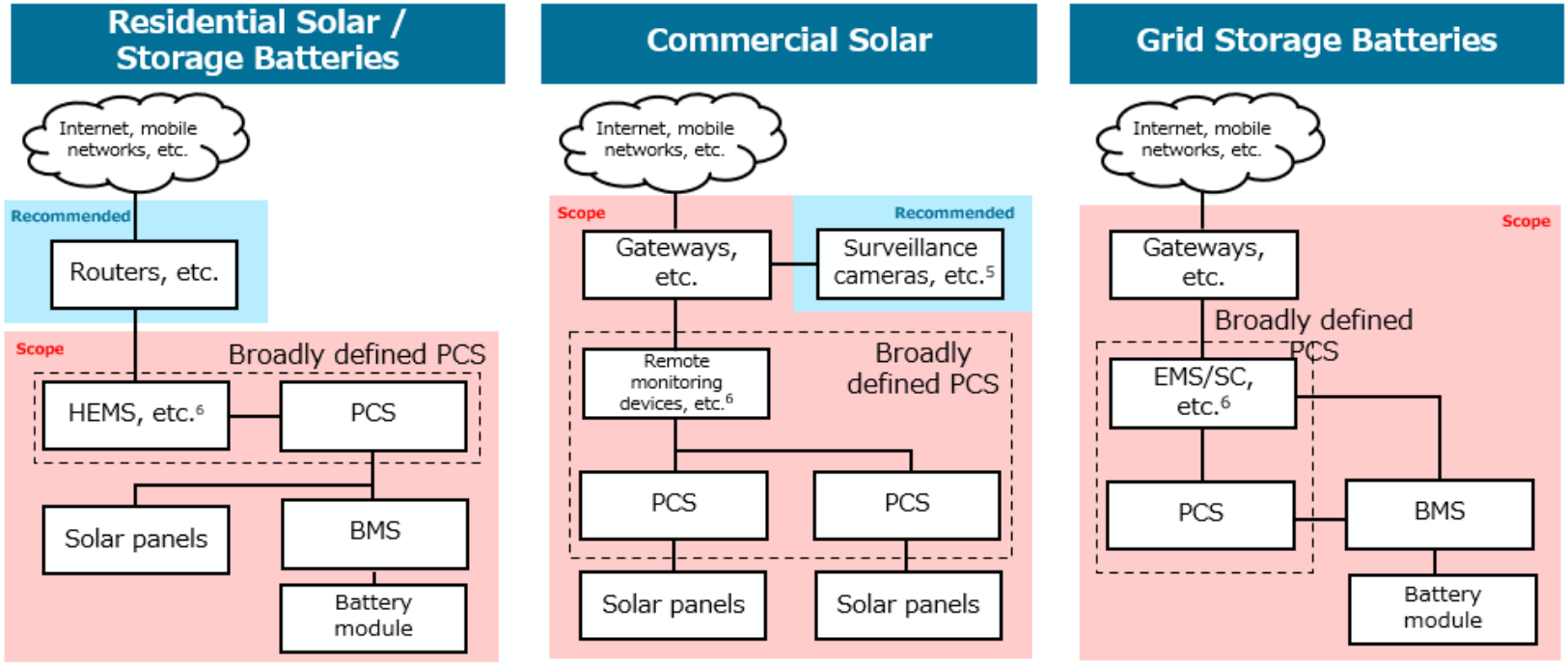
Cybersecurity Measures for Solar Power Generation and Storage Batteries

- **We are continuing to review the utilization of the JC-STAR scheme**, which was discussed at last year's SWG meeting.
- At the Grid Code Review Meeting held in December, it was decided that **solar power generation systems and battery storage systems newly connected to the grid on or after April 2027[1]** shall be required, **under the Grid Interconnection Technical Requirements,[2] to utilize control systems (such as PCSs and EMSs) equipped with communication functions that have been granted the conformance label JC-STAR★1.[3]**

1. For products interconnected at low voltage (below 50 kW), a transitional period of approximately six months has been established in consideration of existing distribution inventory,and the requirement will take effect in October 2027.
2. Technical requirements for grid interconnection established by each general transmission and distribution utility based on the Guidelines for Transmission and Distribution Operations established by the Organization for Cross-regional Coordination of Transmission Operators (OCCTO).
3. Among the components within the scope shown in the diagram below,[4] devices (systems) using IP communications will become subject to the requirement to acquire the conformance label JC-STAR★1. From the perspective of cybersecurity measures, the use of products granted the conformance label JC-STAR is also recommended for IP communication devices that fall outside the defined scope.



4. This is an example system configuration. Control systems equipped with communication functions adopted by distributed energy resources fall within the scope in other cases as well.
5. Even for equipment outside the defined scope, if the equipment has control functions affecting power-generation facilities, or if it connects directly to key system components without passing through a gateway, it will also be subject to the requirement to acquire the conformance label of JC-STAR.
6. If output control functions are included.

Future Considerations and Issues

- **Under the Grid Interconnection Technical Requirements, the use of products granted the conformance label of JC-STAR★1 will become mandatory for solar power generation and battery storage systems.** As a result, **control systems such as PCSs will be required to implement fundamental cybersecurity measures that are expected of general IoT devices.**

- Going forward, **the requirements for solar power generation and battery storage** must also apply to systems connected at low voltage (below 50 kW). **This will be announced in collaboration with relevant industry organizations.** In addition, for technologies such as **wind power and fuel cells, the government and the private sector will coordinate on determining the applicable scope and the timeline for mandating the use of products granted the conformance label of JC-STAR★1.**

- However, **JC-STAR★1 does not cover all cybersecurity measures required to address threats expected in solar power systems, battery storage systems, and similar equipment.** Certain power-related devices possess characteristics not found in general IoT products, and some of these devices cannot be fully addressed by the JC-STAR★1 criteria alone. As the power sector constitutes critical infrastructure, addressing supply-chain risks is also essential to ensuring a stable power supply. Accordingly, additional cybersecurity measures will also be required for these specific devices.

- In order to develop cybersecurity measures that **appropriately reflect the unique threats and characteristics of the power sector, as well as the functional requirements of control systems such as PCSs**, further discussion and measures—**such as the development and introduction of higher-level standards（JC-STAR★2 and above）that provide conformity requirements tailored to specific IoT product categories**— is necessary on the following points:
  - ○ The particularly high cybersecurity risks that equipment and electronic devices present within the power sector
  - ○ The potential threats and cyberattack methods that may be anticipated for such equipment and electronic devices
  - ○ Security requirements for electronic devices to address the anticipated threats and cyberattack methods
  - ○ Cybersecurity measures required not only for the devices themselves but also for system installers and operators