位付けのための標準化された方法を確立し、周知する。	例 1:サイバーセキュリティリスク分析に定量的アプローチを使用するための基準を確立し、確率とエクスポージャーの公式を明示する。
			例 2:サイバーセキュリティリスク情報（リスクの説明、曝露、処置、所有者など）を文書化するためのテンプレート（リスク登録簿など）を作成し、使用する。
			例 3:企業内の適切なレベルでリスクの優先順位付けの基準を確立する。
			例 4:リスクカテゴリの一貫したリストを使用して、サイバーセキュリティリスクの統合、集約、比較をサポートする。
		GV.RM-07:戦略的機会（すなわち、ポジティブリスク）が特徴づけられ、組織のサイバーセキュリティリスクの議論に含まれる。	例 1:機会を特定し、リスクディスカッションに含めるための、ガイダンスと方法を定義・伝達する（例:強み、弱み、機会、脅威[SWOT]分析)。
			例 2:ストレッチゴールを特定し、文書化する。 ※ストレッチゴール ビジネスにおける部下育成のための目標設定手法である。現在のスキルや経験に加えて最大限の努力が必要な目標を設定することで、背伸びをした目標を設定することができる。
			例 3:ポジティブリスクとネガティブリスクを計算、文書化、優先順位付けする。 ※ポジティブリスク 資産、知識、改善、またはデータの潜在的な利益を指す。

			※ネガティブリスク 潜在的な損失を指す。
	役割、責任、および権限（GV.RR）:サイバーセキュリティの役割、責任、および説明責任、パフォーマンス評価、および継続的な改善を促進するための権限が確立され、伝達される。	GV.RR-01:組織のリーダーシップは、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を醸成する。	例 1:リーダー（取締役など）は、組織のサイバーセキュリティ戦略の策定、実施、評価における各自の役割と責任について合意する。
			例 2:特に、現在の出来事がサイバーセキュリティリスク管理の肯定的または否定的な例を強調する機会を提供する場合安全で倫理的な文化に関するリーダーの期待を共有する。
			例 3:リーダーは CISO に、包括的なサイバーセキュリティリスク戦略を維持し、少なくとも年に一度、および主要なイベント後にそれを見直して更新するように指示する。
			例 4:サイバーセキュリティリスクの管理責任者間で適切な権限と調整を確保するためのレビューを実施する。
		GV.RR-02:サイバーセキュリティリスク管理に関連する役割、責任、および権限が確立され、伝達され、理解され、実施される。	例 1:リスク管理の役割と責任をポリシーに文書化する。
			例 2:サイバーセキュリティリスク管理活動の責任者と説明責任、およびそれらのチームと個人にどのように相談し、通知するかを文書化する。
			例 3:サイバーセキュリティの責任とパフォーマンス要件を人事記述に含める。
			例 4:サイバーセキュリティリスク管理を担当する要員のパフォーマンス目標を文書化し、定期的にパフォーマンスを測定して改善点を特定する。
			例 5:業務、リスク機能、内部監査機能におけるサイバーセキュリティの責任を明確にする。
		GV.RR-03:サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースを配分する。	例 1:定期的なマネジメントレビューを実施し、サイバーセキュリティリスクマネジメントの責任者に必要な権限が与えられていることを確認する。
			例 2:リスク許容度と対応に沿ったリソース配分と投資を特定する。
			例 3:サイバーセキュリティ戦略を支援するために、適切かつ十分な人材、プロセス、技術的リソースを提供する。
		GV.RR-04:サイバーセキュリティは人事慣行に含まれる。	例 1:サイバーセキュリティリスク管理への配慮を人事プロセス（人事審査、入社手続き、変更通知、退社手続きなど）に組み込む。

			例 2:サイバーセキュリティの知識は、雇用、トレーニング、定着の決定においてプラス要因であると考える。
			例 3:機密性の高い役割の従業員をオンボーディングする前に身元調査を実施し、そのような役割の担当者の身元調査を定期的に繰り返す。
			例 4:各自の役割に関連するセキュリティポリシーを認識し、順守し、維持するための要員の義務を定義し、実施する。
	ポリシー（GV.PO）：組織のサイバーセキュリティポリシーが確立され、伝達され、実施される。	GV.PO-01:サイバーセキュリティリスクの管理方針が、組織の状況、サイバーセキュリティ戦略、優先事項に基づいて策定され、周知され、実施される。	例 1:経営陣の意図、期待、方向性を記述した、理解しやすく使いやすいリスク管理ポリシーを作成、普及、維持する。
			例 2:ポリシーとそれをサポートするプロセスと手順を定期的に見直して、リスク管理戦略の目標と優先事項、およびサイバーセキュリティポリシーの高レベルの方向性と一致していることを確認する。
			例 3:ポリシーについて上級管理職の承認を必要とする。
			例 4:サイバーセキュリティリスク管理ポリシーとそれをサポートするプロセスと手順を組織全体に伝達する。
			例 5:最初に採用されたとき、毎年、およびポリシーが更新されるたびに、ポリシーの受領を確認するように担当者に要求する。
		GV.PO-02:サイバーセキュリティリスクの管理方針は、要件、脅威、技術、組織ミッションの変化を反映するよう、見直し、更新、伝達、実施される。	例 1:サイバーセキュリティリスク管理の結果の定期的なレビューに基づいてポリシーを更新し、ポリシーとサポートプロセスと手順がリスクを許容可能なレベルで適切に維持するようにする。
			例 2:組織のリスク環境に対する変更（リスクや組織のミッション目標の変更など）をレビューするためのタイムラインを提供し、推奨されるポリシーの更新を伝える。
			例 3:法的要件および規制要件の変更を反映するようにポリシーを更新する。
			例 4:テクノロジーの変更（人工知能の採用など）とビジネスの変更（新しいビジネスの買収、新しい契約要件など）を反映するようにポリシーを更新する。
	監視（GV.OV）:組織全体のサイバーセキュ	GV.OV-01:サイバーセキュリティリスク管理戦略の成果を	例 1:リスク管理戦略とリスク結果が、リーダーが意思決定を行い、組織の目標を達成するのにどの程度役立ったかを測

	リティリスク管理活動と実績の結果が、リスク管理戦略の情報提供、改善、調整に利用される。	レビューし、戦略と方向性に反映・調整する。	定する。
			例 2:運用やイノベーションを阻害するサイバーセキュリティリスク戦略を調整すべきか否かを検討する。
		GV.OV-02:組織の要求事項とリスクを確実にカバーするために、サイバーセキュリティリスク管理戦略がレビューされ、調整される。	例 1:監査結果を見直して、既存のサイバーセキュリティ戦略が内部および外部の要件への準拠を確保しているか否かを確認する。
			例 2:サイバーセキュリティ関連の役割を担う人々のパフォーマンス監視を見直して、ポリシーの変更が必要か否かを判断する。
			例 3:サイバーセキュリティインシデントを踏まえた戦略の見直し。
		GV.OV-03:組織のサイバーセキュリティリスク管理のパフォーマンスが評価され、必要な調整のために再確認される。	例 1:重要業績評価指標（KPI）を組織全体のポリシーと手順が目標の達成を保証するために再確認する。
			例 2:重要リスク指標（KRI）を見直して、組織が直面するリスク（可能性と潜在的な影響を含む）を特定する。
			例 3:上級管理職にサイバーセキュリティリスク管理に関する指標を収集し、伝達する。
	サイバーセキュリティサプライチェーンリスク管理（GV.SC）:サイバーサプライチェーンのリスク管理プロセスは、組織の利害関係者によって特定、確立、管理、監視、および改善される。	GV.SC-01:サイバーセキュリティのサプライチェーンリスク管理プログラム、戦略、目的、方針、およびプロセスが確立され、組織の利害関係者によって合意されている。	例 1:サイバーセキュリティサプライチェーンリスク管理プログラムの目的を表現する戦略を確立する。
			例 2:プログラムの実施と改善に導く計画（マイルストーンを含む）、ポリシー、手順を含むサイバーセキュリティサプライチェーンリスク管理プログラムを開発し、ポリシーと手順を組織の利害関係者と共有する。
			例 3:組織の利害関係者が合意し、実行する戦略、目的、ポリシー、および手順に基づいて、プログラムプロセスを開発および実装する。
			例 4:サイバーセキュリティ、IT、運用、法務、人事、エンジニアリングなど、サイバーセキュリティサプライチェーンのリスク管理に貢献する機能間の整合性を確保するための組織横断的なメカニズムを確立する。
		GV.SC-02:サプライヤー、顧客、パートナーに対するサイバーセキュリティの役割と責	例 1:サイバーセキュリティサプライチェーンのリスク管理活動の計画、リソース、および実行に責任を持ち、説明責任を負う 1 つ以上の特定の役割またはポジションを特定する。

