今すぐ実践できる工場セキュリティハンドブック

サイバー対応 IT-BCP 編　第 1.0 版

2025 年 5 月

JNSA 日本ネットワークセキュリティ協会

西日本支部

今すぐ実践できる工場セキュリティ対策のポイント検討 WG

目次

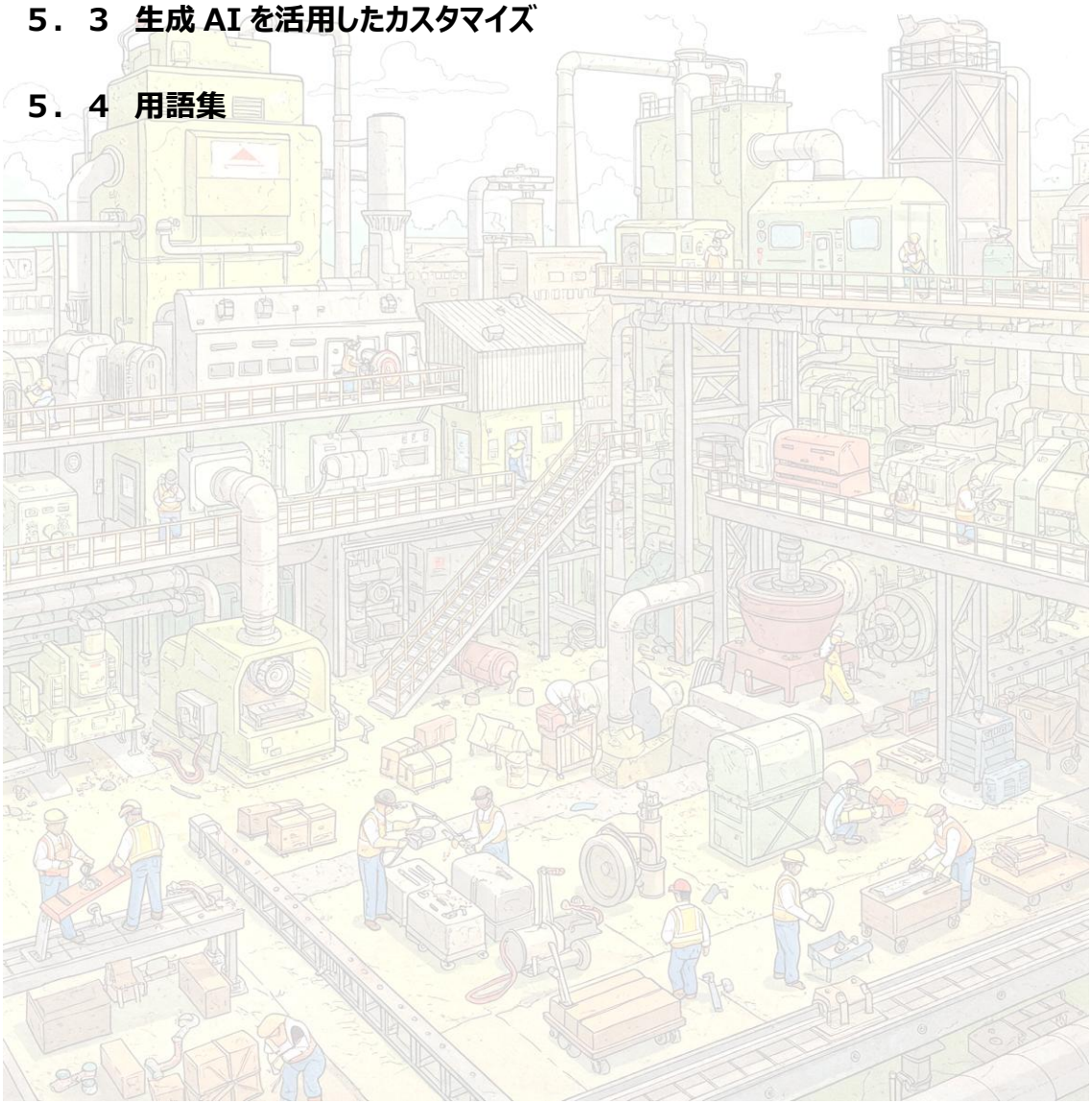
５．　付録

５．１　サイバーBCP ひな形

５．２　カスタマイズ要件定義

５．３　生成 AI を活用したカスタマイズ

５．４　用語集



工場セキュリティハンドブック・サイバー対応 IT-BCP 編

1．はじめに

これまで工場のセキュリティレベル向上を目的とした「リスクアセスメント編」および「リスク対策編」のハンドブックを公開してきました。これらのハンドブックは、中小の工場でも取り組めるリスクアセスメントを通じてリスクを把握し、情報セキュリティ対策の実行の指針を示すことで防御の備えを支援することを目的としています。しかし、防御の備えは重要ですが、万全の対策を行うことは困難であり、インシデントのリスクをゼロにすることはできません。インシデント発生時には、その影響を最小限に抑え、迅速な復旧を行うことが重要です。

本書は、**工場のサイバーインシデントに特化した IT 面での BCP（事業継続計画）策定**を支援するガイドブックです。特にサイバー攻撃の検知から被害に遭ったシステムの復旧までにフォーカスしています。なお、システム復旧と並行して、一般的な BCP に従って事業を継続することになります。

本書では、基本的なサイバー対応 IT-BCP（以下、サイバーBCP と略す）が自分たちの手で作成できるように、ひな形と生成 AI を活用したカスタマイズ方法もご用意しました。ぜひ、本書を有効に活用し、サイバーセキュリティインシデントに対するリスク軽減対策を進めてください。

1.1 サイバーBCP 策定にあたって

サイバー攻撃の代表的な例であるランサムウェアの感染を取り上げて、サイバーBCP 策定にどのような準備が必要かを整理します。

【ランサムウェア侵入から工場停止までの一般的な流れ】

- ●第 1 段階　ランサムウェアが何らかの方法で外部との接続口より工場内のネットワークに侵入する
- ●第 2 段階　ランサムウェアに感染した装置から他の装置へ徐々に感染が広がる
  （感染する装置は必ずしもパソコンやサーバだけとは限りません）
- ●第 3 段階　ランサムウェアが感染拡大と同時に情報の窃取（外部へ流出）と装置内のファイルの暗号化を始める
- ●第 4 段階　ファイルが暗号化された装置はファイルが読み込めず、正常な動作ができなくなる
- ●第 5 段階　工場内の装置が次々と停止し、最終的には工場の稼働が継続できなくなる

ランサムウェアが工場内の装置に侵入する経路は実はたくさんあります。また、意図的に狙われなくても感染してしまうケースもあります。上記の第 1 段階で被害を食い止めるためには、**リスクを把握し、必要な対策を行う**必要があります。しかし、残念ながら完全に侵入を阻止することはできません。その場合、第 2 、第 3 段階に至ります。この時点で工場内の異変に気が付き、**迅速に適切な行動**が取れれば、被害を最小限に留めることができる可能性があります。さらに、第 4 、第 5 段階に至ってしまったとしても、**復**

