System Defense Technologies That Enables Safe Continuation of Operation Even in the Event That an Abnormality Has Been Detected

Protecting the entire control system from high-precision attacks that are difficult to detect, in order to continue safe operation

Characteristics
(1) Quickly specifies locations where abnormalities have occurred in a control system
Commands and instructions issued to control systems are hierarchically monitored in three layers: at a monitoring device (host), at a communication device (intermediate), and at a controller (subordinate). This uses an inspection function that makes use of the characteristics of devices at each layer, including monitoring of the host level which does not exist in current technologies, in order to quickly specify and protect locations to which attacks are made in the control system (hierarchical inspection function).

(2) Continues safe operation even when an abnormality has occurred
The communication and processing of a device against which an attack has been detected is restricted by the coordination device within the scope that allows for operation to continue. This protects controllers from suspension and malfunction due to attacks, while continuing operation (coordination function).

Necessity to Prepare for High-Precision Attacks That Are Difficult to Detect

Risk that targets controllers
High-precision cyberattacks can launch an attack that can not be blocked with a single defense condition.

Control system

Protects the Entire Control System from High-Precision Attacks

Control network

Operation center of critical infrastructure system

Securing monitoring defense function

Controller

Monitoring device

Communication device

Coordination device

Plant

Defence far from local site

In order to safely operate the entire plant, it is possible to contain attacks as much as possible at the host level.

Protects all layers, from top to bottom

Hierarchical defense in which a defense web is established in multiple stages prevents the evasion of each high-precision attacks.

Tackling Social Implementation for the Actualization of the TOP Plan

Risks that target controllers
Cyberattacks targeted at devices functions that maintain the safety of plants can cause major accidents.

Implementation Status
Development of an experimental model for hierarchical protection has already begun. The elements of this research are built while referring to the opinions of persons engaged in the actual operation. At the same time, investigations are making progress in regards to supporting the demonstration of communication devices having a whitelist function to providers of critical infrastructure and the introduction of whitelist functions for next-generation environments.

Schedule
By FY2020, there is a plan to introduce current products and research technology to be applied to power companies, in two steps.

From 2020 as well, the aim is to expand locations where these technologies are applied and for earnest expansion, through the implementation of introduction strategies that take into account system life cycles.

Developing core technology based on the TOP plan
Initially, the aim is to perform R&D in collaboration with providers of critical infrastructure, in order to produce technical evaluations and introduction/operation procedures as results.