		任が確立され、伝達され、社内外で調整される。	例 2:サイバーセキュリティサプライチェーンのリスク管理の役割と責任をポリシーに文書化する。
			例 3:サイバーセキュリティサプライチェーンのリスク管理活動の全体の責任と説明責任を誰が負うか、そしてそれらのチームと個人にどのように相談し、通知するかを文書化するための責任マトリックスを作成する。
			例 4:サイバーセキュリティサプライチェーンのリスク管理の責任とパフォーマンス要件を人事記述に含めて、明確にし、また説明責任を向上させる。
			例 5:サイバーセキュリティリスク管理固有の責任を持つ担当者のパフォーマンス目標を文書化し、定期的に測定してパフォーマンスを実証および改善する。
			例 6:サプライヤー、顧客、ビジネスパートナーが、該当するサイバーセキュリティリスクに対する共通の責任に対処するための役割と責任を開発し、それらを組織のポリシーと該当するサードパーティ契約に統合する。
			例 7:サイバーセキュリティサプライチェーンのリスク管理の役割と第三者に対する責任を社内で伝達する。
			例 8:組織とそのサプライヤー間の情報共有および報告プロセスに関するルールとプロトコルを確立する。
		GV.SC-03:サイバーセキュリティのサプライチェーンリスクマネジメントは、サイバーセキュリティおよび企業のリスクマネジメント、リスク評価、改善プロセスに統合する。	例 1:サイバーセキュリティとエンタープライズリスク管理との整合性と重複する領域を特定する。
			例 2:サイバーセキュリティリスク管理とサイバーセキュリティサプライチェーンリスク管理のための統合制御セットを確立する。
			例 3:サイバーセキュリティサプライチェーンのリスク管理を改善プロセスに統合する。
			例 4:サプライチェーンにおける重大なサイバーセキュリティリスクを上級管理職にエスカレーションし、企業リスク管理レベルで対処する。
		GV.SC-04:サプライヤーを把握し、重要度に応じて優先順位を付ける。	例 1:サプライヤーによって処理または所有されるデータの機密性、組織のシステムへのアクセスの程度、組織のミッションに対する製品またはサービスの重要性などに基づいて、サプライヤーの重要度の基準を作成する。

			例 2:すべてのサプライヤーの記録を保持し、重要度基準に基づいてサプライヤーに優先順位を付ける。
		GV.SC-05:サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件は設定され、順位付けられ、サプライヤーやそのほかの関連する第三者との契約やそのほかの合意に組み込まれる。	例 1:サプライヤー、製品、サービスの重要度レベルと、侵害された場合の潜在的な影響に見合ったセキュリティ要件を確立する。
			例 2:第三者が従うべきすべてのサイバーセキュリティおよびサプライチェーン要件と、デフォルトの契約言語で要件の順守を確認する方法を含める。
			例 3:組織とそのサプライヤーおよび契約上のサブ・ティアサプライヤー間の情報共有に関するルールとプロトコルを定義する。
			例 4:セキュリティ要件の重要性と侵害された場合の潜在的な影響に基づいて、セキュリティ要件を契約に含めることでリスクを管理する。
			例 5:サプライヤー関係のライフサイクルを通じて許容可能なセキュリティパフォーマンスについてサプライヤーを監視するためのサービスレベルアグリーメント（SLA）でセキュリティ要件を定義する。
			例 6:契約上、サプライヤーに対して、製品の寿命またはサービスの期間中、自社の製品およびサービスのサイバーセキュリティの特徴、機能、および脆弱性を開示するよう要求する。
			例 7:重要な製品の最新のコンポーネント在庫（ソフトウェアまたはハードウェアの部品表など）を提供し、維持することをサプライヤーに契約上要求する。
			例 8:契約上、サプライヤーに従業員を審査し、インサイダー脅威から保護することを要求する。
			例 9:契約上、サプライヤーに対して、自己証明、既知の標準への準拠、認証、検査などを通じて、許容可能なセキュリティ慣行を実施している証拠を提供するよう要求する。
			例 10:契約およびその他の合意において、潜在的なサイバーセキュリティリスクに関して、組織、そのサプライヤー、およびそれらのサプライチェーンの権利と責任を明記する。

		GV.SC-06:正式なサプライヤーやそのほかの第三者との関係を結ぶ前に、リスクを低減するための計画やデューデリジェンスが実施されている。 ※デューデリジェンス企業などに要求される当然に実施すべき注意義務および努力のこと。	例 1:調達計画と整合し、各サプライヤーとの関係のリスク、重要性、複雑さのレベルに見合った、見込みサプライヤーに対する徹底的なデューデリジェンスを実施する。
			例 2:テクノロジーとサイバーセキュリティ機能の適合性、および将来のサプライヤーのリスク管理慣行を評価する。
			例 3:ビジネスおよび適用されるサイバーセキュリティ要件に対するサプライヤーリスク評価を実施する。
			例 4:重要な製品を購入して使用する前に、信頼性、完全性、セキュリティを評価する。
		GV.SC-07:サプライヤー、その製品・サービス、そのほかの第三者によってもたらされるリスクを理解し、記録し、優先順位を付け、評価し、対応し、関係を通じて監視する。	例 1:評価の形式と頻度を、第三者の評判と提供する製品またはサービスの重要性に基づいて調整する。
			例 2:自己証明、保証、認証、そのほかの成果物など、契約上のサイバーセキュリティ要件に準拠しているという第三者の証拠を評価する。
			例 3:重要なサプライヤーを監視し、検査、監査、テスト、そのほかの形式の評価など、さまざまな方法と手法を使用して、サプライヤー関係のライフサイクル全体を通じてセキュリティ義務を果たしていることを確認する。
			例 4:重要なサプライヤー、サービス、製品のリスクプロファイルの変化を監視し、それに応じてサプライヤーの重要度とリスクの影響を再評価する。
			例 5:ビジネスの継続性を確保するために、予期しないサプライヤーとサプライチェーン関連の中断を計画する。
		GV.SC-08:インシデント発生時の計画、対応、復旧活動に、関連するサプライヤーやそのほかの第三者が含まれる。	例 1:インシデント対応と復旧活動、および組織とそのサプライヤー間のステータスを報告するためのルールとプロトコルを定義して使用する。
			例 2:インシデント対応に関する組織とそのサプライヤーの役割と責任を特定し、文書化する。
			例 3:インシデント対応の演習とシミュレーションに重要なサプライヤーを含める。
			例 4:組織とその重要なサプライヤーとの間の危機管理コミュニケーションの方法とプロトコルを定義し、調整する。

			例 5:重要なサプライヤーと共同で教訓セッションを実施する。
		GV.SC-09:サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリスク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイクル全体を通じて監視される。	例 1:ポリシーと手順により、取得したすべてのテクノロジー製品およびサービスの来歴記録を必要とする。
			例 2:買収したコンポーネントが改ざんされていないため、本物であることが証明された方法について、リーダーに定期的にリスクレポートを提供する。
			例 3:サイバーセキュリティのリスクマネージャーと運用担当者の間で、認証された信頼できるソフトウェアプロバイダーからのみソフトウェアのパッチ、アップデート、アップグレードを取得する必要があることについて定期的に連絡を取る。
			例 4:ポリシーを見直して、承認されたサプライヤー担当者がサプライヤー製品のメンテナンスを行うことを要求していることを確認する。
			例 5:ポリシーと手順では、重要なハードウェアのアップグレードに不正な変更がないか確認する必要がある。
		GV.SC-10:サイバーセキュリティのサプライチェーンリスクマネジメント計画には、パートナーシップまたはサービス契約締結後に発生する活動に関する規定が含まれる。	例 1:正常な状況と不利な状況の両方で重要な関係を終了するためのプロセスを確立する。
			例 2:コンポーネントの寿命終了時の保守サポートと陳腐化の計画を定義して実装する。
			例 3:組織のリソースへのサプライヤーのアクセスが不要になったときに、すぐに非アクティブ化していることを確認する。
			例 4:組織のデータを含む資産が、タイムリーに、管理された、安全な方法で返却または適切に廃棄されていることを確認する。
			例 5:サプライヤーとの関係を終了または移行するための計画を策定し、実行し、サプライチェーンのセキュリティリスクとレジリエンスを考慮に入れる。
			例 6:サプライヤーの終了によって生じるデータとシステムへのリスクを軽減する。
			例 7:サプライヤーの契約に関連するデータ漏えいリスクを管理する。

