組織対応力ベンチマークチェックシート（詳細版）

実施日
評価者

Ver.1.0

No	内容	評価欄	
3.1. 文書類の整備状況			
①	マネジメント層の責任表明を含む「インシデント対応ポリシー」を策定し、組織全体に周知徹底していますか？		
1-1-1	□ マネジメント層の責任表明。（1-1-1）		
1-1-2	□ ポリシーの目的と目標。（1-1-2）		
1-1-3	□ ポリシーの範囲。（1-1-3）		
1-1-4	□ インシデントの定義と、それらのインシデントが自組織にもたらす影響（1-1-4）		
1-1-5	□ インシデント対応チームの組織構造と、役割、責任、権限レベルを表す記述。（1-1-5）		
1-1-6	□ インシデントの優先順位付けまたは重大さの格付け。（1-1-6）		
1-1-7	□ インシデント対応についての事後評価の方法。（1-1-7）		
1-1-8	□ 報告および連絡のための必要事項の明確化。（1-1-8）		
②	インシデント対応にかかわる組織の役割や目標を明記した「インシデント対応計画」を策定し、インシデント対応機能の確立を推進していますか？		
1-2-1	□ インシデント対応チームの役割。（1-2-1）		
1-2-2	□ 戦略および目標。（短期および長期の目標）（1-2-2）		
1-2-3	□ マネジメント層による承認。（1-2-3）		
1-2-4	□ インシデント対応への組織的な取り組みの内容。（1-2-4）		
1-2-5	□ インシデント対応チームによる他の職員への連絡方法。（1-2-5）		
1-2-6	□ インシデント対応機能を評価するためのチェックリスト。（1-2-		
1-2-7	□ インシデント対応機能を向上させるための手引き。（トレーニングの実施等）（1-2-7）		
1-2-8	□ インシデント対応計画をどのようにして組織全体に適合させるかの方法。（1-2-8）		
③	「インシデント対応ポリシー」と「インシデント対応計画」に基づき「インシデント対応手順」を策定し、標準となる対応手順を関係組織に周知徹底していますか？		
1-3-1	□ 各手順は、インシデント対応ポリシーとインシデント対応計画を踏まえている。（1-3-1）		
1-3-2	□ 特定の技術手順、手法が記載されている。（1-3-2）		
1-3-3	□ インシデント対応についてのガイドラインが記載されている。（1-		
1-3-4	□ チェックリストや確認のための様式が記述あるいは添付されている。（1-3-4）		
1-3-5	□ 組織の優先順位が反映された対応活動が記載されている。（1-3-		
1-3-6	□ テストを行い、正確さと有用性を検証した後、チームの全メンバーに配布されている。（1-3-6）		
④	インシデント関連の情報共有に関するポリシーと手順を策定し、組織外に向けた情報提供について関係組織に周知徹底していますか？		
1-4-1	□ 記載内容についてマネジメント層と合意している。（1-4-1）		
1-4-2	□ 記載内容について組織の広報部門と合意している。（1-4-2）		
1-4-3	□ 記載内容について組織の法務部門と合意している。（1-4-3）		
1-4-4	□ （マスコミ等の外部関係者とやりとりする際に使用する）組織の現行ポリシーと手順に従っている。（1-4-4）		
3.2. インシデント対応チームの構成			
①	インシデント対応チーム構成を検討する際に、適切なインシデント対応チームモデルを選択し、適切なスキルをもった人材要員を検討していますか？		
2-1-1	□ 組織の現状を踏まえたうえで、インシデント対応チームの組織体制を決定していること。（2-1-1）		
2-1-2	□ 組織の要件や利用できるリソースに照らし、慎重に検討を行ったうえで、要員配置を行っている。（2-1-2）		
2-1-3	□ チームリーダーは、インシデント対応における組織内外との調整能力、コミュニケーション能力を有する。（2-1-3）		
2-1-4	□ チームメンバーは、システム管理、ネットワーク管理、プログラミング、技術サポート、セキュリティ管理、いずれかのスキルを有する。（2-1-4）		
2-1-5	□ 各メンバーのスキルを総合し、チーム全体として上記スキルを網羅している。（2-1-5）		
2-1-6	□ 各メンバーは、スキルの向上や獲得、最新の知識習得のための教育研究を行っている。（2-1-6）		
2-1-7	□ チームワークを尊重できる要員であること。（2-1-7）		
2-1-8	□ チーム内だけでなく、組織内の他のグループや外部組織とも円滑なコミュニケーションを図ることができる。（2-1-8）		
②	インシデント対応に参加してもらう必要がある、組織内の他のグループが明確になっていますか？		

