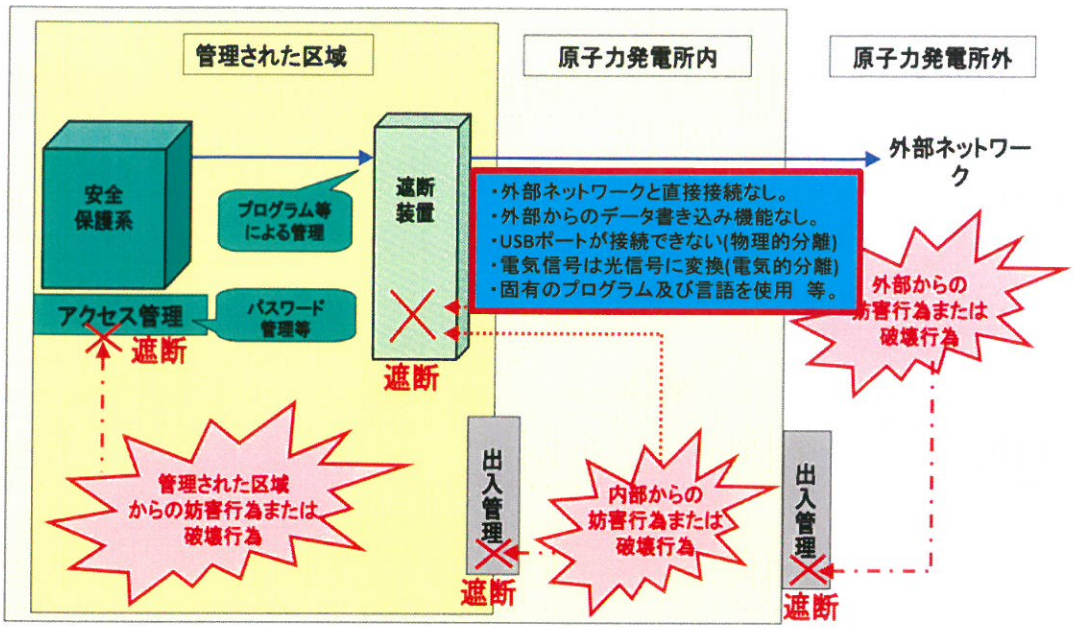
①原子力発電所のサイバー対策（新規制基準）

資料4

■『実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則』（設置許可基準規則）
第24条第1項第6号（安全保護回路）「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。」
■『実用発電用原子炉及びその附属施設の技術基準に関する規則』（技術基準規則）
第35条第1項 第5号（安全保護装置）「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。」



→ ： 許可されている情報の流れ（電気通信回線）

⇢ ： 許可されていない情報の流れ（電気通信回線）　　-·▶ ： 許可されていない人のアクセス

（出典）原子力規制委員会HP：関西電力株式会社「高浜1、2号炉 設置許可基準規則等への適合性について」https://www.nsr.go.jp/data/000130054.pdf
（出典）原子力規制委員会HP：四国電力株式会社「伊方発電所3号炉安全保護回路説明資料」https://www.nsr.go.jp/data/000038177.pdf
（出典）原子力規制委員会HP：中部電力株式会社「浜岡原子力発電所4号炉安全保護回路について」https://www.nsr.go.jp/data/000097590.pdf

②標準化・オープン化・IoT化、インダストリー4.0で制御システムのセキュリティが決定的に重要に！

●一般に産業用のシステムは、オフィスネットワーク等の情報系システムと、機器制御等を行う制御系システムに大別される。重要インフラサービスは、基本的に制御系システムによってコントロールされる。

●制御系システムは情報系システムに比べ、①外部との直接の接続が少なく、②事業者毎に固有の使用部分が多く、詳細な内部使用等を把握できない限り、外部からの攻撃が困難だった。

●しかし、標準技術・汎用製品の増加、外部ネットワークへの接続などにより、制御系システムでも、外部からのサイバー攻撃の可能性は増してきている。攻撃の脅威が存在することを前提とした対策が必要とされている。

（出典）技術研究組合制御システムセキュリティセンター「サイバーセキュリティ演習」http://www.css-center.or.jp/pdf/cybersecurity-exercises_outline.pdf
（出典）資源エネ庁「電力分野のサイバーセキュリティ対策について」http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/004_06_00.pdf

平成28年4月19日　参議院 総務委員会　民進党・新緑風会　石上俊雄