EC-Council

ECIH™
EC-Council Certified Incident Handler

ECIH試験ブループリント v2

項目番号	ドメイン	サブドメイン	配点
1	**インシデント対応および処理プロセス**	1.1 情報セキュリティインシデント 1.2 インシデント管理 1.3 インシデント対応の自動化とオーケストレーション 1.4 インシデント対応基準とフレームワーク 1.5 インシデント対応に関する法律と規制 1.6 インシデント対応と処理プロセス a) 準備 b) インシデントの記録と割り当て c) インシデントの優先順位付け d) 通知 e) 封じ込め f) 証拠収集とフォレンジック分析 g) 根絶 h) 復旧 i) 事後対応活動	11
2	**最初の対応**	2.1 最初の対応者 2.2 犯罪現場の保全と記録 2.3 犯罪現場での証拠の収集 2.4 証拠の保存、梱包、および輸送	11

3	**マルウェア事案**	3.1 マルウェアインシデント対応準備 3.2 マルウェアインシデントの検出 3.3 マルウェアインシデントの封じ込めと根絶	11
		3.4 マルウェアインシデント後の復旧 3.5 マルウェアインシデント防止ガイドライン	
4	**メールセキュリティインシデント**	4.1 メールセキュリティインシデントの種類 4.2 メールセキュリティインシデントの対応準備 4.3 メールセキュリティインシデントの検出と封じ込め 4.4 メールセキュリティインシデントの根絶 4.5 メールセキュリティインシデント後の復旧 4.6 メールセキュリティインシデントに対するベストプラクティス	12
5	**ネットワークレベルでのインシデント**	5.1 ネットワークセキュリティインシデント対応の準備 5.2 ネットワークセキュリティインシデントの検出と検証 5.3 不正アクセスインシデントの対応 5.4 不適切な使用インシデントの対応 5.5 サービス拒否（DoS）攻撃の対応 5.6 無線ネットワークセキュリティインシデントの対応	12

6	**アプリケーションレベル障害**	6.1 ウェブアプリケーションセキュリティインシデント対応の準備 6.2 ウェブアプリケーションセキュリティインシデントの検出と分析 6.3 ウェブアプリケーションセキュリティインシデントの封じ込めと根絶 6.4 Webアプリケーションセキュリティインシデントからの復旧 6.5 ウェブアプリケーションのセキュリティ確保のためのベストプラクティス	11
7	**クラウドセキュリティインシデント**	7.1 クラウドインシデントの対応と復旧における課題	10
		7.2 クラウドセキュリティインシデントの対応 7.3 Azureセキュリティインシデントの対応 7.4 AWSセキュリティインシデントの対応 7.5 Google Cloudセキュリティインシデントの対応 7.6 クラウドセキュリティインシデントへの対応ベストプラクティス	
8	**内部脅威**	8.1 内部脅威の種類 8.2 内部脅威への対応準備手順 8.3 内部脅威の検出、封じ込め、および根絶 8.4 内部攻撃後の復旧 8.5 内部脅威に対するベストプラクティス	11

9	**エンドポイントセキュリティインシデント**	9.1 エンドポイントセキュリティインシデントの対応と復旧の必要性 9.2 エンドポイントセキュリティインシデント対応の準備 9.3 エンドポイントセキュリティインシデントの検出と検証 9.4 モバイルベースのセキュリティインシデントの対応 9.5 IoTベースのセキュリティインシデントの対応 9.6 OTベースのセキュリティインシデントの対応	11%