2-2-1	□ 参加を依頼する組織の役割が明確になっている。（2-2-1）		
2-2-2	□ 上記組織には、マネジメント層、情報セキュリティ部門、ITサポート部門、法務部門、広報部門、設備管理部門が含まれる。（2-2-2）		
③	インシデント対応チームが担う、インシデント対応以外の役割を明確にしていますか？		
2-3-1	□ インシデント対応チームがインシデント対応以外に行う業務や役割が明確になっている。（2-3-1）		
2-3-2	□ インシデント対応以外で情報共有及び連携する組織内の他のグループや外部組織との協力関係が明確になっている。（2-3-2）		
3.3. インシデント対応の準備			
①	社内外からのインシデントに関する情報について、インシデント対応担当者への連絡手段および連絡するための設備が準備されていますか？		
3-1-1	□ インシデント発生時の連絡先が明確である。（3-1-1）		
3-1-2	□ 社内のエスカレーションルートを整備している。（3-1-2）		
3-1-3	□ 社内及び社外からのインシデント報告窓口を用意している。（3-1-		
3-1-4	□ 携帯電話等、リモートでインシデント対応チームと連絡をとる手段を用意している。（3-1-4）		
3-1-5	□ チームのメンバー間、組織内、外部の関係者との間で情報伝達を行う場合に使用する暗号化ソフトウェアを準備している。（3-1-5）		
3-1-6	□ インシデント対応の中心となって組織内外の連絡・調整を行うための対応本部が常設されている。または、常設ではないが必要時に対応本部を確保する手順を策定している。（3-1-6）		
②	インシデント分析のためのハードウェアとソフトウェアが準備されていますか？		
3-2-1	□ 証拠物や機密物を安全に保管するための手段を用意している。（3-		
3-2-2	□ コンピュータフォレンジックワークステーションとバックアップ装置を用意している。（ディスクイメージ作成、ログファイル保存、その他データ保管用）（3-2-2）		
3-2-3	□ インシデント分析のためのPCを用意している。（3-2-3）		
3-2-4	□ 予備のワークステーション、サーバ、ネットワーク機器を用意している。（3-2-4）		
3-2-5	□ 未使用媒体を用意している。（証拠保全用のCD-R、DVD-R等）		
3-2-6	□ 簡単に持ち運びができるプリンターを用意している。（3-2-6）		
3-2-7	□ パケットスニッファとプロトコルアナライザを用意している。（3-		
3-2-8	□ コンピュータフォレンジックソフトウェアを用意している。（3-2-		
3-2-9	□ インシデント分析に利用するプログラム・ツール用のCD等を用意している。（3-2-9）		
3-2-10	□ 証拠収集アクセサリを用意している。（3-2-10）		
③	重要資産の一覧を準備する等、インシデント分析のための準備がされていますか？		
3-3-1	□ 一般に使用されるポートとトロイの木馬のポートリストを用意している。（3-3-1）		
3-3-2	□ OS、アプリケーション、プロトコル、侵入検知とアンチウイルスシグネチャなどのマニュアルを用意している。（3-3-2）		
3-3-3	□ ネットワーク図と重要な資産の一覧を用意している。（3-3-3）		
3-3-4	□ 予想されるネットワークの活動、システムの活動、アプリケーションの活動の基準を整備している。（3-3-4）		
3-3-5	□ インシデントの分析、検証、根絶を迅速に行うための、重要なファイルのハッシュリストを準備している。（3-3-5）		
④	インシデント鎮静化（対処・復旧）のためのソフトウェアが準備されていますか？		
3-4-1	□ OSのブートディスクやCD-ROM、OSの媒体、アプリケーションの媒体などを用意している。（3-4-1）		
3-4-2	□ OSやアプリケーションのセキュリティパッチを用意している。		
3-4-3	□ OS、アプリケーションおよびデータのバックアップイメージを用意している。（3-4-3）		
3.4. 予防			
①	システムとアプリケーションのリスク評価を定期的に行っていますか？		
4-1-1	□ 保護すべき情報資産を把握している。（4-1-1）		
4-1-2	□ 脅威と脆弱性の組み合わせから、どのようなリスクがあるかを判断している。（4-1-2）		
4-1-3	□ 明らかになったリスクへの対応方針を明確にしている。（4-1-3）		
②	パッチ管理ができていますか？		
4-2-1	□ 対象の分類分けができている。（4-2-1）		
4-2-2	□ 全ての対象に対して確実に実施している。（4-2-2）		
4-2-3	□ パッチ管理プログラムを使用し、システム管理者によるパッチの識別、取得、テスト、配布を支援している。（4-2-3）		