旧のための備えがあれば、長期間の稼働停止を免れることができます。

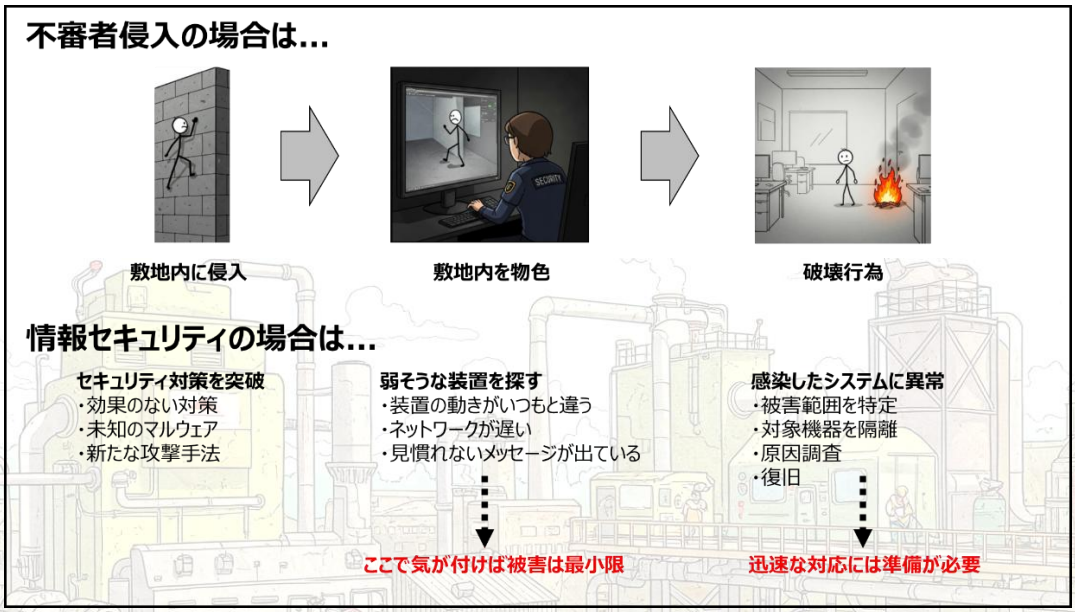


図 1-1 被害を最小限に抑えるために必要なこと

サイバー攻撃の被害を最小限に抑える、迅速に復旧させるためには、サイバーBCP が必要です。このサイバーBCP を策定する前に、下記に挙げた事項を確認してください。

- **リスクの把握と現在の対策の状況（何ができていて何ができていないか）**
- **情報セキュリティ被害に遭った際に対応できる知識やスキルの有無**
- **自力で対応できない場合は、調査や復旧に協力してもらえる外部協力者とのリレーションの構築**
- **工場の稼働が停止した場合の損失と許容できる停止期間**

これらが明確ではない場合は、有効なサイバーBCP の策定はできません。まずはこれらを整理することから始めて下さい。

1.2 サイバーBCP 策定の重要性

中小企業は大企業に比べて経営資源が限られているため、災害や緊急事態が発生した場合、事業の中断や廃業・倒産に追い込まれるリスクが高くなります。また、サイバーセキュリティインシデントは攻撃者により意図的に発生させることができる人災で、自社工場を含むサプライチェーン全体で考えると被害が大きくなる可能性があります。サプライチェーンの一部を担う中小の工場がサプライチェーンに対する攻撃の起点として狙われることも少なくありません。サイバーBCP を策定しておくことで、緊急事態が発生した際に迅速にシステムを復旧させる手順が明確になり、自社事業の中断とサプライチェーン全体への影響を最小限に抑えることができます。

サイバーBCP を策定し公表することにより顧客や取引先からの信頼を獲得し、企業の危機管理能力を示すことができます。また、サイバーBCP 策定後に、これに基づく緊急時対応訓練を実施して、その実

効性と従来の BCP との整合性を確認し、サイバーBCP を見直すことなども重要です。

1.3 サイバーBCP とこれまでの BCP の関係

これまで IT システム全般の BCP に取り組んできた企業にとっても、サービス継続のためにどのようにサイバーセキュリティインシデントへ備えるかが重要な課題となっています。本書ではサイバーセキュリティに特化した対策や運用を基礎としたシステム復旧計画をサイバーBCP と定義しています。

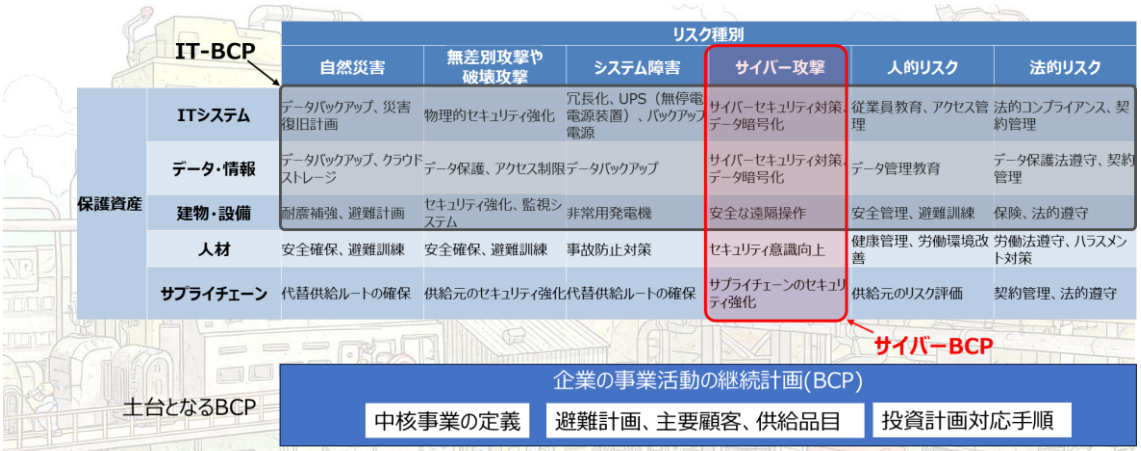


図 1-2 IT-BCP とサイバーBCP のカバー範囲

参考　IT-BCP とサイバーBCP の異なるポイントとは

サイバー攻撃は、人為的であり、攻撃者の意図や手法が多様で予想が難しく、事前準備と迅速な初動対応が被害低減に大きく寄与します。サイバーBCP では、リスクの特性に応じた対策と迅速なインシデント対応、個々の攻撃に応じた再発防止策の実施がポイントになります。

	IT-BCP	サイバーBCP
リスクの特性	自然災害やハードウェアの故障など、比較的予測可能なリスクに対する対策が中心です。これらのリスクは発生頻度や影響範囲がある程度予測可能です。	サイバー攻撃は人為的であり、攻撃者の意図や手法が多様で予測が難しいです。攻撃の種類や手法が日々進化しているため、**常に最新の情報を取り入れた対策が必要**です。
迅速性と初動対応	自然災害や停電などの場合、発生が確認され次第、計画に基づいて対応を開始します。初動対応のスピードも重要ですが、サイバー攻撃ほどの即時対応は求められないことが多いです。	サイバー攻撃は**迅速な初動対応**が求められます。攻撃が発生してからの対応が遅れると、被害が拡大し、復旧が困難になる可能性が高いです。**インシデント対応チーム（CSIRT）の設置や迅速な対応手順**が重要です。
復旧と再発防止	自然災害やハードウェア故障の場合、システムの物理的な復旧やデータの復元が主な対応となります。再発防止策も重要ですが、サイバー攻撃ほど複雑ではないことが多いです。	サイバー攻撃後の復旧には、システムの復旧だけでなく、**攻撃の原因特定と再発防止策の実施**が必要です。攻撃者が再度侵入しないように、セキュリティ対策の強化やシステムの見直しが求められます。

図 1-3 IT-BCP とサイバーBCP の相違点

2　情報セキュリティ脅威

サイバーセキュリティを含む情報セキュリティ上の「脅威」にはそれを引き起こす者がいます。悪意を持って意図的に攻撃（意図的脅威）をする者や、悪意がなかったとしても操作ミス等で偶発的に被害が発生（偶発的脅威）してしまう場合もあります。