識別（ID）:組織の現在のサイバーセキュリティリスクを把握する。	資産管理（ID.AM）：組織がビジネス目的を達成できるようにする資産（データ、ハードウェア、ソフトウェア、システム、施設、サービス、人など）は、組織の目標と組織のリスク戦略に対する相対的な重要性と一致して特定および管理される。	ID.AM-01:組織が管理するハードウェアのインベントリを保持する。	例 1:IT、IoT、OT、モバイルデバイスなど、あらゆる種類のハードウェアの在庫を維持する。
			例 2:ネットワークを常に監視して新しいハードウェアを検出し、インベントリを自動的に更新する。
		ID.AM-02:組織が管理するソフトウェア、サービス、システムのインベントリを管理する。	例 1:商用オフザシェルフ、オープンソース、カスタムアプリケーション、API サービス、クラウドベースのアプリケーションとサービスなど、あらゆる種類のソフトウェアとサービスのインベントリを維持する。
			例 2:コンテナや仮想マシンを含むすべてのプラットフォームを常時監視し、ソフトウェアとサービスのインベントリの変更を確認する。
			例 3:組織のシステムのインベントリを維持する。
		ID.AM-03:組織の許可されたネットワーク通信と内部および外部のネットワークデータフローの表現が維持される。	例 1:組織の有線および無線ネットワーク内の通信とデータフローのベースラインを維持する。
			例 2:組織とサードパーティ間のコミュニケーションとデータフローのベースラインを維持する。
			例 3:組織の IaaS（Infrastructure-as-a-Service）の使用に関する通信とデータフローのベースラインを維持する。
			例 4:許可されたシステム間で通常使用される予想されるネットワークポート、プロトコル、およびサービスのドキュメントを維持する。
		ID.AM-04:サプライヤーが提供するサービスの在庫を管理する。	例 1:API のおよびそのほかの外部でホストされているアプリケーションサービス、サードパーティの Infrastructure-as-a-Service（IaaS）、Platform-as-a-Service（PaaS）、Software-as-a-Service（SaaS）オファリングなど、組織が使用するすべての外部サービスのインベントリを作成する。
			例 2:新しい外部サービスを利用する場合はインベントリを更新して、組織によるそのサービスの使用の適切なサイバーセキュリティリスク管理監視を確保する。
		ID.AM-05:資産は、分類、重要度、リソース、ミッションへの影響に基づいて優先順位が付けられる。	例 1:各クラスの資産の優先順位付けの基準を定義する。
			例 2:資産に優先順位付け基準を適用する。
			例 3:資産の優先順位を追跡し、定期的に更新するか、組織に大幅な変更が発生したときに更新する。

		ID.AM-06:[撤回:GV.RR-02、GV.SC-02 に編入する。]	
		ID.AM-07:指定されたデータ型のデータと対応するメタデータのインベントリが維持される。	例 1:指定された関心のあるデータタイプ（個人を特定できる情報、保護医療情報、金融口座番号、組織の知的財産、運用技術データなど）のリストを維持する。
			例 2:アドホックデータを継続的に検出および分析して、指定されたデータタイプの新しいインスタンスを特定する。
			例 3:タグまたはラベルを使用して、指定したデータ型にデータ分類を割り当てる。
			例 4:指定されたデータタイプの各インスタンスの出所、データ所有者、およびジオロケーションを追跡する。
		ID.AM-08: システム、ハードウェア、ソフトウェア、サービス、データは、そのライフサイクル全体を通じて管理される。	例 1:システム、ハードウェア、ソフトウェア、サービスのライフサイクル全体を通じてサイバーセキュリティの考慮事項を統合する。
			例 2:サイバーセキュリティに関する考慮事項を製品ライフサイクルに統合する。
			例 3:ミッション目標を達成するためのテクノロジーの非公式な使用（例:「シャドーIT」）を特定する。
			例 4:組織の攻撃対象領域を不必要に拡大する冗長なシステム、ハードウェア、ソフトウェア、サービスを定期的に特定する。
			例 5:システム、ハードウェア、ソフトウェア、サービスを本番環境に導入する前に、適切に構成し、保護する。
			例 6:システム、ハードウェア、ソフトウェア、およびサービスが組織内で移動または転送されたときにインベントリを更新する。
			例 7:組織のデータ保持ポリシーに基づき、保存されているデータを所定の破棄方法により安全に破棄し、破棄の記録を保持・管理する。
			例 8:ハードウェアが廃止、廃止、再割り当て、または修理や交換のために送られるときに、データストレージを安全に削除する。
			例 9:紙、記憶媒体、そのほかの物理的なデータストレージを破壊する方法を提供する。

	リスク評価（ID.RA）：組織、資産、および個人に対するサイバーセキュリティリスクは、組織によって理解される。	ID.RA-01:資産の脆弱性を特定、検証、記録する。	例 1:脆弱性管理テクノロジーを使用して、パッチが適用されていないソフトウェアや誤って構成されたソフトウェアを特定する。
			例 2:ネットワークとシステムアーキテクチャを評価し、サイバーセキュリティに影響を与える設計と実装の弱点を検出する。
			例 3:組織が開発したソフトウェアをレビュー、分析、またはテストして、設計、コーディング、およびデフォルト設定の脆弱性を特定する。
			例 4:重要なコンピューティング資産を収容する施設の物理的な脆弱性とレジリエンスの問題を評価する。
			例 5:サイバー脅威インテリジェンスのソースを監視して、製品やサービスの新たな脆弱性に関する情報を入手する。
			例 6:サイバーセキュリティに影響を与えるために悪用される可能性のある弱点について、プロセスと手順を確認する。
		ID.RA-02:情報共有フォーラムや情報源からサイバー脅威インテリジェンスを受け取る。	例 1:サイバーセキュリティツールとテクノロジーを検出または対応機能で構成し、サイバー脅威インテリジェンスフィードを安全に取り込む。
			例 2:現在の脅威アクターとその戦術、技術、手順（TTP）に関するアドバイザリを、信頼できる第三者から受け取り、レビューする。
			例 3:サイバー脅威インテリジェンスのソースを監視して、新興技術が持つ可能性のある脆弱性の種類に関する情報を入手する。
		ID.RA-03:組織に対する内部および外部の脅威を特定し、記録する。	例 1:サイバー脅威インテリジェンスを使用して、組織を標的にする可能性が高い脅威アクターの種類と、彼らが使用する可能性が高い TTP の認識を維持する。
			例 2:脅威ハンティングを実行して、環境内の脅威アクターの兆候を探す。
			例 3:内部の脅威アクターを特定するためのプロセスを実装する。
		ID.RA-04:脆弱性を悪用する脅威の潜在的な影響と可能性を特定し、記録する。	例 1:ビジネスリーダーとサイバーセキュリティリスクマネジメントの実務者が協力して、リスクシナリオの可能性と影響を見積り、リスク登録簿に記録する。

			例 2:組織の通信、システム、およびこれらのシステムで処理される、あるいはこれらのシステムによって処理されるデータへの不正アクセスが、ビジネスに及ぼしうる影響を列挙する。
			例 3:システムのシステムに対する連鎖的な障害の潜在的な影響を考慮する。
		ID.RA-05:脅威、脆弱性、可能性、影響は、固有のリスクを理解し、リスク対応の優先順位付けを通知するために使用される。	例 1:脅威モデルを開発して、データに対するリスクをよりよく理解し、適切なリスク対応を特定する。
			例 2:推定される可能性と影響に基づいて、サイバーセキュリティリソースの割り当てと投資に優先順位を付ける。
		ID.RA-06:リスク対応は選択、優先順位付け、計画、追跡、および伝達される。	例 1:リスクを受け入れるか、移転するか、軽減するか、回避するかを決定するための脆弱性管理計画の基準を適用する。
			例 2:リスクを軽減するための補償制御を選択するための脆弱性管理計画の基準を適用する。
			例 3:リスク対応の実施の進捗状況を追跡する（行動計画とマイルストーン[POA&M]、リスク登録、リスク詳細レポートなど）。
			例 4:リスク評価の結果を使用して、リスク対応の決定とアクションを通知する。
			例 5:影響を受けるステークホルダーに、優先順位を付けて計画されたリスク対応を伝える。
		ID.RA-07:変更と例外は管理され、リスクの影響について評価され、記録され、追跡される。	例 1:提案された変更と要求された例外の正式な文書化、レビュー、テスト、および承認のための手順を実装し、それに従う。
			例 2:提案された各変更を行うか、または行わない場合に発生する可能性のあるリスクを文書化し、変更のロールバックに関するガイダンスを提供する。
			例 3:リクエストされた各例外に関連するリスクと、それらのリスクに対応するための計画を文書化する。
			例 4:計画された将来のアクションまたはマイルストーンに基づいて受け入れられたリスクを定期的に見直す。

