組織対応力ベンチマークチェックシート

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？			
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？			
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？			
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？			
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	インシデント対応に参加してもらう必要がある、組織内のほかのグループが明確になっていますか？			
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？			
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？			
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	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？			
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. 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？			
②	パッチ管理ができていますか？			
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	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？			
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？			
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？			
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？			
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？			
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？			
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？			
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？			
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？			
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？			
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？			

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