悪意を持って攻撃をする者は、金銭目的や恨みや不満を晴らす目的を持っています。そのために、インターネットを通じて、ウイルスを送りつけたり、企業のサーバやシステムに不正アクセスを行ったりします。その他、政治目的やいたずらなどで同じような行為をする者もいます。これにより、工場のサーバやシステムが停止したり、ホームページが改ざんされたり、重要情報が盗みとられたりするのです。

ここでは、このようなサイバーインシデントに係る「意図的脅威」を中心に解説します。

2.1 主な意図的脅威

脅威の種類	攻撃手段・経路	具体的な被害例
マルウェア	不正なウェブサイト、メールの添付ファイル、USBメモリなどから感染し、コンピュータを乗っ取り、個人情報や機密情報を盗み出す、他のコンピュータに感染を広げるなど。	ファイルの暗号化によるデータの利用不能（ランサムウェア）、図面や生産レシピなどの機密情報や個人情報の窃盗、他のコンピュータへの攻撃の踏み台にされる。
フィッシング	偽のウェブサイトやメールで、IDやパスワードなどの個人情報を騙し取る。	工場システムへの不正ログインによる工場システムの情報窃盗、情報改ざん、システム停止など
サービス停止	複数のコンピュータから同時多量にアクセスし、サーバーをダウンさせる。	ウェブサイトへのアクセス不能、オンラインサービスの利用不可、ビジネスへの影響（売上減少など）
システム侵入	Webアプリケーションの脆弱性を悪用し、データベースに不正な命令を実行させる（SQLインジェクション）など。	データベース内の情報の改ざん、削除、個人情報漏洩、システムの乗っ取り
ゼロデイ攻撃	まだパッチが提供されていないソフトウェアの脆弱性を悪用する。	新しいタイプのマルウェアの拡散、システムの乗っ取り、データの窃盗
ソーシャルエンジニアリング	言葉巧みに騙し、情報を聞き出したり、行動を誘導する。建屋への不正侵入などもある。	パスワードの聞き出し、機密情報窃盗、システム破壊

図 2-1 主な意図的脅威

2.2 脅威の入口

本ハンドブックシリーズでは、上記のような脅威が生産現場（工場）に入り込む入口を下記の 13 個と定義しています。過去のサイバーセキュリティインシデント事例（2.3 項参照）を見ても、その原因の多くは、この 13 個の入口に合致します。

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	WiFi（無線AP）	WiFI通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワークからマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

図 2-2 脅威の入口一覧

2.3 過去のサイバーセキュリティインシデント事例

［事例１］“USB メモリー”からのマルウェア感染、それによる工場の稼働停止

攻撃者は、取引先を装って、悪意のある細工を施した USB メモリーを攻撃先対象企業に郵送。受け取った人が、その USB メモリーをパソコンに接続するとマルウェアに感染。USB メモリーは、非常に巧妙に細工されており、パソコンに接続するだけで被害に遭ってしまう。細工された USB メモリーをパソコンに接続するだけで、悪意あるプログラムをパソコン上で実行させるといった手口です。

悪意あるプログラムが実行されると、攻撃者が管理する外部のサーバからマルウェアをダウンロードして実行します。マルウェアは攻撃者のサーバと通信するなど、攻撃者の意のままに動作させることができます。攻撃者は攻撃対象の工場内ネットワークを動き回って各種システムの管理者権限を奪取したり、更に様々なツールをダウンロードして、工場システムの稼働を思うがままに停止させることが可能となりました。

［事例 2］“保守用ネットワーク”からの悪意ある侵入、それによる工場の稼働停止

工場内ネットワークと社外のシステムを接続するリモート接続機器に脆弱性があり、攻撃者はそのリモート接続機器の脆弱性を悪用し工場内ネットワークに侵入。これにより、工場内のサーバやパソコン端末へ攻撃を受けた痕跡があったと報道されています。

このサイバー攻撃は、システムへのアクセス制限をかけて身代金を要求する「ランサムウェア」によるもので、サーバやパソコン端末の一部でデータが暗号化されたとされています。これにより、工場の受発注システムなどが停止し、部品などの生産ができなくなり、工場の復旧には数日を要しました。

3．サイバーBCP 策定の基本

サイバーBCP を策定する上で基本となる考え方を示します。

3.1 サイバーBCP 策定の目的

サイバーBCP の策定は、中小製造業がサイバー攻撃に直面した際に、被害を最小限に抑え、迅速かつ効果的にシステムを復旧させるために不可欠です。具体的な目的としては以下のような点が挙げられます

◇リスク軽減

サイバーリスクを事前に評価し、適切な対策を講じることで、攻撃の影響を最小限に抑える。

◇迅速な対応

サイバー攻撃を受けた際、被害を最小限に抑えるための行動を予め計画し、迅速で適切な対応がとれるようにする。

◇法令遵守と信頼性の確保

個人情報保護や情報セキュリティに関する法令遵守を徹底し、企業の信頼性を高める。

◇従業員の意識向上

従業員に対してサイバーリスクの重要性を理解させ、緊急時に適切な対応ができるようにする。

3.2 サイバーBCP 策定のプロセス

サイバーBCP を策定する際のプロセスは以下の６つのステップに分けられます

①事前対策を実施する

・リスクアセスメント

一般的には、自社の情報資産やシステムに対する脅威を評価し、どのようなリスクが存在するのかを明確にすることです。詳しくは、別冊「工場セキュリティハンドブック・リスクアセスメント編」を参考にして下さい。

https://www.jnsa.org/result/west/2022/index.html

・リスク対策

リスクアセスメントで特定された脅威に対して、予防策や対応策を講じることです。詳しくは、別冊「工場セキュリティハンドブック・リスク対策編」を参考にして下さい。

https://www.jnsa.org/result/west/2023/index.html

②基本方針を決める

サイバーBCP は既存の BCP（事業継続計画）と整合性を持たせることが重要です。これにより全社的なリスク管理体制が一貫性を持ち、効果的な対応が可能となります。

例えば、大規模な自然災害を除く工場の再稼働目標時間を４８時間以内と定めている場合、

サイバー攻撃によって被害を受けた工場システムの復旧も４８時間以内を目標とする必要があります。

③判断基準を決める

事前にリスク対策を行っていても、サイバー攻撃の影響を受ける可能性は残ります。現在起きている事象（例えば、事務室で使用しているパソコンの画面表示がおかしい、動作が停止したなど）の原因がサイバー攻撃である場合、放置すれば短時間の内に工場全体に被害が広がる可能性があります。従って単純な故障や不具合なのか、サイバー攻撃の影響なのかを見極める方法や基準（トリアージ基準）を決めておくことが重要です。

例えば、数台のパソコンで同時に不調が発生した場合などは、内部でウイルスが拡散している可能性を考慮してサイバー攻撃を受けていると判断するなどです。

④運用体制を決める

緊急時における対応体制を決定します。例えば、意思決定者、対応チームの編成、役割分担、協力ベンダー、緊急連絡先リストなどです。

参考　サイバーインシデント緊急対応企業一覧

JNSA 所属企業の中で緊急対応が可能な企業を一覧にしたものを示します。ただし、事が起こってからではなく、どのような対応が可能なのか、前提条件や費用についても事前に確認をしておくことをお勧めします。 https://www.jnsa.org/emergency_response/