		ID.RA-08:脆弱性の開示を受領、分析、対応するためのプロセスを確立している。	例 1:契約で定義されたルールとプロトコルに従って、組織とそのサプライヤー間で脆弱性情報の共有を行う。
			例 2:サプライヤー、顧客、パートナー、政府のサイバーセキュリティ組織によるサイバーセキュリティの脅威、脆弱性、またはインシデントの開示の処理、影響の分析、および対応のための責任を割り当て、手順の実行を確認する。
		ID.RA-09:ハードウェアとソフトウェアの真正性と完全性は、取得および使用前に評価される。	例 1:重要なテクノロジー製品およびサービスを取得して使用する前に、信頼性とサイバーセキュリティを評価する。
		ID.RA-10:重要なサプライヤーは買収前に評価される。	例 1:サプライチェーンを含む、ビジネスおよび適用されるサイバーセキュリティ要件に対してサプライヤーリスク評価を実施する。
	改善（ID.IM）:組織のサイバーセキュリティリスク管理プロセス、手順、および活動の改善は、すべての CSF 機能で特定される。	ID.IM-01:評価から改善点を抽出する。	例 1:現在の脅威と TTP を考慮した重要なサービスの自己評価を実行する。
			例 2:組織のサイバーセキュリティプログラムの有効性に関する第三者評価または独立した監査に投資して、改善が必要な領域を特定する。
			例 3:自動化された手段を通じて、選択したサイバーセキュリティ要件への準拠を常に評価する。
		ID.IM-02:サプライヤーや関連する第三者との連携によるものを含め、セキュリティテストや演習から改善点が特定される。	例 1:インシデント対応評価の結果に基づいて、将来のインシデント対応活動の改善点を特定する（例:机上演習とシミュレーション、テスト、内部レビュー、独立監査）。
			例 2:重要なサービスプロバイダーや製品サプライヤーと連携して実施された演習に基づいて、将来のビジネス継続性、災害復旧、インシデント対応活動の改善点を特定する。
			例 3:必要に応じて、社内の利害関係者（上級管理職、法務部門、人事部など）をセキュリティテストと演習に参加させる。
			例 4:ペネトレーションテストを実施して、リーダーシップによって承認された、選択した高リスクシステムのセキュリティ体制を改善する機会を特定する。
			例 5:製品またはサービスが契約したサプライヤーまたはパートナーから発信されたものではない、または受領前に変更

			されたという発見に対応し、回復するための緊急時対応計画を行使する。
			例 6:セキュリティツールとサービスを使用してパフォーマンスメトリックを収集および分析し、サイバーセキュリティプログラムの改善を通知する。
		ID.IM-03:業務プロセス、手順、活動の実行から改善を特定する。	例 1:サプライヤーとの共同教訓セッションを実施する。
			例 2:サイバーセキュリティのポリシー、プロセス、手順を毎年見直し、学んだ教訓を考慮に入れる。
			例 3:メトリクスを使用して、運用上のサイバーセキュリティパフォーマンスを経時的に評価する。
		ID.IM-04:業務に影響を及ぼすインシデント対応計画およびそのほかのサイバーセキュリティ計画が策定され、伝達され、維持され、改善される。	例 1:運用に支障をきたす、機密情報を漏えいさせる、または組織の使命と実行可能性を危険にさらす可能性のある有害事象への対応と回復のための緊急時対応計画（インシデント対応、事業継続性、災害復旧など）を確立する。
			例 2:連絡先とコミュニケーションの情報、一般的なシナリオを処理するためのプロセス、優先順位付け、エスカレーション、昇格の基準をすべてのコンティンジェンシープランに含める。
			例 3:脆弱性管理計画を作成して、あらゆる種類の脆弱性を特定および評価し、リスク対応に優先順位を付け、テストし、実装する。
			例 4:サイバーセキュリティ計画（更新を含む）を、その実施責任者および影響を受ける当事者に伝達する。
			例 5:すべてのサイバーセキュリティ計画を毎年、または大幅な改善の必要性が特定された場合に、見直して更新する。
	ビジネス環境（ID.BE）:撤回:GV.OC に編入する。	ID.BE-01:[撤回:GV.OC-05 に編入する。]	
		ID.BE-02:[撤回: GV.OC-01 に編入する。]	
		ID.BE-03:[撤回: GV.OC-01 に編入する。]	
		ID.BE-04:[撤回: GV.OC-04、GV.OC-05 に編入する。]	

		ID.BE-05:[撤回: GV.OC-04 に編入する。]	
	ガバナンス（ID.GV）:撤回:GV に編入する。	ID.GV-01:[撤回:GV.PO、GV.PO-01、GV.PO-02 に編入する。]	
		ID.GV-02:[撤回:GV.OC-02、GV.RR、GV.RR-02 に編入する。]	
		ID.GV-03:[撤回:GV.OC-03 に移動する。]	
		ID.GV-04:[撤回:GV.RM-04 に移動する。]	
	リスクマネジメント戦略（ID.RM）:撤回:GV.RM に編入する。	ID.RM-01:[撤回:GV.RM-01、GV.RM-06、GV.RR-03 に編入する。]	
		ID.RM-02:[撤回:GV.RM-02、GV.RM-04 に編入する。]	
		ID.RM-03:[撤回: GV.RM-02 に移動する。]	
	サプライチェーンリスク管理（ID.SC）:撤回:ＧＶ.SC に編入する	ID.SC-01:[撤回:RM-05、GV.SC-01、GV.SC-06、GV.SC-09、GV.SC-10 に編入する。]	
		ID.SC-02:[撤回: GV.OC-02、GV.SC-03、GV.SC-04、GV.SC-07、ID.RA-10 に編入する。]	
		ID.SC-03:[撤回:GV.SC-05 に移動する。]	
		ID.SC-04:[撤回:GV.SC-07、ID.IM-02 に編入する。]	
		ID.SC-05:[撤回:GV.SC-08、ID.IM-02 に編入する。]	

防御（PR）:組織のサイバーセキュリティリスクを管理するための保護手段が使用される。	ID 管理、認証、およびアクセス制御（PR.AA）:物理的および論理的な資産へのアクセスは、許可されたユーザー、サービス、およびハードウェアに限定され、不正アクセスの評価されたリスクに見合った方法で管理される。	PR.AA-01:許可されたユーザー、サービス、およびハードウェアの ID とクレデンシャルが組織によって管理される。	例 1:従業員、請負業者、そのほかの新しいアクセスまたは追加のアクセスの要求を開始し、必要に応じてシステムまたはデータ所有者の許可を得て、要求を追跡、レビュー、および実行する。
			例 2:暗号化証明書と ID トークン、暗号化キー（つまり、キー管理）、およびそのほかの資格情報を発行、管理、および取り消す。
			例 3:不変のハードウェア特性から各デバイスの一意の識別子を選択するか、デバイスに安全にプロビジョニングされた識別子を選択する。
			例 4:インベントリとサービスの目的で、承認されたハードウェアに識別子を物理的にラベル付けする。
		PR.AA-02:アイデンティティは、相互作用のコンテキストに基づいて証明され、クレデンシャルにバインドされる。	例 1:登録時に政府発行の ID 資格情報（パスポート、ビザ、運転免許証など）を使用して、個人の主張する ID を確認する。
			例 2:各人に異なる資格情報を発行する（つまり、資格情報を共有しない）。
		PR.AA-03:ユーザー、サービス、ハードウェアを認証する。	例 1:多要素認証を要求する。
			例 2:パスワード、PIN、および同様の認証子の最小強度に関するポリシーを適用する。
			例 3:リスクに基づいてユーザー、サービス、ハードウェアを定期的に再認証する（ゼロトラストアーキテクチャなど）。
			例 4:緊急時下においてセキュリティ確保に必要不可欠なアカウントにアクセス可能な担当者を確保する。
		PR.AA-04:アイデンティティ・アサーションは保護、伝達、検証される。	例 1:シングルサインオンシステムを通じて認証とユーザー情報の伝達に使用される ID アサーションを保護する。
			例 2:連携システム間で認証とユーザー情報の伝達に使用されるアイデンティティ・アサーションの保護。
			例 3:権限のある担当者が、緊急時の安全を守るために不可欠なアカウントにアクセスできるようにすること。
		PR.AA-05:アクセス許可、資格、および権限がポリシーで定義され、管理され、実施さ	例 1:論理的および物理的なアクセス権限を定期的に、および誰かがロールを変更したり組織を離れたりするたびに確認し、不要になった権限を速やかに取り消す。

