

10 章 補足資料 (p.402)

表 10・18 スマートグリッドセキュリティ要求事項の論理インタフェースへの適用の例

セキュリティ要件グループ	セキュリティ要求事項	SG サイバーセキュリティ要件名	論理インタフェース分類における適用性																						
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
Access Control (SG.AC)	SG.AC-5	InformationFlow Enforcement																							
	SG.AC-6	Separation of Duties	Applies at moderate and high impact levels																						
	SG.AC-8	Unsuccessful Login Attempts	Applies at all impact levels																						
	SG.AC-10	Previous Logon Notification																							
	SG.AC-11	Concurrent Session Control																							
	SG.AC-12	Session Lock							H	H									L				L	H	
	SG.AC-13	Remote Session Termination																	M		M				
	SG.AC-14	Permitted Actions without Identification or Authentication	H	H	H	H	H	H	M	M	M	H				H	H	M	M	H	H		H	H	H
	SG.AC-16	Wireless Access Restrictions	Applies at all impact levels																						
	SG.AC-18	Use of External Information Control Systems	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																						
	SG.AC-19	Control System Access Restrictions	Applies at all impact levels																						
	SG.AC-20	Publicly Accessible Content	Applies at all impact levels																						
	SG.AC-21	Passwords	Applies at all impact levels																						
Awareness and Training (SG.AT)	SG.AT-5	Contact with Security Groups and Associations																							
	SG.AT-6	Security Responsibility Training	Applies at all impact levels																						
Audit and Accountability (SG.AU)	SG.AU-4	Audit Storage Capacity	Applies at all impact levels																						
	SG.AU-5	Response to Audit Processing Failures	Applies at all impact levels with additional requirement enhancements at high impact level																						
	SG.AU-7	Audit Reduction and Report Generation	Applies at moderate and high impact levels																						
	SG.AU-8	Time Stamps	Applies at all impact levels with additional requirement enhancements at moderate and high																						
	SG.AU-11	Conduct and Frequency of Audits	Applies at all impact levels																						
	SG.AU-12	Auditor Qualification	Applies at all impact levels																						
	SG.AU-13	Audit Tools	Applies at all impact levels																						
	SG.AU-14	Security Policy Compliance	Applies at all impact levels																						
	SG.AU-15	Audit Generation	Applies at all impact levels																						
	SG.AU-16	Non-Repudiation							M	M	M					H	H		M				H	H	H
Security Assessment and Authorization (SG.CA)	SG.CA-1	Security Assessment and Authorization Policy and Procedures	Applies at all impact levels																						
	SG.CA-2	Security Assessments	Applies at all impact levels																						
	SG.CA-3	Continuous Improvement	Applies at all impact levels																						
	SG.CA-5	Security Authorization to Operate	Applies at all impact levels																						
	SG.CA-6	Continuous Monitoring	Applies at all impact levels																						

セキュリティ要件グループ	セキュリティ要求事項	SG サイバーセキュリティ要件名	論理インタフェース分類における適用性																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Configuration Management (SG.CM)	SG.CM-7	Configuration for Least Functionality	Applies at all impact levels																					
	SG.CM-8	Component Inventory	Applies at all impact levels																					
	SG.CM-11	Configuration Management Plan	Applies at all impact levels																					
Continuity of Operations (SG.CP)	SG.CP-1	Continuity of Operations Policy and Procedures	Applies at all impact levels																					
	SG.CP-4	Continuity of Operations Training	Applies at all impact levels																					
	SG.CP-7	Alternate Storage Sites	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.CP-8	Alternate Telecommunication Services	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.CP-9	Alternate Control Center	Applies at moderate and high impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.CP-11	Fail-Safe Response	Applies at high impact levels																					
Identification and Authentication (SG.IA)	SG.IA-1	Identification and Authentication Policy and Procedures	Applies at all impact levels																					
	SG.IA-2	Identifier Management	Applies at all impact levels																					
	SG.IA-5	Device Identification and Authentication	H	H	H	H			M	M				M					H		H	H	H	H
	SG.IA-6	Authenticator Feedback	L	L	L	L	L	L	H	H	L	L				H	H	L	H	L	L		L	L
Information and Document Management (SG.ID)	SG.ID-1	Information and Document Management Policy and Procedures	Applies at all impact levels																					
	SG.ID-4	Information Exchange	Applies at all impact levels																					
	SG.ID-5	Automated Labeling																						
Incident Response (SG.IR)	SG.IR-1	Incident Response Policy and Procedures	Applies at all impact levels																					
	SG.IR-3	Incident Response Training	Applies at all impact levels																					
	SG.IR-4	Incident Response Testing and Exercises	Applies at all impact levels																					
	SG.IR-5	Incident Handling	Applies at all impact levels																					
	SG.IR-6	Incident Monitoring	Applies at all impact levels																					
	SG.IR-7	Incident Reporting	Applies at all impact levels																					
	SG.IR-10	Smart Grid Information System Backup	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
Smart Grid Information System Development and Maintenance (SG.MA)	SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	Applies at all impact levels																					
	SG.MA-2	Legacy Smart Grid Information System Updates	Applies at all impact levels																					
	SG.MA-3	Smart Grid Information System Maintenance	Applies at all impact levels with additional requirement enhancements at high impact levels																					
	SG.MA-4	Maintenance Tools	Applies at all impact levels																					
	SG.MA-5	Maintenance Personnel	Applies at all impact levels																					
	SG.MA-6	Remote Maintenance	Applies at all impact levels with additional requirement enhancements at high impact levels																					
Media Protection (SG.MP)	SG.MP-1	Media Protection Policy and Procedures	Applies at all impact levels																					
	SG.MP-3	Media Marking	Applies at moderate and high impact levels																					
	SG.MP-4	Media Storage	Applies at all impact levels																					
	SG.MP-5	Media Transport	Applies at all impact levels																					

