【付録】B.インシデント対応フロー

以下の標準的なインシデント対応フローを参考に自組織における役割分担の想定、対応詳細方法について整理しましょう。

プロセス	対応のポイント
検知/連絡受付	**◆保守作業等における異常検知** ・外部ベンダーの定期保守等において、あらかじめ定めた異常検知の基準をもとに異常がないかチェックする ・異常を検知した場合は記録する **◆インシデントまたはその可能性がある通報の受付** ・通報内容を確認する ＜検知、連絡受付時の記録事項例＞ ・検知日時/受付日時 ・発見者/通報者/連絡着 ・想定される事象の発生日時(分かる範囲で) ・当該事業の検知/発見日時、箇所 ・インシデント発生箇所(サーバー、ネットワーク機器、システム名称等) ・発生した事象の分類(情報漏えい、マルウェア感染、システムへの侵入等) ◇不審なメールを受信した場合は、不用意な操作は行わない（標的型メール攻撃の場合）
トリアージ	**◆通報内容に関する発生事象の事実確認** ・マルウェア感染の疑いがある場合は、感染有無の確認や感染状況の把握等を行う ・不正アクセスの疑いがある場合は、Webサイト改ざん、情報漏えい、不正アクセスの痕跡があるかの確認等を外部ベンダー等に依頼する ・通報内容に関係する組織等と連携し、インシデントか否かの評価に必要な情報を確認する(被害の有無、影響範囲・内容、事象が継続しているか 等) **◆インシデントか否かの検討・評価** 【インシデントであると判断した場合】 ・組織内外への連絡、報告、情報共有を行う ・インシデントが複数発生している場合は、緊急度、重大度に基づき優先順位付けを行う 【インシデントではないと判断した場合】 ・注意喚起が必要と考えられる場合は、組織内外の関係者に情報を共有する ◇なりすまされた不審なメールを受信した場合は、なりすまされた本人へヒアリングを行う（標的型メール攻撃の場合） ◇ウィルス対策ソフトでスキャンする（標的型メール攻撃の場合） ◇メールサーバログの確認をベンダー等へ依頼する（標的型メール攻撃の場合）
インシデントレスポンス	**◆詳細状況の確認** ・対応策を検討するために、外部ベンダー等に調査を依頼し、状況を把握する ・状況把握の結果に基づき、外部ベンダー等と連携して対応方針を検討する **◆証拠（ログ等）の取得・保全** ・時間が経つと消えてしまう情報から順に、外部ベンダー等に証拠保全を依頼する **◆応急処置の実施** ・通報者に感染端末の隔離を依頼する　/ネットワークのフィルタリングや遮断を行う　/インシデントが発生した原因を解消する **◆復旧対応** ・システムやサービスの復旧を外部ベンダー等に依頼する /復旧した対象が正常に機能していることを確認する ◇被害を免れたバックアップの保護（ランサムウェアの場合） ◇暗号化されたファイルのバックアップからの復元（ランサムウェアの場合） ◇復号ツール有無の確認（ランサムウェアの場合）
報告/情報公開	◆組織内責任者への報告 ・必要に応じて、経営層に報告・情報共有する ◆関係組織への連絡 ・インシデント内容、対象システム、業務への影響、報道有無及び報道内容等を連絡する ◆外部機関への通報・相談 ・個人情報漏えい等の被害が発生した場合は、個人情報の本人、取引先等への通知、所管官庁・個人情報保護委員会等への届出、Webページ等での公表を検討する ・サイバー攻撃と判断した場合は、情報処理推進機構（IPA）、JPCERT/CC等に相談する ・警察に届出（発見者に確認した事項の報告や証拠書類の提出等）を行う ◆広報発表等の対外対応 ・広報部門に、対外発表に必要な情報を提供する ◇身代金の支払いや攻撃者との交渉は実施しない（ランサムウェアの場合）

各対応は順序性があるわけではありません。特にトリアージ以降の対応は、プロセス内で状況に応じた対応の優先順位付けが必要です。

【出典】JPCERT/CC：「インシデントハンドリングマニュアル」https://www.jpcert.or.jp/csirt_material/operation_phase.html