		れ、レビューされ、最小特権と職務分離の原則が組み込まれている。	例 2:リクエスターとリクエストされたリソースの属性を認証決定に考慮する（ジオロケーション、曜日/時間、リクエスターエンドポイントのサイバーヘルスなど）。
			例 3:アクセスと権限を必要最小限に制限する（例:ゼロトラストアーキテクチャ）。
			例 4:重要なビジネス機能に関連する権限を定期的に見直して、職務の適切な分離を確認する。
		PR.AA-06:資産への物理的なアクセスは、リスクに見合った形で管理、監視、実施される。	例 1:警備員、防犯カメラ、施錠された入り口、警報システム、およびそのほかの物理的制御を使用して、施設を監視し、アクセスを制限する。
			例 2:リスクの高い資産を含むエリアに対して、追加の物理的セキュリティ制御を採用する。
			例 3:ビジネスに不可欠な資産を含むエリア内で、ゲスト、ベンダー、そのほかの第三者をエスコートする。
	意識向上とトレーニング（PR.AT）:組織の要員は、サイバーセキュリティに関する意識向上とトレーニングを受け、サイバーセキュリティ関連の業務を遂行できるようになる。	PR.AT-01:要員は、サイバーセキュリティリスクを念頭において一般的な業務を遂行するための知識と技能を有するよう、意識向上とトレーニングを受ける。	例 1:従業員、請負業者、パートナー、サプライヤー、および組織の非公開リソースのそのほかすべてのユーザーに、基本的なサイバーセキュリティの認識とトレーニングを提供する。
			例 2:ソーシャルエンジニアリングの試みやそのほかの一般的な攻撃を認識し、攻撃や疑わしい活動を報告し、利用規定を順守し、基本的なサイバーハイジーンタスク（ソフトウェアのパッチ適用、パスワードの選択、資格情報の保護など）を実行するように、従業員を訓練する。
			例 3:サイバーセキュリティポリシー違反の結果について、個々のユーザーと組織全体の両方に説明する。
			例 4:基本的なサイバーセキュリティの実践に関するユーザーの理解度を定期的に評価またはテストする。
			例 5:既存のプラクティスを強化し、新しいプラクティスを導入するために、毎年のリフレッシャーを義務付ける。
		PR.AT-02:専門的な役割を担う個人が、サイバーセキュリティリスクを念頭に置いて関連業務を遂行するための知識	例 1:物理的なセキュリティおよびサイバーセキュリティの担当者、財務担当者、上級管理職、ビジネスクリティカルなデータにアクセスできる人など、追加のサイバーセキュリティトレーニングが必要な組織内の専門的な役割を特定する。

		と技能を有するよう、意識向上とトレーニングを提供する。	例 2:請負業者、パートナー、サプライヤー、そのほかの第三者を含む、専門的な役割を担うすべての人々に、役割ベースのサイバーセキュリティの認識とトレーニングを提供する。
			例 3:ユーザーがそれぞれの専門的な役割におけるサイバーセキュリティの実践を理解しているか否か、定期的に評価またはテストする。
			例 4:既存のプラクティスを強化し、新しいプラクティスを導入するために、毎年のリフレッシャーを必須にする。
		PR.AT-03:[撤回:PR.AT-01、PR.AT-02 に編入する。]	
		PR.AT-04:[撤回:PR.AT-02 に編入する。]	
		PR.AT-05:[撤回:PR.AT-02 に編入する。]	
	データセキュリティ（PR.DS）:情報の機密性、完全性、可用性を保護するために、組織のリスク戦略に沿ってデータを管理する。	PR.DS-01:静止データの機密性、完全性、可用性を保護する。	例 1:暗号化、デジタル署名、暗号化ハッシュを使用して、ファイル、データベース、仮想マシンディスクイメージ、コンテナイメージ、およびそのほかのリソースに格納されたデータの機密性と整合性を保護する。
			例 2:フルディスク暗号化を使用して、ユーザーエンドポイントに保存されているデータを保護する。
			例 3:署名の検証によるソフトウェアの整合性を確認する。
			例 4:リムーバブルメディアの使用を制限してデータ流出を防ぐ。
			例 5:暗号化されていない機密情報を含む物理的に安全なリムーバブルメディア（施錠されたオフィスやファイルキャビネット内など）。
		PR.DS-02:転送中のデータの機密性、完全性、および可用性を保護する。	例 1:暗号化、デジタル署名、および暗号化ハッシュを使用して、ネットワーク通信の機密性と整合性を保護する。
			例 2:データの分類に応じて、機密データを含む送信メールやそのほかの通信を自動的に暗号化またはブロックする。
			例 3:組織のシステムやネットワークから、個人の電子メール、ファイル共有、ファイルストレージサービス、そのほかの個人のコミュニケーションアプリケーションやサービスへ

			のアクセスをブロックする。
			例 4:本番環境の機密データ（顧客レコードなど）が開発、テスト、そのほかの非本番環境で再利用されるのを防ぐ。
		PR.DS-03:[撤回:ID.AM-08、PR.PS-03 に編入する。]	
		PR.DS-04:[撤回:PR.IR-04 に移動する。]	
		PR.DS-05:[撤回:PR.DS-01、PR.DS-02、PR.DS-10 に編入する。]	
		PR.DS-06:[撤回:PR.DS-01、DE.CM-09 に編入する。]	
		PR.DS-07:[撤回:PR.IR-01 に編入する。]	
		PR.DS-08:[撤回:ID.RA-09、DE.CM-09 に編入する。]	
		PR.DS-10:使用中のデータの機密性、完全性、および可用性が保護されている。	例 1:機密を保持する必要があるデータ（プロセッサやメモリなど）が不要になったらすぐに削除する。
			例 2:同じプラットフォームの他のユーザーやプロセスによるアクセスから使用中のデータを保護する。
		PR.DS-11:データのバックアップが作成、保護、維持、およびテストされる。	例 1:重要なデータをほぼリアルタイムで継続的にバックアップし、他のデータは合意されたスケジュールで頻繁にバックアップする。
			例 2:すべての種類のデータソースのバックアップと復元を少なくとも年に 1 回テストする。
			例 3:一部のバックアップをオフラインおよびオフサイトに安全に保管して、インシデントや災害によって損傷を受けないようにする。
			例 4:データバックアップストレージの地理的な分離と地理的な制限を適用する。
	プラットフォームのセキュリティ（PR.PS）:物理プラ	PR.PS-01:構成管理プラクティスが確立され、適用されている。	例 1:組織のサイバーセキュリティポリシーを適用し、必要な機能のみを提供する強化されたベースラインを確立、テスト、デプロイ、および維持する（つまり、最小機能の原

	ットフォームおよび仮想プラットフォームのハードウェア、ソフトウェア（ファームウェア、オペレーティングシステム、アプリケーションなど）、およびサービスが、組織のリスク戦略に従って管理され、機密性、完全性、および可用性を保護する。		則）。
			例 2:ソフトウェアをインストールまたはアップグレードする際に、サイバーセキュリティに影響を与える可能性のあるすべてのデフォルト設定を確認する。
			例 3:実装されたソフトウェアを監視し、承認されたベースラインからの逸脱がないか確認する。
		PR.PS-02:ソフトウェアはリスクに見合った保守、交換、削除が行われる。	例 1:脆弱性管理計画で指定された期間内に定期的および緊急のパッチ適用を実行する。
			例 2:コンテナイメージを更新し、既存のインスタンスを更新するのではなく、置き換えるために新しいコンテナインスタンスをデプロイする。
			例 3:サポートが終了したソフトウェアとサービスのバージョンを、サポートされ保守されているバージョンに置き換える。
			例 4:過度のリスクをもたらす不正なソフトウェアやサービスをアンインストールして削除する。
			例 5:攻撃者が悪用する可能性のある不要なソフトウェアコンポーネント（オペレーティングシステムユーティリティなど）をアンインストールして削除する。
			例 6:ソフトウェアとサービスの保守サポート終了と陳腐化の計画を定義して実装する。
		PR.PS-03:ハードウェアはリスクに見合った保守、交換、撤去を行う。	例 1:必要なセキュリティ機能がない場合、または必要なセキュリティ機能を備えたソフトウェアをサポートできない場合は、ハードウェアを交換する。
			例 2:ハードウェアのサポート終了と陳腐化の計画を定義して実装する。
			例 3:ハードウェアの廃棄を、安全で責任を持って、監査可能な方法で実行する。
		PR.PS-04:ログ記録を作成し、継続的なモニタリングに利用できるようにする。	例 1:すべてのオペレーティングシステム、アプリケーション、サービス（クラウドベースのサービスを含む）を構成して、ログレコードを生成する。
			例 2:組織のログ記録インフラストラクチャシステムおよびサービスとログを安全に共有するようにログジェネレーターを構成する。

