室管理等）かつ論理的（データやシステム等へのアクセス制御）に適切に制限していたことを確認している。 ※　特定重要設備の供給者を通じて確認している場合も含む。		
⑥　特定社会基盤事業者は、特定重要設備をインターネット回線と接続する場合には、特定重要設備に、不正なアクセス等を防ぐための機能を実装し、その利用マニュアル・ガイダンス等を自ら適切に整備・実施している。	□	
⑦　特定社会基盤事業者は、特定重要設備の供給者及び特定重要設備の導入に携わる者が、特定重要設備の設置等に際して不正な変更を加えることを防止する体制の下、設置等を行ったことを確認している。	□	
⑧－１　特定社会基盤事業者は、導入した特定重要設備に不正な変更やそのおそれがあることを発見した場合には、特定重要設備の供給者が詳細な調査や立入検査等に協力をすることが担保されていることを確認している。	□	
⑧－２　特定社会基盤事業者※は、導入した特定重要設備の構成設備に不正な変更やそのおそれがあることを発見した場合には、構成設備の供給者が、詳細な調査や立入検査等に協力をすることが担保されていることを確認している。 ※　特定重要設備の供給者を通じて確認している場合も含む。	□	
（２）特定重要設備又は構成設備について、将来的に保守・点検等が必要となることが見込まれる場合に、当該保守・点検等を行うことができる者が特定重要設備又は構成設備の供給者に限られるかどうか等の実態も踏まえ、供給者を選定している。		
⑨－１　特定社会基盤事業者は、特定重要設備の供給者によるサービス保証（故障対応や脆弱性対応等）が十分に講じられることを確認している。	□	
⑨－２　特定社会基盤事業者※は、構成設備の供給者によるサービス保証（故障対応や脆弱性対応等）が十分に講じられることを確認している。 ※　特定重要設備の供給者を通じて確認している場合も含む。	□	
⑩－１　特定社会基盤事業者は、特定重要設備のサービス保証（故障対応や脆弱性対応等）が受けられなくなった場合を想定して、代替手段の検討等の必要な対策を自ら講じている。	□	
⑩－２　特定社会基盤事業者※は、構成設備のサービス保証（故障対応や脆弱性対応等）が受けられなくなった場合を想定して、代替手段の検討等の必要な対策を自ら講じている。 ※　特定重要設備の供給者において検討している場合も含む。	□	
（３）特定重要設備及び構成設備について、不正な妨害が行われる兆候を把握可能な体制がとられており、不正な妨害が加えられた場合であっても、冗長性が確保されているなど、役務の提供に支障を及ぼさない構成となっている。		
⑪　特定社会基盤事業者は、ランサムウェアに感染した場合等の特定重要設備に対する不正な妨害が行われたときであっても役務の提供が継続できる体制（バックアップの取得・隔離管理、復旧手順の明確化・具体化、代替設備との交換等）について、自ら整備している。	□	
⑫　特定社会基盤事業者は、情報の漏洩等の情報セキュリティインシデントが発生した場合の対応方針・体制（マニュアル等の整備、定期的なインシデント対応の訓練等）を自ら整備している。	□	