③	ホスト（クライアント端末／サーバ等）のセキュリティは適切に管理されていますか？		
4-3-1	□ 各端末に対し、適切にパッチが適用されるよう管理している。（4-		
4-3-2	□ 最低限のサービスが適切なユーザと端末だけに提供されるよう設定している。（4-3-2）		
4-3-3	□ 安全でないデフォルト設定(デフォルトのパスワード、安全でない共有など)を変更している。（4-3-3）		
4-3-4	□ セキュリティ対策が実施されたリソースにユーザがアクセスしようとした場合、警告バナーが表示されるようにしている。（4-3-4）		
4-3-5	□ 端末の監査が実施できるようになっており、重要なセキュリティ関連のイベントについてはログを取得している。（4-3-5）		
4-3-6	□ 管理者が端末のセキュリティ対策を首尾一貫して効果的に実施できるよう、オペレーティングシステム（以下、「OS」という）とアプリケーションの管理手順を用意している。（4-3-6）		
④	ネットワークセキュリティは適切に管理されていますか？		
4-4-1	□ ネットワークの境界では、明示的に許可されていないすべての活動を拒否するように設定している。（4-4-1）		
4-4-2	□ 組織が適切に機能するために必要な活動だけを許可している。（4-		
4-4-3	□ VPN (virtual private network)、ほかの組織への専用線接続といったすべての接続ポイントのセキュリティを高めている。（4-4-3）		
⑤	ウイルスなどの悪意のコードを予防する仕組みを導入していますか？		
4-5-1	□ ウイルス、ワーム、トロイの木馬などの悪意のコードを検知して阻止するソフトウェアを組織全体に配布している。（4-5-1）		
4-5-2	□ 悪意のコードの予防策を行っている。（4-5-2）		
⑥	トレーニングや訓練によって、ユーザのセキュリティ意識向上に努めていますか？		
4-6-1	□ ユーザに対し、ネットワーク、システム、アプリケーションの適正な利用に関するポリシーや手順について情報提供を行っている。（4-		
4-6-2	□ 過去の事件の教訓をユーザ間で共有し、自分たちの行動が組織にどのような影響を与えるかを認識させるようにしている。（4-6-2）		
4-6-3	□ 悪意のコードに関係する事件や、利用ポリシー違反に関係する事件を共有し、事件に関するユーザの意識向上に努めている。（4-6-3）		
4-6-4	□ 情報技術(IT)スタッフは、ネットワーク、システム、アプリケーションを組織のセキュリティ標準に従って維持できるように訓練を行っている。（4-6-4）		
3.5. 検知と分析			
①	IDSなどの攻撃を検知する仕組みがありますか？		
5-1-1	□ 組織内には、IDS/IPSやウイルス対策ソフトウェア、ファイル完全性チェックソフトウェア、もしくはパケットフルキャプチャ製品が導入されており、セキュリティインシデントを検知することができる。		
5-1-2	□ 新しい脆弱性とエクスプロイトに関する情報や他組織でのセキュリティインシデントに関する情報を定期的に収集している。（5-1-2）		
5-1-3	□ ポリシーに準拠し、主要なシステムに対してログ取得に関する基準が策定されている。（5-1-3）		
5-1-4	□ ポリシーに準拠し、主要なシステムで監査機能を有効にし、監査イベントを取得している（5-1-4）		
5-1-5	□ 主要なシステムにおいて、ログ取得が適切に機能していること、及びログ取得の基準に準拠していることを定期的に確認している。（5-		
5-1-6	□ 取得したログを保存する際は、ファイルの完全性チェックを行い、ログが改ざんされていないことを確認している。（5-1-6）		
②	ネットワークとシステムの使用率や、正常な動作を把握し、異常を検知できる仕組みがありますか？		
5-2-1	□ ネットワークの帯域使用率を監視している。（5-2-1）		
5-2-2	□ 各ホストのリソース使用率を監視している。（5-2-2）		
5-2-3	□ ネットワークや各ホストにおける、平均及びピーク時の使用率レベルを把握している。（5-2-3）		
5-2-4	□ ネットワークにおける、正常時の動作を把握している。（5-2-4）		
5-2-5	□ 各ホスト及びホスト上で稼動するアプリケーションおける、正常時の動作を把握している。（5-2-5）		
③	ポリシーに基づくログの取得と保管を実施するとともに、各イベントを相関分析する仕組みがありますか？		
5-3-1	□ 各システムで取得したログはログサーバに送信し、管理している。（5-3-1）		
5-3-2	□ ログの保持期間等を規定したログ保管ポリシーを策定し、準拠している。（5-3-2）		
5-3-3	□ 複数のシステムで検知したイベントの相関分析を実施している。		