			例 3:ゼロトラストアーキテクチャに必要なデータを記録するようにログジェネレーターを設定する。
		PR.PS-05:不正なソフトウェアのインストールと実行を防止する。	例 1:リスクが正当化される場合は、ソフトウェアの実行を許可された製品のみに制限するか、禁止および許可されていないソフトウェアの実行を拒否する。
			例 2:新しいソフトウェアをインストールする前に、そのソフトウェアの提供元と完全性を確認する。
			例 3:既知の悪意のあるドメインへのアクセスをブロックする承認された DNS サービスのみを使用するようにプラットフォームを構成する。
			例 4:組織が承認したソフトウェアのみのインストールを許可するようにプラットフォームを構成する。
		PR.PS-06:セキュアなソフトウェア開発プラクティスを統合し、ソフトウェア開発ライフサイクル全体を通じてそのパフォーマンスを監視する。	例 1:組織が開発したソフトウェアのすべてのコンポーネントを改ざんや不正アクセスから保護する。
			例 2:組織が作成したすべてのソフトウェアを、リリースの脆弱性を最小限に抑えて保護する。
			例 3:本番環境で使用するソフトウェアをメンテナンスし、不要になったソフトウェアは安全に廃棄する。
	技術基盤の回復力（PR.IR）:資産の機密性、完全性、可用性、および組織の回復力を保護するために、組織のリスク戦略に基づいてセキュリティアーキテクチャを管理する。	PR.IR-01:ネットワークと環境は、不正な論理アクセスや使用から保護されている。	例 1:信頼境界とプラットフォームタイプ（IT、IoT、OT、モバイル、ゲストなど）に従って、組織のネットワークとクラウドベースのプラットフォームを論理的にセグメント化し、セグメント間で必要な通信のみを許可する。
			例 2:組織のネットワークを外部ネットワークから論理的にセグメント化し、必要な通信のみが外部ネットワークから組織のネットワークに入ることを許可する。
			例 4:エンドポイントに運用リソースへのアクセスと使用を許可する前に、エンドポイントのサイバーヘルスを確認する。
			例 4:エンドポイントに運用リソースへのアクセスと使用を許可する前に、エンドポイントのサイバーヘルスを確認する。
		PR.IR-02:組織の技術資産を環境脅威から保護する。	例 1:洪水、火災、風、過度の熱と湿度などの既知の環境脅威から組織の機器を保護する。

			例 2:環境の脅威からの保護と、組織に代わってシステムを運用するサービスプロバイダーの要件に、適切な運用インフラストラクチャに関する規定を含める。
		PR.IR-03:平常時および不利な状況における回復力要件を達成するためのメカニズムが導入されている。	例 1:システムとインフラストラクチャの単一障害点を回避する。
			例 2:負荷分散を使用して容量を増やし、信頼性を向上させる。
			例 3:冗長ストレージや電源などの高可用性コンポーネントを使用して、システムの信頼性を向上させる。
		PR.IR-04:可用性を確保するために十分なリソース容量が維持されていること。	例 1:ストレージ、電源、コンピューティング、ネットワーク帯域幅、そのほかのリソースの使用状況を監視する。
			例 2:将来のニーズを予測し、それに応じてリソースを拡張する。
	ID 管理、認証、アクセス制御 (PR.AC):[撤回:PR.AA に移動する。]	PR.AC-01:[撤回:PR.AA-01、PR.AA-05 に編入する。]	
		PR.AC-02:[撤回:PR.AA-06 に移動する。]	
		PR.AC-03:[撤回:PR.AA-03、PR.AA-05、PR.IR-01 に編入する。]	
		PR.AC-04:[撤回: PR.IR-01 に移動する。]	
		PR.AC-05:[撤回:PR.IR-01 に編入する。]	
		PR.AC-06:[撤回: PR.IR-02 に移動する。]	
		PR.AC-07:[撤回: PR.IR-03 に移動する。]	
	情報保護のプロセスと手順 (PR.IP):[撤回: 他のカテゴリー・機能に組み込まれる。]	PR.IP-01:[撤回: PR.PS-01 に編入する。]	
		PR.IP-02:[撤回: ID.AM-08、PR.PS-06 に編入する。]	
		PR.IP-03:[撤回: PR.PS-01、ID.RA-07 に編入する。]	

		PR.IP-04:[撤回:PR.DS-11 に移動する。]	
		PR.IP-05:[撤回:PR.IR-02 に移動する。]	
		PR.IP-06:[撤回:ID.AM-08 に編入する。]	
		PR.IP-07:[撤回:ID.IM、ID.IM-03 に編入する。]	
		PR.IP-08:[撤回:ID.IM-03 に移動する。]	
		PR.IP-09:[撤回: ID.IM-04 に移動する。]	
		PR.IP-10:[撤回:ID.IM-02、ID.IM-04 に編入する。]	
		PR.IP-11:[撤回:GV.RR-04 に移動する。]	
		PR.IP-12:[撤回:ID.RA-01、PR.PS-02 に編入する。]	
	メンテナンス(PR.MA):撤回:ID.AM-08 に編入する。	PR.MA-01:[撤回:ID.AM-08、PR.PS-03 に編入する。]	
		PR.MA-02:[撤回: ID.AM-08、PR.PS-02 に編入する。]	
	保護技術 (PR.PT):撤回:他の保護カテゴリーに組み込まれる。	PR.PT-01:[撤回:PR.PS-04 に編入する。]	
		PR.PT-02:[撤回:PR.DS-01、PR.PS-01 に編入する。]	
		PR.PT-03:[撤回:PR.PS-01 に編入する。]	
		PR.PT-04:[撤回:PR.AA-06、PR.IR-01 に編入する。]	
		PR.PT-05:[撤回:PR.IR-03 に移動する。]	
検知（DE）:サイバーセキュリティ	継続的モニタリング（DE.CM）:異常、侵	DE.CM-01:ネットワークとネットワークサービスは、潜在	例 1:DNS、BGP、およびそのほかのネットワークサービスで有害事象を監視する。

攻撃や侵害の可能性を発見し、分析する。	害の指標、そのほかの潜在的な有害事象を発見するために資産を監視する。	的に有害な事象を発見するために監視される。	例 2:有線および無線ネットワークを監視して、許可されていないエンドポイントからの接続を確認する。
			例 3:許可されていないワイヤレスネットワークまたは不正なワイヤレスネットワークのための施設を監視する。
			例 4:実際のネットワークフローをベースラインと比較して、偏差を検出する。
			例 5:ネットワーク通信を監視して、ゼロトラストの目的でセキュリティ体制の変更を特定する。
		DE.CM-02:潜在的に有害な事象を発見するために、物理的環境をモニターする。	例 1:物理的なアクセス制御システム（バッジリーダーなど）からのログを監視して、異常なアクセスパターン（標準からの逸脱など）と失敗したアクセス試行を見つける。
			例 2:物理的なアクセス記録（訪問者登録、サインインシートなど）を確認および監視する。
			例 3:物理的なアクセス制御（ロック、ラッチ、ヒンジピン、アラームなど）を監視して、改ざんの兆候がないか確認する。
			例 4:警報システム、カメラ、警備員を使用して物理的環境を監視する。
		DE.CM-03:潜在的な有害事象を発見するため、従業員の活動および技術利用を監視する。	例 1:行動分析ソフトウェアを使用して異常なユーザーアクティビティを検出し、内部脅威を軽減する。
			例 2:論理アクセス制御システムからのログを監視して、異常なアクセスパターンと失敗したアクセス試行を見つける。
			例 3:ユーザーアカウントを含む欺瞞技術を継続的に監視し、あらゆる使用について監視する。
		DE.CM-04:[撤回。DE.CM-01 および DE.CM-09 に編入する。]	
		DE.CM-05:[撤回。DE.CM-01 および DE.CM-09 に編入する。]	
		DE.CM-06:外部サービス提供者の活動およびサービスは、	例 1:外部プロバイダーが組織システムに対して実行するリモートおよびオンサイトの管理および保守活動を監視する。

		潜在的に有害な事象を発見するために監視される。	例 2:クラウドベースのサービス、インターネットサービスプロバイダー、およびそのほかのサービスプロバイダーからのアクティビティを監視して、予想される動作からの逸脱を確認する。
		DE.CM-07:[撤回:DE.CM-01、DE.CM-03、DE.CM-06、DE.CM-09 に編入する。]	
		DE.CM-08:[撤回:ID.RA-01 に編入する。]	
		DE.CM-09:コンピューティングのハードウェアとソフトウェア、ランタイム環境、およびそれらのデータを監視し、潜在的に有害な事象を発見する。	例 1:メール、Web、ファイル共有、コラボレーションサービス、そのほかの一般的な攻撃ベクトルを監視して、マルウェア、フィッシング、データ漏えいと流出、そのほかの有害事象を検出する。
			例 2:認証の試行を監視して、資格情報に対する攻撃と資格情報の不正な再利用を特定する。
			例 3:ソフトウェア構成のセキュリティベースラインからの逸脱を監視する。
			例 4:ハードウェアとソフトウェアを改ざんの兆候がないか監視する。
			例 5:エンドポイントに存在するテクノロジーを使用して、サイバーヘルスの問題（パッチの欠落、マルウェア感染、未承認のソフトウェアなど）を検出し、アクセスが承認される前にエンドポイントを修復環境にリダイレクトする。
	有害事象分析（DE.AE）:異常、侵害の指標、そのほかの潜在的な有害事象を分析して事象を特徴づけ、サイバーセキュリティインシデントを検出する。	DE.AE-01:[撤回:ID.AM-03 に編入する。]	
		DE.AE-02:潜在的有害事象を分析し、関連する活動をよりよく理解する。	例 1:セキュリティ情報およびイベント管理（SIEM）またはそのほかのツールを使用して、既知の悪意のあるアクティビティや疑わしいアクティビティのログイベントを継続的に監視する。

