記入日 201X/YY/ZZ

JNSA全国横断サイバーセキュリティセミナー
セキュリティ対応組織と成熟度診断
補足資料

※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。

機能	役割		領域	インソース						アウトソース						備考
				0 インソースでの実装を検討したものの、結果として実施しないと判断した	1 実施できていない	2 運用が明文化されておらず、担当者が業務を実施できる	3 運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	4 運用が明文化されており、担当者と交代して他者が業務を実施できる	5 明文化された運用はCISOなど権限ある組織長に承認されている	0 アウトソースでの実装を検討したものの、結果として実施しないと判断した	1 結果や報告を確認できていない	2 サービス内容と得られる結果を理解できていない	3 サービス内容、得られる結果のいずれかが理解できていない	4 サービス内容と得られる結果を理解できているが、想定未満	5 サービス内容と得られる結果を理解でき、想定通り	
A. セキュリティ対応組織運営	A-1.	全体方針管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-2.	トリアージ基準管理	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-3.	アクション方針管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-4.	品質管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-5.	セキュリティ対応効果測定	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-6.	リソース管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
B. リアルタイムアナリシス（即時分析）	B-1.	リアルタイム基本分析	領域Ⅳ	◉	○	○	○	○	○	○	○	○	○	○	○	
	B-2.	リアルタイム高度分析	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	B-3.	トリアージ情報収集	領域Ⅳ	◉	○	○	○	○	○	○	○	○	○	○	○	
	B-4.	リアルタイム分析報告	領域Ⅳ	◉	○	○	○	○	○	○	○	○	○	○	○	
	B-5.	分析内容問合受付	領域Ⅳ	◉	○	○	○	○	○	○	○	○	○	○	○	
C. ディープアナリシス（深掘分析）	C-1.	ネットワークフォレンジック	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	C-2.	デジタルフォレンジック	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	C-3.	検体解析	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	C-4.	サイバーキルチェーン分析	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	C-5.	証拠保全	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
D. インシデント対応	D-1.	インシデント受付	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-2.	インシデント管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-3.	インシデント分析	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-4.	リモート対処	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-5.	オンサイト対処	領域Ⅲ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-6.	インシデント対応内部連携	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	D-7.	インシデント対応外部連携	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	