⑤緊急時対応の流れを決める

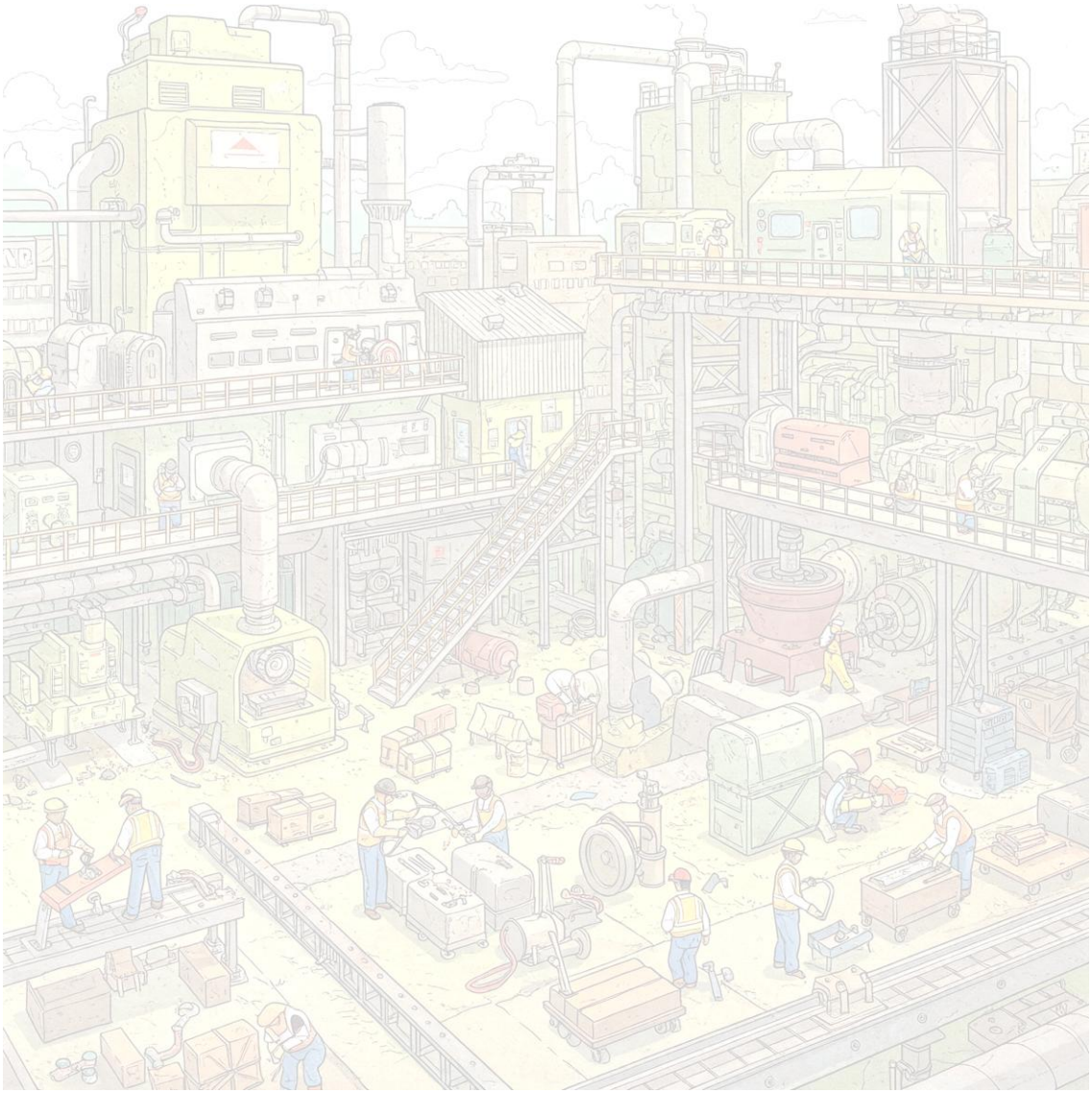
サイバー攻撃によるシステム障害が発生した際の具体的な対応手順を策定します。例えば、初動対応、被害拡大防止、システム復旧、情報共有などです。特にシステム復旧は自然災害におけるシステム障害からの復旧と異なる点が多くあります。

	自然災害	サイバー攻撃
初動対応	・安全確認：従業員の安全を最優先し、避難を指示 ・物理的被害の評価：建物や設備の損傷状況を確認	・インシデントの特定：サイバー攻撃の種類を特定し、影響範囲を把握 ・システムの隔離：影響を受けたシステムをネットワークから切り離す
復旧手段	・修理・復旧作業：損傷した設備やインフラの修理 ・外部業者の手配：建設業者や専門業者による復旧作業	・データ復元：バックアップからデータを復元 ・セキュリティ強化：攻撃を受けた原因を分析し、再発防止策を講じる
フォロー	・代替資材の確保：自然災害で影響を受けた資材の調達計画を策定	・情報伝達：従業員やステークホルダーに対して状況を説明し、透明性を確保
業務再開	・段階的な業務再開：安全が確認された後、徐々に生産を再開	・システムチェック：復旧後、システムの安全性を確認してから業務を再開
レビューと改善	・災害後の教訓：自然災害に対する耐性を高めるための改善点を洗い出し、BCPを見直す	・インシデント後の評価：攻撃の影響を評価し、サイバーセキュリティ対策を強化。BCPの見直しを行う

図 3-1　自然災害とサイバー攻撃における対応の違い

⑥訓練とブラッシュアップ

定期的にインシデント対応訓練を実施し、実際の緊急時に迅速かつ適切に対応できるようにします。また、訓練結果や実際のインシデント対応を通じて、従来の BCP との整合性も確認し、サイバーBCP を継続的に改善していきます。



4．サイバーBCP のひな形とカスタマイズ

付録 5.1 に記載した「サイバーBCP ひな形」の活用方法について解説します。中小製造業の皆様が、自社の状況に合わせて適切にサイバーBCP を策定できるよう、ひな形の活用方法とカスタマイズの手順を説明します。

4.1 サイバーBCP ひな形の活用

付録 5.1 に記載されている「サイバーBCP ひな形」は、中小製造業向けに作成された汎用的なテンプレートです。このひな形は、サイバーセキュリティインシデントに特化した BCP の基本的な構造と内容を提供しています。

●ひな形の主な特徴：

・中小製造業の一般的な環境を想定
・サイバーセキュリティインシデントへの対応に焦点
・簡潔で理解しやすい構成
・カスタマイズが容易な形式

4.2 カスタマイズのための要件定義

ひな形を自社の状況に合わせてカスタマイズするために、付録 5.2「カスタマイズ要件定義」の質問事項に対して回答を検討します。

4.3 ひな形のカスタマイズ方法

ひな形のカスタマイズには、以下の 2 つの方法があります。状況に応じて適切な方法を選択してください。

① 人手によるカスタマイズ

・5.2 で定義した要件に基づき、ひな形内の「＃No＃」部分をそれぞれ適切な内容に置き換えます。
・「＃No＃」の付いていない項目については、必要に応じて書き加えます。
・項目の追加や削除、文言の修正を行います。
・ひな形とカスタマイズ要件定義は JNSA のホームページからダウンロードできます。

② 生成 AI 活用によるカスタマイズ

・5.3 「生成 AI 活用方法」に従って、ひな形とカスタマイズ要件定義から自社向けにカスタマイズされた文書を生成 AI によって生成します。詳細は付録 5.3 を参照して下さい。
・生成された文書は必ず人が確認し、必要に応じて修正を加えます。
・生成 AI を活用するためのツールは JNSA のホームページからダウンロードできます。