			例 2:ログ分析ツールで最新のサイバー脅威インテリジェンスを活用して、検出精度を向上させ、脅威アクター、その方法、および侵害の兆候を特徴づける。
			例 3:自動化では十分に監視できないテクノロジーのログイベントについて、定期的に手動レビューを実施する。
			例 4:ログ分析ツールを使用して、調査結果に関するレポートを生成する。
		DE.AE-03:情報は複数の情報源から関連付けられている。	例 1:他のソースから生成されたログデータを比較的少数のログサーバに常に転送する。
			例 2:イベント相関技術（SIEM など）を使用して、複数のソースから取得した情報を収集する。
			例 3:サイバー脅威インテリジェンスを活用して、ログソース間でイベントを関連付ける。
		DE.AE-04:有害事象の推定影響と範囲が理解されている。	例 1:SIEM またはそのほかのツールを使用して、影響と範囲を見積り、見積りを確認して調整する。
			例 2:人が影響と範囲について自分で見積りを作成する。
		DE.AE-05:[撤回。DE.AE-08 に移動する。]	
		DE.AE-06:有害事象に関する情報は、権限を与えられたスタッフおよびツールに提供される。	例 1:サイバーセキュリティソフトウェアを使用してアラートを生成し、セキュリティオペレーションセンター（SOC）、インシデント対応者、インシデント対応ツールに提供する。
			例 2:インシデント対応者およびそのほかの権限のある担当者は、ログ分析の結果にいつでもアクセスできる。
			例 3:特定の種類のアラートが発生したときに、組織のチケットシステムでチケットを自動的に作成して割り当てる。
			例 4:技術スタッフが侵害の兆候を発見したときに、組織のチケットシステムでチケットを手動で作成して割り当てる。
		DE.AE-07:サイバー脅威インテリジェンスとそのほかの文脈情報が分析に統合される。	例 1:サイバー脅威インテリジェンスフィードを検知技術、プロセス、および担当者に安全に提供する。
			例 2:資産インベントリから検出技術、プロセス、人員まで情報を安全に提供する。

			例 3:サプライヤー、ベンダー、サードパーティのセキュリティアドバイザリから組織のテクノロジーの脆弱性開示を迅速に取得して分析する。
		DE.AE-08:インシデントは、有害事象が定義されたインシデント基準を満たす場合に宣言される。	例 1:インシデントを宣言すべきか否かを判断するために、アクティビティの既知および想定される特性にインシデント基準を適用する。
			例 2:インシデント基準を適用する際に既知の誤検知を考慮に入れる。
	検出プロセス (DE.DP):[撤回:他のカテゴリーおよび機能に編入する。]	DE.DP-01:[撤回:GV.RR-02 に編入する。]	
		DE.DP-02:[撤回:DE.AE に編入する。]	
		DE.DP-03:[撤回:ID.IM-02 に編入する。]	
		DE.DP-04:[撤回:DE.AE-06 に編入する。]	
		DE.DP-05:[撤回:ID.IM、ID.IM-03 に編入する。]	
対応（RS）:検出されたサイバーセキュリティインシデントに関する対応を行う。	インシデント管理（RS.MA）:検出されたサイバーセキュリティインシデントへの対応を管理する。	RS.MA-01:インシデント対応計画は、インシデントが宣言された後、関連する第三者と連携して実行される。	例 1:検知技術が確認済みのインシデントを自動的に報告する。
			例 2:組織のインシデント対応アウトソーシング業者にインシデント対応支援を依頼する。
			例 3:インシデントごとにインシデントリードを指名する。
			例 4:インシデント対応（ビジネス継続性やディザスターリカバリーなど）をサポートするために、必要に応じて追加のサイバーセキュリティ計画の実行を開始する。
		RS.MA-02:インシデント報告はトリアージされ、検証される。	例 1:インシデントレポートを事前にレビューして、サイバーセキュリティ関連であり、インシデント対応活動が必要であることを確認する。
			例 2:インシデントの重大度を見積る条件を適用する。
		RS.MA-03:インシデントは分類と優先順位付けされる。	例 1:インシデントの種類（データ侵害、ランサムウェア、DDoS、アカウント侵害など）に基づいてインシデントをさらにレビューし、分類する。

			例 2:インシデントの範囲、予想される影響、およびタイムクリティカルな性質に基づいてインシデントに優先順位を付ける。
			例 3:インシデントから迅速に復旧する必要性と、攻撃者を観察したり、より徹底的な調査を実施したりする必要性とのバランスを取ることで、アクティブなインシデントのインシデント対応戦略を選択する。
		RS.MA-04:インシデントは必要に応じてエスカレーションまたは昇格される。	例 1:進行中のすべてのインシデントのステータスを追跡して検証する。
			例 2:インシデントのエスカレーションまたは昇格を、指定された内部および外部の利害関係者と調整する。
		RS.MA-05:事故復旧の開始基準が適用される。	例 1:インシデントの既知および想定される特性にインシデント復旧基準を適用して、インシデント復旧プロセスを開始する必要があるか否かを判断する。
			例 2:インシデント復旧活動の運用中断の可能性を考慮に入れる。
	インシデント分析（RS.AN）:効果的な対応を確保し、フォレンジックと復旧活動をサポートするために調査を実施する。	RS.AN-01:[撤回:RS.MA-02 に編入する。]	
		RS.AN-02:[撤回:RS.MA-02、RS.MA-03、RS.MA-04 に編入する。]	
		RS.AN-03:インシデント発生時に何が起こったか、またその根本原因を特定するために分析を行う。	例 1:インシデント中に発生したイベントのシーケンスと、各イベントに関与した資産とリソースを特定する。
			例 2:インシデントに直接的または間接的に関与した脆弱性、脅威、および脅威アクターの特定を試みる。
			例 3:インシデントを分析して、根底にある体系的な根本原因を見つける。
			例 4:サイバーデセプションテクノロジーで攻撃者の行動に関する追加情報を確認する。
		RS.AN-04:[撤回:RS.MA-03 に移動する。]	
		RS.AN-05:[撤回:ID.RA-08 に移動する。]	

		RS.AN-06:調査中に行われた行為は記録され、記録の完全性と出所は保全される。	例 1:各インシデント対応者と、インシデント対応タスクを実行する他の人（システム管理者、サイバーセキュリティエンジニアなど）に、自分の行動を記録し、記録を不変にするように要求する。
			例 2:インシデントのリーダーにインシデントを詳細に文書化し、文書化の完全性と報告されるすべての情報のソースを維持する責任を持つように要求する。
		RS.AN-07:インシデントデータとメタデータを収集し、その完全性と出所を保全する。	例 1:証拠保全と CoC（Chain of Custody）の手続きに基づいて、関連するすべてのインシデントデータとメタデータ（データソース、収集日時など）の完全性を収集、保存、保護する。
		RS.AN-08:事故の規模を推定し、検証する。	例 1:インシデントのほかの潜在的なターゲットを確認して、侵害の兆候と永続性の証拠を検索する。
			例 2:ターゲットに対してツールを自動的に実行して、侵害の兆候と永続性の証拠を探す。
	インシデントレスポンスの報告とコミュニケーション（RS.CO）：対応活動は、法律、規制、またはポリシーの要求に従って、社内外の利害関係者と調整される。	RS.CO-01:[撤回:PR.AT-01 に編入する。]	
		RS.CO-02:社内外の利害関係者にインシデントを通知する。	例 1:データ侵害インシデントを発見した後、影響を受けた顧客への通知を含む、組織の侵害通知手順に従う。
			例 2:契約上の要件に従って、ビジネスパートナーや顧客にインシデントを通知する。
			例 3:インシデント対応計画の基準と経営陣の承認に基づいて、法執行機関および規制機関にインシデントを通知する。
		RS.CO-03:指定された社内外のステークホルダーと情報を共有する。	例 1:対応計画と情報共有契約に則った情報を安全に共有する。
			例 2:攻撃者が観測した TTP に関する情報を、すべての機密データを削除した状態で、情報共有分析センター（ISAC）と自発的に共有する。
			例 3:悪意のある内部関係者の活動が発生したときに人事部に通知する。
			例 4:重大インシデントの状況について、上級管理職に定期的に最新情報を提供する。
			例 5:組織とそのサプライヤー間のインシデント情報共有に関する契約で定義されているルールとプロトコルに従う。

