A-1　サービスインフラを作る（構築まで）

組織・機能			経営層		企画		指示 設計		調達（購買）		工作（構築）		構築管理/品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
Management(M) / Technology(T)			M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎										◎															
	RA	リスク評価	★				◎				◎		○		○	○	○													
	CP	緊急時対応計画	★				◎	◎			○	○			○	○											△		○	
設計・構築	IA	識別および認証					◎	◎			◎	○			○	◎														
	AC	アクセス制御					◎	◎			◎	○			○	◎														
	CM	構成管理					◎	◎			◎	◎			○	○														
	MP	メディアの保護					◎	◎			◎	○			○	○														
	PE	物理的および環境的な保護			△		◎	◎			◎	○																		
	PM	プログラム管理					◎	◎			◎	○																		
	SA	システムおよびサービスの調達					◎	◎	○																					
	SC	システムと通信の保護					◎	◎			◎	○			○	○														
	SI	システムおよび情報の完全性					◎	◎			◎	○			○	○														
	PS	人的セキュリティ			△		△				△																◎		○	
	CA	セキュリティ評価および運用認可	★				○	○			△	△			○	○	◎	◎												
	IP	個人参加の原則	★				△	△			△	△															◎			
	PA	プライバシーの承認	★		△		○	○			○	○			○	○											◎			
	AU	監査および責任追跡性	☆				△	△			△	△			○	○	◎	◎												
事後	IR	インシデント対応	★				◎	◎			◎	◎			○	○											△		○	
	MA	保守																												
	AT	意識向上およびトレーニング	★		△		△	○	△		△	○	△		○	◎	△										◎		△	

※NIST 800-53 rev5 draftの区分を採用

■ 簡単な定義：

◎ （実施主体として）主担当
○ （実施主体として）副担当、または兼務
△ （実施対象者側）関係者・関係部署
★ （理想的には）経営層から強い指示・承認を行なうこと。
☆ 経営層から指示・承認を行なうこと。
□ 主たる運営主体者・運営責任者

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

A-2　サービスインフラを作る（インフラ構築後の運用）

A-2 ⇒ “インフラ構築側” の視点

	組織		経営層		製造企画 製造開発		指示 → 設計		調達 （購買）		工作/運用		品質管理		IT部門		セキュリティ 監査部門		運用		保守		監視 モニタリング		PSIRT		人事、総務		法務、広報	
	Management(M) / Technology(T)		M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎										◎															
	RA	リスク評価	★				◎	◎			◎	○	○		○	○	○													
	CP	緊急時対応計画	★				◎	◎			○	○			○	○			△	△	△						△		○	
設計・構築	IA	識別および認証					◎	◎			◎	○			○	◎														
	AC	アクセス制御					◎	◎			◎	○			○	◎														
	CM	構成管理					○	○			○	○			○	○			◎	◎										
	MP	メディアの保護						○	△	△	△	△			○	○			◎	◎	○	○								
	PE	物理的および環境的な保護			△			○				○							◎	◎	○	○								
	PM	プログラム管理					◎	◎			◎	○							○	○	○	○								
	SA	システムおよびサービスの調達							◎			○							○	◎	○	○								
	SC	システムと通信の保護					○	○	○			○			○	○			◎	◎										
	SI	システムおよび情報の完全性					○	○			○	○			○	○			◎	◎	○	○								
	PS	人的セキュリティ			△		△				△								○		△						◎			
	CA	セキュリティ評価および運用認可	★				○	○			△	△			○	○	◎	◎		○		△							○	
	IP	個人参加の原則	★				△	△			△	△							○		△						◎			
	PA	プライバシーの承認	★		△		○	○			○	○			○	○			○		△						◎			
	AU	監査および責任追跡性	☆				△	△			△	△			○	○	◎	◎												
事後	IR	インシデント対応	★				○	○			○	○			○	○			◎	◎	○	○					△		○	
	MA	保守						△				△			○	○			○	○	◎	◎								
	AT	意識向上およびトレーニング	★		△		△	○	△		△	○	△		○	◎	△										◎		△	

※NIST 800-53 rev5 draftの区分を採用

■ 簡単な定義：

◎ （実施主体として）主担当
○ （実施主体として）副担当、または兼務
△ （実施対象者側）関係者・関係部署
★ （理想的には）経営層から強い指示・承認を行なうこと。
☆ 経営層から指示・承認を行なうこと。
□ 主たる運営主体者・運営責任者

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

B-1　サービスインフラを利用して製品を作る

B-1 ⇒ 設備・ラインの視点（インフラ活用側の視点）

	組織		経営層		製品企画/製品開発		指示 設計		調達（購買）		工作/運用		品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
	Management(M) / Technology(T)		M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎										◎															
	RA	リスク評価	★				◎	◎			◎	○			○	○	○													
	CP	緊急時対応計画	★				◎	◎			○	○			○	○			△	△	△						△		○	
設計・構築	IA	識別および認証					◎	◎			◎	○			○	◎														
	AC	アクセス制御					◎	◎			◎	○			○	◎														
	CM	構成管理					○	○			○	○			○	○			◎	◎										
	MP	メディアの保護						○	△	△	△	△			○	○			◎	◎	○	○								
	PE	物理的および環境的な保護			△			○				○							◎	◎	○	○								
	PM	プログラム管理					◎	◎			◎	○							○	○	○	○								
	SA	システムおよびサービスの調達							◎			○							○	◎	○	○								
	SC	システムと通信の保護					○	○	○			○			○	○			◎	◎										
	SI	システムおよび情報の完全性					○	○			○	○			○	○			◎	◎	○	○								
	PS	人的セキュリティ			△		△				△								○		△						◎			
	CA	セキュリティ評価および運用認可	★				○	○			△	△			○	○	◎	◎		○		△							○	
	IP	個人参加の原則	★				△	△			△	△							○		△						◎			
	PA	プライバシーの承認	★		△		○	○			○	○			○	○			○		△						◎			
	AU	監査および責任追跡性	☆				△	△			△	△			○	○	◎	◎												
事後	IR	インシデント対応	★				○	○			○	○			○	○			◎	◎	○	○					△		○	
	MA	保守						△				△			○	○			○	○	◎	◎								
	AT	意識向上およびトレーニング	★		△		△	○	△		△	○			○	◎	△										◎		△	