注意点：生成 AI を使用する際は、セキュリティとプライバシーに十分注意を払い、機密情報の取り扱いには細心の注意を払ってください。

4.4 カスタマイズ後の確認と改善

カスタマイズしたサイバーBCP は、以下の観点から確認と改善を行ってください。

① 整合性チェック

各項目間の整合性を確認し、矛盾がないことを確認する。

② 実現可能性の検証

定義した対策や手順が、自社のリソースと能力で実行可能であることを確認する。

③ ステークホルダーレビュー

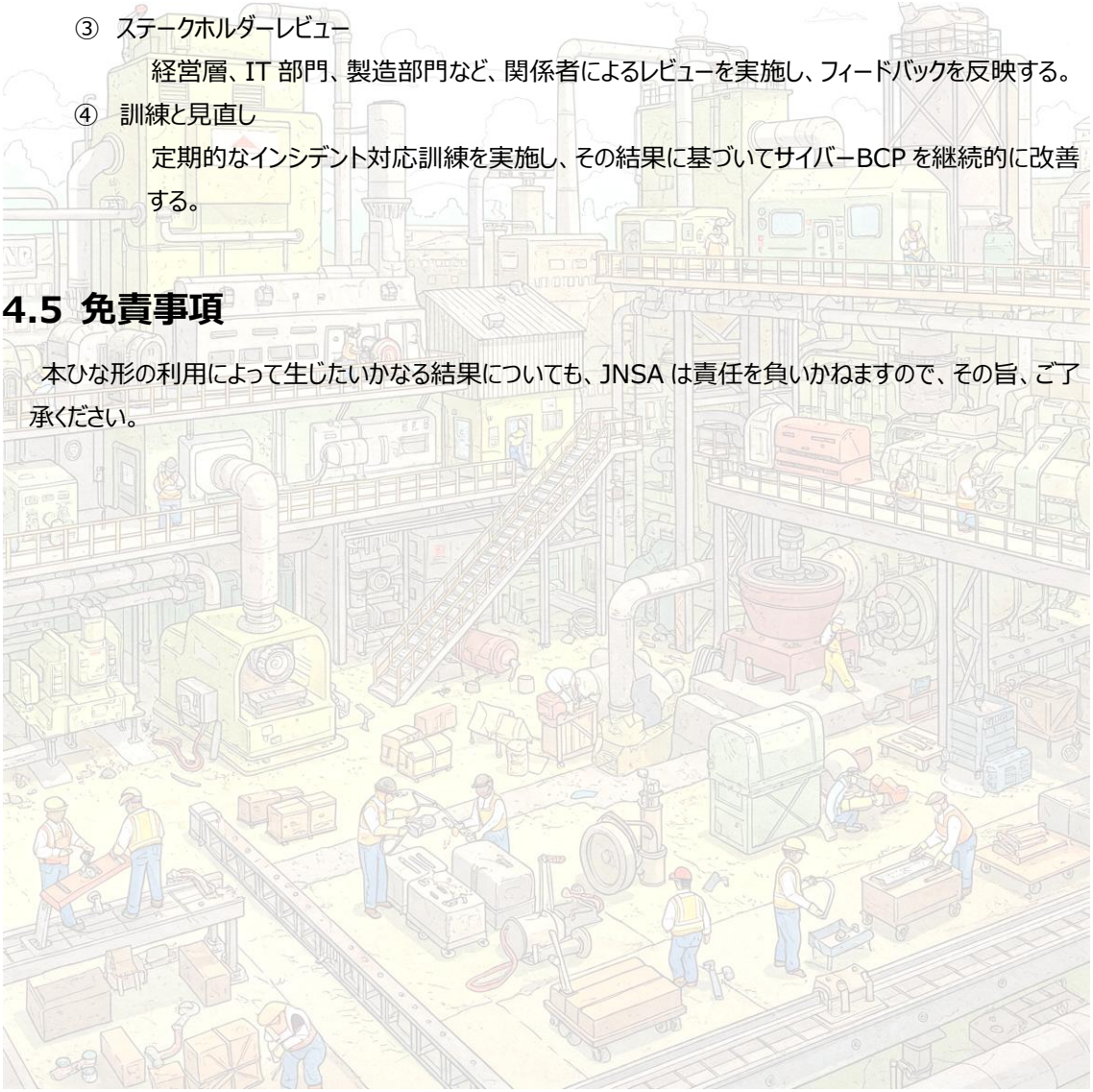
経営層、IT 部門、製造部門など、関係者によるレビューを実施し、フィードバックを反映する。

④ 訓練と見直し

定期的なインシデント対応訓練を実施し、その結果に基づいてサイバーBCP を継続的に改善する。

4.5 免責事項

本ひな形の利用によって生じたいかなる結果についても、JNSA は責任を負いかねますので、その旨、ご了承ください。



5. 付録

5. 1 サイバーBCP ひな形

中小製造業向けサイバー対応 IT-BCP サンプル Ver. 1.0

1. はじめに

当社の製造現場において、サイバー攻撃は深刻な事業リスクとなり、工場の停止は社外へも大きな影響を及ぼす。本サイバー対応 IT-BCP は、当社が既に実施しているリスクアセスメントに基づき、サイバー攻撃発生時の対応を定めることで、速やかに情報セキュリティ脅威に対処し、結果として事業継続性を高めることを目的とする。

2. 基本方針

サイバー攻撃による事業中断を最小限に抑え、迅速なシステム復旧を実現するため、以下の基本方針に基づき対策を実施する。

- ●統治：役割と責任を明確にし、緊急対応体制図を作成の上、組織的に対応する。
- ●特定：潜在するリスクとその影響範囲を特定する。
- ●防御：脅威の入口に対して必要な防御対策を行う。
- ●検知：異常な活動を早期に検知し、被害の拡大を防ぐ。
- ●対応：インシデント発生時には、サプライチェーンへの影響も考慮し、手順に従い迅速かつ適切な対応を行う。
- ●復旧：影響を受けたシステム・データを迅速に復旧し、業務が継続できる環境を維持する。
- ●改善：定期的な見直しと改善により、サイバー対応 IT-BCP の有効性を維持する。

3. サイバー攻撃発生時の対応フロー

3.1 発見・通報

①発見：異常なシステム動作、ネットワークの遅延、データの消失など、サイバーセキュリティインシデント発生を示す兆候を早期に発見できるよう、従業員への周知徹底を行う。

②通報：異常を発見した場合、速やかに#1#情報セキュリティ担当者＃1#または＃2#指定された窓口＃2#に報告する。

③判断：製造現場で生産に対する何らかの支障が発生した場合、その原因がサイバー攻撃であると判断するための基準は以下の通りとする。

- ・実施している情報セキュリティ対策からの異常を示すアラートがある場合
- ・ディスプレイ装置等に攻撃者からのメッセージなど不審な表示が出力された場合
- ・#4#工場内でアラートが発生し、＃4#製造装置やパソコンが同時に複数個所で異常な動作をする場合
- ・#5#工場内のネットワークトラフィック監視により#5#トラフィック量が通常時と比較して大幅に増大していることを確認した場合、もしくは輻輳状態で通信ができないか