5-3-4	□ すべてのシステムで時刻の同期ができている。（5-3-4）		
④	インシデント対応に必要な知識やスキルを向上し、攻撃検知の仕組みに反映していますか？		
5-4-1	□ インシデント対応に有用なナレッジ（セキュリティベンダーサイトの情報、過去のインシデント情報等）を二次利用し易い方法（Excel、データベース、専用ツール等）でまとめ、定期的に更新し		
5-4-2	□ 検出されたインシデントの分類や確認に係る方法を明文化した、チェックリストが整備されている。（5-4-2）		
5-4-3	□ インシデントが検出された時点から、最終的に解決されるまでのすべてのステップを記録し、タイムスタンプを付加している。（5-4-		
5-4-4	□ インシデントに係るデータは、許可された人間だけがアクセスできるように論理的かつ物理的に制限されている。（5-4-4）		
5-4-5	□ 影響のあるリソースの重要性やインシデントの技術的な影響に基づき、ビジネスインパクトごとに対処するインシデントの優先順位をつけている。（5-4-5）		
3.6. 封じ込め･根絶･復旧および事後活動			
①	インシデントを封じ込めるための手順や戦略･許容できるリスク定義は出来ていますか？		
6-1-1	□ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が成されている。（6-1-1）		
6-1-2	□ インシデント発生時の封じ込めのための具体的な対応手順／想定フローが作成されている。（6-1-2）		
6-1-3	□ インシデント発生時の封じ込めのための意思決定プロセスが明確になっている。（6-1-3）		
6-1-4	□ インシデント発生時の封じ込めのための許容できる範囲／レベルが明確になっている。（6-1-4）		
6-1-5	□ インシデント発生時の封じ込めのための許容できる範囲／レベルを既存のSLA（合意されたサービスレベル）等と照らし合わせて決定し、実態に即した封じ込めとして実効性がある。（6-1-5）		
②	証拠保全（証拠収集や処理）の方法について、文書で確立された手順に従って対応できますか？		
6-2-1	□ インシデントの種類（サービス不能攻撃・悪意のコード・不正アクセス・不適切な使用・複合要素）のいずれかまたは複数を想定して、検討が成されている。（6-2-1）		
6-2-2	□ 何を証拠とすべきかが明確になっている。（6-2-2）		
6-2-3	□ 証拠保全の方法について手順の作成等がされている。（6-2-3）		
6-2-4	□ 証拠保全の手順等の作成は、関係第三者機関（法執行機関等）や法務スタッフなどの組織内関係者との協議のもとで実施している。（6-		
③	不用意に変更･破壊することなく、揮発性データを証拠としてシステムから取得することができますか？また、フォレンジックに適した完全なディスクイメージ（単なるファイルシステムのバックアップではなく）を収集できますか？		
6-3-1	□ 保全すべき揮発性データを漏れなく迅速に収集できるように、収集過程がある程度自動化されている。（6-3-1）		
6-3-2	□ 揮発性データの証拠が不用意に変更や改ざんなどされないような媒体（再書き込み不可メディア：DVD、CD等）に保存できる。（6-3-		
6-3-3	□ ディスクイメージを保存する先として、未使用（ゼロクリア、初期化済み）のデバイスを準備する。（6-3-3）		
6-3-4	□ ディスクイメージ取得前に元のディスクイメージデータが不用意に改変されないように、再書き込み・上書き禁止などの配慮ができている。（6-3-4）		
6-3-5	□ 完全なディスクイメージを取得するツールやコマンドを問題なく使用できること。（6-3-5）		
④	インシデント対応のレビュープロセスが入っていますか？		
6-4-1	□ レビュープロセスが定義されている。（6-4-1）		
6-4-2	□ レビューするための適切なメンバーが選出されている。（6-4-2）		
6-4-3	□ レビュー責任者が明確である。（6-4-3）		
6-4-4	□ レビューメンバーにマネジメント層が含まれている。（6-4-4）		
6-4-5	□ レビューのルールが決められている（再発防止のためにも建設的なレビューに努めることなど）。（6-4-5）		

集計

3.1	文書類の整備状況	
3.2	インシデント対応チームの構成	
3.3	インシデント対応の準備	
3.4	予防	
3.5	検知と分析	
3.6	封じ込め･根絶･復旧および事後活動