※NIST 800-53 rev5 draftの区分を採用

■ 簡単な定義：

◎ （実施主体として）主担当
○ （実施主体として）副担当、または兼務
△ （実施対象者側）関係者・関係部署
★ （理想的には）経営層から強い指示・承認を行なうこと。
☆ 経営層から指示・承認を行なうこと。
□ 主たる運営主体者・運営責任者

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

B-2　サービスインフラを利用して製品を作る

B-2 ⇒ "製品" の視点

	組織		経営層		製品企画/製品開発		指示 製品設計		調達（購買）		工作（構築）		品質管理		IT部門		セキュリティ監査部門		製造・包装（運用）		保守/修理/アフターケア		監視モニタリング		PSIRT		人事、総務		法務、広報	
	Management(M) / Technology(T)		M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎										◎															
	RA	リスク評価	★				◎	◎							○	○	○								△					
	CP	緊急時対応計画	★				◎	◎							○	○			○	○	△				○	△	△		○	
設計・構築	IA	識別および認証					◎	◎							○	◎														
	AC	アクセス制御					◎	◎							○	◎														
	CM	構成管理					○	○							○	○			◎	◎					○	△				
	MP	メディアの保護						○	△	△					○	○			◎	◎	○	○			○	△				
	PE	物理的および環境的な保護			△			○											◎	◎	○	○			○	△				
	PM	プログラム管理					◎	◎											○	○	○	○			○	△				
	SA	システムおよびサービスの調達							◎										○	◎	○	○			○	△				
	SC	システムと通信の保護					○	○	○						○	○			◎	◎					○	△				
	SI	システムおよび情報の完全性					○	○							○	○			◎	◎	○	○			○	△				
	PS	人的セキュリティ			△		△												○		△						◎			
	CA	セキュリティ評価および運用認可	★				○	○							○	○	◎	◎		○		△			△				○	
	IP	個人参加の原則	★				△	△											○		△				△		◎			
	PA	プライバシーの承認	★		△		○	○							○	○			○		△				△		◎			
	AU	監査および責任追跡性	☆				△	△							○	○	◎	◎							△					
事後	IR	インシデント対応	★				○	○							○	○			◎	◎	○	○					△		○	
	MA	保守						△							○	○			○	○	◎	◎								
	AT	意識向上およびトレーニング	★		△		△	○	△						○	◎	△										◎		△	

※NIST 800-53 rev5 draftの区分を採用

■ 簡単な定義：

◎ （実施主体として）主担当
○ （実施主体として）副担当、または兼務
△ （実施対象者側）関係者・関係部署
★ （理想的には）経営層から強い指示・承認を行なうこと。
☆ 経営層から指示・承認を行なうこと。
□ 主たる運営主体者・運営責任者

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.

C　サービスインフラおよび製品を利用して、サービスを提供する

	組織		経営層		製品企画/製品開発		指示 設計		調達（購買）		工作（構築）		品質管理		IT部門		セキュリティ監査部門		運用		保守		監視モニタリング		PSIRT		人事、総務		法務、広報	
	Management(M) / Technology(T)		M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T	M	T
計画	PL	計画作成	★		◎										◎															
	RA	リスク評価	★				◎	◎							○	○	○													
	CP	緊急時対応計画	★				◎	◎							○	○			△	△	△						△		○	
設計・構築	IA	識別および認証					◎	◎							○	◎														
	AC	アクセス制御					◎	◎							○	◎														
	CM	構成管理					○	○							○	○			◎	◎										
	MP	メディアの保護						○	△	△					○	○			◎	◎	○	○								
	PE	物理的および環境的な保護			△			○											◎	◎	○	○								
	PM	プログラム管理					◎	◎											○	○	○	○								
	SA	システムおよびサービスの調達							◎										○	◎	○	○								
	SC	システムと通信の保護					○	○	○						○	○			◎	◎			○	○						
	SI	システムおよび情報の完全性					○	○							○	○			◎	◎	○	○	○	○						
	PS	人的セキュリティ			△		△												○		△		○				◎			
	CA	セキュリティ評価および運用認可	★				○	○							○	○	◎	◎		○		△							○	
	IP	個人参加の原則	★				△	△											○		△						◎			
	PA	プライバシーの承認	★		△		○	○							○	○			○		△						◎			
	AU	監査および責任追跡性	☆				△	△							○	○	◎	◎												
事後	IR	インシデント対応	★				○	○							○	○			◎	◎	○	○	○	△			△		○	
	MA	保守						△							○	○			○	○	◎	◎								
	AT	意識向上およびトレーニング	★		△		△	○	△						○	◎	△						○				◎		△	

※NIST 800-53 rev5 draftの区分を採用

■ 簡単な定義：

◎ （実施主体として）主担当
○ （実施主体として）副担当、または兼務
△ （実施対象者側）関係者・関係部署
★ （理想的には）経営層から強い指示・承認を行なうこと。
☆ 経営層から指示・承認を行なうこと。
□ 主たる運営主体者・運営責任者

copyright© 産業横断サイバーセキュリティ人材育成検討会. all rights reserved.