（注）本資料は、ワーキングチームにおける論点及び検証結果を分かりやすく表現することを目的とし、できる限り平易な記載としています。

テロ対策　－サイバーテロへの対策－

ワーキングの詳細はこちらから

論点No.161

最近は政府機関や企業などがサイバー攻撃を受けることが増えているが、東海第二発電所ではサイバーテロ対策をしているのか。

第29回ワーキング（2024.11.25）で議論

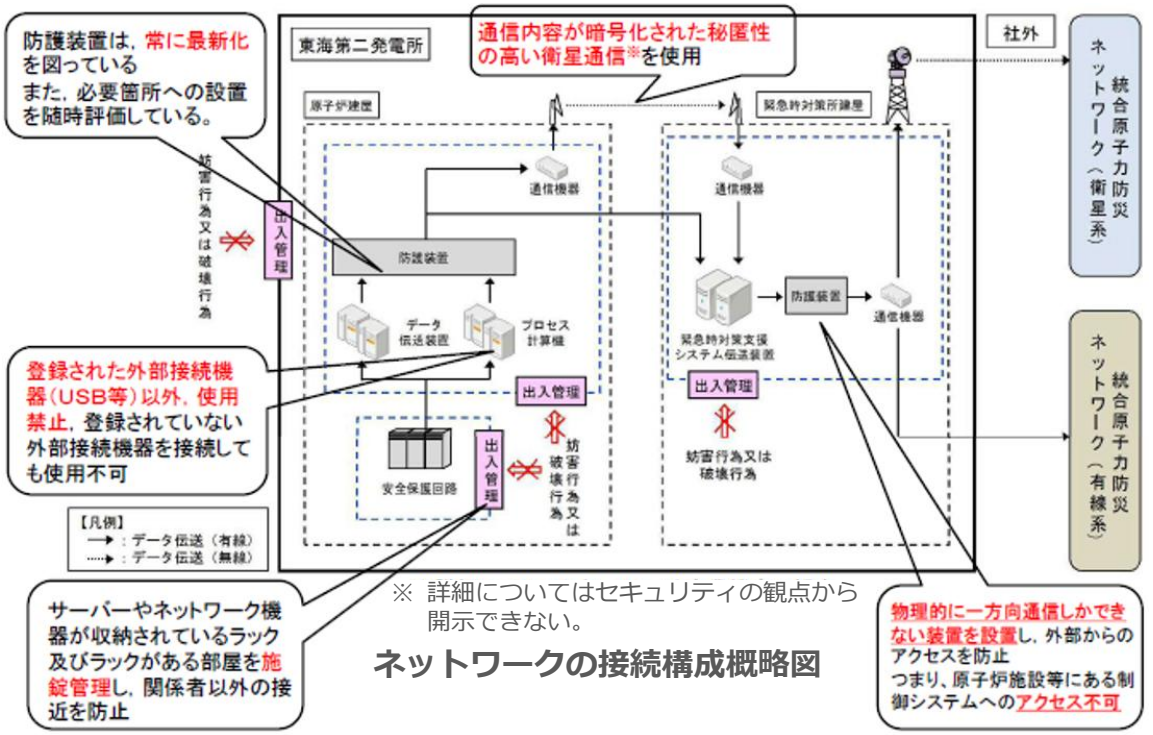
ワーキングチーム検証結果

原子炉の制御システムへ外部からアクセスができないよう、物理的に一方向通信しかできない装置を設置すること、サーバーセキュリティの防護装置は常に最新化するなどの対策を講じていることを確認。

ワーキングチーム検証結果（抜粋）

○不正アクセス行為（サイバーテロ含む）への対応

- 不正アクセス行為を防止するため、原子炉の制御システムや核燃料物質の防護のために必要な設備または操作に関する情報システムに対し、**外部からのアクセスを遮断**
- 外部接続機器（USBメモリ等）は、登録されたもの以外は使用不可とする措置を実施
- **防護装置は常に最新化**するとともに、随時対策を評価
- サーバーやネットワーク機器が収納されているラック及びラックがある部屋は施錠管理し、関係者以外の接近を防止
- **物理的に一方向通信しかできない装置を設置**し、外部からのアクセスを防止



ネットワークの接続構成概略図