セキュリティ要件グループ	セキュリティ要求事項	SG サイバーセキュリティ要件名	論理インタフェース分類における適用性																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Physical and Environmental Security (SG.PE)	SG.PE-8	Emergency Shutoff Protection	Applies at all impact levels																					
	SG.PE-9	Emergency Power	Applies at all impact levels with additional requirement enhancements at moderate and high																					
	SG.PE-10	Delivery and Removal	Applies at all impact levels																					
	SG.PE-11	Alternate Work Site	Applies at all impact levels																					
	SG.PE-12	Location of Smart Grid Information System Assets	Applies at all impact levels with additional requirement enhancements at high impact level																					
Planning (SG.PL)	SG.PL-1	Strategic Planning Policy and Procedures	Applies at all impact levels																					
	SG.PL-2	Smart Grid Information System Security Plan	Applies at all impact levels																					
	SG.PL-3	Rules of Behavior	Applies at all impact levels																					
	SG.PL-4	Privacy Impact Assessment	Applies at all impact levels																					
Security Program Management (SG.PM)	SG.PM-2	Security Program Plan	Applies at all impact levels																					
	SG.PM-3	Senior Management Authority	Applies at all impact levels																					
	SG.PM-4	Security Architecture	Applies at all impact levels																					
	SG.PM-5	Risk Management Strategy	Applies at all impact levels																					
	SG.PM-6	Security Authorization to Operate Process	Applies at all impact levels																					
	SG.PM-7	Mission/Business Process Definition	Applies at all impact levels																					
Personnel Security (SG.PS)	SG.PS-6	Access Agreements	Applies at all impact levels																					
	SG.PS-8	Personnel Accountability	Applies at all impact levels																					
	SG.PS-9	Personnel Roles	Applies at all impact levels																					
Risk Management and Assessment (SG.RA)	SG.RA-3	Security Impact Level	Applies at all impact levels																					
Smart Grid Information System and Services Acquisition (SG.SA)	SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	Applies at all impact levels																					
	SG.SA-2	Security Policies for Contractors and Third Parties	Applies at all impact levels																					
	SG.SA-3	Life-Cycle Support	Applies at all impact levels																					
	SG.SA-4	Acquisitions	Applies at all impact levels																					
	SG.SA-5	Smart Grid Information System Documentation	Applies at all impact levels																					
	SG.SA-6	Software License Usage Restrictions	Applies at all impact levels																					
	SG.SA-7	User-Installed Software	Applies at all impact levels																					
	SG.SA-8	Security Engineering Principles	Applies at all impact levels																					
	SG.SA-9	Developer Configuration Management	Applies at all impact levels																					
	SG.SA-10	Developer Security Testing	Applies at all impact levels																					
	SG.SA-11	Supply Chain Protection	Applies at all impact levels																					

セキュリティ要件グループ	セキュリティ要求事項	SG サイバーセキュリティ要件名	論理インタフェース分類における適用性																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Smart Grid Information System and Information Integrity (SG.SI)	SG.SI-1	System and Information Integrity Policy and Procedures	Applies at all impact levels																					
	SG.SI-5	Security Alerts and Advisories	Applies at all impact levels																					
	SG.SI-7	Software and Information Integrity	H	H	H	H	H	H	M	M	M	H		M	H	H	M	M	H					
	SG.SI-9	Error Handling	Applies at all impact levels																					
Smart Grid Information System and Communication Protection (SG.SC)	SG.SC-2	Communications Partitioning																						
	SG.SC-3	Security Function Isolation	H	H	H	H			M	M					H	H	M	M		H		H	H	H
	SG.SC-4	Information Remnants																						
	SG.SC-5	Denial-of-Service Protection	H	M	H	M	M	M			M	M		M		H	M				M			H
	SG.SC-6	Resource Priority					H									H								H
	SG.SC-8	Communication Integrity	H	H	H	H	H	H	M	M	M	H	M	M	H	H	M	M		H	H	H	H	H
	SG.SC-9	Communication Confidentiality													H	H		H						H
	SG.SC-10	Trusted Path																						
	SG.SC-11	Cryptographic Key Establishment and Management	Applies at all impact levels with additional requirement enhancements at high impact levels																					
	SG.SC-12	Use of Validated Cryptography	Applies at all impact levels																					
	SG.SC-13	Collaborative Computing	Applies at all impact levels																					
	SG.SC-14	Transmission of Security Parameters																						
	SG.SC-15	Public Key Infrastructure Certificates	Applies at all impact levels																					
	SG.SC-16	Mobile Code	Applies at moderate and high impact levels																					
	SG.SC-17	Voice-Over Internet Protocol																						
	SG.SC-20	Message Authenticity	Applies at all impact levels																					
	SG.SC-21	Secure Name/Address Resolution Service	Applies at all impact levels																					
	SG.SC-22	Fail in Known State	Applies at moderate and high impact levels																					
	SG.SC-23	Thin Nodes																						
	SG.SC-24	Honeypots																						
	SG.SC-25	Operating System-Independent Applications																						
	SG.SC-26	Confidentiality of Information at Rest							H	H					H	H		H						H
	SG.SC-27	Heterogeneity																						
	SG.SC-28	Virtualization Technique																						
	SG.SC-29	Application Partitioning	H	H	H	H	H	H				H			H	H			H	H	H	H	H	H
	SG.SC-30	Information System Partitioning	Applies at moderate and high impact levels																					

(出典) NISTIR 7628.