大幅に遅延が発生する場合

・重要な情報やデータを保管するサーバのログにログイン失敗が大量に記録されている場合

④初期対応: ＃3#情報セキュリティ担当者＃3#は下記の初期対応を行う。

・攻撃が及んでいる範囲を特定し、被害拡大防止を講じる。

被害拡大防止策 ⇒ リスクアセスメントの結果、残存リスクが大きいと認識されている脅威の入口の使用停止や分離

・ログを収集するシステムがある場合は、証拠となるデータやログを改ざんされないように記憶媒体を切り離すかファイルを安全に取り出す。

保全対象：＃6#ログを収集しているシステム＃6#

・攻撃を受けたシステムをネットワークから隔離し、他のシステムへの感染拡大を防ぐ。

3.2 状況把握と報告

①状況把握: ＃3#情報セキュリティ担当者＃3#または外部の専門家が、サイバーセキュリティインシデントの詳細な状況と影響範囲を把握する。

目標：検知から＃7#２時間以内＃7#に概略の状況を把握

②関係者への報告: 経営層、関係部署、取引先など、必要な関係者に状況を報告する。

エスカレーションルート ⇒ ＃8#情報セキュリティ担当者 → ・・・・ → 取引先＃8#

エスカレーションルール ⇒ ＃9#１時間以内に＃9#最終エスカレーション先に報告する

③対策本部設置: 必要に応じて、インシデント対応対策本部を設置し、対応を円滑に進める。

対策本部責任者：＃10#製造部門担当役員＃10#

④公的機関

個人情報の漏えいが疑われる場合や脅迫を受けている場合などは、＃14#法務部門＃14#が然るべき公的機関の窓口に連絡をする。

3.3 原因究明と対策

①原因究明: サイバーセキュリティインシデントの原因（脅威の入口）を特定し、再発防止策を検討する。合わせて他の脅威の入口の対策も確認する。

②対策実施: 原因究明の結果に基づき、必要な対策を実施する。特にアクセス権限が悪用された場合は、利用されたアカウントのアクセス権限の無効化とその他の特権アカウントのパスワード変更を必ず実施する。

③システム復旧: システムのバックアップがある場合は、復旧担当部署もしくは外部の専門家の指示に従い、影響を受けたシステムをバックアップから復旧し、速やかに稼働を再開させる。バックアップがない、もしくはバックアップからの復旧が困難な場合はシステムの再構築が必要となるため、関連するシステム設計書などを事前に準備しておく。