			例 6:組織とその重要なサプライヤーとの間の危機管理コミュニケーション方法を調整する。
		RS.CO-04:[撤回:RS.MA-01、RS.MA-04 に編入する。]	
		RS.CO-05:[撤回:RS.CO-03 に編入する。]	
	事故の緩和（RS.MI）:事象の拡大を防ぎ、その影響を緩和するための活動。	RS.MI-01:インシデントを封じ込める。	例 1:サイバーセキュリティ技術（ウイルス対策ソフトウェアなど）と他の技術のサイバーセキュリティ機能（オペレーティングシステム、ネットワークインフラストラクチャデバイスなど）は、自動的に封じ込めアクションを実行する。
			例 2:インシデント対応者が手動で封じ込めアクションを選択して実行できるようにする。
			例 3:第三者（インターネットサービスプロバイダー、マネージドセキュリティサービスプロバイダーなど）が組織に代わって封じ込めアクションを実行できるようにする。
			例 4:侵害されたエンドポイントを修復仮想ローカルエリアネットワーク（VLAN）に自動的に転送する。
		RS.MI-02:インシデントを根絶する。	例 1:サイバーセキュリティ技術と他の技術（オペレーティングシステム、ネットワークインフラストラクチャデバイスなど）のサイバーセキュリティ機能は、自動的に根絶アクションを実行する。
			例 2:インシデント対応者が手動で根絶アクションを選択して実行できるようにする。
			例 3:第三者（マネージドセキュリティサービスプロバイダーなど）が組織に代わって根絶アクションを実行できるようにする。
		RS.MI-03:[ID.RA-06 に編入する。]	
	対応計画(RS.RP):[撤回:RS.MA に編入する。]	RS.RP-01:[撤回:RS.MA-01 に編入する。]	
	改善点(RS.IM):[撤回:ID.IM に編入する。]	RS.IM-01:[撤回:ID.IM-03、ID.IM-04 に編入する。]	
		RS.IM-02:[撤回:ID.IM-03 に	

		編入する。]	
復旧（RC）:サイバーセキュリティインシデントの影響を受けた資産や業務を復旧させる。	インシデント復旧計画の実行（RC.RP）:サイバーセキュリティインシデントの影響を受けたシステムとサービスの運用可用性を確保するための復旧活動を実施する。	RC.RP-01:インシデント対応計画の復旧部分は、インシデント対応プロセスから開始されると実行される。	例 1:インシデント対応プロセス中またはインシデント対応プロセス後に復旧手順を開始する。
			例 2:回復の責任を負うすべての個人に、回復の計画と、計画の各側面を実装するために必要な権限を認識させる。
		RC.RP-02:復旧アクションの選択、範囲設定、優先順位付け、実行を行う。	例 1:インシデント対応計画と利用可能なリソースで定義された基準に基づいて復旧アクションを選択する。
			例 2:組織のニーズとリソースの再評価に基づいて計画された復旧アクションを変更する。
		RC.RP-03:バックアップやそのほかのリストア資産をリストアに使用する前に、その完全性を検証する。	例 1:使用前に、復元資産に侵害、ファイルの破損、そのほかの整合性の問題の兆候がないか確認する。
		RC.RP-04:重要なミッション機能とサイバーセキュリティのリスク管理は、事故後の運用規範を確立するために考慮される。	例 1:ビジネスへの影響とシステムの分類レコード（サービス提供目標を含む）を使用して、重要なサービスが適切な順序で復元されていることを検証する。
			例 2:システム所有者と協力して、システムの正常な復元と通常の運用への復帰を確認する。
			例 3:復元されたシステムのパフォーマンスを監視して、復元の適切性を確認する。
		RC.RP-05:復旧した資産の完全性が検証され、システムとサービスが復旧し、正常な運用状態が確認される。	例 1:復元された資産で侵害の兆候を確認し、本番環境で使用する前にインシデントの根本原因を修復する。
			例 2:復元されたシステムをオンラインにする前に、実行された復元アクションの正確性と妥当性を確認する。
		RC.RP-06:基準に基づいて事故復旧の終了が宣言され、事故関連の文書化が完了する。	例 1:インシデント自体、実行された対応措置と復旧措置、および学んだ教訓を文書化した事後処理レポートを作成する。
			例 2:基準が満たされたら、インシデント復旧の終了を宣言する。
	事故復旧コミュニケーション（RC.CO）:復旧活動を社内外の関係者と調整する。	RC.CO-01:[撤回:RC.CO-04 に編入する。]	
		RC.CO-02:[撤回:RC.CO-04 に編入する。]	

		RC.CO-03:復旧活動と業務能力回復の進捗状況を、指定された社内外の利害関係者に伝達する。	例 1:復旧の進行状況を含む復旧情報を安全に共有し、対応計画と情報共有契約に則った対応する。
			例 2:重大インシデントの復旧状況と復旧の進捗状況について、上級管理職に定期的に最新情報を提供する。
			例 3:組織とそのサプライヤー間のインシデント情報共有に関する契約で定義されたルールとプロトコルに従う。
			例 4:組織とその重要なサプライヤーとの間の危機管理コミュニケーションを調整する。
		RC.CO-04:承認された方法とメッセージングを使用し、事故復旧に関する一般向けの最新情報を共有する。	例 1:データ侵害インシデントから回復するための組織の侵害通知手順に従う。
			例 2:インシデントから回復し、再発を防ぐために実行している手順を説明する。
	改善点 (RC.IM):撤回:ID.IM に編入する。	RC.IM-01:[撤回:ID.IM-03、ID.IM-04 に編入する。]	
		RC.IM-02:[撤回:ID.IM-03 に編入する。]	

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework （CSF） 2.0 Reference Tool	https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all

中小企業向けスタートアップガイドの活用方法

中小企業が、CSF2.0 を使用してセキュリティ対策を開始するにあたり、クイックスタートガイド（Small Business Quick-Start Guide）が参考になります。このガイドは、セキュリティ対策が十分でない中小企業に対して、セキュリティ対策を始めるための基本的なステップを提供します。ガバナンス、識別、防御、検知、対応、復旧、各機能それぞれにおいて、段階的に対策を進める方法を示しています。

このガイドは、必要に応じて外部の専門家やサービスの利用を検討するための指針にもなります。

各機能の活動の中から 1 つを例にとり、どのような内容が記載してあるかを説明します。

ガバナンス

ガバナンス機能は、ビジネスのサイバーセキュリティリスク管理戦略、期待値、ポリシーを確立し、監視するのに役立ちます。

考慮すべきアクション

理解
● サイバーセキュリティリスクが、ビジネスの目標達成をどのように妨げる可能性があるかを理解する。（GV.OC-01） ● 法的、規制上、および契約上のサイバーセキュリティ要件を理解する。（GV.OC-03） ● ビジネス内で誰がサイバーセキュリティ戦略を策定し、実行する責任を負うかを理解する。（GV.RR-02）
評価
● ビジネスにとって大事な資産や運営がすべて、または一部失われた場合にどんな影響が出るかを評価する。（GV.0C-04） ● 自社にサイバーセキュリティ保険が必要か否かを評価する。（GV.RM-04） ● 取引を開始する前に、取引先や他の第三者がもたらすサイバーセキュリティリスクを評価する。（GV.SC-06）
優先
● サイバーセキュリティリスクを、他のビジネスリスクと同じように優先して管理する。（GV.RM-03）
コミュニケーション
● 経営陣がリスクに気を配り、倫理的で常に改善を目指す姿勢をサポートしていることを伝える。（GV.RR-01） ● サイバーセキュリティリスクを管理するためのポリシーを伝達し、実施し、維持する。（GV.PO-01）

サイバーセキュリティ統制の始め方

以下の表を使って、サイバーセキュリティ統制戦略について考え始めることができます。

組織の目的や状況の整理	
組織の使命や目標	
組織の使命や目標の達成を妨げる可能性があるセキュリティリスクは何か？	

セキュリティ要件の文書化	
法的要件をリスト化する	
規制要件をリスト化する	
契約上の要件をリスト化する	

サイバーセキュリティ統制の始め方

（出典）NIST「NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide」をもとに作成

考慮すべきポイント

- ビジネスが成長するにつれて、どのくらいの頻度でサイバーセキュリティ戦略を見直していますか？
- 既存従業員のスキルアップが必要ですか？または、専門知識を持つ新しい人材を採用するか、外部のパートナーと協力してサイバーセキュリティ計画を確立し、管理する必要がありますか？
- 会社のデバイスおよび従業員の私物デバイスが会社の資産にアクセスする際の、適切な利用ポリシーは整っていますか？従業員はこれらのポリシーについて教育を受けていますか？

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1300