**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。**

**付録「サイバーセキュリティインシデント対応チェックリスト」を活用する。**

**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