3.4 事後対応

①記録作成: サイバーセキュリティインシデント発生から対応までの経緯を記録し、今後の教訓とする。

生成 AI で、「カスタマイズされた中小製造業向けサイバー対応 IT-BCP」と一緒に

「サイバーセキュリティサイバーインシデント対応チェックリスト」が作成されます。インシデント対応にあたり、こちらも活用ください。

②従業員教育：従業員に対するセキュリティ意識向上のための教育を実施する。

③関係者への報告：関係者にサイバーセキュリティインシデント対応の結果を報告する。

４．関係者と役割分担

・＃3#情報セキュリティ担当者＃3#：サイバーセキュリティインシデント発生時の初期対応、状況把握、関係者への連絡、対策本部運営などを中心に実施する。

・経営層：サイバーセキュリティインシデント発生時の意思決定、資源の配分、外部への連絡などを担当する。

・各部署責任者：自身が担当するシステムや業務への影響を把握し、＃3#情報セキュリティ担当者＃3#に協力する。

・外部専門家：必要に応じて、下記外部のセキュリティ専門家に支援を依頼する。

＃11#xx システム株式会社＃11#（電話番号：＃12#xxxxxx-xxxx＃12#）

５．コミュニケーション計画

①内部への連絡

・定期的な進捗報告は毎日＃13#情報セキュリティ担当者から経営層＃13#へ実施する。

・全社員への情報共有（メール、社内報など）を定期的に実施する。

②外部への連絡

・顧客への影響が大きい場合は、顧客への連絡と状況説明を実施する。

・＃14#法務部門＃14#と連携し、プレスリリースの作成・発表を検討する。

・個人情報の漏えいなど、法的な対応が必要な場合は、速やかに実施する。

６．定期的な見直しと改善

①定期的な見直し：本サイバー対応 IT-BCP を＃15#年１回＃15#見直し、最新の脅威や自社の状況に合わせて改訂する。

②教育の実施：従業員に対して、本サイバー対応 IT-BCP の内容やセキュリティに関する教育を＃16#年１回＃16６＃実施する。

③訓練の実施：定期的にサイバーセキュリティインシデント発生を想定した訓練（＃17#年１回＃17#）を実施し、対応能力の向上を図る。

7．法令遵守

①関連法令

自社の事業継続や顧客からの信頼確保のためにも、下記の関連法令を理解し、適切な対策を講じる。

・サイバーセキュリティ基本法

・個人情報保護法

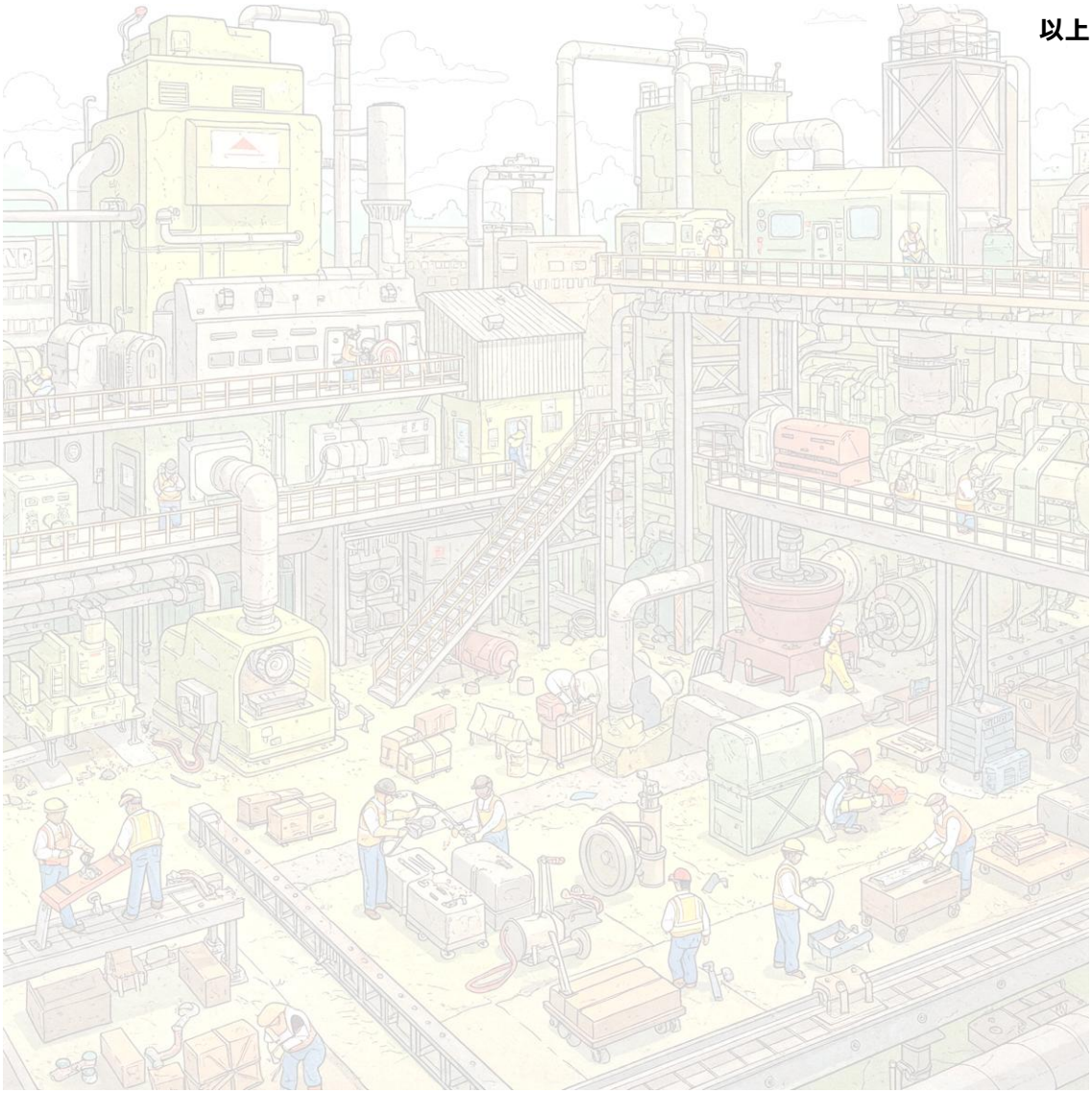
・不正アクセス禁止法

・製品安全基本法
・産業安全衛生法
・その他、関連する法規制

②内部監査

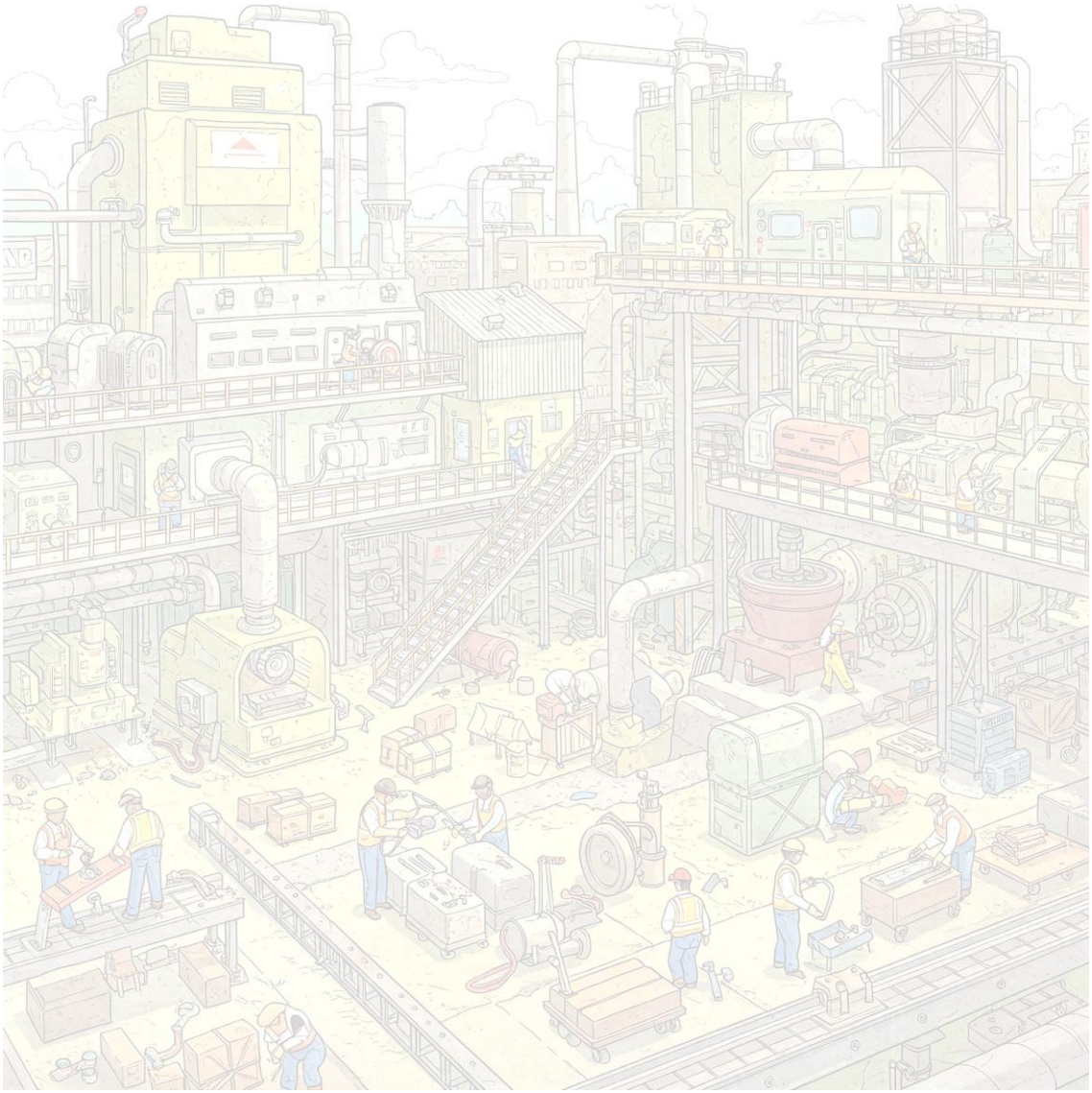
#18#年 1 回以上#18#の内部監査を実施し、法令遵守状況を確認する。
監査結果に基づき、改善策を実施する。

以上



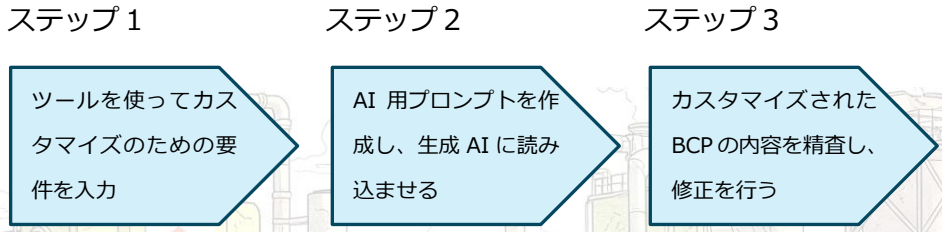
5.2 カスタマイズ要件定義

別紙 「カスタマイズ要件定義 Ver1.0.xlsx」を参照して下さい。



5.3 生成 AI を活用したカスタマイズ

生成 AI を使ってひな形 BCP を自社用にカスタマイズする方法を説明します。おおまかな手順としては次の 3 ステップです。



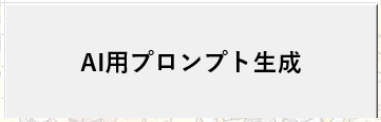
カスタマイズを支援するツールは JNSA のホームページからダウンロードして下さい。支援ツールは EXCEL 版と HTML 版の 2 種類があります。どちらのツールを使用しても、作成されるプロンプトは同じです。
※貴社のセキュリティ対策によっては、EXCEL 版が使用できない場合があります。

また、AI を使用する場合は、カスタマイズ要件定義の回答に担当者として**個人名などは入力しない**ようにして下さい。

【EXCEL 版】

① ダウンロードした「EXCEL 版カスタマイズツール.xlsm」ファイルを開き、F 列に自社の状況を入力します。（カスタマイズ要件定義と同じ内容です）

② Excel シートの下部にある「AI 用プロンプト生成」ボタンを押し、プロンプトファイルを保存するパス名とファイル名を入力します。（拡張子は.txt が自動的に付与されます）



※マクロの実行がブロックされた場合は、貴社のセキュリティルールに基づき対応をお願いします。

③ 生成されたプロンプトファイルをメモ帳などのテキストエディタで開きます。

④ 生成 AI（ChatGPT、Copilot、Gemini など）を起動し、質問内容に上記③の内容をすべてコピーしてペーストします。

⑤ 生成 AI を実行します。（出力が途中までになった場合は、「続きをお願いします」と入力する）

⑥ 出力された回答をすべてコピーし、テキストエディタや Word などにペーストします。

⑦ カスタマイズされた BCP を確認し、適切な内容となるように加筆・修正を行って下さい。

【HTML 版】

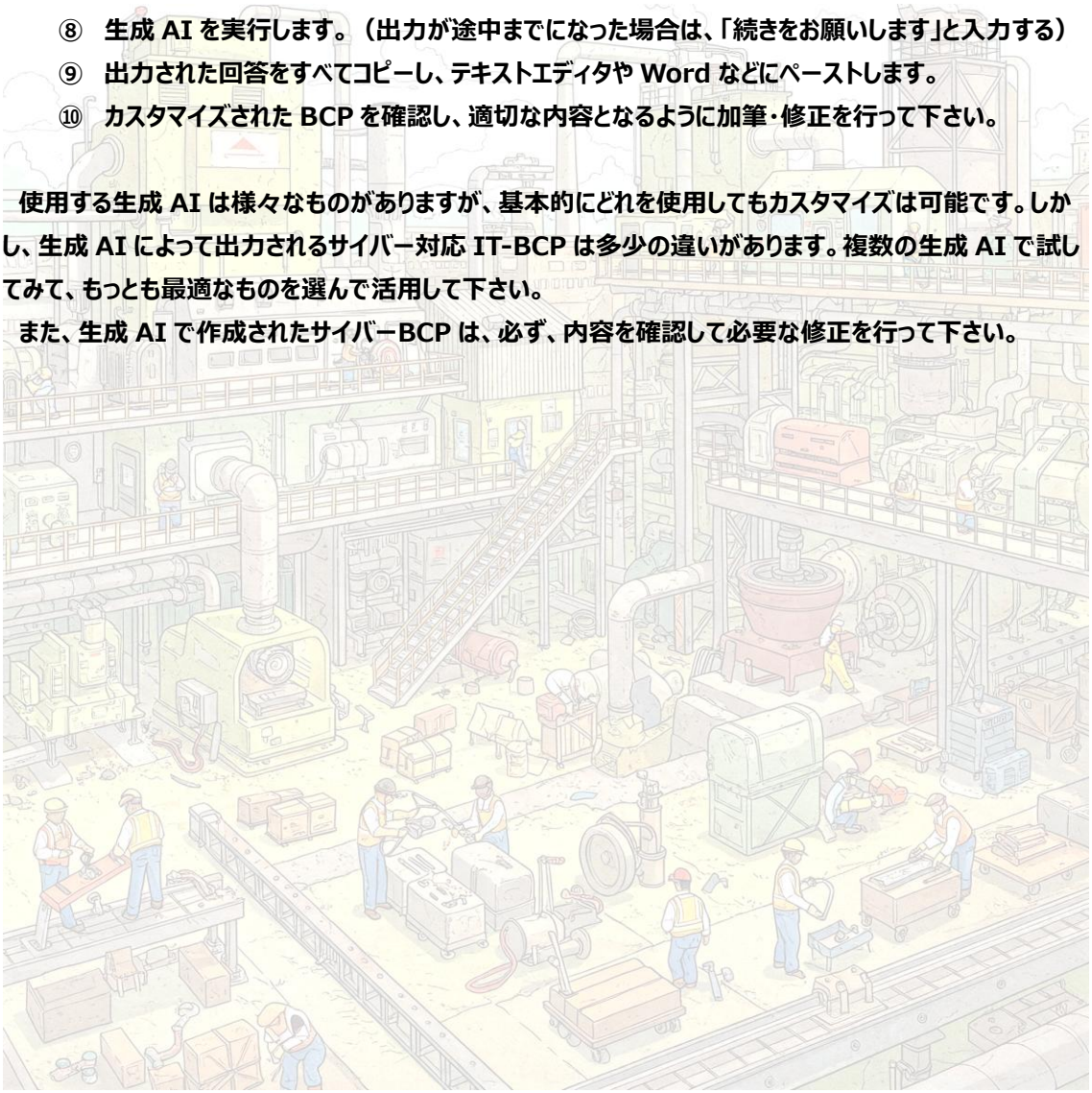
① ダウンロードした「HTML 版カスタマイズツール.zip」を解凍します。

② 「BCP_カスタマイズ.html」をダブルクリックし、表示される質問に対する回答を入力します。（カスタマイズ要件定義と同じ内容です）

③ 回答入力が終了したら、「回答を保存」ボタンを押します。
④ Download フォルダに「answer.txt」 がダウンロードされます。
⑤ 先に解凍したフォルダ内の「bcp_カスタマイズプロンプト.txt」をメモ帳などのテキストエディタで開き、内容をすべてコピーします。
⑥ 生成 AI（ChatGPT、Copilot、Gemini など）を起動し、先のコピー内容をペーストします。
⑦ 次に Download フォルダの「answer.txt」の内容を同様にコピーし、⑥の続きにペーストします。
⑧ 生成 AI を実行します。（出力が途中までになった場合は、「続きをお願いします」と入力する）
⑨ 出力された回答をすべてコピーし、テキストエディタや Word などにペーストします。
⑩ カスタマイズされた BCP を確認し、適切な内容となるように加筆・修正を行って下さい。

使用する生成 AI は様々なものがありますが、基本的にどれを使用してもカスタマイズは可能です。しかし、生成 AI によって出力されるサイバー対応 IT-BCP は多少の違いがあります。複数の生成 AI で試してみて、もっとも最適なものを選んで活用して下さい。

また、生成 AI で作成されたサイバーBCP は、必ず、内容を確認して必要な修正を行って下さい。



5.4 用語集

【サイバー攻撃】

コンピュータやネットワークシステムを標的とした攻撃行為の総称です。

【マルウェア】

コンピュータに侵入し、不正な動作を行う悪意のあるソフトウェアの総称です。ウイルス、ワーム、トロイの木馬などが代表的です。

【ランサムウェア】

マルウェアの一種で、コンピュータ内のデータを暗号化し、復号と引き換えに金銭を要求するものです。

【フィッシング】

偽のウェブサイトやメールなどで、個人情報やパスワードなどの情報を不正に入手しようとする攻撃手法です。

【標的型攻撃】

特定の組織や個人を標的に、高度な手法を用いて行われる攻撃です。

【脆弱性】

システムやソフトウェアに存在する欠陥で、攻撃者が不正に侵入するための経路となる可能性があります。

【パッチ】

ソフトウェアの脆弱性を修正するためのプログラムです。

【ファイアウォール】

ネットワークへの不正なアクセスを防止するためのセキュリティ対策機器です。

【IDS（侵入検知システム）】

ネットワークやシステムへの不正な侵入を検知するシステムです。

【IPS（侵入防止システム）】

侵入検知に加え、不正な通信を遮断する機能も備えたシステムです。

【BCP（事業継続計画）】

災害や事故など、予期せぬ事態が発生した場合でも、事業を継続するための計画です。

【サイバー対応 BCP】

IT システムに特化した BCP で、サイバー攻撃が発生した場合の対応を具体的に定めた計画です。

【リスクアセスメント】

発生する可能性のあるリスクを特定し、その影響度を評価するプロセスです。

【サイバーセキュリティインシデント】

サイバー攻撃によってセキュリティに関する問題が発生した事象を指します。

【インシデント対応】

インシデント発生時に、被害の拡大を防ぎ、復旧を行うための活動です。

WG メンバー（カッコ内は 2025 年 3 月末時点のものです）

秋山　健一（株式会社 NTT ファシリティーズ）
大財　健治（ケー・コンサルタント）
岡本　登　（WG リーダー／富士通株式会社）
金子　啓子（JNSA 西日本支部顧問）
河島　君知（株式会社 NTT データ先端技術）
木村　哲也（兼松エレクトロニクス株式会社）
小柴　宏記（ジーブレイン株式会社）
近藤　伸明（株式会社神戸デジタル・ラボ）
塩田　廣美（協力者）
嶋倉　文裕（富士通株式会社）
芹川　正孝（オムロンソフトウェア株式会社）
田中　駿悟（フューチャー株式会社）
谷川　貴幸（フューチャー株式会社）
西川　和予（プライムコンサルティング）
西本　敦司（アイネット・システムズ株式会社）
藤田　和弘（龍谷大学教授）
古川　佳和（大阪商工会議所）
松谷　和博（株式会社ソリトンシステムズ）
元持　哲郎（アイネット・システムズ株式会社）
安井　康二（株式会社サイバーディフェンス研究所）
米澤　美奈（西日本支部長／株式会社ソリトンシステムズ）

敬称略･五十音順